SIEMENS

SIMATIC NET

Industrial Ethernet Switches SCALANCE XB-200/XC-200/ XF-200BA/XP-200/XR-300WG Web Based Management

Projektierungshandbuch

Einleitung 1

Beschreibung 2

Vergabe einer IP-Adresse 3

Technische Grundlagen 4

Konfigurieren mit dem Web Based Management 5

Troubleshooting/FAQ 6

Anhang A

12/2018
C79000-G8900-C360-08

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

⚠ GEFAHR
bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠ WARNUNG
bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠ VORSICHT
bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG
bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

⚠ WARNUNG
Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

C79000-G8900-C360-08
℗ 11/2018 Änderungen vorbehalten

Inhaltsverzeichnis

1 Einleitung 9

1.1 Security-Empfehlungen 13

2 Beschreibung 15

2.1 Systemfunktionen und Hardware-Ausstattung 15

2.2 Produkteigenschaften 18

2.3 Voraussetzungen für Installation und Betrieb 19

2.4 Protokolle 20

3 Vergabe einer IP-Adresse 23

3.1 Aufbau einer IP-Adresse 23

3.2 Erstmalige Vergabe einer IP-Adresse 24

3.3 Adressvergabe über DHCP 26

4 Technische Grundlagen 27

4.1 Mengengerüst 27

4.2 PROFINET 29

4.3 EtherNet/IP 30

4.4 Redundanzverfahren 31
4.4.1 Spanning Tree 31
4.4.1.1 RSTP, MSTP, CIST 32
4.4.2 RSTP+ 33
4.4.2.1 Eigenschaften und Funktion von RSTP+ 33
4.4.2.2 Topologie für RSTP+ 33
4.4.2.3 RSTP+ konfigurieren 36
4.4.2.4 Spanning Tree für RSTP+ konfigurieren 37
4.4.2.5 Ringredundanz für RSTP+ konfigurieren 38
4.4.2.6 RSTP+ einschalten und Leitungen stecken 39
4.4.3 HRP 39
4.4.4 MRP 40
4.4.4.1 MRP - Media Redundancy Protocol 40
4.4.4.2 Projektierung im WBM 43
4.4.4.3 Projektierung in STEP 7 44
4.4.5 Standby 49
4.4.6 Parallel Redundancy Protocol 51
4.4.7 DLR 52

4.5 VLAN 54
4.5.1 Grundlagen 54
4.5.2 VLAN-Tagging 54
4.5.3 Private VLAN 56
4.5.4 VLAN-Tunnel 58

4.6 Mirroring....59
4.7 SNMP....60
4.8 Quality of Service....61
4.9 NAT/NAPT....62
4.10 Single-Hop Inter-VLAN-Routing....65
5 Konfigurieren mit dem Web Based Management....67
5.1 Web Based Management....67
5.2 Login....68
5.3 Das Menü "Information"....71
5.3.1 Startseite....71
5.3.2 Versionen....77
5.3.3 I&M....78
5.3.4 ARP-Tabelle....80
5.3.5 Log-Tabelle....80
5.3.6 Fehler....82
5.3.7 Redundanz....84
5.3.7.1 Spanning Tree....84
5.3.7.2 Ringredundanz....87
5.3.7.3 Standby....89
5.3.7.4 Link Check....91
5.3.8 Ethernet-Statistiken....93
5.3.8.1 Schnittstellenstatistik....93
5.3.8.2 Telegrammlänge....94
5.3.8.3 Telegrammtyp....95
5.3.8.4 Telegrammfehler....96
5.3.8.5 History....98
5.3.9 Unicast....99
5.3.10 Multicast....101
5.3.11 LLDP....102
5.3.12 Fiber Monitoring Protocol....104
5.3.13 Routing....106
5.3.13.1 Routing-Tabelle....106
5.3.13.2 NAT-Übersetzungen....107
5.3.14 DHCP-Server....107
5.3.15 Diagnose....108
5.3.16 SNMP....110
5.3.17 Security....111
5.3.17.1 Übersicht....111
5.3.17.2 Unterstützte Funktionsrechte....114
5.3.17.3 Rollen....114
5.3.17.4 Gruppen....115
5.4 Das Menü "System"....116
5.4.1 Konfiguration....116
5.4.2 Allgemein....120
5.4.2.1 Gerät....120
5.4.2.2 Koordinaten....121
5.4.3 Agent-IP....122

5.4.4 Neustart....124
5.4.5 Laden & Speichern....127
5.4.5.1 HTTP....128
5.4.5.2 TFTP....132
5.4.5.3 SFTP....136
5.4.5.4 Passwörter....140
5.4.6 Ereignisse....141
5.4.6.1 Konfiguration....141
5.4.6.2 Severity-Filter....145
5.4.7 SMTP-Client....146
5.4.8 DHCP....148
5.4.8.1 DHCP-Client....148
5.4.8.2 DHCP-Server....150
5.4.8.3 Zuordnung Port zu IP-Adresse....155
5.4.8.4 Port-Bereich....157
5.4.8.5 DHCP-Optionen....158
5.4.8.6 Relay Agent-Information....161
5.4.8.7 Statische Zuordnung....162
5.4.9 SNMP....164
5.4.9.1 Allgemein....164
5.4.9.2 Traps....166
5.4.9.3 v3-Gruppen....168
5.4.9.4 v3-Benutzer....170
5.4.10 Systemzeit....172
5.4.10.1 Manuelle Einstellung....173
5.4.10.2 DST-Übersicht....174
5.4.10.3 DST-Konfiguration....176
5.4.10.4 SNTP-Client....179
5.4.10.5 NTP-Client....182
5.4.10.6 SIMATIC Time Client....185
5.4.11 Automatische Abmeldung....187
5.4.12 Konfiguration des SELECT/SET-Tasters....187
5.4.13 Syslog-Client....188
5.4.14 Ports....190
5.4.14.1 Übersicht....190
5.4.14.2 Konfiguration....193
5.4.15 Fehlerkontrolle....199
5.4.15.1 Spannungsversorgung....199
5.4.15.2 Link Change....200
5.4.15.3 Redundanz....202
5.4.16 PROFINET....203
5.4.17 EtherNet/IP....204
5.4.18 PLUG....205
5.4.18.1 Konfiguration....205
5.4.19 Ping....209
5.4.20 DCP Discovery....210
5.4.21 Power over Ethernet (PoE)....212
5.4.21.1 Allgemein....212
5.4.21.2 Port....213
5.4.22 Port-Diagnose....216
5.4.22.1 Kabel-Tester....216
5.4.22.2 SFP-Diagnose....217

5.5 Das Menü "Layer 2"....220
5.5.1 Konfiguration....220
5.5.2 Quality of Service (QoS)....224
5.5.2.1 Allgemein....224
5.5.2.2 CoS-Zuordnung....226
5.5.2.3 DSCP-Zuordnung....227
5.5.2.4 QoS-Priorisierung....229
5.5.2.5 CoS Port-Neuzuordnung....231
5.5.3 Lastkontrolle....232
5.5.4 VLAN....234
5.5.4.1 Allgemein....234
5.5.4.2 GVRP....239
5.5.4.3 Port-basiertes VLAN....240
5.5.5 Private VLAN....243
5.5.5.1 Allgemein....243
5.5.5.2 IP-Schnittstellen-Zuordnung....244
5.5.6 Provider Bridge....246
5.5.6.1 Tunnel-Ports....246
5.5.7 Mirroring....248
5.5.7.1 Allgemein....248
5.5.7.2 Port....251
5.5.8 Dynamic MAC Aging....252
5.5.9 Ringredundanz....253
5.5.9.1 Ring....253
5.5.9.2 Standby....257
5.5.9.3 Link Check....260
5.5.10 Spanning Tree....263
5.5.10.1 Allgemein....263
5.5.10.2 CIST Allgemein....265
5.5.10.3 CIST-Port....267
5.5.10.4 MST Allgemein....272
5.5.10.5 MST-Port....273
5.5.10.6 Enhanced Passive Listening Compatibility....276
5.5.11 Loop Detection....276
5.5.12 Link Aggregation....279
5.5.12.1 Allgemein....279
5.5.12.2 LACP Timeout....282
5.5.13 DCP-Weiterleitung....283
5.5.14 LLDP....285
5.5.15 Fiber Monitoring Protocol....286
5.5.16 Unicast....288
5.5.16.1 Filtering....288
5.5.16.2 Gesperrte Ports....291
5.5.16.3 Learning....293
5.5.16.4 Blocking....294
5.5.17 Multicast....296
5.5.17.1 Gruppen....296
5.5.17.2 IGMP....299
5.5.17.3 GMRP....300
5.5.17.4 Multicast Blocking....303
5.5.18 Broadcast....304
5.5.19 RMON....306

5.5.19.1 Statistik....306
5.5.19.2 History....308

5.6 Das Menü "Layer 3"....310
5.6.1 Subnetze....310
5.6.1.1 Übersicht....310
5.6.1.2 Konfiguration....313
5.6.1.3 Default-Gateway....314
5.6.2 DHCP Relay Agent....315
5.6.2.1 Allgemein....315
5.6.2.2 Option....316
5.6.3 NAT....320
5.6.3.1 NAT....320
5.6.3.2 Statisch....322
5.6.3.3 Pool....323
5.6.3.4 NAPT....325

5.7 Das Menü "Security"....327
5.7.1 Benutzerverwaltung....327
5.7.2 Benutzer....329
5.7.2.1 Lokale Benutzer....329
5.7.2.2 Rollen....332
5.7.2.3 Gruppen....334
5.7.3 Passwörter....335
5.7.3.1 Passwörter....335
5.7.3.2 Optionen....337
5.7.4 AAA....338
5.7.4.1 Allgemein....338
5.7.4.2 RADIUS-Client....339
5.7.4.3 802.1X Authenticator....342
5.7.5 Management ACL....346

6 Troubleshooting/FAQ....351

6.1 Laden einer neuen Firmware über TFTP ohne WBM und CLI....351

6.2 Meldung: SINEMA-Konfiguration noch nicht akzeptiert....352

6.3 Austausch von Konfigurationsdaten mit STEP7 Basic/Professional über eine Datei....353

A Anhang A....355

A.1 Parameter in Syslog-Meldungen....355

A.2 Syslog-Meldungen....357

Index....363

Einleitung

1

Gültigkeitsbereich dieses Projektierungshandbuchs

Dieses Projektierungshandbuch behandelt folgende Produkte:

- SCALANCE XB-200
- SCALANCE XC-200
- SCALANCE XF-200BA
- SCALANCE XP-200
- SCALANCE XR-300WG

Nachfolgend werden die Produkte auch als IE-Switch, Gerät oder Netzwerkkomponente bezeichnet.

Von einigen Geräten gibt es zwei Varianten mit unterschiedlichen Artikelnummern. Die beiden Varianten unterscheiden sich nur in ihren Werkseinstellungen. Alle anderen Eigenschaften sind identisch.

Das Projektierungshandbuch gilt für folgende Software-Versionen:

- SCALANCE XB-200 Firmware ab Version 4.1
- SCALANCE XC-200 Firmware ab Version 4.1
- SCALANCE XF-200BA Firmware ab Version 4.1
- SCALANCE XP-200 Firmware ab Version 4.1
- SCALANCE XR-300WG Firmware ab Version 4.1

Werkseinstellungen

PROFINET-Varianten

- Industrial-Ethernet-Protokoll: PROFINET
- Base Bridge-Modus: 802.1D Transparent Bridge
- Redundanzverfahren: Ringredundanz
- Priorisierungsmodus: Priorisierung nach COS
- IGMP Snooping/IGMP Querier: Aus
- Erkennung von IPv4-Adresskollisionen: Never give up

EtherNet/IP-Varianten

- Industrial-Ethernet-Protokoll: EtherNet/IP
- Base Bridge-Modus: 802.1Q VLAN Bridge
- Redundanzverfahren: RSTP

- Priorisierungsmodus: Priorisierung nach COS-DSCP
- IGMP Snooping/IGMP Querier: An
- Erkennung von IPv4-Adresskollisionen: Attempt to defend

Industrial Ethernet-Profil

- Industrial-Ethernet-Protokoll: PROFINET
- Base Bridge-Modus: 802.1Q VLAN Bridge
- Redundanzverfahren: RSTP
- Priorisierungsmodus: Priorisierung nach COS-DSCP
- IGMP Snooping/IGMP Querier: Aus
- Erkennung von IPv4-Adresskollisionen: Never give up

Verwendete Bezeichnungen

Einteilung	Beschreibung	Verwendete Begriffe
Produktgruppe	Gilt eine Information für alle Geräte und Varianten einer Produktgruppe, wird die Produktgruppe genannt.	z. B. SCALANCE XC-200
Gerät	Gilt eine Information für ein spezifisches Gerät, wird der Gerätename verwendet.	z. B. SCALANCE XC206-2SFP
Gerätegruppe	Gilt eine Information für ein spezifische Gruppe der Geräte, wird eine entsprechende Abkürzung verwendet.	-
	Gilt eine Information für alle Gigabit-Varianten von SCALANCE XC-200, wird der folgende Begriff verwendet.	SCALANCE XC-200G

Zweck dieses Projektierungshandbuchs

Dieses Projektierungshandbuch soll Sie in die Lage versetzen, IE-Switches in Betrieb zu nehmen und zu bedienen. Es vermittelt die notwendigen Kenntnisse für die Konfiguration der IE-Switches.

Einordnung in die Dokumentationslandschaft

Zu den Produkten gibt es außer dem Projektierungshandbuch, das Sie gerade lesen, noch folgende Dokumentationen:

- Projektierungshandbuch "SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG Command Line Interface"
  Dieses Dokument enthält die CLI-Befehle, die von den IE-Switches unterstützt werden.
- Betriebsanleitung "SCALANCE XB-200", "SCALANCE XC-200", "SCALANCE XF-200BA", "SCALANCE XP-200" und "SCALANCE XR-300WG"
  Diese Dokumente enthalten Informationen zum Montieren, Anschließen und zu Zulassungen der Produkte.

Sie finden die Dokumentationen hier:

- Auf dem Datenträger, der manchen Produkten beiliegt:
  - Produkt-CD / Produkt-DVD
  - SIMATIC NET Manual Collection
- Auf den Internetseiten des Siemens Industry Online Support unter:
  - SCALANCE XB-200 (https://support.industry.siemens.com/cs/ww/de/ps/15291/man)
  - SCALANCE XC-200 (https://support.industry.siemens.com/cs/ww/de/ps/24185/man)
  - SCALANCE XF-200BA (https://support.industry.siemens.com/cs/ww/de/ps/15287/man)
  - SCALANCE XP-200 (https://support.industry.siemens.com/cs/ww/de/ps/21869/man)
  - SCALANCE XR-300WG (https://support.industry.siemens.com/cs/ww/de/ps/15296/man)

Weiterführende Dokumentation

In den Systemhandbüchern "Industrial Ethernet / PROFINET Industrial Ethernet" und "Industrial Ethernet / PROFINET Passive Netzkomponenten" erhalten Sie Hinweise zu weiteren SIMATIC NET-Produkten, die Sie gemeinsam mit den Geräten dieser Produktlinie in einem Industrial Ethernet-Netzwerk betreiben können.

Sie finden dort u. a. optische Leistungsdaten der Kommunikationspartner, die Sie für den Aufbau benötigen.

Sie finden die Systemhandbücher hier:

- Auf dem Datenträger, der manchen Produkten beiliegt:
  - Produkt-CD / Produkt-DVD
  - SIMATIC NET Manual Collection
- Auf den Internet-Seiten des Siemens Industry Online Support:
  - Industrial Ethernet / PROFINET Industrial Ethernet Systemhandbuch (https://support.industry.siemens.com/cs/ww/de/view/27069465)
  - Industrial Ethernet / PROFINET Passive Netzkomponenten Systemhandbuch (https://support.industry.siemens.com/cs/ww/de/view/84922825)

SIMATIC NET-Handbücher

Sie finden die SIMATIC NET-Handbücher hier:

- Auf dem Datenträger, der manchen Produkten beiliegt:
  - Produkt-CD / Produkt-DVD
  - SIMATIC NET Manual Collection
- Auf den Internetseiten des Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/de/ps/15247).

SIMATIC NET-Glossar

Erklärungen zu vielen Fachbegriffen, die in dieser Dokumentation vorkommen, sind im SIMATIC NET-Glossar enthalten.

Sie finden das SIMATIC NET-Glossar im Internet unter folgender Adresse:

50305045 (https://support.industry.siemens.com/cs/ww/de/view/50305045)

Security-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z. B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter folgender Adresse:
https://www.siemens.com/industrialsecurity (https://www.siemens.com/industrialsecurity)

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Aktualisierungen durchzuführen, sobald die entsprechenden Updates zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter folgender Adresse:
https://www.siemens.com/industrialsecurity (https://www.siemens.com/industrialsecurity)

Lizenzbedingungen

Hinweis

Open Source Software

Lesen Sie die Lizenzbedingungen zur Open Source Software genau durch, bevor Sie das Produkt nutzen.

Sie können die Lizenzbedingungen im WBM auf der Seite "System > Laden & Speichern > Copyright" herunterladen.

Marken

Folgende und eventuell weitere nicht mit dem Schutzrechtsvermerk ® gekennzeichnete Bezeichnungen sind eingetragene Marken der Siemens AG:

SIMATIC NET, SCALANCE, C-PLUG, OLM

Firmware

Die Firmware ist signiert und verschlüsselt. Es ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.

1.1 Security-Empfehlungen

Software (Security-Funktionen)

- Halten Sie die Firmware aktuell. Informieren Sie sich regelmäßig über Sicherheitsupdates für das Gerät. Informationen hierzu finden Sie auf den Internetseiten Industrial Security (https://www.siemens.com/industrialsecurity).
- Informieren Sie sich regelmäßig über Security-Empfehlungen, die vom Siemens ProductCERT (https://www.siemens.com/cert/de/cert-security-advisories.htm) veröffentlicht werden.
- Aktivieren Sie nur Protokolle, die Sie für den Einsatz des Geräts benötigen.
- Beschränken Sie den Zugriff auf das Management des Geräts durch Regeln in einer Zugriffsliste (Management ACL - Access Control List).
- Die Möglichkeit der VLAN-Strukturierung bietet Schutz gegen DoS-Attacken und nicht autorisierte Zugriffe. Prüfen Sie, ob dies in Ihrem Umfeld sinnvoll ist.
- Nutzen Sie einen zentralen Logging-Server, um Änderungen und Zugriffe zu protokollieren. Betreiben Sie Ihren Logging-Server innerhalb des geschützten Netzwerkbereichs und prüfen Sie regelmäßig die Logging-Informationen.

Passwörter

- Definieren Sie Regeln für die Vergabe von Passwörtern.
- Ändern Sie regelmäßig Ihre Passwörter, um die Sicherheit zu erhöhen.
- Verwenden Sie Passwörter mit hoher Passwortstärke.
- Stellen Sie sicher, dass alle Passwörter geschützt und unzugänglich für unbefugte Personen sind.
- Verwenden Sie dasselbe Passwort nicht für verschiedene Benutzer und Systeme.

Zertifikate und Schlüssel

- Im Gerät ist ein voreingestelltes SSL-Zertifikat mit Schlüssel vorhanden. Ersetzen Sie dieses Zertifikat durch ein selbst erstelltes Zertifikat mit Schlüssel. Es wird empfohlen, ein Zertifikat zu verwenden, das entweder durch eine zuverlässige externe oder interne Zertifizierungsstelle signiert ist.
- Nutzen Sie eine Zertifizierungsstelle inklusive Schlüsselwiderruf und -verwaltung, um Zertifikate zu signieren.

- Stellen Sie sicher, dass benutzerdefinierte private Schlüssel geschützt und unzugänglich für unbefugte Personen sind.
- Es wird empfohlen, passwortgeschützte Zertifikate im PKCS #12-Format zu verwenden.
- Verifizieren Sie Zertifikate und Fingerprints auf Server- und Clientseite, um "Man-in-the-middle"-Angriffe zu verhindern.
- Es wird empfohlen, Zertifikate mit einer Schlüssellänge von mindestens 2048 Bit zu verwenden.
- Ändern Sie Zertifikate und Schlüssel umgehend, wenn der Verdacht auf Kompromittierung besteht.

Beschreibung

2

2.1 Systemfunktionen und Hardware-Ausstattung

Verfügbarkeit der Systemfunktionen

Die nachfolgende Tabelle zeigt die Verfügbarkeit der Systemfunktionen auf den IE-Switches. Beachten Sie, dass in diesem Projektierungshandbuch und der Online-Hilfe alle Funktionen beschrieben sind. Abhängig von Ihrem IE-Switch stehen Ihnen manche Funktionen nicht zur Verfügung.

Technische Änderungen sind vorbehalten.

		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XP-200	SCALANCE XF-200BA
Informationen	ARP-Tabelle	✓	✓	✓	✓	✓
	Log-Tabelle	✓	✓	✓	✓	✓
	Ethernet-Statistiken	✓	✓	✓	✓	✓
	Diagnose (Temperatur)	-	✓	✓	✓	✓
System	SMTP-Client	✓	✓	✓	✓	✓
	DHCP-Client	✓	✓	✓	✓	✓
	DHCP-Server	✓ 1)	✓ 1)	✓	✓	✓
	SNMP	✓	✓	✓	✓	✓
	Manuelle Zeiteinstellung	✓	✓	✓	✓	✓
	DST	-	-	✓	✓	✓
	SNTP	✓	✓	✓	✓	✓
	NTP	✓	✓	✓	✓	✓
	SIMATIC Time Client	✓	✓	✓	✓	✓
	Auto-Logout	✓	✓	✓	✓	✓
	Syslog-Client	✓	✓	✓	✓	✓
	Fehlerkontrolle	✓	✓	✓	✓	✓
	PROFINET	✓	✓	✓	✓	✓
	EtherNet/IP	✓	✓	✓	✓	✓ 2)
	DLR-Kompatibilität	✓	✓	✓	✓	✓ 2)
	Kabeltester	✓	✓	✓	✓	✓
	SFP-Diagnose	-	✓	✓	-	-
	Fiber Monitoring	-	-	✓	-	-

		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XP-200	SCALANCE XF-200BA
Layer 2	Sendeprioritäten	-	-	✓	✓	✓
	CoS-Zuordnung	✓	✓	✓	✓	✓
	DSCP-Zuordnung	✓	✓	✓	✓	✓
	QoS-Priorisierung	✓	✓	✓	✓	✓
	CoS Port-Neuzuordnung	-	-	✓	✓	✓
	Lastkontrolle	✓	✓	✓	✓	✓
	GVRP	-	-	✓	✓	✓
	Port-basiertes VLAN	✓	✓	✓	✓	✓ 2)
	Private VLAN	-	-	✓	✓	-
	Provider Bridge	-	-	✓	✓	✓
	Switch-Port VLAN Trunk	-	-	✓	✓	✓ 2)
	Port-basiertes Mirroring	✓	✓	✓	✓	✓
	Dynamic MAC Aging	✓	✓	✓	✓	✓
	Ringredundanz	✓	✓	✓	✓	✓
	H-Sync-Unterstützung	-	-	✓	✓	✓
	S2-Geräte	-	-	✓	✓	✓
	CiR/H-CiR-Unterstützung	-	-	✓	✓	✓
	Ring mit RSTP	-	-	✓	✓	✓
	Standby (HRP)	✓	✓	✓	✓	✓
	Observer (HRP)	-	-	✓	✓	✓
	Link Check	✓	✓	✓	-	✓
	Spanning Tree	✓	✓	✓	✓	✓
	RSTP	✓	✓	✓	✓	✓
	RSTP+	✓	✓	✓	✓	✓
	MSTP	-	-	✓	✓	-
	Enhanced Passive Listening Compatibility	✓	✓	✓	✓	✓
	Loop Detection	✓	✓	✓	✓	✓
	Link Aggregation	-	-	✓	✓	✓
	DCP-Weiterleitung	✓	✓	✓	✓	✓
	LLDP	✓	✓	✓	✓	✓
	Unicast-Filter	✓	✓	✓	✓	✓
	Locked Ports	✓	✓	✓	✓	✓
	Unicast-Learning	✓	✓	✓	✓	✓
	Unicast-Blocking	✓	✓	✓	✓	✓
	Multicast-Gruppen	✓	✓	✓	✓	✓
	IGMP	✓	✓	✓	✓	✓
	GMRP	-	-	✓	✓	✓
	Multicast-Blocking	✓	✓	✓	✓	✓
	Broadcast-Blocking	✓	✓	✓	✓	✓
	RMON	✓	✓	✓	✓	✓

		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XP-200	SCALANCE XF-200BA
	RMON-History	✓	✓	✓	✓	✓
Layer 3	Single-Hop Inter-VLAN-Routing	-	-	✓	✓	-
	DHCP Relay Agent	✓	✓	✓	✓	✓
	Gemeinsame Agent-Adresse	-	-	✓	✓	-
	NAT/NAPT	-	-	✓	✓	-
Security	Benutzer	✓	✓	✓	✓	✓
	Passwörter	✓	✓	✓	✓	✓
	RADIUS-Authentifizierung	✓	✓	✓	✓	✓
	MAC-Authentifizierung	-	-	✓	✓	✓
	Guest VLAN	-	-	✓	✓	✓
	802.1X Reauthentifizierung	✓	✓	✓	✓	✓
	Management ACL	✓	✓	✓	✓	✓

1) Eingeschränkt

2) Nicht bei DNA-Geräten

Verfügbarkeit der Hardware-Ausstattung

Die nachfolgende Tabelle zeigt die Hardware-Ausstattung der IE-Switches.

Technische Änderungen sind vorbehalten.

	SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XP-200	SCALANCE XF-200BA
C-PLUG-Unterstützung	-	-	✓	✓	✓
SELECT/SET-Taster	-	-	✓ 2) 3)	✓ 3)	-
RESET-Taster	✓ 2)	✓ 2)	-	✓ 2)	-
SET-Taster	-	-	-	-	✓ 2)
Meldekontakt	-	-	✓	✓	✓
Serielle Schnittstelle	✓	✓	✓	✓	-
Anzeigemodi	-	-	✓	✓	-
Stecktransceiver-Steckplätze	-	-	✓	-	-
Combo Ports	-	✓	-	-	-
BusAdapter-Steckplätze	-	-	-	-	✓
Power over Ethernet	-	-	-	✓ 1)	-

1) Kennzeichnung "PoE" im Gerätenamen

Funktion der Taster:

2) Auf Werkseinstellungen zurücksetzen

3) Meldemaske aktivieren

2.2 Produkteigenschaften

Die IE-Switches verfügen über folgende Eigenschaften:

- Die Ethernet-Schnittstellen unterstützen folgende Betriebsarten und Modi:
  - 10 MBit/s und 100 MBit/s jeweils Voll- und Halb-Duplex
  - 1000 MBit/s Voll-Duplex (SCALANCE XC206-2SFP mit den entsprechenden Stecktransceivern, SCALANCE XC-200G, SCALANCE XP216 und SCALANCE XR-300WG)
  - Autonegotiation
  - Auto-Crossing
  - Auto-Polarity
- EtherNet/IP
  EtherNet/IP (Ethernet/Industrial Protocol) ist ein offener Industriestandard für industrielles Echtzeit-Ethernet, basierend auf TCP/IP und UDP/IP.
- PROFINET
  PROFINET (Process Field Network) ist ein offener Industriestandard für industrielles Echtzeit-Ethernet, basierend auf TCP/IP und IT-Standards. Über PROFINET können dezentrale Peripheriegeräte an eine Steuerung (Controller) angebunden werden.
- Redundanzverfahren Spanning Tree Protocol
  Das Redundanzverfahren Spanning Tree definiert in einem Netzwerk mehrere Verbindungswege zwischen Netzteilnehmern, von denen nur einer aktiv ist. Damit werden Schleifen unterdrückt und die Pfade optimiert.
- Virtuelle Netze (VLAN)
  Zur Strukturierung von Industrial Ethernet-Netzen mit stark wachsender Teilnehmeranzahl kann ein physikalisch vorhandenes Netz in mehrere virtuelle Teilnetze unterteilt werden.
- Lastbegrenzung bei Einsatz von Multicast- und Broadcast-Protokollen, z. B. Video-Übertragung
  Durch Lernen der Multicast-Quellen und -Ziele (IGMP-Snooping, IGMP-Querier) können die IE-Switches Multicast-Datenverkehr filtern und damit die Last im Netz begrenzen. Multicast- und Broadcast-Datenverkehr können begrenzt werden.
- Uhrzeitsynchronisation
  Diagnosemeldungen, wie Einträge in der Log-Tabelle oder E-Mails, werden mit Zeitstempeln versehen. Die lokale Zeit ist durch Synchronisation mit einem SICLOCK-Uhrzeitsender oder SNTP-/NTP-Server netzweit einheitlich und erleichtert damit die Zuordnung von Diagnosemeldungen mehrerer Geräte.
- Quality of Service zur Klassifizierung des Netzwerkverkehrs nach CoS (Class of Service - IEEE 802.11Q) und DSCP (Differentiated Services Code Point - RFC 2474)
- Port Mirroring
  Mirroring ermöglicht es, den Datenverkehr eines Ports auf einen anderen Port (Monitor-Port) abzubilden. Am Monitor-Port kann dann rückwirkungsfrei der Datenverkehr analysiert werden.
- Netzzugriffsschutz nach dem Standard IEEE 802.1X
  Ports können für Endgeräte konfiguriert werden, die die Authentifizierung nach IEEE 802.1X unterstützen. Die Authentifizierung erfolgt über einen RADIUS-Server, der über das Netz erreichbar sein muss.

- Log-Tabelle
  In die Log-Tabelle werden Ereignisse protokolliert, die während des Betriebs auftreten. Der Benutzer kann festlegen, welche Ereignisse zu einem Tabelleneintrag führen.
- Link Aggregation (IEEE 802.1AX) zur Bündelung von Ports (SCALANCE XC-200/ SCALANCE XP-200)
- H-Sync-Unterstützung
  Für weitere Informationen siehe Kapitel "Ring (Seite 253)"
- S2-Geräte (PROFINET-Konfiguration mit einfacher Systemredundanz)
  S2-Geräte können zwei Verbindungen zum Automatisierungssystem aufbauen, je eine Applikationsbeziehung (AR) zu beiden IO-Controllern. Wenn eine Kommunikationsverbindung unterbrochen wird, stehen alle Daten und Diagnosefunktionen über die zweite Verbindung weiterhin zur Verfügung.
  Welche IE-Switches als S2-Gerät eingesetzt werden können, entnehmen Sie dem Kapitel "Systemfunktionen und Hardware-Ausstattung".
  Sie konfigurieren S2-Geräte nur über STEP 7 Basic bzw. Professional.
  Für weitere Informationen siehe auch: PROFINET in SIMATIC PCS 7 (https://support.industry.siemens.com/cs/ww/de/view/72887082)
- CiR/H-CiR-Unterstützung (Konfiguration im laufenden Betrieb)
  Configuration in Run (CiR) ist eine Funktion, um Anlagen- und Konfigurationsänderungen im laufenden Betrieb durchzuführen. Diese Funktion ist in unterschiedlichem Umfang sowohl für Standard-Automatisierungssysteme als auch H-Systeme (H-CiR) verfügbar.
  Welche IE-Switches CiR unterstützen, entnehmen Sie dem Kapitel "Systemfunktionen und Hardware-Ausstattung".
  Sie konfigurieren CiR nur über STEP 7 Basic bzw. Professional.
  Für weitere Informationen siehe auch: PROFINET in SIMATIC PCS 7 (https://support.industry.siemens.com/cs/ww/de/view/72887082)

2.3 Voraussetzungen für Installation und Betrieb

Voraussetzungen für die Installation und den Betrieb der IE-Switches

Für die Konfiguration der IE-Switches muss ein PG/PC mit Netzwerkanschluss vorhanden sein. Dem IE-Switch muss eine IP-Adresse zugewiesen sein und er muss im Netzwerk verfügbar sein, siehe auch "Erstmalige Vergabe einer IP-Adresse (Seite 24)".

2.4 Protokolle

Sichere/Unsichere Protokolle und Dienste

- Vermeiden oder deaktivieren Sie unsichere Protokolle und Dienste, wie z. B. HTTP, Telnet und TFTP. Diese Protokolle sind aus historischen Gründen verfügbar, jedoch nicht für einen sicheren Einsatz gedacht. Setzen Sie unsichere Protokolle auf dem Gerät mit Bedacht ein.
- Prüfen Sie die Notwendigkeit der Nutzung folgender Protokolle und Dienste:
  - Nicht authentifizierte und unverschlüsselte Ports
  - MRP, HRP
  - IGMP Snooping
  - LLDP
  - Syslog
  - RADIUS
  - DHCP-Optionen 66/67
  - TFTP
  - GMRP und GVRP
- Die folgenden Protokolle bieten sichere Alternativen:
  - HTTP → HTTPS
  - Telnet → SSH
  - SNMPv1/v2c → SNMPv3
    Prüfen Sie die Notwendigkeit der Nutzung von SNMPv1/v2c. SNMPv1/v2c sind als unsicher eingestuft. Nutzen Sie die Möglichkeit, den Schreibzugriff zu unterbinden. Das Gerät bietet entsprechende Einstellmöglichkeiten.
    Wenn SNMP aktiviert ist, ändern Sie die Community-Namen. Wenn kein uneingeschränkter Zugriff erforderlich ist, beschränken Sie den Zugriff über SNMP. Nutzen Sie die Authentifizierungs- und Verschlüsselungsmechanismen von SNMPv3.
- Nutzen Sie sichere Protokolle, wenn der Zugriff auf das Gerät nicht durch physische Schutzvorkehrungen gesichert ist.
- Wenn Sie unsichere Protokolle und Dienste benötigen, betreiben Sie diese nur innerhalb eines geschützten Netzwerkbereichs.
- Beschränken Sie die nach außen angebotenen Dienste und Protokolle auf das erforderliche Mindestmaß.
- Aktivieren Sie für die DCP-Funktion nach der Inbetriebnahme den Modus "Schreibgeschützt".
- Wenn Sie RADIUS für den Management-Zugriff auf das Gerät verwenden, aktivieren Sie sichere Protokolle und Dienste.

Verfügbare Protokolle

Die folgende Liste gibt Ihnen einen Überblick über die offenen Protokoll-Ports.

Die Tabelle umfasst folgende Spalten:

- **Protokoll**
- **Port**
- **Voreingestellter Portstatus**
  - Offen
    Die Werkseinstellung des Ports ist "Offen".
  - Geschlossen
    Die Werkseinstellung des Ports ist "Geschlossen".
- **Port konfigurierbar**
  - ✓
    Der Portstatus kann geändert werden.
  - --
    Der Portstatus kann nicht geändert werden.
- **Authentifizierung**
  Gibt an, ob eine Authentifizierung des Kommunikationspartners stattfindet.
- **Verschlüsselung**
  Gibt an, ob die Übertragung verschlüsselt ist.

Liste verfügbarer Protokolle (lokaler Zugriff über ein lokales Netzwerk)

Nachfolgend werden alle verfügbaren Protokolle und deren Ports aufgelistet, über die auf das Gerät zugegriffen werden kann.

Protokoll	Protokoll/ Portnummer	Voreingestellter Portstatus	Port konfigurierbar	Authentifizierung	Verschlüsselung
TELNET	TCP/23	Offen		Ja	Nein
SSH	TCP/22	Offen	--	Ja	Ja
HTTP	TCP/80	Offen	--	Ja	Nein
HTTPS	TCP/443	Offen	✓	Ja	Ja
SNMP	UDP/161	Offen	✓	Ja	Ja (wenn konfiguriert)
PROFINET	UDP/34964 UDP/49154 - 49157 [1]	Offen		Nein	Nein
EtherNet/IP	TCP/44818 UDP/2222 UDP/44818	Geschlossen (Offen bei EtherNetIP-Varianten)	✓	Nein	Nein
DHCP	UDP/67 UDP/68	Geschlossen	✓	Nein	Nein

[1] Port-Nummer ist über das WBM konfigurierbar.

Vergabe einer IP-Adresse

3

3.1 Aufbau einer IP-Adresse

Adressklassen

IP-Adressbereich	Max. Anzahl der Netzwerke	Max. Anzahl Hosts/Netzwerk	Klasse	CIDR
1.x.x.x bis 126.x.x.x	126	16777214	A	/8
128.0.x.x bis 191.255.x.x	16383	65534	B	/16
192.0.0.x bis 223.255.255.x	2097151	254	C	/24
224.0.0.0 - 239.255.255.255	Multicast-Anwendungen		D	
240.0.0.0 - 255.255.255.255	reserviert für zukünftige Anwendungen		E	

Eine IP-Adresse besteht aus 4 Byte. Jedes Byte wird dezimal dargestellt und ist durch einen Punkt vom vorherigen getrennt. Es ergibt sich also folgender Aufbau, wobei für XXX eine Zahl zwischen 0 und 255 zu setzen ist:

XXX.XXX.XXX.XXX

Die IP-Adresse besteht aus zwei Teilen, der Netzwerkadresse und der Endteilnehmeradresse. Dadurch ist es möglich, verschiedene Teilnetze zu bilden. Abhängig davon, welche Bytes der IP-Adresse als Netzwerkadresse und welche als Endteilnehmeradresse genutzt werden, kann eine IP-Adresse einer bestimmten Adressklasse zugeordnet werden.

Subnetzmaske

Die Bits der Endteilnehmer-Adresse können für die Bildung von Subnetzen verwendet werden. Dabei stellen die führenden Bits die Adresse des Subnetzes dar, die restlichen Bits werden als Adresse des Rechners im Subnetz interpretiert.

Ein Subnetz wird durch die Subnetzmaske definiert. Der Aufbau der Subnetzmaske entspricht dem einer IP-Adresse. Ist in der Subnetzmaske an einer Bitposition eine "1" gesetzt, gehört das Bit an der entsprechenden Stelle in der IP-Adresse zur Subnetzadresse, andernfalls zur Adresse des Rechners.

Beispiel für ein Klasse B-Netz:

Die Standard-Subnetz-Adresse für Klasse B-Netze ist 255.255.0.0, es stehen also die letzten beiden Bytes für die Festlegung eines Subnetzes zur Verfügung. Wenn 16 Teilnetze definiert werden sollen, muss das dritte Byte der Subnetzadresse auf 11110000 (Binärdarstellung) gesetzt werden. In diesem Fall ergibt sich die Subnetzmaske 255.255.240.0.

Um festzustellen, ob zwei IP-Adressen zum gleichen Subnetz gehören, werden auf die beiden IP-Adressen und die Subnetzmaske eine bitweise UND-Verknüpfung angewendet. Wenn beide Verknüpfungen das gleiche Ergebnis haben, gehören beide IP-Adressen zum gleichen Subnetz, wie z. B. 141.120.246.210 und 141.120.252.108.

Außerhalb des lokalen Netzwerks ist die beschriebene Aufteilung der Endteilnehmer-Adresse ohne Bedeutung, dort ist für die Paketvermittlung nur die IP-Adresse in ihrer Gesamtheit von Interesse.

Hinweis

In der Bit-Darstellung der Subnetzmaske müssen die "Einsen" linksbündig gesetzt sein, d. h. es dürfen keine "Nullen" zwischen den "Einsen" stehen.

3.2 Erstmalige Vergabe einer IP-Adresse

Konfigurationsmöglichkeiten

Die erstmalige Vergabe einer IP-Adresse für einen IE-Switch kann nicht mit dem Web Based Management (WBM) erfolgen, weil dieses Konfigurationswerkzeug bereits eine IP-Adresse voraussetzt.

Es gibt folgende Möglichkeiten, einem unkonfigurierten Gerät eine IP-Adresse zuzuweisen:

- **DHCP** (Werkseinstellung)
- **Primary Setup Tool** (PST)
  - Um dem IE-Switch mit dem PST eine IP-Adresse zuweisen zu können, muss der IE-Switch über Ethernet erreichbar sein.
  - Sie finden das PST auf den Internetseiten des Siemens Industry Online Support unter der Beitrags-ID 19440762 (https://support.industry.siemens.com/cs/ww/de/view/19440762).
  - Beachten Sie für weitere Informationen zur Vergabe der IP-Adresse mit dem PST die Dokumentation "Primary Setup Tool (PST)".

- **STEP 7**
  Sie können in STEP 7 die Topologie, den Gerätenamen und die IP-Adresse projektieren. Wenn Sie einen unkonfigurierten IE-Switch mit dem Controller verbinden, weist der Controller dem IE-Switch den projektierten Gerätenamen und die IP-Adresse automatisch zu.
  - **STEP 7**
    SCALANCE XB-200: ab V5.5.4
    SCALANCE XP-200: ab V5.5.4 HF9
    SCALANCE XC-200: ab V5.5.4 HF11
    SCALANCE XR-300WG: ab V5.6
    SCALANCE XF-200BA: ab V5.6 HF3
    SCALANCE XC-200G: ab V5.6 HSP11
    Beachten Sie für weitere Informationen zur Vergabe der IP-Adresse über STEP 7 die Dokumentation "Hardware konfigurieren und Verbindungen projektieren mit STEP 7", Abschnitt "Schritte zum Konfigurieren eines PROFINET IO-Systems".
  - **STEP 7 Basic bzw. Professional**
    SCALANCE XB-200: ab V13 SP1
    SCALANCE XC-200: ab V14
    SCALANCE XP-200: ab V14
    SCALANCE XR-300WG: ab V15
    Beachten Sie für weitere Informationen zur Vergabe der IP-Adresse über STEP 7 die Online-Hilfe "Informationssystem", Abschnitt "Adressierung von PROFINET-Geräten".
- **CLI** über die serielle Schnittstelle
  Beachten Sie für weitere Informationen zur Vergabe der IP-Adresse über die serielle Schnittstelle die Betriebsanleitung des jeweiligen Geräts, siehe auch Kapitel "Einleitung", Abschnitt "Einordnung in die Dokumentationslandschaft".
- **NCM PC**
  Beachten Sie für weitere Informationen zur Vergabe der IP-Adresse über NCM PC die Dokumentation "PC-Stationen in Betrieb nehmen - Anleitung und Schnelleinstieg", Abschnitt "PROFINET IO-System anlegen".

Hinweis

DHCP ist im Auslieferungszustand und nach dem Wiederherstellen der Werkseinstellungen eingeschaltet. Wenn ein DHCP-Server im lokalen Netz verfügbar ist und dieser auf den DHCP-Request eines IE-Switches antwortet, werden beim ersten Hochlauf automatisch IP-Adresse, Subnetzmaske und Gateway zugeteilt.

3.3 Adressvergabe über DHCP

Eigenschaften von DHCP

DHCP (Dynamic Host Configuration Protocol) ist ein Verfahren zur automatischen Vergabe von IP-Adressen. Es hat folgende Eigenschaften:

- DHCP kann sowohl während des Hochlaufs eines Geräts als auch im laufenden Betrieb eingesetzt werden.
- Die vergebene IP-Adresse bleibt nur für eine begrenzte Zeitdauer (Lease Time) gültig. Nachdem die Gültigkeitsdauer zur Hälfte abgelaufen ist, kann der DHCP-Client die vergebene IPv4-Adresse verlängern. Nach Ablauf der gesamten Zeitdauer muss der DHCP-Client eine neue IPv4-Adresse anfordern.
- Ist die Anforderung einer neuen IP-Adresse nach Ablauf der Lease Time nicht erfolgreich, wird die IP-Konfiguration auf 0.0.0.0 ("Nicht konfiguriert") zurückgesetzt.
- Wurde eine IP-Adresse über DHCP konfiguriert und wird DHCP ausgeschaltet, wird die IP-Konfiguration auf 0.0.0.0 ("Nicht konfiguriert") zurückgesetzt.
- Wurde eine IP-Adresse über DHCP konfiguriert und wird die Verbindung zum Netzwerk kurzfristig unterbrochen (Zustand der Schnittstelle "Up", "Down" und wieder "Up"), muss die IP-Konfiguration zunächst vom DHCP-Server bestätigt werden. Ist eine Bestätigung nicht möglich, wird die IP-Konfiguration auf 0.0.0.0 ("Nicht konfiguriert") zurückgesetzt und eine neue IP-Konfiguration vom DHCP-Server angefordert.
- War bei einem Gerät DHCP aktiv, muss nach einem Neustart erst eine neue IP-Adresse beim DHCP-Server angefordert werden.
- Normalerweise erfolgt keine feste Adresszuordnung, d. h. wenn ein Client erneut eine IP-Adresse anfordert, erhält er in der Regel eine andere Adresse als bei der vorhergehenden Anforderung. Es ist möglich, den DHCP-Server so zu konfigurieren, dass der DHCP-Client auf seine Anfrage immer dieselbe feste Adresse zugeordnet bekommt. Über welchen Parameter der DHCP-Client für die feste Adresszuordnung identifiziert wird, wird im DHCP-Client und -Server eingestellt. Die Adresse kann über die MAC-Adresse, die DHCP-Client-ID, den PROFINET- oder Systemnamen zugeordnet werden. Den Parameter konfigurieren Sie unter "System > DHCP > DHCP-Client".
- Wurde eine statische IP-Adresse konfiguriert und wird DHCP aktiviert, so wird die statische IP-Konfiguration gelöscht.

Technische Grundlagen

4

4.1 Mengengerüst

Mengengerüst des Geräts

In der folgenden Tabelle ist das Mengengerüst für das Web Based Management und das Command Line Interface des Geräts aufgeführt.

Abhängig von Ihrem IE-Switch stehen Ihnen manche Funktionen nicht zur Verfügung.

	Konfigurierbare Funktion	Maximale Anzahl				
		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XP-200	SCALANCE XF-200BA
System	Maximale Framegröße (Ingress)	1632/2048 Byte [7]				
	Syslog-Server	3				
	E-Mail-Server	3				
	DHCP-Pools	16 [1]	28 [1]	24		
	IPv4-Adressen pro DHCP-Pool	1		24		
	IPv4-Adressen, die der DHCP-Server verwaltet (dynamisch + statisch)	16 [1]	28 [1]	576		
	DHCP statische Zuordnungen pro DHCP-Pool	-		24		
	SNMPv1-Trapempfänger	10				
	SNTP-Server	1				
	NTP-Server	-		1 [8]		
	Agent-/TIA-Schnittstellen [2]	1				
	Angezeigte Geräte über DCP Discovery	100				

	Konfigurierbare Funktion	Maximale Anzahl				
		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XP-200	SCALANCE XF-200BA
Layer 2	QoS-Priority-Queues	4		4/8 [6]	4	
	Virtuelle LANs (portbasiert, inklusive VLAN 1)	257 [3]				
	Private VLAN	-		1		-
	Primary PVLANs	-		1		-
	Secondary Isolated PVLANs	-		24		-
	Secondary Community PVLANs	-		256		-
	Mirroring-Sessions	1				
	Standby-Ports	1				
	Multiple Spanning Tree-Instanzen	-		4		-
	Link Aggregationen	-		4/8 [5]		
	Ports in einer Link Aggregation	-		8		4
	Statische Unicast-Adressen	128				
	Statische Multicast-Adressen ohne aktiviertes GMRP	256				
	Statische Multicast-Adressen mit aktiviertem GMRP	-		50		
	Über IGMP-Snooping gelernte Adressen	512				
Layer 3	VLAN-IP-Schnittstellen	1		24		1
	DHCP Relay Agent-Schnittstellen	1		24		1
	DHCP Relay Agent-Server	4				
	NAT-Schnittstellen	-		1		-
	Dynamische NAT-Konfigurationen (Pools)			100		
	Statische NAT-Konfigurationen	-		100		-
Security	Benutzer	18 (inkl. werkseitig voreingestelltem Benutzer "admin")				
	Rollen	29				
	Gruppen	32				
	IP-Adressen von RADIUS-Servern	4				
	Gleichzeitige MAC-Authentifizierungen (authentifiziert und geblockt) pro Gerät [4]	4000				
	Gleichzeitige MAC-Authentifizierungen (authentifiziert und geblockt) pro Port (konfigurierbar) [4]	100				
	Management ACLs (Zugriffsregeln für das Management)	10				

[1] Beim SCALANCE XB-200 und SCALANCE XR-300WG ist die Anzahl der DHCP-Pools und verwaltbaren IPv4-Adressen von der Anzahl der Ports abhängig. Die Anzahl der Ports entspricht der maximalen Anzahl an DHCP-Pools und verwaltbaren IPv4-Adressen.

[2] Hierbei handelt es sich um eine IP-Schnittstelle.

[3] Geräte mit Y-Funktionalität unterstützen keine VLANs.

[4] Wenn die maximale Anzahl der MAC-Authentifizierungen pro Gerät überschritten wird, werden alle MAC-Authentifizierungen des Ports zurückgesetzt, an dem der Wert überschritten wurde.
Wenn die maximale Anzahl der MAC-Authentifizierungen pro Port überschritten wird, werden alle MAC-Authentifizierungen des Ports zurückgesetzt.

[5] Für Geräte der Produktgruppen SCALANCE XC-200 und SCALANCE XP-200 gilt Folgendes:
Da eine Link Aggregation aus mindestens 2 Ports besteht, ist die maximale Anzahl der Link Aggregationen von der Anzahl der Ports abhängig. Bei Geräten mit bis zu 8 Ports sind maximal 4 Link Aggregationen möglich, bei Geräten mit mehr als 8 Ports sind maximal 8 Link Aggregationen möglich.

[6] Die Geräte der Gerätegruppe SCALANCE XC-200G unterstützen 8 Queues. Alle anderen XC-200-Geräte unterstützen 4 Queues.

[7] Bei Geräten der Gerätegruppe SCALANCE XC-200G beträgt die maximale Framegröße (Ingress) 2048 Byte. Bei allen anderen Geräten beträgt sie 1632 Byte.

[8] Maximale Anzahl von NTP/SNTP-Servern, die für einen SCALANCE X-200 konfiguriert werden können.

4.2 PROFINET

PROFINET

PROFINET ist ein offener Ethernet-Standard (IEC 61158/61784) für die industrielle Automatisierung basierend auf Industrial Ethernet. PROFINET nutzt existierende IT-Standards und ermöglicht eine durchgängige Kommunikation von der Feldebene bis in die Leitebene sowie ein anlagenweites Engineering. Weitere Eigenschaften von PROFINET sind:

- Nutzung von TCP/IP
- Automatisierung von Applikationen mit Echtzeit-Bedarf
  - Real-Time (RT)-Kommunikation
  - Isochronous Real-Time (IRT)-Kommunikation
- Nahtlose Integration von Feldbus-Systemen

PROFINET konfigurieren Sie unter "System > PROFINET (Seite 203)".

PROFINET IO

Im Rahmen von PROFINET ist PROFINET IO ein Kommunikationskonzept für die Realisierung modularer, dezentraler Applikationen. Die Umsetzung von PROFINET IO wird durch den PROFINET-Standard für Automatisierungsgeräte (IEC 61158-x-10) realisiert.

4.3 EtherNet/IP

EtherNet/IP

EtherNet/IP (Ethernet/Industrial Protocol) ist ein offener Industriestandard für industrielles Echtzeit-Ethernet, basierend auf TCP/IP und UDP/IP. Mit EtherNet/IP wird Ethernet um das Common Industrial Protocol (CIP) auf der Anwendungsschicht erweitert. In EtherNet/IP werden die unteren Schichten des OSI-Referenzmodells von Ethernet mit den Übertragungs-, Vermittlungs-, Netzwerk- und Transportfunktionen übernommen.

EtherNet/IP konfigurieren Sie unter "System > EtherNet/IP (Seite 204)".

Common Industrial Protocol

Das Common Industrial Protocol (CIP) ist ein Anwendungsprotokoll der Automatisierung, das den Übergang der Feldbusse in industrielles Ethernet und in IP-Netze unterstützt. Dieses Industrieprotokoll benutzen Feldbusse/Industrienetzwerke wie DeviceNet, ControlNet und EtherNet/IP in der Anwendungsschicht als Schnittstelle zwischen der deterministischen Feldbus-Welt und der Automatisierungsapplikation (Steuerung, E/A, HMI, OPC, ...). Das CIP liegt oberhalb der Transportschicht und erweitert die reinen Transportdienste um Kommunikationsdienste für die Automatisierungstechnik. Dazu gehören Dienste für den zyklischen, den zeitkritischen und den ereignisgesteuerten Datenverkehr. CIP unterscheidet zwischen den zeitkritischen E/A-Nachrichten (implicit messages) und individuellen Frage/Antwort-Telegrammen zur Konfiguration und Datenerfassung (explicit messages). CIP ist objekt-orientiert; alle von außen "sichtbaren" Daten sind in Form von Objekten zugänglich. CIP hat eine gemeinsame Konfigurationsgrundlage: EDS (Electronic Data Sheet).

Electronic Data Sheet

Electronic Data Sheet (EDS) ist ein elektronisches Datenblatt zur Beschreibung von Geräten.

Das für den EtherNet/IP-Betrieb benötigte EDS finden Sie unter "System > Laden & Speichern (Seite 127)".

4.4 Redundanzverfahren

4.4.1 Spanning Tree

Vermeidung von Schleifenbildung bei redundanten Verbindungen

Das Spanning Tree-Verfahren ermöglicht es, Netzwerkstrukturen aufzubauen, bei denen es mehrere Verbindungen zwischen zwei IE-Switches/-Bridges gibt. Ein Spanning Tree verhindert, dass es zu einer Schleifenbildung im Netz kommt, indem er genau einen Pfad zulässt und die anderen (redundanten) Ports für den Datenverkehr deaktiviert. Bei einer Unterbrechung können die Daten über einen alternativen Pfad gesendet werden. Die Funktionalität des Spanning Tree-Verfahrens basiert auf dem Austausch von Konfigurations- und Topologieänderungs-Telegrammen.

Definition der Netztopologie durch Konfigurationstelegramme

Die Geräte tauschen zur Berechnung der Topologie untereinander Konfigurationstelegramme aus, sogenannte BPDUs (Bridge Protocol Data Units). Mit diesen Telegrammen wird die Root Bridge ausgewählt und die Netztopologie erstellt. Darüber hinaus bewirken BPDU-Telegramme den Statuswechsel der Root-Ports.

Die Root Bridge ist die Bridge, die das Spanning Tree-Verfahren für alle beteiligten Komponenten steuert.

Nachdem die Root Bridge festgelegt ist, bestimmt jedes Gerät einen Root-Port. Der Root-Port ist der Port mit den geringsten Pfadkosten zur Root Bridge.

Verhalten bei Veränderungen der Netztopologie

Wenn Teilnehmer zu einem Netz hinzukommen oder wegfallen, kann das Auswirkungen auf die optimale Wegewahl der Datenpakete haben. Um diese Änderungen zu berücksichtigen, versendet die Root Bridge in regelmäßigen Abständen Konfigurationsmeldungen. Der Zeitabstand zwischen zwei Konfigurationsmeldungen lässt sich mit dem Parameter "Hello Time" einstellen.

Aktualität der Konfigurationsinformation

Mit dem Parameter "Max Age" legen Sie das maximale Alter von Konfigurationsinformationen fest. Erhält eine Bridge Konfigurationsinformationen, die älter sind als in "Max Age" festgelegt, verwirft sie diese Meldung und veranlasst eine Neuberechnung der Wege.

Neue Konfigurationsinformationen werden von einer Bridge jedoch nicht sofort, sondern erst nach dem im Parameter "Forward Delay" festgelegten Zeitraum angewendet. So wird sichergestellt, dass der Betrieb entsprechend der neuen Topologie erst gestartet wird, wenn alle Bridges die notwendigen Informationen haben.

4.4.1.1 RSTP, MSTP, CIST

Rapid Spanning Tree Protocol (RSTP)

Ein Nachteil des STP ist, dass sich das Netz bei einer Störung oder einem Geräteausfall rekonfigurieren muss: Die Geräte beginnen erst im Moment der Unterbrechung, neue Pfade auszuhandeln. Dieser Vorgang dauert bis zu 30 Sekunden. Aus diesem Grunde wurde STP zum "Rapid Spanning Tree Protocol" (RSTP, IEEE 802.1w) erweitert. Dies unterscheidet sich vom STP im Wesentlichen dadurch, dass die Geräte bereits zum Zeitpunkt des ungestörten Betriebs Informationen über Alternativrouten sammeln, die sie sich dann nicht erst beschaffen müssen, wenn eine Störung eingetreten ist. Damit lässt sich die Rekonfigurationszeit für ein RSTP-gesteuertes Netz auf wenige Sekunden reduzieren.
Das wird durch folgende Funktionen erreicht:

- Edge-Ports (Endteilnehmer-Port)
  Edge-Ports sind Ports, die mit einem Endgerät verbunden sind.
  Ein Port, der als Edge-Port definiert ist, wird direkt nach einem Verbindungsaufbau aktiviert. Wenn an einem Edge-Port eine Spanning Tree-BPDU empfangen wird, verliert der Port die Rolle als Edge-Port und nimmt wieder am (R)STP teil. Wird nach Ablauf einer Zeitspanne (3x Hello-Time) kein BPDU-Telegramm mehr empfangen, geht der Port wieder in den Edge-Port-Status über.
- Punkt-zu-Punkt (direkte Kommunikation zweier benachbarter Geräte)
  Durch die direkte Kopplung der Geräte kann eine Zustandsänderung (Umkonfiguration der Ports) ohne Verzögerungen durchgeführt werden.
- Alternativ-Port (Ersatz für den Root-Port)
  Es ist ein Ersatz für den Root-Port konfiguriert. Bei einem Verbindungsverlust zur Root-Bridge kann das Gerät deshalb ohne Verzögerung durch Neukonfiguration eine Verbindung über den Alternativ-Port aufbauen.
- Reaktion auf Ereignisse
  Ein Rapid Spanning Tree reagiert auf Ereignisse, beispielsweise einen Verbindungsabbruch, ohne Verzögerung. Es müssen also keine Zeitgeber wie beim Spanning Tree abgewartet werden.
- Zähler maximale Bridge-Sprünge
  Anzahl der Bridge-Sprünge, die ein Paket maximal ausführen darf, bevor es automatisch ungültig wird.

Prinzipiell werden also beim Rapid Spanning Tree für viele Parameter Alternativen vorkonfiguriert oder bestimmte Eigenschaften der Netzstruktur berücksichtigt, um die Rekonfigurationszeit zu verkürzen.

Multiple Spanning Tree Protocol (MSTP)

Das Multiple Spanning Tree Protocol (MSTP) ist eine Weiterentwicklung des Rapid Spanning Tree Protocols. Es bietet u. a. die Möglichkeit, mehrere RSTP-Instanzen innerhalb verschiedener VLANs oder VLAN-Gruppen zu betreiben und so z. B. Pfade, die das einfache Rapid Spanning Tree Protocol für den Datenverkehr global sperren würde, innerhalb einzelner VLANs verfügbar zu machen.

Common and Internal Spanning Tree (CIST)

CIST bezeichnet die intern vom Switch verwendete Instanz, die im Prinzip einer internen RSTP-Instanz gleicht.

4.4.2 RSTP+

4.4.2.1 Eigenschaften und Funktion von RSTP+

Der Hauptanwendungsfall von RSTP+ ist die redundante Integration von MRP-Ringen in ein RSTP-Netzwerk. Grundsätzlich wäre es möglich, ein solches Netzwerk ausschließlich mit RSTP zu verwalten. In einer Ringtopologie ist MRP aber das effizientere und schnellere Verfahren. Das Ringredundanzverfahren MRP wird von RSTP+ nicht beeinträchtigt, weil beide Verfahren unabhängig voneinander funktionieren.

Ein weiterer Einsatzfall ist die redundante Kopplung von MRP-Ringen. Außerdem ist es mit RSTP+ möglich, zwei RSTP-Netzwerke über einen MRP-Ring zu verbinden. Ohne RSTP+ ist das nicht möglich, weil Spanning Tree an den Ring-Ports abgeschaltet ist.

Kompatibilität von Geräten ohne RSTP+

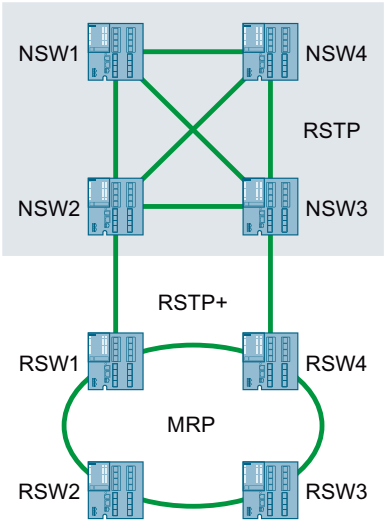
Grundsätzlich gilt, dass alle Geräte an den Verbindungsstellen zwischen RSTP-Netzwerk und MRP-Ring das Verfahren RSTP+ unterstützen müssen. Alle übrigen Geräte im MRP-Ring müssen BPDUs (Bridge Protocol Data Unit) weiterleiten.

4.4.2.2 Topologie für RSTP+

RSTP-Netzwerk und MRP-Ring

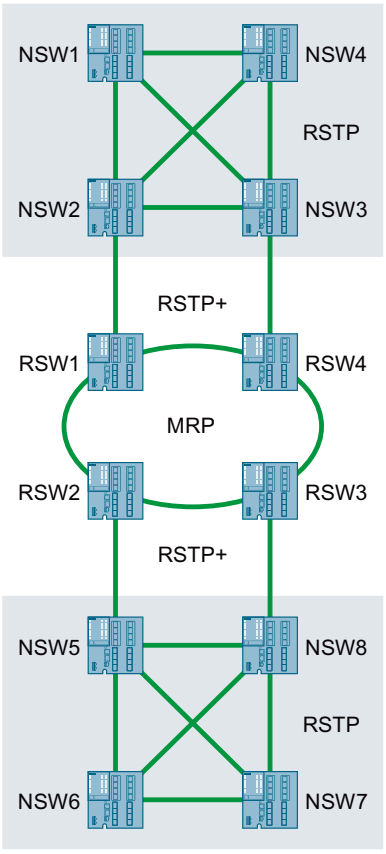
Die redundante Integration von MRP-Ringen in ein RSTP-Netzwerk ist ohne RSTP+ nicht möglich, weil der Parallelbetrieb von RSTP und MRP an einem Port unzulässig ist. Nur die Geräte des MRP-Rings, die Verbindung zum RSTP-Netzwerk haben, müssen RSTP+ unterstützen. In der dargestellten Beispieltopologie sind das die beiden Geräte RSW1 und RSW4. Die anderen Geräte müssen BPDUs weiterleiten.

Die Kennzeichnung der Geräte in den Grafiken nimmt Bezug auf die jeweilige Funktion des Geräts. "NSW" ist die Abkürzung für Netzwerk-Switch, "RSW" ist die Abkürzung für Ring-Switch.



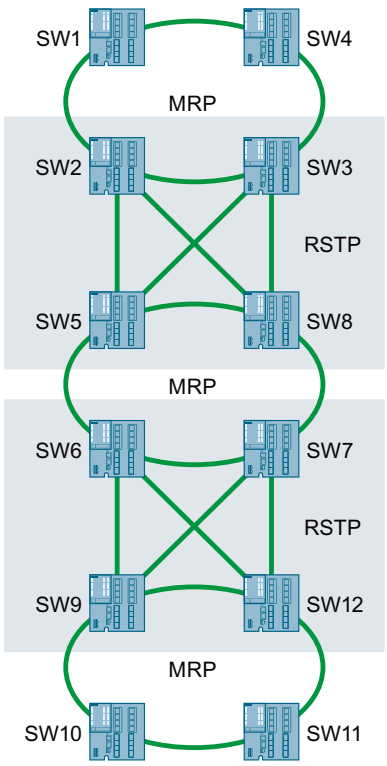
Mehrere RSTP-Netzbereiche und MRP-Ring

Ein weiterer Einsatzfall von RSTP+ ist die Verbindung von zwei oder mehr RSTP-Netzbereichen über einen MRP-Ring. RSTP+ muss für alle Geräte im MRP-Ring aktiviert sein, die Verbindung zu einem der RSTP-Netzwerke haben. Im dargestellten Beispiel sind das die Geräte RSW1, RSW2, RSW3 und RSW4.



Mehrere MRP-Ringe

RSTP+ kann auch dazu genutzt werden, mehrere MRP-Ringe über RSTP miteinander zu verbinden. RSTP+ stellt in diesem Fall sicher, dass MRP weiterhin unbeeinträchtigt von RSTP die Ringredundanz verwaltet.

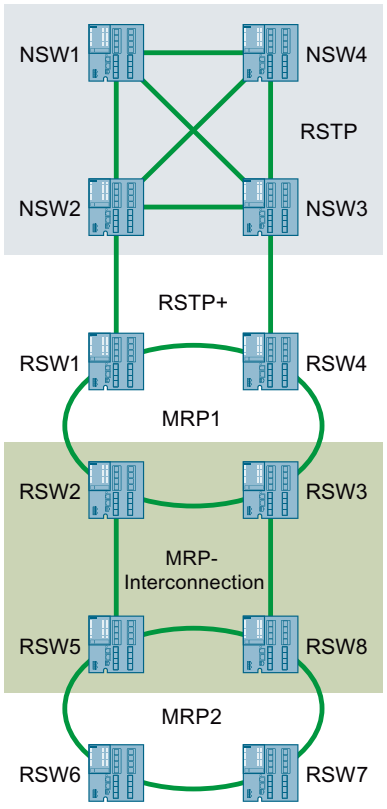


RSTP-Netzwerk und zwei MRP-Ringe mit MRP-Interconnection

RSTP+ kann auch ein RSTP-Netzwerk mit zwei MRP-Ringen verbinden, die über MRP-Interconnection gekoppelt sind. Die beiden Geräte RSW1 und RSW4 in der dargestellten Beispieltopologie müssen RSTP+ unterstützen. Die an der Verbindung der beiden MRP-Ringe beteiligten Geräte (RSW2, RSW3, RSW5 und RSW8) müssen MRP-Interconnection unterstützen. Zusätzlich müssen die Geräte RSW2 und RSW3 BPDUs (Bridge Protocol Data Unit) weiterleiten.

Für die RSTP+ MRP-Interconnection-Domain-ID gelten im dargestellten Beispiel folgende Regeln:

- Für die Geräte RSW1 und RSW4 muss die gleiche RSTP+ MRP-Interconnection-Domain-ID konfiguriert sein.
- Für die Geräte RSW2, RSW3, RSW5 und RSW8 muss die gleiche RSTP+ MRP-Interconnection-Domain-ID konfiguriert sein.
- Die RSTP+ MRP-Interconnection-Domain-ID der Geräte RSW1 und RSW4 muss sich von der RSTP+ MRP-Interconnection-Domain-ID der Geräte RSW2, RSW3, RSW5 und RSW8 unterscheiden.



4.4.2.3 RSTP+ konfigurieren

Dieses Kapitel beschreibt die Vorgehensweise bei der Konfiguration von RSTP+ im Detail. Führen Sie die Konfigurationsschritte für alle Geräte durch, bei denen RSTP+ aktiviert werden soll. Die Positionsnummern in den Screenshots beziehen sich auf die jeweilige Nummer der Schrittfolge. Die Beschreibung gilt für Geräte, die noch nicht konfiguriert wurden (Werkseinstellungen).

Die Beschreibung gliedert sich in drei Abschnitte:

- Spanning Tree konfigurieren (Schritt 1 bis 4)
- Ringredundanz konfigurieren (Schritt 5 bis 7)
- RSTP+ aktivieren und Leitungen stecken (Schritt 8 bis 9)

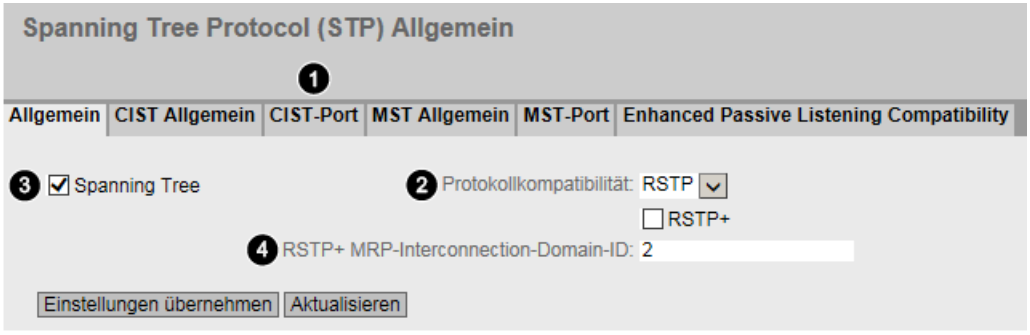
Allgemeine Konfigurationsregeln

Halten Sie bei der Konfiguration die folgenden Regeln ein, die unabhängig von einer bestimmten Netzwerk-Topologie gelten:

- Die Funktion des Redundanzmanagers sollte nicht von einem der beiden Geräte der RSTP/MRP-Kopplung übernommen werden.
- Zwischen den beiden Ring-Ports der Koppel-Geräte sollte eine direkte LAN-Verbindung bestehen.

4.4.2.4 Spanning Tree für RSTP+ konfigurieren

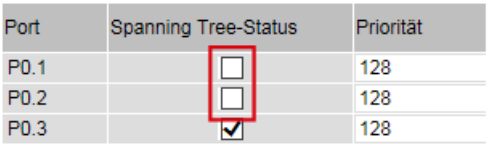
Im WBM gibt es für die Konfiguration von Spanning Tree das Menü „Layer 2 > Spanning Tree“. Führen Sie die Schritte 1 bis 4 für jedes Gerät durch, bei dem RSTP+ aktiviert werden soll.



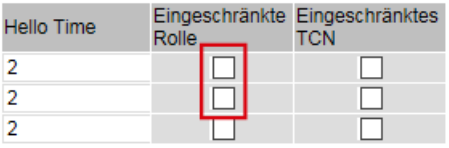
Schritt 1: Ring-Ports konfigurieren

Sie konfigurieren die Ring-Ports im Register "CIST-Port":

- Deaktivieren Sie die Optionskästchen für die beiden Ring-Ports in der Tabellenspalte "Spanning Tree-Status".



- Deaktivieren Sie die Optionskästchen für die beiden Ring-Ports in der Tabellenspalte "Eingeschränkte Rolle". Das ist erforderlich, damit das Verhalten der Ring-Ports ausschließlich von MRP - also vom Redundanzmanager - gesteuert wird. Die Funktion von MRP wird von RSTP+ nicht beeinträchtigt.



Schritt 2: Protokollkompatibilität konfigurieren

Wählen Sie aus der Klappliste "Protokollkompatibilität" der Eintrag "RSTP".

Schritt 3: Spanning Tree einschalten

Es gibt Geräte, bei denen Spanning Tree bereits ab Werk aktiviert ist. Wenn Spanning Tree noch nicht eingeschaltet ist, aktivieren Sie das Optionskästchen "Spanning Tree".

Die Tabelle im Register "CIST-Port" bietet die Möglichkeit, Spanning Tree für einzelne Ports zu konfigurieren. Die Optionskästchen der Ports für die Verbindung zum RSTP-Netzwerk müssen aktiviert sein.

Schritt 4: RSTP+ MRP-Interconnection-Domain-ID festlegen

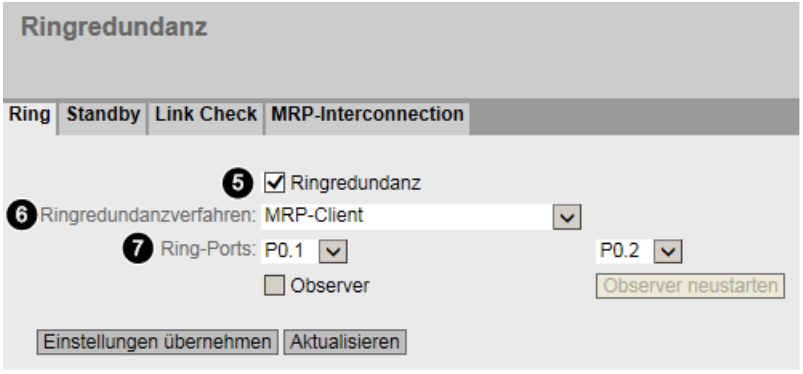
Die RSTP+ MRP-Interconnection-Domain-ID muss netzwerkweit eindeutig sein und sich von einer gegebenenfalls zu konfigurierenden MRP-Interconnection-Domain-ID unterscheiden. Unterschiedliche IDs sind notwendig, um TCNs (Topology Change Notifications) des RSTP-Netzwerks von TCNs des MRP-Rings unterscheiden zu können. Diese Zuordnung ermöglicht es, nur solche FDB-Einträge (Forwarding Database-Einträge) zu löschen, die von der Topologieänderung betroffen sind.

Jedes Gerät überprüft, ob für diese beiden Parameter unterschiedliche Werte konfiguriert wurden. Bei übereinstimmenden IDs gibt das Gerät eine Fehlermeldung aus. Es liegt in der Verantwortung des Netzwerkadministrators, dass diese IDs auch netzwerkweit eindeutig sind. Eine solche Überprüfung kann von einem einzelnen Geräte nicht vorgenommen werden.

Klicken Sie abschließend die Schaltfläche "Einstellungen übernehmen", um die Konfiguration zu speichern.

4.4.2.5 Ringredundanz für RSTP+ konfigurieren

Im WBM gibt es für die Konfiguration der Ringredundanz das Menü „Layer 2 > Ringredundanz“. Führen Sie im Register „Ring“ die Schritte 5 bis 7 für jedes Gerät durch, bei dem RSTP+ aktiviert werden soll.



Schritt 5: Ringredundanz einschalten

Aktivieren Sie das Optionskästchen „Ringredundanz“, um MRP einzuschalten.

Schritt 6: MRP-Rolle zuweisen

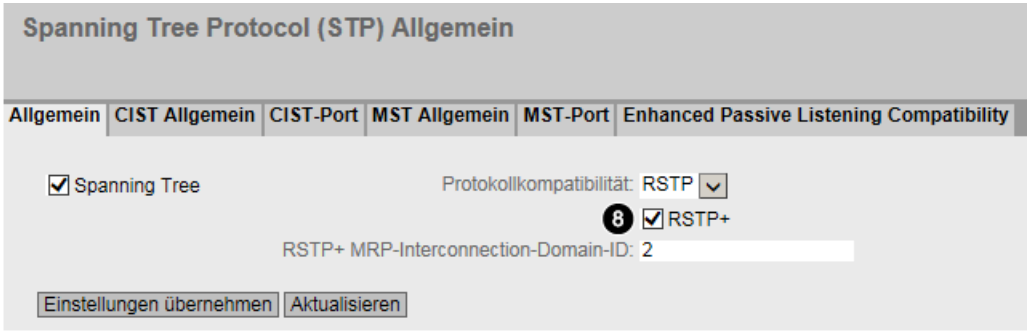
Wählen Sie aus der Klappliste "Ringredundanzverfahren" den Eintrag "MRP-Client" oder "MRP-Auto-Manager". Die Funktion des Redundanzmanagers sollte nicht von einem der beiden Geräte der RSTP-MRP-Kopplung übernommen werden.

Schritt 7: Ring-Ports festlegen

Wählen Sie aus den beiden Klapplisten die passenden Einträge für die Ring-Ports.

Klicken Sie abschließend die Schaltfläche "Einstellungen übernehmen", um die Konfiguration zu speichern.

4.4.2.6 RSTP+ einschalten und Leitungen stecken



Schritt 8: RSTP+ einschalten

Aktivieren Sie das Optionskästchen "RSTP+". Es erscheint ein Dialogfeld mit der Meldung "Spanning Tree ist auf den Ringports aktiviert, weil RSTP+ aktiviert ist.". Diese Meldung wird angezeigt, weil normalerweise ein Parallelbetrieb von Ringredundanz (MRP) und RSTP an einem Port nicht möglich ist. Klicken Sie die Schaltfläche "OK", um das Dialogfeld zu schließen.

Wenn RSTP+ eingeschaltet ist, können Sie die zuvor konfigurierten Parameter nicht mehr ändern. Klicken Sie abschließend die Schaltfläche "Einstellungen übernehmen", um die Konfiguration zu speichern.

Schritt 9: Stecken der Leitungen

Wenn Sie alle Geräte konfiguriert haben, stecken Sie die Leitungen entsprechend der geplanten Topologie. Das Verfahren RSTP+ ist nun aktiviert.

4.4.3 HRP

HRP - High Speed Redundancy Protocol

HRP bezeichnet ein Redundanz-Verfahren für Netze in Ring-Topologie. Die Switches sind über Ringports miteinander verbunden. Einer der Switches wird zum Redundanzmanager (RM) konfiguriert. Die anderen Switches sind Redundanz-Clients. Mit Testtelegrammen prüft der Redundanzmanager den Ring auf Unterbrechungsfreiheit. Der Redundanzmanager sendet Testtelegramme über die Ringports und prüft deren Empfang am jeweils anderen Ringport. Die Redundanz-Clients leiten die Testtelegramme weiter.

Wenn die Testtelegramme des RM bei einer Unterbrechung des Rings nicht mehr am anderen Ringport ankommen, schaltet der RM seine beiden Ringports durch und informiert die Redundanz-Clients umgehend über den Wechsel. Die Rekonfigurationszeit nach Unterbrechung des Rings beträgt maximal 300 ms.

Standby-Redundanz

Standby-Redundanz ist ein Verfahren, bei dem Ringe, die jeder für sich durch High-Speed Redundancy gesichert sind, redundant gekoppelt werden. Im Ring wird ein Master-/Slave-Gerätepaar konfiguriert, das sich gegenseitig über seine Ringports überwacht. Der

Datenverkehr wird im Fehlerfall von einer Ethernet-Verbindung (Standby-Port des Master bzw. Standby-Server) zu einer anderen Ethernet-Verbindung (Standby-Port des Slave) umgeleitet.

Voraussetzungen

HRP

- HRP wird in Ringtopologien mit bis zu 50 Geräten unterstützt.
  Eine Überschreitung der Geräteanzahl kann zum Ausfall des Datenverkehrs führen.
- Für HRP dürfen im Ring nur Geräte verwendet werden, die diese Funktion auch unterstützen.
- Geräte, die HRP nicht unterstützen, müssen über spezielle HRP-fähige Geräte an den jeweiligen Ring angebunden werden. Diese Verbindung ist bis zum Ring nicht redundant.
- Alle Geräte müssen über ihre Ringports miteinander verbunden sein. Dabei sind Multimodeverbindungen bis 3 km und Singlemodeverbindungen bis 26 km zwischen zwei IE-Switches möglich. Bei größeren Entfernungen kann es zu einer Verlängerung der angegebenen Rekonfigurationszeit kommen.
- Ein Gerät im Ring muss durch Auswahl der Einstellung "HRP-Manager" als Redundanzmanager konfiguriert werden. Bei allen übrigen Geräten im Ring muss entweder die Betriebsart "HRP-Client" oder die Betriebsart "Automatic Redundancy Detection" aktiviert werden.
- Die Standby-Ports müssen im Spanning Tree deaktiviert sein.
- Sie konfigurieren HRP über Web Based Management, Command Line Interface oder SNMP.

Standby-Redundanz

- Bei Standby-Koppelpartnern muss HRP fest eingestellt sein.
- Die Ports der Standby-Koppelpartner müssen im Spanning Tree deaktiviert sein.
- Sie konfigurieren die Standby-Redundanz über Web Based Management, Command Line Interface oder SNMP.

4.4.4 MRP

4.4.4.1 MRP - Media Redundancy Protocol

Das Verfahren "MRP" arbeitet konform zum Media Redundancy Protocol (MRP), das in folgender Norm spezifiziert ist:

IEC 62439-2 Ausgabe 1.0 (2010-02) Industrial communication networks - High availability automation networks Part 2: Media Redundancy Protocol (MRP)

Die Rekonfigurationszeit nach Unterbrechung des Rings beträgt maximal 200 ms.

Topologie

Die folgende Abbildung zeigt eine mögliche Topologie für Geräte in einem Ring mit MRP.

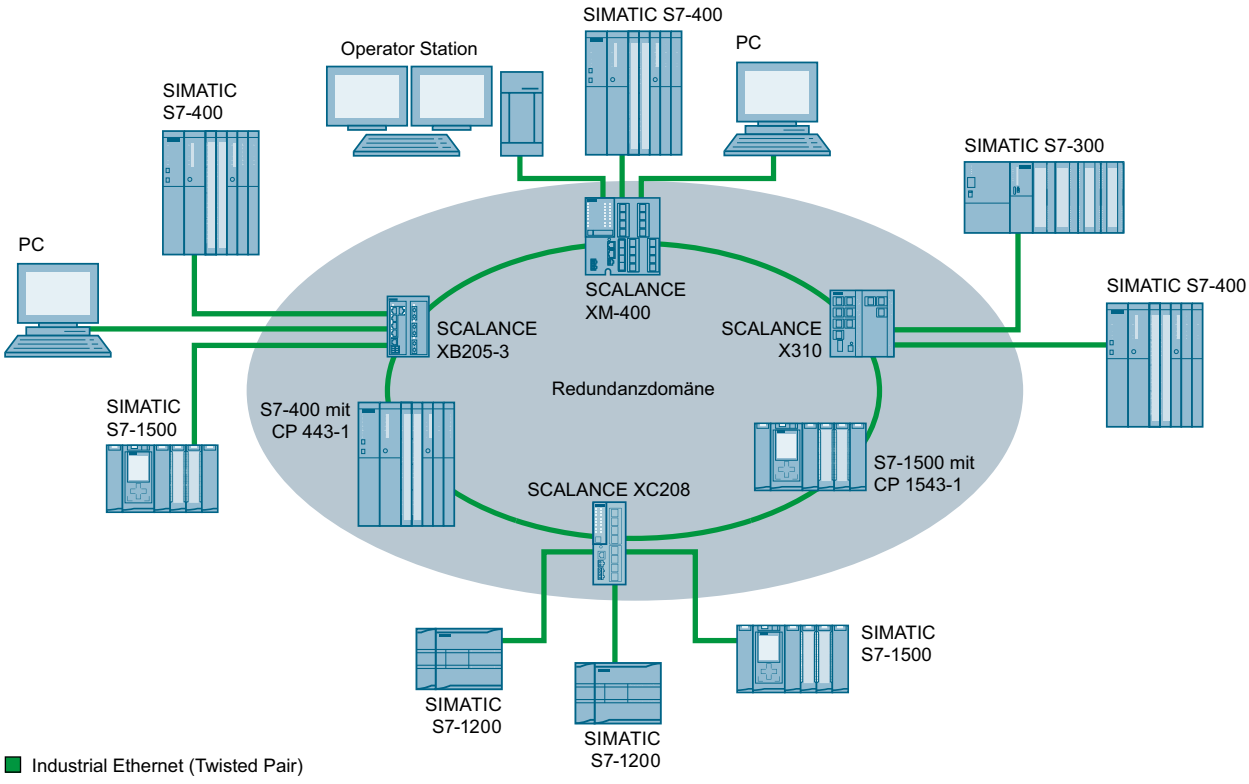


Bild 4-1 Beispiel einer Ringtopologie mit dem Medienredundanzverfahren MRP

Für die Ringtopologie mit Medienredundanz nach dem Verfahren MRP gelten folgende Regeln:

- Alle innerhalb der Ringtopologie verbundenen Geräte sind Mitglieder der gleichen Redundanz-Domäne.
- Ein Gerät im Ring ist Redundanzmanager.
- Alle anderen Geräte im Ring sind Redundanz-Clients.

Nicht MRP-fähige Geräte können über einen Switch SCALANCE X oder einen PC mit MRP-fähigem CP an den Ring angebunden werden.

Voraussetzungen

Voraussetzungen für den störungsfreien Betrieb mit dem Medienredundanzverfahren MRP sind:

- MRP wird in Ringtopologien mit bis zu 50 Geräten unterstützt.
  Eine Überschreitung der Geräteanzahl kann zum Ausfall des Datenverkehrs führen.
- Der Ring, in dem Sie MRP einsetzen wollen, darf nur aus Geräten bestehen, die diese Funktion unterstützen.
  Dies sind beispielsweise einige der Industrial Ethernet Switches SCALANCE X, einige der Kommunikationsprozessoren (CPs) für die SIMATIC S7 und PG/PC oder Nicht-Siemens-Geräte, die diese Funktion unterstützen.

- Alle Geräte müssen über ihre Ringports miteinander verbunden sein.
  Dabei sind Multimodeverbindungen bis 3 km und Singlemodeverbindungen bis 26 km zwischen zwei IE-Switches SCALANCE X möglich. Bei größeren Entfernungen kann es zu einer Verlängerung der angegebenen Rekonfigurationszeit kommen.
- Bei allen Geräten im Ring muss "MRP" aktiviert sein.
- Die Verbindungseinstellungen (Übertragungsmedium / Duplex) müssen für alle Ringports auf Vollduplex und mindestens 100 Mbit/s eingestellt sein. Andernfalls kann es zum Ausfall des Datenverkehrs kommen.
  - STEP 7: Setzen Sie im Eigenschaftendialog aller am Ring beteiligten Ports die Verbindung im Register "Optionen" auf "Automatische Einstellung".
  - WBM: Bei Projektierung über Web Based Management werden die Ringports automatisch auf Autonegotiation eingestellt.

4.4.4.2 Projektierung im WBM

Rolle

Die Auswahl der Rolle ist von den folgenden Einsatzfällen abhängig:

- Sie wollen MRP in einer Ringtopologie nur mit Siemens-Geräten einsetzen:
  - Wählen Sie bei mindestens einem Gerät im Ring "Automatic Redundancy Detection" bzw. "MRP Auto-Manager" aus.
  - Wählen Sie bei allen anderen Geräten im Ring "MRP-Client" oder "Automatic Redundancy Detection" aus.
- Sie wollen MRP in einer Ringtopologie einsetzen, die auch Nicht-Siemens-Geräte enthält:
  - Wählen Sie bei genau einem Gerät im Ring die Rolle "MRP Auto-Manager" aus.
  - Wählen Sie bei allen anderen Geräten der Ringtopologie die Rolle "MRP-Client" aus.

Hinweis

Die Verwendung von "Automatic Redundancy Detection" ist beim Einsatz von Nicht-Siemens-Geräten nicht möglich.

- Sie projektieren die Geräte in einer MRP-Ringtopologie teilweise über WBM und teilweise über Step 7:
  - Wählen Sie bei den Geräten, die Sie über WBM projektieren, für alle Geräte "MRP-Client" aus.
  - Wählen Sie bei den Geräten, die Sie über Step 7 projektieren, für genau ein Gerät "Manager" oder "Manager (Auto)" und für alle anderen Geräte "MRP-Client" aus.

Hinweis

Wenn einem Gerät über Step 7 die Rolle "Manager" zugeordnet wird, muss allen anderen Geräten im Ring die Rolle "MRP-Client" zugeordnet werden. Wenn es in einem Ring ein Gerät mit der Rolle "Manager" und ein Gerät mit der Rolle "Manager (Auto)"/"MRP Auto-Manager" gibt, kann es zu kreisenden Frames und damit zum Ausfall des Netzwerks kommen.

Projektierung

Im WBM projektieren Sie MRP auf folgenden Seiten:

- Konfiguration (Seite 220)
- Ring (Seite 253)

4.4.4.3 Projektierung in STEP 7

Projektierung in STEP 7

Wählen Sie zur Projektierung in STEP 7 die Parametergruppe "Medienredundanz" an der PROFINET-Schnittstelle.

Stellen Sie folgende Parameter zur MRP-Konfiguration des Geräts ein:

- Domäne
- Rolle
- Ringport
- Diagnosealarme

Diese Einstellungen werden nachfolgend beschrieben.

Hinweis

Gültige MRP-Projektierung

Stellen Sie bei der MRP-Projektierung in STEP 7 sicher, dass alle Geräte im Ring eine gültige MRP-Projektierung besitzen, bevor Sie den Ring zusammenschließen. Andernfalls kann es zu kreisenden Frames und damit zum Ausfall des Netzwerks kommen.

Ein Gerät im Ring müssen Sie als "Redundanzmanager" konfigurieren, alle anderen Geräte im Ring als "Client".

Hinweis

Werkseinstellungen beachten

Bei folgenden fabrikneuen und auf Werkseinstellungen gesetzten IE-Switches ist MRP deaktiviert und Spanning Tree aktiviert:

- SCALANCE XB-200 (EtherNet/IP-Varianten)
- SCALANCE XC-200 (EtherNet/IP-Varianten)
- SCALANCE XP-200 (EtherNet/IP-Varianten)
- SCALANCE XR-300WG
- SCALANCE XM-400
- SCALANCE XR-500

Um eine PROFINET-Konfiguration mit MRP in eines der genannten Geräte zu laden, deaktivieren Sie auf dem Gerät zunächst Spanning Tree.

Hinweis

Umkonfiguration nur bei geöffnetem Ring

Öffnen Sie zunächst den Ring, bevor Sie

- die MRP-Rolle ändern oder
- Ringports umkonfigurieren.

Hinweis

Neustart und Wiederanlauf

Die MRP-Einstellungen sind auch nach einem Neustart des Geräts oder nach einem Spannungsausfall und Wiederanlauf wirksam, sofern der Spannungsausfall nicht innerhalb von 90 Sekunden nach der Konfigurationsänderung stattfindet.

Hinweis

Priorisierter Hochlauf

Wenn Sie MRP in einem Ring projektieren, dann können Sie in den beteiligten Geräten in PROFINET-Applikationen die Funktion "Priorisierter Hochlauf" nicht nutzen.

Wenn Sie die Funktion "Priorisierter Hochlauf" nutzen wollen, dann müssen Sie MRP in der Projektierung deaktivieren.

Setzen Sie in der STEP 7-Projektierung des betreffenden Geräts die Rolle auf "Nicht Teilnehmer des Rings".

Domäne

Einfache MRP-Ringe

Wenn Sie einen einzelnen MRP-Ring konfigurieren wollen, belassen Sie in der Klappliste "Domain" den werkseitig vorbelegten Eintrag "mrpdomain-1".

Alle Geräte, die in einem Ring mit MRP projektiert werden, müssen der gleichen Redundanz-Domäne angehören. Ein Gerät kann nicht mehreren Redundanz-Domänen in einem Einfachring angehören.

Mehrere MRP-Ringe

Wenn Sie mehrere einzelne MRP-Ringe konfigurieren, werden die Ringteilnehmer über den Parameter "Domain" den einzelnen Ringen zugeordnet. Stellen Sie für alle Geräte innerhalb eines Rings die gleiche Domäne ein. Stellen Sie für die unterschiedlichen Ringe unterschiedliche Domänen ein. Geräte, die nicht zum gleichen Ring gehören, müssen unterschiedliche Domänen haben.

Wenn Sie MRP-Mehrfachringe projektieren möchten, wählen sie als zentralen Redundanzmanager für bis zu vier Ringe ein mehrfachringfähiges Gerät aus. Legen Sie für alle Ring-Instanzen unterschiedliche Domänen fest und ordnen Sie diese den zugehörigen

Ringports des Redundanzmanagers zu. Projektieren sie die übrigen Geräte als Clients. Dabei muss bei allen Geräten innerhalb eines Rings die gleiche Domäne eingestellt werden.

Hinweis

Geeignete Geräte für MRP-Mehrfachringe

Als Redundanzmanager, der mehrere Ringe verbindet, können Sie alle Geräte der folgenden Produktlinien einsetzen:

- SCALANCE X-300 ab Firmware-Version V4.0
- SCALANCE X-400 SCALANCE
  - X408-2 ab Firmware-Version V4.0
  - X414-3E ab Firmware-Version V3.10

Hinweis

Geeignete Geräte für MRP-Interconnection

Als Medienredundanz Interconnection Manager und Medienredundanz Interconnection Client können Sie alle Geräte der folgenden Produktlinien einsetzen:

- SCALANCE XM-400 ab Firmware-Version V6.2
- SCALANCE XR-500 ab Firmware-Version V6.2

Rolle

Hinweis

Umkonfiguration nur bei geöffnetem Ring!

Die Auswahl der Rolle ist von den folgenden Einsatzfällen abhängig.

- Sie wollen MRP in einer Topologie mit **einem Ring** nur mit Siemens-Geräten einsetzen und keine Diagnosealarme überwachen:
  Ordnen Sie alle Geräte der Domäne "mrpdomain-1" und der Rolle "Manager (Auto)" zu. Das Gerät, welches im Betrieb tatsächlich die Rolle des Redundanzmanagers übernimmt, wird unter Siemens-Geräten automatisch ausgehandelt.
- Sie wollen MRP in einer Topologie mit **mehreren Ringen** nur mit Siemens-Geräten einsetzen und keine Diagnosealarme überwachen:
  - Ordnen Sie allen Instanzen des Geräts, das die Ringe verbindet, die Rolle "Manager" zu.
  - Wählen Sie bei allen anderen Geräten der Ringtopologie die Rolle "Client".

- Sie wollen MRP in einer Ringtopologie einsetzen, die auch Nicht-Siemens-Geräte enthält, oder Sie wollen Diagnosealarme zum MRP-Zustand von einem Gerät erhalten (siehe "Diagnosealarme"):
  - Ordnen Sie genau einem Gerät im Ring die Rolle "Manager (Auto)" zu.
  - Wählen Sie bei allen anderen Geräten der Ringtopologie die Rolle "Client".
- Sie wollen MRP deaktivieren:
  Wählen Sie die Option "Nicht Teilnehmer des Rings", wenn Sie das Gerät nicht innerhalb einer Ringtopologie mit MRP betreiben wollen.

Hinweis

Rolle beim Rücksetzen auf Werkseinstellungen

Bei fabrikneuen und auf Werkseinstellungen gesetzten Siemens-Geräten ist folgende MRP-Rolle eingestellt:

- "Manager (Auto)"
  - CPs
- "Automatic Redundancy Detection"
  - SCALANCE X-200
  - SCALANCE XB-200 (PROFINET-Varianten)
  - SCALANCE XC-200 (PROFINET-Varianten)
  - SCALANCE XF-200BA
  - SCALANCE XP-200 (PROFINET-Varianten)
  - SCALANCE X-300
  - SCALANCE X-400

Wenn Sie im Ring ein Nicht-Siemens-Gerät als Redundanzmanager betreiben, kann dies zum Ausfall des Datenverkehrs führen.

Bei folgenden fabrikneuen und auf Werkseinstellungen gesetzten IE-Switches ist MRP deaktiviert und Spanning Tree aktiviert:

- SCALANCE XB-200 (EtherNet/IP-Varianten)
- SCALANCE XC-200 (EtherNet/IP-Varianten)
- SCALANCE XP-200 (EtherNet/IP-Varianten)
- SCALANCE XR-300WG
- SCALANCE XM-400
- SCALANCE XR-500

Ringport 1 / Ringport 2

Wählen Sie hier jeweils den Port aus, den Sie als Ringport 1 bzw. als Ringport 2 projektieren möchten.

Bei Geräten mit mehr als 8 Ports sind gegebenenfalls nicht alle Ports als Ringport auswählbar.

Die Klappliste zeigt für jeden Gerätetyp die Auswahl der möglichen Ports an. Wenn die Ports werkseitig festgelegt sind, dann sind die Felder gegraut.

ACHTUNG
Ringports beim Rücksetzen auf Werkseinstellungen Mit dem Rücksetzen auf Werkseinstellungen werden auch die Ringport-Einstellungen zurückgesetzt. Wenn vor dem Rücksetzen andere Ports als Ringports verwendet wurden, kann bei entsprechendem Anschluss ein zuvor korrekt konfiguriertes Gerät kreisende Frames und damit den Ausfall des Datenverkehrs verursachen.

Hinweis

Umkonfiguration nur bei geöffnetem Ring

Öffnen Sie zunächst den Ring, bevor Sie die Ringports eines Ring-Managers umkonfigurieren.

Diagnosealarme

Aktivieren Sie die Option "Diagnose Alarme", wenn Diagnosealarme zum MRP-Zustand in der lokalen CPU ausgegeben werden sollen.

Folgende Diagnosealarme können gebildet werden:

- Verdrahtungs- bzw. Port-Fehler
  Bei folgenden Fehlern an den Ringports werden Diagnosealarme generiert:
  - Verbindungsabbruch an einem Ringport
  - Ein Nachbar des Ringports unterstützt nicht MRP.
  - Ein Ringport ist mit einem Nicht-Ringport verbunden.
  - Ein Ringport ist mit dem Ringport einer anderen MRP-Domäne verbunden.
- Statuswechsel Aktiv/Passiv (nur Redundanzmanager)
  Wenn sich in einem Ring der Status ändert (Aktiv/Passiv), wird ein Diagnosealarm generiert.

Parametrierung der Redundanz nicht durch STEP 7 vorgegeben (Alternative Redundanz)

Diese Option betrifft alle SCALANCE X-Switches. Wählen Sie diese Option, wenn die Eigenschaften zur Medienredundanz durch alternative Mechanismen wie WBM, CLI oder SNMP parametriert werden sollen.

Wenn Sie diese Option aktivieren, bleiben bestehende Redundanzeinstellungen erhalten und werden nicht überschrieben. Die Parameter im Feld "MRP-Konfiguration" werden daraufhin zurückgesetzt und gegraut dargestellt. Die Einträge sind dann ohne Bedeutung.

4.4.5 Standby

Allgemeines

SCALANCE X Switches unterstützen neben der Ringredundanz innerhalb eines Ringes auch die redundante Kopplung von Ringen oder offenen Netzsegmenten (Linien). Bei der redundanten Kopplung werden Ringe über zwei Ethernet-Verbindungen miteinander gekoppelt. Hierzu wird in einem Ring ein Master-/Slave-Gerätepaar konfiguriert, das sich gegenseitig überwacht und den Datenverkehr im Fehlerfall von der im Regelfall genutzten Master-Ethernet-Verbindung zur Ausweich-(Slave-)Ethernet-Verbindung umleitet.

Standby-Redundanz

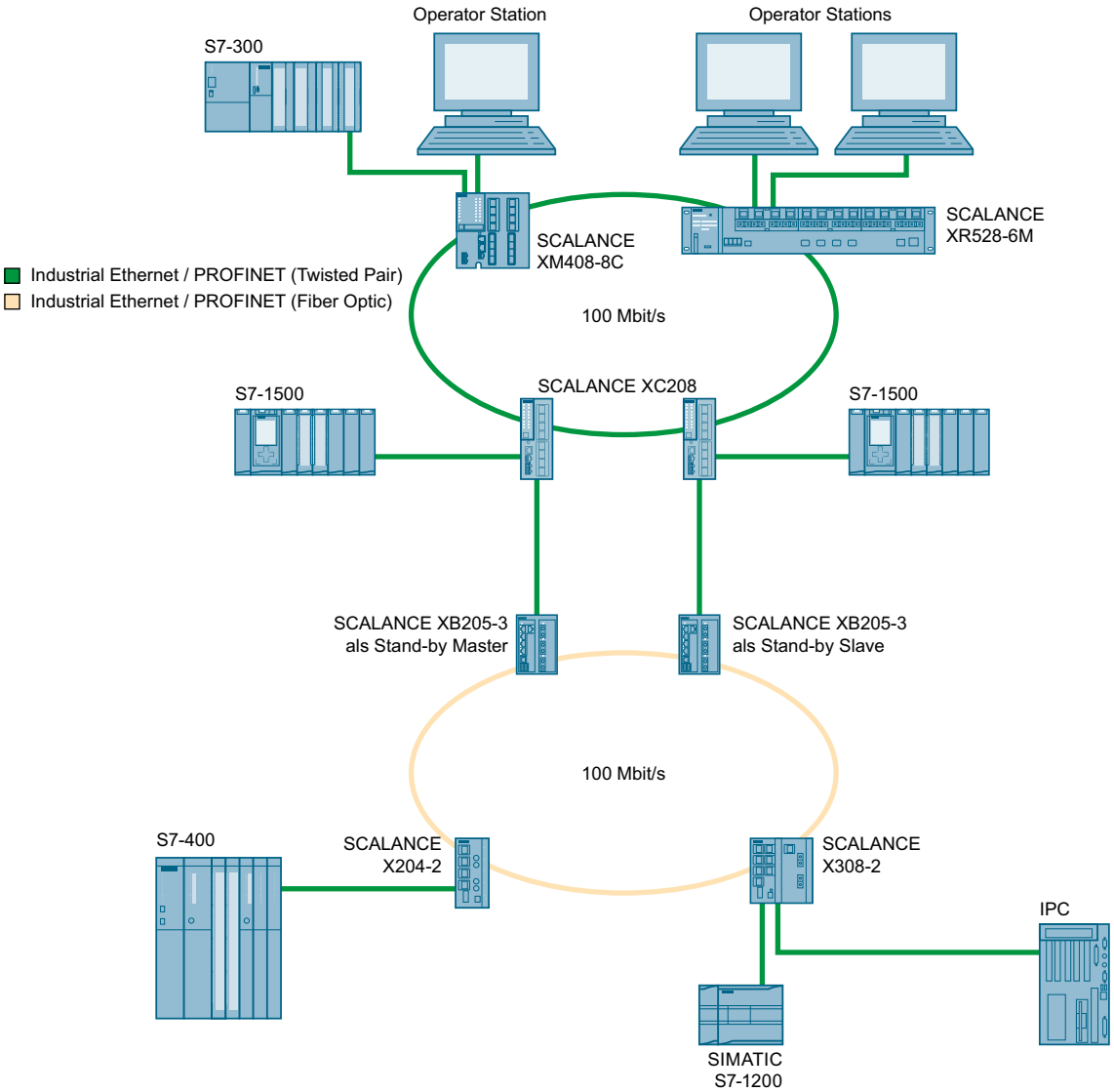


Bild 4-2 Beispiel einer redundanten Kopplung von zwei Ringen

Für eine redundante Kopplung, wie im Bild dargestellt, müssen zwei Geräte innerhalb eines Netzsegments als Standby-Redundanz-Switches projektiert werden. Netzsegmente sind hier Ringe mit einem Redundanzmanager. An die Stelle der Ringe können dabei auch Netzsegmente in Linien-Form treten.

