SIEMENS

SIMATIC NET

Industrial Ethernet Switches SCALANCE X-300 / X-400

Projektierungshandbuch

03/2022
C79000-G8900-C187-33

Vorwort

Empfehlungen zur Netzwerksicherheit 1

Einleitung 2

Netzwerkmanagement für industrielle Netze 3

Vergabe einer IP-Adresse 4

Konfiguration über Web Based Management und Command Line Interface 5

Konfiguration und Diagnose über SNMP 6

PROFINET IO-Funktionalität 7

C-PLUG 8

Firmwareupdate 9

Anhang A A

Anhang B B

Anhang C C

Anhang D D

Anhang E E

Verwendete Verschlüsselungsverfahren (Ciphers) F

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
Digital Industries
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

C79000-G8900-C187-33
Ⓟ 03/2022 Änderungen vorbehalten

Copyright © Siemens AG 2006 - 2022.
Alle Rechte vorbehalten

Vorwort

Zweck des Handbuchs

Dieses Handbuch unterstützt Sie bei der Konfiguration der Industrial Ethernet Switches SCALANCE X-300 und X-400. Es zeigt die technischen Möglichkeiten, die ein SCALANCE X-300/ X-400 bietet und beschreibt die Durchführung der Konfiguration mit dem Web Based Management und dem Command Line Interface.

Gültigkeitsbereich dieses Handbuchs

Dieses Handbuch ist für folgende Software-Versionen gültig:

- SCALANCE X-300/X408-2 ab Firmware-Version 4.1.4
- SCALANCE X414-3E ab Firmware-Version 3.10.2
- SINEC PNI ab Version 1.0
- SNMP/OPC-Server ab Version 6.2.1

Dieses Handbuch ist für folgende Produktlinien gültig:

- SCALANCE X-300
- SCALANCE X-400

Innerhalb der Produktlinie SCALANCE X-300 gibt es mehrere Produktgruppen (siehe dazu auch Produktübersicht in der "Betriebsanleitung Industrial Ethernet Switches SCALANCE X-300").

Bezeichnung der Geräte in diesem Projektierungshandbuch

Die Beschreibungen in diesem Projektierungshandbuch gelten, falls die Beschreibung sich nicht auf ein spezielles Gerät der Produktlinie bezieht, immer für die Geräte der Produktlinien SCALANCE X-300 und SCALANCE X-400 die im Gültigkeitsbereich von diesem Projektierungshandbuch genannt sind. Im Weiteren werden die Geräte als "IE-Switches" bezeichnet.

SIMATIC NET-Glossar

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

Sie finden das SIMATIC NET-Glossar hier:

- SIMATIC NET Manual Collection oder Produkt-DVD
  Die DVD liegt einigen SIMATIC NET-Produkten bei.
- Im Internet unter folgender Adresse:
  50305045 (http://support.automation.siemens.com/WW/view/de/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:
http://www.siemens.com/industrialsecurity (http://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:
http://www.siemens.com/industrialsecurity (http://www.siemens.com/industrialsecurity)

Hinweis zum Firmware-/Software-Support

Informieren Sie sich regelmäßig über neue Firmware-/Software-Versionen oder Sicherheits-Updates und wenden Sie diese an. Ab der Veröffentlichung einer neuen Version werden Vorgängerversionen nicht mehr unterstützt und nicht gewartet.

Marken

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

SCALANCE, C-PLUG, OLM

Lizenzbedingungen

Hinweis

Open Source Software

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

Sie finden die Lizenzbedingungen in folgenden Dokumenten, die sich auf dem mitgelieferten Datenträger befinden:

- OSS_Siemens_86.pdf
- OSS_SCALANCE-X-300-X408_86.pdf
- OSS_SCALANCE-X414_74.pdf

Sie finden diese Dokumente auf der Produkt-DVD in folgendem Verzeichnis: /Open Source Information

Inhaltsverzeichnis

Vorwort ... **3**

1 Empfehlungen zur Netzwerksicherheit ... **13**

2 Einleitung ... **19**

2.1 Technische Dokumentation für SCALANCE X-300/X-400 ... 19

3 Netzwerkmanagement für industrielle Netze ... **21**

3.1 Konfigurationsmöglichkeiten eines SCALANCE X-300/X-400 ... 21

3.2 Funktion und Eigenschaften eines SCALANCE X-300/X-400 ... 22

3.3 Möglichkeiten der Medienredundanz ... 27
3.3.1 Medienredundanz in Ringtopologien ... 28
3.3.2 MRP ... 29
3.3.3 MRP-Mehrfachringe ... 33
3.3.4 HRP ... 34

4 Vergabe einer IP-Adresse ... **35**

4.1 Aufbau einer IP-Adresse ... 35

4.2 Erstmalige Vergabe einer IP-Adresse ... 36

4.3 Vergabe einer IP-Adresse über die serielle Schnittstelle der SCALANCE X-400 ... 38

4.4 Adressvergabe mit dem BOOTP-Client ... 39

4.5 Adressvergabe mit dem DHCP-Client ... 39

4.6 Adressvergabe mit SINEC PNI ... 40

5 Konfiguration über Web Based Management und Command Line Interface ... **41**

5.1 Allgemeine Informationen über Web Based Management und Command Line Interface ... 42
5.1.1 Einleitung ... 42
5.1.2 Die Leuchtdiodensimulation des Web Based Managements (WBM) ... 44
5.1.3 Bedienung des Web Based Managements ... 45
5.1.4 Command Line Interface (CLI) ... 46

5.2 Das Menü System ... 49
5.2.1 System Configuration ... 49
5.2.2 System Identification & Maintenance (I&M) ... 51
5.2.3 System Restart & Defaults ... 52
5.2.4 System Save & Load via HTTP ... 55
5.2.5 System Save & Load via TFTP ... 60
5.2.6 System Version Numbers ... 63
5.2.7 System Passwords & Login Mode ... 64
5.2.8 System Select/Set Button ... 66
5.2.9 System Event Log Table ... 68
5.2.10 C-PLUG Information ... 69
5.2.11 Geografische Koordinaten ... 72

5.3 Das Menü X-300/X-400 ... 73
5.3.1 X-300/X-400 Status Page ... 73
5.3.2 Ring Redundancy ... 77
5.3.2.1 X-300/X-400 Ring Redundancy Information ... 77
5.3.2.2 X-300/X-400 Ring Configuration ... 81
5.3.2.3 X-300/X-400 HRP Redundanzmanager Observer ... 85
5.3.2.4 X-300/X-400 Standby Mask ... 86
5.3.2.5 X-300/X-400 Standby-Observer ... 90
5.3.3 X-300/X-400 Fault Mask ... 93
5.3.4 X-300/X-400 Counters ... 96

5.4 Das Menü Agent ... 97
5.4.1 Agent Configuration ... 97
5.4.2 Ping ... 105
5.4.3 SNMP ... 106
5.4.3.1 Agent SNMP Configuration ... 106
5.4.3.2 SNMPv1 Trap Configuration ... 110
5.4.3.3 SNMPv3 Group Configuration ... 111
5.4.3.4 SNMPv3 Users Configuration ... 114
5.4.4 Agent Timeout Configuration ... 118
5.4.5 Agent Event Configuration ... 119
5.4.6 Agent Digital Input Configuration (SCALANCE X414-3E) ... 124
5.4.7 Agent E-Mail Configuration ... 126
5.4.8 Agent Syslog Configuration ... 128
5.4.9 Agent DHCP Configuration ... 129
5.4.10 Time Config ... 130
5.4.10.1 Agent Time Configuration ... 130
5.4.10.2 SNTP Client Configuration ... 132
5.4.10.3 NTP Client Configuration ... 134
5.4.10.4 Daylight Saving Time ... 136
5.4.11 Agent PNIO Configuration ... 140
5.4.12 Management Access Control List ... 141

5.5 Das Menü Switch ... 145
5.5.1 Switch Configuration ... 146
5.5.2 Port Status ... 151
5.5.3 Link Check (SCALANCE X-300/X408-2) ... 157
5.5.4 Port Mirroring ... 162
5.5.5 Link Aggregation ... 164
5.5.5.1 Link Aggregation ... 164
5.5.5.2 LACP Configuration ... 170
5.5.6 IEEE 802.1x ... 170
5.5.6.1 802.1x RADIUS Configuration ... 170
5.5.6.2 802.1x Port Parameters ... 173
5.5.6.3 802.1x Port Configuration ... 174
5.5.7 Unicast Filter (ACL) ... 178
5.5.7.1 Current Unicast Filter (Access Control List) ... 178
5.5.7.2 Access Control List Learning ... 182
5.5.7.3 Access Control Port Configuration ... 184
5.5.7.4 Unknown Unicast Blocking Mask ... 185
5.5.8 Multicast Groups ... 186
5.5.8.1 Current Multicast Groups ... 186
5.5.8.2 GMRP Configuration ... 191

5.5.8.3 IGMP Configuration ... 192
5.5.8.4 Unknown Multicast Blocking Mask ... 193
5.5.9 Broadcast Blocking Mask ... 194
5.5.10 Fast Learning ... 195
5.5.11 Load Limits Configuration (SCALANCE X414-3E) ... 196
5.5.12 Load Limits Rates (SCALANCE X-300/X408-2) ... 199
5.5.13 VLAN ... 202
5.5.13.1 Current VLAN Configuration ... 202
5.5.13.2 VLAN Port Parameters ... 208
5.5.13.3 GVRP Configuration ... 211
5.5.13.4 VLAN Learning ... 212
5.5.13.5 X-300 VLAN Port Priority Mapping ... 213
5.5.14 STP/RSTP ... 215
5.5.14.1 Spanning Tree Configuration ... 215
5.5.14.2 Spanning Tree Port Parameters ... 219
5.5.14.3 Spanning Tree Port Configuration ... 221
5.5.15 MSTP (SCALANCE X-300/X408) ... 225
5.5.15.1 Multiple Spanning Tree Configuration ... 225
5.5.15.2 CIST Port Parameters ... 228
5.5.15.3 MSTP Instances Configuration ... 233
5.5.15.4 Multiple Spanning Tree Port Configuration ... 235
5.5.16 QoS ... 239
5.5.16.1 QoS Configuration ... 239
5.5.16.2 CoS to Queue Mapping ... 241
5.5.16.3 DSCP to Queue Mapping ... 242
5.5.17 LLDP ... 243
5.5.17.1 LLDP Configuration ... 243
5.5.17.2 LLDP Neighbors ... 245
5.5.18 Fiber Monitoring Protocol ... 246
5.5.19 DCP Configuration ... 251
5.5.20 DHCP Relay Agent ... 252
5.5.20.1 DHCP Relay Agent Configuration ... 252
5.5.20.2 DHCP Relay Agent Port Configuration ... 254
5.5.21 Precision Time Protocol (PTP) entsprechend IEEE 1588 ... 256
5.5.22 Konfiguration des Precision Time Protocols mit dem WBM ... 263
5.5.23 Konfiguration des Precision Time Protocols mit dem CLI ... 267
5.5.24 Port Diagnostics ... 268
5.5.24.1 Cable Tester (SCALANCE X-300/X408-2) ... 268
5.5.24.2 SFP Diagnostics ... 269
5.5.24.3 POF Diagnostics ... 271
5.5.24.4 FM Diagnostics ... 273
5.5.24.5 POF-Ports ... 274
5.5.25 Loop Detection ... 277
5.5.26 NAT - Network Address Translation ... 284
5.5.27 Statistics ... 287
5.5.27.1 Packet Size Statistic ... 289
5.5.27.2 Packet Type Statistic ... 291
5.5.27.3 Error Statistic ... 293

5.6 Der Menüpunkt PoE ... 296

5.7 Das Menü Router (SCALANCE X414-3E) ... 299
5.7.1 Router Configuration ... 300

5.7.2 Router Subnets ... 301
5.7.3 Current Routes ... 304
5.7.4 RIPv2 Configuration ... 307
5.7.5 RIPv2 Interfaces ... 308
5.7.6 OSPFv2 Configuration ... 313
5.7.7 OSPFv2 Areas ... 315
5.7.8 OSPFv2 Area Ranges ... 319
5.7.9 OSPFv2 Interfaces ... 320
5.7.10 OSPFv2 Virtual Links ... 325
5.7.11 OSPFv2 Neighbors ... 329
5.7.12 OSPFv2 State Database ... 331
5.7.13 VRRP ... 332
5.7.14 VRRP Virtual Routers ... 332
5.7.15 VRRP Associated IP Adresses ... 336
5.7.16 VRRP Statistics ... 338

6 Konfiguration und Diagnose über SNMP ... 341

7 PROFINET IO-Funktionalität ... 345

7.1 Projektieren mit PROFINET IO ... 345
7.2 Einstellungen in HW Konfig ... 352
7.3 Zugriffsmöglichkeiten über PROFINET IO ... 358
7.4 Datensatz 0x802A (PDPortDataReal) ... 367
7.5 MRP-Projektierung ... 371

8 C-PLUG ... 379

9 Firmwareupdate ... 383

9.1 Firmwareupdate bei funktionsfähiger Firmware ... 383
9.1.1 Firmwareupdate über HTTP/HTTPS ... 383
9.1.2 Firmwareupdate über TFTP ... 383
9.1.3 Firmwareupdate über FTP ... 383
9.2 Firmwareupdate über die Boot-Software beim IE-Switch X-400/XR-300 ... 384
9.2.1 Firmwareupdate über die serielle Schnittstelle ... 385
9.2.2 Firmwareupdate über eine Ethernet-Schnittstelle und FTP ... 387
9.3 Firmware-Downgrade ... 387

A Anhang A ... 389

A.1 PC-Anschluss an die serielle Schnittstelle eines SCALANCE X400 ... 389
A.2 PC-Anschluss an die serielle Schnittstelle eines SCALANCE XR300 ... 390

B Anhang B ... 393

B.1 MIB-Variablen eines SCALANCE X300/X400 ... 393

C Anhang C ... 401

C.1 Tagging von Frames ... 401

D Anhang D ... 403

D.1 Fehlermeldungen des SCALANCE X300 / X400 ... 403

E Anhang E 409
E.1 Gleiche Konfiguration auf mehreren IE-Switches verwenden 409
F Verwendete Verschlüsselungsverfahren (Ciphers) 419
Index 421

Empfehlungen zur Netzwerksicherheit

1

ACHTUNG
Informationssicherheit Verbinden Sie sich mit dem Gerät und ändern Sie die Standard-Passwörter für die Benutzer "admin" und "user", bevor Sie das Gerät betreiben. Um Passwörter ändern zu können, müssen Sie mit schreibendem Zugriff auf die Konfigurationsdaten angemeldet sein.

Um unbefugten Zugriff auf das Gerät und/oder Netzwerk zu verhindern, beachten Sie folgende Security-Empfehlungen.

Allgemein

- Prüfen Sie das Gerät regelmäßig, um sicherzustellen, dass diese Empfehlungen und/oder andere interne Sicherheitsrichtlinien eingehalten werden.
- Bewerten Sie die Sicherheit Ihres Standorts und verwenden Sie ein Zellenschutzkonzept mit geeigneten Produkten (https://www.industry.siemens.com/topics/global/de/industrial-security/Seiten/default.aspx).
- Wenn das interne und externe Netzwerk entkoppelt sind, kann ein Angreifer nicht auf interne Daten zugreifen. Betreiben Sie das Gerät daher nur innerhalb eines geschützten Netzwerkbereichs.
- Für den Betrieb von unsicherer Infrastruktur wird keine Produkthaftung übernommen.
- Nutzen Sie VPN, um die Kommunikation von und zu den Geräten zu verschlüsseln und zu authentifizieren.
- Nutzen Sie für die Datenübertragung über ein unsicheres Netzwerk einen verschlüsselten VPN-Tunnel (IPsec, OpenVPN).
- Trennen Sie Verbindungen ordnungsgemäß (WBM, SSH usw.).
- Prüfen Sie die Benutzerdokumentation anderer Siemens-Produkte, die zusammen mit dem Gerät verwendet werden, auf weitere Sicherheitsempfehlungen.
- Sorgen Sie mit Hilfe des Remote-Logging dafür, dass die Systemprotokolle an einen zentralen Logging-Server weitergeleitet werden. Achten Sie darauf, dass der Server sich innerhalb des geschützten Netzwerks befindet, und schauen Sie regelmäßig in den Protokollen nach, ob potenzielle Sicherheitsverletzungen oder Schwachstellen vorliegen.

Physischer Zugang

- Beschränken Sie den physischen Zugang zu dem Gerät auf qualifiziertes Personal, da das steckbare Speichermedium sensible Daten enthalten kann.
- Sperren Sie ungenutzte physische Schnittstellen auf dem Gerät. Ungenutzte Schnittstellen können verwendet werden, um unerlaubt auf die Anlage zuzugreifen.

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.

Authentifizierung

Hinweis

Zugänglichkeitsrisiko - Gefahr des Datenverlusts

Verlieren Sie die Passwörter für das Gerät nicht. Der Zugriff auf das Gerät kann nur durch Zurücksetzen des Geräts auf die Werkseinstellungen wiederhergestellt werden, wodurch sämtliche Konfigurationsdaten entfernt werden.

- Ersetzen Sie die Standardpasswörter für alle Benutzerkonten, Zugriffsmodi und Anwendungen (sofern zutreffend), bevor Sie das Gerät einsetzen.
- Definieren Sie Regeln für die Vergabe von Passwörtern.
- Verwenden Sie Passwörter mit hoher Passwortstärke. Vermeiden Sie schwache Passwörter (wie Passwort1, 123456789, abcdefgh) oder sich wiederholende Zeichen (wie abcabc). Diese Empfehlung gilt auch für auf dem Gerät konfigurierte symmetrische Passwörter/ Schlüssel.
- Stellen Sie sicher, dass Passwörter geschützt werden und nur berechtigtem Personal mitgeteilt werden.
- Verwenden Sie nicht für mehrere Benutzernamen und Systeme die gleichen Passwörter.
- Bewahren Sie Passwörter an einem sicheren Ort (nicht online) auf, damit Sie sie bei Verlust zur Hand haben.
- Ändern Sie regelmäßig Ihre Passwörter, um die Sicherheit zu erhöhen.
- Ein Passwort muss gewechselt werden, wenn es unbefugten Personen bekannt geworden ist oder der Verdacht dazu besteht.

- Wenn die Benutzerauthentifizierung über RADIUS ausgeführt wird, stellen Sie sicher, dass sämtliche Kommunikation innerhalb des Sicherheitsumfelds erfolgt oder durch einen sicheren Kanal geschützt wird.
- Achten Sie auf Link-Layer-Protokolle, die keine eigene Authentifizierung zwischen den Endpunkten bieten, wie ARP oder IPv4. Ein Angreifer könnte Schwachstellen in diesen Protokollen ausnutzen, um mit Ihrem Layer-2-Netzwerk verbundene Hosts, Switches und Router anzugreifen, zum Beispiel durch Manipulation (Poisoning) der ARP-Caches von Systemen im Subnetz und anschließendem Abfangen des Datenverkehrs. Gegen nicht sichere Layer-2-Protokolle sind angemessene Sicherheitsvorkehrungen zu ergreifen, um unbefugten Zugriff auf das Netzwerk zu verhindern. Unter anderem kann der physische Zugriff auf das lokale Netzwerk gesichert oder es können sichere höherschichtige Protokolle verwendet werden.

Zertifikate und Schlüssel

Hinweis

ECDSA-Zertifikate für SCALANCE X300 und SCALANCE X408-2

Für Geräte der Produktlinie SCALANCE X-300 und Geräte des Typs SCALANCE X408-2 gilt Folgendes (Geräte des Typs SCALANCE X414-3E sind nicht betroffen):

Ab Firmware-Version V4.1.4 wurde von RSA-Zertifikaten auf Zertifikate für Elliptische-Kurven-Kryptografie ("ECDSA-Zertifikate") umgestellt. Verwenden Sie nur ECDSA-Zertifikate im PEM-Format, die mit den folgenden Kurven erzeugt wurden:

- secp256r1 (NIST P-256)
- secp384r1 (NIST P-384)
- secp521r1 (NIST P-521)

RSA-Zertifikate werden ab dieser Firmware-Version nicht mehr unterstützt. Die auf dem Gerät vorhandenen RSA-Zertifikate werden automatisch durch selbstsignierte ECDSA-Zertifikate ersetzt.

- Im Gerät ist ein voreingestelltes SSL-Zertifikat mit der Schlüssellänge 256 Bit für die Elliptische-Kurven-Kryptografie 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.
- 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 256 Bit zu verwenden.
- Ändern Sie Zertifikate und Schlüssel umgehend, wenn der Verdacht auf Kompromittierung besteht.

Sichere/Unsichere Protokolle

- Vermeiden oder deaktivieren Sie unsichere Protokolle, wie z. B. 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
  - LLDP
  - DHCP-Optionen 66/67

  Die folgenden Protokolle bieten sichere Alternativen:
  - HTTP → HTTPS
  - TFTP → FTPS
  - Telnet → SSH
  - SNTP → NTP
    Prüfen Sie die Notwendigkeit der Nutzung von NTP. NTP wird als unsicher eingestuft. Aktivieren Sie Secure NTP, wenn der NTP-Server dieses Protokoll unterstützt und nutzen Sie die Authentifizierungs- und Verschlüsselungsmechanismen von Secure NTP.
  - 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 "DCP Read Only"-Modus.

Verfügbare Protokolle

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

Die Tabelle umfasst folgende Spalten:

- **Protokoll**
- **Portnummer**
- **Portzustand**
  - Offen
  - Geschlossen

- **Werkseinstellung**
  Gibt an, in welchem Zustand sich der Port im Auslieferungszustand oder nach dem Zurücksetzen auf Werkseinstellungen befindet.
- **Authentifizierung**
  Gibt an, ob eine Authentifizierung des Kommunikationspartners stattfindet.
- **Verschlüsselung**
  Gibt an, ob die Übertragung verschlüsselt ist.

Protokoll	Portnummer	Portzustand	Werkseinstellung	Authentifizierung	Verschlüsselung [1]
FTP	TCP/21	Offen	Offen	✓	-
SSH Server	TCP/22	Offen	Offen	✓	✓
TELNET	TCP/23	Offen (wenn konfiguriert)	Geschlossen	✓	-
HTTP	TCP/80	Offen (wenn konfiguriert)	Offen	✓	-
PROFINET Service	TCP/84	Offen	Offen	-	-
SSL Server	TCP/443	Offen	Offen	✓	✓
DHCP	UDP/68	Offen (wenn konfiguriert)	Offen	-	-
SNTP	UDP/123	Offen (wenn konfiguriert)	Geschlossen	-	-
NTP (secure)					✓
SNMP	UDP/161	Offen (wenn konfiguriert)	Offen	✓	✓ (SNMPv3)
RADIUS Client	UDP/1812, 1813	Offen	Offen	✓	-
PROFINET	UDP/34964 UDP/49152, 49153 *)	Offen (wenn konfiguriert)	Offen	-	-

[1] Weiterführende Informationen zu verwendeten Verschlüsselungsverfahren finden Sie im Anhang zum WBM "Verwendete Verschlüsselungsverfahren (Ciphers) (Seite 419)".

*) Diese Ports werden dynamisch vergeben und können von den hier angegebenen Werten abweichen.

Außerbetriebnahme

Nehmen Sie das Gerät ordnungsgemäß außer Betrieb, um zu verhindern, dass unbefugte Personen an vertrauliche Daten im Gerätespeicher gelangen.

Setzen Sie das Gerät hierzu auf Werkseinstellungen zurück.

Setzen Sie auch das Speichermedium auf Werkseinstellungen zurück.

Einleitung 2

2.1 Technische Dokumentation für SCALANCE X-300/X-400

Inhalt des Projektierungshandbuchs

Das vorliegende Handbuch beschreibt die Konfiguration von IE-Switches.

Sie müssen IE-Switches konfigurieren, wenn Sie Funktionen wie z.B. SNMP, Rapid Spanning Tree, VLAN, Routing (SCALANCE X414-3E) oder E-Mail nutzen wollen. Außerdem wird auf die Frage des Firmwareupdates und auf den C-PLUG eingegangen.

Voraussetzung für die Konfiguration ist, dass Sie das Gerät bereits montiert und angeschlossen haben. Eine Beschreibung der dafür notwendigen Handlungsschritte finden Sie in der Betriebsanleitung.

Die folgende Tabelle zeigt, welche Informationen Sie in welchem Kapitel finden.

Thema	Kapitel
Sie wollen sich einen Überblick über die Dokumentation eines IE-Switches verschaffen.	Kapitel 1
Sie möchten erfahren, welche Funktionen und Konfigurationsmöglichkeiten ein IE-Switch zur Verfügung stellt.	Kapitel 2
Sie möchten wissen, wie eine IP-Adresse aufgebaut ist und welche Möglichkeiten es gibt, einem IE-Switch eine IP-Adresse zuzuweisen.	Kapitel 3
Sie wollen einen IE-Switch konfigurieren und benötigen Informationen über die entsprechenden CLI-Befehle bzw. welche Seiten im Web Based Management Sie bearbeiten müssen.	Kapitel 4
Sie möchten wissen, wie Sie einen IE-Switch über SNMP verwalten können.	Kapitel 5
Sie möchten wissen, wie die Möglichkeiten von PROFINET IO für einen angeschlossenen IE-Switch genutzt werden können.	Kapitel 6
Sie möchten sich über die Möglichkeiten des Wechselmediums C-PLUG informieren.	Kapitel 7
Sie möchten ein Firmwareupdate durchführen.	Kapitel 8

Inhalt der Betriebsanleitung

Die "Betriebsanleitung Industrial Ethernet Switches SCALANCE X-400" und die "Betriebsanleitung Industrial Ethernet Switches SCALANCE X-300" enthalten neben Grundlageninformationen zum Thema Switches Produktbeschreibungen zu IE-Switches, Medienmodulen und Extendermodulen. Darüber hinaus beschreibt es die Inbetriebnahme von IE-Switches (Montage, Verdrahten, Einsetzen von Modulen usw.).

Übersicht der technischen Dokumentation der IE-Switches X-300 und X-400

Die Technische Dokumentation der Produktlinie X-300 finden Sie, aufgeteilt nach Hardware und Software, in folgenden Dokumenten:

- **PH** - Projektierungshandbuch (PDF)
  Die Software wird im Projektierungshandbuch (PH) für die beiden Produktlinien X-300 und X-400 beschrieben.
- **BAK** - Kompaktbetriebsanleitung in Papierform
  Die Hardware für jede Produktgruppe wird in einer Kompaktbetriebsanleitung (BAK) beschrieben.
- **BA** - Betriebsanleitung (PDF)
  Die Hardware für alle Produktgruppen sowie übergeordnete Informationen finden Sie in der Betriebsanleitung (BA).

Inhalt	Produktgruppe	Dokumentart	Dokument-Identifikations-nummer
Software-Be-schreibung	Alle Geräte der Produktlinien X-300 und X-400	**PH X-300/X-400**	C79000-G89000-C187
Hardware-Be-schreibung	Alle Geräte der Produktlinie X-300	**BA X-300**	A5E01113043
	X-300	**BAK X-300**	A5E00982643
	X-300M	**BAK X-300M**	A5E02630801
	XR-300M	**BAK XR-300M**	A5E02661171
	X-300 EEC	**BAK X-300 EEC**	A5E02630809
	XR-300M EEC	**BAK XR-300M EEC**	A5E02661176
	X-300 PoE	**BAK X-300 PoE**	A5E02630809
	XR-300M PoE	**BAK XR-300M PoE**	A5E02630810
	MM900 (Medienmodule)	**BAK MM900**	A5E02661178
	SFP (Stecktransceiver)	**BAK SFP** **Hinweisblatt**	A5E02630804 A5E02648904
	Alle Geräte der Produktlinie X-400	**BA X-400**	C79000-G8900-C186
	X-400	**BAK X-400**	A5E01020054
	X-400EM (Extendermodule)	**BAK X-400EM**	A5E00367421
	X-400 Medienmodule	**BAK X-400 Medienmodule**	A5E00367420

Netzwerkmanagement für industrielle Netze 3

3.1 Konfigurationsmöglichkeiten eines SCALANCE X-300/X-400

Ethernet-Schnittstelle

Die IE-Switches können über die Switch-Ports (In-Band-Ports) konfiguriert werden, wenn vorher eine IP-Adresse vergeben wurde (siehe Kapitel "Vergabe einer IP-Adresse").

Über die Ethernet-Schnittstelle können Sie folgende Protokolle bzw. Dienste nutzen:

- Web Based Management (HTTP- und HTTPS-basiert)
- TELNET
- SSH
- SNMP
- Traps
- FTP
- TFTP
- E-Mail
- Syslog

Hinweis

Beim SCALANCE X414-3E steht zusätzlich eine Fast-Ethernet-Schnittstelle (Out-Band-Port) auf dem CPU-Modul zur Verfügung.

- SMTP

RS 232-Schnittstelle

Die IE-Switches X-400/XR-300 sind mit einer RS 232-Schnittstelle ausgestattet. Sie können dort einen PC oder ein PG mit einem Nullmodemkabel anschließen und ein Terminalprogramm (z. B. HyperTerminal bei Windows, siehe auch Anhang A) nutzen. Sie verwenden diese Schnittstelle für die manuelle Vergabe einer IP-Adresse für die Out-Band-Port-Schnittstelle (nur SCALANCE X414-3E) oder die In-Band-Port-Schnittstelle (siehe Kapitel "Vergabe einer IP-Adresse über die serielle Schnittstelle"). Außerdem steht der komplette Satz an CLI-Befehlen zur Verfügung.

Hinweis

Der Zugang zum IE-Switches Management über die serielle Schnittstelle bzw. über die Ethernet-Schnittstelle des CPU-Moduls ist auch bei gestörtem Netz möglich (Out of Band Management).

3.2 Funktion und Eigenschaften eines SCALANCE X-300/X-400

Integration vorhandener Teilnetze mit 10 Mbit/s und 100 Mbit/s

Ein IE-Switch erkennt an seinen Twisted Pair-Ports automatisch die folgenden Parameter:

- Sende- und Empfangsleitungspaare (Auto-Crossover)
- Datenrate (10 Mbit/s oder 100 Mbit/s)
- Betriebsart (Voll- oder Halbduplexbetrieb)

Dadurch können Sie mit IE-Switches problemlos Teilnetze über Twisted Pair integrieren.

Hinweis

Auch beim Einsatz nicht gekreuzter Leitungen kann eine unzulässige Schleife im Ethernet Netz z.B. durch Verbindung zweier Ports an einem IE-Switch entstehen. Eine solche Schleife kann zu Netzüberlast und zu Netzausfällen führen.

Hinweis

Wird ein IE-Switch Port an ein Partnergerät angeschlossen, das nicht im Autonegotiation-Modus arbeitet, dann muss der Port fest auf die Parameter des Partners eingestellt werden.

Wenn nicht beide Seiten der Verbindung manuell eingestellt sind, wird der Duplex-Mode nicht erkannt. Es wird der Halbduplex-Mode verwendet, der zu einer schlechten Performance und zu Kollisionen führt.

Ist Autonegotiation ausgeschaltet, dann ist auch Auto-Crossing deaktiviert und es müssen gegebenenfalls gekreuzten Netzwerkleitungen eingesetzt werden.

Gigabit Ethernet-Ports

Diese Ports sind besonders für eine performante Verbindung der Switches untereinander geeignet und verfügen über folgende Eigenschaften:

- Automatische Erkennung der Sende- und Empfangsleitungspaare (Auto-Crossover)
- Datenraten 10 Mbit/s, 100 Mbit/s oder 1000 Mbit/s
- Vollduplexbetrieb

Hinweis

Für die Datenübertragung mit 1 Gbit/s ist mindestens eine Cat 5e Twisted Pair Verkabelung mit 4x2 Adern erforderlich. Bei einer vieradrigen Leitung (2x2 Adern) ist eine maximale Datenübertragungsrate von 100 Mbit/s möglich.

Schnelle Redundanz im Ring

Ab Firmware Version V3.0.0 beherrschen die IE-Switches folgende Redundanzverfahren:

- MRP im Ring mit maximal 200 ms Rekonfigurationszeit
- HRP mit maximal 300 ms Rekonfigurationszeit

Redundante Kopplung von Netzsegmenten

Ringe oder Linien aus IE-Switches (SCALANCE X-200 oder X-300/X-400 oder OSM/ESM) können durch geeignete Verkabelung und entsprechende Projektierung redundant gekoppelt werden. (Siehe auch Kapitel "Menüpunkt X-400 Standby Mask").
Die maximale Umschaltzeit beträgt 300 ms.

Weitere Informationen zur redundanten Kopplung von Netzsegmenten und zu Medienredundanz in Ringtopologien finden Sie in der Betriebsanleitung "Industrial Ethernet Switches SCALANCE X-400" bzw. "Industrial Ethernet Switches SCALANCE X-300".

Store and Forward

Ein IE-Switch berechnet die CRC-Summe eingehender Datenpakete und leitet nur Daten mit einer gültigen Prüfsumme weiter (Store-and-Forward-Verfahren). Fehlerhafte Pakete werden durch den Switch nicht weitergeleitet. Außerdem kann durch Store-and-Forward in einem Netzwerk auf verschiedenen Übertragungsstrecken mit unterschiedlichen Übertragungsgeschwindigkeiten gearbeitet werden.

Unterstützung von Virtuellen Netzen (VLAN portbasiert)

Ein virtuelles Netz (VLAN) unterscheidet sich physikalisch nicht von einem normalen LAN. Das besondere Merkmal eines VLANs ist, dass per Projektierung Geräte einer Gerätegruppe zugeordnet werden können. Mehrere dieser Gerätegruppen nutzen dabei eine physikalisch nur einmal vorhandene Netzwerkinfrastruktur. Auf dem physikalisch nur einmal vorhandenen Netz entstehen damit mehrere "virtuelle" Netze. Datenaustausch, auch die Übertragung von Broadcasts, findet nur innerhalb eines VLAN statt.

Die Zuordnung zu VLANs erfolgt durch Erweiterung der Frames. Nach Ziel- und Quelladresse werden 4 Byte Zusatzinformation eingefügt. Detailinformationen zum sogenannten Tagging von Frames finden Sie im Anhang C.

Um auch Endgeräte und Teilnetze, die keine VLAN unterstützen, in virtuelle Netze einbinden zu können, können Switches das Hinzufügen und auch das Entfernen der VLAN-Zusatzinformation (VLAN-Tags) übernehmen. IE-Switches unterstützen die Zuordnung auf Basis des Ports, über den die Geräte angeschlossen sind (Port based VLAN).

- X-400
  Es können bis zu 62 Port Based VLAN und die beiden vordefinierten VLAN projektiert werden. VLANs entsprechen dem Standard IEEE 802.1Q.
- X-300
  Es können bis zu 253 Port Based VLAN und die beiden vordefinierten VLAN projektiert werden. VLANs entsprechen dem Standard IEEE 802.1Q.

Spanning Tree

Das Spanning Tree-Verfahren (STP) ermöglicht es, Netzwerkstrukturen aufzubauen, bei denen es mehrere Verbindungen zwischen zwei Stationen gibt. Spanning Tree lässt genau einen Pfad zu und deaktiviert die anderen (redundanten) Ports für den Datenverkehr. Dadurch wird verhindert, dass es zu einer Schleifenbildung im Netz kommt. Bei einer Unterbrechung wird ein alternativer Pfad ermittelt, über den die Daten gesendet werden.

Spanning Tree ist im Standard IEEE 802.1D-1998 definiert.

Rapid Spanning Tree

Das Rapid Spanning Tree Protocol (RSTP) ist eine Erweiterung des Spanning Tree Protocols (STP). RSTP entscheidet sich vom STP im Wesentlichen dadurch, dass die Geräte bereits zum Zeitpunkt des ungestörten Betriebs Informationen über Alternativrouten sammeln. Wenn eine Störung eintritt, stehen diese Informationen sofort zur Verfügung. Damit lässt sich die Rekonfigurationszeit für ein RSTP-gesteuertes Netz auf wenige Sekunden reduzieren. IE-Switches unterstützen sowohl Rapid Spanning Tree als auch Spanning Tree.

Rapid Spanning Tree ist im Standard IEEE 802.1D-2004 definiert.

Multiple Spanning Tree

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

Multiple Spanning Tree ist im Standard IEEE 802.1Q definiert.

C-PLUG

Der C-PLUG ist ein Wechselmedium, auf dem alle Konfigurationsinformationen eines IE-Switches gespeichert sind. Beim Austausch eines IE-Switches braucht lediglich der C-PLUG des bisherigen Geräts in das neue Gerät gesteckt zu werden. Der Hochlauf des neuen IE-Switch erfolgt dann mit der Konfiguration des bisherigen Geräts.

MAC-Adresstabelle

In der MAC-Adresstabelle eines IE-Switches ist die Information hinterlegt, an welche(n) Port(s) ein empfangener Frame weitergeleitet werden soll. Diese Tabelle kann sowohl statische Einträge (vom Benutzer hinzugefügt) als auch dynamische Einträge (durch empfangene Frames von einem IE-Switches gelernt) enthalten.

Access Control

Hinweis

Diese Eigenschaft heißt in Firmwareständen vor 2.2.0 "Locked Ports".

Wenn diese Funktion für einen Port aktiviert ist, leitet ein IE-Switch an diesem Port empfangene Frames nur weiter, wenn deren Quelladresse in der Adresstabelle vorhanden ist.

Es ist möglich automatisch alle angeschlossenen Teilnehmer in die Access Control List eintragen zu lassen.

Hinweis

Die Ringports können nicht auf Access-Control *enabled* konfiguriert 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.

Mirroring

Mirroring ermöglicht es, den Datenverkehr eines Ports auf einen anderen Port abzubilden. An diesem sogenannten Monitor Port kann dann rückwirkungsfrei der Datenverkehr analysiert werden.

E-Mail-Funktion

IE-Switch können so konfiguriert werden, dass sie beim Auftreten bestimmter Ereignisse eine E-Mail versenden.

Event Log Tabelle

In die Event Log Tabelle werden Ereignisse, die während des Betriebs eines IE-Switches auftreten, protokolliert. Der Benutzer kann festlegen, welche Ereignisse zu einem Tabelleneintrag führen.

Uhrzeitsynchronisation

IE-Switches bieten die Möglichkeit, die Systemzeit mit externen Zeitgebern zu synchronisieren. Dazu muss beispielsweise ein SICLOCK-Uhrzeitsender, ein SNTP-Server oder ein NTP-Server verfügbar sein, dessen Frames der IE-Switch auswertet. Einträge in der Event Log Tabelle werden dann mit einem anlagenweit einheitlichen Zeitstempel versehen. Damit können Ereignisse anlagenweit zeitlich sortiert werden, was erheblich zur schnelleren Ermittlung von Störungsursachen beiträgt.

Flusskontrolle

IE-Switches unterstützen Flusskontrolle im Halbduplex- und Vollduplexbetrieb.

BOOTP/DHCP

IE-Switches können Ihre IP-Adresse dynamisch von einem BOOTP- oder DHCP-Server beziehen.

Ab Firmwarestand Version 2.0 kann bei aktiviertem DHCP die DHCP-Betriebsart ausgewählt werden. In den vorherigen FW-Ständen wird DHCP via Mac Address betrieben.

Hinweis

Wenn die Routing-Funktionen (nur bei SCALANCE X414-3E) aktiv sind, sind DHCP und BOOTP nicht wirksam.

Hinweis

DHCP und BOOTP sind nur wirksam hinsichtlich der In-Band-Agent IP-Konfiguration. Die Out-Band-Agent IP-Konfiguration des SCALANCE X414-3E kann nur manuell eingestellt werden.

Über die DHCP-Option 66 bzw. 67 kann auch eine Konfigurationsdatei geladen werden.

PROFINET IO

Ab Firmwarestand Version 2.0 wird der Betrieb des Switches als PROFINET IO Device unterstützt.

TELNET

Das Command Line Interface von IE-Switches kann mit TELNET über ein LAN bzw. das Internet bedient werden.

Hinweis

Es sind maximal drei CLI-Verbindungen (seriell (nur bei IE-Switches X-400) und LAN) gleichzeitig möglich.

Ab Firmware-Version 4.1.3 ist TELNET im Auslieferungszustand oder nach dem Zurücksetzen des Geräts auf Werkseinstellungen deaktiviert. Aus Sicherheitsgründen wird die Verwendung von SSH empfohlen.

SSH

Das Command Line Interface von IE-Switches kann mit SSH über ein LAN bzw. das Internet bedient werden.

Hinweis

Es sind maximal drei CLI-Verbindungen (seriell (nur bei IE-Switches X-400) und LAN) gleichzeitig möglich.

SNMPv3

IE-Switches unterstützen SNMPv1, SNMPv2c und SNMPv3. SNMPv3 bietet unter anderem eine Benutzerverwaltung auf Protokollebene sowie Sicherheitsfunktionen (z. B. Authentifizierung). Die Konfiguration von Benutzern und Gruppen für SNMPv3 ist über das Web Based Management, über das Command Line Interface oder durch direkten Zugriff auf die MIB-Objekte (nur für Experten empfehlenswert) möglich.

Syslog

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

DHCP Option 82

Die DHCP Relay Funktion bietet die Möglichkeit, die IP-Adresstaufe eines Endgerätes abhängig vom angeschlossenen Switch Port zu vergeben. Über diese Funktion wird DHCP Option 82 unterstützt.

IGMP Snooping und IGMP Querier

IE-Switches unterstützen neben IGMP Snooping auch die IGMP Querier Funktion. Ist IGMP Snooping aktiviert, so werden IGMP-Pakete ausgewertet und mit diesen Informationen die Multicast-Filtertabelle aktualisiert. Ist zusätzlich IGMP Query aktiviert, so versenden IE-Switches auch IGMP-Anfragen, die bei IGMP-fähigen Teilnehmern Antworten auslösen.

Nur bei SCALANCE X414-3E: Layer-3-Funktionalität (Routing)

Den SCALANCE X414-3E können Sie auch als Router konfigurieren. Damit ist es möglich, verschiedene IP-Subnetze miteinander zu verbinden. Sie können statische Routen eintragen und/oder Router-Protokolle RIP/OSPF und VRRP aktivieren. Über diese standardisierten Protokolle kann SCALANCE X414-3E mit anderen Routern im Netz die Konfiguration abgleichen.

3.3 Möglichkeiten der Medienredundanz

Zur Erhöhung der Netzverfügbarkeit eines Industrial Ethernet-Netzwerks mit optischen oder elektrischen Linientopologien stehen verschiedene Möglichkeiten zur Verfügung:

- Vermaschung von Netzwerken
- Parallelschaltung von Übertragungswegen
- Zusammenschluss einer Linientopologie zu einer Ringtopologie

3.3.1 Medienredundanz in Ringtopologien

Aufbau einer Ringtopologie

Teilnehmer von Ringtopologien können externe Switches und/oder die integrierten Switches von Kommunikationsbaugruppen sein.

Zum Aufbau einer Ringtopologie mit Medienredundanz müssen Sie die beiden freien Enden einer linienförmigen Netztopologie in einem Gerät zusammenführen. Der Zusammenschluss der Linientopologie zu einem Ring erfolgt über zwei Ports (Ringports) eines Geräts im Ring. Dieses Gerät ist der Redundanzmanager. Alle anderen Geräte im Ring sind Redundanz-Clients.

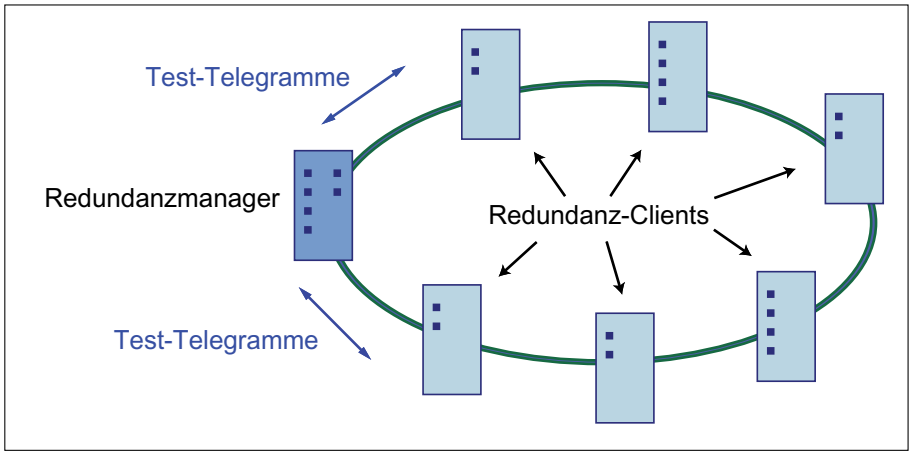


Bild 3-1 Geräte in einer Ringtopologie mit Medienredundanz

Die zwei Ringports eines Geräts sind die Ports, die in einer Ringtopologie die Verbindung zu den beiden Nachbargeräten herstellen. Die Auswahl und Festlegung der Ringports erfolgt in der Projektierung des jeweiligen Geräts. In STEP 7 sowie auf den S7-Ethernet-CP-Baugruppen selbst sind die Ringports hinter der Port-Nummer mit "R" gekennzeichnet.

Hinweis

Laden Sie vor dem physischen Zusammenschluss des Rings die Projektierung Ihres STEP 7-Projekts in die einzelnen Geräte.

Funktion der Medienredundanz in einer Ringtopologie

Unter Verwendung von Medienredundanz werden die Datenwege zwischen den einzelnen Geräten rekonfiguriert, wenn der Ring an einer Stelle unterbrochen wird. Nach der Rekonfiguration der Topologie sind die Geräte in der neu entstandenen Topologie wieder erreichbar.

Im Redundanzmanager werden die 2 Ringports bei unterbrechungsfreiem Netzwerkbetrieb voneinander getrennt, damit keine Datenframes kreisen. Die Ringtopologie wird aus Sicht der Datenübertragung zu einer Linie. Der Redundanzmanager überwacht die Ringtopologie. Hierzu schickt er Test-Frames sowohl von Ringport 1 als auch von Ringport 2. Die Test-Frames durchlaufen den Ring in beiden Richtungen, bis sie am jeweils anderen Ringport des Redundanzmanagers ankommen.

Eine Unterbrechung des Rings kann durch Ausfall der Verbindung zwischen zwei Geräten oder durch Ausfall eines Geräts im Ring erfolgen.

Wenn die Test-Frames des Redundanzmanagers bei einer Unterbrechung des Rings nicht mehr zum anderen Ringport durchgeleitet werden, schaltet der Redundanzmanager seine beiden Ringports durch. Über diesen Ersatzweg wird wieder eine funktionierende Verbindung zwischen allen verbleibenden Geräten in Form einer linienförmigen Netztopologie hergestellt.

Sobald die Unterbrechung beseitigt ist, werden die ursprünglichen Übertragungswege wiederhergestellt, die beiden Ringports im Redundanzmanager voneinander getrennt und die Redundanz-Clients über den Wechsel informiert. Die Redundanz-Clients benutzen dann die neuen Wege zu den anderen Geräten.

Die Zeit zwischen Ringunterbrechung und Wiederherstellung einer funktionsfähigen Linientopologie wird Rekonfigurationszeit genannt.

Wenn der Redundanzmanager ausfällt, dann wird der Ring zu einer funktionsfähigen Linie.

Medienredundanzverfahren

Folgende Medienredundanzverfahren für Ringtopologien werden von SIMATIC NET Produkten unterstützt:

- HRP (High Speed Redundancy Protocol)
  Rekonfigurationszeit: 0,3 Sekunden
- MRP (Media Redundancy Protocol)
  Rekonfigurationszeit: 0,2 Sekunden

Die Mechanismen der Verfahren sind ähnlich. HRP und MRP können in einem Ring nicht gleichzeitig eingesetzt werden.

3.3.2 MRP

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

IEC 62439-2:2016 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.

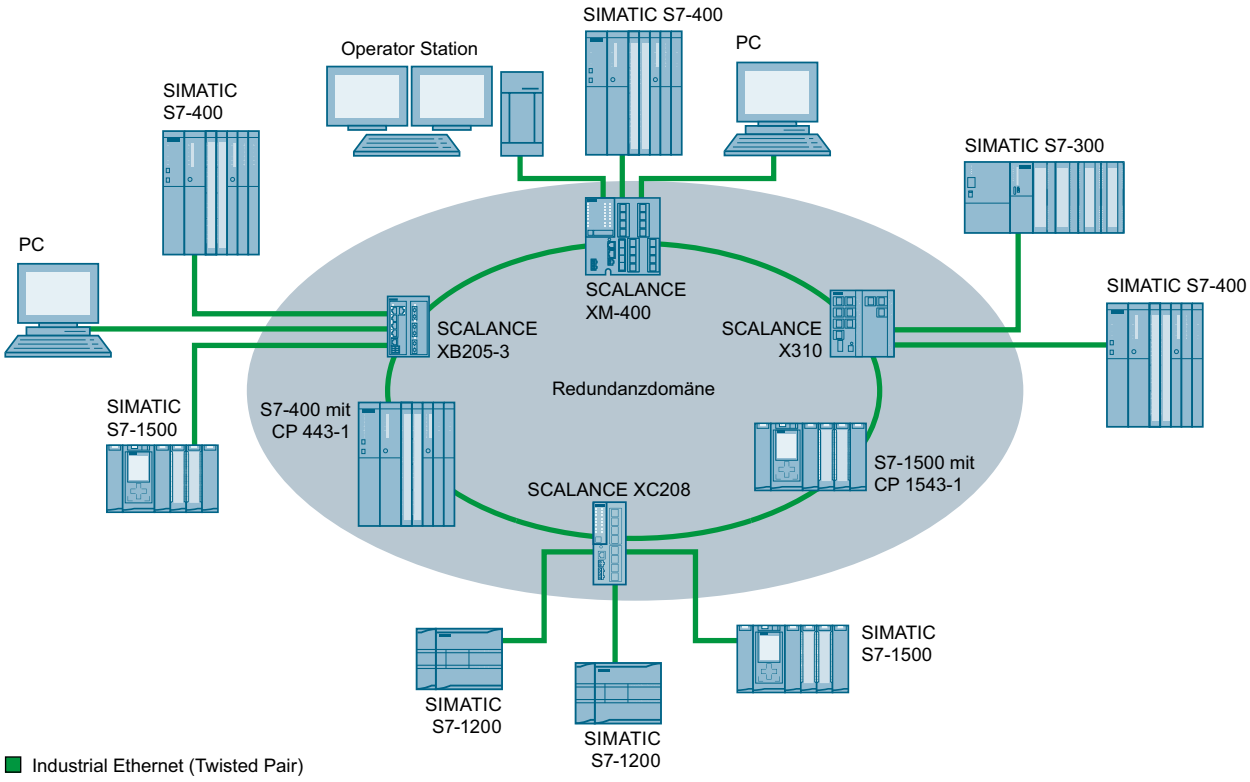


Bild 3-2 Beispiel einer Ringtopologie mit dem Medienredundanzverfahren MRP

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.

Siehe auch

X-300/X-400 Ring Configuration (Seite 81)

Hinweis

Geräteanzahl

Außer in PROFINET IO-Anlagen, wurden Topologien mit bis zu 100 IE-Switches SCALANCE X-200 und SCALANCE X-300 erfolgreich getestet.

Projektierung

Sie können einfache MRP-Ringe wie folgt projektieren:

- über das Web Based Management, siehe Kapitel "Ring Redundancy (Seite 77)"
- über STEP 7, siehe Kapitel "MRP-Projektierung (Seite 371)"

Geräte mit Unterstützung von MRP

Eine Ringtopologie, in der Sie MRP einsetzen wollen, darf nur aus Geräten bestehen, die diese Funktion unterstützen. Dies sind beispielsweise folgende Geräte:

- Industrial Ethernet Switches
  - SCALANCE X-200 ab Firmware-Version V4.0
  - SCALANCE X-200IRT ab Firmware-Version V4.0
  - SCALANCE X-300 ab Firmware-Version V3.0
  - SCALANCE X-400 ab Firmware-Version V3.0
- Kommunikationsprozessoren
  - CP 443-1 Advanced (6GK7 443-1GX20-0XE0) ab Firmware-Version V2.0
  - CP 343-1 Advanced (6GK7 343-1GX30-0XE0) ab Firmware-Version V1.0
  - CP 1616 (6GK1 161-6AA00) ab Firmware-Version V2.2
  - CP 1604 (6GK1 160-4AA00) ab Firmware-Version V2.2
- Nicht-Siemens-Geräte, die MRP unterstützen

Anschluss von Modularen Switches SCALANCE X-300

Hinweis

SCALANCE X-300 - Modulare Geräte (M)

Achten Sie darauf, dass sich bei den Modularen Switches die Ringports auf den Medienmodulen MM900 befinden.

3.3.3 MRP-Mehrfachringe

Topologie

Mit der Funktion MRP-Mehrfachringe ist es möglich, bis zu 4 MRP-Ringe mit einem zentralen Redundanzmanager zu steuern.

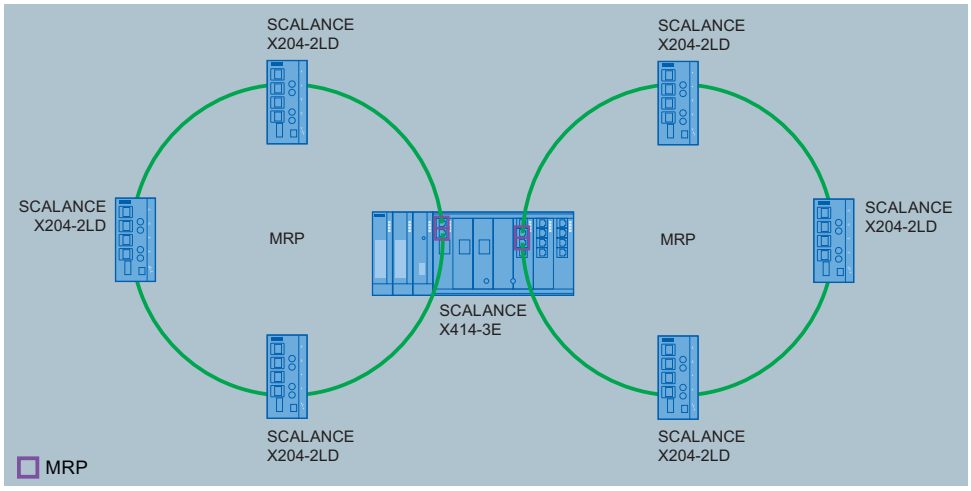


Bild 3-3 MRP-Mehrfachringe

Projektierung

MRP-Mehrfachringe können Sie nur über PROFINET projektieren, siehe Kapitel "MRP-Projektierung (Seite 371)".

Redundanzmanager bei MRP-Mehrfachringen

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
  - SCALANCE X414-3E ab Firmware-Version V3.10

3.3.4 HRP

Hinweis

Namensänderung

Die Abkürzung des Medienredundanzverfahrens "High Speed Redundancy Protocol" wurde von HSR in HRP geändert.

Es handelt sich hierbei nur um eine Namensänderung, die Funktion wurde nicht geändert. HSR- und HRP-Teilnehmer können gemeinsam in einem Ring betrieben werden.

Das Medienredundanzverfahren "HRP" bietet nach Ringunterbrechung eine Rekonfigurationszeit von 0,3 Sekunden.

Voraussetzungen

Folgende Bedingungen sind Voraussetzungen für den störungsfreien Betrieb mit HRP:

- HRP wird in Ringtopologien mit bis zu 50 Geräten unterstützt.
  In Topologien mit IE-Switches SCALANCE X-200 und SCALANCE X-300 werden bis zu 100 Teilnehmer unterstützt.
  Eine Überschreitung der Geräteanzahl kann zum Ausfall des Datenverkehrs führen.
- Der Ring, in dem Sie HRP einsetzen wollen, darf nur aus Geräten bestehen, die diese Funktion unterstützen. Dies sind beispielsweise folgende Geräte: IE Switches X-400, IE Switches X-300, IE Switches X-200 sowie OSM / ESM.
- Alle Geräte müssen über ihre Ringports miteinander verbunden sein.
  Dabei sind Multimodeverbindung bis 3 km und Singlemodeverbindung bis 26 km zwischen zwei IE-Switches möglich. Bei größeren Entfernungen kann es zu einer Verlängerung der angegeben Rekonfigurationszeit kommen.
- Ein Gerät im Ring muss durch Auswahl der Einstellung "HRP Manager" als Redundanzmanager konfiguriert werden. Dies kann per Taster an der Gerätefront, per Web Based Management, CLI oder SNMP durchgeführt werden.
- Bei allen übrigen Geräten im Ring muss entweder die Betriebsart "HRP Client" oder die Betriebsart "Automatic Redundancy Detection" aktiviert werden.
  Dies kann über Web Based Management, CLI oder SNMP geschehen.
- Im Grundzustand sind die Betriebsarten "HRP Client" oder "Automatic Redundancy Detection" voreingestellt.

Vergabe einer IP-Adresse

4

Einleitung

IE-Switches bieten umfangreiche Funktionen zur Einstellung und Diagnose. Für den Zugriff auf diese Funktionen über das Netz wird das Internet-Protokoll eingesetzt.

Das Internet-Protokoll besitzt einen eigenen Adressmechanismus mit sogenannten IP-Adressen. Als Protokoll der Schicht 3 des ISO/OSI-Referenzmodells ist das IP-Protokoll hardwareunabhängig, was eine flexible Adressvergabe ermöglicht. Anders als bei der Ebene 2-Kommunikation mit einer fest einem Gerät zugeordneten MAC-Adresse ergibt sich daraus die Notwendigkeit, einem Gerät explizit eine Adresse zuzuweisen.

Dieses Kapitel beschreibt den Aufbau einer IP-Adresse und die verschiedenen Möglichkeiten der Adressvergabe bei einem IE-Switch.

IP-Adressarten bei IE-Switches

IE-Switches können mehrere IP-Adressen besitzen:

- Out-Band-IP-Adresse (nur bei SCALANCE X414-3E), wird zum Administrieren verwendet.
- In-Band-Agent-IP-Adresse, wird zum Administrieren verwendet.
- Weitere IP-Adressen
  Diese IP-Adressen können nur für Routing-Zwecke (nur bei SCALANCE X414-3E) eingestellt werden. Sie können nicht über DHCP konfiguriert werden, sondern müssen über WBM, CLI oder SNMP vergeben werden.

4.1 Aufbau einer IP-Adresse

Adressklassen nach RFC 1518 und RFC 1519

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
Multicast-Gruppen			D	
Reserviert für Experimente			E	

Eine IP-Adresse besteht aus 4 Bytes. 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.