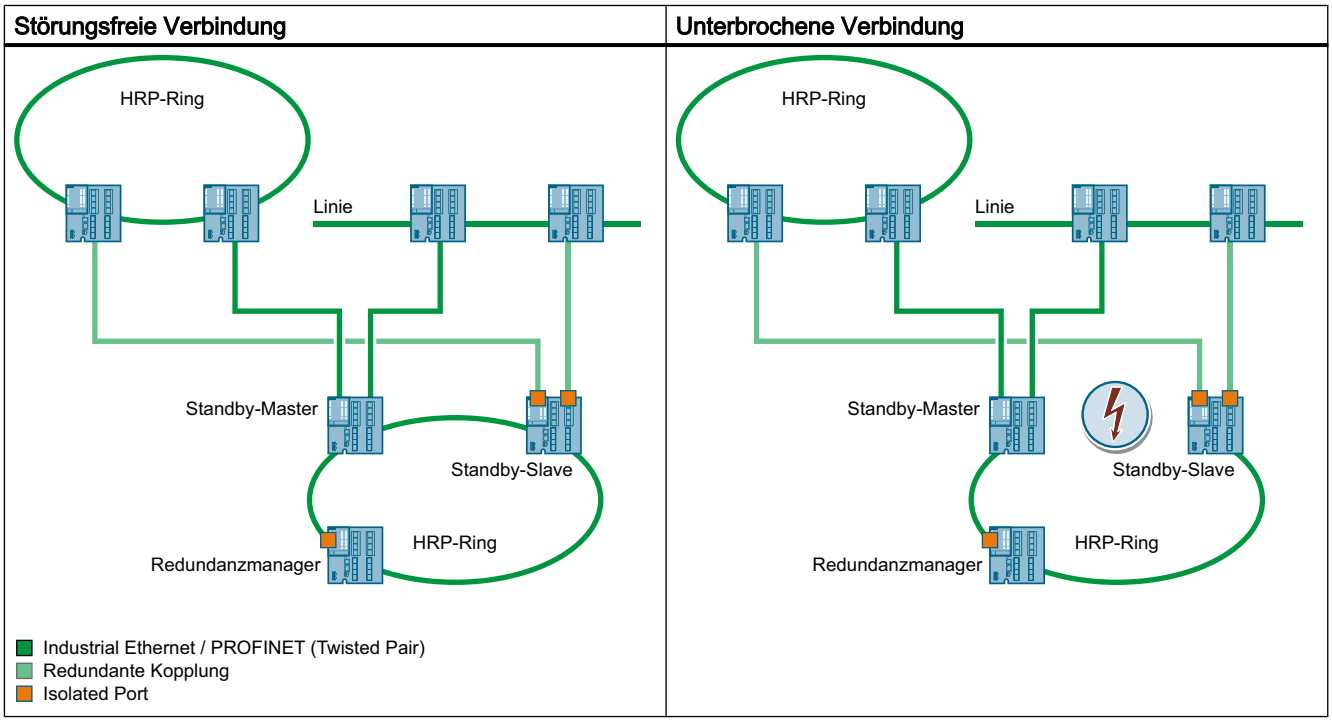
Die beiden per Projektierung verbundenen Standby-Redundanz-Switches tauschen Datentelegramme miteinander aus und synchronisieren damit ihren Betriebsstatus (ein Gerät wird Master und das andere Slave). Im fehlerfreien Zustand ist nur beim Master die Koppelstrecke zum anderen Netzsegment aktiv. Fällt diese Koppelstrecke aus (z.B. infolge eines Link-Down oder eines Geräteausfalls), so aktiviert der Slave seine Koppelstrecke, solange der Fehler ansteht.

Kopplung mehrerer HRP-Netzsegmente

Wenn Sie mehrere HRP-Ringe oder Linien über Standby-Redundanz verbinden, müssen sich der Standby-Master und der Standby-Slave in einem geschlossenen Netzsegment befinden. Dieses Netzsegment darf keinesfalls offen, d. h. eine Linie, sein.

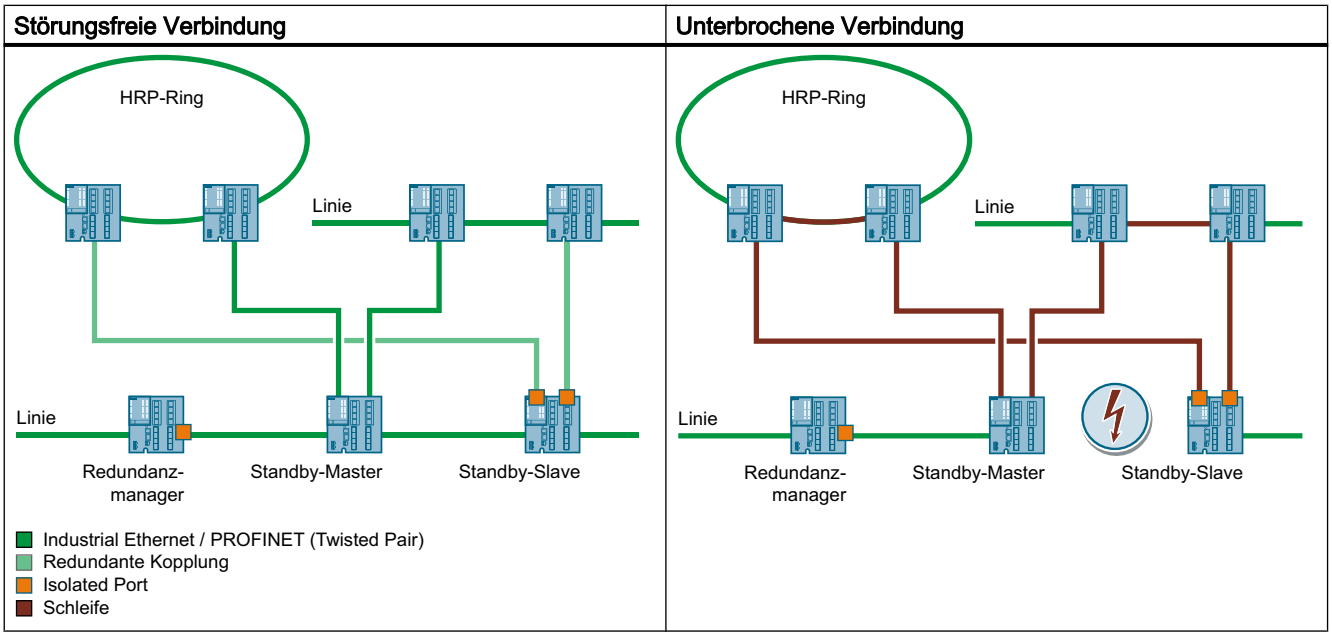
Standby-Master und -Slave in einem geschlossenen Netzsegment

Wenn die Verbindung zwischen Standby-Master und -Slave unterbrochen wird, können die beiden Geräte weiterhin über die redundante Strecke des HRP-Redundanzmanagers kommunizieren.



Standby-Master und -Slave in einem offenen Netzsegment

Wenn die Verbindung zwischen Standby-Master und -Slave unterbrochen wird, können die beiden Geräte nicht mehr kommunizieren. Dies führt zu einer Schleife über die gekoppelten Netzsegmente.



4.4.6 Parallel Redundancy Protocol

Parallel Redundancy Protocol

Das "Parallel Redundancy Protocol" (PRP) ist ein Redundanzprotokoll für Ethernet-Netzwerke. Es ist im Teil 3 des IEC 62439 Standards definiert. Dieses Redundanzverfahren ermöglicht bei Netzwerkunterbrechungen die Datenkommunikation ohne Unterbrechung/Rekonfigurationszeit aufrechtzuerhalten.

Das PRP-Verfahren wird z. B. von den Geräten der Produktlinie SCALANCE X-200RNA unterstützt.

Überlange Frames

Beim Versenden von PRP-Frames erweitert der IE-Switch das Frame um einen PRP-Trailer. Bei Frames mit maximaler Länge entsteht durch den angehängten PRP-Trailer ein überlanges Frame, das die zulässige Framelänge überschreitet (nach IEEE 802.3-Standard).

Um Datenverluste bei überlangen Frames auszuschließen, müssen alle Netzkomponenten, die sich in einem PRP-Netzwerk befinden, eine Framelänge von mindestens 1528 Bytes unterstützen.

Die Geräte, die in diesem Handbuch beschrieben sind, können in PRP-Netzwerken eingesetzt werden, siehe auch Kapitel "Mengengerüst (Seite 27)".

4.4.7 DLR

DLR (Device Level Ring) ist das Redundanzverfahren des Protokolls EtherNet/IP. Die IE-Switches können auch in einem Ring verwendet werden, in dem das Redundanzverfahren DLR genutzt wird. Welche IE-Switches DLR unterstützen, entnehmen Sie der Tabelle mit den Systemfunktionen (Seite 15). Ein IE-Switch verhält sich entsprechend den Vorgaben der Open DeviceNet Vendor Association (ODVA) wie ein "Non-DLR Device". Die folgenden Abschnitte beschreiben die notwendigen Konfigurationsschritte, damit die Nutzung mit DLR problemlos funktioniert.

DLR-kompatible Werkseinstellungen

Für die folgenden Parameter ist keine Änderung der Werkseinstellungen erforderlich:

- Übertragungsmodus "Auto negotiation" mit 10/100 MBit/s
- Auto MDI-X
- Weiterleitungs-Warteschlange mit hoher Priorität für DLR-Pakete

Stellen Sie sicher, dass die Werkseinstellungen für diese Parameter nicht verändert wurden und konfigurieren Sie die folgenden Einstellungen.

EtherNet/IP aktivieren

Aktivieren Sie EtherNet/IP für das Gerät.

Sie aktivieren EtherNet/IP auf der folgenden WBM-Seite:

System > EtherNet/IP

Priorisierungsmodus für die DLR-Ports konfigurieren

Konfigurieren Sie für die Ports, die mit dem DLR verbunden sind, den Priorisierungsmodus "Priorisierung nach DSCP".

Sie konfigurieren den Priorisierungsmodus auf der folgenden WBM-Seite:

Layer 2 > QoS > QoS-Priorisierung > Priorisierungsmodus

Base Bridge-Modus konfigurieren

Für das Gerät muss ein VLAN projektiert sein, das dem DLR-VLAN entspricht (gleiche VLAN-ID). Dafür muss für das Gerät der Base Bridge-Modus "802.1Q VLAN Bridge" aktiviert sein.

Sie konfigurieren den Base Bridge-Modus "802.1Q VLAN Bridge" auf der folgenden WBM-Seite:

Layer 2 > VLAN > Allgemein > Base Bridge-Modus

DLR-Ports als Tagged Member im DLR-VLAN konfigurieren

Die DLR-Ports müssen Tagged Member in dem DLR-VLAN sein.

Sie konfigurieren die DLR-Ports als Tagged Member im DLR-VLAN, indem Sie auf der folgenden WBM-Seite für die DLR-Ports den Eintrag "M" konfigurieren:

Layer 2 > VLAN > Allgemein > Liste der Ports

Ringredundanz und Spanning Tree für DLR-Ports deaktivieren

Deaktivieren Sie Ringredundanz und Spanning Tree für die Ports, die mit dem DLR verbunden sind. Sie verhindern dadurch, dass diese Ports blockiert werden.

Sie deaktivieren die Ringredundanz auf der folgenden WBM-Seite:

Layer 2 > Ringredundanz > Ring > Ringredundanz

Sie deaktivieren Spanning Tree auf der folgenden WBM-Seite:

Layer 2 > Spanning Tree > CIST-Port > Spanning Tree-Status

Statische Multicast-Adressen für DLR-Ports konfigurieren

Legen Sie fest, dass die folgenden drei Multicast-Adressen nur an die beiden Ports weitergeleitet werden, die mit dem DLR verbunden sind:

- 01-21-6C-00-00-01 (Beacons)
- 01-21-6C-00-00-02 (Neighbor check)
- 01-21-6C-00-00-03 (Announce frames)

Multicast-Adressen konfigurieren Sie auf der folgenden WBM-Seite:

Layer 2 > Multicast > Gruppen

Multicast-Blocking für die DLR-Ports deaktivieren

Deaktivieren Sie für die Ports, die mit dem DLR verbunden sind, die Funktion Multicast-Blocking.

Sie deaktivieren Multicast-Blocking auf der folgenden WBM-Seite:

Layer 2 > Multicast > Blocking

Unicast-Learning für DLR-Ports deaktivieren

Deaktivieren Sie Unicast-Learning für die Ports, die mit dem DLR verbunden sind. Dadurch verhindern Sie den unerwünschten Verlust von Unicast-Telegrammen, die zur Rekonfiguration des Rings oder zum Zweck der Fehlersuche versendet werden. Sie deaktivieren das Unicast-Learning mit dem folgenden CLI-Befehl im Interface Konfigurationsmodus:

```
no unicast mac learning
```

Detailinformationen zu diesem Befehl finden Sie im Projektierungshandbuch Command Line Interface (CLI).

Wenn das Unicast-Learning deaktiviert ist, werden eingehende Datenpakete an alle Ports weitergeleitet. Entgegen den Empfehlungen der ODVA ist es deshalb nicht erforderlich, die MAC-Adresse des DLR-Supervisors zu konfigurieren.

4.5 VLAN

4.5.1 Grundlagen

Netzwerkdefinition unabhängig von der räumlichen Lage der Teilnehmer

VLAN (Virtual Local Area Network) teilt ein physikalisches Netzwerk in mehrere logische Netzwerke, die voneinander abgeschirmt sind. Hierbei werden Geräte zu logischen Gruppen zusammengefasst. Nur Teilnehmer des gleichen VLANs können sich untereinander adressieren. Da auch Multicast- und Broadcast-Telegramme nur innerhalb des jeweiligen VLANs weitergeleitet werden, wird von Broadcast-Domänen gesprochen.

Daraus ergibt sich als besonderer Vorteil von VLANs eine geringere Netzlast für die Teilnehmer bzw. Netzsegmente anderer VLANs.

Für die Kennung, welches Paket welchem VLAN zugeordnet ist, wird das Telegramm um 4 Byte erweitert (VLAN-Tagging (Seite 54)). Diese Erweiterung enthält neben der VLAN-ID auch Prioritätsinformationen.

Möglichkeiten der VLAN-Zuordnung

Jedem Port eines Geräts wird eine VLAN-ID zugewiesen (Port-basiertes VLAN). Port-basiertes VLAN konfigurieren Sie unter "Layer 2 > VLAN > Port-basiertes VLAN (Seite 240)".

4.5.2 VLAN-Tagging

Erweiterung der Ethernet-Telegramme um vier Byte

Für CoS (Class of Service, Telegrammpriorisierung) und für VLAN (Virtuelles Netzwerk) wurde in der Norm IEEE 802.1Q die Erweiterung der Ethernet-Telegramme um das VLAN-Tag festgelegt.

Hinweis

Durch das VLAN-Tag erhöht sich die zulässige Gesamtlänge des Telegramms von 1518 auf 1522 Byte.
Es muss geprüft werden, ob die Endteilnehmer im Netz diese Länge / diesen Telegrammtyp verarbeiten können. Ist dies nicht der Fall, dürfen an diese Teilnehmer nur Telegramme mit der Standardlänge gesendet werden.

Die zusätzlichen 4 Bytes befinden sich im Header des Ethernet-Telegramms zwischen der Quelladresse und dem Ethernet-Typ-/Längenfeld:

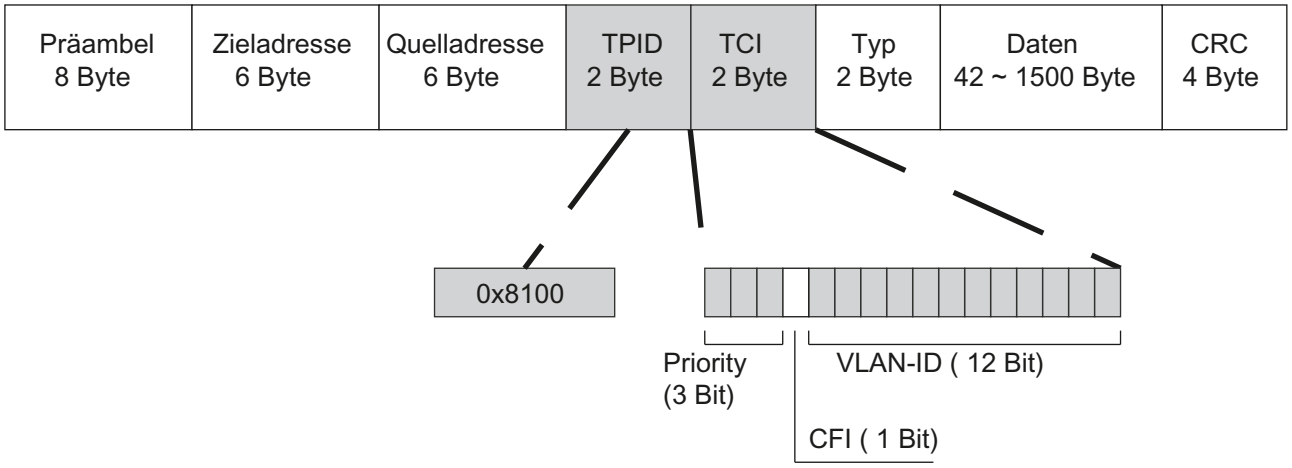


Bild 4-3 Aufbau des erweiterten Ethernet-Telegramms

Die zusätzlichen Bytes beinhalten den Tag Protocol Identifier (TPID) und die Tag Control Information (TCI).

Tag Protocol Identifier (TPID)

Die ersten 2 Bytes bilden den Tag Protocol Identifier (TPID) und sind fest mit 0x8100 belegt. Dieser Wert gibt an, dass das Datenpaket VLAN-Informationen oder Prioritätsangaben beinhaltet.

Tag Control Information (TCI)

Die 2 Bytes der Tag Control Information (TCI) beinhalten folgende Informationen:

CoS-Priorisierung

In dem getaggten Telegramm gibt es 3 Bits für die Priorität, die auch als Class of Service (CoS) bezeichnet werden, siehe auch IEEE 802.1Q.

CoS-Bits	Priorität	Art des Datenverkehrs
000	0 (niedrigste)	Background (Hintergrund)
001	1	Best Effort
010	2	Excellent Effort
011	3	Critical Applications (Kritische Anwendungen)
100	4	Video, < 100 ms Verzögerung (Latenz und Jitter)
101	5	Voice (Sprache), < 10 ms Verzögerung (Latenz und Jitter)
110	6	Internetwork Control
111	7 (höchste)	Network Control

Die Priorisierung der Datenpakete setzt eine Warteschlange in den Komponenten voraus, in der sie die Datenpakete mit der niedrigeren Priorität puffern können.

Das Gerät besitzt mehrere parallele Warteschlangen, in denen die verschieden priorisierten Telegramme abgearbeitet werden. Standardmäßig werden zuerst die Telegramme mit der höchsten Priorität abgearbeitet. Dieses Verfahren gewährleistet auch bei einem hohen

Datenaufkommen, dass die Telegramme mit der höchsten Priorität auf jeden Fall gesendet werden.

Canonical Format Identifier (CFI)

Der CFI wird für die Kompatibilität zwischen Ethernet und Token Ring benötigt.
Die Werte haben folgende Bedeutung:

Wert	Bedeutung
0	Das Format der MAC-Adresse ist kanonisch. Bei kanonischer Darstellung der MAC-Adresse wird das niederwertigste Bit zuerst übertragen. Standardeinstellung für Ethernet-Switches.
1	Das Format der MAC-Adresse ist nicht kanonisch.

VLAN-ID

Im 12 Bit-Datenfeld können bis zu 4096 VLAN-IDs gebildet werden. Dabei gelten folgende Festlegungen:

VLAN-ID	Bedeutung
0	Das Telegramm beinhaltet nur Prioritätsinformation (Priority Tagged Frames) und keine gültige VLAN-Kennung.
1 - 4094	Gültige VLAN-Kennung, das Telegramm ist einem VLAN zugeordnet, es kann zusätzlich auch Prioritätsinformationen beinhalten.
4095	Reserviert

4.5.3 Private VLAN

Mit einem Private VLAN (PVLAN) können Sie die Layer 2-Broadcastdomäne eines VLANs unterteilen.

Ein Private VLAN besteht aus folgenden Einheiten:

- Einem Primary Private VLAN (Primary PVLAN)
  Das VLAN, das unterteilt wird, wird Primary Private VLAN genannt.
- Secondary Private VLANs (Secondary PVLAN)
  Secondary PVLANs existieren nur innerhalb eines Primary PVLANs. Jedes Secondary PVLAN hat eine spezifische VLAN-ID und ist mit dem Primary PVLAN verbunden. Secondary PVLANs werden in folgende Typen unterteilt:
  - Isolated Secondary PVLAN
    Geräte innerhalb eines Isolated Secondary PVLANs können nicht über Layer 2 miteinander kommunizieren.
  - Community Secondary PVLAN
    Geräte innerhalb eines Community Secondary PVLANs können über Layer 2 direkt miteinander kommunizieren. Die Geräte können nicht mit Geräten in anderen Communities des PVLANs über Layer 2 kommunizieren.

Hinweis

VLAN-ID bei Secondary PVLANs

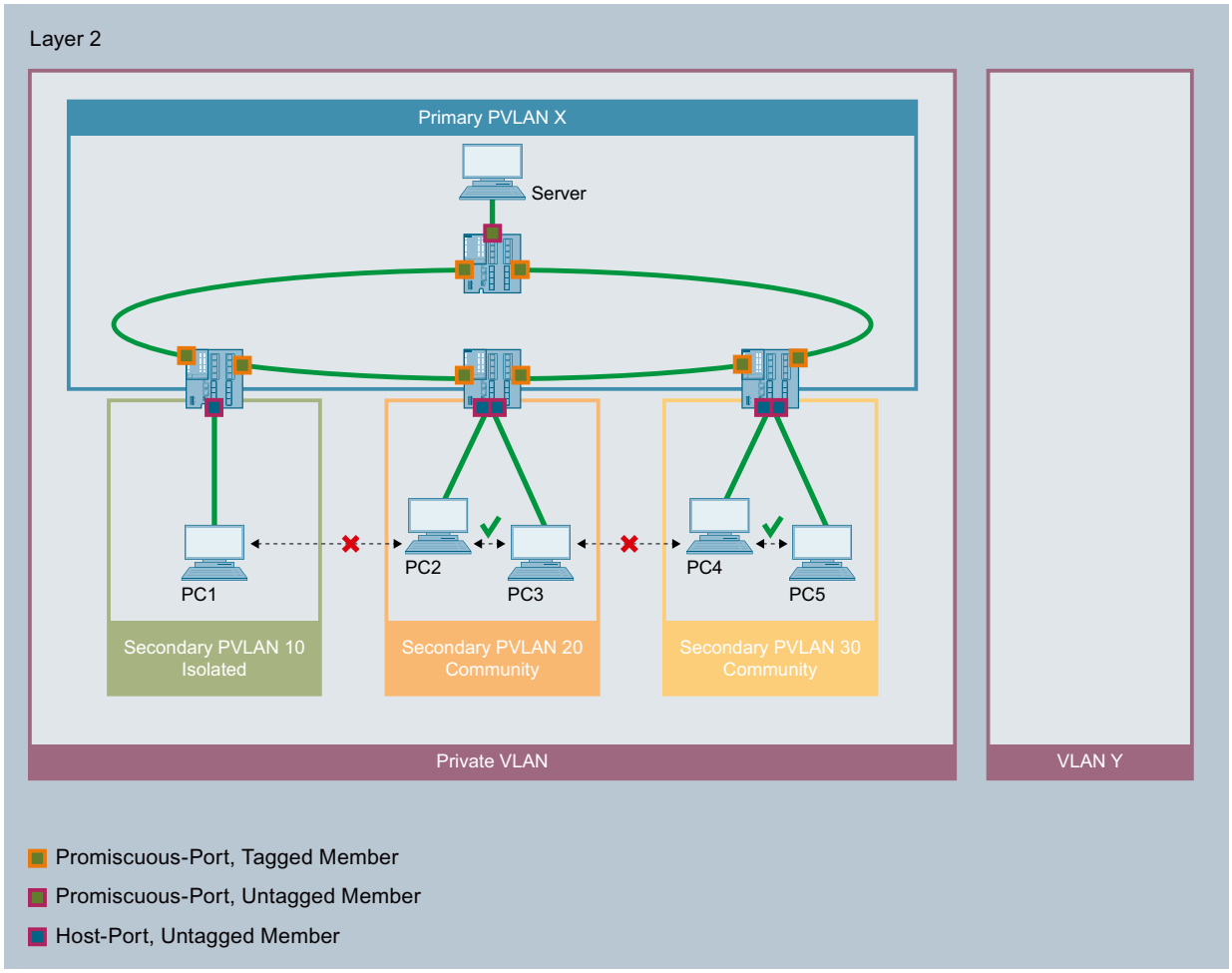
Wenn Sie auf unterschiedlichen IE-Switches die gleiche VLAN-ID für Secondary PVLANs verwenden, können die Endgeräte in diesen Secondary PVLANs switchübergreifend über Layer 2 miteinander kommunizieren.

Hinweis

Private VLAN-Funktionalität und RADIUS-Authentifizierung

Wenn die VLAN-Zuweisung über RADIUS-Authentifizierung für einen oder mehrere Ports eines VLAN aktiviert ist, sollten Sie dieses VLAN nicht zusätzlich als Private VLAN konfigurieren.

Die Private VLAN-Funktionalität in Zusammenhang mit der VLAN-Zuweisung über RADIUS-Authentifizierung kann zu einem inkonsistenten Systemzustand führen.



In diesem Beispiel sind die Ports der IE-Switches, die sie mit anderen IE-Switches verbinden, Promiscuous-Ports. Diese Netzwerkports sind Tagged Member in allen PVLANs: Primary PVLAN und allen Secondary PVLANs.

Die Ports, an denen die PCs angeschlossen sind, sind Host-Ports. Die Host-Ports sind jeweils Untagged Member im Primary PVLAN und in ihrem entsprechenden Secondary PVLAN.

Der Port, an dem der Server angeschlossen ist, ist ein Promiscuous Port. Dieser Promiscuous Port ist Untagged Member in allen PVLANs: Primary PVLAN und allen Secondary PVLANs.

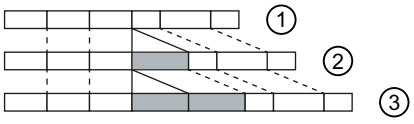
In diesem Beispiel können alle PCs mit dem Server kommunizieren. Der Server kann mit allen PCs kommunizieren. Der PC1 kann mit keinem anderen PC kommunizieren. Die PCs innerhalb eines Community Secondary PVLANs können miteinander kommunizieren, jedoch nicht mit den PCs in einem anderen Secondary PVLAN.

4.5.4 VLAN-Tunnel

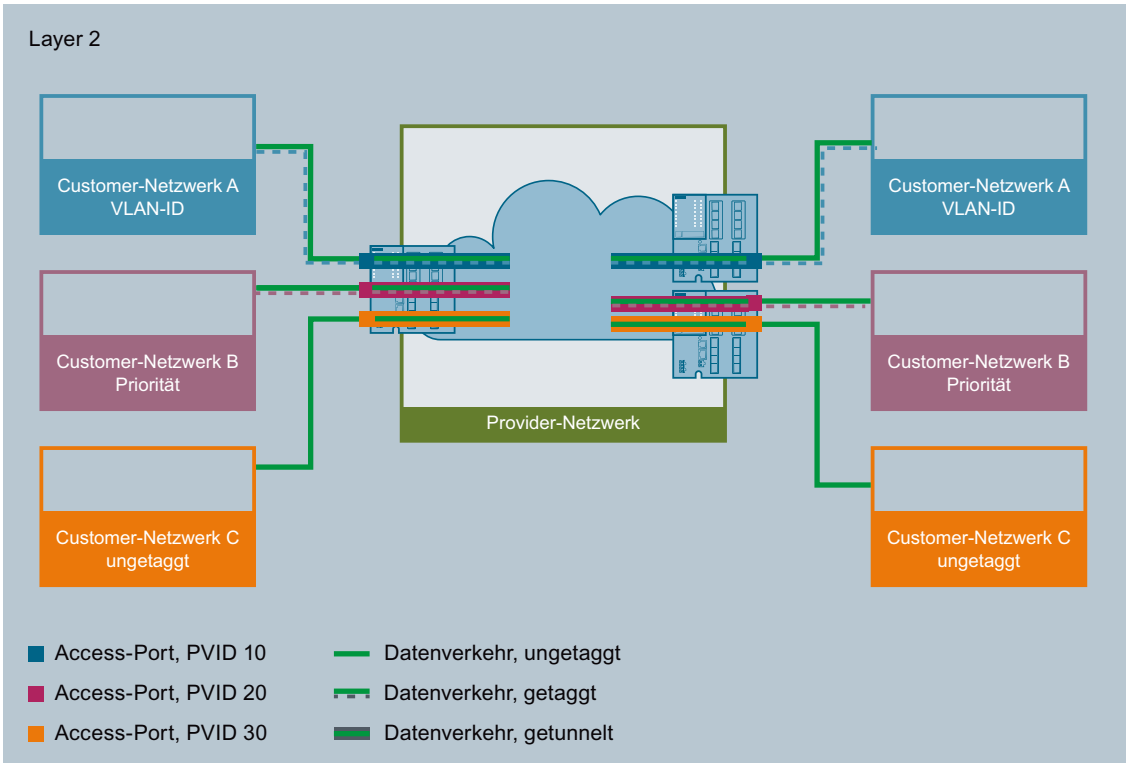
Mit der Funktion Q-in-Q VLAN-Tunnel ist es möglich, den Datenverkehr von verschiedenen Customer-Netzwerken mittels VLAN-Tunnel über ein Provider-Netzwerk weiterzuleiten. Dabei kann jedes Customer-Netzwerk über die volle Anzahl an möglichen VLANs verfügen.

Ein VLAN-Tunnel wird zwischen Provider-Switches aufgebaut, die an den Grenzen eines Provider-Netzwerks konfiguriert sind. Ein Provider-Switch verfügt über die folgenden Typen von Ports:

- Access-Port
  Über einen Access-Port ist der Provider-Switch mit einem Customer-Netzwerk verbunden.
  - Eingehender Datenverkehr
    Der eingehende Datenverkehr an einem Access-Port wird behandelt, als wäre er ungetagged ①. Alle eingehenden Telegramme werden um ein Tag mit der Port-VID des Access-Ports erweitert ②. Bei bereits getaggten Telegrammen bedeutet dies, dass sie um ein zweites 802.1Q-Tag erweitert werden ③, das äußere VLAN-Tag.

  - Ausgehender Datenverkehr
    Bei dem ausgehenden Datenverkehr an einem Access-Port wird das äußere VLAN-Tag wieder entfernt.
- Core-Port
  Über einen Core-Port ist der Provider-Switch mit einem Provider-Netzwerk verbunden. Core-Ports sind Mitglieder im Port-VLAN des Access-Ports oder mit dem Port-Typ "Switch-Port VLAN Trunk" konfiguriert.



In diesem Beispiel werden der Datenverkehr aus den Custmer-Nertzwerken A, B und C mittels VLAN-Tunnel über das Provider-Netzwerk weitergeleitet. Die Telegramme aus dem Customer-Netzwerk A sind mit einer VLAN-ID getaggt. Die Telegramme aus dem Customer-Netzwerk B sind mit einer Priorität getaggt. Die Telegramme aus dem Customer-Netzwerk C sind ungetaggt.

Wenn die Telegramme den entsprechenden Access-Port erreichen, werden sie um ein Tag mit der Port-VID des Access-Ports erweitert und durch das Provider-Netzwerk getunnelt. Sobald die Telegramme das Provider-Netzwerk velassen, wird das äußere VLAN-Tag (PVID) wieder entfernt. Die Telegramme werden in ihrer ursprünglichen Form weitergeleitet. Die Priorität des Telegramms bleibt dabei erhalten.

4.6 Mirroring

Das Gerät bietet die Möglichkeit, ein- oder ausgehende Datenströme parallel auf andere Schnittstellen zur Analyse oder Beobachtung auszuleiten. Dabei gibt es keine Rückwirkung auf die betrachteten Datenströme. Das Verfahren wird Mirroring genannt. In diesem Menüabschnitt schalten Sie das Mirroring ein oder aus und stellen die Parameter ein.

Ports spiegeln

Einen Port spiegeln bedeutet, dass der Datenverkehr an einem Port (gespiegelter Port) des IE-Switches auf einen anderen Port (Monitor-Port) kopiert wird. Sie können einen oder mehrere Ports auf einen Monitor-Port spiegeln.

Wird am Monitor-Port ein Protokollanalysator angeschlossen, kann damit der Datenverkehr am gespiegelten Port aufgezeichnet werden, ohne dass die Verbindung dort unterbrochen

wird. Dadurch ist eine rückwirkungsfreie Untersuchung des Datenverkehrs möglich. Voraussetzung hierfür ist, dass am Gerät ein freier Port als Monitor-Port zur Verfügung steht.

4.7 SNMP

Einleitung

Mit Hilfe des Simple Network Management Protocol (SNMP) überwachen und steuern Sie Netzwerkkomponenten, z. B. Router oder Switches, von einer zentralen Station aus. SNMP regelt dabei die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation.

Aufgaben von SNMP:

- Überwachung von Netzwerkkomponenten
- Fernsteuerung und Fernparametrierung von Netzwerkkomponenten
- Fehlererkennung und Fehlerbenachrichtigung

In den Versionen v1 und v2c verfügt SNMP über keine Sicherheitsmechanismen. Jeder Nutzer im Netzwerk kann mit geeigneter Software auf die Daten zugreifen und auch Parametrierungen verändern.

Für die einfache Steuerung von Zugriffsrechten ohne Sicherheitsaspekte werden Community-Strings verwendet.

Der Community-String wird zusammen mit der Anfrage übertragen. Wenn der Community-String korrekt ist, antwortet der SNMP-Agent und sendet die geforderten Daten. Wenn der Community-String nicht korrekt ist, verwirft der SNMP-Agent die Anfrage. Für Lese- und Schreibrechte definieren Sie verschiedene Community-Strings. Die Community-Strings werden in Klartext übertragen.

Standardwerte der Community-Strings:

- public
  besitzt nur Leserechte
- private
  besitzt Lese- und Schreibrechte

Hinweis

Da es sich bei den SNMP-Community Strings um einen Zugriffsschutz handelt, verwenden Sie nicht die Standardwerte "public" oder "private". Ändern Sie diese Werte nach der Erst-Inbetriebnahme.

Weitere einfache Schutzmechanismen auf Geräteebene:

- Allowed Host
  Dem überwachten System sind die IP-Adressen der überwachenden Systeme bekannt.
- Read Only
  Wenn Sie einem überwachten Gerät "Read Only" zuweisen, können Überwachungsstationen nur Daten auslesen, aber nicht ändern.

SNMP-Datenpakete sind nicht verschlüsselt und können einfach mitgelesen werden.

Die zentrale Station wird auch als Management-Station bezeichnet. Auf den zu überwachenden Geräten ist ein SNMP-Agent installiert, mit dem die Management-Station Daten austauscht.

Die Management-Station sendet Datenpakete folgenden Typs:

- GET
  Anfordern eines Datensatzes vom SNMP-Agent
- GETNEXT
  Ruft den nächsten Datensatz auf.
- GETBULK (verfügbar ab SNMPv2c)
  Fordert mehrere Datensätze auf einmal an, z. B. mehrere Zeilen einer Tabelle.
- SET
  Beinhaltet Parametrierungsdaten für das entsprechende Gerät.

Der SNMP-Agent sendet Datenpakete folgenden Typs:

- RESPONSE
  Der SNMP-Agent sendet die vom Manager angeforderten Daten zurück.
- TRAP
  Wenn ein bestimmtes Ereignis eintritt, sendet der SNMP-Agent eigenständig Traps.

SNMPv1/v2c/v3 verwenden UDP (User Datagram Protocol) und nutzen die UDP-Ports 161 und 162. Die Beschreibung der Daten erfolgt in einer Management Information Base (MIB).

SNMPv3

SNMPv3 führt gegenüber den Vorgängerversionen SNMPv1 und SNMPv2c ein umfangreicheres Sicherheitskonzept ein.

SNMPv3 unterstützt:

- Vollständig verschlüsselte Benutzerauthentifizierung
- Verschlüsselung des gesamten Datenverkehrs
- Zugriffskontrolle der MIB-Objekte auf Benutzer-/Gruppenebene

4.8 Quality of Service

Quality of Service (QoS) ist ein Verfahren, um die vorhandene Bandbreite in einem Netzwerk effizient zu nutzen.

QoS wird durch die Priorisierung des Datenverkehrs realisiert. Ankommende Frames werden nach einer bestimmten Priorisierung in eine Warteschlange (Queue) einsortiert und weiterverarbeitet. Dadurch wird bestimmten Frames Vorrang gewährt.

Die unterschiedlichen QoS-Verfahren beeinflussen sich gegenseitig und werden daher in folgender Reihenfolge berücksichtigt:

1. Der Switch prüft zunächst, ob es sich bei dem ankommenden Frame um ein Broadcast- oder Agent-Frame handelt.
   → Wenn die 1. Bedingung erfüllt ist, berücksichtigt der Switch die eingestellte Priorität auf der Seite "Allgemein (Seite 224)".
   Der Switch sortiert das Frame in eine Queue ein, entsprechend der Zuordnung auf der Seite "CoS-Zuordnung (Seite 226)".
2. Wenn die 1. Bedingung nicht erfüllt ist, prüft der Switch, ob das Frame ein VLAN-Tag enthält.
   → Wenn die 2. Bedingung erfüllt ist, prüft der Switch die Einstellungen zur Priorität auf der Seite "Allgemein (Seite 234)". Der Switch prüft, ob für die Priorität ein anderer Wert als "Nicht überschreiben" eingestellt ist.
   Wenn eine Priorität eingestellt ist, sortiert der Switch das Frame in eine Queue ein, entsprechend der Zuordnung auf der Seite "CoS-Zuordnung (Seite 226)".
3. Wenn die 2. Bedingung ebenfalls nicht erfüllt ist, werden die Frames entsprechend des Priorisierungsmodus weiterverarbeitet. Den Priorisierungsmodus konfigurieren Sie auf der Seite "QoS-Priorisierung (Seite 229)".

4.9 NAT/NAPT

Hinweis

NAT/NATP ist nur auf Layer 3 des ISO/OSI-Referenzmodells möglich. Zur Nutzung der NAT-Funktion müssen die Netze das IP-Protokoll verwenden.

Bei Verwendung des ISO-Protokolls, das auf Layer 2 arbeitet, ist keine Nutzung von NAT möglich.

Bei der Network Address Translation (NAT) werden IP-Subnetze in "Inside" und "Outside" unterteilt. Die Unterteilung erfolgt aus der Sicht einer NAT-Schnittstelle. Alle Netze, die über die NAT-Schnittstelle selbst erreichbar sind, gelten für diese Schnittstelle als "Outside". Alle Netze, die über andere IP-Schnittstellen des selben Geräts erreichbar sind, gelten für die NAT-Schnittstelle als "Inside".

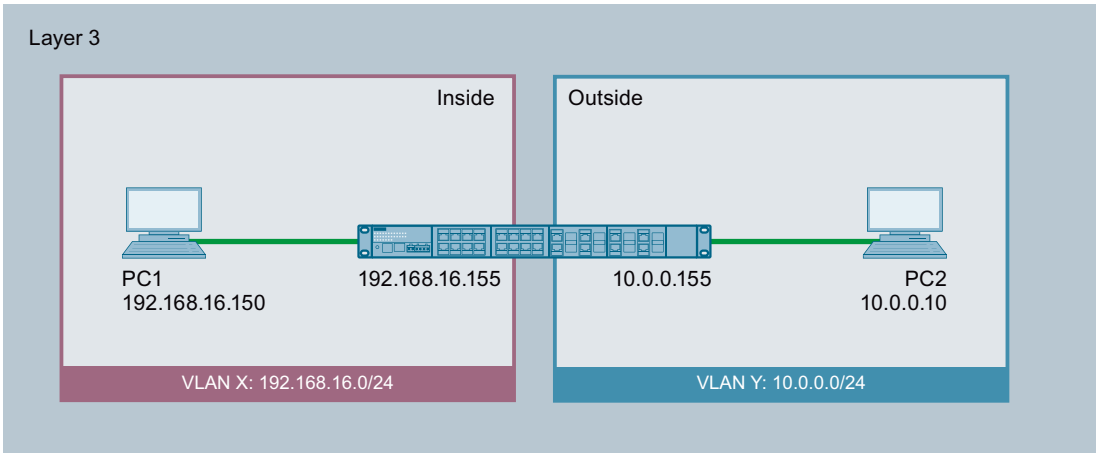
Wenn über eine NAT-Schnittstelle geroutet wird, werden die Quell- oder Ziel-IP-Adressen der übertragenen Datenpakete beim Übergang zwischen "Inside" und "Outside" geändert. Ob die Quell- oder Ziel-IP-Adresse geändert wird, ist von der Kommunikationsrichtung abhängig. Es wird immer die IP-Adresse des Kommunikationsteilnehmers angepasst, der sich "Inside"

befindet. Abhängig von der Perspektive wird die IP-Adresse eines Kommunikationsteilnehmers als "Local" oder "Global" bezeichnet.

		Perspektive	
		Local	**Global**
Position	**Inside**	Eine tatsächliche IP-Adresse, die einem Gerät im internen Netz zugewiesen ist. Diese Adresse ist aus dem externen Netz nicht erreichbar.	Eine IP-Adresse, unter der ein internes Gerät aus dem externen Netz erreichbar ist.
	Outside	Eine tatsächliche IP-Adresse, die einem Gerät im externen Netz zugewiesen ist. Da nur "Inside"-Adressen umgesetzt werden, wird nicht zwischen Outside Local und Outside Global unterschieden.	

Beispiel

In dem Beispiel werden zwei IP-Subnetze über einen IE-Switch miteinander verbunden. Die Unterteilung erfolgt aus der Sicht der NAT-Schnittstelle 10.0.0.155. Die Kommunikation von PC2 mit PC1 wird über NAT/NAPT umgesetzt.



Die tatsächliche IP-Adresse von PC1 (Inside Local) wird statisch mit NAT umgesetzt. Für PC2 ist PC1 unter der Inside Global Adresse erreichbar.

		Perspektive	
		Local	**Global**
Position	**Inside**	192.168.16.150	10.0.0.7
	Outside	10.0.0.10	

Die tatsächliche IP-Adresse von PC1 (Inside Local) wird mit NAPT (Network Address and Port Translation) umgesetzt. Für PC2 ist PC1 unter der Inside Global Adresse erreichbar.

		Perspektive	
		Local	**Global**
Position	**Inside**	192.168.16.150:80	10.0.0.7:80
	Outside	10.0.0.10:1660	

Rechenkapazität

Der Paketempfang des Geräts ist aufgrund der Lastbegrenzung zur CPU auf 300 Pakete pro Sekunde limitiert. Das entspricht einem maximalen Datendurchsatz von 1,7 MBit/s. Diese Lastbegrenzung gilt nicht pro Schnittstelle, sondern generell für alle Pakete, die zur CPU gehen.

Die gesamte NAT-Kommunikation läuft über die CPU und steht damit in Konkurenz zur IP-Kommunikation, die zur CPU geht, z. B. WBM und Telnet.

Beachten Sie, dass ein großer Teil der Rechenkapazität belegt ist, wenn Sie NAT einsetzen. Dadurch kann der Zugriff über Telnet oder WBM verlangsamt werden.

NAT

Mit "Network Address Translation" (NAT) wird die IP-Adresse in einem Datenpaket durch eine andere ersetzt. NAT wird in der Regel an einem Netzübergang zwischen einem internen Netz und einem externen Netz eingesetzt.

Beim Source-NAT wird die Inside Local-Quell-Adresse eines IP-Pakets von einem Gerät im internen Netz durch ein NAT-Gerät am Netzübergang in eine Inside Global-Adresse umgeschrieben.

Beim Destination-NAT wird die Inside Global-Ziel-Adresse eines IP-Pakets von einem Gerät im externen Net durch ein NAT-Gerät am Netzübergang in eine Inside Local-Adresse umgeschrieben.

Zur Übersetzung der internen in die externe IP-Adresse und zurück pflegt das NAT-Gerät eine Übersetzungsliste. Die Adresszuordnung kann dynamisch oder statisch sein. Sie konfigurieren NAT unter "Layer 3 (IPv4) > NAT (Seite 320)".

NAPT

Bei "Network Address Port Translation" (NAPT) werden mehrere interne IP-Adressen in die gleiche externe IP-Adresse umgeschrieben. Zur Identifikation der einzelnen Teilnehmer wird auch der Port des internen Geräts in der Übersetzungsliste des NAT-Geräts gespeichert und für die externe Adresse umgeschrieben.

Wenn mehrere interne Geräts über das NAT-Gerät eine Anfrage an die gleiche externe Ziel-IP-Adresse senden, trägt das NAT-Gerät jeweils seine eigene externe Quell-IP-Adresse in den Header dieser weitergeleiteten Telegramme ein. Da die weitergeleiteten Telegramme die gleiche externe Quell-IP-Adresse haben, ordnet das NAT-Gerät die Telegramme den Geräten über eine unterschiedliche Portnummer zu.

Wenn ein Gerät aus dem externen Netz einen Dienst im internen Netz nutzen möchte, muss die Übersetzungsliste für die statische Adresszuordnung konfiguriert werden. Sie konfigurieren NAPT unter "Layer 3 (IPv4) > NAT > NAPT (Seite 325)".

NAT/NAPT und IP-Routing

Sie können NAT/NAPT und IP-Routing gleichzeitig aktivieren. In diesem Fall müssen Sie die Erreichbarkeit interner Adressen aus externen Netzwerken durch ACL-Regeln regulieren.

4.10 Single-Hop Inter-VLAN-Routing

Einleitung

Ein physikalisches Netzwerk wird durch VLANs in Broadcastdomänen und Subnetze unterteilt.

Geräte (Hosts) innerhalb eines VLANs können über Layer 2 direkt miteinander kommunizieren. Die Telegramme werden anhand der MAC-Adresse an das entsprechende Gerät weitergeleitet.

Geräte aus unterschiedlichen VLANs können nicht über Layer 2 direkt miteinander kommunizieren. Der Datenverkehr muss anhand der IP-Adresse geroutet werden.

Mit der Funktion Single-Hop Inter-VLAN-Routing ist es möglich, dass Geräte aus unterschiedlichen VLANs miteinander kommunizieren, ohne dass ein Router benötigt wird.

Voraussetzungen

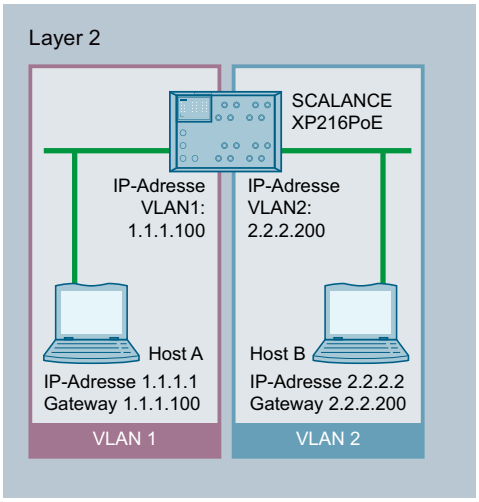
- Der IE-Switch kann mehrere IP-Schnittstellen verwalten.
- Der IE-Switch ist Mitglied in den VLANs, zwischen denen geroutet werden soll.
- Bei den Hosts ist die IP-Adresse des VLANs als Default-Gateway eingetragen.

Single-Hop Inter-VLAN-Routing

Der IE-Switch erhält ein Telegramm und erkennt, dass es an ein Gerät in einem anderen VLAN adressiert ist. Er leitet das Telegramm an den entsprechenden Port in dem VLAN weiter.

Der IE-Switch kennt nur VLANs, mit denen er direkt verbunden ist (Connected). Beim Single-Hop Inter-VLAN-Routing ist es daher nur möglich zwischen zwei lokalen IP-Schnittstellen zu routen.

Beispiel



In diesem Beispiel ist der Host A über das VLAN 1 mit dem IE-Switch verbunden. Host B ist über VLAN 2 mit dem IE-Switch verbunden. Bei Host A ist die IP-Adresse von VLAN 1 als Default-Gateway eingetragen. Bei Host B ist die IP-Adresse von VLAN 2 als Default-Gateway eingetragen.

Wenn die Funktion Single-Hop Inter-VLAN-Routing auf dem SCALANCE XP216PoE aktiviert ist, können Host A und Host B miteinander kommunizieren.

Konfigurieren mit dem Web Based Management 5

5.1 Web Based Management

Funktionsprinzip

Das Gerät verfügt über einen integrierten HTTP-Server für das Web Based Management (WBM). Wird das Gerät über einen Internet-Browser angesprochen, liefert es abhängig von den Benutzereingaben HTML-Seiten an den Client-PC zurück.

Der Benutzer trägt seine Konfigurationsdaten in die vom Gerät gesendeten HTML-Seiten ein. Das Gerät wertet diese Informationen aus und erzeugt dynamisch Antwortseiten.

Der Vorteil dieses Funktionsprinzips ist, dass auf der Client-Seite nur ein Internet-Browser erforderlich ist.

Hinweis

Sichere Verbindung

Das WBM bietet auch die Möglichkeit, eine gesicherte Verbindung via HTTPS herzustellen.

Verwenden Sie HTTPS für die geschützte Übertragung Ihrer Daten. Wenn Sie auf das WBM ausschließlich über eine sichere Verbindung zugreifen möchten, aktivieren Sie unter "System > Konfiguration" die Option "Nur HTTPS-Server".

Voraussetzungen

Darstellung des WBM

- Das Gerät verfügt über eine IP-Adresse.
- Zwischen dem Gerät und dem Client-PC besteht eine Verbindung. Mit dem Ping-Befehl können Sie prüfen, ob das Gerät erreichbar ist.
- Der Zugriff über HTTP(S) ist aktiviert.
- Im Internet-Browser ist JavaScript aktiviert.
- Der Internet-Browser darf nicht so eingestellt sein, dass er bei jedem Zugriff auf die Seite diese neu vom Server laden soll. Die Aktualität der dynamischen Seiteninhalte wird über andere Mechanismen sichergestellt. Beim Internet Explorer finden Sie eine entsprechende Einstellmöglichkeit im Menü "Extras > Internetoptionen > Allgemein" im Abschnitt "Browserverlauf" über die Schaltfläche "Einstellungen". Aktivieren Sie bei "Neuere Versionen der gespeicherten Seite suchen" "Automatisch".
- Wenn eine Firewall eingesetzt wird, müssen die entsprechenden Ports freigeschaltet sein.
  - Für den Zugriff über HTTP: TCP-Port 80
  - Für den Zugriff über HTTPS: TCP-Port 443

Die Darstellung des WBM wurde mit folgenden Desktop Internet-Browsern getestet:

- Microsoft Internet Explorer 11
- Mozilla Firefox 60
- Google Chrome V67

Hinweis

Kompatibilitätsansicht

Deaktivieren Sie im Microsoft Internet Explorer die Kompatibilitätsansicht, damit eine korrekte Darstellung gewährleistet und die einwandfreie Konfiguration über das WBM möglich ist.

Darstellung des WBM auf mobilen Geräten

Für mobile Geräte gelten folgende minimale Voraussetzungen:

Auflösung	Betriebssystem
960 x 640 Pixel	Android ab Version 4.2.1 iOS ab Version 6.0.2

Getestet mit folgenden Internet-Browsern für mobile Geräte:

- Apple Safari ab Version 8 auf iOS ab Version 8.1.3 (iPad Mini Model A1432)
- Google Chrome ab Version 40 auf Android ab Version 5.0.2 (Nexus 7C Asus)
- Mozilla Firefox ab Version 35 auf Android ab Version 5.0.2 (Nexus 7C Asus)

Hinweis

Seitendarstellung und Bedienung des WBM auf mobilen Geräten

Die Darstellung und Bedienung der WBM-Seiten auf mobilen Geräten kann von der Darstellung und Bedienung derselben Seiten auf Desktop-Geräten abweichen. Einige Seiten liegen auch in einer für mobile Geräte optimierten Darstellung vor.

5.2 Login

Verbindung zu einem Gerät herstellen

Führen Sie folgende Schritte durch, um mit einem Internet-Browser eine Verbindung zu einem Gerät herzustellen:

1. Zwischen dem Gerät und dem Client-PC besteht eine Verbindung. Mit dem Ping-Befehl können Sie prüfen, ob das Gerät erreichbar ist.
2. Geben Sie im Adressfeld des Internet-Browsers die IP-Adresse oder die URL des Geräts ein. Wenn eine Verbindung zum Gerät besteht, erscheint die Anmeldeseite des Web Based Managements (WBM).

Anmeldung mit Hilfe des Internet-Browsers

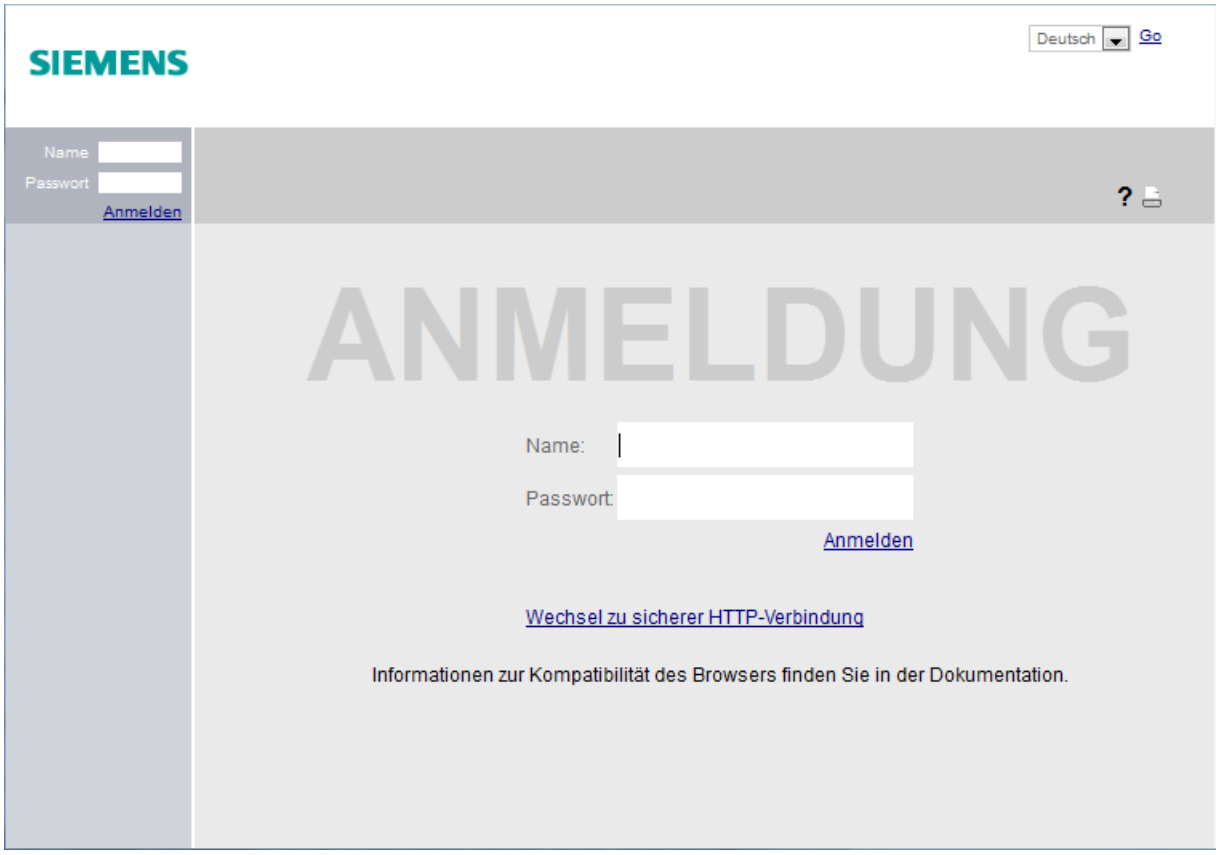
Auswahl der Sprache des WBM

1. Wählen Sie aus der Klappliste im oberen rechten Bereich die Sprachversion der WBM-Seiten aus.
2. Klicken Sie auf die Schaltfläche "Go", um zur ausgewählten Sprache zu wechseln.

Hinweis

Verfügbare Sprachen

In dieser Version sind Deutsch und Englisch verfügbar.



Anmeldung über HTTP

Sie haben zwei Möglichkeiten, sich über HTTP anzumelden. Entweder benutzen Sie die Anmeldemöglichkeit in der Mitte des Browser-Fensters oder die Anmeldemöglichkeit im linken oberen Bereich des Browser-Fensters. Für beide Möglichkeiten gelten die gleichen Schritte.

Bei einem Gerät mit Werkseinstellungen anmelden

Wenn Sie sich das erste Mal oder nach einem Wiederherstellen der Werkseinstellungen anmelden, gehen Sie wie folgt vor:

1. Geben Sie im Eingabefeld "Name" den werkseitig voreingestellten Benutzer "admin" ein. Mit diesem Benutzerkonto können Sie Einstellungen des Geräts verändern (lesender und schreibender Zugriff auf die Konfigurationsdaten).

   Hinweis

   Werkseitig voreingestellter Benutzer "user"

   Ab der Firmware-Version 2.1 ist der werkseitig voreingestellte Benutzer "user" im Auslieferzustand nicht mehr verfügbar.

   Wenn Sie ein Gerät auf die Firmware V2.1 aktualisieren, ist der Benutzer "user" zunächst noch verfügbar. Wenn Sie das Gerät auf die Werkseinstellungen zurücksetzen ("Auf Werkseinstellungen zurücksetzen und Neustart"), wird der Benutzer "user" gelöscht.

   Sie können Benutzer mit der Rolle "user" anlegen.

2. Geben Sie im Eingabefeld "Passwort" das Passwort des werkseitig voreingestellten Benutzers "admin" ein: "admin".
3. Klicken Sie auf die Schaltfläche "Anmelden" oder bestätigen Sie die Eingabe mit "Enter". Die folgende Seite erscheint.

4. Geben Sie im Feld "Aktuelles Benutzerpasswort" erneut das Passwort des werkseitig voreingestellten Benutzers "admin" ein.
5. Geben Sie im Feld "Neuer Name für das Admin-Benutzerkonto" ggf. einen neuen Benutzernamen ein.
   Wenn Sie sich das erste Mal oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" anmelden, können Sie einmalig den werksseitig voreingestellten Benutzer "admin" umbenennen. Danach ist ein Umbenennen von "admin" nicht mehr möglich.

6. Geben Sie im Feld "Neues Passwort" das neue Passwort für den Benutzer ein.
   Das neue Passwort muss die folgenden Passwortrichtlinien erfüllen:
   - Passwortlänge: mindestens 8 Zeichen, maximal 32 Zeichen
   - Mindestens 1 Großbuchstabe
   - Mindestens 1 Sonderzeichen
   - Mindestens 1 Zahl
7. Geben Sie im Feld "Passwort bestätigen" das Passwort erneut ein. Beide Passworteingaben müssen übereinstimmen.
   Klicken Sie auf die Schaltfläche "Einstellungen übernehmen", um den Vorgang abzuschließen und das neue Passwort zu aktivieren.

Wenn Sie sich erfolgreich angemeldet haben, erscheint die Startseite.

Bei einem konfigurierten Gerät anmelden

Wenn Sie sich bei einem konfigurierten Gerät anmelden, gehen Sie wie folgt vor:

1. Geben Sie im Eingabefeld "Name" den Benutzernamen des angelegten Benutzerkontos ein.
   Lokale Benutzerkonten konfigurieren Sie unter "Security > Benutzer".
2. Geben Sie im Eingabefeld "Passwort" des entsprechenden Benutzerkontos ein.
3. Klicken Sie auf die Schaltfläche "Anmelden" oder bestätigen Sie die Eingabe mit "Enter".

Wenn Sie sich erfolgreich angemeldet haben, erscheint die Startseite.

Anmeldung über HTTPS

Wenn Sie sich über HTTPS mit dem Gerät verbinden möchten, gehen Sie wie folgt vor:

1. Klicken Sie auf den Link "Wechsel zu sicherer HTTP-Verbindung" in der Anmeldeseite oder geben Sie im Adressfeld des Internet-Browsers "https://" und die IP-Adresse des Geräts ein.
2. Prüfen Sie die angezeigte Zertifikatswarnung und bestätigen Sie diese gegebenenfalls. Die Anmeldeseite des Web Based Management erscheint.
3. Folgen Sie danach den Anweisungen unter "Anmeldung über HTTP".

5.3 Das Menü "Information"

5.3.1 Startseite

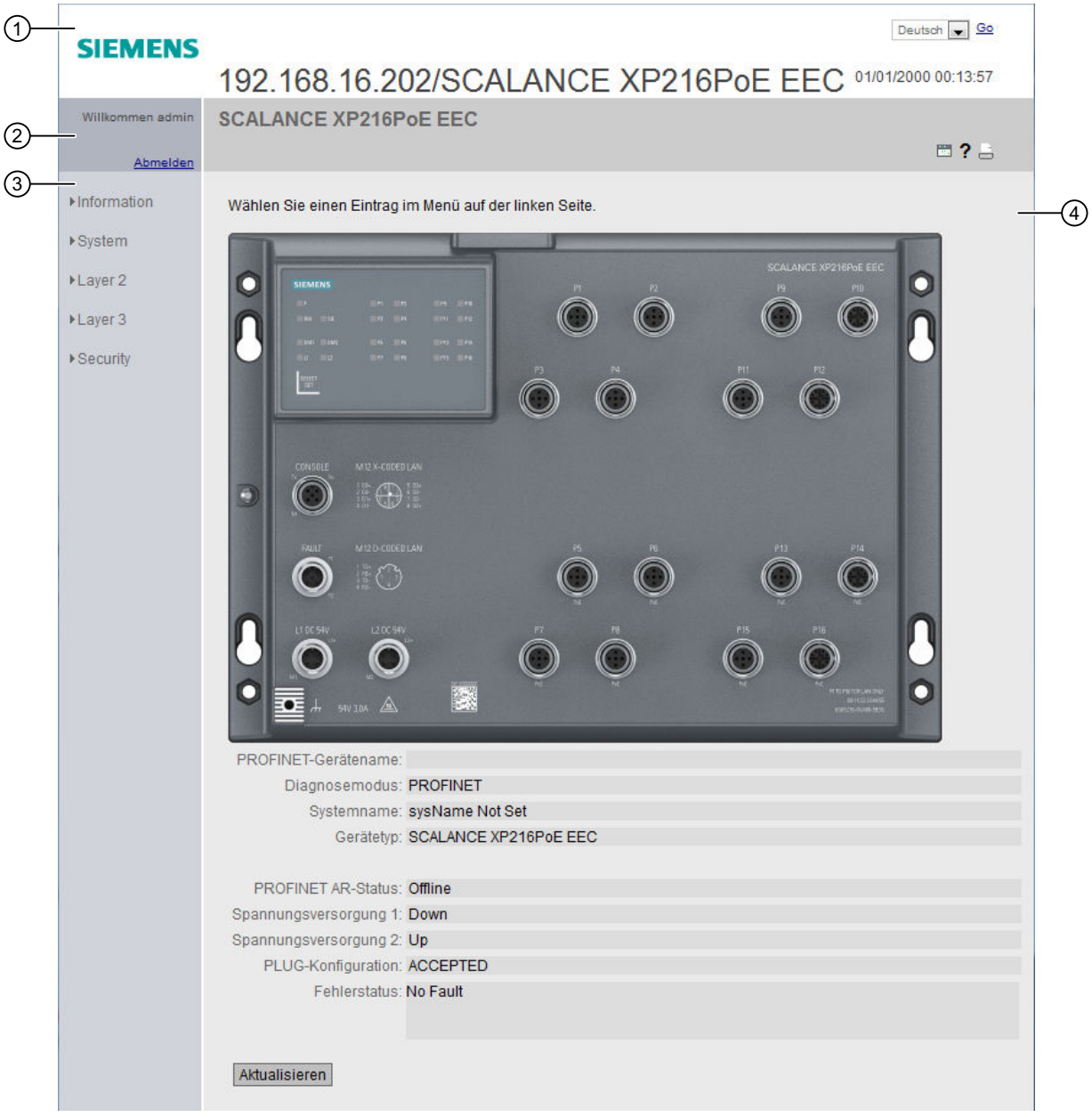
Ansicht der Startseite

Wenn Sie die IP-Adresse des Geräts eingeben, dann wird Ihnen nach erfolgreicher Anmeldung die Startseite angezeigt. Sie können auf dieser Seite keine Konfigurationen vornehmen.

Allgemeiner Aufbau der WBM-Seiten

Ihnen stehen allgemein folgende Bereiche auf jeder WBM-Seite zur Verfügung:

- Auswahlbereich (1): Oberer Bereich
- Anzeigebereich (2): Oberer Bereich
- Navigationsbereich (3): Linker Bereich
- Inhaltsbereich (4): Mittlerer Bereich



Auswahlbereich (1)

Im Auswahlbereich wird Ihnen Folgendes angeboten:

- Logo der Siemens AG
  Wenn Sie auf das Logo klicken, gelangen Sie auf die Internetseite des entsprechenden Grundgeräts im Siemens Industry Online Support.
- Anzeige von: "Gerätestandort / Systemname"
  - "Gerätestandort" enthält die Ortsangabe des Geräts.
    Im Auslieferzustand wird die IP-Adresse angezeigt.
  - "Systemname" ist der Gerätename.
    Im Auslieferzustand wird der Gerätetyp angezeigt.

  Den Inhalt dieser Anzeige können Sie unter "System > Allgemein > Gerät" ändern.
- Klappliste für die Sprachauswahl
- Systemdatum und Systemzeit mit Statusanzeige
  Den Inhalt dieser Anzeige können Sie unter "System > Systemzeit" ändern.
  Wenn die Systemzeit nicht eingestellt ist, ist der Status . Ist die Systemzeit konfiguriert, aber die Systemzeit ist nicht synchronisierbar, ist ein gelbes Warndreieck zu sehen. Prüfen Sie, ob der Zeitserver erreichbar ist. Passen Sie gegebenfalls Ihre Projektierung an. Wenn die Systemzeit eingestellt und/oder synchronisierbar ist, ist der Status .

Anzeigebereich (2)

Im oberen Teil des Anzeigebereichs befindet sich der Name des aktuell angemeldeten Benutzers sowie der vollständige Titel des aktuell gewählten Menüpunkts.

Im unteren Teil des Anzeigebereichs befindet sich Folgendes:

- **Abmelden**
  Sie können sich auf jeder WBM-Seite abmelden, indem Sie auf den Link "Abmelden" klicken.
- **Leuchtdiodensimulation**
  Jedes Gerät verfügt über mehrere Leuchtdioden, die Informationen über den Betriebszustand des Geräts liefern. Abhängig vom Aufstellort ist der direkte Zugang zum Gerät jedoch nicht immer möglich. Aus diesem Grund bietet das Web Based Management eine Simulationsdarstellung für die Leuchtdioden. Nicht belegte Anschlüsse werden als graue LEDs dargestellt. Die Bedeutung der Leuchtdiodenanzeigen ist in der Betriebsanleitung beschrieben.
  Wenn Sie diese Schaltfläche anklicken, rufen Sie das Fenster der Leuchtdiodensimulation auf. Sie können dieses Fenster während des Menüwechsels einblenden und beliebig verschieben. Um die Leuchtdiodensimulation zu schließen, klicken Sie innerhalb des Fensters der Leuchtdiodensimulation auf die Schließen-Schaltfläche.

- **Hilfe** 
  Wenn Sie diese Schaltfläche anklicken, wird die Hilfeseite des aktuell gewählten Menüpunktes in einem neuen Browser-Fenster aufgerufen. Auf der Hilfeseite finden Sie eine Beschreibung des Inhaltsbereichs. Unter Umständen sind Optionen beschrieben, die auf dem Gerät nicht zur Verfügung stehen.
  Auf jeder Hilfeseite gibt es am oberen Rand ein Eingabefeld für die Suchfunktion. Geben Sie dort einen Begriff ein, zu dem Sie weitere Informationen benötigen und starten Sie die Suche durch Betätigen der Eingabetaste. In einem Dialogfeld wird eine Liste mit WBM-Seiten angezeigt, die den gesuchten Begriff enthalten. Nach dem Anklicken eines Listenelements wird die entsprechende WBM-Seite in einem neuen Register des Browsers geöffnet.
- **Drucken** 
  Wenn Sie diese Schaltfläche anklicken, wird ein Popup-Fenster geöffnet. Das Popup-Fenster enthält eine Ansicht des Seiteninhalts, die für Drucker optimiert ist.

  Hinweis

  Drucken großer Tabellen

  Wenn Sie große Tabellen ausdrucken wollen, verwenden Sie bitte die "Druckvorschau" Funktion Ihres Internet-Browsers.

- **Favoriten**
  Im Lieferzustand ist die Schaltfläche auf allen Seiten deaktiviert  .
  Wenn Sie diese Schaltfläche anklicken, ändert sich das Symbol und die aktuell geöffnete Seite oder das aktuell geöffnete Register wird als Favorit markiert. Sobald Sie die Schaltfläche einmal aktiviert haben, wird der Navigationsbereich in zwei Register unterteilt. Das erste Register "Menü" enthält alle verfügbaren Menüs, wie bisher. Das zweite Register "Favoriten" enthält alle Seiten/Register, die Sie als Favoriten markiert haben. Im Register "Favoriten" werden die Seiten/Register entsprechend der Struktur im Register "Menü" angeordnet.
  Wenn Sie alle angelegten Favoriten wieder deaktivieren, wird auch das Register "Favoriten" wieder entfernt. Klicken Sie hierzu auf den entsprechenden Seiten/Registern die Schaltfläche  an.
  Sie können die Favoriten-Konfiguration eines Geräts auf der Seite "System > Laden & Speichern" über HTTP oder TFTP speichern, hochladen und löschen.

Navigationsbereich (3)

Im Navigationsbereich stehen Ihnen verschiedene Menüs zur Verfügung. Klicken Sie die einzelnen Menüs an, um sich die Untermenüs anzeigen zu lassen. Die Untermenüs enthalten Seiten, aus denen man Informationen entnehmen kann oder mit denen Sie Konfigurationen vornehmen können. Diese Seiten werden immer im Inhaltsbereich angezeigt.

Wenn Sie Favoriten angelegt haben, ist der Navigationsbereich in zwei Register unterteilt: "Menü" und "Favoriten".

Inhaltsbereich (4)

Der Inhaltsbereich enthält eine Grafik des Geräts. Die Grafik zeigt immer das Gerät, dessen WBM Sie aufgerufen haben.

Unter dem Gerätebild wird Folgendes angezeigt:

- **PROFINET-Gerätename**
  Zeigt den PROFINET-Gerätenamen an.
- **Diagnosemodus**
  Zeigt an, ob EtherNet/IP oder PROFINET IO aktiviert ist.
- **Systemname**
  Zeigt den Namen des Geräts an.
- **Gerätetyp**
  Zeigt die Typenbezeichnung des Geräts an.
- **PROFINET AR-Status**
  Zeigt den PROFINET Application Relation Status an.
  - Online
    Zu einem PROFINET-Controller besteht eine Verbindung. Der PROFINET-Controller hat seine Konfigurationsdaten in das Gerät geladen. Das Gerät kann Statusdaten zum PROFINET-Controller senden.
    In diesem Zustand sind die Parameter, die über den PROFINET-Controller eingestellt werden, nicht am Gerät konfigurierbar.
  - Offline
    Zu einem PROFINET-Controller besteht keine Verbindung.
- **Spannungsversorgung 1 / Spannungsversorgung 2**
  - Up
    Die Versorgungsspannung 1 bzw. 2 liegt an
  - Down
    Die Versorgungsspannung 1 bzw. 2 liegt nicht an oder die zulässige Spannung ist unterschritten.
- **PLUG-Konfiguration**
  Zeigt den Status der Konfigurationsdaten auf dem PLUG an, siehe Kapitel "System > PLUG > Konfiguration".
- **Fehlerstatus**
  Zeigt den Fehlerstatus des Geräts an.

Häufig verwendete Schaltflächen

Die Seiten des WBM enthalten standardmäßig folgende Schaltflächen:

- **Aktualisieren der Anzeige mit "Aktualisieren"**
  Seiten des Web Based Managements, die aktuelle Parameter anzeigen, haben am unteren Rand die Schaltfläche "Aktualisieren". Klicken Sie auf diese Schaltfläche, wenn Sie für die angezeigte Seite aktuelle Daten vom Gerät anfordern wollen.

  Hinweis

  Wenn Sie auf die Schaltfläche "Aktualisieren" klicken, bevor Sie Ihre Konfigurationsänderungen mit Hilfe der Schaltfläche "Einstellungen übernehmen" auf das Gerät übertragen haben, werden Ihre Änderungen gelöscht und die bisherige Konfiguration wird aus dem Gerät geladen und hier angezeigt.

- **Speichern von Einträgen mit "Einstellungen übernehmen"**
  Seiten, auf denen Sie Konfigurationseinstellungen festlegen können, haben am unteren Rand die Schaltfläche "Einstellungen übernehmen". Die Schaltfläche wird erst aktiv, wenn Sie auf der Seite mindestens einen Wert ändern. Klicken Sie auf die Schaltfläche, um eingegebene Konfigurationsdaten im Gerät zu speichern. Nach dem Speichern ist die Schaltfläche wieder inaktiv.

  Hinweis

  Das Ändern der Konfigurationsdaten ist nur mit der Rolle "admin" möglich.

- **Anlegen von Einträgen mit "Erstellen"**
  Seiten, auf denen Sie neue Einträge erstellen können, haben am unteren Rand die Schaltfläche "Erstellen". Klicken Sie auf diese Schaltfläche, um einen neuen Eintrag zu erstellen. Beim Erstellen eines Eintrags wird die Seite aktualisiert.
- **Löschen von Einträgen mit "Löschen"**
  Seiten, auf denen Sie Einträge löschen können, haben am unteren Rand die Schaltfläche "Löschen". Klicken Sie auf diese Schaltfläche, um die zuvor markierten Einträge aus dem Gerätespeicher zu löschen. Beim Löschen eines Eintrags wird die Seite aktualisiert.
- **Vorwärts blättern mit "Weiter"**
  Auf Seiten mit sehr vielen Datensätzen ist die Anzahl der auf einer Seite darstellbaren Datensätze beschränkt. Klicken Sie auf die Schaltfläche "Weiter", um innerhalb der Datensätze vorwärts zu blättern.
- **Rückwärts blättern mit "Zurück"**
  Auf Seiten mit sehr vielen Datensätzen ist die Anzahl der auf einer Seite darstellbaren Datensätze beschränkt. Klicken Sie auf die Schaltfläche "Zurück" um innerhalb der Datensätze rückwärts zu blättern.

Meldungen

Wenn Sie die Betriebsart "Automatisches Speichern" aktiviert haben und einen Parameter ändern, erscheint im Anzeigebereich folgende Meldung "Die Änderungen werden automatisch in x Sekunden gespeichert. Um die Änderungen sofort zu speichern, klicken Sie auf 'Schreiben der Startkonfiguration'."

Hinweis

Unterbrechung des Speichervorgangs

Der Speichervorgang startet erst, nachdem der Timer in der Meldung abgelaufen ist. Hierzu erscheint folgende Meldung "Die Konfigurationsdaten werden gespeichert. Schalten Sie das Gerät nicht aus.". Die Dauer des Speichervorgangs ist vom Gerät abhängig.

- Schalten Sie das Gerät nicht sofort aus, nachdem der Timer abgelaufen ist.

5.3.2 Versionen

Versionen von Hardware und Software

Diese Seite zeigt die Ausgabestände der Hardware und der Software des Geräts. Sie können auf dieser Seite keine Konfigurationen vornehmen.

Beschreibung der angezeigten Werte

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Hardware -** Basic Device
  Zeigt das Grundgerät an.
- **Name**
  Zeigt den Namen des Geräts oder des Moduls an.
- **Ausgabestand**
  Zeigt den Hardware-Ausgabestand des Geräts an.
- **Artikelnummer**
  Zeigt die Artikelnummer des Geräts oder des beschriebenen Moduls an.

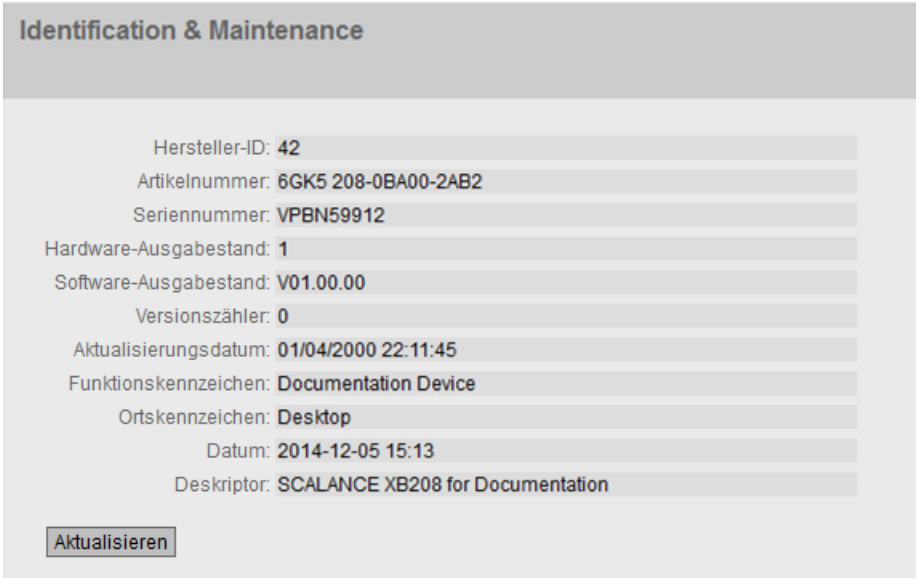
Die Tabelle 2 gliedert sich in folgende Spalten:

- **Software**
  - Firmware
    Zeigt die aktuelle Firmware-Version an. Wenn eine neue Firmware-Datei geladen wurde und das Gerät noch nicht neu gestartet ist, wird hier die Firmware-Version der geladenen Firmware-Datei angezeigt. Nach dem nächsten Neustart wird die geladene Firmware aktiviert und verwendet.
  - Bootloader
    Zeigt die Version der Boot-Software an, die im Gerät gespeichert ist.
  - Firmware_Running
    Zeigt die Firmware-Version an, die aktuell im Gerät verwendet wird.
- **Beschreibung**
  Zeigt die Kurzbeschreibung der Software an.
- **Version**
  Zeigt die Versionsnummer des Software-Ausgabestands an.
- **Datum**
  Zeigt das Erstellungsdatum des Software-Ausgabestands an.

5.3.3 I&M

Hersteller- und Wartungsdaten

Diese Seite beinhaltet Informationen zu gerätespezifischen Hersteller- und Wartungsdaten wie Bestellnummer, Seriennummer, Versionsnummern etc. Sie können auf dieser Seite keine Konfigurationen vornehmen.



Beschreibung der angezeigten Werte

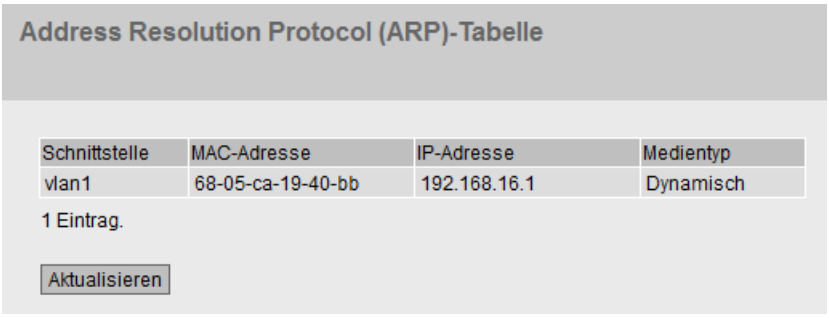
Die Tabelle gliedert sich in folgende Zeilen:

- **Hersteller-ID**
  Zeigt die Herstellerkennung an.
- **Artikelnummer**
  Zeigt die Bestellnummer an.
- **Seriennummer**
  Zeigt die Seriennummer an.
- **Hardware-Ausgabestand**
  Zeigt den Hardware-Ausgabestand an.
- **Software-Ausgabestand**
  Zeigt den Software-Ausgabestand an.
- **Versionszähler**
  Unabhängig von einer Versionsänderung, zeigt dieses Feld immer den Wert "0" an.
- **Aktualisierungsdatum**
  Zeigt Datum und Uhrzeit der letzten Versionsänderung an.
- **Funktionskennzeichen**
  Zeigt das Funktionskennzeichen (Anlagenkennzeichen) des Geräts an. Das Anlagenkennzeichen (AKZ) wird bei der Projektierung des Geräts mit HWKonfig von STEP7 angelegt.
- **Ortskennzeichen**
  Zeigt das Ortskennzeichen des Geräts an. Das Ortskennzeichen (OKZ) wird bei der Projektierung des Geräts mit HWKonfig von STEP7 angelegt.
- **Datum**
  Zeigt das Datum, das bei der Projektierung des Geräts mit HWKonfig von STEP7 angelegt wurde.
- **Deskriptor**
  Zeigt die Beschreibung, die bei der Projektierung des Geräts mit HWKonfig von STEP7 angelegt wurde.

5.3.4 ARP-Tabelle

Zuordnung von MAC-Adresse und IPv4-Adresse

Über das Address Resolution Protocol (ARP) erfolgt die eindeutige Zuordnung von MAC-Adresse zu IPv4-Adresse. Diese Zuordnung wird von jedem Netzteilnehmer in seiner eigenen ARP-Tabelle gepflegt. Die WBM-Seite zeigt die ARP-Tabelle des Geräts.



Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Spalten:

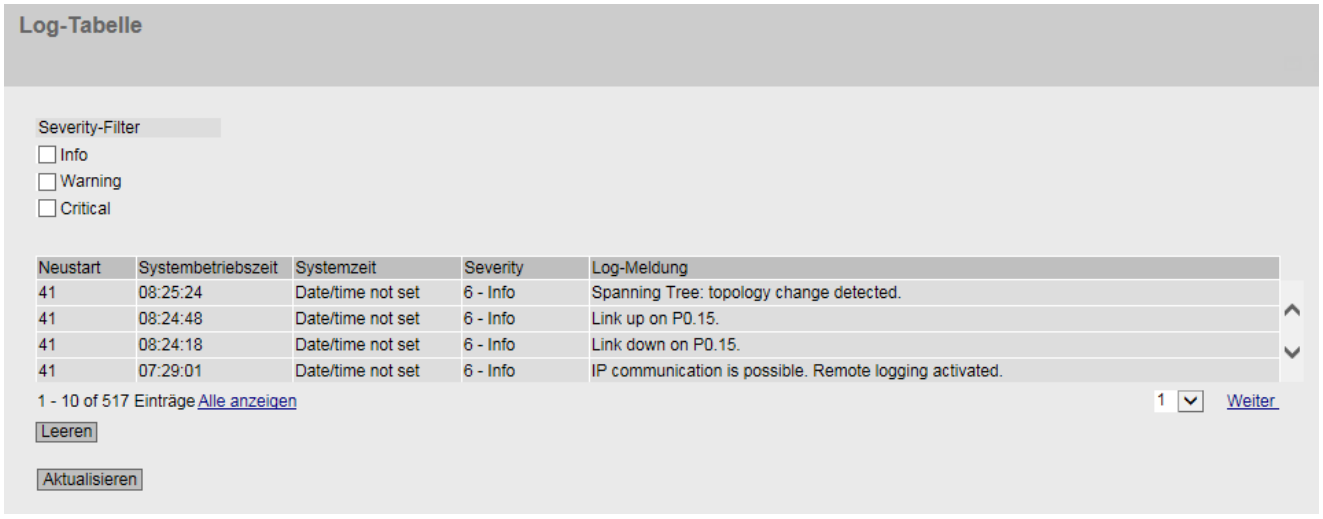
- **Schnittstelle**
  Zeigt die Schnittstelle an, über die der Zeileneintrag gelernt wurde.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Ziel- oder Quellgeräts an.
- **IP-Adresse**
  Zeigt die IPv4-Adresse des Zielgeräts an.
- **Medientyp**
  Zeigt die Art der Verbindung.
  - Dynamisch
    Das Gerät hat die Adressdaten automatisch erkannt.
  - Statisch
    Die Adressen wurden als statische Adressen eingetragen.

5.3.5 Log-Tabelle

Protokollierung von Ereignissen

Das Gerät bietet die Möglichkeit, auftretende Ereignisse zu protokollieren, die Sie zum Teil auf der Seite des Menüs "System > Ereignisse" festlegen können. So kann beispielsweise festgehalten werden, wann ein Authentifizierungsversuch fehlgeschlagen ist oder wann sich der Verbindungsstatus eines Ports geändert hat.

Der Inhalt der Ereignisprotokoll-Tabelle bleibt auch nach dem Ausschalten des Geräts erhalten.



Beschreibung der angezeigten Werte

Severity-Filter

Sie können die Einträge der Tabelle nach Fehlerschwere filtern. Wählen Sie in den Optionskästchen oberhalb der Tabelle die gewünschten Einträge aus.

- **Info**
  Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorie "Info" angezeigt.
- **Warning**
  Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorie "Warning" angezeigt.
- **Critical**
  Wenn dieser Parameter aktiviert ist, werden alle Einträge der Kategorie "Critical" angezeigt.

Um alle Einträge anzuzeigen, wählen Sie entweder alle aus oder lassen Sie die Optionskästchen leer.

Die Tabelle gliedert sich in folgende Spalten:

- **Neustart**
  Zählt die Anzahl der Neustarts seit dem letzten Zurücksetzen auf Werkseinstellungen und gibt an, nach welchem Neustart des Geräts das entsprechende Ereignis eingetreten ist.
- **Systembetriebszeit**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an, zu der das beschriebene Ereignis eingetreten ist.
- **Systemzeit**
  Wenn die Systemzeit gesetzt ist, werden Datum und Uhrzeit angezeigt, bei der das Ereignis eingetreten ist.
- **Severity**
  Einordnung des Eintrags in obige Kategorien.
- **Log-Meldung**
  Zeigt eine Kurzbeschreibung des eingetretenen Ereignisses an.

Beschreibung der Schaltflächen und Eingabefelder

Schaltfläche "Leeren"

Klicken Sie auf diese Schaltfläche, um den Inhalt der Ereignisprotokolldatei zu löschen. Es werden alle Einträge gelöscht, unabhängig davon, was Sie unter "Severity-Filter" ausgewählt haben.

Die Anzeige wird dabei ebenfalls geleert. Erst wenn nach einem Wiederherstellen der Werkseinstellungen das Gerät neu gestartet ist, wird der Neustart-Zähler zurückgesetzt.

Hinweis

Die Anzahl der Einträge in dieser Tabelle ist auf 1200 beschränkt. Die Tabelle kann für jede Severity 400 Einträge enthalten. Wenn diese Zahl erreicht ist, werden die ältesten Einträge der jeweiligen Severity verworfen. Die Tabelle verbleibt permanent im Speicher.

Schaltfläche "Alle anzeigen"

Klicken Sie auf diese Schaltfläche, um alle Einträge auf der WBM-Seite anzuzeigen. Beachten Sie, dass das Anzeigen aller Meldungen einige Zeit beanspruchen kann.

Schaltfläche "Weiter"

Klicken Sie auf diese Schaltfläche, um zur nächsten Seite zu navigieren.

Schaltfläche "Zurück"

Klicken Sie auf diese Schaltfläche, um zur vorherigen Seite zu navigieren.

Klappliste für Seitenwechsel

Wählen Sie aus der Klappliste die gewünschte Seite aus, um zu einer bestimmten Seite zu navigieren.

Schaltfläche "Aktualisieren"

Erneuert die Anzeige der Werte in der Tabelle.

5.3.6 Fehler

Fehlerstatus

Wenn ein Fehler auftritt, wird er auf dieser Seite angezeigt. Am Gerät werden Fehler dadurch signalisiert, dass die rote Fehler-LED leuchtet.

Gemeldet werden interne Fehler des Geräts sowie Fehler, die Sie auf folgenden Seiten konfigurieren:

- "System > Ereignisse"
- "System > Fehlerkontrolle"

Die Berechnung des Fehlerzeitpunkts beginnt jeweils nach dem letzten Systemstart. Wenn keine Fehler vorliegen, schaltet sich die Fehler-LED ab.

Beschreibung

- **Anzahl der gemeldeten Fehler**
  Zeigt an, wie oft die Fehler-LED eingeschaltet wurde und nicht wie viele Fehler aufgetreten sind.
- **Schaltfläche Zähler zurücksetzen**
  Über die Schaltfläche wird die Anzahl zurückgesetzt. Der Zähler wird durch einen Neustart zurückgesetzt.

Die Tabelle enthält die folgenden Spalten:

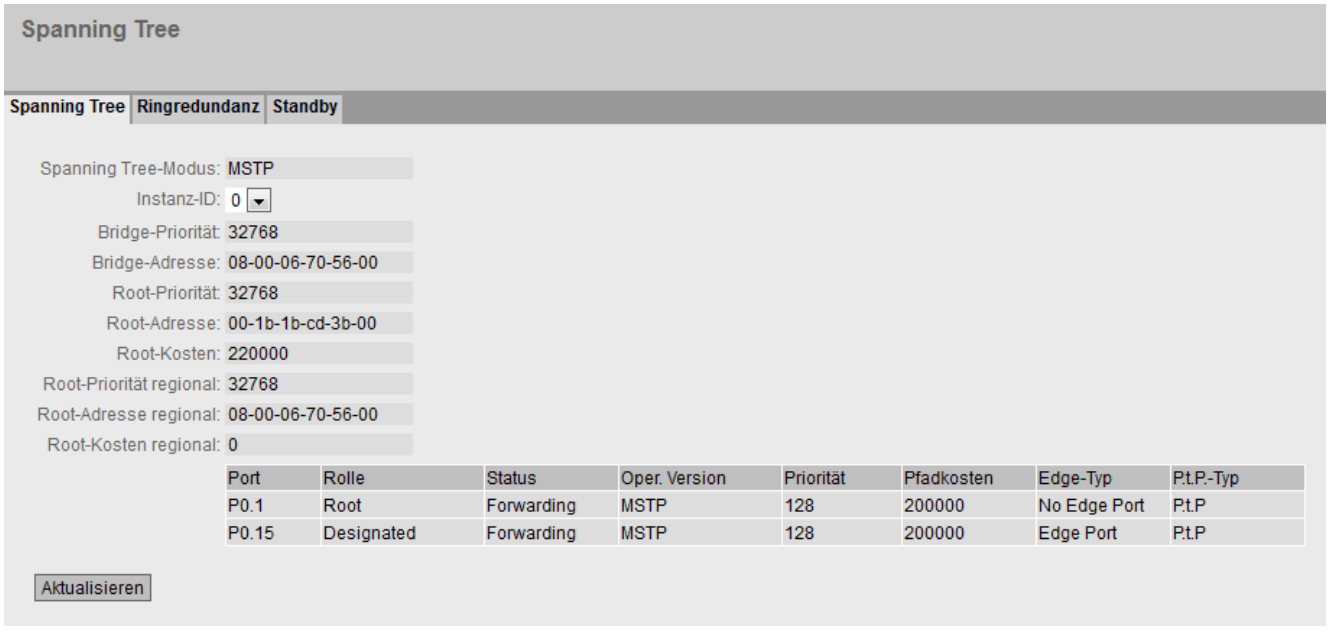
- **Fehlerzeitpunkt**
  Zeigt die Laufzeit des Geräts seit dem letzten Systemstart an, zu der der beschriebene Fehler aufgetreten ist.
- **Fehlerbeschreibung**
  Zeigt eine Kurzbeschreibung des aufgetretenen Fehlers an.
- **Fehlerstatus löschen**
  Manche Fehler lassen sich quittieren und damit aus der Fehlerliste entfernen, z. B. ein Fehler des Ereignisses "Kalt-/Warmstart". Wenn die Schaltfläche "Fehlerstatus löschen" aktiv ist, können Sie den Fehler löschen.

5.3.7 Redundanz

5.3.7.1 Spanning Tree

Einleitung

Die Seite zeigt die aktuellen Informationen zu Spanning Tree und die Einstellungen der Root Bridge an.



Beschreibung der angezeigten Werte

Folgende Felder werden angezeigt:

- **Spanning Tree-Modus**
  Zeigt den eingestellten Modus an. Den Modus legen Sie bei "Layer 2 > Konfiguration" und bei "Layer 2 > Spanning Tree > Allgemein" fest.
  Folgende Werte sind möglich:
  - '-'
  - STP
  - RSTP
  - MSTP
- **Instanz-ID**
  Zeigt die Nummer der Instanz an. Der Parameter ist abhängig vom projektierten Modus.

- **Bridge-Priorität / Root-Priorität**
  Anhand der Bridge-Priorität wird festgelegt, welches Gerät Root Bridge wird. Die Bridge mit der höchsten Priorität (d. h. dem kleinsten Wert für diesen Parameter) wird Root Bridge. Wenn in einem Netz mehrere Geräte die gleiche Priorität besitzen, dann wird das Gerät Root Bridge, dessen MAC-Adresse den niedrigsten Zahlenwert hat. Beide Parameter, Bridge-Priorität und MAC-Adresse, bilden zusammen die Bridge-Kennung. Da die Root Bridge alle Wegeänderungen verwaltet, sollte sie wegen der Laufzeit der Telegramme möglichst zentral angeordnet sein. Der Wert für die Bridge-Priorität ist ein ganzzahliges Vielfaches von 4096 mit einem Wertebereich von 0 bis 32768.
- **Bridge-Adresse / Root-Adresse**
  Die Bridge-Adresse zeigt die MAC-Adresse des Geräts und die Root-Adresse zeigt die MAC-Adresse des Root-Switches an.
- **Root-Kosten**
  Zeigt die Pfadkosten von dem Gerät bis zur Root Bridge.
- **Bridge-Status**
  Zeigt den Status der Bridge an, z. B. ob das Gerät die Root Bridge ist.
- **Root-Priorität regional** (nur bei MSTP verfügbar)
  Beschreibung siehe Bridge-Priorität / Root-Priorität
- **Root-Adresse regional** (nur bei MSTP verfügbar)
  Zeigt die MAC-Adresse des Geräts an.
- **Root-Kosten regional** (nur bei MSTP verfügbar)
  Zeigt die Pfadkosten von der regionalen Root Bridge bis zur Root Bridge an.

Die Tabelle gliedert sich in folgende Spalten:

- **Port**
  Zeigt den Port an, über den das Gerät kommuniziert. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Rolle**
  Zeigt den Status des Ports an. Folgende Werte sind möglich:
  - Disabled
    Der Port wurde manuell aus dem Spanning Tree entfernt und wird vom Spanning Tree nicht mehr berücksichtigt.
  - Designated
    Die Ports, die von der Root-Bridge wegführen.
  - Alternate
    Der Port mit einem alternativen Weg zu einem Netzwerksegment.
  - Backup
    Wenn ein Switch mehrere Ports zu dem gleichen Netzwerksegment hat, wird der "schlechtere" Port zum Backup-Port.
  - Root
    Der Port, der den besten Weg zur Root Bridge bietet.
  - Master
    Dieser Port zeigt zu einer Root Bridge, die außerhalb der MST-Region liegt.

- **Status**
  Zeigt den momentanen Status an, in dem sich der Port befindet. Die Werte werden nur angezeigt. Der Parameter ist abhängig vom projektierten Protokoll. Folgende Werte sind möglich:
  - Discarding
    Der Port empfängt BPDU-Telegramme. Andere aus- oder eingehende Telegramme werden verworfen.
  - Listening
    Der Port empfängt und sendet BPDU-Telegramme. Der Port ist in den Spanning Tree-Algorithmus einbezogen. Andere aus- und eingehende Telegramme werden verworfen.
  - Learning
    Der Port lernt aktiv die Topologie, d. h. die Teilnehmeradressen. Andere aus- und eingehende Telegramme werden verworfen.
  - Forwarding
    Der Port ist nach der Umkonfigurationszeit aktiv im Netz. Der Port empfängt und sendet Datentelegramme.
- **Oper. Version**
  Zeigt den Kompatibilitätsmodus von Spanning Tree, der vom Port verwendet wird.
- **Priorität**
  Kann der vom Spanning-Tree ermittelte Weg alternativ über mehrere Ports eines Geräts führen, so wird der Port mit der höchsten Priorität (d. h. dem kleinsten Wert für diesen Parameter) ausgewählt. Für die Priorität kann ein Wert von 0 bis 240 in 16er Schritten eingegeben werden. Wenn Sie einen Wert eingeben, der nicht durch 16 teilbar ist, wird der Wert automatisch angepasst. Der Standardwert ist 128.
- **Pfadkosten**
  Dieser Parameter dient zur Berechnung des zu wählenden Wegs. Es wird die Strecke mit dem geringsten Wert als Weg ausgewählt. Haben mehrere Ports eines Geräts den gleichen Wert, wird der Port mit der niedrigsten Portnummer ausgewählt.
  Ist der Wert im Feld "Kalk. Kosten" "0", so wird der automatisch ermittelte Wert angezeigt. Andernfalls wird der Wert des Feldes "Kalk. Kosten" angezeigt.
  Die Ermittlung der Wegekosten richtet sich maßgeblich nach der Übertragungsgeschwindigkeit. Je höher die erzielbare Übertragungsgeschwindigkeit ist, umso kleiner ist der Wert für die Wegekosten.
  Typische Werte für Wegekosten bei Rapid Spanning Tree:
  - 10.000 Mbit/s = 2.000
  - 1000 Mbit/s = 20.000
  - 100 Mbit/s = 200.000
  - 10 Mbit/s = 2.000.000

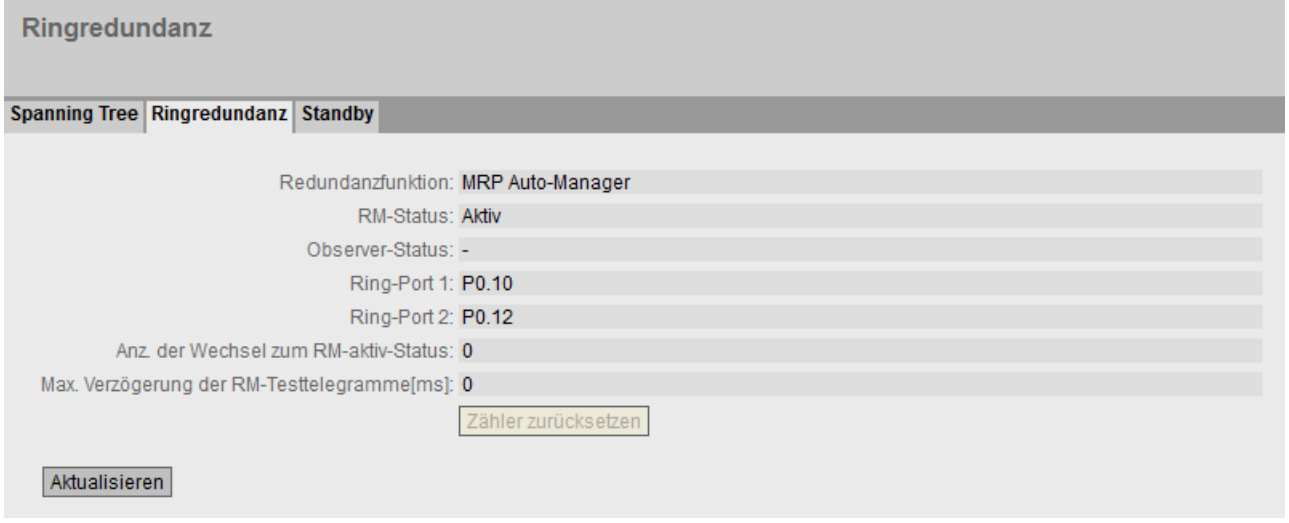
  Sie konfigurieren die "Kalk. Kosten" auf den Seiten "Layer 2 > Spanning Tree > CIST-Port" und "Layer 2 > Spanning Tree > MST-Port".

- **Edge-Typ**
  Zeigt den Typ der Verbindung an. Folgende Werte sind möglich:
  - Edge Port
    An diesem Port befindet sich ein Endgerät.
  - No Edge Port
    An diesem Port befindet sich ein Spanning Tree-Gerät.
- **P.t.P.-Typ**
  Zeigt die Art der Punkt-zu-Punkt-Verbindung an. Folgende Werte sind möglich:
  - P.t.P.
    Bei Halbduplex wird von einer Punkt-zu-Punkt-Verbindung ausgegangen.
  - Shared Media
    Bei einer Vollduplexverbindung wird nicht von einer Punkt-zu-Punkt-Verbindung ausgegangen.

5.3.7.2 Ringredundanz

Informationen zur Ringredundanz

Unter diesem Reiter erhalten Sie Informationen zum Status des Geräts bezogen auf Ringredundanz. Die Textfelder dieser Seite sind nur lesbar.



Beschreibung der angezeigten Werte

Folgende Felder werden angezeigt:

- **Redundanzfunktion**
  Die Spalte "Redundanzfunktion" zeigt die Rolle des Geräts innerhalb des Rings an:
  - Keine Ringredundanz
    Der IE-Switch arbeitet ohne Redundanz-Funktion.
  - HRP-Client
    Der IE-Switch arbeitet als HRP-Client.
  - HRP-Manager
    Der IE-Switch arbeitet als HRP-Manager.
  - MRP-Client
    Der IE-Switch arbeitet als MRP-Client.
  - MRP-Manager
    Der IE-Switch arbeitet als MRP-Manager. Über STEP 7 wurde die Rolle "Manager" für das Gerät eingestellt.
  - MRP Auto-Manager
    Der IE-Switch arbeitet als MRP-Manager. Über WBM bzw. CLI wurde die Rolle "MRP Auto-Manager" oder über STEP 7 die Rolle "Manager (Auto") eingestellt.
- **RM-Status**
  Die Spalte "RM-Status" zeigt an, ob der IE-Switch als Redundanzmanager arbeitet und ob er in dieser Funktion den Ring geöffnet oder durchgeschaltet hat.
  - Passiv
    Der IE-Switch arbeitet als Redundanzmanager und hat den Ring geöffnet, d.h. die an die Ringports angeschlossene Linie von Switches arbeitet fehlerfrei. Der Zustand "Passiv" wird auch angezeigt, wenn der IE-Switch nicht als Redundanzmanager arbeitet (Redundanzmanager deaktiviert).
  - Aktiv
    Der IE-Switch arbeitet als Redundanzmanager und hat den Ring geschlossen, d.h. die an die Ringports angeschlossene Linie von Switches ist unterbrochen (Fehlerfall). Der Redundanzmanager schaltet die Verbindung zwischen seinen Ringports durch und stellt damit wieder eine durchgehende Linientopologie her.
  - "-"
    Die Redundanzfunktion ist deaktiviert.
- **Observer-Status**
  Zeigt den aktuellen Zustand des Observers an.
- **Ring-Port 1/Ring-Port 2**
  Die Spalten "Ring-Port 1" und "Ring-Port 2" zeigen die Ports an, die als Ringports verwendet werden. Wenn die Medienredundanz in Ringtopologien komplett abgeschaltet ist, dann werden die zuletzt konfigurierten Ringports angezeigt.

- **Anz. der Wechsel zum RM-aktiv-Status**
  Zeigt an, wie oft das Gerät als Redundanzmanager in den aktiven Zustand geschaltet hat, d. h. den Ring geschlossen hat.
  Wenn die Redundanzfunktion deaktiviert ist oder das Gerät "HRP-/MRP-Client" ist, dann erscheint der Text "Redundanzmanager deaktiviert".
- **Max. Verzögerung der RM-Testtelegramme[ms]**
  Zeigt die maximale Verzögerungszeit für Testtelegramme des Redundanzmanagers an.
  Wenn die Redundanzfunktion deaktiviert ist oder das Gerät "HRP-/MRP-Client" ist, dann erscheint der Text "Redundanzmanager deaktiviert".

Beschreibung der Schaltfläche

Schaltfläche "Zähler zurücksetzen"

Klicken Sie auf "Zähler zurücksetzen", um alle Zähler zurückzusetzen. Die Zähler werden durch einen Neustart zurückgesetzt.

5.3.7.3 Standby

Informationen zur Standby-Redundanz

Unter diesem Reiter erhalten Sie Informationen zum Status des Geräts bezogen auf Standby-Redundanz. Die Textfelder dieser Seite sind nur lesbar.

Hinweis

Gerät mit höherer MAC-Adresse wird Master

Für die redundante Kopplung von HRP-Ringen werden immer zwei Geräte als Master-/Slave-Gerätepaar konfiguriert. Dies gilt auch für unterbrochene HRP-Ringe = Linien. Im fehlerfreien Zustand übernimmt immer das Gerät mit der höheren MAC-Adresse die Funktion des Masters.

Wichtig ist diese Art der Zuordnung insbesondere bei einem Gerätetausch. Abhängig von den MAC-Adressen kann das bisherige Gerät mit Slave-Funktion die Rolle des Standby-Masters übernehmen.

Unter dem Reiter Standby finden Sie den Status der Standby-Funktion:

Beschreibung der angezeigten Werte

Folgende Felder werden angezeigt:

- **Standby-Ports**
  Zeigt den Standby-Port an.
- **Standby-Name**
  Name der Standby-Verbindung
- **Standby-Funktion**
  - Master
    Das Gerät hat Verbindung zum Partnergerät und arbeitet als Master. Im fehlerfreien Betrieb ist bei diesem Gerät der Standby-Port aktiv.
  - Slave
    Das Gerät hat Verbindung zum Partnergerät und arbeitet als Slave. Im fehlerfreien Betrieb ist bei diesem Gerät der Standby-Port inaktiv.
  - Deaktiviert
    Standby-Kopplung ist deaktiviert. Das Gerät arbeitet weder als Master noch als Slave. Ein als Standby-Port konfigurierter Port arbeitet als normaler Port ohne Standby-Funktion.
  - Verbindungsaufbau
    Es wurde noch keine Verbindung zum Partnergerät aufgenommen. Der Standby-Port ist inaktiv. In diesem Fall ist entweder die Projektierung auf dem Partnergerät nicht konsistent (z.B. falscher Verbindungsname, Standby-Kopplung deaktiviert) oder es liegt ein physikalischer Fehler vor (z.B. Geräteausfall, Link-Down).
  - Verbindungsverlust
    Bestehende Verbindung zum Partnergerät verloren. In diesem Fall wurde entweder die Projektierung auf dem Partnergerät geändert (z.B. anderer Verbindungsname, Standby-Kopplung deaktiviert) oder es liegt ein physikalischer Fehler vor (z.B. Geräteausfall, Link-Down).

- **Standby-Status**
  Das Anzeigefeld "Standby Status" zeigt den Status des Standby-Ports an:
  - Aktiv
    Der Standby-Port dieses Geräts ist aktiv, d. h. für den Telegrammverkehr freigeschaltet.
  - Passiv
    Der Standby-Port dieses Geräts ist inaktiv, d. h. für den Telegrammverkehr gesperrt.
  - "-":
    Die Standby-Funktion ist deaktiviert.
- **Anz. der Wechsel zum Standby-aktiv-Status**
  Zeigt an, wie oft der IE-Switch den Standby-Status vom Zustand "Passiv" in den Zustand "Aktiv" geändert hat. Wenn die Verbindung eines Standby-Ports beim Standby-Master ausfällt, wechselt der IE-Switch in den Zustand "Aktiv".
  Wenn die Standby-Funktion deaktiviert ist, erscheint der Text "Standby deaktiviert" in diesem Feld.

Beschreibung der Schaltfläche

Schaltfläche "Zähler zurücksetzen"

Klicken Sie auf "Zähler zurücksetzen", um den Zähler zurückzusetzen. Der Zähler wird durch einen Neustart zurückgesetzt.

5.3.7.4 Link Check

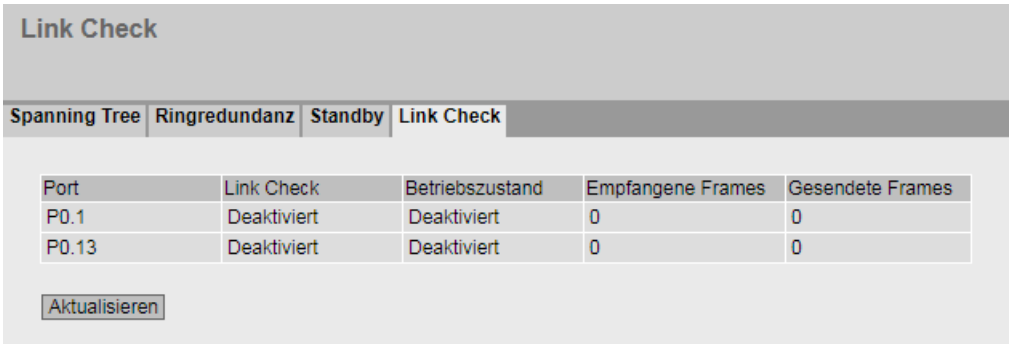
Überwachung optischer Verbindungen im Ring

Die Seite zeigt die folgende Informationen zu Link Check an:

- Die Ports, auf denen Sie Link Check aktivieren können
- Den aktuellen Status
- Die Statistik gesendeter und empfangener Link Check-Telegramme der überwachten Verbindungen

Hinweis

Wenn Sie Link Check zusammen mit einem Redundanzprotokoll (z. B. HRP) verwenden, können die Werte für die gesendeten und die empfangenen Link Check-Telegramme unterschiedlich sein.



Beschreibung der angezeigten Werte

Folgende Felder werden angezeigt:

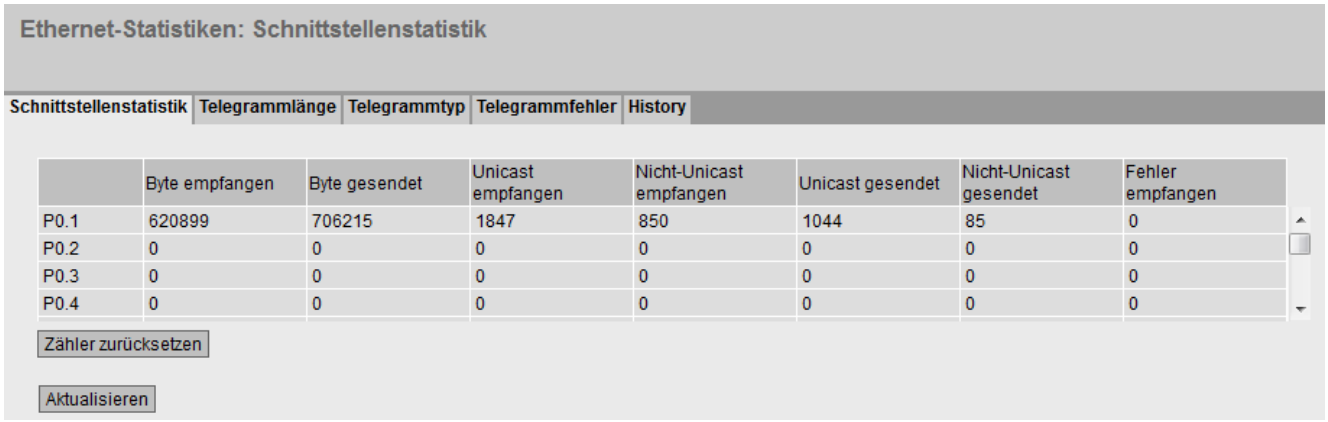
- **Port**
  Zeigt den Port an, auf den sich die nachfolgenden Informationen beziehen. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Link Check**
  Zeigt an, ob die Funktion Link Check aktiviert oder deaktiviert ist.
- **Betriebszustand**
  Zeigt den Status der Funktion Link Check. Es gibt folgende Zustände:
  - Deaktiviert
    Die Funktion ist deaktiviert.
  - Aktiviert
    Die Funktion ist aktiviert. Der Verbindungspartner hat die Überwachung noch nicht bestätigt.
  - Running
    Die Funktion ist aktiviert. Die Verbindungsüberwachung ist aktiv. Die ausgehenden und eingehenden Testtelegramme werden gezählt und abgeglichen.
  - Fehler
    Die Funktion ist aktiviert. Link Check hat einen Fehler auf der überwachten Strecke detektiert und den Port abgeschaltet.
- **Empfangene Frames**
  Zeigt an, wie viele Link Check-Testtelegramme empfangen wurden.
- **Gesendete Frames**
  Zeigt an, wie viele Link Check-Testtelegramme gesendet wurden.

5.3.8 Ethernet-Statistiken

5.3.8.1 Schnittstellenstatistik

Schnittstellenstatistik

Die Seite zeigt die Statistik aus der Schnittstellentabelle der Management Information Base (MIB).



Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Spalten:

- **Byte empfangen**
  Zeigt die Anzahl der empfangenen Bytes an.
- **Byte gesendet**
  Zeigt die Anzahl der gesendeten Bytes an.
- **Unicast empfangen**
  Zeigt die Anzahl der empfangenen Unicast-Telegramme an.
- **Nicht-Unicast empfangen**
  Zeigt die Anzahl der empfangenen Telegramme an, die nicht vom Telegrammtyp Unicast sind.
- **Unicast gesendet**
  Zeigt die Anzahl der gesendeten Unicast-Telegramme an.
- **Nicht-Unicast gesendet**
  Zeigt die Anzahl der gesendeten Telegramme an, die nicht vom Telegrammtyp Unicast sind.
- **Fehler empfangen**
  Zeigt die Anzahl aller möglichen RX-Fehler an, siehe Register "Telegrammfehler".

Beschreibung der Schaltfläche

Schaltfläche "Zähler zurücksetzen"

Klicken Sie auf "Zähler zurücksetzen", um alle Zähler zurückzusetzen. Die Zähler werden durch einen Neustart zurückgesetzt.

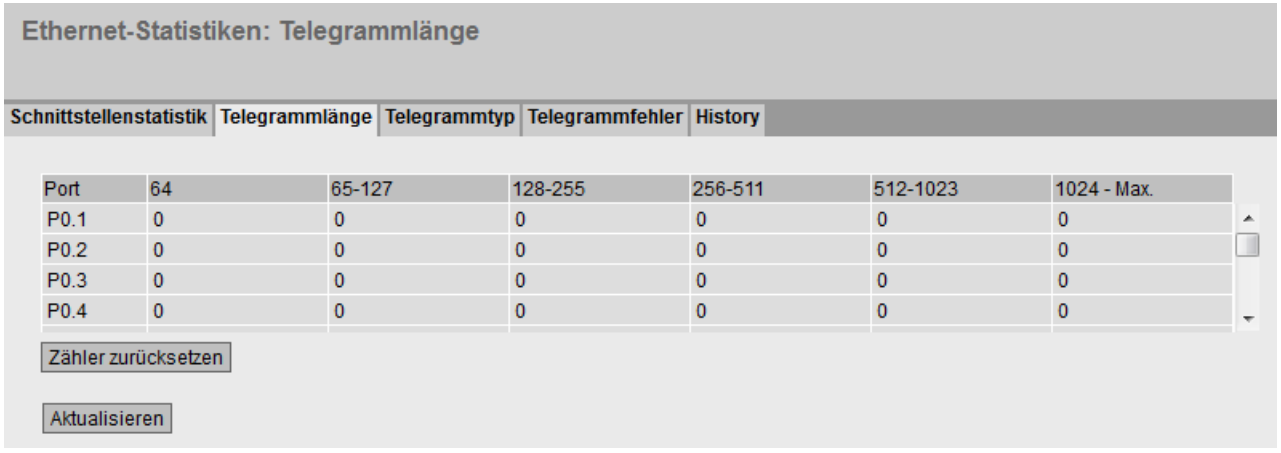
5.3.8.2 Telegrammlänge

Telegramme sortiert nach Länge

Diese Seite zeigt, wie viele Telegramme mit welcher Länge an jedem Port gesendet und empfangen wurden. Sie können auf dieser Seite keine Konfigurationen vornehmen.

Die angezeigten Werte werden durch RMON übermittelt.

Auf der Seite "Layer 2 > RMON > Statistik" können Sie einstellen, für welche Ports Werte angezeigt werden sollen.



Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports und Link Aggregationen an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.

  Hinweis

  Anzeige der Telegrammstatistik

  Beachten Sie bei der Statistik der Telegrammlängen, dass sowohl eingehende als auch ausgehende Telegramme gezählt werden.

- **Telegrammlängen**
  Die weiteren Spalten hinter der jeweiligen Portnummer enthalten die absoluten Zahlen der Telegramme entsprechend ihrer Telegrammlänge.
  Dabei wird in folgenden Telegrammlängen unterschieden:
  - 64 Byte
  - 65 - 127 Byte
  - 128 - 255 Byte
  - 256 - 511 Byte
  - 512 - 1023 Byte
  - 1024 - Max.

Hinweis

Datenverkehr auf geblockten Ports

Aus technischen Gründen können auf geblockten Ports Datenpakete angezeigt werden.

Beschreibung der Schaltfläche

Schaltfläche "Zähler zurücksetzen"

Klicken Sie auf "Zähler zurücksetzen", um alle Zähler zurückzusetzen. Die Zähler werden durch einen Neustart zurückgesetzt.

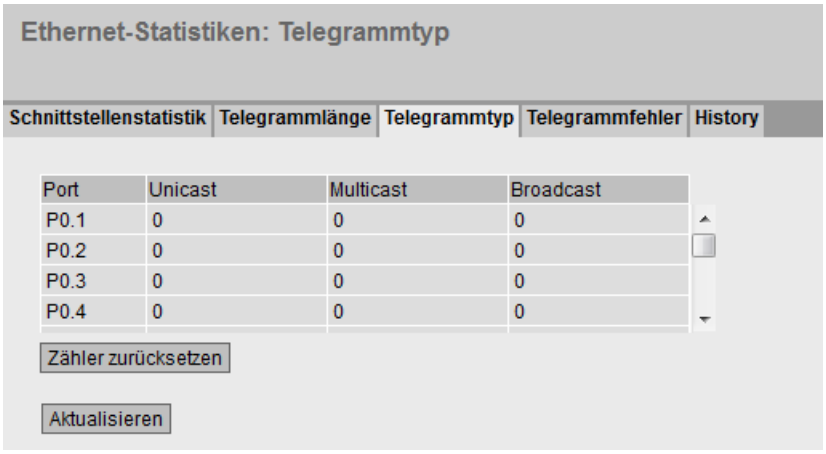
5.3.8.3 Telegrammtyp

Empfangene Telegramme sortiert nach Telegrammtyp

Diese Seite zeigt, wie viele Telegramme der Typen "Unicast", "Multicast" und "Broadcast" an jedem Port empfangen wurden. Sie können auf dieser Seite keine Konfigurationen vornehmen.

Die angezeigten Werte werden durch RMON übermittelt.

Auf der Seite "Layer 2 > RMON > Statistik" können Sie einstellen, für welche Ports Werte angezeigt werden sollen.



Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports und Link Aggregationen an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Unicast / Multicast / Broadcast**
  Die weiteren Spalten hinter der jeweiligen Portnummer enthalten die absoluten Zahlen der eingegangenen Telegramme entsprechend der Telegrammtypen "Unicast", "Multicast" und "Broadcast".

Beschreibung der Schaltfläche

Schaltfläche "Zähler zurücksetzen"

Klicken Sie auf "Zähler zurücksetzen", um alle Zähler zurückzusetzen. Die Zähler werden durch einen Neustart zurückgesetzt.

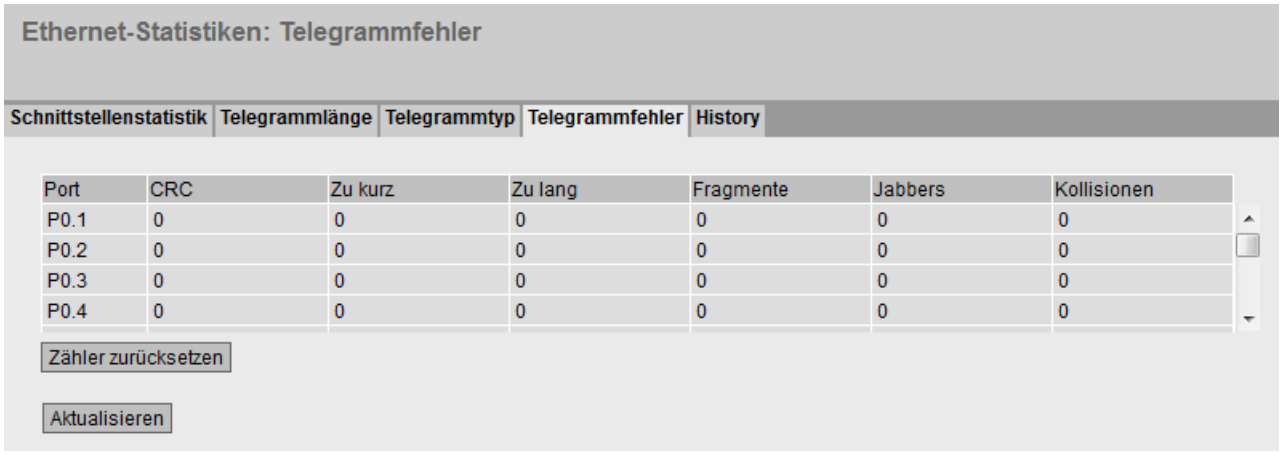
5.3.8.4 Telegrammfehler

Fehlerhaft empfangene Telegramme

Die Seite zeigt, wie viele fehlerhafte Telegramme pro Port empfangen wurden. Sie können auf dieser Seite keine Konfigurationen vornehmen.

Die angezeigten Werte werden durch RMON übermittelt.

Auf der Seite "Layer 2 > RMON > Statistik" können Sie einstellen, für welche Ports Werte angezeigt werden sollen.



Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in Spalten wie folgt:

- **Port**
  Zeigt die verfügbaren Ports und Link Aggregationen an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Fehlertypen**
  Die weiteren Spalten hinter der jeweiligen Portnummer enthalten die absoluten Zahlen der eingegangenen Telegramme entsprechend ihres Fehlertyps.
  Dabei wird in den Spalten der Tabelle nach folgenden Fehlertypen unterschieden:
  - CRC
    Pakete, deren Inhalt nicht mit der zugehörigen CRC-Prüfsumme übereinstimmt.
  - Zu kurz
    Pakete mit einer Länge kleiner als 64 Byte.
  - Zu lang
    Pakete, die aufgrund einer zu großen Länge verworfen wurden.
  - Fragmente
    Pakete mit einer Länge kleiner als 64 Byte und einer falschen CRC-Prüfsumme.
  - Jabbers
    VLAN-getaggte Pakete mit einer falschen CRC-Prüfsumme, die aufgrund einer zu großen Länge verworfen wurden.
  - Kollisionen
    Erkannte Kollisionen.

Beschreibung der Schaltfläche

Schaltfläche "Zähler zurücksetzen"

Klicken Sie auf "Zähler zurücksetzen", um alle Zähler zurückzusetzen. Die Zähler werden durch einen Neustart zurückgesetzt.

5.3.8.5 History

Stichproben der Statistiken

Die Seite zeigt pro Port Stichproben mit Informationen aus den RMON-Statistiken an.

Auf der Seite "Layer 2 > RMON > History" können Sie einstellen, für welche Ports Stichproben genommen werden sollen.

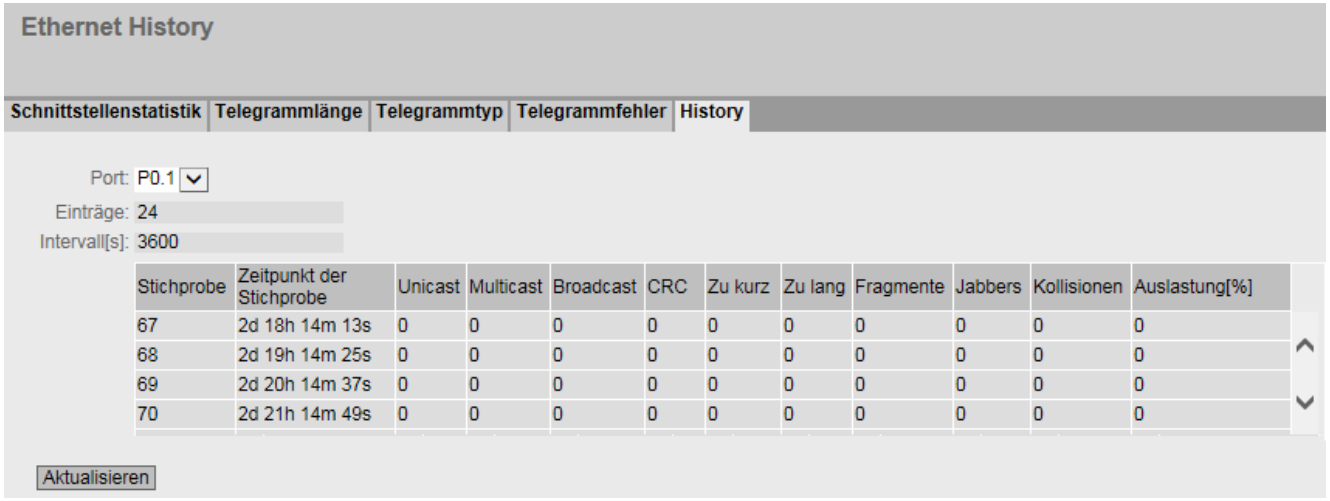


Bild 5-1 History

Einstellungen

- **Port**
  Wählen Sie den Port, für den die History angezeigt werden soll.

Beschreibung der angezeigten Werte

- **Einträge**
  Maximale Anzahl der Stichproben, die gleichzeitig gespeichert werden.
- **Intervall[s]**
  Intervall, nachdem der aktuelle Stand der Statistik als Stichprobe gespeichert wird.

Die Tabelle gliedert sich in folgende Spalten:

- **Stichprobe**
  Nummer der Stichprobe
- **Zeitpunkt der Stichprobe**
  Systembetriebszeit, zu der die Stichprobe genommen wurde.
- **Unicast**
  Anzahl der empfangenen Unicast-Telegramme.
- **Multicast**
  Anzahl der empfangenen Multicast-Telegramme.

- **Broadcast**
  Anzahl der empfangenen Broadcast-Telegramme.
- **CRC**
  Anzahl von Telegrammen mit fehlerhafter CRC-Prüfsumme.
- **Zu kurz**
  Anzahl der Telegramme, die kleiner als 64 Bytes sind.
- **Zu lang**
  Anzahl der Telegramme, die verworfen werden, weil sie zu groß sind.
- **Fragmente**
  Anzahl der Telegramme, die kleiner als 64 Bytes sind und eine fehlerhafte CRC-Prüfsumme haben.
- **Jabbers**
  Anzahl der Telegramme mit VLAN-Tag, die eine fehlerhafte CRC-Prüfsumme haben und verworfen werden, weil sie zu groß sind.
- **Kollisionen**
  Anzahl der Kollisionen empfangener Telegramme.
- **Auslastung[%]**
  Auslastung des Ports während einer Stichprobe.

5.3.9 Unicast

Status der Unicast-Filtertabelle

Diese Seite zeigt den aktuellen Inhalt der Unicast-Filtertabelle. In dieser Tabelle sind die Quelladressen von Unicast-Adresstelegrammen aufgeführt. Einträge können entweder dynamisch erfolgen, wenn ein Teilnehmer ein Telegramm an einen Port sendet, oder statisch durch Parametrierung seitens des Anwenders.

Abhängigkeit vom "Base Bridge-Modus"

Die angezeigten Spalten sind davon abhängig, welcher "Base Bridge-Modus" eingestellt ist. Wenn Sie den "Base Bridge-Modus" ändern, gehen die bestehenden Einträge verloren.

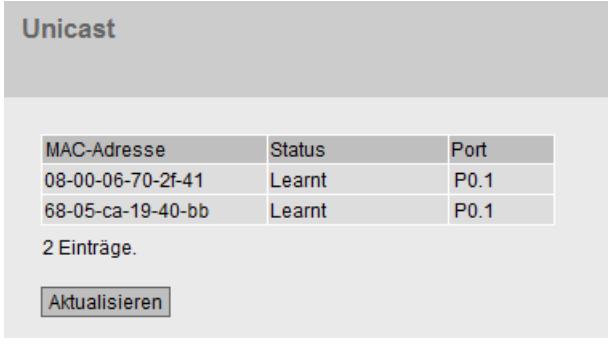


Bild 5-2 Base Bridge-Modus: 802.1D Transparent Bridge

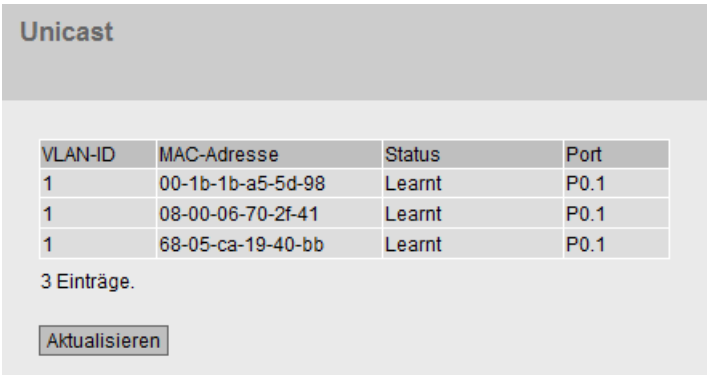


Bild 5-3 Base Bridge-Modus: 802.1Q VLAN Bridge

Beschreibung

Die Tabelle kann folgende Spalten enthalten:

- **VLAN-ID**
  Zeigt die VLAN-ID, die dieser MAC-Adresse zugeordnet ist.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Teilnehmers, die das Gerät gelernt hat oder die der Anwender projektiert hat.
- **Status**
  Zeigt den Status jedes Adresseintrags:
  - Learnt
    Die angegebene Adresse wurde durch Empfang eines Telegramms dieses Teilnehmers gelernt und wird nach Ablauf der Aging Time wieder gelöscht, sollten keine weiteren Pakete dieses Teilnehmers empfangen werden.

    Hinweis

    Bei einem Link-Down werden gelernte MAC-Einträge gelöscht.
  - Static
    Vom Anwender projektiert. Statische Adressen sind permanent gespeichert, d.h. sie werden nach Ablauf der Aging Time oder beim Neustart des Switches nicht gelöscht.
  - Other
    Die angegebene Adresse wurde durch Private VLAN indirekt gelernt.
- **Port**
  Zeigt an, über welchen Port der Teilnehmer mit der angegebenen Adresse erreichbar ist. Vom Gerät empfangene Telegramme, deren Zieladresse mit dieser Adresse übereinstimmt, werden an diesen Port weitergegeben.

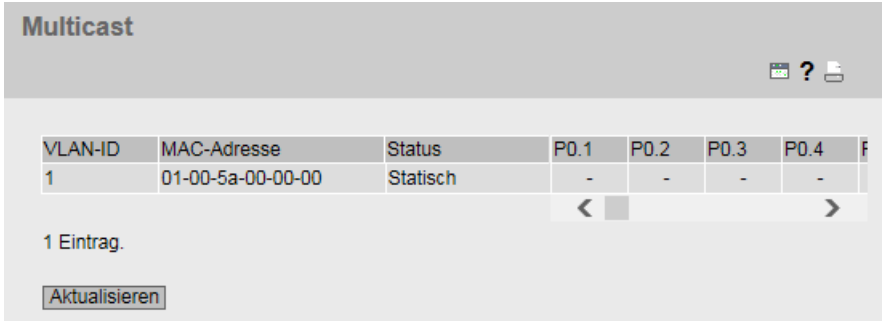
5.3.10 Multicast

Status der Multicast-Filtertabelle

Diese Tabelle zeigt die aktuell in der Filtertabelle eingetragenen Multicast-Telegramme mit ihren Zielports. Die Einträge können dynamisch (das Gerät hat sie gelernt) oder statisch (der Anwender hat sie parametriert) erfolgt sein.

Abhängigkeit vom "Base Bridge-Modus"

Wenn Sie den "Base Bridge-Modus" ändern, gehen die bestehenden Einträge verloren.



Beschreibung

Die Tabelle kann folgende Spalten enthalten:

- **VLAN-ID**
  Zeigt die VLAN-ID des VLANs an, dem die MAC-Multicast-Adresse zugeordnet ist.
- **MAC-Adresse**
  Zeigt die MAC-Multicast-Adresse an, die das Gerät gelernt hat oder die der Anwender projektiert hat.

- **Status**
  Zeigt den Status jedes Adress-Eintrags. Dabei sind folgende Angaben möglich:
  - Statisch
    Die Adresse wurde vom Anwender statisch eingetragen. Statische Adressen sind permanent gespeichert, d.h. sie werden nicht nach Ablauf der Aging Time oder beim Neustart des Geräts gelöscht. Sie können vom Anwender gelöscht werden.
  - IGMP
    Der Zielport für diese Adresse wurde über IGMP ermittelt.
  - GMRP
    Der Zielport für diese Adresse wurde über ein empfangenes GMRP-Telegramm registriert.
- **Liste der Ports**
  Für jeden Steckplatz gibt es eine Spalte. Innerhalb einer Spalte wird für jeden Port die Zugehörigkeit zur Multicast-Gruppe angezeigt:
  - M
    (Member) Über diesen Port werden Multicast-Telegramme gesendet.
  - R
    (Registered) Mitglied der Multicast-Gruppe, die Registrierung erfolgte über ein GMRP-Telegramm.
  - I
    (IGMP) Mitglied der Multicast-Gruppe, die Registrierung erfolgte über ein IGMP-Telegramm.
  - –
    Kein Mitglied der Multicast-Gruppe. Über diesen Port werden keine Multicast-Telegramme mit der definierten Multicast-MAC-Adresse gesendet.
  - F
    (Forbidden) Kein Mitglied der Multicast-Gruppe. Außerdem darf an diesem Port nicht dynamisch über IGMP gelernt werden.

5.3.11 LLDP

Status der Nachbarschaftstabelle

Diese Seite zeigt den aktuellen Inhalt der Nachbarschaftstabelle. In dieser Tabelle sind die Informationen gespeichert, die der LLDP-Agent von angeschlossenen Geräten empfangen hat.

Über welche Schnittstellen der LLDP-Agent Informationen empfängt bzw. versendet, legen Sie in folgendem Kapitel fest: "Layer 2 > LLDP".

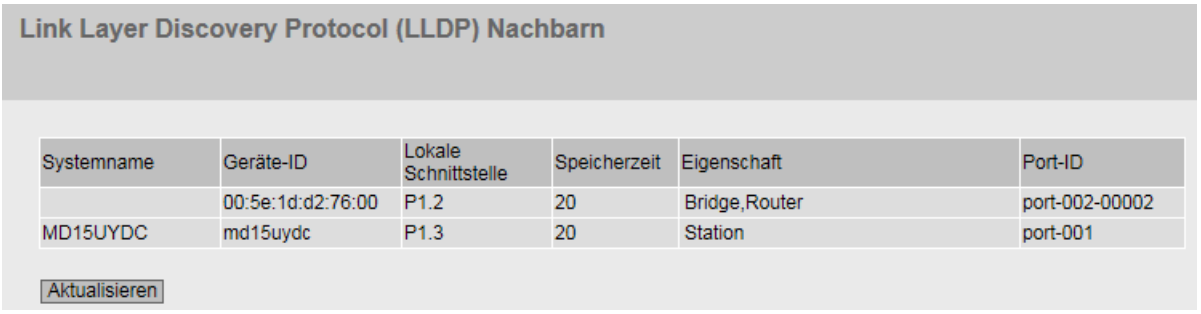


Bild 5-4 Information LLDP

Beschreibung der angezeigten Werte

Die Tabelle enthält folgende Spalten:

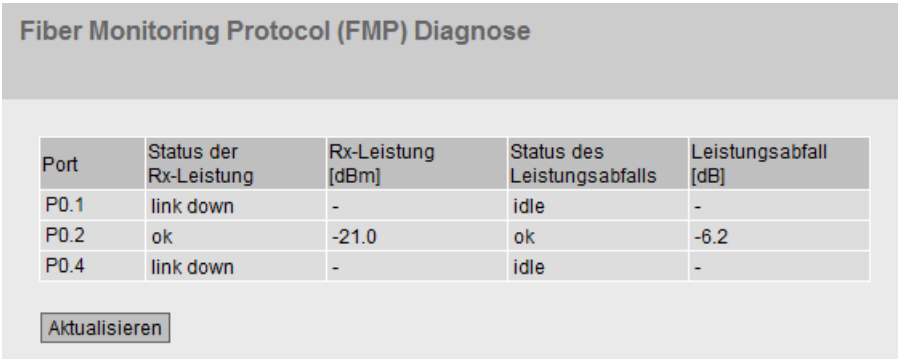
- **Systemname**
  Systemname des angeschlossenen Geräts.
- **Geräte-ID**
  Gerätekennung des angeschlossenen Geräts. Die Geräte-ID entspricht dem Gerätenamen, der über PST (STEP 7) vergeben wird. Wenn kein Gerätename vergeben ist, wird die MAC-Adresse des Geräts angezeigt.
- **Lokale Schnittstelle**
  Port, an dem der IE-Switch die Informationen empfangen hat.
- **Speicherzeit**
  Ein Eintrag bleibt für die hier angegebene Zeit im Gerät gespeichert. Wenn der IE-Switch in dieser Zeit keine neuen Informationen von dem angeschlossenen Gerät erhält, wird der Eintrag gelöscht.
- **Eigenschaft**
  Zeigt die Eigenschaften des angeschlossenen Geräts an:
  - Router
  - Bridge
  - Telephone
  - DOCSIS Cable Device
  - WLAN Access Point
  - Repeater
  - Station
  - Other
- **Port-ID**
  Port des Geräts, der mit dem IE-Switch verbunden ist.

5.3.12 Fiber Monitoring Protocol

Überwachung optischer Strecken

Mit Fiber Monitoring können Sie optische Strecken überwachen. Die Tabelle zeigt den aktuellen Zustand der Ports.

Welche Werte überwacht werden, stellen Sie auf folgender Seite ein: "Layer 2 > FMP".



Beschreibung der angezeigten Werte

Port

Zeigt die optischen Ports an, die Fiber Monitoring unterstützen. Dies ist von den Transceivern abhängig.

Status der Rx-Leistung

- **disabled**
  Fiber Monitoring ist deaktiviert.
- **ok**
  Der Wert für die Empfangsleistung der optischen Strecke liegt innerhalb der eingestellten Grenzen.
- **maint. req.**
  Die Strecke sollte überprüft werden.
  Es wird eine Warnung gemeldet.
- **maint. dem.**
  Die Strecke muss überprüft werden.
  Es wird ein Alarm gemeldet und die Fehler-LED leuchtet.
- **link down**
  Die Verbindung zum Kommunikationspartner ist unterbrochen. Es wird kein Link detektiert.

Rx-Leistung[dBm]

Zeigt den aktuellen Wert der Empfangsleistung an. Der Wert kann eine Toleranz von +/- 3 dB haben.

Wenn keine Verbindung (Link down) besteht oder Fiber Monitoring deaktiviert ist, wird "-" angezeigt. Wenn bei dem Partner-Port Fiber Monitoring nicht aktiviert ist, wird der Wert 0.0 angezeigt.

Status des Leistungsabfalls

Um den Leistungsabfall der Verbindung überwachen zu können, muss für den optischen Port des Verbindungspartners die Funktion Fiber Monitoring aktiviert sein.

- **disabled**
  Fiber Monitoring ist deaktiviert.
- **ok**
  Der Wert für den Leistungsabfall der optischen Strecke liegt innerhalb der definierten Grenzen.
- **maint. req.**
  Die Strecke sollte überprüft werden.
  Es wird eine Warnung gemeldet.
- **maint. dem.**
  Die Strecke muss überprüft werden.
  Es wird ein Alarm gemeldet und die Fehler-LED leuchtet.
- **idle**
  Der Port hat keine Verbindung zu einem anderen Port mit aktiviertem Fiber Monitoring. Wenn 5 Zyklen lang keine Diagnoseinformationen vom optischen Port des Verbindungspartners empfangen wurden, gilt die Fiber Monitoring-Verbindung als unterbrochen. Ein Zyklus dauert 5 Sekunden.

Leistungsabfall[dB]

Zeigt den aktuellen Wert des Leistungsabfalls an. Der Wert kann eine Toleranz von +/- 3 dB haben.

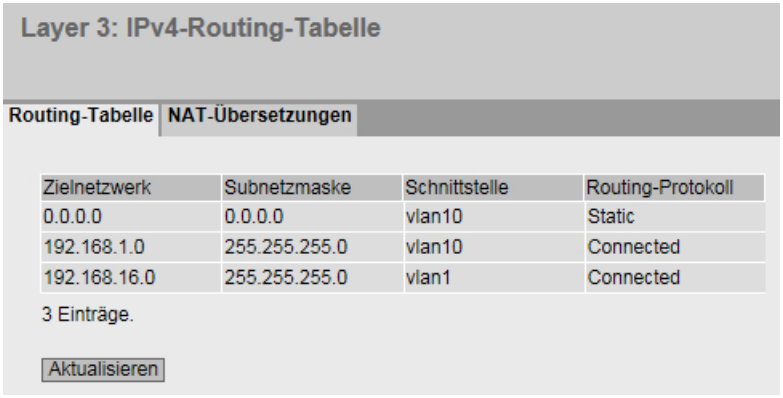
Wenn keine Verbindung (Link down) besteht, Fiber Monitoring deaktiviert ist oder der Partner-Port Fiber Monitoring nicht unterstützt, wird "-" angezeigt.

5.3.13 Routing

5.3.13.1 Routing-Tabelle

Einleitung

Diese Seite zeigt die Routen an, die aktuell verwendet werden.



Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Spalten:

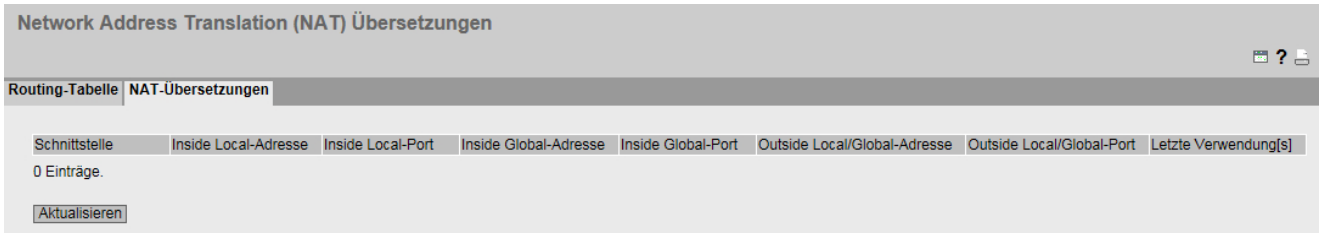
- **Zielnetzwerk**
  Zeigt die Ziel-Adresse dieser Route an.
- **Subnetzmaske**
  Zeigt die Subnetzmaske dieser Route an.
- **Schnittstelle**
  Zeigt die Schnittstelle für diese Route an.
- **Routing-Protokoll**
  Zeigt an, aus welchem Routing-Protokoll der Eintrag der Routingtabelle stammt. Folgende Einträge sind möglich:
  - Connected: Verbundene Routen
  - Static: Statische Routen
  - RIP: Routen über RIP
  - OSPF: Routen über OSPF
  - Other: Sonstige Routen

5.3.13.2 NAT-Übersetzungen

Übersicht

Diese Seite zeigt die aktiven NAT-Verbindungen an.

Beschreibung der angezeigten Werte



Die Tabelle gliedert sich in folgende Spalten:

- **Schnittstelle**
  Zeigt die IP-Schnittstelle an.
- **Inside Local-Adresse**
  Zeigt die tatsächliche Adresse des Geräts an, das von extern erreichbar sein soll.
- **Inside Local-Port**
  Zeigt den Port an, der der Inside Local-Adresse zugeordnet ist.
- **Inside Global-Adresse**
  Zeigt die Adresse an, unter der das Gerät von extern erreichbar ist.
- **Inside Global-Port**
  Zeigt den Port an, der der Inside Global-Adresse zugeordnet ist.
- **Outside Local/Global-Adresse**
  Zeigt die Adresse des Kommunikationspartners an.
- **Outside Local/Global-Port**
  Zeigt den Port des externen Kommunikationspartners an.
- **Letzte Verwendung[s]**
  Zeigt den Zeitpunkt an, zu dem das letzte Paket übertragen wurde.

5.3.14 DHCP-Server

Diese Seite zeigt an, welche IPv4-Adressen den Geräten vom DHCP-Server zugeordnet wurden.

Beschreibung

- **IP-Adresse**
  Zeigt die IPv4-Adresse an, die dem DHCP-Client zugeordnet ist.
- **Pool-ID**
  Zeigt die Nummer des IPv4-Adressbands an.
- **Identifikationsmethode**
  Zeigt die Methode an, nach der der DHCP-Client identifiziert wird.
- **Identifikationswert**
  Zeigt die MAC-Adresse oder die Client-ID des DHCP-Clients an.
- **Zuordnungsmethode**
  Zeigt an, ob die IPv4-Adresse statisch oder dynamisch vergeben wurde. Die statischen Einträge konfigurieren Sie unter "System > DHCP > Statische Zuordnung".
- **Zuordnungsstatus**
  Zeigt den Status der Zuordnung an.
  - Zugeordnet
    Die Zuordnung wird verwendet.
  - Nicht verwendet
    Die Zuordnung wird nicht verwendet.
  - Wird geprüft
    Die Zuordnung wird geprüft.
  - Unbekannt
    Der Status der Zuordnung ist unbekannt.
- **Ablaufzeit**
  Zeigt an, bis wann die vergebene IPv4-Adresse noch gültig ist. Bis zu diesem Zeitpunkt muss der DHCP-Client entweder eine neue IPv4-Adresse anfordern oder die Gültigkeitsdauer der vergebenen IPv4-Adresse verlängern.

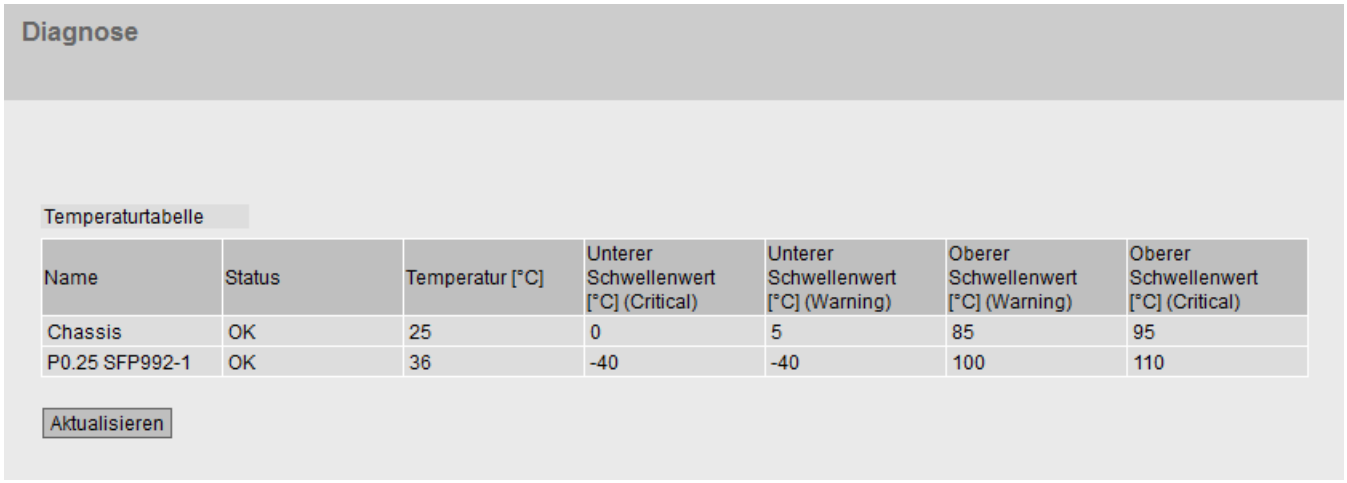
5.3.15 Diagnose

Diese Seite zeigt die Temperaturwerte interner sowie externer Baugruppen des Geräts an. Die Baugruppen werden nur angezeigt, wenn sie Temperaturinformationen zur Verfügung stellen. Wenn Sie eine Baugruppe hinzufügen oder entfernen, wird die Anzeige automatisch angepasst.

Wenn der Temperaturwert die angezeigten Schwellenwerte unter- bzw. überschreitet, ändert sich der Status entsprechend.

Die Schwellenwerte werden vom Gerät vorgegeben und können nicht geändert werden. Wenn keine Schwellenwerte vorgegeben werden, wird "-" angezeigt.

Auf der Seite "System > Ereignisse > Konfiguration" können Sie einstellen, wie das Gerät die Statusänderung meldet.



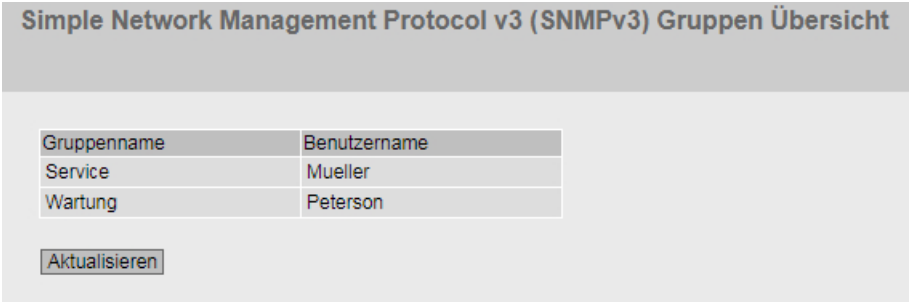
Beschreibung

- **Name**
  Zeigt den Namen der Baugruppe an.
  Die Angaben in der Zeile "Chassis" beziehen sich auf die Innentemperatur des Gehäuses.
  Bei Stecktransceivern werden der Port und der Typ angegeben.
- **Status**
  Abhängig von dem Verhältnis zwischen den Schwellenwerten und der aktuellen Temperatur werden folgende Statuswerte mit aufsteigender Priorität angezeigt:
  - OK
    Der Temperaturwert liegt innerhalb der vorgegebenen Schwellenwerte.
  - WARNING
    Der untere oder obere Schwellenwert des Severity-Levels "Warning" wurde unter- bzw. überschritten. Die Temperatur befindet sich noch in einem normalen Bereich. Das Gerät hat einen Abfall bzw. Anstieg der Temperatur erkannt, z. B. durch eine veränderte Kühlung des Schaltschranks. Die Temperatur sollte überprüft werden.
  - CRITICAL
    Der untere oder obere Schwellenwert des Severity-Levels "Critical" wurde unter- bzw. überschritten. Das Gerät muss überprüft werden. Eine zu geringe bzw. zu hohe Temperatur kann zu einer eingeschränkten Leistung oder Schäden am Gerät führen.
  - INVALID
    Der Wert konnte nicht ausgelesen werden oder ist ungültig. Im Feld "Temperatur [°C]" wird "-" angezeigt.
  - INITIAL
    Es wurden noch keine Daten ausgelesen. In allen Feldern wird "-" angezeigt.
- **Temperatur [°C]**
  Zeigt den aktuellen Wert der Temperatur an. Die Anzeige wird in regelmäßigen Abständen aktualisiert.
  Der Wert kann eine Toleranz von +/- 3 °C haben. Dadurch kann sich der Wert bei gleichen Geräten mit ähnlichen Umgebungsbedingungen unterscheiden.

- **Unterer Schwellenwert [°C] (Critical)**
  Wenn dieser Wert unterschritten wird, ändert sich der Status in "CRITICAL". Sie können konfigurieren, dass Sie durch eine Meldung informiert werden.
- **Unterer Schwellenwert [°C] (Warning)**
  Wenn dieser Wert unterschritten wird, ändert sich der Status in "WARNING". Sie können konfigurieren, dass Sie durch eine Meldung informiert werden.
- **Oberer Schwellenwert [°C] (Warning)**
  Wenn dieser Wert überschritten wird, ändert sich der Status in "WARNING". Sie können konfigurieren, dass Sie durch eine Meldung informiert werden.
- **Oberer Schwellenwert [°C] (Critical)**
  Wenn dieser Wert überschritten wird, ändert sich der Status in "CRITICAL". Sie können konfigurieren, dass Sie durch eine Meldung informiert werden.

5.3.16 SNMP

Diese Seite zeigt die angelegten SNMPv3-Gruppen an. Die SNMPv3-Gruppen konfigurieren Sie unter "System > SNMP".



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Gruppenname**
  Zeigt den Gruppennamen an.
- **Benutzername**
  Zeigt den Benutzer an, welcher der Gruppe zugeordnet ist.

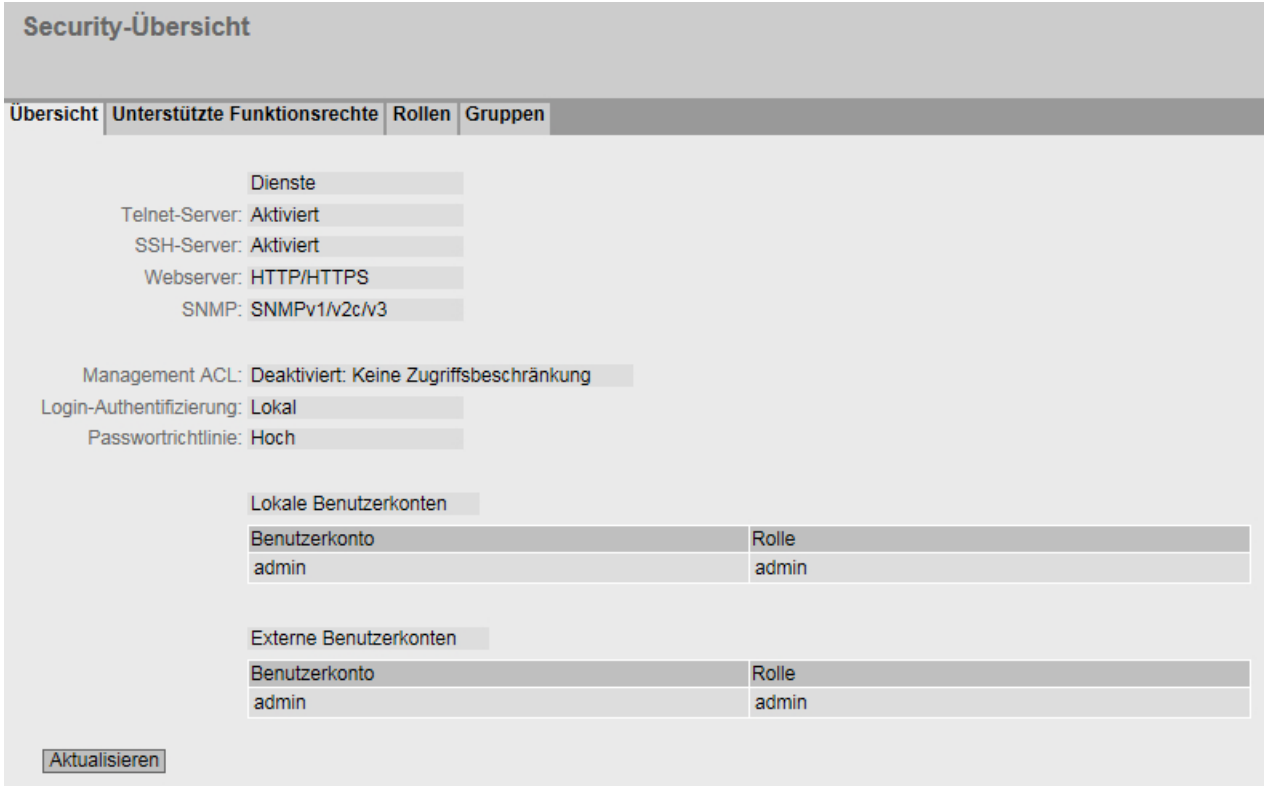
5.3.17 Security

5.3.17.1 Übersicht

Hinweis

Es ist von den Rechten des angemeldeten Benutzers abhängig, welche Werte angezeigt werden.

Die Seite zeigt die Sicherheitseinstellungen sowie die lokalen und externen Benutzerkonten an.



Beschreibung

Dienste

Die Liste "Dienste" zeigt die Sicherheitseinstellungen an.

- **Telnet-Server**
  Die Einstellung konfigurieren Sie unter "System > Konfiguration".
  - Aktiviert: Unverschlüsselter Zugriff auf das CLI
  - Deaktiviert: Kein unverschlüsselter Zugriff auf das CLI
- **SSH-Server**
  Die Einstellung konfigurieren Sie unter "System > Konfiguration".
  - Aktiviert: Verschlüsselter Zugriff auf das CLI
  - Deaktiviert: Kein verschlüsselter Zugriff auf das CLI
- **Webserver**
  Die Einstellung konfigurieren Sie unter "System > Konfiguration"
  - HTTP/HTTPS: Der Zugriff auf das WBM ist über HTTP und HTTPS möglich.
  - HTTPS: Der Zugriff auf das WBM ist nur noch über HTTPS möglich.
- **SNMP**
  Die Einstellung konfigurieren Sie unter "System > SNMP > Allgemein".
  - "-" (SNMP deaktiviert)
    Ein Zugriff auf die Geräteparameter ist über SNMP nicht möglich.
  - SNMPv1/v2c/v3
    Ein Zugriff auf die Geräteparameter ist mit den SNMP Versionen 1, 2c oder 3 möglich.
  - SNMPv3
    Ein Zugriff auf die Geräteparameter ist nur mit der SNMP Version 3 möglich.
- **Management ACL**
  Einstellung konfigurieren Sie unter "Security > Management ACL"
  - Aktiviert: Nur eingeschränkter Zugriff: Der Zugang wird über eine Access Control List (ACL) eingeschränkt.
  - Deaktiviert: Keine Zugriffsbeschränkung: Management ACL ist nicht aktiviert.
  - Aktiviert: Keine Zugriffsbeschränkung: Management ACL ist aktiviert, aber der Zugang wird nicht über eine Access Control List (ACL) eingeschränkt.

- **Login-Authentifizierung**
  Die Einstellung konfigurieren Sie unter "Security > AAA > Allgemein".
  - Lokal
    Die Authentifizierung muss lokal auf dem Gerät erfolgen.
  - RADIUS
    Die Authentifizierung muss über einen RADIUS-Server erfolgen.
  - Lokal und RADIUS
    Die Authentifizierung kann sowohl über die im Gerät vorhandenen Benutzer (Benutzername und Passwort) als auch über einen RADIUS-Server erfolgen.
    Es wird zuerst in der lokalen Datenbank nach dem Benutzer gesucht. Wenn der Benutzer dort nicht vorhanden ist, wird eine RADIUS-Anfrage geschickt.
  - RADIUS mit Fallback Lokal
    Die Authentifizierung muss über einen RADIUS-Server erfolgen.
    Nur wenn der RADIUS-Server im Netz nicht erreichbar ist, wird eine lokale Authentifizierung durchgeführt.
- **Passwortrichtlinie**
  Zeigt an, welche Passwortrichtlinie aktuell verwendet wird.

Lokale und externe Benutzerkonten

Lokale Benutzerkonten und Rollen konfigurieren Sie unter "Security > Benutzer".

Wenn Sie ein lokales Benutzerkonto anlegen, wird automatisch auch ein externes Benutzerkonto erzeugt.

Bei lokalen Benutzerkonten handelt es sich um Benutzer mit jeweils einem Passwort zur Anmeldung auf dem Gerät.

In der Tabelle "Externe Benutzerkonten" wird ein Benutzer mit einer Rolle verknüpft. In diesem Beispiel wird der Benutzer "Observer" mit der Rolle "user" verknüpft. Der Benutzer ist auf einem RADIUS-Server definiert. Die Rolle ist lokal auf dem Gerät definiert. Wenn ein RADIUS-Server einen Benutzer authentifiziert, die zugehörige Gruppe jedoch unbekannt oder nicht vorhanden ist, prüft das Gerät, ob es für den Benutzer einen Eintrag in der Tabelle "Externe Benutzerkonten" gibt. Wenn ein entsprechender Eintrag existiert, wird der Benutzer mit den Rechten der verknüpften Rolle angemeldet. Wenn die zugehörige Gruppe auf dem Gerät bekannt ist, werden beide Tabellen ausgewertet. Dem Benutzer wird die Rolle mit den größeren Rechten zugewiesen.

Hinweis

Die Tabelle "Externe Benutzerkonten" wird nur ausgewertet, wenn Sie im RADIUS-Autorisierungsmodus "Herstellerspezifisch" eingestellt haben.

Über CLI können Sie auf die externen Benutzerkonten zugreifen.

Die Tabellen "Lokale Benutzerkonten" und "Externe Benutzerkonten" gliedern sich in folgende Spalten:

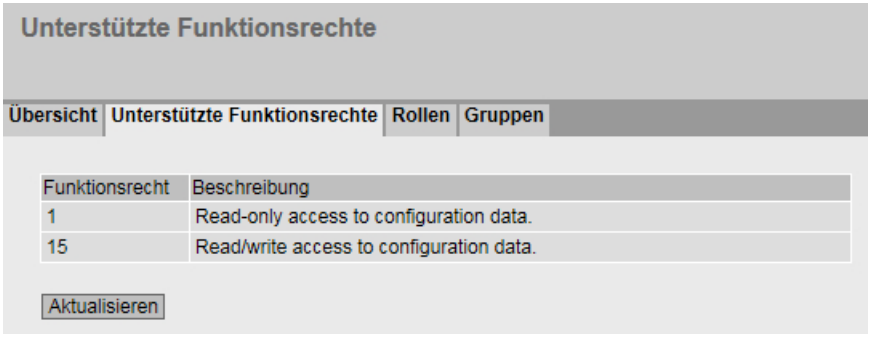
- **Benutzerkonto**
  Zeigt den Namen des lokalen Benutzers an.
- **Rolle**
  Zeigt die Rolle des Benutzers an. Weitere Informationen zu den Funktionsrechten der Rolle erhalten Sie unter "Information > Security > Rollen".

5.3.17.2 Unterstützte Funktionsrechte

Hinweis

Es ist von der Rolle des angemeldeten Benutzers abhängig, welche Werte angezeigt werden.

Die Seite zeigt die Funktionsrechte an, die lokal auf dem Gerät verfügbar sind.



Beschreibung der angezeigten Werte

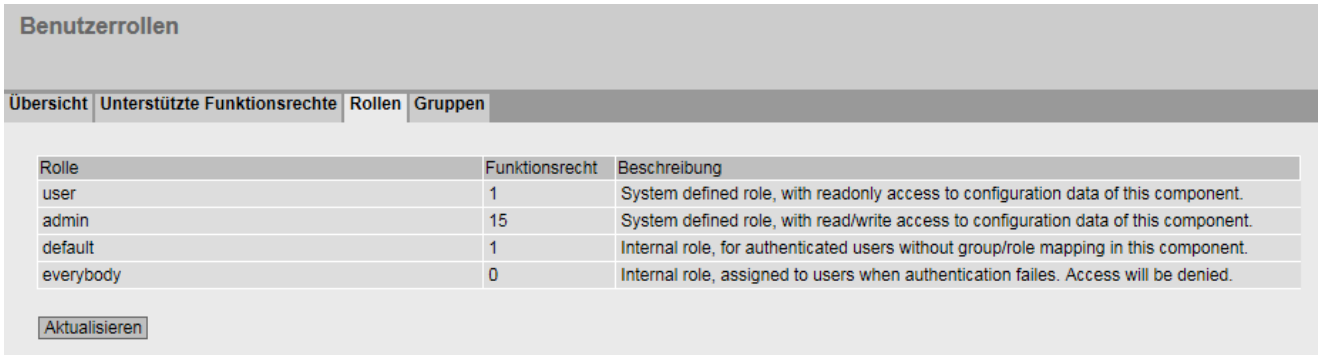
- **Funktionsrecht**
  Zeigt die Nummer des Funktionsrechts an. Den Nummern sind unterschiedliche Rechte in Bezug auf die Geräteparameter zugeordnet.
- **Beschreibung**
  Zeigt die Beschreibung des Funktionsrechts an.

5.3.17.3 Rollen

Hinweis

Es ist von der Rolle des angemeldeten Benutzers abhängig, welche Werte angezeigt werden.

Die Seite zeigt die Rollen an, die lokal auf dem Gerät gültig sind.



Beschreibung

Die Tabelle enthält folgende Spalten:

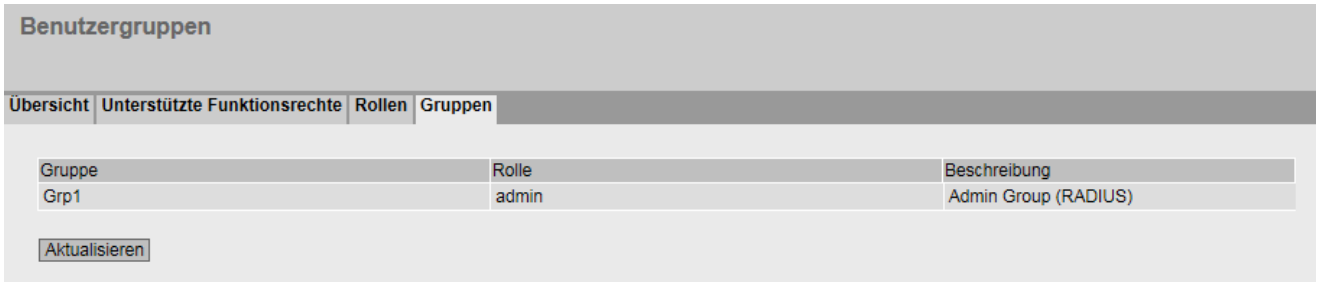
- **Rolle**
  Zeigt den Namen der Rolle an.
- **Funktionsrecht**
  Zeigt das Funktionsrecht der Rolle an:
  - 1
    Benutzer mit dieser Rolle können Geräteparameter lesen, aber nicht verändern.
  - 15
    Benutzer mit dieser Rolle können Geräteparameter sowohl lesen als auch verändern.
  - 0
    Hierbei handelt es sich um eine Rolle, die das Gerät intern vergibt, wenn ein Benutzer nicht authentifiziert werden konnte. Dem Benutzer wird der Zugriff auf das Gerät verweigert.
- **Beschreibung**
  Zeigt eine Beschreibung der Rolle an.

5.3.17.4 Gruppen

Hinweis

Es ist von der Rolle des angemeldeten Benutzers abhängig, welche Werte angezeigt werden.

Diese Seite zeigt an, welche Gruppe mit welcher Rolle verknüpft ist. Die Gruppe ist auf einem RADIUS-Server definiert. Die Rolle ist lokal auf dem Gerät definiert.



Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Spalten:

- **Gruppe**
  Zeigt den Namen der Gruppe an. Der Name entspricht der Gruppe auf dem RADIUS-Server.
- **Rolle**
  Zeigt den Namen der Rolle an. Benutzer, die über den RADIUS-Server mit der verknüpften Gruppe authentifiziert werden, erhalten die Rechte dieser Rolle lokal auf dem Gerät.
- **Beschreibung**
  Zeigt die Beschreibung für die Verknüpfung an.

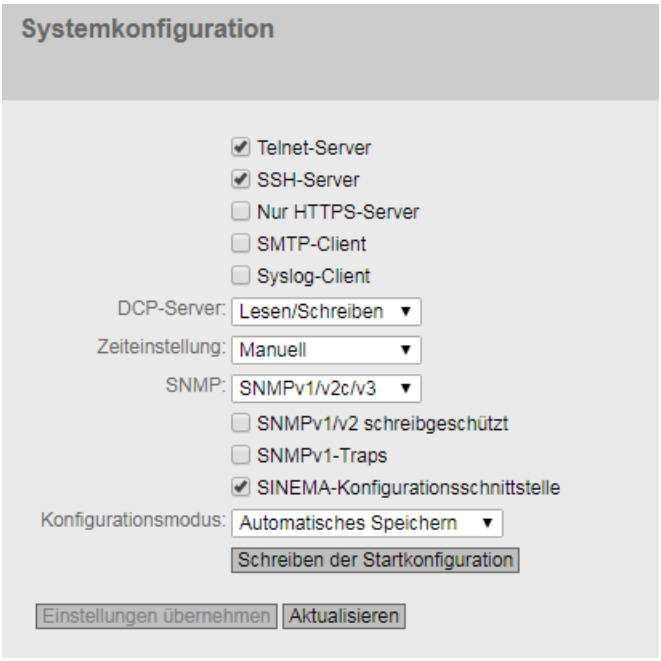
5.4 Das Menü "System"

5.4.1 Konfiguration

Systemkonfiguration

Die WBM-Seite enthält die Konfigurationsübersicht über die Zugriffsmöglichkeiten des Geräts.

Legen Sie fest, über welche Dienste auf das Gerät zugegriffen wird. Zu einigen Diensten gibt es weitere Konfigurationsseiten, auf denen detailliertere Einstellungen möglich sind.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Telnet-Server**
  Aktivieren oder deaktivieren Sie den Dienst Telnet-Server für den unverschlüsselten Zugriff auf das CLI.
- **SSH-Server**
  Aktivieren oder deaktivieren Sie den Dienst SSH-Server für den verschlüsselten Zugriff auf das CLI.
- **Nur HTTPS-Server**
  Wenn diese Funktion aktiviert ist, können Sie nur über HTTPS auf das WBM zugreifen.
- **SMTP-Client**
  Aktivieren oder deaktivieren Sie den SMTP-Client. Weitere Einstellungen konfigurieren Sie unter "System > SMTP-Client".
- **Syslog-Client**
  Aktivieren oder deaktivieren Sie den Syslog-Client. Weitere Einstellungen konfigurieren Sie unter "System > Syslog-Client".
- **DCP-Server**
  Legen Sie fest, ob auf das Gerät mit DCP (Discovery and Configuration Protocol) zugegriffen werden kann:
  - "-" (Deaktiviert)
    DCP ist deaktiviert. Geräteparameter können weder gelesen noch geändert werden.
  - Lesen/Schreiben
    Mit DCP können Geräteparameter sowohl gelesen als auch verändert werden.
  - Schreibgeschützt
    Mit DCP können Geräteparameter zwar gelesen aber nicht verändert werden.

- **Zeiteinstellung**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungen sind möglich:
  - Manuell
    Die Systemzeit wird manuell eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > Systemzeit > Manuelle Einstellung".
  - SIMATIC Time
    Die Systemzeit wird über einen SIMATIC Zeitgeber eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > Systemzeit > SIMATIC Time Client".
  - SNTP-Client
    Die Systemzeit wird über einen SNTP-Server eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > Systemzeit > SNTP-Client".
  - NTP-Client
    Die Systemzeit wird über einen NTP-Server eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > Systemzeit > NTP-Client".
- **SNMP**
  Wählen Sie aus der Klappliste das Protokoll. Folgende Einstellungen sind möglich:
  - "-" (SNMP deaktiviert)
    Ein Zugriff auf die Geräteparameter ist über SNMP nicht möglich.
  - SNMPv1/v2c/v3
    Ein Zugriff auf die Geräteparameter ist mit den SNMP Versionen 1, 2c oder 3 möglich. Weitere Einstellungen konfigurieren Sie unter "System > SNMP > Allgemein".
  - SNMPv3
    Ein Zugriff auf die Geräteparameter ist nur mit SNMP Version 3 möglich. Weitere Einstellungen konfigurieren Sie unter " System > SNMP > Allgemein".
- **SNMPv1/v2 schreibgeschützt**
  Aktivieren oder deaktivieren Sie den schreibenden Zugriff auf SNMP-Variablen bei SNMPv1/v2c.
- **SNMPv1-Traps**
  Aktivieren oder deaktivieren Sie das Versenden von SNMPv1-Traps (Alarmtelegramme). Weitere Einstellungen konfigurieren Sie unter "System > SNMP > Traps".

- **SINEMA-Konfigurationsschnittstelle**
  Wenn die SINEMA Konfigurationsschnittstelle aktiviert ist, können Sie Konfigurationen über STEP 7 Basic / Professional auf den IE-Switch laden.
- **Konfigurationsmodus**
  Wählen Sie aus der Klappliste die Betriebsart. Folgende Betriebsarten sind möglich:
  - Automatisches Speichern
    Automatischer Sicherungsbetrieb. Ca. 1 Minute nach der letzten Parameteränderung oder vor dem Neustart des Geräts wird die Konfiguration automatisch abgespeichert. Zusätzlich erscheint im Anzeigebereich folgende Meldung "Die Änderungen werden automatisch in x Sekunden gespeichert. Um die Änderungen sofort zu speichern, klicken Sie auf 'Schreiben der Startkonfiguration'."

    Hinweis

    Unterbrechung des Speichervorgangs

    Der Speichervorgang startet erst nachdem der Timer in der Meldung abgelaufen ist. Die Dauer des Speichervorgangs ist vom Gerät abhängig.
    - Schalten Sie das Gerät nicht sofort aus, nachdem der Timer abgelaufen ist.
  - Trial
    Trial-Modus. Im Trial-Modus werden Änderungen zwar übernommen aber nicht in der Konfigurationsdatei (Startup Configuration) gespeichert.
    Um Änderungen in der Konfigurationsdatei abzuspeichern, verwenden Sie die Schaltfläche "Schreiben der Startkonfiguration". Zusätzlich wird im Anzeigebereich die Meldung "Der Konfigurationsmodus Trial ist aktiv - Klicken Sie auf die Schaltfläche "Schreiben der Startkonfiguration" um Ihre Einstellungen zu speichern" angezeigt, sobald es ungespeicherte Änderungen gibt. Diese Meldung ist auf jeder WBM-Seite sichtbar, bis die vorgenommenen Änderungen entweder gespeichert werden oder das Gerät neu gestartet wird.

Vorgehensweise zur Konfiguration

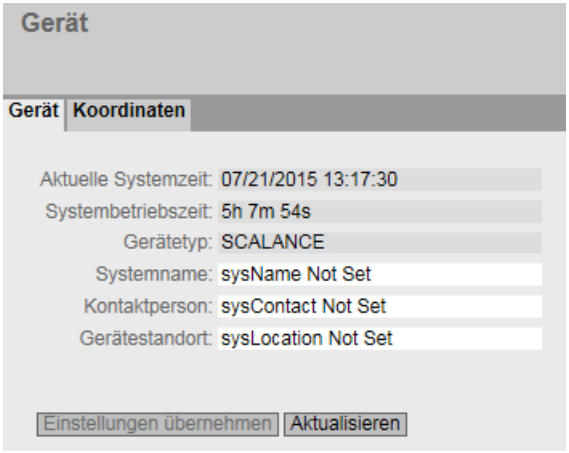
1. Um die gewünschte Funktion zu nutzen, aktivieren Sie das entsprechende Optionskästchen.
2. Wählen Sie aus den Klapplisten die gewünschten Optionen.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.4.2 Allgemein

5.4.2.1 Gerät

Allgemeine Geräteinformationen

Diese Seite enthält die allgemeinen Geräteinformationen.



Die Felder "Aktuelle Systemzeit", "Systembetriebszeit" und "Gerätetyp" können nicht geändert werden.

Beschreibung

Die Seite enthält folgende Felder:

- **Aktuelle Systemzeit**
  Zeigt die aktuelle Systemuhrzeit an. Die Systemuhrzeit wird entweder vom Anwender eingestellt oder per Uhrzeittelegramm synchronisiert: entweder SINEC H1 Uhrzeittelegramm, NTP oder SNTP. (Nur lesbar)
- **Systembetriebszeit**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an. (Nur lesbar)
- **Gerätetyp**
  Zeigt die Typenbezeichnung des Geräts an. (Nur lesbar)
- **Systemname**
  Sie können den Namen des Geräts eintragen. Der eingetragene Name wird im Auswahlbereich angezeigt. Es sind maximal 255 Zeichen möglich.
  Der Systemname wird auch in der CLI-Eingabeaufforderung (Prompt) angezeigt. In der CLI-Eingabeaufforderung ist die Anzahl der Zeichen begrenzt. Der Systemname wird nach 16 Zeichen abgeschnitten.

- **Kontaktperson**
  Sie können den Namen einer Kontaktperson eintragen, die für die Verwaltung des Geräts zuständig ist. Es sind maximal 255 Zeichen möglich.
- **Gerätestandort**
  Sie können den Montageort des Geräts eintragen. Der eingetragene Montageort wird im Auswahlbereich angezeigt. Es sind maximal 255 Zeichen möglich.

Hinweis

In den Eingabefeldern wird der ASCII-Code 0x20 bis 0x7e verwendet.

Vorgehensweise

1. Tragen Sie in das Eingabefeld "Kontaktperson" den für das Gerät zuständigen Ansprechpartner ein.
2. Tragen Sie in das Eingabefeld "Gerätestandort" die Ortsbezeichnung des Aufstellungsorts ein.
3. Tragen Sie in das Eingabefeld "Systemname" den Namen des Geräts ein.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.4.2.2 Koordinaten

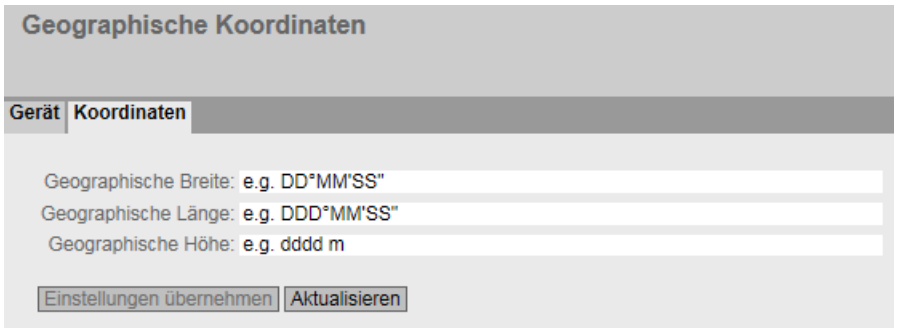
Informationen über die geografischen Koordinaten

Im Fenster "Geografische Koordinaten" können Informationen über die geografischen Koordinaten eingetragen werden. Die Parameter der geografischen Koordinaten (Breitengrad, Längengrad und die Höhe über dem Ellipsoid gemäß WGS84) werden direkt in die Eingabefelder im Fenster "Geografische Koordinaten" eingetragen.

Ermittlung der Koordinaten

Nutzen Sie zur Ermittlung der geografischen Koordinaten des Geräts entsprechendes Kartenmaterial.

Die geografischen Koordinaten können auch durch einen GPS-Empfänger ermittelt werden. Meist werden die geografischen Koordinaten von diesen Geräten direkt angezeigt und müssen nur noch in die Eingabefelder dieser Seite übertragen werden.



Beschreibung

Die Seite enthält folgende Eingabefelder mit einer maximalen Länge von 32 Zeichen:

- **Eingabefeld "Geographische Breite"**
  Geografische Breite: Hier wird der Wert für nördliche oder südliche Breite für den Standort des Geräts eingegeben.
  Der Wert +49° 1´31.67" bedeutet, dass sich das Gerät auf 49 Grad, 1 Bogenminute und 31.67 Bogensekunden nördlicher Breite befindet.
  Die südliche Breite wird mit einem führenden Minuszeichen dargestellt.
  Sie können auch die Buchstaben N (nördliche Breite) oder S (südliche Breite) an die Zahlenangabe anhängen (49° 1´31.67" N).
- **Eingabefeld "Geographische Länge"**
  Geografische Länge: Hier wird der Wert für östliche oder westliche Länge für den Standort des Geräts eingegeben.
  Der Wert +8° 20´58.73" bedeutet, dass sich das Gerät auf 8 Grad, 20 Bogenminuten und 58.73 Bogensekunden östlicher Länge befindet.
  Die westliche Länge wird mit einem führenden Minuszeichen dargestellt.
  Sie können auch die Buchstaben O bzw. E (östliche Länge) oder W (westliche Länge) an die Zahlenangabe anhängen (8° 20´58.73" E).
- **Eingabefeld: "Geographische Höhe"**
  Geografische Höhe: Hier wird der Wert für geografische Höhe über oder unter normal Null (Meereshöhe) in Metern eingegeben.
  Z.B. 158 m bedeutet, dass sich das Gerät in einer Höhe von 158 m über normal Null befindet.
  Höhenangaben unterhalb von normal Null (z. B. am Toten Meer) werden mit einem führenden Minuszeichen dargestellt.

Vorgehensweise

1. Geben Sie in das Eingabefeld "Geographische Breite" den ermittelten Breitengrad ein.
2. Geben Sie in das Eingabefeld "Geographische Länge" den ermittelten Längengrad ein.
3. Geben Sie in das Eingabefeld "Geographische Höhe" die ermittelte Höhe über dem Meeresspiegel ein.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

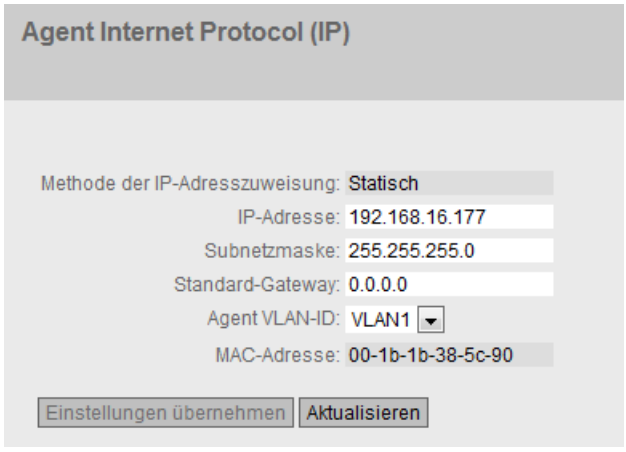
5.4.3 Agent-IP

Hinweis

Bei Geräten mit mehreren IP-Schnittstellen verweist dieser Aufruf auf den Menüpunkt "Subnetze > Konfiguration" im Menü "Layer 3" und die dortige Konfiguration der TIA-Schnittstelle.

Konfiguration der IP-Adresse

Auf dieser WBM-Seite konfigurieren Sie die IP-Adresse für das Gerät.



Beschreibung

Die Seite enthält folgende Felder:

- **Methode der IP-Adresszuweisung**
  Zeigt an, wie die IP-Adresse zugeordnet wird.
  - Statisch
    Die IP-Adresse ist statisch. Die IP-Einstellungen tragen Sie in den Eingabefeldern "IP-Adresse" und "Subnetzmaske" ein.
  - Dynamisch (DHCP)
    Das Gerät bezieht eine dynamische IP-Adresse von einem DHCP-Server.
- **IP-Adresse**
  Tragen Sie die IP-Adresse des Geräts ein.
  Nach dem Anklicken der Schaltfläche "Einstellungen übernehmen" passiert Folgendes:
  - DHCP-Client wird deaktiviert. Sie aktivieren DHCP-Client auf der Seite "System > DHCP > DHCP-Client".
  - Die IP-Adresse wird auch in der Adresszeile des Internet-Browsers angezeigt. Sollte dies nicht automatisch erfolgen, müssen Sie die IP-Adresse manuell in die Adresszeile des Internet-Browsers eintragen.
- **Subnetzmaske**
  Tragen die Subnetzmaske des Geräts ein.
- **Standard-Gateway**
  Tragen Sie die IP-Adresse des Standard-Gateways ein, um mit Geräten in einem anderen Subnetz zu kommunizieren, z. B. Diagnosestationen, E-Mail-Server.

- **Agent VLAN-ID**
  Wählen Sie aus der Klappliste die VLAN-ID. Sie können nur aus bereits konfigurierten VLANs auswählen.
  In dem Modus "802.1D Transparent Bridge" ist diese Klappliste ausgegraut, siehe auch "Layer 2 > VLAN > Allgemein".

  Hinweis
  Ändern der Agent VLAN-ID

  Wenn der Konfigurations-PC direkt über Ethernet mit dem Gerät verbunden ist und Sie die Agent VLAN-ID ändern, ist nach der Änderung das Gerät über Ethernet nicht mehr erreichbar.

- **MAC-Adresse**
  Zeigt die MAC-Adresse des Geräts an. Die MAC-Adresse ist hardwaregebunden und kann nicht geändert werden.

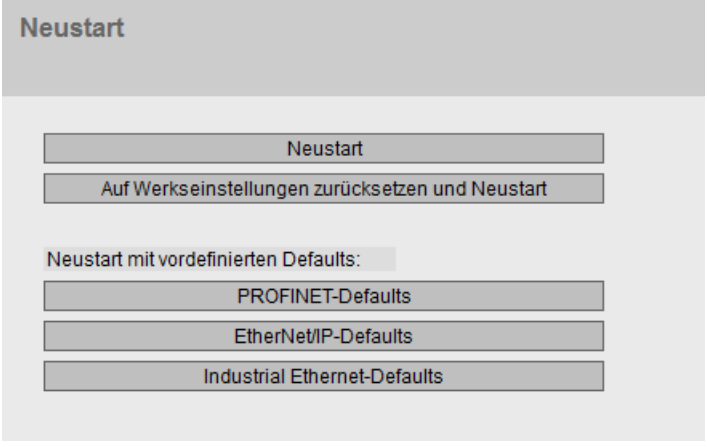
Vorgehensweise

1. Tragen Sie in die Eingabefelder die IP-Adresse, die Subnetzmaske und das Standard-Gateway ein.
2. Wählen Sie aus der Klappliste "Agent VLAN-ID" die gewünschte VLAN-ID.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.4.4 Neustart

Zurücksetzen der Voreinstellungen

In diesem Menü finden Sie eine Schaltfläche zum Neustart des Geräts sowie die Möglichkeit, das Gerät auf die Werkseinstellungen bzw. die Defaulteinstellungen verschiedener Profile zurückzusetzen.



Neustart

Beachten Sie folgende Punkte beim Neustart eines Geräts:

- Sie können einen Neustart des Geräts nur mit Administrator-Rechten durchführen.
- Der Neustart eines Geräts sollte nur durch die Schaltflächen dieses Menüs oder durch die entsprechenden CLI-Befehle und nicht durch Aus- und Einschalten der Spannungsversorgung am Gerät erfolgen.
- Wenn sich das Gerät im Modus "Trial" befindet, müssen Konfigurationsänderungen vor einem Neustart manuell abgespeichert werden. Vorgenommene Änderungen werden erst nach dem Anklicken der Schaltfläche "Einstellungen übernehmen" auf der jeweiligen WBM-Seite im Gerät wirksam.
- Wenn sich das Gerät im Modus "Automatisches Speichern" befindet, werden die letzten Änderungen automatisch vor einem Neustart gespeichert.

Auf Werkseinstellungen zurücksetzen

Durch das Zurücksetzen aller Einstellungen auf die Werkseinstellungen gehen auch die IP-Adresse und die Passwörter verloren. Das Gerät ist danach nur über die serielle Schnittstelle, das Primary Setup Tool oder über DHCP ansprechbar.

ACHTUNG
Bei entsprechendem Anschluss kann ein zuvor korrekt konfiguriertes Gerät nach dem Zurücksetzten kreisende Telegramme und damit den Ausfall des Datenverkehrs verursachen.

Auf Defaults zurücksetzen (Profile)

Die Profile bieten eine Vorkonfiguration für verschiedene Einsatzfälle der Geräte.

Wenn Sie ein Gerät mit den Defaulteinstellungen eines Profils neustarten, werden die Einstellungen auf die Werkseinstellungen zurückgesetzt und einige Parameter so gesetzt, dass sie für einen bestimmten Einsatzfall ausgelegt sind. Im Gegensatz zum Zurücksetzen auf Werkseinstellungen bleiben Benutzer und Passwörter nach dem Neustart erhalten. Die konfigurierte IP-Adresse geht verloren, sodass das Gerät danach nur über die serielle Schnittstelle, das Primary Setup Tool oder über DHCP ansprechbar ist.

ACHTUNG
Bei entsprechendem Anschluss kann ein zuvor korrekt konfiguriertes Gerät nach dem Zurücksetzten kreisende Telegramme und damit den Ausfall des Datenverkehrs verursachen.

Welche Einstellungen speziell für ein Profil gesetzt werden, wird vor dem Neustart angezeigt.

Die Profile können unabhängig von der Werkseinstellung des Geräts genutzt werden.

Beschreibung der angezeigten Felder

Hinweis

Beachten Sie die Auswirkungen der einzelnen Funktionen, die in den oberen Abschnitten beschrieben sind.

Für den Neustart des Geräts stehen Ihnen mit den Schaltflächen auf dieser Seite folgende Möglichkeiten zur Verfügung:

- **Neustart**
  Klicken Sie auf diese Schaltfläche, um das System neu zu starten. Sie müssen den Neustart in einer Dialogbox bestätigen. Bei einem Neustart wird das Gerät neu initialisiert, die interne Firmware wird neu geladen und das Gerät führt einen Selbsttest durch. Die Einstellungen der Startkonfiguration bleiben erhalten, z. B. die IP-Adresse des Geräts. Die gelernten Einträge in der Adresstabelle werden gelöscht. Sie können das Browser-Fenster geöffnet lassen, während das Gerät neu startet. Nach dem Neustart müssen Sie sich wieder neu anmelden.
- **Auf Werkseinstellungen zurücksetzen und Neustart**
  Klicken Sie auf diese Schaltfläche, um die Werkseinstellungen des Geräts wiederherzustellen und das Gerät neu zu starten. Sie müssen den Neustart in einer Dialogbox bestätigen.
  Die Werkseinstellungen sind vom Gerät abhängig.

Für den Neustart des Geräts mit einem vordefinierten Profil stehen Ihnen mit den Schaltflächen auf dieser Seite folgende Möglichkeiten zur Verfügung:

- **PROFINET-Defaults**
  Klicken Sie auf diese Schaltfläche, um die Defaulteinstellungen des PROFINET-Profils wiederherzustellen und das Gerät neu zu starten. Sie müssen den Neustart in einer Dialogbox bestätigen. In der Dialogbox werden die Einstellungen angezeigt, die speziell auf den Betrieb mit dem Protokoll PROFINET abgestimmt sind.
- **EtherNet/IP-Defaults**
  Klicken Sie auf diese Schaltfläche, um die Defaulteinstellungen des EtherNet/IP-Profils wiederherzustellen und das Gerät neu zu starten. Sie müssen den Neustart in einer Dialogbox bestätigen. In der Dialogbox werden die Einstellungen angezeigt, die speziell auf den Betrieb mit dem Protokoll EtherNet/IP abgestimmt sind.
- **Industrial Ethernet-Defaults**
  Klicken Sie auf diese Schaltfläche, um die Defaulteinstellungen des Industrial Ethernet-Profils wiederherzustellen und das Gerät neu zu starten. Sie müssen den Neustart in einer Dialogbox bestätigen. In der Dialogbox werden die Einstellungen angezeigt, die speziell auf den Betrieb im Industrial Ethernet-Umfeld abgestimmt sind.

5.4.5 Laden & Speichern

Übersicht der Dateitypen

Dateityp	Beschreibung
Config	Diese Datei enthält die Startkonfiguration. Diese Datei enthält unter anderem die Definitionen der Benutzer. Die Passwörter sind in der Datei "Users" abgespeichert.
ConfigPack	Detaillierte Konfigurationsinformationen z. B. Startkonfiguration, Benutzer, Zertifikate und WBM-Favoriten. ZIP-Datei, die aus der Config-, Users- und LSYS-Datei besteht.
Debug	Diese Datei beinhaltet Informationen für den Siemens Support. Sie ist verschlüsselt und kann ohne Sicherheitsrisiko per E-Mail an den Siemens Support gesendet werden.
DebugExt	Diese Datei beinhaltet ausführlichere Informationen für den Siemens Support. Sie ist verschlüsselt und kann ohne Sicherheitsrisiko per E-Mail an den Siemens Support gesendet werden. Das Speichern der Datei kann einige Zeit in Anspruch nehmen.
EDS	Electronic Data Sheet (EDS) Elektronisches Datenblatt zur Beschreibung von Geräten im EtherNet/IP-Betrieb
Firmware	Die Firmware ist signiert und verschlüsselt. Damit ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.
GSDML	PROFINET-Informationen über die Geräteeigenschaften
HTTPSCert	Voreingestellte HTTPS-Zertifikate inkl. Schlüssel Die voreingestellten und automatisch erstellten HTTPS-Zertifikate sind selbstsigniert. Es wird dringend empfohlen eigene HTTPS-Zertifikate zu erstellen und bereitzustellen. Es wird empfohlen HTTPS-Zertifikate zu verwenden, die entweder durch eine zuverlässige externe oder eine interne Zertifizierungsstelle signiert sind. Das HTTPS-Zertifikat überprüft die Identität des Geräts und regelt den verschlüsselten Datenaustausch. Zertifikate mit einem anderen Format können nicht eingespielt werden.
LogFile	Datei mit Einträgen aus der Ereignisprotokolltabelle
MIB	Private MSPS MIB-Datei
RunningCLI	Textdatei mit CLI-Befehlen Diese Datei enthält eine Übersicht der aktuellen Konfiguration in Form von CLI-Befehlen. Sie können die Textdatei herunterladen. Die Datei ist nicht dafür vorgesehen, dass Sie sie unverändert wieder hochladen.
RunningSINEMA-Config	In diesen Dateityp speichern Sie die aktuelle Konfiguration des Geräts für eine Übergabe an STEP7 Basic/Professional. Die Datei kann in STEP7 Basic/Professional importiert und auf ein Gerät mit gleicher Artikelnummer und Firmware-Version aufgespielt werden. Bevor Sie eine Datei abspeichern können, müssen Sie im WBM unter "System > Laden&Speichern > Passwörter" ein Passwort für die "RunningSINEMAConfig" vergeben. Dieses Passwort benötigen Sie auch, um die Datei in STEP7 Basic/Professional zu importieren. siehe auch "SINEMAConfig"

Dateityp	Beschreibung
Script	Textdatei mit CLI-Befehlen Sie können eine Skriptdatei in ein Gerät hochladen. Die enthaltenen CLI-Befehle werden entsprechend ausgeführt.
SINEMAConfig	Über diesen Dateityp laden Sie Konfigurationsdaten, die über STEP7 Basic/Professional für eine Übergabe an das WBM exportiert wurden. Um eine Datei laden zu können, müssen Sie unter "System > Laden&Speichern > Passwörter" ein Passwort für die "SINEMAConfig" vergeben. Dieses Passwort benötigen Sie auch, um die Datei aus STEP7 Basic/Professional zu exportieren. siehe auch "RunningSINEMAConfig"
StartupInfo	Startup Logdatei Diese Datei enthält die Meldungen die während des letzten Hochlaufs im Logbuch eingetragen wurden.
Users	Diese Datei enthält die Zuordnung der Benutzernamen zu den entsprechenden Passwörtern.
WBMFav	WBM Favoriten Diese Datei enthält die Favoriten, die Sie im WBM angelegt haben. Sie können diese Datei herunterladen und in anderen Geräten hochladen.

5.4.5.1 HTTP

Laden und Speichern von Daten über HTTP

Das WBM bietet die Möglichkeit, Gerätedaten in einer externen Datei auf Ihrem Client-PC zu speichern bzw. solche Daten aus einer externen Datei vom Client-PC in das Gerät zu laden. So können Sie z. B. eine neue Firmware aus einer Datei von Ihrem Client-PC laden.

Hinweis

Diese WBM-Seite ist sowohl für Verbindungen über HTTP als auch für Verbindungen über HTTPS verfügbar.

Firmware

Die Firmware ist signiert und verschlüsselt. Es ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.

Hinweis

Inkompatibilität zu Firmware-Vorgängerversionen ohne/mit gestecktem PLUG

Bei der Installation einer Vorgängerversion kann es zu Verlust der Konfigurationsdaten kommen. In diesem Fall startet das Gerät nach der Installation der Firmware mit den Werkseinstellungen.

Wenn in diesem Fall ein PLUG im Gerät gesteckt ist, hat dieser nach dem Neustart den Status "Not Accepted", da sich auf dem PLUG weiterhin die Konfigurationsdaten der vorherigen, aktuelleren Firmware befinden. Somit kann ohne Konfigurationsdatenverlust zur vorherigen, aktuelleren Firmware zurückgekehrt werden. Falls die ursprüngliche Konfiguration auf dem PLUG nicht mehr benötigt wird, kann der PLUG manuell über die WBM-Seite "System > PLUG" gelöscht oder neu beschrieben werden.

Konfigurationsdateien

Hinweis

Konfigurationsdateien und Modus Trial/Automatisches Speichern

Im Modus "Automatisches Speichern" wird eine automatische Sicherung durchgeführt, bevor die Konfigurationsdateien (ConfigPack und Config) übertragen werden.
Im Modus "Trial" werden Änderungen zwar übernommen aber nicht in den Konfigurationsdateien (ConfigPack und Config) gespeichert. Verwenden Sie die Schaltfläche "Schreiben der Startkonfiguration" auf der WBM-Seite "System > Konfiguration", um Änderungen in den Konfigurationsdateien abzuspeichern.

CLI-Skriptdatei

Sie können bestehende CLI-Konfigurationen herunterladen (RunningCLI) und eigene CLI-Skripte hochladen (Script).

Hinweis

Das herunterladbare CLI-Skript ist nicht dafür vorgesehen, dass Sie es unverändert wieder hochladen.

Austausch von Konfigurationsdaten mit STEP7 Basic/Professional über eine Datei

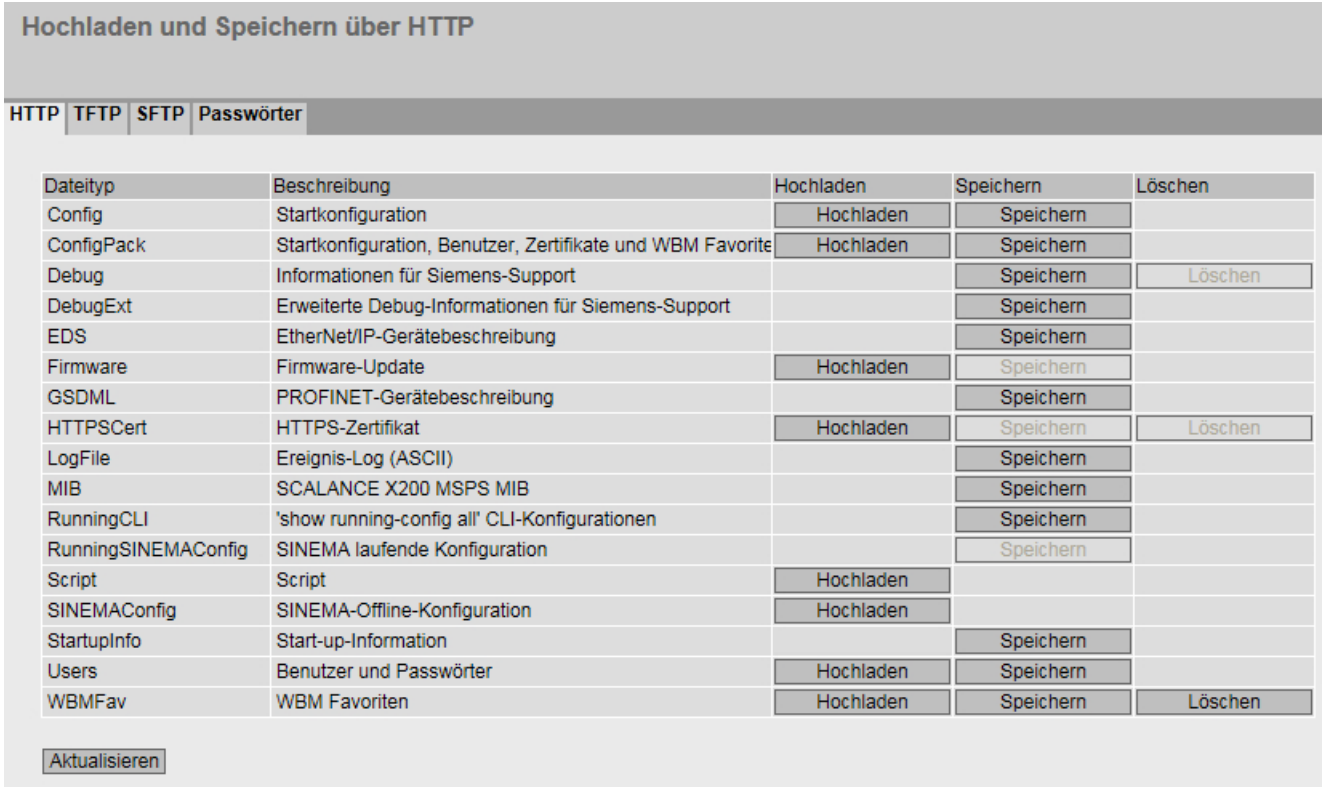
Über die beiden Dateitypen "RunningSINEMAConfig" und "SINEMAConfig" können Sie Konfigurationsdaten zwischen einem Gerät (WBM) und STEP7 Basic/Professional über eine Datei austauschen.

Voraussetzungen:

- Gleiche Artikelnummer
- Gleiche Firmware-Version
- Passwort
  Das Passwort vergeben Sie im WBM unter "System > Laden&Speichern > Passwörter".

Die Dateitypen können wie folgt genutzt werden:

- Zur Offline-Diagnose
  Sie können die fehlerhafte Konfiguration eines Geräts als "RunningSINEMAConfig" über das WBM speichern und in STEP7 Basic/Professional importieren. Die Diagnose in STEP7 Basic/Professional erfolgt, ohne dass eine Verbindung zu einem realen Gerät besteht. Eine korrigierte Konfiguration kann exportiert und als "SINEMAConfig" wieder über das WBM geladen werden.
- Zur Konfiguration
  Sie können ein Gerät in STEP7 Basic/Professional konfigurieren, ohne dass eine Verbindung zu einem realen Gerät besteht. Die Konfiguration kann exportiert und als "SINEMAConfig" über das WBM in das reale Gerät geladen werden.



Beschreibung der angezeigten Felder

Die Tabelle gliedert sich in folgende Spalten:

- **Dateityp**
  Zeigt den Dateityp an.
- **Beschreibung**
  Zeigt die Kurzbeschreibung des Dateityps an.
- **Hochladen**
  Mit dieser Schaltfläche können Sie Dateien auf das Gerät hochladen. Die Schaltfläche ist aktivierbar, wenn diese Funktion für den Dateityp unterstützt wird.
- **Speichern**
  Mit dieser Schaltfläche können Sie Dateien vom Gerät herunterladen. Die Schaltfläche ist nur aktivierbar, wenn diese Funktion für den Dateityp unterstützt wird und die Datei auf dem Gerät vorhanden ist.
- **Löschen**
  Mit dieser Schaltfläche können Sie Dateien vom Gerät löschen. Die Schaltfläche ist nur aktivierbar, wenn diese Funktion für den Dateityp unterstützt wird und die Datei auf dem Gerät vorhanden ist.

Hinweis

Löschen Sie nach einem Firmware-Update den Cache Ihres Internet-Browsers.

Vorgehensweise zur Konfiguration

Daten über HTTP hochladen

1. Starten Sie das Hochladen durch Anklicken einer der Schaltflächen "Hochladen".
   Es öffnet sich ein Dialogfenster zum Hochladen einer Datei.
2. Wählen Sie die gewünschte Datei aus und bestätigen Sie das Hochladen.
   Die Datei wird hochgeladen.
3. Wenn ein Neustart notwendig ist, wird eine entsprechende Meldung ausgegeben. Klicken Sie auf die Schaltfläche "OK", um den Neustart durchzuführen. Wenn Sie auf die Schalfläche "Abbrechen" klicken, wird kein Neustart des Geräts durchgeführt. Erst nach einem Neustart werden die Änderungen wirksam.

Daten über HTTP herunterladen

1. Starten Sie das Herunterladen durch Anklicken einer der Schaltflächen "Speichern".
2. Wählen Sie einen Speicherort und einen Namen für die Datei.
3. Speichern Sie die Datei.
   Die Datei wird heruntergeladen und gespeichert.

Daten über HTTP löschen

1. Starten Sie das Löschen durch Anklicken einer der Schaltflächen "Löschen".
   Die Datei wird gelöscht.

Konfigurationsdaten wiederverwenden

Wenn mehrere identische Geräte die gleiche Konfiguration erhalten sollen und die Zuweisung der IP-Adressen über DHCP erfolgt, kann durch Abspeichern und Einlesen von Konfigurationsdaten der Aufwand zur Neukonfiguration reduziert werden.

Gehen Sie folgendermaßen vor, um Konfigurationsdaten wiederzuverwenden:

1. Speichern Sie die Konfigurationsdaten eines konfigurierten Geräts auf Ihrem PC.
2. Laden Sie diese Konfigurationsdateien auf alle weiteren Geräte, die Sie so konfigurieren wollen.
3. Falls für einzelne Geräte individuelle Einstellungen erforderlich sind, müssen Sie diese online am betreffenden Gerät vornehmen.

Hinweis

Konfigurationsdaten sind mit einer Prüfsumme versehen. Wenn Sie die Daten verändern, können Sie sie nicht mehr auf den IE-Switch hochladen.

5.4.5.2 TFTP

Laden und Speichern von Daten über einen TFTP-Server

Auf dieser Seite können Sie den TFTP-Server und die Dateinamen konfigurieren. Das WBM bietet die Möglichkeit, Gerätedaten in einer externen Datei auf einem TFTP-Server zu speichern bzw. solche Daten aus einer externen Datei vom TFTP-Server in die Geräte zu laden. So können Sie z. B. eine neue Firmware aus einer Datei von einem TFTP-Server laden.