Subnetz-Maske

Die Bits der Endteilnehmer-Adresse können für die Bildung von Subnetzen verwendet werden. Dabei stellen die führenden Bits die Adresse des Subnetzwerks 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, wird 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 Subnetz-Maske müssen die "Einsen" linksbündig gesetzt sein (es dürfen keine "Nullen" zwischen den "Einsen" stehen).

4.2 Erstmalige Vergabe einer IP-Adresse

Konfigurationsmöglichkeiten

Die erstmalige Vergabe einer IP-Adresse für einen IE-Switch kann nicht mit dem Web Based Management oder dem Command Line Interface über TELNET bzw. SSH erfolgen, weil diese Konfigurations-Werkzeuge bereits eine IP-Adresse voraussetzen.

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

- CLI über die serielle Schnittstelle (nur IE-Switches X-400)
- DHCP (nur über In-Band-Port)
- BOOTP (nur über In-Band-Port)

- STEP 7 (nur über In-Band-Port)
- NCM PC
- SINEC PNI (nur über In-Band-Port)

Hinweis

DHCP ist im Auslieferungszustand und nach *Reset to Factory Defaults* per Default eingeschaltet. Wenn ein DHCP Server im lokalen Netz verfügbar ist und dieser auf den DHCP Request des IE-Switch antwortet, so werden schon beim ersten Hochlauf automatisch IP-Adresse, Subnetzmaske und Gateway zugeteilt. DHCP und BOOTP werden ebenso wie fest eingestellte IP-Adressen durch einen *Reset to Memory Defaults* nicht gelöscht.

Hinweis

Beim SCALANCE X414-3E müssen die IP-Adressen des Out-Band-Ports und der In-Band-Ports verschiedenen Subnetzen angehören.

Beispiel:

IP-Adresse (Out-Band-Port): 140.90.45.66

IP-Adresse (In-Band-Port): 140.91.23.66

Subnetz-Maske

(Out-Band-Port/In-Band-Port): 255.255.0.0

Mit der Routing-Funktion kann der SCALANCE X414-3E mehrere In-Band Adressen besitzen. Über SINEC PNI kann nur eine In-Band Adresse (die Agent IP-Adresse) vergeben werden. Die weiteren Adressen müssen über WBM, CLI oder SNMP vergeben werden.

Hinweis

Die Routing-Funktion ist nur beim SCALANCE X414-3E verfügbar.

Hinweis

Ist die Routing-Funktionalität eingeschaltet, kann über DHCP/BOOTP keine Adresse eingestellt werden.

4.3 Vergabe einer IP-Adresse über die serielle Schnittstelle der SCALANCE X-400

Anschluss über Nullmodemkabel und Login

Führen Sie folgende Schritte durch, um die IP-Adresse eines IE-Switches X-400 über die serielle Schnittstelle festzulegen:

1. Verbinden Sie die serielle Schnittstelle des IE-Switches X-400 über ein Nullmodemkabel mit einem PC.
2. Starten Sie ein Programm zur Terminalemulation, beispielsweise das unter Windows verfügbare Programm HyperTerminal (Einstellungen siehe Anhang A).
3. Nach dem Verbindungsaufbau erscheint die Meldung "Login": Geben Sie entsprechend Ihrem Zugriffsrecht "admin" (für Administrator) ein und drücken Sie die Return-Taste.
4. Geben Sie bei der Meldung "Password:" Ihr Passwort ein. Beachten Sie auch die nachfolgenden Hinweise.
5. Geben Sie "AGENT" ein, wenn die Meldung CLI> erscheint, um in das entsprechende Untermenü zu wechseln. Anschließend können Sie die Befehle zur Konfiguration der IP-Adresse eingeben. Eine Beschreibung dieser Befehle finden Sie im nächsten Abschnitt.

Hinweis

Wenn keine neuen Passwörter vergeben wurden (Werkseinstellung), ist das gültige Passwort "admin" für das Administrator-Login und "user" für das Benutzer-Login mit eingeschränkten Rechten.

Nach einem erfolgreichen Login können über die serielle Schnittstelle solange Kommandos eingegeben werden, bis Sie sich mit dem Befehl "exit" ausloggen. Nach 5 Minuten ohne weitere Aktivität wird die Sitzung automatisch beendet.

Hinweis

Bei Verlust des Passwortes können Sie einen IE-Switch X-300/X-400 über den Taster SET/SEL des CPU-Moduls auf Werkseinstellung zurücksetzen. Drücken Sie hierzu den Taster SET/SEL im Grundzustand Display Mode A (die LEDs D1 und D2 sind aus) für 12 Sekunden. Den Vorgang des Rücksetzens können Sie durch Loslassen des Tasters vor Ablauf der 12 Sekunden abbrechen. Alle Einstellungen, die Sie vorher gemacht haben, werden durch die werksseitige Voreinstellung überschrieben. Die Passwörter "admin" bzw. "user" sind dann wieder gültig.

Befehle für das Command Line Interface

Die Befehle, die das CLI in Untermenü AGENT für die Konfiguration der IP-Adresse zur Verfügung stellt, sind im Kapitel "Menüpunkt Agent Configuration" beschrieben.

Allgemeine Informationen zum Command Line Interface finden Sie im Kapitel "Command Line Interface (CLI)".

4.4 Adressvergabe mit dem BOOTP-Client

Ablauf der Adressvergabe

BOOTP (Bootstrap Protocol) ist ein Protokoll zur automatischen Vergabe von IP-Adressen. Voraussetzung für diese Art der Adressvergabe ist, dass ein BOOTP-Server im Netz vorhanden ist.

Ein Teilnehmer ohne IP-Adresse (BOOTP-Client) sendet seine MAC-Adresse mit einer BOOTP-Anfrage an alle Geräte (MAC-Broadcastadresse FF-FF-FF-FF-FF-FF) im Netz. Die Antwort des Servers wird ebenfalls als Broadcast versendet und enthält neben der IP-Adresse auch die MAC-Adresse des Clients. Ein Client, der eine solche Antwort erhält, kann anhand der MAC-Adresse feststellen, ob die zugehörige IP-Adresse für ihn bestimmt ist.

BOOTP setzt auf dem UDP-Protokoll auf, es benutzt den UDP-Port 67 für den BOOTP-Server und den Port 68 für den Client.

BOOTP beim IE-Switch

Im Auslieferungszustand ist DCP (und damit der Zugang über SINEC PNI bzw. NCM) sowie DHCP aktiviert, BOOTP ist deaktiviert.

4.5 Adressvergabe mit dem DHCP-Client

Eigenschaften von DHCP

DHCP (Dynamic Host Configuration Protocol) ist eine Erweiterung von BOOTP, allerdings gibt es die folgenden wichtigen Unterschiede zu BOOTP:

- Die Verwendung von DHCP ist nicht auf die Phase des Hochlaufs beschränkt, DHCP kann auch im laufenden Betrieb eingesetzt werden.
- Die vergebene IP-Adresse bleibt nur für einen bestimmten Zeitraum, die sogenannte Lease Time, gültig. Nach Ablauf dieser Zeitdauer muss der Client entweder eine neue IP-Adresse anfordern oder die Gültigkeitsdauer der vorhandenen IP-Adresse verlängern.
- Es erfolgt normalerweise 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 gibt aber die Möglichkeit, den DHCP-Server so zu konfigurieren, dass er eine feste Adresszuordnung vornimmt.

Hinweis

Sobald die IP-Adresse einmal von einem PROFINET IO-Controller vergeben wurde, schaltet sich DHCP automatisch ab und muss bei Bedarf wieder aktiviert werden.

Hinweis

DHCP sieht einen Mechanismus vor, nach dem die IP-Adresse nur für eine begrenzte Zeitdauer (Lease Time) zugeteilt wird. Wenn nach Ablauf der LeaseTime der IE-Switch den DHCP Server nicht für einen erneuten Request erreicht, werden die zugewiesene IP-Adresse, die Subnetz-Maske und das Gateway in statische Einträge überführt.

Das Gerät ist folglich auch ohne DHCP Server weiterhin unter der zuletzt vergebenen IP-Adresse erreichbar. Dies entspricht nicht dem Standard-Verhalten von Office Geräten, ist jedoch für einen reibungslosen Anlagenbetrieb notwendig.

Da der DHCP-Client aber zusätzlich ein RELEASE an den Server absetzt, kann der Server diese Adresse an ein weiteres Gerät vergeben, wodurch es zu Inkonsistenzen im Netz kommen kann.

Abhilfe:

Nach dem Abschalten von DHCP sollten Sie deshalb entweder

- die IP-Adresse des IE-Switch auf eine nicht von DHCP vergebene Adresse ändern oder
- die dem Gerät zugeordnete IP-Adresse aus dem Adressband des DHCP-Servers entfernen.

Ein Mischbetrieb von dynamischer Adressvergabe und statisch vergebenen Adressen ist grundsätzlich nicht empfehlenswert.

4.6 Adressvergabe mit SINEC PNI

Einleitung

SINEC PNI (SINEC Primary Network Initialization) nutzt für die Erstinbetriebnahme von Netzwerkgeräten das Protokoll DCP, um Geräte in einem Netzwerk zu erkennen und um eine IP-Adresse zuzuweisen.

Voraussetzung

Voraussetzung ist, dass die Geräte über Ethernet erreichbar sind.

Hinweis

Weitere Informationen zur Benutzung finden Sie in der Dokumentation von SINEC PNI.

Für weitere Informationen siehe PNI (https://support.industry.siemens.com/cs/de/de/ps/26672)

Konfiguration über Web Based Management und Command Line Interface

5

Einleitung

Um die technischen Möglichkeiten der IE-Switches optimal zu nutzen, können Sie die Konfiguration des Geräts an die konkreten Einsatzbedingungen anpassen. Es gibt zwei Möglichkeiten, einen IE-Switch zu konfigurieren:

- Mit dem Command Line Interface können Sie die IE-Switches über Telnet bzw. SSH (Voraussetzung ist eine Ethernet-Verbindung) oder über die serielle Schnittstelle (nur IE-Switches X-400) erreichen.
- Das Web Based Management greift über einen Web-Browser auf die Konfiguration der IE-Switches zu. Voraussetzung ist eine Ethernet-Verbindung zum IE-Switch.

Hinweis

Abhängig vom gewählten Konfigurationsweg sind folgende Mechanismen eingebaut, um einen unberechtigten Zugriff auf einen IE-Switch zu verhindern:

- CLI über serielle Schnittstelle (nur IE-Switches X-400), TELNET bzw. SSH
- Web Based Management

Es erfolgt ein automatischer Logout nach 5 Minuten (CLI) bzw. 15 Minuten (WBM) oder je nach der im Menü Agent Timeout Configuration konfigurierten Zeit. Ein Logout kann auch manuell über eine entsprechende Schaltfläche auf der Oberfläche durchgeführt werden. Das Schließen des verwendeten Browsers beendet die Sitzung nicht. Wird innerhalb des Timeouts der Browser erneut geöffnet, wird die Sitzung weiter genutzt.

Hinweis

Alle Konfigurationsänderungen werden erst nach ca. 1 Minute oder vor einem Warmstart in den Flash-Speicher übernommen. Führen Sie deshalb den Befehl "Restart" im Command Line Interface oder Web Based Management aus, bevor Sie das Gerät stromlos schalten. Dann ist sichergestellt, dass alle Konfigurationsänderungen gespeichert werden.

Hinweis

Zur Nutzung von SNMP Management, RMON und Traps ist eine Netzwerkmanagement-Station erforderlich. Diese ist nicht im Lieferumfang eines IE-Switch enthalten.

5.1 Allgemeine Informationen über Web Based Management und Command Line Interface

5.1.1 Einleitung

Hinweis

Die in diesem Kapitel beschriebenen Masken gelten sowohl für den SCALANCE X-300 als auch für den SCALANCE X-400. Beispielhaft sind hier für die Darstellungen Masken des SCALANCE X-400 gewählt. Je nach Ausstattung und Gerät sind Abweichungen möglich.

Prinzip des Web Based Managements

IE-Switches verfügen über einen integrierten HTTP-Server für das Web Based Management. Wird ein IE-Switch über einen Web-Browser angesprochen, liefert er abhängig von den Benutzereingaben HTML-Seiten an den Client-Rechner zurück.

Der Benutzer trägt seine Konfigurationsdaten in die vom IE-Switch gesendeten HTML-Seiten ein. Ein IE-Switch wertet diese Informationen aus und erzeugt dynamisch Antwortseiten. Der besondere Vorteil dieses Funktionsprinzips ist, dass auf der Client-Seite außer einem Web-Browser keine besondere Software erforderlich ist.

Voraussetzungen für Web Based Management

- Ein IE-Switch muss über eine IP-Adresse verfügen, damit Sie das Web Based Management einsetzen können.
- Um das Web Based Management nutzen zu können, muss eine Ethernet-Verbindung zwischen dem IE-Switch und dem Clientcomputer bestehen.
- Es wird empfohlen, einen Microsoft Internet Explorer ab Version 5.5 zu verwenden.
- Alle Seiten des Web Based Managements erfordern JavaScript. Achten Sie deshalb bei den Browser-Einstellungen darauf, dass JavaScript aktiviert ist.

Hinweis

Der 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 *Temporäre Internetdateien* über die Schaltfläche Einstellungen.

Unter dem Text *Neuere Versionen der gespeicherten Seite* suchen muss dort *Automatisch* markiert sein.

- Da das Web Based Management HTTP- bzw. HTTPS-basiert ist, müssen Sie bei installierter Firewall den Zugriff auf Port 80 bzw. 443 ermöglichen.

Starten des Web Based Managements und Anmeldung

Hinweis

Ändern Sie aus Sicherheitsgründen unbedingt die Passwörter des Auslieferungszustands:

- Benutzername "admin" = Passwort "admin"
- Benutzername "user" = Passwort "user".

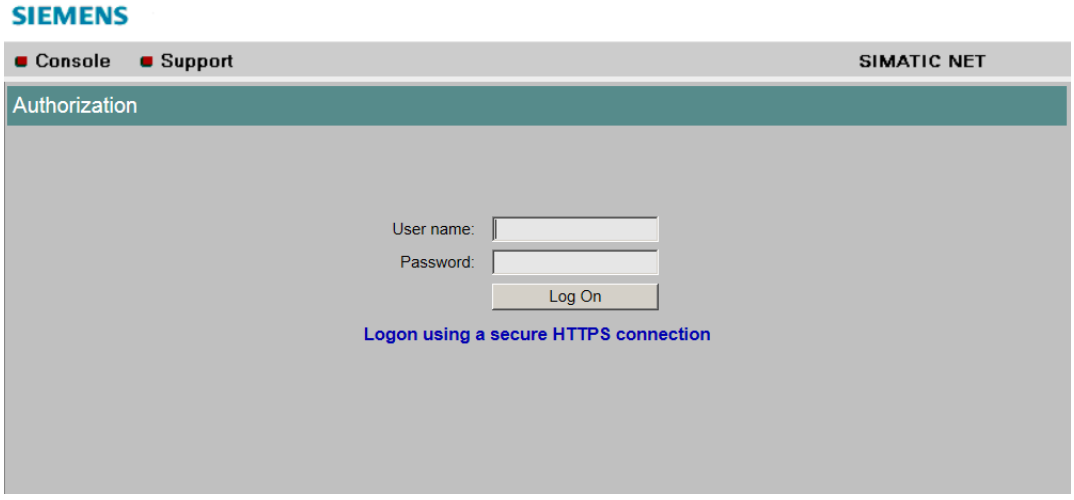


Bild 5-1 Log on-Maske

1. Geben Sie im Adressfeld des Web-Browsers die IP-Adresse oder die URL des IE-Switch ein. Wenn eine einwandfreie Verbindung zum IE-Switch besteht, erscheint die oben abgebildete Logon-Maske des Web Based Managements.
2. Geben Sie im Eingabefeld "User name" einen Benutzernamen ein.
   Folgende Eingaben sind möglich:
   - admin: Mit diesem Benutzernamen haben Sie Lese- und Schreibzugriff.
   - user: Mit diesem Benutzernamen haben Sie nur Lesezugriff.
   - Der auf einem Radius-Server hinterlegte Benutzername: Siehe Kapitel System Passwords & Login Mode (Seite 64) und Kapitel 802.1x RADIUS Configuration (Seite 170).
3. Geben Sie Ihr Passwort ein.
4. Klicken Sie die Schaltfläche "Log On", um die Anmeldung zu starten.

5.1.2 Die Leuchtdiodensimulation des Web Based Managements (WBM)

Darstellung des Betriebszustands

Jede Komponente der IE-Switches verfügt über mehrere Leuchtdioden, die Informationen über den Betriebszustand des Geräts liefern. Abhängig vom Aufstellort ist der direkte Zugang zum IE-Switch jedoch nicht immer möglich. Aus diesem Grund bietet das Web Based Management eine Simulationsdarstellung für die Leuchtdioden.

Das obere Bildschirmviertel zeigt eine schematische Darstellung des IE-Switches X-300 bzw. des IE-Switches X-400 mit den vorhandenen Modulen sowie den entsprechenden LEDs. Die Traffic-Anzeige wird nicht real dargestellt (kein Blinken der LEDs). Die Bedeutung der Leuchtdiodenanzeigen ist in der Betriebsanleitung "Industrial Ethernet Switches SCALANCE X-300" bzw. Betriebsanleitung "Industrial Ethernet Switches SCALANCE X-400" beschrieben.

Durch Anklicken der Beschriftungen oberhalb der symbolisch dargestellten Module können Sie den Display Mode (LEDs DM bzw. D1/D2) der Anzeige in der Simulation wie mit dem Taster am Gerät umschalten.

Hinweis

Der Medienmodul-Extender des SCALANCE X414-3E wird in der Simulation nur dargestellt, wenn er mit mindestens einem Modul bestückt ist.

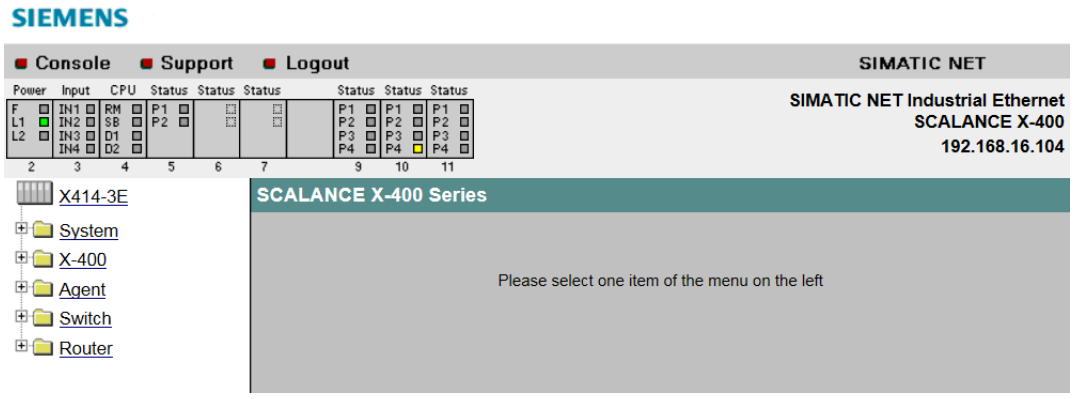


Bild 5-2 Leuchtdiodensimulation SCALANCE X414-3E

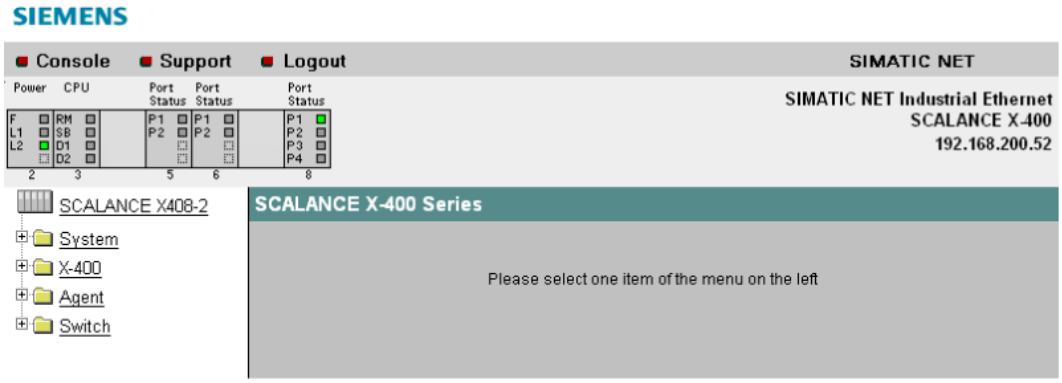


Bild 5-3 Leuchtdiodensimulation SCALANCE X408-2



Bild 5-4 Leuchtdiodensimulation SCALANCE X308-2M

5.1.3 Bedienung des Web Based Managements

Navigationsleiste

In der oberen Menüleiste des WBM befinden sich folgende Links:

- Console
  Dieser Link öffnet ein Konsolen-Fenster, in dem Sie CLI-Befehle eingeben können. Über eine TELNET-Verbindung sind Sie dann mit dem Switch verbunden.
- Support
  Durch Anklicken dieses Links rufen Sie eine Support-Seite der SIEMENS AG auf. Der SIEMENS-Support ist allerdings nur erreichbar, wenn Ihr PC eine Verbindung zum Internet hat.
- Logout
  Durch Anklicken dieses Links melden Sie sich bei dem Gerät ab.

Aktualisieren der Anzeige mit "Refresh"

Seiten des Web Based Managements, die Konfigurationsdaten anzeigen, haben am unteren Rand die Schaltfläche "Refresh". Klicken Sie diese Schaltfläche, wenn Sie für die angezeigte Seite aktuelle Daten vom IE-Switch anfordern wollen.

Speichern von Einträgen mit "Set Values"

Seiten, auf denen Sie Konfigurationsdaten festlegen können, haben am unteren Rand die Schaltfläche "Set Values". Klicken Sie diese Schaltfläche, um eingegebene Konfigurationsdaten im IE-Switch zu speichern.

Hinweis

Das Ändern der Konfigurationsdaten ist nur mit dem Login "Administrator" möglich.

5.1.4 Command Line Interface (CLI)

Starten des CLI in einer Windows-Konsole

Führen Sie folgende Schritte aus, um das Command Line Interface in einer Windows-Konsole aufzurufen:

1. Öffnen Sie eine Windows-Konsole und geben Sie den Befehl telnet gefolgt von der IP-Adresse des IE-Switches ein: *C:\>ssh <IP-Adresse>*
2. Geben Sie Ihr Login und Ihr Passwort ein.

Starten des CLI über das Web Based Management

Klicken Sie auf den Eintrag "Console" in der oberen Menüleiste des Web Based Management. Es wird automatisch eine Telnet-Verbindung geöffnet, in der Sie sich mit User-Name und Passwort anmelden können.

Verkürzte Befehlseingabe

Alternativ zur vollständigen Eingabe von CLI-Befehlen können Sie den/die ersten Buchstaben eingeben und dann die Tabulator-Taste drücken. Das Command Line Interface zeigt dann einen Befehl an, der mit dem/den eingegebenen Buchstaben anfängt. Wenn nicht das gewünschte Kommando angezeigt wird, drücken Sie erneut die Tabulator-Taste, um den nächsten Befehl anzuzeigen.

Verzeichnisstruktur

Bevor Sie im Command Line Interface einen Befehl eingeben können, müssen Sie erst das entsprechende Menü oder Untermenü aufrufen. In diesem Kapitel sind die Befehle eines Menüs jeweils in einer Tabelle zusammengefasst. In der Tabelle sind nur die Befehle selbst aufgeführt.

Adressierungsschema der Ports beim IE-Switch X-400

Für die Port-Bezeichnungen des IE-Switches X-400 gilt dabei folgendes Adressierungsschema:

- Die erste Zahl gibt den Steckplatz an.
- Die zweite Zahl ist durch einen Punkt getrennt und gibt den Port an.

Beispielsweise steht die Bezeichnung 6.2 für den zweiten Port auf dem sechsten Steckplatz.

Adressierungsschema der Ports beim IE-Switch X-300

Für die Port-Bezeichnungen des IE-Switches X-300 gilt folgendes Adressierungsschema:

- Die Zahl gibt direkt den Port an.

So steht die Bezeichnung 2 auch für den zweiten Port auf dem IE-Switch X-300.

Symbolik für die Darstellung der CLI-Befehle

CLI-Befehle haben in der Regel einen oder mehrere Parameter, die in der Syntaxbeschreibung wie folgt dargestellt werden:

Syntax CLI-Befehl		**Einsatz Parameter**	**Beschreibung**	**Beispiel**	
< >	Spitze Klammer	notwendig	Notwendige Parameter sind durch spitze Klammer gekennzeichnet. Hinweis: Wenn notwendige Parameter weggelassen werden, geben die meisten Befehle den aktuellen Wert aus.	<ip-adresse>	
[ ]	Eckige Klammer	optional	Optionale Parameter sind durch eckige Klammer gekennzeichnet.	[D|A]	
|	Senkrechter Strich, Pipe-Symbol	alternativ	Alternative Parameter sind durch Pipe-Symbol gekennzeichnet. Eingabe entweder a oder b bzw. Wertebereich 1 oder Wertebereich 2	<a | b> <... | ....>	[a | b] [.... | ...]
...	Punkte	Werte-bereich	Wertebereiche von Parametern sind durch drei Punkte gekennzeichnet.	<0...255>	[0...255]
string		Text	Text wird als string gekennzeichnet. (siehe Beispiele)	• Dateiname • Geografische Koordinaten • Namen und Bezeichnungen • Passwörter	
Port		Port-bezeichnung	Portbezeichnung	5.1 bei X-400 bzw. 7 bei X-300	
Number		Zahlenwert	Zahlenwert	1	
MAC		MAC-Adresse	MAC-Adresse	80:fe:11:f3:4d:d6	

Syntax CLI-Befehl	Einsatz Parameter	Beschreibung	Beispiel
IP	IP-Adresse	IP-Adresse	192.168.1.1
mode	Modi einer Funktion	Gibt es für eine Funktion mehrere Betriebsmodi wird dies durch den Parameter mode gekennzeichnet. Alle verfügbaren Modi können über den Parameter "?" angezeigt werden	• D Deaktiviert die Funktion

Menüunabhängige Befehle

Die Befehle in der folgenden Tabelle können Sie in jedem Menü oder Untermenü aufrufen.

Tabelle 5-1 Command Line Interface - CLI\ ... >

Befehl	Beschreibung	Kommentar
/	Wechselt auf die oberste Menüebene.	Administrator und User
..	Wechselt eine Menüebene nach oben.	Administrator und User
?	Zeigt die im jeweiligen Menü verfügbaren Befehle an.	Administrator und User
exit	Beendet die CLI-Sitzung.	Administrator und User
restart	Neustart des IE-Switches	Nur Administrator
Info	Zeigt Informationen zum jeweiligen Menüpunkt an.	Administrator und User

Befehle in der obersten Menüebene des Command Line Interface

Die Befehle in der folgenden Tabelle können Sie im Menü CLI> aufrufen.

Tabelle 5-2 Command Line Interface - CLI>

Befehl	Beschreibung	Kommentar
service debugloginenable <password>	Aktiviert einen temporären Diagnosezugang mit dem Benutzernamen "debug" und einem entsprechenden Passwort. Dieser wird nach dem Neustart automatisch deaktiviert. Die Nutzung des Diagnosezugangs ist nur für Siemens-Personal vorgesehen. Eine unsachgemäße Nutzung des Zugangs kann zu Störungen des Betriebs führen.	Nur Administrator
service debuglogindisable	Deaktiviert den Benutzer "debug".	Nur Administrator

Hilfe zu CLI-Befehlen

- Weitere Informationen können über den Parameter "?" abgerufen werden (sofern für einen Befehl notwendig und vorhanden).
- Sind keine weiteren Informationen vorhanden wird die Befehlssyntax aus der Menüübersicht angezeigt.

5.2 Das Menü System

5.2.1 System Configuration

Allgemeine Geräteinformationen

Diese Bildschirmmaske erscheint, wenn Sie das Ordnersymbol *System* angeklickt haben:

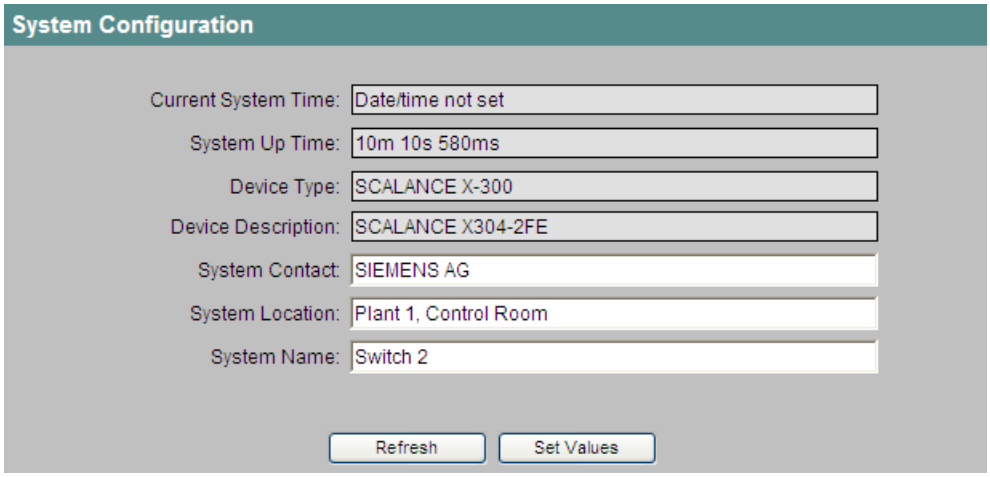


Bild 5-5 System Configuration

Current SystemTime (nur lesbar)
Die Systemuhrzeit wird entweder vom Anwender eingestellt oder per Uhrzeit-Frame synchronisiert (entweder SINEC H1 Uhrzeit-Frame oder SNTP). Es wird auch angegeben, wann und wie sie eingestellt wurden:

- (**m**) Die Einstellung erfolgte manuell.
- (**t**) Die Einstellung erfolgte per SIMATIC Uhrzeit-Frame, ist aber nicht synchron mit dem Uhrzeitsender.
- (**s**) Die Einstellung erfolgte per SIMATIC Uhrzeit-Frame und ist synchron mit dem Uhrzeitsender.
- (**p**) Die Einstellung erfolgte per SNTP-Protokoll.

System Up Time (nur lesbar)
Die Zeitdauer seit dem letzten Reboot.

Device Type (nur lesbar)
Die Typenbezeichnung des Geräts.

Device Description (nur lesbar)
Die Beschreibung des Geräts.

System Contact
Geben Sie in dieses Feld den Namen einer Kontaktperson ein, die für die Verwaltung des Gerätes zuständig ist.

System Location
Geben Sie in dieses Feld eine Ortsangabe für das Gerät ein, beispielsweise eine Raumnummer.

System Name
Geben Sie in dieses Feld eine Beschreibung des Gerätes ein.

Syntax Command Line Interface

Tabelle 5-3 System Configuration - CLI\SYSTEM>

Befehl	Beschreibung	Kommentar
syscon [string]	Setzen/Anzeigen der MIB-Variablen syscontact.	Nur Administrator.
sysloc [string]	Setzen/Anzeigen der MIB-Variablen syslocation.	Nur Administrator.
sysname [string]	Setzen/Anzeigen der MIB-Variablen sysname.	Nur Administrator.
debug.bin* [create | delete]	Erzeugt oder löscht eine Datei mit Diagnosedaten. Diese Datei kann von einem eingeloggten Administrator per Web-Browser über die Adresse "http(s)://<IP-Adresse>/debug.bin" vom Gerät geladen werden. Die Datei mit Diagnosedaten ist passwortgeschützt und nur für die Auswertung durch Siemens-Personal bestimmt. Kontaktieren Sie hierzu Ihren Siemens-Ansprechpartner.	Nur Administrator.

5.2.2 System Identification & Maintenance (I&M)

System Identification & Maintenance

Die folgende Maske beinhaltet Informationen zu gerätespezifischen Hersteller- und Wartungsdaten wie Bestellnummer, Seriennummer, Versionsnummern etc.

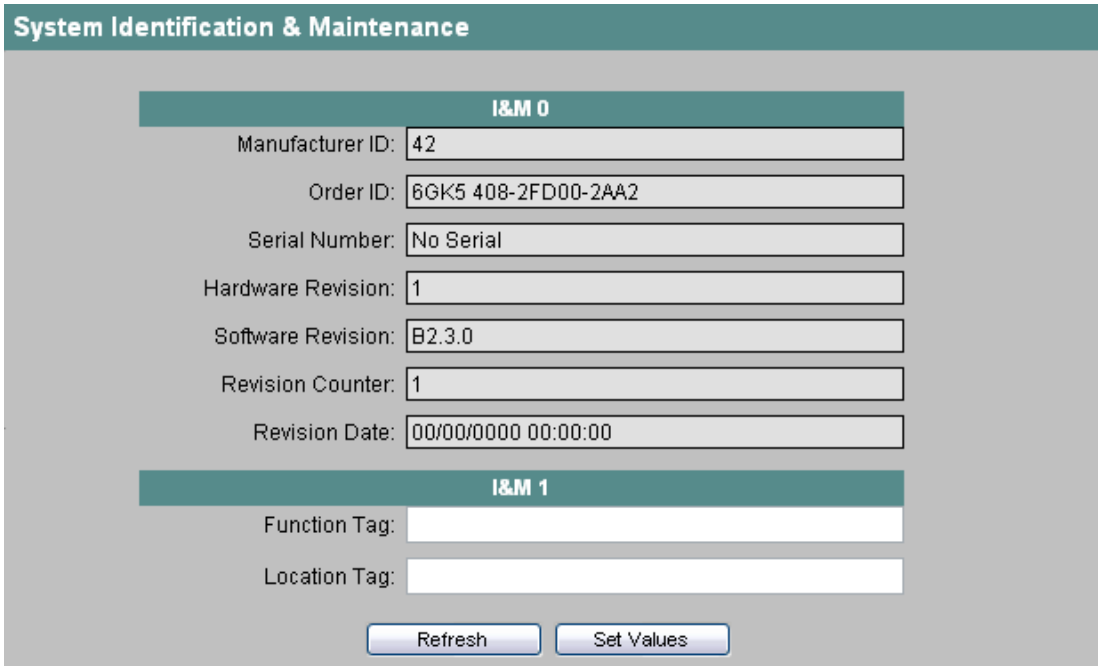


Bild 5-6 System Identification & Maintenance

I&M 0
Hier können die einzelnen Parameter zu Identification & Maintenance abgelesen werden.

I&M 1
Function Tag
Hier kann das Function Tag (Anlagenkennzeichen) eingetragen werden.

Location Tag
Hier kann das Location Tag (Ortskennzeichen) eingetragen werden.

Syntax Command Line Interface

Tabelle 5-4 System Identification & Maintenance - CLI\SYSTEM\IM>

Befehl	Beschreibung	Kommentar
info	Zeigt Informationen über den Menüpunkt "Identification & Maintenance" an.	-
revcnt [E|D]	Aktiviert/deaktiviert den Revision Counter. Ohne Parameter zeigt dieser Befehl an, ob der Revision Counter aktiviert oder deaktiviert ist.	Nur Administrator.
function [string]	Legt das Anlagenkennzeichen fest (max. 32 Zeichen).	Nur Administrator.
location [string]	Legt das Ortskennzeichen fest (max. 32 Zeichen).	Nur Administrator.

5.2.3 System Restart & Defaults

Zurücksetzen der Voreinstellungen

In diesem Menü finden Sie eine Schaltfläche zum Neustart des IE-Switches sowie verschiedene Möglichkeiten, die Voreinstellungen des IE-Switches zurückzusetzen.

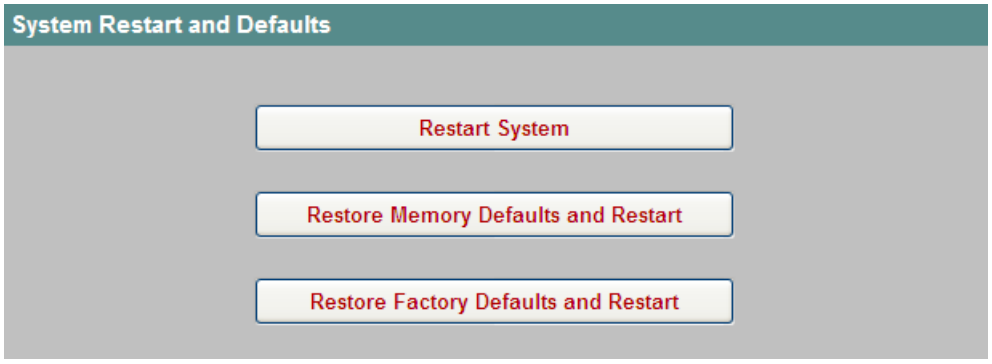


Bild 5-7 System Restart and Defaults

Hinweis

Beachten Sie folgende Punkte beim Neustart eines IE-Switches:

- Sie können einen Neustart des IE-Switches nur mit Administrator-Rechten durchführen.
- Der Neustart eines IE-Switches sollte nur durch die Schaltflächen dieses Menüs oder durch die entsprechenden CLI-Befehle und nicht durch Spannung aus / Spannung ein am Gerät erfolgen.
- Vorgenommene Änderungen sind erst nach dem Anklicken der Schaltfläche "Set Value" auf der jeweiligen Seite des WBM im Gerät gespeichert, ein erneutes Speichern der Konfigurationsdaten vor einem Neustart ist nicht notwendig und auch nicht möglich.
- Der 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 *Temporäre Internetdateien* über die Schaltfläche Einstellungen.
- Unter dem Text *Neuere Versionen der gespeicherten Seite suchen* muss dort *Automatisch* markiert sein.

Restart System

Klicken Sie auf diese Schaltfläche, um den IE-Switch neu zu starten. Sie müssen den Neustart in einer Dialogbox bestätigen. Bei einem Neustart wird der IE-Switch neu initialisiert, die interne Firmware wird neu geladen und das Gerät führt einen Selbsttest durch. Die gelernten Einträge in der Adresstabelle werden gelöscht. Sie können das Browser–Fenster geöffnet lassen, während der IE-Switch neu startet.

Restore Memory Defaults and Restart

Klicken Sie diese Schaltfläche, um die werkseitigen Konfigurationseinstellungen mit Ausnahme der folgenden Parameter zurückzusetzen:

- IP-Adressen (In-Band und Out-Band)
- Subnetz-Masken (In-Band und Out-Band)
- IP-Adresse des Default Gateways
- DHCP/BOOTP-Flag
- System Name
- System Location
- System Contact
- Ring Redundancy
- Standby-Funktionalität
- (R)STP
- PNIO Device Name (Name of Station)

Es wird ein automatischer Neustart ausgeführt.

Restore Factory Defaults and Restart

Klicken Sie diese Schaltfläche, um die werkseitigen Konfigurationseinstellungen wiederherzustellen. Es werden auch die geschützten Voreinstellungen zurückgesetzt. Es wird ein automatischer Neustart ausgeführt.

Hinweis

Durch das Zurücksetzen aller Voreinstellungen geht auch die IP-Adresse verloren. Ein IE-Switch ist danach nur über SINEC PNI oder die serielle Schnittstelle (nur IE-Switches X-400) ansprechbar.

Syntax Command Line Interface

Tabelle 5-5 System Restart & Defaults - CLI>

Befehl	Beschreibung	Kommentar
restart	Neustart des IE-Switches.	Nur Administrator. Dieser Befehl kann aus allen Menüs aufgerufen werden.

Tabelle 5-6 System Restart & Defaults - CLI\SYSTEM>

Befehl	Beschreibung	Kommentar
defaults	Stellt die werksseitigen Einstellungen wieder her. Auch die geschützten Voreinstellungen werden zurückgesetzt. Es wird ein Neustart des Geräts durchgeführt.	Nur Administrator. Dieser Befehl hat die gleichen Auswirkungen wie das Betätigen der Schaltfläche *Restore Factory Defaults and Restart* im WBM.
memreset	Stellt die werksseitigen Einstellungen wieder her. Die geschützten Einstellungen bleiben erhalten. Es wird automatisch ein Neustart des Geräts durchgeführt.	Nur Administrator. Dieser Befehl hat die gleichen Auswirkungen wie das Betätigen der Schaltfläche *Restore Memory Defaults and Restart* im WBM.

5.2.4 System Save & Load via HTTP

System Save & Load HTTP

Das WBM bietet die Möglichkeit, Konfigurationsinformationen in einer externen Datei auf Ihrem Client-PC zu speichern bzw. solche Daten aus einer externen Datei vom PC in die IE-Switchs zu laden. Außerdem können Sie eine neue Firmware aus einer Datei von Ihrem Client-PC laden.

Hinweis

Löschen Sie nach einem Firmwareupdate den Cache des Web-Browsers.

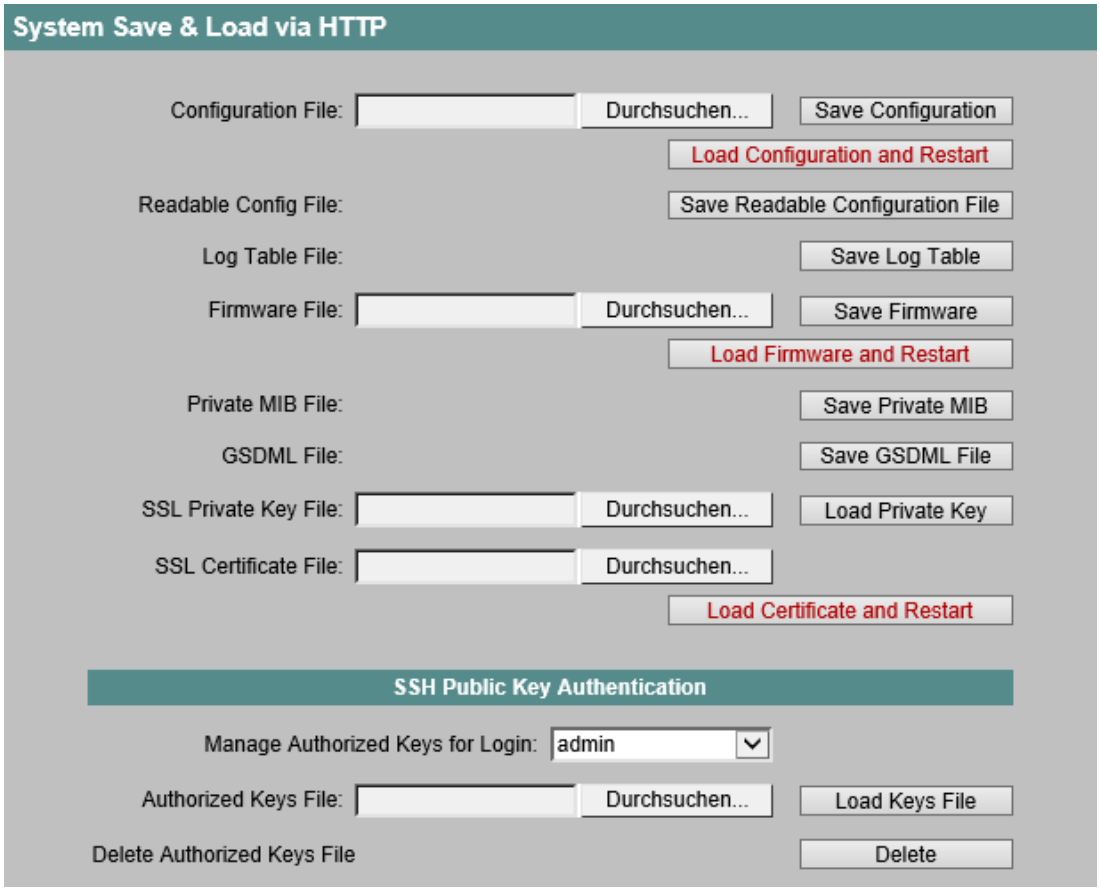


Bild 5-8 System Save & Load via HTTP

Configuration File
Name und Verzeichnispfad der Konfigurationsdatei, die Sie auf den IE-Switch laden wollen.

Readable Config File
Sie können die Konfigurationsdatei des IE-Switch als Textdatei mit CLI-Befehlen abspeichern.

Log Table File
Sie können die Einträge der Event Log-Tabelle des IE-Switchs abspeichern.

Firmware File
Name und Verzeichnispfad der Datei, aus der Sie die neue Firmware laden wollen.

Private MIB File
Sie können die private MIB-Datei abspeichern.

GSDML File
Sie können PROFINET-Informationen über die Geräteeigenschaften abspeichern.

SSL Private Key File
Name und Verzeichnispfad der Datei, aus der Sie den privaten SSL-Schlüssel ins Gerät laden wollen.

SSL Certificate File
Name und Verzeichnispfad der Datei, aus der Sie das SSL-Zertifikat ins Gerät laden wollen.

Hinweis

Da der private Schlüssel und das Zertifikat zusammengehören, werden die Dateien erst gespeichert, nachdem sowohl Schlüssel als auch Zertifikat geladen wurden. Beim Laden des Zertifikats wird überprüft, ob es zum geladenen Schlüssel passt. Ein Neustart ist erforderlich, damit die neuen SSL Dateien übernommen werden.

Für Geräte des Typs SCALANCE X414-3E gilt Folgendes:

Es werden nur private RSA Schlüssel mit max. Länge von 2048 Bytes akzeptiert. Private Schlüssel dürfen nicht mit einem Passwort geschützt sein. Das SSL-Zertifikat muss PEM-codiert sein.

Für Geräte der Produktlinie SCALANCE X-300 und Geräte des Typs SCALANCE X408-2 gilt Folgendes:

Ab Firmware-Version V4.1.4 wurde von RSA-Zertifikaten auf Zertifikate für Elliptische-Kurven-Kryptografie ("ECDSA-Zertifikate") umgestellt. Verwenden Sie nur ECDSA-Zertifikate im PEM-Format, die mit den folgenden Kurven erzeugt wurden:

- secp256r1 (NIST P-256)
- secp384r1 (NIST P-384)
- secp521r1 (NIST P-521)

RSA-Zertifikate werden ab dieser Firmware-Version nicht mehr unterstützt. Die auf dem Gerät vorhandenen RSA-Zertifikate werden automatisch durch selbstsignierte ECDSA-Zertifikate ersetzt.

Funktionsweise der SSH Public Key Authentifizierung

Bei SSH kann die Authentifizierung über ein Passwort oder ein Public Key-Verfahren erfolgen. Die Public Key Authentifizierung bietet den Vorteil, dass die entsprechenden Schlüssel in Dateien gepeichert werden und keine manuelle Eingabe erforderlich ist. Für jeden Client, der eine SSH-Verbindung mit Public Key Authentifizierung zu einem Switch aufbauen soll, müssen Sie ein Schlüsselpaar generieren. Die öffentlichen Schlüssel werden auf dem Switch hinterlegt, zu dem der Client eine SSH-Verbindung aufbaut. Die geheimen Schlüssel werden nur im jeweiligen Client gespeichert. Beim SSH-Verbindungsaufbau erzeugt der Client mithilfe des geheimen Schlüssels eine Signatur und sendet diese an den Switch. Der Switch überprüft die Signatur anhand des öffentlichen Schlüssels und kann dadurch den Client authentifizieren.

SSH Public Key Authentifizierung bei SCALANCE-Geräten

SCALANCE-Geräte bis zur **Firmware-Version V4.1.3** unterstützen die folgenden Public Key-Typen und Schlüssellängen:

Verfahren	Maximale Schlüssellänge
SSH-RSA	16 kbit
SSH-DSS	8 kbit (DSA-Schlüssel)

SCALANCE-Geräte ab **Firmware-Version V4.1.4** unterstützen nur noch die folgenden Verfahren:

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp512
- ssh-ed25519

Hinweis

Firmware-Update von V4.1.3 auf V4.1.4

Bei einem Update von Firmware-Version V4.1.3 auf Firmware-Version V4.1.4 oder höher werden die bisher hinterlegten öffentlichen Schlüssel automatisch entfernt. Der Benutzer muss neue Schlüssel mit einem der neuen Verfahren hinterlegen.

Die Schlüssel müssen im OpenSSH Public Key Format vorliegen. Für die Erzeugung der Schlüsselpaare stehen unter anderem die folgenden beiden Programme zur Verfügung:

- **ssh-keygen**
  Bestandteil von SSH-Implementierungen für verschiedene Betriebssysteme.
- **PUTTYgen**
  Ein Client für Windows-Betriebssysteme.

Alle autorisierten öffentlichen Schlüssel eines Logins müssen in einer gemeinsamen Textdatei mit einer maximalen Größe von 32 kByte gespeichert werden. Für die Benutzer "admin" und "user" gibt es jeweils eine eigene Datei für die Schlüssel. Kommentarzeilen müssen mit dem Zeichen "#" beginnen. Sie können diese Datei als Benutzer "admin" in ein SCALANCE-Gerät laden.

Beispiel für eine Datei mit öffentlichen Schlüsseln:

```
. . .
# public key for host 1.2.3.4
ecdsa-sha2-nistp256 AAAAB3N[... long string of characters ...]UH0=
key-comment
# public key for host 1.2.3.5
ssh-ed25519 AAAAB3N[... long string of characters ...]UH0= key-
```

```
comment
. . .
```

Hinweis

Die auf einem SCALANCE-Gerät gespeicherten öffentlichen Schlüssel werden beim Stecken des C-PLUG in ein anderes Gerät übertragen. Die gespeicherten öffentlichen Schlüssel sind nicht Bestandteil der Konfigurationsdatei.

Die SSH Public Key Authentifizierung ist bei folgenden Geräten nur dann möglich, wenn ein C-PLUG gesteckt wurde:

Gerät	Artikelnummer
SCALANCE X307-3	6GK5307-3BL00-2AA3
SCALANCE X307-3LD	6GK5307-3BM00-2AA3
SCALANCE X308-2	6GK5308-2FL00-2AA3
SCALANCE X308-2LD	6GK5308-2FM00-2AA3
SCALANCE X308-2LH	6GK5308-2FN00-2AA3
SCALANCE X308-2LH+	6GK5308-2FP00-2AA3
SCALANCE X310FE	6GK5310-0BA00-2AA3
SCALANCE X310	6GK5310-0FA00-2AA3

Konfiguration der SSH Public Key Authentifizierung

Managed Authorized Keys for Login
Wählen Sie, für welches Login die SSH Public Key-Authentifizierung gelten soll. Für jedes Login können Sie eine eigene Datei mit öffentlichen Schlüsseln laden.

Authorized Keys File
Laden Sie eine Datei mit öffentlichen Schlüsseln für die SSH Public Key-Authentifizierung.

Delete Authorized Keys File
Löschen Sie die zuvor geladene öffentliche Schlüssel. Dadurch wird gleichzeitig die SSH Public Key-Authentifizierung deaktivieren.

So laden Sie Daten über HTTP / HTTPS

1. Geben Sie im entsprechenden Textfeld einen Namen und Verzeichnispfad für die Datei ein, aus der Sie Daten übernehmen wollen.
2. Starten Sie das Laden der entsprechenden Datei durch Anklicken einer der Schaltflächen "Load Firmware and Restart", "Load Configuration and Restart", "Load Private Key", "Load Certificate and Restart"
   Nach dem Laden erfolgt automatisch ein Neustart außer bei "Load Private Key" und das Gerät läuft mit den neuen Daten hoch.

So speichern Sie Daten über HTTP / HTTPS

1. Starten Sie das Speichern durch Anklicken einer der Schaltflächen "Save Configuration", "Save Log Table", "Save Firmware", "Save Private MIB" oder "Save GSDML File".
2. Sie werden aufgefordert einen Speicherort und einen Namen für die Datei zu wählen bzw. den vorgeschlagenen Dateinamen zu übernehmen.

Wiederverwendung von Konfigurationsdaten

Das Abspeichern und Einlesen von Konfigurationsdaten reduziert den Aufwand, wenn mehrere IE-Switch die gleiche Konfiguration erhalten sollen und wenn die Zuweisung der IP-Adressen über DHCP erfolgt.

Hinweis

Gleiche Konfiguration auf mehreren IE-Switchen verwenden

Die Konfiguration eines IE-Switches kann nicht auf jeden anderen IE-Switch geladen werden.

Eine Liste mit kompatiblen Geräten finden Sie im Kapitel "Gleiche Konfiguration auf mehreren IE-Switches verwenden (Seite 409)".

Speichern Sie die Konfigurationsdaten auf Ihrem Rechner, nachdem Sie einen IE-Switch konfiguriert haben. Alternativ können Sie die Daten auf einem TFTP-Server (Seite 60) speichern.

Laden Sie diese Datei auf alle weiteren IE-Switches, die Sie konfigurieren wollen.

Falls für einzelne Geräte individuelle Einstellungen erforderlich sind, müssen Sie diese online vornehmen.

Die Konfigurationsdaten werden kodiert gespeichert, deshalb können Sie diese Dateien nicht mit einem Texteditor bearbeiten.

Konfigurationsdatei über FTP laden

Außer über HTTP/HTTPS und TFTP, können Sie eine Konfigurationsdatei auch über FTP auf das Gerät laden. Führen Sie folgende Schritte durch, um eine Konfigurationsdatei über FTP auf das Gerät zu laden:

1. Öffnen Sie ein Konsolen-Fenster und geben Sie den Befehl "ftp" gefolgt von der IP-Adresse des IE-Switchs ein.
   Beispiel:
   `ftp 192.168.20.54`
2. Geben Sie für Login und Passwort die gleichen Werte ein, die Sie auch für WBM und CLI verwenden.
3. Geben Sie den Befehl "put" gefolgt vom Namen der Konfigurationsdatei ein.
   Beispiel:
   `put X308-2M.cfg`
4. Nach dem Abschluss des Ladevorgangs beendet der IE-Switch die FTP-Verbindung und startet neu.

5.2.5 System Save & Load via TFTP

Datenaustausch mit einem TFTP-Server

Das WBM bietet die Möglichkeit, Konfigurationsinformationen in einer externen Datei zu speichern bzw. solche Daten aus einer externen Datei in den IE-Switch zu laden. Außerdem können Sie auch die Log-Informationen in einer Datei speichern oder eine neue Firmware aus einer Datei laden. Die dafür notwendigen Eingaben können Sie auf der Seite des Menüs Save & Load machen.

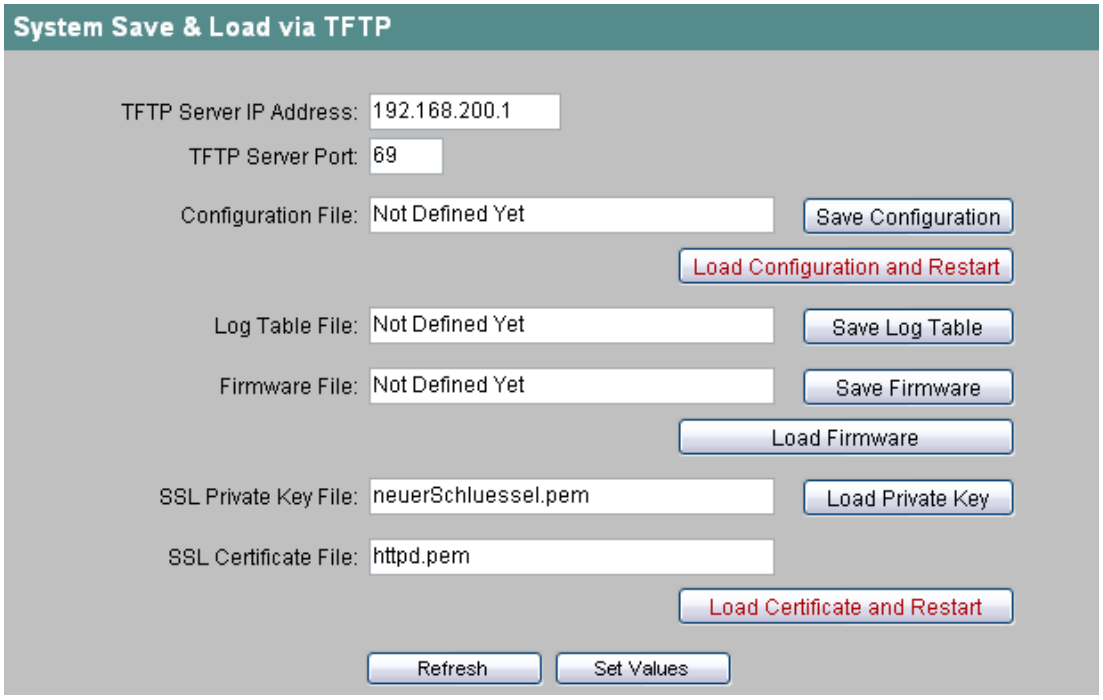


Bild 5-9 System Save & Load

TFTP Server IP Address
Die IP-Adresse des TFTP-Servers, mit dem Sie Daten austauschen wollen.

TFTP Server Port
Der Port des TFTP-Servers, über den der Datenaustausch abgewickelt wird. Gegebenenfalls können Sie den Default-Wert 69 entsprechend Ihren spezifischen Anforderungen ändern.

Configuration File
Namen und gegebenenfalls Verzeichnispfad der Konfigurationdatei (maximal 32 Zeichen), die Sie auf den IE-Switch laden wollen oder in die Sie die aktuellen Konfigurationsinformationen speichern wollen.

Log Table File
Name und gegebenenfalls Verzeichnispfad der Datei (maximal 32 Zeichen), in der Sie den Inhalt der Logtabelle speichern wollen.

Firmware File
Name und gegebenenfalls Verzeichnispfad der Datei (maximal 32 Zeichen), aus der Sie die neue Firmware laden wollen oder in die Sie die aktuelle Firmware speichern wollen.

SSL Private Key File
Name und Verzeichnispfad der Datei, aus der Sie den privaten SSL Schlüssel ins Gerät laden wollen. Diese Angaben in diesem Feld sind auf max. 32 Zeichen beschränkt.

SSL Certificate File
Name und Verzeichnispfad der Datei, aus der Sie das SSL-Zertifikat ins Gerät laden wollen. Diese Angaben in diesem Feld sind auf max. 32 Zeichen beschränkt.

Hinweis

Da der private Schlüssel und das Zertifikat zueinander gehören, werden die Dateien erst gespeichert, nachdem sowohl Schlüssel als auch das Zertifikat geladen wurden. Beim Laden des Zertifikats wird überprüft, ob es zum geladenen Schlüssel passt. Ein Neustart ist erforderlich, damit die neuen SSL Dateien übernommen werden.