Firmware

Die Firmware ist signiert und verschlüsselt. Es ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.

Hinweis

Inkompatibilität zu Firmware-Vorgängerversionen ohne/mit gestecktem PLUG

Bei der Installation einer Vorgängerversion kann es zu Verlust der Konfigurationsdaten kommen. In diesem Fall startet das Gerät nach der Installation der Firmware mit den Werkseinstellungen.

Wenn in diesem Fall ein PLUG im Gerät gesteckt ist, hat dieser nach dem Neustart den Status "Not Accepted", da sich auf dem PLUG weiterhin die Konfigurationsdaten der vorherigen, aktuelleren Firmware befinden. Somit kann ohne Konfigurationsdatenverlust zur vorherigen, aktuelleren Firmware zurückgekehrt werden. Falls die ursprüngliche Konfiguration auf dem PLUG nicht mehr benötigt wird, kann der PLUG manuell über die WBM-Seite "System > PLUG" gelöscht oder neu beschrieben werden.

Konfigurationsdateien

Hinweis

Konfigurationsdateien und Modus Trial/Automatisches Speichern

Im Modus "Automatisches Speichern" wird eine automatische Sicherung durchgeführt, bevor die Konfigurationsdateien (ConfigPack und Config) übertragen werden.
Im Modus "Trial" werden Änderungen zwar übernommen aber nicht in den Konfigurationsdateien (ConfigPack und Config) gespeichert. Verwenden Sie die Schaltfläche "Schreiben der Startkonfiguration" auf der WBM-Seite "System > Konfiguration", um Änderungen in den Konfigurationsdateien abzuspeichern.

CLI-Skriptdatei

Sie können bestehende CLI-Konfigurationen herunterladen (RunningCLI) und eigene CLI-Skripte hochladen (Script).

Hinweis

Das herunterladbare CLI-Skript ist nicht dafür vorgesehen, dass Sie es unverändert wieder hochladen.

Austausch von Konfigurationsdaten mit STEP7 Basic/Professional über eine Datei

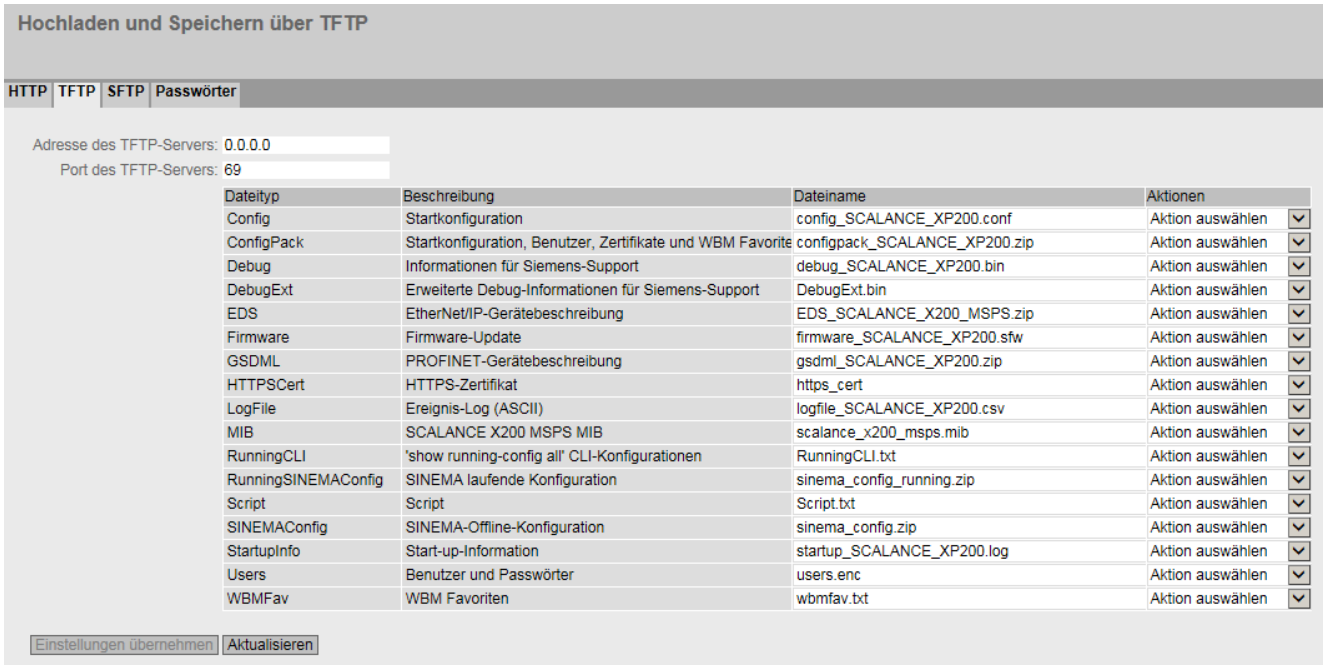
Über die beiden Dateitypen "RunningSINEMAConfig" und "SINEMAConfig" können Sie Konfigurationsdaten zwischen einem Gerät (WBM) und STEP7 Basic/Professional über eine Datei austauschen.

Voraussetzungen:

- Gleiche Artikelnummer
- Gleiche Firmware-Version
- Passwort
  Das Passwort vergeben Sie im WBM unter "System > Laden&Speichern > Passwörter".

Die Dateitypen können wie folgt genutzt werden:

- Zur Offline-Diagnose
  Sie können die fehlerhafte Konfiguration eines Geräts als "RunningSINEMAConfig" über das WBM speichern und in STEP7 Basic/Professional importieren. Die Diagnose in STEP7 Basic/Professional erfolgt, ohne dass eine Verbindung zu einem realen Gerät besteht. Eine korrigierte Konfiguration kann exportiert und als "SINEMAConfig" wieder über das WBM geladen werden.
- Zur Konfiguration
  Sie können ein Gerät in STEP7 Basic/Professional konfigurieren, ohne dass eine Verbindung zu einem realen Gerät besteht. Die Konfiguration kann exportiert und als "SINEMAConfig" über das WBM in das reale Gerät geladen werden.



Dateityp	Beschreibung	Dateiname	Aktionen
Config	Startkonfiguration	config_SCALANCE_XP200.conf	Aktion auswählen
ConfigPack	Startkonfiguration, Benutzer, Zertifikate und WBM Favorite	configpack_SCALANCE_XP200.zip	Aktion auswählen
Debug	Informationen für Siemens-Support	debug_SCALANCE_XP200.bin	Aktion auswählen
DebugExt	Erweiterte Debug-Informationen für Siemens-Support	DebugExt.bin	Aktion auswählen
EDS	EtherNet/IP-Gerätebeschreibung	EDS_SCALANCE_X200_MSPS.zip	Aktion auswählen
Firmware	Firmware-Update	firmware_SCALANCE_XP200.sfw	Aktion auswählen
GSDML	PROFINET-Gerätebeschreibung	gsdml_SCALANCE_XP200.zip	Aktion auswählen
HTTPSCert	HTTPS-Zertifikat	https_cert	Aktion auswählen
LogFile	Ereignis-Log (ASCII)	logfile_SCALANCE_XP200.csv	Aktion auswählen
MIB	SCALANCE X200 MSPS MIB	scalance_x200_msps.mib	Aktion auswählen
RunningCLI	'show running-config all' CLI-Konfigurationen	RunningCLI.txt	Aktion auswählen
RunningSINEMAConfig	SINEMA laufende Konfiguration	sinema_config_running.zip	Aktion auswählen
Script	Script	Script.txt	Aktion auswählen
SINEMAConfig	SINEMA-Offline-Konfiguration	sinema_config.zip	Aktion auswählen
StartupInfo	Start-up-Information	startup_SCALANCE_XP200.log	Aktion auswählen
Users	Benutzer und Passwörter	users.enc	Aktion auswählen
WBMFav	WBM Favoriten	wbmfav.txt	Aktion auswählen

Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Adresse des TFTP-Servers**
  Tragen Sie hier die IP-Adresse des TFTP-Servers ein, mit dem Sie Daten austauschen.
- **Port des TFTP-Servers**
  Tragen Sie hier den Port des TFTP-Servers ein, über den der Datenaustausch abgewickelt werden soll. Gegebenenfalls können Sie den Standardwert 69 entsprechend Ihren spezifischen Anforderungen ändern.

Die Tabelle gliedert sich in folgende Spalten:

- **Dateityp**
  Zeigt den Dateityp an.
- **Beschreibung**
  Zeigt die Kurzbeschreibung des Dateityps an.

- **Dateiname**
  Für jeden Dateityp ist hier ein Dateiname vorgegeben.

  Hinweis
  Änderung des Dateinamens

  Sie können den in dieser Spalte vorgegebenen Dateinamen ändern. Nach dem Anklicken der Schaltfläche "Einstellungen übernehmen" ist der geänderte Name im Gerät gespeichert und kann auch mit dem Command Line Interface genutzt werden.

- **Aktionen**
  Wählen Sie aus der Klappliste die Aktion aus. Die Auswahl ist abhängig vom gewählten Dateityp. z. B. können Sie die Log-Datei nur speichern.
  Folgende Aktionen sind möglich:
  - **Datei speichern**
    Mit dieser Auswahl speichern Sie eine Datei auf dem TFTP-Server.
  - **Datei hochladen**
    Mit dieser Auswahl laden Sie eine Datei vom TFTP-Server.

Vorgehensweise zur Konfiguration

Daten über TFTP laden bzw. speichern

1. Tragen Sie im Eingabefeld "Adresse des TFTP-Servers" die IP-Adresse des TFTP-Servers ein.
2. Tragen Sie im Eingabefeld "Port des TFTP-Servers" den verwendeten Port des TFTP-Servers ein.
3. Tragen Sie ggf. im Eingabefeld "Dateiname" den Namen einer Datei ein, in die Sie speichern bzw. aus der Sie Daten übernehmen wollen.
4. Wählen Sie aus der Klappliste "Aktionen" die Aktion, die Sie durchführen wollen.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen", um die ausgewählte Aktion zu starten.
6. Wenn ein Neustart notwendig ist, wird eine entsprechende Meldung ausgegeben. Klicken Sie auf die Schaltfläche "OK", um den Neustart durchzuführen. Wenn Sie auf die Schalfläche "Abbrechen" klicken, wird kein Neustart des Geräts durchgeführt. Erst nach einem Neustart werden die Änderungen wirksam.

Konfigurationsdaten wiederverwenden

Wenn mehrere identische Geräte die gleiche Konfiguration erhalten sollen und die Zuweisung der IP-Adressen über DHCP erfolgt, kann durch Abspeichern und Einlesen von Konfigurationsdaten der Aufwand zur Neukonfiguration reduziert werden.

Gehen Sie folgendermaßen vor, um Konfigurationsdaten wiederzuverwenden:

1. Speichern Sie die Konfigurationsdaten eines konfigurierten Geräts auf Ihrem PC.
2. Laden Sie diese Konfigurationsdateien auf alle weiteren Geräte, die Sie so konfigurieren wollen.
3. Falls für einzelne Geräte individuelle Einstellungen erforderlich sind, müssen Sie diese online am betreffenden Gerät vornehmen.

Hinweis

Konfigurationsdaten sind mit einer Prüfsumme versehen. Wenn Sie die Daten verändern, können Sie sie nicht mehr auf den IE-Switch hochladen.

5.4.5.3 SFTP

Laden und speichern von Daten über einen SFTP-Server

SFTP (SSH File Transfer Protocol) überträgt die Dateien verschlüsselt. Auf dieser Seite konfigurieren Sie die Zugangsdaten für den SFTP-Server.

Weiter bietet das WBM die Möglichkeit, Gerätedaten in einer externen Datei auf Ihrem Client-PC zu speichern bzw. solche Daten aus einer externen Datei vom PC in die Geräte zu laden. So können Sie z. B. eine neue Firmware aus einer Datei von Ihrem Admin-PC laden.

Zudem lassen sich auf dieser Seite die Zertifikate laden, die für den Aufbau einer gesicherten VPN-Verbindung notwendig sind.

Firmware

Die Firmware ist signiert und verschlüsselt. Es ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.

Konfigurationsdateien

Hinweis

Konfigurationsdateien und Modus Trial/Automatisches Speichern

Im Modus "Automatisches Speichern" wird eine automatische Sicherung durchgeführt, bevor die Konfigurationsdateien (ConfigPack und Config) übertragen werden.
Im Modus "Trial" werden Änderungen zwar übernommen aber nicht in den Konfigurationsdateien (ConfigPack und Config) gespeichert. Verwenden Sie die Schaltfläche "Schreiben der Startkonfiguration" auf der WBM-Seite "System > Konfiguration", um Änderungen in den Konfigurationsdateien abzuspeichern.

CLI-Skriptdatei

Sie können bestehende CLI-Konfigurationen herunterladen (RunningCLI) und eigene CLI-Skripte hochladen (Script).

Hinweis

Das herunterladbare CLI-Skript ist nicht dafür vorgesehen, dass Sie es unverändert wieder hochladen.

CLI-Befehle zum Speichern und Laden von Dateien können nicht über die CLI-Skriptdatei (Script) ausgeführt werden.

Austausch von Konfigurationsdaten mit STEP7 Basic/Professional über eine Datei

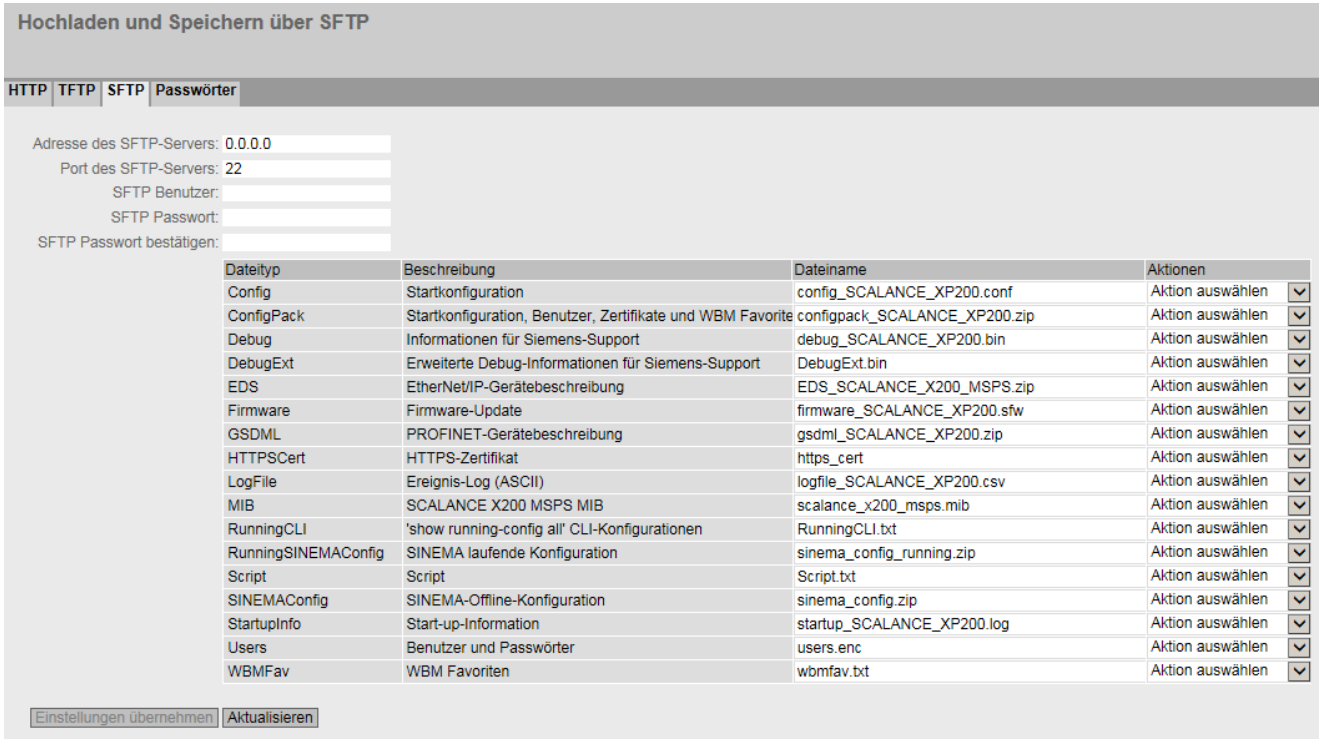
Über die beiden Dateitypen "RunningSINEMAConfig" und "SINEMAConfig" können Sie Konfigurationsdaten zwischen einem Gerät (WBM) und STEP7 Basic/Professional über eine Datei austauschen.

Voraussetzungen:

- Gleiche Artikelnummer
- Gleiche Firmware-Version
- Passwort
  Das Passwort vergeben Sie im WBM unter "System > Laden&Speichern > Passwörter".

Die Dateitypen können wie folgt genutzt werden:

- Zur Offline-Diagnose
  Sie können die fehlerhafte Konfiguration eines Geräts als "RunningSINEMAConfig" über das WBM speichern und in STEP7 Basic/Professional importieren. Die Diagnose in STEP7 Basic/Professional erfolgt, ohne dass eine Verbindung zu einem realen Gerät besteht. Eine korrigierte Konfiguration kann exportiert und als "SINEMAConfig" wieder über das WBM geladen werden.
- Zur Konfiguration
  Sie können ein Gerät in STEP7 Basic/Professional konfigurieren, ohne dass eine Verbindung zu einem realen Gerät besteht. Die Konfiguration kann exportiert und als "SINEMAConfig" über das WBM in das reale Gerät geladen werden.



Beschreibung

Die Seite enthält folgende Felder:

- **Adresse des SFTP-Servers**
  Geben Sie die IP-Adresse des SFTP-Servers ein, mit dem Sie Daten austauschen.
- **Port des SFTP-Servers**
  Geben Sie den Port des SFTP-Servers ein, über den der Datenaustausch abgewickelt werden soll. Gegebenenfalls können Sie den Standardwert 22 entsprechend Ihren spezifischen Anforderungen ändern.
- **SFTP Benutzer**
  Geben Sie den Benutzer für den Zugriff auf den SFTP-Server ein. Vorausgesetzt, auf dem SFTP-Server ist ein Benutzer mit den entsprechenden Rechten angelegt.
- **SFTP Passwort**
  Geben Sie das Passwort für den Benutzer ein
- **SFTP Passwort bestätigen**
  Bestätigen Sie das Passwort.

Die Tabelle gliedert sich in folgende Spalten:

- **Dateityp**
  Zeigt den Dateityp an.
- **Beschreibung**
  Zeigt die Kurzbeschreibung des Dateityps an.
- **Dateiname**
  Für jeden Dateityp ist hier ein Dateiname vorgegeben.

  Hinweis

  Änderung des Dateinamens

  Sie können den in dieser Spalte vorgegebenen Dateinamen ändern. Nach dem Anklicken der Schaltfläche "Einstellungen übernehmen" ist der geänderte Name im Gerät gespeichert und kann auch mit dem Command Line Interface genutzt werden.

- **Aktionen**
  Wählen Sie aus der Klappliste die Aktion aus. Die Auswahl ist abhängig vom gewählten Dateityp. z. B. können Sie die Log-Datei nur speichern.
  Folgende Aktionen sind möglich:
  - **Datei speichern**
    Mit dieser Auswahl speichern Sie eine Datei auf dem SFTP-Server.
  - **Datei hochladen**
    Mit dieser Auswahl laden Sie eine Datei vom SFTP-Server.

Vorgehensweise

Daten über SFTP laden bzw. speichern

1. Geben Sie bei "Adresse des SFTP-Servers" die Adresse des SFTP-Servers ein.
2. Geben Sie bei "Port des SFTP-Servers" den verwendeten Port des SFTP-Servers ein.

3. Geben Sie die Benutzerdaten (Benutzername und Passwort) ein, die für den Zugriff auf den SFTP-Server notwendig sind.
4. Geben Sie ggf. bei "Dateiname" den Namen einer Datei ein, in die Sie speichern bzw. aus der Sie Daten übernehmen wollen.

   Hinweis

   Dateien, deren Zugriff passwortgeschützt ist

   Um diese Dateien erfolgreich ins Gerät zuladen, müssen Sie unter "System" > "Laden & Speichern" > "Passwörter" das für die Datei festgelegte Passwort eingeben.

5. Wählen Sie in der Klappliste "Aktionen" die Aktion aus, die Sie durchführen wollen.
6. Klicken Sie auf "Einstellungen übernehmen", um die ausgewählte Aktion zu starten.
7. Wenn ein Neustart notwendig ist, wird eine entsprechende Meldung ausgegeben. Klicken Sie auf die Schaltfläche "OK", um den Neustart durchzuführen. Wenn Sie auf die Schalfläche "Abbrechen" klicken, wird kein Neustart des Geräts durchgeführt. Erst nach einem Neustart werden die Änderungen wirksam.

Konfigurationsdaten wiederverwenden

Wenn mehrere identische Geräte die gleiche Konfiguration erhalten sollen und die Zuweisung der IP-Adressen über DHCP erfolgt, kann durch Abspeichern und Einlesen von Konfigurationsdaten der Aufwand zur Neukonfiguration reduziert werden.

Gehen Sie folgendermaßen vor, um Konfigurationsdaten wiederzuverwenden:

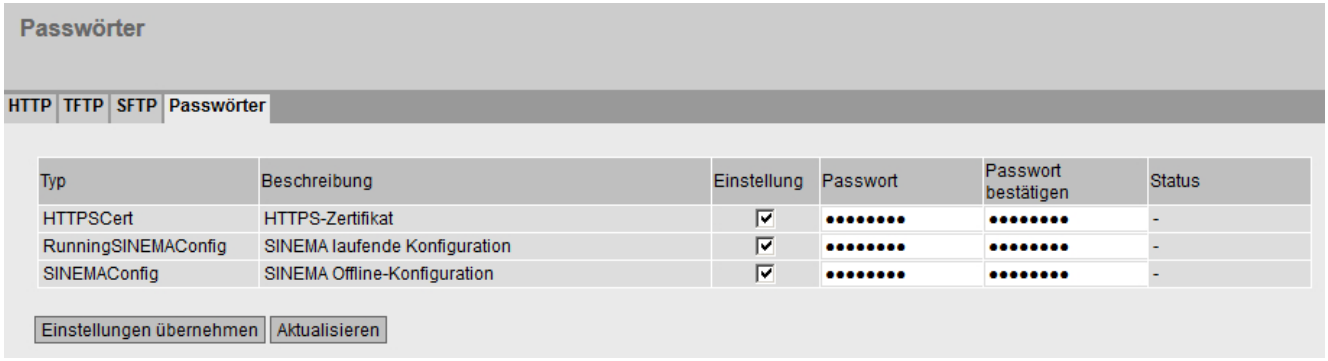
1. Speichern Sie die Konfigurationsdaten eines konfigurierten Geräts auf Ihrem PC.
2. Laden Sie diese Konfigurationsdateien auf alle weiteren Geräte, die Sie so konfigurieren wollen.
3. Falls für einzelne Geräte individuelle Einstellungen erforderlich sind, müssen Sie diese online am betreffenden Gerät vornehmen.

Hinweis

Konfigurationsdaten sind mit einer Prüfsumme versehen. Wenn Sie die Daten verändern, können Sie sie nicht mehr auf den IE-Switch hochladen.

5.4.5.4 Passwörter

Es gibt Dateien, deren Zugriff passwortgeschützt ist. Um z. B. das HTTPS-Zertifikat verwenden zu können, müssen Sie auf dieser WBM-Seite das entsprechende Passwort angeben.



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Typ**
  Zeigt den Dateityp an.
- **Beschreibung**
  Zeigt die Kurzbeschreibung des Dateityps an.
- **Einstellung**
  Wenn aktiviert, wird die Datei verwendet. Nur aktivierbar, wenn das Passwort konfiguriert ist.
- **Passwort**
  Geben Sie das Passwort für die Datei ein.
- **Passwort bestätigen**
  Bestätigen Sie das Passwort.
- **Status**
  Zeigt an, ob das Passwort zur Datei auf dem Gerät passen.
  - gültig
    Das Optionskästchen "Einstellung" ist aktiviert und das Passwort passt zu der Datei.
  - ungültig
    Das Optionskästchen "Einstellung" ist aktiviert, aber das Passwort passt nicht zur Datei oder es ist noch keine Datei geladen.
  - '-'
    Das Passwort kann nicht ausgewertet werden oder wird noch nicht verwendet. Das Optionskästchen "Einstellung" ist nicht aktiviert.

Vorgehensweise

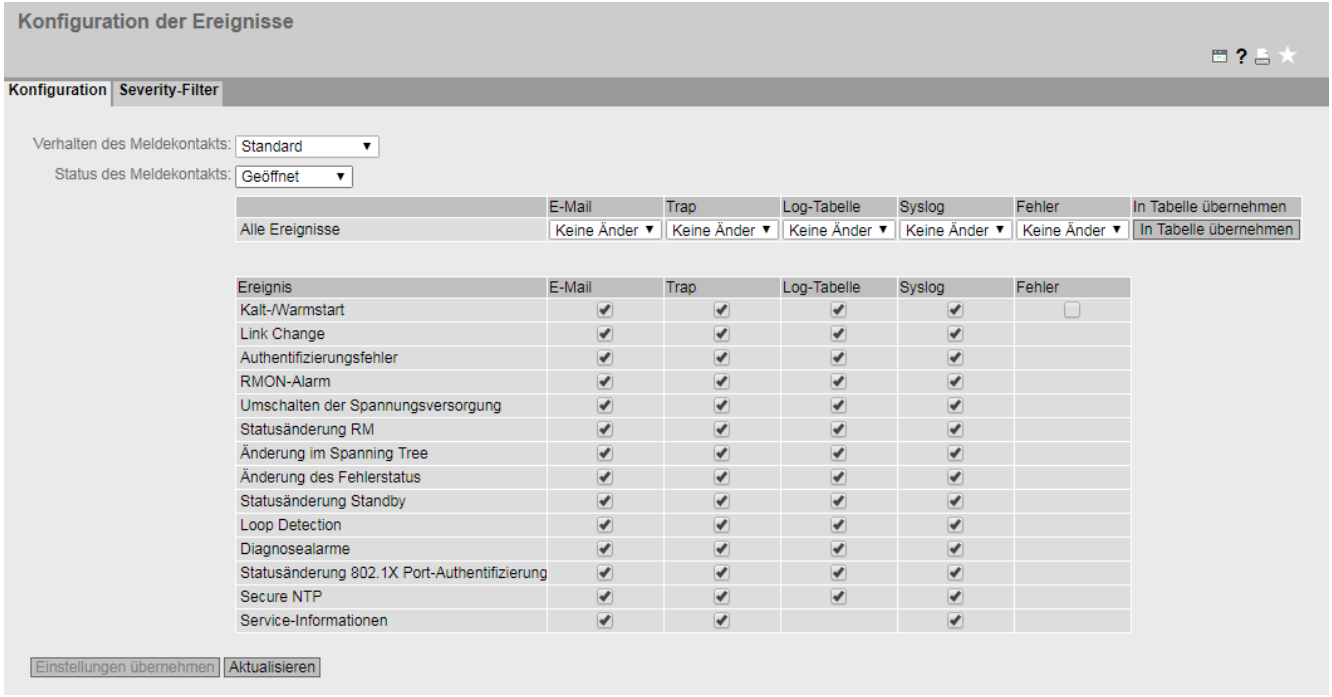
1. Tragen Sie bei "Passwort" das Passwort ein.
2. Um das Passwort zu bestätigen, tragen Sie bei "Passwort bestätigen" das Passwort nochmals ein.
3. Aktivieren Sie die Option "Einstellung".
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.4.6 Ereignisse

5.4.6.1 Konfiguration

Systemereignisse auswählen

Auf dieser Seite legen Sie fest, wie ein Gerät auf Systemereignisse reagiert. Klicken Sie zum Aktivieren oder Deaktivieren der Optionen in die entsprechenden Optionskästchen der jeweiligen Spalte.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Verhalten des Meldekontakts**
  Wählen Sie aus der Klappliste das Verhalten des Meldekontakts. Folgende Verhalten sind möglich:
  - Standard
    Standardeinstellung für den Meldekontakt. Ein auftretender Fehler wird durch die Fehler-LED angezeigt und der Meldekontakt wird geöffnet. Wenn der Fehlerzustand nicht mehr besteht, erlischt die Fehler-LED und der Meldekontakt wird geschlossen.
  - Benutzerdefiniert
    Die Funktion des Meldekontakts ist unabhängig vom auftretenden Fehler. Der Meldekontakt kann durch Benutzeraktionen beliebig geöffnet oder geschlossen werden.
- **Status des Meldekontakts**
  Um den Zustand des Meldekontakts zu ändern, wählen Sie in der Klappliste "Verhalten des Meldekontakts" das Verhalten "Benutzerdefiniert" aus.
  Wählen Sie aus der Klappliste den Zustand des Meldekontakts. Folgende Zustände sind möglich:
  - Geschlossen
    Meldekontakt ist geschlossen.
  - Geöffnet
    Meldekontakt ist geöffnet.

Mit Tabelle 1 können Sie alle Optionskästchen einer Spalte von Tabelle 2 auf einmal aktivieren oder deaktivieren. Die Tabelle 1 gliedert sich in folgende Spalten:

- **Alle Ereignisse**
  Zeigt an, dass die Einstellungen für alle Ereignisse der Tabelle 2 gültig sind.
- **E-Mail / Trap / Log-Tabelle / Syslog / Fehler**
  Aktivieren oder deaktivieren Sie die gewünschte Art der Benachrichtigung für alle Ereignisse. Wenn "Keine Änderung" ausgewählt ist, bleiben die Einträge der entsprechenden Spalte in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ereignisse der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Ereignis**
  Die Spalte enthält folgende Werte:
  - Kalt-/Warmstart
    Das Gerät wurde eingeschaltet oder vom Anwender neu gestartet. Im Fehlerspeicher des Geräts wird ein neuer Eintrag mit der Art des durchgeführten Neustarts erzeugt.
  - Link Change
    Dieses Ereignis tritt nur auf, wenn der Port-Status überwacht wird und sich entsprechend geändert hat, siehe "System > Fehlerkontrolle > Link Change".
  - Authentifizierungsfehler
    Dieses Ereignis tritt beim Versuch eines Zugriffs mit fehlerhaftem Passwort auf.
  - RMON-Alarm
    Ein Alarm oder ein Ereignis ist im Zusammenhang mit der Fernüberwachung des Systems aufgetreten.
  - Umschalten der Spannungsversorgung
    Dieses Ereignis tritt nur auf, wenn die Spannungsversorgungsleitungen 1 und 2 überwacht werden. Es zeigt an, dass ein Wechsel auf Leitung 1 bzw. auf Leitung 2 stattgefunden hat. Siehe "System > Fehlerkontrolle > Spannungsversorgung".
  - Statusänderung RM
    Der Redundanzmanager hat eine Unterbrechung oder Wiederherstellung des Rings erkannt und hat die Strecke um- bzw. zurückgeschaltet.
  - Änderung im Spanning Tree
    Die Spanning Tree-Topologie hat sich geändert.
  - Änderung des Fehlerstatus
    Der Fehlerstatus hat sich geändert. Der Fehlerstatus kann sich auf die aktivierte Portüberwachung, auf das Ansprechen des Meldekontakts oder die Spannungsüberwachung beziehen.
  - Statusänderung Standby
    Ein Gerät mit aufgebauter Standby-Verbindung (Master oder Slave) hat die Koppelstrecke zum anderen Ring (Standby-Port) aktiviert oder deaktiviert. Der Datenverkehr wurde von einer Ethernet-Verbindung (Standby-Port des Master) zu der anderen Ethernet-Verbindung (Standby-Port des Slave) umgeleitet.
  - Loop Detection
    Es wurde eine Schleife im Netzsegment erkannt.
  - Diagnosealarme
    Ein Diagnosewert hat eine bestimmte Grenze unter- bzw. überschritten.
  - Statusänderung 802.1X Port-Authentifizierung
    Dieses Ereignis tritt bei 802.1X-Authentifizierungen auf.
  - Link Check
    Es wurde eine Störungen bei einer optischen Übertragungsstrecke erkannt.

    Hinweis

    Dieses Ereignis können Sie nur bei Geräten mit optischen Schnittstellen konfigurieren.

  - Statusänderung PoE
    Der Zustand von PoE hat sich geändert.

    Hinweis

    Dieses Ereignis können Sie nur bei Geräten mit Unterstützung für PoE konfigurieren.

  - Secure NTP
    Bei der Nutzung von Secure NTP ist ein Fehler aufgetreten, z. B. wurde ein Schlüssel mit falscher Länge angegeben.
  - Service-Informationen
    Für bestimmte Ereignisse werden auch ohne Konfiguration Einträge in der Log-Tabelle erstellt. Für diese Ereignisse können Sie hier weitere Folgeaktionen konfigurieren (E-Mail, Trap, Syslog).

- **E-Mail**
  Das Gerät sendet eine E-Mail. Voraussetzung ist, dass der SMTP-Server eingerichtet und die Funktion "SMTP-Client" aktiviert ist.
- **Trap**
  Das Gerät löst einen SNMP-Trap aus. Voraussetzung ist, dass unter "System > Konfiguration" "SNMPv1-Traps" aktiviert ist.
- **Log-Tabelle**
  Das Gerät schreibt einen Eintrag in die Ereignisprotokoll-Tabelle, siehe "Information > Log-Tabelle"
- **Syslog**
  Das Gerät schreibt einen Eintrag auf den Systemprotokoll-Server. Voraussetzung ist, dass der Systemprotokoll-Server eingerichtet und die Funktion "Syslog-Client" aktiviert ist.
- **Fehler**
  Das Gerät löst einen Fehler aus. Die Fehler-LED leuchtet auf

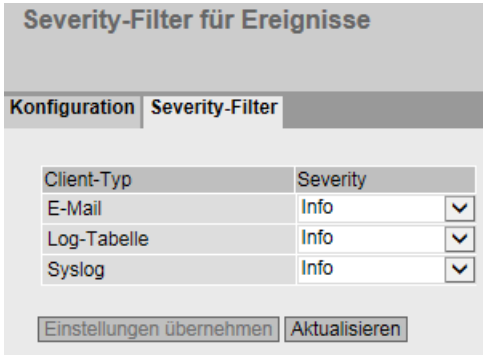
Vorgehensweise zur Konfiguration

1. Aktivieren Sie das Optionskästchen in der Zeile des gewünschten Ereignisses. Wählen Sie dabei das Ereignis in der Spalte unter den folgenden Aktionen aus:
   - E-Mail
   - Trap
   - Log-Tabelle
   - Syslog
   - Fehler
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.4.6.2 Severity-Filter

Einstellung der Severity-Filter

Stellen Sie auf dieser Seite die Schwellwertstufen für das Versenden von Systemereignisbenachrichtigungen ein.



In der ersten Tabellenspalte ist der Client-Typ angegeben, für den Sie die Einstellungen vornehmen:

- **E-Mail**
  Versand von Systemereignismeldungen per E-Mail
- **Log-Tabelle**
  Eintragen von Systemereignissen in die Log-Tabelle
- **Syslog**
  Versand von Systemereignismeldungen an einen Syslog-Server

Wählen Sie aus den Klapplisten der zweiten Tabellenspalte die gewünschte Stufe aus.

Sie haben folgende Werte zur Auswahl:

- **Critical**
  Systemereignisse werden ab dem Severity-Level Critical bearbeitet.
- **Warning**
  Systemereignisse werden ab dem Severity-Level Warning bearbeitet.
- **Info**
  Systemereignisse werden ab dem Severity-Level Info bearbeitet.

Vorgehensweise

Gehen Sie folgendermaßen vor, um die gewünschte Stufe zu konfigurieren:

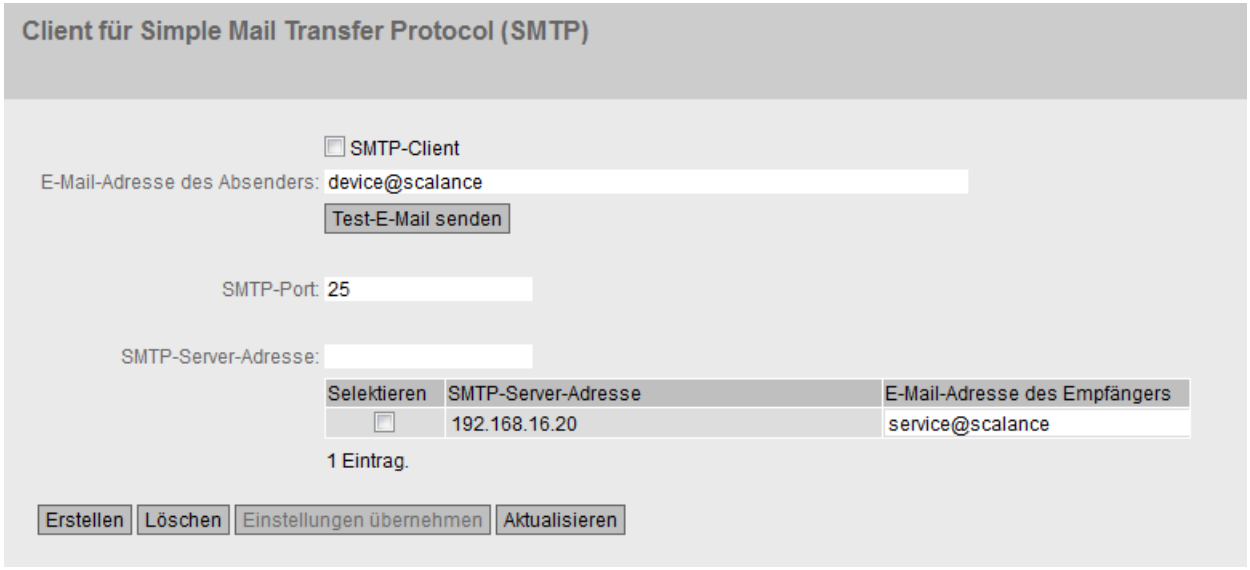
1. Wählen Sie aus den Klapplisten in der zweiten Tabellenspalte hinter den Client-Typen die gewünschten Werte aus.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.4.7 SMTP-Client

Netzüberwachung durch E-Mails

Das Gerät bietet die Möglichkeit, beim Auftreten eines Alarmereignisses automatisch eine E-Mail (z.B. an den Netzwerkadministrator) zu senden. Die E-Mail enthält die Identifikation des absendenden Geräts, eine Beschreibung der Alarmursache in Klartext sowie einen Zeitstempel. Damit kann für Netze mit wenigen Teilnehmern eine einfache zentrale Netzüberwachung auf Basis eines E-Mail-Systems aufgebaut werden. Bei eintreffenden E-Mail-Störmeldungen kann über die Identifikation des Absenders per Internet-Browser das WBM gestartet werden, um weitere Diagnoseinformationen auszulesen.

Auf dieser Seite können Sie bis zu drei SMTP-Server und die dazugehörigen E-Mail-Adressen konfigurieren.



Beschreibung

Die Seite enthält folgende Felder:

- **SMTP-Client**
  Aktivieren oder deaktivieren Sie den SMTP-Client.
- **E-Mail-Adresse des Absenders**
  Geben Sie den Absendernamen ein, der in der E-Mail angegeben werden soll, z. B. den Gerätenamen.
  Diese Einstellung gilt für alle konfigurierten SMTP-Server.
- **Test-E-Mail senden**
  Verschicken Sie eine Test-E-Mail, um Ihre Konfiguration zu prüfen.

- **SMTP-Port**
  Geben Sie den Port ein, über den Ihr SMTP-Server erreichbar ist.
  Werkseinstellung: 25
  Diese Einstellung gilt für alle konfigurierten SMTP-Server.
- **SMTP-Server-Adresse**
  Geben Sie die IP-Adresse des SMTP-Servers ein.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in einer zu löschenden Zeile das Optionskästchen.
- **SMTP-Server-Adresse**
  Zeigt die IP-Adresse des SMTP-Servers.
- **E-Mail-Adresse des Empfängers**
  Geben Sie die E-Mail-Adresse ein, an die das Gerät im Fehlerfall eine E-Mail sendet.

Vorgehensweise

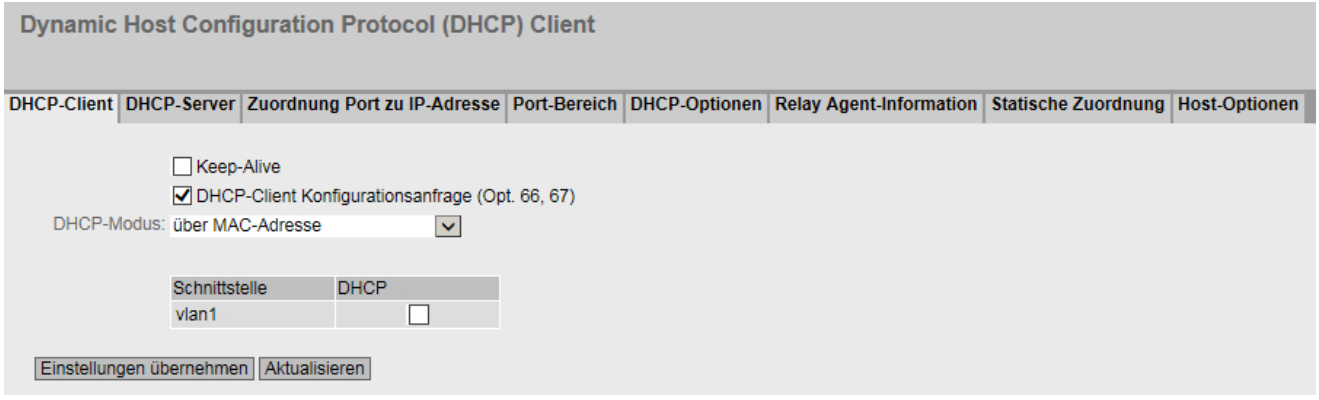
1. Aktivieren Sie die Option "SMTP-Client".
2. Geben Sie in das Eingabefeld "E-Mail-Adresse des Absenders" die entsprechende E-Mail-Adresse ein.
3. Senden Sie ggf. eine Test-E-Mail.
4. Geben Sie in das Eingabefeld "SMTP-Server-Adresse" die IP-Adresse des SMTP-Servers ein.
5. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.
6. Geben Sie in das Eingabefeld "Email-Adresse des Empfängers" die E-Mail-Adresse ein, an die das Gerät im Fehlerfall eine E-Mail senden soll.
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.4.8 DHCP

5.4.8.1 DHCP-Client

Einstellung des DHCP-Modus

Wenn das Gerät als DHCP-Client konfiguriert ist, startet es eine DHCP-Anfrage. Das Gerät erhält vom DHCP-Server als Antwort eine IPv4-Adresse zugewiesen. Der Server verwaltet einen Adressbereich, aus welchem er IPv4-Adressen vergibt. Es ist auch möglich, den Server so zu konfigurieren, dass der Client auf seine Anfrage immer dieselbe IPv4-Adresse zugewiesen bekommt.



Beschreibung

Die Seite enthält folgende Felder:

- **Keep-Alive**
  Wenn aktiviert, wird die IP-Adresse bei einem Verbindungsabbruch beibehalten und nicht auf 0.0.0.0 zurückgesetzt. Keep-Alive ist per Default aktiviert. Wenn Keep-Alive deaktiviert ist, wird die IP-Adresse bei einem Verbindungsabbruch auf 0.0.0.0 zurückgesetzt.
- **DHCP-Client Konfigurationsanfrage (Opt. 66, 67)**
  Wenn aktiviert, verwendet der DHCP-Client die Optionen dazu, die Konfigurationsdatei (Option 67) vom TFTP-Server (Option 66) herunterzuladen. Nach dem Neustart verwendet das Gerät die Daten aus der Konfigurationsdatei.

  Hinweis

  Konfigurationsdatei und Firmware-Version

  Die Konfigurationsdatei dient zum Abspeichern und Einlesen von Konfigurationsdaten innerhalb einer Firmware-Version z. B. 6.2. Konfigurationsdateien, die mit einer Firmware-Version kleiner oder gleich 6.1 erstellt wurden, können nicht auf einem Gerät mit einer Firmware-Version 6.2 eingelesen werden.

- **DHCP-Modus**
  Legen Sie fest, mit welcher Art von Kennung sich der DHCP-Client bei seinem DHCP-Server anmeldet:
  - über MAC-Adresse
    Die Identifikation läuft über die MAC-Adresse ab.
  - über DHCP-Client-ID
    Die Identifikation läuft über eine frei definierte DHCP-Client-ID ab.
  - über Systemname
    Die Identifikation läuft über den Systemnamen ab. Ist der Systemname 255 Zeichen lang, dann wird das letzte Zeichen nicht zur Identifikation benutzt.
  - über PROFINET-Gerätename
    Die Identifikation läuft über den PROFINET-Gerätenamen ab.

Die Tabelle gliedert sich in folgende Spalten:

- **Schnittstelle**
  Schnittstelle, auf die sich die Einstellung bezieht.
- **DHCP**
  Aktivieren oder deaktivieren Sie den DHCP-Client für die entsprechende Schnittstelle.

RADIUS-Authentifizierung und DHCP

Der DHCP-Client kann erst dann mit dem DHCP-Server kommunizieren, wenn die RADIUS-Authentifizierung auf dem SCALANCE X erfolgreich abgeschlossen ist. Wenn der DHCP-Client in den Ruhemodus wechselt, bevor der Authentifizierungsprozess erfolgreich abgeschlossen ist, erhält der Client zunächst keine IP-Adresse vom DHCP-Server. Der Authentifizierungsprozess kann sich aus folgenden Gründen verzögern:

- Der erste konfigurierte RADIUS-Server ist nicht erreichbar.
- Es findet ein Fallback auf MAC-Authentifizierung statt (nur bei SCALANCE XP-200).

Es gibt folgende Möglichkeiten, um eine gültige IP-Adresse für den DHCP-Client zu erhalten:

- Warten Sie, bis der DHCP-Client den Ruhemodus verlässt und automatisch wieder DHCP-Discover-Telegramme versendet.
- Starten Sie den DHCP-Client manuell neu.

Vorgehensweise

Gehen Sie folgendermaßen vor, um die IP-Adresse via DHCP Client ID zu konfigurieren:

1. Wählen Sie in der Klappliste "DHCP-Modus" die Identifikationsmethode aus.
   Wenn Sie den DHCP-Modus "über DHCP-Client-ID" auswählen, erscheint ein Eingabefeld. Geben Sie in das aktivierte Eingabefeld "DHCP-Client-ID" eine Zeichenkette zur Identifikation des Geräts ein. Diese wird dann vom DHCP-Server ausgewertet.
2. Wählen Sie die Option "DHCP-Client Konfigurationsanfrage (Opt. 66, 67)", wenn der DHCP-Client die Optionen 66 und 67 dazu verwenden soll, eine Konfigurationsdatei herunterzuladen und diese dann zu aktivieren.
3. Aktivieren Sie die Option "DHCP" in der Tabelle.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Hinweis

Wird eine Konfigurationsdatei heruntergeladen, so kann dies einen Neustart des Systems auslösen. Wenn sich die aktuell laufende Konfiguration und die Konfiguration in der heruntergeladenen Konfigurationsdatei unterscheiden, startet das System neu.

Achten Sie darauf, dass in dieser Konfigurationsdatei die Option "DHCP-Client Konfigurationsanfrage (Opt. 66, 67)" nicht mehr gesetzt ist.

5.4.8.2 DHCP-Server

Das Gerät können Sie als DHCP-Server betreiben. Damit ist es möglich, den angeschlossenen Geräten automatisch IP-Adressen zuzuweisen. Die IP-Adressen werden entweder dynamisch aus einem von Ihnen vergebenen Adressband (Pool) verteilt oder es wird eine bestimmte IP-Adresse einem bestimmten Gerät zugewiesen.

Hinweis

DHCP-Server-Zuordnungen löschen

Wenn Sie ein IPv4-Adressband deaktivieren bzw. löschen oder den DHCP-Server aus- und wieder einschalten, werden die DHCP-Server-Zuordnungen gelöscht, siehe "Information > DHCP-Server".

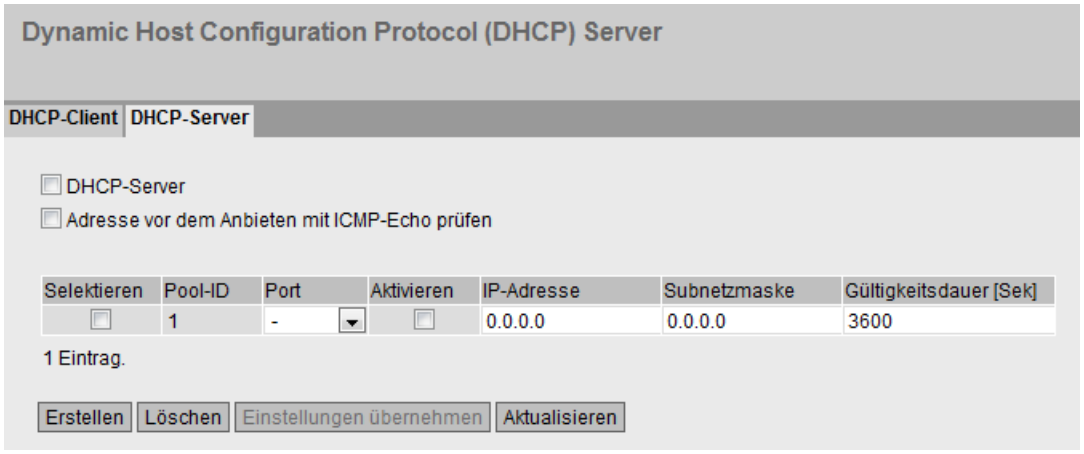
Der Aufbau dieser Seite ist davon abhängig, über wie viele VLAN-IP-Schnittstellen das Gerät verfügt.

Voraussetzung

Die angeschlossenen Geräte sind so konfiguriert, dass sie die IP-Adresse von einem DHCP-Server beziehen.

Geräte mit einer VLAN-IP-Schnittstelle

Auf dieser Seite legen Sie IPv4-Adressen fest, die über bestimmte Ports vergeben werden.



Beschreibung

Die Seite enthält folgende Felder:

- **DHCP-Server**
  Aktivieren oder deaktivieren Sie den DHCP-Server auf dem Gerät.

  Hinweis

  Damit keine Konflikte mit IPv4-Adressen entstehen, darf im Netzwerk nur ein Gerät als DHCP-Server konfiguriert sein.

- **Adresse vor dem Anbieten mit ICMP-Echo prüfen**
  Wenn aktiviert, prüft der DHCP-Server, ob eine IP-Adresse schon vergeben ist. Dazu sendet der DHCP-Server ICMP-Echomeldungen (Ping) an diese IPv4-Adresse. Wenn keine Antwort zurückkommt, wird die IPv4-Adresse vergeben.

  Hinweis

  Bei statischen Zuordnungen wird diese Prüfung nicht durchgeführt.

  Hinweis

  Wenn es in Ihrem Netzwerk Geräte gibt, bei denen der Echo-Dienst standardmäßig deaktiviert ist, kann es zu Konflikten bei den IPv4-Adressen kommen. Um dies zu vermeiden, vergeben Sie diesen Geräten eine IPv4-Adresse, die außerhalb des vom DHCP-Server verwendeten IPv4-Adressbands liegt.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Pool-ID**
  Zeigt die Nummer des IPv4-Adressbands an. Wenn Sie auf die Schaltfläche "Erstellen" klicken, wird eine neue Zeile mit einer eindeutigen Nummer (Pool-ID) angelegt.

- **Port**
  Legen Sie fest, über welchen Port die IPv4-Adresse dieses DHCP-Pools vergeben werden sollen.
- **Aktivieren**
  Legen Sie fest, ob diese IPv4-Adresse verwendet wird.

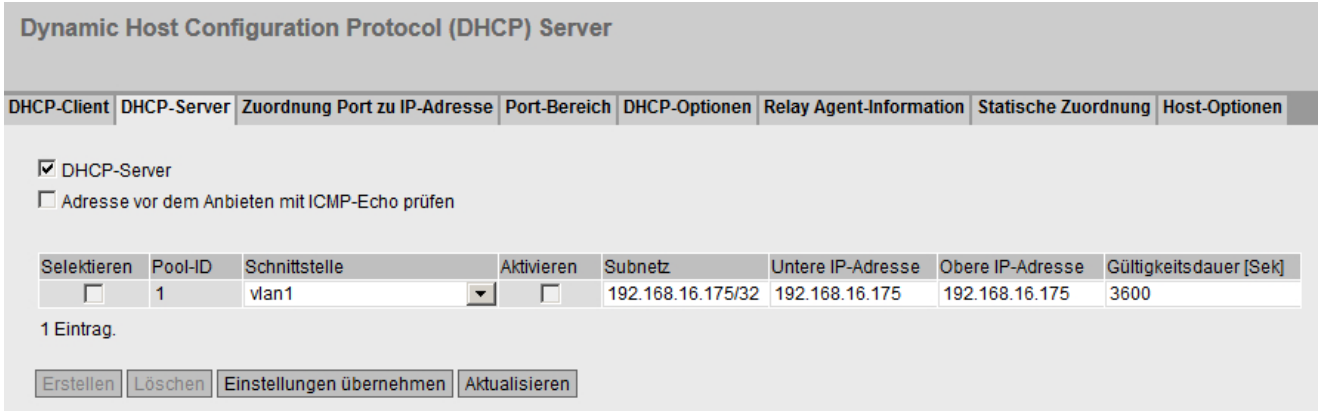
  Hinweis

  Wenn Sie die IPv4-Adresse aktivieren, werden deren Einstellungen in diesem DHCP-Register ausgegraut und sind nicht mehr editierbar.

- **IP-Adresse**
  Tragen Sie die IPv4-Adresse ein, die über den angegebenen Port vergeben werden soll.
- **Subnetz**
  Tragen Sie die Subnetzmaske passend zu der IPv4-Adresse ein. Verwenden Sie die CIDR-Schreibweise.
- **Gültigkeitsdauer [Sek]**
  Legen Sie fest, für wie viele Sekunden die vergebene IPv4-Adresse gültig bleibt. Nachdem die Gültigkeitsdauer zur Hälfte abgelaufen ist, kann der DHCP-Client die vergebene IPv4-Adresse verlängern. Nach Ablauf der gesamten Zeitdauer muss der DHCP-Client eine neue IPv4-Adresse anfordern.

Geräte mit mehreren VLAN-IP-Schnittstellen

Auf dieser Seite legen Sie das Adressband fest, aus dem das angeschlossene Gerät eine beliebige IP-Adresse erhält. Die statische Zuordnung der IP-Adressen konfigurieren Sie unter "Statische Zuordnung".



Beschreibung

Die Seite enthält folgende Felder:

- **DHCP-Server**
  Aktivieren oder deaktivieren Sie den DHCP-Server auf dem Gerät.

  Hinweis

  Damit keine Konflikte mit IPv4-Adressen entstehen, darf im Netzwerk nur ein Gerät als DHCP-Server konfiguriert sein.

- **Adresse vor dem Anbieten mit ICMP-Echo prüfen**
  Wenn aktiviert, prüft der DHCP-Server, ob eine IP-Adresse schon vergeben ist. Dazu sendet der DHCP-Server ICMP-Echomeldungen (Ping) an diese IPv4-Adresse. Wenn keine Antwort zurückkommt, wird die IPv4-Adresse vergeben.

  Hinweis

  Wenn es in Ihrem Netzwerk Geräte gibt, bei denen der Echo-Dienst standardmäßig deaktiviert ist, kann es zu Konflikten bei den IPv4-Adressen kommen. Um dies zu vermeiden, vergeben Sie diesen Geräten eine IPv4-Adresse, die außerhalb des vom DHCP-Server verwendeten IPv4-Adressbands liegt.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Pool-ID**
  Zeigt die Nummer des IPv4-Adressbands an. Wenn Sie auf die Schaltfläche "Erstellen" klicken, wird eine neue Zeile mit einer eindeutigen Nummer (Pool-ID) angelegt.
- **Schnittstelle**
  Wählen Sie eine VLAN-IP-Schnittstelle aus. Über diese Schnittstelle werden die IPv4-Adressen dynamisch vergeben.
  Voraussetzung für die Vergabe ist, dass die IPv4-Adresse der Schnittstelle im Subnetz des IPv4-Adressbands liegt. Wenn das nicht der Fall ist, vergibt die Schnittstelle keine IPv4-Adressen.
- **Aktivieren**
  Legen Sie fest, ob dieses IPv4-Adressband verwendet wird.

  Hinweis

  Wenn Sie das IPv4-Adressband aktivieren, werden dessen Einstellungen in diesem sowie in den weiteren DHCP-Registern ausgegraut und sind nicht mehr editierbar.

- **Subnetz**
  Tragen Sie den Netzadressbereich ein, der den Geräten zugewiesen wird. Verwenden Sie die CIDR-Schreibweise.

  Hinweis

  Auswirkungen auf andere Register

  Wenn Sie die Felder "Subnetz", "Untere IP-Adresse" und "Obere IP-Adresse" konfigurieren, wird die Zeile des entsprechenden DHCP-Pools im Register "Zuordnung Port zu IP-Adresse" gelöscht. Wenn Sie die Konfiguration löschen, ist die Zeile im Register "Zuordnung Port zu IP-Adresse" wieder verfügbar.

- **Untere IP-Adresse**
  Tragen Sie die IPv4-Adresse ein, die den Anfang des dynamischen IPv4-Adressbands festlegt. Die IPv4-Adresse muss innerhalb des Netzadressbereichs liegen, den Sie bei "Subnetz" konfiguriert haben.
- **Obere IP-Adresse**
  Tragen Sie die IPv4-Adresse ein, die das Ende des dynamischen IPv4-Adressbands festlegt. Die IPv4-Adresse muss innerhalb des Netzadressbereichs liegen, den Sie bei "Subnetz" konfiguriert haben.
- **Gültigkeitsdauer [Sek]**
  Legen Sie fest, für wie viele Sekunden die vergebene IPv4-Adresse gültig bleibt. Nachdem die Gültigkeitsdauer zur Hälfte abgelaufen ist, kann der DHCP-Client die vergebene IPv4-Adresse verlängern. Nach Ablauf der gesamten Zeitdauer muss der DHCP-Client eine neue IPv4-Adresse anfordern.

Vorgehensweise

DHCP-Server global aktivieren

1. Aktivieren Sie das Optionskästchen "DHCP-Server".
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Konfiguration für Geräte mit einer VLAN-IP-Schnittstelle

1. Klicken Sie auf die Schaltfläche "Erstellen".
   Es wird eine neue Zeile mit einer eindeutigen Nummer (Pool-ID) angelegt.
2. Wählen Sie den gewünschten Port aus.
3. Geben Sie die IPv4-Adresse und die Subnetzmaske ein.
4. Geben Sie die Gültigkeitsdauer ein.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
6. Aktivieren Sie in diesem Register das Optionskästchen "Aktivieren".
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Konfiguration für Geräte mit mehreren VLAN-IP-Schnittstellen

1. Klicken Sie auf die Schaltfläche "Erstellen".
   Es wird eine neue Zeile mit einer eindeutigen Nummer (Pool-ID) angelegt.
2. Wählen Sie eine VLAN-IP-Schnittstelle aus.

3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
   Im Register "Zuordnung Port zu IP-Adresse" wird eine neue Zeile für die Pool-ID angelegt. In der Spalte "Port" stehen alle Ports zur Auswahl, die derzeit zu dem ausgewählten VLAN gehören.
   Im Register "Port-Bereich" wird eine neue Zeile für die Pool-ID angelegt. In der Zeile werden alle Ports aktiviert, die derzeit zu dem ausgewählten VLAN gehören.
   Im Register "DHCP-Optionen" werden die Standardoptionen für den Pool angelegt.
4. Sie haben folgende Möglichkeiten, den Pool zu konfigurieren:
   DHCP-Pool für ein IPv4-Adressband konfigurieren
   - Geben Sie das Subnetz, die untere und obere IPv4-Adresse ein.
   - Geben Sie die Gültigkeitsdauer ein.
   - Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

   DHCP-Pool für eine IPv4-Adresse konfigurieren
   - Wechseln Sie in das Register "Zuordnung Port zu IP-Adresse".
   - Wählen Sie den gewünschten Port aus.
     Im Register "Port-Bereich" ist nur noch der ausgewählte Port aktiviert.
   - Geben Sie die IPv4-Adresse und die Subnetzmaske ein.
   - Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
     Im Register "DHCP-Server" sind die Felder "Subnetz", "Untere IP-Adresse" und "Obere IP-Adresse" entsprechend ausgefüllt.
   - Konfigurieren Sie im Register "DHCP-Server" die Gültigkeitsdauer.
5. Nehmen Sie die gewünschten Einstellungen für den Pool in den weiteren DHCP-Registern vor.

DHCP-Pool aktivieren

1. Aktivieren Sie im Register "DHCP-Server" das Optionskästchen "Aktivieren".
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

DHCP-Pool löschen

Hinweis

Sie können nur Einträge löschen, die nicht aktiviert sind.

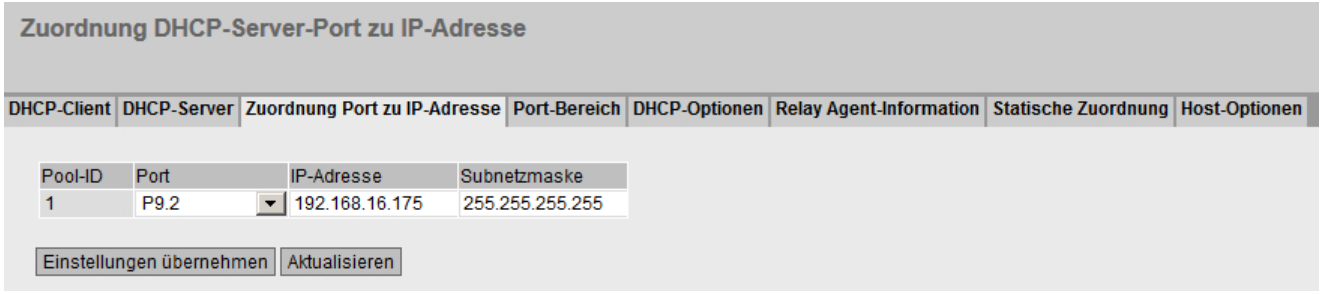
1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen "Selektieren".
   Wiederholen Sie den Vorgang für alle Einträge, die Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Löschen".
   Der Eintrag wird gelöscht.

5.4.8.3 Zuordnung Port zu IP-Adresse

Auf dieser Seite ordnen Sie einem bestimmten Port genau eine IP-Adresse zu.

Nachdem Sie im Register "DHCP-Server" ein IPv4-Adressband angelegt haben, wird in diesem Register eine neue Zeile angelegt.

Die Konfiguration auf dieser Seite wirkt sich auf die Register "DHCP-Server" und "Port-Bereich" aus.



Beschreibung

Die Tabelle enthält folgende Spalten:

- **Pool-ID**
  Zeigt die Nummer des IPv4-Adressbands an. Für jedes Adressband wird eine Zeile angelegt.
- **Port**
  Wählen Sie aus der Klappliste die Einstellung. Sie haben folgende Einstellungsmöglichkeiten:
  - Px.y
    Legen Sie fest, über welchen Port die IPv4-Adresse vergeben werden sollen. Sie können nur Ports auswählen, die sich in dem entsprechenden VLAN befinden.
    Wenn Sie einen Port auswählen, ist im Register "Port-Bereich" nur noch dieser Port aktiviert.
  - Nicht ausgewählt
    Bei dieser Einstellung sind im Register "Port-Bereich" keine Ports oder mehr als ein Port ausgewählt.
    Wenn Sie die Einstellung "Nicht ausgewählt" auswählen, werden alle Ports im Register "Port-Bereich" deaktiviert.
- **IP-Adresse**
  Geben Sie eine IPv4-Adresse an.
  Im Register "DHCP-Server" werden die Felder "Untere IP-Adresse" und "Obere IP-Adresse" entsprechend ausgefüllt.
- **Subnetzmaske**
  Geben Sie eine dazugehörige Subnetzmaske an.
  Im Register "DHCP-Server" wird das Feld "Subnetz" entsprechend ausgefüllt.

Vorgehensweise

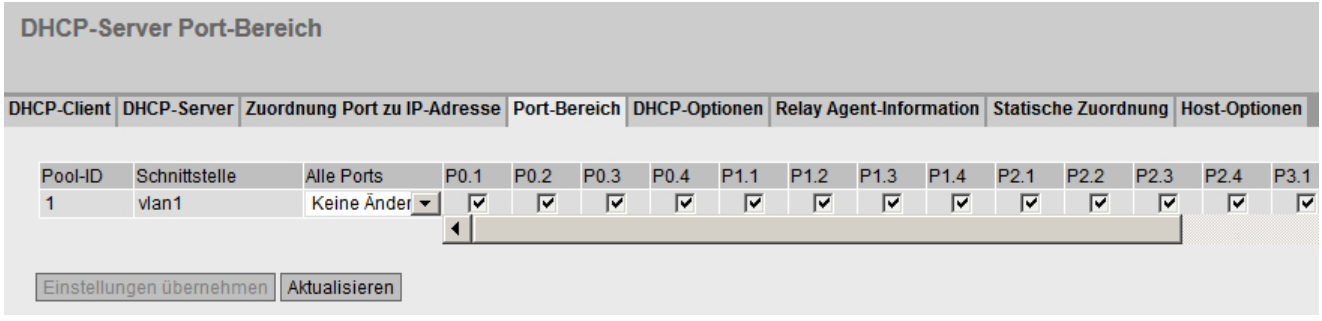
Port einer IP-Adresse zuordnen

1. Wählen Sie den gewünschten Port aus.
2. Geben Sie die IPv4-Adresse und die Subnetzmaske ein.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
   Im Register "Port-Bereich" ist für den entsprechenden DHCP-Pool nur noch der ausgewählte Port aktiviert.
   Im Register "DHCP-Server" sind für den entsprechenden DHCP-Pool die Felder "Subnetz", "Untere IP-Adresse" und "Obere IP-Adresse" entsprechend ausgefüllt.

5.4.8.4 Port-Bereich

Auf dieser Seite definieren Sie die Ports, über die die IPv4-Adressen eines Adressbands vergeben werden.

Nachdem Sie im Register "DHCP-Server" ein IPv4-Adressband angelegt haben, wird in diesem Register eine neue Zeile angelegt und alle Ports ausgewählt, die sich zu diesem Zeitpunkt in dem entsprechenden VLAN befinden. Wenn Sie nachträglich Ports zu dem VLAN hinzufügen, werden die Ports in diesem Register nicht automatisch aktiviert.



Beschreibung

Die Tabelle enthält folgende Spalten:

- **Pool-ID**
  Zeigt die Nummer des IPv4-Adressbands an. Für jedes Adressband wird eine Zeile angelegt.
- **Schnittstelle**
  Zeigt die zugeordnete IP-Schnittstelle an.

- **Alle Ports**
  Wählen Sie aus der Klappliste die Einstellung. Sie haben folgende Einstellungsmöglichkeiten:
  - Aktiviert
    Das Optionskästchen wird bei allen Ports des entsprechenden VLANs aktiviert.
  - Deaktiviert
    Das Optionskästchen wird bei allen Ports entsprechenden VLANs deaktiviert.
  - Keine Änderung
    Die Tabelle bleibt unverändert.
- **Px.y**
  Legen Sie fest, über welche Ports die IPv4-Adressen des Adressbands vergeben werden sollen.
  Sie können nur Ports auswählen, die sich in dem entsprechenden VLAN befinden.

Hinweis

Auswirkungen auf andere Register

Wenn Sie genau einen Port aktivieren, ist dieser Port im Register "Zuordnung Port zu IP-Adresse" ausgewählt.

Wenn Sie keinen Port oder mehr als einen Port aktivieren, ist im Register "Zuordnung Port zu IP-Adresse" die Einstellung "Nicht ausgewählt" ausgewählt.

Vorgehensweise

Ports einzeln konfigurieren

1. Aktivieren bzw. deaktivieren Sie das Optionskästchen bei den gewünschten Ports.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

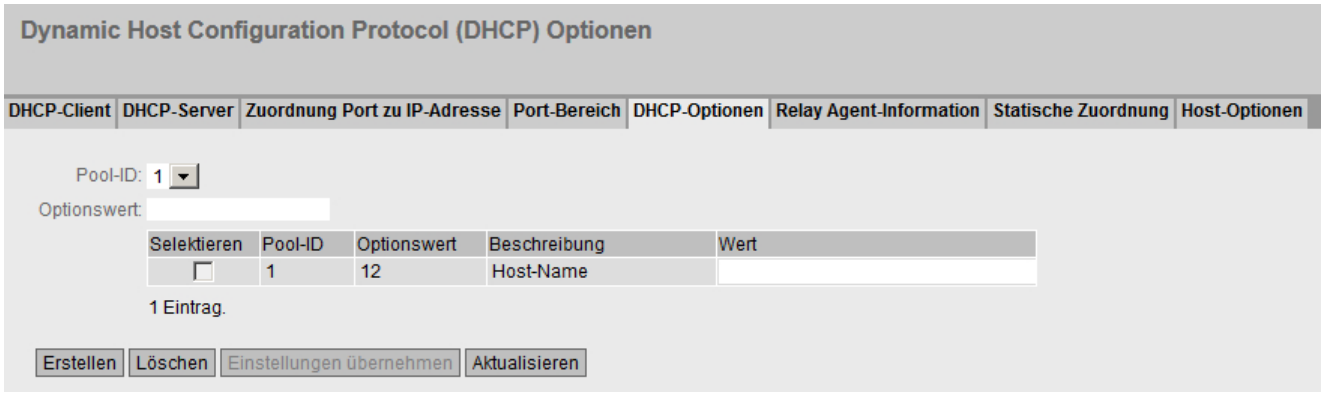
Alle Ports konfigurieren

1. Wählen Sie in der Klappliste "Alle Ports" den gewünschten Eintrag.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.4.8.5 DHCP-Optionen

Auf dieser Seite legen Sie fest, welche DHCP-Optionen der DHCP-Server unterstützt. Die verschiedenen DHCP-Optionen sind im RFC 2132 definiert.

Die DHCP-Optionen 1, 3, 6, 66 und 67 werden automatisch beim Erstellen des IPv4-Adressbands angelegt. Mit Ausnahme der DHCP-Option 1 sind die Optionen löschbar. Bei der DHCP-Option 1 wird automatisch die Subnetzmaske eingestellt, die Sie unter "DHCP-Server" für das Adressband eingegeben haben. Bei der DHCP-Option 3 können Sie über ein Optionskästchen die interne IPv4-Adresse des DHCP-Servers als DHCP-Parameter einstellen.



Beschreibung

Die Seite enthält folgende Felder:

- **Pool-ID**
  Wählen Sie das gewünschte IPv4-Adressband aus.
- **Optionswert**
  Geben Sie die Nummer der gewünschten DHCP-Option ein. Die verschiedenen DHCP-Optionen sind im RFC 2132 definiert. Die unterstützten DHCP-Optionen werden im folgenden Absatz aufgeführt.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Pool-ID**
  Zeigt die Nummer des IPv4-Adressbands an.
- **Optionswert**
  Zeigt die Nummer der DHCP-Option an.
- **Beschreibung**
  Zeigt eine Beschreibung der DHCP-Option an.

- **Schnittstellen-IP verwenden**
  Wenn Sie das Optionskästchen aktivieren, wird die IPv4-Adresse als Default-Gateway verwendet, die der IP-Schnittstelle des Adressbands zugeordnet ist. Wenn das Optionskästchen deaktiviert ist, können Sie eine IPv4-Adresse eingeben.
- **Wert**
  Geben Sie den DHCP-Parameter ein, der dem DHCP-Client übergeben wird. Der Inhalt ist abhängig von der DHCP-Option.
  - DHCP-Option 3 (Default-Gateway):
    Geben Sie den DHCP-Parameter als IPv4-Adresse an, z. B. 192.168.100.2.
  - DHCP-Option 6 (DNS):
    Geben Sie den DHCP-Parameter als IPv4-Adresse an, z. B. 192.168.100.2. Sie können bis zu drei IPv4-Adressen durch Komma getrennt angeben.
  - DHCP-Option 12 (Host-Name)
    Geben Sie den Hostnamen im String-Format an.
  - DHCP-Option 66 (TFTP-Server):
    Geben Sie den DHCP-Parameter als IPv4-Adresse an, z. B. 192.168.100.2.
  - DHCP-Option 67 (Bootfile-Name)
    Geben Sie den Namen der Bootdatei im String-Format an.

Unterstützte DHCP-Optionen

Folgende DHCP-Optionen werden unterstützt:

- Option 1
- Option 3
- Option 6
- Option 12
- Option 66
- Option 67

Vorgehensweise

DHCP-Option anlegen

1. Wählen Sie eine Pool-ID aus.
2. Geben Sie den Optionswert ein.
3. Klicken Sie auf die Schaltfläche "Erstellen".
4. Geben Sie einen Wert ein.
5. Aktivieren Sie bei der Option 3 ggf. das Optionskästchen "Schnittstellen-IP verwenden".
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

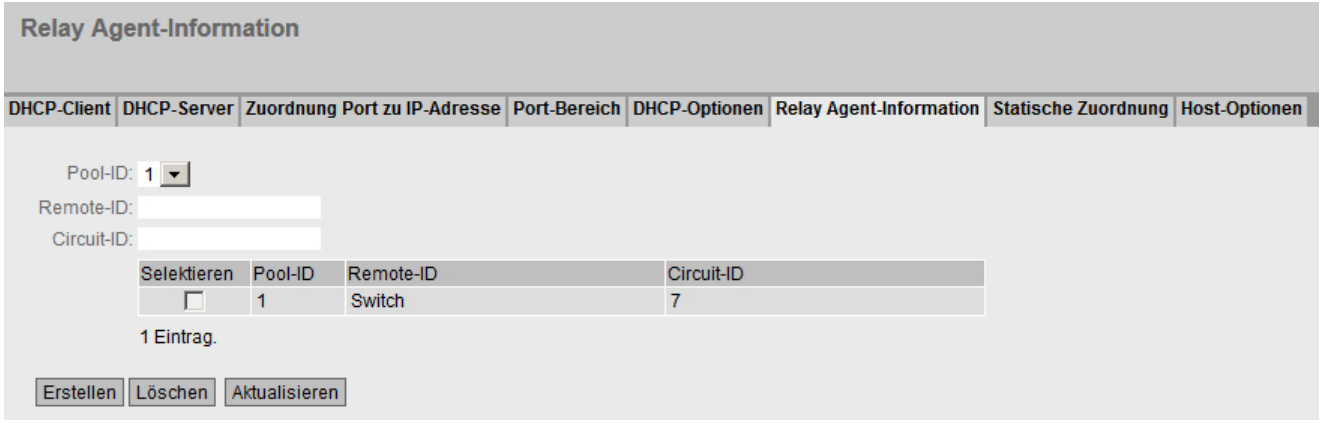
DHCP-Option löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen "Selektieren". Wiederholen Sie den Vorgang für alle Einträge, die Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Löschen". Der Eintrag wird gelöscht.

5.4.8.6 Relay Agent-Information

Auf dieser Seite definieren Sie, dass Geräten mit einer bestimmten Remote-ID und Circuit-ID die IPv4-Adressen aus einem bestimmten Adressband zugeordnet werden.

Wenn Sie für ein Adressband einen solchen Eintrag erstellen, reagieren die Ports des Adressbands nur auf DHCP-Anfragen über einen DHCP Relay Agent (Option 82). Sie können weitere Adressbänder für die gleichen IP-Schnittstellen anlegen, sodass die Ports auf verschiedene Anfragen reagieren.



Beschreibung

Die Seite enthält folgende Felder:

- **Pool-ID**
  Wählen Sie das gewünschte IPv4-Adressband aus.
- **Remote-ID**
  Tragen Sie die Remote-ID ein.
- **Circuit-ID**
  Tragen Sie die Circuit-ID ein.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Pool-ID**
  Zeigt die Nummer des IPv4-Adressbands an.

- **Remote-ID**
  Zeigt die Remote-ID an.
- **Circuit-ID**
  Zeigt die Circuit-ID an.

Vorgehensweise

Eintrag anlegen

1. Wählen Sie eine Pool-ID aus.
2. Geben Sie die Remote-ID ein.
3. Geben Sie die Circuit-ID ein.
4. Klicken Sie auf die Schaltfläche "Erstellen".

Eintrag löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen "Selektieren". Wiederholen Sie den Vorgang für alle Einträge, die Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Löschen".
   Der Eintrag wird gelöscht.

5.4.8.7 Statische Zuordnung

Auf dieser Seite definieren Sie, dass DHCP-Clients abhängig von ihrer Client-ID bzw. MAC-Adresse eine vorgegebene IPv4-Adresse zugeordnet wird.

Beschreibung

Die Seite enthält folgende Felder:

- **Pool-ID**
  Wählen Sie das gewünschte IPv4-Adressband aus.
- **Identifikationsmethode des Clients**
  Wählen Sie die Methode, nach der ein Client identifiziert wird.
  - Ethernet MAC
    Der Client wird über seine MAC-Adresse identifiziert.
  - Client-ID
    Der Client wird über eine frei definierte DHCP-Client-ID identifiziert.
- **Wert**
  Tragen Sie die MAC-Adresse (Ethernet MAC) oder die Client-ID (Client-ID) des Clients ein.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Pool-ID**
  Zeigt die Nummer des IPv4-Adressbands an.
- **Identifikationsmethode**
  Zeigt an, ob der Client über seine MAC-Adresse oder die Client-ID identifiziert wird.
- **Wert**
  Zeigt die MAC-Adresse oder Client-ID des Clients an.
- **IP-Adresse**
  Legen Sie die IPv4-Adresse fest, die dem Client zugewiesen wird. Die IPv4-Adresse muss innerhalb des IPv4-Adressbands liegen.

Vorgehensweise

Statische Zuordnung anlegen

1. Wählen Sie eine Pool-ID aus.
2. Wählen Sie die Identifikationsmethode des Clients aus.
3. Geben Sie den Wert ein.
4. Klicken Sie auf die Schaltfläche "Erstellen".
5. Legen Sie die IPv4-Adresse fest, die dem Client zugewiesen wird.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Statische Zuordnung löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen "Selektieren".
   Wiederholen Sie den Vorgang für alle Einträge, die Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Löschen".
   Der Eintrag wird gelöscht.

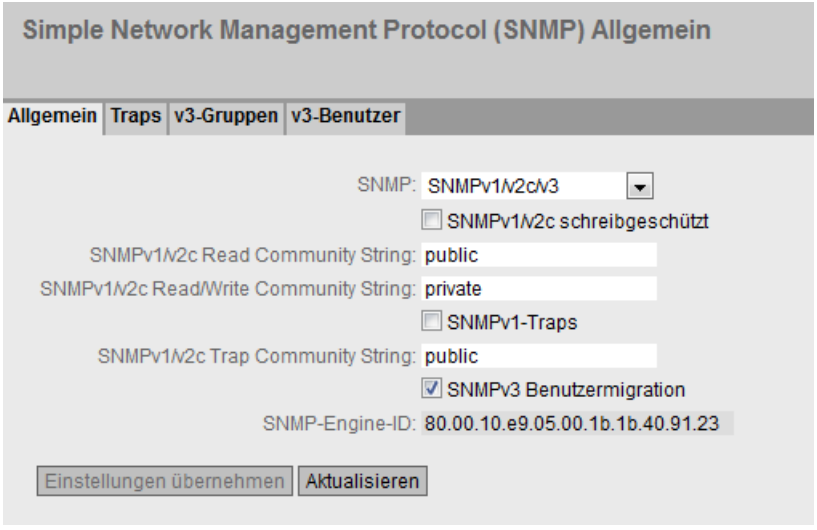
5.4.9 SNMP

Beachten Sie hierzu auch das Kapitel "Technische Grundlagen", Abschnitt "SNMP (Seite 60)".

5.4.9.1 Allgemein

Konfiguration von SNMP

Auf dieser Seite treffen Sie grundlegende Einstellungen für SNMP. Aktivieren Sie die Optionen abhängig von der Funktion, die Sie nutzen wollen.



Beschreibung

Die Seite enthält folgende Felder:

- **SNMP**
  Wählen Sie aus der Klappliste das SNMP-Protokoll. Folgende Einstellungen sind möglich:
  - "-" (Deaktiviert)
    SNMP deaktiviert.
  - SNMPv1/v2c/v3
    SNMPv1/v2c/v3 wird unterstützt.

    Hinweis

    Beachten Sie, dass SNMP in den Versionen 1 und 2c über keine Sicherheitsmechanismen verfügt.
  - SNMPv3
    Nur SNMPv3 wird unterstützt.
- **SNMPv1/v2c schreibgeschützt**
  Wenn Sie diese Option aktivieren, kann SNMPv1/v2c nur lesend auf die SNMP-Variablen zugreifen.

  Hinweis

  Community String

  Verwenden Sie aus Sicherheitsgründen nicht die Standardwerte "public" oder "private". Ändern Sie die Community Strings nach der Erst-Installation.

  Die empfohlene Mindestlänge für Community Strings sind 6 Zeichen.

  Aus Sicherheitsgründen ist mit dem SNMPv1/v2c Read Community String nur eingeschränkter Zugriff auf Objekte der SNMPCommunityMIB möglich. Mit dem SNMPv1/v2c Read/Write Community String haben Sie vollen Zugriff auf die SNMPCommunityMIB.
- **SNMPv1/v2c Read Community String**
  Tragen Sie den Community String für den lesenden Zugriff des SNMP-Protokolls ein.
- **SNMPv1/v2c Read/Write Community String**
  Tragen Sie den Community String für den lesenden und schreibenden Zugriff des SNMP-Protokolls ein.
- **SNMPv1-Traps**
  Aktivieren oder deaktivieren Sie das Senden von SNMPv1-Traps (Alarmtelegramme). Im Register "Trap" legen Sie die IP-Adressen der Geräte fest, an die SNMPv1-Traps gesendet werden.
- **SNMPv1/v2c Trap Community String**
  Tragen Sie den Community String für das Senden von SNMPv1/v2c-Meldungen ein.

- **SNMPv3 Benutzermigration**
  - Aktiviert
    Wenn die Funktion aktiviert ist, wird eine SNMP-Engine-ID generiert, die migriert werden kann. Sie können konfigurierte SNMPv3-Benutzer auf ein anderes Gerät übertragen. Wenn Sie diese Funktion aktivieren und die Konfiguration des Geräts auf ein anderes Gerät laden, bleiben konfigurierte SNMPv3-Benutzer erhalten.
  - Deaktiviert
    Wenn die Funktion deaktiviert ist, wird eine gerätespezifische SNMP-Engine-ID generiert. Um die ID zu generieren, wird die Agent-MAC-Adresse des Geräts verwendet. Sie können diese SNMP-Benutzerkonfiguration nicht auf andere Geräte übertragen. Wenn Sie die Konfiguration des Geräts auf ein anderes Gerät laden, werden alle konfigurierten SNMPv3-Benutzer gelöscht.
- **SNMP-Engine-ID**
  Zeigt die SNMP-Engine-ID an.

Vorgehensweise

1. Wählen Sie aus der Klappliste "SNMP" die gewünschte Option:
   - "-" (Deaktiviert)
   - SNMPv1/v2c/v3
   - SNMPv3
2. Aktivieren Sie das Optionskästchen "SNMPv1/v2c schreibgeschützt", wenn Sie mit SNMPv1/v2c nur lesend auf SNMP-Variablen zugreifen wollen.
3. Tragen Sie im Eingabefeld "SNMPv1/v2c Read Community String" die gewünschte Zeichenkette ein.
4. Tragen Sie im Eingabefeld "SNMPv1/v2c Read/Write Community String" die gewünschte Zeichenkette ein.
5. Aktivieren Sie ggf. die SNMPv3 Benutzermigration.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

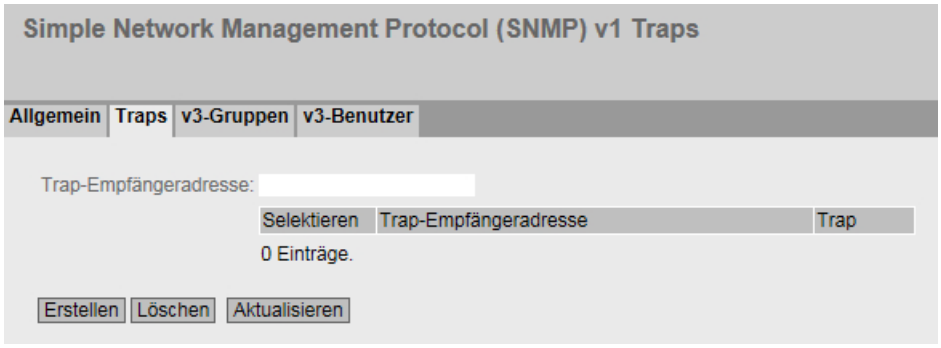
5.4.9.2 Traps

SNMP-Traps bei Alarmereignissen

Beim Eintreten eines Alarmereignisses kann das Gerät SNMP-Traps (Alarmtelegramme) an bis zu zehn verschiedene Management-Stationen gleichzeitig senden. Es werden nur bei solchen Ereignissen Traps gesendet, die im Menüpunkt "System > Ereignisse" festgelegt wurden.

Hinweis

Traps werden nur dann versendet, wenn Sie im Register "Allgemein" oder unter "System > Konfiguration" die Option "SNMPv1-Traps" aktiviert haben.



Beschreibung

- **Trap-Empfängeradresse**
  Tragen Sie die IP-Adresse der Station ein, an die das Gerät SNMP-Traps sendet. Sie können bis zu zehn verschiedene Empfänger angeben.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Trap-Empfängeradresse**
  Ändern Sie bei Bedarf die IP-Adressen der Stationen.
- **Trap**
  Aktivieren oder deaktivieren Sie das Senden von Traps. Stationen, die eingetragen, aber nicht aktiviert sind, erhalten keine SNMP-Traps.

Vorgehensweise

Trap-Eintrag erstellen

1. Tragen Sie bei "Trap-Empfängeradresse" die IP-Adresse der Station ein, an die das Gerät Traps senden soll.
2. Klicken Sie auf die Schaltfläche "Erstellen", um einen neuen Trap-Eintrag zu erstellen.
3. Aktivieren Sie in der gewünschten Zeile "Trap".
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

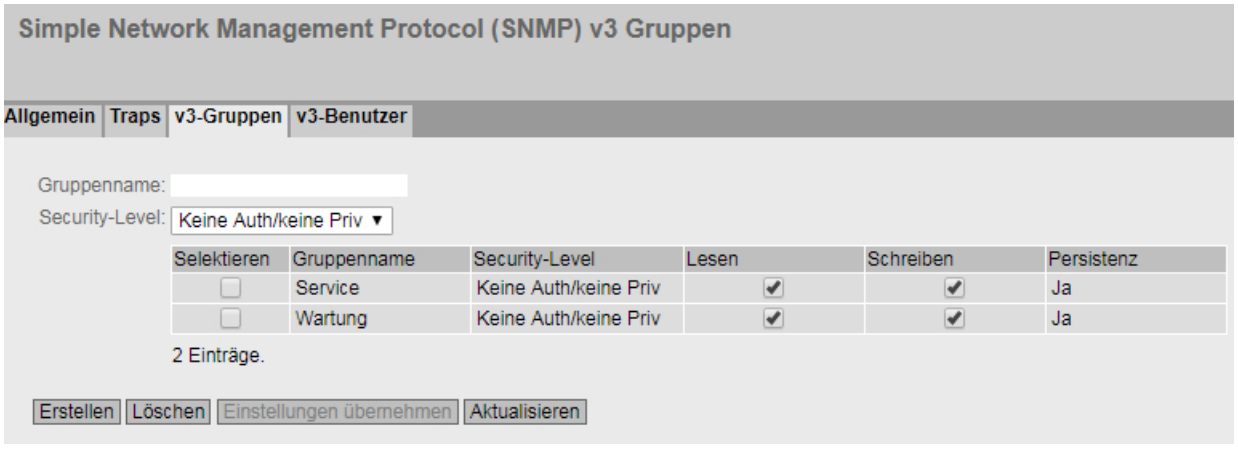
Trap-Eintrag löschen

1. Aktivieren Sie in der zu löschenden Zeile "Selektieren".
2. Klicken Sie auf die Schaltfläche "Löschen". Der Eintrag wird gelöscht.

5.4.9.3 v3-Gruppen

Security-Einstellungen und Rechtevergabe

SNMP Version 3 bietet eine Rechtevergabe, Authentifizierung und Verschlüsselung auf Protokollebene. Das Security-Level und die Lese-/Schreibrechte werden gruppenspezifisch definiert. Für jedes Mitglied einer Gruppe gelten automatisch die entsprechenden Einstellungen.



Beschreibung

Die Seite enthält folgende Felder:

- **Gruppenname**
  Tragen Sie den Namen der Gruppe ein. Die maximale Länge beträgt 32 Zeichen.
- **Security-Level**
  Wählen Sie die Sicherheitsstufe (Authentifizierung, Verschlüsselung) aus, die für die gewählte Gruppe gültig ist. Es gibt folgende Möglichkeiten:
  - Keine Auth/keine Priv
    Keine Authentifizierung aktiviert / keine Verschlüsselung aktiviert.
  - Auth/keine Priv
    Authentifizierung aktiviert / keine Verschlüsselung aktiviert.
  - Auth/Priv
    Authentifizierung aktiviert / Verschlüsselung aktiviert.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Gruppenname**
  Zeigt die definierten Gruppennamen an.
- **Security-Level**
  Zeigt die konfigurierte Sicherheitsstufe an.

- **Lesen**
  Aktivieren oder deaktivieren Sie den Lesezugriff für die gewünschte Gruppe.
- **Schreiben**
  Aktivieren oder deaktivieren Sie den Schreibzugriff für die gewünschte Gruppe.

  Hinweis

  Damit der Schreibzugriff funktioniert, müssen Sie ebenfalls den Lesezugriff aktivieren.

- **Persistenz**
  Zeigt an, ob die Gruppe einem SNMPv3-Benutzer zugeordnet ist. Wenn die Gruppe keinem SNMPv3-Benutzer zugeordnet ist, wird kein automatisches Speichern ausgelöst und die konfigurierte Gruppe ist nach einem Neustart des Geräts gelöscht.
  - Ja
    Die Gruppe ist einem SNMPv3-Benutzer zugeordnet.
  - Nein
    Die Gruppe ist keinem SNMPv3-Benutzer zugeordnet.

Vorgehensweise

Anlegen einer neuen Gruppe

1. Geben Sie bei "Gruppenname" den gewünschten Gruppennamen ein.
2. Wählen Sie aus der Klappliste "Security-Level" die gewünschte Sicherheitsstufe aus.
3. Klicken Sie auf die Schaltfläche "Erstellen", um einen neuen Eintrag zu erzeugen.
4. Legen Sie bei "Lesen" die gewünschten Leserechte für die Gruppe fest.
5. Legen Sie bei "Schreiben" die gewünschten Schreibrechte für die Gruppe fest.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Ändern einer Gruppe

1. Legen Sie bei "Lesen" die gewünschten Leserechte für die Gruppe fest.
2. Legen Sie bei "Schreiben" die gewünschten Schreibrechte für die Gruppe fest.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Hinweis

Der einmal vergebene Gruppenname und die Sicherheitsstufe können nach dem Anlegen nicht mehr geändert werden. Wenn Sie den Gruppennamen oder die Sicherheitsstufe ändern wollen, müssen Sie die Gruppe löschen und mit dem neuen Namen neu anlegen und neu konfigurieren.

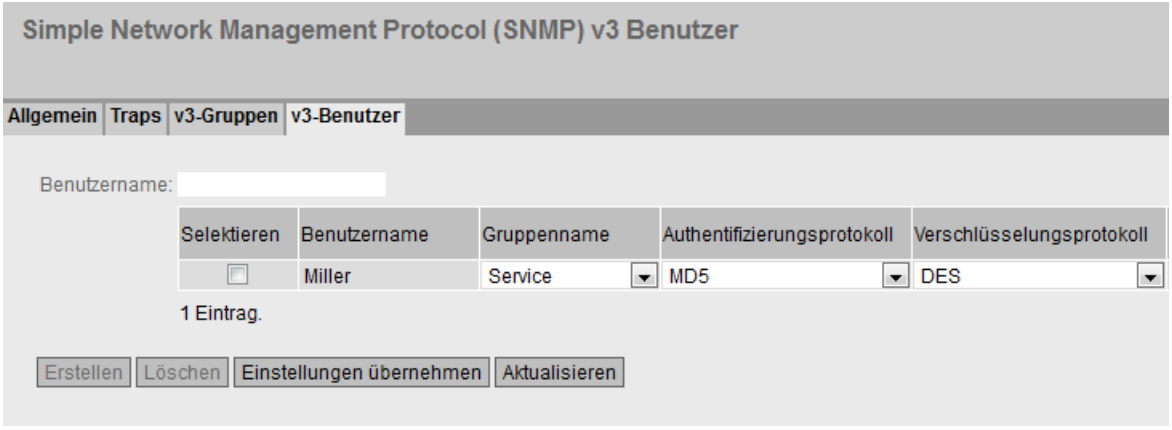
Löschen einer Gruppe

1. Aktivieren Sie in der zu löschenden Zeile "Selektieren".
   Wiederholen Sie den Vorgang für alle Gruppen, die Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Löschen". Die Einträge werden gelöscht.

5.4.9.4 v3-Benutzer

Benutzerspezifische Sicherheitseinstellungen

Auf der WBM-Seite können Sie SNMPv3-Benutzer neu anlegen, ändern oder löschen. Das benutzerbasierte Sicherheitsmodell arbeitet mit dem Konzept des Benutzernamens, d. h. jedes Telegramm wird mit einer Benutzerkennung versehen. Diesen Benutzernamen und die betreffenden Sicherheitseinstellungen überprüfen sowohl der Absender wie auch der Empfänger.



SNMPv3-Benutzer - erster Teil der Tabelle

SNMPv3-Benutzer - zweiter Teil der Tabelle

Beschreibung

Die Seite enthält folgende Felder:

- **Benutzername**
  Tragen Sie einen frei wählbaren Benutzernamen ein. Nach der Datenübernahme können Sie den Namen nicht mehr ändern.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Benutzername**
  Zeigt die angelegten Benutzer an.
- **Gruppenname**
  Wählen Sie die Gruppe aus, die dem Benutzer zugeordnet wird.
- **Authentifizierungsprotokoll**
  Legen Sie das Authentifizierungsprotokoll fest, für das ein Passwort hinterlegt werden soll. Folgende Einstellungen gibt es:
  - Keine
  - MD5
  - SHA
- **Verschlüsselungsprotokoll**
  Legen Sie fest, ob ein Passwort zur Verschlüsselung mit dem DES-Algorithmus hinterlegt werden soll. Nur aktivierbar, wenn auch ein Authentifizierungsprotokoll ausgewählt wurde.
- **Authentifizierungspasswort**
  Geben Sie in das erste Eingabefeld das Authentifizierungspasswort ein. Das Passwort muss mindestens 1 Zeichen lang sein, die maximale Länge beträgt 32 Zeichen.

  Hinweis

  Länge des Passworts

  Als wichtige Maßnahme zur Erhöhung der Sicherheit empfehlen wir, dass das Passwort mindestens 6 Zeichen lang ist und Sonderzeichen, Groß-/Kleinschreibung sowie Zahlen enthält.
- **Authentifizierungspasswort bestätigen**
  Bestätigen Sie das Passwort durch die Wiederholung der Eingabe.
- **Verschlüsselungspasswort**
  Geben Sie Ihr Verschlüsselungspasswort ein. Das Passwort muss mindestens 1 Zeichen lang sein, die maximale Länge beträgt 32 Zeichen.

  Hinweis

  Länge des Passworts

  Als wichtige Maßnahme zur Erhöhung der Sicherheit empfehlen wir, dass das Passwort mindestens 6 Zeichen lang ist und Sonderzeichen, Groß-/Kleinschreibung sowie Zahlen enthält.

- **Verschlüsselungspasswort bestätigen**
  Bestätigen Sie das Verschlüsselungspasswort durch die Wiederholung der Eingabe.
- **Persistenz**
  Zeigt an, ob der Benutzer einer SNMPv3-Gruppe zugeordnet ist. Wenn der Benutzer keiner SNMPv3-Gruppe zugeordnet ist, wird kein automatisches Speichern ausgelöst und der konfigurierte Benutzer ist nach einem Neustart des Geräts gelöscht.
  - Ja
    Der Benutzer ist einer SNMPv3-Gruppe zugeordnet.
  - Nein
    Der Benutzer ist keiner SNMPv3-Gruppe zugeordnet.

Vorgehensweise

Neuen Benutzer anlegen

1. Geben Sie im Eingabefeld "Benutzername" den Namen des neuen Benutzers ein.
2. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.
3. Wählen Sie bei "Gruppenname" die Gruppe aus, der der neue Benutzer angehören soll. Wenn die Gruppe noch nicht angelegt ist, wechseln Sie auf die Seite "v3-Gruppen" und legen Sie die Einstellungen für diese Gruppe fest.
4. Wenn für die ausgewählte Gruppe eine Authentifizierung notwendig ist, wählen Sie bei "Authentifizierungsprotokoll" den Authentifizierungsalgorithmus.
   Tragen Sie in die entsprechenden Eingabefelder das Authentifizierungspasswort sowie dessen Bestätigung ein.
5. Wenn für die Gruppe eine Verschlüsselung festgelegt wurde, wählen Sie bei "Verschlüsselungsprotokoll" den Algorithmus aus. Tragen Sie in die entsprechenden Eingabefelder das Verschlüsselungspasswort sowie dessen Bestätigung ein.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Benutzer löschen

1. Aktivieren Sie in der zu löschenden Zeile "Selektieren".
   Wiederholen Sie den Vorgang für alle Benutzer, die Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Löschen". Der Eintrag wird gelöscht.

5.4.10 Systemzeit

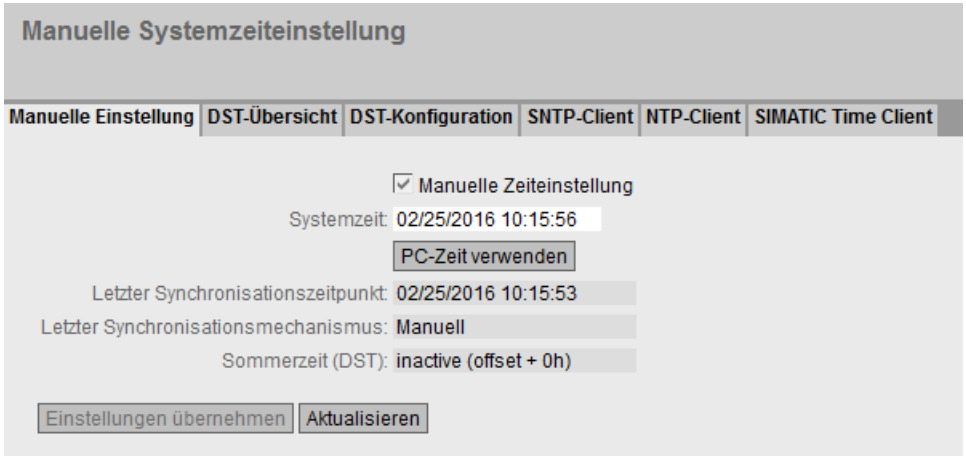
Um die Systemzeit des Geräts einzustellen, gibt es unterschiedliche Methoden. Es kann immer nur eine Methode aktiv sein.

Wenn eine Methode aktiviert wird, dann wird automatisch die bisher aktivierte Methode deaktiviert.

5.4.10.1 Manuelle Einstellung

Manuelle Einstellung der Systemzeit

Auf dieser Seite stellen Sie selbst das Datum und die Uhrzeit des Systems ein. Damit diese Einstellung verwendet wird, müssen Sie "Manuelle Zeiteinstellung" aktivieren.



Beschreibung

Die Seite enthält folgende Felder:

- **Manuelle Zeiteinstellung**
  Aktivieren Sie die manuelle Zeiteinstellung. Wenn Sie die Option aktivieren, wird das Eingabefeld "Systemzeit" editierbar.
- **Systemzeit**
  Geben Sie Datum und Uhrzeit im Format "MM/DD/YYYY HH:MM:SS" ein.
  Nach einem Neustart beginnt die Uhrzeit mit 01/01/2000 00:00:00.
- **PC-Zeit verwenden**
  Klicken Sie auf die Schaltfläche, um die Zeiteinstellung des PCs zu übernehmen.
- **Letzter Synchronisationszeitpunkt**
  Zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat. Wenn keine Uhrzeitsynchronisation möglich war, enthält das Feld die Angabe "Date/time not set".

- **Letzter Synchronisationsmechanismus**
  Zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde.
  - Nicht eingestellt
    Die Zeit wurde nicht eingestellt.
  - Manuell
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm
- **Sommerzeit (DST)**
  Zeigt an, ob die Umstellung der Sommerzeit aktiv ist.
  - active (offset +1 h)
    Die Systemzeit wurde auf Sommerzeit umgestellt, d. h. es wird eine Stunde hinzugezählt. Die aktuelle Systemzeit sehen Sie oben rechts im Auswahlbereich des WBM.
    In dem Feld "Systemzeit" wird die aktuelle Zeit inklusive der Sommerzeit angezeigt.
  - inactive (offset +0 h)
    Die aktuelle Systemzeit wird nicht verändert.

Vorgehensweise

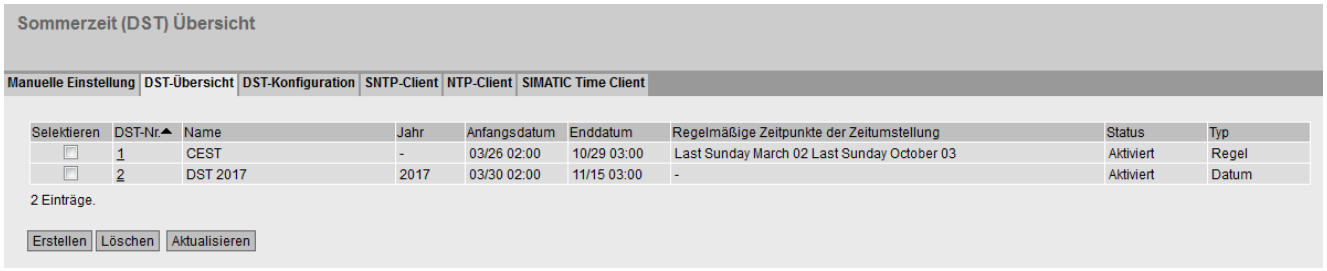
1. Aktivieren Sie die Option "Manuelle Zeiteinstellung".
2. Geben Sie im Eingabefeld "Systemzeit" Datum und Uhrzeit im Format " MM/DD/YYYY HH:MM:SS" ein.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
   Datum und Uhrzeit werden übernommen und im Feld "Letzter Synchronisationsmechanismus" wird "Manuell" eingetragen.

5.4.10.2 DST-Übersicht

Auf dieser Seite können Sie neue Einträge für die Umstellung der Sommerzeit anlegen.

Die Tabelle gibt Ihnen einen Überblick über die vorhanden Einträge.

Einstellungen



- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **DST-Nr.**
  Zeigt die Nummer des Eintrags an.
  Wenn Sie einen neuen Eintrag anlegen, wird eine neue Zeile mit einer eindeutigen Nummer angelegt.
- **Name**
  Zeigt den Namen des Eintrags an.
- **Jahr**
  Zeigt das Jahr an, für das der Eintrag angelegt wurde.
- **Anfangsdatum**
  Zeigt Monat, Tag und Uhrzeit für den Start der Sommerzeit an.
- **Enddatum**
  Zeigt Monat, Tag und Uhrzeit für das Ende der Sommerzeit an.
- **Regelmäßige Zeitpunkte der Zeitumstellung**
  Bei einem Eintrag des Typs "Regel" wird die Zeitspanne angezeigt, bestehend aus Woche, Tag, Monat und Uhrzeit, in der die Sommerzeit aktiv ist.
  Bei einem Eintrag des Typs "Datum" wird ein "-" angezeigt.
- **Status**
  Zeigt der Status des Eintrags an:
  - Aktiviert
    Der Eintrag wurde korrekt angelegt.
  - Ungültig
    Der Eintrag wurde neu angelegt und Anfangs- und Enddatum sind identisch.
- **Typ**
  Zeigt an, wie die Umstellung der Sommerzeit erfolgt:
  - Datum
    Es ist ein festes Datum für die Umstellung der Sommerzeit eingetragen.
  - Regel
    Es ist eine Regel für die Umstellung der Sommerzeit definiert.

Vorgehensweise

Eintrag anlegen

1. Klicken Sie auf die Schaltfläche "Erstellen".
   In der Tabelle wird ein neuer Eintrag angelegt.
2. Klicken Sie in der Spalte "DST-Nr." auf den gewünschten Eintrag.
   Sie wechseln auf die Seite "DST-Konfiguration".
3. Wählen Sie in der Klappliste "Typ" den gewünschten Typ aus.
   Abhängig von dem gewählten Typ stehen Ihnen verschiedene Einstellungen zur Verfügung.
4. Geben Sie im Feld "Name" einen Namen ein.
5. Wenn Sie den Typ "Datum" ausgewählt haben, füllen Sie folgende Felder aus:
   - Jahr
   - Tag (für Anfangs- und Enddatum)
   - Stunde (für Anfangs- und Enddatum)
   - Monat (für Anfangs- und Enddatum)
6. Wenn Sie den Typ "Regel" ausgewählt haben, füllen Sie folgende Felder aus:
   - Stunde (für Anfangs- und Enddatum)
   - Monat (für Anfangs- und Enddatum)
   - Woche (für Anfangs- und Enddatum)
   - Tag (für Anfangs- und Enddatum)
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Eintrag löschen

1. Aktivieren Sie in der zu löschenden Zeile "Selektieren".
2. Klicken Sie auf die Schaltfläche "Löschen". Der Eintrag wird gelöscht.

5.4.10.3 DST-Konfiguration

Auf dieser Seite können Sie die Einträge für die Umstellung der Sommerzeit konfigurieren. Durch die Umstellung auf Sommer- bzw. Winterzeit ist die Systemzeit für die lokale Zeitzone korrekt eingestellt.

Sie können eine Regel für die Umstellung der Sommerzeit definieren oder ein festes Datum angeben.

Einstellungen

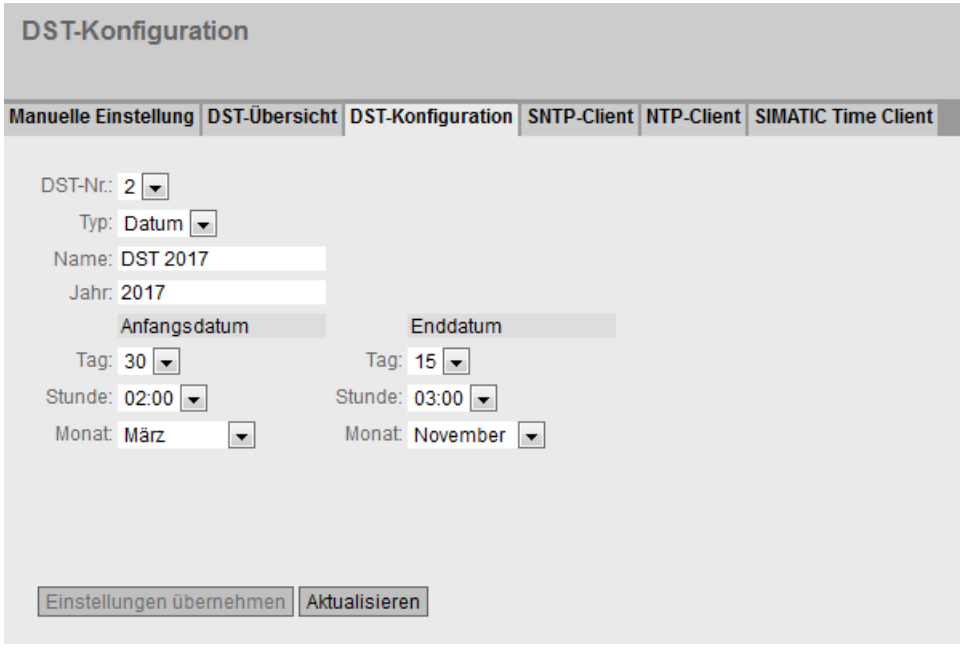
Hinweis

Der Inhalt dieser Seite ist abhängig davon, was Sie im Feld "Typ" auswählen.

Die Felder "DST-Nr.", "Typ" und "Name" werden immer angezeigt.

- **DST-Nr.**
  Wählen Sie die Nummer des Eintrags aus.
- **Typ**
  Wählen Sie aus, wie die Umstellung der Sommerzeit erfolgen soll:
  - Datum
    Sie können ein festes Datum für die Umstellung der Sommerzeit angeben.
    Diese Einstellung eignet sich für Regionen, in denen die Umstellung der Sommerzeit keiner Regel folgt.
  - Regel
    Sie können eine Regel für die Umstellung der Sommerzeit definieren.
    Diese Einstellung eignet sich für Regionen, in denen die Sommerzeit immer an einem bestimmten Wochentag beginnt bzw. endet.
- **Name**
  Geben Sie einen Namen für den Eintrag an.
  Der Name kann maximal 16 Zeichen lang sein.

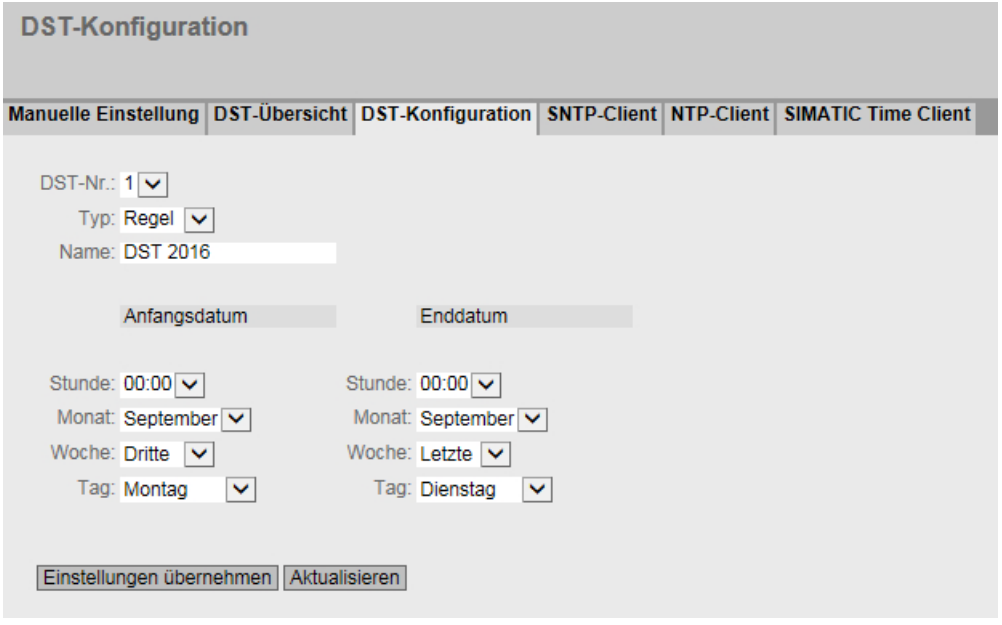
Einstellungen bei der Auswahl "Datum"



Sie können ein festes Datum für den Beginn und das Ende der Sommerzeit angeben.

- **Jahr**
  Geben Sie das Jahr für die Umstellung der Sommerzeit an.
- **Anfangsdatum**
  Geben Sie folgende Werte für den Beginn der Sommerzeit an:
  - Tag
    Geben Sie den Tag an.
  - Stunde
    Geben Sie die Stunde an.
  - Monat
    Geben Sie den Monat an.
- **Enddatum**
  Geben Sie folgende Werte für das Ende der Sommerzeit an:
  - Tag
    Geben Sie den Tag an.
  - Stunde
    Geben Sie die Stunde an.
  - Monat
    Geben Sie den Monat an.

Einstellungen bei der Auswahl "Regel"



Sie können eine Regel für die Umstellung der Sommerzeit erstellen.

- **Anfangsdatum**
  Geben Sie folgende Werte für den Beginn der Sommerzeit an:
  - Stunde
    Geben Sie die Stunde an.
  - Monat
    Geben Sie den Monat an.
  - Woche
    Geben Sie die Woche an.
    Sie können die erste bis fünfte oder die letzte Woche des Monats auswählen.
  - Tag
    Geben Sie den Wochentag an.
- **Enddatum**
  Geben Sie folgende Werte für das Ende der Sommerzeit an:
  - Stunde
    Geben Sie die Stunde an.
  - Monat
    Geben Sie den Monat an.
  - Woche
    Geben Sie die Woche an.
    Sie können die erste bis fünfte oder die letzte Woche des Monats auswählen.
  - Tag
    Geben Sie den Wochentag an.

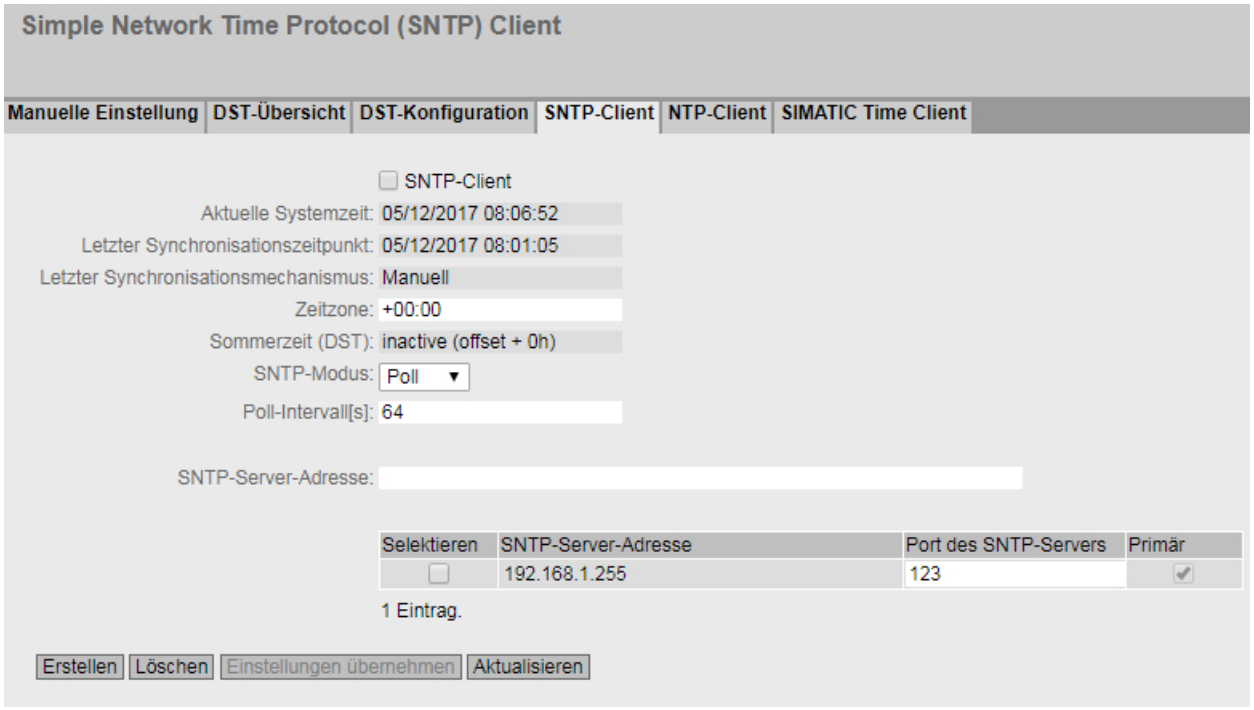
5.4.10.4 SNTP-Client

Uhrzeitsynchronisation im Netzwerk

Das SNTP (Simple Network Time Protocol) dient zur Zeitsynchronisation im Netzwerk. Die entsprechenden Telegramme werden von einem SNTP-Server im Netz versendet.

Hinweis

Um Zeitsprünge zu vermeiden, stellen Sie sicher, dass sich nur ein Zeitserver im Netz befindet.



Beschreibung

Die Seite enthält folgende Felder:

- **SNTP-Client**
  Aktivieren oder deaktivieren Sie die automatische Zeitsynchronisation über SNTP.
- **Aktuelle Systemzeit**
  Zeigt das aktuelle Datum und die aktuelle Normalzeit an, die vom Server empfangen wurden. Wenn Sie eine Zeitzone angeben, wird die Zeitangabe entsprechend angepasst.
- **Letzter Synchronisationszeitpunkt**
  Zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.
- **Letzter Synchronisationsmechanismus**
  Zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde. Folgende Arten gibt es:
  - Nicht eingestellt
    Die Zeit wurde nicht eingestellt.
  - Manuell
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm

- **Zeitzone**
  Geben Sie in diesem Feld Ihre verwendete Zeitzone im Format "+/- HH:MM" an. Die Zeitzone bezieht sich auf UTC Standard-Weltzeit.
  Die Zeitangabe im Feld "Aktuelle Systemzeit" wird entsprechend angepasst.
- **Sommerzeit (DST)**
  Zeigt an, ob die Umstellung der Sommerzeit aktiv ist.
  - active (offset +1 h)
    Die Systemzeit wurde auf Sommerzeit umgestellt, d. h. es wird eine Stunde hinzugezählt. Die aktuelle Systemzeit sehen Sie oben rechts im Auswahlbereich des WBM.
    In dem Feld "Aktuelle Systemzeit" wird weiterhin die Normalzeit inkl. Zeitzone angezeigt.
  - inactive (offset +0 h)
    Die aktuelle Systemzeit wird nicht verändert.
- **SNTP-Modus**
  Wählen Sie aus der Klappliste die Synchronisationsart aus. Folgende Synchronisierungsarten sind möglich:
  - Listen
    Bei diesem Modus ist das Gerät passiv und empfängt SNTP-Telegramme, die die Uhrzeit liefern. Einstellungen in den Eingabefeldern "SNTP-Server-Adresse" und "Port des SNTP-Servers" haben in diesem Modus keine Wirkung.
  - Poll
    Wenn Sie diesen Modus wählen, wird das Eingabefeld "Poll-Intervall[s]" zur weiteren Konfiguration eingeblendet. In diesem Modus werden die Einstellungen in den Eingabefeldern "SNTP-Server-Adresse" und "Port des SNTP-Servers" berücksichtigt. Bei dieser Synchronisationsart ist das Gerät aktiv und sendet eine Zeitabfrage an den SNTP-Server.
- **SNTP-Server-Adresse**
  Geben Sie die IPv4-Adresse des SNTP-Servers ein.
- **Port des SNTP-Servers**
  Geben Sie den Port des SNTP-Servers ein.
  Folgende Ports sind möglich:
  - 123 (Standard-Port)
  - 1025 bis 36564
- **Poll-Intervall[s]**
  Geben Sie den Zeitabstand zwischen zwei Zeitanfragen ein. In diesem Feld geben Sie das Abfrageintervall in Sekunden an. Mögliche Werte sind 16 bis 16284 Sekunden.

Vorgehensweise

1. Klicken Sie in das Optionskästchen "SNTP-Client", um die automatische Zeiteinstellung zu aktivieren.
2. Geben Sie in das Eingabefeld "Zeitzone" die lokale Zeitdifferenz zur Weltzeit (UTC) ein. Das Eingabeformat ist "+/-HH:MM" (z.B. +02:00 für MESZ, die mitteleuropäische Sommerzeit), da der SNTP-Server immer die UTC-Zeit sendet. Diese Zeit wird dann mithilfe der Angabe für die Zeitzone in die lokale Zeit umgerechnet. Im Gerät erfolgt keine Umstellung auf Sommerzeit oder Winterzeit. Dies müssen Sie ebenfalls bei der Eingabe in das Eingabefeld "Zeitzone" berücksichtigen.
3. Wählen Sie aus der Klappliste "SNTP-Modus" aus folgenden Optionen aus:
   - Listen
     Für diese Betriebsart müssen Sie Folgendes konfigurieren:
     - Zeitdifferenz zu der vom Server gesendeten Zeit (Schritt 2)
     - Schließen Sie die Konfiguration mit Schritt 7 ab.
   - Poll
     Klicken Sie auf die Schaltfläche "Einstellungen übernehmen". Es werden weitere Felder für die Konfiguration des SNTP-Modus "Poll" angezeigt.
     Für diese Betriebsart müssen Sie Folgendes konfigurieren:
     - Zeitdifferenz zu der vom Server gesendeten Zeit (Schritt 2)
     - Zeit-Server (Schritt 4)
     - Port (Schritt 5)
     - Abfrageintervall (Schritt 6)
     - Schließen Sie die Konfiguration mit Schritt 7 ab.
4. Geben Sie im Eingabefeld "SNTP-Server-Adresse" die IPv4-Adresse des SNTP-Servers ein, dessen Telegramme für die Synchronisation der Uhrzeit verwendet werden sollen.
5. Geben Sie im Eingabefeld "Port des SNTP-Servers" den Port ein, über den der SNTP-Server verfügbar ist. Der Port kann nur geändert werden, wenn die IPv4-Adresse des SNTP-Servers eingetragen ist.
6. Geben Sie in das Eingabefeld "Poll-Intervall[s]" die Zeitspanne in Sekunden ein, nach der eine neue Zeitanfrage beim Zeit-Server gestartet werden soll.
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen", um Ihre Änderungen in das Gerät zu übertragen.

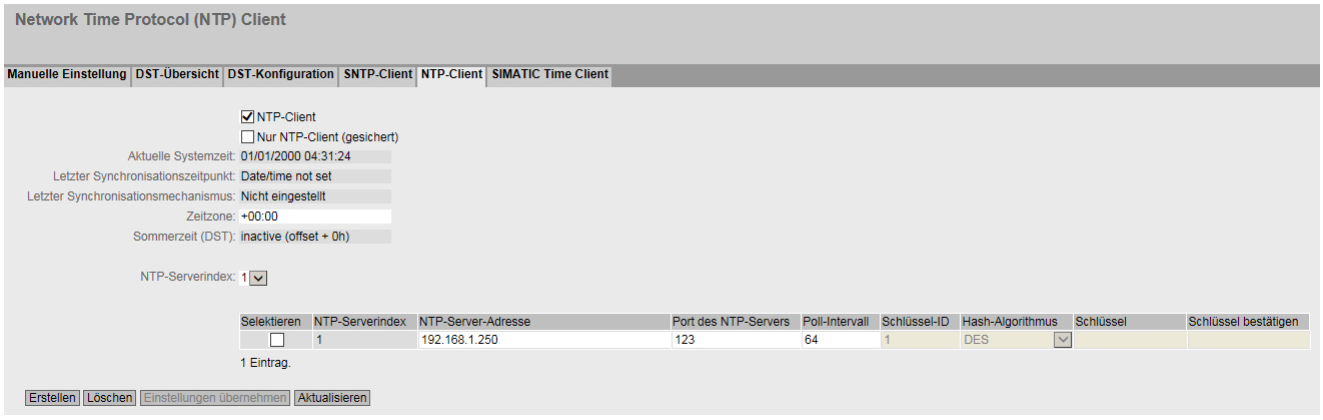
5.4.10.5 NTP-Client

Automatische Zeiteinstellung über NTP

Wenn die Uhrzeitsynchronisation über NTP erfolgen soll, können Sie hier die entsprechenden Einstellungen vornehmen.

Hinweis

Um Zeitsprünge zu vermeiden, stellen Sie sicher, dass sich nur ein Zeitserver im Netz befindet.



Beschreibung

Die Seite enthält folgende Felder:

- **NTP-Client**
  Wenn aktiviert, erhält das Gerät die Systemzeit von einem NTP-Server.
- **Nur NTP-Client (gesichert)**
  Wenn aktiviert, erhält das Gerät die Systemzeit von einem gesicherten NTP-Server. Die Einstellung gilt für alle Servereinträge.
  Um den gesicherten NTP-Client zu aktivieren, konfigurieren Sie die Parameter für die Authentifizierung (Schlüssel-ID, Hash-Algorithmus, Schlüssel).
- **Aktuelle Systemzeit**
  Zeigt das aktuelle Datum und die aktuelle Normalzeit an, die vom IE-Switch empfangen wurden. Wenn Sie eine Zeitzone angeben, wird die Zeitangabe entsprechend angepasst.
- **Letzter Synchronisationszeitpunkt**
  Zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.
- **Letzter Synchronisationsmechanismus**
  Zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde. Folgende Arten gibt es:
  - Nicht eingestellt
    Die Zeit wurde nicht eingestellt.
  - Manuell
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm
- **Zeitzone**
  Geben Sie in diesem Feld Ihre verwendete Zeitzone im Format "+/- HH:MM" an. Die Zeitzone bezieht sich auf UTC Standard-Weltzeit.
  Die Zeitangabe im Feld "Aktuelle Systemzeit" wird entsprechend angepasst.

- **Sommerzeit (DST)**
  Zeigt an, ob die Umstellung der Sommerzeit aktiv ist.
  - active (offset +1 h)
    Die Systemzeit wurde auf Sommerzeit umgestellt, d. h. es wird eine Stunde hinzugezählt. Die aktuelle Systemzeit sehen Sie oben rechts im Auswahlbereich des WBM.
    In dem Feld "Aktuelle Systemzeit" wird weiterhin die Normalzeit inkl. Zeitzone angezeigt.
  - inactive (offset +0 h)
    Die aktuelle Systemzeit wird nicht verändert.
- **NTP-Serverindex**
  Wählen Sie den Index des NTP-Servers aus. Sie können bis zu vier NTP-Server bzw. SecureNTP-Server konfigurieren. Die NTP-Server werden in der Reihenfolge des NTP-Serverindex angefragt. Die Zeit des zuerst gefundenen Servers wird übernommen. Werden Zeit-Telegramme eines NTP-Servers mit einem kleineren Stratum-Wert empfangen, wird diese Zeit übernommen. Die Umschaltung auf die Zeit mit dem kleineren Stratum dauert ca. 30 Minuten.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **NTP-Serverindex**
  Der Index des NTP-Servers.
- **NTP-Server-Adresse**
  Geben Sie die IPv4-Adresse des NTP-Servers an.
- **Port des NTP-Servers**
  Geben Sie den Port des NTP-Servers an.
  Folgende Ports sind möglich:
  - 123 (Standard-Port)
  - 1025 bis 36564
- **Poll-Intervall[s]**
  Legen Sie den Zeitabstand zwischen zwei Uhrzeitanfragen fest. Mögliche Werte sind 64 bis 1024 Sekunden.

Die folgenden Felder sind nur für einen gesicherten NTP-Client von Bedeutung. Wenn das Optionskästchen "Nur NTP-Client (gesichert)" nicht aktiviert ist, sind diese Felder gegraut:

- **Schlüssel-ID**
  Geben Sie die ID des Authentifizierungsschlüssels ein.
- **Hash-Algorithmus**
  Legen Sie das Format für den Authentifizierungsschlüssel fest.
- **Schlüssel**
  Geben Sie den Authentifizierungsschlüssel ein.
- **Schlüssel bestätigen**
  Geben Sie nochmals den Authentifizierungsschlüssel ein, um ihn zu bestätigen.

Vorgehensweise

Uhrzeitsynchronisation über NTP-Server

1. Klicken Sie in das Optionskästchen "NTP-Client", um die automatische Zeiteinstellung über NTP zu aktivieren.
2. Geben Sie in das Eingabefeld "Zeitzone" die lokale Zeitdifferenz zur Weltzeit (UTC) ein. Das Eingabeformat ist "+/-HH:MM", da der NTP-Server immer die UTC-Zeit sendet, z. B. +02:00 für MESZ, die mitteleuropäische Sommerzeit. Diese Zeit wird mithilfe der Angabe für die Zeitzone in die lokale Zeit umgerechnet.
3. Wählen Sie den "NTP-Serverindex" aus.
4. Klicken Sie auf die Schaltfläche "Erstellen".
   In der Tabelle wird eine Zeile für den NTP-Server angelegt.
5. Geben Sie bei "NTP-Server-Adresse" die Adresse des NTP-Servers ein, dessen Telegramme für die Synchronisation der Uhrzeit verwendet wird.
6. Geben Sie bei "Port des NTP-Servers" den Port ein, über den der NTP-Server verfügbar ist. Der Port ist nur änderbar, wenn Adresse des NTP-Servers eingetragen ist.
7. Geben Sie in der Spalte "Poll-Intervall" die Zeitspanne in Sekunden ein, nach der eine neue Uhrzeitanfrage beim Zeitserver gestartet wird.
8. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Uhrzeitsynchronisation über einen gesicherten NTP-Server

Um die Uhrzeit über einen gesicherten NTP-Server zu synchronisieren, sind folgende zusätzliche Schritte notwendig:

1. Klicken Sie in das Optionskästchen "Nur NTP-Client (gesichert)", um die automatische Zeiteinstellung über gesichertes NTP zu aktivieren.
2. Konfigurieren Sie die Authentifizierung.
   - Geben Sie bei "Schlüssel-ID" die ID des Authentifizierungsschlüssels ein.
   - Wählen Sie bei "Hash-Algorithmus" das entsprechende Format aus.
   - Geben Sie bei "Schlüssel" den Authentifizierungsschlüssel ein.

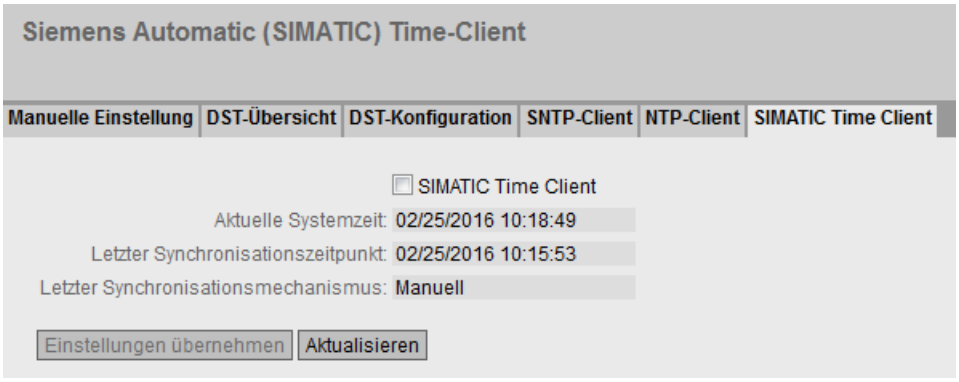
   Mit diesen Eingaben authentifiziert sich der NTP-Client am gesicherten NTP-Server. Auf dem gesicherten NTP-Server müssen diese Einträge vorhanden sein.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.4.10.6 SIMATIC Time Client

Zeiteinstellung über SIMATIC Time Client

Hinweis

Um Zeitsprünge zu vermeiden, stellen Sie sicher, dass sich nur ein Zeitserver im Netz befindet.



Beschreibung

Die Seite enthält folgende Felder:

- **SIMATIC Time Client**
  Markieren Sie dieses Optionskästchen, um das Gerät als SIMATIC Time Client zu aktivieren.
- **Aktuelle Systemzeit**
  Zeigt die aktuelle Systemzeit an.
- **Letzter Synchronisationszeitpunkt**
  Zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.
- **Letzter Synchronisationsmechanismus**
  Zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde. Folgende Arten gibt es:
  - Nicht eingestellt
    Die Zeit wurde nicht eingestellt.
  - Manuell
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm

Vorgehensweise

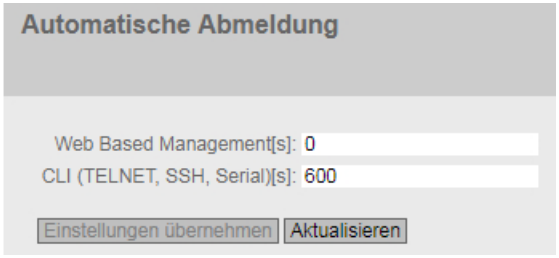
1. Klicken Sie in das Optionskästchen "SIMATIC Time Client", um den SIMATIC Time Client zu aktivieren.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.4.11 Automatische Abmeldung

Einstellung der automatischen Abmeldung

Stellen Sie auf dieser Seite die Zeitintervalle ein, nach denen bei Inaktivität des Benutzers automatisch eine Abmeldung vom WBM oder CLI erfolgt.

Wenn Sie automatisch abgemeldet wurden, dann müssen Sie sich wieder neu anmelden.



Konfiguration

1. Tragen Sie in das Eingabefeld "Web Based Management[s]" einen Wert von 60-3600 Sekunden ein. Wenn Sie den Wert 0 eintragen, ist die automatische Abmeldung deaktiviert.
2. Tragen Sie in das Eingabefeld "CLI (TELNET, SSH, Serial)[s]" einen Wert von 60-600 Sekunden ein. Wenn Sie den Wert 0 eintragen, ist die automatische Abmeldung deaktiviert.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.4.12 Konfiguration des SELECT/SET-Tasters

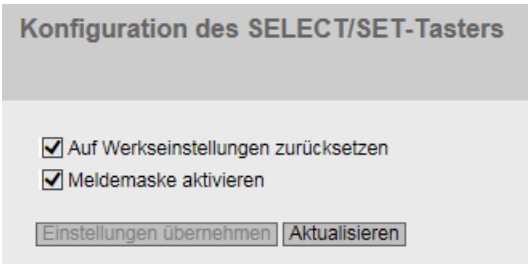
Verfügbarkeit der Taster

Abhängig von Ihrem IE-Switch stehen Ihnen unterschiedliche Taster und Funktionen zur Verfügung, siehe Kapitel "Systemfunktionen und Hardware-Ausstattung (Seite 15)".

Funktionalität der Taster

Eine detaillierte Beschreibung der Funktion, die über den Taster bedient werden kann, finden Sie in der Betriebsanleitung des Geräts.

Auf dieser Seite kann die Funktionalität des Tasters ein- bzw. ausgeschaltet werden.



Beschreibung der angezeigten Felder

Folgende Funktionalitäten sind möglich:

- **Auf Werkseinstellungen zurücksetzen**
  Wenn Sie das Optionskästchen aktivieren, können Sie über den Taster die Funktion "Auf Werkseinstellungen zurücksetzen" ausführen.

  ⚠ VORSICHT

  Tasterfunktion "Auf Werkseinstellungen zurücksetzen" beim Hochlauf aktiv

  Wenn Sie diese Funktion in ihrer Projektierung deaktiviert haben, ist die Deaktivierung nur im laufenden Betrieb gültig. Bei einem Hochlauf, z.B. nach "Stromaus", ist die Funktion bis zum Laden der Projektierung aktiv und das Gerät kann so auch unbeabsichtigt auf die Werkseinstellungen zurückgesetzt werden. Dies kann zu unerwünschten Störungen des Netzwerkbetriebs führen, da das Gerät dann neu projektiert werden muss. Ein gesteckter PLUG wird dabei ebenfalls gelöscht und in den Auslieferungszustand versetzt.

- **Meldemaske aktivieren**
  Wenn Sie das Optionskästchen aktivieren, können Sie über den Taster die Meldemaske definieren.

Vorgehensweise zur Konfiguration

1. Um die Funktionalität zu nutzen, aktivieren Sie das entsprechende Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.4.13 Syslog-Client

Syslog nach RFC 3164 wird für die Übermittlung von kurzen, unverschlüsselten Textmeldungen per UDP im IP-Netz verwendet. Dazu wird ein Syslog-Server benötigt.

Voraussetzungen für das Versenden von Log-Einträgen

- Die Syslog-Funktion ist im Gerät aktiviert.
- Die Syslog-Funktion für das jeweilige Ereignis ist aktiviert.

- In Ihrem Netz befindet sich ein Syslog-Server, der die Log-Einträge entgegen nimmt. Da es sich um eine UDP-Verbindung handelt, gibt es keine Rückmeldung an den Absender.
- Die IP-Adresse des Syslog-Servers ist im Gerät eingetragen.

Beschreibung

Die Seite enthält folgende Felder:

- **Syslog-Client**
  Aktivieren oder deaktivieren Sie die Syslog-Funktion.
- **Adresse des Syslog-Servers**
  Geben Sie die IP-Adresse des Syslog-Servers an.

Die Tabelle enthält folgende Spalten

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Adresse des Syslog-Servers**
  Zeigt die IP-Adresse des Syslog-Servers an.
- **Server-Port**
  Geben Sie den verwendeten Port des Syslog-Servers ein.

Vorgehensweise

Funktion aktivieren

1. Aktivieren Sie das Optionskästchen "Syslog-Client".
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Neuen Eintrag anlegen

1. Geben Sie in das Eingabefeld "Adresse des Syslog-Servers" die IP-Adresse des Syslog-Servers ein, auf dem die Log-Einträge gespeichert werden sollen.
2. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird eine neue Zeile eingefügt.

3. Geben Sie in das Eingabefeld "Server-Port" die Nummer des UDP-Ports des Servers ein.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Hinweis

Die Standardeinstellung des Server-Ports ist Port 514.

Eintrag ändern

1. Löschen Sie den Eintrag.
2. Legen Sie einen neuen Eintrag an.

Eintrag löschen

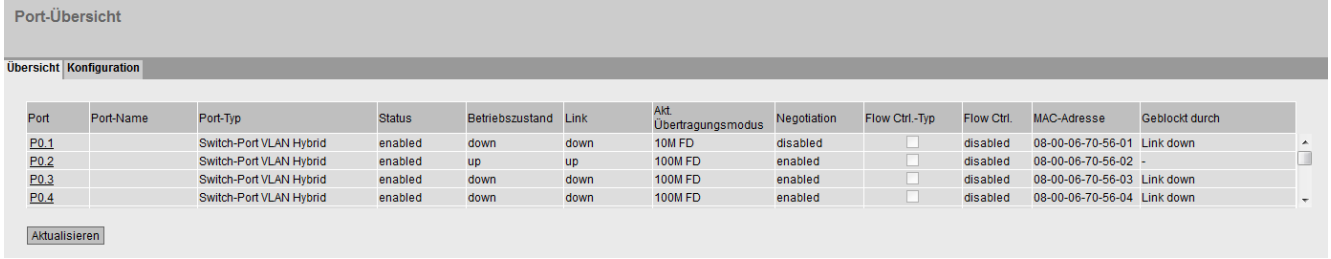
1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Löschen". Alle markierten Einträge werden gelöscht und die Anzeige wird aktualisiert.

5.4.14 Ports

5.4.14.1 Übersicht

Portkonfiguration im Überblick

Die Seite zeigt für alle Ports des Geräts die Konfiguration für den Datentransfer an. Sie können auf dieser Seite keine Konfigurationen vornehmen.



Beschreibung der angezeigten Felder

Die Tabelle gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an. Wenn Sie auf den Port klicken, wird die entsprechende Konfigurationsseite geöffnet. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Port-Name**
  Zeigt den Namen des Ports an.

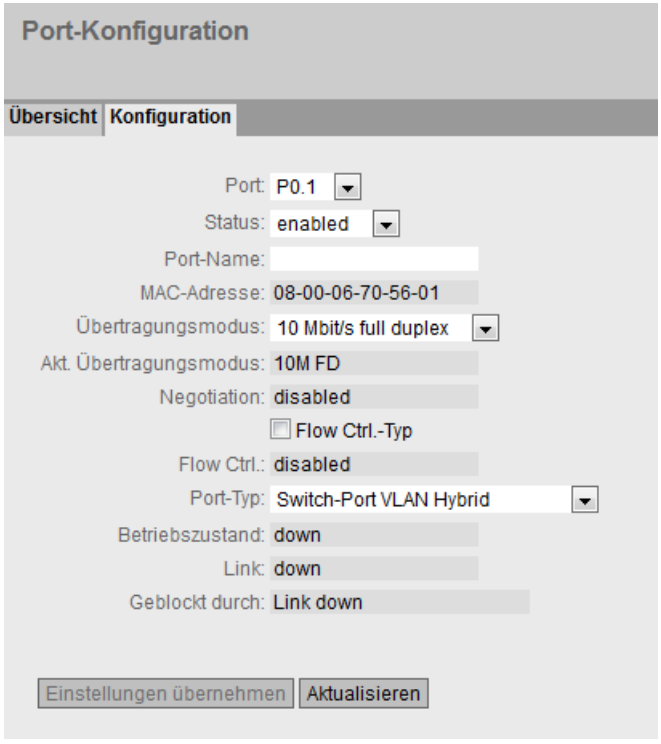
- **Port-Typ**
  Zeigt den Typ des Ports an. Folgende Typen sind möglich:
  - Switch-Port VLAN Hybrid
  - Switch-Port VLAN Trunk
  - Switch-Port PVLAN Host
  - Switch-Port PVLAN Promiscuous
  - Switch-Port VLAN Access
- **Combo Port Medientyp**
  Diese Spalte enthält nur bei Combo Ports einen Wert.
  Zeigt den Modus des Combo Ports an:
  - auto
  - rj45
  - sfp
- **Status**
  Zeigt an, ob der Port ein- oder ausgeschaltet ist. Datenverkehr ist nur über einen eingeschalteten Port möglich.
- **Betriebszustand**
  Zeigt den aktuellen Betriebszustand an. Der Betriebszustand ist vom konfigurierten "Status" und dem "Link" abhängig. Es gibt folgende Möglichkeiten:
  - up
    Sie haben für den Port den Status "enabled" konfiguriert und der Port hat eine gültige Verbindung zum Netzwerk.
  - down
    Sie haben für den Port den Status "disabled" oder "Link down" konfiguriert oder der Port hat keine Verbindung.
  - not present
    Bei modularen Geräten wird dieser Status angezeigt, wenn z. B. kein Medienmodul gesteckt ist.
- **Link**
  Zeigt den Verbindungsstatus zum Netzwerk an. Beim Verbindungsstatus ist Folgendes möglich:
  - up
    Der Port hat eine gültige Verbindung zum Netzwerk, es wird ein "Link Integrity Signal" empfangen.
  - down
    Die Verbindung ist unterbrochen, weil beispielsweise das angeschlossene Gerät ausgeschaltet ist.
- **Akt. Übertragungsmodus**
  Zeigt die Übertragungsparameter des Ports an.
- **Negotiation**
  Zeigt an, ob die automatische Konfiguration aktiviert oder deaktiviert ist.

- **Flow Ctrl. Type**
  Gibt an, ob für den Port die Flusskontrolle aktiviert oder deaktiviert ist.
- **Flow Ctrl.**
  Gibt an, ob bei diesem Port die Flusskontrolle arbeitet.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Ports an.
- **Geblockt durch**
  Zeigt an, warum sich der Port im Zustand "blocked" befindet:
  - -
    Der Port ist nicht geblockt.
  - Ringredundanz
    Der Port gehört zu einem Redundanzmanager. Wenn sich der Redundanzmanager im Status "Passive" befindet, ist einer der Ring-Ports im Zustand "blocking".
  - Spanning Tree
    Der Port hat im Spanning Tree den Status "Discarding". Der Port ist Teil eines Spanning Trees, jedoch liegt er auf einem redundanten Pfad und ist für den Datenverkehr deaktiviert.
  - Loop Detection
    Es wurde ein Loop erkannt und als Reaktion auf einen Loop wurde für den Port der Zustand "disable" konfiguriert.
  - Link Check
    Es wurde eine Störungen bei einer optischen Übertragungsstrecke erkannt und als Reaktion wurde für den Port der Zustand "disable" konfiguriert.
  - Link Aggregation-Mitglied
    Der Port ist Teil einer Link Aggregation und wurde durch LACP deaktiviert.
  - Link Aggregation (LoopD)
    Der Port ist Teil einer Link Aggregation. Es wurde ein Loop erkannt und als Reaktion auf einen Loop wurde für die Link Aggregation der Zustand "disable" konfiguriert.
  - Link Aggregation (STP)
    Der Port ist Teil einer Link Aggregation. Die Link Aggregation wurde durch Spanning Tree in den Status "Discarding" geschaltet.
  - Admin down
    Für den Port ist der Status "disabled" konfiguriert, siehe "System > Ports > Konfiguration".
  - Link down
    Für den Port ist der Status "enabled" konfiguriert, aber es besteht keine Verbindung, siehe "System > Ports > Konfiguration".
  - Power down
    Für den Port ist der Status "Link down" konfiguriert, siehe "System > Ports > Konfiguration".
  - Standby
    Auf dem Gerät ist die Standby-Redundanz aktiviert. Der Port ist ein Standby-Port mit dem Status "Passive".

5.4.14.2 Konfiguration

Ports konfigurieren

Auf dieser Seite können Sie alle Ports des Geräts konfigurieren.



Beschreibung der angezeigten Felder

Die Tabelle gliedert sich in folgende Zeilen:

- **Port**
  Wählen Sie aus der Klappliste den zu konfigurierenden Port aus. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Status**
  Legen Sie fest, ob der Port ein- oder ausgeschaltet ist.
  - enabled
    Der Port ist eingeschaltet. Datenverkehr ist nur über einen eingeschalteten Port möglich.
  - disabled
    Der Port ist ausgeschaltet, aber die Verbindung besteht noch.
  - link down
    Der Port ist ausgeschaltet und die Verbindung zum Partnergerät ist abgebaut.

  Hinweis

  Reduzierte Stromaufnahme

  Für jeden optischen Port, den Sie auf "link down" setzen, verringert sich die Stromaufnahme des Geräts um 30 mA.
- **Port-Name**
  Tragen Sie hier einen Namen für den Port ein.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Ports an.

- **Übertragungsmodus**
  Wählen Sie aus der Klappliste die Übertragungsgeschwindigkeit und das Übertragungsverfahren des Ports aus.
  Wenn Sie den Modus "Auto negotiation" einstellen, werden diese Parameter automatisch mit dem angeschlossenen Partner-Port ausgehandelt.
  Damit der Port und der Partner-Port miteinander kommunizieren können, müssen die Einstellungen auf beiden Seiten übereinstimmen.

  Hinweis

  Modus "Auto negotiation"

  - Wenn ein Port fest auf Vollduplex eingestellt wird, dann muss der angeschlossene Partner-Port ebenfalls auf Vollduplex eingestellt werden.
  - Wenn ein Port, der im Modus "Auto negotiation" arbeitet, an einen Partner-Port angeschlossen wird, der nicht im Modus "Auto negotiation" arbeitet, dann muss der Partner-Port fest eingestellt sein.
  - Geräte, die kein "Auto negotation" unterstützen, müssen auf 100 MBit/s bzw. 10 MBit/s Halbduplex-Betrieb fest eingestellt werden.

  Hinweis

  "Auto negotiation" und Autocrossover

  - SCALANCE XB-200/SCALANCE XC-200/XR-300WG: Wenn Sie die Funktion "Auto negotiation" ausschalten, wird auch die Funktion "MDI/MDI-X Autocrossover" ausgeschaltet. Verwenden Sie dann ein gekreuztes Kabel.
  - SCALANCE XP-200: Wenn Sie die Funktion "Auto negotiation" ausschalten, bleibt die Funktion "MDI/MDI-X Autocrossover" aktiv.

- **Akt. Übertragungsmodus**
  Zeigt die Übertragungsgeschwindigkeit und das Übertragungsverfahren des Ports an. Die Übertragungsgeschwindigkeit kann 10 Mbit/s, 100 Mbit/s oder 1000 Mbit/s betragen. Als Übertragungsverfahren können Vollduplex (FD) oder Halbduplex (HD) konfiguriert werden.
- **Negotiation**
  Zeigt an, ob die automatische Anschlusskonfiguration zum Partner-Port aktiviert oder deaktiviert ist.
- **Flow Ctrl. Type**
  Aktivieren oder deaktivieren Sie die Funktion Flow Control (Flusskontrolle) für den Port.

  Hinweis

  Um die Funktion Flusskontrolle zu nutzen, aktivieren Sie die Flusskontrolle auf den entsprechenden Eingangs- und Ausgangsports.

  Wenn ein Paket von einem Eingangsport mit aktivierter Flusskontrolle an einen Ausgangsport mit aktivierter Flusskontrolle geleitet wird, wird das Paket bei Überlast nicht verworfen. Wenn die Flusskontrolle nur auf dem Eingangsport aktiviert ist, kann das Paket bei Überlast verworfen werden.

  Hinweis

  Ein-/Ausschalten der Flusskontrolle bei "Auto Negotiation"

  Sie können die Flusskontrolle nur aktivieren oder deaktivieren, wenn die Funktion "Auto Negotiation" ausgeschaltet ist. Sie können "Auto Negotiation" danach wieder aktivieren.

- **Flow Ctrl.**
  Zeigt an, ob bei diesem Port die Flusskontrolle arbeitet.
- **Port-Typ**
  Wählen Sie aus der Klappliste die Art des Ports aus.

  Hinweis

  Private VLAN-Funktionalität und RADIUS-Authentifizierung

  Wenn die VLAN-Zuweisung über RADIUS-Authentifizierung für einen oder mehrere Ports eines VLAN aktiviert ist, sollten Sie dieses VLAN nicht zusätzlich als Private VLAN konfigurieren.

  Die Private VLAN-Funktionalität in Zusammenhang mit der VLAN-Zuweisung über RADIUS-Authentifizierung kann zu einem inkonsistenten Systemzustand führen.

  – Switch-Port VLAN Hybrid
    Der Port sendet getaggte und ungetaggte Telegramme. Er ist nicht automatisch Mitglied eines VLANs.
  – Switch-Port VLAN Trunk
    Der Port sendet nur getaggte Telegramme und ist automatisch Mitglied in allen VLANs.
  – Switch-Port PVLAN Host
    Host-Ports gehören zu einem Secondary PVLAN.
    Schließen Sie an Host-Ports Geräte an, die nur mit bestimmten Geräten des PVLANs kommunizieren sollen.
  – Switch-Port PVLAN Promiscuous
    Promiscuous-Ports gehört zu einem Primary PVLAN.
    Schließen Sie an Promiscuous-Ports Geräte an, die mit allen anderen Geräten des PVLANs kommunizieren sollen.
  – Switch-Port VLAN Access
    Access-Ports gehört zu einem Provider-Switch, der die Funktion Q-in-Q VLAN-Tunnel unterstützt.
    Schließen Sie an Access-Ports ein Customer-Netzwerk an.

- **Combo Port Medientyp**
  Legen Sie den Modus des Combo Ports fest:
  - auto
    Wenn Sie diesen Modus wählen, hat der Stecktransceiver-Port Priorität.
    Sobald ein Stecktransceiver gesteckt wird, wird eine bestehende Verbindung am festen RJ45-Port getrennt. Wenn kein Stecktransceiver gesteckt ist, kann eine Verbindung über den festen RJ45-Port hergestellt werden.
  - rj45
    Wenn Sie diesen Modus wählen, wird der feste RJ45-Port verwendet, unabhängig vom Stecktransceiver-Port.
    Wenn ein Stecktransceiver gesteckt ist, wird er deaktiviert und stromlos geschaltet.
  - sfp
    Wenn Sie diesen Modus wählen, wird der Stecktransceiver-Port verwendet, unabhängig vom festen RJ45-Port.
    Wenn eine RJ45-Verbindung besteht, wird diese getrennt, da der RJ45-Port stromlos geschaltet wird.

  Die Werkseinstellung für die Combo Ports ist der Modus auto.

  Hinweis

  Automatische Anpassung durch PROFINET-Konfiguration

  Beim Aufbau einer PROFINET-Verbindung wird auch der die Einstellung des Combo Port Medientyps automatisch angepasst:
  - Wenn eine Stecktransceiver konfiguriert ist, wird der Combo Port Medientyp auf "sfp" gesetzt.
  - Wenn der feste RJ45-Port konfiguriert ist, wird der Combo Port Medientyp auf "rj45" gesetzt.

  Damit die automatische Anpassung durchgeführt werden kann, muss der Combo Port Medientyp auf "auto" gesetzt sein.

  Konfigurieren Sie den Combo Port Medientyp entsprechend über das WBM oder CLI.

- **Betriebszustand**
  Zeigt den aktuellen Betriebszustand an. Der Betriebszustand ist vom konfigurierten "Status" und dem "Link" abhängig. Es gibt folgende Möglichkeiten:
  - up
    Sie haben für den Port den Status "enabled" konfiguriert und der Port hat eine gültige Verbindung zum Netzwerk.
  - down
    Sie haben für den Port den Status "disabled" oder "Link down" konfiguriert oder der Port hat keine Verbindung.
  - not present
    Bei modularen Geräten wird dieser Status angezeigt, wenn z. B. kein Medienmodul gesteckt ist.

- **Link**
  Zeigt den Verbindungsstatus zum Netzwerk an. Es gibt folgende Möglichkeiten:
  - up
    Der Port hat eine gültige Verbindung zum Netzwerk, es wird ein "Link IntegritySignal" empfangen.
  - down
    Die Verbindung ist unterbrochen, weil z. B. das angeschlossene Gerät ausgeschaltet ist.
- **Geblockt durch**
  Zeigt an, warum sich der Port im Zustand "blocked" befindet:
  - -
    Der Port ist nicht geblockt.
  - Ringredundanz
    Der Port gehört zu einem Redundanzmanager. Wenn sich der Redundanzmanager im Status "Passive" befindet, ist einer der Ring-Ports im Zustand "blocking".
  - Spanning Tree
    Der Port hat im Spanning Tree den Status "Discarding". Der Port ist Teil eines Spanning Trees, jedoch liegt er auf einem redundanten Pfad und ist für den Datenverkehr deaktiviert.
  - Loop Detection
    Es wurde ein Loop erkannt und als Reaktion auf einen Loop wurde für den Port der Zustand "disable" konfiguriert.
  - Link Check
    Es wurde eine Störungen bei einer optischen Übertragungsstrecke erkannt und als Reaktion wurde für den Port der Zustand "disable" konfiguriert.
  - Link Aggregation-Mitglied
    Der Port ist Teil einer Link Aggregation und wurde durch LACP deaktiviert.
  - Link Aggregation (LoopD)
    Der Port ist Teil einer Link Aggregation. Es wurde ein Loop erkannt und als Reaktion auf einen Loop wurde für die Link Aggregation der Zustand "disable" konfiguriert.
  - Link Aggregation (STP)
    Der Port ist Teil einer Link Aggregation. Die Link Aggregation wurde durch Spanning Tree in den Status "Discarding" geschaltet.
  - Admin down
    Für den Port ist der Status "disabled" konfiguriert, siehe "System > Ports > Konfiguration".
  - Link down
    Für den Port ist der Status "enabled" konfiguriert, aber es besteht keine Verbindung, siehe "System > Ports > Konfiguration".
  - Power down
    Für den Port ist der Status "Link down" konfiguriert, siehe "System > Ports > Konfiguration".
  - Standby
    Auf dem Gerät ist die Standby-Redundanz aktiviert. Der Port ist ein Standby-Port mit dem Status "Passive".

Veränderung der Port-Konfiguration

Klicken Sie in das entsprechende Feld, um die Konfiguration zu ändern.

Hinweis

Optische Ports arbeiten immer mit dem Übertragungsverfahren Vollduplex und mit maximaler Übertragungsgeschwindigkeit. Deshalb können Sie bei optischen Ports folgende Einstellungen nicht vornehmen:

- Automatische Konfiguration
- Übertragungsgeschwindigkeit
- Übertragungsverfahren

Hinweis

Das Gerät verhindert oder reduziert bei Überlastung eines Ports durch verschiedene Automatismen die Rückwirkung auf andere Ports und Prioritätsklassen (Class of Service). Dies kann auch bei aktivierter Flusskontrolle dazu führen, dass Telegramme verworfen werden.

Port-Überlastungen treten auf, wenn das Gerät mehr Telegramme empfängt, als es senden kann, z.B. infolge unterschiedlicher Übertragungsgeschwindigkeiten.

Vorgehensweise zur Konfiguration

1. Ändern Sie die Einstellungen entsprechend Ihrer Konfiguration.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.4.15 Fehlerkontrolle

5.4.15.1 Spannungsversorgung

Einstellungen zur Überwachung der Spannungsversorgung

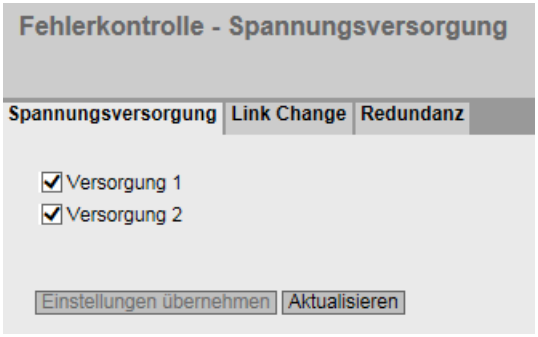
Konfigurieren Sie, ob die Spannungsversorgung durch das Meldesystem überwacht werden soll. Je nach Hardware-Variante gibt es ein oder zwei Spannungsanschlüsse (Versorgung 1 / Versorgung 2). Bei redundanter Spannungsversorgung konfigurieren Sie die Überwachung für jede einzelne Zuleitung getrennt.

Es wird dann ein Fehler durch das Meldesystem signalisiert, wenn an einem überwachten Anschluss (Versorgung 1 oder Versorgung 2) keine oder eine zu geringe Spannung anliegt.

Hinweis

Die zulässigen Betriebsspannungsgrenzen entnehmen Sie der Betriebsanleitung des Geräts.

Ein Fehler führt zum Auslösen des Meldekontakts und zum Aufleuchten der Fehler-LED am Gerät und kann abhängig von der Konfiguration einen Trap, eine E-Mail oder einen Eintrag in der Ereignisprotokoll-Tabelle auslösen.



Vorgehensweise

1. Klicken Sie in das Optionskästchen vor dem entsprechenden Anschlussnamen, den Sie überwachen wollen, um die Überwachungsfunktion ein- oder auszuschalten.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.4.15.2 Link Change

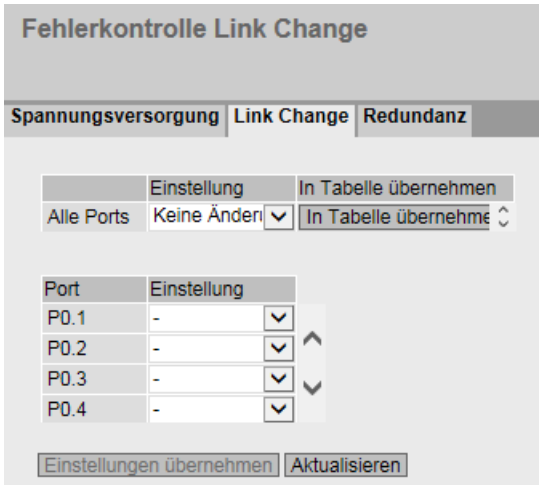
Konfiguration der Fehlerüberwachung von Zustandsänderungen bei Verbindungen

Auf dieser Seite konfigurieren Sie, ob bei einer Zustandsänderung einer Netzwerkverbindung eine Fehlermeldung ausgelöst wird.

Bei aktivierter Verbindungsüberwachung wird ein Fehler signalisiert, wenn:

- an einem Port ein Link vorhanden sein soll und dieser fehlt
- wenn an einem Port kein Link vorhanden sein soll, aber ein Link erkannt wird

Ein Fehler führt zum Auslösen des Meldekontakts und zum Aufleuchten der Fehler-LED am Gerät und kann abhängig von der Konfiguration einen Trap, eine E-Mail oder einen Eintrag in der Ereignisprotokoll-Tabelle auslösen.



Beschreibung der angezeigten Felder

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports gültig sind.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - "-" (Deaktiviert)
  - Up
  - Down
  - Keine Änderung: Einstellung in der Tabelle 2 bleibt unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung aus. Folgende Möglichkeiten haben Sie:
  - Up
    Die Fehlerbehandlung wird beim Übergang in den aktiven Zustand des Ports ausgelöst.
    (Von "Link down" nach "Link up")
  - Down
    Die Fehlerbehandlung wird beim Übergang in den inaktiven Zustand des Ports ausgelöst.
    (Von "Link up" nach "Link down")
  - "-" (Deaktiviert)
    Die Fehlerbehandlung wird nicht ausgelöst.

Vorgehensweise zur Konfiguration

Fehlerüberwachung für einen Port konfigurieren

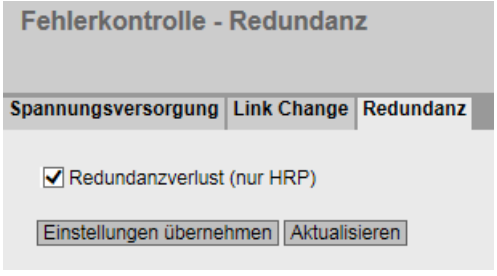
1. Wählen Sie aus der entsprechenden Klappliste die Optionen der Steckplätze/Ports, deren Verbindungsstatus Sie überwachen wollen.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Fehlerüberwachung für alle Ports konfigurieren

1. Wählen Sie in der Klappliste der Spalte "Einstellung" die gewünschte Einstellung aus.
2. Klicken Sie auf die Schaltfläche "In Tabelle übernehmen". Die Einstellung wird für alle Ports der Tabelle 2 übernommen.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.4.15.3 Redundanz

Auf dieser Seite konfigurieren Sie, ob bei einer Zustandsänderung einer redundanten Verbindung eine Fehlermeldung ausgelöst wird.



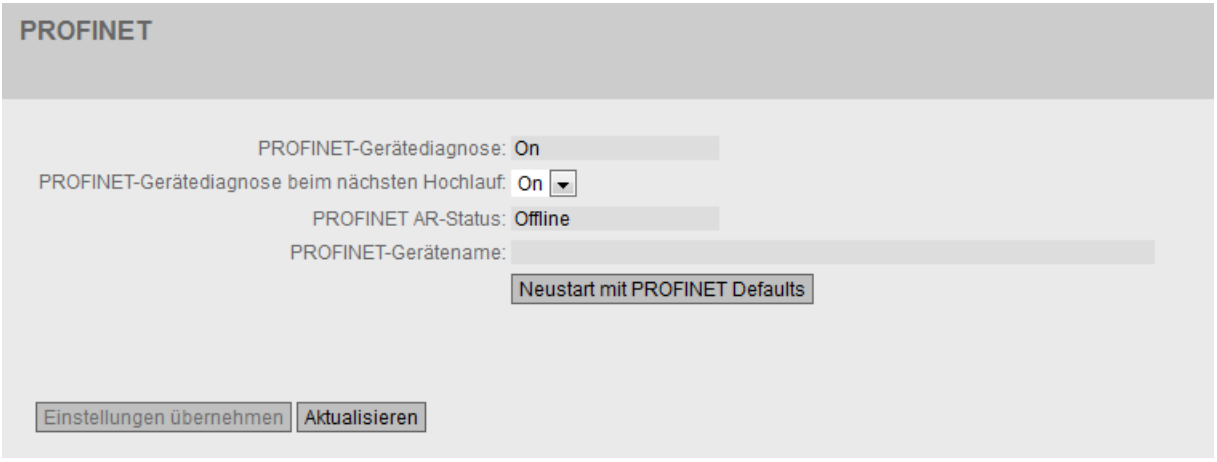
Einstellung

- **Redundanzverlust (nur HRP)**
  Aktivieren oder deaktivieren Sie die Verbindungsüberwachung. Wenn die Redundanz der Verbindung verloren geht, wird ein Fehler signalisiert.

5.4.16 PROFINET

Einstellungen für PROFINET

Auf dieser Seite konfigurieren Sie den Modus von PROFINET.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **PROFINET-Gerätediagnose**
  Zeigt an, ob PROFINET aktiviert ("On") oder deaktiviert ("Off") ist.
- **PROFINET-Gerätediagnose beim nächsten Hochlauf**
  Stellen Sie ein, ob PROFINET nach dem nächsten Neustart des Geräts aktiviert ("On") oder deaktiviert ("Off") sein soll.

Hinweis

PROFINET und EtherNet/IP

Wenn PROFINET eingeschaltet wird, wird EtherNet/IP ausgeschaltet. Das Umschalten von PROFINET und EtherNet/IP hat keine Auswirkungen auf DCP.

Hinweis

PROFINET AR-Status

Wenn eine PROFINET-Verbindung aufgebaut ist, d. h. der PROFINET AR-Status "Online" ist, können Sie PROFINET nicht deaktivieren.

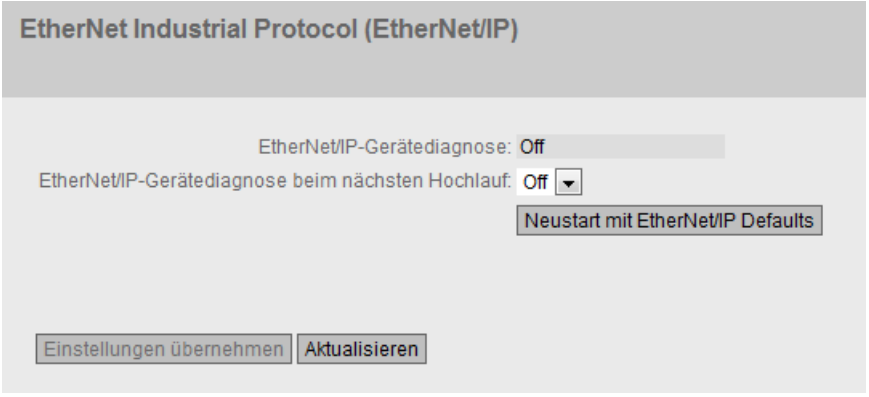
- **PROFINET AR-Status**
  Dieses Feld zeigt den Status des PROFINET-Verbindungsverhältnisses an, d.h. ob das Gerät mit einem PROFINET-Controller "Online" oder "Offline" verbunden ist.
  Online bedeutet hierbei, dass eine Verbindung zu einem PROFINET-Controller besteht, dass dieser seine Konfigurationsdaten auf das Gerät geladen hat und das Gerät Statusdaten zum PROFINET-Controller senden kann. In diesem Zustand, der auch "in Data exchange" genannt wird, sind die Parameter, die über den PROFINET-Controller eingestellt werden, nicht konfigurierbar.
- **PROFINET-Gerätename**
  In diesem Feld erscheint der PROFINET-Gerätenamen gemäß der Projektierung in der HW-Konfig von STEP 7.
- **Neustart mit PROFINET Defaults**
  Klicken Sie auf diese Schaltfläche, um die Defaulteinstellungen des PROFINET-Profils wiederherzustellen und das Gerät neu zu starten. Sie müssen den Neustart in einer Dialogbox bestätigen. In der Dialogbox werden die Einstellungen angezeigt, die speziell auf den Betrieb mit dem Protokoll PROFINET abgestimmt sind.

ACHTUNG
Durch das Zurücksetzen der Einstellungen auf die Defaulteinstellungen eines Profils geht auch die IP-Adresse verloren. Das Gerät ist danach nur über die serielle Schnittstelle, das Primary Setup Tool oder über DHCP ansprechbar. Bei entsprechendem Anschluss kann ein zuvor korrekt konfiguriertes Gerät nach dem Zurücksetzen kreisende Telegramme und damit den Ausfall des Datenverkehrs verursachen.

5.4.17 EtherNet/IP

EtherNet Industrial Protocol (EtherNet/IP)

Auf dieser Seite konfigurieren Sie den Modus von EtherNet/IP.



Beschreibung

Die Seite enthält folgende Felder:

- **EtherNet/IP-Gerätediagnose**
  Zeigt an, ob EtherNet/IP aktiviert ("On") oder deaktiviert ("Off") ist.
- **EtherNet/IP-Gerätediagnose beim nächsten Hochlauf**
  Stellen Sie ein, ob EtherNet/IP nach dem nächsten Neustart des Geräts aktiviert ("On") oder deaktiviert ("Off") sein soll.

Hinweis

EtherNet/IP und PROFINET

Wenn EtherNet/IP eingeschaltet wird, wird PROFINET ausgeschaltet. Das Umschalten von EtherNet/IP und PROFINET hat keine Auswirkungen auf DCP.

Hinweis

PROFINET AR-Status

Wenn eine PROFINET-Verbindung aufgebaut ist, d. h. der PROFINET AR-Status "Online" ist, können Sie EtherNet/IP nicht aktivieren.

- **Neustart mit EtherNet/IP Defaults**
  Klicken Sie auf diese Schaltfläche, um die Defaulteinstellungen des EtherNet/IP-Profils wiederherzustellen und das Gerät neu zu starten. Sie müssen den Neustart in einer Dialogbox bestätigen. In der Dialogbox werden die Einstellungen angezeigt, die speziell auf den Betrieb mit dem Protokoll EtherNet/IP abgestimmt sind.

ACHTUNG
Durch das Zurücksetzen der Einstellungen auf die Defaulteinstellungen eines Profils geht auch die IP-Adresse verloren. Das Gerät ist danach nur über die serielle Schnittstelle, das Primary Setup Tool oder über DHCP ansprechbar. Bei entsprechendem Anschluss kann ein zuvor korrekt konfiguriertes Gerät nach dem Zurücksetzen kreisende Telegramme und damit den Ausfall des Datenverkehrs verursachen.

5.4.18 PLUG

5.4.18.1 Konfiguration

ACHTUNG
PLUG nicht im laufenden Betrieb ziehen oder stecken Ein PLUG darf nur bei ausgeschaltetem Gerät entnommen oder eingesetzt werden. Das Gerät überprüft im Sekundenabstand, ob ein PLUG gesteckt ist. Wenn der PLUG im laufenden Betrieb entfernt wird, kann es zu Datenverlusten kommen.

Informationen über die Konfiguration des C-PLUG

Diese Seite liefert Detailinformationen über die Konfiguration, die im C-PLUG abgelegt ist. Darüber hinaus gibt es die Möglichkeit, den PLUG auf "Factory Default" zurückzusetzen oder mit einem neuen Inhalt zu versehen.

Hinweis

Die Aktion wird erst dann durchgeführt, wenn Sie auf die Schaltfläche "Einstellungen übernehmen" klicken.

Die Aktion kann nicht rückgängig gemacht werden.

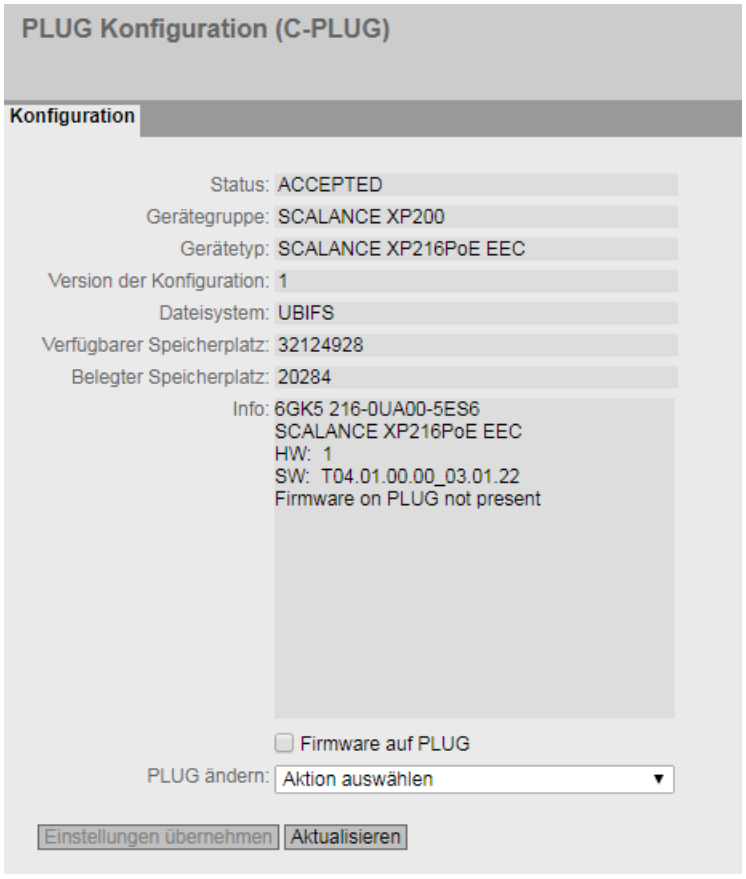
Wenn Sie sich nach der Auswahl gegen die Ausführung entscheiden, dann klicken Sie auf die Schaltfläche "Aktualisieren". Dadurch werden die Daten dieser Seite aus dem Gerät neu ausgelesen und Ihre Auswahl wird aufgehoben.

Hinweis

Inkompatibilität zu älteren Firmwareversionen mit gestecktem PLUG

Bei der Installation einer älteren Firmwareversion kann es zu Verlust der Konfigurationsdaten kommen. In diesem Fall startet das Gerät nach der Installation der Firmware mit den Werkseinstellungen. Wenn in diesem Fall ein PLUG im Gerät gesteckt ist, hat dieser nach dem Neustart den Status "NOT ACCEPTED", da sich auf dem PLUG weiterhin die Konfigurationsdaten der vorherigen, aktuelleren Firmware befinden. Somit kann ohne Konfigurationsdatenverlust zur vorherigen, aktuelleren Firmware zurückgekehrt werden.

Falls die ursprüngliche Konfiguration auf dem PLUG nicht mehr benötigt wird, kann der PLUG manuell über "System > PLUG" gelöscht oder neu beschrieben werden.



Beschreibung der angezeigten Felder

Die Tabelle gliedert sich in folgende Zeilen:

- **Status**
  Zeigt den Status des PLUG an. Es gibt die folgenden Möglichkeiten:
  - ACCEPTED
    Es ist ein PLUG mit einer gültigen und passenden Konfiguration im Gerät vorhanden.
  - NOT ACCEPTED
    Ungültige bzw. inkompatible Konfiguration auf dem gesteckten PLUG.
  - NOT PRESENT
    Im Gerät ist kein C-PLUG gesteckt.
  - FACTORY
    PLUG ist gesteckt und enthält keine Konfiguration. Dieser Status wird auch angezeigt, wenn der PLUG im Betrieb formatiert wurde.
- **Gerätegruppe**
  Zeigt an, von welcher SIMATIC NET-Produktlinie der C-PLUG im vorangegangenen Betrieb genutzt wurde.
- **Gerätetyp**
  Zeigt den Gerätetyp innerhalb der Produktlinie an, von dem der C-PLUG im vorangegangenen Betrieb genutzt wurde.

- **Version der Konfiguration**
  Die Version der Konfigurationsstruktur. Diese Angabe betrifft die vom Gerät unterstützten Konfigurationsmöglichkeiten und hat nichts mit der konkreten Hardware-Konfiguration zu tun. Diese Revisionsangabe ändert sich also nicht, wenn Sie Zusatzkomponenten (z.B. Module bzw. Extender) hinzufügen oder entfernen, sie kann sich aber ändern, wenn Sie ein Firmware-Update durchführen.
- **Dateisystem**
  Zeigt den Typ des Dateisystems an, das auf dem PLUG vorhanden ist.
- **Verfügbarer Speicherplatz**
  Zeigt die maximale Speicherkapazität des Dateisystems in Byte an, das auf dem PLUG vorhanden ist.
- **Belegter Speicherplatz**
  Zeigt den belegten Speicherplatz im Dateisystem des PLUG in Byte an.
- **Info**
  Zeigt zusätzliche Informationen über das Gerät an, das den PLUG im vorangegangenen Betrieb genutzt hatte, z. B. Bestellnummer, Typenbezeichnung sowie die Ausgabestände von Hard- und Software. Der angezeigte Software-Ausgabestand entspricht dem Ausgabestand, in dem zuletzt die Konfiguration geändert wurde. Beim Status "NOT ACCEPTED" werden weitere Informationen zur Problemursache angezeigt.
- **Firmware auf PLUG**
  Wenn die Funktion aktiviert ist, wird die Firmware auf dem PLUG abgespeichert. Damit können mit dem PLUG automatische Firmware-Updates/Downgrades durchgeführt werden. In dem Feld "Info" wird angezeigt, ob die Firmware auf dem PLUG gespeichert ist oder nicht.
- **PLUG ändern**
  Wählen Sie aus der Klappliste die Einstellung. Sie haben folgende Möglichkeiten, um die Konfiguration auf dem C-PLUG zu ändern:
  - Aktuelle Konfiguration auf den PLUG schreiben
    Diese Option ist nur verfügbar, wenn der Status des PLUG "NOT ACCEPTED" oder "FACTORY" ist.
    Die im internen Flash-Speicher des Geräts vorhandene Konfiguration wird auf den PLUG kopiert.
  - PLUG auf Werkseinstellungen zurücksetzen
    Löscht alle Daten vom PLUG und führt eine Low-Level-Formatierung durch.

Vorgehensweise zur Konfiguration

1. Sie können in diesem Feld nur dann Einstellungen vornehmen, wenn Sie als "Administrator" angemeldet sind. Wählen Sie hier aus, wie Sie den Inhalt des PLUG verändern wollen.
2. Wenn Sie die Firmware auf dem PLUG speichern wollen, aktivieren Sie das Optionskästchen "Firmware auf PLUG".
3. Wählen Sie aus der Klappliste "PLUG ändern" die gewünschte Option aus.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.4.19 Ping

Erreichbarkeit einer Adresse in einem IPv4-Netzwerk

Mit der Ping-Funktion können Sie überprüfen, ob eine bestimmte IPv4-Adresse im Netzwerk erreichbar ist.

Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Zieladresse**
  Geben Sie die IPv4-Adresse des Geräts ein.
- **Wiederholen**
  Tragen Sie die Anzahl der Ping-Anforderungen ein.
- **Ping**
  Klicken Sie diese Schaltfläche, um die Ping-Funktion zu starten.
- **Ping-Ausgabe**
  Dieses Feld zeigt die Ausgabe der Ping-Funktion an.
- **Leeren**
  Klicken Sie diese Schaltfläche, um das Feld "Ping-Ausgabe" zu leeren.

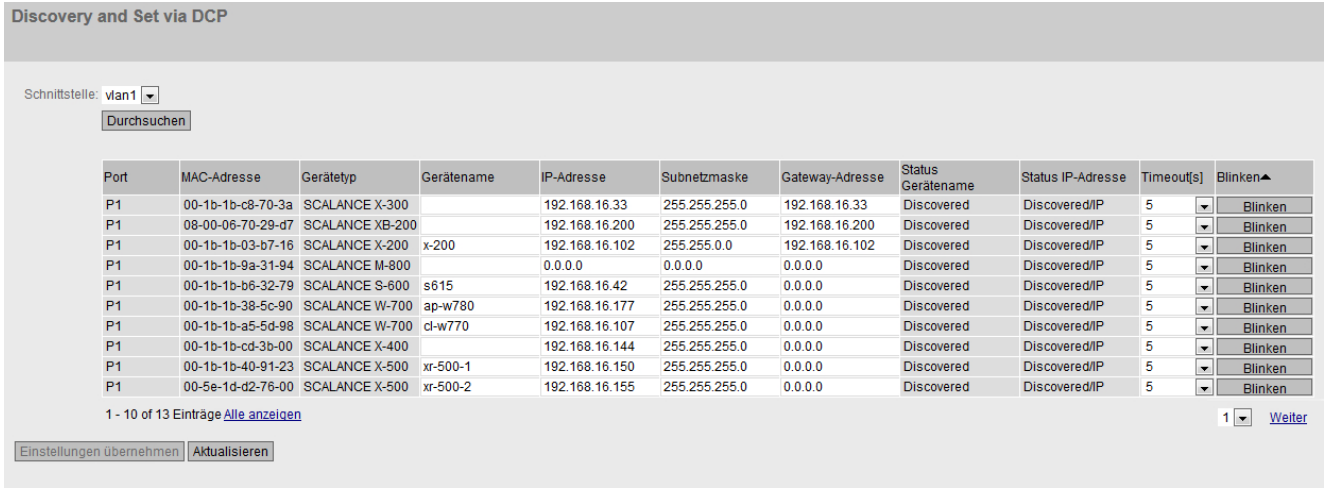
5.4.20 DCP Discovery

Auf dieser Seite können Sie eine Schnittstelle auswählen und nach den Geräten suchen, die über die Schnittstelle erreichbar sind und DCP unterstützen. DCP Discovery sucht nur nach Geräten, die im gleichen Subnetz liegen wie die Schnittstelle. Die erreichbaren Geräte werden in einer Tabelle aufgelistet. In der Tabelle können Sie die Netzwerkparameter der Geräte überprüfen und anpassen. Zum Identifizieren und zum Konfigurieren der Geräte wird das Discovery Configuration Protocol (DCP) verwendet.

Hinweis

DCP Discovery

Die Funktion ist nur in dem mit der TIA-Schnittstelle assoziierten VLAN verfügbar. Die TIA-Schnittstelle konfigurieren Sie unter "System > Agent IP".



Voraussetzung:

Um die Netzwerkparameter anzupassen, benötigt DCP Schreibrechte auf dem Gerät. Wenn der Zugriff schreibgeschützt ist, sind die Netzwerkparameter nicht konfigurierbar.

Auf den SCALANCE-Geräten konfigurieren Sie den Zugriff konfigurieren unter "System > Konfiguration".

Beschreibung

Die Seite enthält folgende Felder:

- **Schnittstelle**
  Wählen Sie die gewünschte Schnittstelle aus.
- **Durchsuchen**
  Startet die Suche nach Geräten, die über die gewählte Schnittstelle erreichbar sind. Nach dem Abschluss der Suche werden die erreichbaren Geräte in der Tabelle aufgelistet. Die Tabelle ist auf 100 Einträge begrenzt.

Die Tabelle gliedert sich in folgende Spalten:

- **Port**
  Zeigt den Port an, über den das Gerät erreichbar ist.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Geräts an.
- **Gerätetyp**
  Zeigt an, zu welcher Produktlinie bzw. Produktgruppe das Gerät gehört.
- **Gerätename**
  Passen Sie bei Bedarf den PROFINET-Gerätenamen an. Der Gerätename muss DNS-konform sein.
  Wenn der Gerätename nicht verwendet wird, ist das Feld leer.
- **IP-Adresse**
  Passen Sie bei Bedarf die IPv4-Adresse des Geräts an.
  Die IPv4-Adresse sollte innerhalb Ihres Netzwerks eindeutig sein und zum Netzwerk passen. Die IPv4-Adresse 0.0.0.0 bedeutet, dass noch keine IPv4-Adresse eingestellt ist.
- **Subnetzmaske**
  Passen Sie bei Bedarf die Subnetzmaske des Geräts an.
- **Gateway-Adresse**
  Passen Sie bei Bedarf die IPv4-Adresse des Gateways an.
- **Status Gerätename**
  - None: Der Gerätename wird nicht verwendet.
  - Discoverd: Der eingestellte Gerätename wird verwendet.
  - Configured: Dem Gerät wurde ein neuer Gerätename zugewiesen.
- **Status IP-Adresse**
  - Discovered/IP: Das Gerät verwendet eine statische IPv4-Adresse.
  - Discovered/DHCP: Das Gerät hat die IPv4-Adresse von einem DHCP-Server bezogen.
  - Configured: Dem Gerät wurde eine neue IPv4-Adresse zugewiesen.
- **Timeout[s]**
  Legen Sie die Zeitdauer für das Blinken fest. Wenn die Zeit abgelaufen ist, wird das Blinken beendet.
- **Blinken**
  Lässt die Port-LEDs des ausgewählten Geräts blinken.

Vorgehensweise zur Konfiguration

1. Wählen Sie die TIA-Schnittstelle aus.
2. Um alle Geräte anzuzeigen, die über die TIA-Schnittstelle erreichbar sind, klicken Sie auf die Schaltfläche "Durchsuchen".
3. Passen Sie die gewünschten Eigenschaften an.

4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
   Der Status der geänderten Eigenschaften ändert sich in "Configured".
5. Um sicherzustellen, dass die Eigenschaften korrekt übernommen wurden, klicken Sie erneut auf die Schaltfläche "Durchsuchen".
   Der Status der geänderten Eigenschaften ändert sich in "Discovered".

5.4.21 Power over Ethernet (PoE)

5.4.21.1 Allgemein

Einstellungen für Power over Ethernet (PoE)

Auf dieser Seite sehen Sie Informationen zu der Leistung, die der IE-Switch über PoE liefert.

Die PoE-Varianten des SCALANCE XP-200 stellen PSEs (Power Sourcing Equipment) dar.

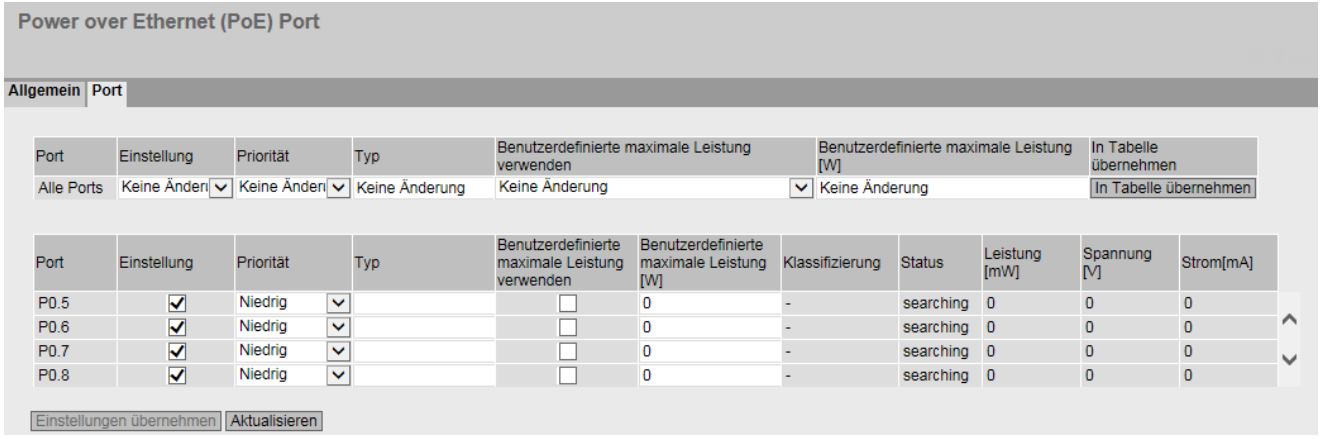
Beschreibung der angezeigten Felder

- **PSE (nur lesbar)**
  Zeigt die Nummer des PSE an.
- **Maximale Leistung [W] (nur lesbar)**
  Maximale Leistung, die ein PSE für die Versorgung von PoE-Geräten zur Verfügung stellt.
- **Zugeteilte Leistung [W] (nur lesbar)**
  Summe der durch die PoE-Geräte entsprechend der "Klassifizierung" reservierten Leistung.
- **Genutzte Leistung [W] (nur lesbar)**
  Summe der von den Endgeräten genutzten Leistung.
- **Schwellenwert der Leistung [%]**
  Sobald die von den Endgeräten verbrauchte Leistung größer ist als der hier angegebene Prozentanteil, wird ein Event ausgelöst.

5.4.21.2 Port

Einstellungen für die Ports

Für jeden einzelnen PoE-Port können Sie festlegen, ob eine Spannungsversorgung über Ethernet erfolgen soll. Außerdem können Sie für jeden angeschlossenen Verbraucher eine Priorität festlegen. Geräte, für die eine hohe Priorität festgelegt wurde, werden im Bedarfsfall gegenüber anderen bei der Spannungsversorgung bevorzugt.
Auf dieser Seite sehen Sie Detailinformationen zu den einzelnen PoE-Ports.



Beschreibung der angezeigten Felder

Die Seite enthält zwei Tabellen. In der Tabelle 1 können Sie Einstellungen vornehmen und diese allen Ports gleichzeitig zuweisen. In der Tabelle 2 können Sie für jeden Port unterschiedliche Einstellungen vornehmen.

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Port**
  Zeigt an, dass die Einstellungen für alle Ports gültig sind.
- **Einstellung**
  Wählen Sie die gewünschte Einstellung.
  Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **Priorität**
  Wählen Sie die gewünschte Priorität.
  Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **Typ**
  Hier können Sie eine Zeichenkette eingeben, die das angeschlossene Gerät näher beschreibt. Die maximale Länge beträgt 255 Zeichen.
- **Benutzerdefinierte maximale Leistung verwenden**
  Wählen Sie, ob die benutzerdefinierte maximale Leistung verwendet werden soll.
  Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.

- **Benutzerdefinierte maximale Leistung [W]**
  Geben Sie die maximale Leistung an, die ein Port für die Versorgung eines angeschlossenen Geräts zur Verfügung stellt.
  Dieser Wert wird nur berücksichtigt, wenn das dazugehörige Optionskästchen "Benutzerdefinierte maximale Leistung verwenden" aktiviert ist.
  Wenn "Keine Änderung" eingetragen ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, werden die Einstellungen für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die konfigurierbaren PoE-Ports an.
  Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Einstellung**
  Schalten Sie die PoE-Spannungsversorgung für diesen Port frei oder unterbrechen Sie sie.
- **Priorität**
  Wählen Sie aus der Klappliste die Priorität, mit der dieser Port bei der Spannungsversorgung berücksichtigt wird.
  Es gibt folgende Einstellmöglichkeiten mit aufsteigender Relevanz:
  - Niedrig
  - Hoch
  - Kritisch

  Wenn die Leistung der angeschlossenen Spannungsversorgung nicht ausreicht, um alle angeschlossenen Geräte zu versorgen, werden Geräte mit einer höheren Priorität vorrangig versorgt.
  Ist für zwei Ports die gleiche Priorität vorgegeben, wird im Bedarfsfall der Port mit der niedrigeren Nummer bevorzugt.
- **Typ**
  Hier können Sie eine Zeichenkette eingeben, die das angeschlossene Gerät näher beschreibt. Die maximale Länge beträgt 255 Zeichen.
- **Benutzerdefinierte maximale Leistung verwenden**
  Wenn Sie dieses Optionskästchen für einen Port aktivieren, wird die benutzerdefinierte maximale Leistung verwendet.

- **Benutzerdefinierte maximale Leistung [W]**
  Geben Sie die maximale Leistung an, die ein Port für die Versorgung eines angeschlossenen Geräts zur Verfügung stellt.
  Dieser Wert wird nur berücksichtigt, wenn das dazugehörige Optionskästchen "Benutzerdefinierte maximale Leistung verwenden" aktiviert ist.
  Die benutzerdefinierte Leistung wird mit dem Wertebereich der Klasse abgeglichen, die das angeschlossene Gerät angibt:
  - Wenn die benutzerdefinierte Leistung innerhalb der Klasse des angeschlossenen Geräts liegt, wird der benutzerdefinierte Wert verwendet.
  - Wenn die benutzerdefinierte Leistung über der Klasse des angeschlossenen Geräts liegt, wird der höchste Wert der Klasse verwendet.
  - Wenn die benutzerdefinierte Leistung unter der Klasse des angeschlossenen Geräts liegt, wird der niedrigste Wert der Klasse verwendet.

  Wenn die Leistungsaufnahme des angeschlossenen Geräts die definierte bzw. verwendete maximale Leistung überschreitet, wird das angeschlossene Gerät abgeschaltet.
- **Klassifizierung (nur lesbar)**
  Die Klassifizierung gibt die Klasse des Geräts an.
- **Status (nur lesbar)**
  Zeigt an, in welchem Zustand sich der Port befindet.
  Es gibt folgende Zustände:
  - disabled
    Die PoE-Spannungsversorgung für diesen Port ist deaktiviert.
  - delivering
    Die PoE-Spannungsversorgung für diesen Port ist aktiviert und es ist ein Gerät angeschlossen.
  - searching
    Die PoE-Spannungsversorgung für diesen Port ist aktiviert, aber es ist kein Gerät angeschlossen.

  Hinweis

  Wenn ein Gerät an einen PoE-fähigen Port angeschlossen wird, wird geprüft, ob die Leistung des Ports für das angeschlossene Gerät ausreicht.

  Wenn die Leistung des Ports nicht ausreicht, ist PoE zwar unter Einstellung aktiviert, der Port hat jedoch den Status disabled. Der Port wurde dann vom PoE-Power Management deaktiviert.

- **Leistung [mW] (nur lesbar)**
  Zeigt die Leistung an, die der SCALANCE an diesem Port liefert.
- **Spannung [V] (nur lesbar)**
  Zeigt die Spannung an, die an diesem Port anliegt.
- **Strom [mA] (nur lesbar)**
  Zeigt den Strom an, mit dem ein Gerät an diesem Port versorgt wird.

5.4.22 Port-Diagnose

5.4.22.1 Kabel-Tester

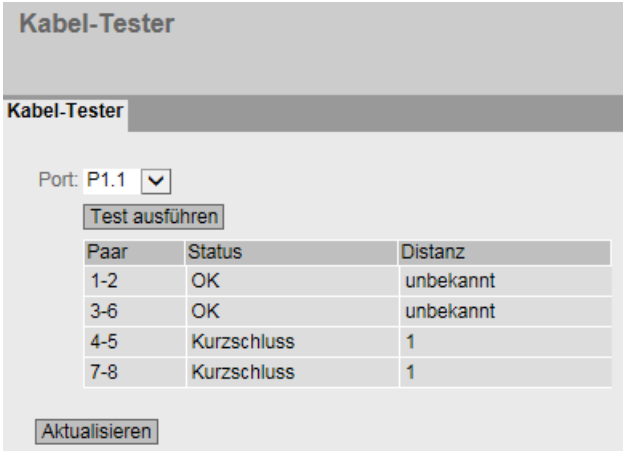
Mit dieser Seite kann jeder einzelne Ethernet-Port eine unabhängige Fehlerdiagnose am Kabel durchführen. Dieser Test wird durchgeführt, ohne dass das Kabel ausgesteckt, ein Kabeltester angeschlossen und am anderen Ende ein Loopback-Modul installiert ist. Kurzschlüsse sowie Leitungsunterbrechungen können auf wenige Meter genau lokalisiert werden.

Hinweis

Bitte beachten Sie, dass dieser Test nur zulässig ist, wenn auf dem zu testenden Port keine Datenverbindung aufgebaut ist.

Sollte dennoch auf dem zu testenden Port eine Datenverbindung bestehen, so wird diese kurzzeitig unterbrochen.

Ein automatischer Wiederaufbau der Verbindung kann scheitern und muss dann manuell erfolgen.



Beschreibung

Die Seite enthält folgende Felder:

- **Port**
  Wählen Sie aus der Klappliste den gewünschten Port aus.
- **Test ausführen**
  Aktiviert die Fehlerdiagnose. Das Ergebnis wird in der Tabelle dargestellt.

Die Tabelle enthält folgende Spalten:

- **Paar**
  Zeigt das Adernpaar im Kabel an.

  Hinweis

  Adernpaare

  Bei 10/100 MBit/s Netzwerkkabeln werden die Adernpaare 4-5 und 7-8 nicht verwendet.

  Dabei ist die Zuordnung Adernpaar - Pinbelegung wie folgt (DIN EN 50173):

  Paar 1 = Pin 1-2

  Paar 2 = Pin 3-6

  Paar 3 = Pin 4-5

  Paar 4 = Pin 7-8

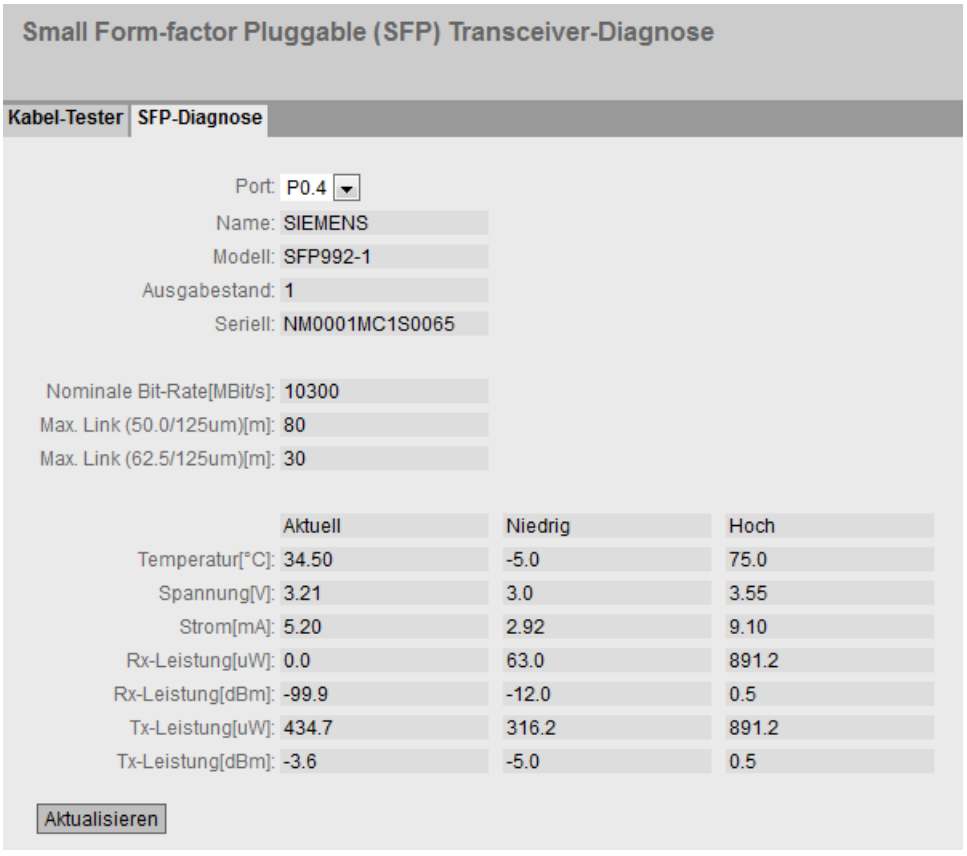
- **Status**
  Zeigt den Status der Leitung an.
- **Distanz**
  Zeigt die Entfernung zum offenen Kabelende, Kabelbruch oder zum Kurzschluss in Metern an. Der Wert für die Entfernung hat eine Toleranz von +/- 1 m.
  Wenn der Status "OK" ist, wird die Länge mit "unbekannt" angegeben.

5.4.22.2 SFP-Diagnose

Mit dieser Seite führen Sie für jeden einzelnen SFP-Port eine unabhängige Fehlerdiagnose durch. Dieser Test wird durchgeführt, ohne dass ein Kabel ausgesteckt, ein Kabeltester angeschlossen und am anderen Ende ein Loopback-Modul installiert werden muss.

Hinweis

Bitte beachten Sie, dass dieser Test nur zulässig ist, wenn auf dem zu testenden Port keine Datenverbindung aufgebaut ist. Sollte dennoch auf dem zu testenden Port eine Datenverbindung bestehen, so wird diese kurzzeitig unterbrochen. Ein automatischer Wiederaufbau der Verbindung kann scheitern und muss dann manuell erfolgen.



Beschreibung

Die Seite enthält folgende Felder:

- **Port**
  Wählen Sie aus der Klappliste den gewünschten Port aus.
- **Aktualisieren**
  Erneuert die Anzeige der Werte des eingestellten Ports. Das Ergebnis wird in der Tabelle dargestellt.

Die Werte werden in den folgenden Feldern angezeigt:

- **Name**
  Zeigt den Namen der Schnittstelle an.
- **Modell**
  Zeigt die Art der Schnittstelle an.
- **Ausgabestand**
  Zeigt den Hardware Ausgabestand des SFP an.
- **Seriell**
  Zeigt die Seriennummer des SFP an.
- **Nominale Bit-Rate[MBit/s]**
  Zeigt die Nenn-Bitrate der Schnittstelle an.

- **Max. Link (50.0/125um)[m]**
  Zeigt die maximale Distanz in Metern an, die mit diesem Medium möglich sind.
- **Max. Link (62.5/125um)[m]**
  Zeigt die maximale Distanz in Metern an, die mit diesem Medium möglich sind.

Die folgende Tabelle zeigt die Werte des in diesem Port eingesetzten SFP-Stecktransceivers an:

Hinweis

Abweichungen der angezeigten Werte von den technischen Daten

Die angezeigten Werte für die minimale und maximale Sende- bzw. Empfangsleistung können sich geringfügig von den in der Betriebsanleitung angegebenen Werten unterscheiden. Maßgeblich sind die auf der WBM-Seite angezeigten Werte.

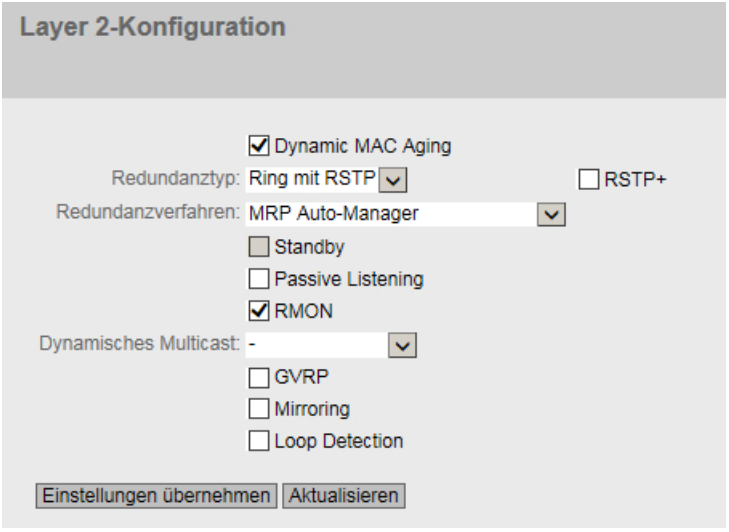
- **Temperatur[°C]**
  Zeigt die Temperatur der Schnittstelle an.
- **Spannung[V]**
  Zeigt die an der Schnittstelle anliegende Spannung in Volt an.
- **Strom[mA]**
  Zeigt die Stromaufnahme der Schnittstelle in Milliampere an.
- **Rx-Leistung[µW]/Rx-Leistung[dBm]**
  Zeigt die Empfangsleistung der Schnittstelle in Mikrowatt/Dezibel Milliwatt an.
- **Tx-Leistung[µW]/Tx-Leistung[dBm]**
  Zeigt die Sendeleistung der Schnittstelle in Mikrowatt/Dezibel Milliwatt an.
- **Spalte Aktuell**
  Zeigt den aktuellen Wert an.
- **Spalte Niedrig**
  Zeigt den niedrigsten Wert an.
- **Spalte Hoch**
  Zeigt den höchsten Wert an.

5.5 Das Menü "Layer 2"

5.5.1 Konfiguration

Layer 2 konfigurieren

Auf dieser Seite nehmen Sie eine Basiskonfiguration der Funktionen von Layer 2 vor. Auf den jeweiligen Konfigurationsseiten dieser Funktionen sind detailliertere Einstellungen möglich. Auf den Konfigurationsseiten können Sie auch die Einstellungen prüfen.



Beschreibung der angezeigten Felder

- **Dynamc MAC Aging**
  Aktivieren oder deaktivieren Sie den Mechanismus "Aging". Weitere Einstellungen konfigurieren Sie unter "Layer 2 > Dynamic MAC Aging".
- **Redundanztyp**
  Folgende Einstellungen gibt es:
  - **"-" (Deaktiviert)**
    Die Redundanzfunktion ist deaktiviert.
  - **Spanning Tree**
    Wenn Sie diese Option auswählen, legen Sie in der Klappliste "Redundanzverfahren" den gewünschten Redundanzmodus fest.
  - **Ring**
    Wenn Sie diese Option auswählen, legen Sie in der Klappliste "Redundanzverfahren" den gewünschten Redundanzmodus fest.
  - **Ring mit RSTP**
    Wenn Sie diese Option auswählen, ist der Kompatibilitätsmodus für Spanning Tree fest auf RSTP gesetzt. In der Klappliste "Redundanzverfahren" legen Sie den Redundanzmodus der Ringredundanz fest.
    Die aktuelle Einstellung können Sie in den Menüs "Ring-Redundanz" und "Spanning Tree" ändern.

    Hinweis

    Einschränkung bzgl. Ports bei der Option "Ring mit RSTP“

    Wenn Sie die Option "Ring mit RSTP" aktiviert haben, dürfen folgende Ports nicht im Spanning Tree enthalten sein:
    - Ring-Ports
    - Standby-Ports
    - Standby-Koppelports
- **RSTP+**
  Aktiviert RSTP+. Sie können dieses Optionskästchen nur aktivieren, wenn als Redundanzverfahren MRP konfiguriert wurde.

- **Redundanzverfahren**
  Wenn Sie in der Klappliste "Redundanztyp" "Ring" oder "Ring with RSTP" auswählen, stehen Ihnen folgende Auswahlmöglichkeiten zur Verfügung:

  – Automatic Redundancy Detection
    Wählen Sie diese Einstellung, um eine automatische Konfiguration der Redundanzbetriebsart vorzunehmen.
    Im Modus "Automatic Redundancy Detection" stellt das Gerät automatisch fest, ob sich ein Gerät mit der Rolle "HRP Manager" im Ring befindet. Ist dies der Fall, so nimmt das Gerät die Rolle "HRP Client" ein.
    Wird kein HRP Manager gefunden, so handeln alle Geräte mit der Einstellung "Automatic Redundancy Detection" oder "MRP Auto-Manager" untereinander aus, welches Gerät die Rolle "MRP Manager" einnimmt. Dabei wird immer das Gerät mit der niedrigsten MAC-Adresse zum "MRP Manager". Die übrigen Geräte stellen sich automatisch auf die Betriebsart "MRP Client" ein.