Es werden nur private RSA Schlüssel mit max. Länge von 1280 Bytes akzeptiert; private Schlüssel dürfen nicht Passwort geschützt sein.

SSL Zertifikat muss PEM codiert sein, seine Länge darf 2560 Bytes nicht überschreiten.

So laden bzw. speichern Sie Daten über TFTP

1. Geben Sie die IP-Adresse des TFTP-Servers im Textfeld "TFTP Server IP Address" ein.
2. Geben Sie im entsprechenden Textfeld einen Namen (maximal 32 Zeichen) für die Datei ein, in die Sie speichern bzw. aus der Sie Daten übernehmen wollen.
3. Klicken Sie die Schaltfläche "Set Values", bevor Sie weitere Eingaben für das Speichern oder Laden von Daten machen.
4. Starten Sie das Speichern / Laden durch Anklicken der entsprechenden Schaltfläche "Save" bzw. "Load".

Anschließend erfolgt beim Laden der Konfiguration und des SSL-Zertifikats ein Neustart und das Gerät läuft mit den neuen Daten hoch.

Wiederverwendung von Konfigurationsdaten

Das Abspeichern und Einlesen von Konfigurationsdaten reduziert den Aufwand, wenn mehrere IE-Switch die gleiche Konfiguration erhalten sollen und wenn die Zuweisung der IP-Adressen über DHCP erfolgt.

Hinweis

Gleiche Konfiguration auf mehreren IE-Switchen verwenden

Die Konfiguration eines IE-Switches kann nicht auf jeden anderen IE-Switch geladen werden.

Eine Liste mit kompatiblen Geräten finden Sie im Kapitel "Gleiche Konfiguration auf mehreren IE-Switches verwenden (Seite 409)".

Speichern Sie die Konfigurationsdaten auf einem TFTP-Server, nachdem Sie einen IE-Switch konfiguriert haben. Alternativ können Sie die Daten auf Ihrem Rechner (Seite 55) speichern.

Laden Sie diese Datei auf alle weiteren IE-Switches, die Sie konfigurieren wollen.

Falls für einzelne Geräte individuelle Einstellungen erforderlich sind, müssen Sie diese online vornehmen.

Die Konfigurationsdaten werden kodiert gespeichert, deshalb können Sie diese Dateien nicht mit einem Texteditor bearbeiten.

Syntax Command Line Interface

Tabelle 5-7 System Save & Load - CLI\SYSTEM\SAVELOAD>

Befehl	Beschreibung	Kommentar
server [<ip>[:port]]	Legt die IP-Adresse und optional den Port des TFTP-Servers fest, mit dem der Datenaustausch erfolgen soll.	Nur Administrator. Default-Wert: 0.0.0.0
cfgname <string>	Legt den Namen einer Datei (max. 32 Zeichen) fest, aus der die Konfigurationsdaten geladen werden oder in die die Konfigurationsdaten gespeichert werden.	Nur Administrator.
cfgsave	Speichert die Konfigurationsdaten in einer Datei auf dem TFTP-Server.	Nur Administrator.
cfgload	Lädt die Konfigurationsdaten aus einer Datei auf dem TFTP-Server.	Nur Administrator.
logname <string>	Legt den Namen einer Datei (max. 32 Zeichen) fest, in die die Logtabelle gespeichert wird.	Nur Administrator.
logsave	Speichert die Protokolltabelle in eine Datei auf dem TFTP-Server.	Nur Administrator.
fwname <string>	Legt den Namen einer Datei (max. 32 Zeichen) fest, aus der die Firmware geladen wird.	Nur Administrator. Default-Wert: Nicht definiert.
fwload	Lädt die Firmware aus einer Datei.	Nur Administrator.
fwsave	Speichert die Firmware in einer Datei auf TFTP-Server.	Nur Administrator.
keyload	Lädt den privaten SSL Schlüssel aus einer Datei.	Nur Administrator.
certload	Lädt ein SSL Zertifikat aus einer Datei.	Nur Administrator.

Tabelle 5-8 System Save & Load - CLI\SYSTEM>

Befehl	Beschreibung	Kommentar
authkeys [admin | user]	Zeigt die SSH-Fingerprints der geladenen öffentlichen Schlüssel an. Als Parameter müssen Sie das Login angeben, für das der SSH-Fingerprint angezeigt werden sollen.	Nur Administrator.

5.2.6 System Version Numbers

Versionen von Hardware und Software

Diese Seite zeigt, mit welchen Ausgabeständen von Hardware und Software der IE-Switch betrieben wird:

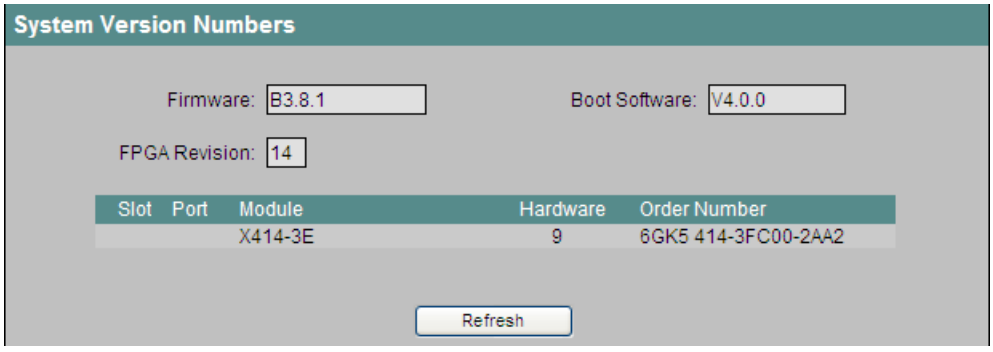


Bild 5-10 System Version Numbers

Firmware
Die Version der im IE-Switch ablaufenden Firmware.

Boot Software
Hier wird die Version der Boot-Software angezeigt. Die Boot-Software ist fest im IE-Switch gespeichert.

FPGA Revision
Die im IE-Switch verwendete FPGA Revision.

Tabelle mit Einträgen für das Grundgerät und die Module
Die erste Tabellenzeile gibt die Version des IE-Switches an. In der Spalte Slot wird der Steckplatz auf dem Grundgerät angegeben. Bezieht sich die Information auf das Grundgerät selbst, ist in dieser Spalte ein "-" angegeben. In der Spalte Hardware wird der Ausgabestand und in der Spalte Order Number die Bestellnummer des IE-Switches oder Moduls angezeigt.

Syntax Command Line Interface

Tabelle 5-9 System Version Numbers - CLI>

Befehl	Beschreibung	Kommentar
info	Neben anderen Informationen zeigt dieser Befehl mit welchen Ausgabeständen von Software der IE-Switch betrieben wird.	-

Tabelle 5-10 System Version Numbers - CLI\SYSTEM>

Befehl	Beschreibung	Kommentar
version	Zeigt die Firmware-, Hardware- und Boot-Software-Version des IE-Switches an und liefert nähere Informationen zum Grundgerät und ggf. den Modulen.	-

5.2.7 System Passwords & Login Mode

Passwörter und Login-Modus

Hinweis

Voreinstellung der Passwörter bei Auslieferung

Admin-Passwort: admin
User-Passwort: user

In dieser Maske können Sie als Administrator die Passwörter für Admin und User ändern. Ein Passwort darf maximal 16 Zeichen (7-Bit-ASCII) lang sein.

Außerdem legen Sie durch Auswahl eines Login-Modus fest, mit welchen Benutzernamen der Login möglich ist.

Hinweis

RADIUS

Um den Login-Modus "RADIUS" bzw. "RADIUS and Local" nutzen zu können, muss ein RADIUS-Server hinterlegt und für die Benutzerauthentifizierung konfiguriert sein. Diese Konfiguration wird im Menü "Switch" auf der Seite "802.1x RADIUS Configuration" vorgenommen.

Hinweis

SSH Public Key Authentifizierung

Für die SSH Public Key Authentifizierung muss der Login Mode "Local" oder "RADIUS and Local" aktiviert sein. Bei "RADIUS and Local" gilt die SSH Public Key Authentifizierung für den lokalen Benutzer. Im Login Mode "RADIUS" ist die SSH Public Key Authentifizierung nicht möglich.

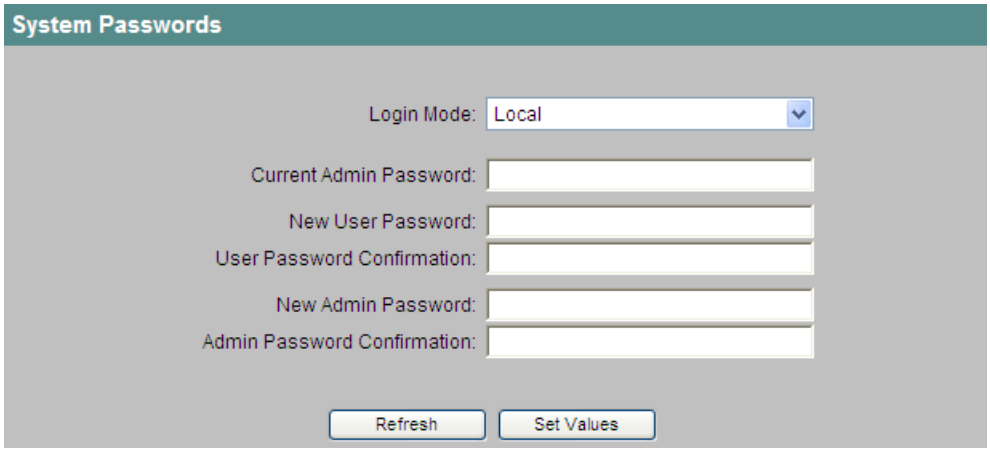


Bild 5-11 System-Passwörter

Auswahlfeld "Login Mode"

Der Login-Modus stellt folgende Optionen zur Verfügung:

Local:	Der Login kann nur über die in der Firmware vorhandenen Benutzer (User und Admin) erfolgen.
RADIUS and Local:	Der Login kann sowohl über die in der Firmware vorhandenen Benutzer (User und Admin) als auch über einen RADIUS-Server erfolgen. Benutzernamen auf dem RADIUS-Server haben dabei Vorrang.
RADIUS:	Der Login kann ausschließlich über die Login-Daten erfolgen, die auf einem RADIUS-Server hinterlegt sind. Die lokalen Benutzernamen sind deaktiviert.

Speichern

Speichern Sie Ihre Angaben durch Klicken auf die Schaltfläche "Set Values".

Hinweis

Radius-Authentifizierung schlägt fehl

Falls der als primär konfigurierte RADIUS-Server ausfällt, dann schlägt die Authentifizierung zunächst fehl. Erst bei einem weiteren Anmeldeversuch wird die Anfrage zum Backup-Server geschickt.

Syntax Command Line Interface

Tabelle 5-11 System Passwords - CLI\SYSTEM>

Befehl	Beschreibung	Kommentar
passwd [admin | user]	Setzt das Passwort für "Admin" bzw. "User" neu.	Nur Administrator.
loginmod [L | B | R]	Legt den Login-Modus fest: • **L** Ausschließlich Benutzernamen, die in der Firmware vorhanden sind. • **B** Sowohl in der Firmware vorhandene als auch auf einem RADIUS-Server hinterlegte Benutzernamen (letztere haben Vorrang). • **R** Ausschließlich Benutzernamen, die auf einem RADIUS-Server hinterlegt sind.	Nur Administrator.

5.2.8 System Select/Set Button

Sperren des Select/Set Tasters

Am IE-Switch dient der Taster SELECT/SET zum.

- Umschalten des Anzeigemodus
- Zurücksetzen auf werkseitige Voreinstellungen (Factory default)
- Definieren der Meldemaske und der LED-Anzeige
- Aktivieren/Deaktivieren des Redundanzmanagers.

Eine detaillierte Beschreibung der einzelnen Funktionen, die am Taster bedient werden können, finden Sie in der Betriebsanleitung SCALANCE X-400.

Auf dieser Seite kann die Funktionalität des Select/Set-Tasters eingeschränkt oder komplett deaktiviert werden. Dies ist für folgende drei Funktionalitäten möglich:

- Restore Factory Defaults
- Enable/Disable Redundancy Manager
- Set Fault Mask



Bild 5-12 Select/Set Button Configuration

Enable Select/Set Functions

Durch Anklicken der Auswahlkästchen aktivieren/deaktivieren Sie die einzelnen Funktionen des Tasters.

System Command Line Interface

Tabelle 5-12 System Configuration - CLI\SYSTEM\SELSET>

Befehl	Beschreibung	Kommentar
info	Zeigt die Funktionalität des Tasters an.	-
defaults	Aktiviert/deaktiviert die "Restore Factory Defaults"-Funktion am Taster.	Nur Administrator.
rm [E|D]	Aktiviert/deaktiviert die "Enable/Disable Redundancy Manager"-Funktion am Taster.	Nur Administrator.
faultmsk	Aktiviert/deaktiviert die "Set Fault Mask"-Funktion am Taster.	Nur Administrator.

5.2.9 System Event Log Table

Protokollierung von Ereignissen

Ein IE-Switch bietet die Möglichkeit, auftretende Ereignisse zu protokollieren und auf der Seite des Menüs "Log Table" anzuzeigen. So kann beispielsweise festgehalten werden, wann ein SNMP-Authentifizierungsversuch fehlgeschlagen ist, oder wann sich der Verbindungs-Status eines Ports geändert hat. Welche Ereignisse protokolliert werden, können Sie unter dem Menüpunkt "Agent Event Configuration" festlegen. Der Inhalt der Log-Tabelle bleibt auch nach dem Ausschalten des IE-Switches erhalten.

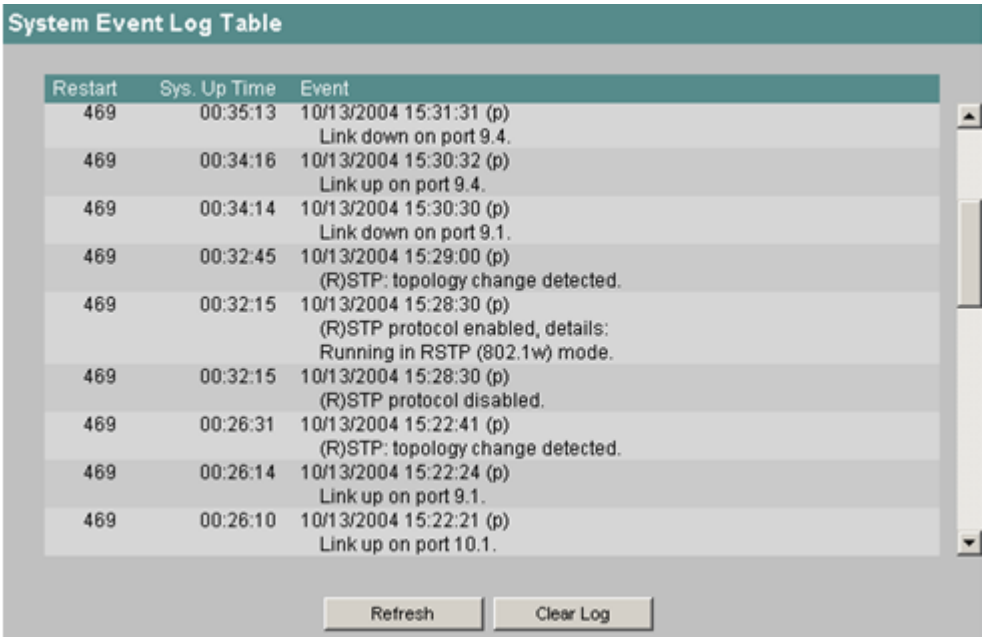


Bild 5-13 System Event Log Table

Die Spalte "Restart" gibt an, nach welchem Neustart des Geräts das entsprechende Ereignis aufgetreten ist.

Die Spalte "Sys.Up Time" zeigt die Zeit seit dem letzten Neustart des IE-Switch im Format HH:MM:SS an.

Hinweis

Bei der Zeitsynchronisation über NTP oder Siclock wird die reale Zeit des Eintrags in die Log-Tabelle eingetragen, nicht die Zeit seit dem letzten Restart.

Refresh
Klicken Sie diese Schaltfläche, um die Anzeige zu aktualisieren.

Clear Log
Mit dieser Schaltfläche können Sie den Inhalt der Log Table löschen.

Syntax Command Line Interface

Tabelle 5-13 System Event Log Table - CLI\SYSTEM>

Befehl	Beschreibung	Kommentar
events [clear]	Zeigt den Inhalt der Log-Tabelle. Mit dem Parameter [clear] kann der Inhalt der Log-Tabelle gelöscht werden.	Nur der Administrator kann die Log Table löschen. Der Inhalt der Log Table bleibt auch nach dem Ausschalten des IE-Switch erhalten.
addlog <string>	Fügt einen Text in die Log Table ein. Leerzeichen in der Zeichenkette werden ebenfalls übernommen.	Nur Administrator.

5.2.10 C-PLUG Information

Informationen über den Inhalt des Wechselmediums

Dieses Menü liefert Detailinformationen über den C-PLUG. Darüber hinaus gibt es die Möglichkeit, den C-PLUG zu formatieren oder mit einem neuen Inhalt zu versehen.

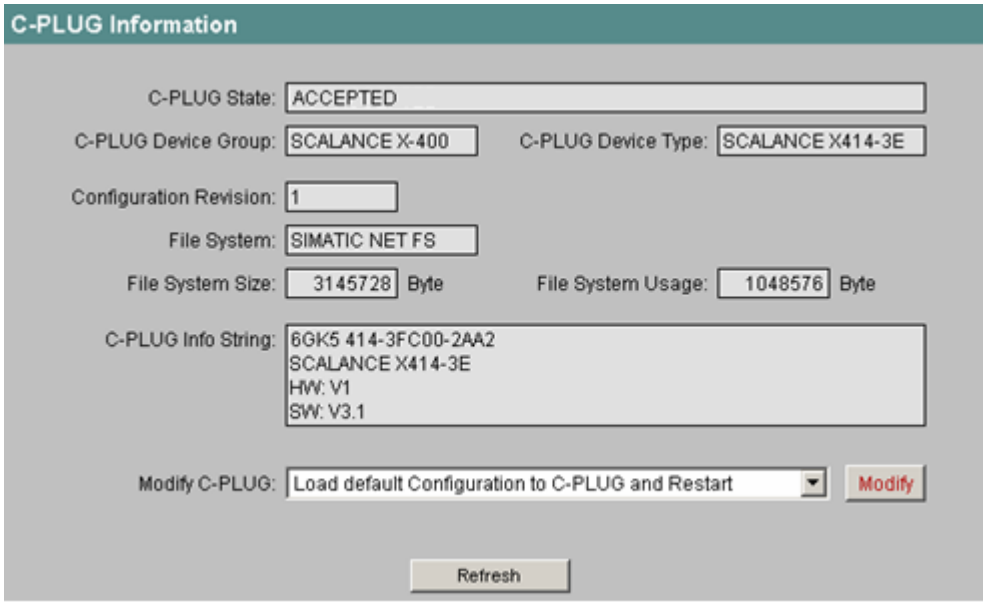


Bild 5-14 C-PLUG Information

Alle Textfelder dieses Menüs sind nur lesbar.

C-PLUG State
Hier wird der Status des C-PLUG angezeigt. Es gibt die folgenden Möglichkeiten:

- ACCEPTED
  Es ist ein C-PLUG mit einem gültigen und passenden Inhalt im IE-Switch vorhanden.
- NOT ACCEPTED
  Ungültiger bzw. inkompatibler Inhalt eines gesteckten C-PLUG. Dieser Status wird auch angezeigt, wenn der C-PLUG im Betrieb formatiert wurde.
- NOT ACCEPTED, HEADER CRC ERROR
  Es ist ein C-PLUG mit fehlerhaftem Inhalt gesteckt.
- NOT PRESENT
  Im IE-Switch ist kein C-PLUG gesteckt.

C-PLUG Device Group
Gibt an, von welcher SIMATIC NET-Produktlinie der C-PLUG im vorangegangenen Betrieb genutzt wurde.

C-PLUG Device Type
Gibt den Gerätetyp innerhalb der Produktlinie an, von dem der C-PLUG im vorangegangenen Betrieb genutzt wurde.

Configuration Revision
Die Version der Konfigurations-Struktur. Diese Angabe betrifft die vom IE-Switch unterstützten Konfigurationsmöglichkeiten und hat nichts mit der konkreten Hardwarekonfiguration zu tun. Diese Revisionsangabe ändert sich also nicht, wenn Sie Module bzw. Extender hinzufügen oder entfernen, sie kann sich aber ändern, wenn Sie ein Firmwareupdate durchführen.

File System
Zeigt den Typ des Dateisystems an, das auf dem C-PLUG vorhanden ist.

File System Size
Zeigt die maximale Speicherkapazität des Dateisystems an, das auf dem C-PLUG vorhanden ist.

File System Usage
Zeigt den belegten Speicherplatz im Dateisystem des C-PLUG an.

C-PLUG Info String
Hier werden zusätzliche Informationen über das Gerät angezeigt, das den C-PLUG im vorangegangenen Betrieb genutzt hatte, z. B. Bestellnummer, Typenbezeichnung sowie die Ausgabestände von Hardware und Software.

Modify C-PLUG, Modify
Sie können in diesem Feld nur dann Einstellungen vornehmen, wenn Sie als "Administrator"

eingeloggt sind. Wählen Sie hier aus, wie Sie den Inhalt des C-PLUG verändern wollen. Es gibt folgende Alternativen:

- Copy internal Configuration to C-PLUG and Restart
  Die im internen Flash des IE-Switches vorhandene Konfiguration wird auf den C-PLUG kopiert, anschließend erfolgt ein Neustart.
  Für diese Funktion gibt es folgenden wichtigen Einsatzfall: Der IE-Switch ist mit einem C-PLUG hochgelaufen, der eine vom IE-Switch abweichende oder fehlerhafte Konfiguration enthält. Wenn Sie nach dem Gerätehochlauf noch keine Konfigurationsänderung durchgeführt haben, können Sie mit dieser Funktion den Inhalt des C-PLUG mit der ursprünglichen Gerätekonfiguration überschreiben.
- Copy default Configuration to C-PLUG and Restart
  Eine Konfiguration mit allen Factory Default-Werten wird auf dem C-PLUG gespeichert. Anschließend erfolgt ein Neustart, wobei der IE-Switch mit diesen Defaultwerten hochläuft.
- Clean C-PLUG (Low Level Format, Configuration lost)
  Löscht alle Daten vom C-PLUG und führt eine Low Level-Formatierung durch. Es erfolgt kein automatischer Neustart und der IE-Switch zeigt einen Fehler an. Sie können diesen Fehlerstatus beseitigen, indem Sie einen Neustart durchführen oder den C-PLUG entnehmen.

Markieren Sie den notwendigen Eintrag in der Klappliste und klicken Sie die Schaltfläche "Modify, um den C-Plug in der gewünschten Form zu verändern.

Syntax Command Line Interface

Tabelle 5-14 C-PLUG Information - CLI\SYSTEM\C-PLUG>

Befehl	Beschreibung	Kommentar
info	Zeigt den aktuellen Status des C-PLUGs an.	Es werden die gleichen Informationen angezeigt, die auch auf der "Seite X-400 C-PLUG Information" des WBM enthalten sind.
copyint	Überschreibt den C-PLUG mit dem Inhalt des Hauptspeichers.	Nur Administrator. Gleiche Funktion wie der Befehl "Copy internal Configuration to C-PLUGand Restart" im WBM.
copydef	Initialisiert den C-PLUG mit den Default-Parametern.	Nur Administrator. Gleiche Funktion wie der Befehl "Copy default Configuration to C-PLUG and Restart" im WBM.
clean	Löscht alle Daten vom C-PLUG und führt eine Low Level-Formatierung durch.	Nur Administrator. Gleiche Funktion wie der Befehl "Clean C-PLUG" im WBM.

5.2.11 Geografische Koordinaten

Informationen über die geografischen Koordinaten

Im Fenster "Geographic Coordinates" können Informationen über die geografischen Koordinaten eingetragen oder ausgelesen werden. Um die geografischen Koordinaten auslesen zu können, muss der geografische Ort des Gerätes einmal in die geografischen Koordinaten korrekt eingetragen worden sein. Die Parameter der geografischen Koordinaten (Breitengrad, Längengrad und die Höhe über dem Ellipsoid gemäß WGS84) werden direkt im Fenster "Geographic Coordinates" eingetragen.

Die geografischen Koordinaten können z.B. durch einen GPS-Empfänger ermittelt werden. Meist werden die geografischen Koordinaten von diesen Geräten direkt angezeigt. Das SCALANCE Gerät stellt Ihnen nach der Konfiguration diese geografischen Daten für Management Zwecke über SNMP private MIBs, Telnet oder WEB zur Verfügung.

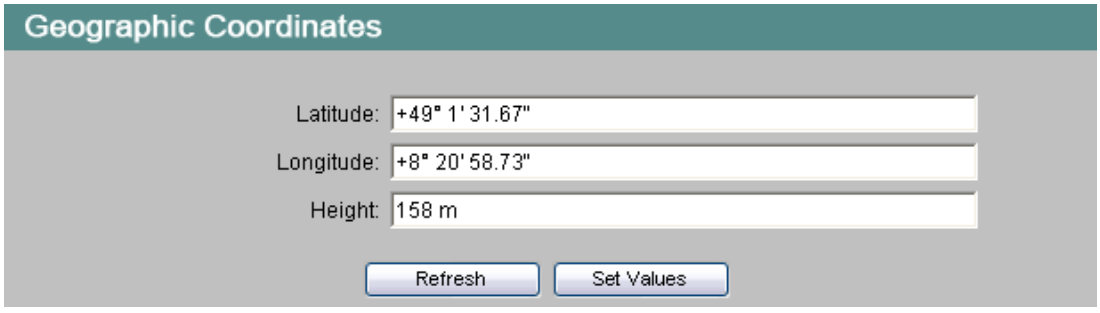


Bild 5-15 Geografische Koordinaten

Latitude (geografische Breite)
Hier wird der Wert für nördliche oder südliche Breite für den Standort des Gerätes eingegeben. z.B. +49° 1´ 31.67" bedeutet, dass sich das Gerät auf 49 Grad, 1 Bogenminute und 31.67 Bogensekunden nördliche 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).

Longitude (geografische Länge)
Hier wird der Wert für östliche oder westliche Länge für den Standort des Gerätes eingegeben. z.B. +8° 20´ 58.73" bedeutet, dass sich das Gerät auf 8 Grad, 20 Bogenminuten und 58.73 Bogensekunden östliche 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).

Height (geografische Höhe)
Hier wird der Wert für geografische Höhe über oder unter normal Null 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 werden mit einem führenden Minuszeichen dargestellt.

Eingabe der geografischen Koordinaten

Die Werte der geografischen Koordinaten können in die Textfelder eingegeben werden, z.B.

- als Grad-Angabe mit Bogenminuten und Bogensekunden in den Formaten: DD°MM.MMM´, DD°MM´SS, DD°MM´SS.SSS
- als dezimale Gradangaben in dem Format: DD.DDD°
- mit oder ohne Vorzeichen bzw. mit den angehängten Buchstaben S, N, O bzw. E, W

Syntax Command Line Interface für die geografischen Koordinaten

Tabelle 5-15 Geografische Koordinaten - CLI\SYSTEM\GEO>

Befehl	Beschreibung	Kommentar
info	Zeigt den aktuellen Status der Geografischen Koordinaten an.	-
lat [string]	Zeigt/Setzt die geografische Breitengrad- Koordinate.	Nur Administrator.
long [string]	Zeigt/Setzt die geografische Längengrad-Koordinate.	Nur Administrator.
height [string]	Zeigt/Setzt die geografische Höhe-Koordinate.	Nur Administrator.

5.3 Das Menü X-300/X-400

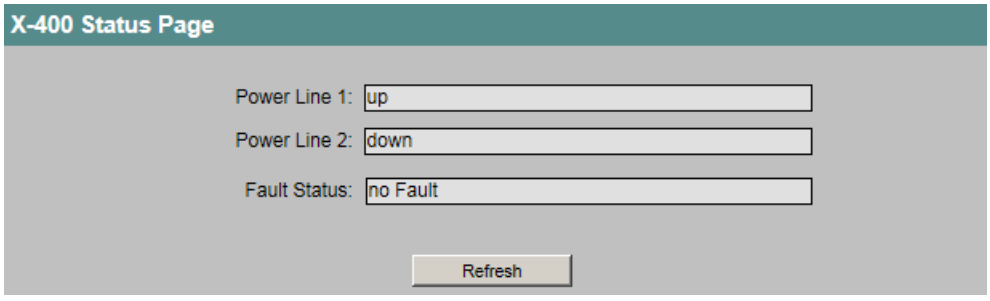
5.3.1 X-300/X-400 Status Page

Informationen über den Betriebszustand

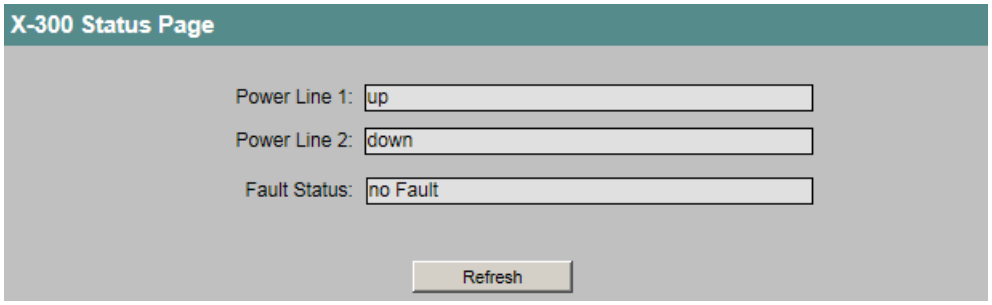
Diese Maske erscheint, wenn Sie das Ordnersymbol "X-400" bzw. "X-300" angeklickt haben.

Die Informationen auf dieser Maske sind vom IE-Switch abhängig. Bei IE-Switchen X-400 zeigt die Maske Informationen über die Spannungseinspeisung und den Fehlerstatus an. Bei IE-Switchen X-300 zeigt die Maske zusätzlich Informationen zu Ring-Redundanz und Standby Funktion.
Die Textfelder dieser Maske sind nur lesbar.

X-400 Status Page



X-300 Status Page



Redundancy Function

Die Spalte "Redundancy Function" zeigt die Rolle des Geräts innerhalb des Rings an:

- No Ring Redundancy (off)
  Der IE-Switch arbeitet ohne Redundanz-Funktion.
- HRP Client (HRP-Clt)
  Der IE-Switch arbeitet als HRP Client.
- HRP Manager (HRP-Mgr)
  Der IE-Switch arbeitet als HRP Manager.
- MRP Client (MRP-Clt)
  Der IE-Switch arbeitet als MRP Client.
- MRP Manager (MRP-Mgr)
  Der IE-Switch arbeitet als MRP Manager.

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.

- Passive
  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 (RM Function Disabled).
- Active:
  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.
- Wenn die Medienredundanz in Ringtopologien komplett abgeschaltet ist, dann werden keine Ringports angezeigt und es erscheint der Text "Ring Redundancy disabled".

Ring Ports

Zeigt die Ports an, die als Ringports verwendet werden.

Standby Function

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.

Zeigt den Status der Standby-Funktion an:

- Master
  Das Gerät hat Verbindung zum Partnergerät und arbeitet als Master. Im fehlerfreien Betrieb sind bei diesem Gerät die Standby-Ports aktiv.
- Slave
  Das Gerät hat Verbindung zum Partnergerät und arbeitet als Slave. Im fehlerfreien Betrieb sind bei diesem Gerät die Standby-Ports inaktiv.
- Disabled
  Standby-Kopplung ist deaktiviert. Das Gerät arbeitet weder als Master noch als Slave. Die Standby-Ports arbeiten als normale Ports ohne Standby-Funktion.
- Waiting for Connection...
  Es wurde noch keine Verbindung zum Partnergerät aufgenommen. Die Standby-Ports sind 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).
- Connection Lost
  Bestehende Verbindung zum Partnergerät verloren. In diesem Fall liegt entweder ein physikalischer Fehler vor (z.B. Geräteausfall, Link-Down), oder die Projektierung auf dem Partnergerät wurde geändert (z.B. anderer Verbindungsname, Standby-Kopplung deaktiviert).

Standby Status

Zeigt den Status der Standby-Ports an:

- Active
  Die Standby-Ports dieses Geräts sind aktiv, d. h. für den Frame-Verkehr freigeschaltet.
- Passive
  Die Standby-Ports dieses Geräts sind inaktiv, d. h. für den Frame-Verkehr gesperrt.

Standby Ports

Zeigt die Standby-Ports an.

Power Line 1

- Up:
  Die Versorgungsspannung 1 (Line 1) liegt an.
- Down:
  Die Versorgungsspannung 1 liegt nicht an oder die zulässige Spannung ist unterschritten.

Power Line 2

- Up:
  Die Versorgungsspannung 2 (Line 2) liegt an.
- Down:
  Die Versorgungsspannung 2 liegt nicht an oder die zulässige Spannung ist unterschritten.

Fault Status
Hier wird der Fehlerstatus für den IE-Switch angezeigt. Die folgende Tabelle enthält **beispielhaft** einige mögliche Fehlermeldungen. Wenn mehrere Fehler aufgetreten sind, werden sie im Textfeld untereinander aufgeführt. Eine vollständige Auflistung aller Fehlermeldungen finden Sie im Kapitel "Fehlermeldungen des SCALANCE X300 / X400 (Seite 403)".

Fehlermeldung	Bedeutung
Redundant power line down	Die redundante Versorgungsspannung ist ausgefallen.
Link down on monitored port	Die Verbindung an einem überwachten Port ist unterbrochen.
More than one RM in ring	Mehrere Geräte im Ring haben die Funktion des Redundanzmanagers übernommen.
Non-recoverable ring error	Diese Fehler können vom Redundanzmanager nicht aufgelöst werden. Zum Beispiel kann es zu einem einseitigen Verlust von Redundanz-Frames kommen, die vom Redundanzmanager gesendet werden, ohne dass ein Link-Down stattfindet. Auch ein fälschlich konfigurierter zweiter Redundanzmanager im Ring verursacht diese Fehlermeldung. Überprüfen Sie im ersten Fall die Konfiguration der Ring-Ports: • Passende Einstellung für die Betriebsart (Vollduplex/Halbduplex)? • Bei Lichtwellenleitern: Sende- und Empfangsleitungen richtig gesteckt? Im zweiten Fall: Konfigurieren Sie den zweiten Redundanzmanager im Ring um, sodass dieser die entsprechende Client-Rolle einnimmt oder entfernen Sie das Gerät aus dem Ring.
No Fault	Der Switch hat keinen Fehler erkannt (die Meldekontakte sprechen nicht an und die Fehler-LED leuchtet nicht).

Syntax Command Line Interface

Tabelle 5-16 X-400 Status - CLI\X-400> bzw.
X-300 Status - CLI\X-300>

Befehl	Beschreibung	Kommentar
info	Zeigt die Statusinformationen für den IE-Switch an.	-

5.3.2 Ring Redundancy

5.3.2.1 X-300/X-400 Ring Redundancy Information

Informationen zur Ring-Redundanz

Diese Maske erscheint, wenn Sie das Ordnersymbol "Ring Redundancy" angeklickt haben.

Die Maske zeigt den Status des Gerätes bezogen auf Ringredundanz, Standby Funktion und RM Observer an. Die Textfelder dieser Seite sind nur lesbar.

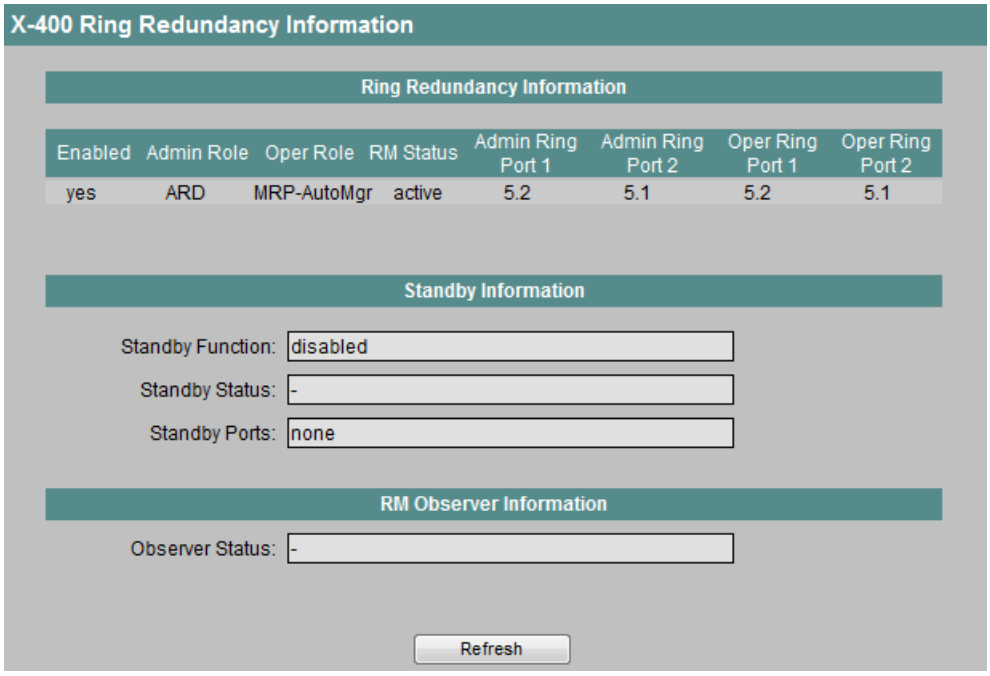


Bild 5-16 SCALANCE X-300/X-400 Ring Redundancy Information

Die Maske enthält folgende Abschnitte und Felder:

Abschnitt "Ring Redundancy Information"

Die Tabelle gliedert sich in folgende Spalten:

- **Enabled**
  Die Spalte "Enabled" zeigt an, ob der konfigurierte Ring aktiviert oder deaktiviert ist.
- **Admin Role**
  Die Spalte "Admin Role" zeigt an, welche Betriebsart Sie für des Gerät konfiguriert haben:
  - No Ring Redundancy (off)
    Der IE-Switch arbeitet ohne Redundanzfunktion.
  - HRP Client (HRP-Clt)
    Der IE-Switch arbeitet als HRP Client.
  - HRP Manager (HRP-Mgr)
    Der IE-Switch arbeitet als HRP Manager.
  - MRP Client (MRP-Clt)
    Der IE-Switch arbeitet als MRP Client.
  - MRP Manager (MRP-Mgr)
    Der IE-Switch arbeitet als MRP Manager.
- **Oper Role**
  Die Spalte "Oper Role" zeigt die Betriebsart, die des Gerät innerhalb des Rings angenommen hat:
  - No Ring Redundancy (off)
    Der IE-Switch arbeitet ohne Redundanzfunktion.
  - HRP Client (HRP-Clt)
    Der IE-Switch arbeitet als HRP Client.
  - HRP Manager (HRP-Mgr)
    Der IE-Switch arbeitet als HRP Manager.
  - MRP Client (MRP-Clt)
    Der IE-Switch arbeitet als MRP Client.
  - MRP Manager (MRP-Mgr)
    Der IE-Switch arbeitet als MRP Manager.

- **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.
  - Passive:
    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 (RM Function Disabled).
  - Active:
    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.
  - Wenn die Medienredundanz in Ringtopologien komplett abgeschaltet ist, dann werden keine Ringports angezeigt und es erscheint der Text "Ring Redundancy disabled".
- **Admin Ring Port 1 und Admin Ring Port 2**
  Die Spalten "Admin Ring Port 1" und "Admin Ring Port 2" zeigen die Ports an, die Sie als Ringports konfiguriert haben.
- **Oper Ring Port 1 und Oper Ring Port 2**
  Die Spalten "Oper Ring Port 1" und "Oper Ring Port 2" zeigen die Ports an, die als Ringports verwendet werden.

Abschnitt "Standby Information"

- **Standby Function**

  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.

  Das Anzeigefeld "Standby Function" zeigt den Status der Standby-Funktion an:

  – Master:
    Das Gerät hat Verbindung zum Partnergerät und arbeitet als Master. Im fehlerfreien Betrieb sind bei diesem Gerät die Standby-Ports aktiv.

  – Slave:
    Das Gerät hat Verbindung zum Partnergerät und arbeitet als Slave. Im fehlerfreien Betrieb sind bei diesem Gerät die Standby-Ports inaktiv.

  – Disabled:
    Standby-Kopplung ist deaktiviert. Das Gerät arbeitet weder als Master noch als Slave. Die Standby-Ports arbeiten als normale Ports ohne Standby-Funktion.

  – Waiting for Connection...:
    Es wurde noch keine Verbindung zum Partnergerät aufgenommen. Die Standby-Ports sind 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).

  – Connection Lost:
    Bestehende Verbindung zum Partnergerät verloren. In diesem Fall liegt entweder ein physikalischer Fehler vor (z.B. Geräteausfall, Link-Down), oder die Projektierung auf dem Partnergerät wurde geändert (z.B. anderer Verbindungsname, Standby-Kopplung deaktiviert).

- **Standby Status**
  Das Anzeigefeld "Standby Status" zeigt den Status der Standby-Ports an:

  – Active:
    Die Standby-Ports dieses Geräts sind aktiv, d. h. für den Frame-Verkehr freigeschaltet.

  – Passive:
    Die Standby-Ports dieses Geräts sind inaktiv, d. h. für den Frame-Verkehr gesperrt.

- **Standby Ports**
  Das Anzeigefeld "Standby Ports" zeigt die Standby-Ports an.

Abschnitt "RM Observer Information"

- **Observer Status**
  Das Anzeigefeld "Observer Status" zeigt den aktuellen Zustand des Observers an:
  - passive
    Der Observer hat keinen Fehler festgestellt.
  - active
    Der Observer hat einen Fehler festgestellt.
  - -
    Die Observer-Funktion ist ausgeschaltet.

Syntax Command Line Interface

Tabelle 5-17 X-300 Ring Redundancy - CLI\X-300\RING>
X-400 Ring Redundancy - CLI\X-400\RING>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuelle Ring-Konfiguration des IE-Switch an.	-

5.3.2.2 X-300/X-400 Ring Configuration

Media Redundancy Protocol (MRP)

Das Media Redundancy Protocol (MRP) ist ab Firmware V 3.0.0 verfügbar. Automatic Redundancy Detection (ARD) ist bei Auslieferung des IE-Switches voreingestellt. Soll das bisherige High Speed Redundancy Protocol (HRP) eingesetzt werden, muss HRP konfiguriert werden.

- Rekonfigurationszeit des Frame-Verkehrs nach einer Redundanzumschaltung bei MRP: 200 ms
- Rekonfigurationszeit des Frame-Verkehrs nach einer Redundanzumschaltung bei HRP: 300 ms

Hinweis

Nähere Informationen siehe Betriebsanleitung SCALANCE X-300 bzw. SCALANCE X-400.

Ring-Konfiguration des IE-Switch

Hinweis

Beim SCALANCE X414-3E ist eine Konfiguration über Software (CLI oder WBM) nur möglich, wenn die beiden DIP-Schalter R1 und R2 auf "ON" stehen. Andernfalls gelten die Einstellungen wie in der Betriebsanleitung "Industrial Ethernet Switches SCALANCE X-400" Kapitel "DIP-Schalter des SCALANCE X414-3E."

Hinweis

Beim SCALANCE X414-3E können die Medienredundanz in Ringtopologien und die Ringports auch über DIP-Schalter eingestellt werden.

Die Maske "Ring Configuration" erscheint, wenn Sie auf den Menüpunkt "Ring Config" geklickt haben.

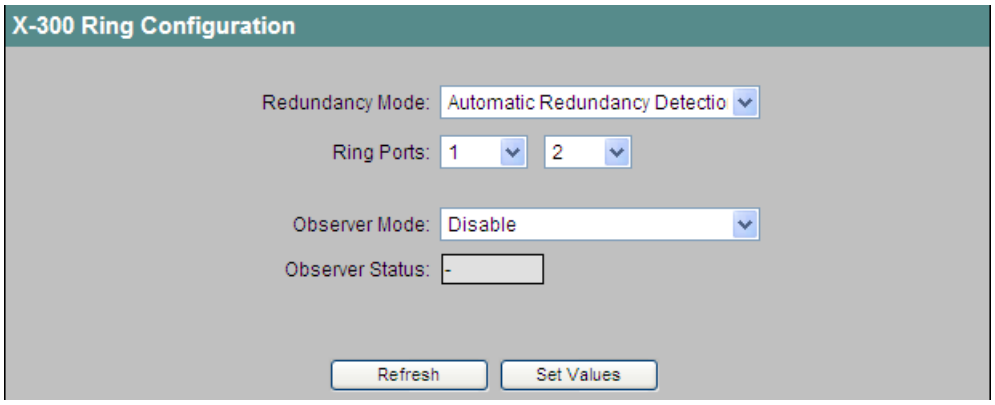


Bild 5-17 SCALANCE X-300/X-400 Ring Configuration

Redundancy Mode

Wählen Sie in der Klappliste "Redundancy Mode" aus, wie die Rolle eines Geräts innerhalb des Rings festgelegt werden soll:

- Disabled
- Automatic Redundancy Detection (ARD)
  Wählen Sie diese Einstellung, um eine automatische Konfiguration der Redundanzbetriebsart vorzunehmen.
  Im Modus "Automatic Redundancy Detection" stellt der IE-Switch 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
  Geräte mit der Einstellung "Automatic Redundancy Manager" oder "MRP Auto-Manager" handeln untereinander aus, welches Gerät die Rolle "MRP Manager" einnimmt. Dabei wird immer das Gerät mit der niedrigsten MAC-Adresse zum "MRP Manager". Im Gegensatz zur Einstellung "Automatic Redundancy Detection" sind die Geräte nicht in der Lage zu erkennen, ob ein HRP-Manager im Ring ist. Sie nehmen also nie die Rolle "HRP-Client" ein.

- MRP Client
  Hier können Sie die Rolle "MRP Client" auswählen.
  In einem Ring, dessen Geräte mit MRP projektiert sind, muss mindestens ein Gerät auf eine der Betriebsarten "Automatic Redundancy Detection" oder "MRP Auto-Manager" eingestellt sein. Bei allen übrigen Geräten kann außerdem auch die Rolle "MRP Client" eingestellt sein. Werden alle bis auf ein Gerät im Ring als "MRP Client" konfiguriert, so nimmt dieses eine Gerät automatisch die Rolle "MRP Manager" ein.
  Wählen Sie die Betriebsart "MRP Client", wenn Sie das Gerät zusammen mit Komponenten im Ring, die nicht von Siemens stammen, betreiben möchten.
- HRP Client
  Hier können Sie die Rolle "HRP Client" auswählen.
- HRP Manager
  Hier können Sie die Rolle "HRP Manager" auswählen. Bei Projektierung eines HRP-Ringes muss ein Gerät als HRP Manager eingestellt werden. Alle übrigen Geräte müssen als HRP Client konfiguriert werden.

Hinweis

Bei Wiederherstellen der Werkeinstellungen (Reset to Factory Defaults) wird die Redundanzbetriebsart Automatic Redundancy Detection (ARD) aktiv.
Außerdem wird die Konfiguration der Ringports auf die werkseitig eingestellten Ports zurückgesetzt:

- X-300: Port 9 und Port 10
- X-300 EEC: Port 8 und Port 9
- X304-2: Port 5 und 6
- X308-2M: Port 1 und Port 2
- XR324-4M: Port 1 und Port 2
- XR324-12M: Port 1.1 und Port 1.2
- X408-2: Ports 5.1 und 5.2
- X414-3E: Ports 5.1 und 5.2

Wenn zuvor andere Ports als Ringports verwendet wurden, dann kann bei entsprechendem Anschluss ein zuvor korrekt konfiguriertes Gerät kreisende Frames und damit den Ausfall des Datenverkehrs verursachen.

Ring Ports

Wählen Sie in den beiden Klapplisten die Ports aus, die als Ringports verwendet werden sollen.

Observer Mode

Hinweis

Informationen zur Observer-Funktion finden Sie im Kapitel "X-300/X-400 HRP Redundanzmanager Observer (Seite 85)".

Der Observer überwacht Fehlfunktionen des Redundanzmanagers oder Fehlkonfigurationen eines HRP-Ringes. Zusätzlich ist er in der Lage, bei erkannten Fehlern den angeschlossenen Ring zu unterbrechen (Protection Mode).

Stellen Sie über die Klappliste "Observer Mode" die Funktionalität des Observer ein:

- Disable
  Die Observer-Funktion ist ausgeschaltet.
- Protection Mode
  Die Observer-Funktion arbeitet im Protection Mode
- Restart Observer
  Die Observer-Funktion wird zurückgesetzt und der Protection Mode wird erneut aktiviert.

Observer Status

Das Anzeigefeld "Observer Status" zeigt den aktuellen Zustand des Observers an:

- Wenn der Observer keinen Fehler feststellt, erscheint "passive" in der Anzeige.
- Wenn der Observer einen Fehler feststellt, erscheint "active" in der Anzeige.
- Wenn die Observer-Funktion ausgeschaltet ist, erscheint in der Anzeige ein kleiner Strich.

Syntax Command Line Interface

Tabelle 5-18 X-300 Ring Configuration - CLI\X-300\RING>
X-400 Ring Configuration - CLI\X-400\RING>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuelle Ring-Konfiguration des IE-Switches an.	-
red [mode]	Aktiviert/Deaktiviert die Medienredundanz in Ringtopologien. Die folgenden Modi sind möglich: • D Deaktiviert die Medienredundanz in Ringtopologien . • HRPCL Der IE-Switch ist ein HRP-Client. • HRPMGR Der IE-Switch ist ein HRP-Manager. • MRPCL Der IE-Switch ist ein MRP-Client. • MRP Der IE-Switch läuft mit MRP und kann automatisch zum Redundanzmanager werden. • ARD Automatische Redundanz-Erkennung.	Nur Administrator.

Befehl	Beschreibung	Kommentar
ports [<port1> <port2>]	Legt die Ring-Ports fest. Es müssen beide Ports angegeben werden.	Nur Administrator.
observer [D|R|P]	Legt die Observer-Funktion fest: • D Deaktiviert die Observer-Funktion. • R Führt einen Restart der Observer-Funktion aus. • P Aktiviert die Observer-Funktion.	Nur Administrator.

5.3.2.3 X-300/X-400 HRP Redundanzmanager Observer

Observer im HRP-Ring

Die HRP Redundanzmanager Observer-Funktion bietet zusätzliche Möglichkeiten der Fehlerdiagnose und des Fehlerschutzes für HRP. Hiermit können Fehlfunktionen des Redundanzmanagers oder Fehlkonfigurationen eines HRP-Ringes überwacht werden. Wenn der Observer aktiviert ist (Protection Mode), dann ist er in der Lage bei erkannten Fehlern den angeschlossenen Ring zu unterbrechen. Dazu wechselt der Observer seinen Status von passiv zu aktiv und schaltet einen Ringport (Observer-Port) in den Zustand "blocking". Wenn der Fehler aufgelöst wird, schaltet der Observer den Port wieder frei.

Sollten innerhalb einer bestimmten Zeit zu viele Fehler zu schnell hintereinander auftreten, dann schaltet der Observer seinen Port nicht mehr selbstständig frei und bleibt dauerhaft im Zustand "aktiv". Dies wird durch die Fehler-LED und folgenden Meldetext signalisiert: "Observer stopped recovering because of too many (<Anzahl der Fehler>) repeated errors". Aus diesem Zustand muss der Observer nach der Fehlerbehebung durch den Anwender reaktiviert werden (Restart Observer).

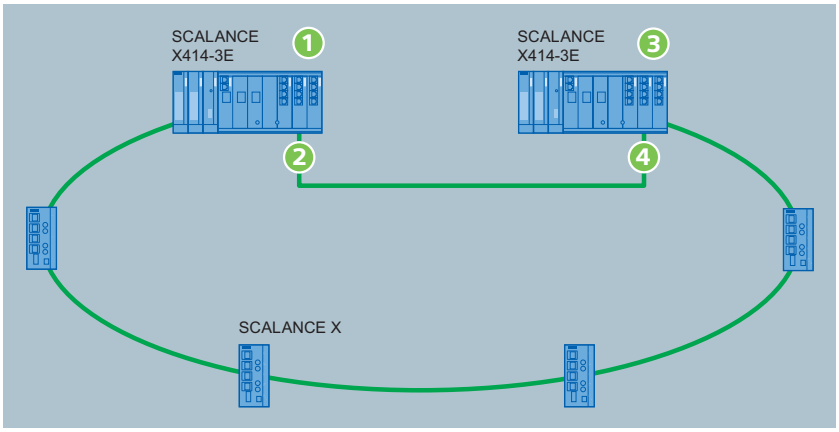
Beim Aufbau eines Rings mit HRP Redundanzmanager Observer ist Folgendes zu beachten:

- Der erst-konfigurierte Ringport vom HRP-Manager (geblockter Port) muss direkt mit dem erst-konfigurierten Ringport des Observers (Observer-Port) verbunden werden.
- An einem IE-Switch kann die Observer-Funktion über das Command Line Interface (CLI) oder das Web Based Management (WBM) aktiviert werden.
- Observer und Redundanzmanager müssen beide Firmwarestand V2.2 oder höher besitzen.

Hinweis

Um die Observer-Funktion zu nutzen, muss HRP aktiviert sein.

Beispielkonfiguration



① SCALANCE X414-3E konfiguriert als Redundanzmanager
② Geblockter Port des Redundanzmanagers
③ SCALANCE X414-3E konfiguriert als Observer
④ Erst-konfigurierter Observer-Port

Bild 5-18 Redundanter Ring mit Überwachung des Redundanzmanagers durch einen Observer

Aktivieren bzw. Deaktivieren

Die Observer-Funktion ist optional nutzbar. Im Auslieferungszustand ist sie ausgeschaltet.

Sie können die Observer-Funktion im Menü "Ring Config" konfigurieren.

Fehlermeldungen

Fehler, die vom Observer erkannt werden, werden mittels Fehler-LED, Meldekontakt und entsprechendem Meldetext signalisiert. Dies geschieht über den Meldeweg, der für das Alarmereignis "Fault State Change" konfiguriert wurde, siehe Kapitel "Agent Event Configuration".

Mögliche Meldewege sind E-Mail, Trap und/oder Event-Log-Table-Eintrag.

Die Auflistung der Meldetexte finden Sie im Anhang D "Fehlermeldungen des SCALANCE X-300 / X-400".

5.3.2.4 X-300/X-400 Standby Mask

Redundante Kopplung von Ringen

IE Switches unterstützen neben der Medienredundanz in Ringtopologien ab Firmware-Stufe 1.2 auch die redundante Kopplung von HRP-Ringen (auch unterbrochene HRP-Ringe = Linien). Bei der redundanten Kopplung werden zwei HRP-Ringe über zwei Ethernet-Verbindungen miteinander gekoppelt. Hierzu wird in einem Ring ein Master-/Slave-Gerätepaar konfiguriert, das sich gegenseitig über seine Ringports überwacht und den Datenverkehr im Fehlerfall von einer Ethernet-Verbindung (Standby-Port des Master) zu einer anderen Ethernet-Verbindung (Standby-Port des Slave) umleitet.

Weitere Informationen zur Ethernet-Verkabelung und der topologischen Platzierung von Master und Slave finden Sie in der "Betriebsanleitung Industrial Ethernet Switches SCALANCE X-400".

Hinweis

Um die Funktion Redundante Kopplung von Ringen zu nutzen, muss HRP aktiviert sein.

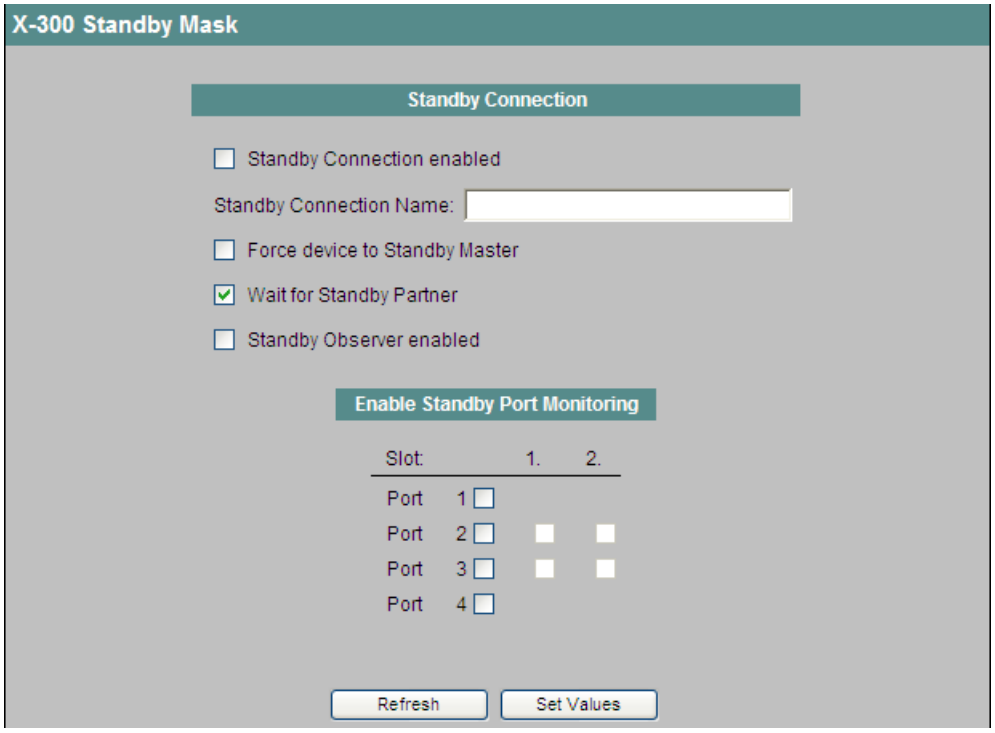


Bild 5-19 X-300 Standby Mask

Standby Connection enabled

Hier legen Sie fest, ob die Standby-Funktion aktiviert oder deaktiviert sein soll.

Standby Connection Name

Tragen Sie hier den Namen für die Standby-Verbindung ein. Durch diesen Namen wird das Master-/Slave-Gerätepaar definiert (beide müssen im selben Ring liegen). Hierzu wird der gleiche Name auf zwei Geräten eines Rings eingetragen. Der Name kann frei gewählt werden, darf im ganzen Netz jedoch nur für ein Gerätepaar verwendet werden.

Force Device to Standby Master

Wenn Sie dieses Optionskästchen markieren, wird das Gerät unabhängig von seiner MAC-Adresse als Standby-Master konfiguriert. Wenn bei keinem der beiden Geräte, bei denen die Standby-Funktion eingeschaltet ist, dieses Optionskästchen markiert ist, übernimmt im fehlerfreien Zustand das Gerät mit der höheren MAC-Adresse die Funktion des Standby-Masters. Ist diese Option bei beiden Geräten ausgewählt oder wird die Eigenschaft "Force device to Standby Master" nur von einem Gerät unterstützt, 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.

Wait for Standby Partner (nur bei SCALANCE X-300)

- 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.

Standby Observer enabled

Schalten Sie die Funktion durch Anklicken des Optionskästchen ein bzw. aus.

Nähere Information zu dieser Funktion finden Sie im Kapitel X-300/X-400 HRP Redundanzmanager Observer (Seite 85).

Enable Standby Port Monitoring

Hinweis

Wenn die Funktion Standby-Observer aktiviert ist, dann dürfen Sie nur einen einzelnen Standby-Port auswählen.

Hier legen Sie fest, welche Ports Standby-Ports sind. Standby-Ports sind an der Umleitung des Datenverkehrs beteiligt. Im ungestörten Fall sind nur die Standby-Ports des Masters aktiv und übernehmen den Datenverkehr in die angeschlossenen HRP-Ringe bzw. HRP-Linien. Fällt der Master oder die Ethernet-Verbindung (Link) eines der Standby-Ports des Masters aus, dann werden alle Standby-Ports des Masters abgeschaltet und die Standby-Ports des Slaves aktiviert. Damit wird wieder eine funktionierende Ethernet-Verbindung in die angeschlossenen Netzsegmente (HRP-Ringe bzw. HRP-Linien) hergestellt.

Hinweis

Standby Master und Standby Slave dürfen bei Kopplung zu mehreren Ringen (mehr als ein Port ist im "Standby Port Monitoring" aktiviert) nur eine Ethernet-Verbindung zu je einem Ring haben. Anderenfalls kommt es zu kreisenden Frames und damit zum Ausfall des Datenverkehrs.

Syntax Command Line Interface

Tabelle 5-19 X-400 Standby-Mask - CLI\X-400\STANDBY> bzw.
X-300 Standby-Mask - CLI\X-300\STANDBY>

Befehl	Beschreibung	Kommentar
info	Zeigt Informationen über die Standby-Konfiguration an.	-
standby [E|D]	Einschalten/Ausschalten (enable/ disable) der Standby-Funktionalität.	Nur Administrator
conname [string]	Anzeigen/Festlegen des Standby-Connection Namens.	Nur Administrator
stbports [E|D> [ports]]	Einschalten/Ausschalten (enable/ disable) der Standby-Port-Überwachung.	Nur Administrator
wait [E|D]	Legt fest, ob eine Standby-Verbindung erst aktiviert wird, wenn der Standby-Master und der Standby-Slave sowie deren Standby-Partner eine Verbindung aufgebaut haben.	Nur Administrator
observer [E|D]	Einschalten/Ausschalten (enable/ disable) der Standby-Observer-Überwachung.	Nur Administrator

Konfiguration einer redundanten Kopplung von Ringen

Gehen Sie wie folgt vor, um eine redundante Kopplung von HRP-Ringen zu konfigurieren:

1. Planen Sie, welche Geräte des Rings die Rolle des "Standby Master" und welche die Rolle des "Standby Slave" einnehmen. Planen Sie außerdem, an welche Ports von Standby Master und Standby Slave die Ethernet-Verbindungen zu den anderen Ringen gesteckt werden.
   Laut Werkeinstellungen nimmt das Gerät mit der höherwertigen MAC-Adresse die Rolle des "Standby Master" ein. Wenn beide Geräte die Funktion "Force Device to Standby Master", unterstützen, dann können Sie ein Gerät unabhängig von seiner MAC-Adresse als Standby Master konfigurieren.

   Hinweis

   Stellen Sie sicher, dass die redundanten Ethernet-Verbindungen nicht gesteckt sind, solange Sie die Konfiguration noch nicht abgeschlossen haben. Anderenfalls kommt es zu kreisenden Frames und hierdurch zum Ausfall des Datenverkehrs. Gleiches gilt für das Deaktivieren der redundanten Kopplung.

2. Legen Sie einen Namen für die Standby-Verbindung fest und tragen Sie diesen sowohl beim Standby Master- Gerät als auch beim Standby Slave-Gerät ein.

   Hinweis

   Achten Sie darauf, dass der Standby-Connection Name (für ein Gerätepaar) nur einmal im Netz verwendet wird.

3. Durch markieren der entsprechenden Optionskästchen unter "Enable Standby Port Monitoring" legen Sie sowohl beim Standby Master, als auch beim Standby Slave fest, welche Ports Standby-Ports sind.
4. Aktivieren Sie die Option "Standby Connection enabled".
5. Bestätigen Sie die Konfiguration mit "Set Values".
6. **Erst jetzt** dürfen Sie die redundanten Ethernet-Verbindungen stecken.

Hinweis

Achten Sie darauf, dass die redundanten Ethernet-Verbindungen auf die richtigen Ports, d.h. auf die projektierten Standby-Ports gesteckt werden. Anderenfalls kommt es zu kreisenden Frames und hierdurch zum Ausfall des Datenverkehrs.

5.3.2.5 X-300/X-400 Standby-Observer

Standby-Observer

Der Standby-Observer ist eine Erweiterung der einfachen redundanten Ringkopplung. Es handelt sich um eine zweite, unabhängige Standby-Kopplung an Master und Slave. Die vollständige Standby-Observer-Kopplung besteht aus zwei gegeneinander geschalteten Master-Slave-Paaren, wie nachfolgende Abbildung zeigt:

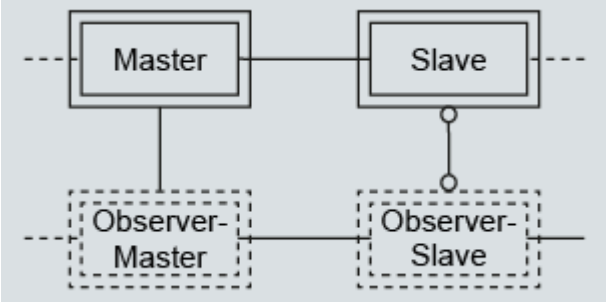


Bild 5-20 Standby-Observer-Kopplung im HRP-Ring

Beide Master-Slave-Paare sorgen eigenständig dafür, dass jeweils nur einer der beiden Koppelpfade freigeschaltet wird. Dadurch werden kreisende Frames verhindert.

Fehlfunktionen werden erkannt, indem jedes Gerät seinen aktuellen Zustand mit dem des gekoppelten Geräts vergleicht.

Um zu überprüfen, ob eine Kopplung aktiv ist, müssen Sie allerdings die Zustände beider Geräte einer Kopplung, also z. B. Slave und Observer-Slave, abfragen.

Aktivieren bzw. Deaktivieren

Die Standby-Observer-Funktion wird unterschiedlich aktiviert:

- Durch Gerätekonfiguration auf der Seite "Standby Mask" beim Master oder Slave.
  Bei der Verbindungsaufnahme zum gekoppelten Gerät startet die Observer-Funktion automatisch. Daher reicht es aus, wenn auf einem der beiden gekoppelten Geräte die Funktion aktiviert ist.
- Bei den gekoppelten Geräten "Observer-Master" bzw. "Observer-Slave" wird die Funktion automatisch beim Empfang eines Observer Frames aktiviert.

ACHTUNG
Anzahl Standby-Ports Wenn die Funktion Standby-Observer aktiviert ist, dann dürfen Sie auf der Seite "Standby Mask" nur einen einzelnen Standby-Port auswählen.

Hinweis

Unbeabsichtigtes Erzeugen von Standby-Observer-Instanzen

Wenn Sie einen Standby-Port mit aktivierter Standby-Observer-Funktion mit einem anderen Switch verbinden, aktivieren Sie dadurch eine weitere Standby-Observer-Instanz auf dem angeschlossenen Switch. Auf diese Weise können beliebig viele Standby-Observer in einer Topologie erzeugt werden.

Die Topologie des Netzes hat keinen Einfluss auf das Erzeugen der Standby-Observer-Instanzen.

Hinweis

Einschränkungen bei Linien-Topologie

Beachten Sie bei der redundanten Kopplung von Linien mit aktiver Standby-Observer-Funktion Folgendes:
Die Redundanz beschränkt sich ausschließlich auf die Koppelpfade zwischen den Linien. Wenn die Linie zwischen Standby-Master und Standby-Slave oder Observer-Master und Observer-Slave unterbrochen wird, dann bleibt der jeweilige Slave passiv. Das bedeutet, dass die Kommunikation zum Slave und zu allen mit dem Slave verbundenen Geräten unterbrochen ist.

Fehlende Unterstützung der Standby-Observer-Funktion beim Partnergerät

Wird die Standby-Observer Funktion aktiviert, obwohl die Koppelpartner (SCALANCE X-200 oder SCALANCE X-300/X-400 mit alter Firmware) diese Funktion nicht unterstützen, so ist dies eine Fehlkonfiguration. Diese Fehlkonfiguration wird von mindestens einem Standby-Observer-Gerät mit der roten Fehler-LED und folgender Fehlermeldung angezeigt: "New Fault state: "Standby observer's "master" ("slave") role conflicts with own "slave" ("master") role."

In diesem Fall müssen Sie die Standby-Observer-Funktion deaktivieren. Sollte das entsprechende Gerät nicht erreichbar sein, müssen Sie die aktive Standby-Strecke unterbrechen.

Meldungen zur Funktion Standby-Observer

In den Zustands- und Ereignismeldungen wird mit "Partner" das Gerät bezeichnet, das sich im selben Ring befindet. Demnach sind in der oben gezeigten Abbildung Master und Slave Partner bzw. Observer-Master und Observer-Slave sind Partner. Als "Observer" wird das jeweils gekoppelte Gerät im anderen Ring bezeichnet.

Folgende Zustandsmeldungen können auftreten:

- "Standby is waiting for <partner / observer>."
  Die Standby-Observer-Funktion wurde aktiviert und bis zu diesem Zeitpunkt wurde noch kein Kontakt zum Partner bzw. Observer hergestellt.
- "Standby <partner / observer> connected to <master / slave> <MAC-Adresse> <Portnummer>."
  Die Verbindung zum Partner bzw. Observer wurde hergestellt.
- "Standby <partner / observer> lost connection to <master / slave> <MAC-Adresse> <Portnummer>."
  Eine bereits bestehende Verbindung zum Partner bzw. Observer wurde unterbrochen.
- "Standby <partner / observer> conflicts with <active / passive> state."
  Der vom Partner bzw. Observer signalisierte Zustand steht im Konflikt zum eigenen aktuellen Aktiv-/Passiv-Zustand. Die Integrität des Netzwerkes bleibt erhalten. In extremen Fällen (mehrfache Fehler) kann eine Unterbrechung der Standby-Kopplung die Folge sein. Dieser Fehler deutet z. B. auf einen Verbindungsabbruch zwischen Standby-Partnern hin oder auf ein Geräteversagen.
- "Standby <partner's / observer's> state conflict resolved."
  Der oben beschriebene Zustand hat sich aufgelöst, z. B. nach der Fehlerbehebung.
- "Standby <partner / observer> conflicts with <master / slave> role."
  Die vom Partner bzw. Observer signalisierte Funktion steht im Konflikt mit der eigenen Master- / Slave-Rolle.
  Dies ist der Fall, wenn in einem Ring beide Standby-Geräte die gleiche Master- / Slave-Rolle einnehmen, oder wenn beide verbundenen Observer ungleiche Master- / Slave-Rollen einnehmen. Die Integrität des Netzwerkes bleibt erhalten. In extremen Fällen (mehrfache Fehler) kann eine Unterbrechung der Standby-Kopplung die Folge sein. Dieser Fehler deutet z. B. auf einen Verbindungsabbruch zwischen Standby-Partnern hin oder auf ein Geräteversagen.
- "Standby <partner / observer> conflicts with <master / slave> role resolved."
  Der oben beschriebene Zustand hat sich aufgelöst, z. B. nach der Fehlerbehebung.
- "Standby <partner / observer> conflicts with observer <on / off> configuration."
  Die vom Partner bzw. Observer signalisierte Konfiguration steht im Konflikt zur eigenen aktuellen Standby-Observer-Einstellung.
- "Standby <partner / observer> observer configuration conflict resolved."
  Der oben beschriebene Zustand hat sich aufgelöst, die Konfiguration des Partnes bzw. Observers passt zur eigenen aktuellen Standby-Observer-Einstellung.

- "Standby slave - at least one standby port has no link."
  Mindestens ein Standby-Port des Slaves hat keine Verbindung.
  Wenn in diesem Zustand ein Standby-Port des dazugehörigen Masters ausfällt, kann der Slave die Verbindung nicht über seinen Standby-Port herstellen.
- "Standby slave - all standby ports linked up."
  Der oben beschriebene Zustand hat sich aufgelöst, alle Standby-Ports des Slaves haben eine Verbindung.

Folgende Ereignismeldungen können auftreten:

- "Standby observer function <started / stopped>."
  Die Standby-Observer-Funktion wurde gestartet bzw. gestoppt.
- "Standby function <started / stopped>."
  Die Standby-Funktion wurde gestartet bzw. gestoppt.
- "Standby - take on the <master / slave> role."
  Die Rolle Master bzw. Slave wurde eingenommen.

5.3.3 X-300/X-400 Fault Mask

Funktion der Meldemaske

Mit der Meldemaske legen Sie fest, welche Fehlerzustände vom IE-Switch überwacht werden und zum Auslösen des Meldekontaktes führen. Mögliche Fehlerzustände sind fehlende oder zu geringe Versorgungsspannung bzw. eine unterbrochene Verbindung oder unerwartet hergestellte Verbindung zu einem Partnergerät. Das Auslösen des Meldekontakts führt auch zum Aufleuchten der Fehler-LED am Gerät und kann abhängig von der Konfiguration der Ereignistabelle einen Trap, eine E-Mail oder einen Eintrag in der Logtabelle auslösen.

Gerätebezogene Link-Überwachung der Ports

Ein IE-Switch verfügt über eine gerätebezogene Link-Überwachung. Ein Link-Up bzw. Link-Down wirkt sich auch auf das Meldesystem aus, falls der IE-Switch entsprechend konfiguriert wurde.

Einstellung der Meldemaske am Gerät

Die Meldemaske kann wahlweise auch über den SET/SEL-Taster an der Frontplatte des IE-Switches vorbelegt werden, weitere Informationen dazu finden Sie in der "Betriebsanleitung Industrial Ethernet Switches SCALANCE X-400".

Einstellungen im WBM

Im WBM können Sie die Überwachung der Spannungsversorgung und die gerätebezogene Link-Überwachung einstellen. Die Einstellungen erfolgen in drei unterschiedlichen Masken:

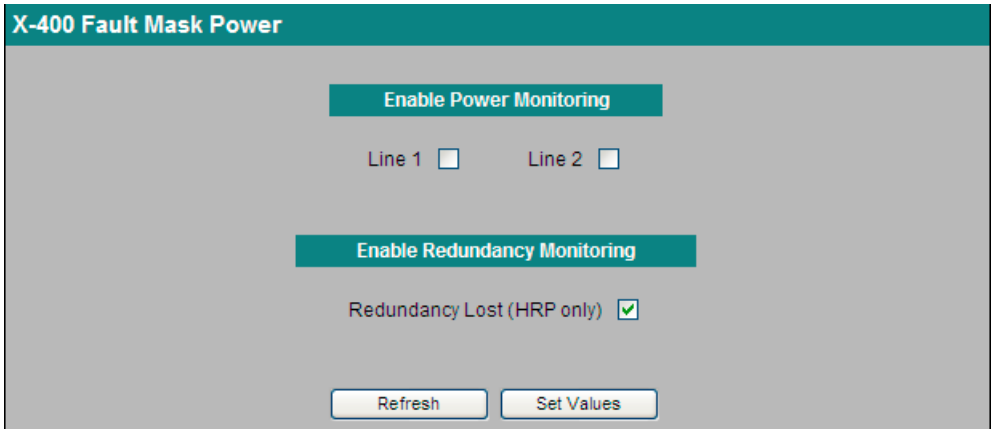


Bild 5-21 X-400 Fault Mask Power

Enable Power Monitoring

Hier legen Sie fest, welche der beiden Spannungsversorgungen Line 1 und Line 2 überwacht wird. Es wird dann ein Fehler durch das Meldesystem signalisiert, wenn an einem überwachten Anschluss (Line 1 oder Line 2) keine oder eine zu geringe Spannung (weniger als 14 V) anliegt.

Signal Redundancy Lost by Fault LED (HRP only)

Bei markiertem Optionskästchen wird ein HRP-Redundanzverlust durch die Fehler-LED des Redundanzmanagers angezeigt, sowie durch den Fehlermeldekontakt signalisiert. Den Redundanzverlust einer Standby-Kopplung zeigt der Standby-Slave durch die Fehler-LED sowie den Fehlermeldekontakt an. In der Werkseinstellung ist diese Funktion aktiviert (enable).

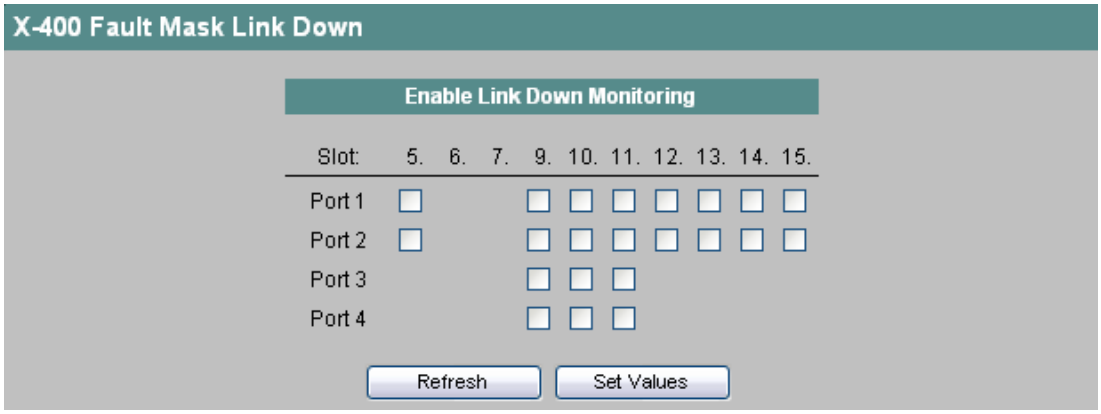


Bild 5-22 X-400-Fault Mask Link Down

Enable Link Down Monitoring

Aktivieren Sie die Optionen der Steckplätze / Ports, deren Verbindungsstatus Sie überwachen wollen. Bei aktivierter Verbindungsüberwachung wird ein Fehler signalisiert, wenn an diesem Port keine gültige Verbindung (Link) vorhanden ist, weil zum Beispiel das Kabel nicht gesteckt oder das angeschlossene Gerät abgeschaltet ist.

Ein Fehler kann, je nach Projektierung des IE-Switches, über folgende Wege signalisiert werden: Meldekontakt, Fehler-LED, SNMP-Trap, E-Mail, Eintrag in der Logtabelle, Syslog.

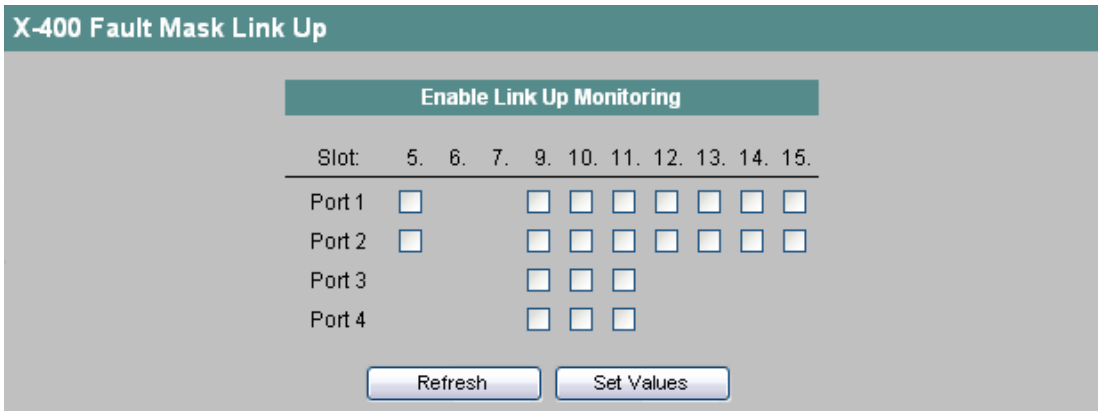


Bild 5-23 X-400 Fault Mask Link Up

Enable Link Up Monitoring
Aktivieren Sie die Optionen der Steckplätze / Ports, deren Verbindungsstatus Sie überwachen wollen. Bei aktivierter Verbindungsüberwachung wird ein Fehler signalisiert, wenn an diesem Port eine gültige Verbindung (Link) vorhanden ist, weil zum Beispiel das Kabel unerlaubt gesteckt ist.

Ein Fehler kann, je nach Projektierung des IE-Switches, über folgende Wege signalisiert werden: Meldekontakt, Fehler-LED, SNMP-Trap, E-Mail, Eintrag in der Logtabelle, Syslog.

Syntax Command Line Interface

Tabelle 5-20 X-400 Fault Mask - CLI\X-400> bzw.
X-300 Fault Mask - CLI\X-300>

Befehl	Beschreibung	Kommentar
power [<E|D> [lines]	Aktiviert / deaktiviert die Überwachung für die Spannungsversorgungsanschlüsse L1 und L2.	Nur Administrator.
hrpfled [E|D]	Aktiviert/Deaktiviert die Anzeige eines HRP-Redundanzverlusts durch die Fehler-LED sowie die Signalisierung durch den Fehlermeldekontakt.	Nur Administrator.
linkdown [<E|D> [ports]]	Aktiviert / deaktiviert die Linküberwachung (Link Monitoring) für die angegebenen Ports. Wenn Sie keine Ports angeben, werden alle Ports aktiviert / deaktiviert.	Nur Administrator. Wenn Sie mehrere Ports als Parameter angeben, müssen die einzelnen Angaben durch Leerzeichen getrennt sein.
linkup [<E|D> [ports]]	Aktiviert / deaktiviert die Linküberwachung (Link Monitoring) für die angegebenen Ports. Wenn Sie keine Ports angeben, werden alle Ports aktiviert / deaktiviert.	Nur Administrator. Wenn Sie mehrere Ports als Parameter angeben, müssen die einzelnen Angaben durch Leerzeichen getrennt sein.

5.3.4 X-300/X-400 Counters

Ansprechen des Meldekontakts und Redundanzschaltung

Mit den Zählern wird überwacht, ob und wie oft im laufenden Betrieb Störungen (z.B. Ansprechen des Meldekontakts) vorgekommen sind.

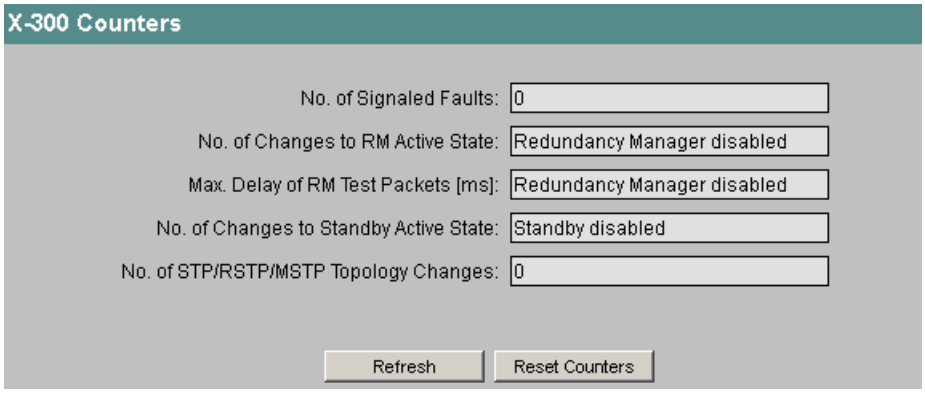


Bild 5-24 X-300 Counters

No. of Signaled Faults
Zeigt an, wie oft der Meldekontakt des IE-Switches angesprochen hat.

Der Zähler wird bei jedem Neustart des Geräts zurückgesetzt.

No. of Changes to RM Active State
Hier wird nur dann ein Wert angezeigt, wenn der IE-Switch als HRP-Manager arbeitet (siehe Kapitel "X-300/X-400 Ring Configuration").

Der Wert gibt an, wie oft der HRP-Manager in den aktiven Zustand gewechselt ist. Dieser Zustand wird eingenommen, wenn der Redundanzmanager eine Unterbrechung der Linie erkannt hat, die an die Ringports angeschlossen ist.

Der Zähler wird bei jedem Neustart des Geräts zurückgesetzt.

Max. Delay of RM Test Packets [ms]
Hier wird nur dann ein Wert angezeigt, wenn der IE-Switch als HRP-Manager arbeitet (Optionskästchen "Redundancy Manager enabled" aktiviert).

Im Redundanzmanagerbetrieb sendet ein IE-Switch Test-Frames über die Ringports an der angeschlossenen Linie von Switches und misst die Durchlaufzeit dieser Test-Frames. Es wird angezeigt, welche maximale Verzögerung bei diesen Test-Frames aufgetreten ist.

No. of Changes to Standby Active State
Hier wird nur dann ein Wert angezeigt, wenn die Standby-Funktion aktiviert ist (siehe Kapitel "X-300/X-400 Standby Mask").

Der Wert gibt an, wie oft der IE-Switch den Standby-Status von passiv nach aktiv geändert hat. Dieser Zustand wird eingenommen, wenn die Verbindung eines Standby Ports beim Standby Masters ausfällt.

Der Zähler wird bei jedem Neustart des Geräts zurückgesetzt.

No. of STP/RSTP/MSTP Topology Changes
Zeigt an, wie oft aufgrund des Spanning Tree-Mechanismus umkonfiguriert wurde.

Reset Counters
Betätigen Sie diese Schaltfläche, um die Zähler des IE-Switches zurückzusetzen. Auch ein Neustart, beispielsweise durch Unterbrechung der Spannungsversorgung des IE-Switches, bewirkt ein Zurücksetzen der Zähler.

Syntax Command Line Interface

Tabelle 5-21 X-400 Counters - CLI\X-400> bzw. X-300 Counters - CLI\X-300>

Befehl	Beschreibung	Kommentar
counters	Zeigt folgende Zählerstände an: • Changes to RM active state Gibt an, wie oft der als Redundanzmanager arbeitende IE-Switch den Ring geschlossen hat. • Max. delay of RM Test Packets Gibt die maximale Verzögerung von Test-Frames an, die vom Redundanzmanager versendet werden.	-
resetc	Setzt die IE-Switch-Zähler zurück.	Nur Administrator.

5.4 Das Menü Agent

5.4.1 Agent Configuration

Einleitung

Die Maske "Agent Configuration" erscheint, wenn Sie das Ordnersymbol "Agent" angeklickt haben. Diese Maske bietet Einstellmöglichkeiten für die IP-Adresse. Sie können festlegen, ob ein IE-Switch die IP-Adresse dynamisch bezieht oder eine feste Adresse vergeben. Außerdem können Sie hier Zugriffsmöglichkeiten auf den IE-Switch, wie zum Beispiel SSH oder RMON, aktivieren.

IP-Konfiguration für den SCALANCE X414-3E

Hier nehmen Sie die IP-Konfiguration für den SCALANCE X414-3E vor. Dabei wird zwischen den Switch-Ports (Spalte In-Band) und dem Ethernet-Port der Switch CPU (Spalte Out-Band) unterschieden.

Hinweis

Die IP-Adressen der CPU und der Switch-Ports müssen unterschiedlichen Subnetzen angehören.

IP Address

IP-Adresse des SCALANCE X414-3E bzw. des CPU-Moduls. Wenn Sie die IP-Adresse ändern, sollten Sie automatisch auf die neue Adresse geleitet werden. Falls dies nicht geschieht, geben Sie bitte die neue Adresse manuell im Web Browser ein.

Subnet Mask

Hier tragen Sie die Subnetz-Maske des SCALANCE X414-3E bzw. des CPU-Moduls ein.

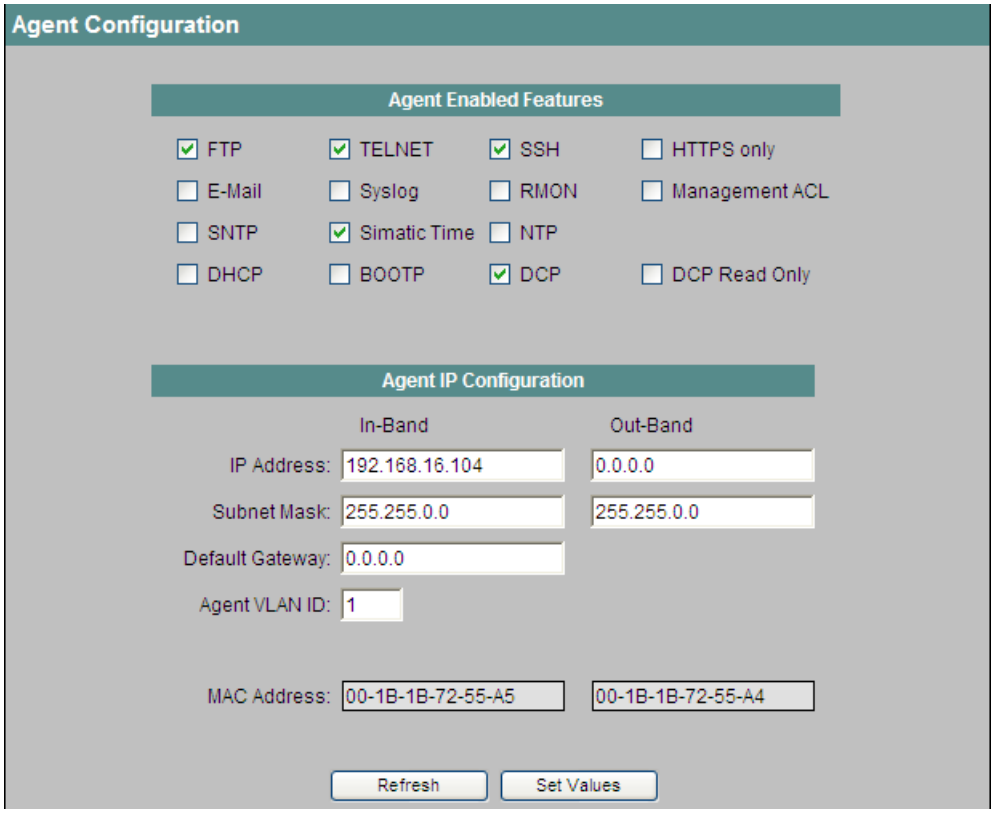


Bild 5-25 Agent Configuration SCALANCE X414-3E

IP-Konfiguration für den SCALANCE X-300/X408-2

Hier nehmen Sie die IP-Konfiguration für den SCALANCE X-300/X408-2 vor.

Hinweis

Beim SCALANCE X-300/X408-2 ist kein CPU-Ethernet-Port (Out-Band-Port) konfigurierbar. Sie können nur die Switch-Ports konfigurieren.

Subnet Mask

Hier tragen Sie die Subnetz-Maske ein.

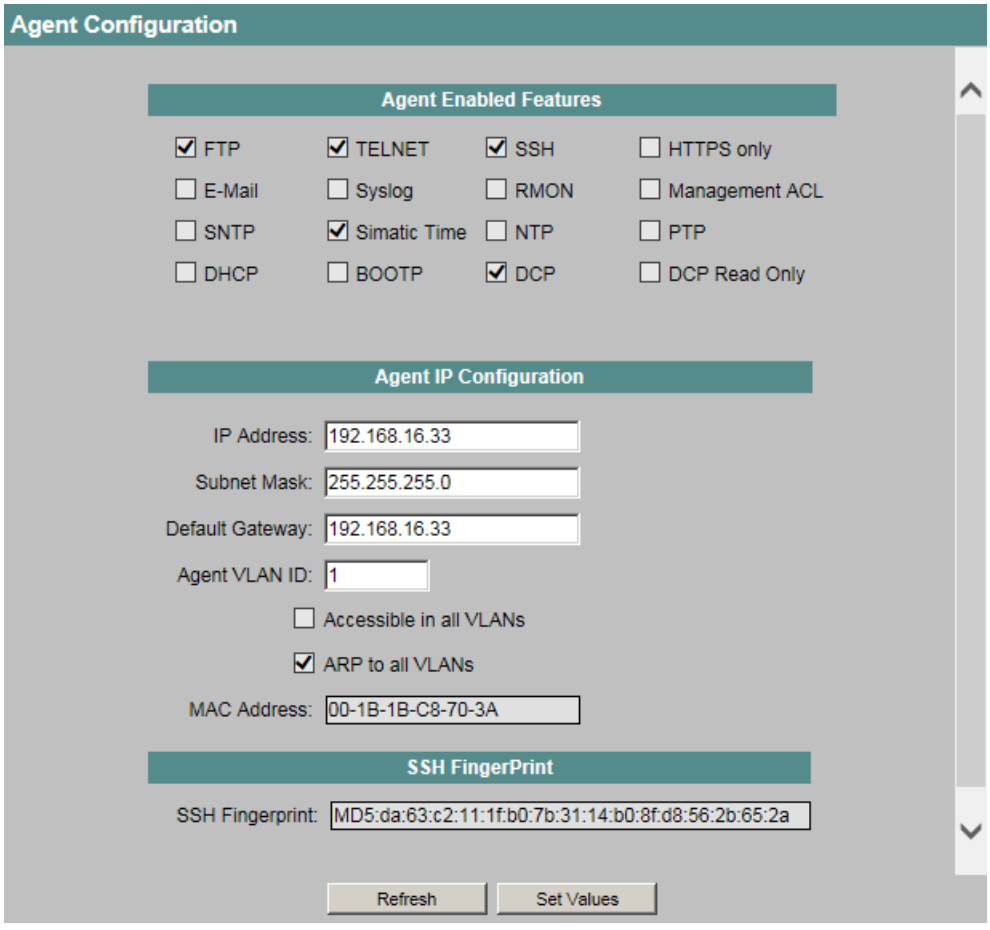


Bild 5-26 Agent Configuration SCALANCE X300

Einstellungen für den IE-Switch

FTP

Aktiviert / deaktiviert den FTP-Server. Über FTP kann ein Download der Firmware erfolgen, Detailinformationen zu diesem Thema finden Sie in Kapitel "Firmwareupdate". Außerdem können Sie über FTP die Konfigurationsdaten laden oder sichern.

Wenn ein IE-Switch über eine IP-Adresse verfügt und eine Ethernet-Verbindung zu einem PC bzw. PG besteht, müssen Sie folgende Schritte durchführen, um Konfigurationsdaten zu laden:

1. Öffnen Sie ein Konsolen-Fenster und geben Sie den Befehl ftp gefolgt von der IP-Adresse des IE-Switches ein. Beispiel:
   ftp 192.168.20.54
2. Geben Sie für Login und Passwort die gleichen Werte ein, das Sie auch für WBM und CLI verwenden.

3. Geben Sie den Befehl "put" gefolgt vom Namen der Firmwaredatei ein.
   Beispiel:
   put cfgdata.txt
4. Nach dem Abschluss des Ladevorgangs beendet der IE-Switch die FTP-Verbindung und führt einen Neustart durch.

TELNET

Hier legen Sie fest, ob der IE-Switch über TELNET erreichbar ist.

Hinweis

Ab Firmware-Version 4.1.3 ist TELNET im Auslieferungszustand oder nach dem Zurücksetzen des Geräts auf Werkseinstellungen deaktiviert. Aus Sicherheitsgründen wird die Verwendung von SSH empfohlen.

SSH

Hier legen Sie fest, ob der IE-Switch über SSH erreichbar ist.

HTTPS-Only

Hier legen Sie fest, ob der IE-Switch nur über HTTPS erreichbar sein soll. Ist diese Option nicht aktiviert, kann er auch über HTTP erreicht werden.

E-Mail

Damit aktivieren / deaktivieren Sie die E-Mail-Funktion des IE-Switch. Ausführliche Informationen zu dieser Funktionalität finden Sie im Kapitel "Menüpunkt Agent E-Mail Configuration".

Syslog

Hier legen Sie fest, ob der IE-Switch Logbucheinträge auf einem Syslog-Server ablegen soll. Ausführliche Informationen zu dieser Funktionalität finden Sie im Kapitel "Menüpunkt Agent Syslog Configuration".

RMON

Ein IE-Switch unterstützt Remote Monitoring, abgekürzt RMON. Remote Monitoring ermöglicht es, Diagnosedaten im IE-Switch zu sammeln, aufzubereiten und über SNMP von einer Netzwerkmanagementstation, die ebenfalls RMON unterstützt, auszulesen. Diese Diagnosedaten, wie zum Beispiel portbezogene Lastverläufe, ermöglichen es, Probleme im Netzwerk frühzeitig zu erkennen und zu beseitigen. Die Einstellung für RMON beeinflusst nicht die Statistik-Funktionen (siehe Kapitel "Menü Statistics").

Management ACL

Hinweis

Beachten Sie beim Aktivieren dieser Funktion: Eine fehlerhafte Projektierung auf der Seite "Management ACL Configuration" kann dazu führen, dass Sie nicht mehr auf das Gerät zugreifen können. Projektieren Sie daher eine Zugriffsregel, die Ihnen den Zugriff auf das Management erlaubt, bevor Sie die Funktion aktivieren.

Durch Anklicken des Optionskästchens aktivieren bzw. deaktivieren Sie die Zugriffskontrolle auf das Management des IE-Switches.

Im Auslieferungszustand ist die Funktion deaktiviert.

Die Zugriffsregeln werden auf der Seite "Management ACL Configuration" verwaltet, siehe Kapitel Management Access Control List (Seite 141)

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.

SNTP

Aktiviert / Deaktiviert die Synchronisation der IE-Switch-Systemzeit über einen SNTP-Server im Netz.

Unterstützte Version: SNTP V2

SIMATIC Time

Aktiviert / Deaktiviert die Synchronisation der IE-Switch-Systemzeit über das SIMATIC Zeit Protokoll.

Die Synchronisation erfolgt hier durch Multicast-Frames, die an die Adresse 09-00-06-01-FF-EF versendet werden.

Ein IE-Switch wertet SIMATIC Time Frames auch dann aus, wenn er bei einem SNTP-Server angemeldet ist.

NTP

Aktiviert / Deaktiviert die Synchronisation der IE-Switch-Systemzeit über einen NTP-Server im Netz.

Unterstützte Version: NTP V3

PTP

Hinweis

Diese Option ist nur bei PTP-fähigen Switchen vorhanden.

Aktiviert / Deaktiviert die Synchronisation der IE-Switch-Systemzeit auf die vom Master ausgesendete PTP-Zeit. Der IE-Switch muss hierzu in einem PTP-Netzwerk als "Transparent Clock" betrieben werden.

Weitere Informationen zu PTP finden Sie in den Kapiteln "Precision Time Protocol (PTP) entsprechend IEEE 1588 (Seite 256)" und "Konfiguration des Precision Time Protocols mit dem WBM (Seite 263)".

Hinweis

Zeitsprünge vermeiden

Um Zeitsprünge zu vermeiden, stellen Sie sicher, dass sich nur ein Zeitserver (SICLOCK Uhrzeitsender, (S)NTP Server, PTP Master) im Netz befindet.

Wenn sich mehrere Zeitserver im Netz befinden, aktivieren Sie nur ein Zeitprotokoll.

DHCP

Wenn Sie diese Option aktivieren, sucht der IE-Switch im Netz nach einem DHCP-Server und konfiguriert seine IP-Parameter entsprechend den Daten, die dieser Server liefert. Ausführliche Informationen zu dieser Funktionalität finden Sie im Kapitel "Adressvergabe mit dem DHCP-Client des IE-Switch".

Hinweis

Sobald die IP-Adresse einmal von einem PROFINET IO-Controller vergeben wurde, schaltet sich DHCP automatisch ab und muss bei Bedarf wieder aktiviert werden.

BOOTP

Wenn Sie diese Option aktivieren, sucht der IE-Switch im Netz nach einem BOOTP-Server und konfiguriert seine IP-Parameter entsprechend den Daten, die dieser Server liefert. Ausführliche Informationen zu dieser Funktionalität finden Sie im Kapitel "Adressvergabe mit dem BOOTP-Client des IE-Switch".

DCP

Wenn Sie diese Option aktivieren, kann das Gerät über DCP (SINEC PNI und Step7) erreicht und konfiguriert werden.

DCP Read Only

Wenn Sie diese Option aktivieren, können die Konfigurationsdaten über DCP (SINEC PNI und Step7) nur gelesen werden.

Default Gateway

Soll der IE-Switch mit Geräten (Diagnosestationen, E-Mail Server, etc.) in einem anderen Subnetz kommunizieren können, müssen Sie hier die IP-Adresse des Default-Gateways eintragen.

Agent VLAN ID

Tragen Sie hier die VLAN-ID des Agenten ein.

Accessible in all VLANs

Wird diese Option aktiviert sind alle Agent-Funktionen (Ping, Telnet, Webinterface usw.) über alle VLANs erreichbar; ist sie deaktiviert, sind die Funktionen nur über das Agent VLAN erreichbar. Die Funktion "Accessible in all VLANs" hat keine Auswirkungen auf DCP.

ARP to all VLANs

Diese Option ist nur dann relevant, wenn die Option "Accessible in all VLANs" aktiviert ist. Wird diese Option aktiviert, werden vom Management Agent ARP-Pakete in alle VLANs verschickt. Ist sie deaktviert, werden vom Management Agent ARP-Pakete nur in das VLAN geschickt, das unter "Agent VLAN ID" konfiguriert ist.

MAC Address

Die MAC-Adresse des IE-Switches bzw. des CPU-Moduls.

SSH Fingerprint (Nur beim SCALANCE X-300)

Der SSH Fingerprint ist eine verkürzte Form des öffentlichen Schlüssels, den das SSH-Protokoll zur Authentifizierung des Switches verwendet. Anhand des SSH Fingerprints können Sie überprüfen, ob der Schlüssel korrekt ist.

Syntax Command Line Interface

Tabelle 5-22 Agent Configuration - CLI\AGENT>

Befehl	Beschreibung	Kommentar
ip [IP-Adresse]	Legt die In-Band IP-Adresse für den IE-Switch fest. Die Eingabe erfolgt mit vier Dezimalziffern, durch Punkte getrennt. Zeigt ohne Angabe eines Parameters die zurzeit eingestellte In-Band IP-Adresse an.	Nur Administrator. Die IP-Adresse muss eingetragen sein, wenn Sie über einen Web Browser, TELNET oder SNMP auf einen IE-Switch zugreifen möchten. Die IP-Adress-Zuweisung kann jedoch automatisch über BOOTP/DHCP erfolgen.
subnet [Subnetzmaske]	Legt die Subnetzmaske für die In-Band-Ports des IE-Switches fest. Die Eingabe erfolgt mit vier Dezimalziffern, durch Punkte getrennt.	Nur Administrator. Die Subnetzmaske muss eingetragen sein, wenn Sie über einen Web Browser, TELNET oder SNMP auf einen IE-Switch zugreifen möchten. Die IP-Adress-Zuweisung kann jedoch automatisch über BOOTP/DHCP erfolgen.
gateway [IP-Adresse]	Legt die IP-Adresse des Default-IP-Gateways fest. Die Eingabe erfolgt mit vier Dezimalziffern, durch Punkte getrennt.	Nur Administrator. Die IP-Adresse muss eingetragen sein, wenn Sie über einen Router auf den IE-Switch zugreifen möchten und der Kommunikationspartner nicht dem gleichen Subnetz angehört wie der IE-Switch. Dabei muss das Gateway entweder im Subnetz der In-Band-IP-Adresse oder der Out-Band-IP-Adresse liegen. Die IP-Adress-Zuweisung kann jedoch automatisch über BOOTP/DHCP erfolgen.

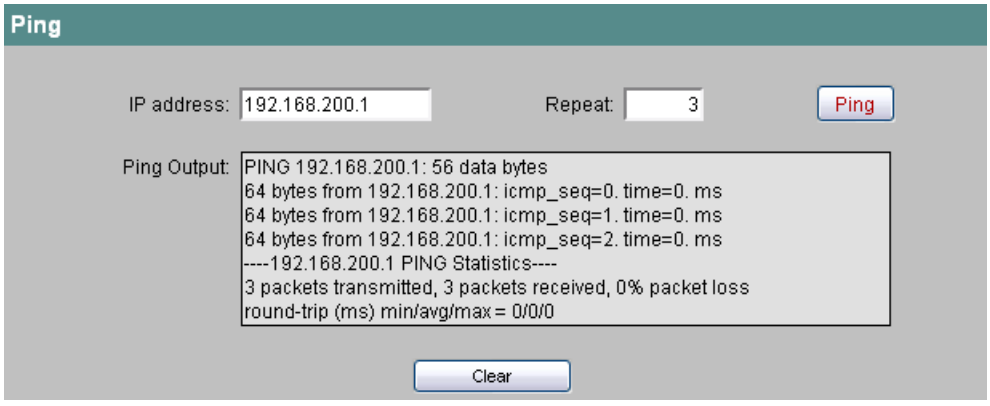
Befehl	Beschreibung	Kommentar
vid [number]	Legt die Agent-VLAN-ID fest.	Nur Administrator. Default-Wert: 1
allvlans [E|D]	Legt fest, ob die Agent-Funktionalitäten über alle VLANs erreichbar sein sollen oder nur über das Agent-VLAN.	Nur Administrator. Default-Wert: Deaktiviert
bootp [E|D]	Aktiviert/Deaktiviert BOOTP.	Nur Administrator. Default-Wert: Deaktiviert
dhcp [E|D]	Aktiviert/Deaktiviert DHCP.	Nur Administrator. Default-Wert: Aktiviert.
mail [E|D]	Aktiviert/Deaktiviert die E-Mail-Funktion.	Nur Administrator. Default-Wert: Deaktiviert.
ftp [E|D]	Aktiviert/Deaktiviert FTP.	Nur Administrator. Default-Wert: Aktiviert
dcp [D|RO|RW]	Aktiviert/Deaktiviert DCP • D Disabled • RO Read Only • RW Read Write	Nur Administrator. Default-Wert: Read Write
telnet [E|D]	Aktiviert/Deaktiviert TELNET.	Nur Administrator. Default-Wert: Aktiviert.
rmon [E|D]	Aktiviert/Deaktiviert Remote Monitoring.	Nur Administrator. Default-Wert: Deaktiviert
macl [E|D]	Aktiviert/Deaktiviert Management Access Control List.	Nur Administrator.
sntp [E|D]	Aktiviert/Deaktiviert SNTP.	Nur Administrator. Default-Wert: Deaktiviert
siclock	Aktiviert/Deaktiviert die Zeitsynchronisation über das SIMATIC Zeit Protokoll.	Nur Administrator. Default-Wert: Aktiviert
ntp [E|D]	Aktiviert/Deaktiviert NTP.	Nur Administrator. Default-Wert: Deaktiviert
ptp [E|D]	Aktiviert/Deaktiviert PTP.	Nur Administrator. Default-Wert: Deaktiviert
ping [-c Anzahl] [-s Länge] <IP-Adresse>	Sendet eine Anzahl Pakete an die angegebene IP-Adresse. Werden die Parameter für Anzahl und Länge weggelassen, sendet ein IE-Switch zehn Pakete mit einer Länge von 128 Byte. Beispiel: ping -c 5 -s 256 192.168.1.1 Es werden fünf Pakete der Länge 256 Byte an die IP-Adresse 192.168.1.1 gesendet.	-

Befehl	Beschreibung	Kommentar
ssh [E|D]	Aktiviert/Deaktiviert SSH.	Nur Administrator. Default-Wert: Aktiviert
httpso [E|D]	Legt fest, ob der IE-Switch nur über HTTPS erreichbar sein soll (deaktiviert=auch über HTTP erreichbar).	Nur Administrator. Default-Wert: Deaktiviert.
slog [E|D]	Aktiviert/Deaktiviert Syslog.	Nur Administrator.

5.4.2 Ping

Erreichbarkeit einer Adresse in einem IP-Netzwerk

Die Funktion Ping im Web Based Management hat die identische Funktion wie die gleichnamigeTerminalfunktion. Sie prüft, ob eine Adresse in einem IP-Netzwerk vorhanden ist.



IP address
Tragen Sie hier die IP-Adresse des Netzwerkgeräts ein, dessen Erreichbarkeit Sie prüfen wollen.

Repeat
Geben Sie hier ein, wie viel Datenpakete versendet werden sollen.

Ping
Klicken Sie diese Schaltfläche, um die Versendung der Datenpakete zu starten.

Ping Output
Dieses Feld zeigt die Ausgabe der Ping-Funktion an.

5.4.3 SNMP

5.4.3.1 Agent SNMP Configuration

Funktionsprinzip von SNMP

Über SNMP (Simple Network Management Protocol) kann eine Netzwerkmanagementstation SNMP-fähige Teilnehmer wie z.B. einen IE-Switch konfigurieren und überwachen. Hierzu ist im IE-Switch ein Management Agent installiert, mit dem die Managementstation Daten austauscht. Es gibt drei Pakettypen:

- Lesen (Managementstation holt Werte aus einem IE-Switch)
- Schreiben (Managementstation schreibt Werte in einen IE-Switch)
- Ereignisse an angemeldete Teilnehmer versenden (Traps)
  Der Agent versendet Meldungen an angemeldete Managementstationen.

Erweiterung von SNMPv3 (und SNMPv2) gegenüber SNMPv1

SNMPv3 (und SNMPv2) verfügt gegenüber der Ursprungsversion SNMPv1 über folgende Erweiterungen:

- Managementstationen können untereinander kommunizieren.
- Mehrstufiges Sicherheitskonzept (Verschlüsselung der Daten, Authentifizierung der Benutzer über eine im Netzwerk eindeutige SNMP-Engine-ID)
- Benutzerdefinierte Sicherheitseinstellungen

Zugriffsrechte bei SNMP

Die Festlegung von Zugriffsrechten beim SNMP-Protokoll erfolgt über den sogenannten Community-String. Ein Community-String beinhaltet die Informationen von Benutzername und Passwort in einem String. Für Lese- und Schreibrechte sind verschiedene Community-Strings definiert. Erst in einigen SNMPv2-Varianten und in SNMPv3 sind komplexere und sicherere Authentifizierungen möglich.

Hinweis

Aus Sicherheitsgründen sollten Sie nicht die Default-Werte public oder private verwenden.

Konfiguration von SNMP bei einem IE-Switch

Die Maske "Agent SNMP Configuration" erscheint, wenn Sie das Ordnersymbol "SNMP" angeklickt haben.

In der Maske SNMP Configuration treffen Sie grundlegende Einstellungen für SNMP. Aktivieren Sie die Optionen abhängig von der SNMP-Funktionalität, die Sie nutzen wollen. Für Detaileinstellungen (Traps, Groups, Users) gibt es eigene Menüpunkte im WBM. Sie können dort auch Eingaben machen, wenn Sie die Option SNMPv3 enabled nicht aktiviert haben, bleiben die Eintragungen allerdings wirkungslos.

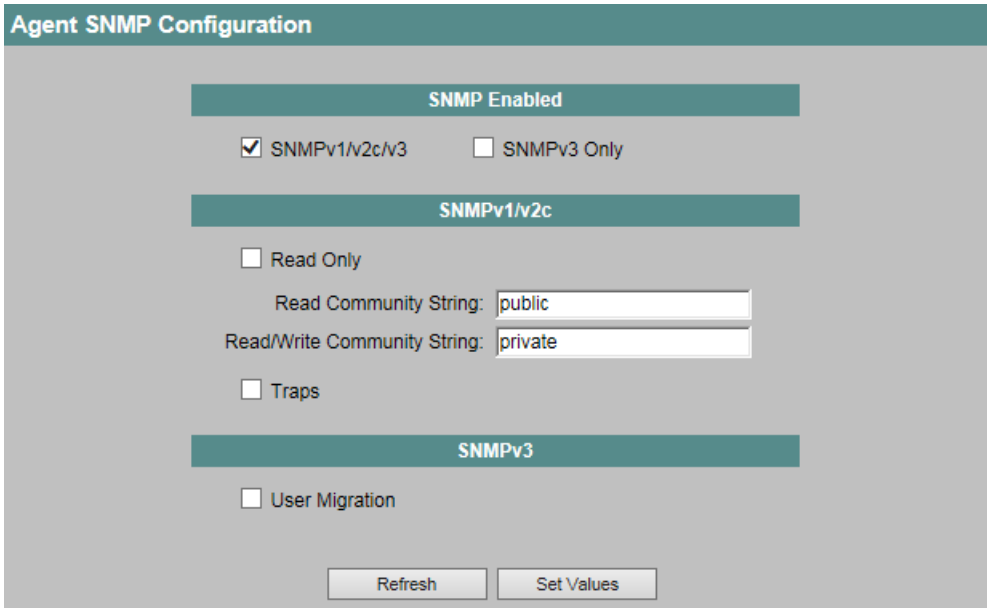


Bild 5-27 Agent SNMP Configuration

SNMP Enable

- **SNMPv1/v2/v3**
  Hier aktivieren / deaktivieren Sie SNMPv1, SNMPv2 und SNMPv3 für einen IE-Switch.
- **SNMPv3 only**
  Wenn Sie diese Option aktivieren, aktivieren Sie nur SNMPv3, die Funktionalität von SNMPv1 und SNMPv2 steht nicht zur Verfügung.

SNMPv1/V2c

- **Read Only**
  Wenn diese Option aktiviert ist, können Sie mit SNMPv1/v2c nur lesend auf SNMP-Variablen zugreifen.
- **Read Community String**
  Tragen Sie hier den Read Community String (maximal 20 Zeichen) für das SNMP-Protokoll ein.
- **Read/Write Community String**
  Tragen Sie hier den Write Community String (maximal 20 Zeichen) für das SNMP-Protokoll ein.
- **Traps**
  Damit aktivieren / deaktivieren Sie das Versenden von SNMPv1/v2c-Traps.

SNMPv3

Mit der Einführung von SNMPv3 können Sie User-Konfigurationen nicht mehr ohne Weiteres auf andere Geräte übertragen, z. B. indem Sie eine Konfigurationsdatei laden oder den C-PLUG austauschen.

Das SNMPv3-Protokoll verwendet gemäß des Standards eine eindeutige SNMP-Engine-ID als internen Bezeichner für einen SNMP-Agenten. Diese ID muss im Netzwerk eindeutig sein. Sie wird verwendet, um die Zugangsdaten von SNMPv3 Usern zu authentifizieren und zu verschlüsseln.

Abhängig davon, ob Sie die Funktion "SNMPv3 User Migration" aktiviert oder deaktiviert haben, wird die SNMP-Engine-ID unterschiedlich generiert.

- **User Migration** (SCALANCE X-300/X408-2)
  - **Aktiviert**
    Wenn die Funktion aktiviert ist, wird eine SNMP-Engine-ID generiert, die migriert werden kann. Sie können konfigurierte SNMPv3 User auf ein anderes Gerät übertragen.
    Wenn Sie diese Funktion aktivieren und die Konfiguration des Geräts auf ein anderes Gerät laden, bleiben konfigurierte SNMPv3 User 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-User-Konfiguration nicht auf andere Geräte übertragen.
    Wenn Sie die Konfiguration des Geräts auf ein anderes Gerät laden, werden alle konfigurierten SNMPv3 User gelöscht.

Hinweis

Immer wenn Sie die Funktion "SNMPv3 User Migration" aktivieren bzw. deaktivieren, werden die konfigurierten SNMPv3 User gelöscht. Wenn Sie die Funktion "SNMPv3 User Migration" deaktivieren, wird die SNMP-Engine-ID auf einen gerätespezifischen Wert zurückzusetzen.

Einschränkung bei der Verwendung der Funktion
Verwenden Sie die Funktion "SNMPv3 User Migration" nur, um im Ersatzteilfall Ihre konfigurierten SNMPv3 User auf ein Ersatzgerät zu übertragen.
Verwenden Sie die Funktion nicht, um konfigurierte SNMPv3 User auf mehrere Geräte zu übertragen. Wenn Sie eine Konfiguration mit angelegten SNMPv3 Usern in mehrere Geräte laden, verwenden diese Geräte hierdurch die gleiche SNMP-Engine-ID. Wenn Sie diese Geräte im gleichen Netzwerk verwenden, widerspricht Ihre Konfiguration dem SNMP-Standard.
Default-Wert

- Nach einem Upgrade auf die Firmware-Version 4.0.2:
  Deaktiviert
- Nach dem Zurücksetzen auf werkseitige Voreinstellungen (Reset to Factory Defaults):
  Aktiviert

Kompatibilität mit Vorgängerprodukten
Sie können SNMPv3 User nur auf ein anderes Gerät übertragen, wenn Sie die User als migrierbare User erstellt haben. Um einen migrierbaren User zu erstellen, muss die Funktion "SNMPv3 User Migration" aktiviert sein, wenn Sie den User erstellen.
Wenn Sie SNMPv3 User mit einer Firmware-Version < 4.0.2 erstellt haben, werden diese User gelöscht, wenn Sie die Konfiguration auf ein anderes Gerät übertragen.

Syntax Command Line Interface

Hinweis

Eingabe von Leerzeichen bei CLI-Befehlen, die SNMP betreffen

Soll ein Leerzeichen als Bestandteil eines Parameters eingegeben werden, muss dieses durch ein Tilde-Zeichen (~) ersetzt werden.