  – MRP Auto-Manager
    Im Modus "MRP Auto-Manager" handeln die Geräte untereinander aus, welches Gerät die Rolle "MRP Manager" einnimmt. Dabei wird immer das Gerät mit der niedrigsten MAC-Adresse zum "MRP Manager". Die übrigen Geräte stellen sich automatisch auf die Betriebsart "MRP Client" ein.
    Im Gegensatz zur Einstellung "Automatic Redundancy Detection" sind die Geräte nicht in der Lage zu erkennen, ob ein HRP-Manager im Ring ist.

    Hinweis

    MRP-Projektierung in STEP 7

    Wenn Sie über STEP 7 die Rolle "Manager (Auto)" oder "Manager" für das Gerät einstellen, wird auf dieser WBM-Seite in beiden Fällen "MRP Auto-Manager" angezeigt. In der Anzeige im CLI wird zwischen den beiden Rollen unterschieden.

  – MRP-Client
    Das Gerät nimmt die Rolle MRP-Client ein.

  – HRP-Client
    Das Gerät nimmt die Rolle HRP-Client ein.

  – HRP-Manager
    Das Gerät nimmt die Rolle HRP-Manager ein.
    Bei der Projektierung eines HRP-Rings muss ein Gerät als HRP-Manager eingestellt werden. Bei allen übrigen Geräten muss "HRP Client" oder "Automatic Redundancy Detection" eingestellt sein.

  Wenn Sie in der Klappliste "Redundanztyp" "Spanning Tree" auswählen, stehen Ihnen folgende Auswahlmöglichkeiten zur Verfügung:

  – **STP**
    Aktiviert das Spanning Tree Protocol (STP). Typische Rekonfigurationszeiten bei Spanning Tree liegen zwischen 20 und 30 Sekunden. Weitere Einstellungen konfigurieren Sie unter "Layer 2 > Spanning Tree".

- **RSTP**
  Aktiviert das Rapid Spanning Tree Protocol (RSTP). Wenn an einem Port ein Spanning Tree-Telegramm erkannt wird, fällt dieser Port von RSTP auf Spanning Tree zurück. Weitere Einstellungen konfigurieren Sie unter "Layer 2 > Spanning Tree".

  Hinweis

  Bei RSTP kann es zu kurzzeitiger Schleifenbildung mit Telegrammverdoppelung oder zu Telegrammüberholungen kommen. Wenn das in Ihrem Anwendungsfall nicht akzeptabel sein sollte, müssen Sie das langsamere Standardverfahren Spanning Tree benutzen.

- **MSTP**
  Aktiviert das Multiple Spanning Tree Protocol (MSTP). Weitere Einstellungen konfigurieren Sie unter "Layer 2 > Spanning Tree".

Wenn Sie in der Klappliste "Redundanztyp" "Ring mit RSTP" auswählen, wird Ihnen der aktuelle Redundanzmodus des Spanning Tree und der Ringredundanz angezeigt.

- **Standby**
  Aktivieren oder deaktivieren Sie die Funktion Standby-Redundanz. Weitere Einstellungen finden Sie unter "Layer 2 > Ring-Redundanz".
- **Passive Listening**
  Aktivieren oder deaktivieren Sie die Funktion Passive Listening.
  Mit Passive Listening können Sie Spanning Tree-Netze mit MRP-/HRP-Ringen verbinden. Die Ringteilnehmer leiten Spanning Tree BPDUs weiter und reagieren somit auf Topologieänderungen. Beim Empfang eines Topology Change-Frames wird die MAC-Adress-Tabelle gelöscht.
- **RMON**
  Wenn Sie dieses Optionskästchen aktivieren, ermöglicht Remote Monitoring (RMON), Diagnosedaten im Gerät zu sammeln, aufzubereiten und über SNMP von einer Netzwerkmanagement-Station, die ebenfalls RMON unterstützt, auszulesen. Diese Diagnosedaten, wie zum Beispiel portbezogene Lastverläufe, ermöglichen es, Probleme im Netzwerk frühzeitig zu erkennen und zu beseitigen. Die "Ethernet Statistics Counter" sind zum Teil Bestandteil der RMON Funktion. Wenn Sie RMON deaktivieren, wird der "Ethernet Statistic Counter" bei "Information > Ethernet-Statistiken" nicht weiter aktualisiert.
- **Dynamisches Multicast**
  Folgende Einstellung sind möglich:
  - **"-" (Deaktiviert)**
  - **IGMP Snooping**
    Aktiviert IGMP (Internet Group Management Protocol). Weitere Einstellungen konfigurieren Sie unter "Layer 2 > Multicast > IGMP".
  - **GMRP**
    Aktiviert GMRP (GARP Multicast Registration Protocol). Weitere Einstellungen konfigurieren Sie unter "Layer 2 > Multicast > GMRP".

    Hinweis

    GMRP und IGMP können nicht gleichzeitig betrieben werden.

- **GVRP**
  Aktivieren oder deaktivieren Sie "GVRP" (GARP VLAN Registration Protocol). Weitere Einstellungen konfigurieren Sie unter "Layer 2 > VLAN > GVRP".
- **Mirroring**
  Aktivieren oder deaktivieren Sie die Port-Spiegelung. Weitere Einstellungen konfigurieren Sie unter "Layer 2 > Mirroring".
- **Loop Detection**
  Aktivieren oder deaktivieren Sie die Funktion Loop Detection. Damit werden Schleifen im Netzwerk erkannt. Weitere Einstellungen finden Sie unter "Layer 2 > Loop Detection"

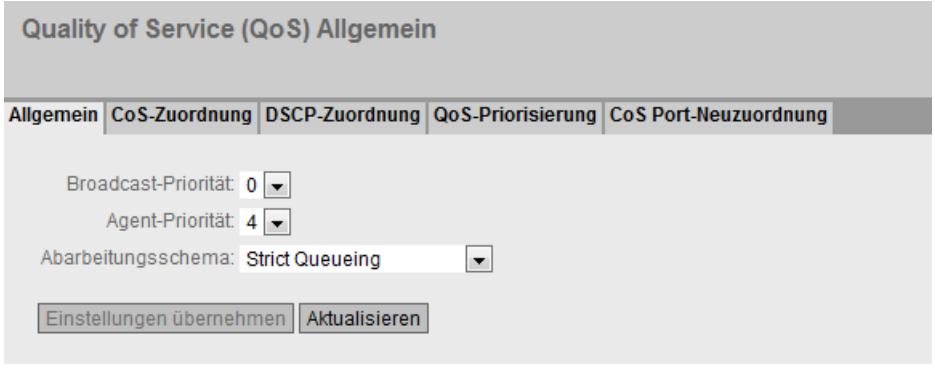
5.5.2 Quality of Service (QoS)

Beachten Sie hierzu auch das Kapitel "Technische Grundlagen", Abschnitt "Quality of Service (Seite 61)".

5.5.2.1 Allgemein

Übertragungsprioritäten

Auf dieser Seite können Sie die Prioritäten verschiedener Frames festlegen. Außerdem können Sie abhängig von der Priorität einstellen, nach welcher Methode die Abarbeitungsreihenfolge der Frames festgelegt wird.



Beschreibung der angezeigten Werte

Die Seite enthält folgende Felder:

- **Broadcast-Priorität**
  Legen Sie die Priorität von Broadcast-Frames fest. Der Switch sortiert das Frame entsprechend dieser Priorisierung in eine Warteschlange (Queue) ein. Die Zuordnung der Priorität zu einer Queue konfigurieren Sie auf der Seite "Layer 2 > QoS > CoS-Zuordnung".
- **Agent-Priorität**
  Legen Sie die Priorität von Agent-Frames fest. Der Switch sortiert das Frame entsprechend dieser Priorisierung in eine Queue ein. Die Zuordnung der Priorität zu einer Queue konfigurieren Sie auf der Seite "Layer 2 > QoS > CoS-Zuordnung".
- **Abarbeitungsschema**
  Wählen Sie aus, in welcher Reihenfolge die Frames in den Queues verarbeitet werden.
  - Strict Queueing
    Solange sich Frames mit einer hohen Priorität in der Queue befinden, werden nur diese hoch priorisierten Frames abgearbeitet.
  - Weighted Fair Queueing
    Auch wenn sich Frames mit einer hohen Priorität in der Queue befinden, werden gelegentlich Frames mit einer niedrigeren Priorität abgearbeitet.

Hinweis

Geräte, bei denen Sie das Abarbeitungsschema nicht einstellen können, nutzen die Methode "Strict Queueing".

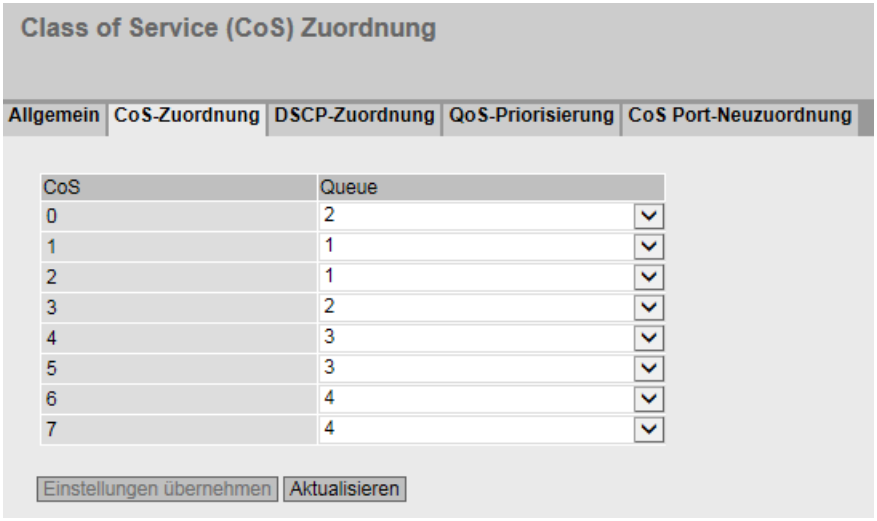
Vorgehensweise zur Konfiguration

1. Wählen Sie in den Klapplisten "Broadcast-Priorität" und "Agent-Priorität" aus, mit welcher Priorität die Frames intern verarbeitet werden.
2. Wählen Sie in der Klappliste "Abarbeitungsschema" aus, nach welcher Methode die Abarbeitungsreihenfolge der Frames festgelegt wird.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.2.2 CoS-Zuordnung

CoS-Zuordnung

Auf dieser Seite können Sie CoS-Prioritäten verschiedenen Queues zuordnen.



Beschreibung der angezeigten Felder

Die Tabelle gliedert sich in folgende Spalten:

- **CoS**
  Zeigt die CoS-Priorität der eingehenden Frames an.
- **Queue**
  Wählen Sie aus der Klappliste die Queue aus, die der CoS-Priorität zugeordnet wird.
  Je höher die Nummer der Queue desto höher die Abarbeitungspriorität.

Die Service-Klassen (CoS) sind den Queues standardmäßig wie folgt zugeordnet:

COS	Geräte mit 4 Queues	Geräte mit 8 Queues
0	Queue 2	Queue 2
1	Queue 1	Queue 1
2	Queue 1	Queue 3
3	Queue 2	Queue 4
4	Queue 3	Queue 5
5	Queue 3	Queue 6
6	Queue 4	Queue 7
7	Queue 4	Queue 8

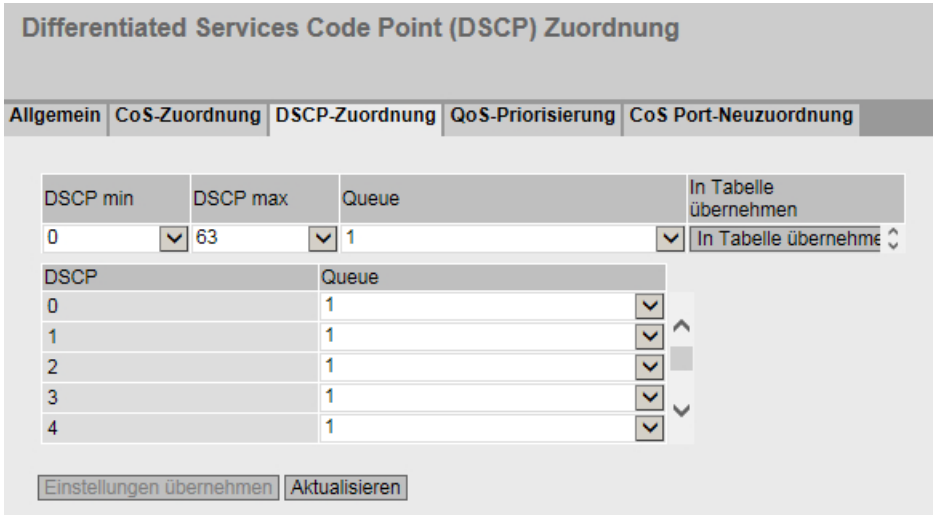
Vorgehensweise zur Konfiguration

1. Wählen Sie zu jedem Wert der Spalte "CoS" mit Hilfe der Klappliste "Queue" die Warteschlange aus.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.2.3 DSCP-Zuordnung

DSCP Warteschlange

Auf dieser Seite können Sie DSCP-Prioritäten verschiedenen Warteschlangen (Queues) zuordnen.



Beschreibung der angezeigten Werte

Die Tabelle 1 gliedert sich in folgende Spalten:

- **DSCP min**
  Wählen Sie aus der Klappliste den minimalen Wert für einen Bereich von DSCP-Codes aus, denen Sie eine Queue zuweisen wollen.
- **DSCP max**
  Wählen Sie aus der Klappliste den maximalen Wert für einen Bereich von DSCP-Codes aus, denen Sie eine Queue zuweisen wollen.
- **Queue**
  Wählen Sie aus der Klappliste die Weiterleitungs-Warteschlange (Sendepriorität) aus, welcher dem Bereich von DSCP-Codes zugeordnet wird.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, werden den DSCP-Codes im angegebenen Bereich die gewählte Weiterleitungs-Warteschlange (Sendepriorität) zugewiesen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **DSCP**
  Zeigt die DSCP-Priorität der eingehenden Frames an.
- **Queue**
  Wählen Sie aus der Klappliste die Queue aus, die der DSCP-Priorität zugeordnet wird. Je höher die Queue-Nummer desto höher die Abarbeitungspriorität.

Die DSCP-Prioritäten sind den Queues standardmäßig wie folgt zugeordnet:

DSCP-Codes	Geräte mit 4 Queues
0 - 15	Queue 1
16 - 31	Queue 2
32 - 47	Queue 3
48 - 63	Queue 4

DSCP-Codes	Geräte mit 8 Queues
0 - 7	Queue 2
8 - 15	Queue 1
16 - 23	Queue 3
24 - 31	Queue 4
32 - 39	Queue 5
40 - 47	Queue 6
48 - 55	Queue 7
56 - 63	Queue 8

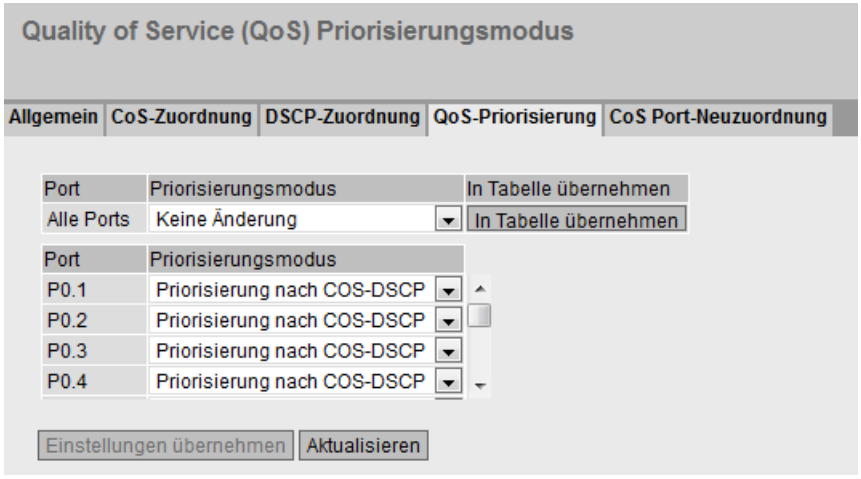
Vorgehensweise zur Konfiguration

1. Wählen Sie zu jedem Wert der Spalte "DSCP" mithilfe der Klappliste "Queue" die Warteschlange aus.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.2.4 QoS-Priorisierung

Festlegen der Priorität

Auf dieser Seite können Sie portgranular einstellen, nach welchem Verfahren weiterzuleitende Frames priorisiert werden.



Beschreibung der angezeigten Werte

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Port**
  Zeigt an, dass die Einstellung für alle Ports der Tabelle 2 gültig ist.
- **Priorisierungsmodus**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellmöglichkeiten haben Sie:
  - Portpriorisierung
  - Priorisierung nach COS
  - Priorisierung nach DSCP
  - Priorisierung nach COS-DSCP
  - Keine Änderung
    Tabelle 2 bleibt unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die konfigurierbaren Ports an.
  Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Priorisierungsmodus**
  Wählen Sie aus der Klappliste den gewünschten Modus:

  Hinweis

  Die Priorisierung des Empfangsports konfigurieren Sie auf der Seite "Layer 2 > VLAN > Port-basiertes VLAN".

  Die Zuordnung der folgenden Prioritäten zu einer Queue konfigurieren Sie auf der Seite "Layer 2 > QoS > CoS-Zuordnung":

  - Empfangsport
  - VLAN-Tag
  - Broadcast- und Agent-Frame

  Die Zuordnung der DSCP-Priorisierung zu einer Queue konfigurieren Sie auf der Seite "Layer 2 > QoS > DSCP-Zuordnung".

  – Portpriorisierung
  Der Switch sortiert ankommende Frames entsprechend der Priorisierung des Empfangsports in eine Queue ein.
  Wenn ein DSCP-Wert im IP-Header vorhanden ist, wird dieser nicht berücksichtigt.
  Wenn ein VLAN-Tag vorhanden ist, wird dessen Prioritätswert durch den Prioritätswert des Empfangsports ersetzt.

  – Priorisierung nach COS
  Wenn ein ankommendes Frame ein VLAN-Tag enthält, sortiert der Switch es entsprechend dieser Priorisierung in eine Queue ein.
  Wenn das Frame kein VLAN-Tag enthält, sortiert der Switch das Frame entsprechend der Priorisierung des Empfangsports in eine Queue ein.
  Wenn ein DSCP-Wert im IP-Header vorhanden ist, wird dieser nicht berücksichtigt.

  – Priorisierung nach DSCP
  Wenn ein ankommendes Frame eine DSCP-Priorisierung enthält, sortiert der Switch es entsprechend dieser Priorisierung in eine Queue ein.
  Wenn das Frame keine DSCP-Priorisierung enthält, sortiert der Switch das Frame entsprechend der Priorisierung des Empfangsports in eine Queue ein.
  Wenn das Frame ein VLAN-Tag enthält, wird dieses nicht berücksichtigt.

  – Priorisierung nach COS-DSCP
  Bei einem ankommenden Frame wird sequenziell geprüft, welche Priorisierung es enthält.
  Wenn das Frame eine DSCP-Priorisierung enthält, wird es wie im Modus "Priorisierung nach DSCP" behandelt.
  Wenn das Frame keine DSCP-Priorisierung enthält, prüft der Switch, ob das Frame ein VLAN-Tag enthält. Wenn es ein VLAN-Tag enthält, sortiert der Switch es entsprechend dieser Priorisierung in eine Queue ein.
  Wenn das Frame weder eine DSCP-Priorisierung noch ein VLAN-Tag enthält, sortiert der Switch das Frame entsprechend der Priorisierung des Empfangsports in eine Queue ein.

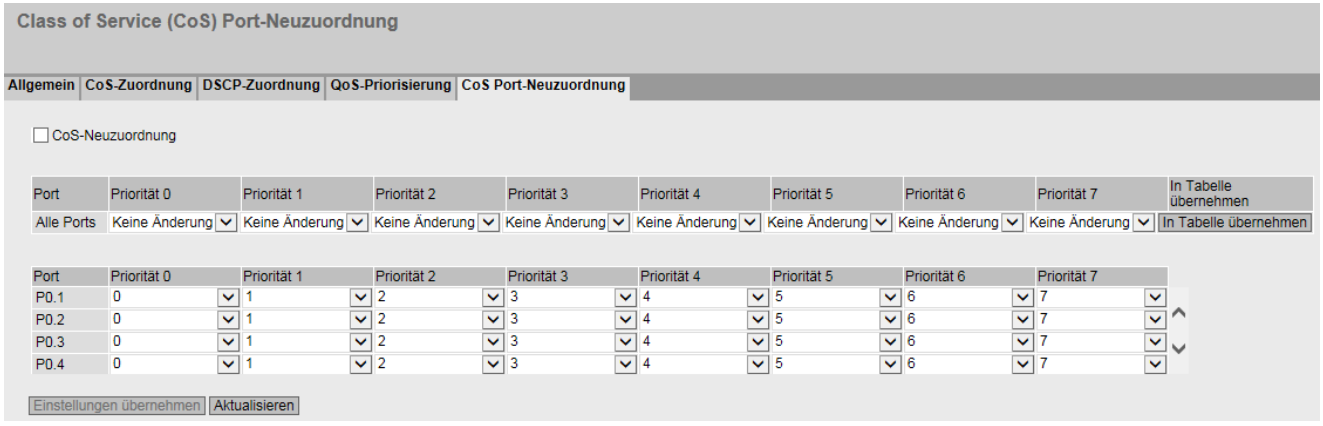
Vorgehensweise zur Konfiguration

1. Wählen Sie aus der Klappliste den gewünschten Priorisierungsmodus aus.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.2.5 CoS Port-Neuzuordnung

Priorität beim Versenden ändern

Auf dieser Seite können Sie abhängig von der Priorität beim Empfangen eines Frames, die Priorität ändern, mit der es versendet wird. Die neue Priorität wirkt sich nur auf folgende Geräte aus, die das Frame empfangen.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **CoS-Neuzuordnung**
  Aktivieren oder deaktivieren Sie, dass Frames mit geänderten Prioritäten entsprechend Tabelle 2 versendet werden.

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Port**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Priorität 0 - 7**
  Die Priorität der Spalte steht für die Priorität, mit der ein Frame empfangen wird.
  - 0 - 7
    Wählen Sie die Priorität aus, mit der ein Frame versendet werden soll.
  - Keine Änderung
    Keine Änderung in Tabelle 2.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt alle verfügbaren Ports an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Priorität 0 - 7**
  Die Priorität der Spalte steht für die Priorität, mit der ein Frame empfangen wird. Wählen Sie in der Klappliste die Priorität aus, mit der ein Frame versendet werden soll.

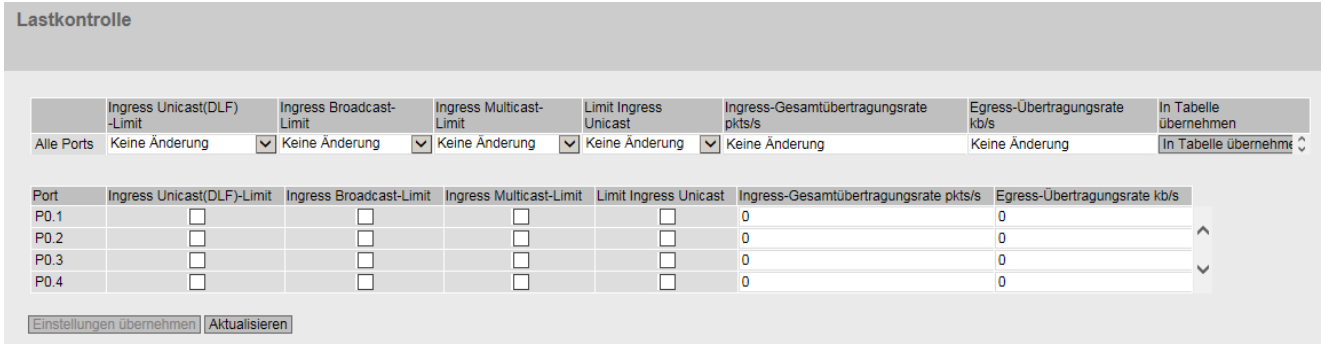
Vorgehensweise zur Konfiguration

1. Aktivieren Sie das Optionskästchen "CoS-Neuzuordnung".
2. Wählen Sie mithilfe der Klapplisten zu jeder Empfangspriorität pro Port die Priorität für das Versenden aus.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.3 Lastkontrolle

Begrenzung der Transferrate eingehender und ausgehender Daten

Auf dieser Seite konfigurieren Sie die Lastbegrenzung für die einzelnen Ports. Sie können festlegen, für welche Kategorie von Telegrammen diese Grenzwerte gelten sollen.



Beschreibung der angezeigten Werte

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports gültig sind.
- **Ingress Unicast(DLF)-Limit / Ingress Broadcast-Limit / Ingress Multicast-Limit / Ingress Unicast-Limit**
  Wählen Sie in der Klappliste die gewünschte Einstellung aus.
  - Aktiviert: Aktiviert die Funktion.
  - Deaktiviert: Deaktiviert die Funktion
  - Keine Änderung: Einstellung in der Tabelle 2 bleibt unverändert
- **Ingress-Gesamtübertragungsrate kb/s**
  Legen Sie die Datenrate für alle eingehenden Telegramme fest. Wenn "Keine Änderung" eingetragen ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **Egress-Übertragungsrate kb/s**
  Legen Sie die Datenrate für alle ausgehenden Telegramme fest. Wenn "Keine Änderung" eingetragen ist, bleibt der Eintrag in der Tabelle 2 unverändert
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, werden die Einstellungen für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt alle verfügbaren Ports an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Ingress Unicast (DLF)-Limit**
  Aktivieren oder deaktivieren Sie die Datenrate zur Begrenzung der eingehenden Unicast-Telegramme mit nicht auflösbarer Adresse (Destination Lookup Failure).
- **Ingress Broadcast-Limit**
  Aktivieren oder deaktivieren Sie die Datenrate zur Begrenzung der eingehenden Broadcast-Telegramme.
- **Ingress Multicast-Limit**
  Aktivieren oder deaktivieren Sie die Datenrate zur Begrenzung der eingehenden Multicast-Telegramme.
- **Ingress Unicast-Limit**
  Aktivieren oder deaktivieren Sie die Datenrate zur Begrenzung der eingehenden Unicast-Telegramme mit auflösbarer Adresse.

- **Ingress-Gesamtübertragungsrate kb/s**
  Legen Sie die Datenrate für alle eingehenden Telegramme fest.
- **Egress-Übertragungsrate kb/s**
  Legen Sie die Datenrate für alle ausgehenden Telegramme fest.

Hinweis

Rundung der Werte, Abweichung vom Sollwert

Beachten Sie bei der Eingabe, dass das WBM auf korrekte Werte rundet.

Sind Werte für die Ingress-Gesamtübertragungsrate und die Egress-Übertragungsrate konfiguriert, können die tatsächlichen Werte im Betrieb leicht von den eingestellten Werten abweichen.

Vorgehensweise zur Konfiguration

1. Tragen Sie in der Zeile des zu konfigurierenden Ports die entsprechenden Werte in die Spalten "Ingress-Gesamtübertragungsrate" und "Egress-Übertragungsrate" ein.
2. Um die Begrenzung für die eingehenden Telegramme zu verwenden, aktivieren Sie in der Zeile die Optionskästchen. Für die ausgehenden Telegramme wird der Wert in der Spalte "Egress-Übertragungsrate" verwendet.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.4 VLAN

5.5.4.1 Allgemein

VLAN-Konfigurationsseite

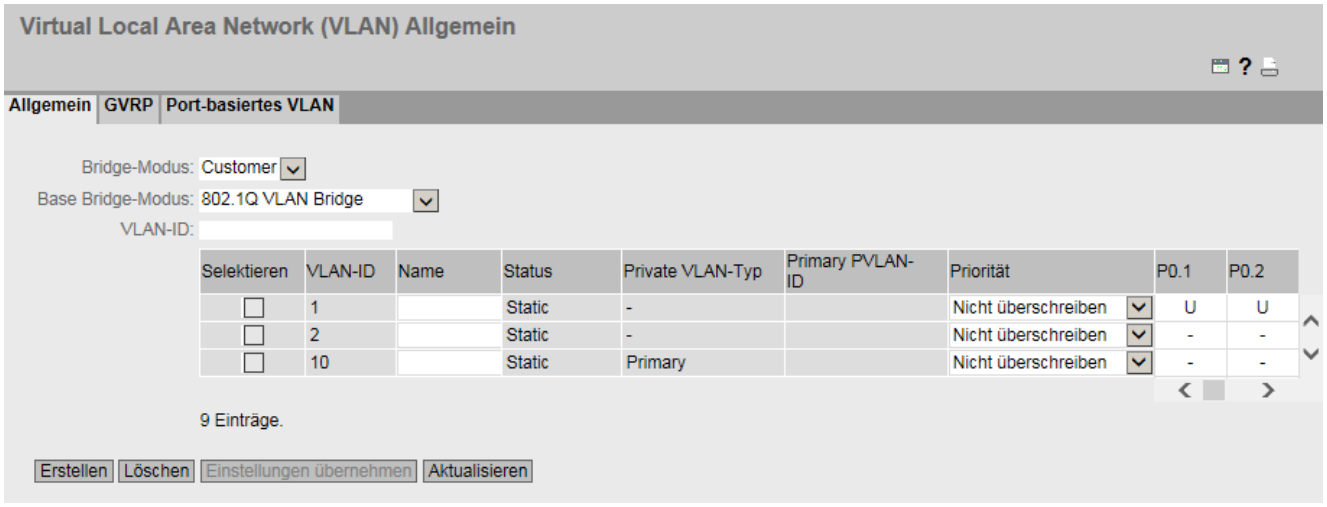
Auf dieser Seite legen Sie fest, ob das Gerät Telegramme mit VLAN-Tags transparent weiterleitet (IEEE 802.1D/VLAN-unaware-Modus) oder VLAN-Informationen berücksichtigt (IEEE 802.1Q/VLAN-aware-Modus). Wenn sich das Gerät im Modus "802.1Q VLAN Bridge" befindet, können Sie VLANs definieren und die Verwendung der Ports festlegen.

Die Einstellmöglichkeiten auf dieser Seite sind abhängig davon, was Sie im Feld "Base Bridge-Modus" auswählen.

Hinweis

Ändern der Agent VLAN ID

Wenn der Konfigurations-PC direkt über Ethernet mit dem Gerät verbunden ist und Sie die Agent VLAN-ID ändern, ist nach der Änderung das Gerät über Ethernet nicht mehr erreichbar.


Virtual Local Area Network (VLAN) Allgemein
Allgemein
GVRP
Port-basiertes VLAN
Bridge-Modus: Customer
Base Bridge-Modus: 802.1Q VLAN Bridge
VLAN-ID:
Selektieren
VLAN-ID
Name
Status
Private VLAN-Typ
Primary PVLAN-ID
Priorität
P0.1
P0.2
1 Static - Nicht überschreiben U U
2 Static - Nicht überschreiben - -
10 Static Primary Nicht überschreiben - -
9 Einträge.
Erstellen
Löschen
Einstellungen übernehmen
Aktualisieren

Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Bridge-Modus**
  Wählen Sie die Rolle des Geräts. Folgende Rollen gibt es:
  - Customer
    Wenn Sie das Gerät mit der Rolle "Customer" betreiben, verhält es sich wie ein Standard-IE-Switch.
  - Provider
    Wenn Sie das Gerät mit der Rolle "Provider" betreiben, verfügt es zusätzlich zu den Eigenschaften der Rolle "Customer" über die Möglichkeit, äußere VLAN-Tags zu verwalten. In dieser Rolle können Sie die Funktion Q-in-Q VLAN-Tunnel verwenden.

    Hinweis

    Die Rolle Provider hat folgende Auswirkung auf den VLAN-Tag: Alle Datenpakete, die nicht von einem Access-Port versendet werden, erhalten ein VLAN-Tag. Wenn die VLAN-Konfiguration der übrigen Geräte nicht entsprechend angepasst wird, können Netzwerkschleifen entstehen oder Netzsegmente nicht mehr erreichbar sein.

- **Base Bridge-Modus**

  Hinweis

  Base Bridge-Modus wechseln

  Beachten Sie den Abschnitt "Base Bridge-Modus wechseln" in diesem Kapitel. Der Abschnitt beschreibt, wie sich ein Wechsel auf die bestehende Konfiguration auswirkt.

  Wählen Sie aus der Klappliste den gewünschten Modus aus. Folgende Modi sind möglich:
  - 802.1Q VLAN Bridge
    Stellt bei dem Gerät den Modus "VLAN-aware" ein. In diesem Modus werden VLAN-Informationen berücksichtigt.
  - 802.1D Transparent Bridge
    Stellt bei dem Gerät den Modus "VLAN-unaware" ein. In diesem Modus werden VLAN-Tags nicht verändert, sondern transparent weitergeleitet. Die VLAN-Priorität wird für CoS ausgewertet. Sie können in diesem Modus keine VLANs anlegen. Es ist nur ein Management-VLAN verfügbar: VLAN 1.
- **VLAN-ID**
  Tragen Sie im Eingabefeld "VLAN-ID" die VLAN-ID ein.
  Wertebereich: 1 ... 4094

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **VLAN-ID**
  Zeigt die VLAN-ID an. Die VLAN-ID (eine Zahl zwischen 1 und 4094) kann nur beim Anlegen eines neuen Datensatzes einmalig vergeben werden und ist danach nicht mehr änderbar. Zur Änderung muss der gesamte Datensatz gelöscht und neu angelegt werden.

- **Name**
  Tragen Sie einen Namen für das VLAN ein. Der Name hat nur informativen Charakter und keine Auswirkungen auf die Konfiguration.
  Länge: max. 32 Zeichen
- **Status**
  Zeigt die Statusart des Eintrags in der internen Portfiltertabelle an. Dabei bedeutet "Static", dass das VLAN vom Anwender statisch eingetragen wurde.
- **Private VLAN-Typ**
  Zeigt den Typ des PVLANs an.
- **Primary VLAN-ID**
  Zeigt bei Secondary PVLANs die ID des dazugehörigen Primary PVLANs an.
- **Priorität**
  Wählen Sie eine Priorität, die für das VLAN erzwungen werden soll. In alle eingehenden Frames dieses VLANs wird die gewählte Priorität eingetragen. Die Frames werden gemäß der gewählten Priorität vom Switch weiterverarbeitet, unabhängig von der Port-Priorität oder der Priorisierung bei ungetaggten Frames. Die im Frame enthaltenen VLAN-Tags werden nicht geändert.
  Wenn Sie "Nicht überschreiben" auswählen, bleibt die Priorität der Frames unverändert. Die Frames werden entsprechend der Port-Priorität oder des VLAN-Tags priorisiert.
- **Liste der Ports**
  Legen Sie die Verwendung der Ports fest. Folgende Möglichkeiten gibt es:
  - "-"
    Der Port ist kein Mitglied des angegebenen VLANs.
    Bei der Neudefinition sind alle Ports mit der Kennung "-" belegt.
  - M
    Der Port ist Mitglied des VLANs. In diesem VLAN gesendete Telegramme werden mit dem entsprechenden VLAN-Tag weitergeleitet.
  - R
    Der Port ist Mitglied des VLANs. Die Registrierung erfolgt über ein GVRP-Telegramm.
  - U (Großbuchstabe)
    Der Port ist ungetaggtes Mitglied des VLANs. In diesem VLAN gesendete Telegramme werden ohne VLAN-Tag weitergeleitet. Von diesem Port werden Telegramme ohne VLAN-Tag gesendet.
  - u (Kleinbuchstabe)
    Der Port ist ungetaggtes Mitglied des VLANs, jedoch ist das VLAN nicht als Port-VLAN konfiguriert. In diesem VLAN gesendete Telegramme werden ohne VLAN-Tag weitergeleitet.
  - F
    Der Port ist kein Mitglied des angegebenen VLANs und kann kein Mitglied dieses VLAN werden, auch dann nicht, wenn er als Trunk-Port konfiguriert wird.
  - T
    Diese Option wird nur angezeigt und kann im WBM nicht ausgewählt werden.
    Dieser Port ist Trunk-Port und wurde dadurch Mitglied in allen VLANs.

Base Bridge-Modus wechseln

VLAN-unaware (802.1D Transparent Bridge) → VLAN-aware (802.1Q VLAN Bridge)

Wenn Sie den Base Bridge-Modus von VLAN-unaware in VLAN-aware ändern, hat dies folgende Auswirkungen:

- Alle statischen und dynamischen Unicast-Einträge werden gelöscht.
- Alle statischen und dynamischen Multicast-Einträge werden gelöscht.
- Bei Spanning Tree können Sie die folgende Protokollkompatibilität einstellen: STP, RSTP und MSTP.

VLAN-aware (802.1Q VLAN Bridge) → VLAN-unaware (802.1D Transparent Bridge)

Wenn Sie den Base Bridge-Modus von VLAN-aware in VLAN-unaware ändern, hat dies folgende Auswirkungen:

- Alle VLAN-Konfigurationen werden gelöscht.
- Es wird ein Management-VLAN angelegt: VLAN 1.
- Alle statischen und dynamischen Unicast-Einträge werden gelöscht.
- Alle statischen und dynamischen Multicast-Einträge werden gelöscht.
- Bei Spanning Tree können Sie die folgende Protokollkompatibilität einstellen: STP und RSTP.
- Sie können GVRP nicht nutzen.
- Sie können Guest VLAN nicht nutzen.
- Die VLAN-Zuordnung kann nicht vom RADIUS-Server übernommen werden.
- Sie können den Port-Typ nicht konfigurieren.
- Definierte Zugriffsregeln müssen für alle VLANs gültig sein. Auf der Seite "Security > Management ACL" muss für den Parameter "Zulässige VLANs" der Wert "1-4094" definiert sein.

802.1Q VLAN Bridge: Wichtige Regeln für VLANs

Berücksichtigen Sie bei der Konfiguration und beim Betrieb Ihrer VLANs folgende Regeln:

- Telegramme mit der VLAN-ID "0" werden wie ungetaggte Telegramme behandelt, behalten jedoch ihren Prioritätswert.
- Alle Ports am Gerät senden standardmäßig Telegramme ohne VLAN-Tag, um sicher zu gehen, dass der Endteilnehmer diese Telegramme empfangen kann.
- Bei SCALANCE X-Geräten ist an allen Ports die VLAN-ID "1" voreingestellt.
- Wenn an einem Port ein Endteilnehmer angebunden ist, dann sollen ausgehende Telegramme ohne Tag versendet werden (statischer Zugriffs-Port). Wenn sich an dem Port ein weiterer Switch befindet, so ist das Telegramm mit einem Tag zu versehen (Trunk-Port).

Vorgehensweise zur Konfiguration

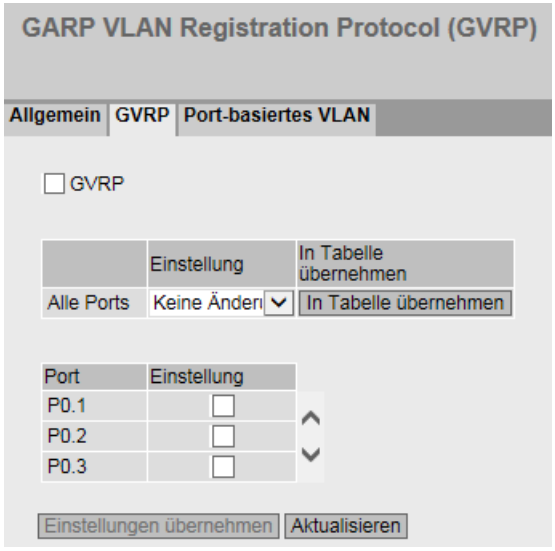
1. Wenn "802.1Q VLAN Bridge" nicht eingestellt ist, wählen Sie in der Klappliste "Base Bridge-Modus" den Eintrag "802.1Q VLAN Bridge" aus. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
2. Tragen Sie im Eingabefeld "VLAN-ID" eine ID ein.
3. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt. Die Felder sind standardmäßig mit "-" belegt.
4. Tragen Sie ggf. einen Namen für das VLAN ein.
5. Legen Sie die Verwendung der Ports in dem VLAN fest. Wenn Sie z. B. "M" auswählen, ist der Port Mitglied des VLANs. In diesem VLAN gesendete Telegramme werden mit dem entsprechenden VLAN-Tag weitergeleitet.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.4.2 GVRP

Konfiguration der GVRP-Funktion

Über ein GVRP-Telegramm kann sich ein anderes Gerät am Port des Geräts für eine bestimmte VLAN-ID registrieren. Ein anderes Gerät kann z. B. ein Endteilnehmer oder ein Switch sein. Das Gerät kann außerdem GVRP-Telegramme über diesen Port senden.

Auf dieser Seite können Sie jeden Port für die GVRP-Funktionalität aktivieren.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **GVRP**
  Aktivieren oder deaktivieren Sie die Funktion "GVRP".

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - Aktiviert
    Aktiviert das Senden von GVRP-Telegrammen.
  - Deaktiviert
    Deaktiviert das Senden von GVRP-Telegrammen.
  - Keine Änderung
    Keine Änderung in Tabelle 2.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt alle verfügbaren Ports an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Einstellung**
  Aktivieren oder deaktivieren Sie das Senden von GVRP-Telegrammen.

Vorgehensweise zur Konfiguration

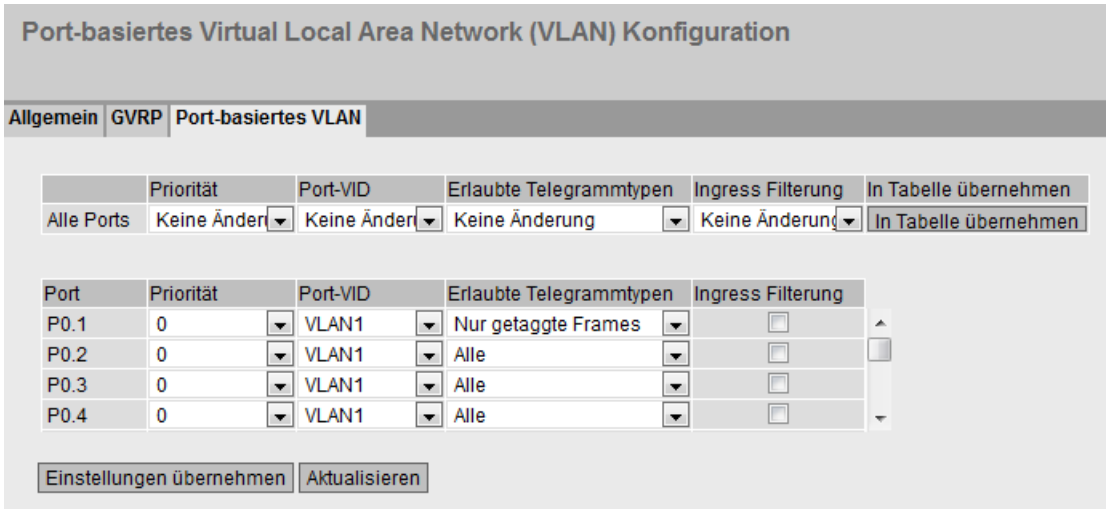
1. Klicken Sie in das Optionskästchen "GVRP".
2. Klicken Sie in das Optionskästchen hinter jedem Port in der Spalte "Einstellung", um GVRP für diesen Port zu aktivieren oder zu deaktivieren.
   Wiederholen Sie den Vorgang für jeden Port, für den Sie die Funktion freischalten oder sperren wollen.
3. Klicken sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.4.3 Port-basiertes VLAN

Verarbeitung empfangener Telegramme

Auf dieser Seite legen Sie die Konfiguration der Port-Eigenschaften für den Telegrammempfang fest.

Sie können die Einstellungen auf dieser Seite nur dann konfigurieren, wenn Sie auf dem Reiter "Allgemein" zuvor den "Base Bridge-Modus" "802.1Q VLAN Bridge" ausgewählt haben.



Beschreibung der angezeigten Felder

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports gültig sind.
- **Priorität / Port-VID / Erlaubte Telegrammtypen / Ingress Filterung**
  Wählen Sie in der Klappliste die Einstellung aus. Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Priorität**
  Die CoS-Priorität (Class of Service), die in einem VLAN-Tag verwendet wird. Wird ein Telegramm ohne Tag empfangen, wird ihm diese Priorität zugeordnet. Die Priorität legt fest, wie dieses Telegramm im Vergleich zu anderen Telegrammen weiterhin bearbeitet wird.
  Es gibt insgesamt acht Prioritäten, mit den Werten 0 bis 7, wobei 7 der höchsten Priorität entspricht (IEEE 802.1P Port Priority).
  Wählen Sie aus der Klappliste die Priorität aus, mit der ungetaggte Telegramme versehen werden.
- **Port-VID**
  Wählen Sie aus der Klappliste die VLAN-ID aus. Nur die VLAN-IDs sind wählbar, die Sie auf der Seite "VLAN > Allgemein" definiert haben.
  Wenn ein empfangenes Telegramm kein VLAN-Tag hat, so wird es um ein Tag mit der hier angegebenen VLAN-ID ergänzt und entsprechend den Regeln am Port gesendet.

- **Erlaubte Telegrammtypen**
  Legen Sie fest, welche Arten von Telegrammen akzeptiert werden. Es gibt folgende Alternativen:
  - Nur getaggte Frames
    Das Gerät verwirft alle ungetaggten Telegramme. Andernfalls gelten die Weiterleitungsregeln entsprechend der Konfiguration.
  - Alle
    Das Gerät leitet alle Telegramme weiter.
  - Nur ungetaggte und mit Priorität getaggte Frames
    Das Gerät verwirft alle getaggten Telegramme. Das Gerät leitet alle ungetaggten Telegramme sowie Telegramme mit einer Priorität (Priority Tagged Frames) weiter. Andernfalls gelten die Weiterleitungsregeln entsprechend der Konfiguration.
    Wenn Sie den Bridge-Modus "Provider" konfiguriert haben, bedeutet diese Einstellung für das Gerät, dass es alle eingehenden Telegramme als ungetaggte Telegramme behandelt.
- **Ingress Filterung**
  Legen Sie fest, ob die VID von empfangenen Telegrammen ausgewertet wird.
  Sie haben folgende Möglichkeiten:
  - Aktiviert
    Die VLAN-ID empfangener Telegramme bestimmt die Weiterleitung: Für die Weiterleitung eines VLAN-getaggten Telegramms muss der Empfangsport Mitglied im selben VLAN sein. Am Empfangsport werdenTelegramme aus unbekannten VLANs verworfen.
  - Deaktiviert
    Alle Telegramme werden weitergeleitet.

Vorgehensweise zur Konfiguration

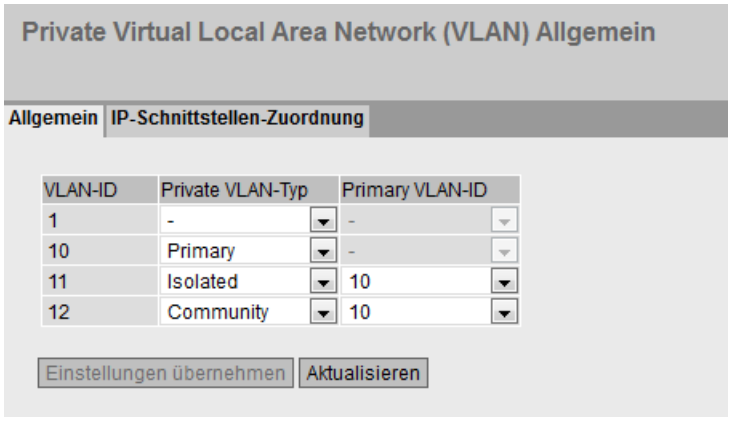
1. Klicken Sie in der Zeile des zu konfigurierenden Ports in das entsprechende Feld der Tabelle, um es zu konfigurieren.
2. Tragen Sie in die Eingabefelder die einzustellenden Werte ein.
3. Wählen Sie aus den Klapplisten die einzustellenden Werte aus.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.5 Private VLAN

5.5.5.1 Allgemein

Private VLAN-Konfigurationsseite

Auf dieser Seite definieren Sie die Typen der PVLANs und ordnen Secondary PVLANs einem Primary PVLAN zu.



Beschreibung der angezeigten Felder

Die Tabelle gliedert sich in folgende Spalten:

- **VLAN-ID**
  Zeigt die VLAN-ID an.
- **Private VLAN-Typ**
  Legen Sie den Typ des PVLANs fest:
  - -
    Diese VLANs sind keine Private VLANs.
  - Primary
    Mit diesem Typ definieren Sie ein Primary PVLAN. Sie können in einem PVLAN nur ein Primary PVLAN definieren. Das Primary PVLAN verwendet die VLAN-ID des VLANs.
  - Isolated
    Mit diesem Typ definieren Sie ein Secondary PVLAN. Geräte innerhalb eines Isolated Secondary PVLANs können nicht über Layer 2 miteinander kommunizieren. Das Secondary PVLAN hat eine spezifische VLAN-ID.
  - Community
    Mit diesem Typ definieren Sie ein Secondary PVLAN. Die Geräte in diesem Secondary PVLAN können über Layer 2 miteinander kommunizieren. Das Secondary PVLAN hat eine spezifische VLAN-ID.
- **Primary VLAN-ID**
  Wählen Sie bei Secondary PVLANs die VLAN-ID des Primary PVLANs aus.

Vorgehensweise zur Konfiguration

1. Legen Sie die gewünschten VLANs an, auf der Seite "Layer 2 > VLAN > Allgemein".

   Hinweis

   Auf allen IE-Switches eines PVLANs müssen alle Secondary PVLANs bekannt sein. Auch wenn ein IE-Switch keinen Host-Port in einem Secondary PVLAN hat, muss das Secondary PVLAN auf dem IE-Switch bekannt sein.

2. Wechseln Sie auf die Seite "Layer 2 > Private VLAN> Allgemein". Dort wird für jedes VLAN eine Zeile angelegt.
3. Legen Sie auf dieser Seite den "Private VLAN-Typ" fest.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
5. Geben Sie bei den Secondary PVLANs das zugehörige Primary PVLAN an.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
7. Wählen Sie bei den gewünschten Ports den entsprechenden Port-Typ aus, auf der Seite "System > Ports > Konfiguration":
   - Switch-Port PVLAN Promiscuous
   - Switch-Port PVLAN Host
8. Legen Sie die Verwendung der Ports fest, auf der Seite "Layer 2 > VLAN > Allgemein".
   - Wählen Sie für Promiscuous-Ports, die mit einem anderen Promiscuous-Port verbunden sind, in allen PVLANs die Einstellung "M" aus.
   - Wählen Sie für Promiscuous-Ports, die mit einem Endgerät verbunden sind, in allen PVLANs die Einstellung "u" (Kleinbuchstabe) aus.
     Im Primary PVLAN wird die Einstellung nach dem Speichern automatisch in "U" (Großbuchstabe) geändert.
   - Wählen Sie für Host-Ports im Primary PVLAN und in seinem Secondary PVLAN die Einstellung "u" (Kleinbuchstabe) aus.
     In seinem Secondary PVLAN wird die Einstellung nach dem Speichern automatisch in "U" (Großbuchstabe) geändert.

   Bei ankommenden ungetaggten Frames wird die Port-VLAN-ID des VLANs gesetzt, in dem der Port mit der Einstellung "U" (Großbuchstabe) eingetragen ist.

5.5.5.2 IP-Schnittstellen-Zuordnung

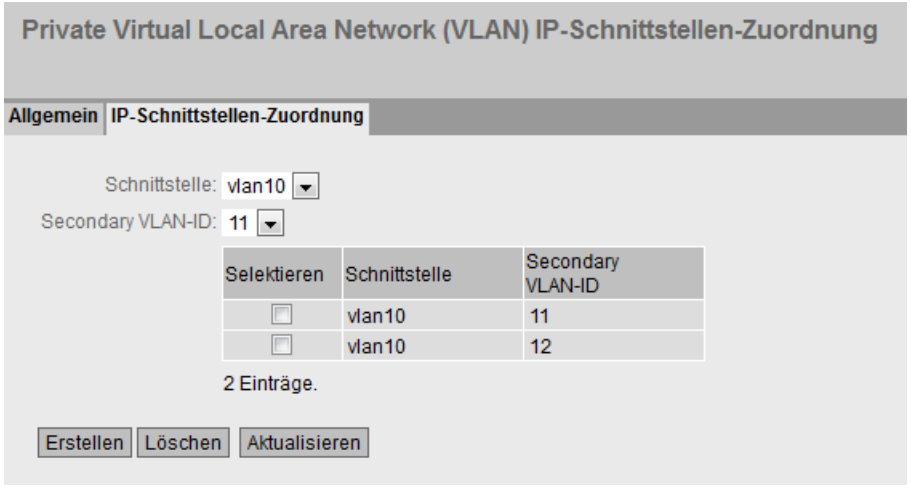
Private VLAN-Konfigurationsseite

Auf dieser Seite legen Sie fest, aus welchen Secondary PVLANs die IP-Schnittstelle des Primary PVLANs erreichbar sein soll.

Konfigurieren Sie die IP-Schnittstellen-Zuordnung für alle Funktionen, bei denen ein Endgerät aus dem Secondary PVLAN über die IP-Schnittstelle des Primary PVLANs kommunizieren muss.

Beispiele:

- Ein Endgerät im Secondary PVLANs ist als DHCP-Client konfiguriert. Es ist ein Remote DHCP-Server eingerichtet. Ein PVLAN-Switch ist als DHCP Relay Agent konfiguriert. Konfigurieren Sie eine IP-Schnittstelle im Primary PVLAN des DHCP Relay Agents. Ordnen Sie die Secondary PVLANs, in denen sich DHCP-Clients befinden, dieser IP-Schnittstelle zu.
- Ein PVLAN-Switch ist als Router konfiguriert. Konfigurieren Sie eine IP-Schnittstelle im Primary PVLAN des Routers. Ordnen Sie die Secondary PVLANs dieser IP-Schnittstelle zu, in denen sich Endgeräte befinden, die den Router als Gateway verwenden.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Schnittstelle**
  Wählen Sie das Primary PVLAN mit einer IP-Schnittstelle aus.
- **Secondary VLAN-ID**
  Wählen Sie ein Secondary VLAN-ID aus, aus dem die IP-Schnittstelle des Primary PVLANs erreichbar sein soll.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Schnittstelle**
  Zeigt die IP-Schnittstelle an.
- **Secondary VLAN-ID**
  Zeigt die Secondary VLAN-ID des Secondary PVLANs an, aus dem die IP-Schnittstelle des Primary PVLANs erreichbar ist.

Vorgehensweise zur Konfiguration

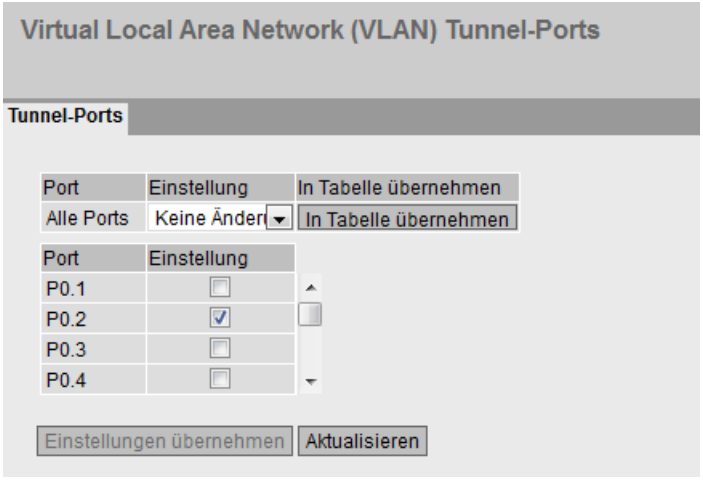
1. Erstellen Sie für das Primary PVLAN eine IP-Schnittstelle.
2. Wählen Sie das Primary PVLAN mit einer IP-Schnittstelle aus.
3. Wählen Sie eine Secondary VLAN-ID aus.
4. Klicken Sie auf die Schaltfläche "Erstellen".

5.5.6 Provider Bridge

5.5.6.1 Tunnel-Ports

Konfigurationsseite für Tunnel-Ports

Auf dieser Seite aktivieren Sie die Funktion Q-in-Q VLAN-Tunnel. Telegramme, die ein Tunnel-Port empfängt, werden um ein äußeres VLAN-Tag, die PVID des Ports, erweitert.



Beschreibung der angezeigten Felder

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - Aktiviert
    Aktiviert die Funktion Q-in-Q VLAN-Tunnel auf allen Ports.
  - Deaktiviert
    Deaktiviert die Funktion Q-in-Q VLAN-Tunnel auf allen Ports.
  - Keine Änderung
    Tabelle 2 bleibt unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, werden die Einstellungen für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt alle verfügbaren Ports an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Einstellung**
  Aktivieren oder deaktivieren Sie die Funktion für diesen Port.

Vorgehensweise zur Konfiguration

Um einen Port als Tunnel-Port zu konfigurieren, gehen Sie wie folgt vor:

1. Wechseln Sie auf die Seite "Layer 2 > VLAN > Allgemein".
2. Konfigurieren Sie den Bridge-Modus "Provider".
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
   Die Layer 2-Porteinstellungen (VLAN, Spanning Tree) werden auf die Werkseinstellungen zurückgesetzt und das Gerät wird neugestartet.
4. Wechseln Sie auf die Seite "Layer 2 > VLAN > Allgemein".
5. Geben Sie die gewünschte VLAN-ID ein.
6. Klicken Sie auf die Schaltfläche "Erstellen".
7. Wechseln Sie auf die Seite "Layer 2 > VLAN > Port-basiertes VLAN".
8. Wählen Sie bei dem Port die Port-VID des erstellten VLANs aus.
9. Wählen Sie für den Port bei "Erlaubte Telegrammtypen" die Einstellung "Nur ungetaggte und mit Priorität getaggte Frames" aus.
10. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
11. Wechseln Sie auf die Seite "Layer 2 > VLAN > Allgemein".

12. Wählen Sie für den Port in dem gewünschten VLAN die Einstellung "U" (Großbuchstabe) aus.
13. Wählen Sie für den Port in allen anderen VLANs die Einstellung "-" aus.
14. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
15. Deaktivieren Sie folgende Protokolle auf dem Port:
    - Auf der Seite "Layer 2 > VLAN > GVRP" das Optionskästchen bei "Einstellung".
    - Auf der Seite "Layer 2 > Spanning Tree > CIST-Port" das Optionskästchen bei "Spanning Tree-Status".
    - Auf der Seite "Layer 2 > Multicast > GMRP" das Optionskästchen bei "Einstellung".
16. Wechseln Sie auf die Seite "System > Ports > Konfiguration".
17. Wählen Sie den gewünschten Port aus.
18. Wählen Sie den Port-Typ "Switch-Port VLAN Access" aus.
19. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
20. Wechseln Sie auf die Seite "Layer 2 > Provider-Bridge > Tunnel-Ports".
21. Aktivieren Sie bei dem gewünschten Port das Optionskästchen.
22. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
    Auf der Seite "Layer 2 > VLAN > Allgemein" wird die Einstellung nach dem Speichern automatisch in "Q" geändert.

5.5.7 Mirroring

5.5.7.1 Allgemein

Auf dieser Seite können Sie die Funktion Mirroring ein- bzw. ausschalten und die Basiseinstellungen vornehmen.

Hinweis

Es kann nicht garantiert werden, dass beim Mirroring des Datenverkehrs alle Pakete gespiegelt werden. Dies ist insbesondere abhängig von der Last auf den gespiegelten Ports und der Anzahl der Sessions. Um die höchste Genauigkeit zu erzielen, wird die Begrenzung auf eine Session empfohlen.

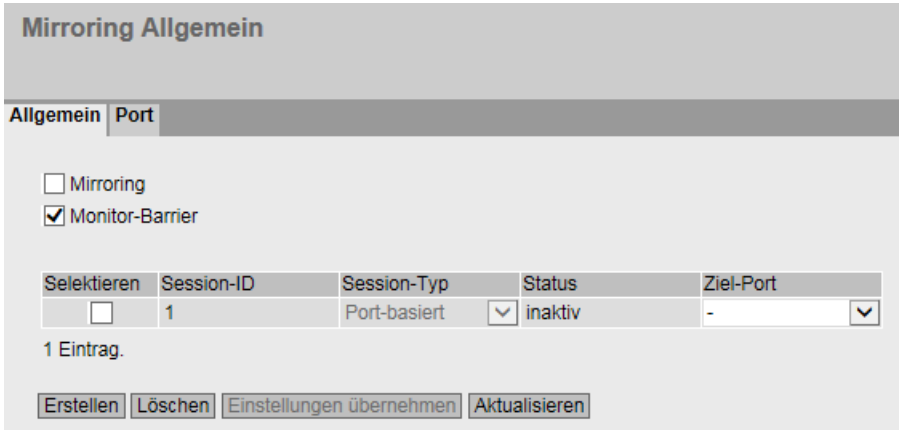
Datenrate beachten

Wenn die maximale Datenrate des gespiegelten Ports höher ist als die des Monitor-Ports, kann es zu Datenverlusten kommen und der Monitor-Port gibt nicht mehr die Abläufe am gespiegelten Port wieder. Auf einem Monitor-Port können mehrere Ports gleichzeitig gespiegelt werden.

Mehrere Quell-Ports aus dem gleichen VLAN

Wenn Sie aus einem VLAN mehr als einen Quell-Port für das Port-basierte Egress-Mirroring auswählen, werden unbekannte Unicast- und Multicast-Telegramme sowie Broadcast-Telegramme nur einmal an den Ziel-Port weitergeleitet.

Einstellungen



Die Seite enthält folgende Felder:

- **Mirroring**
  Klicken Sie in dieses Optionskästchen, um das Mirroring zu aktivieren bzw. zu deaktivieren.

  Hinweis

  Sie müssen die Portspiegelung ausschalten, wenn Sie an den Monitor-Port ein normales Endgerät anschließen.

- **Monitor-Barrier**
  Klicken Sie in dieses Optionskästchen, um Monitor-Barrier zu aktivieren bzw. zu deaktivieren.

  Hinweis

  Auswirkungen von Monitor-Barrier

  Wenn Sie diese Option einschalten, ist das Management des Switches über den Monitor-Port nicht mehr erreichbar. Folgende portspezifische Funktionen werden geändert:
  - Die DCP-Weiterleitung wird ausgeschaltet.
  - LLDP wird ausgeschaltet.
  - Unicast-, Multicast- und Broadcast-Blocking werden eingeschaltet.

  Die vorherigen Zustände dieser Funktionen werden nach Beendigung von Monitor-Barrier nicht wieder hergestellt. Sie werden auf die Default-Werte zurückgesetzt und müssen eventuell neu konfiguriert werden.

  Sie können diese Funktionen manuell konfigurieren, auch wenn Monitor-Barrier eingeschaltet ist. Sie erlauben damit aber auch wieder den entsprechenden Datenverkehr auf dem Monitor-Port. Wenn Sie dies nicht wünschen, achten Sie darauf, dass nur der zu beobachtende Datenverkehr auf die Schnittstelle geleitet wird.

  Wird Mirroring ausgeschaltet, dann werden die genannten portspezifischen Funktionen auf die Default-Werte zurückgesetzt. Das Zurücksetzen erfolgt unabhängig davon, ob die Funktionen manuell oder automatisch durch das Einschalten von Monitor-Barrier konfiguriert wurden.

Die Tabelle für die Basiseinstellungen enthält folgende Felder:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Session-ID**
  Die Session-ID wird automatisch vergeben, wenn ein neuer Eintrag angelegt wird. Sie können genau eine Session anlegen.
- **Session-Typ**
  Zeigt die Art der Mirroring-Session an.
- **Status**
  Zeigt an, ob Mirroring aktiv ist.
- **Ziel-Port**
  Wählen Sie aus der Klappliste den Ausgangsport aus, auf den in dieser Session gespiegelt werden soll.

Vorgehensweise

Mirroring-Session anlegen

1. Aktivieren Sie Mirroring.
2. Klicken Sie auf die Schaltfläche "Erstellen", um in der Tabelle einen Eintrag anzulegen. Die Session-ID wird dabei automatisch vergeben.
3. Wählen Sie einen Zielport aus.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen", um die gewählten Einstellungen zu speichern und zu aktivieren.
5. Wechseln Sie zu dem folgenden Reiter, um zu der Session-ID weitere Detaileinstellungen vorzunehmen.

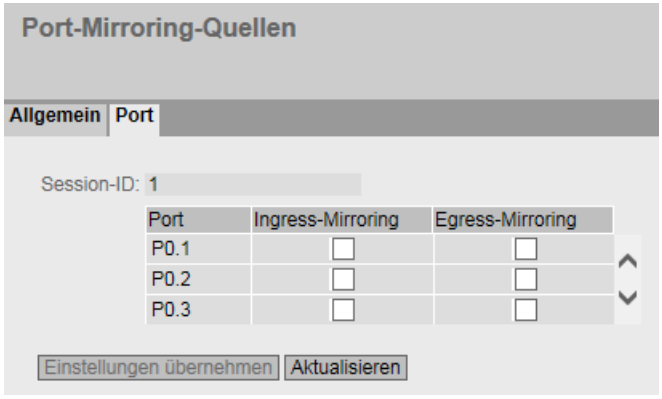
Mirroring-Session löschen

1. Klicken Sie in der ersten Spalte in das Optionskästchen, um die Zeile zu markieren.
2. Klicken Sie auf die Schaltfläche "Löschen", um die markierte Zeile zu löschen.

5.5.7.2 Port

Ports spiegeln

Sie können die Einstellungen auf dieser Seite nur dann konfigurieren, wenn auf dem Register "Allgemein" zuvor eine Session-ID mit dem Session-Type "Port-basiert" erzeugt wurde.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Session-ID**
  Zeigt die Session an.
- **Port**
  Zeigt alle verfügbaren Ports an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.

- **Ingress-Mirroring**
  Aktivieren oder deaktivieren Sie am gewünschten Port das Mithören der eingehenden Pakete.
- **Egress-Mirroring**
  Aktivieren oder deaktivieren Sie am gewünschten Port das Mithören der ausgehenden Pakete.

Hinweis

Mirroring bei Ring-Ports

Wenn Sie bei einem Ring-Port die Funktion Mirroring aktivieren, sendet der Ring-Port Testframes, selbst wenn er sich im Zustand "link down" befindet.

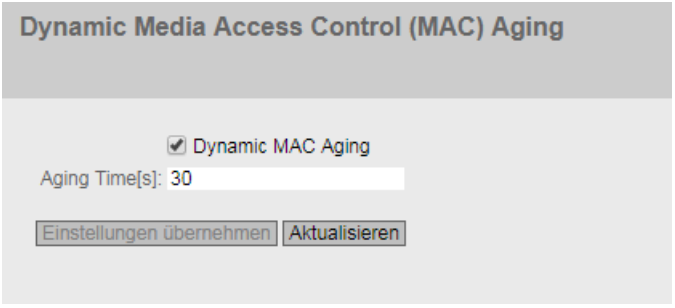
Vorgehensweise zur Konfiguration

1. Klicken Sie in der Tabelle in die Optionskästchen der Zeile hinter dem zu spiegelnden Port. Wählen Sie dabei aus, ob Sie eingehende oder ausgehende Pakete mithören wollen. Zum Mithören des gesamten Datenverkehrs eines Ports müssen Sie beide Optionskästchen markieren.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.8 Dynamic MAC Aging

Protokolleinstellungen und Switch-Funktionalität

Das Gerät lernt automatisch die Quelladressen der angeschlossenen Teilnehmer. Diese Information wird dazu benutzt, um Datentelegramme gezielt an die betroffenen Teilnehmer weiterzuleiten. Dadurch wird die Netzlast für die anderen Teilnehmer reduziert.
Erhält ein Gerät innerhalb einer bestimmten Zeitspanne kein Telegramm, dessen Quelladresse mit einer gelernten Adresse übereinstimmt, dann löscht es die gelernte Adresse. Dieser Mechanismus wird als "Aging" bezeichnet. Durch Aging wird verhindert, dass Telegramme fehlgeleitet werden, wenn z.B. ein Endgerät an einen anderen Port angeschlossen wird.
Wenn die Option nicht aktiviert ist, löscht ein Gerät gelernte Adressen nicht automatisch.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Dynamic MAC Aging**
  Aktivieren oder deaktivieren Sie die Funktion zum automatischen Aging von gelernten MAC-Adressen.
- **Aging Time[s]**
  Tragen Sie die Zeitspanne in Sekunden in 15er-Schritten ein. Nach dieser Zeitspanne wird eine gelernte Adresse gelöscht, wenn das Gerät keine weiteren Telegramme von dieser Absenderadresse mehr empfängt.
  Wertebereich: 15 - 630 Sekunden
  Werkseinstellung: 30

Hinweis

Rundungen der Werte, Abweichung vom Sollwert

Beachten Sie bei der Eingabe der Aging Time, dass auf korrekte Werte gerundet wird. Wenn Sie einen Wert eingeben, der nicht durch 15 teilbar ist, wird der Wert automatisch abgerundet.

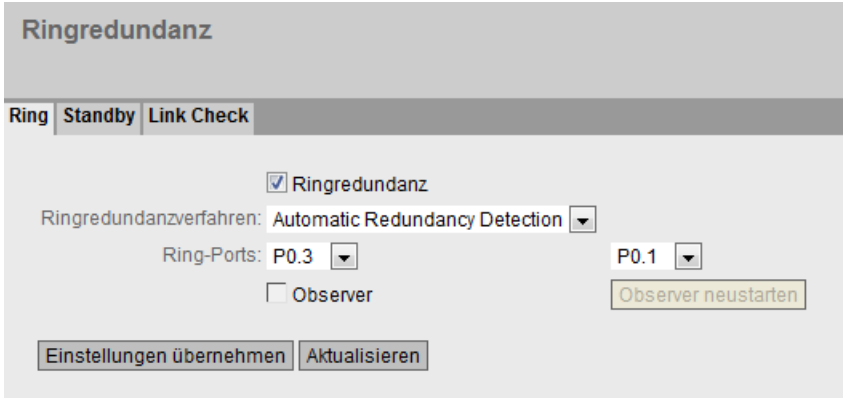
Vorgehensweise zur Konfiguration

1. Aktivieren Sie das Optionskästchen "Dynamic MAC Aging".
2. Tragen Sie in das Eingabefeld "Aging Time[s]" die Zeitspanne in Sekunden ein.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.9 Ringredundanz

5.5.9.1 Ring

Konfiguration der Ringredundanz



- **Ringredundanz**
  Wenn Sie das Optionskästchen "Ringredundanz" aktivieren, schalten Sie die Ringredundanz ein. Es werden die auf dieser Seite eingestellten Ringports verwendet.
- **Ringredundanzverfahren**
  Hier stellen Sie die Betriebsart der Ringredundanz ein.
  Folgende Betriebsarten stehen zur Verfügung:
  - Automatic Redundancy Detection
    Wählen Sie diese Einstellung, um eine automatische Konfiguration der Redundanzbetriebsart vorzunehmen.
    Im Modus "Automatic Redundancy Detection" stellt das Gerät automatisch fest, ob sich ein Gerät mit der Rolle "HRP Manager" im Ring befindet. Ist dies der Fall, so nimmt das Gerät die Rolle "HRP Client" ein.
    Wird kein HRP Manager gefunden, so handeln alle Geräte mit der Einstellung "Automatic Redundancy Detection" oder "MRP Auto-Manager" untereinander aus, welches Gerät die Rolle "MRP Manager" einnimmt. Dabei wird immer das Gerät mit der niedrigsten MAC-Adresse zum "MRP Manager". Die übrigen Geräte stellen sich automatisch auf die Betriebsart "MRP Client" ein.
  - MRP Auto-Manager
    Im Modus "MRP Auto-Manager" handeln die Geräte untereinander aus, welches Gerät die Rolle "MRP Manager" einnimmt. Dabei wird immer das Gerät mit der niedrigsten MAC-Adresse zum "MRP Manager". Die übrigen Geräte stellen sich automatisch auf die Betriebsart "MRP Client" ein.
    Im Gegensatz zur Einstellung "Automatic Redundancy Detection" sind die Geräte nicht in der Lage zu erkennen, ob ein HRP-Manager im Ring ist.

    Hinweis

    MRP-Projektierung in STEP 7

    Wenn Sie über STEP 7 die Rolle "Manager (Auto)" oder "Manager" für das Gerät einstellen, wird auf dieser WBM-Seite in beiden Fällen "MRP Auto-Manager" angezeigt. In der Anzeige im CLI wird zwischen den beiden Rollen unterschieden.

  - MRP-Client
    Das Gerät nimmt die Rolle MRP-Client ein.
  - HRP-Client
    Das Gerät nimmt die Rolle HRP-Client ein.
  - HRP-Manager
    Das Gerät nimmt die Rolle HRP-Manager ein.
    Bei der Projektierung eines HRP-Rings muss ein Gerät als HRP-Manager eingestellt werden. Bei allen übrigen Geräten muss "HRP Client" oder "Automatic Redundancy Detection" eingestellt sein.

- **Ring-Ports**
  Hier stellen Sie die Ports ein, die bei der Ringredundanz als Ringports verwendet werden sollen.
  Der Ringport, den Sie in der linken Klappliste auswählen, ist bei HRP der "Isolated Port".
  Die Werkseinstellung definiert folgende Ring-Ports:

Geräte	Werkseinstellung Ring-Ports
SCALANCE XB208 und XB216	P0.1 und P0.2
SCALANCE XB205-3	P0.7 und P0.8
SCALANCE XB213-3	P0.15 und P0.16
SCALANCE XC206-2SFP, XC206-2SFP G, XC206-2SFP EEC, XC206-2SFP G EEC, XC208, XC208G, XC208EEC, XC208G EEC, XC216, XC216EEC und XC224	P0.1 und P0.2
SCALANCE XC206-2	P0.7 und P0.8
SCALANCE XF-200BA	P1.1 und P2.1
SCALANCE XP208	P0.1 und P0.2
SCALANCE XP216	P0.10 und P0.12
SCALANCE XR324WG, XR328-4C WG (GE)	P0.1 und P0.2
SCALANCE XR328-4C WG	P0.25 und P0.26

H-Sync
H-Sync ist ein Layer 2-Protokoll, mit dem Prozessdaten in Systemen mit redundanter Steuerung über PROFINET synchronisiert werden.
Die beiden Steuerungen sind redundant über einen MRP-Ring verbunden. Dabei müssen die beiden Steuerungen auf einem Pfad direkt miteinander verbunden sein. Beide Steuerungen sind als "MRP Auto-Manager" konfiguriert, sodass eine der Steuerungen der MRP-Manager wird. Alle anderen Geräte im Ring sind MRP-Clients. Die beiden Steuerungen senden H-Sync-Frames in beide Richtungen des Rings (Provider). H-Sync-Frames, die sie empfangen, werden nicht weitergeleitet (Consumer). Alle anderen Geräte im Ring leiten die H-Sync-Frames nur zwischen ihren Ring-Ports in beide Richtungen weiter (Forwarder). Auf allen anderen Ports werden die H-Sync-Frames gefiltert.
H-Sync ist für die IE-Switches ein transpartentes Protokoll. Welche IE-Switches als H-Sync-Forwarder eingesetzt werden können, entnehmen Sie dem Kapitel "Systemfunktionen und Hardware-Ausstattung".
Sie konfigurieren H-Sync nur über STEP 7 Basic bzw. Professional. Beachten Sie dennoch, dass von den folgenden Regeln abweichende Einstellungen zu Komplikationen bei der Konfiguration führen können:

  – Redundanzverfahren: MRP-Client

  – Ring-Ports:
    - Nutzen Sie die werkseitig voreingestellten Ring-Ports. Detailinformationen hierzu finden Sie in der Tabelle im vorangegangenen Abschnitt "Ring-Ports".
    - Nutzen Sie die ersten beiden optischen Schnittstellen.
    - Nutzen Sie die ersten beiden Gigabit-Schnittstellen.
    - Nutzen Sie Port 1 und Port 2.

- **Observer**
  Aktivieren/Deaktivieren Sie den Observer. Die Funktion "Observer" steht nur in HRP-Ringen zur Verfügung.
  Der Ringport, der in der linken Klappliste ausgewählt ist, wird an den "Isolated Port" eines HRP-Managers angeschlossen.
  Der Observer überwacht Fehlfunktionen des Redundanzmanagers oder Fehlkonfigurationen eines HRP-Rings.
  Wenn der Observer aktiviert ist, dann kann er bei erkannten Fehlern den angeschlossenen Ring unterbrechen. Dazu schaltet der Observer einen Ringport in den Zustand "blocking". Wenn der Fehler aufgelöst wird, schaltet der Observer den Port wieder frei.
- **Observer neu starten**
  Wenn viele Fehler schnell hintereinander auftreten, schaltet der Observer seinen Port nicht mehr selbstständig frei. Der Ringport bleibt dauerhaft im Zustand "blocking". Dies wird durch die Fehler-LED und einen Meldetext signalisiert.
  Nach der Fehlerbehebung können Sie den Port über die Schaltfläche "Observer neustarten" wieder freischalten.

Vorgehensweise zur Konfiguration

1. Aktivieren Sie das Optionskästchen "Ringredundanz".
2. Wählen Sie die Redundanzbetriebsart aus.
3. Legen Sie die Ring-Ports fest.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Werkseinstellungen wiederherstellen

EtherNet/IP-/Industrial Ethernet-Varianten

Wenn Sie die Werkseinstellungen wiederherstellen, dann ist die Ringredundanz deaktiviert und die Ringport-Einstellungen sind zurückgesetzt. Spanning Tree ist aktiviert.

PROFINET-Varianten

Wenn Sie die Werkseinstellungen wiederherstellen, dann ist die Ringredundanz aktiviert. Mit dem Zurücksetzen auf Werkseinstellungen werden auch die Ringport-Einstellungen zurückgesetzt. Wenn Sie vor dem Zurücksetzen andere Ports als Ringports verwendet haben, dann kann ein zuvor korrekt konfiguriertes Gerät kreisende Telegramme und damit den Ausfall des Datenverkehrs verursachen.

Zustand der Ring-Ports beim Redundanzmanager tauschen (HRP)

Wenn Sie einen Redundanzmanager konfigurieren, stellen Sie den Zustand der Ring-Ports fest ein. Der erste Ring-Port geht in den Zustand "blocking" und der zweite Ring-Port in den Zustand "forwarding". Bei aktivierter Ringredundanz können Sie den Zustand dieser Ring-Ports tauschen.

Hinweis

Achten Sie darauf, dass Sie zunächst den Ring öffnen, damit es nicht zu kreisenden Telegrammen kommt.

Ring-Ports ändern

Um die Ring-Ports zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie den Ring.
2. Wählen Sie die neuen Ring-Ports aus.
3. Stecken Sie die Kabel um.
4. Schließen Sie den Ring.

5.5.9.2 Standby

Redundante Kopplung von Ringen

Die Standby-Redundanz erlaubt die redundante Kopplung von HRP-Ringen.

Um eine Standby-Verbindung zu etablieren, konfigurieren Sie innerhalb eines Rings zwei benachbarte Geräte als Standby-Master bzw. Standby-Slave. Der Standby-Master und der Standby-Slave müssen über parallele Leitungen mit zwei Geräten in einem anderen Ring verbunden werden.

Im ungestörten Zustand laufen Nachrichten zwischen den beiden Ringen über den Master. Wenn die Leitung des Masters gestört wird, übernimmt der Slave die Weiterleitung von Nachrichten zwischen beiden Ringen.

Aktivieren sie die Standby-Redundanz für beide Standby-Partner und wählen Sie, über welche Ports das Gerät mit den zu koppelnden Ringen verbunden ist.

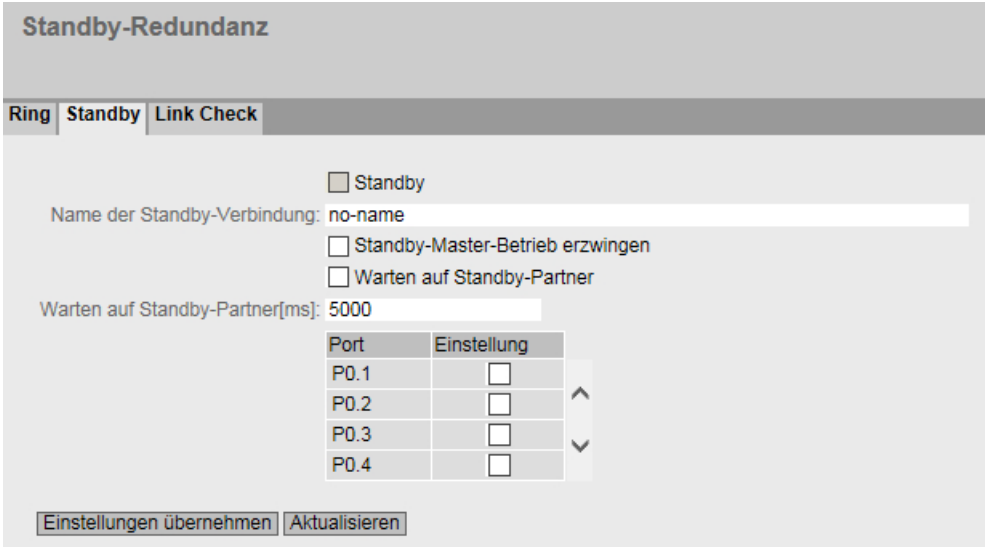
Als "Name der Standby-Verbindung" muss für beide Partner ein eindeutiger Name im Ring vergeben werden, mit dem die beiden zusammengehörenden Geräte als Standby-Partner identifiziert werden.

Hinweis

Um die Funktion nutzen zu können, muss HRP aktiviert sein.

Hinweis

Wird die Verbindung von Standby-Master und Standby-Slave in einer Linientopologie nach einer Unterbrechung wiederhergestellt, kann es kurzzeitig zu einem erhöhten Datenverkehr kommen.



Beschreibung der angezeigten Felder

- **Standby**
  Aktivieren oder deaktivieren Sie die Funktion Standby.

  Hinweis

  Sind zwei Geräte über Standby gekoppelt, muss die Funktion "Standby" an beiden Geräten aktiviert sein.

- **Name der Standby-Verbindung**
  Durch diesen Namen wird das Master-/Slave-Gerätepaar definiert. Beide Geräte müssen im gleichen Ring liegen.
  Tragen Sie hier den Namen für die Standby-Verbindung ein. Dieser muss identisch sein mit dem beim Standby-Partner eingetragenen Namen. Der Name kann frei gewählt werden, darf im ganzen Netz jedoch nur für ein Gerätepaar verwendet werden.

- **Standby-Master-Betrieb erzwingen**
  Wenn Sie dieses Optionskästchen markieren, wird das Gerät unabhängig von seiner MAC-Adresse als Standby-Master konfiguriert.
  - Wenn bei keinem der beiden Geräte, für die der Standby-Manager eingeschaltet ist, dieses Optionskästchen markiert ist, dann übernimmt im fehlerfreien Zustand das Gerät mit der höheren MAC-Adresse die Funktion des Standby-Masters.
  - Wenn diese Option bei beiden Geräten ausgewählt ist, oder wenn die Eigenschaft "Standby-Master-Betrieb erzwingen" nur von einem Gerät unterstützt wird, dann wird der Standby-Master ebenfalls anhand der MAC-Adresse ausgewählt.

  Wichtig ist diese Art der Zuordnung insbesondere bei einem Gerätetausch. Abhängig von den MAC-Adressen kann das bisherige Gerät mit Slave-Funktion die Rolle des Standby-Masters übernehmen.

  Hinweis

  Wenn die Option „Standby-Master-Betrieb erzwingen“ an beiden Geräten einer Standby-Kopplung aktiviert ist, kann es zu kreisenden Telegrammen und damit dem Ausfall des Datenverkehrs kommen. Aktivieren Sie die Option „Standby-Master-Betrieb erzwingen“ nur an einem Gerät einer Standby-Kopplung.

- **Warten auf Standby-Partner**
  - Aktiviert
    Eine Standby-Verbindung wird erst aktiviert, wenn der Standby-Master und der Standby-Slave sowie deren Standby-Partner eine Verbindung aufgebaut haben. Dadurch wird sichergestellt, dass die redundante Verbindung auch wirklich zur Verfügung steht, bevor die Kommunikation über eine Standby-Verbindung aktiviert wird.
  - Deaktiviert
    Eine Standby-Verbindung wird aktiviert, auch wenn der Standby-Master noch keine Verbindung zu dem Standby-Slave aufgebaut hat.
    Dies kann kreisende Telegramme und den Ausfall des Datenverkehrs verursachen, wenn bereits eine andere Standby-Verbindung aktiviert wurde. Mehrere Standby-Verbindungen können z. B. durch Konfigurationsfehler entstehen, wenn bei Standby-Master und Standby-Slave unterschiedliche Standby Connection Namen vergeben wurden.

- **Warten auf Standby-Partner [ms]**
  Dieses Eingabefeld wird nur angezeigt, wenn das Optionskästchen "Warten auf Standby-Partner" deaktiviert ist. In diesem Fall können Sie hier die Zeit festlegen, die das Gerät wartet, bis es eine Standby-Verbindung aufbaut. Nach dieser Zeitdauer wird eine Standby-Verbindung aktiviert, auch wenn der Standby-Master noch keine Verbindung zu dem Standby-Slave aufgebaut hat.
- **Standby-Port**
  Wählen Sie aus, welcher Port Standby-Port ist. Über den Standby-Port erfolgt die Kopplung zum anderen Ring.
  Der Standby-Port ist an der Umleitung des Datenverkehrs beteiligt. Im ungestörten Fall ist nur der Standby-Port des Masters aktiv und übernimmt den Datenverkehr in den angeschlossenen HRP-Ring bzw. die angeschlossene HRP-Linie.
  Wenn der Master oder die Ethernet-Verbindung des Standby-Ports des Masters ausfällt, dann wird der Standby-Port des Masters abgeschaltet und der Standby-Port des Slaves aktiviert. Damit wird wieder eine funktionierende Ethernet-Verbindung in das angeschlossene Netzsegment (HRP-Ring bzw. HRP-Linie) hergestellt.

5.5.9.3 Link Check

Voraussetzungen

- Sie können Link Check nicht auf Ports mit 10 GBit/s aktivieren.
- Sie können die Funktion Link Check nur bei optischen Ring-Ports eines HRP- oder MRP-Rings aktivieren.

  Hinweis

  Medienmodule tauschen: optisch → elektrisch

  Wenn Sie Link Check auf einem optischen Port eines Medienmoduls betreiben, beachten Sie Folgendes:
  - Link Check ist auf dem optischen Port eines Medienmoduls aktiviert.
  - Sie wollen das Medienmodul gegen ein Modul ohne optische Ports austauschen.

  1. Deaktivieren Sie Link Check auf den Ports des gesteckten Moduls.
  2. Tauschen Sie das Medienmodul.

- Link Check muss jeweils auf zwei benachbarten Geräten (Verbindungspartnern) innerhalb eines HRP- oder MRP-Rings aktiviert werden.
- Die Ring-Ports, an denen Sie Link Check aktivieren, müssen miteinander verbunden sein.

Überwachung optischer Verbindungen im Ring

Mit der Funktion Link Check können Sie die Übertragungsqualität optischer Strecken innerhalb eines HRP- oder MRP-Rings überwachen, gestörte Übertragungsstrecken identifizieren und unter bestimmten Bedingungen abschalten. Wenn die gestörte Strecke abgeschaltet ist, kann der Redundanzmanager den Ring schließen und die Kommunikation wiederherstellen.

ACHTUNG
Stellen Sie sicher, dass die Telegramme, die von Link Check zur Überwachung der optischen Verbindungen genutzt werden, nicht durch eine Überlast an hoch priorisierten Telegrammen im Netzwerk verdrängt werden. Eine Überlast an hoch priorisierten Telegrammen kann z. B. folgende Ursachen haben: • Netzwerkschleifen, durch die es zu einer Vervielfältigung der hoch priorisierten Telegramme kommen kann • Ändern der Prioritäten für die Weiterleitung von Telegrammen

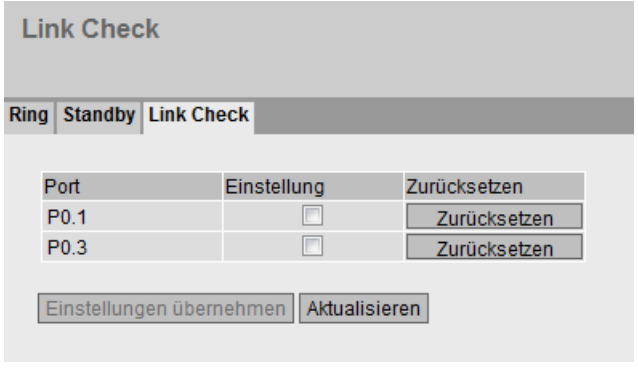
Hinweis

Aktivieren Sie Link Check nicht nur bei einem von zwei Verbindungspartnern. Dies kann zu fehlerhaftem Verhalten führen.

Hinweis

Wenn Link Check bei allen Geräten eines Rings zeitgleich eingeschaltet ist und mehrere Verbindungen innerhalb des Rings gestört sind, führt dies zu einer Fragmentierung des Rings.

1. Schalten Sie bei der Inbetriebnahme die Funktion Link Check für eine Verbindungsstrecke nach der anderen ein, indem Sie jeweils bei den beiden Verbindungspartnern, die an eine Strecke angeschlossen sind, Link Check aktivieren.
2. Um eine fehlerfreie Verbindung zu gewährleisten, warten Sie jeweils 1 min, bevor Sie Link Check für die nächste Verbindungsstrecke aktivieren.



Beschreibung der angezeigten Felder

Die Tabelle enthält folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Einstellung**
  Mit diesem Optionskästchen aktivieren bzw. deaktivieren Sie die Funktion Link Check für einen Port.
  Bei aktiver Verbindungsüberwachung können Sie die Anzahl der gesendeten und empfangenen Link Check-Testtelegrammen auf der Seite "Information > Redundanz > Link Check" einsehen.
- **Zurücksetzen**
  Nach dem Zurücksetzen von Link Check wird die Funktion auf dem Port erneut gestartet und die Statistik wird zurückgesetzt.
  Wenn Sie die Schaltfläche "Zurücksetzen" verwenden, muss das Zurücksetzen auf beiden Verbindungspartnern innerhalb von 30 s erfolgen.

Hinweis

Wenn Sie die Schaltfläche "Zurücksetzen" verwenden, kann es zu kurzfristiger Schleifenbildungen und damit zum Ausfall des Datenverkehrs kommen. Die Schleife wird automatisch wieder aufgelöst.

Wenn das in Ihrem Anwendungsfall nicht akzeptabel ist, setzen Sie Link Check zurück, indem Sie das Verbindungskabel ziehen und wieder stecken.

Vorgehensweise zur Konfiguration

Link Check aktivieren

Um die Überwachung eines Ring-Ports zu aktivieren, gehen Sie wie folgt vor:

1. Aktivieren Sie das entsprechende Optionskästchen in der Spalte "Einstellung".
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Link Check deaktivieren

Um die Überwachung eines Ring-Ports zu deaktivieren, gehen Sie wie folgt vor:

1. Deaktivieren Sie das entsprechende Optionskästchen in der Spalte "Einstellung".
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.10 Spanning Tree

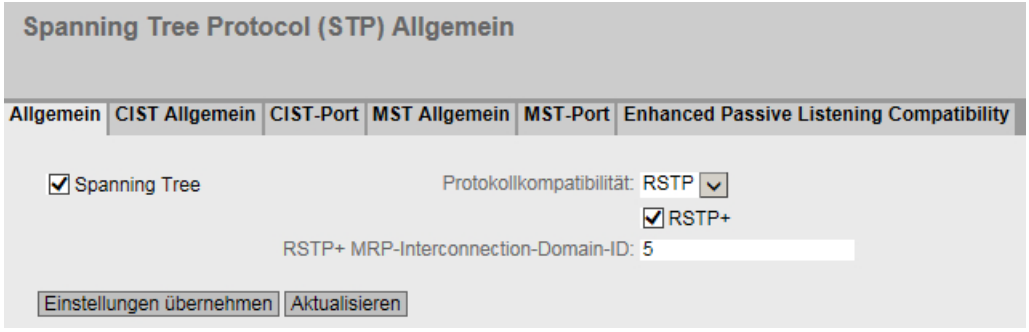
5.5.10.1 Allgemein

Allgemeine Einstellungen von Spanning Tree

Dies ist die Basisseite zu Spanning Tree. Wählen Sie aus der Klappliste den Kompatibilitätsmodus aus.

In der jeweiligen Konfigurationsseite der Funktionen sind weitere Einstellungen möglich.

Je nach Kompatibilitätsmodus können Sie in der jeweiligen Konfigurationsseite die entsprechende Funktion konfigurieren.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Spanning Tree**
  Aktivieren oder deaktivieren Sie Spanning Tree.
- **Protokollkompatibilität**
  Wählen Sie die Protokollkompatibilität. Folgende Einstellungen gibt es:
  - STP
  - RSTP
  - MSTP

- **RSTP+**
  RSTP+ ermöglicht die Kopplung eines Netzsegments, in dem Spanning Tree aktiviert ist, mit einem MRP-Ring. Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind, bevor Sie dieses Kontrollkästchen aktivieren:
  - MRP muss als Redundanverfahren aktiviert sein.
  - Bei aktivierter Ringredundanz müssen Sie die Ringports für Spanning Tree deaktivieren.

  Wenn Sie RSTP+ aktivieren, werden die Ringports sowohl Teil des MRP-Rings als auch Teil des Spanning Tree-Netzsegments.
- **RSTP+ MRP-Interconnection-Domain-ID**
  Konfigurieren Sie hier die MRP-Interconnection-Domain-ID für RSTP+. Dieser Wert darf nicht mit der MRP-Interconnection-Domain-ID übereinstimmen, die für die aktive MRP-Interconnection-Verbindung konfiguriert wurde.

Vorgehensweise zur Konfiguration

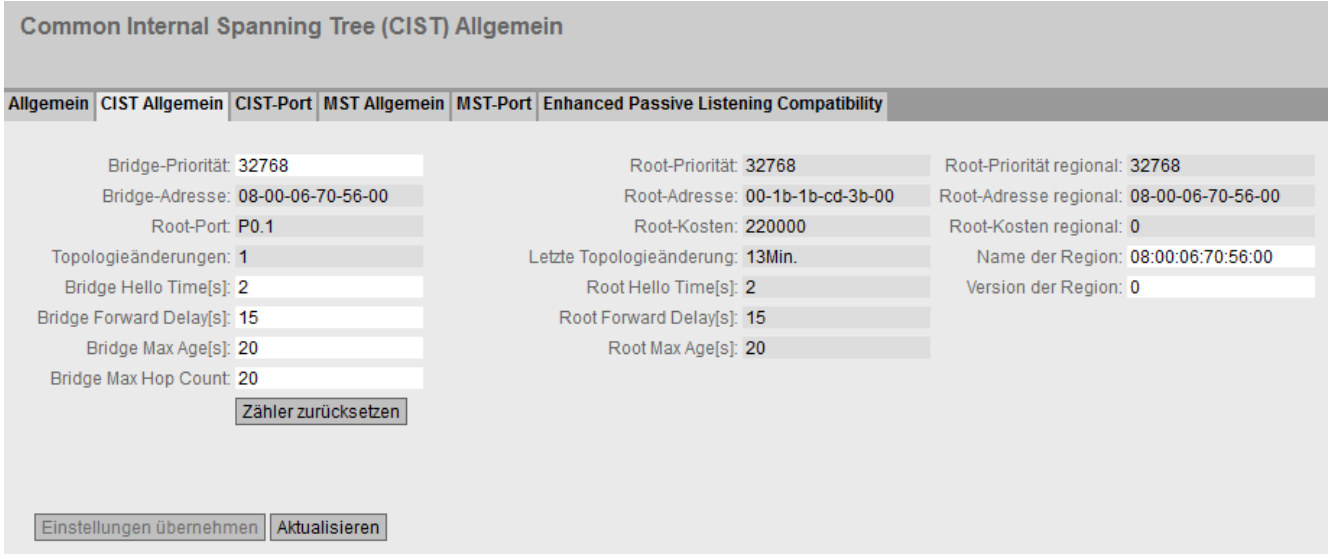
1. Aktivieren Sie das Optionskästchen "Spanning Tree".
2. Wählen Sie aus der Klappliste "Protokollkompatibilität" die Kompatibilitätsart aus.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.10.2 CIST Allgemein

Konfiguration MSTP-CIST

Die Seite besteht aus folgenden Teilen:

- Der linke Teil der Seite zeigt die Konfiguration des Geräts.
- Der mittlere Teil zeigt die Konfiguration der Root-Bridge, wie sie aus Spanning Tree-Telegrammen abgeleitet werden kann, die ein Gerät empfangen hat.
- Der rechte Teil zeigt die Konfiguration der regionalen Root-Bridge, wie sie aus den MSTP-Telegrammen abgeleitet werden kann. Die angezeigten Daten sind nur dann sichtbar, wenn auf der Seite "Allgemein" "Spanning Tree" aktiviert und bei "Protokollkompatibilität" "MSTP" eingestellt ist. Das gilt auch für den Parameter "Bridge Max Hop Count". Wenn das Gerät eine Root-Bridge ist, stimmen die Informationen des linken und des rechten Teils überein.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Bridge-Priorität / Root-Priorität**
  Anhand der Bridge-Priorität wird festgelegt, welches Gerät Root-Bridge wird. Die Bridge mit der höchsten Priorität wird Root-Bridge. Je kleiner der Wert, desto höher die Priorität. Wenn in einem Netz mehrere Geräte die gleiche Priorität besitzen, wird das Gerät Root-Bridge, dessen MAC-Adresse den niedrigsten Zahlenwert hat. Beide Parameter, Bridge-Priorität und MAC-Adresse, bilden zusammen die Bridge-Kennung. Da die Root Bridge alle Wegeänderungen verwaltet, sollte sie wegen der Laufzeit der Telegramme möglichst zentral angeordnet sein.
  Der Wert für die Bridge-Priorität ist ein ganzzahliges Vielfaches von 4096. Wertebereich: 0 - 61440
- **Bridge-Adresse / Root-Adresse**
  Die Bridge-Adresse zeigt die MAC-Adresse des Geräts und die Root-Adresse zeigt die MAC-Adresse der Root-Bridge an.

- **Root-Port**
  Zeigt den Port an, über den der Switch mit der Root-Bridge kommuniziert.
- **Root-Kosten**
  Die Pfadkosten von diesem Gerät bis zur Root-Bridge
- **Topologieänderungen / Letzte Topologieänderung**
  Die Angabe für das Gerät nennt die Zahl der Umkonfigurationen aufgrund des Spanning Tree-Mechanismus seit des letzten Hochlaufs. Für die Root-Bridge wird die Zeitdauer seit der letzten Umkonfiguration wie folgt angezeigt:
  - Sekunden: Zusatz "Sek." hinter der Zahlenangabe
  - Minuten: Zusatz "Min." hinter der Zahlenangabe
  - Stunden: Zusatz "Std." hinter der Zahlenangabe
- **Bridge Hello Time[s] / Root Hello Time[s]**
  Jede Bridge versendet regelmäßig Konfigurationstelegramme (BPDUs). Der Zeitabstand zwischen zwei Konfigurationstelegrammen ist die "Hello Time".
  Werkseinstellung: 2 Sekunden

  Hinweis

  Die Einstellung der "Bridge Hello Time" ist nur mit der Protokollkompatibilität RSTP möglich. Wenn die Protokollkompatibilität MSTP eingestellt ist, wird der Parameter "Hello Time" auf der Seite "Layer 2 > Spanning Tree > CIST-Port" verwendet.

- **Bridge Forward Delay[s] / Root Forward Delay[s]**
  Neue Konfigurationsinformationen werden von einer Bridge nicht sofort angewendet, sondern erst nach dem im Parameter "Forward Delay" festgelegten Zeitraum. So wird sichergestellt, dass der Betrieb entsprechend der neuen Topologie erst gestartet wird, wenn alle Bridges die notwendigen Informationen haben.
  Werkseinstellung: 15 Sekunden
- **Bridge Max Age[s] / Root Max Age[s]**
  Wenn die BPDU älter ist als das angegebene "Max Age", wird sie verworfen.
  Werkseinstellung: 20 Sekunden
- **Root-Priorität regional**
  Beschreibung siehe Bridge Priority / Root Priority
- **Root-Adresse regional**
  Die MAC-Adresse des Geräts
- **Root-Kosten regional**
  Die Pfadkosten von diesem Gerät bis zur Root-Bridge
- **Bridge Max Hop Count**
  Dieser Parameter gibt an, wie viele MSTP-Teilnehmer eine BPDU passieren darf. Wird eine MSTP-BPDU empfangen, deren Hop Count den hier konfigurierten Wert übersteigt, wird sie verworfen. Der Standardwert für diesen Parameter beträgt 20.
- **Name der Region**
  Tragen Sie den Namen der MSTP-Region ein, zu der dieses Gerät gehört. Defaultmäßig ist hier die MAC-Adresse des Geräts eingetragen. Dieser Wert muss auf allen Geräten die zur selben MSTP-Region gehören gleich sein.

- **Version der Region**
  Tragen Sie die Versionsnummer der MSTP-Region ein, in der sich das Gerät befindet. Dieser Wert muss auf allen Geräten die zur selben MSTP-Region gehören gleich sein.
- **Zähler zurücksetzen**
  Klicken Sie auf diese Schaltfläche, um die Zähler auf dieser Seite zurückzusetzen.

Vorgehensweise zur Konfiguration

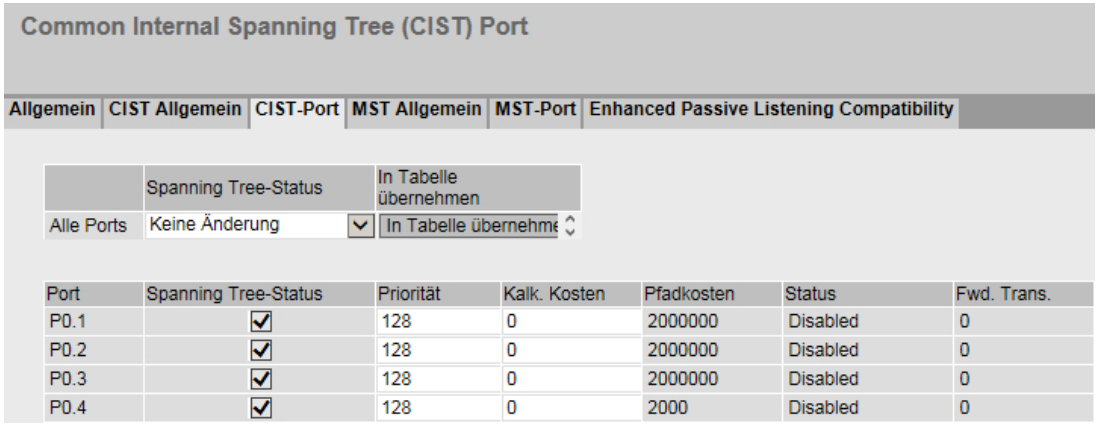
1. Tragen Sie in die Eingabefelder die für die Konfiguration benötigten Daten ein.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.10.3 CIST-Port

Konfiguration der MSTP-CIST-Ports

In der Tabelle wird beim Aufruf der Seite der aktuelle Stand der Konfiguration der Port-Parameter angezeigt.

Klicken Sie zur Konfiguration in die entsprechenden Felder der Port-Tabelle.



(Fortsetzung der Tabelle)

Edge-Typ	Edge	P.t.P.-Typ	P.t.P.	Hello Time	Eingeschränkte Rolle	Eingeschränktes TCN	Limitiertes TCN
Auto	☐	-	☐	2	☐	☐	☐
Auto	☐	-	☐	2	☐	☐	☐
Auto	☐	-	☐	2	☐	☐	☐
Auto	☐	-	☑	2	☐	☐	☐

Beschreibung der angezeigten Felder

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Spanning Tree-Status**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - Aktiviert
    Port ist im Spanning-Tree integriert.
  - Deaktiviert
    Port ist im Spanning-Tree nicht integriert.
  - Keine Änderung
    Tabelle 2 bleibt unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt alle verfügbaren Ports an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Spanning Tree-Status**
  Legen Sie fest, ob der Port im Spanning-Tree integriert ist oder nicht.

  Hinweis

  Wenn Sie die Option "Spanning Tree Status" für einen Port deaktivieren, kann es zur Schleifenbildung kommen. Die Topologie muss beachtet werden.

- **Priorität**
  Tragen Sie die Priorität des Ports ein. Die Priorität wird nur ausgewertet, wenn die Pfadkosten gleich sind.
  Der Wert muss durch 16 teilbar sein. Wenn der Wert nicht durch 16 teilbar ist, wird der Wert automatisch angepasst.
  Wertebereich: 0 - 240.
  Der Standardwert ist 128.
- **Kalk. Kosten**
  Tragen Sie die Wegekostenberechnung ein. Wenn Sie den Wert "0" eintragen, wird im Feld "Pfadkosten" der automatisch ermittelte Wert angezeigt.

- **Pfadkosten**
  Dieser Parameter dient zur Berechnung des zu wählenden Weges. Die Strecke mit dem geringsten Wert wird als Weg ausgewählt. Haben mehrere Ports eines Geräts den gleichen Wert bei gleichen Pfadkosten, wird der Port mit der niedrigsten Portnummer ausgewählt. Wenn im Feld "Kalk. Kosten" der Wert "0" ist, wird der automatisch ermittelte Wert angezeigt. Wenn ein Wert ungleich "0" eingetragen wird, wird der Wert des Feldes "Kalk. Kosten" angezeigt.
  Die Ermittlung der Wegekosten richtet sich maßgeblich nach der Übertragungsgeschwindigkeit. Je höher die erzielbare Übertragungsgeschwindigkeit ist, umso kleiner ist der Wert für die Wegekosten.
  Typische Werte für Wegekosten bei Rapid Spanning Tree:
  - 10.000 Mbit/s = 2.000
  - 1000 Mbit/s = 20.000
  - 100 Mbit/s = 200.000
  - 10 Mbit/s = 2.000.000

  Die Werte können aber auch individuell parametriert werden.
- **Status**
  Zeigt den momentanen Status an, in dem sich der Port befindet. Die Werte werden nur angezeigt und können nicht parametriert werden. Der Parameter "Status" ist abhängig von dem projektierten Protokoll. Folgende Werte sind möglich:
  - Disabled
    Der Port empfängt nur und nimmt nicht am STP, MSTP und RSTP teil.
  - Discarding
    In der Betriebsart "Discarding" werden BPDU-Telegramme empfangen. Andere aus- oder eingehende Telegramme werden verworfen.
  - Listening
    In diesem Status werden sowohl BPDU-Telegramme empfangen als auch gesendet. Der Port ist in den Spanning Tree-Algorithmus einbezogen.
  - Learning
    Vorstufe zum Status "Forwarding", der Port lernt aktiv die Topologie (d. h. die Teilnehmeradressen).
  - Forwarding
    Der Port ist nach der Umkonfigurationszeit aktiv im Netz, er empfängt und sendet Datentelegramme.
- **Fwd. Trans**
  Gibt die Anzahl der Wechsel vom Status "Discarding" zum Status "Forwarding" an.

- **Edge Type**
  Legen Sie die Art des "Edge Port" fest. Sie haben folgende Möglichkeiten:
  - "-"
    Edge Port ist deaktiviert. Der Port wird wie ein "no Edge Port" behandelt.
  - Admin
    Wählen Sie diese Option, wenn sich an diesem Port immer ein Endgerät befindet. Sonst wird bei jeder Verbindungsänderung eine Rekonfiguration des Netzwerks ausgelöst.
  - Auto
    Wählen Sie diese Option, wenn an diesem Port automatisch erkannt werden soll, ob ein Endgerät angeschlossen ist. Beim ersten Verbindungsaufbau wird der Port wie ein "no Edge Port" behandelt.
  - Admin/Auto
    Wählen Sie diese Optionen, wenn Sie an diesem Port eine Kombination aus beidem betreiben. Beim ersten Verbindungsaufbau wird der Port als "Edge Port" behandelt.
- **Edge**
  Zeigt an, in welchem Status der Port ist.
  - Aktiviert
    An diesem Port befindet sich ein Endgerät.
  - Deaktiviert
    An diesem Port befindet sich ein Spanning Tree- oder Rapid Spanning Tree-Gerät.

  Bei einem Endgerät kann ein Switch ohne Rücksicht auf Spanning Tree-Telegramme schneller den Port umschalten. Wird entgegen dieser Einstellung ein Spanning Tree-Telegramm empfangen, wechselt der Port automatisch auf die Einstellung "Deaktiviert".
- **P.t.P.-Typ**
  Wählen Sie in der Klappliste die gewünschte Option aus. Die Auswahl ist abhängig vom eingestellten Port.
  - "-"
    Punkt zu Punkt wird automatisch ermittelt. Steht der Port auf Halbduplex, wird nicht von einer Punkt zu Punkt-Verbindung ausgegangen.
  - P.t.P.
    Auch bei Halbduplex wird von einer Punkt zu Punkt-Verbindung ausgegangen.
  - Shared Media
    Auch bei einer Vollduplexverbindung wird nicht von einer Punkt zu Punkt-Verbindung ausgegangen.

    Hinweis

    Punkt zu Punkt-Verbindung bedeutet eine direkte Verbindung zwischen zwei Geräten. Eine Shared Media-Verbindung ist z.B. eine Verbindung zu einem Hub.

- **Hello Time**
  Tragen Sie das Intervall ein, nach der die Bridge Konfigurationstelegramme (BPDUs) sendet. Standardmäßig sind 2 Sekunden eingestellt.
  Wertebereich: 1-2 Sekunden

  Hinweis

  Die portspezifische Einstellung der Hello Time ist nur mit der Protokollkompatibilität MSTP möglich. Wenn die Protokollkompatibilität RSTP eingestellt ist, wird der Parameter "Bridge Hello Time" auf der Seite "Layer 2 > Spanning Tree > CIST Allgemein" verwendet.

- **Eingeschränkte Rolle**
  Bei aktiviertem Optionskästchen wird der entsprechende Port nicht als Root-Port ausgewählt, unabhängig vom Wert für die Priorität. Auch der Port mit der niedrigsten Priorität wird bei aktiviertem Optionskästchen nicht zum Root-Port. Aktivieren Sie diese Option nur dann, wenn Sie den Einfluss von Bridges außerhalb des administrierten Bereichs auf die Spanning Tree-Topologie beschränken wollen.
- **Eingeschränktes TCN**
  Bei aktiviertem Optionskästchen leitet der entsprechende Port weder erhaltene noch erkannte Topologieänderungen (Topology Change Notifications) an andere Ports weiter. Aktivieren Sie diese Option nur dann, wenn Sie den Einfluss von Bridges außerhalb des administrierten Bereichs auf die Spanning-Tree Topologie beschränken wollen.
- **Limitiertes TCN**
  Bei aktiviertem Optionskästchen akzeptiert der entsprechende Port erhaltene und erkannte Topologieänderungen, leitet Topologieänderungen aber nicht an andere Ports weiter. Sie können die Optionskästchen in dieser Spalte nur dann aktivieren, wenn folgende Voraussetzungen erfüllt sind:
  - RSTP+ muss aktiviert sein.
  - Das Optionskästchen "Eingeschränktes TCN" muss für diesen Port deaktiviert sein.

  Wenn die genannten Voraussetzungen nicht erfüllt sind, werden die Optionskästchen in dieser Spalte gegraut dargestellt.

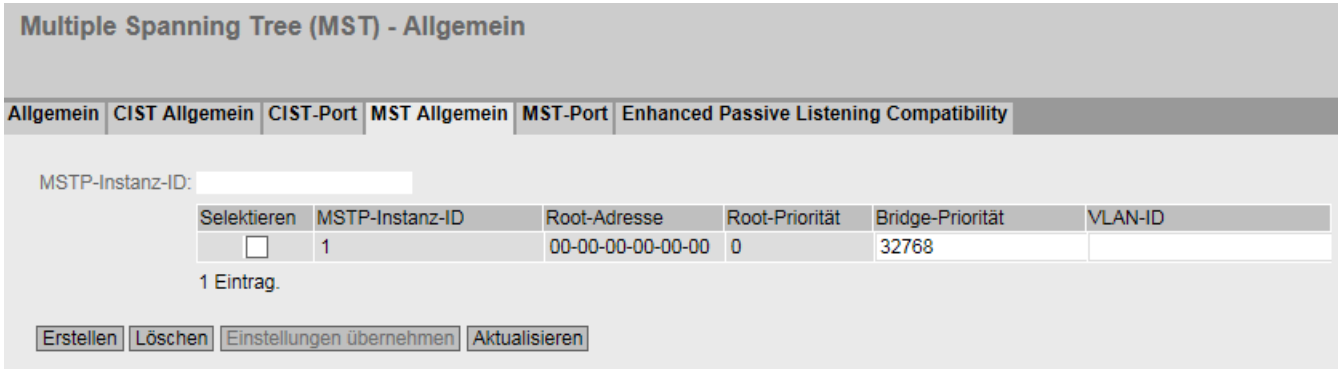
Vorgehensweise zur Konfiguration

1. Tragen Sie in den Eingabefeldern der Tabellenzeile des zu konfigurierenden Ports die Werte ein.
2. Wählen Sie aus den Klapplisten der Felder der Tabellenzeile des zu konfigurierenden Ports die Werte aus.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.10.4 MST Allgemein

Multiple Spanning Tree-Konfiguration

Bei MSTP können zusätzlich zu RSTP mehrere VLANs in einem LAN mit eigenen RSTP-Bäumen verwaltet werden.



Beschreibung

Die Seite enthält folgendes Feld:

- **MSTP-Instanz-ID**
  Tragen Sie die Nummer der MSTP-Instanz ein.
  Zulässige Werte: 1 - 64

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **MSTP-Instanz-ID**
  Zeigt die Nummer der MSTP-Instanz an.
- **Root-Adresse**
  Zeigt die MAC-Adresse der Root-Bridge an.
- **Root-Priorität**
  Zeigt die Priorität der Root-Bridge an.
- **Bridge-Priorität**
  Tragen Sie in dieses Feld die Bridge-Priorität ein. Der Wert für die Bridge-Priorität ist ein ganzzahliges Vielfaches von 4096 mit einem Wertebereich von 0 bis 61440.
- **VLAN-ID**
  Tragen Sie die VLAN-ID ein. Sie können hier auch Bereiche mit Start-ID, "-", End-ID angeben. Mehrere Bereiche oder IDs werden durch "," separiert.
  Zulässige Werte: 1- 4094

Vorgehensweise

Neuen Eintrag erstellen

1. Tragen Sie in das Feld "MSTP-Instanz-ID" die Nummer der MSTP Instanz ein.
2. Klicken Sie auf die Schaltfläche "Erstellen".
3. Tragen Sie in das Feld "VLAN-ID" die ID des VLANs ein.
4. Tragen Sie in das Feld "Bridge-Priorität" die Priorität der Bridge ein.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

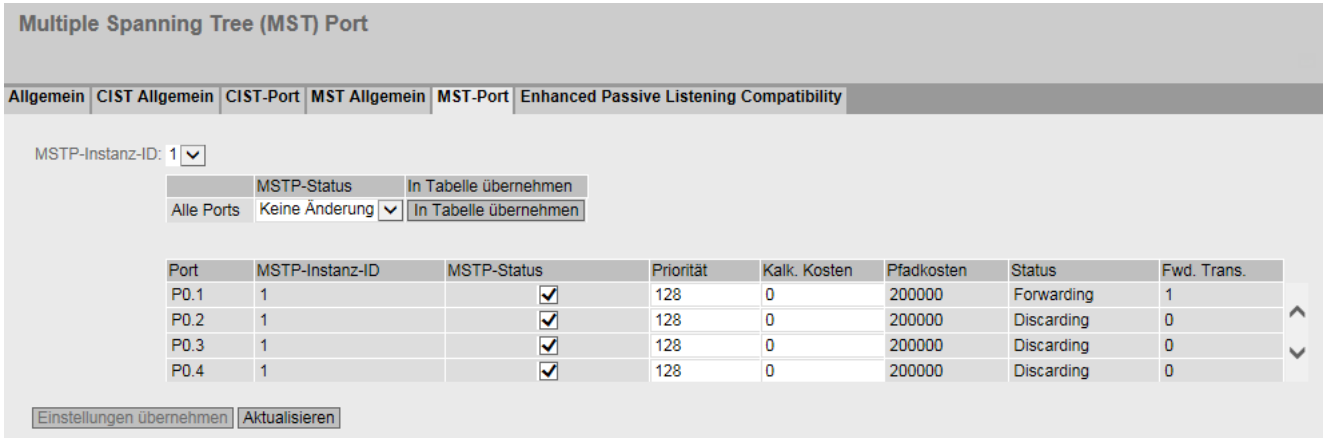
Einträge löschen

1. Markieren Sie mit Hilfe der Optionskästchen vor der entsprechenden Zeile die zu löschenden Einträge.
2. Klicken Sie auf die Schaltfläche "Löschen", um die markierten Einträge aus dem Speicher zu entfernen. Die Einträge werden aus dem Speicher des Geräts gelöscht und die Darstellung dieser Seite wird aktualisiert.

5.5.10.5 MST-Port

Konfiguration der Multiple Spanning Tree Port Parameter

Auf dieser Seite stellen Sie die Parameter für die Ports der konfigurierten Multiple Spanning Tree Instanzen ein.



Beschreibung der angezeigten Felder

Die Seite enthält folgendes Feld:

- **MSTP-Instanz-ID**
  Wählen Sie in der Klappliste die ID der MSTP-Instanz aus.

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports gültig sind.
- **MSTP-Status**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - Aktiviert
  - Deaktiviert
  - Keine Änderung: Tabelle 2 bleibt unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt alle verfügbaren Ports und Link Aggregationen an.
- **MSTP-Instanz-ID**
  ID der MSTP-Instanz.
- **MSTP-Status**
  Klicken Sie in das Optionskästchen, um diese Option zu aktivieren oder zu deaktivieren.
- **Priorität**
  Tragen Sie die Priorität des Ports ein. Die Priorität wird nur dann ausgewertet, wenn die Pfadkosten gleich sind.
  Der Wert muss durch 16 teilbar sein. Wenn der Wert nicht durch 16 teilbar ist, wird der Wert automatisch angepasst.
  Wertebereich: 0 - 240.
  Werkseinstellung: 128
- **Kalk. Kosten**
  Tragen Sie in das Eingabefeld die Wege-Kostenberechnung ein. Wenn Sie hier "0" eintragen, wird im nächsten Feld "Pfadkosten" der automatisch ermittelte Wert angezeigt.

- **Pfadkosten**
  Die Pfadkosten von diesem Port zur Root-Bridge. Die Strecke mit dem geringsten Wert wird als Weg ausgewählt. Haben mehrere Ports eines Geräts den gleichen Wert, wird der Port mit der niedrigsten Portnummer ausgewählt.
  Wenn im Feld "Kalk. Kosten" der Wert "0" ist, wird der automatisch ermittelte Wert angezeigt. Wenn ein Wert ungleich "0" eingetragen wird, wird der Wert des Feldes "Kalk. Kosten" angezeigt.
  Die Ermittlung der Wegekosten richtet sich maßgeblich nach der Übertragungsgeschwindigkeit. Je höher die erzielbare Übertragungsgeschwindigkeit ist, umso kleiner ist der Wert für die Wegekosten.
  Typische Werte für Wegekosten bei Rapid Spanning Tree:
  - 10.000 Mbit/s = 2.000
  - 1000 Mbit/s = 20.000
  - 100 Mbit/s = 200.000
  - 10 Mbit/s = 2.000.000

  Die Werte können aber auch individuell parametriert werden.
- **Status**
  Zeigt den momentanen Status an, in dem sich der Port befindet. Die Werte werden nur angezeigt und können nicht konfiguriert werden. Beim Status ist Folgendes möglich:
  - **Discarding**
    Der Port tauscht MSTP-Informationen aus, nimmt aber nicht am Datenverkehr teil.
  - **Blocked**
    Im Blocking-Modus werden BPDU-Telegramme empfangen.
  - **Forwarding**
    Der Port empfängt und sendet Datentelegramme.
- **Fwd. Trans.**
  Gibt die Anzahl der Statuswechsel Discarding - Forwarding bzw. Forwarding - Discarding für einen Port an.

Vorgehensweise zur Konfiguration

1. Tragen Sie in den Eingabefeldern der Tabellenzeile des zu konfigurierenden Ports die Werte ein.
2. Wählen Sie aus den Klapplisten der Felder der Tabellenzeile des zu konfigurierenden Ports die Werte aus.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

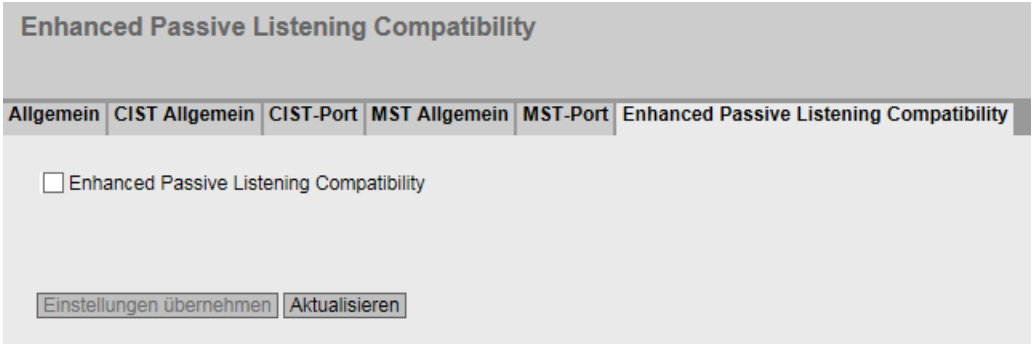
5.5.10.6 Enhanced Passive Listening Compatibility

Spanning Tree und Ringredundanz

Wenn Sie Enhanced Passive Listening Compatibility aktivieren, werden Topologieänderungen (Topology Change Notifications) über RSTP-Edge-Ports versendet. In Verbindung mit der Funktion "Edge-Typ" (siehe "Layer 2 > Spanning Tree > CIST-Port") ist dieser Parameter notwendig, um Spanning Tree-Netze mit HRP-Ringen zu koppeln. Über Edge-Ports werden sonst keine TCN-Frames versendet, dies ist aber für die Passive Listening Funktion auf den Ringteilnehmern notwendig.

Aktivieren der Funktion

Auf dieser Seite können Sie die Funktion "Enhanced Passive Listening Compatibility" aktivieren.



Beschreibung der angezeigten Felder

Die Seite enthält folgendes Feld:

- **Enhanced Passive Listening Compatibility**
  Aktivieren oder deaktivieren Sie diese Funktion für das gesamte Gerät.

Vorgehensweise zur Konfiguration

1. Aktivieren oder deaktivieren Sie "Enhanced Passive Listening Compatibility"
2. Klicken sie auf die Schaltfläche "Einstellungen übernehmen"

5.5.11 Loop Detection

Mit der Funktion "Loop Detection" legen Sie fest, für welche Ports Schleifenerkennung aktiviert werden soll. Von den betreffenden Ports werden spezielle Testtelegramme, die Loop-Detection-Telegramme, gesendet. Wenn diese Telegramme wieder zum Gerät zurück gesendet werden, dann liegt eine Schleife ("Loop") vor.

Von einem "Local Loop" unter Beteiligung dieses Geräts spricht man, wenn die Telegramme an einem anderen Port desselben Geräts wieder empfangen werden. Wenn die

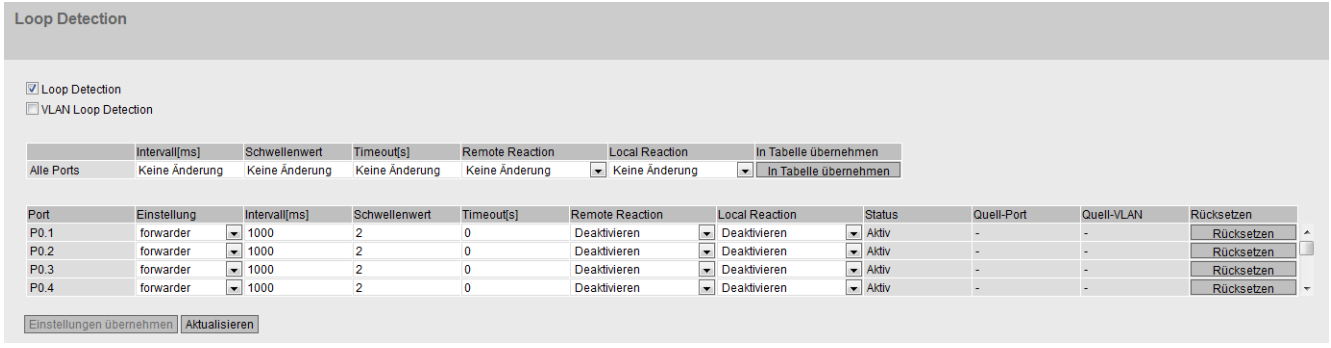
ausgesendeten Telegramme wieder am gleichen Port empfangen werden, ist eine Schleife an anderen Netzkomponenten aufgetreten "Remote Loop".

Hinweis

Eine Schleife ist ein Fehler im Netzaufbau, der beseitigt werden muss. Die Schleifenerkennung kann helfen, den Fehler schneller zu finden, behebt ihn jedoch nicht. Die Schleifenerkennung ist nicht dazu geeignet, die Netzwerkverfügbarkeit durch den gezielten Einbau von Schleifen zu erhöhen.

Hinweis

Beachten Sie, dass die Schleifenerkennung nur auf Ports möglich ist, die nicht als Ring-Port oder Standby-Port konfiguriert wurden.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Loop Detection**
  Aktivieren oder deaktivieren Sie die Schleifenerkennung.
  Wenn die Option aktiviert ist, sendet das Gerät ungetaggte LLC-Frames.
- **VLAN Loop Detection**
  Aktivieren oder deaktivieren Sie die Schleifenerkennung bei VLAN.
  Wenn die Option aktiviert ist, nutzt das Gerät die am entsprechenden Port eingestellten VLAN-Informationen, um LLC-Frames zu senden.

Die Tabelle 1 enthält folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Intervall[ms] / Schwellenwert / Timeout[s] / Remote Reaction / Local Reaction**
  Legen Sie die gewünschten Einstellungen fest.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 enthält folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an.
- **Einstellung**
  Legen Sie fest, wie der Port mit Loop-Detection-Telegrammen verfahren soll. Wählen Sie aus der Klappliste eine der folgenden Optionen:

  Hinweis

  Durch die Testtelegramme entsteht zusätzliche Netzlast. Es wird empfohlen, nur einzelne Switches, z. B. an den Abzweigungen des Rings, als "Sender" zu konfigurieren und die anderen als "Forwarder".

  – sender
    Loop-Detection-Telegramme werden ausgesendet und weitergeleitet.
  – forwarder
    Loop-Detection-Telegramme von anderen Geräten werden weitergeleitet.
  – blocked
    Die Weiterleitung der Loop-Detection-Telegramme wird blockiert.
- **Intervall[ms]**
  Legt das Sendeintervall für Loop Detection-Telegramme in Millisekunden fest.
- **Schwellenwert**
  Legen Sie durch Eingabe einer Zahl fest, nach wie vielen empfangenen Loop-Detection-Telegrammen von einer Schleife ausgegangen wird.
- **Timeout[s]**
  Legen Sie fest, nach wie vielen Sekunden das Gerät automatisch wieder in den Zustand wechselt, in dem es sich vor dem Loop befunden hat. Wenn der Wert "0" eingestellt ist, müssen Sie den Port nach einem Loop manuell wieder aktivieren, mit der Schaltfläche "Rücksetzen".
- **Remote Reaction**
  Legen Sie fest, wie der Port bei Auftreten eines Remote-Loop reagieren soll. Wählen Sie aus der Klappliste eine der beiden Optionen:
  – Keine Aktion: Eine Schleife hat keine Auswirkungen auf den Port.
  – Deaktivieren: Der Port wird geblockt.
- **Local Reaction**
  Legen Sie fest, wie der Port bei Auftreten eines Local Loop reagieren soll. Wählen Sie aus der Klappliste eine der beiden Optionen:
  – Keine Aktion: Eine Schleife hat keine Auswirkungen auf den Port.
  – Deaktivieren: Der Port wird geblockt
- **Status**
  Zeigt an, ob die Schleifenerkennung für diesen Port ein- oder ausgeschaltet ist.
- **Quell-Port**
  Zeigt den Empfänger-Port des Loop-Detection-Telegramms an, das die letzte Reaktion ausgelöst hat.

- **Quell-VLAN**
  Dieses Feld zeigt die VLAN-ID des Loop-Detection-Telegramms an, das die letzte Reaktion ausgelöst hat.
  Voraussetzung dafür ist, dass das Optionskästchen "VLAN Loop Detection" aktiviert ist.
- **Rücksetzen**
  Nachdem eine Schleife im Netzwerk beseitigt wurde, klicken Sie auf die Schaltfläche "Rücksetzen", um den Port wieder zurückzusetzen.

Änderung des konfigurierten Port-Status durch Loop Detection

Die Konfiguration des Port-Status kann durch die Funktion "Loop Detection" verändert werden. Wenn der Administrator z. B. einen Port deaktiviert hat (disabled), kann der Port nach einem Geräteneustart durch „Loop Detection“ wieder aktiviert werden (enabled). Der Port-Status "Link down" wird durch "Loop Detection" nicht verändert.

5.5.12 Link Aggregation

5.5.12.1 Allgemein

Bündelung von Netzwerkverbindungen für Redundanz und höhere Bandbreite

Die Link Aggregation nach IEEE 802.3AD erlaubt es, mehrere Verbindungen zwischen benachbarten Geräten zu bündeln, um so höhere Bandbreiten zu erreichen und zusätzlich für Ausfallsicherheit zu sorgen.

Hierbei werden Ports auf beiden Partnergeräten in Verbindungsbündel eingebunden und dann die Geräte über diese Ports miteinander verbunden. Um Ports korrekt einem Partnergerät zuzuordnen, wird das Link Aggregation Control Protocol (LACP) aus dem Standard IEEE 802.3AD verwendet.

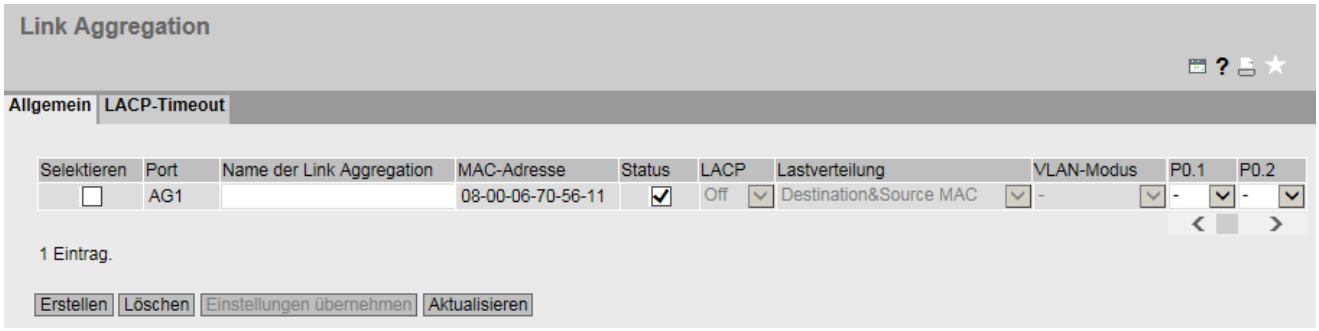
Hinweis

Wenn ein Port einer Link Aggregation zugewiesen ist, aber nicht aktiv ist (z. B. Link-Down), können die angezeigten Werte von den Werten abweichen, die für die Link Aggregation konfiguriert wurden.

Wenn der Port in der Link Aggregation aktiv wird, werden individuelle Portkonfigurationen wie z. B. DCP-Forwarding mit den konfigurierten Werten der Link Aggregation überschrieben.

Anzeige der konfigurierten Bündelung

Auf dieser Seite werden alle konfigurierten Link Aggregationen angezeigt.



Beschreibung der angezeigten Felder

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Port**
  Zeigt die virtuelle Port-Nummer dieser Link Aggregation an. Die Bezeichnung wird intern von der Firmware vergeben.
- **Name der Link Aggregation**
  Zeigt den Namen der Link Aggregation an. Dieser Name kann bei der Konfiguration vom Benutzer angegeben werden. Der Name ist nicht zwingend notwendig, kann aber hilfreich sein, die verschiedenen Link Aggregationen zu unterscheiden.
- **MAC-Adresse**
  Zeigt die MAC-Adresse an.
- **Status**
  Aktivieren oder deaktivieren Sie die Link Aggregation.
- **LACP**
  - An
    Aktiviert das Senden von LACP-Telegrammen.
  - Aus
    Deaktiviert das Senden von LACP-Telegrammen.
- **Lastverteilung** - Destination&Source MAC
  Die Verteilung von Paketen auf die einzelnen Links einer Aggregation basiert auf einer Kombination der Ziel- und Quell-MAC-Adresse.

- **VLAN-Modus**
  Legen Sie fest, wie die Link Aggregation in einem VLAN eingetragen wird:
  - Hybrid
    Die Link Aggregation sendet getaggte und ungetaggte Telegramme. Sie ist nicht automatisch Mitglied eines VLANs.
  - Trunk
    Die Link Aggregation sendet nur getaggte Telegramme und ist automatisch Mitglied in allen VLANs.
  - Access
    Der Port gehört zu einem Provider-Switch, der die Funktion Q-in-Q VLAN-Tunnel unterstützt.
- **Port**
  Zeigt die Ports an, die zu dieser Link Aggregation gehören. Dabei können aus der Klappliste folgende Werte gewählt werden:
  - "-" (Deaktiviert)
    Link Aggregation ist deaktiviert.
  - "a" (Aktiv)
    Der Port sendet LACP-Telegramme und nimmt nur an der Link Aggregation teil, wenn LACP-Telegramme empfangen werden.
  - "p" (Passiv)
    Der Port nimmt nur an der Link Aggregation teil, wenn LACP-Telegramme empfangen werden.
  - "o" (Ein)
    Der Port nimmt an der Link Aggregation teil und sendet keine LACP-Telegramme.

  Hinweis

  Innerhalb einer Link Aggregation sind immer nur Ports folgender Konfiguration möglich:
  - alle Ports mit "o"
  - alle Ports mit "a" oder "p".

Vorgehensweise zur Konfiguration

Grundlegendes vor der Konfiguration

1. Suchen Sie sich zunächst die Ports aus, die Sie zwischen den Geräten zu einer Link Aggregation verbinden wollen.
2. Konfigurieren Sie die Link Aggregation auf den Geräten.
3. Übernehmen Sie die Konfiguration für alle Geräte.
4. Führen Sie als letzten Schritt die Verkabelung durch.

Hinweis

Wenn Sie die Verkabelung von gebündelten Verbindungen vor der Konfiguration durchführen, können Sie Schleifen im Netzwerk erzeugen. Das betreffende Netzwerk wird dadurch stark beeinträchtigt oder es kann eine Störung auftreten.

Anlegen einer neuen Link Aggregation

1. Klicken Sie auf die Schaltfläche "Erstellen", um eine neue Link Aggregation anzulegen. Damit wird eine neue leere Zeile angelegt.
2. Wählen Sie die Ports aus, die zu dieser Link Aggregation gehören sollen.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Löschen einer Link Aggregation

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
   Wiederholen Sie den Vorgang für alle Einträge, die Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Löschen".

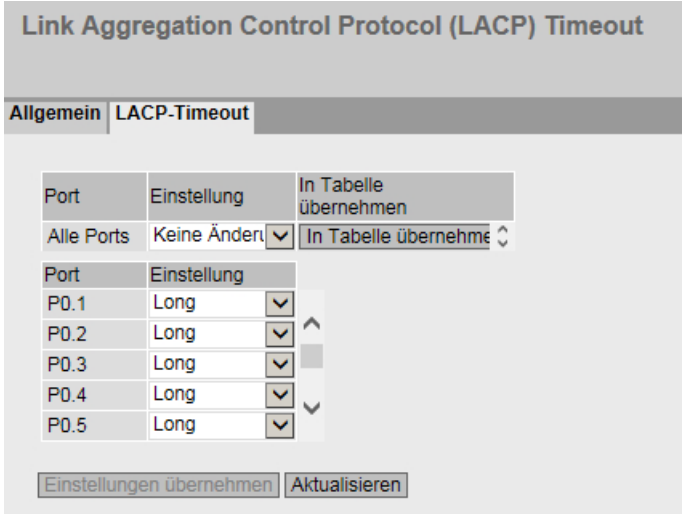
Ändern einer Link Aggregation

1. Klicken Sie in der Übersicht auf den entsprechenden Tabelleneintrag, um die Konfiguration einer angelegten Link Aggregation zu ändern.
2. Führen Sie alle Änderungen durch.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.12.2 LACP Timeout

Konfiguration des LACP Timeouts

Im Standard IEEE 802.3ad sind für die Länge des Timeouts zwei mögliche Werte festgelegt, "Long" (90 Sekunden) und "Short" (3 Sekunden). Dieser Wert definiert, in welchem zeitlichen Abstand LACPDUs gesendet werden. Als Defaultwert ist für alle Ports der Wert "Long" konfiguriert. Um eine symetrische LACP-Konfiguration zu ermöglichen, kann wahlweise der Wert "Short" eingestellt werden. Wählen Sie für alle Ports einer Link Aggregation den gleichen Wert für den Timeout.



Beschreibung der angezeigten Felder

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - Short
    Der Wert für den LACP Timeout beträgt 3 Sekunden.
  - Long
    Der Wert für den LACP Timeout beträgt 90 Sekunden.
  - Keine Änderung
    Tabelle 2 bleibt unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, werden die Einstellungen für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt alle verfügbaren Ports an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Einstellung**
  Wählen Sie den Wert "Short" oder "Long" für diesen Port.

5.5.13 DCP-Weiterleitung

Anwendungen

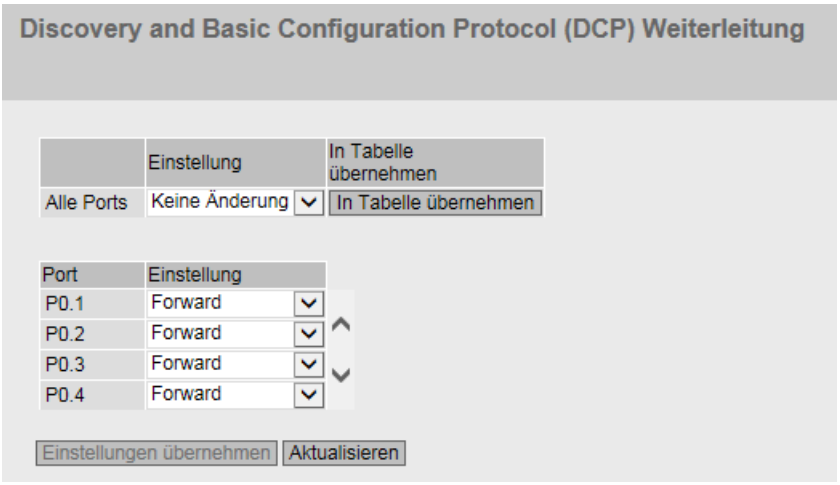
Das DCP-Protokoll wird von STEP 7 und dem Primary Setup Tool (PST) für die Konfiguration und Diagnose verwendet. In der Werkseinstellung ist DCP auf allen Ports aktiviert, d.h. empfangene DCP-Telegramme werden auf allen Ports weitergeleitet. Mit dieser Option haben Sie die Möglichkeit, das Weiterleiten der Telegramme für einzelne Ports auszuschalten, um z.B. einzelne Netzbereiche von der Konfiguration per PST abzuschotten, bzw. um das gesamte Netz in kleinere Teilnetze für die Konfiguration und Diagnose zu unterteilen.

Hinweis

PROFINET Konfiguration

Da es sich bei DCP um ein PROFINET-Protokoll handelt ist die hier vorgenommene Konfiguration nur in dem mit der TIA-Schnittstelle assoziierten VLAN wirksam.

Auf dieser Seite werden alle Ports des Geräts angezeigt. Hinter jedem angezeigten Port befindet sich eine Klappliste zur Funktionsauswahl.



Beschreibung der angezeigten Werte

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung. Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Einstellung**
  Wählen Sie aus der Klappliste aus, ob der Port DCP-Telegramme ausgangsseitig blocken oder weiterleiten soll. Sie haben die folgenden Möglichkeiten zur Auswahl:
  - Forward
    An diesem Port werden DCP-Telegramme weitergeleitet.
  - Block
    An diesem Port werden ausgangsseitig keine DCP-Telegramme weitergeleitet. Ein Empfangen ist jedoch über diesen Port weiterhin möglich.

Vorgehensweise zur Konfiguration

1. Wählen Sie aus den Optionen der Klappliste in der Zeile hinter der Portnummer aus, welche Ports den DCP-Versand unterstützen sollen.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.14 LLDP

Bestimmung der Netzwerktopologie

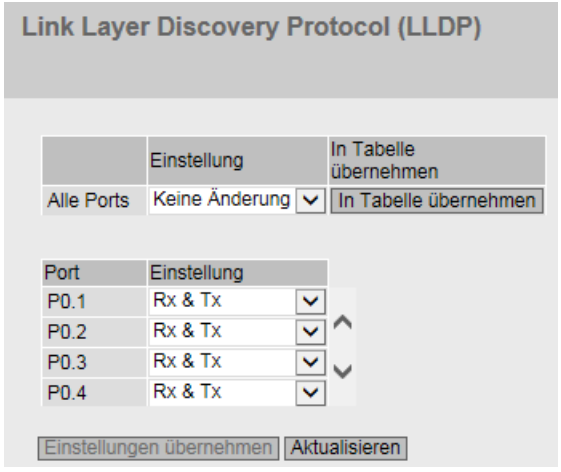
LLDP (Link Layer Discovery Protocol) ist im Standard IEEE 802.1AB definiert.

LLDP ist ein Verfahren zur Bestimmung der Netzwerktopologie. Netzwerkkomponenten tauschen über LLDP Informationen mit ihren Nachbargeräten aus.

Netzwerkkomponenten, die LLDP unterstützen, verfügen über einen LLDP-Agenten. Der LLDP-Agent versendet in periodischen Abständen Informationen über sich selbst und empfängt Informationen von angeschlossenen Geräten. Die empfangenen Informationen werden im Gerät gespeichert.

Anwendungen

PROFINET benutzt LLDP für die Topologie-Diagnose. In der Werkseinstellung ist LLDP für alle Ports aktiviert, d. h. es werden LLDP-Telegramme auf allen Ports gesendet und empfangen. Mit dieser Funktion haben Sie die Möglichkeit, das Aussenden und/oder Empfangen pro Port ein- oder auszuschalten.



Beschreibung der angezeigten Felder

Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports gültig sind.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung. Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Einstellung**
  Wählen Sie aus der Klappliste aus, ob der Port LLDP-Telegramme senden oder empfangen soll. Sie haben die folgenden Möglichkeiten zur Auswahl:
  - Rx
    Dieser Port kann LLDP-Telegramme nur empfangen.
  - Tx
    Dieser Port kann LLDP-Telegramme nur senden.
  - Rx & Tx
    Dieser Port kann LLDP-Telegramme empfangen und senden.
  - "-" (Deaktiviert)
    Dieser Port kann LLDP-Telegramme weder empfangen noch senden.

Vorgehensweise zur Konfiguration

1. Wählen Sie aus der Klappliste "Einstellung" die LLDP-Funktionalität des Ports aus.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.15 Fiber Monitoring Protocol

Voraussetzungen

- Sie können Fiber Monitoring nur bei diagnosefähigen Transceivern verwenden. Beachten Sie hierzu die Dokumentation der Geräte.
- Um die Funktion Fiber Monitoring nutzen zu können, aktivieren Sie LLDP. Die Fiber Monitoring-Informationen werden an die LLDP-Pakete angehängt.

Überwachung optischer Strecken

Mit Fiber Monitoring können Sie die Empfangsleistung und den Leistungsabfall auf optischen Strecken zwischen zwei Switches überwachen.

Wenn Sie Fiber Monitoring an einem optischen Port aktivieren, übermittelt das Gerät über LLDP-Pakete den aktuellen Wert für die Sendeleistung des Ports an seinen Verbindungspartner. Parallel zum Sendevorgang prüft das Gerät, ob entsprechende Informationen vom Verbindungspartner empfangen werden.

Unabhängig davon, ob der IE-Switch Diagnoseinformationen von seinem Verbindungspartner empfängt, überwacht er die am optischen Port gemessene Empfangsleistung auf die eingestellten Grenzwerte.

Wenn bei dem Verbindungspartner Fiber Monitoring aktiviert ist, übermittelt der Verbindungspartner den aktuellen Wert für die Sendeleistung des Ports an das Gerät. Das

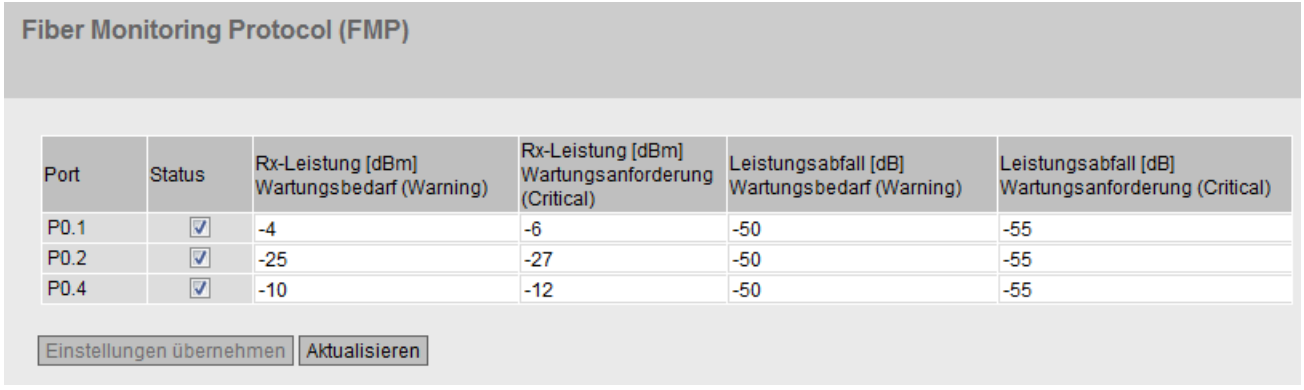
Gerät vergleicht den Wert, den es für die Sendeleistung erhalten hat, mit der tatsächlich empfangenen Leistung. Aus der Differenz von Empfangsleistung und Sendeleistung ergibt sich der Leistungsabfall auf der Strecke. Der berechnete Leistungsabfall wird ebenfalls auf die eingestellten Grenzwerte überwacht.

Wenn der Wert der Empfangsleistung bzw. der Betrag des Leistungsabfalls die eingestellten Grenzwerte unter- bzw. überschreitet, wird ein Event ausgelöst. Sie können in zwei Stufen Grenzwerte einstellen, für Meldungen mit den Severity Levels "Warning" und "Critical".

Unter "System > Ereignisse > Konfiguration" können Sie einstellen, wie der IE-Switch das Event anzeigt.

Hinweis

Wenn Sie Fiber Monitoring aktiviert haben und ein diagnosefähiger Stecktransceiver gezogen wird, wird automatisch Fiber Monitoring für diesen Port deaktiviert und die eingestellten Grenzwerte sowie ein möglicher anstehender Fehlerzustand werden gelöscht.



Beschreibung der angezeigten Felder

In der Tabelle können Sie die zu überwachenden Grenzwerte für die gemessene Empfangsleistung und den berechneten Leistungsabfall festlegen.

- **Port**
  Zeigt die optischen Ports an, die Fiber Monitoring unterstützen. Dies ist von den Transceivern abhängig.
- **Status**
  Aktivieren oder deaktivieren Sie Fiber Monitoring.
  Defaultmäßig ist die Funktion deaktiviert.
- **Rx-Leistung [dBm] Wartungsbedarf (Warning)**
  Tragen Sie den Wert ein, bei dem Sie durch eine Meldung des Severity-Levels "Warning" über die Verschlechterung der Empfangsleistung informiert werden.
  Wenn Sie den Wert "0" eintragen, wird die Empfangsleistung nicht überwacht.
  Der Default-Wert ist von dem jeweiligen Transceiver abhängig.

- **Rx-Leistung [dBm] Wartungsanforderung (Critical)**
  Tragen Sie den Wert ein, bei dem Sie durch eine Meldung des Severity-Levels "Critical" über die Verschlechterung der Empfangsleistung informiert werden.
  Wenn Sie den Wert "0" eintragen, wird die Empfangsleistung nicht überwacht.
  Der Default-Wert ist von dem jeweiligen Transceiver abhängig.
- **Leistungsabfall [dB] Wartungsbedarf (Warning)**
  Tragen Sie den Wert ein, bei dem Sie durch eine Meldung des Severity-Levels "Warning" über den Leistungsabfall der Verbindung informiert werden.
  Wenn Sie den Wert "0" eintragen, wird der Leistungsabfall nicht überwacht.
  Default-Wert: -50 dB
- **Leistungsabfall [dB] Wartungsanforderung (Critical)**
  Tragen Sie den Wert ein, bei dem Sie durch eine Meldung des Severity-Levels "Critical" über den Leistungsabfall der Verbindung informiert werden.
  Wenn Sie den Wert "0" eintragen, wird der Leistungsabfall nicht überwacht.
  Default-Wert: -55 dB

Vorgehensweise zur Konfiguration

Fiber Monitoring aktivieren

Um die Überwachung eines Ports zu aktivieren, gehen Sie wie folgt vor:

1. Aktivieren Sie das entsprechende Optionskästchen in der Spalte "Status".
2. Tragen Sie für Ihren Aufbau sinnvolle Werte ein, bei denen Sie über eine Verschlechterung der Empfangsleistung und des Leistungsabfalls der Verbindung informiert werden wollen.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Fiber Monitoring deaktivieren

Um die Überwachung eines Ports zu deaktivieren, gehen Sie wie folgt vor:

1. Deaktivieren Sie das entsprechende Optionskästchen in der Spalte "Status".
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Um nur die Überwachung der Rx-Leistung bzw. des Leistungsabfalls zu deaktivieren, gehen Sie wie folgt vor:

1. Tragen Sie in das entsprechende Feld den Wert "0" ein.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.16 Unicast

5.5.16.1 Filtering

Adressfilterung

Diese Tabelle zeigt die Quelladressen von Unicast-Adresstelegrammen, die statisch durch Parametrierung des Anwenders eingetragen wurden.

Auf dieser Seite definieren Sie auch die statischen Unicast-Filter.

Abhängigkeit vom "Base Bridge-Modus"

Die angezeigten Felder sind davon abhängig, welcher "Base Bridge-Modus" eingestellt ist. Wenn Sie den "Base Bridge-Modus" ändern, gehen die bestehenden Einträge verloren.

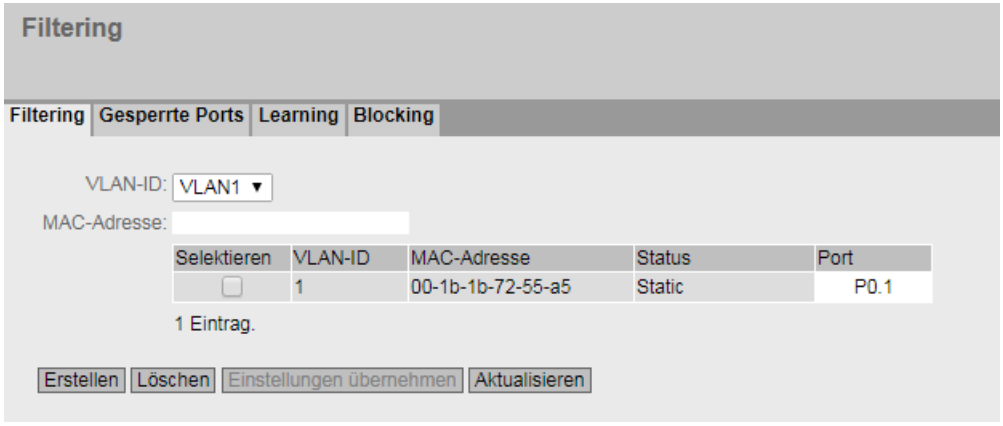


Bild 5-5 Base Bridge-Modus: 802.1Q VLAN Bridge

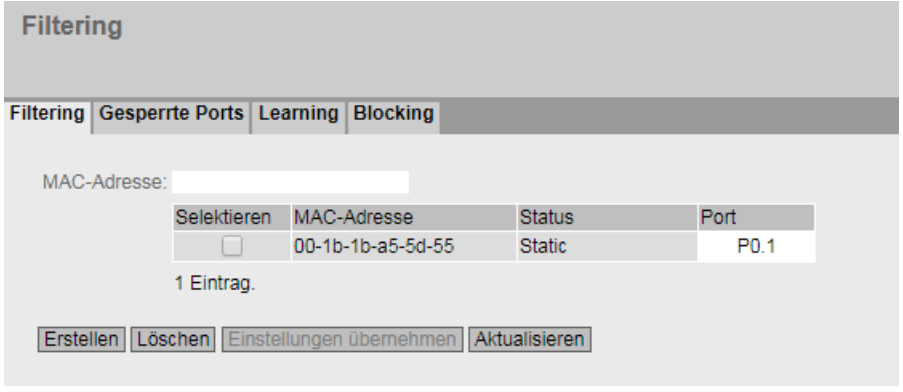


Bild 5-6 Base Bridge-Modus: 802.1D Transparent Bridge

Beschreibung der angezeigten Felder

Die Seite kann folgende Felder enthalten:

- **VLAN-ID**
  Wählen Sie die VLAN-ID aus, für die Sie eine neue MAC-Adresse statisch konfigurieren. Wenn nichts vorgegeben wird, ist "VLAN1" als Grundeinstellung parametriert.
- **MAC-Adresse**
  Tragen Sie hier die MAC-Adresse ein.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **VLAN-ID**
  Zeigt die VLAN-ID, der diese MAC-Adresse zugeordnet ist.
- **MAC-Adresse**
  Zeigt die MAC-Adresse des Teilnehmers, die das Gerät gelernt hat oder die der Anwender projektiert hat.
- **Status** - Static
  Zeigt den Status jedes Adress-Eintrags. Die Adresse wurde vom Anwender statisch eingetragen. Statische Adressen sind permanent gespeichert, d.h. sie werden nicht nach Ablauf der Aging-Time oder beim Neustart des Geräts gelöscht. Sie müssen vom Anwender gelöscht werden.
- **Port**
  Zeigt an, über welchen Port der Teilnehmer mit der angegebenen Adresse erreichbar ist. Vom Gerät empfangene Telegramme, deren Zieladresse mit dieser Adresse übereinstimmt, werden an diesen Port weitergegeben.

Hinweis

Für Unicast-Adressen können Sie nur **einen** Port angeben.

Vorgehensweise zur Konfiguration

Zur Bearbeitung der Einträge gehen Sie folgendermaßen vor.

Neuen Eintrag erstellen

1. Wählen Sie im "Base Bridge-Modus: 802.1Q VLAN Bridge" die entsprechende VLAN-ID aus.
2. Geben Sie die MAC-Adresse in das Eingabefeld "MAC-Adresse" ein.
3. Klicken Sie auf die Schaltfläche "Erstellen", um einen neuen Eintrag in der Tabelle zu erstellen.
4. Klicken Sie auf die Schaltfläche "Aktualisieren".
5. Wählen Sie aus der Klappliste den entsprechenden Port aus.
6. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Eintrag ändern

1. Wählen Sie den entsprechenden Port aus.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Eintrag löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
   Wiederholen Sie den Vorgang für alle Einträge, die Sie löschen wollen.
2. Um die selektierten Einträge aus der Filtertabelle zu löschen, klicken Sie auf die Schaltfläche "Löschen".
3. Klicken Sie auf die Schaltfläche "Aktualisieren".

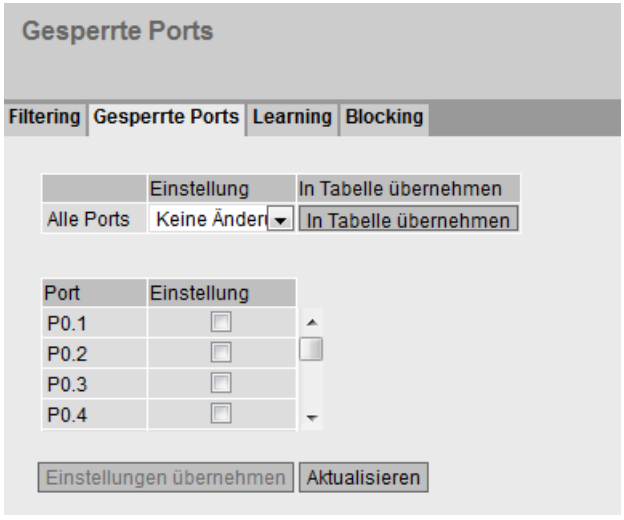
5.5.16.2 Gesperrte Ports

Aktivierung der Zugangskontrolle

Auf dieser Seite können Sie einzelne Ports für unbekannte Teilnehmer sperren.

Wenn die Port Lock-Funktion aktiviert ist, werden Pakete an diesem Port, die von unbekannten MAC-Adressen kommen, sofort verworfen. Die Pakete von bekannten Teilnehmern werden vom Port angenommen.
Da Ports mit aktivierter Port Lock-Funktion auch keine MAC-Adressen lernen, werden gelernte Adressen auf diesen Ports nach Aktivieren der Port Lock-Funktion automatisch ausgetragen. Der Port akzeptiert nur statische MAC-Adressen, die vorher entweder manuell oder mit der "Lernprozess starten"-Funktion und der "Lernprozess stoppen"-Funktion erstellt wurden.

Um alle angeschlossenen Teilnehmer automatisch statisch einzutragen, gibt es eine Funktion zum automatischen Lernen (siehe "Layer 2 > Unicast > Learning").



Beschreibung der angezeigten Felder

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - Aktiviert
    Aktiviert die Port Lock-Funktion.
  - Deaktiviert
    Deaktiviert die Port Lock-Funktion.
  - Keine Änderung
    Tabelle 2 bleibt unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  In dieser Spalte werden alle in diesem Gerät verfügbaren Ports aufgeführt.
- **Einstellung**
  Aktivieren oder deaktivieren Sie die Zugriffssteuerung für den Port.

Vorgehensweise zur Konfiguration

Zugriffssteuerung für einen einzelnen Port aktivieren

1. Aktivieren Sie in der Tabelle 2 in der entsprechenden Zeile das Optionskästchen.
2. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Zugriffssteuerung für alle Ports aktivieren

1. Wählen Sie in der Tabelle 1 in der Klappliste "Einstellung" den Eintrag "Aktiviert".
2. Klicken Sie auf die Schaltfläche "In Tabelle übernehmen". In der Tabelle 2 wird bei allen Ports das Optionskästchen aktiviert.
3. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

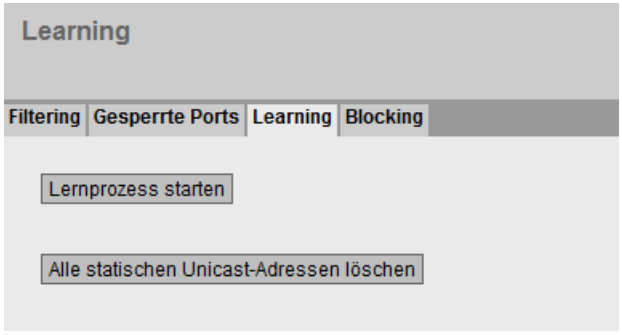
5.5.16.3 Learning

Lernprozess starten/stoppen

Mit Hilfe des automatischen Lernens können alle angeschlossenen Geräte automatisch statisch in die Unicast-Filtertabelle eingetragen werden.
Der Lernvorgang wird erst wieder durch Klicken auf die Schaltfläche "Lernprozess stoppen" beendet. Auf diese Weise kann wenige Minuten oder in größeren Netzen auch mehrere Stunden lang gelernt werden, um alle Teilnehmer zu finden. Es können nur Teilnehmer gefunden werden, die während des Lernens Pakete senden.
Durch anschließendes Aktivieren der Port Lock-Funktion werden auf den entsprechenden Ports nur noch Pakete von den nach Beendigung des Lernvorgangs bekannten Teilnehmern (statische Unicast-Einträge) angenommen.

Hinweis

Ist die Port Lock-Funktion auf einzelnen Ports bereits vor dem automatischen Lernen aktiv, werden auf diesen Ports keine Adressen gelernt. Auf diese Weise ist es möglich nur auf bestimmten Ports zu lernen. Aktivieren Sie hierzu vorher die Port Lock-Funktion auf den Ports, die keine Adressen lernen sollen.



Vorgehensweise zur Konfiguration

Adressen lernen

1. Klicken Sie auf die Schaltfläche "Lernprozess starten", um den Lernvorgang zu starten. Nach dem Starten des Lernvorgangs wird die Schaltfläche "Lernprozess starten" durch die Schaltfläche "Lernprozess stoppen" ersetzt.
   Das Gerät trägt nun solange die Adressen angeschlossener Geräte ein, bis Sie den Vorgang anhalten.
2. Klicken Sie auf die Schaltfläche "Lernprozess stoppen", um den Lernvorgang anzuhalten. Die Schaltfläche wird wieder durch die Schaltfläche "Lernprozess starten" ersetzt. Die gelernten Einträge werden gespeichert und sind unter "Layer 2 > Unicast > Filtering" aufgelistet.

Hinweis

Bei einer sehr hohen Datenrate kann es dazu kommen, dass statisch eingetragene Unicast-Adressen in der Unicast-Tabelle als gelernte Adressen angezeigt werden. In diesem Fall ist folgende Vorgehensweise empfehlenswert:

1. Klicken Sie auf die Schaltfläche "Lernprozess starten", um den Lernvorgang zu starten.
2. Starten Sie den Datenverkehr.
3. Warten Sie, bis die Unicast-Tabelle alle MAC-Adressen als "Learnt" anzeigt (Menü "Information > Unicast").
4. Sperren Sie die Ports (Menü "Layer 2 > Unicast > Gesperrte Ports").
5. Klicken Sie auf die Schaltfläche "Lernprozess stoppen", um den Lernvorgang anzuhalten.

Alle statischen Unicast-Adressen löschen

1. Klicken Sie auf die Schaltfläche "Alle statischen Unicast-Adressen löschen", um alle statischen Einträge zu löschen.
   In großen Netzen mit sehr vielen Teilnehmern kann das automatische Lernen eventuell zu vielen unerwünschten statischen Einträgen führen. Um diese nicht einzeln löschen zu müssen, gibt es über diese Schaltfläche die Möglichkeit, alle statischen Einträge zu löschen. Diese Funktion ist während des automatischen Lernens deaktiviert.

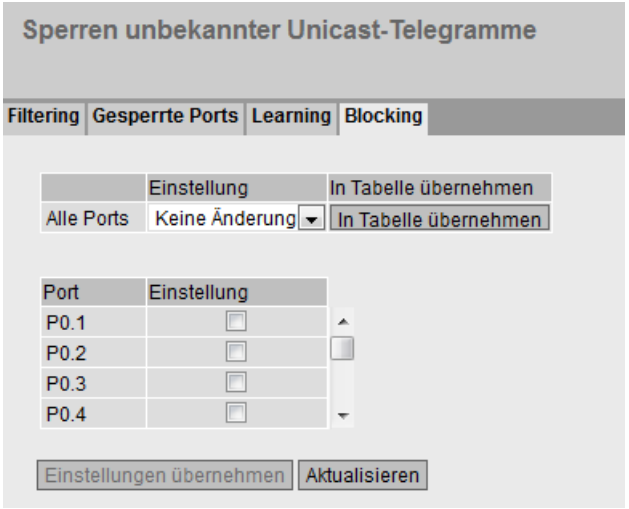
   Hinweis

   Das Löschen kann je nach Anzahl der Einträge einige Zeit in Anspruch nehmen.

5.5.16.4 Blocking

Weiterleitung von unbekannten Unicast-Telegrammen sperren

Auf dieser Seite wird das Weiterleiten von unbekannten Unicast-Telegrammen für einzelne Ports gesperrt.



Beschreibung der angezeigten Werte

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - Aktiviert
    Blocken von Unicast-Telegrammen ist aktiviert.
  - Deaktivert
    Blocken von Unicast-Telegrammen ist deaktiviert.
  - Keine Änderung
    Tabelle 2 bleibt unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.

  Hinweis

  Ringredundanz/Standby

  Wenn Ringredundanz oder Standby aktiviert sind, werden die hierfür konfigurierten Ports vom Unicast Blocking ausgenommen.

- **Einstellung**
  Aktivieren oder deaktivieren Sie das Sperren von Unicast-Telegrammen.

Vorgehensweise zu Konfiguration

Das Blocken für einen einzelnen Port aktivieren

1. Aktivieren Sie in der Tabelle 2 in der entsprechenden Zeile das Optionskästchen.
2. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Das Blocken für alle Ports aktivieren

1. Wählen Sie in der Tabelle 1 in der Klappliste "Einstellung" den Eintrag "Aktiviert".
2. Klicken Sie auf die Schaltfläche "In Tabelle übernehmen". In der Tabelle 2 wird bei allen Ports das Optionskästchen aktiviert.
3. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.17 Multicast

5.5.17.1 Gruppen

Multicast-Anwendungen

In der Mehrzahl der Fälle wird ein Telegramm mit einer Unicast-Adresse an einen bestimmten Empfänger gesendet. Wenn eine Anwendung die gleichen Daten an mehrere Empfänger senden soll, kann das zu sendende Datenvolumen reduziert werden, indem die Daten über eine Multicast-Adresse an alle gesendet werden. Für manche Anwendungen gibt es feste Multicast-Adressen (NTP, IETF1-Audio, IETF1-Video usw.).

Reduzierung der Netzlast

Im Gegensatz zu Unicast-Telegrammen bewirken Multicast-Telegramme eine höhere Last für das Gerät. Generell werden Multicast-Telegramme an allen Ports versendet. Es gibt folgende Möglichkeiten, die Last durch Multicast-Telegramme zu reduzieren:

- Statischer Eintrag der Adressen in die Multicast-Filtertabelle.
- Dynamischer Eintrag der Adressen durch Mithören von IGMP-Parametriertelegrammen (IGMP-Konfiguration).
- Aktive dynamische Vergabe von Adressen durch GMRP-Telegramme.

Alle genannten Verfahren haben zur Folge, dass Multicast-Telegramme nur an solche Ports versendet werden, für die eine entsprechende Adresse eingetragen ist.

Der Menüpunkt "Multicast " zeigt die aktuell in der Filtertabelle eingetragenen Multicast-Telegramme mit ihren Zielports, die der Anwender parametriert hat (statisch).

Abhängigkeit vom "Base Bridge-Modus"

Die angezeigten Felder sind davon abhängig, welcher "Base Bridge-Modus" eingestellt ist. Wenn Sie den "Base Bridge-Modus" ändern, gehen die bestehenden Einträge verloren.

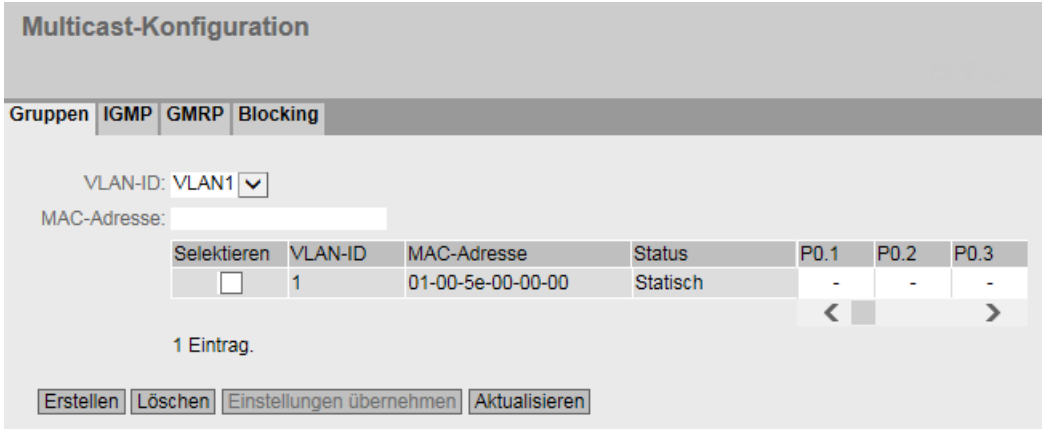


Bild 5-7 Base Bridge-Modus: 802.1Q VLAN Bridge

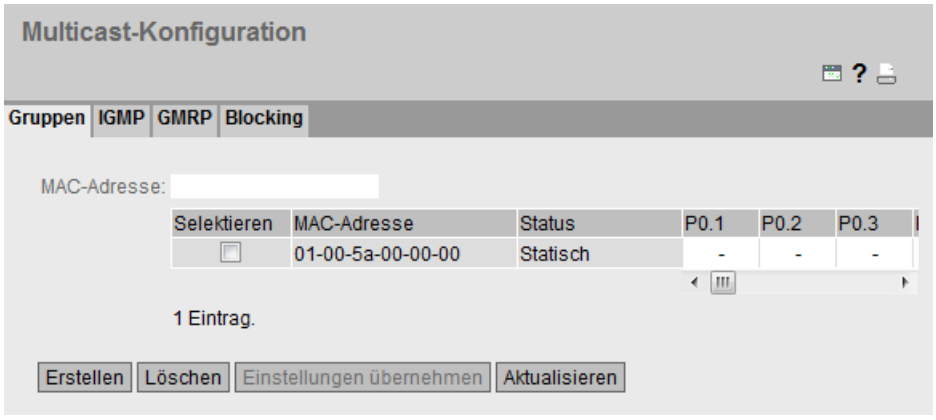


Bild 5-8 Base Bridge-Modus: 802.1D Transparent Bridge

Beschreibung der angezeigten Felder

Die Seite kann folgende Felder enthalten:

- **VLAN-ID**
  Wenn Sie auf dieses Textfeld klicken, wird Ihnen eine Klappliste angeboten. Hier können Sie die VLAN-ID einer neu zu projektierenden MAC-Adresse auswählen.
- **MAC-Adresse**
  Hier geben Sie eine neu zu projektierende MAC-Multicast-Adresse ein.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **VLAN-ID**
  Hier wird die VLAN-ID des VLANs angezeigt, dem die MAC-Multicast-Adresse dieser Zeile zugeordnet ist.
- **MAC-Adresse**
  Hier wird die MAC-Multicast-Adresse angezeigt, die das Gerät gelernt hat oder die der Anwender projektiert hat.

- **Status -** Statisch
  Zeigt den Status jedes Adress-Eintrags. Die Adresse wurde vom Anwender statisch eingetragen. Statische Adressen sind permanent gespeichert, d.h. sie werden nicht nach Ablauf der Aging-Time oder beim Neustart des Geräts gelöscht. Sie müssen vom Anwender gelöscht werden.
- **Liste der Ports**
  Für jeden Port gibt es eine Spalte. In jeder Spalte wird die Zugehörigkeit zur Multicast-Gruppe angegeben. Folgende Auswahlmöglichkeiten gibt es bei der Klappliste:
  - M
    (Member) Über diesen Port werden Multicast-Telegramme gesendet.
  - R
    (Registered) Mitglied der Multicast-Gruppe, die Registrierung erfolgte über ein GMRP-Telegramm.
  - I
    (IGMP) Mitglied der Multicast-Gruppe, die Registrierung erfolgte über ein IGMP-Telegramm. Dieser Wert wird nur dynamisch vergeben.
  - –
    Kein Mitglied der Multicast-Gruppe. Über diesen Port werden keine Multicast-Telegramme mit der definierten Multicast-MAC-Adresse gesendet.
  - F
    (Forbidden) Kein Mitglied der Multicast-Gruppe. Außerdem darf diese Adresse nicht dynamisch über GMRP oder IGMP gelernt werden.

Vorgehensweise zur Konfiguration

Neuen Eintrag erstellen

Hinweis

Sie können keine statischen Multicast-Einträge anlegen, wenn GMRP aktiviert ist.

1. Wählen Sie im "Base Bridge-Modus: 802.1Q VLAN Bridge" aus der Klappliste "VLAN-ID" die gewünschte VLAN-ID aus.
2. Tragen Sie in das Eingabefeld "MAC-Adresse" die MAC-Adresse ein.
3. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.
4. Weisen Sie der MAC-Adresse die entsprechenden Ports zu.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Eintrag löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Löschen".
   Alle markierten Einträge werden gelöscht und die Anzeige wird aktualisiert.

Layer 2-Multicast-Adressen über ein Skript anlegen und GMRP

Wenn Sie mehrere Layer 2-Multicast-Adressen über ein Skript anlegen wollen, muss GMRP deaktiviert sein, solange das Skript ausgeführt wird. Gehen Sie wie folgt vor:

1. Wenn GMRP aktiviert ist, deaktivieren Sie es. GMRP konfigurieren Sie auf der Seite "Layer 2 > Multicast > GMRP".
2. Führen Sie das Skript aus.
3. Aktivieren Sie GMRP erst, nachdem das Skript vollständig durchgelaufen ist und die Layer 2-Multicast-Adressen angelegt sind.

5.5.17.2 IGMP

Funktion

Das Gerät unterstützt "IGMP Snooping" und die "IGMP Querier"-Funktion. Ist "IGMP Snooping" aktiviert, so werden IGMP-Telegramme (Internet Group Management Protocol) ausgewertet und mit diesen Informationen die Multicast-Filtertabelle aktualisiert. Ist zusätzlich "IGMP Querier" aktiviert, so versendet das Gerät auch IGMP-Anfragen, die bei IGMP-fähigen Teilnehmern Antworten auslösen.

IGMP Snooping Aging Time

Mit diesem Menü können Sie die Aging-Time für die IGMP-Konfiguration festlegen. Nach Ablauf dieser Zeit werden durch IGMP erzeugte Einträge aus der Adresstabelle gelöscht, wenn diese nicht durch ein neues IGMP-Telegramm aktualisiert werden.

Die Festlegung gilt für alle Ports und VLANs, eine spezifische Konfiguration ist nicht möglich.

IGMP Snooping Aging Time in Anhängigkeit des Queriers

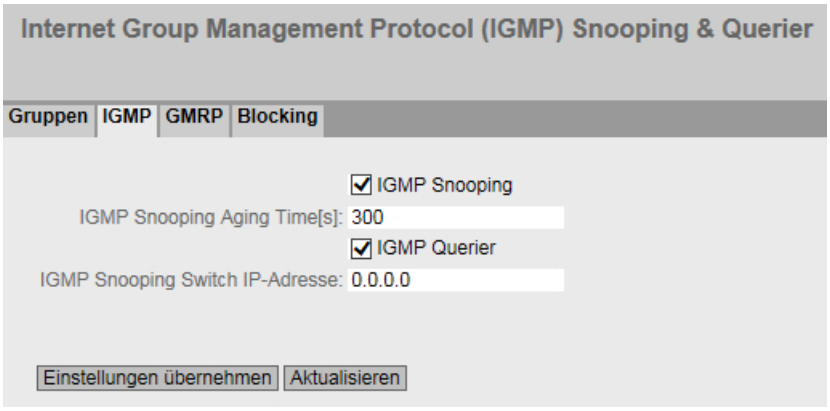
Der IE-Switch als IGMP-Querier

Wenn der IE-Switch als IGMP-Querier verwendet wird, beträgt das Query-Intervall 125 Sekunden. Stellen Sie bei der "IGMP Snooping Aging Time" mindestens 250 Sekunden ein.

Andere IGMP-Querier

Wenn ein anderer IGMP-Querier verwendet wird, sollte der Wert der "IGMP Snooping Aging Time" mindestens doppelt so groß sein wie das Query-Intervall.

Beschreibung der angezeigten Felder



Die Seite enthält folgende Felder:

- **IGMP Snooping**
  Aktivieren oder deaktivieren Sie IGMP Snooping. Die Funktion ermöglicht die Zuordnung von IP-Adressen zu Multicast-Gruppen. Wenn die Option aktiviert ist, werden IGMP-Einträge in die Multicast-Filtertabelle aufgenommen und IGMP-Telegramme weitergeleitet.
- **IGMP Snooping Aging Time[s]**
  Tragen Sie in dieses Feld den Wert für die Aging Time in Sekunden ein. Standardmäßig sind 300 Sekunden eingestellt
  Gültige Werte: 130 - 1225 Sekunden
- **IGMP Querier**
  Aktivieren oder deaktivieren Sie "IGMP Querier". Das Gerät verschickt IGMP-Anfragen.
- **IGMP Snooping Switch IP Address**
  Nach dem Aktivieren des Optionskästchens "IGMP Querier" wird hier die IP-Adresse des Geräts angezeigt. Optional können Sie die IP-Adresse eines anderen Geräts eintragen, das die Funktion des IGMP Queriers übernehmen soll.

Vorgehensweise zur Konfiguration

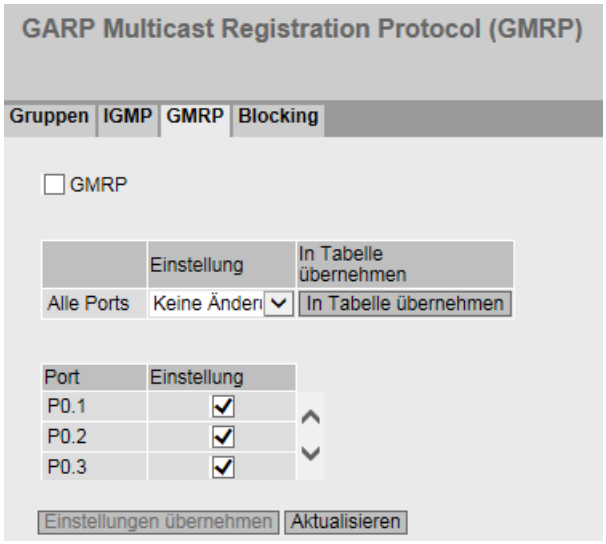
1. Aktivieren Sie das Optionskästchen "IGMP Snooping".
2. Tragen Sie in das Feld "IGMP Snooping Aging Time" den Wert für die Aging-Time in Sekunden ein.
3. Aktivieren Sie das Optionskästchen "IGMP Querier".
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.17.3 GMRP

Aktivierung von GMRP

Auf dieser Seite legen Sie individuell für jeden Port fest, ob GMRP angewendet wird. Wenn für einen Port "GMRP" deaktiviert ist, werden für ihn keine Registrierungen durchgeführt und er kann keine GMRP-Telegramme versenden.

Damit GMRP funktioniert, müssen Sie die Funktion global und auf den Ports aktivieren.



Beschreibung der angezeigten Felder

Die Seite enthält folgendes Feld:

- **GMRP**
  Aktivieren oder deaktivieren Sie die GMRP-Funktion.

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - Aktiviert
    Aktiviert das Versenden von GMRP-Telegrammen.
  - Deaktiviert
    Deaktiviert das Versenden von GMRP-Telegrammen.
  - Keine Änderung
    Tabelle 2 bleibt unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, werden die Einstellungen für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  In dieser Spalte werden alle im Gerät verfügbaren Ports und auch die Link-Aggregationen angezeigt.
- **Einstellung**
  Mit Hilfe dieses Optionskästchens aktivieren oder deaktivieren Sie GMRP für den Port oder die Link-Aggregation.

Vorgehensweise zur Konfiguration

Senden von GMRP-Telegrammen für einen einzelnen Port aktivieren

1. Aktivieren Sie das Optionskästchen "GMRP".
2. Aktivieren Sie in der Tabelle 2 in der entsprechenden Zeile das Optionskästchen.
3. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

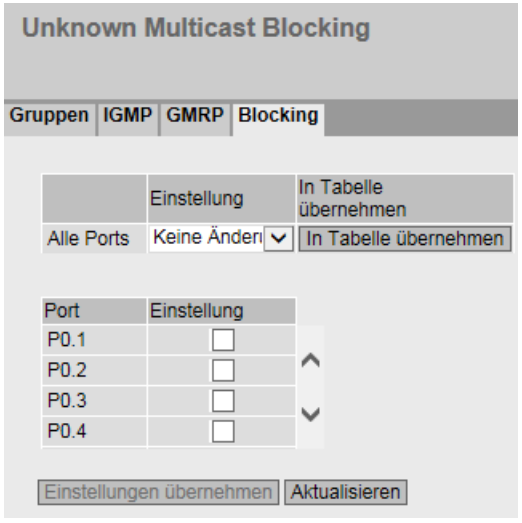
Senden von GMRP-Telegrammen für alle Ports aktivieren

1. Aktivieren Sie das Optionskästchen "GMRP".
2. Wählen in der Klappliste "Einstellung" den Eintrag "Aktiviert".
3. Klicken Sie auf die Schaltfläche "In Tabelle übernehmen". In der Tabelle 2 wird bei allen Ports das Optionskästchen aktiviert.
4. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.17.4 Multicast Blocking

Sperrung der Weiterleitung von unbekannten Multicast-Telegrammen

Auf der Seite wird das Weiterleiten von unbekannten Multicast-Telegrammen für einzelne Ports gesperrt.



Beschreibung der angezeigten Werte

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - Aktiviert
    Blocken von Multicast-Telegrammen ist aktiviert.
  - Deaktiviert
    Blocken von Multicast-Telegrammen ist deaktiviert.
  - Keine Änderung
    Tabelle 2 bleibt unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Alle verfügbaren Ports werden in dieser Spalte aufgeführt. Nicht verfügbare Ports werden nicht angezeigt.
- **Einstellung**
  Aktivieren oder deaktivieren Sie das Blocken von Multicast-Telegrammen.

Vorgehensweise zu Konfiguration

Das Blocken für einen einzelnen Port aktivieren

1. Aktivieren Sie in der Tabelle 2 in der entsprechenden Zeile das Optionskästchen.
2. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Das Blocken für alle Ports aktivieren

1. Wählen in der Klappliste "Einstellung" den Eintrag "Aktiviert".
2. Klicken Sie auf die Schaltfläche "In Tabelle übernehmen". In der Tabelle 2 wird bei allen Ports das Optionskästchen aktiviert.
3. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

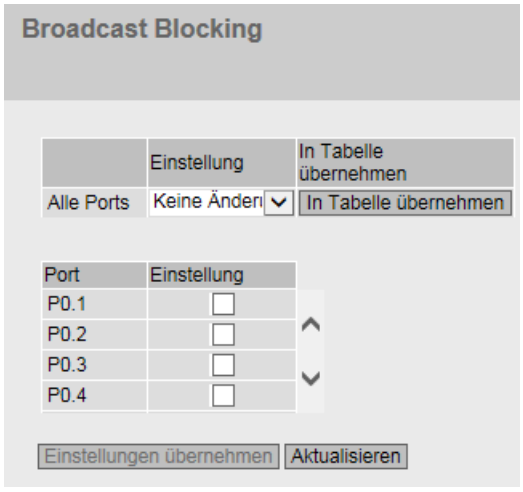
5.5.18 Broadcast

Sperrung der Weiterleitung von Broadcast-Telegrammen

Auf dieser Seite kann das Weiterleiten von Broadcast-Telegrammen für einzelne Ports gesperrt werden.

Hinweis

Einige Kommunikationsprotokolle funktionieren nur mit Unterstützung von Broadcast. In diesen Fällen kann das Sperren zum Ausfall der Datenkommunikation führen. Sperren Sie Broadcast nur, wenn Sie sicher sind, dass Sie auf den ausgewählten Ports darauf verzichten können.



Beschreibung der angezeigten Felder

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Einstellung**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - Aktiviert
    Das Blocken von Broadcast-Telegrammen ist aktiviert.
  - Deaktiviert
    Das Blocken von Broadcast-Telegrammen ist deaktiviert.
  - Keine Änderung
    Tabelle 2 bleibt unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Alle verfügbaren Ports werden angezeigt.
- **Einstellung**
  Aktivieren oder deaktivieren Sie das Blocken von Broadcast-Telegrammen.

Vorgehensweise zur Konfiguration

Das Blocken von Broadcast-Telegrammen für einen einzelnen Port aktivieren

1. Aktivieren Sie in der Tabelle 2 in der entsprechenden Zeile das Optionskästchen.
2. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Das Blocken von Broadcast-Telegrammen für alle Ports aktivieren

1. Wählen in der Klappliste "Einstellung" in Tabelle 1 den Eintrag "Aktiviert".
2. Klicken Sie auf die Schaltfläche "In Tabelle übernehmen". In der Tabelle 2 wird bei allen Ports das Optionskästchen aktiviert.
3. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.5.19 RMON

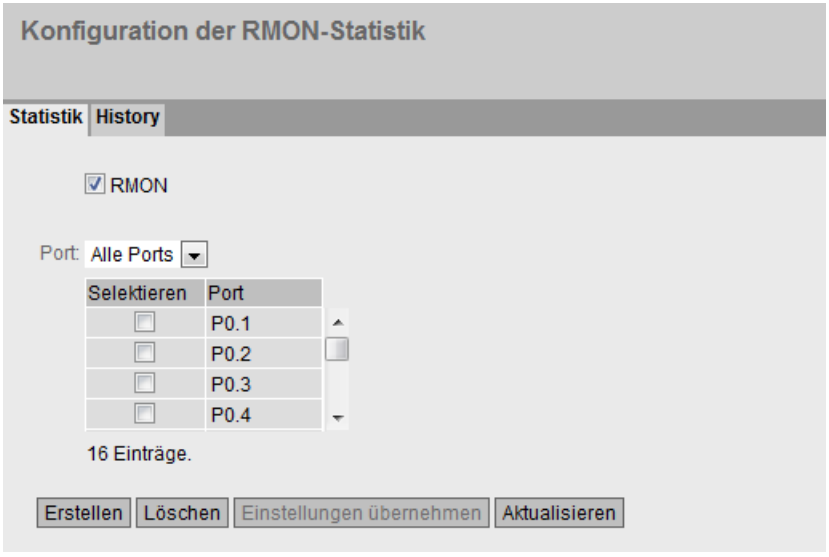
5.5.19.1 Statistik

Statistik

Auf dieser Seite können Sie festlegen, für welche Ports RMON-Statistiken angezeigt werden.

Die RMON-Statistiken werden auf der Seite "Information > Ethernet-Statistiken" in den Reitern "Telegrammlänge", "Telegrammtyp" und "Telegrammfehler" angezeigt.

Einstellungen



- **RMON**
  Wenn Sie dieses Optionskästchen aktivieren, ermöglicht Remote Monitoring (RMON), Diagnosedaten im Gerät zu sammeln, aufzubereiten und über SNMP von einer Netzwerkmanagement-Station, die ebenfalls RMON unterstützt, auszulesen. Diese Diagnosedaten, wie zum Beispiel portbezogene Lastverläufe, ermöglichen es, Probleme im Netzwerk frühzeitig zu erkennen und zu beseitigen.

  Hinweis

  Wenn Sie RMON deaktivieren, werden die Statistiken nicht gelöscht, sondern sie bleiben auf dem letzten Stand stehen.

- **Port**
  Wählen Sie die Ports aus, für die Statistiken angezeigt werden sollen.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Port**
  Zeigt die Ports an, für die Statistiken angezeigt werden.

Vorgehensweise zur Konfiguration

Funktion aktivieren

1. Aktivieren Sie das Optionskästchen "RMON".
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
   Die Funktion "RMON" ist aktiviert.

RMON-Statistiken für Ports aktivieren

Hinweis

Voraussetzung

Damit RMON-Statistiken für einen Port angezeigt werden können, muss die Funktion "RMON" aktiviert sein.

1. Wählen Sie aus der Klappliste "Port" den gewünschten Port oder den Eintrag "Alle Ports" aus.
2. Klicken Sie auf die Schaltfläche "Erstellen".
   Für den gewählten Port bzw. alle Ports können RMON-Statistiken angezeigt werden.

RMON-Statistiken für Ports deaktivieren

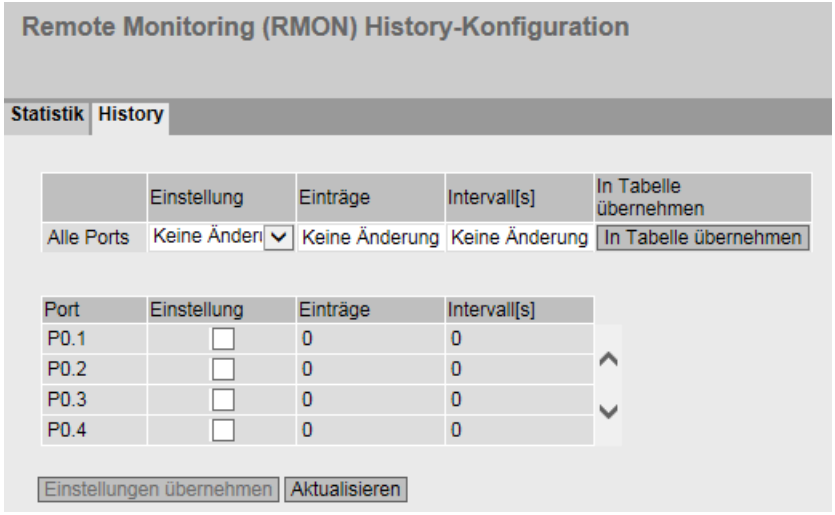
1. Aktivieren Sie in der Spalte "Selektieren" die Zeile, die Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Löschen".
   Für den gewählten Port werden keine RMON-Statistiken angezeigt.

5.5.19.2 History

Stichproben der Statistiken

Auf dieser Seite können Sie festlegen, ob für einen Port Stichproben der Statistiken abgespeichert werden sollen. Sie können festlegen, wie viele Einträge gespeichert werden sollen und in welchem Intervall Stichproben genommen werden sollen.

Einstellungen



Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports gültig sind.
- **Einstellung**
  Wählen Sie die gewünschte Einstellung. Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **Einträge**
  Tragen Sie die maximale Anzahl der Stichproben ein, die gleichzeitig gespeichert werden sollen. Wenn "Keine Änderung" eingetragen ist, bleibt der Eintrag in der Tabelle 2 unverändert.

- **Intervall[s]**
  Tragen Sie ein Intervall ein, nachdem der aktuelle Stand der Statistik als Stichprobe gespeichert werden soll. Wenn "Keine Änderung" eingetragen ist, bleibt der Eintrag in der Tabelle 2 unverändert.

  Hinweis

  Beachten Sie bei der Festlegung der Intervalldauer, dass nur ein Vielfaches von 3 Sekunden als Intervalldauer sinnvoll ist. Die Statistiken werden alle 3 Sekunden aktualisiert. In den Zeiträumen dazwischen wird der Wert "0" ausgegeben.

- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, werden die Einstellungen für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt den Port an, auf den sich die Einstellungen beziehen.
- **Einstellung**
  Aktivieren oder deaktivieren Sie die Aufzeichnung der History auf dem entsprechenden Port.
- **Einträge**
  Tragen Sie die maximale Anzahl der Stichproben ein, die gleichzeitig gespeichert werden sollen.
  Die maximale Anzahl an Einträgen kann durch die Kapazität des Geräts beschränkt werden.
  Wertebereich: 1 - 65535
  Werkseinstellung: 24
- **Intervall[s]**
  Tragen Sie ein Intervall ein, nachdem der aktuelle Stand der Statistik als Stichprobe gespeichert werden soll.
  Wertebereich: 1 - 3600
  Werkseinstellung: 3600

  Hinweis

  Beachten Sie bei der Festlegung der Intervalldauer, dass nur ein Vielfaches von 3 Sekunden als Intervalldauer sinnvoll ist. Die Statistiken werden alle 3 Sekunden aktualisiert. In den Zeiträumen dazwischen wird der Wert "0" ausgegeben.

Vorgehensweise zur Konfiguration

RMON-Statistiken für einzelne Ports aktivieren

1. Aktivieren Sie in der Tabelle 2 das Optionskästchen "Einstellung" in der entsprechenden Zeile.
   Die Felder "Einträge" und "Intervall[s]" werden mit den Werkseinstellungen aktiv.
2. Geben Sie in den Feldern "Einträge" und "Intervall[s]" die gewünschten Werte ein.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

RMON-Statistiken für alle Ports aktivieren

1. Wählen Sie in der Tabelle 1 in der Klappliste "Einstellung" den Eintrag "Aktiviert".
2. Geben Sie in den Feldern "Einträge" und "Intervall[s]" die gewünschten Werte ein. Wenn Sie die Einträge in den beiden Feldern nicht ändern, werden für alle Ports die Werkseinstellungen verwendet.
3. Klicken Sie auf die Schaltfläche "In Tabelle übernehmen".
   Die Einstellungen werden für alle Ports der Tabelle 2 übernommen.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.6 Das Menü "Layer 3"

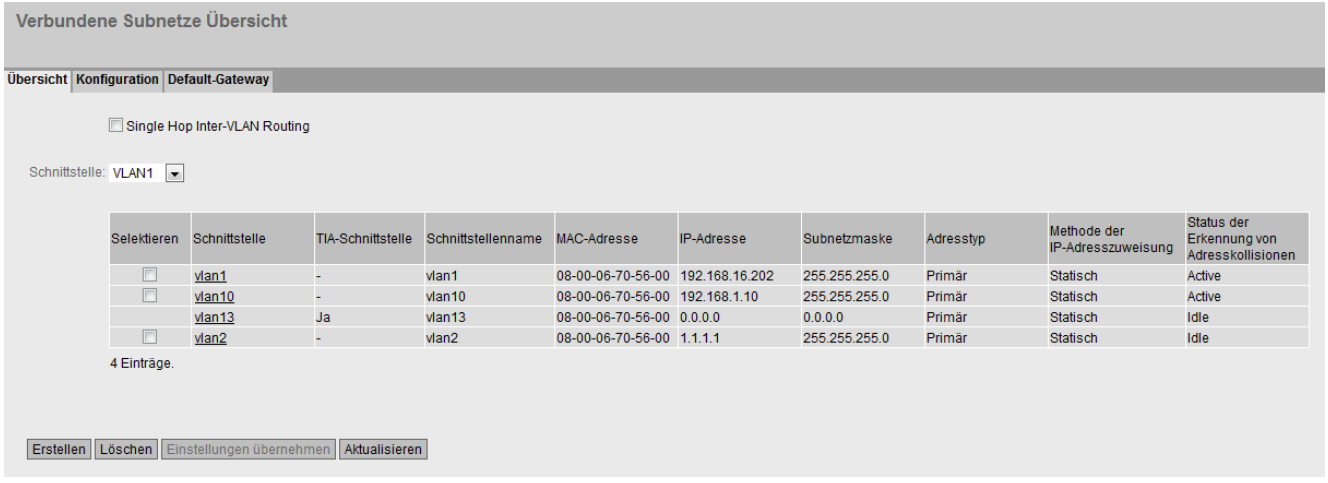
5.6.1 Subnetze

5.6.1.1 Übersicht

Erstellen von Subnetzen

Auf dieser Seite können Sie für das Gerät mehrere VLAN-IP-Schnittstellen erstellen.

Ein Subnetz bezieht sich immer auf ein VLAN. Die IP-Adresse wird in dem Register "Konfiguration" zugeordnet.



Beschreibung der angezeigten Werte

Die Seite enthält folgende Felder:

- **Single-Hop Inter-VLAN-Routing**
  Aktivieren oder deaktivieren Sie das Routing zwischen lokalen IP-Schnittstellen.
- **Schnittstelle**
  Wählen Sie die gewünschte Schnittstelle aus, für die Sie ein weiteres IP-Subnetz projektieren.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Schnittstelle**
  Zeigt die Schnittstelle an.
- **TIA-Schnittstelle**
  Zeigt die ausgewählte TIA-Schnittstelle an.
- **Schnittstellenname**
  Zeigt den Namen der Schnittstelle.
- **MAC-Adresse**
  Zeigt die MAC-Adresse an.
- **IP-Adresse**
  Zeigt die IPv4-Adresse des Subnetzes an.
- **Subnetzmaske**
  Zeigt die Subnetzmaske.
- **Adresstyp**
  Zeigt den Adressentyp an. Folgende Werte sind möglich:
  - Primär
    Die erste IPv4-Adresse, die auf einem IPv4-Schnittstelle konfiguriert wurde.

- **Methode der IP-Adresszuweisung**
  Zeigt an, wie die IPv4-Adresse zugeordnet wird. Folgende Werte sind möglich:
  - Statisch
    Die IPv4-Adresse ist statisch. Tragen Sie die Einstellungen bei "IP-Adresse" und "Subnetzmaske" ein.
  - Dynamisch (DHCP)
    Das Gerät bezieht eine dynamische IPv4-Adresse von einem DHCPv4-Server.
- **Status der Erkennung von Adresskollisionen**
  Wenn neue IPv4-Adressen im Netz aktiv werden, prüft die Funktion "Erkennung von Adresskollisionen ", ob es zu Adresskollisionen kommen kann. Dadurch werden IPv4-Adressen erkannt, die doppelt vergeben werden sollen.

  Hinweis

  Die Funktion führt keine zyklische Prüfung durch.

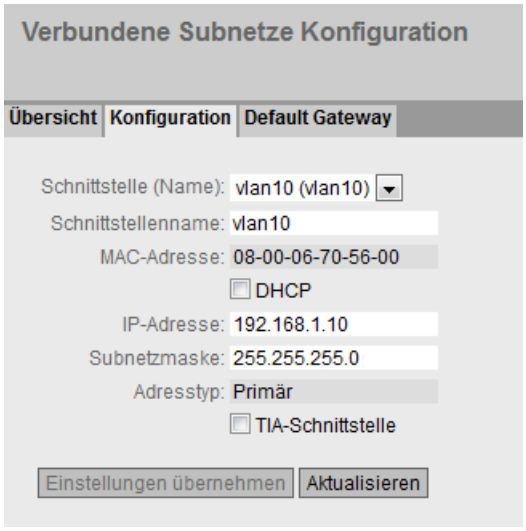
  Diese Spalte zeigt an, in welchem Status sich die Funktion befindet. Folgende Werte sind möglich:
  - Idle
    Die Schnittstelle ist nicht aktiv und besitzt keine IPv4-Adresse.
  - Starting
    Dieser Status bezeichnet die Anlaufphase. In dieser Phase sendet das Gerät zunächst eine Anfrage, ob es die geplante IPv4-Adresse bereits gibt. Wenn die Adresse noch nicht vergeben ist, sendet das Gerät die Mitteilung, dass es ab jetzt diese IP-Adresse verwendet.
  - Conflict
    Die Schnittstelle ist nicht aktiv. Die Schnittstelle versucht eine IPv4-Adresse zu verwenden, die bereits vergeben ist.
  - Defending
    Die Schnittstelle verwendet eine eindeutige IPv4-Adresse. Eine andere Schnittstelle versucht die gleiche IPv4-Adresse zu verwenden.
  - Active
    Die Schnittstelle verwendet eine eindeutige IPv4-Adresse. Es gibt keine Kollisionen.
  - Not supported
    Die Funktion zur Erkennung von Adresskollisionen wird nicht unterstützt.
  - Disabled
    Die Funktion zur Erkennung von Adresskollisionen ist deaktiviert.

Vorgehensweise zur Konfiguration

1. Wählen Sie aus der Klappliste "Schnittstelle" die Schnittstelle.
2. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird eine neue Zeile eingefügt.
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
4. Konfigurieren Sie das Subnetz in dem Register "Konfiguration".

5.6.1.2 Konfiguration

Auf dieser Seite konfigurieren Sie die IPv4-Schnittstelle.



Beschreibung der angezeigten Werte

Die Seite enthält folgende Felder:

- **Schnittstelle (Name)**
  Wählen Sie aus Klappliste die Schnittstelle aus.
- **Schnittstellenname**
  Tragen Sie den Namen für die Schnittstelle ein.
- **MAC-Adresse**
  Zeigt die MAC-Adresse der ausgewählten Schnittstelle an.
- **DHCP**
  Aktivieren oder deaktivieren Sie den DHCP-Client für dieses IPv4-Schnittstelle.
- **IP-Adresse**
  Tragen Sie die IPv4-Adresse der Schnittstelle ein. Die IPv4-Adressen dürfen nicht mehrfach verwendet werden.
- **Subnetzmaske**
  Tragen Sie die Subnetzmaske des zu erstellenden Subnetzes ein. Subnetze an unterschiedlichen Schnittstellen dürfen sich nicht überlappen.
- **Adresstyp**
  Zeigt den Typ der Adresse an. Folgende Werte sind möglich:
  - Primär
    Das erste Subnetz der Schnittstelle.
- **TIA-Schnittstelle**
  Wählen Sie aus, ob diese Schnittstelle zur TIA-Schnittstelle werden soll.

Vorgehensweise zur Konfiguration

1. Wählen Sie aus der Klappliste "Schnittstelle (Name)" die Schnittstelle.
2. Tragen Sie in bei "Schnittstellenname" einen Namen für die Schnittstelle ein.
3. Tragen Sie in der Spalte "IP-Adresse" die IPv4-Adresse des Subnetzes ein.
4. Tragen Sie in der Spalte "Subnetzmaske" die zur IPv4-Adresse gehörende Subnetzmaske ein
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

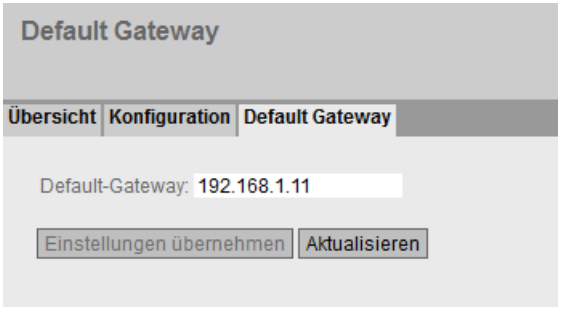
5.6.1.3 Default-Gateway

Erstellen von Subnetzen

Auf dieser Seite definieren Sie das Default-Gateway.

Hinweis

Wenn Sie für das Default-Gateway eine statische IP-Adresse konfigurieren, wird automatisch DHCP für das TIA-Interface deaktiviert. Dadurch wird verhindert, dass die Gateway-Adresse durch DHCP überschrieben wird. Falls erforderlich, können Sie DHCP anschließend wieder aktivieren.



Beschreibung der angezeigten Werte

Die Seite enthält folgende Felder:

- **Default-Gateway**
  Geben Sie die IP-Adresse der Schnittstelle ein, die als Default-Gateway verwendet wird.

Vorgehensweise zur Konfiguration

1. Geben Sie das Default-Gateway ein.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.6.2 DHCP Relay Agent

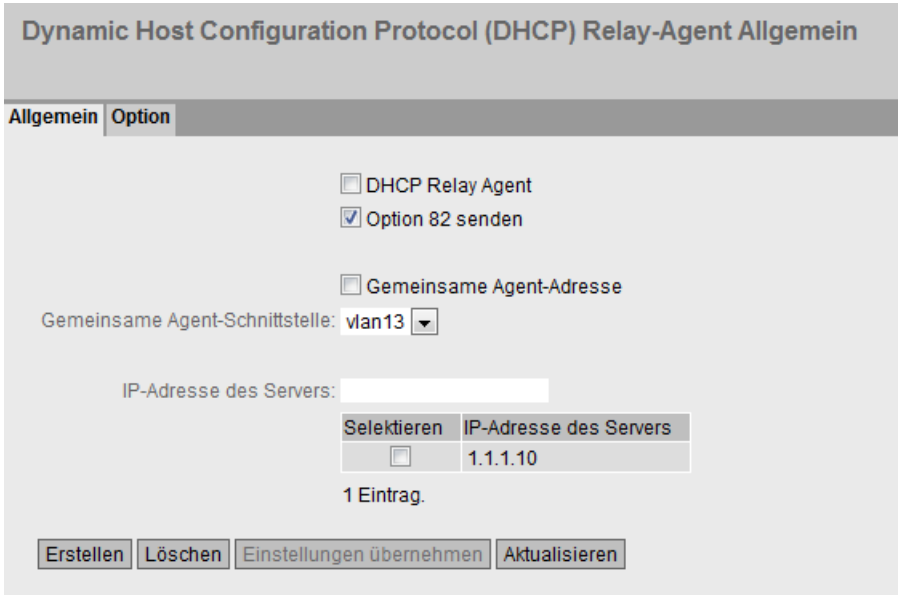
5.6.2.1 Allgemein

DHCP Relay Agent

Wenn sich der DHCP-Server in einem anderen Netz befindet als der DHCP-Client, kann der Client den Server nicht erreichen. Der DHCP Relay Agent vermittelt zwischen DHCP-Server und DHCP-Client.