Beispiel:
Wenn ein SNMP-Benutzername aus zwei durch ein Leerzeichen getrennten Strings besteht, ist folgende Eingabe notwendig:
<String1>~<String2>

Tabelle 5-23 Agent SNMP Configuration - CLI\AGENT\SNMP>

Befehl	Beschreibung	Kommentar
snmp [D|3|A]	Deaktiviert / Aktiviert SNMP. Die Parameter haben folgende Bedeutung: • D Schaltet SNMP aus. • 3 Aktiviert nur SNMPv3. • A Aktiviert SNMPv1, SNMPv2 und SNMPv3.	Nur Administrator. Default-Wert: SNMPv1, v2 und v3 sind aktiviert.
getcomm [String]	Legt den Read-Community-String fest (maximale Länge 20 Zeichen). Die Voreinstellung ist "public".	Nur Administrator.
setcomm [String]	Legt den Read/Write-Community-String fest (maximale Länge 20 Zeichen). Die Voreinstellung ist "private".	Nur Administrator.
traps [E|D]	Aktiviert / Deaktiviert SNMPv1-Traps.	Nur Administrator.
usermigr [E|D]	Aktiviert / Deaktiviert die Übertragung von konfigurierten SNMPv3 Usern per Konfigurationsdatei/C-PLUG im Ersatzteilfall.	Nur Administrator. Nur bei SCALANCE X-300/X408-2 Default-Wert: • Nach einem Upgrade auf die Firmware-Version 4.0.2: Deaktiviert • Nach dem Zurücksetzen auf werkseitige Voreinstellungen (Reset to Factory Defaults): Aktiviert

5.4.3.2 SNMPv1 Trap Configuration

SNMP-Traps bei Alarmereignissen

Beim Eintreten eines Alarmereignisses kann ein IE-Switch Traps (Alarm-Frames) an bis zu 10 verschiedene (Netzwerkmanagement-) Stationen gleichzeitig senden. Es werden nur bei solchen Ereignissen Traps gesendet, für die das im Menüpunkt Agent Event Configuration (siehe Kapitel "Agent Event Configuration") festgelegt wurde.

Hinweis

Traps werden nur dann versendet, wenn im Menü "SNMP Configuration" die Option "Traps" aktiviert wurde.

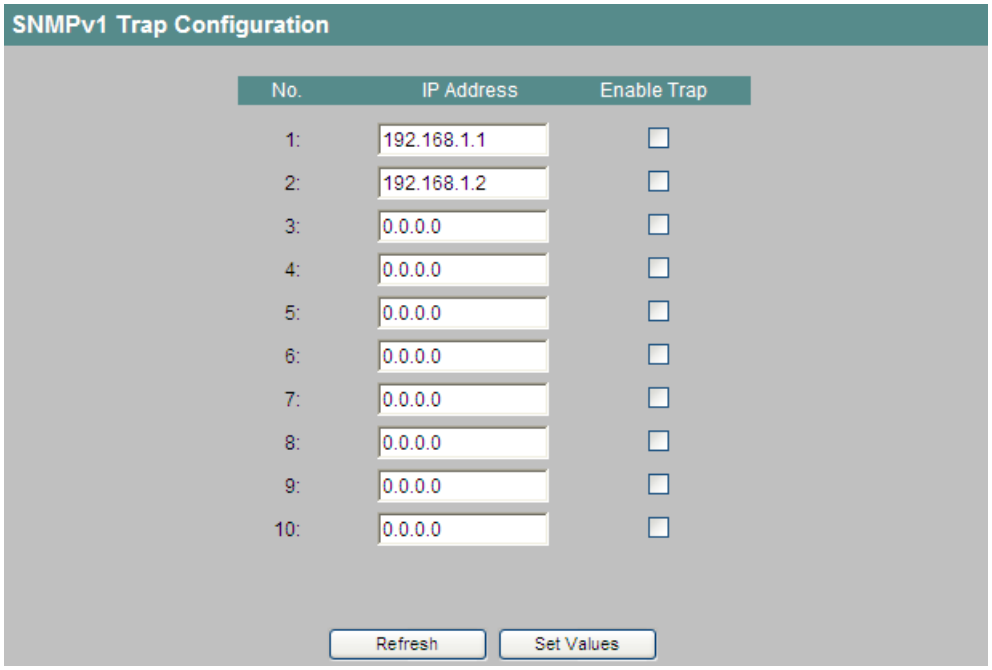


Bild 5-28 SNMPv1 Trap Configuration

IP-Adresse
Hier tragen Sie die Adressen der Stationen ein, an die ein IE-Switch Traps senden soll.

Enable Trap
Klicken Sie die Optionskästchen neben den IP-Adressen an, um das Versenden von Traps an die entsprechenden Stationen zu aktivieren.

Syntax Command Line Interface

Tabelle 5-24 SNMPv1 Trap Configuration - CLI\AGENT\SNMP\TRAPCONF>

Befehl	Beschreibung	Kommentar
Info	Zeigt die aktuelle Trap-Konfiguration.	-
ip <entry> <ip>	Legt die IP-Adresse des Trap-Empfängers entry (entry zwischen 1 und 10) fest.	Nur Administrator. Default-Wert: 0.0.0.0
state <entry><E|D>	Aktiviert/Deaktiviert die Versendung von Traps an den Empfänger entry (entry zwischen 1 und 10)	Nur Administrator. Default-Wert: D

5.4.3.3 SNMPv3 Group Configuration

Sicherheitseinstellungen und Rechtevergabe

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

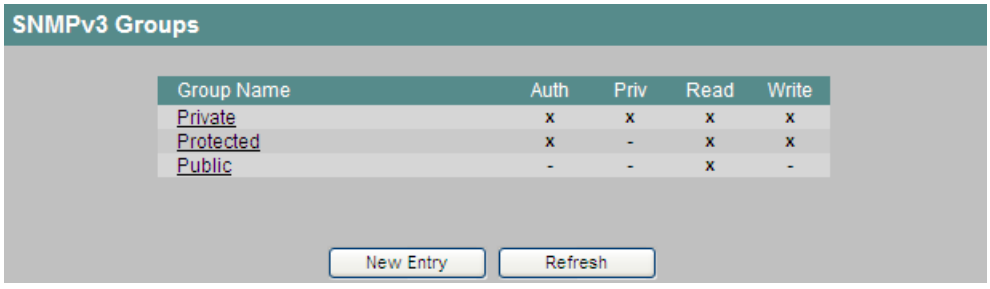


Bild 5-29 SNMPv3 Groups

Group Name

Hier sind alle Gruppen-Namen aufgeführt, die bisher definiert wurden. Wenn Sie einen Gruppen-Namen anklicken, öffnet sich ein neues Fenster, wo Sie die Parameter einer Gruppe ändern können.

Auth
Ein Kreuz in dieser Spalte zeigt an, dass für die entsprechende Gruppe die Authentifizierung aktiviert ist.

Priv
Ein Kreuz in dieser Spalte zeigt an, dass für die entsprechende Gruppe die Verschlüsselung aktiviert ist.

Read
Ein Kreuz in dieser Spalte zeigt an, dass für die entsprechende Gruppe der Lesezugriff aktiviert ist.

Write
Ein Kreuz in dieser Spalte zeigt an, dass für die entsprechende Gruppe der Schreibzugriff aktiviert ist.

New Entry
Klicken Sie diese Schaltfläche, um eine neue Gruppe anzulegen.

Konfiguration der SNMPv3-Gruppen

Nach dem Anklicken eines Gruppen-Namens gelangen Sie zur Seite für die Konfiguration der Gruppen-Eigenschaften:

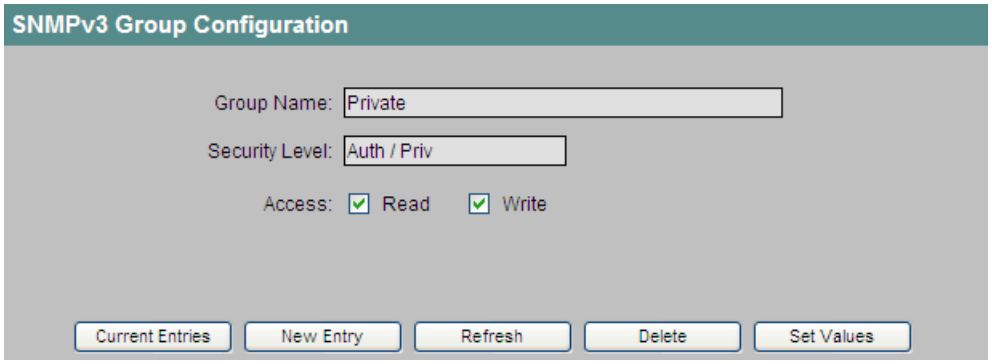


Bild 5-30 SNMPv3 Group Configuration

Group Name
Hier wird der Name der Gruppe angezeigt. Dieses Textfeld ist nur lesbar, den Gruppen-Namen können Sie nur beim Anlegen einer Gruppe vergeben und nachträglich nicht mehr ändern.

Security Level
Dieses Textfeld zeigt die Authentifizierung und die Verschlüsselung an. Bei den Sicherheitsstufen gibt es die folgenden drei Möglichkeiten:

Sicherheitsstufe	Besonderheiten	Kommentar
no Auth / no Priv	Keine Authentifizierung, keine Verschlüsselung.	-
Auth	Authentifizierung mit dem MD5 oder SHA-Algorithmus, keine Verschlüsselung.	-
Auth / Priv	Authentifizierung mit dem MD5 oder SHA-Algorithmus, Verschlüsselung mit dem DES3-Algorithmus.	-

Read und Write
Hier aktivieren bzw. deaktivieren Sie den Schreibzugriff, den Lesezugriff und die Benachrichtigung.

Current Entries
Durch Anklicken dieser Schaltfläche gelangen Sie zurück zur Liste mit den SNMPv3-Gruppen.

New Entry
Nach dem Anklicken dieser Schaltfläche erscheint die Seite zum Anlegen einer neuen Gruppe.

Delete
Klicken Sie diese Schaltfläche, um eine Gruppe zu löschen. Falls in der Gruppe bereits Mitglieder eingetragen sind, können Sie die Gruppe nicht löschen und auch eine Veränderung der Sicherheitsstufe für die Gruppe ist nicht möglich.

Anlegen einer neuen Gruppe

Nach dem Anklicken der Schaltfläche "New Entry" im Fenster "SNMPv3 Group Configuration" erscheint das Fenster zum Anlegen einer neuen Gruppe:

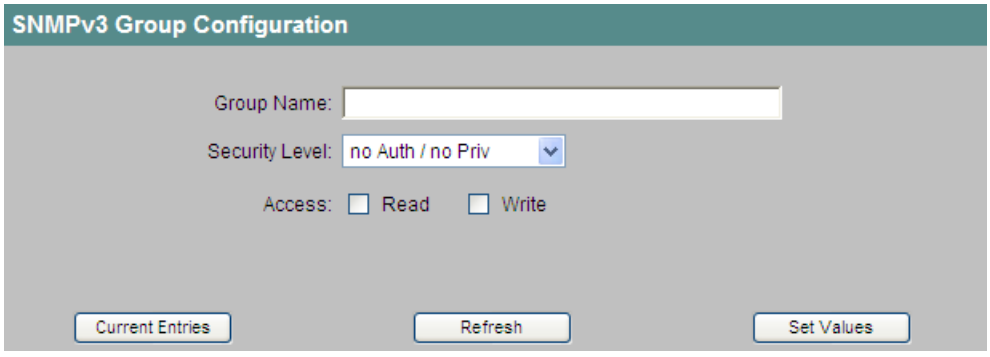


Bild 5-31 SNMPv3 Group Configuration II

Group Name
Geben Sie hier den Namen für die Gruppe ein. Dieser Name muss mindestens zwei Zeichen lang sein, die maximale Länge beträgt 32 Zeichen.

Security Level
Wählen Sie hier aus, welche Sicherheitsstufe für die Gruppe gelten soll.

Read und **Write**
Legen Sie hier fest, ob die Mitglieder der Gruppe Lesezugriff, Schreibzugriff oder beides haben sollen.

Syntax Command Line Interface

Tabelle 5-25 SNMPv3 Groups - CLI\AGENT\SNMP\GROUP>

Befehl	Beschreibung	Kommentar
info	Zeigt eine Liste aller SNMPv3-Gruppen an.	-
add <Gruppenname> [Sicherheitsstufe]	Fügt eine neue SNMPv3-Gruppe hinzu. Die Sicherheitsstufe legen Sie mit folgenden Parametern fest: • NOAUTH Keine Authentifizierung, keine Verschlüsselung. • AUTH Authentifizierung mit dem MD5 oder SHA-Algorithmus, keine Verschlüsselung. • PRIV Authentifizierung mit dem MD5 oder SHA-Algorithmus, Verschlüsselung mit dem DES3 Algorithmus.	Nur Administrator.
access <Gruppenname> <Zugriffsrechte>	Setzt die Zugriffsrechte. Für die Festlegung des Schreib- und Lesezugriffs gibt es folgende Parameter: • - Weder Schreib- noch Lesezugriff erlauben. • RO Nur Lesezugriff erlauben. • RW Lese- und Schreibzugriff erlauben.	Nur Administrator.
delete <Gruppenname>	Löscht die SNMPv3-Gruppe mit dem angegebenen Namen.	Nur Administrator.
clearall	Löscht alle SNMPv3-Gruppen aus der Liste.	Nur Administrator.

5.4.3.4 SNMPv3 Users Configuration

Benutzerspezifische Sicherheitseinstellungen

Das benutzerbasierte Sicherheitsmodell arbeitet mit dem Konzept des Benutzernamen, d. h. jeder Frame wird mit einer Benutzerkennung versehen. Diesen Benutzernamen und die betreffenden Sicherheitseinstellungen überprüfen sowohl der Absender wie auch der Empfänger. Ein Benutzer wird durch folgende Parameter definiert:

- Benutzername:
  Ein frei wählbarer Name.
- Sicherheitsnamen:
  Name, der dem Authentifizierungs-Protokoll entspricht.

- Authentication Protocol:
  Art des Authentifizierungs-Protokolls.
- Authentication Key:
  Der private Schlüssel des Authentifizierungs-Protokolls.
- Privacy Protocol:
  Typ der Verschlüsselung.
- Privacy Key:
  Das private Kennwort für die Verschlüsselung.

Diese Seite zeigt die SNMPv3-Benutzer an. In der Spalte "User Name" wird der Benutzername angezeigt, in der Spalte "Group" der Name der Gruppe, der der Benutzer zugeordnet ist:

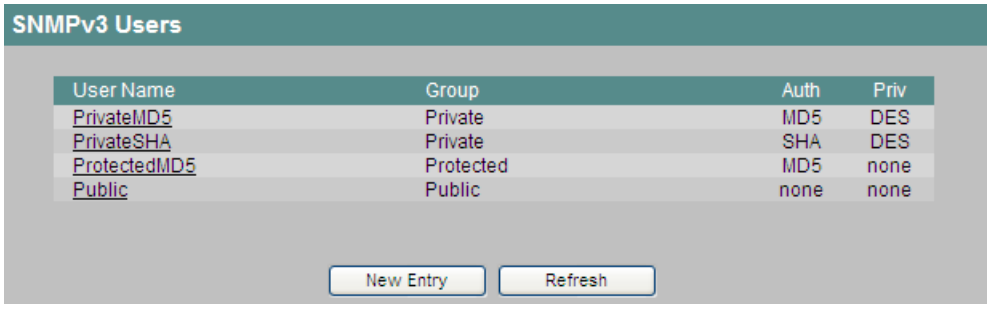


Bild 5-32 SNMPv3 Users

User Name
Hier sind alle Benutzernamen aufgeführt, die bisher definiert wurden. Wenn Sie einen Benutzernamen anklicken, öffnet sich ein neues Fenster, wo Sie die Passwörter eines Benutzers ändern können.

Group
Die Einträge dieser Spalte zeigen an, welcher Gruppe ein Benutzer angehört.

Auth
Diese Spalte zeigt den Authentifizierungsalgorithmus an, der für den Benutzer verwendet wird.

Priv
Diese Spalte zeigt das Verschlüsselungsverfahren an, das für den Benutzer verwendet wird.

New Entry
Klicken Sie diese Schaltfläche, um einen neuen Benutzer anzulegen.

Konfiguration der SNMPv3-Benutzer

Nach dem Anklicken eines Benutzer-Namens gelangen Sie zur Seite für die Benutzer-Konfiguration:

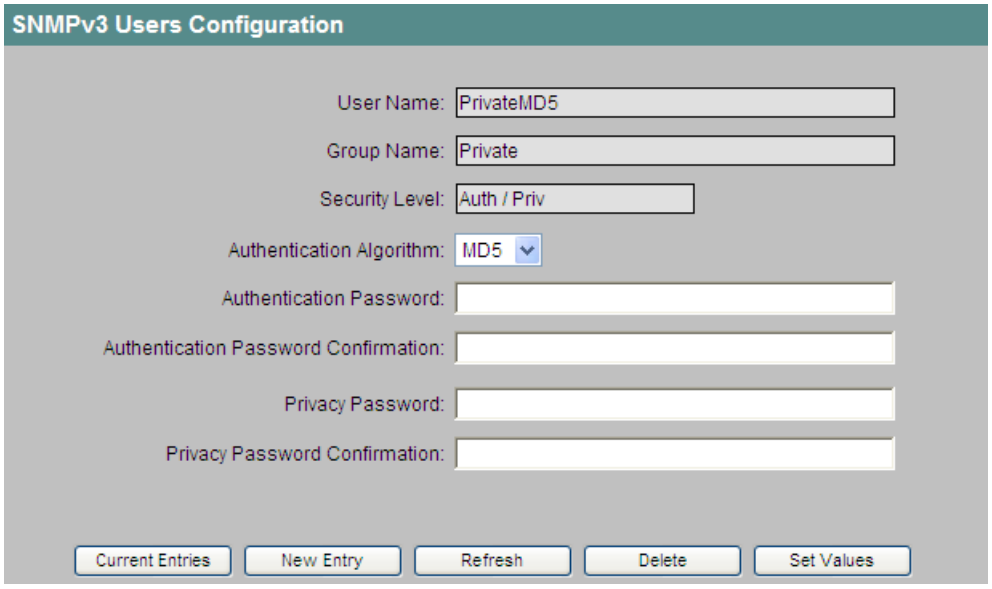


Bild 5-33 SNMPv3 Users Configuration

User Name
Hier wird der Benutzername angezeigt. Dieses Feld ist nur lesbar, weil der Name nach dem Anlegen eines Benutzers nicht mehr änderbar ist.

Group Name
Dieses Feld zeigt die Gruppe an, die dem Benutzer zugeordnet wurde.

Falls für die ausgewählte Gruppe eine Authentifizierung notwendig ist, müssen Sie einen Authentifizierungs-Algorithmus auswählen und das Authentifizierungskennwort eingeben. Falls für die Gruppe zusätzlich noch Verschlüsselung festgelegt wurde, müssen Sie auch das Verschlüsselungskennwort eingegeben.

Security Level
Hier wird die Sicherheitsstufe (Authentifizierung, Verschlüsselung) angezeigt, die für die Gruppe gilt. Die verschiedenen Sicherheitsstufen sind auf der Seite 70 beschrieben.

Authentication Algorithm
Sie können zwischen dem MD5- und dem SHA-Algorithmus auswählen.

Authentication password / Authentication password confirmation
Geben Sie in diese Felder das Authentifizierungs-Kennwort ein. Das Kennwort darf maximal 32 Zeichen lang sein. Es können alle verfügbaren Zeichen verwendet werden.

Privacy password / Privacy password confirmation
Geben Sie in diese Felder das Verschlüsselungs-Kennwort ein. Das Kennwort darf maximal 32 Zeichen lang sein.

Current Entries
Durch Anklicken dieser Schaltfläche gelangen Sie zurück zur Liste mit den SNMPv3-Benutzern.

New Entry
Sie legen einen neuen Benutzer an, indem Sie die Schaltfläche New Entry anklicken und den Gruppennamen und die Gruppenzugehörigkeit festlegen.

Delete
Klicken Sie diese Schaltfläche, um einen Benutzer zu löschen.

Anlegen eines neuen Benutzers

Nach dem Anklicken der Schaltfläche "New Entry" im Fenster "SNMPv3 Users Configuration" erscheint das Fenster zum Anlegen eines neuen Benutzers:

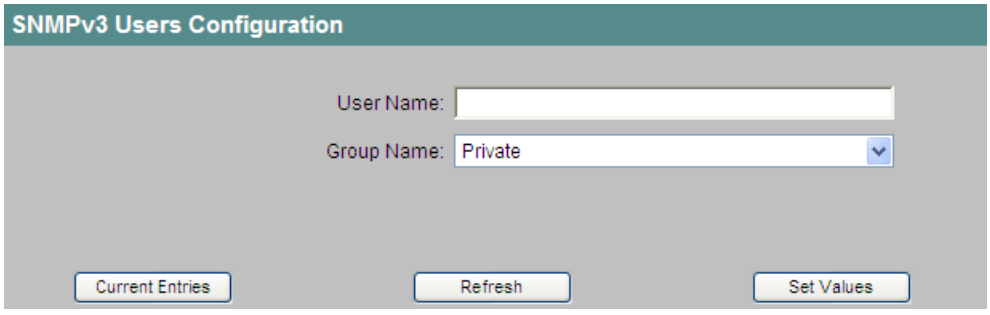


Bild 5-34 SNMPv3 Users Configuration II

User Name
Tragen Sie hier den Namen des neuen Benutzers ein.

Group Name
Wählen Sie hier aus, welcher Gruppe der neue Benutzer angehören soll.

Syntax Command Line Interface

Tabelle 5-26 SNMPv3 Users - CLI\AGENT\SNMP\USER>

Befehl	Beschreibung	Kommentar
info	Zeigt eine Liste aller SNMPv3-Benutzer an.	-
add <Benutzername> <Gruppenname>	Fügt einen neuen SNMPv3-Benutzer zu einer Gruppe hinzu. Falls für die Gruppe eine Authentifizierung notwendig ist, wird als Algorithmus per default MD5 ausgewählt.	Nur Administrator.
auth <Benutzername><MD5|SHA>	Ändert den Authentifizierungs-Algorithmus (MD5 bzw. SHA) eines SNMPv3-Benutzers. Dieser Befehl kann nur auf Mitglieder einer Gruppe angewendet werden, für diese Authentifizierung notwendig ist.	Nur Administrator.

Befehl	Beschreibung	Kommentar
pass <Benutzername><Authent.-Kennwort> [Verschl.-Kennwort]	Ändert die Kennwörter eines SNMPv3-Benutzers (maximale Länge 32 Zeichen). Dieser Befehl kann nur auf Mitglieder einer Gruppe angewendet werden, für diese Authentifizierung notwendig ist. Das Verschlüsselungs-Kennwort kann nur wenn es notwendig ist angegeben werden.	Nur Administrator.
delete <Benutzername>	Löscht den SNMPv3-Benutzer mit dem angegebenen Namen.	Nur Administrator.
clearall	Löscht alle SNMPv3-Benutzer aus der Liste.	Nur Administrator.

5.4.4 Agent Timeout Configuration

Einstellung der Timeout

Hier können die Zeiten eingestellt werden, nach denen automatisch ein Logout im WBM oder CLI erfolgt.

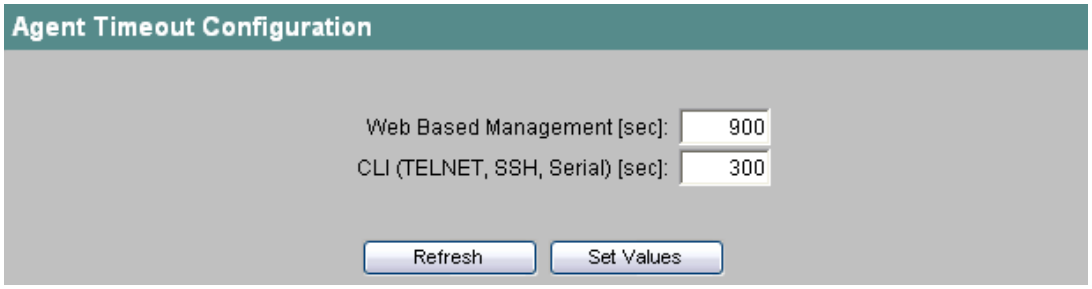


Bild 5-35 Agent Timeout Configuration

Web Based Management (sec)
Hier geben Sie den WBM-Timeout an.
Erlaubte Werte für den WBM-Timeout: 60-3600 (Sekunden)

0 bedeutet: Es erfolgt kein automatischer Logout.

CLI (TELNET, SSH, Serial) (sec)
Hier geben Sie den CLI-Timeout an.
Erlaubte Werte für den CLI-Timeout: 60-600 Sekunden

0 bedeutet: Es erfolgt kein automatischer Logout.

Syntax Command Line Interface

Tabelle 5-27 CLI\AGENT\TIMEOUT>

Befehl	Beschreibung	Kommentar
info	Zeigt aktuelle Timeout-Einstellungen an.	-
wbmtime	Stellt den WBM-Timeout (in Sekunden) ein.	Nur Administrator. Defaultwert: 900
clitime	Stellt den CLI-Timeout (in Sekunden) ein.	Nur Administrator. Defaultwert 300

5.4.5 Agent Event Configuration

Systemereignisse des IE-Switch

Auf dieser Seite legen Sie fest, wie ein IE-Switch auf Systemereignisse reagiert. Durch Aktivieren der entsprechenden Optionen legen Sie fest, bei welchen Ereignissen welche Reaktionen des IE-Switches erfolgen. Es gibt folgende Optionen:

- Der IE-Switch sendet eine E-Mail.
- Der IE-Switch löst einen SNMP-Trap aus.
- Der IE-Switch schreibt einen Eintrag in die Log-Datei.
- Der IE-Switch schreibt einen Eintrag auf den Syslog-Server.

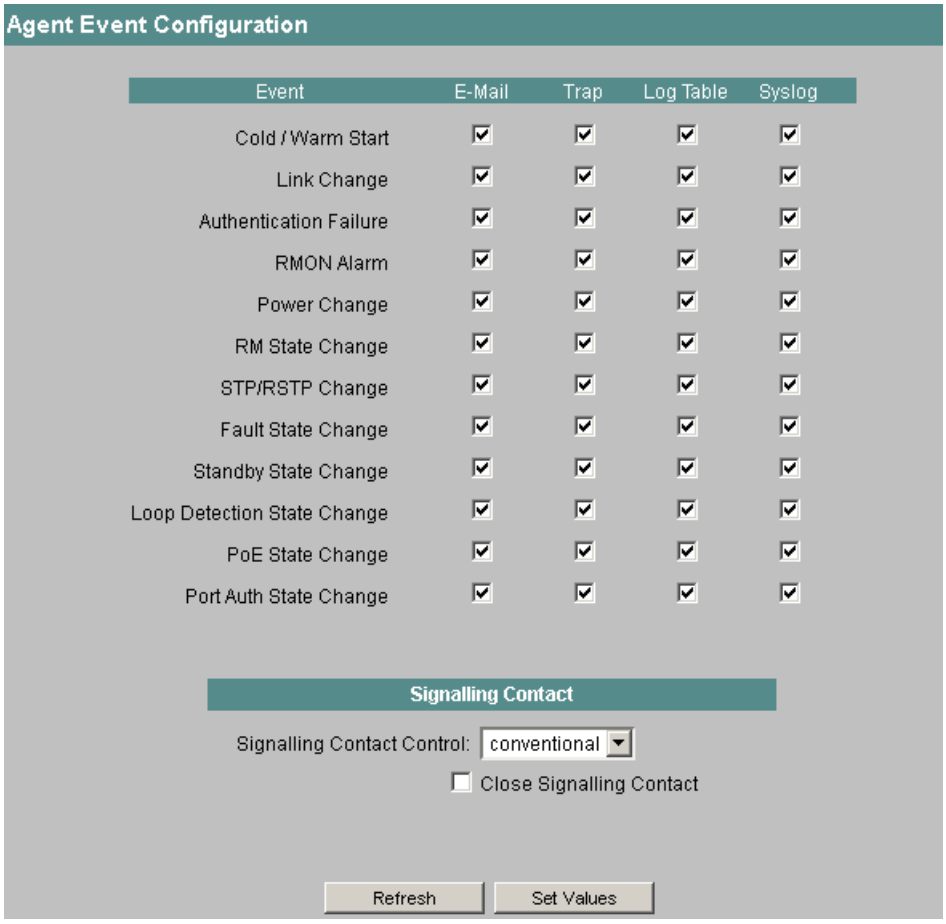


Bild 5-36 Agent Event Configuration

Sie können für folgende Ereignisse die Reaktion des IE-Switch konfigurieren:

Cold/Warm Start
Der IE-Switch wurde eingeschaltet oder vom Anwender neu gestartet.

Link Change
Ein Port ist ausgefallen bzw. über einen Port, der ausgefallen war, wird wieder Datenverkehr abgewickelt.

Authentication Failure
Es hat ein SNMP-Zugriff mit fehlerhaftem Passwort oder nicht ausreichenden Zugriffsrechten stattgefunden.

RMON Alarm
Es ist ein Alarm oder Ereignis (Event) im Zusammenhang mit dem Remote Monitoring aufgetreten.

Power Change
Dieses Ereignis tritt nur auf, wenn die Spannungsversorgung Linie 1 und Linie 2 überwacht wird. Es zeigt an, dass ein Wechsel auf Line 1 bzw. auf Line 2 stattgefunden hat.

RM State Change
Der Redundanzmanager hat eine Unterbrechung oder Wiederherstellung des Rings erkannt und hat die Strecke um- bzw. zurückgeschaltet. Damit ein IE-Switch als Redundanzmanager arbeiten

kann, müssen Sie das Gerät entsprechend konfigurieren (siehe Kapitel "Menüpunkt X-400 Ring Configuration" bzw. "Menüpunkt X-300 Ring Configuration").

Standby State Change
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, siehe Kapitel "Menüpunkt X-400 Standby Mask" bzw. "Menüpunkt X-300 Standby Mask".

Fault State Change
Der Fehlerstatus hat sich geändert. Der Fehlerstatus kann sich auf die aktivierte Portüberwachung, auf das Ansprechen der Meldekontakte oder die Spannungsüberwachung beziehen.

STP/RSTP Change
Die STP- bzw. RSTP-Topologie hat sich geändert, d. h. ein Passive Listening-Ereignis ist aufgetreten.

Loop Detection State Change
Der Status der Loop Detection Funktion hat sich geändert:

- Das Gerät hat einen Port abgeschaltet, weil eine Schleife erkannt wurde.
- Das Gerät hat einen Port wieder eingeschaltet, nachdem eine Schleife aufgelöst wurde.

VRRP State Change (Nur SCALANCE X414)
Der Zustand des virtuellen Routers hat sich geändert.

PoE State Change
Der Zustand von PoE hat sich geändert.

Port Auth State Change
Der Authentifizierungsstatus des Ports hat sich geändert.

Fiber Optic Diagnostics
Ein Ereignis ist im Zusammenhang mit der Port-Diagnose aufgetreten.

Signaling Contact Control
Mit dieser Klappliste können Sie das Verhalten des Meldekontakts festlegen:

- **conventional**
  Standardeinstellung für den Meldekontakt. Ein auftretender Fehler wird durch die Fehler-LED angezeigt und der Meldekontakt öffnet. Wenn der Fehlerzustand nicht mehr besteht, erlischt die Fehler-LED und der Meldekontakt schließt.
- **aligned**
  Die Funktion des Meldekontakts ist unabhängig vom auftretenden Fehlern. Der Meldekontakt kann durch Benutzeraktionen beliebig geöffnet oder geschlossen werden.

Close Signaling Contact
Markieren Sie dieses Optionskästchen, wenn Sie den Meldekontakt schließen wollen.

Hinweis

Der Zustand des Kontrollkästchens "Close Signaling Contact" wirkt sich nur dann aus, wenn in der Klappliste "Signaling Contact Control" die Einstellung "aligned" gewählt wurde.

Syntax Command Line Interface

Tabelle 5-28 Agent Event Configuration - CLI\AGENT\EVENT>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuelle Event-Konfiguration an.	-

Befehl	Beschreibung	Kommentar
setec [event] <E|D> <E|D> <E|D> <E|D>	Legt fest, wie ein IE-Switch auf Systemereignisse reagiert. Für den Parameter event stehen die folgenden Abkürzungen zur Verfügung: • CW Cold/Warm Start • LC Link Change • AF Authentification Failure • RA RMON Alarm • PC Power Change • RC RM State Change • SC Standby State Change • FC Fault State Change • RS STP/RSTP Change • LD Loop Detection State Change • PA Port Auth State Change • VE VRRP State Change (nur X414) • FO Fiber Optic Diagnostics Wird kein Ereignis angegeben, werden die konfigurierten Aktionen bei jedem Ereignis durchgeführt. Die vier darauffolgenden Parameter <E> oder <D> konfigurieren die Reaktionen des IE-Switch in der Reihenfolge: • E-Mail • Trap • Eintrag in die Log-Tabelle • Eintrag auf den Syslog-Server Beispiel: • setec LC E D D D Versendet bei einem Link Change nur eine E-Mail.	Nur Administrator.

Befehl	Beschreibung	Kommentar
scontrol [C|A]	Legt das Verhalten des Meldekontakt fest: conventional Ein auftretender Fehler wird durch die LED angezeigt und der Meldekontakt öffnet. aligned Der Meldekontakt kann unabhängig von einem Fehler beliebig geöffnet oder geschlossen werden.	Nur Administrator.
sclose [yes|no]	Schaltet den Meldekontakt: YesDer Kontakt wird geschlossen. NoDer Kontakt wird geöffnet	Nur Administrator.

5.4.6 Agent Digital Input Configuration (SCALANCE X414-3E)

Hinweis

Digitale Inputs und die damit verbundenen Funktionen sind nur beim SCALANCE X414-3E verfügbar.

Anwendungsbeispiele für digitale Eingänge

Ein SCALANCE X414-3E verfügt über acht digitale Eingänge, die sehr vielseitig eingesetzt werden können:

- **Beispiel 1, Überwachung eines OLM bei peripherieloser Leitsteuerung**
  Gegeben sei eine S7-400-Steuerung ohne zentrale EA-Baugruppe, Peripherie wird optisch über PROFIBUS OLM angebunden. Der Meldekontakt des OLM kann auf einen digitalen Eingang des SCALANCE X414-3E gelegt und diagnostiziert werden.
  Wenn die Meldekontakte eines ebenfalls vorhandenen OLM auf die digitalen Eingänge des SCALANCE X414-3E gelegt werden, kann der OLM ohne zusätzliche Komponenten überwacht werden.
- **Beispiel 2, Türkontakt**
  Der Türkontakt eines Schaltschranks ist mit digitalen Eingängen eines SCALANCE X414-3E verbunden. Über entsprechend projektierte Ereignisse kann so überwacht werden, wann Eingriffe in den Schaltschrank erfolgen.

Ereignisse für Änderungen an den digitalen Eingängen

Für jeden einzelnen digitalen Eingang können Sie festlegen, welches Ereignis bei einer Statusänderung (sowohl steigende als auch fallende Flanke) des Eingangs ausgelöst wird. Es gibt folgende Optionen:

- Der SCALANCE X414-3E sendet eine E-Mail.
- Der SCALANCE X414-3E löst einen SNMP-Trap aus.

- Der SCALANCE X414-3E schreibt einen Eintrag in die Log-Datei.
- Der SCALANCE X414-3E schreibt einen Eintrag auf den Syslog-Server.

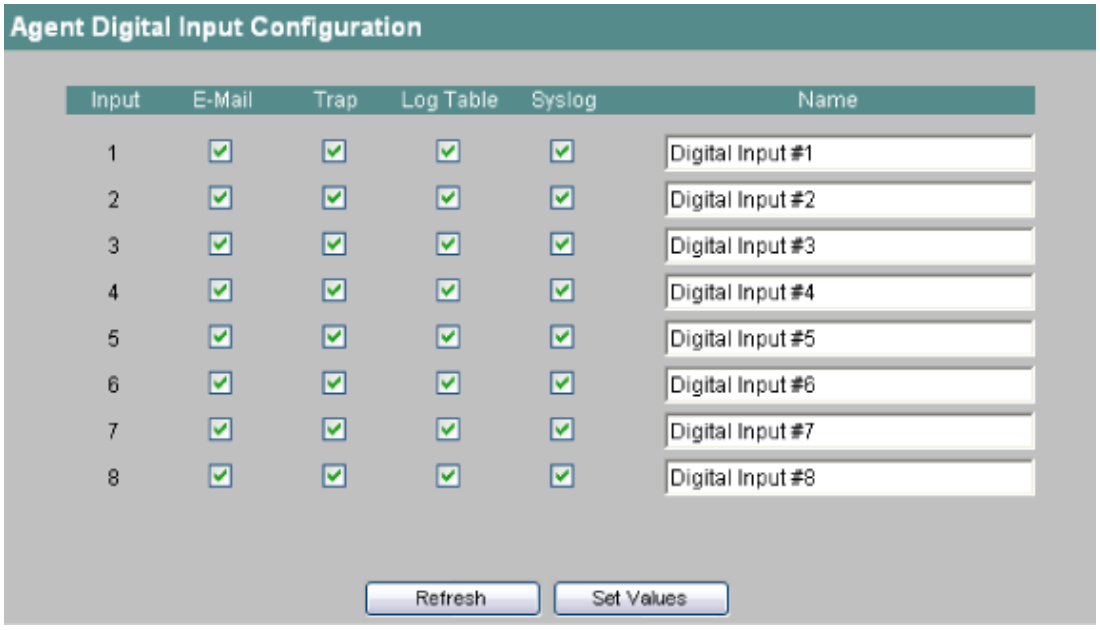


Bild 5-37 Agent Digital Input Configuration

Name
Hier können Sie für jeden digitalen Eingang einen aussagekräftigen Namen vergeben.

Syntax Command Line Interface

Tabelle 5-29 Agent Digital Input Configuration - CLI\AGENT\DIGIN>

Befehl	Beschreibung	Kommentar
info	Zeigt den Zustand der digitalen Eingänge des SCALANCE X414-3E.	-
showdic	Zeigt die Konfiguration der digitalen Eingänge des SCALANCE X414-3E.	-

Befehl	Beschreibung	Kommentar
setdic [Eingang] <E|D> <E|D> <E|D> <E|D>	Setzt die Event-Konfiguration für die digitalen Eingänge in der Reihenfolge E-Mail, Trap, Logtabelleneintrag, Eintrag auf dem Syslog-Server. Wird kein Eingang angegeben, gilt die angegebene Konfiguration für alle Eingänge. Beispiel: • setdic 5 E D E D Wird der Eingang 5 gesetzt, versendet der SCALANCE X414-3E eine E-Mail und macht einen Eintrag in die Logtabelle. Es wird kein Trap gesendet und kein Eintrag auf dem Syslog-Server gemacht.	Nur Administrator.
name <1 ... 8> <string>	Ordnet einem digitalen Eingang einen symbolischen Namen zu. Dieser Name kann maximal 64 Zeichen lang sein.	Nur Administrator.

5.4.7 Agent E-Mail Configuration

Netzüberwachung mit E-Mails

Ein IE-Switch 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 im 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 Browser das WBM gestartet werden, um weitere Diagnoseinformationen auszulesen.

Voraussetzung für das Versenden von E-Mails ist, dass

- die E-Mail-Funktion im IE-Switch aktiviert und die E-Mail Adresse des Empfängers konfiguriert ist (siehe "Menüpunkt Agent Configuration").
- für das jeweilige Ereignis die E-Mail-Funktion aktiviert ist (siehe Menüpunkt "Agent Event Configuration").

- sich in Ihrem Netz ein SMTP-Server befindet, der vom IE-Switch erreichbar ist.
- die IP-Adresse des SMTP-Servers im IE-Switch eingetragen ist.

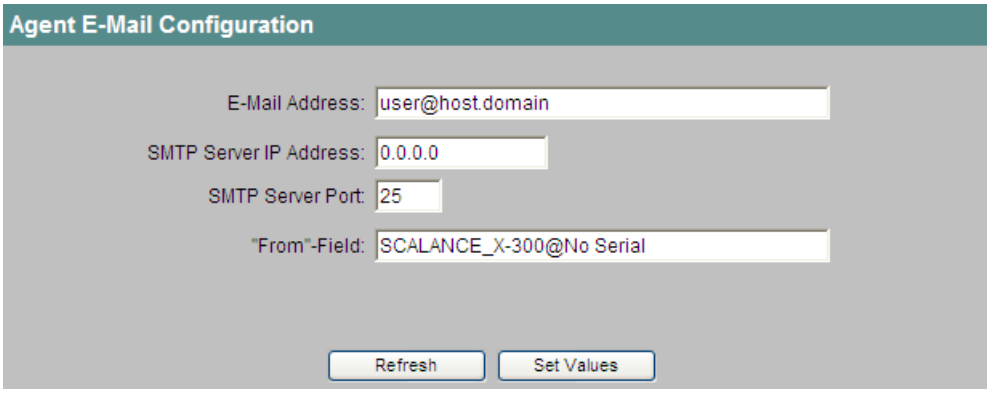


Bild 5-38 Agent E-Mail Configuration

E-Mail Address
Hier tragen Sie die E-Mail-Adresse ein, an die der IE-Switch im Fehlerfall eine E-Mail sendet.

SMTP Server IP Address
Hier müssen Sie die IP-Adresse des SMTP-Servers eintragen, über die die E-Mail gesendet wird.

SMTP Server Port
Der IP-Port, über den die Mail versendet wird. Gegebenenfalls können Sie den Default-Wert 25 entsprechend Ihren spezifischen Anforderungen ändern.

"From"-Field
Die Absender-Adresse der E-Mail.

Hinweis

Je nach Eigenschaft und Konfiguration des SMTP-Servers kann es notwendig sein, das "From"-Feld für die E-Mails anzupassen. Informieren Sie sich beim Administrator des SMTP-Servers. Das "From"-Feld können Sie über WBM, CLI oder direkten SNMP-Zugriff vorgeben.

Syntax Command Line Interface

Tabelle 5-30 Agent E-Mail Configuration - CLI\AGENT\EMAIL>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuelle E-Mail-Konfiguration an.	-
server [<ip>[:port]]	Legt die IP-Adresse und Port-Nummer des SMTP-Servers fest.	Nur Administrator. Default-Wert: 0.0.0.0:25

Befehl	Beschreibung	Kommentar
email <EMail-Adresse>	Legt fest, an welche Adresse ein IE-Switch eine E-Mail versendet. Diese Adresse darf maximal 50 Zeichen lang sein.	Nur Administrator. Default-Wert: Deaktiviert. Default-Adresse: user@host.domain
from [EMail-Adresse]	Legt den Absender für E-Mails vom IE-Switch fest. Diese Adresse darf maximal 50 Zeichen lang sein.	Nur Administrator.

5.4.8 Agent Syslog Configuration

Anwendung

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

Voraussetzung für das Versenden der Logbucheinträge ist, dass

- die Syslog-Funktion im IE-Switch aktiviert ist (siehe Kapitel "Agent Configuration")
- für das jeweilige Ereignis die Syslog-Funktion aktiviert ist (siehe Menüpunkt Agent Event Configuration)
- sich in Ihrem Netz ein Syslog-Server befindet, der die Log-Einträge vom IE-Switch entgegen nimmt. (Da es sich um eine UDP-Verbindung handelt gibt es keine Rückmeldung an den IE-Switch)
- die IP-Adresse des Syslog-Servers im IE-Switch eingetragen ist.

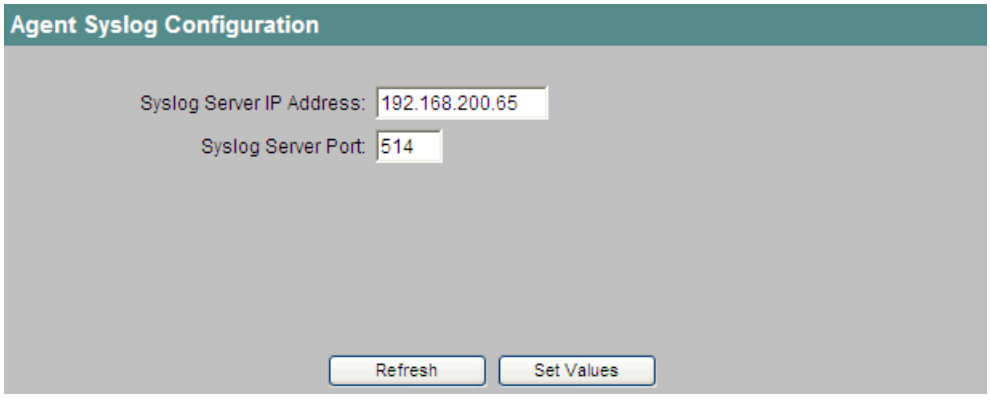


Bild 5-39 Agent Syslog Configuration

Syslog Server IP Address
Hier müssen Sie die IP-Adresse des Syslog-Servers eintragen auf welchem die Log-Einträge gespeichert werden sollen.

Syslog Server Port
Der UDP-Port über den die Log-Einträge auf dem Server gespeichert werden sollen.

Syntax Command Line Interface

Tabelle 5-31 Agent Syslog Configuration - CLI\AGENT\SYSLOG>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuelle Syslog-Konfiguration.	-
server [<ip>[:port]]	Legt die IP-Adresse und Port-Nummer des Syslog-Servers fest.	Nur Administrator. Default-Wert: 0.0.0.0:514

5.4.9 Agent DHCP Configuration

Einstellung der DHCP-Betriebsart

Für die Identifikation des SCALANCE X408-2 in der Konfiguration des DHCP-Servers gibt es mehrere Möglichkeiten:

- durch die MAC-Adresse
- durch eine frei definierte Client-ID
- durch den Systemnamen
- durch den PROFINET IO Gerätenamen

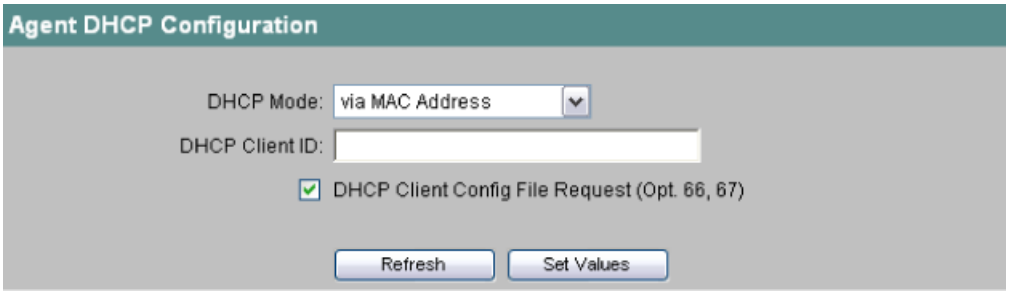


Bild 5-40 Agent DHCP Configuration

DHCP Mode
Hier stellen Sie die DHCP Betriebsart ein.

Hinweis

Ist DHCP im Menüpunkt Agent Configuration nicht aktiviert, kann keine Betriebsart ausgewählt werden und es erscheint der Text "disabled".

DHCP Client ID
Hier können Sie für die DHCP-Betriebsart "via Client ID" einem IE-Switch zugeordneten und vom DHCP Server auszuwertenden Identifikationsstring frei vergeben.

DHCP Client Config File Request (Op. 66, 67)
Wählen Sie diese Option, wenn der DHCP Client die Optionen 66, und 67 dazu verwenden soll, eine Konfigurationsdatei herunterzuladen und diese dann zu aktivieren.

Hinweis

Wird eine Konfigurationsdatei heruntergeladen, so löst dies einen Neustart des Systems aus. Achten Sie darauf, dass in dieser Konfigurationsdatei die Option "DHCP Client Config File Request" nicht mehr gesetzt ist.

Syntax Command Line Interface

Tabelle 5-32 Agent DHCP Configuration - CLI\AGENT\DHCPCONF>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuelle DHCP-Konfiguration an	-
dhcpmode [mode]	Stellt den DHCP-Mode ein. Mögliche Modi sind: • MAC Mac-Adresse • CLID Client-ID • SYSN Gerätenamen • DEVN PNIO-Devicename	Nur Administrator.
clientid [ClientID]	Setzt die DHCP-Client-ID fest. Dieser Wert wird verwendet, wenn DHCP via Client ID eingestellt ist. Die Client ID ist frei definierbar.	Nur Administrator.
cfgreq [E|D]	Aktiviert/deaktiviert Config File Request (Opt. 66, 67)	Nur Administrator.

5.4.10 Time Config

5.4.10.1 Agent Time Configuration

Uhrzeitsynchronisation im Netzwerk

Die folgenden Protokolle stehen Ihnen zur Zeitsynchronisation im Netzwerk zur Verfügung:

- SNTP (Simple Network Time Protocol)
- NTP (Network Time Protocol)

- SIMATIC Time
- PTP (Precision Time Protocol)

Nehmen Sie die allgemeinen Einstellungen in der Maske "Agent Time Configuration" vor.

SNTP und NTP benötigen weitere Einstellungen, die Sie in den Menüpunkten "SNTP Client" und "NTP Client" vornehmen können.

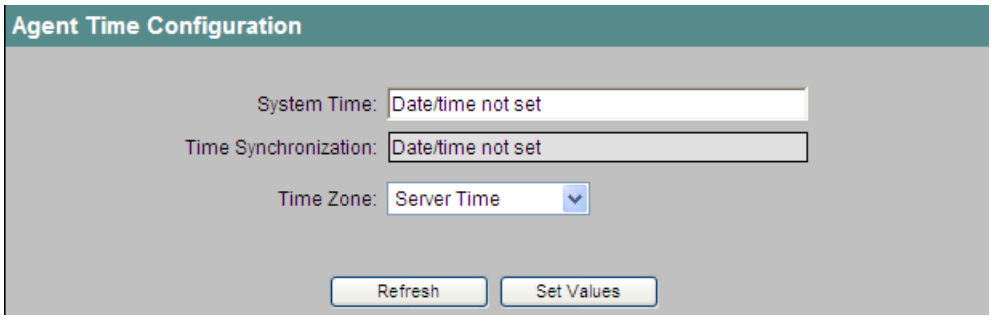


Bild 5-41 Agent Time Configuration

System Time

Dieses Feld zeigt die aktuelle Systemzeit an.
An dem Zusatz hinter Datum und Uhrzeit können Sie erkennen, wie die Systemzeit gesetzt wurde:

- (p)
  Die Systemzeit wurde per SNTP gesetzt.
- (n)
  Die Systemzeit wurde per NTP gesetzt.
- (i)
  Die Systemzeit wurde per PTP gesetzt.
- (s)
  Die Systemzeit wurde per SIMATIC Uhrzeit-Frame gesetzt und ist synchron mit dem Uhrzeitsender.
- (t)
  Die Systemzeit wurde per SIMATIC Uhrzeit-Frame gesetzt, ist aber nicht synchron mit dem Uhrzeitsender.
- (m)
  Die Systemzeit ist manuell gesetzt.
  Sie können Datum und Uhrzeit auch manuell setzen. Das notwendige Eingabeformat dafür ist: MM/TT/JJJJ HH:MM:SS.

Wenn keine Uhrzeitsynchronisation möglich war, enthält das Feld die Angabe "Date/time not set".

Time Synchronization

Dieses Feld ist nur lesbar und zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.

Time Zone

Wählen Sie hier die Zeitzone für den Standort des IE-Switches aus, da der SNTP-Server immer die UTC-Zeit sendet. Diese Zeit wird dann mit der Angabe für die Zeitzone in die lokale Zeit umgerechnet. Im IE-Switch erfolgt keine Sommerzeit/Winterzeit-Umstellung.

Syntax Command Line Interface

Tabelle 5-33 Agent Time Configuration - CLI\AGENT\TIME>

Befehl	Beschreibung	Kommentar
time [Datum][Uhrzeit]	Zeigt das Datum und die Uhrzeit des IE-Switches an oder stellt sie ein. Bei der Anzeige von Datum und Uhrzeit wird auch angegeben, wann und wie sie eingestellt wurden: • p Die Einstellung erfolgte per SNTP. • n Die Einstellung erfolgte per NTP. • i Die Einstellung erfolgte per PTP. • t Die Einstellung erfolgte per SIMATIC Uhrzeit-Frame, ist aber nicht synchron mit dem Uhrzeitsender. • s Die Einstellung erfolgte per SIMATIC Uhrzeit-Frame und ist synchron mit dem Uhrzeitsender. • m Die Einstellung erfolgte manuell.	Nur Administrator. Eingabeformat: MM/TT/JJJJ HH:MM:SS
timezone [-12 ... 13]	Stellt die Zeitdifferenz in Stunden zwischen dem Server und der Systemzeit ein.	Nur Administrator.

5.4.10.2 SNTP Client Configuration

Uhrzeitsynchronisation mit SNTP

Das SNTP (Simple Network Time Protocol) dient zur Zeitsynchronisation im Netzwerk. Die entsprechenden Frames werden von einem Server im Netz versendet. Ein IE-Switch meldet sich als Client bei diesem Server als Empfänger von Uhrzeit-Frames an.

Die Maske "SNTP Client Configuration" erscheint, wenn Sie das Untermenü "SNTP Client" angeklickt haben.

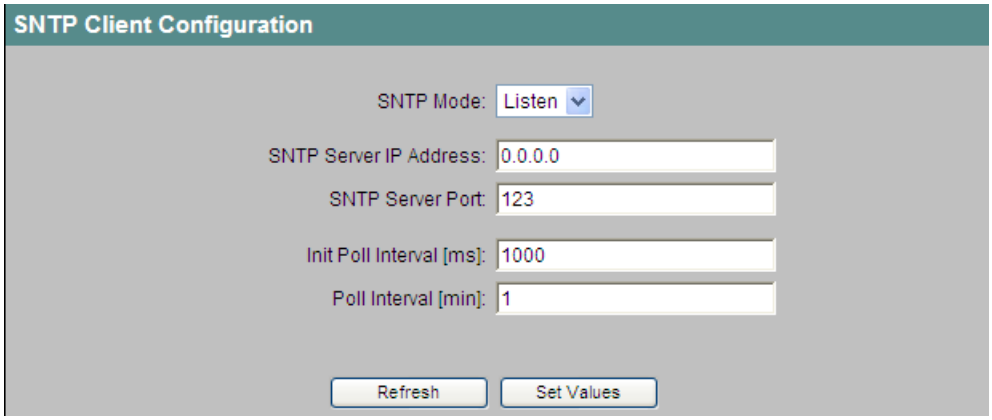


Bild 5-42 SNTP Client Configuration

SNTP Mode

Sie können zwischen folgenden Protokollarten wählen:

- Poll
  Wenn Sie diese Protokollart wählen, müssen Sie die SNTP Server IP Address einstellen.
  Folgende Einstellungen können Sie ändern:
  SNTP Server Port, Init poll interval, Poll interval, Time Zone Offset.
- Listen
  Wenn Sie diese Protokollart wählen, können Sie zusätzlich zu der vom Server empfangenen Zeit ein Time Zone Offset wählen.

Hinweis

Time Zone Offset

Die Einstellung Time Zone Offset befindet sich im Menü Agent Time Configuration (Seite 130).

SNTP Server IP Address

Tragen Sie die IP-Adresse des SNTP-Servers ein, dessen Frame ein IE-Switch für die Synchronisation der Uhrzeit verwenden soll.

SNTP Server Port

Tragen Sie den Port ein, über den der SNTP-Server verfügbar ist.

Init poll interval

Tragen Sie die Wiederholrate ein, mit der ein IE-Switch beim ersten Setzen der Systemzeit die Abfrage wiederholt, falls diese nicht erfolgreich durchgeführt wurde.

Poll interval

Nachdem die Systemzeit erstmalig vom Time-Server übernommen wurde, wird sie zyklisch durch erneute Anfragen an den Time-Server aktualisiert. Geben Sie an, wie oft die Systemzeit aktualisiert werden soll.

Syntax Command Line Interface

Tabelle 5-34 SNTP Client Configuration - CLI\AGENT\TIME\SNTP>

Befehl	Beschreibung	Kommentar
server [<ip> [:port]]	Stellt die IP-Adresse und optional den Port des SNTP-Servers ein.	Nur Administrator.
sntpmode [mode]	Legt den SNTP-Mode fest. Mögliche Modi sind: • POLL IE-Switch frägt die Uhrzeit beim SNTP-Server ab • LISTEN IE-Switch wartet auf SNTP Uhrzeit-Frames	Nur Administrator.
initint [1 ... 1000]	Legt das Wählintervall im Bereich von 1-10000 ms fest	Nur Administrator.
Interval [1 ... 1440]	Legt das Wählintervall im Bereich von 1-1440 s fest	Nur Administrator.

5.4.10.3 NTP Client Configuration

Uhrzeitsynchronisation mit NTP

Das NTP (Network Time Protocol) dient zur Zeitsynchronisation im Netzwerk. Ein IE-Switch meldet sich als Client bei einem oder mehreren Servern als Empfänger von Uhrzeit-Frames an. Die entsprechenden Frames werden dann von den NTP-Servern im Netz versendet. Bei mehreren Servern vergleicht NTP die erhaltene Systemzeit und entscheidet, welche die höchste Qualität aufweist.

Die Maske "NTP Client Configuration" erscheint, wenn Sie das Untermenü "NTP Client" angeklickt haben.

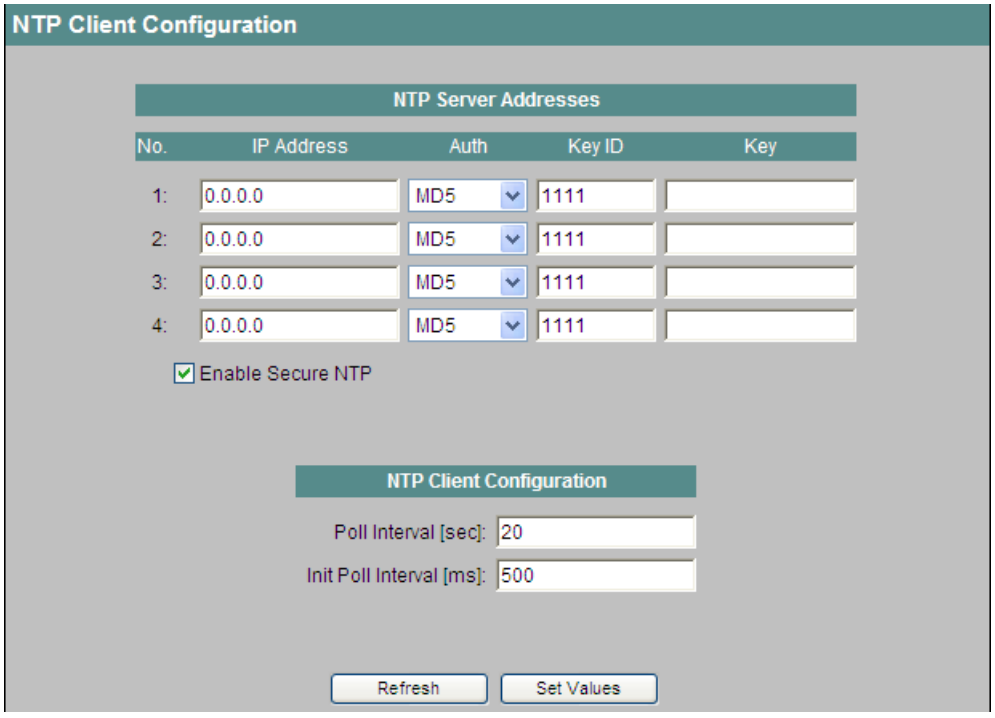


Bild 5-43 NTP Client Configuration

IP Adresse

Tragen Sie die IP-Adresse des NTP-Servers ein, an den ein Client Frames für die Synchronisation der Uhrzeit senden soll.
Sie können bis zu vier verschiedene NTP-Server angeben.

Auth

Wählen Sie, wie die Frames signiert werden.
Sie haben zwei Auswahlmöglichkeiten: MD5 und SHA.

Key ID

Tragen Sie eine Key ID für die Verschlüsselung ein. Erlaubte Werte für die Key ID: 1-65534.

Key

Tragen Sie einen ASCII-String mit maximal 11 Zeichen als Schlüssel ein. Die Eingabe von Hexadezimalzahlen ist weder im WBM noch im CLI möglich.

Enable Secure NTP

Aktivieren Sie diese Funktion, um Frames verschlüsselt zu versendet.

Poll Interval [sec]

Tragen Sie ein, in welchen Abständen der Client Anfragen an den Time Server sendet und die Systemzeit aktualisiert.

Init Poll Interval [ms]

Tragen Sie die Zeit ein, nach der ein Client nach dem ersten Verbinden die Systemzeit beim Server anfragt.

Syntax Command Line Interface

Tabelle 5-35 NTP Client Configuration - CLI\AGENT\TIME\NTP>

Befehl	Beschreibung	Kommentar
server [<number><IP>]	Legt die Server-Nummer und die IP-Adresse des NTP-Servers fest.	Nur Administrator.
initint [1...10000]	Legt das Interval für die Anfrage der Systemzeit nach der ersten Verbindung fest. Erlaubte Werte: 1...10000ms.	Nur Administrator.
interval [1...160]	Legt das Interval für die Anfrage und Aktualisierung der Systemzeit fest. Erlaubte Werte: 1...160s.	Nur Administrator.
secure <Server No.><KeyID><MD5|SHA><Key>	Legt die Server-Nummer, die Key ID, den Algorithmus und den Key für eine sichere Übertragung der Frames fest.	Nur Administrator.
security [E|D]	Aktiviert/Deaktiviert NTP Security.	Nur Administrator.

5.4.10.4 Daylight Saving Time

Daylight Saving Time Table

Hinweis

Diese Funktion gibt es nur bei den Geräten SCALANCE X-300 und SCALANCE X408, nicht beim SCALANCE X414.

Auf dieser Seite können Sie die Umstellung der Sommerzeit regeln, damit die Systemzeit für die lokale Zeitzone korrekt eingestellt ist.

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

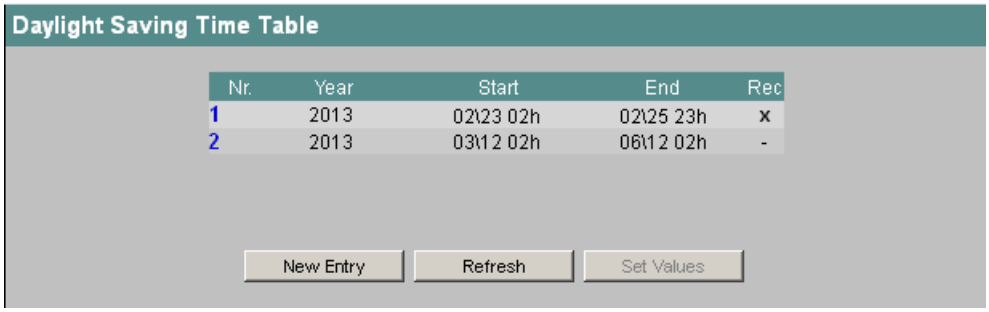


Bild 5-44 Daylight Saving Time Table

Die Tabelle gibt Ihnen einen Überblick über die vorhanden Einträge zur Umstellung der Sommerzeit.
Sobald der End-Termin eines Eintrags überschritten ist, werden bei einer definierten Regel die Daten für die nächste Umstellung angezeigt. Bei festen Einträgen wird die Zeile gelöscht.

Nr.

Zeigt die Nummer des Eintrags an.
Wenn Sie einen neuen Eintrag anlegen, wird eine neue Zeile mit einer eindeutigen Nummer angelegt.

Year

Zeigt das Jahr an, für das der Eintrag angelegt wurde.

Start

Zeigt Monat, Tag und Uhrzeit für den Start der Sommerzeit an.

End

Zeigt Monat, Tag und Uhrzeit für das Ende der Sommerzeit an.

Rec

Zeigt an, ob für die Umstellung der Sommerzeit eine Regel definiert wurde:

- x
  Es ist eine Regel für die Umstellung der Sommerzeit definiert.
- -
  Es wurde ein festes Datum für die Umstellung der Sommerzeit eingetragen.

Daylight Saving Time Table New Entry

Um einen neuen Eintrag anzulegen, klicken Sie auf der Seite "Daylight Saving Time Table" auf die Schaltfläche "New Entry".

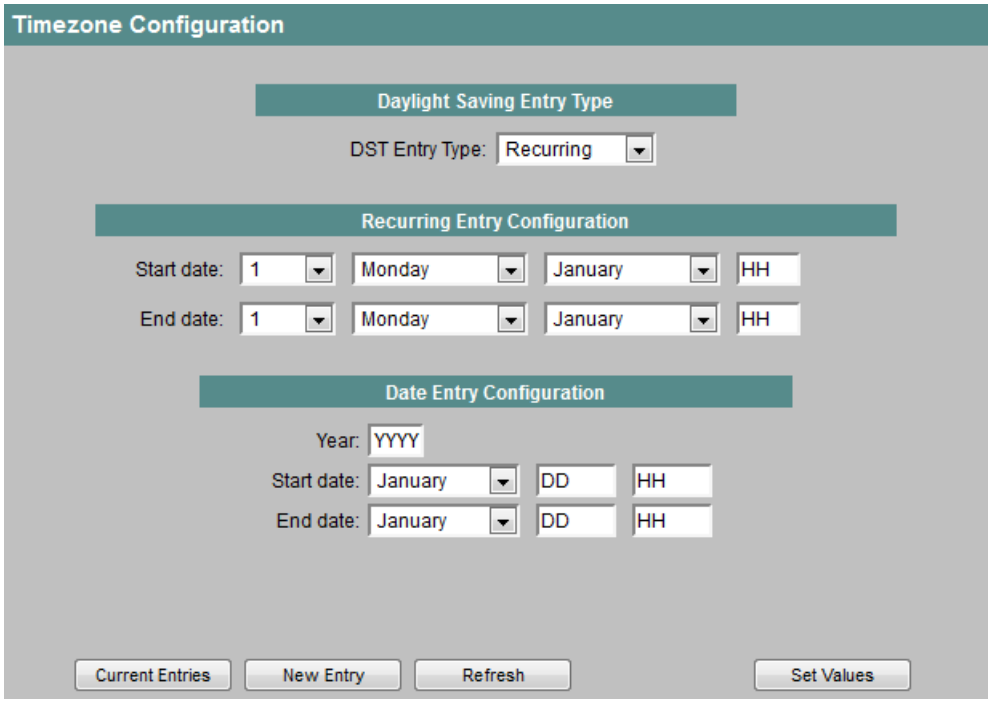
Einstellungen bei Daylight Saving Entry Type

Legen Sie fest, wie die Umstellung der Sommerzeit erfolgen soll.

DST Entry Type

Wählen Sie aus dieser Klappliste einen der folgenden beiden Einträge:

- **Recurring**
  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.
- **Date**
  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.



Einstellungen bei "Recurring Entry Configuration"

Sie können eine Regel für die Umstellung der Sommerzeit erstellen

Start date

Geben Sie folgende Werte für den Beginn der Sommerzeit an:

- Woche des Monats
  Sie können die 1. bis 5. oder die letzte Woche des Monats auswählen.
- Wochentag
- Monat
- Uhrzeit in Stunden

End date

Geben Sie folgende Werte für das Ende der Sommerzeit an:

- Woche des Monats
  Sie können die 1. bis 5. oder die letzte Woche des Monats auswählen.
- Wochentag
- Monat
- Uhrzeit in Stunden

Einstellungen bei der Auswahl "Date Entry Configuration"

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

Year

Geben Sie das Jahr für die Umstellung der Sommerzeit an.

Start date

Geben Sie folgende Werte für den Beginn der Sommerzeit an:

- Monat
- Tag
- Uhrzeit in Stunden

End date

Geben Sie folgende Werte für das Ende der Sommerzeit an:

- Monat
- Tag
- Uhrzeit in Stunden

Syntax Command Line Interface

Tabelle 5-36 Daylight Saving Time Table - CLI\AGENT\TIME\DST>

Befehl	Beschreibung	Kommentar
info	Zeigt Informationen über die Zeitzone und die Umstellung der Sommerzeit an.	
recurring <start date> <end date>	Legt einen Eintrag des Typs "Recurring" an. Für die Parameter <start date> und <end date> müssen Sie jeweils folgende Angaben machen: • 1-5 oder Last • Weekday • Month • Hour	Nur Administrator Beispiel: recurring last sunday march 02 last sunday october 03
date <yyyy> <start date> <end date>	Legt einen Eintrag des Typs "Date" an. Für die Parameter <start date> und <end date> müssen Sie jeweils Monat, Tag und Stunde in folgender Form angeben: • mmddhh	Nur Administrator Beispiel: date 2010 040102 100103
delete <index>	Löscht einen Eintrag. Der Index des zu löschenden Eintrags muss über den Befehl "info" ermittelt werden.	Nur Administrator

5.4.11 Agent PNIO Configuration

Einstellungen für PROFINET IO

Hier wird der PROFINET IO Gerätename so eingestellt, wie er für den IE-Switch im Zuge der PROFINET IO Hardware-Konfiguration mittels NCM vergeben wurde.

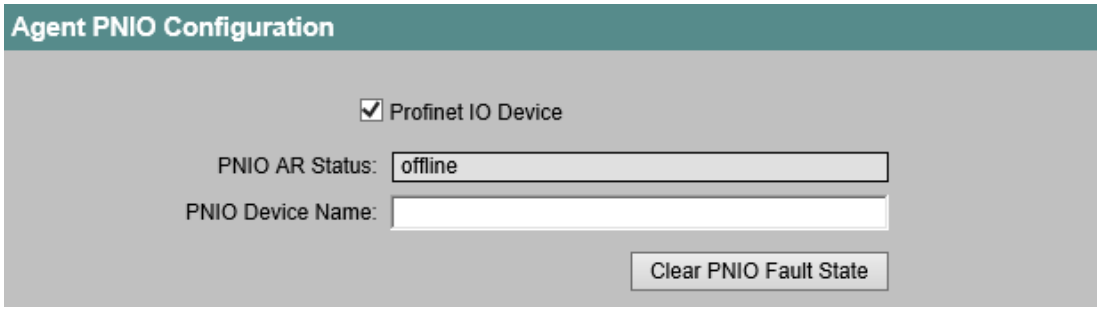


Bild 5-45 Agent PROFINET IO Configuration

PROFINET IO Device
Bei aktiviertem Optionskästchen ist die PROFINET IO-Device-Funktionalität eingeschaltet. Nach einer Änderung dieser Einstellung wird der Switch automatisch neu gestartet.

PNIO AR Status
Dieses Feld zeigt den PROFINET IO Application Relation Status an, d.h. ob der IE-Switch mit einem PROFINET Controller "online" oder "offline" verbunden ist.

Online bedeutet hierbei, dass eine Verbindung zu einem PROFINET IO Controller besteht, dass dieser seine Konfigurationsdaten auf den IE-Switch geladen hat und das Gerät Statusdaten zum PROFINET IO Controller senden kann. In diesem Zustand, der auch "in Data exchange" genannt wird, sind die Parameter, die über den PROFINET IO Controller eingestellt werden, nicht am IE-Switch konfigurierbar.

PNIO Device Name
Hier geben Sie den PROFINET IO-Gerätenamen (Name of Station) gemäß der Projektierung in HW Konfig ein.

Clear PNIO Fault State
Wurde der IE-Switch in eine PROFINET IO-Umgebung (mit Controller) eingebunden und wird dann aus dem PROFINET IO-Betrieb wieder herausgenommen, wird über die Fehler-LED signalisiert, dass der Controller fehlt. Diese Fehleranzeige kann über diese Schaltfläche gelöscht werden.

Syntax Command Line Interface

Tabelle 5-37 Agent PROFINET IO Configuration - CLI\AGENT\PNIOCONF>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuelle PROFINET IO-Konfiguration an	-
devname [string]	Stellt den PROFINET IO-Device-Name ein.	Nur Administrator.

Befehl	Beschreibung	Kommentar
clear	Löscht einen evtl. vorhandenen PROFINET IO-Fehlerzustand	Nur Administrator.
pnio [E|D]	Aktiviert/Deaktiviert die PROFINET IO-Device-Funktionalität. Nach einer Änderung dieser Einstellung wird der Switch automatisch neu gestartet.	Nur Administrator.

5.4.12 Management Access Control List

Die Management Access Control List im Überblick

Auf dieser Seite können Sie die Sicherheit Ihres IE-Switches erhöhen. Um festzulegen, welcher Host mit welcher IP-Adresse auf das Management Ihres IE-Switches zugreifen darf, projektieren Sie die Zugriffsregeln für einzelne Hosts, Subnetze oder alle Hosts.

Die Liste der Zugriffsregeln stellt diese Angaben übersichtlich dar, wie nachfolgende Abbildung beispielhaft zeigt:

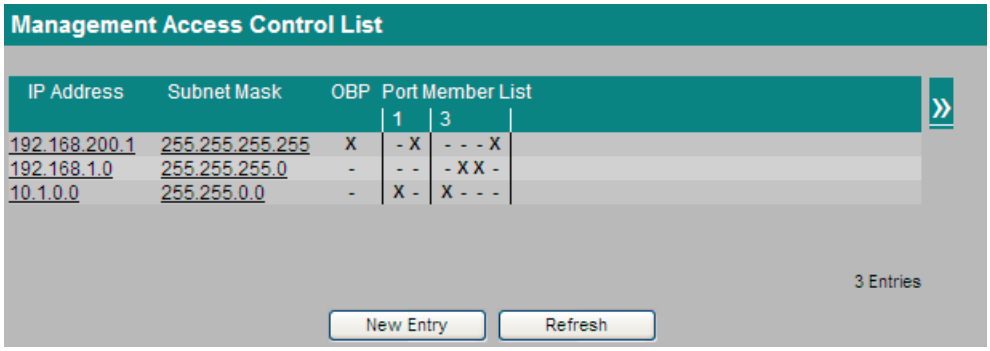


Bild 5-46 Übersicht Management Access Control List

Hinweis

Die Option "Out-Band Port Enabled" (OBP) steht nur beim SCALANCE X414 zur Verfügung.

Seiten wechseln

Wählen Sie die Schaltflächen ">>" und "<<", um zwischen den Seiten hin und her zu schalten. Auf der zweiten Seite werden statt der Ports eventuell eingerichtete Link-Aggregationen angezeigt.

Zugriffsregeln

Sobald Sie eine Zugriffsregel definiert haben, sind zunächst alle anderen Zugriffsmöglichkeiten gesperrt, die nicht in dieser Regel definiert sind. Wenn Sie den Zugriff anderer Hosts bzw. Services erlauben wollen, müssen Sie dafür weitere Zugriffsregeln definieren.

Sie können Zugriffsregeln wie folgt definieren:

- für einen Host:
  Verwenden Sie eine Host-IP-Adresse mit der Subnetzmaske 255.255.255.255.
- für alle Hosts eines definierten Subnetzes:
  Verwenden Sie eine gültige Kombination aus IP-Adresse und Subnetzmaske.
- für alle Hosts:
  Tragen Sie jeweils unter IP-Adresse und Subnetzmaske 0.0.0.0 ein.

Wenn für den Zugriff eines Hosts mehrere Regeln passen, dann greift die enger gefasste Regel, "Best Match". Wenn z. B. sowohl die Zugriffsregel für einen einzelnen Host passt als auch die Regel für ein gesamtes Subnetz, dann greift die Host-Regel.

Management ACL Configuration

Sie können einstellen, welcher Host über welche Ports und über welche Services auf den IE-Switch zugreifen kann.

Hinweis

Beachten Sie: Eine fehlerhafte Projektierung kann dazu führen, dass Sie nicht mehr auf das Gerät zugreifen können. Projektieren Sie daher eine Zugriffsregel, die Ihnen den Zugriff auf das Management erlaubt, bevor Sie die Funktion auf der Seite Agent Configuration (Seite 97) aktivieren.

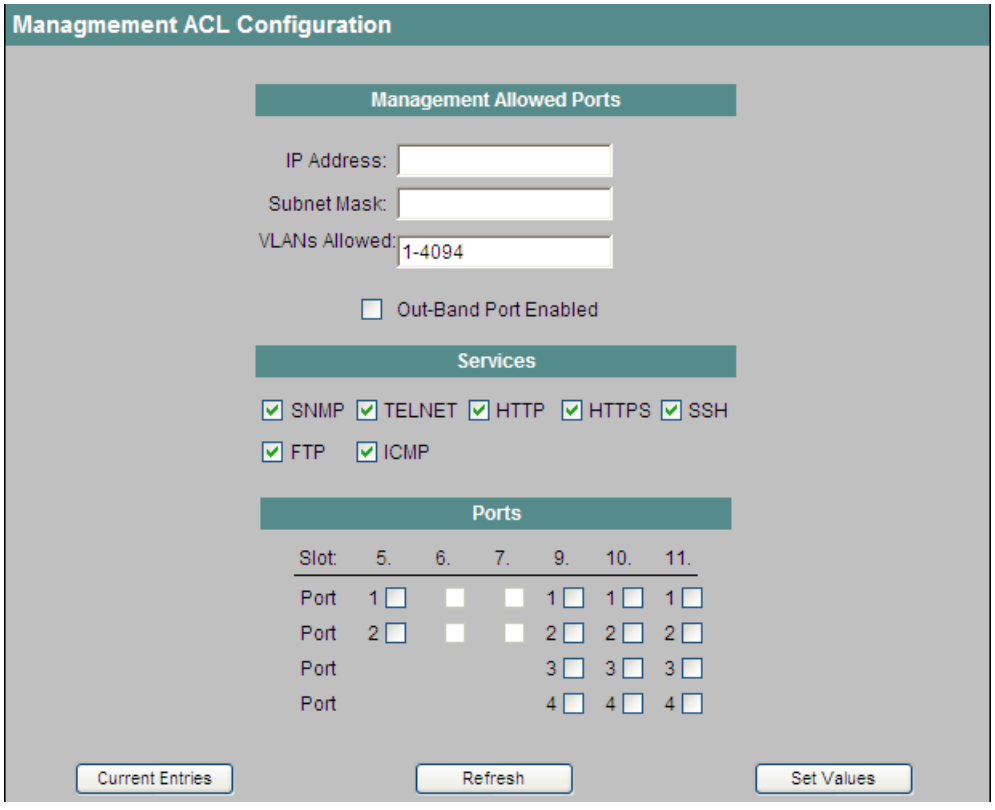


Bild 5-47 Management ACL Configuration (SCALANCE X-400)

Management Allowed Ports

IP Address

Tragen Sie die IP-Adresse ein, für die die Regel gelten soll.
Wenn Sie die IP-Adresse 0.0.0.0 verwenden, gelten die Einstellungen für alle IP-Adressen.

Subnet Mask

Tragen Sie die Subnetz-Maske ein.
Die Subnetz-Maske 255.255.255.255 ist für eine bestimmte IP-Adresse. Möchten Sie ein Subnetz zulassen, tragen Sie z. B. für ein C-Subnetz 255.255.255.0 ein. Die Subnetz-Maske 0.0.0.0 gilt für alle Subnetze.

VLANs Allowed

Tragen Sie die Nummer der VLANs ein, aus denen der Zugriff erlaubt ist.
Sie können mehrere einzelne VLANs sowie VLAN-Bereiche durch Kommas getrennt eingeben, z. B. 1,5,10-12.

Out-Band Port Enabled

Wenn Sie "Out-Band Port Enabled" aktivieren, kann die IP-Adresse über den Out-Band Port auf den Switch zugreifen.

Services

Wenn Sie einen der folgenden Services aktivieren, ermöglichen Sie damit den Zugriff über diesen Service:

- SNMP
- TELNET
- HTTP
- HTTPS
- SSH
- FTP
- ICMP

Der folgende Service ist nur bei SCALANCE X300 verfügbar:

- DHCP-Relay
  Wenn Sie diesen Service aktivieren, vermittelt DHCP-Relay zwischen einem Endgerät und einem DHCP-Server, die sich in unterschiedlichen Netz befinden, sodass dem Endgerät eine IP-Adresse zugewiesen werden kann.

  Hinweis

  Ausführliche Informationen zu dieser Funktionalität finden Sie in den Kapiteln "DHCP Relay Agent Configuration" und "DHCP Relay Agent Port Configuration".

Ports

Aktivieren Sie die Ports, über die auf das Gerät zugegriffen werden darf.

Einen neuen Eintrag anlegen

Gehen Sie wie folgt vor, um einen neuen Eintrag anzulegen:

1. Klicken Sie auf der Seite "Management Access Control List" auf die Schaltfläche "New Entry". Die Seite "Management ACL Configuration" erscheint.
2. Tragen Sie in das erste Eingabefeld die IP-Adresse ein.
3. Tragen Sie in das zweite Eingabefeld die Subnetz-Maske ein.
4. Tragen Sie in das dritte Eingabefeld VLANs bzw. VLAN-Bereiche ein.
5. Nur bei X414:
   Aktivieren Sie die Option "Out-Band Port Enabled", wenn die IP-Adresse über den Out-Band Port auf den Switch zugreifen soll.
6. Aktivieren Sie die gewünschten Ports.
7. Aktivieren Sie die gewünschten Services.
8. Um die geänderten Angaben ins Gerät zu übertragen, klicken Sie auf die Schaltfläche "Set Values".
9. Um zurück zur Übersicht "Management Access Control List" zu gelangen, klicken Sie auf die Schaltfläche "Current Entries".

Einen vorhandenen Eintrag bearbeiten

Gehen Sie wie folgt vor, um einen vorhandenen Eintrag zu ändern:

1. Klicken Sie auf der Seite "Management Access Control List" auf die IP-Adresse des zu ändernden Eintrags.
2. Nehmen Sie die gewünschten Änderungen vor.
   Die Einträge in den Feldern "IP Address" und "Subnet Mask" sind nur lesbar.
3. Um die geänderten Angaben ins Gerät zu übertragen, klicken Sie auf die Schaltfläche "Set Values".
4. Um zurück zur Übersicht "Management Access Control List" zu gelangen, klicken Sie auf die Schaltfläche "Current Entries".

Einen Eintrag löschen

Wenn Sie einen vorhandenen Eintrag löschen möchten, gehen Sie folgendermaßen vor:

1. Klicken Sie auf der Seite "Management Access Control List" auf die IP-Adresse des zu löschenden Eintrags.
   Die Seite "Management ACL Configuration" erscheint.
2. Klicken Sie auf die Schaltfläche "Delete".
   Der Eintrag wird gelöscht.

Syntax Command Line Interface

Tabelle 5-38 **Management Access Control List - CLI\AGENT\MGMNTACL\>**

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen Einstellungen der Management Access Control List an.	
add <IP> <subnet>	Legt einen neuen Eintrag in der Management Access Control List an.	Nur Administrator.
ports <IP> <subnet> <E|D> [ports]	Legt die Ports fest, über die auf das Gerät zugegriffen werden darf.	Nur Administrator.
outband <IP> <subnet> <E|D>	Gilt nur für den X414: Legt fest, ob die IP-Adresse über den Out-Band-Port auf den Switch zugreifen kann.	Nur Administrator.
vlans <IP> <subnet> [1-4094]	Entspricht der Nummer des VLANs ein, in dem sich das Gerät befindet. Legt fest, dass nur Hosts aus dem gleichen VLAN auf das Gerät zugreifen können.	Nur Administrator.
services <IP> <subnet> <E|D> [services...]	Legt fest, über welche Protokolle auf das Gerät zugegriffen werden kann.	Nur Administrator.
delete <IP> <subnet>	Entfernt einen Eintrag aus der Management Access Control List.	Nur Administrator.

Siehe auch

Adressvergabe mit dem DHCP-Client (Seite 39)

5.5 Das Menü Switch

Einleitung

In diesem Menü parametrieren Sie die Switch-Funktionalität (dem Layer 2 zuzuordnen) des IE-Switches. Dazu gehören folgende Funktionen:

- Allgemeine Switch-Einstellungen wie Mirroring, Aging und Flusskontrolle.
- Die Filtertabelle für Unicast-, Multicast- und Broadcast-Frames.
- Die Verwaltung von Multicast-Gruppen mittels IGMP/GMRP.
- Die Nutzung des Spanning-Tree-Protokolls.
- Konfiguration von VLANs und deren dynamische Konfiguration mit GVRP-Frames.
- Das Festlegen von Übertragunsprioritäten durch CoS to Queue und DSCP to Queue Mapping.
- DCP-Port-Filter
- Topologie-Diagnose mit LLDP
- IP-Adresstaufe mit DHCP Relay

- Schleifenerkennung
- 1:1-NAT
- Statistikzähler für Frames je Port

5.5.1 Switch Configuration

Protokolleinstellungen und Switch-Funktionalität

Die Maske "Switch Configuration" erscheint, wenn Sie das Ordnersymbol "Switch" angeklickt haben. In dieser Maske legen Sie fest, welche Funktionalität beim IE-Switch aktiviert ist und welche Protokolle für die Verwaltung des Datenverkehrs verwendet werden sollen.

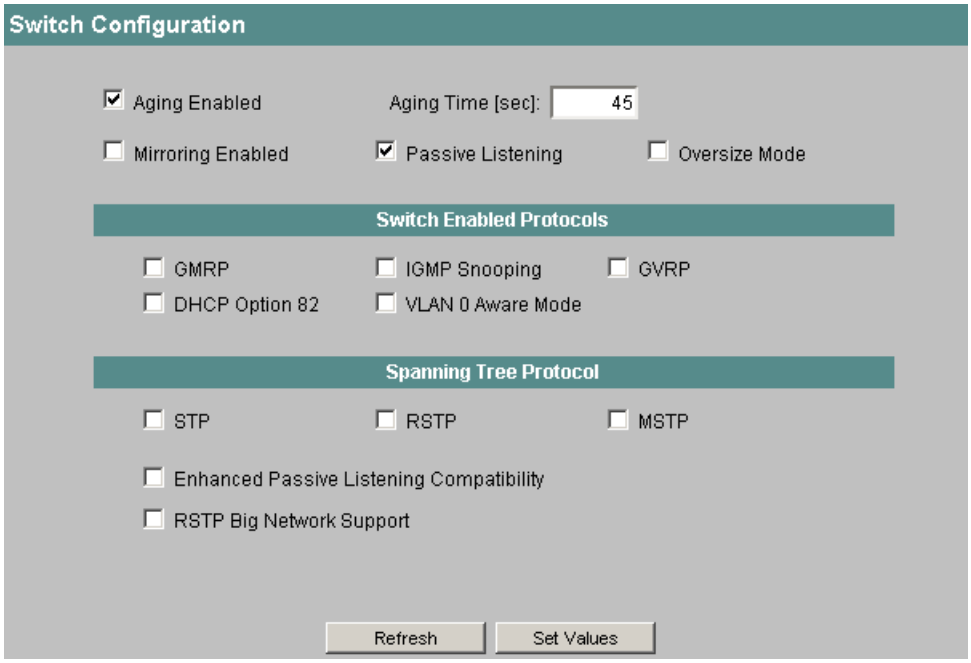


Bild 5-48 Switch Configuration

Mirroring und Aging

Im oberen Bereich der Maske können Sie folgende Funktionen des IE-Switches einschalten bzw. ausschalten:

Aging Enabled

Ein IE-Switch lernt automatisch die Quelladressen der an ihm angeschlossenen Teilnehmer. Diese Information wird im IE-Switch dazu benutzt, um Datenframes gezielt an die betroffenen Teilnehmer weiterzuleiten. Dadurch wird die Netzlast für die anderen Teilnehmer reduziert.

Erhält ein IE-Switch innerhalb einer bestimmten Zeitspanne kein Frame, dessen Quelladresse mit einer gelernten Adresse übereinstimmt, dann löscht er die gelernte Adresse. Dieser Mechanismus wird als Aging bezeichnet. Durch Aging wird verhindert, dass Frames fehlgeleitet

werden, wenn z. B. ein Endgerät (z. B. ein Programmiergerät) an einen anderen Switch-Port angeschlossen wird.

Wenn Sie Aging Enabled aktivieren, löscht ein IE-Switch die gelernten Adressen automatisch nach einer eingestellten Zeit (Aging Time).

Aging Time [sec]

Tragen Sie ein, nach welcher Zeitdauer der IE-Switch eine Adresse löscht, wenn er keine Frames mit einer solchen Absenderadresse erhalten hat.

Beim SCALANCE X408-2 beträgt die Voreinstellung für die Aging Time 30 s. Sie können die Aging Time im Bereich von 15 bis 3825 Sekunden in 15s-Schritten einstellen.

Beim SCALANCE X414-3E beträgt die Voreinstellung für die Aging Time 40 s. Sie können die Aging Time im Bereich von 10 bis 1000000 Sekunden beliebig einstellen.

Mirroring Enabled

Mirroring bedeutet, dass der Datenverkehr eines Ports des IE-Switches (Mirrored Port) auf einen anderen Port (Monitor Port) kopiert wird.

Wenn Sie Mirroring Enabled aktivieren, können Sie einen oder mehrere Ports auf einen Monitor Port spiegeln.

Passive Listening

Wenn Sie Passive Listening aktivieren, reagiert der IE-Switch auch im Nicht-(R)STP-Betrieb auf Umkonfigurationen. Beim Empfang eines RSTP Topology Change Frames wird die MAC-Adress-Tabelle gelöscht. Außerdem werden Spanning Tree BPDUs weitergeleitet.

Hinweis

Im Passive Listening-Betrieb ist der IE-Switch nicht kompatibel zu IEEE 802.1d, welcher das Weiterleiten von Spanning Tree BPDUs im Nicht-(R)STP-Betrieb untersagt.

Hinweis

Wird an einem Switch, der Teilnehmer in einem redundanten Ring ist, die Funktion (R)STP eingeschaltet, dann werden über die Ringports keine Spanning Tree BPDUs mehr weitergeleitet. Dies gilt auch, wenn die Funktion Passive Listening eingeschaltet ist.

In diesem Fall dürfen über den redundanten Ring keinesfalls (R)STP-Netzsegmente gekoppelt werden, da dies zu Schleifenbildung führen würde.

Oversize Mode

Wenn Sie Oversize Mode aktivieren, sind Frames mit einer Größe von bis zu 1.632 Byte statt 1.522 Byte zugelassen.

Hinweis

Überlange Frames in PRP-Netzwerken

Wenn Sie einen IE-Switch SCALANCE X-300 oder X-400 in einem PRP-Netzwerk einsetzen, aktivieren Sie die Option "Oversize Mode".

Innerhalb eines PRP-Netzwerks können überlange Frames mit einer Länge von bis zu 1528 Bytes auftreten. Wenn Sie die Option "Oversize Mode" aktivieren, werden überlange Frames weitergeleitet.

Switch Enabled Protocols

Im mittleren Bereich der Maske können Sie folgende Protokolle für die Verwaltung des Datenverkehrs einschalten bzw. ausschalten:

GMRP

GMRP ist die Abkürzung für GARP Multicast Registration Protocol. Dabei steht GARP für Generic Attribute Registration Protocol. GMRP ist ein Verfahren für die effiziente Weiterleitung von Multicast-Frames.

Mit einem GARP Information Declaration (GID) kann sich ein Teilnehmer beim IE-Switch als Empfänger für eine Multicast-Adresse registrieren. Ein IE-Switch sendet diese Registrierung in Form des GARP Information Propagation (GIP) Frames an seinen Ports aus. Somit ist auch anderen Switches diese Adresse bekannt und sie senden Multicast-Frames für diese Adresse nur an den Ports heraus, die eine Registrierung für diese Adresse empfangen haben. Damit wird die durch Multicast-Frames generierte Last im Gesamtnetz und bei Teilnehmern, die nicht für einen Multicast registriert sind, reduziert.

Wenn Sie GMRP aktivieren, werden für alle Ports GMRP Registrierungen in der Multicast-Filtertabelle eingetragen und selbstständig generiert.

Wenn GMRP nicht aktiviert ist

- wertet ein IE-Switch empfangene GMRP Frames nicht aus.
- versendet ein IE-Switch keine eigenen GMRP Frames.

IGMP Snooping

IGMP ist die Abkürzung für Internet Group Management Protocol. Es ist eine Erweiterung des IP-Protokolls und ermöglicht die Zuordnung von IP-Adressen zu Multicast-Gruppen.

Ein IE-Switch wertet IGMP-Pakete von Multicast-Empfängern aus und speichert die gewonnenen Informationen in seiner Multicast-Filtertabelle. Filtereinträge aufgrund der IGMP Configuration werden in der Filtertabelle als solche gekennzeichnet.

Wenn Sie IGMP Snooping aktivieren, werden IGMP-Einträge in die Filtertabelle aufgenommen und IGMP-Pakete entsprechend weitergeleitet.

Es werden IGMPv1, IGMPv2 und IGMPv3 unterstützt.

Hinweis

GMRP und IGMP können nicht gleichzeitig betrieben werden.

GVRP

GVRP ist die Abkürzung für GARP VLAN Registration Protocol.

Wenn Sie GVRP aktivieren, kann die Portzugehörigkeit zu einem VLAN dynamisch über GVRP gesetzt werden.

Hinweis

GVRP und MSTP können nicht gleichzeitig betrieben werden.

DHCP Option 82

Wenn Sie DHCP Option 82 aktivieren, fügt der IE-Switch an DHCP-Anfragen ein "Option 82"-Feld an, bevor die Anfrage an den DHCP-Server weitergeleitet wird (sofern die empfangene Anfrage kein entsprechendes Feld besitzt). Das "Option 82"-Feld enthält Informationen zur Lokalisierung des neuen Clients im Netz.

Als Gerätekennung des IE-Switches kann wahlweise die IP-Adresse oder die MAC-Adresse eingestellt werden. Die Gerätekennung sowie die Adressen eines oder mehrerer DHCP-Server können im Menüpunkt DHCP Relay Agent Configuration konfiguriert werden.

VLAN 0 Aware Mode (nur bei SCALANCE X-300)

Wenn Sie VLAN 0 Aware Mode aktivieren, wird bei Frames mit VLAN-ID 0 das VLAN-Tag nicht geändert bzw. gelöscht.

Diese Einstellung hat nur Einfluss auf Ports, die Untagged Member in VLAN-ID 1 sind.

Wenn die Option VLAN 0 Aware Mode aktivert ist, können Sie keine VLAN-Konfigurationen vornehmen. Um die VLAN-IDs der Ports zu ändern, müssen Sie diese Option deaktivieren.

Spanning Tree Protocol

Im unteren Bereich der Maske können Sie folgende Redundanzverfahren einschalten bzw. ausschalten:

STP

STP (Spanning Tree Protocol) ist eine Methode, mit der bei redundanten Netzstrukturen Schleifen verhindert werden.

Wenn Sie STP aktivieren, ist die Spanning Tree-Funktionalität aktiviert.

Typische Rekonfigurationszeiten bei Spanning Tree liegen zwischen 20 und 30 Sekunden.

RSTP

RSTP (Rapid Spanning Tree Protocol) ist eine Weiterentwicklung des Spanning Tree Protocols. Das Ziel von RSTP ist es, eine schnellere Rekonfiguration im Sekundenbereich zu erreichen.

Wenn Sie RSTP aktivieren, ist die Rapid Spanning Tree-Funktionalität aktiviert.

Wenn an einem Port ein Spanning Tree Frame erkannt wird, fällt dieser Port von RSTP auf STP zurück.

MSTP (nur bei SCALANCE X-300 und SCALANCE X408)

MSTP (Multiple Spanning Tree Protocol) ist eine Weiterentwicklung des Rapid Spanning Tree Protocols. Das Ziel von MSTP ist es, auf einem IE-Switch unabhängige RSTP-Instanzen innerhalb verschiedener VLANs zu betreiben.

Wenn Sie MSTP aktivieren, ist die Multiple Spanning Tree-Funktionalität aktiviert.

Hinweis

Bei aktiviertem Passive Listening leitet der IE-Switch (R/M)STP-Konfigurations-Frames transparent weiter, auch wenn für ihn selbst (R/M)STP deaktiviert ist. Erkennt er ein Topology Change Frame, setzt er die Aging Time für eine begrenzte Zeit herab, um die Teilnehmerliste schneller zu aktualisieren.

Anschließend gilt wieder der ursprüngliche Wert für die Aging Time.

Enhanced Passive Listening Compatibility

Wenn Sie Enhanced Passive Listening Compatibility aktivieren, werden TCN (Topology Change Notifications)-Frames auch dann versendet, wenn Edge-Ports auf Link Up gehen. Bei einem Link Up an Edge Ports werden sonst keine TCN-Frames versendet. In Verbindung mit der Funktion "Auto Edge Port" (Kapitel Spanning Tree Port Parameters (Seite 219)) ist dieser Parameter notwendig, um (R)STP-Netze mit HRP-Ringen zu koppeln. Über Edge Ports werden sonst keine TCN-Frames versendet, dies ist aber für die Passive Listening Funktion (siehe Betriebsanleitung des entsprechenden Switches) auf den Ring-Teilnehmern notwendig.

RSTP Big Network Support

Wenn Sie RSTP Big Network Support aktivieren, werden große RSTP Ringe mit bis zu 80 Bridges unterstützt.

Syntax Command Line Interface

Tabelle 5-39 Switch Configuration - CLI\SWITCH>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen Einstellungen im Switch-Menü an.	-
aging [E|D]	Aktiviert/Deaktiviert die Aging-Funktionalität.	Nur Administrator Default-Wert: Aktiviert
agetime [seconds]	Legt die Aging-Zeit in Sekunden fest.	Nur Administrator Default-Wert ist 30 Sekunden (gilt für SCALANCE X408-2) bzw. 40 Sekunden (gilt für SCALANCE X414-3E).
mirror [E|D]	Aktiviert/Deaktiviert das Port Mirroring.	Nur Administrator
plisten [E|D]	Aktiviert/Deaktiviert Passive Listening.	Nur Administrator

Befehl	Beschreibung	Kommentar
oversize [E|D]	Aktiviert/Deaktiviert die Funktion Oversize Mode.	Nur Administrator
gmrp [E|D]	Aktiviert/Deaktiviert die GMRP-Funktionalität für alle IE-Switch-Ports.	Nur Administrator
igmp [E|D]	Aktiviert/Deaktiviert die IGMP-Funktionalität für alle IE-Switch-Ports.	Nur Administrator
gvrp [E|D]	Aktiviert/Deaktiviert die GVRP-Funktionalität für alle IE-Switch-Ports.	Nur Administrator
opt82 [E|D]	Aktiviert/Deaktiviert die DHCP-Option 82.	Nur Administrator
vlan0 [E|D]	Aktiviert/Deaktiviert den VLAN 0 Aware Mode.	Nur Administrator
rstp [D|S|R|M]	Aktiviert/Deaktiviert die Rapid Spanning Tree-Funktionalität für alle IE-Switch Ports. Die Parameter haben folgende Bedeutung: • D Deaktiviert STP/RSTP • S Aktiviert STP • R Aktiviert RSTP • M Aktiviert MSTP	Nur Administrator
eplc [E|D]	Aktiviert/Deaktiviert die Enhanced Passive Listening Compatibility.	Nur Administrator
bnsupp [E|D]	Aktiviert/Deaktiviert den Big Network Support.	Nur Administrator
macl [E|D]	Aktiviert/Deaktiviert die Funktion Management ACL	Nur Administrator
blkucast [<E|D> [ports]]	Anzeigen/Einstellen von Unknown Unicast Blocking Mask.	Nur Administrator
blkmcast [<E|D> [ports]]	Anzeigen/Einstellen von Unknown Multicast Blocking Mask.	Nur Administrator
blkbcast [<E|D> [ports]]	Anzeigen/Einstellen von Broadcast Blocking Mask.	Nur Administrator
fastlrn [<E|D> [ports]]	Anzeigen/Einstellen von Fast Learning Configuration.	Nur Administrator

5.5.2 Port Status

Konfiguration der Ports im Überblick

Die Maske "Port Status" erscheint, wenn Sie das Ordnersymbol "Ports" angeklickt haben.

Die Maske zeigt für alle Ports des IE-Switches (und gegebenenfalls für die Ports des Extenders) die Konfiguration für den Datentransfer.

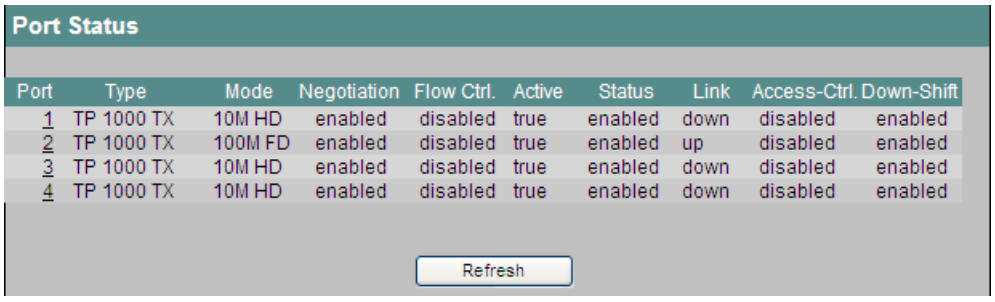


Bild 5-49 Port Status

In den acht Spalten der Tabelle sind folgende Informationen dargestellt:

Port
Hier wird der Steckplatz und der Port angegeben, auf den sich die nachfolgenden Informationen beziehen.

Type
Zeigt Art des Ports an. Diese Angabe ist wichtig, weil auf einigen Steckplätzen verschiedene Module und damit Ports einsetzbar sind. Es gibt folgende Port-Typen:

- TP 100 TX
- FO 100 FX
- FO 100 LD
- FO 100 LH+
- TP 1000 TX
- FO 1000 SX
- FO 1000 LD
- FO 1000 LH
- FO 1000 LH+

Mode
Die Übertragungsgeschwindigkeit (10, 100 oder 1000 Mbit/s) und das Übertragungsverfahren (Vollduplex (FD) oder Halbduplex (HD)).

Negotiation
Zeigt an, ob Autonegotiation aktiviert (enabled) oder deaktiviert (disabled) ist.

Flow Ctrl.
Gibt an, ob für den Port die Flusskontrolle aktiviert (enabled) oder deaktiviert (disabled) ist.

Active
Zeigt an, ob der Port aktiv (true) oder inaktiv (false) ist. Für einen inaktiven Port zeigt der Kommunikationspartner den Verbindungsstatus "Link Down" an.

Status
Zeigt an, ob der Port eingeschaltet (enabled) oder abgeschaltet (disabled) ist. Datenverkehr ist

nur über einen eingeschalteten Port möglich. Allerdings wird beim Kommunikationspartner eines abgeschalteten Ports der Verbindungsstatus "Link Up" angezeigt.

Hinweis

Die Zustände "Active" und "Status" haben bei PoE-Ports keinen Einfluss auf die Spannungsversorgung. Die Konfiguration der Spannungsversorgung erfolgt davon unabhängig über den Menüpunkt "PoE".

Link
Der Verbindungsstatus zum Netzwerk Es gibt folgende Möglichkeiten:

- 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.

Access Control
Die "Access Control" ist ein Eingangsfilter und zeigt an, ob der Port für nicht bekannte MAC-Adressen gesperrt ist. Es gibt die folgenden zwei Zustände:

- enabled
  Ein Frame mit einer Zieladresse, die nicht in der Adresstabelle des IE-Switches vorhanden ist, wird verworfen. Der IE-Switch nimmt die Quelladresse des zugehörigen Teilnehmers nicht in die Adresstabelle auf.
- disabled (Defaultwert)
  Ein Frame mit einer Zieladresse, die nicht in der Adresstabelle des IE-Switches vorhanden ist, wird weitergeleitet. Der IE-Switch nimmt die Quelladresse des zugehörigen Teilnehmers zusätzlich in die Adresstabelle auf.

  Hinweis

  Die "Access Control" steht seit Firmwarestand 2.2 zur Verfügung und hat die vormalige Funktion "Lock" abgelöst.

Down-Shift

Zeigt an, ob Down-Shift aktiviert (enabled) oder deaktiviert (disabled) ist.

Veränderung der Portkonfiguration

Klicken Sie auf eine Portbezeichnung in der Spalte "Port", um die Seite "Port Configuration" zu öffnen. Sie können dort festlegen, wie der Datenverkehr über diesen Port erfolgen soll.

Hinweis

Optische Ports arbeiten immer mit dem Übertragungsverfahren Vollduplex und mit maximaler Übertragungsgeschwindigkeit. Deshalb können Sie bei optischen Ports folgende Einstellungen nicht vornehmen:

- Autonegotiation
- Übertragungsgeschwindigkeit
- Übertragungsverfahren

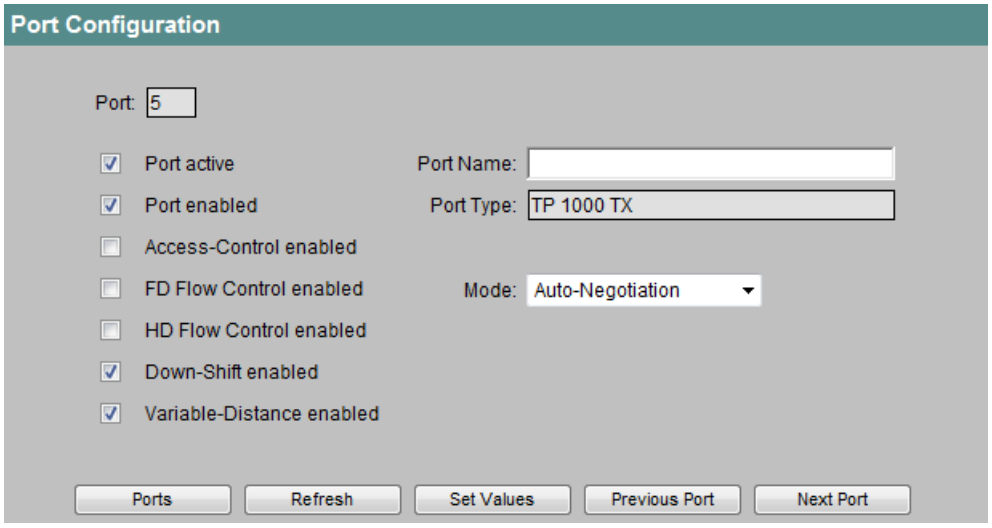


Bild 5-50 Port Configuration

Port
Gibt Port und Steckplatz an, dessen Konfiguration auf der Seite angezeigt wird.

Port active

Mit diesem Optionskästchen können Sie die Zustände "Link Up" und "Link Down" auch für abgeschaltete Ports ("Port enabled" ohne Haken) setzen. Bei markiertem Optionskästchen wird auch für einen abgeschalteten Port dem Kommunikationspartner der Zustand "Link Up" angezeigt.

Port enabled
Aktivieren Sie diese Option, um den Port für den Datenverkehr freizuschalten. Wenn dieses Kontrollkästchen nicht markiert ist, wird dem Kommunikationspartner dieses Ports gleichwohl der Status "Link up" angezeigt. Mit dem Optionskästchen "Port active" kann der Verbindungs-Status verändert werden.

Access-Control enabled
Wenn diese Option aktiviert ist, lernt der IE-Switch an diesem Port keine Unicast-Adressen.

FD Flow Control enabled
Aktiviert / deaktiviert die Flusskontrolle für den Vollduplex-Modus. Die Flusskontrolle ist allerdings nur wirksam, wenn der Port in der Betriebsart Vollduplex arbeitet. Ist die

Flusskontrolle aktiviert aber unwirksam, so verschwindet das gesetzte Häkchen nach einem Refresh der Maske wieder, muss aber bei wirksam werden der Flusskontrolle nicht erneut gesetzt werden.

HD Flow Control enabled
Aktiviert / deaktiviert die Flusskontrolle für den Halbduplex-Modus. Die Flusskontrolle ist allerdings nur wirksam, wenn der Port in der Betriebsart Halbduplex arbeitet.

Hinweis

Bei einer Festeinstellung der Port-Konfiguration auf Ring-Ports, ist ein korrekter Betrieb der Redundanz-Funktion nicht mehr möglich. Für einen korrekten Betrieb ist der Vollduplex-Betrieb der Ring-Ports notwendig. Es wird empfohlen Ring-Ports auf Auto-Negotiation zu stellen.

Hinweis

Der IE-Switch 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 Frames verworfen werden.

Port-Überlastungen treten auf, wenn der IE-Switch mehr Frames empfängt als er senden kann, z.B. infolge unterschiedlicher Übertragungsgeschwindigkeiten.

Down-Shift enabled
Diese Einstellung ist nur bei SCALANCE X-300/X408-2 für Gigabit-Ports mit Twisted Pair-Verkabelung verfügbar.
Wenn diese Option aktiviert ist, kann der Port seine Leistung auf 100 MBit/s verringern, wenn z. B. Probleme mit der Leitung auftreten.

Variable-Distance enabled
Diese Einstellung ist nur verfügbar, wenn sich der Port auf einem Medienmodul MM992-2VD befindet.
Wenn diese Option aktiviert ist, arbeitet der Port in der Betriebsart "Variable Distance" (VD).
Wenn diese Option deaktiviert ist, arbeitet der Port wie ein Standard Gigabit-Port.

Mode
Im Auswahlfeld Mode können Sie die Übertragungsgeschwindigkeit und die Duplexität des Ports einstellen. Wenn Sie den Mode auf Auto-Negotiation stellen, werden diese Parameter automatisch vom IE-Switch mit dem angeschlossenen Endgerät ausgehandelt.

Hinweis

Stellen Sie den Mode auf Auto-Negotiation, falls Sie Auto-Crossover zum Partnerport verwenden möchten.

Port Name
Sie können hier einen Namen für den Port eintragen.

Port Type
Hier wird der Typ des Ports angezeigt. Sie können dieses Feld nicht editieren, weil diese Information hardwareabhängig ist.

Syntax Command Line Interface

Tabelle 5-40 Port-Status - CLI\SWITCH\PORTS>

Befehl	Beschreibung	Kommentar
info [ports]	Zeigt die aktuellen Einstellungen der Ports (den Ist-Zustand) für den Datenverkehr an.	-
cfg [ports]	Zeigt die konfigurierten Einstellungen der Ports (den Soll-Zustand) für den Datenverkehr an.	-
active [<T|F> [ports]]	Aktiviert (T) bzw. deaktiviert (F) die angegebenen Ports.	Nur Administrator.
status [<E|D> [ports]]	Aktiviert/Deaktiviert die angegebenen Port für den Datenverkehr.	Nur Administrator.
fd_flow [<E|D> [ports]]	Aktiviert/Deaktiviert die Flusskontrolle im Vollduplex-Modus.	Nur Administrator.
hd_flow [<E|D> [ports]]	Aktiviert/Deaktiviert die Flusskontrolle im Halbduplex-Modus.	Nur Administrator.
autoneg [<E|D> [ports]]	Aktiviert/Deaktiviert Autonegotiation.	Nur Administrator.
name <port> [string]	Vergibt einen Namen (maximal 64 Zeichen lang) für den angegebenen Port.	Nur Administrator.
actrl [<E|D> [ports]]	Aktiviert/Deaktiviert Access-Control. Der Befehl "actrl" löst mit Firmwarestand 2.2 den Befehl "lock" ab.	Nur Administrator.
speed [<speed>[ports]]	Legt die Übertragungsgeschwindigkeit und Duplexität des Ports fest: • 10H 10 Mbit/Halbduplex • 10F 10 Mbit/Vollduplex • 100H 100 Mbit/Halbduplex • 100F 100 Mbit/Vollduplex	Nur Administrator.
dwnshift [<E|D> [ports]]	Aktiviert/Deaktiviert Down-Shift für den entsprechenden Port.	Nur Administrator.
vd [<E|D>] [ports]	Aktiviert/Deaktiviert die Betriebsart "Variable Distance" (VD) für den entsprechenden Port.	Nur Administrator.
vd_info	Zeigt Informationen zu den Ports in der Betriebsart "Variable Distance" (VD) an.	-

5.5.3 Link Check (SCALANCE X-300/X408-2)

Überwachung optischer Verbindungen im Ring

Bei optischen Übertragungsstrecken sind Störungen möglich, bei denen die optische Verbindung nicht vollständig unterbrochen wird, sondern nur sporadisch Telegramme verloren gehen. Solche Störungen können z. B. durch defekte optische Kabel, verschmutzte Steckverbindungen oder Gerätedefekte verursacht werden.

Der Redundanzmanager eines HRP- oder MRP-Rings mit optischen Verbindungen erkennt bei einer solchen Störung einen "Non-Recoverable Ring Error". Der Redundanzmanager kann die Störung nicht beheben, indem er den Ring schließt. Ein Schließen des Rings würde in diesem Fall zu kreisenden Telegrammen führen.

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.

Voraussetzungen

- Sie können die Funktion Link Check nur bei optischen Ring- und Standby-Ports eines HRP-Rings oder den optischen Ring-Ports eines MRP-Rings aktivieren.

  Hinweis

  Einsatz von Medienmodulen

  Wenn Sie Link Check auf einem optischen Port eines Medienmoduls betreiben, beachten Sie Folgendes:
  - Link Check ist auf dem optischen Port eines Medienmoduls aktiviert.
  - Das Medienmodul soll gegen ein Modul ohne optische Ports ausgetauscht werden.
  - Deaktivieren Sie Link Check, bevor Sie das Medienmodul tauschen.

- 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.
- Bei Mehrfachringen können Sie Link Check nur auf der ersten MRP-Ring-Instanz aktivieren.

Funktionsweise von Link Check

Verhalten bei einer ungestörten Verbindung

Wenn Sie Link Check an zwei verbundenen Ring-Ports aktivieren, tauschen die beiden Verbindungspartner auf diesen Ports zyklisch Link Check-Testtelegramme aus. Die Telegramme, die der eine Verbindungspartner erhält, sendet er an den anderen zurück.

Wenn die Geräte ihre versendeten Telegramme vom Verbindungspartner zurückerhalten, ist die Verbindung für Link Check vorbereitet. Daraufhin erhöhen die Verbindungspartner die Sendefrequenz der Link Check-Testtelegramme und die eigentliche Verbindungsüberwachung ist aktiv.

Verhalten bei einer Störung

Bei aktiver Verbindungsüberwachung können Sie die Anzahl der gesendeten und empfangenen Link Check-Testtelegrammen auf der Seite "Link Check Status" einsehen. Anhand dieser Statistik können Sie bereits kleinere Störungen erkennen, bei denen die Störung noch nicht zum Abschalten der Übertragungsstrecke durch Link Check führt.

Link Check ist ein Point to Point-Protokoll, deshalb dürfen die Link Check-Testtelegramme von einem Switch nicht weitergeleitet werden. Zu diesem Zweck wird die MAC-Adresse des Link Check-Partners beim Starten von Link Check registriert. Ändert sich diese MAC-Adresse ohne Link-Ereignis, wird ein Fault State ausgelöst. Dieser Fehlerzustand wird erst durch einen Link Down zur Problembehebung beendet.

Link Check erkennt eine Verbindung als fehlerhaft und schaltet diese ab, wenn innerhalb bestimmter Zeiträume zu viele Testtelegramme verloren gehen. Link Check verwendet dabei mehrere Zeitintervalle, um sowohl ein sprunghaftes Auftreten von Fehlern als auch eine kontinuierliche, niedrige Fehlerrate erkennen zu können.

Ein Port, der durch Link Check abgeschaltet wurde, muss zurückgesetzt werden, um wieder kommunizieren zu können. Um den Port zurückzusetzen, haben Sie 2 Möglichkeiten:

- Ziehen Sie das Verbindungskabel und stecken Sie es wieder.
- Setzen Sie die Funktion auf beiden Verbindungspartnern über die Schaltfläche "Reset" zurück. Dies muss bei beiden Geräten innerhalb von 30 s erfolgen.

Hinweis

Wenn Sie die Schaltfläche "Reset" 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.

Nach dem Zurücksetzen von Link Check wird die Funktion auf dem Port erneut gestartet und die Statistik wird zurückgesetzt.

Projektierung über einen PROFINET IO-Controller

Wenn MRP über einen PROFINET IO-Controller projektiert wird, können Sie die Funktion Link Check per WBM oder CLI für die optischen Ringports der 1. MRP-Ring-Instanz zuschalten.

Wenn eine neue Projektierung übertragen wird, wird Link Check auf allen Ports automatisch deaktiviert, die nicht als Ringports der 1. MRP-Ring-Instanz konfiguriert wurden.

Hinweis

Ereignisse, die die Funktion Link Check betreffen, werden nur indirekt durch PROFINET IO gemeldet. Falls die MRP-Diagnosealarme aktiviert sind und ein Ringport durch LinkCheck deaktiviert wird, wird von Profinet IO eine Fehlermeldung generiert, dass diese Verbindung nicht mehr besteht.

Überwachung der Verbindung

Die Maske "Link Check Status" erscheint, wenn Sie den Menüpunkt "Link Check" angeklickt haben.

Die Maske zeigt Folgendes an:

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

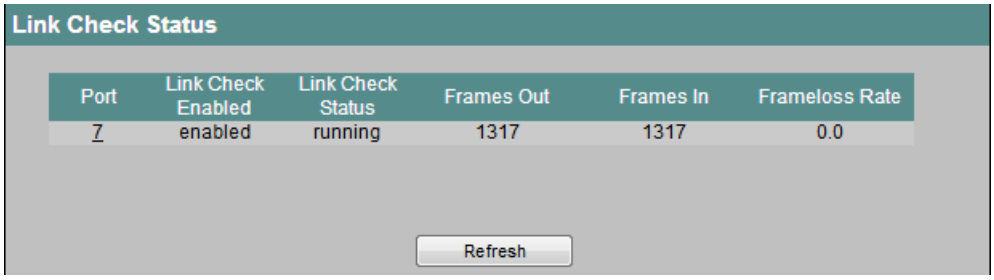


Bild 5-51 Link Check Status

In der Tabelle sind folgende Informationen dargestellt:

Port

Zeigt Steckplatz und Port an, auf den sich die nachfolgenden Informationen beziehen.