Wenn Sie die Option 82 konfigurieren, erweitert der DHCP Relay Agent die Pakete an den DHCP-Server um eine Circuit-ID und eine Remote-ID.

Sie können für den DHCP Relay Agent bis zu 4 DHCP-Server angeben. Wenn ein DHCP-Server nicht erreichbar ist, kann das Gerät auf einen anderen DHCP-Server ausweichen.



Beschreibung der angezeigten Werte

Die Seite enthält folgende Felder:

- **DHCP Relay Agent**
  Aktivieren oder deaktivieren Sie den DHCP Relay Agent.
- **Option 82 senden**
  Aktivieren oder deaktivieren Sie die Option 82.
- **Gemeinsame Agent-Adresse**
  Aktivieren oder deaktivieren Sie die gemeinsame Agent-Adresse.
  Wenn die Funktion aktiviert ist, ersetzt der Relay Agent in der DHCP-Anfrage die Adresse des Empfangsports durch die Adresse der Schnittstelle, die Sie unter "Gemeinsame Agent-Schnittstelle" konfigurieren.

- **Gemeinsame Agent-Schnittstelle**
  Der Relay Agent verwendet die IP-Adresse der hier ausgewählten Schnittstelle als Quelladresse (giaddr) in DHCP-Anfragen.
- **IP-Adresse des Servers**
  Tragen Sie die IPv4-Adresse des DHCP-Servers ein.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **IP-Adresse des Servers**
  Zeigt die IPv4-Adresse des DHCP-Servers an.

Vorgehensweise zur Konfiguration

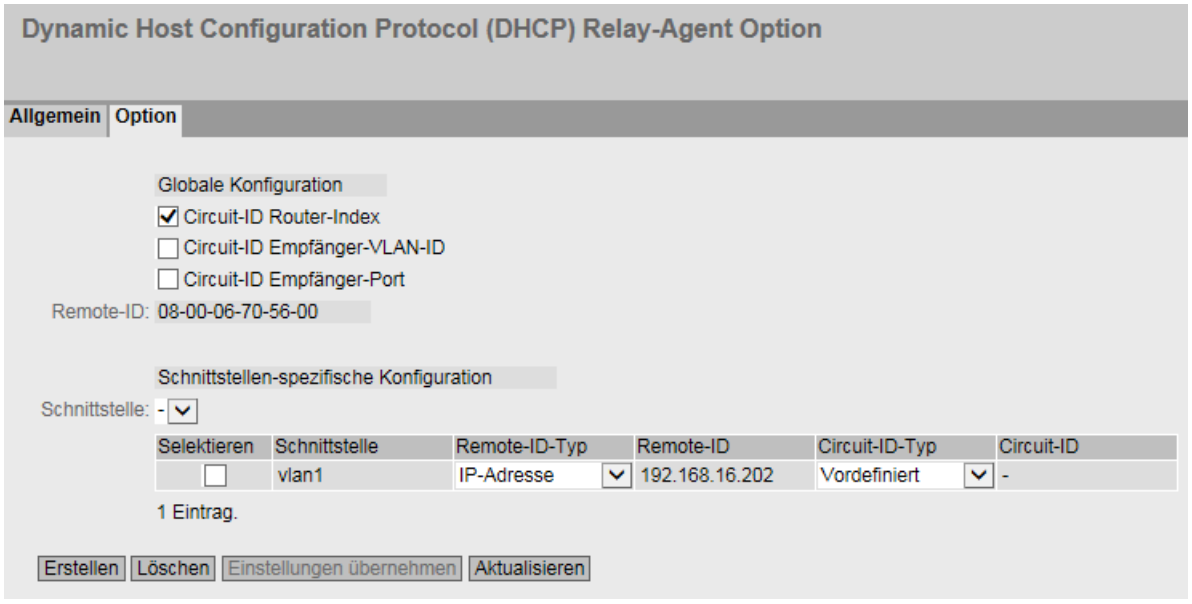
1. Tragen Sie in das Eingabefeld "IP-Adresse des Servers" die IPv4-Adresse des DHCP-Servers ein.
2. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt.
3. Aktivieren Sie das Optionskästchen "DHCP Relay Agent".
4. Aktivieren Sie das Optionskästchen "Option 82 senden".
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.6.2.2 Option

Parameter des DHCP Relay Agent

Auf dieser Seite können Sie Parameter für den DHCP-Server festlegen, z. B. die Circuit-ID. Die Circuit-ID beschreibt die Herkunft der DHCP-Anfrage, z. B. welcher Port die DHCP-Anfrage empfangen hat.

Die DHCP-Server legen Sie im Register "Allgemein" fest.



Beschreibung der angezeigten Werte

Die Seite enthält folgende Felder:

Globale Konfiguration

- **Circuit-ID Router-Index**
  Aktivieren oder deaktivieren Sie das Optionskästchen. Wenn Sie das Optionskästchen aktivieren, wird der erzeugten Circuit-ID der Router-Index hinzugefügt.
- **Circuit-ID Empfänger-VLAN-ID**
  Aktivieren oder deaktivieren Sie das Optionskästchen. Wenn Sie das Optionskästchen aktivieren, wird der erzeugten Circuit-ID die VLAN-ID hinzugefügt.
- **Circuit-ID Empfänger-Port**
  Aktivieren oder deaktivieren Sie das Optionskästchen. Wenn Sie das Optionskästchen aktivieren, wird der erzeugten Circuit-ID der Empfangsport hinzugefügt.

  Hinweis

  Sie müssen mindestens eine Option auswählen.

  Weiterführende Informationen zum Router-Index (Circuit-ID Router-Index) und Port-Index (Circuit-ID Empfänger-Port) finden Sie in der IfTable über SNMP.

  Die VLAN-ID finden Sie auf der WBM-Seite "Layer 2 > VLAN > Allgemein".

- **Remote-ID**
  Zeigt die Gerätekennung an.

Schnittstellen-spezifische Konfiguration

- **Schnittstelle**
  Wählen Sie aus der Klappliste die Schnittstelle.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Schnittstelle**
  Zeigt die Schnittstelle an.

  Hinweis

  Wenn Sie keine Schnittstellen-spezifische Konfiguration angelegt haben, wird die globale Konfiguration mit der MAC-Adresse als Gerätekennung verwendet.

- **Remote-ID-Typ**
  Wählen Sie aus der Klappliste die Art der Gerätekennung aus. Sie haben folgende Möglichkeiten:
  - IP-Adresse
    Als Gerätekennung wird die IPv4-Adresse des Geräts verwendet.
  - MAC-Adresse
    Als Gerätekennung wird die MAC-Adresse des Geräts verwendet.
  - Beliebiger Text
    Wenn Sie "Beliebiger Text" verwenden, können Sie bei "Remote-ID" den Gerätenamen als Gerätekennung eintragen.
- **Remote-ID**
  Tragen Sie den Gerätenamen ein. Das Feld ist nur editierbar, wenn Sie bei "Remote-ID-Typ" den Eintrag "Beliebiger Text" auswählen.
- **Circuit-ID-Typ**
  Wählen Sie aus der Klappliste die Art der Circuit-ID aus. Sie haben folgende Möglichkeiten:
  - Vordefiniert
    Die Circuit-ID wird automatisch erstellt, basierend auf Router Index, VLAN-ID oder Port.
  - Beliebige Nummer
    Wenn Sie "Beliebige Nummer" verwenden, können Sie bei "Circuit-ID" die ID eingeben.
- **Circuit-ID**
  Tragen Sie die Circuit-ID ein. Das Feld ist nur editierbar, wenn Sie bei "Circuit-ID-Typ" den Eintrag "Beliebige Nummer" auswählen.

Vorgehensweise zur Konfiguration

Automatische Vergabe der Parameter

Gehen Sie folgendermaßen vor, um die automatische Vergabe der Parameter festzulegen:

1. Aktivieren Sie die gewünschte Option unter "Globale Konfiguration":
   - Circuit-ID Router-Index
   - Circuit-ID Empfänger-VLAN-ID
   - Circuit-ID Empfänger-Port
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Manuelle Konfiguration der Parameter

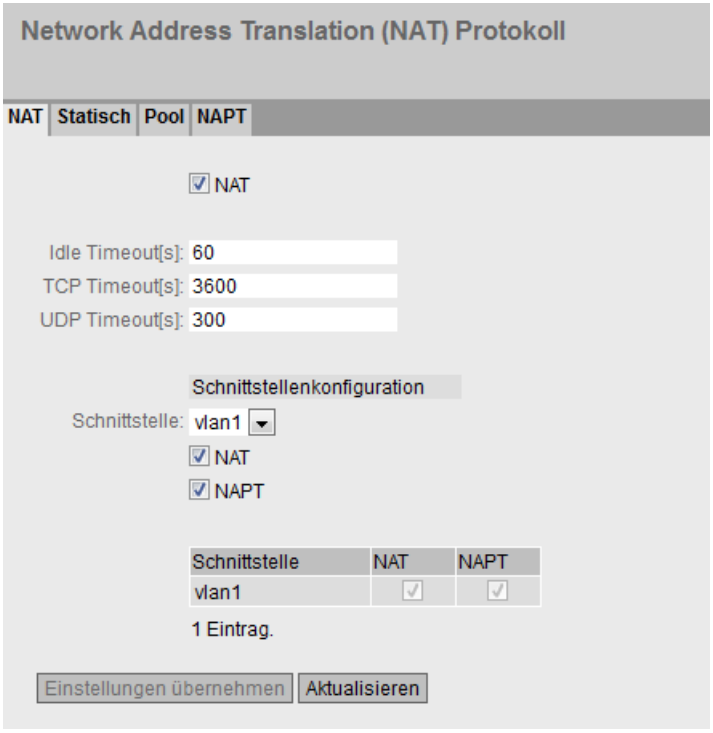
Gehen Sie folgendermaßen vor, um die Parameter manuell festzulegen:

1. Aktivieren Sie die gewünschte Option unter "Globale Konfiguration":
   - Circuit-ID Router-Index
   - Circuit-ID Empfänger-VLAN-ID
   - Circuit-ID Empfänger-Port
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
3. Wählen Sie in der Klappliste "Schnittstelle" die Schnittstelle aus.
4. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird eine neue Zeile eingefügt.
5. Wählen Sie in der Klappliste "Remote-ID-Typ" den gewünschten Eintrag:
   - IP-Adresse
     Als Gerätekennung wird die IPv4-Adresse verwendet.
   - MAC-Adresse
     Als Gerätekennung wird die MAC-Adresse verwendet.
   - Beliebiger Text
     Tragen Sie bei "Remote-ID" die Gerätekennung ein.
6. Wählen Sie in der Klappliste "Circuit-ID-Typ" den gewünschten Eintrag:
   - Vordefiniert
     Der erzeugten Circuit-ID wird der Router Index hinzugefügt.
   - Beliebige Nummer
     Tragen Sie bei "Circuit-ID" die ID ein.
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.6.3 NAT

5.6.3.1 NAT

Auf dieser WBM-Seite legen Sie die Grundeinstellungen für NAT fest.



Beschreibung

Die Seite enthält folgende Felder:

- **NAT**
  Aktivieren oder deaktivieren Sie NAT/NAPT für das gesamte Gerät. Wenn aktiviert, fungiert das Gerät als NAT-Router.
- **Idle Timeout[s]**
  Geben Sie die gewünschte Zeitspanne ein. Das Gerät prüft zyklisch, nach Ablauf der angegebenen Zeitspanne, ob die Aging Time von TCP- und UDP-Verbindungen abgelaufen ist. Die Verbindungen, deren Aging Time seit der letzten Prüfung abgelaufen ist, werden aus der Tabelle "NAT-Übersetzungen" gelöscht.
- **TCP Timeout[s]**
  Geben Sie die gewünschte Aging Time für TCP-Verbindungen ein. TCP-Verbindungen werden solange gespeichert, bis für die angegebene Zeitspanne kein Datenaustausch stattgefunden hat. Abhängig von der zyklischen Prüfung nach Ablauf des Idle Timeouts werden die Verbindungen aus der Tabelle "NAT-Übersetzungen" gelöscht.

- **UDP Timeout[s]**
  Geben Sie die gewünschte Aging Time für UDP-Verbindungen ein. UDP-Verbindungen werden solange gespeichert, bis für die angegebene Zeitspanne kein Datenaustausch stattgefunden hat. Abhängig von der zyklischen Prüfung nach Ablauf des Idle Timeouts werden die Verbindungen aus der Tabelle "NAT-Übersetzungen" gelöscht.
- **Schnittstelle**
  Wählen Sie aus der Klappliste eine IP-Schnittstelle aus, auf der Sie NAT konfigurieren wollen.
  Sobald Sie eine Schnittstelle als NAT-Schnittstelle konfiguriert haben, werden alle weiteren Konfigurationen ausgehend von dieser Schnittstelle betrachtet. Das bedeutet, für diese Schnittstelle sind alle über die Schnittstelle selbst erreichbaren Netzwerke "Outside". Alle anderen Netzwerke sind "Inside".

  Hinweis

  Wenn Sie mehrere NAT-Schnittstellen auf einem Gerät konfiguriert haben, ist dadurch ein Netzwerk aus Sicht einer NAT-Schnittstelle "Outside" und aus der Sicht einer anderen NAT-Schnittstelle "Inside".

- **NAT**
  Aktivieren oder deaktivieren Sie NAT für eine IP-Schnittstelle.
  Im Register "Pool" wird automatisch ein Eintrag erstellt. Das Gerät ist aus dem externen Netz über die IP-Adresse der IP-Schnittstelle erreichbar.
  Wenn Sie NAT für eine IP-Schnittstelle deaktivieren und keine Konfigurationen auf der NAT-Schnittstelle vorliegen, wird der Eintrag automatisch aus der Tabelle gelöscht.
- **NAPT**
  Aktivieren oder deaktivieren Sie NAPT für eine IP-Schnittstelle.

Die Tabelle gliedert sich in folgende Spalten:

- **Schnittstelle**
  Schnittstelle, auf der eine NAT-Konfiguration besteht.
- **NAT**
  Zeigt an, ob NAT für die ausgewählte IP-Schnittstelle aktiviert oder deaktiviert ist.
  NAT ist erst aktiv, wenn Sie NAT für das gesamte Gerät aktiviert haben.
- **NAPT**
  Zeigt an, ob NAPT für die ausgewählte IP-Schnittstelle aktiviert oder deaktiviert ist.
  NAPT ist erst aktiv, wenn Sie NAT für das gesamte Gerät aktiviert haben.
  Wenn Sie keine weiteren Konfigurationen für NAPT vornehmen, ist automatisch die dynamische Portumsetzung aktiv.
  Ein Gerät im internen Netz ist standardmäßig nicht aus einem externen Netz erreichbar. Wenn das interne Gerät in ein externes Netz kommunizieren will, werden die Inside Local-Adresse und die IP-Adresse der IP-Schnittstelle um einen Port ergänzt und dem internen Gerät als Inside Local- und Inside Global-Adresse zugeordnet. Über diese Inside Global-Adresse ist das interne Gerät aus dem externen Netz erreichbar, bis der Timer der Verbindung abgelaufen ist.

Vorgehensweise

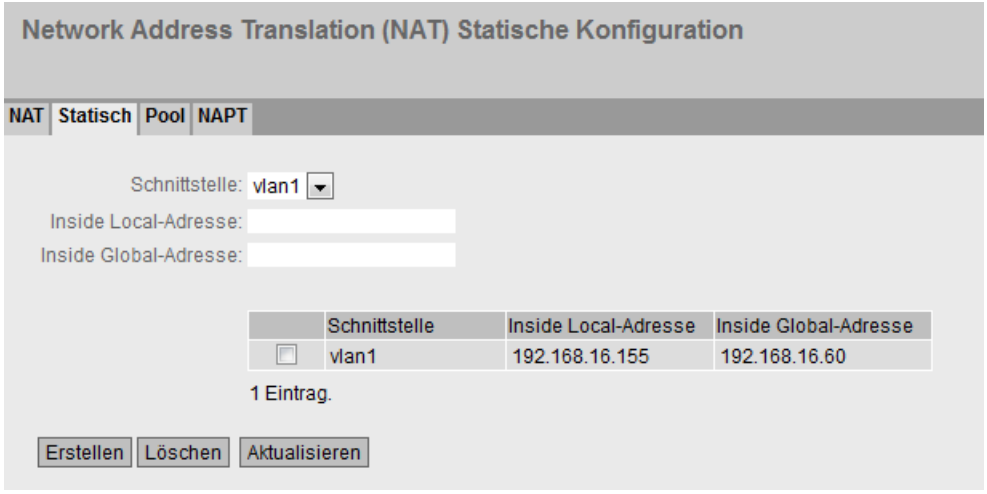
Um NAT/NAPT zu konfigurieren, gehen Sie wie folgt vor:

1. Geben Sie die gewünschten Zeitspannen ein.
2. Wählen Sie die gewünschte IP-Schnittstelle aus.
3. Aktivieren Sie NAT/NAPT für die ausgewählte IP-Schnittstelle.
4. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
5. Nehmen Sie die gewünschten Einstellungen für NAT/NAPT in den NAT/NAPT-Registern vor.
6. Aktivieren Sie in diesem Register das Optionskästchen "NAT".
7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.6.3.2 Statisch

Auf dieser WBM-Seite konfigurieren Sie statische 1:1-Adressumsetzungen.

Sie legen fest, in welche Inside Global-Adresse die Inside Local-Adresse eines Geräts umgesetzt werden soll und umgekehrt. Diese Variante erlaubt den Verbindungsaufbau in beide Richtungen. Das Gerät im internen Netz ist aus dem externen Netz erreichbar.



Beschreibung

Die Seite enthält folgende Felder:

- **Schnittstelle**
  Wählen Sie aus der Klappliste eine NAT-Schnittstelle aus, für die Sie weitere NAT-Konfigurationen vornehmen wollen.
- **Inside Local-Adresse**
  Geben Sie die tatsächliche Adresse des Geräts ein, das von extern erreichbar sein soll.
- **Inside Global-Adresse**
  Geben Sie die Adresse ein, unter der das Gerät von extern erreichbar sein soll.

Die Tabelle gliedert sich in folgende Spalten:

- **1. Spalte**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Schnittstelle**
  NAT-Schnittstelle, auf die sich die Einstellung bezieht.
- **Inside Local-Adresse**
  Zeigt die tatsächliche Adresse des Geräts an, das von extern erreichbar sein soll.
- **Inside Global-Adresse**
  Zeigt die Adresse an, unter der das Gerät von extern erreichbar sein soll.

Vorgehensweise

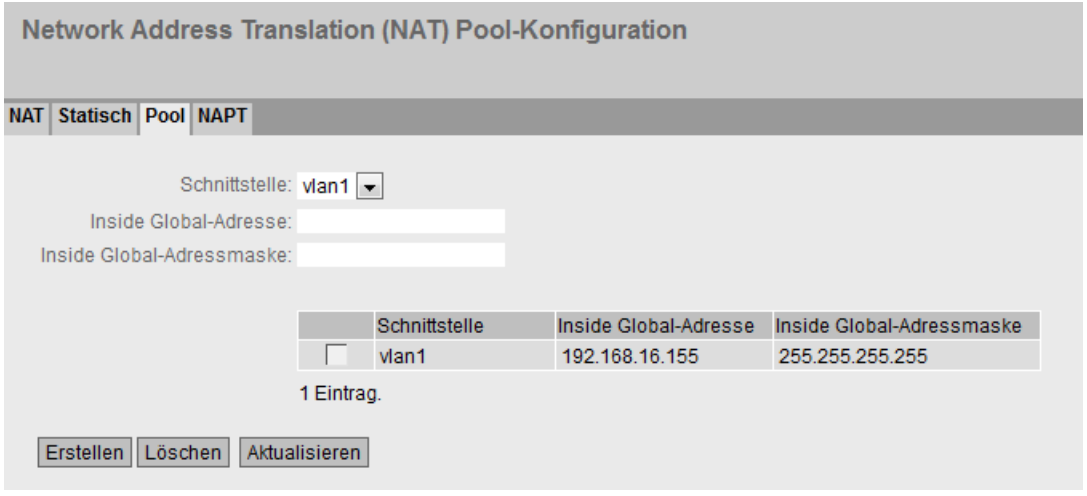
Um eine 1:1-Adressumsetzung anzulegen, gehen Sie wie folgt vor:

1. Wählen Sie aus der Klappliste "Schnittstelle" eine NAT-Schnittstelle aus.
2. Geben Sie unter "Inside Local-Adresse" die tatsächliche Adresse des Geräts ein, das von extern erreichbar sein soll.
3. Geben Sie unter "Inside Global-Adresse" die Adresse ein, unter der das Gerät von extern erreichbar sein soll.

5.6.3.3 Pool

Auf dieser WBM-Seite konfigurieren Sie dynamische Adressumsetzungen.

Ein Gerät im internen Netz ist standardmäßig nicht aus einem externen Netz erreichbar. Wenn das interne Gerät in ein externes Netz kommunizieren will, wird ihm dynamisch eine Inside Global-Adresse zugeordnet. Über diese Inside Global-Adresse ist das interne Gerät aus dem externen Netz erreichbar, bis der Timer der Verbindung abgelaufen ist.



Beschreibung

Die Seite enthält folgende Felder:

- **Schnittstelle**
  Wählen Sie aus der Klappliste eine NAT-Schnittstelle aus, für die Sie weitere NAT-Konfigurationen vornehmen wollen.
- **Inside Global-Adresse**
  Geben Sie die Startadresse für die dynamische Zuordnung von Adressen ein, unter denen Geräte von extern erreichbar sein sollen.
- **Inside Global-Adressmaske**
  Geben Sie die Adressmaske des externen Subnetzes ein.

Die Tabelle gliedert sich in folgende Spalten:

- **1. Spalte**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Schnittstelle**
  NAT-Schnittstelle, auf die sich die Einstellung bezieht.
- **Inside Global-Adresse**
  Zeigt die Startadresse für die dynamische Zuordnung von Adressen an, unter denen Geräte von extern erreichbar sein sollen.
- **Inside Global-Adressmaske**
  Zeigt die Adressmaske des externen Subnetzes an.

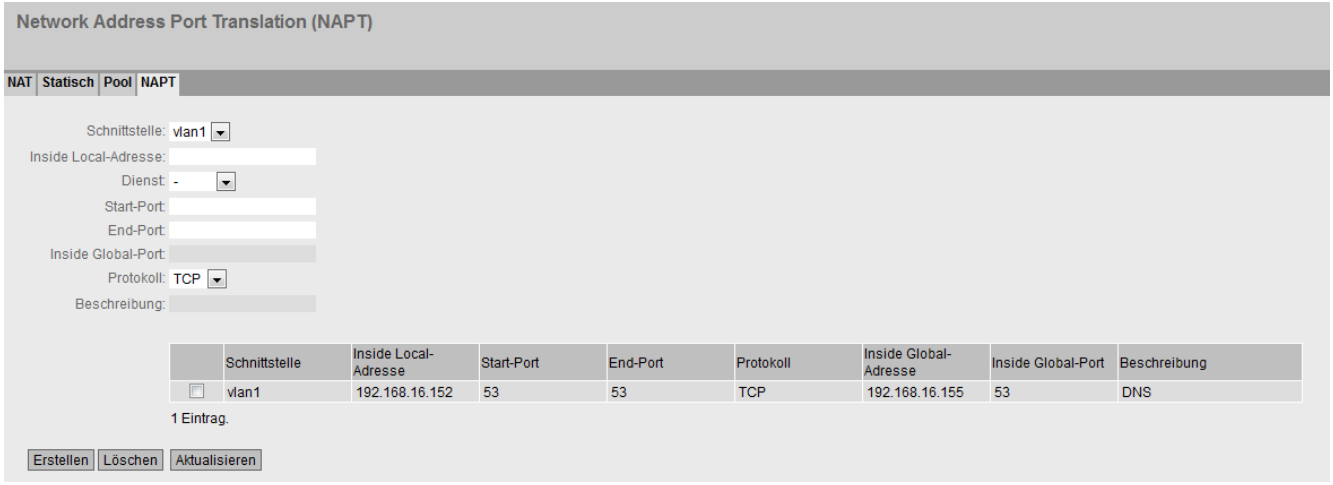
Vorgehensweise

Um eine dynamische Adressumsetzung anzulegen, gehen Sie wie folgt vor:

1. Wählen Sie aus der Klappliste "Schnittstelle" eine NAT-Schnittstelle aus.
2. Geben Sie unter "Inside Global-Adresse" die Startadresse für die dynamische Zuordnung von Adressen ein, unter denen Geräte von extern erreichbar sein sollen.
3. Geben Sie unter "Inside Global-Adressmaske" Adressmaske des externen Subnetzes ein.

5.6.3.4 NAPT

Auf dieser WBM-Seite konfigurieren Sie statische Portumsetzungen.



Beschreibung

Die Seite enthält folgende Felder:

- **Schnittstelle**
  Wählen Sie aus der Klappliste eine NAT-Schnittstelle aus, für die Sie weitere NAT-Konfigurationen vornehmen wollen.
- **Inside Local-Adresse**
  Geben Sie die tatsächliche Adresse des Geräts ein, das von extern erreichbar sein soll.
- **Dienst**
  Wählen Sie aus, für welchen Dienst die Portumsetzung gültig ist.
  Wenn Sie einen Dienst auswählen, werden in den Feldern Start-Port und End-Port der gleiche Port eingetragen. Wenn Sie den Start-Port ändern, wird der End-Port entsprechend geändert.
  Wenn Sie den Eintrag "-" auswählen, können Sie den Start- und End-Port frei eingeben.
- **Start-Port**
  Geben Sie einen Inside Local-Port ein.
- **End-Port**
  Abhängig von Ihrer Auswahl in der Klappliste "Dienst", können Sie einen Inside Local-Port eingeben oder es wird ein Port angezeigt.
  Wenn Sie in den Feldern Start-Port und End-Port unterschiedliche Ports eingeben, wird im Feld Inside Global-Port der gleiche Port-Bereich eingetragen. Ein Port-Bereich kann immer nur auf den gleichen Port-Bereich umgesetzt werden.
  Wenn Sie in den Feldern Start-Port und End-Port den gleichen Port eingeben, können Sie den Inside Global-Port frei eingeben.
- **Inside Global-Port**
  Abhängig von Ihrer Auswahl in der Klappliste "Dienst", können Sie einen Port eingeben oder es wird ein Port angezeigt.

- **Protokoll**
  Wählen Sie aus, für welches Protokoll die Portumsetzung gültig ist.
- **Beschreibung**
  Geben Sie eine Beschreibung für die Portumsetzung ein.

Die Tabelle gliedert sich in folgende Spalten:

- **1. Spalte**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Schnittstelle**
  NAT-Schnittstelle, auf die sich die Einstellung bezieht.
- **Inside Local-Adresse**
  Zeigt die tatsächliche Adresse des Geräts an, das von extern erreichbar sein soll.
- **Start-Port**
  Zeigt den Start-Port an, der der Inside Local-Adresse zugeordnet wird.
- **End-Port**
  Zeigt den End-Port an, der der Inside Local-Adresse zugeordnet wird.
- **Protokoll**
  Zeigt an, für welches Protokoll die Portumsetzung gültig ist.
- **Inside Global-Adresse**
  Zeigt die Adresse an, unter der das Gerät von extern erreichbar sein soll.
- **Inside Global-Port**
  Zeigt den Port an, der der Inside Global-Adresse zugeordnet wird.
- **Beschreibung**
  Zeigt die Beschreibung für die Portumsetzung an.

Vorgehensweise

Um eine statische Portumsetzung anzulegen, gehen Sie wie folgt vor:

1. Wählen Sie aus der Klappliste "Schnittstelle" eine NAT-Schnittstelle aus.
2. Geben Sie unter "Inside Local-Adresse" die tatsächliche Adresse des Geräts ein, das von extern erreichbar sein soll.
3. Wählen Sie einen Dienst aus.
4. Geben Sie abhängig von Ihrer Auswahl in der Klappliste "Dienst" den Start-, End- und Inside Global-Port an.
5. Wählen Sie ein Protokoll aus.
6. Geben Sie eine Beschreibung für die Portumsetzung ein.

5.7 Das Menü "Security"

5.7.1 Benutzerverwaltung

Übersicht zur Benutzerverwaltung

Der Zugriff auf das Gerät wird durch konfigurierbare Benutzereinstellungen verwaltet. Richten Sie Benutzer mit jeweils einem Passwort zur Authentifizierung ein. Weisen Sie den Benutzern eine Rolle mit entsprechenden Rechten zu.

Die Authentifizierung von Benutzern kann entweder vom Gerät lokal oder von einem externen RADIUS-Server durchgeführt werden. Wie die Authentifizierung erfolgen soll, konfigurieren Sie auf der Seite "Security > AAA > Allgemein".

Hinweis

Wenn Sie die Konfiguration eines Geräts nach STEP7 (TIA Portal) übertragen, werden die konfigurierten Benutzer nicht übertragen.

Lokale Anmeldung

Die lokale Anmeldung von Benutzern durch das Gerät läuft wie folgt ab:

1. Der Benutzer meldet sich mit seinem Benutzernamen und Passwort am Gerät an.
2. Das Gerät prüft, ob ein Eintrag für den Benutzer vorhanden ist:
   → Wenn ein entsprechender Eintrag existiert, wird der Benutzer mit den Rechten der verknüpften Rolle angemeldet.
   → Wenn kein entsprechender Eintrag existiert, wird dem Benutzer der Zugriff verweigert.

Anmeldung über einen externen RADIUS-Server

RADIUS (Remote Authentication Dial-In User Service) ist ein Protokoll zur Auhentifizierung und Autorisierung von Benutzern durch Server, auf denen Benutzerdaten zentral abgelegt werden können.

Die Authentifizierung von Benutzern über einen RADIUS-Server läuft wie folgt ab:

1. Der Benutzer meldet sich mit seinem Benutzernamen und Passwort am Gerät an.
2. Das Gerät schickt eine Authentifizierungsanfrage mit den Anmeldedaten an den RADIUS-Server.
3. Der RADIUS-Server führt eine Prüfung durch und meldet das Ergebnis an das Gerät zurück:
   - Der RADIUS-Server meldet eine erfolgreiche Authentifizierung und gibt für das Attribut "Service Type" den Wert "Administrative User" an das Gerät zurück:
     → Der Benutzer wird mit Lese-/Schreibrechten angemeldet.
   - Der RADIUS-Server meldet eine erfolgreiche Authentifizierung und gibt einen anderen oder gar keinen Wert für das Attribut "Service Type" an das Gerät zurück:
     → Der Benutzer wird mit Leserechten angemeldet.
   - Der RADIUS-Server meldet eine fehlgeschlagene Authentifizierung an das Gerät zurück:
     → Dem Benutzer wird der Zugriff verweigert.

Zuweisung eines VLANs über RADIUS oder Guest VLAN im Base Bridge-Modus "802.1Q VLAN Bridge"

Authentifizierung mit Änderung der VLAN-Konfiguration

Wenn ein Port bei der Authentifizierung über die Funktion "VLAN-Zuordnung von RADIUS übernehmen" oder "Guest VLAN" dynamisch einem VLAN zugewiesen wird, gibt es folgende Optionen:

- Wenn das VLAN, das zugewiesen werden soll, nicht auf dem Gerät angelegt ist, wird die Authentifizierung abgelehnt.
- Wenn das VLAN, das zugewiesen werden soll, auf dem Gerät angelegt ist:
  - Der Port wird Untagged Member in dem zugewiesenen VLAN, wenn er es bisher nicht war.
    → Dadurch wird ggf. die statische Konfiguration des Ports in diesem VLAN überschrieben und nicht wiederhergestellt, wenn die Authentifizierung zurückgenommen wird.
  - Die Port-VID des Ports wird auf die ID des zugewiesenen VLANs geändert.

Hinweis

Wenn der Port nur einem VLAN zugeordnet sein soll, müssen Sie die VLAN-Konfiguration manuell anpassen. Alle Ports sind z. B. standardmäßig Untagged Member in "VLAN 1".

Wenn die Authentifizierung zurückgenommen wird, z. B. durch einen Link-Down, werden die dynamischen Änderungen zurückgenommen:

- Der Port ist kein Member mehr in dem zugewiesenen VLAN.
- Die Port-VID des Ports wird auf den Wert zurückgesetzt, den sie vor der Authentifizierung hatte.

Hinweis

Wenn die Port-VID des Ports vor der Authentifizierung der zugewiesenen Port-VID entspricht, bleibt der Port Untagged Member in diesem VLAN.

Authentifizierung ohne Änderung der VLAN-Konfiguration

Wenn bei der Authentifizierung weder durch die Funktion "VLAN-Zuordnung von RADIUS übernehmen" noch durch "Guest VLAN" ein VLAN zugewiesen wird, bleibt die bestehende VLAN-Konfiguration des Ports unverändert.

5.7.2 Benutzer

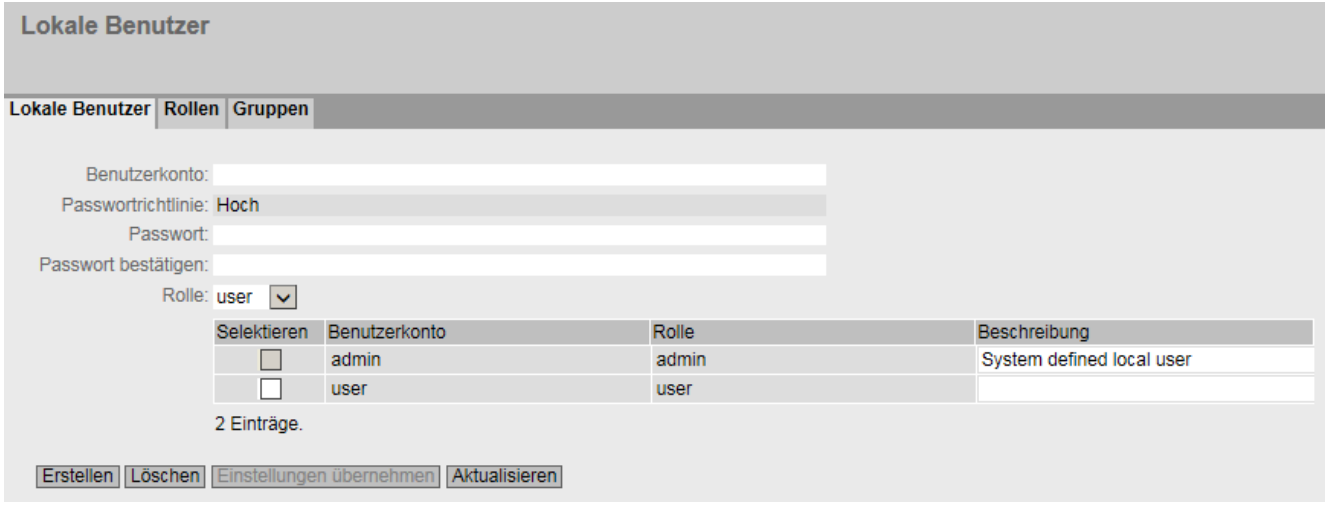
5.7.2.1 Lokale Benutzer

Lokale Benutzer

Auf dieser Seite erstellen Sie lokale Benutzer mit den entsprechenden Rechten.

Hinweis

Es ist von den Rechten des angemeldeten Benutzers abhängig, welche Werte angezeigt werden.



Beschreibung

Die Seite enthält folgende Felder:

- **Benutzerkonto**
  Geben Sie den Namen für den Benutzer ein. Der Name muss folgende Bedingungen erfüllen:
  - Er muss eindeutig sein.
  - Er muss zwischen 1 und 32 Zeichen lang sein.

  Hinweis

  Benutzername nicht änderbar

  Nach dem Anlegen eines Benutzers kann der Benutzername nicht mehr geändert werden.

  Wenn ein Benutzername geändert werden soll, muss der Benutzer gelöscht und ein neuer Benutzer angelegt werden.

  Hinweis

  Werkseitig voreingestellter Benutzer "user"

  Ab der Firmware-Version 2.1 ist der werkseitig voreingestellte Benutzer "user" im Auslieferzustand nicht mehr verfügbar.

  Wenn Sie ein Gerät auf die Firmware V2.1 aktualisieren, ist der Benutzer "user" zunächst noch verfügbar. Wenn Sie das Gerät auf die Werkseinstellungen zurücksetzen ("Auf Werkseinstellungen zurücksetzen und Neustart"), wird der Benutzer "user" gelöscht.

  Sie können neue Benutzer mit der Rolle "user" anlegen.

- **Passwortrichtlinie**
  Zeigt an, welche Passwortrichtlinie im Gerät verwendet wird:
  - Hoch
    Passwortlänge: mindestens 8 Zeichen, maximal 32 Zeichen
    Mindestens 1 Großbuchstabe
    Mindestens 1 Sonderzeichen
    Mindestens 1 Zahl
  - Niedrig
    Passwortlänge: mindestens 6 Zeichen, maximal 32 Zeichen

  Sie konfigurieren die Passwortrichtlinie des Geräts auf der Seite "Security > Passwörter > Optionen".
- **Passwort**
  Geben Sie das Passwort an. Die Stärke des Passworts ist abhängig von der eingestellten Passwortrichtlinie.

- **Passwort bestätigen**
  Geben Sie das Passwort erneut ein, um es zu bestätigen.
- **Rolle**
  Wählen Sie eine Rolle aus:
  - user
    Leserechte: Benutzer mit dieser Rolle können Geräteparameter lesen, aber nicht verändern. Benutzer mit dieser Rolle können ihr eigenes Passwort ändern.
  - admin
    Lese-/Schreibrechte: Benutzer mit dieser Rolle können Geräteparameter sowohl lesen als auch verändern. Benutzer können die Passwörter für alle Benutzeraccounts ändern.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.

  Hinweis

  Werksseitig voreingestellte Benutzer sowie angemeldete Benutzer können nicht gelöscht oder geändert werden.

- **Benutzerkonto**
  Zeigt den Benutzernamen an.
- **Rolle**
  Zeigt die Rolle des Benutzers an.

Vorgehensweise

Hinweis
Änderungen im Modus "Trial"

Auch wenn sich das Gerät im Modus "Trial" befindet, werden Änderungen, die Sie auf dieser Seite durchführen, sofort gespeichert.

Benutzer anlegen

1. Geben Sie den Namen für den Benutzer ein.
2. Geben Sie das Passwort für den Benutzer ein.
3. Geben Sie das Passwort erneut ein, um es zu bestätigen.
4. Wählen Sie die Rolle des Benutzers aus.
5. Klicken Sie auf die Schaltfläche "Erstellen".

Benutzer löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Löschen". Die Einträge werden gelöscht und die Seite wird aktualisiert.

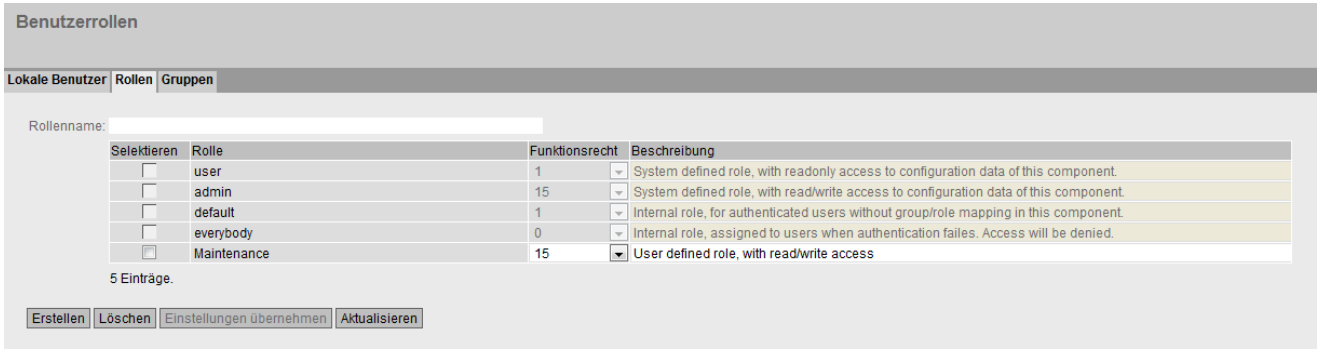
5.7.2.2 Rollen

Rollen

Auf dieser Seite erstellen Sie Rollen, die lokal auf dem Gerät gültig sind.

Hinweis

Es ist von den Rechten des angemeldeten Benutzers abhängig, welche Werte angezeigt werden.



Beschreibung

Die Seite enthält Folgendes:

- **Rollenname**
  Geben Sie den Namen für die Rolle ein. Der Name muss folgende Bedingungen erfüllen:
  - Er muss eindeutig sein.
  - Er muss zwischen 1 und 64 Zeichen lang sein.

  Hinweis

  Rollenname nicht änderbar

  Nach dem Anlegen einer Rolle kann der Rollenname nicht mehr geändert werden.

  Wenn ein Rollenname geändert werden soll, muss die Rolle gelöscht und eine neue Rolle angelegt werden.

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.

  Hinweis

  Die voreingestellten Rollen sowie zugewiesene Rollen können nicht gelöscht oder geändert werden.

- **Rolle**
  Zeigt den Namen der Rolle an.
- **Funktionsrecht**
  Wählen Sie die Funktionsrechte der Rolle aus:
  - 1
    Benutzer mit dieser Rolle können Geräteparameter lesen aber nicht verändern.
    Benutzer mit dieser Rolle können ihr eigenes Passwort ändern.
  - 15
    Benutzer mit dieser Rolle können Geräteparameter sowohl lesen als auch verändern.

  Hinweis

  Funktionsrecht nicht änderbar

  Wenn Sie eine Rolle zugewiesen haben, können Sie das Funktionsrecht der Rolle nicht mehr ändern.

  Wenn Sie das Funktionsrecht einer Rolle ändern wollen, gehen Sie wie folgt vor:

  1. Löschen Sie alle zugewiesenen Benutzer.
  2. Ändern Sie das Funktionsrecht der Rolle.
  3. Weisen Sie die Rolle erneut zu.

- **Beschreibung**
  Geben Sie eine Beschreibung für die Rolle ein. Bei vordefinierten Rollen wird eine Beschreibung angezeigt. Der Beschreibungstext kann bis zu 100 Zeichen lang sein.

Vorgehensweise

Rolle anlegen

1. Geben Sie den Namen für die Rolle ein.
2. Klicken Sie auf die Schaltfläche "Erstellen".
3. Wählen Sie die Funktionsrechte der Rolle aus.
4. Geben Sie eine Beschreibung der Rolle ein.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Rolle löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Löschen". Die Einträge werden gelöscht und die Seite wird aktualisiert.

5.7.2.3 Gruppen

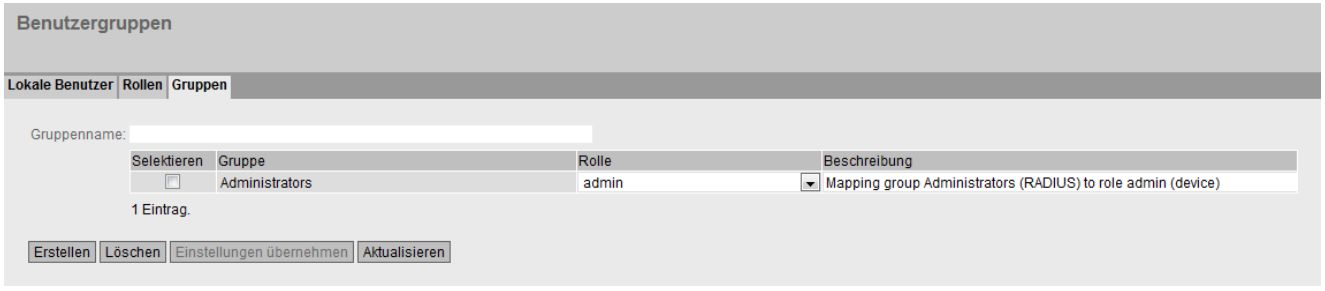
Benutzergruppen

Auf dieser Seite verknüpfen Sie eine Gruppe mit einer Rolle.

In diesem Beispiel wird die Gruppe "Administrators" mit der Rolle "admin" verknüpft. Die Gruppe ist auf einem RADIUS-Server definiert. Die Rolle ist lokal auf dem Gerät definiert. Wenn ein RADIUS-Server einen Benutzer authentifiziert und der Gruppe "Administrators" zuordnet, erhält dieser Benutzer auf dem Gerät die Rechte der Rolle "admin".

Hinweis

Es ist von den Rechten des angemeldeten Benutzers abhängig, welche Werte angezeigt werden.



Beschreibung

Die Seite enthält Folgendes:

- **Gruppenname**
  Geben Sie den Namen der Gruppe ein. Der Name muss der Gruppe auf dem RADIUS-Server entsprechen.
  Der Name muss folgende Bedingungen erfüllen:
  - Er muss eindeutig sein.
  - Er muss zwischen 1 und 64 Zeichen lang sein.
  - Nicht erlaubt sind: § ? " ; :

Die Tabelle enthält folgende Spalten:

- **Selektieren**
  Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
- **Gruppe**
  Zeigt den Namen der Gruppe an.

- **Rolle**
  Wählen Sie eine Rolle aus. Benutzer, die über den RADIUS-Server mit der verknüpften Gruppe authentifiziert werden, erhalten die Rechte dieser Rolle lokal auf dem Gerät.
  Sie können zwischen den voreingestellten und selbst definierten Rollen wählen, siehe Seite "Security > Benutzer > Rollen".
- **Beschreibung**
  Geben Sie eine Beschreibung für die Verknüpfung der Gruppe mit einer Rolle an. Der Beschreibungstext kann bis zu 100 Zeichen lang sein.

Vorgehensweise

Eine Gruppe mit einer Rolle verknüpfen

1. Geben Sie den Namen einer Gruppe ein.
2. Klicken Sie auf die Schaltfläche "Erstellen".
3. Wählen Sie eine Rolle aus.
4. Geben Sie eine Beschreibung für die Verknüpfung einer Gruppe mit einer Rolle ein.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Die Verknüpfung zwischen einer Gruppe und einer Rolle löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Löschen". Die Einträge werden gelöscht und die Seite wird aktualisiert.

5.7.3 Passwörter

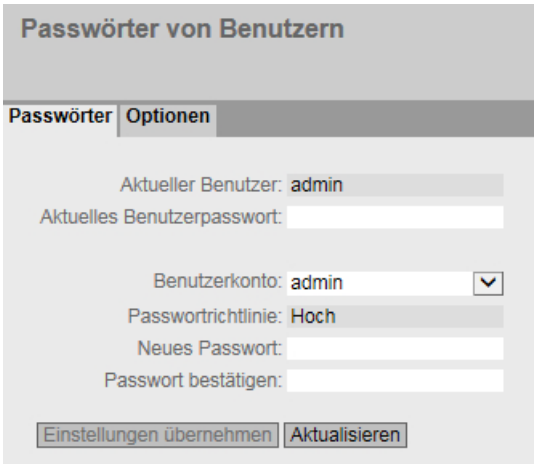
5.7.3.1 Passwörter

Konfiguration der Geräte-Passwörter

Hinweis

Wenn Sie über einen RADIUS-Server angemeldet sind, können Sie keine lokalen Gerätepasswörter ändern.

Auf dieser Seite können Sie Passwörter ändern. Wenn Sie mit Lese-/Schreibrechten angemeldet sind, können Sie die Passwörter für alle Benutzeraccounts ändern. Wenn Sie mit Leserechten angemeldet sind, können Sie nur Ihr eigenes Passwort ändern.



Beschreibung der angezeigten Werte

Die Seite enthält folgende Felder:

- **Aktueller Benutzer**
  Zeigt den Benutzer an, der aktuell angemeldet ist.
- **Aktuelles Benutzerpasswort**
  Geben Sie das Passwort des aktuell angemeldeten Benutzers ein.
- **Benutzerkonto**
  Wählen Sie den Benutzer, dessen Passwort Sie ändern möchten.
- **Passwortrichtlinie**
  Zeigt an, welche Passwortrichtlinie bei der Vergabe von neuen Passwörter verwendet wird.
  - Hoch
    Passwortlänge: mindestens 8 Zeichen, maximal 32 Zeichen
    Mindestens 1 Großbuchstabe
    Mindestens 1 Sonderzeichen
    Mindestens 1 Zahl
  - Niedrig
    Passwortlänge: mindestens 6 Zeichen, maximal 32 Zeichen
- **Neues Passwort**
  Geben Sie das neue Passwort für den ausgewählten Benutzer ein.
  Es darf folgende Zeichen nicht enthalten:
  - § ? " ; :
  - Das Zeichen für Delete und Leerzeichen dürfen auch nicht enthalten sein.
- **Passwort bestätigen**
  Geben Sie das neue Passwort erneut ein, um es zu bestätigen.

Vorgehensweise

Hinweis

Wenn Sie sich das erste Mal oder nach einem "Auf Werkseinstellungen zurücksetzen und Neustart" mit dem voreingestellten Benutzer "admin" anmelden, werden Sie aufgefordert, das Passwort zu ändern. Außerdem können Sie einmalig den werksseitig voreingestellten Benutzer "admin" umbenennen.

Werksseitig sind der Benutzername und das Passwort wie folgt eingestellt:

- admin: admin

Hinweis

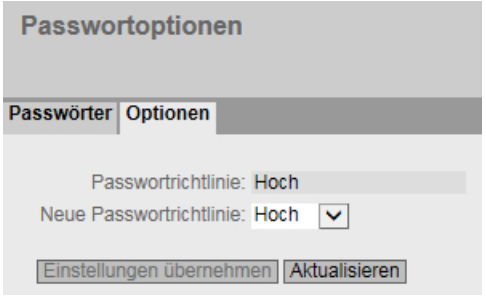
Passwort ändern im Modus "Trial"

Auch wenn Sie im Modus "Trial" das Passwort ändern, wird diese Änderung sofort gespeichert.

1. Geben Sie in das Eingabefeld "Aktuelles Benutzerpasswort" das Passwort des aktuell angemeldeten Benutzers ein.
2. Wählen Sie aus der Klappliste "Benutzerkonto" den Benutzer aus, dessen Passwort Sie ändern möchten.
3. Geben Sie in das Eingabefeld "Neues Passwort" das neue Passwort für den ausgewählten Benutzer ein.
4. Wiederholen Sie das neue Passwort im Eingabefeld "Passwort bestätigen".
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.7.3.2 Optionen

Auf dieser Seite legen Sie fest, welche Passwortrichtlinie bei der Vergabe von neuen Passwörter beachtet wird.



Beschreibung

- **Passwortrichtlinie**
  Zeigt an, welche Passwortrichtlinie aktuell verwendet wird.
- **Neue Passwortrichtlinie**
  Wählen Sie aus der Klappliste die gewünschte Einstellung aus:
  - Hoch
    Passwortlänge: mindestens 8 Zeichen, maximal 32 Zeichen
    Mindestens 1 Großbuchstabe
    Mindestens 1 Sonderzeichen
    Mindestens 1 Zahl
  - Niedrig
    Passwortlänge: mindestens 6 Zeichen, maximal 32 Zeichen

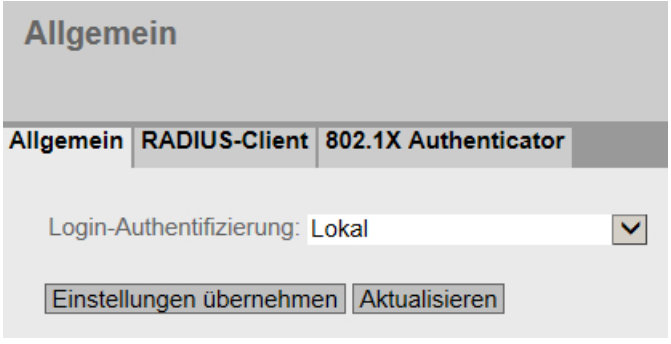
5.7.4 AAA

5.7.4.1 Allgemein

Anmeldung von Netzteilnehmern

Die verwendete Bezeichnung "AAA" steht für "Authentication, Authorization, Accounting". Dieses Feature dient dazu, Netzteilnehmer zu identifizieren und zuzulassen und ihnen die entsprechenden Dienste bereitzustellen.

Auf dieser Seite konfigurieren Sie die Anmeldung.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

Hinweis

Um die Login-Authentifizierung "RADIUS" nutzen zu können, muss ein RADIUS-Server hinterlegt und für die Benutzerauthentifizierung konfiguriert sein.

- **Login-Authentifizierung**
  Legen Sie fest, wie die Anmeldung erfolgt:
  - Lokal
    Die Authentifizierung muss lokal auf dem Gerät erfolgen.
  - RADIUS
    Die Authentifizierung muss über einen RADIUS-Server erfolgen.
  - Lokal und RADIUS
    Die Authentifizierung kann sowohl über die im Gerät vorhandenen Benutzer (Benutzername und Passwort) als auch über einen RADIUS-Server erfolgen. Es wird zuerst in der lokalen Datenbank nach dem Benutzer gesucht. Wenn der Benutzer dort nicht vorhanden ist, wird eine RADIUS-Anfrage geschickt.
  - RADIUS und Fallback Lokal
    Die Authentifizierung muss über einen RADIUS-Server erfolgen.
    Nur wenn der RADIUS-Server im Netz nicht erreichbar ist, wird eine lokale Authentifizierung durchgeführt.

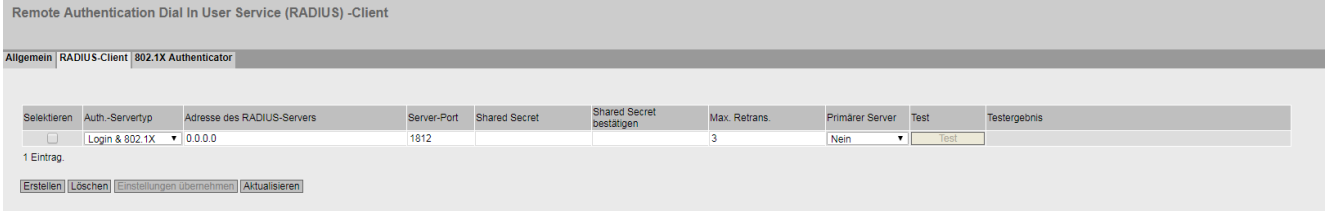
5.7.4.2 RADIUS-Client

Anmeldung über einen externen Server

Das Konzept von RADIUS basiert auf einem externen Authentifizierungsserver.

Jede Zeile der Tabelle enthält die Zugangsdaten für je einen Server. In der Suchreihenfolge wird der primäre Server zuerst angefragt. Ist der primäre Server nicht erreichbar, werden in der eingetragenen Reihenfolge sekundäre Server angefragt.

Wenn keiner der Server antwortet, findet keine Authentifizierung statt.



Beschreibung der angezeigten Felder

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Auth.-Servertyp**
  Wählen Sie aus, für welche Authentifizierungsverfahren der Server verwendet werden soll.
  - Login
    Der Server wird nur für die Login-Authentifizierung verwendet.
  - 802.1X
    Der Server wird nur für die 802.1X-Authentifizierung verwendet.
  - Login & 802.1X
    Der Server wird für beide Authentifizierungsverfahren verwendet.
- **Adresse des RADIUS-Servers**
  Tragen Sie die IPv4-Adresse des RADIUS-Servers ein.
- **Server-Port**
  Tragen Sie hier den Eingangs-Port des RADIUS-Servers ein. Standardmäßig ist der Eingangs-Port 1812 eingestellt.
  Wertebereich: 1 - 65535
- **Shared Secret**
  Geben Sie hier die Zugangskennung des RADIUS-Servers an.
  Wertebereich: 1 - 46 Zeichen
- **Shared Secret bestätigen**
  Geben Sie die Zugangskennung zur Bestätigung erneut ein.
- **Max. Retrans.**
  Geben Sie hier die maximale Anzahl der Wiederholungen eines Anfrageversuchs ein. Der initiale Verbindungsversuch wird um den hier angegebenen Wert wiederholt, bevor ein anderer konfigurierter RADIUS-Server angefragt oder die Anmeldung für gescheitert erklärt wird. Standardmäßig sind 3 Wiederholungen eingestellt, das bedeutet 4 Verbindungsversuche.
  Wertebereich: 1 - 5
- **Primärer Server**
  Legen Sie mit Hilfe der Optionen der Klappliste fest, ob ein Server der primäre Server ist. Sie können aus den Optionen "Ja" oder "Nein" auswählen. Sie können nur einen primären Server definieren.

- **Test**
  Mit dieser Schaltfläche können Sie testen, ob der angegebene RADIUS-Server verfügbar ist oder nicht. Der Test wird einmalig durchgeführt und nicht zyklisch wiederholt.
- **Testergebnis**
  Zeigt an, ob der RADIUS-Server verfügbar ist oder nicht:
  - Fehlgeschlagen, keine Testpakete gesendet
    Die IP-Adresse ist nicht erreichbar.
    Die IP-Adresse ist erreichbar, der RADIUS-Server läuft jedoch nicht.
  - Erreichbar, das Shared Secret wurde nicht akzeptiert
    Die IP-Adresse ist erreichbar, der RADIUS-Server läuft, akzeptiert jedoch das angegebene Shared Secret nicht.
  - Erreichbar, das Shared Secret wurde akzeptiert
    Die IP-Adresse ist erreichbar und der RADIUS-Server akzeptiert das angegebene Shared Secret.

  Das Testergebnis wird nicht automatisch aktualisiert. Das Ergebnis des letzten Tests wird angezeigt, bis Sie es mit der Schaltfläche "Aktualisieren" löschen.

Vorgehensweise zur Konfiguration

Neuen Server eintragen

1. Klicken Sie auf die Schaltfläche "Erstellen". In der Tabelle wird ein neuer Eintrag erzeugt. Folgende Standardwerte werden in die Tabelle eingetragen:
   - Auth.-Servertyp: Login & 802.1X
   - Adresse des RADIUS-Servers: 0.0.0.0
   - Server-Port: 1812
   - Max. Retrans.: 3
   - Primärer Server: Nein
2. Tragen Sie in der jeweiligen Zeile die folgenden Daten in die Eingabefelder ein:
   - Auth.-Servertyp
   - Adresse des RADIUS-Servers
   - Server-Port
   - Shared Secret
   - Shared Secret bestätigen
   - Max. Retrans.: 3
   - Primärer Server: Nein
3. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
4. Testen Sie ggf. die Erreichbarkeit des RADIUS-Servers.

Wiederholen Sie den Vorgang für alle Server, die Sie eintragen wollen.

Server ändern

1. Tragen Sie in der jeweiligen Zeile die folgenden Daten in die Eingabefelder ein:
   - Auth.-Servertyp
   - Adresse des RADIUS-Servers
   - Server-Port
   - Shared Secret
   - Shared Secret bestätigen
   - Max. Retrans
   - Primärer Server
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".
3. Testen Sie ggf. die Erreichbarkeit des RADIUS-Servers.

Wiederholen sie den Vorgang bei allen Servern, deren Eintrag Sie ändern wollen.

Server löschen

1. Klicken Sie in das Optionskästchen in der ersten Spalte vor der zu löschenden Zeile, um den Eintrag zum Löschen zu markieren.
   Wiederholen Sie den Vorgang für jeden Eintrag, den Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Löschen".
   Alle markierten Einträge werden gelöscht und die Anzeige wird aktualisiert.

5.7.4.3 802.1X Authenticator

Netzwerkzugriff einrichten

Für ein Endgerät ist der Zugang zum Netzwerk erst möglich, nachdem das Gerät die Anmeldedaten beim Authentifizierungs-Server verifiziert hat. Die Authentifizierung kann über 802.1X oder die MAC-Adresse erfolgen.

Bei der Authentifizierung über 802.1X müssen sowohl das Endgerät als auch der Authentifizierungs-Server das EAP-Protokoll (Extensive Authentication Protocol) unterstützen.

Aktivierung der Authentifizierung für einzelne Ports

Durch Aktivieren der entsprechenden Optionen legen Sie individuell für jeden Port fest, ob der Netzzugriffsschutz nach IEEE 802.1X auf diesem Port aktiviert ist.

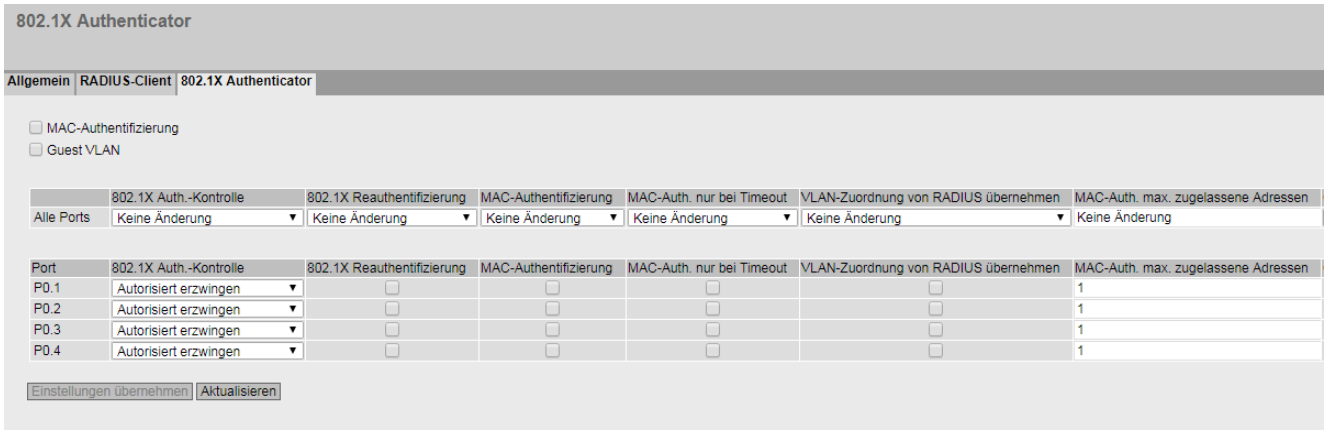


Bild 5-9 802.1X Authenticator - erster Teil der Tabelle

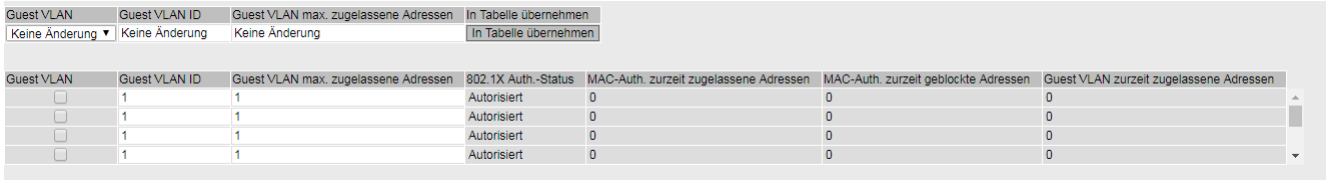


Bild 5-10 802.1X Authenticator - zweiter Teil der Tabelle

Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **MAC-Authentifizierung**
  Aktivieren oder deaktivieren Sie die MAC-Authentifizierung für das Gerät.
- **Guest VLAN**
  Aktivieren oder deaktivieren Sie die Funktion "Guest VLAN" für das Gerät.

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **802.1X Auth.-Kontrolle**
  Wählen Sie die gewünschte Einstellung.
  Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **802.1X Reauthentifizierung**
  Wählen Sie die gewünschte Einstellung.
  Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **MAC-Authentifizierung**
  Wählen Sie die gewünschte Einstellung.
  Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.

- **MAC Auth. only on Timeout**
  Wählen Sie die gewünschte Einstellung.
  Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **VLAN-Zuordnung von RADIUS übernehmen**
  Wählen Sie die gewünschte Einstellung.
  Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.

  Hinweis

  Private VLAN-Funktionalität und RADIUS-Authentifizierung

  Wenn die VLAN-Zuweisung über RADIUS-Authentifizierung für einen oder mehrere Ports eines VLAN aktiviert ist, sollten Sie dieses VLAN nicht zusätzlich als Private VLAN konfigurieren.

  Die Private VLAN-Funktionalität in Zusammenhang mit der VLAN-Zuweisung über RADIUS-Authentifizierung kann zu einem inkonsistenten Systemzustand führen.

- **MAC-Auth. max. zugelassene Adressen**
  Geben Sie an, wie viele MAC-Adressen gleichzeitig an dem Port kommunizieren dürfen.
  Wenn "Keine Änderung" eingetragen ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **Guest VLAN**
  Wählen Sie die gewünschte Einstellung.
  Wenn "Keine Änderung" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **Guest VLAN ID**
  Geben Sie die VLAN-ID des Ports an.
  Wenn "Keine Änderung" eingetragen ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **Guest VLAN max. zugelassene Adressen**
  Geben Sie an, wie viele Endgeräte gleichzeitig an diesem Port im "Guest VLAN" zugelassen sind.
  Wenn "Keine Änderung" eingetragen ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **In Tabelle übernehmen**
  Wenn Sie auf die Schaltfläche klicken, werden die Einstellungen für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  In dieser Spalte werden alle in diesem Gerät verfügbaren Ports aufgeführt.
- **802.1X Auth.-Kontrolle**
  Legen Sie die Authentifizierung des Ports fest:
  - Nicht autorisiert erzwingen
    Der Datenverkehr über den Port ist gesperrt.
  - Autorisiert erzwingen
    Der Datenverkehr über den Port ist ohne Einschränkung erlaubt.
    Werkseinstellung
  - Auto
    Endgeräte werden an dem Port mit dem Verfahren "802.1X" authentifiziert.
    Der Datenverkehr über den Port wird entsprechend des Authentifizierungsergebnisses erlaubt oder gesperrt.

- **802.1X Reauthentifizierung**
  Aktivieren Sie diese Option, wenn für ein bereits authentifiziertes Endgerät zyklisch eine Reauthentifizierung durchführt werden soll.
- **MAC-Authentifizierung**
  Aktivieren Sie diese Option, wenn Endgeräte mit dem Verfahren "MAC-Authentifizierung" authentifiziert werden sollen.
  Wenn die "802.1X Auth.-Kontrolle" auf "Auto" konfiguriert ist und die "MAC-Authentifizierung" aktiviert ist, beträgt der Timeout für das Verfahren "802.1X" 5 Sekunden. Wenn für die Authentifizierung mit dem Verfahren "802.1X" an einem Port eine manuelle Eingabe erforderlich ist, reichen die 5 Sekunden ggf. nicht aus. Um die Authentifizierung über "802.1X" ausführen zu können, deaktivieren Sie die MAC-Authentifizierung an diesem Port.
- **MAC Auth. only on Timeout**
  Bei aktiviertem Optionskästchen ist eine MAC-Authentifizierung nur nach einem 802.1X-Timeout möglich, nicht jedoch nach einer fehlgeschlagenen 802.1X-Authentifizierung. Bei nicht aktiviertem Optionskästchen ist eine MAC-Authentifizierung sowohl nach einem 802.1X-Timeout als auch nach einer fehlgeschlagenen 802.1X-Authentifizierung möglich.
- **VLAN-Zuordnung von RADIUS übernehmen**
  Der RADIUS-Server übermittelt dem IE-Switch, welchem VLAN der Port angehören soll. Aktivieren Sie diese Option, wenn die Informationen des Servers berücksichtigt werden sollen.
  Der Port kann dem entsprechenden VLAN nur zugeordnet werden, wenn das VLAN auf dem Gerät angelegt ist. Die Authentifizierung wird sonst abgelehnt.
- **MAC-Auth. max. zugelassene Adressen**
  Geben Sie an, wie viele MAC-Adressen gleichzeitig an dem Port kommunizieren dürfen.

  Hinweis

  Wenn ein Gerät mehrere MAC-Adressen verwendet, müssen alle MAC-Adressen authentifiziert werden. Hinterlegen Sie alle zu authentifizierenden MAC-Adressen auf dem RADIUS-Server. Tragen Sie die entsprechende Anzahl im Feld "MAC-Auth. max. zugelassene Adressen" ein.

- **Guest VLAN**
  Aktivieren Sie diese Option, wenn das Endgerät bei fehlgeschlagener Authentifizierung im "Guest VLAN" zugelassen werden soll.
  Der Port kann dem entsprechenden VLAN nur zugeordnet werden, wenn das VLAN auf dem Gerät angelegt ist. Die Authentifizierung wird sonst abgelehnt.
  Diese Funktion wird auch als "Authentication failed VLAN" bezeichnet.
- **Guest VLAN ID**
  Geben Sie die VLAN-ID des Guest VLANs an.
- **Guest VLAN max. zugelassene Adressen**
  Geben Sie an, wie viele Endgeräte gleichzeitig an diesem Port im "Guest VLAN" zugelassen sind.
- **802.1X Auth.-Status**
  Zeigt den Status der Authentifizierung des Ports an:
  - Autorisiert
  - Nicht autorisiert

- **MAC-Auth. zurzeit zugelassene Adressen**
  Zeigt die Anzahl der momentan zugelassene MAC-Adressen an.
- **MAC-Auth. zurzeit geblockte Adressen**
  Zeigt die Anzahl der momentan geblockten MAC-Adressen an.
- **Guest VLAN zurzeit zugelassene Adressen**
  Zeigt an, wie viele Endgeräte momentan im "Guest VLAN" zugelassen sind.

Vorgehensweise zur Konfiguration

Authentifizierung für einen einzelnen Port aktivieren

1. Aktivieren Sie in der Tabelle 2 in der entsprechenden Zeile die gewünschten Optionen.
2. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Authentifizierung für alle Ports aktivieren

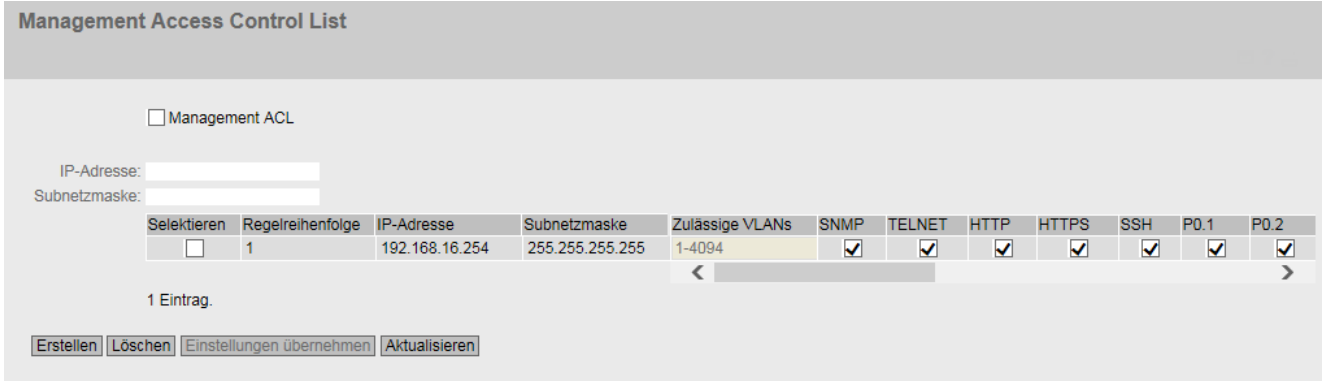
1. Wählen Sie in der Tabelle 1 die gewünschten Optionen.
2. Klicken Sie auf die Schaltfläche "In Tabelle übernehmen". In der Tabelle 2 werden die entsprechenden Einstellungen für alle Ports übernommen.
3. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

5.7.5 Management ACL

Konfigurationsbeschreibung

Auf dieser Seite können Sie die Sicherheit Ihres Geräts erhöhen. Um festzulegen, welche Station mit welcher IP-Adresse auf Ihr Gerät zugreifen darf, konfigurieren Sie die IP-Adresse oder auch ein ganzes Adress-Band.

Sie können einstellen, mit welchen Protokollen und über welche Ports die Station auf das Gerät zugreifen darf.



Beschreibung der angezeigten Felder

Hinweis

Bevor Sie diese Funktion aktivieren, beachten Sie Folgendes

Eine fehlerhafte Projektierung kann dazu führen, dass Sie nicht mehr auf das Gerät zugreifen können. Abhilfe erhalten Sie dann nur durch ein Rücksetzen des Geräts auf die Werkseinstellungen und anschließende Rekonfiguration. Projektieren Sie daher eine Zugriffsregel, die Ihnen den Zugriff auf das Management erlaubt, bevor Sie die Funktion aktivieren.

Die Seite enthält folgende Felder:

- **Management ACL**
  Aktivieren oder deaktivieren Sie die Zugriffskontrolle auf das Management des IE-Switches. Im Auslieferungszustand ist die Funktion deaktiviert.

  Hinweis

  Wenn die Funktion deaktiviert ist, dann besteht uneingeschränkter Zugriff auf das Management des IE-Switches. Erst wenn die Funktion aktiviert ist, werden die projektierten Zugriffsregeln berücksichtigt.

- **IP-Adresse**
  Tragen Sie die IPv4-Adresse oder die Netzadresse ein, für die die Regel gelten soll. Wenn Sie die IPv4-Adresse 0.0.0.0 verwenden, gelten die Einstellungen für alle IPv4-Adressen.
- **Subnetzmaske**
  Tragen Sie die Subnetzmaske ein. Die Subnetzmaske 255.255.255.255 ist für eine bestimmte IPv4-Adresse. Möchten Sie ein Subnetz zulassen, tragen Sie z. B. für ein Klasse C-Subnetz 255.255.255.0 ein. Die Subnetzmaske 0.0.0.0 gilt für alle Subnetze.

Die Tabelle gliedert sich in folgende Spalten:

- **Selektieren**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Regelreihenfolge**
  Zeigt die Reihenfolge an, in der die ACL-Regeln geprüft werden. Sobald eine Regel passt, wird diese angewendet. Die folgenden Regeln werden nicht betrachtet.
- **IP-Adresse**
  Zeigt die IPv4-Adresse an.
- **Subnetzmaske**
  Zeigt die Subnetzmaske an.

- **Zulässige VLANs**
  - Im Base Bridge-Modus "802.1Q VLAN Bridge"
    Tragen Sie die Nummer des VLANs ein, in dem sich das Gerät befindet. Nur die Station kann auf das Gerät zugreifen, wenn es sich in diesem konfigurierten VLAN befindet. Bleibt dieses Eingabefeld leer, gibt es keine Einschränkung bezüglich der VLANs.
  - Im Base Bridge-Modus "802.1D Transparent Bridge"
    Sie können bezüglich VLANs keine Zugriffsregeln definieren. Die Regeln gelten für alle VLANs.

  Hinweis

  Kompatibilität mit älteren Firmware-Versionen

  Falls Sie mit einer Firmware-Version < 1.2 bestimmte VLANs definiert haben, wird die Konfiguration der VLANs bei einem Firmware-Update durch den Default-Wert "1-4094" ersetzt.

- **SNMP**
  Legen Sie fest, ob die Station (bzw. die IPv4-Adresse) über das Protokoll SNMP auf das Gerät zugreifen darf.
- **TELNET**
  Legen Sie fest, ob die Station (bzw. die IPv4-Adresse) über das Protokoll TELNET auf das Gerät zugreifen darf.
- **HTTP**
  Legen Sie fest, ob die Station (bzw. die IPv4-Adresse) über das Protokoll HTTP auf das Gerät zugreifen darf.
- **HTTPS**
  Legen Sie fest, ob die Station (bzw. die IPv4-Adresse) über das Protokoll HTTPS auf das Gerät zugreifen darf.
- **SSH**
  Legen Sie fest, ob die Station (bzw. die IPv4-Adresse) über das Protokoll SSH auf das Gerät zugreifen darf.
- **Px.y**
  Legen Sie fest, ob die Station (bzw. die IPv4-Adresse) über diesen Port auf das Gerät zugreifen darf.
  Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.

Vorgehensweise zur Konfiguration

Hinweis

Bevor Sie diese Funktion aktivieren, beachten Sie Folgendes

Eine fehlerhafte Projektierung kann dazu führen, dass Sie nicht mehr auf das Gerät zugreifen können. Abhilfe erhalten Sie dann nur durch ein Rücksetzen des Geräts auf die Werkseinstellungen und anschließende Rekonfiguration. Projektieren Sie daher eine Zugriffsregel, die Ihnen den Zugriff auf das Management erlaubt, bevor Sie die Funktion aktivieren.

Hinweis

Reihenfolge beachten

Die Reihenfolge, in der Sie die ACL-Regeln anlegen, entspricht der Reihenfolge, in der die Regeln geprüft werden. Sobald eine Regel passt, wird diese angewendet. Die folgenden Regeln werden nicht betrachtet.

Neue Regel anlegen

1. Tragen Sie in das Eingabefeld "IP-Adresse" die IP-Adresse ein.
2. Tragen Sie in das Eingabefeld "Subnetzmaske" die Subnetzmaske ein.
3. Klicken Sie auf die Schaltfläche "Erstellen", um eine neue Zeile in der Tabelle anzulegen.
4. Konfigurieren Sie die Einträge der neuen Zeile.
5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen", um den neuen Eintrag in das Gerät zu übertragen.

Funktion aktivieren

1. Aktivieren Sie das Optionskästchen "Management ACL".
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen", um die projektierten Zugriffsregeln zu aktivieren.

Regel ändern

1. Konfigurieren Sie die Daten der Regel, die Sie ändern wollen.
2. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen", um die Änderungen in das Gerät zu übertragen.

Regel löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Wiederholen Sie den Vorgang für jeden Eintrag, den Sie löschen wollen.
3. Klicken Sie auf die Schaltfläche "Löschen". Die Regeln werden gelöscht und die Seite wird aktualisiert.

Troubleshooting/FAQ

6

6.1 Laden einer neuen Firmware über TFTP ohne WBM und CLI

Firmware

Die Firmware ist signiert und verschlüsselt. Es ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.

Betätigung des Tasters

Um eine neue Firmware zu laden, benötigen Sie den Taster. Beachten Sie zur Betätigung des Tasters unbedingt die Hinweise in der entsprechenden Betriebsanleitung.

Drücken Sie den Taster "RESET" beim SCALANCE XB-200 mit geringem Kraftaufwand.

Drücken Sie den Taster "SELECT/SET" beim SCALANCE XC-200.

Drücken Sie den Taster "SET" beim SCALANCE XF-200BA.

Drücken Sie den Taster "RESET" beim SCALANCE XP-200 bis zum Druckpunkt.

Drücken Sie den Taster "RESET" beim SCALANCE XR-300WG.

Vorgehensweise unter Microsoft Windows

Über TFTP können Sie ein Gerät mit einer neuen Firmware versehen, selbst dann, wenn es nicht über das WBM oder CLI erreichbar ist. In diesem Kapitel wird die Vorgehensweise exemplarisch für Microsoft Windows erklärt.

Um eine neue Firmware über TFTP zu laden, gehen Sie wie folgt vor:

1. Schalten Sie das Gerät spannungslos.
2. Drücken Sie den Taster und schließen Sie das Gerät mit gedrücktem Taster wieder an die Spannungsversorgung an.
3. Halten Sie den Taster so lange gedrückt, bis die rote Fehler-LED "F" anfängt zu blinken.
4. Lassen Sie den Taster los, solange die rote Fehler-LED noch blinkt.

   Hinweis

   Dieses Zeitintervall dauert nur einige Sekunden.

   Der Bootloader des Geräts wartet in diesem Zustand auf eine neue Firmware-Datei, die Sie per TFTP laden können.
5. Verbinden Sie einen PC über ein Ethernet-Kabel mit dem Port "P1".
6. Vergeben Sie über DHCP oder mit dem Primary Setup Tool eine IP-Adresse für das Gerät.

7. Wechseln Sie in einer Windows-Eingabeaufforderung in das Verzeichnis, in dem sich die Datei mit der neuen Firmware befindet und rufen Sie das folgende Kommando auf:
   `tftp -i <IP-Adresse> put <Firmwaredatei>`

   Hinweis

   Sie können TFTP unter Microsoft Windows wie folgt aktivieren:

   "Systemsteuerung" > "Programme und Funktionen" > "Windows-Funktionen aktivieren und deaktivieren" > "TFTP-Client"

8. Nachdem die Firmware komplett auf das Gerät übertragen und validiert wurde, erfolgt ein automatischer Neustart des Geräts. Dieser Vorgang kann einige Minuten in Anspruch nehmen.

6.2 Meldung: SINEMA-Konfiguration noch nicht akzeptiert

Wenn im Anzeigebereich die folgende Meldung angezeigt wird, ist bei der Übertragung der Konfiguration von STEP 7 Basic / Professional ab V13 auf das Gerät ein Fehler aufgetreten:

"Die SINEMA-Konfiguration ist noch nicht akzeptiert. Bei einem Neustart des Geräts gehen alle Konfigurationsänderungen verloren."

Eine mögliche Ursache ist z. B., dass während der Übertragung das Gerät nicht mehr erreichbar war.

Wenn Sie jetzt einen Parameter direkt im Gerät ändern (WBM/CLI/SNMP), gehen diese Änderungen bei einem Neustart des Geräts verloren.

Abhilfe

1. Öffnen Sie das entsprechende STEP 7-Projekt in STEP 7 Basic / Professional.
2. Öffnen Sie die Projektansicht.
3. Selektieren Sie in der Projektnavigation das Gerät.
4. Wählen Sie im Kontextmenü des selektierten Geräts den Befehl "Gehe zu Netzsicht".
5. Selektieren Sie das Gerät in der Netzansicht.
6. Wählen Sie im Kontextmenü des selektierten Geräts den Befehl "SCALANCE-Konfiguration > Als Startkonfiguration speichern".

Ergebnis

Die Konfiguration wird auf dem Gerät gespeichert. Die Meldung im Anzeigebereich ist nicht mehr sichtbar. Eine Konfigurationsänderung direkt am Gerät geht durch einen Neustart des Geräts nicht mehr verloren.

6.3 Austausch von Konfigurationsdaten mit STEP7 Basic/Professional über eine Datei

Über die beiden Dateitypen "RunningSINEMAConfig" und "SINEMAConfig" ("System > Laden&Speichern > HTTP/TFTP/SFTP") können Sie Konfigurationsdaten zwischen einem Gerät (WBM) und STEP7 Basic/Professional über eine Datei austauschen. Der Export/Import einer Datei über STEP 7 Basic/Professional ist im Folgenden beschrieben.

Konfigurationsdaten über STEP 7 Basic/Professional exportieren

Um Konfigurationsdaten über STEP 7 Basic/Professional zu exportieren, gehen Sie wie folgt vor:

1. Öffnen Sie das entsprechende STEP 7-Projekt in STEP 7 Basic/Professional.
2. Öffnen Sie die Projektansicht.
3. Öffnen Sie die Netzsicht bzw. die Topologiesicht.
4. Öffnen Sie den Hardware-Katalog.
5. Navigieren Sie im Hardware-Katalog zu dem Gerät mit der passenden Artikelnummer.
6. Selektieren Sie das ausgewählte Gerät mit einem Mausklick.
7. Stellen Sie die passende Firmware-Version über die Klappliste des Hardware-Katalogs ein.
8. Ziehen Sie das Gerät mit Drag & Drop in die Netzsicht bzw. in die Topologiesicht.
9. Selektieren Sie das Gerät in der Netzsicht bzw. in die Topologiesicht.
10. Konfigurieren Sie das Gerät im Inspektorfenster unter "Eigenschaften > Allgemein".
11. Navigieren Sie im Inspektorfenster unter "Eigenschaften > Allgemein" zum Parameter "Verwaltung".
12. Klicken Sie in der Parametergruppe "Datei importieren/exportieren" auf die Schaltfläche "Nach Datei exportieren".
13. Wählen Sie einen Speicherort für die Datei.
14. Vergeben Sie einen Namen für die Datei.
15. Klicken Sie auf die Schaltfläche "Speichern".
    Der Dialog "Konfigurationsdatei exportieren" wird geöffnet.
16. Vergeben Sie ein Passwort für die Verschlüsselung der Datei.

    Hinweis

    Sie benötigen dieses Passwort, wenn Sie die Datei über das WBM in ein Gerät laden.

17. Klicken Sie auf die Schaltfläche "OK".

Konfigurationsdaten über STEP 7 Basic/Professional importieren

Um Konfigurationsdaten über STEP 7 Basic/Professional zu importieren, gehen Sie wie folgt vor:

1. Öffnen Sie das entsprechende STEP 7-Projekt in STEP 7 Basic/Professional.
2. Öffnen Sie die Projektansicht.
3. Öffnen Sie die Netzsicht bzw. die Topologiesicht.
4. Öffnen Sie den Hardware-Katalog.
5. Navigieren Sie im Hardware-Katalog zu dem Gerät mit der passenden Artikelnummer.
6. Selektieren Sie das ausgewählte Gerät mit einem Mausklick.
7. Stellen Sie die passende Firmware-Version über die Klappliste des Hardware-Katalogs ein.
8. Ziehen Sie das Gerät mit Drag & Drop in die Netzsicht bzw. in die Topologiesicht.
9. Selektieren Sie das Gerät in der Netzsicht bzw. in die Topologiesicht.
10. Navigieren Sie im Inspektorfenster unter "Eigenschaften > Allgemein" zum Parameter "Verwaltung".
11. Klicken Sie in der Parametergruppe "Datei importieren/exportieren" auf die Schaltfläche "Aus Datei importieren".
12. Selektieren Sie die gewünschte Datei.
13. Klicken Sie auf die Schaltfläche "Öffnen".
    Der Dialog "Konfigurationsdatei importieren" wird geöffnet.
14. Geben Sie das Passwort für die Verschlüsselung der Datei ein.

    Hinweis

    Sie vergeben dieses Passwort im WBM unter "System > Laden&Speichern > Passwörter".

15. Klicken Sie auf die Schaltfläche "OK".

Anhang A

A

A.1 Parameter in Syslog-Meldungen

Die Syslog-Meldungen können folgende Parameter beinhalten:

Parameter	Beschreibung	Beispiel
ip address	Quell- oder Ziel-IP-Adresse nach RFC1035 oder RFC4291 Abschnitt 2.2 z. B. IPV4-Format: %d.%d.%d.%d	192.168.1.105 2001:DB8::8:800:200C:417A
client mac	MAC-Adresse des WLAN-Clientgeräts Format: %02x:%02x:%02x;%02x:%02x:%02x	00:0C:29:2F:09:B3
dest mac	MAC-Adresse der Schnittstelle im Ziel-Netzwerk Format: %02x:%02x:%02x;%02x:%02x:%02x	00:0C:29:2F:09:B3
src mac	MAC-Adresse der Schnittstelle im Quell-Netzwerk Format: %02x:%02x:%02x;%02x:%02x:%02x	00:0C:29:2F:09:B3
src port	Quell-Port (0 to 65535) Format: %d	2345
dest port	Ziel-Port (0 to 65535) Format: %d	80
protocol	Bezeichnung des Dienstes, der dieses Ereignis generiert hat, oder des verwendeten Layer-4-Protokolls. Die möglichen Werte sind Protokollnamen wie TCP oder UDP Format: %s	Zeichenketten von: UDP | TCP | WBM | Telnet | SSH | Console | TFTP | SFTP
group	Zeichenkette, die die Gruppe anhand ihres Namens identifiziert Format: %s	it-service
user name	Zeichenkette, die den authentifizierten Benutzer anhand seines Namens identifiziert ohne Leerzeichen Format: %s	maier
local interface	Symbolischer Name für die lokale Schnittstelle Format: %s	Console
action user name	Identifiziert den Benutzer anhand seines Namens. Dies ist nicht der authentifizierte Benutzer Format: %s	Peter.Maier
role	Symbolischer Name für die Gruppenrolle Format: %s	Administrator
time minute timeout	Minutenanzahl Format: %d	44
time second	Sekundenanzahl Format: %d	44

Parameter	Beschreibung	Beispiel
failed login count	Anzahl der fehlgeschlagenen Loggins Format: %d	10
max sessions	Anzahl der Sitzungen Format: %d	10
vap	Symbolischer Name der virtuellen Access Point-Schnittstelle Format: %s	VAP1.1
status reason	Zusätzliche Statusinformation als lesbare Zeichenfolge. Sie kann mehrere Wörter enthalten. Damit die Zeichenfolge analysiert werden kann, muss sie mit „(“ beginnen und mit „)“ enden. Format: (%s) oder (%s %s) usw.	(Invalid group cipher) (Unknown peer)
wlan interface	Symbolischer Name der WLAN-Schnittstelle Format: %s	WLAN1
ssid	SSID in ASCII-Darstellung beliebig viele Leerzeichen Format: %s	MyWLAN
channel	Bezeichnung des Kanals Format %d	12
signal strength	Signalstärke Format %d	12
version	Bezeichnung der Version ohne Leerzeichen Format: %s	V1.0.3SP1
resource	Durch das Schutzstufenkonzept geschützter Ressourcenname ohne Leerzeichen Format: %s	FullReadAccess
trigger condition	Zeichenkette für eine Auslösebedingung, mit der die betreffende Funktion aktiviert wird ohne Leerzeichen Format: %s	E/A-Pin FB-88
trigger pin	Zeichenkette für einen IO-Pin, der das Ereignis ausgelöst ohne Leerzeichen Format: %s	DI1
firewall rule	Zeichenkette für einen Firewall-Regelsatz mit Leerzeichen Format: %s	Rule1
subject	Zeichenkette für den Betreff im Zertifikat. Wird verwendet als Teil der zertifikatbasierten Authentifizierung mit Leerzeichen und muss zusätzlich Unicode-Zeichen enthalten Format: (% S) oder (% S% S) bei UTF8-Code.	(Peter Maier)

Parameter	Beschreibung	Beispiel
config detail	Zeichenkette für die Konfiguration mit Leerzeichen Format: %s	OpenVPN
connection name	Name einer VPN-Verbindung	to_Baugruppe1
firewall accept	Firewall-Aktion ausgeführt (akzeptiertes Paket)	ACCEPT
firewall action reject	Firewall-Aktion ausgeführt (abgelehntes Paket)	REJECT DROP
length	Länge des Netzwerkpakets (in Bytes) Format: %d	52
network interface	Symbolischer Name einer Netzwerkschnittstelle Format:%s	vlan 1

A.2 Syslog-Meldungen

In diesem Kapitel werden mögliche Syslog-Meldungen beschrieben. Sie sind nach ihrem Schweregrad "Severity" sortiert.

Syslog-Meldungen mit Severity-Typ "Warning"

Log-Text	User {user name} account is locked for {time} minutes after {failed login count} unsuccessful login attempts.
Beschreibung	Bei zu vielen fehlgeschlagenen Anmeldungen wurde das entsprechende Benutzerkonto für einen bestimmten Zeitraum gesperrt.
Beispiel	User admin account is locked for 10 minutes after 30 unsuccessful login attempts.
Severity	Warning
Facility	local0

Log-Text	The session of user {user name} was closed after {time} seconds of inactivity.
Beschreibung	Die aktuelle Sitzung wurde aufgrund der Inaktivität gesperrt.
Beispiel	The session of user admin was closed after 60 seconds of inactivity.
Severity	Warning
Facility	local0

Log-Text	Console: User {user name} failed to log in.
Beschreibung	Falscher Benutzername oder falsches Passwort (Anmeldeinformationen) bei der lokalen Anmeldung angegeben.
Beispiel	Console: User testuser failed to log in.
Severity	Warning
Facility	local0

Log-Text	{protocol}: User {user name} failed to log in from {ip address}.
Beschreibung	Falscher Benutzername oder falsches Kennwort (Anmeldeinformationen) bei der Remote-Anmeldung angegeben.
Beispiel	SSH: User testuser failed to log in from 192.168.0.1.
Severity	Warning
Facility	local0

Log-Text	{protocol}: The maximum number of {max sessions} concurrent login session exceeded.
Beschreibung	Die maximale Anzahl gleichzeitiger Sitzungen ist überschritten.
Beispiel	WBM: The maximum number of 8 concurrent login session exceeded.
Severity	Warning
Facility	local0

Log-Text	{protocol}: Failed to load file type Firmware.
Beschreibung	Fehler beim Bereitstellen des Firmware-Updates.
Beispiel	WBM: Failed to load file type Firmware.
Severity	Warning
Facility	local0

Syslog-Meldungen mit Severity-Typ "Info"

Log-Text	Console: User {user name} logged in.
Beschreibung	Gültige Anmeldeinformationen, die bei der lokalen Anmeldung angegeben werden.
Beispiel	Console: User admin logged in.
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} logged in from {ip address}.
Beschreibung	Gültige Anmeldeinformationen, die bei der Remote-Anmeldung angegeben werden.
Beispiel	WBM: User admin logged in from 192.168.0.1.
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} logged out from {ip address}.
Beschreibung	Benutzersitzung beendet - Abmeldung erfolgt.
Beispiel	SSH: User admin logged out from 192.168.0.1.
Severity	Info
Facility	local0

Log-Text	Console: User {user name} logged out.
Beschreibung	Benutzersitzung beendet - Abmeldung erfolgt.
Beispiel	Console: User admin logged out.
Severity	Info
Facility	local0

Log-Text	{protocol}: Default user {user name} logged in from {ip address}.
Beschreibung	User logged in with default user name and password.
Beispiel	SSH: Default user admin logged in from 192.168.0.1.
Severity	Info
Facility	local0

Log-Text	Console: Default user {user name} logged in.
Beschreibung	Benutzer mit Standardbenutzername und Kennwort ist angemeldet.
Beispiel	Console: Default user admin logged in.
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} changed own password.
Beschreibung	Benutzer hat sein Passwort geändert.
Beispiel	WBM: User admin changed own password.
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} changed password of user {action user name}.
Beschreibung	Benutzer hat ein anderes Passwort geändert.
Beispiel	Console: User admin changed password of user test.
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} created user-account {action user name}.
Beschreibung	Der Administrator hat ein neues Konto erstellt.
Beispiel	WBM: User admin created user-account joachim.
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} deleted user-account {action user name}.
Beschreibung	The administrator deleted an existing account.
Beispiel	WBM: User admin deleted user-account joachim.

Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} created group {group}.
Beschreibung	Der Administrator hat ein vorhandenes Konto gelöscht.
Beispiel	WBM: User admin created group it-service.
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} deleted group {group}.
Beschreibung	Der Administrator hat eine vorhandene Gruppe gelöscht.
Beispiel	WBM: User admin deleted group it-service.
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} loaded file type Firmware {version} (restart required).
Beschreibung	Firmware-Update ist erfolgreich implementiert.
Beispiel	WBM: User admin loaded file type Firmware V02.00.00 (restart required).
Severity	Info
Facility	local0

Log-Text	{protocol}: Loaded file type Firmware {version} (restart required).
Beschreibung	Firmware-Update ist erfolgreich implementiert.
Beispiel	TFTP: Loaded file type Firmware V02.00.00 (restart required).
Severity	Info
Facility	local0

Log-Text	Device configuration changed.
Beschreibung	Die Gerätekonfiguration ist dauerhaft geändert.
Beispiel	Device configuration changed.
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} loaded file type Config (restart required).
Beschreibung	Die Konfiguration wird angewendet.
Beispiel	WBM: User admin loaded file type Config (restart required).
Severity	Info
Facility	local0

Log-Text	{protocol}: Loaded file type Config (restart required).
Beschreibung	Die Konfiguration wird angewendet.
Beispiel	TFTP: Loaded file type Config (restart required).
Severity	Info
Facility	local0

Log-Text	{protocol}: User {user name} loaded file type ConfigPack (restart required).
Beschreibung	Die Konfiguration wird angewendet.
Beispiel	WBM: User admin loaded file type ConfigPack (restart required).
Severity	Info
Facility	local0

Log-Text	{protocol}: Loaded file type ConfigPack (restart required).
Beschreibung	Die Konfiguration wird angewendet.
Beispiel	TFTP: Loaded file type ConfigPack (restart required).
Severity	Info
Facility	local0

Index

A

Abmeldung
  automatisch, 187
ACL, 293, 346
Aging
  Dynamic MAC Aging, 252
Aging Time, 299
Alarmereignisse, 146
anmelden
  über HTTP, 69
  über HTTPS, 69
Artikelnummer, 79
Aufstellungsort, 121
Authentifizierung, 171, 343

B

Benutzergruppen, 334
Bridge, 265
  Bridge Priority, 265
  Root Bridge, 265
Bridge Max Age, 266
Bridge Max Hop Count, 266
Broadcast, 304

C

Class of Service, 226
Combo Port Medientyp, 191, 197
Command Line Interface (CLI), 351
Configuration Mode, 119
CoS, 226
  Warteschlange, 226
CoS (Class of Service), 55
CoS-Priorisierung, 55
C-PLUG, 206
  Formatieren, 208
  Konfiguration speichern, 208
CRC, 97

D

DCP Discovery, 210
DCP-Server, 117, 283
DCP-Weiterleitung, 283
DHCP
  Client, 148
  Server, 150
DSCP, 227
DST
  Sommerzeit, 175, 176

E

E-Mail-Funktion, 146
  Alarmereignisse, 146
  Netzüberwachung, 146
Ereignisprotokoll-Tabelle, 80
Ereignisse
  Log-Tabelle, 80
Ethernet-Statistiken
  History, 98
  Schnittstellenstatistik, 93
  Telegrammfehler, 96
  Telegrammlänge, 94
  Telegrammtyp, 95

F

Fehlerstatus, 82
Fehlertyp
  CRC, 97
  Fragmente, 97
  Jabbers, 97
  Kollisionen, 97
  Oversize, 97
  Undersize, 97
  Zu kurz, 97
  Zu lang, 97
Fehlerüberwachung
  Redundanz, 202
  Verbindungszustandsänderung, 200
Filter
  Filterkonfiguration, 290
Firmware, 351
Forward Delay, 266

G

geografische Koordinaten, 121
Glossar, 12
GMRP, 300
Gruppen, 334

Gültigkeitsbereich, 9
GVRP, 239

H

Hardwareausgabestand, 79
Hello Time, 266
Hersteller, 78
Herstellerkennung, 79
HRP, 257
HTTP
    Laden/Speichern, 128
HTTPS
    Server, 117

I

IGMP, 299
Information
    ARP-Tabelle, 80
    Gruppen, 116
    LLDP, 102
    Log-Tabelle, 80
    Ringredundanz, 87
    Ring-Redundanz, 89
    Rolle, 115
    Security, 111, 114
    SNMP, 110
    Spanning Tree, 84
    Start Page, 71
    Versions, 77

K

Kabeltest, 216

L

LACP, 279
LACP Timeout, 282
Layer 2, 220
Link Check, 91
Link Check Status, 91
LLDP, 102, 285
Lokale Benutzer, 329
Loop, 276
Loop Detection, 276

M

Management ACL, 346
Mirroring, 59
    General, 248
    Port, 251
MSTP, 263, 272
    Port, 267
    Portparameter, 273
MSTP-Instanz, 273, 274
Multicast, 296
Multiple Spanning Tree, 267, 272

N

NAPT
    konfigurieren, 325
NAT
    konfigurieren, 320, 322, 324
NAT-Übersetzungen, 107
Negotiation, 191
Netzüberwachung, 146
Neustart, 124
NTP, 296
    Client, 182

P

Passwort, 335
    Optionen, 338
Ping, 209
PLUG, 206
    C-PLUG, (C-PLUG)
PoE, 212, 213
    Port, 213
Port, 193
    Link Check, 91
    Portkonfiguration, 190, 199
Port-Diagnose
    Kabeltest, 216
    SFP-Diagnose, 217
Portkonfiguration, 193, 199
Power over Ethernet, 212
    Port, 213
Primary Setup Tool, 283
Priorisierung, 229
Priorität, 229
Priority, 266
PROFINET, 29, 203
PROFINET IO, 29

PST, 283
Punkt zu Punkt, 32

Q

QoS, 229

R

RADIUS, 339
Rate Control, 232
redundante Netzwerke, 265
Redundanz, 254, 257
Redundanzverfahren
HRP, 39
RESET-Taster, 187
Ringredundanz, 254
HRP, 222, 254
MRP, 222, 254
Ring Ports, 255
Standby, 257
RMON
History, 308
Statistik, 306
Rollen, 332
Root Max Age, 266
Routing
Routing-Tabelle, 106
RSTP, 263
RSTP+
Eigenschaften, 33
Konfiguration, 36
Topologie, 33
Rücksetzen, 124

S

Schleifenerkennung, 276
SELECT/SET-Taster, 187
Seriennummer, 79
SFP-Diagnose, 217
SFTP
Laden/Speichern, 136
SHA-Algorithmus, 168
Sicherheitseinstellungen, 168
SIMATIC NET-Glossar, 12
SIMATIC NET-Handbuch, 11
SMTP
Client, 117
SNMP, 60, 118, 164, 168
Benutzer, 170
Gruppen, 168
SNMPv1, 60
SNMPv2c, 60
SNMPv3, 60
Trap, 166
Übersicht, 110
Softwareausgabestand, 79
Spanning Tree, 263
Enhanced Passive Listening Compatibility, 276
Information, 84
MSTP, 263
Rapid Spanning Tree, 32
RSTP, 263
Spannungsversorgung
Überwachung, 199
SSH
Server, 117
Standby, 257
Standby-Redundanz, 49
Startseite, 71
STEP 7, 283
STP, 263
Subnetze
Default-Gateway, 314
Konfiguration (IPv4), 313
Übersicht (IPv4), 310
Subnetzmaske, 23
Syslog, 188
Client, 117
System
Allgemeine Informationen, 120
Konfiguration, 116
Systemereignisprotokoll
Agent, 188
Systemereignisse
Konfiguration, 141
Severity Filter, 145
Systemhandbuch, 11

T

Taster, 187, 351
Taster RESET, 351
Taster SELECT/SET, 351
Taster SET, 351
Telegrammfehler
CRC, 97
Fragmente, 97
Jabbers, 97
Kollisionen, 97
Zu kurz, 97
Zu lang, 97

Telegrammfehlerstatistik, 96
Telnet
    Server, 117
TFTP
    Laden/Speichern, 132
Trust Mode, 229

U

Uhrzeit
    manuelle Einstellung, 173
    NTP (Network Time Protocol), 182
    SIMATIC Time Client, 185
    SNTP (Simple Network Time Protocol), 179
    Systemzeit, 173
    Uhrzeitsynchronisation, 179, 182
    UTC-Zeit, 182, 183, 185
    Zeitzone, 182, 185

V

Verfügbare Systemfunktionen, 15
VLAN, 54
    Port VID, 241
    Priorität, 241
    Tag, 241
    VLAN-ID, 56
    VLAN-Tag, 54

W

Wartungsdaten, 78
Web Based Management, 67
    Voraussetzung, 67
Web Based Management (WBM), 351

Z

Zeiteinstellung, 118
Zugriffssteuerung, 291, 293
    automatisches Lernen, 293