Link Check Enabled

Zeigt an, ob die Funktion Link Check aktiviert oder deaktiviert ist.

Link Check Status

Zeigt den Status der Funktion Link Check. Es gibt folgende Zustände:

- disabled
  Die Funktion ist deaktiviert.
- enabled
  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.
- fault
  Die Funktion ist aktiviert. Link Check hat einen Fehler auf der überwachten Strecke detektiert und den Port abgeschaltet.

Frames Out

Zeigt an, wie viele Link Check-Testtelegramme gesendet wurden.

Frames In

Zeigt an, wie viele Link Check-Testtelegramme empfangen wurden.

Frameloss Rate

Zeigt die verlorenen Link Check-Testtelegramme in Prozent (%) an. Der Wert bezieht sich immer auf ein Zeitintervall und zeigt keinen Durchschnittswert an.

Wenn sich Link Check im Zustand "running" befindet, zeigt dieser Wert die verlorenen Link Check-Testtelegramme des letzten überwachten Zeitintervalls an. Der Wert eines Zeitintervalls wird so lange angezeigt, bis er durch den Wert des nächsten Intervalls ersetzt wird.

Wenn sich Link Check im Zustand "disabled", "enabled" oder "fault" befindet, ist dieser Wert nicht verfügbar. Es wird "-" angezeigt.

Konfiguration für die Überwachung der Verbindung

Klicken Sie auf eine Portbezeichnung in der Spalte "Port", um die Seite "Link Check Configuration" zu öffnen. Sie können dort Link Check für diesen Port aktivieren bzw. deaktivieren.

ACHTUNG
Stellen Sie sicher, dass die Telegramme, die von Link Check zur Überwachung der optischen Verbindungen genutzt werden, nicht durch eine Überlast an hochprioren Telegrammen im Netzwerk verdrängt werden. Eine Überlast an hochprioren Telegrammen kann z. B. folgende Ursachen haben: • Netzwerkschleifen, durch die es zu einer Vervielfältigung der hochprioren Telegramme kommen kann • Ändern der Prioritäten für die Weiterleitung von Telegrammen bei SCALANCE X-300

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.

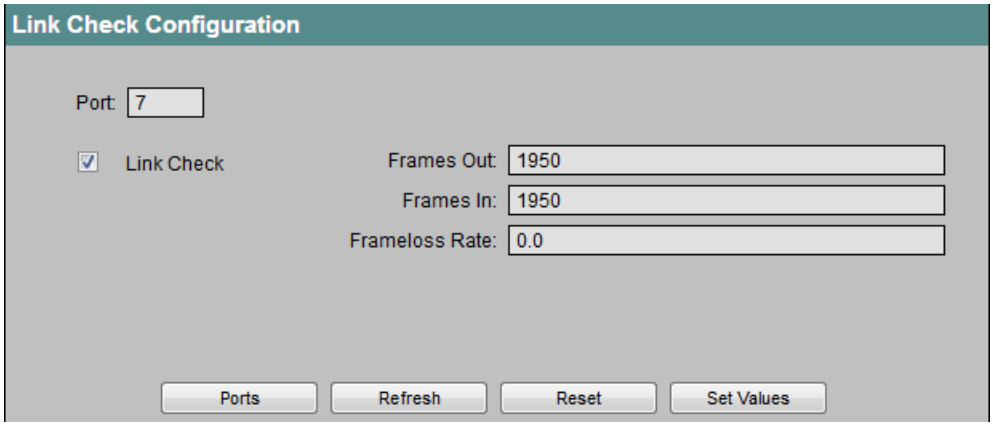


Bild 5-52 Link Check Configuration

Port

Gibt Port und Steckplatz an, dessen Konfiguration auf der Seite angezeigt wird.

Link Check

Mit diesem Optionskästchen aktivieren bzw. deaktivieren Sie die Funktion Link Check für einen Port.

Frames Out

Zeigt an, wie viele Link Check-Testtelegramme gesendet wurden.

Frames In

Zeigt an, wie viele Link Check-Testtelegramme empfangen wurden.

Frameloss Rate

Zeigt die verlorenen Link Check-Testtelegramme in Prozent (%) an. Der Wert bezieht sich immer auf ein Zeitintervall und zeigt keinen Durchschnittswert an.

Wenn sich Link Check im Zustand "running" befindet, zeigt dieser Wert die verlorenen Link Check-Testtelegramme des letzten überwachten Zeitintervalls an. Der Wert eines Zeitintervalls wird so lange angezeigt, bis er durch den Wert des nächsten Intervalls ersetzt wird.

Wenn sich Link Check im Zustand "disabled", "enabled" oder "fault" befindet, ist dieser Wert nicht verfügbar. Es wird "-" angezeigt.

Reset

Nach dem Zurücksetzen von Link Check wird die Funktion auf dem Port erneut gestartet und die Statistik wird zurückgesetzt.

Wenn Sie die Schaltfläche "Reset" verwenden, muss das Zurücksetzen auf beiden Verbindungspartnern innerhalb von 30 s erfolgen.

Hinweis

Wenn Sie die Schaltfläche "Reset" 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.

Syntax Command Line Interface

Tabelle 5-41 Link Check - CLI\SWITCH\LINKCHK>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen Einstellungen der Ports an.	-
linkchk <E|D> [ports]	Aktiviert/Deaktiviert für die angegebenen Ports die Funktion Link Check.	Nur Administrator.
reset <all|ports>	Setzt die Funktion Link Check bei allen oder bestimmten Ports zurück.	Nur Administrator. Wenn Sie den Befehl "reset" 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.

5.5.4 Port Mirroring

Informationen zum Port Mirroring

Datenverlust durch unterschiedliche Datenraten

Wenn die maximale Datenrate des Mirrored Ports höher ist als die des Monitor-Ports, kann es zu Datenverlusten kommen. Der Monitor-Port gibt dann nicht mehr die Abläufe am Mirrored Port wieder.

Einschränkung

Port Mirroring liefert keine 1:1-Darstellung des Netzwerkverkehrs. Defekte Frames werden z. B. bei Empfang verworfen und nicht über den Mirror-Port weitergeleitet.

Konfiguration für die Spiegelung von Ports

Die Maske "Mirroring Configuration" erscheint, wenn Sie den Menüpunkt "Mirroring" angeklickt haben.

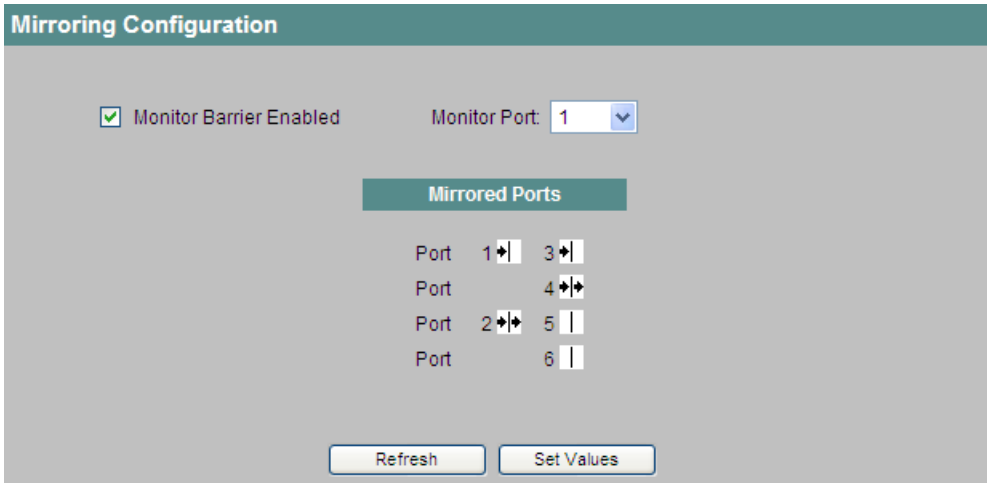


Bild 5-53 Mirroring Configuration

Monitor Barrier Enabled

Mit diesem Kontrollkästchen können Sie die Kommunikation über den Monitor-Port einschränken.

- Aktiviert
  Der Monitor-Port ist vom normalen Switching von Frames ausgenommen.
  Sie können über den Monitor- Port keine Konfiguration oder Diagnose des Gerätes durchführen, z. B. über WBM oder CLI.
- Deaktiviert
  Für die Kommunikation über den Monitor-Port gibt es keine Einschränkung.
  Sie können über den Monitor-Port WBM, CLI und SNMP nutzen.

Diese Option ist im Auslieferungszustand aktiviert.

Monitor-Port

Der Monitor-Port ist der Port, auf den der Datenverkehr von dem/den Mirrored Ports kopiert wird.

Wählen Sie aus der Klappliste den gewünschten Port aus.

Auf einem Monitor-Port können mehrere Ports gleichzeitig gespiegelt werden.

Wenn am Monitor-Port ein Protokollanalysator angeschlossen wird, kann damit der Datenverkehr des Mirrored Ports aufgezeichnet werden, ohne dass die Verbindung am Mirrored Port unterbrochen wird. Dadurch ist eine rückwirkungsfreie Untersuchung des Datenverkehrs möglich. Voraussetzung hierfür ist, dass am IE-Switch ein freier Port als Monitor-Port zur Verfügung steht.

Hinweis

Ein Ringport kann nicht als Monitor-Port verwendet werden.

Mirrored Ports

Die Mirrored Ports sind die Ports, deren Datenverkehr auf den Monitor-Port kopiert wird.

Sie können für jeden Port folgende Einstellungen vornehmen:

- Aktivieren Sie beide Feldhälften.
  Der eingehende und ausgehende Datenverkehr werden kopiert.
- Aktivieren Sie die linke Feldhälfte.
  Nur der eingehende Datenverkehr wird kopiert.
- Aktivieren Sie die rechte Feldhälfte.
  Nur der ausgehende Datenverkehr wird kopiert.

Hinweis

Mehrere Mirrored Ports

Abhängig vom Gerätetyp, können geflutete Frames am Monitor- Port unterschiedlich oft gesendet werden, wenn Sie mehr als einen Port als Mirrored Port ausgewählt haben. Prinzipbedingt sind bei dieser Konfiguration Telegrammverluste am Monitor-Port möglich.

Bei gefluteten Frames handelt es sich um Broadcast-Frames, ungelernte Multicast- oder ungelernte Unicast-Frames.

Syntax Command Line Interface

Tabelle 5-42 Mirroring Configuration - CLI\SWITCH\MIRRORING>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen Einstellungen zu Port-Mirroring.	
mirrport <mode> [ports]	Legt die Ports fest, die überwacht werden (Mirrored Ports).	Nur Administrator
moniport [<port>]	Legt den Monitor-Port fest.	Nur Administrator
barrier [E|D]	Aktiviert/Deaktiviert die Funktion Monitor Barrier.	Nur Administrator

5.5.5 Link Aggregation

5.5.5.1 Link Aggregation

Bündelung von Netzwerk Links für Redundanz und höhere Bandbreite

Die Link Aggregation nach IEEE 802.3ad erlaubt es, mehrere Links zwischen benachbarten Geräten zu bündeln, um so höhere Bandbreiten zu erreichen und zusätzlich für Ausfallsicherheit zu sorgen.

Hierbei werden Ports auf beiden Partnergeräten in Link Aggregationen eingebunden und dann die Geräte über diese Ports miteinander verbunden. Um Ports (also Links) korrekt einem

Partnergerät zuzuordnen, wird das Link Aggregation Control Protokoll (LACP) aus dem Standard IEEE 802.3ad verwendet.

Hinweis

Die zu einer Link Aggregationen gebündelten Ports werden als ein virtueller Port (z.B. AG1) betrachtet und können in CLI-Befehlen anstelle der einzelnen Portnummern verwendet werden.

Vorgehensweise beim Projektieren von Link Aggregations

1. Suchen Sie sich zunächst die Ports aus, die Sie zwischen den Switches zu einer Link Aggregation verbinden wollen.
2. Konfigurieren Sie die Link Aggregation auf beiden Geräten.
3. Führen Sie dann die Verkabelung durch.

Hinweis

Wenn Sie die Verkabelung von aggregierten Links **vor** der Konfiguration durchführen, können Sie Schleifen im Netzwerk erzeugen!

Master Port

Als Master Port einer Link Aggregation wird der Port bezeichnet der seine Einstellungen und auch seine MAC-Adresse an die ganze Link Aggregation vererbt.

Wird beim Anlegen einer Aggregation kein Master Port konfiguriert, wird automatisch der Port mit der kleinsten Portnummer als Master Port verwendet.

Anzeige der konfigurierten Link Aggregations

In dem Menü werden alle konfigurierten Link Aggregationen angezeigt.

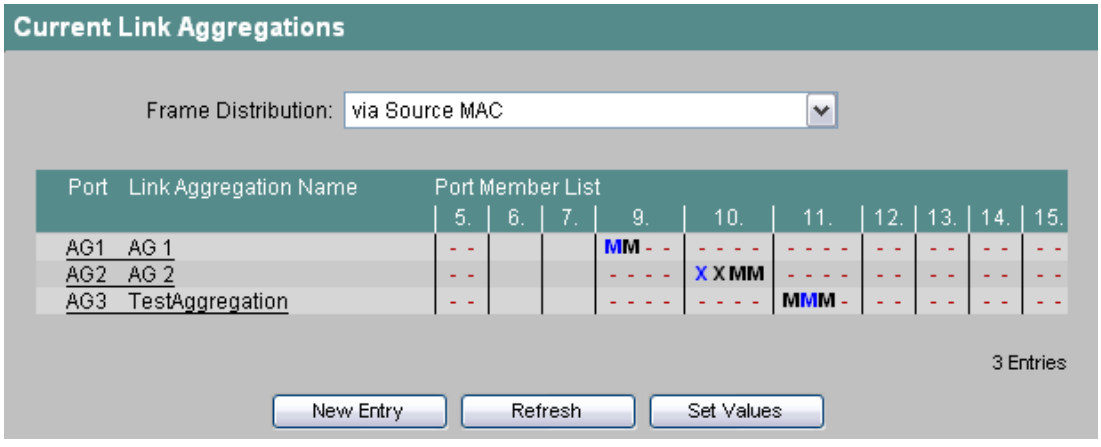


Bild 5-54 Current Link Aggregations

Frame Distribution

Stellt die Art der Verteilung von Paketen auf die einzelnen Links einer Aggregation ein. Es gibt hardwarebedingte unterschiedliche Einstellungsmöglichkeiten bei SCALANCE X-300/408 und SCALANCE X414.

Port

Zeigt die virtuelle Portnummer dieser Link Aggregation. Diese wird intern von der Firmware vergeben.

Link Aggregation Name

Zeigt den frei konfigurierbaren Name der Link Aggregation. Dieser Name kann bei der Konfiguration vom Benutzer angegeben werden.

Port Member List

Zeigt die Ports an, die zu dieser Aggregation gehören. Dabei bedeuten:

- M (schwarz): Der Port ist Mitglied der Aggregation
- M (blau): Der Port ist Mitglied der Aggregation und ist ihr Master Port.
- X (schwarz) Der Port ist Mitglied der Aggregation, jedoch zur Zeit nicht aktiv.
  Port nicht aktiv heißt hier, er wurde dynamisch aus der Aggregation genommen. Gründe dafür können sein:
  - Ports der Aggregation sind unterschiedlich konfiguriert (z. B. Geschwindigkeit)
  - Port ist nicht zum gleichen Gerät verbunden
  - Port hat keinen Link
  - Port wurde nicht per 802.1x authentifiziert
  - ...
- X (blau) Der Port ist Mitglied der Aggregation und ist ihr Master Port und nicht aktiv.

Hinweis

Beim SCALANCE X414-3E können die Gigabit-Ports 5.1 und 5.2 zwar mit einem Fast-Ethernet-Port in eine Aggregation konfiguriert werden, sie werden aber NIE gemeinsam mit anderen Fast-Ethernet-Ports aktiv sein, selbst wenn sie auf Fast-Ethernet eingestellt sind.

Anlegen einer neuen Link Aggregation

Klicken Sie die Schaltfläche New Entry, um eine neue Link Aggregation anzulegen. Folgende Maske erscheint:

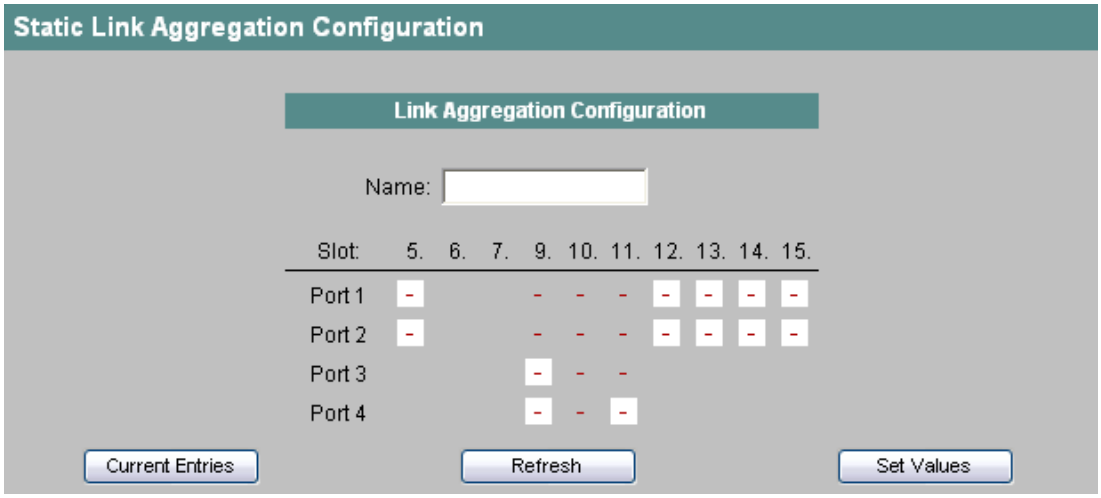


Bild 5-55 Link Aggregation Configuration

Name

Hier können Sie einen symbolischen Namen für die neue Link Aggregation festlegen. Wird hier vom Anwender kein Namen eingetragen, wird er automatisch vom System festgelegt.

Slot/Port

Hier können Sie bestimmte Ports zu der neuen Aggregation hinzuzufügen. Es können nur die Ports hinzugefügt werden, die nicht Mitglied in einer anderen Link Aggregation sind.

Dabei bedeuten:

- M (schwarz): Der Port ist Mitglied der Aggregation
- M (blau): Der Port ist Mitglied der Aggregation und ist ihr Master Port.

Ändern einer Link Aggregation

Klicken Sie in der Maske Current Link Aggregation Übersicht auf die Spalte Port oder Link Aggregation Name, um die Konfiguration einer angelegten Link Aggregation zu ändern.

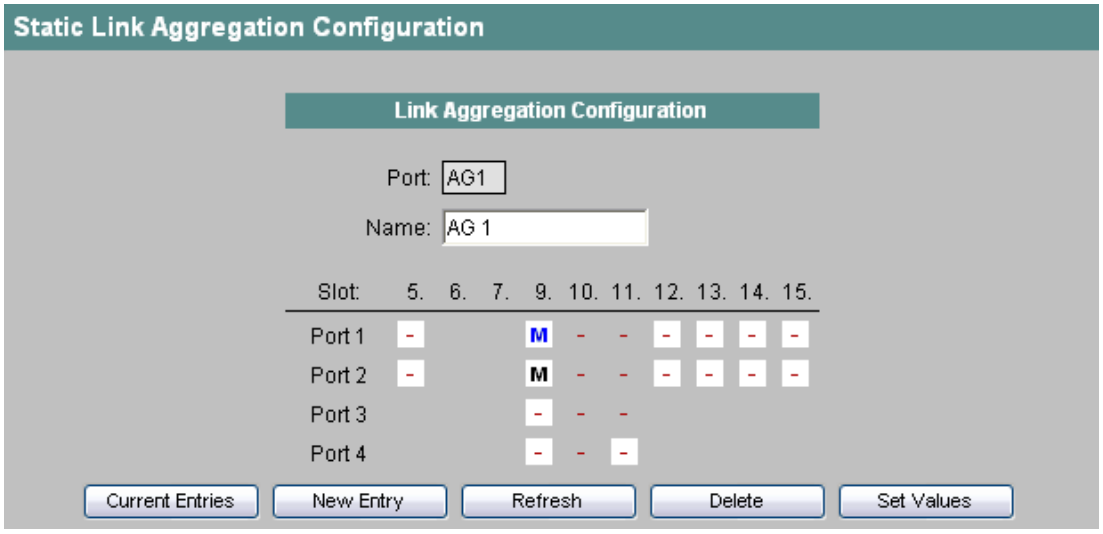


Bild 5-56 Static Link Aggregation Configuration

Port

Zeigt die virtuelle Port Nummer der Aggregation an. Diese wird systemintern vergeben und ist nicht änderbar.

Name

Hier können Sie den Namen der Link Aggregation ändern.

Slot/Port

Hier haben Sie die Möglichkeit, bestimmte Ports zu der Link Aggregation hinzuzufügen oder zu entfernen. Es können nur die Ports geändert werden, die nicht Mitglied in einer anderen Link Aggregation sind.

Dabei bedeuten:

- M (schwarz): Der Port ist Mitglied der Aggregation
- M (blau): Der Port ist Mitglied der Aggregation und ist ihr Master Port.

Ändern des Masterports

Um den Master Port zu ändern gehen Sie wie folgt vor:

1. Klicken Sie auf den ursprünglichen Master Port (blaues M) - die Markierung verschwindet. Soll der Port in der Aggregation bleiben, klicken Sie ein weiteres Mal (schwarzes M)
2. Klicken Sie auf den neuen Master Port bis ein blaues M erscheint.

Syntax Command Line Interface

Current Link Aggregation - CLI\SWITCH\LAG>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen Einstellungen der Link Aggregation (den Ist-Zustand) an.	-
frmdistr [mode]	Stellt die Art der Verteilung von Paketen auf die einzelnen Links einer Aggregation ein. Folgende Modi gibt es für X414: • srcmac Source MAC-Adresse • dstmac Destination MAC-Adresse • mac Source und Dest. MAC-Adresse • srcip Source IP-Adresse • dstip Destination IP-Adresse • ip Source und Dest. IP-Adresse) Folgende Modi gibt es für X408/X-300: • hash Source und Dest. MAC-Adresse Hash • xor Source und Dest. MAC-Adresse Xor	Nur Administrator.
add <masterport>	Erstellt eine neue Link Aggregation mit dem angegebenen Master Port	Nur Administrator.
master <ID> <masterport>	Ändert den Master Port einer Link Aggregation.	Nur Administrator.
name <ID> <string>	Ändert den Namen einer Link Aggregation.	Nur Administrator.
ports <ID> <option> [ports]	Ändert die Mitglieder (Ports) einer Link Aggregation - außer dem Master Port. Folgende Optionen sind möglich: • - Der Port ist nicht Mitglied der Link Aggregation. • M Der Port ist Mitglied der Link Aggregation.	Nur Administrator.
delete <ID>	Löscht eine Link Aggregation.	Nur Administrator.

5.5.5.2 LACP Configuration

Aktivieren der LACP- Funktionalität

Das LACP (Link Aggregation Control Protocol) übernimmt die Auswahl der aktiven Ports einer Link Aggregation. LACP können Sie für jede Link Aggregation aktivieren.

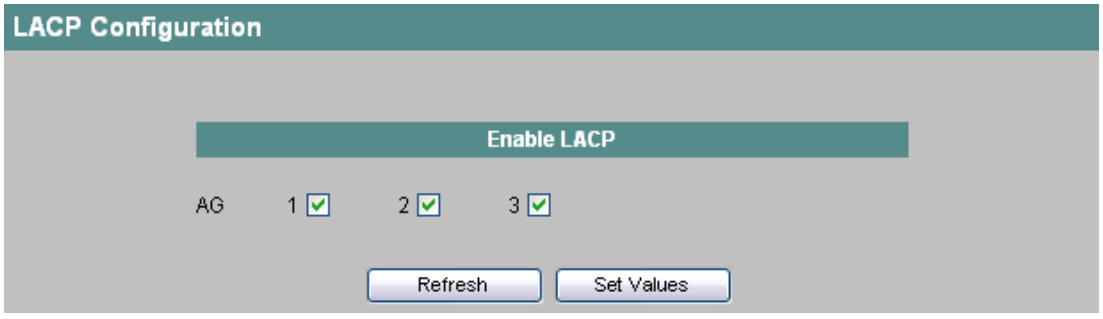


Bild 5-57 LACP Configuration

Enable LACP

Hier aktivieren Sie LACP.

Wenn LACP aktiviert ist, senden die Ports entsprechende LACP-Frames. Wenn das Partner-Gerät LACP-Frames zurücksendet, werden die Ports der LinkAggregation aktiviert.

Wenn LACP deaktiviert ist, werden die Ports der LinkAggregation sofort aktiviert.

Syntax Command Line Interface

Tabelle 5-43 LACP Configuration - CLI\SWITCH\LAG>

Befehl	Beschreibung	Kommentar
lacp [<E|D> [IDs]]	Aktiviert/Deaktiviert LACP für alle Ports der übergebenen Link Aggregation.	Nur Administrator.

5.5.6 IEEE 802.1x

5.5.6.1 802.1x RADIUS Configuration

Authentifizierung über einen externen Server

Das Konzept von RADIUS basiert auf einem externen Authentifizierungsserver. Über diesen Server authentifiziert der IE-Switch angeschlossene Endgeräte. Sie können damit für Endgeräte den Zugang zum Netzwerk über den IE-Switch erlauben bzw. eingeschränken.

Konfigurieren Sie dafür den RADIUS-Server und legen Sie für die Ports die Authentifizierungsverfahren fest.

802.1x RADIUS Configuration

Die Maske "802.1x RADIUS Configuration" erscheint, wenn Sie das Ordnersymbol "RADIUS Config" angeklickt haben.

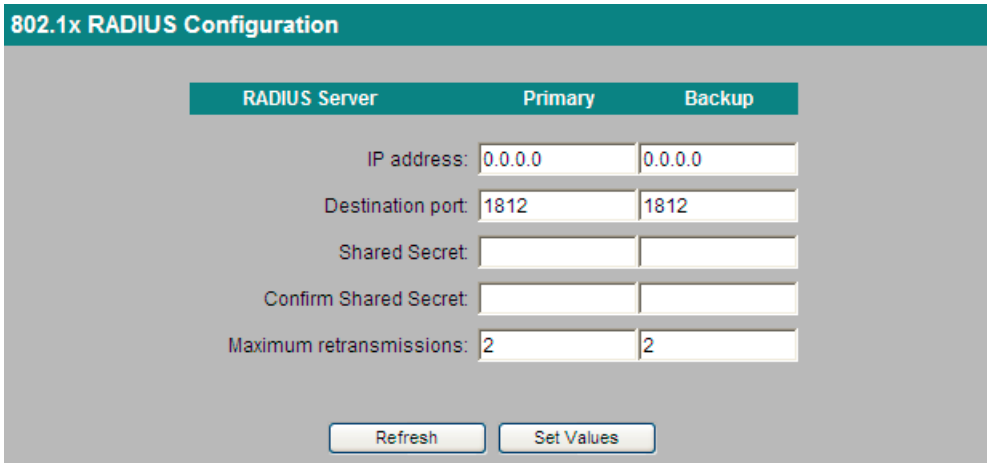


Bild 5-58 802.1x RADIUS Configuration

Legen Sie in dieser Maske den RADIUS-Server für das Authentifizierungsverfahren fest.

Die Maske ist so aufgebaut, dass es jedes Feld einmal für den Primary-Server und einmal für den Backup-Server gibt. Der Primary-Server wird zuerst angefragt. Ist der primäre Server nicht erreichbar, wird der Backup-Server angefragt.

Die Maske enthält folgende Felder:

- **IP address**
  Geben Sie im Eingabefeld "IP address" die IP-Adresse des Servers ein.
- **Destination port**
  Geben Sie im Eingabefeld "Destination port" den Eingangs-Port auf dem RADIUS Server ein. Standardmäßig ist der Eingangs-Port 1812 eingestellt. Der Wertebereich ist 1...65535.
- **Shared Secret**
  Geben Sie im Eingabefeld "Shared Secret" Ihre Zugangskennung ein.
- **Confirm Shared Secret**
  Geben Sie im Eingabefeld "Confirm Shared Secret" die Zugangskennung zur Bestätigung erneut ein.
- **Maximum retransmissions**
  Geben Sie im Eingabefeld "Maximum retransmissions" die maximale Anzahl der Anfrageversuche ein, bevor ein anderer konfigurierter RADIUS Server angefragt wird oder die Anmeldung für gescheitert erklärt wird.
  Standardmäßig ist 2 eingestellt. Der Wertebereich ist 1...254.

RADIUS Server

Sie können die Daten für zwei RADIUS-Server eingeben. Die Angaben in der Spalte "Backup" werden verwendet, wenn der in der Spalte "Primary" definierte Server nicht verfügbar ist.

RADIUS-Server für "Login Mode"

Der hier festgelegte RADIUS-Server dient gleichtzeitig als Authentifizerungsserver für die Login-Modi "RADIUS and Local" und "RADIUS", siehe Kapitel System Passwords & Login Mode (Seite 64).

Syntax Command Line Interface

Tabelle 5-44 802.1x RADIUS Configuration - CLI\SWITCH\DOT1X\RADIUS>

Befehl	Beschreibung	Kommentar
info	Zeigt aktuelle RADIUS-Einstellungen an.	-
server [<ip>[:port]]	Legt IP-Adresse und Port des Primary-Servers fest.	Nur Administrator.
serverb [<ip>[:port]]	Legt IP-Adresse und Port des Backup-Servers fest.	Nur Administrator.
secret <string>	Legt das Passwort für den Primary-Server fest.	Nur Administrator.
secretb <string>	Legt das Passwort für den Backup-Server fest.	Nur Administrator.
maxret [number]	Maximale Anzahl der Anfragen an den Primary-Server.	Nur Administrator.
maxretb [number]	Maximale Anzahl der Anfragen an den Backup-Server.	Nur Administrator.

5.5.6.2 802.1x Port Parameters

802.1x Port Parameters

Die Maske "802.1x Port Parameters" erscheint, wenn Sie das Untermenü "Ports" angeklickt haben. Sie zeigt im Überblick die aktuellen Authentifizierungseinstellungen.

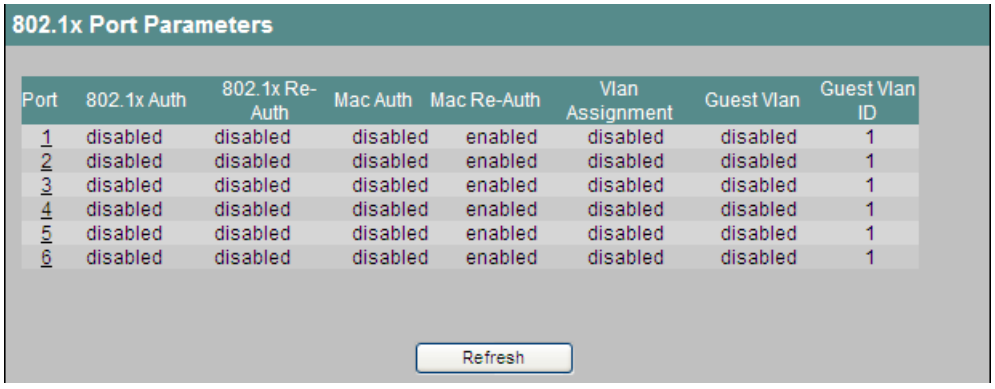


Bild 5-59 802.1x Port Parameters

Die Spalten der Tabelle zeigen folgende Informationen:

- **Port**
  Die Spalte "Port" zeigt die Ports, auf die sich die Informationen beziehen.
- **802.1X Auth**
  Die Spalte "802.1x Auth" zeigt an, ob das Authentifizierungsverfahren "802.1X" für den Port aktiviert (enabled) oder deaktiviert (disabled) ist.
- **802.1X Re-Auth**
  Die Spalte "802.1x Re-Auth" zeigt an, ob die Authentifizierung über "802.1X" für den Port zyklisch wiederholt wird (enabled) oder nicht (disabled).
- **Mac Auth**
  Die Spalte "Mac Auth" zeigt an, ob das Authentifizierungsverfahren "MAC Authentication" für den Port aktiviert (enabled) oder deaktiviert (disabled) ist.
- **Mac Re-Auth**
  Die Spalte "Mac Re-Auth" zeigt an, ob die Authentifizierung über "MAC Authentication" für den Port zyklisch wiederholt wird (enabled) oder nicht (disabled).
- **Vlan Assignment**
  Die Spalte "Vlan Assignment" zeigt an, ob VLAN-Informationen vom Authentifizierungsserver für den Port übernommen (enabled) oder verworfen (disabled) werden.
  Diese Option können Sie nur zusammen mit dem Authentifizierungsverfahren "MAC Authentication" verwenden.
- **Guest Vlan**
  Die Spalte "Guest Vlan" zeigt an, ob die Option "Guest VLAN" für den Port aktiviert (enabled) oder deaktiviert (disabled) ist.
- **Guest Vlan ID**
  Die Spalte "Guest Vlan ID" zeigt die VLAN-ID, die als Guest Vlan für den Port konfiguriert ist.

Syntax Command Line Interface

Tabelle 5-45 802.1x Port Parameters - CLI\SWITCH\DOT1X\PORTS>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen Einstellungen der Ports an.	-

5.5.6.3 802.1x Port Configuration

802.1x Port Configuration

Wenn Sie auf der Seite "802.1x Port Parameters" in der Spalte "Port" eine Portbezeichnung anklicken, gelangen Sie zur Seite "802.1x Port Configuration":

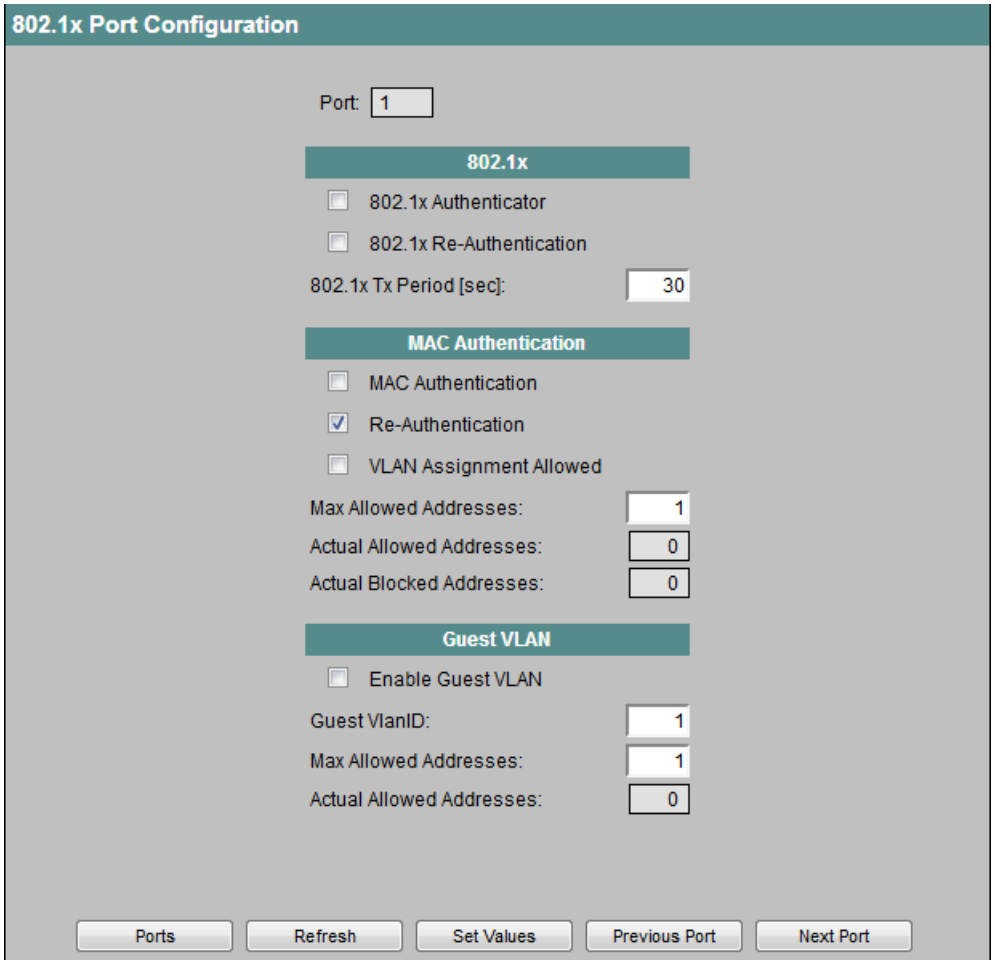


Bild 5-60 802.1x Port Configuration

In dieser Maske können Sie für den jeweils ausgewählten Port die Authentifizierungsverfahren "802.1X" und "MAC Authentication" sowie die Option "Guest VLAN" konfigurieren.

Die Funktionen unterliegen einer hierarchischen Ordnung. Wenn alle drei Funktionen aktiviert sind, wird zunächst versucht, das Endgerät über "802.1X" zu authentifizieren. Ist diese Authentifizierung nicht erfolgreich, wird "MAC Authentication" gestartet. Ist auch diese Authentifizierung nicht erfolgreich, wird das Endgerät im "Guest VLAN" zur Kommunikation freigegeben. "Guest VLAN" kann nur eingesetzt werden, wenn mindestens ein Authentifizierungsverfahren aktiv ist.

Die beiden Authentifizierungsverfahren sind vom Endgerät abhängig. Wenn das Endgerät EAP (Extensible Authentication Protocol) unterstützt, kann es über das Verfahren "802.1X" authentifiziert werden. Wenn das Endgerät kein EAP unterstützt, kann es über "MAC Authentication" authentifiziert werden. In diesem Fall übernimmt der IE-Switch die Rolle des Endgeräts und benutzt die MAC-Adresse des Geräts als Authentifizierungsparameter.

Die Maske enthält folgende Abschnitte und Felder:

Port

Das Anzeigefeld "Port" zeigt den ausgewählten Port an.

Abschnitt "802.1X"

Das Authentifizierungsverfahren "802.1X" läuft wie folgt ab:
Ein Endgerät, das EAP unterstützt, sendet Authentifizierungsinformationen an den IE-Switch. Der IE-Switch übermittelt die Informationen an den RADIUS-Server. Der Authentifizierungsserver prüft die Informationen und ermöglicht bzw. verweigert dem Endgerät den Zugriff auf das Netzwerk.

- **802.1X Authentication**
  Aktivieren Sie diese Option, wenn Endgeräte mit dem Verfahren 802.1X authentifiziert werden sollen.
- **802.1X Re-Authentication**
  Aktivieren Sie diese Option, wenn für ein bereits authentifiziertes Endgerät zyklisch eine Reauthentifizierung durchführt werden soll. Standardmäßig ist eine Stunde (3600 s) fest eingestellt.
- **802.1x Tx Period [sec]**
  Zeitkonstante "txPeriod" in Sekunden, die vom Protokoll 802.1X genutzt wird. Standardmäßig sind 30 Sekunden eingestellt.

Abschnitt "MAC Authentication"

Das Authentifizierungsverfahren "MAC Authentication" läuft wie folgt ab:
Sobald der IE-Switch ein Frame von einem Endgerät empfängt, sendet der IE-Switch eine Anfrage an den RADIUS-Server, um dem Endgerät den Zugang zum Netzwerk zu ermöglichen oder zu verweigern.

- **MAC Authentication**
  Aktivieren Sie diese Option, wenn Endgeräte mit dem Verfahren MAC Authentication authentifiziert werden sollen.
- **MAC Re-Authentication**
  Aktivieren Sie diese Option, wenn für ein bereits authentifiziertes Endgerät zyklisch eine Reauthentifizierung durchführt werden soll. Standardmäßig ist eine Stunde (3600 s) fest eingestellt.

- **VLAN Assignment Allowed**
  Der RADIUS-Server übermittelt dem IE-Switch welchem VLAN das Endgerät angehört. Aktivieren Sie diese Option, wenn die Informationen des Servers berücksichtigt werden sollen. Das Endgerät gehört dann dem entsprechenden VLAN an.
  Wenn die Option deaktiviert ist, werden die VLAN-Informationen verworfen.
- **Max Allowed Addresses**
  Geben Sie im Eingabefeld "Max Allowed Addresses" ein, wie viele Endgeräte gleichzeitig an dem Port angeschlossen sein dürfen.
- **Actual Allowed Addresses**
  Zeigt die Anzahl der momentan an dem Port angeschlossen Endgeräte.
- **Actual Blocked Addresses**
  Zeigt die Anzahl der momentan geblockten Endgeräte.

Abschnitt "Guest VLAN"

Wenn ein Endgerät weder über "802.1X" noch über "MAC Authentication" authentifiziert werden kann, kann das Endgerät in einem vorkonfigurierten Guest VLAN zur Kommunikation freigegeben werden.

- **Enable Guest VLAN**
  Aktivieren Sie diese Option, wenn das Endgerät bei fehlgeschlagener Authentifizierung im Guest VLAN freigeschaltet werden soll.
- **Guest VlanID**
  Geben Sie im Eingabefeld "Guest VlanID" die VLAN-ID des Ports ein.
- **Max Allowed Addresses**
  Geben Sie im Eingabefeld "Max Allowed Addresses" ein, wie viele Endgeräte gleichzeitig an dem Port angeschlossen sein dürfen.
- **Actual Allowed Addresses**
  Zeigt die Anzahl der momentan an dem Port angeschlossen Endgeräte.

Syntax Command Line Interface

Tabelle 5-46 802.1x Port Configuration - CLI\SWITCH\DOT1X\PORTS>

Befehl	Beschreibung	Kommentar
auth [<E|D> [ports]]	Aktiviert / deaktiviert das Authentifizierungsverfahren "802.1X" für den ausgewählten Port.	Nur Administrator.
reauth [<E|D> [ports]]	Aktiviert / deaktiviert die Reauthentication-Funktionalität ("802.1X") für den ausgewählten Port.	Nur Administrator.
macauth [<E|D> [ports]]	Aktiviert / deaktiviert das Authentifizierungsverfahren "MAC Authentication" für den ausgewählten Port.	Nur Administrator.
macreauth[<E|D> [ports]]	Aktiviert / deaktiviert die Reauthentication-Funktionalität ("MAC Authentication") für den ausgewählten Port.	Nur Administrator.

Befehl	Beschreibung	Kommentar
vlanassgn[<E|D> [ports]]	Aktiviert / deaktiviert die Funktion "VLAN Assignment Allowed" für den ausgewählten Port.	Nur Administrator.
guestvlan[<E|D> [ports]]	Aktiviert / deaktiviert die Funktion "Enable Guest VLAN" für den ausgewählten Port.	Nur Administrator.
gvlanid [<1..4094> [ports]]	Zeigt / Setzt die Guest VlanID des ausgewählten Ports.	Nur Administrator.
maxaumac [<1..20> [ports]]	Zeigt / Setzt die Anzahl der Endgeräte, die gleichzeitig an dem Port angeschlossen sein dürfen.	Nur Administrator.
maxaugu [<1..20> [ports]]	Zeigt / Setzt die Anzahl der Endgeräte, die gleichzeitig an dem Port angeschlossen sein dürfen.	Nur Administrator.
txperiod [<1..3600> [ports]]	Zeigt / Setzt die Zeitkonstante "txPeriod" in Sekunden, die vom Protokoll 802.1X genutzt wird. Standardmäßig sind 30 Sekunden eingestellt.	Nur Administrator.

5.5.7 Unicast Filter (ACL)

5.5.7.1 Current Unicast Filter (Access Control List)

Adressfilterung

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

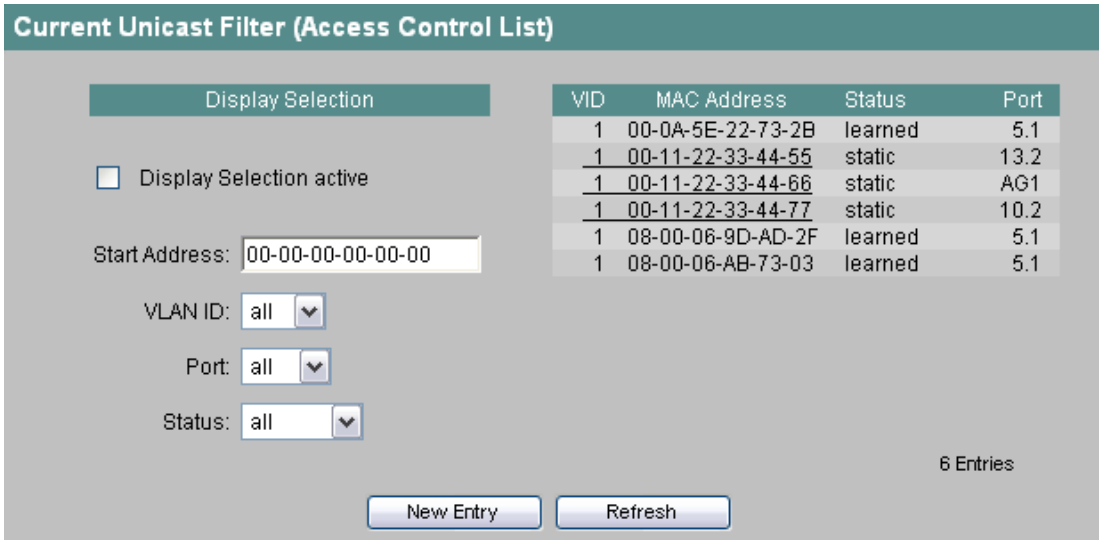


Bild 5-61 Current Unicast Filter

Auswahl der angezeigten Adressen

Display Selection active
Eine Beschränkung der Anzeige auf ausgewählte Elemente erfolgt nur, wenn diese Option aktiviert ist, andernfalls werden alle Adressen angezeigt.

Start Address
Dieser Parameter gibt an, ab welcher Adresse die in der Filtertabelle gespeicherten MAC-Adressen ausgegeben werden sollen. Ist hier nichts eingetragen, dann beginnt die Ausgabe ab der VLAN ID. Wenn Sie hier einen bestimmten Wert eintragen, werden nur Adressen mit einer entsprechenden VLAN ID angezeigt. Gültige Werte für eine VLAN ID liegen zwischen 1 und 4094. Wenn Sie hinsichtlich der VLAN ID keine Auswahl treffen wollen, wählen Sie den Eintrag "all" aus.

Port
Hier können Sie die Anzeige auf Adressen von Teilnehmern an bestimmten Ports beschränken. Wenn Sie den Eintrag "all" auswählen, werden Adressen an allen Ports angezeigt.

Status
Mit diesem Auswahlfeld können Sie die Anzeige auf Adressen beschränken, die einen bestimmten Status haben. Mögliche Werte für den Status sind:

- learned (gelernte Adressen)
- static (vom Anwender projektiert)
- all (gelernte und projektierte Adressen)

Access Control List

Unicast-Filter können für die Zugriffskontrolle verwendet werden. Mithilfe der Access Control-Funktion (ab Firmwarestand 2.2 - davor hieß die Funktion Lock!) einzelner Ports (siehe "Menüpunkt Access Control Port Configuration" bzw. "Das Menü Port Status") können einzelne Ports für unbekannte Teilnehmer gesperrt werden. Ist die Funktion Access Control auf einem Port aktiviert, werden Pakete, die von unbekannten MAC-Adressen kommen sofort verworfen.

Da Ports mit aktivierter Access Control auch keine MAC-Adressen lernen, werden gelernte Adressen auf diesen Ports nach Aktivieren der Access Control automatisch ausgetragen. Um ein Gerät in die Liste der bekannten Teilnehmer aufzunehmen, muss für dessen MAC-Adresse ein Unicast-Eintrag (auf dem entsprechenden Port) angelegt werden.

Um alle angeschlossenen Teilnehmer automatisch einzutragen gibt es eine Funktion zum automatischen Lernen (siehe Kapitel Menüpunkt ACL Learning).

Informationen in der Filtertabelle

Die vier Spalten der Filtertabelle zeigen folgende Informationen:

- **VID**
  Die VLAN-ID, die dieser MAC-Adresse zugeordnet ist. Wenn einer MAC-Adresse keine VLAN-ID zugeordnet ist, wird hier 1 angezeigt
- **MAC Address**
  Die MAC-Adresse des Teilnehmers, die ein IE-Switch gelernt hat oder die der Anwender projektiert hat.
- **Status**
  Zeigt den Status jedes Adress-Eintrags. Dabei bedeutet learned, dass die angegebene Adresse durch Empfang eines Frames dieses Teilnehmers gelernt wurde. Die Angabe static bedeutet, dass die Adresse vom Anwender statisch eingetragen wurde. Statische Adressen sind permanent gespeichert, d.h. sie werden nicht nach Ablauf der Aging time oder beim Restart des Switch gelöscht. Invalid bedeutet, dass diese Werte vom SCALANCE X408 nicht ausgewertet werden. Diese Werte wurden über das Web Based Management ohne Portnummer eingegeben.
- **Port**
  Gibt an, über welchen Steckplatz und welchen Port der Teilnehmer mit der angegebenen Adresse erreichbar ist. Vom IE-Switch empfangene Frames, deren Zieladresse mit dieser Adresse übereinstimmen, werden an diesen Port weitergegeben.

Konfiguration eines Filters

Nach dem Anklicken einer MAC-Adresse mit dem Status *static* gelangen Sie zur Seite für die Filterkonfiguration:

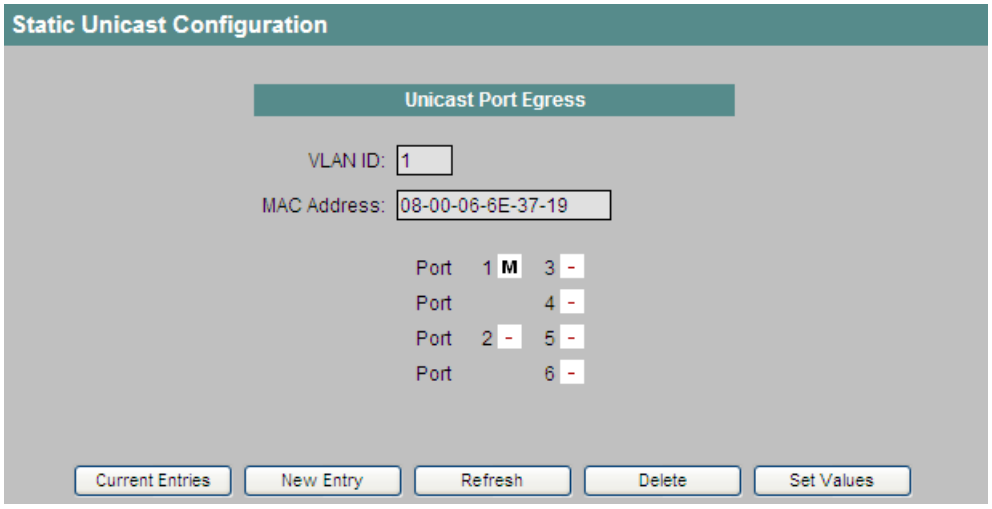


Bild 5-62 Static Unicast Configuration

Slot / Port

Wählen Sie den Steckplatz und den Port aus, an den Frames mit der eingetragenen Zieladresse weitergeleitet werden sollen. Nach dem Anklicken des entsprechenden Feldes erscheint dort eine Statusinformation mit folgender Bedeutung:

- **M**
  (Member) Über diesen Port werden Unicast-Frames gesendet.
- **–**
  Über diesen Port werden Unicast-Frames nicht weitergeleitet.
- **#**
  Der Port ist ungültig.
- **?**
  Die VLAN-Konfiguration steht im Widerspruch zur Unicast-Konfiguration. Das kann der Fall sein, wenn in der Unicast-Konfiguration ein Zielport ausgewählt wurde, der nicht zum VLAN gehört.

Neuen Eintrag erstellen

Klicken Sie die Schaltfläche "New Entry", um der Adresstabelle einen Eintrag hinzuzufügen. Es erscheint die Seite "Static Unicast Configuration", auf der Sie alle notwendigen Eintragungen machen können:

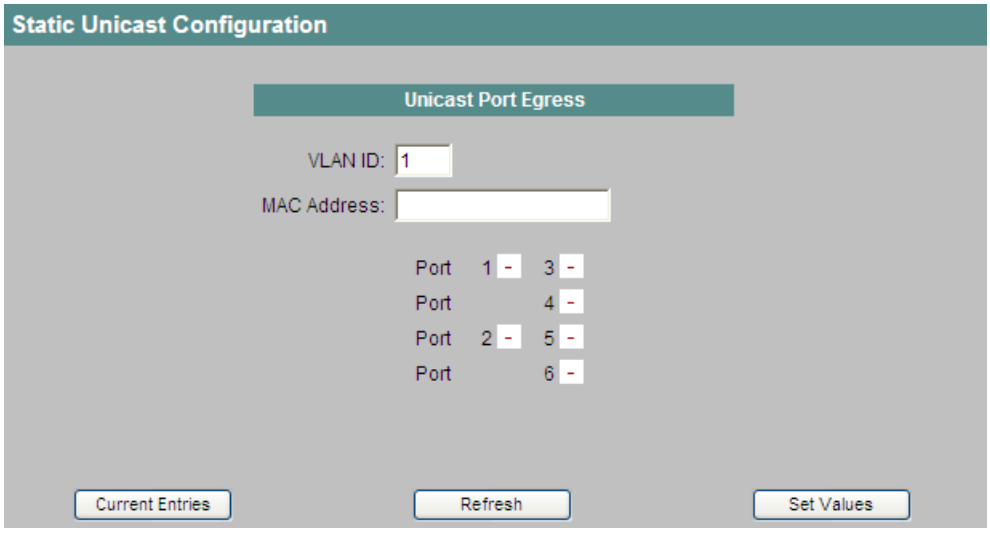


Bild 5-63 Static Unicast Configuration II

VLAN ID
Geben Sie die ID des VLAN ein, zu dem die MAC-Adresse gehört. Wenn nichts vorgegeben wird, ist die VLAN-ID 1 (Default-VLAN) als Grundeinstellung parametriert.

MAC Address
Tragen Sie hier die MAC-Adresse ein, die Sie der Adresstabelle hinzufügen wollen. Diese Adresse entspricht der Zieladresse eines empfangenen Frames.

Slot / Port
Wählen Sie den Steckplatz und den Port aus, an den Frames mit der eingetragenen Zieladresse weitergeleitet werden sollen. Nach dem Anklicken des entsprechenden Feldes erscheint dort ein "M".

Ungültige Ports sind mit einem "#" gekennzeichnet. Für die Ports, die mit einem "?" gekennzeichnet sind, steht die VLAN-Konfiguration im Widerspruch zur Unicast-Konfiguration.

Hinweis

Für Unicast-Adressen können Sie nur **einen** Port angeben.

Current Entries
Durch Anklicken dieser Schaltfläche gelangen Sie zurück zur Liste mit den MAC-Adressen.

New Entry
Klicken Sie diese Schaltfläche, um einen neuen Eintrag in der Filtertabelle zu erstellen.

Delete
Klicken Sie diese Schaltfläche, um den angezeigten Eintrag aus der Filtertabelle zu löschen.

Syntax Command Line Interface

Tabelle 5-47 Current Unicast Filter - CLI\SWITCH\UCAST>

Befehl	Beschreibung	Kommentar
info	Zeigt den Inhalt der Adresstabelle eines IE-Switch an.	-
find [VLAN-ID]<MAC-Adresse> [S|L] [port]	Sucht eine MAC-Adresse in der Adresstabelle eines IE-Switches. Zusätzlich wird angegeben, an welche Ports ein empfangener Frame mit dieser (Ziel)- Adresse gesendet wird. Wenn Sie keine VLAN-ID angeben, werden alle VLANs nach der angegebenen MAC-Adresse durchsucht. Optional können Sie auch einen Port angeben. Die Suche wird dann auf den angegebenen Port beschränkt. Ebenfalls optional können Sie die Suche auf statische und gelernte Einträge beschränken: • S Statische Einträge • L Gelernte Einträge	-
add [VLAN-ID]<MAC-Adresse> <port>	Fügt einen statischen Eintrag für eine Unicast-Adresse in die Adresstabelle ein.	Nur Administrator.
edit [VLAN-ID] <MAC-Adresse> <port>	Ändert einen Eintrag in der Adresstabelle.	Nur Administrator.
delete [VLAN-ID] <MAC-Adresse>	Löscht einen statischen Eintrag aus der Adresstabelle.	Nur Administrator.

5.5.7.2 Access Control List Learning

Start Learning / Stop Learning

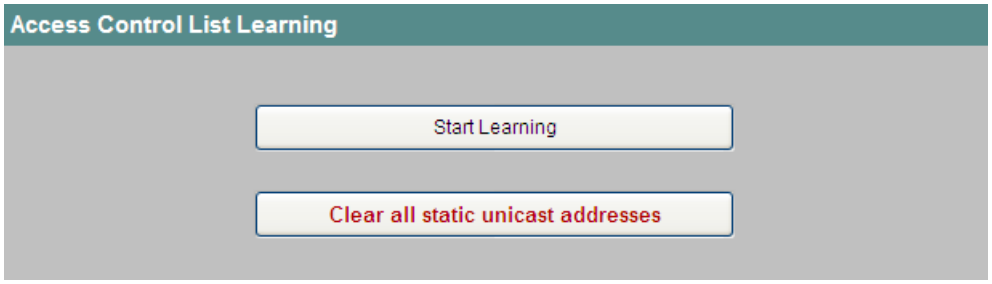


Bild 5-64 Access Control List Learning

Mit Hilfe des Automatischen Lernens können alle am IE-Switch angeschlossenen Geräte automatisch in die Access Control Liste (siehe Kapitel "Menüpunkt Current Unicast-Filter (Access Control List))" eingetragen werden. Solange diese Funktion aktiviert ist, werden alle gelernten Unicast-Adressen sofort als statische Unicast-Einträge angelegt. Das Lernen wird erst wieder durch drücken auf Stop Learning beendet. Auf diese Weise kann wenige Minuten, oder in größeren Netzen auch mehrere Stunden lang gelernt werden, um wirklich alle Teilnehmer zu finden. Es können nur Teilnehmer gefunden werden, die während dem Lernen Pakete senden.

Durch Aktivieren der Access Control-Funktion werden auf den entsprechenden Ports nur noch Pakete von den nach Beendigung des Lernens bekannten Teilnehmern (statische Unicast-Einträge) angenommen.

Hinweis

Ist die Funktion Access Control 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 dann vorher einfach die Access Control auf den Ports, die keine Adressen lernen sollen.

Clear all static unicast addresses
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 diesen Button die Möglichkeit alle statischen Einträge zu löschen. Diese Funktion ist während des automatischen Lernens deaktiviert.

Hinweis

Das Löschen kann je nach Menge der Einträge einige Zeit in Anspruch nehmen.

Syntax Command Line Interface

Tabelle 5-48 Access Control List Learning - CLI\SWITCH\UCAST>

Befehl	Beschreibung	Kommentar
learning [start|stop]	Ohne Parameter: Zeigt den aktuellen Status des automatischen Lernens an. • start Startet das automatische Lernen. • stopp Stoppt das automatische Lernen.	Nur Administrator.
clear	Löscht alle statischen Unicast-Einträge.	Nur Administrator.

5.5.7.3 Access Control Port Configuration

Aktivierung der Funktion Access Control

Durch Aktivieren der entsprechenden Optionen legen Sie individuell für jeden Port fest, ob Access Control aktiviert ist. Wenn für einen Port die Funktion aktiv ist, werden Pakete von unbekannten MAC-Adressen sofort verworfen. Lediglich Pakete von bekannten Teilnehmern (siehe Menüpunkt Current Unicast Filter (Access Control List)) werden angenommen.

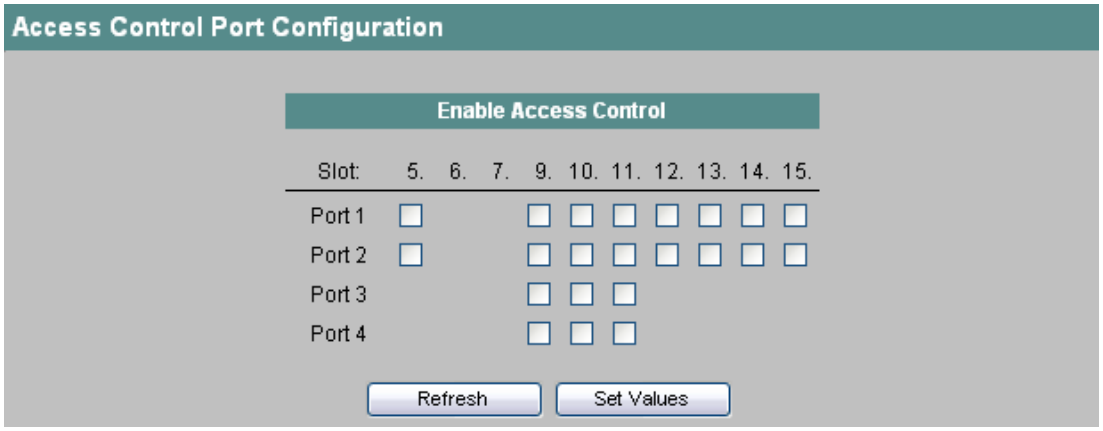


Bild 5-65 Access Control Port Configuration

Syntax Command Line Interface

Tabelle 5-49 Access Control Port Configuration - CLI\SWITCH\UCAST>

Befehl	Beschreibung	Kommentar
actrl [<E|D> [ports]]	Aktiviert/Deaktiviert die Access Control-Funktion für die angegebenen Ports. Wenn Sie keine Ports angeben, wird Access Control für alle Ports aktiviert/deaktiviert.	Nur Administrator.

5.5.7.4 Unknown Unicast Blocking Mask

Sperrung der Weiterleitung von unbekannten Unicast-Frames

In diesem Menü kann das Weiterleiten von unbekannten Unicast-Frames für einzelne Ports gesperrt werden.

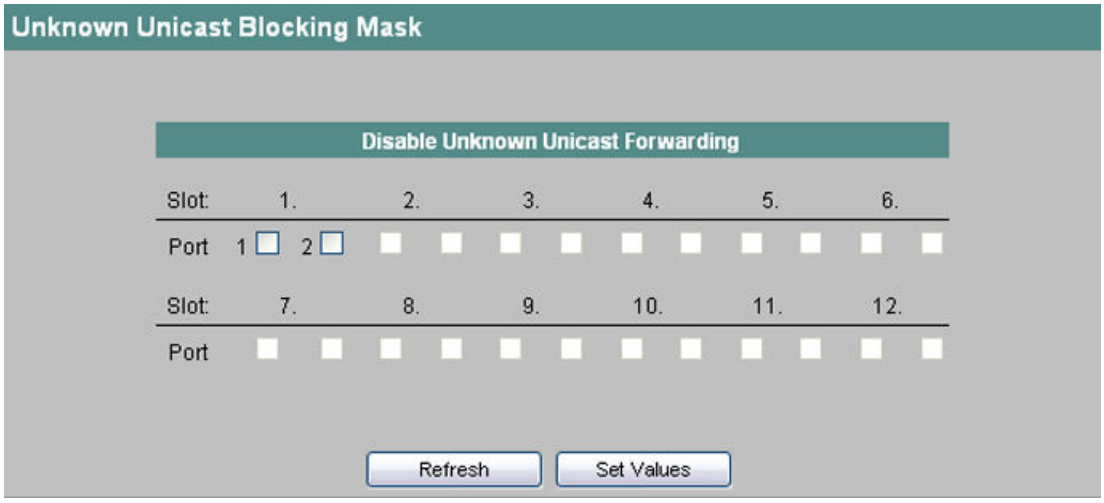


Bild 5-66 Unknown Unicast Blocking Mask

Disable Unknown Unicast Forwarding

Hier legen Sie fest, welche Ports für die Weiterleitung von unbekannten Unicast-Frames gesperrt werden sollen.

Syntax Command Line Interface

Tabelle 5-50 Unknown Unicast Blocking Mask - CLI\SWITCH\>

Befehl	Beschreibung	Kommentar
blkucast [<E|D> [ports]]	Aktiviert/Deaktiviert das Blocken von Unicasts auf den angegebenen Ports.	Nur Administrator.

5.5.8 Multicast Groups

5.5.8.1 Current Multicast Groups

Multicast-Anwendungen

In der Mehrzahl der Fälle wird ein Frame 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 zum Versender von Unicast-Frames bewirken Multicast-Frames bei einem Switch eine höhere Last. Denn generell werden Multicast-Frames an allen Ports eines Switch versendet. Es gibt drei Möglichkeiten, die Last durch Multicast-Frames zu reduzieren:

- Statischer Eintrag der Adressen in die Multicast-Filtertabelle.
- Dynamischer Eintrag der Adressen durch Mithören von IGMP-Parametrierpaketen (IGMP Configuration).
- Aktive dynamische Vergabe von Adressen durch GMRP-Frames.

Alle genannten Verfahren haben zur Folge, dass Multicast-Frames nur an solche Ports versendet werden, für die eine entsprechende Adresse eingetragen ist.

Der Menüpunkt "Multicast Groups" zeigt die aktuell in der Filtertabelle eingetragenen Multicast-Frames mit ihren Zielports. Die Einträge können dynamisch (ein IE-Switch hat sie gelernt) oder statisch (der Anwender hat sie parametriert) erfolgt sein.

Hinweis

Enthält die Filtertabelle bei SCALANCE X414-3E mehr als 500 gelernte Einträge, kann die Rekonfigurationszeit bei redundanten Netzen mehr als 300 Millisekunden bei HRP bzw. 200 Millisekunden bei MRP betragen.

Seiten wechseln

Wählen Sie die Schaltflächen ">>" bzw. "<<", um zwischen den Seiten hin und her zu schalten.

Auf der zweiten Seite werden statt der Ports eventuell eingerichtete Link Aggregationen angezeigt.

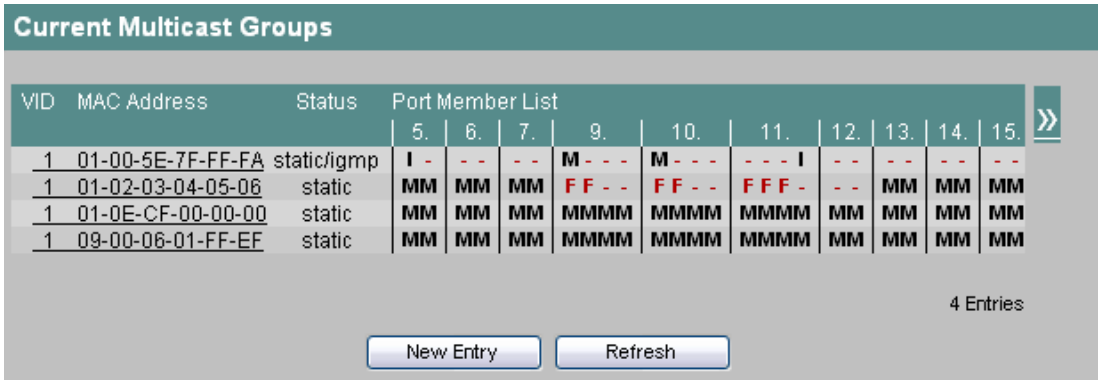


Bild 5-67 Current Multicast Groups

Informationen in der Filtertabelle

Die vier Bereiche der Filtertabelle zeigen folgende Informationen:

VID
Die VLAN-ID, die dieser MAC-Adresse zugeordnet ist.

MAC Address
Die MAC-Adresse des Teilnehmers, die der IE-Switch gelernt hat oder die der Anwender projektiert hat.

Status
Zeigt den Status jedes Adress-Eintrags. Dabei sind folgende Angaben möglich:

- **static**
  Die Adresse wurde vom Anwender statisch eingetragen. Statische Adressen sind permanent gespeichert, d.h. sie werden nicht nach Ablauf der Aging time oder beim Restart des Switch gelöscht.
- **IGMP**
  Der Zielport für diese Adresse wurde über IGMP Configuration ermittelt.
- **GMRP**
  Der Zielport für diese Adresse wurde über einen empfangenen GMRP-Frame registriert.

Port List
Für jeden Steckplatz gibt es eine Spalte. Innerhalb einer Spalte
wird für jeden Port die Zugehörigkeit zur Multicast-Gruppe angegeben:

- **M**
  (Member) Über diesen Port werden Multicast-Frames gesendet.
  M (rote Schrift)
  Der Multicast ist in einem VLAN konfiguriert, das aber nicht an dem betreffenden Port konfiguriert ist. Der Multicast kann aufgrund der abweichenden VLAN-ID nicht über diesen Port weitergeleitet werden.
- **R**
  (Registered) Mitglied der Multicast-Gruppe, die Registrierung erfolgte über ein GMRP-Frame.
- **I**
  (IGMP) Mitglied der Multicast-Gruppe, die Registrierung erfolgte über ein IGMP-Paket.

- **–**
  Kein Mitglied der Multicast-Gruppe über diesen Port werden keine Multicast-Frames gesendet.
- **F**
  (Forbidden) kein Mitglied der Multicast-Gruppe. Außerdem darf diese Adresse auch nicht dynamisch über GMRP oder IGMP gelernt werden.

Neuen Eintrag erstellen

Klicken Sie die Schaltfläche "New Entry", um der Adresstabelle einen Eintrag hinzuzufügen. Es erscheint die Seite Static Multicast Configuration, auf der Sie alle notwendigen Eintragungen machen können:

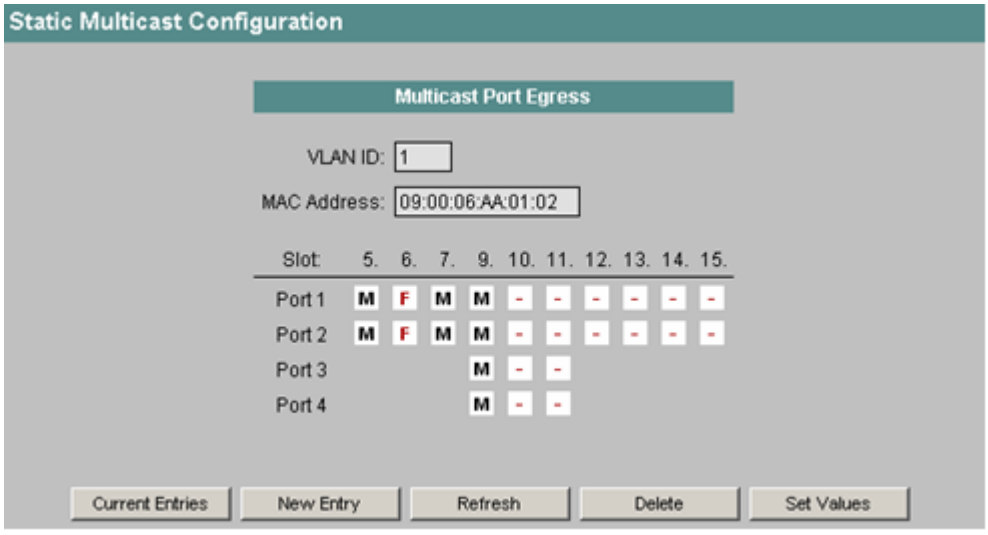


Bild 5-68 Static Multicast Configuration

VLAN ID
Geben Sie die ID des VLAN ein, zu dem die MAC-Adresse gehört. Wenn nichts vorgegeben wird, ist die VLAN ID 1 als Grundeinstellung parametriert.

MAC Address
Tragen Sie hier die MAC-Adresse ein, die Sie der Adresstabelle hinzufügen wollen.

Slot / Port
Wählen Sie hier aus, wie sich ein Port im Bezug auf Multicast-Frames verhalten soll:

- **M**
  Member, über diesen Port werden Multicast-Frames gesendet.
- **–**
  Kein Mitglied der Multicast-Gruppe. Über diesen Port werden keine Multicast-Frames gesendet.
- **F**
  Forbidden, kein Mitglied der Multicast-Gruppe. Außerdem darf diese Adresse auch nicht dynamisch über GMRP gelernt werden.

- **#**
  Der Port ist ungültig.
- **?**
  Der Port ist nicht Mitglied im angegebenen VLAN.

Hinweis

Für Multicast-Adressen können Sie mehrere Ports (Zielteilnehmer) angeben.

Current Entries
Durch Anklicken dieser Schaltfläche gelangen Sie zurück zur Liste mit den MAC-Adressen.

New Entry
Klicken Sie diese Schaltfläche, um einen neuen Eintrag in der Filtertabelle zu erstellen.

Delete
Klicken Sie diese Schaltfläche, um den angezeigten Eintrag aus der Filtertabelle zu löschen.

Adresseintrag verändern

Klicken Sie auf eine MAC-Adresse mit dem Status "static" (in der Adressliste unterstrichen dargestellt), um die Seite "Static Multicast Configuration" für diese Adresse aufzurufen. Nehmen Sie dort die gewünschten Einstellungen vor und bestätigen Sie Ihre Eingaben durch Anklicken der Schaltfläche "Set Values".

Syntax Command Line Interface

Tabelle 5-51 Current Multicast Groups - CLI\SWITCH\MCAST>

Befehl	Beschreibung	Kommentar
info	Zeigt den Inhalt der Adresstabelle eines IE-Switches an.	-
add <VLAN-ID> <MAC-Adresse> [<option> [ports]]	Fügt einen statischen Eintrag für eine Multicastadresse in die Adresstabelle ein. Für den Parameter <option> stehen die folgenden Abkürzungen zur Verfügung: • – Kein Mitglied der Multicast-Gruppe. Über diesen Port werden keine Multicast-Frames gesendet. • m Über diesen Port werden Multicast-Frames gesendet. • f Kein Mitglied der Multicast-Gruppe. Außerdem darf diese Adresse auch nicht dynamisch über GMRP gelernt werden. Beispiele: • add 2 01:02:03:04:05:06 m 5.1-5.2 Ordnet die MAC-Adresse der VLAN-ID 2 zu und die Ports 5.1 und 5.2 sind Member. • add 3 01:02:03:04:05:06 m Legt einen Eintrag für VLAN-ID 3 fest, alle vorhandenen Ports sind Member.	Nur Administrator.
find [VLAN-ID] <MAC-Adresse>	Sucht eine MAC-Adresse in der Adresstabelle eines IE-Switch. Zusätzlich wird angegeben, an welche Ports ein empfangener Frame mit dieser (Ziel)- Adresse gesendet wird. Wenn Sie keine VLAN-ID angeben, werden alle VLANs nach der angegebenen MAC-Adresse durchsucht.	-
edit <VLAN-ID> <MAC-Adresse> <option> [ports]	Ändert einen Eintrag in der Adresstabelle. Für den Parameter <option> stehen die gleichen Abkürzungen zur Verfügung wie beim Befehl add.	Nur Administrator.
delete <VLAN-ID> <MAC-Adresse>	Löscht einen statischen Eintrag aus der Adresstabelle.	Nur Administrator.

5.5.8.2 GMRP Configuration

Aktivierung von GMRP

Durch Aktivieren der entsprechenden Optionen 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 Frames versenden.

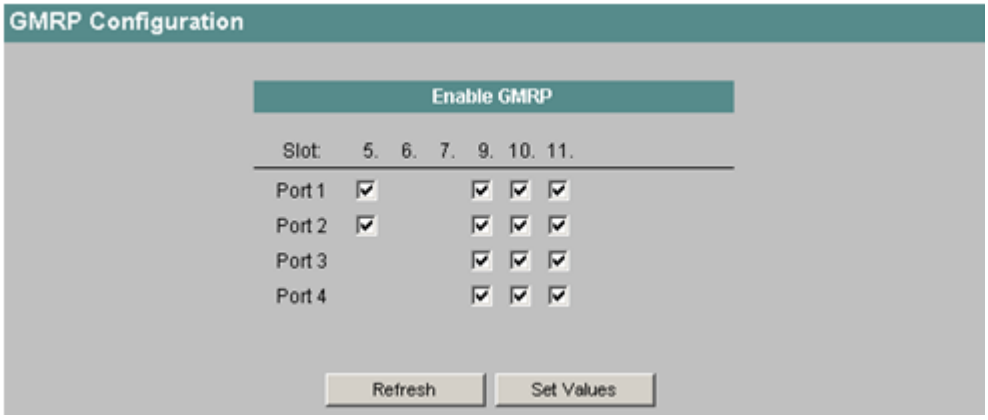


Bild 5-69 GMRP Configuration

Syntax Command Line Interface

Tabelle 5-52 GMRP Configuration - CLI\SWITCH\MCAST>

Befehl	Beschreibung	Kommentar
gmrpport [<E|D> [ports]]	Aktiviert/Deaktiviert die GMRP-Funktionalität für die angegebenen Ports. Wenn Sie keine Ports angeben, wird GMRP für alle Ports aktiviert/deaktiviert.	Nur Administrator.

5.5.8.3 IGMP Configuration

Festlegung der Aging Time

Mit diesem Menü können Sie die Aging Time für die IGMP Configuration festlegen. Nach Ablauf dieser Zeit werden durch IGMP erzeugte Einträge aus der Adresstabelle gelöscht, wenn diese nicht durch ein neues IGMP-Paket aktualisiert werden. Die Festlegung gilt dann für alle Ports, eine portspezifische Konfiguration ist in diesem Fall nicht möglich.

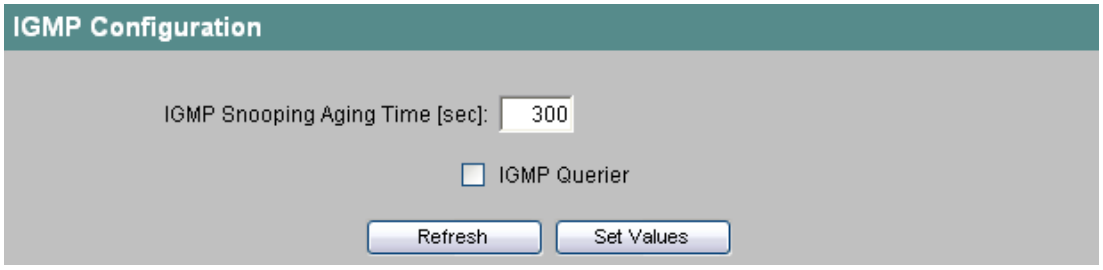


Bild 5-70 IGMP Configuration

IGMP Snooping Aging Time [sec]
Tragen Sie hier den Wert für die Aging Time in Sekunden ein.

IGMP Querier
Aktivieren Sie diese Option, wenn der IE Switch auch IGMP Queries verschicken soll.

Syntax Command Line Interface

Tabelle 5-53 IGMP Configuration - CLI\SWITCH\MCAST\IGMP>

Befehl	Beschreibung	Kommentar
igmptime [number]	Legt die IGMP-Aging-Zeit in Sekunden fest. Ohne Parameter zeigt dieser Befehl die IGMP-Aging-Zeit an.	Nur Administrator.
igmpqry [E|D]	Zeigt/Setzt IGMP Query Enable	Nur Administrator.

5.5.8.4 Unknown Multicast Blocking Mask

Sperrung der Weiterleitung von unbekannten Multicast-Frames

In diesem Menü kann das Weiterleiten von unbekannten Multicast-Frames für einzelne Ports gesperrt werden.

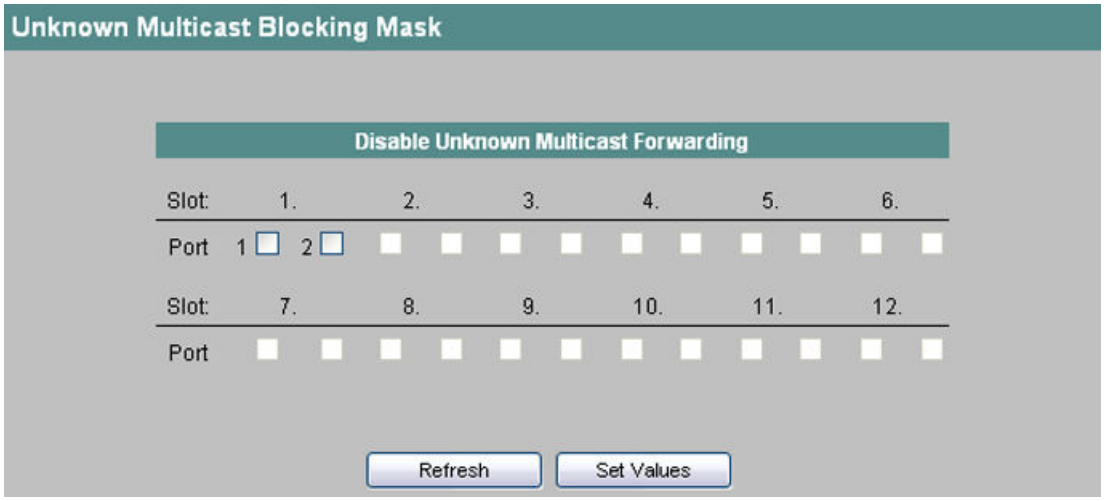


Bild 5-71 Unknown Multicast Blocking Mask

Disable Unknown Multicast Forwarding

Hier legen Sie fest, welche Ports für die Weiterleitung von unbekannten Multicast-Frames gesperrt werden sollen.

Syntax Command Line Interface

Tabelle 5-54 Unknown Multicast Blocking Mask - CLI\SWITCH\>

Befehl	Beschreibung	Kommentar
blkbmcast [<E|D> [ports]]	Aktiviert/Deaktiviert das Blocken von Multicasts auf den angegebenen Ports.	Nur Administrator.

5.5.9 Broadcast Blocking Mask

Sperrung der Weiterleitung von Broadcast-Frames

In diesem Menü kann das Weiterleiten von Broadcast-Frames für einzelne Ports gesperrt werden.

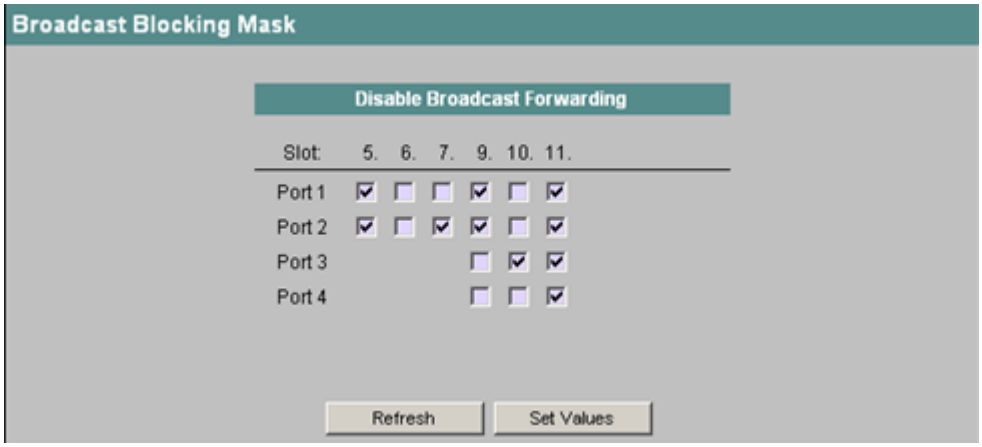


Bild 5-72 Broadcast Blocking Mask

Disable Broadcast Forwarding
Hier legen Sie fest, welche Ports für die Weiterleitung von Broadcast-Frames gesperrt werden sollen.

Hinweis

Einige Kommunikationsprotokolle funktionieren nur mit Unterstützung von Broadcast. In diesen Fällen kann das Sperren zum Ausfall der Datenkommunikation führen. Konfigurieren Sie hier nur, wenn Sie sicher sind, dass Sie auf Broadcast verzichten können und diese explizit vermeiden wollen.

Syntax Command Line Interface

Tabelle 5-55 Broadcast Blocking Mask - CLI\SWITCH\>

Befehl	Beschreibung	Kommentar
blkbcast [<E|D> [ports]]	Aktiviert/Deaktiviert das Blocken von Broadcasts auf den angegebenen Ports.	Nur Administrator.

5.5.10 Fast Learning

Beim Fast Learning werden die an einem Port dynamisch gelernten MAC-Adressen sofort aus der Adresstabelle gelöscht, sobald am betreffenden Port ein Link-Down stattfindet, z. B. durch Umstecken eines Endteilnehmers. Somit erkennt der Switch schneller als herkömmlich, ob eine Portzuweisung noch gültig ist.

Fast Learning wird für jeden Port einzeln festgelegt.

Konfiguration der Ports

In der nachfolgend abgebildeten Maske legen Sie durch Anklicken der entsprechenden Optionskästchen fest, an welchen Ports Fast Learning aktiviert wird.

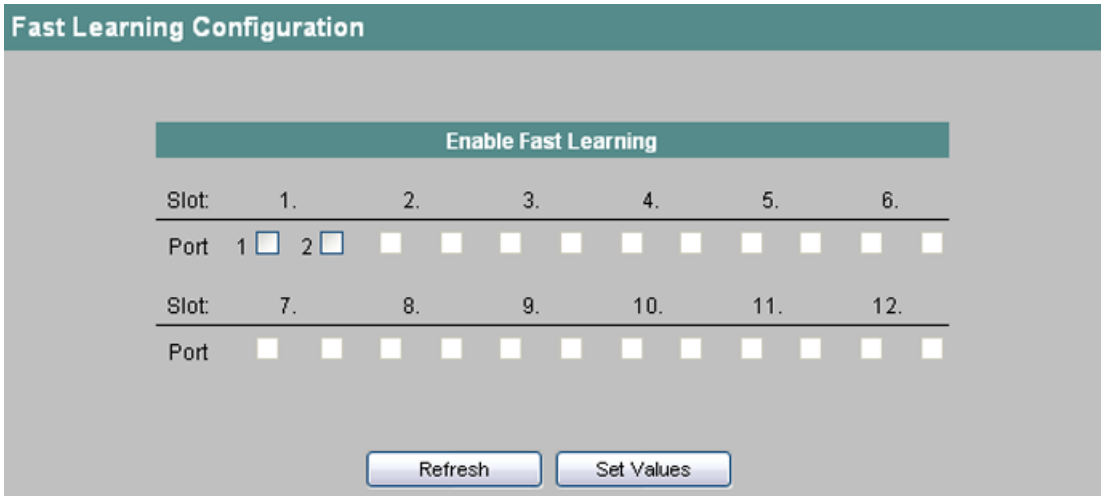


Bild 5-73 Konfiguration für "Fast Learning"

Syntax Command Line Interface

Tabelle 5-56 Fast Learning Configuration - CLI\SWITCH\>

Befehl	Beschreibung	Kommentar
fastlrn [<E|D> [ports]]	Aktiviert/Deaktiviert Fast Learning am entsprechenden Port.	Nur Administrator.

5.5.11 Load Limits Configuration (SCALANCE X414-3E)

Begrenzung der Anzahl eingehender Frames

In diesem Menü können Sie die maximale Anzahl Frames festlegen, die von einem Port pro Sekunde empfangen werden. Hardware-bedingt werden mehrere Ports zu einem Portblock zusammengefasst. Die eingestellten Werte (Packets[s]) sind jedoch pro Port gültig. Sie können festlegen, für welche Kategorie von Frames die eingetragenen Grenzwerte gelten sollen:

- Unicast (Destination Lookup Failure)
- Multicast
- Broadcast

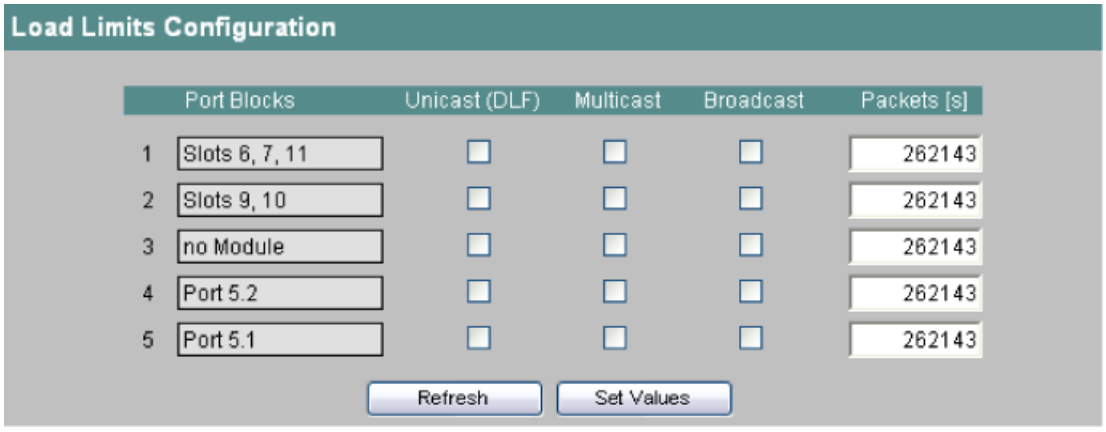


Bild 5-74 Load Limits Configuration

Port Blocks
Die Ports sind folgenden Portblöcken zugeordnet, wobei die Festlegungen für alle Ports eines Portblocks gelten:

- Portblock 1
  Die Ports auf den Steckplätzen 6, 7 und 11.
- Portblock 2
  Die Ports auf den Steckplätzen 9 und 10.
- Portblock 3
  Kein Modul.
- Portblock 4
  Port 2 auf Steckplatz 5.
- Portblock 5
  Port 1 auf Steckplatz 5.

Es werden in dieser Spalte nur die tatsächlich genutzten Steckplätze aufgeführt. Die Textfelder sind nur lesbar.

Unicast (DLF), Multicast, Broadcast
Die maximale Frame-Anzahl pro Sekunde gilt für die Frame-Kategorien, deren Option aktiviert ist.

Packets [s]
Die maximale Anzahl der Frames, die ein Portblock pro Sekunde empfängt. Die über diesen Grenzwert hinaus eintreffenden Pakete werden verworfen.

Hinweis

Die Ringports senden in zyklischen Abständen Multicast-Frames, um Leitungsunterbrechungen zu erkennen. Für Portblöcke, die Ringports beinhalten, sollten Sie deshalb den Empfang von Multicast-Frames nicht beschränken, um die einwandfreie Funktion des Redundanzmanagers zu gewährleisten.

Syntax Command Line Interface

Tabelle 5-57 Load Limits Configuration - CLI\SWITCH\LIMITS>

Befehl	Beschreibung	Kommentar
info <Blocks>	Zeigt die aktuellen Einstellungen für die Limitierung von Paketen an. Die Einstellungen werden nach Portblocks unterteilt angezeigt. Die Portblöcke sind wie folgt definiert: • Port 1 auf Steckplatz 5 • Port 2 auf Steckplatz 5 • Die Ports auf den Steckplätzen 6,7 und 11. • Die Ports auf den Steckplätzen 9 und 10. • Die Ports eines angebauten Extenders, also die Ports der Steckplätze 12 und 13 bei einem Twisted Pair-Extender und die Ports 12 bis 15 bei einem Medienmodul-Extender.	Wird ein Parameter (Blocks) angegeben, zeigt das CLI nur die ausgewählten Werte an.
inmode <E|D> <E|D> <E|D> [blocks]	Legt den Ingress Limitierungs- Modus für Ports fest. Die drei Angaben von E oder D stehen (in dieser Reihenfolge) für • Unicast (DLF) • Multicast • Broadcast Die Portblöcke sind wie beim Befehl info definiert. Beispiele: • inmode E D E 1 Aktiviert Unicast und Broadcast, dekaktiviert Multicast für den Portblock 1. • Inmode D E D Deaktiviert Unicast und Broadcast, aktiviert Multicast für alle Portblöcke.	Nur Administrator. Wird der Parameter (Blocks) nicht angegeben, werden alle Blocks geändert.
ingress <packets> [blocks]	Legt für jeden Portblock die maximale Anzahl der eingehenden Pakete fest, die vom IE-Switch verarbeitet werden. Die Portblöcke sind wie beim Befehl info definiert.	Nur Administrator. Wird der Parameter (Blocks) nicht angegeben, werden alle Blocks geändert.

5.5.12 Load Limits Rates (SCALANCE X-300/X408-2)

Begrenzung der Transferrate eingehender und ausgehender Daten

In diesem Menü wird die konfigurierte Lastbegrenzung (maximale Anzahl Frames pro Sekunde) angezeigt. Die eingestellten Werte sind pro Port gültig. Sie können festlegen, für welche Kategorie von Frames die eingetragenen Grenzwerte gelten sollen. Die Konfiguration können Sie vornehmen, indem Sie auf den jeweiligen Eintrag klicken.

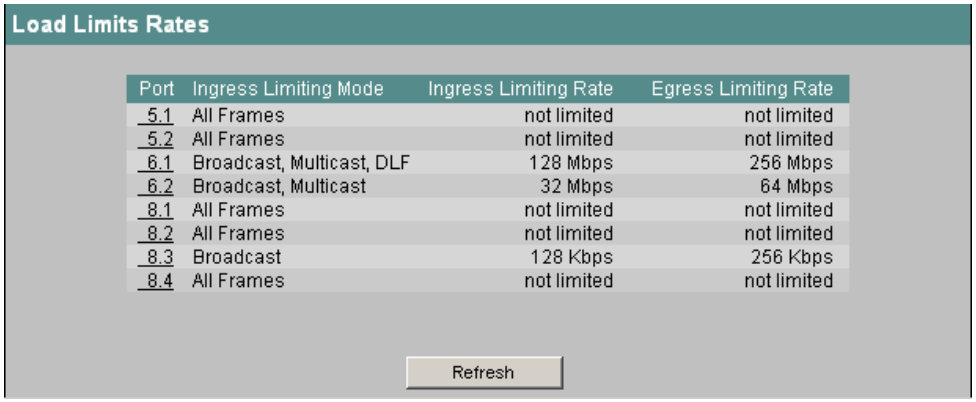


Bild 5-75 Load Limits Rates

Port
Anzeige des jeweiligen Steckplatzes und des dazugehörigen Ports, auf das sich die weiteren Angaben beziehen. Die Konfiguration können Sie ändern, indem Sie auf den jeweiligen Eintrag in der Spalte "Port" klicken.

Ingress Limiting Mode
Anzeige der konfigurierten Frame-Arten, auf die sich die entsprechenden Grenzwerte für die eingehenden Daten beziehen.

Ingress Limiting Rate
Anzeige der konfigurierten Grenzwerte der Transferraten für die eingehenden Daten.

Egress Limiting Rate
Anzeige der konfigurierten Grenzwerte der Transferraten für die ausgehenden Daten.

Hinweis

Die Begrenzung der ausgehenden Daten beziehen sich immer auf sämtliche Frames.

Konfiguration der Begrenzung

Nach dem Anklicken eines Eintrags in der Spalte "Port" wird die Maske "Load Limits Rates Configuration" aufgeblendet.

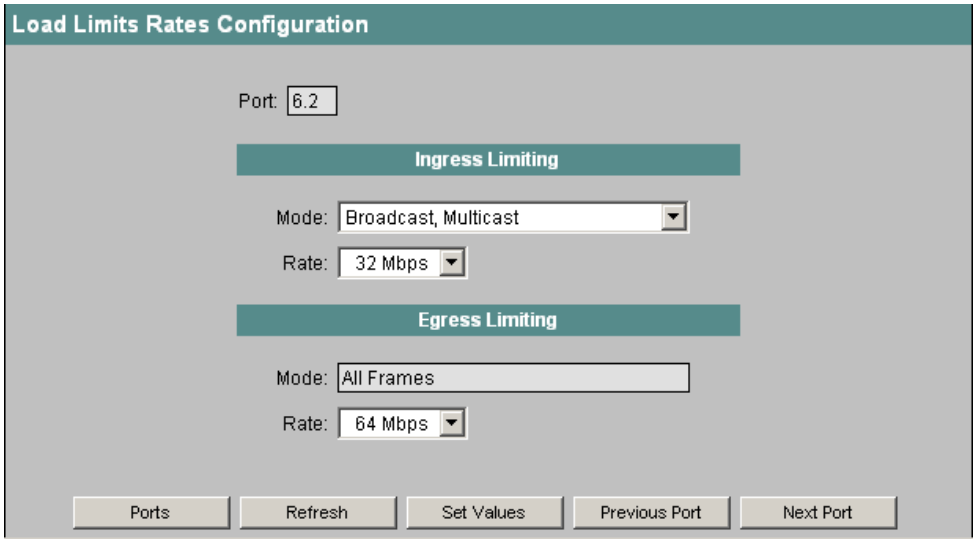


Bild 5-76 Load Limits Rates Configuration

Port
Anzeige des jeweiligen Steckplatzes und des dazugehörigen Ports, auf das sich die weiteren Angaben beziehen. Dieses Feld ist nicht editierbar.

Mode für das Ingress Limiting
Hier können Sie festlegen, auf welche Kategorien von Frames sich die angegebene Transferrate für eingehende Daten beziehen soll:

- Unicast (Destination Lookup Failure)
- Multicast
- Broadcast

Rate für das Ingress Limiting
Hier können Sie die maximale Transferrate für eingehende Daten aus den zur Verfügung stehenden Werten auswählen. Wählen Sie "not limited", also unbegrenzt, so ist der "Ingress Limiting Mode" belanglos.

Mode für das Egress Limiting
Anzeige, dass sich die Transferrate für ausgehende Daten auf alle Frames bezieht. Dieses Feld ist nicht editierbar.

Rate für das Egress Limiting
Hier können Sie die maximale Transferrate für ausgehende Daten aus den zur Verfügung stehenden Werten auswählen.

Hinweis

Die Ringports senden in zyklischen Abständen Multicast-Frames, um Leitungsunterbrechungen zu erkennen. Für Ringports sollten Sie deshalb den Empfang von Multicast-Frames nicht beschränken, um die einwandfreie Funktion des Redundanzmanagers zu gewährleisten.

Syntax Command Line Interface

Tabelle 5-58 Load Limits Configuration - CLI\SWITCH\LIMITS>

Befehl	Beschreibung	Kommentar
info [ports]	Zeigt die aktuellen Einstellungen für die Limitierung von Paketen an. Die Einstellungen werden nach Ports unterteilt angezeigt.	Wird ein Parameter (Ports) angegeben, zeigt das CLI nur die ausgewählten Werte an.
inmode <mode> [ports]	Legt den Ingress Limitierungs Modus für Ports fest. Der Parameter <mode> kann die folgenden Werte annehmen: • B Broadcast • BM Broadcast, Multicast • BMU Broadcast, Multicast, Unicast (DLF) • ALL Alle Frames Beispiel: • inmode B 5.1 Setzt den Limitierungs-Modus für Port 5.1 auf Broadcast.	Wird nur der Parameter <mode> angegeben, werden die Einstellungen für alle Ports geändert.
ingress <rate> [ports]	Legt die Ingress Limitierungs Rate für Ports fest. Der Parameter <rate> kann die folgenden Werte annehmen: • 128k, 256k, 512k • 1m, 2m, 4m, 8m, 16m, 32m, 64m, 128m, 256m • k steht für Kilobit/Sekunde und m für Megabit/Sekunde. Beispiel: • ingress 256k 5.1, 6.2 Setzt die Ingress Limitierungs-Rate für Port 5.1 und 6.2 auf 256 Kilobit/Sekunde.	Wird nur der Parameter <rate> angegeben, werden die Einstellungen für alle Ports geändert.
egress <rate> [ports]	Legt die Egress Limitierungs Rate für Ports fest. Die Abkürzungen für den Parameter <rate> entsprechen denen des Befehls ingress. Beispiel: • egress 2m 5.2, 8.1-8.4 Setzt die Egress Limitierungs-Rate für Port 5.2 und 8.1 bis 8.4 auf 2 Megabit/Sekunde.	Wird nur der Parameter <rate> angegeben, werden die Einstellungen für alle Ports geändert.

5.5.13 VLAN

5.5.13.1 Current VLAN Configuration

Netzwerkdefinition unabhängig von der räumlichen Lage der Teilnehmer

Ein VLAN (Virtuelles LAN) ist ein Netzwerk, dem die Teilnehmer unabhängig von ihrer räumlichen Lage durch Konfiguration zugeordnet werden. Multicast- und Broadcast-Frames sind nur innerhalb der durch die logische Netzstruktur gegebenen Grenzen möglich, auch können solche Frames nicht in das virtuelle Netz hinein gesendet werden. Aus diesem Grund spricht man bei VLANs auch von Broadcastdomänen. Daraus ergibt sich als besonderer Vorteil von VLANs eine geringere Netzlast für die Teilnehmer bzw. Netzsegmente anderer VLANs.

Ausprägungen von VLAN

Es gibt verschiedene Arten von VLAN:

- Port-basiertes VLAN (Ebene 2)
- MAC–Adressen-basiertes VLAN (Ebene2)
- IP-Adressen–basiertes VLAN (Ebene 3)

Ein IE-Switch unterstützt das Port-basierte VLAN. Es besteht dabei die Möglichkeit, den IE-Switch zu parametrieren oder über GVRP-Frames zu konfigurieren.

Vorgehensweise beim Projektieren von Port-basierten VLANs

Führen Sie folgende Schritte durch, um Ihre VLANs zu projektieren:

1. Legen Sie die Teilnehmer für die einzelnen VLANs fest.
2. Vergeben Sie für jeden Teilnehmer und jeden IE-Switch die VLAN-ID und legen Sie fest, zu welchem Gerät und an welchem Port eine Verbindung besteht.
3. Nehmen Sie am IE-Switch folgende Projektierung vor:
   - Definition aller verwendeten VLANs an diesem Gerät.
   - Legen Sie fest, welches VLAN an welchem Port unterstützt werden soll.
   - Legen Sie fest, wie die Frames eingangs- bzw. ausgangseitig an den Ports verarbeitet werden sollen (Ingress- / Egressfilter).
   - Bestimmen Sie, ob Frames am Port mit oder ohne Tag versendet werden sollen.
   - Entscheiden Sie, ob der IE-Switch statisch konfiguriert werden soll oder ob eine dynamische Konfiguration mit GVRP erfolgen darf.

Wichtige Regeln für VLANs

Berücksichtigen Sie bei der Konfiguration und beim Betrieb Ihrer VLANs folgende Regeln:

- Um Umschaltzeiten im Ring von 300 ms bei Nutzung von VLANs oder Multicastgruppen zu erreichen, müssen alle Ringports statisch als Mitglied in allen VLANs und allen Multicastgruppen angelegt werden.
- Frames mit der VLAN-ID "0" (z. B. nur Prioritäts-getaggte Frames) werden wie ungetaggte Frames behandelt.
- Alle Ports am IE-Switch senden standardmäßig Frames ohne VLAN-Tag, um sicher zu gehen, dass der Endteilnehmer diese Frames empfangen kann. Diese Grundeinstellung ist notwendig, da nicht sichergestellt ist, ob ein Teilnehmer getaggte Frames interpretieren kann.
- Standardmäßig ist ein IE-Switch, der VLAN unterstützt, an allen Ports mit der VLAN-Kennung 1 (Default-VLAN) parametriert.

Hinweis

Die VLAN-ID 500 ist für künftige Verwendung reserviert und bereits konfiguriert.

Ist an einem Port ein Endteilnehmer verbunden, dann sollen ausgehende Frames ohne Tag versendet werden (Static Access Port). Befindet sich jedoch an dem Port ein weiterer Switch, so ist der Frame mit einem Tag zu versehen (Trunk Port).

VLANs beim IE-Switch

Die Seite Current VLAN Configuration gibt die momentane Belegung der Ports hinsichtlich der VLAN-Konfiguration an.

Seiten wechseln
Wählen Sie die Schaltflächen ">>" bzw. "<<", um zwischen den Seiten hin und her zu schalten.

Auf der zweiten Seite werden statt der Ports eventuell eingerichtete Link Aggregationen angezeigt.

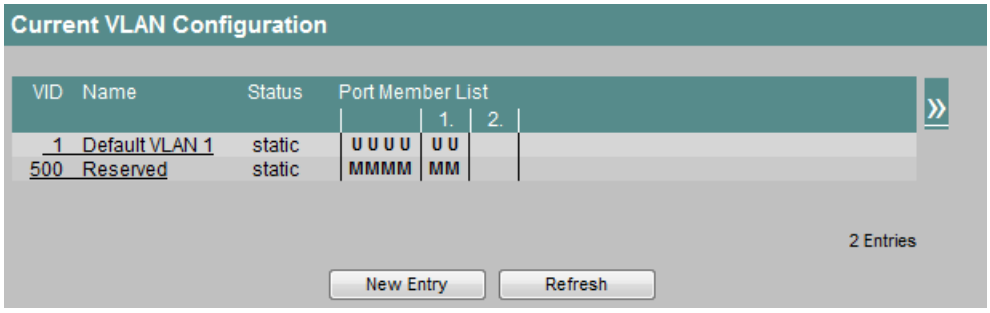


Bild 5-77 Current VLAN Configuration - Seite 1

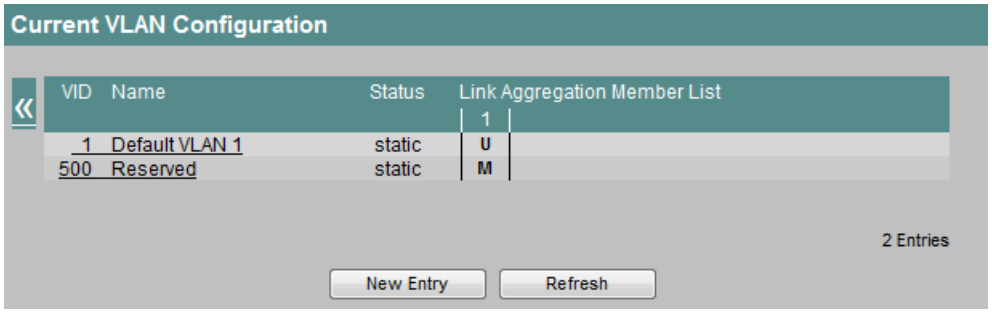


Bild 5-78 Current VLAN Configuration - Seite 2

Die vier Bereiche der Tabelle zeigen folgende Informationen:

VID
Die VLAN-Kennung (VID), eine Zahl zwischen 1 und 4094.

Name
Dieser Name wird bei der Definition eines VLANs vergeben. Er hat nur informativen Charakter und keine Auswirkungen auf die Konfiguration.

Wenn für einen Eintrag der Status static angegeben ist, können Sie VID oder Name anklicken, um die Seite Static VLAN Configuration zu öffnen. Dort können Sie für die einzelnen Ports die Zugehörigkeit zum angegebenen VLAN konfigurieren. VLAN ID und Name können allerdings nur beim Anlegen eines neuen Eintrags festgelegt und nachträglich nicht mehr geändert werden. Wenn Sie einen Eintrag ändern wollen, müssen Sie den betreffenden Eintrag löschen und in geänderter Form neu anlegen.

Status
Zeigt die Art des Eintrags in der Portfiltertabelle. Dabei bedeutet static, dass die Adresse vom Anwender statisch eingetragen wurde. Die Angabe gvrp bedeutet, dass die Konfiguration über einen GVRP-Frame registriert wurde. Voraussetzung dafür ist allerdings, dass GVRP für den IE-Switch aktiviert wurde.

Port Member List
Zeigt die parametrierten VIDs für die Steckplätze bzw. Ports an. Die Einträge haben folgende Bedeutung:

- "-"
  Der Port ist kein Mitglied des angegebenen VLANs.
- M
  (Member) Der Port ist Mitglied des VLANs, gesendete Frames erhalten einen VLAN-Tag mit der in der ersten Spalte angegebenen VID.
- R
  (Registered) Der Port ist Mitglied des VLANs, die Registrierung erfolgte über einen GVRP-Frame.
- U
  (Untagged) Der Port ist Mitglied des VLANs, gesendete Frames erhalten keinen VLAN-Tag.
  U (rote Schrift)
  Dieses VLAN ist nicht als Port-VLAN konfiguriert. Gesendete Frames erhalten keinen VLAN-Tag.
- F
  (Forbidden) Der Port ist nicht Mitglied des VLANs und es ist nicht möglich, dass das VLAN dynamisch über GVRP an diesem Port registriert werden kann.

- G
  (Guest VLAN) Der Port ist Mitglied des Guest VLANs. Die Registrierung erfolgte dynamisch über die Authentifizierung "Guest VLAN", siehe Kapitel "802.1x Port Configuration (Seite 174)".
- A
  (Authenticated) Der Port ist Mitglied des VLANs. Die Registrierung erfolgte dynamisch über das Authentifizierungsverfahren "MAC Authentication", siehe Kapitel "802.1x Port Configuration (Seite 174)".

Bei der Neudefinition sind alle Ports mit der Kennung "-" belegt.

Link Aggregationen Member List
Zeigt die parametrierten Einstellungen der Link Aggregation an. Die Einträge haben folgende Bedeutung:

- "-"
  Der Port ist nicht Mitglied der Link Aggregation.
- M
  (Member) Der Port ist Mitglied der Link Aggregation.

VLAN-Konfiguration

Klicken Sie die Schaltfläche New Entry, um das Sendeverhalten von Frames über Ports bezüglich eines VLAN festzulegen. Es erscheint die Seite Static VLAN Configuration, auf der Sie alle notwendigen Eintragungen machen können:

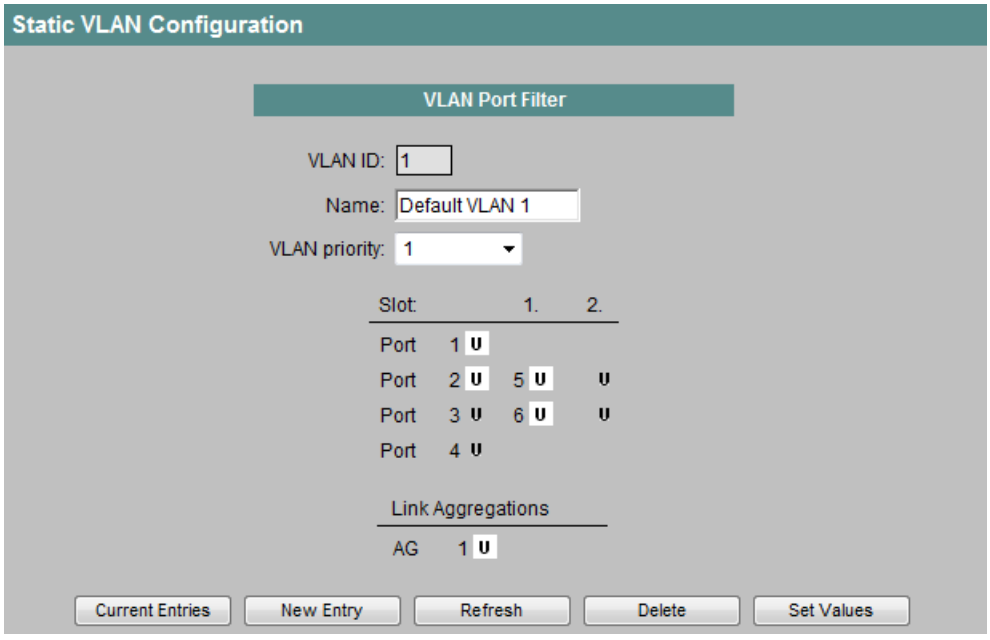


Bild 5-79 Static VLAN Configuration

VLAN ID
Tragen Sie hier die Kennung des VLANs ein. Die VLAN-ID ist eine Zahl zwischen 1 und 4094.

Name
Tragen Sie hier einen Namen für das VLAN ein. Der Name hat keine Auswirkungen auf die Konfiguration.

VLAN priority
Wählen Sie hier eine Priorität, die für das VLAN erzwungen werden soll. In alle eingehenden Frames dieses VLANs wird die gewählte Priorität eingetragen. Die eingehenden Frames werden gemäß der gewählten Priorität vom Switch weitergeleitet.

Wenn Sie "Do not force" auswählen, bleibt die Priorität der Frames unverändert.

Slot/Port
Hier können Sie festlegen, wie sich der Port beim Senden von Frames im Bezug auf das angegebene VLAN verhalten soll. Die Felder sind mit "-" vorbelegt. Durch wiederholtes Anklicken schalten Sie von einem Eintrag zum nächsten. Die Einträge haben folgende Bedeutung:

- **"-"**
  Der Port ist kein Mitglied des angegebenen VLANs.
- **M**
  (Member) Der Port ist Mitglied des VLANs, gesendete Frames erhalten einen VLAN-Tag mit der in der ersten Zeile angegebenen VID.
- **R**
  (Registered) Der Port ist Mitglied des VLANs, die Registrierung erfolgte über einen GVRP-Frame.
- **U**
  (Untagged) Der Port ist Mitglied des VLANs, gesendete Frames erhalten keinen VLAN-Tag. Verwenden Sie U, falls über diesen Port Endgeräte angesprochen werden, die keine VLAN-Tags unterstützen.
- **F**
  (Forbidden) Der Port ist nicht Mitglied des VLANs und es ist nicht möglich, dass das VLAN dynamisch über GVRP an diesem Port registriert werden kann.
- **T**
  (Trunk Port) Der Port ist automatisch Mitglied in allen konfigurierten VLANs und sendet nur getaggte Frames.

Hinweis

Wird ein Port als "F" (Forbidden) für ein VLAN definiert, dann ist dieses VLAN gesperrt, wenn der Port ein Trunk-Port ist. Forbidden hat eine höhere Priorität als Trunk.

Current Entries
Durch Anklicken dieser Schaltfläche gelangen Sie zurück zur Liste mit den VLANs.

New Entry
Klicken Sie diese Schaltfläche, um Festlegungen für ein neues VLAN zu treffen.

Set Values
Klicken Sie diese Schaltfläche, um die eingegebenen Werte in der Konfiguration des IE-Switch zu speichern.

Delete
Klicken Sie diese Schaltfläche, um die angezeigte Konfiguration zu löschen.

VLAN-Konfiguration und Authentifizierung

Wenn ein Port über das Authentifizierungsverfahren "802.1X" authentifiziert werden soll, müssen Sie ein VLAN konfigurieren, dem der Port zugewiesen werden soll. Wenn die "802.1X"-Authentifizierung fehlschägt und der Port über "MAC Authentication" oder "Guest VLAN" authentifiziert wird, wird er als "A" oder "G" definiert.

Wenn ein Port über das Authentifizierungsverfahren "MAC Authentication" authentifiziert wird und die Option "VLAN Assignment Allowed" deaktiviert ist, wird dem Port kein VLAN zugewiesen ("-"). Sie müssen dem Port in diesem Fall vorher ein VLAN zuweisen.

Wenn ein Port über das Authentifizierungsverfahren "MAC Authentication" authentifiziert wird und die Option "VLAN Assignment Allowed" aktiviert ist, wird der Port als "A" definiert.

Syntax Command Line Interface

Tabelle 5-59 Current VLAN Configuration - CLI\SWITCH\VLAN>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuell projektierten VLANs in Bezug zu den Ports an.	
add <VLAN-ID> [<option> [ports]]	Fügt ein neues VLAN hinzu. Für den Parameter <option> stehen die folgenden Abkürzungen zur Verfügung. • - Der Port ist nicht Mitglied des VLANs. • m Der Port ist Mitglied des VLANs, Frames werden mit VLAN-Tag gesendet. • u Der Port ist Mitglied des VLANs, Frames werden ohne VLAN-Tag gesendet. • f Der Port ist nicht Mitglied des VLANs und die Zugehörigkeit kann auch nicht dynamisch über GVRP konfiguriert werden. • t Der Port ist automatisch Mitglied in allen konfigurierten VLANs und sendet nur getaggte Frames. Beispiele: • add 2 Legt einen Eintrag mit der VLAN-ID 2 und dem Defaultnamen "Vlan 2" an. • add 4 m Legt einen Eintrag mit der VLAN-ID 4 und dem Default-Namen "Vlan4" an. Alle vorhandenen Ports sind Member.	Nur Administrator.

Befehl	Beschreibung	Kommentar
edit <VLAN-ID> [<option> [ports]]	Ändert die Zugehörigkeit von Ports zu einem VLAN. Die Abkürzungen für den Parameter <option> entsprechen denen des Befehls add. Beispiele: • edit 3 - 10.1 Entfernt den Port 10.1 aus dem VLAN mit der ID 3.	Nur Administrator.
name <VLAN-ID> <Name>	Ändert den Namen eines VLANS.	Nur Administrator.
delete <VLAN-ID>	Löscht das VLAN mir der angegebenen ID aus der Konfiguration des IE-Switch.	Nur Administrator.

5.5.13.2 VLAN Port Parameters

Verarbeitung empfangener Frames

Diese Seite zeigt die Regeln an, nach denen ein IE-Switch empfangene Frames behandelt:

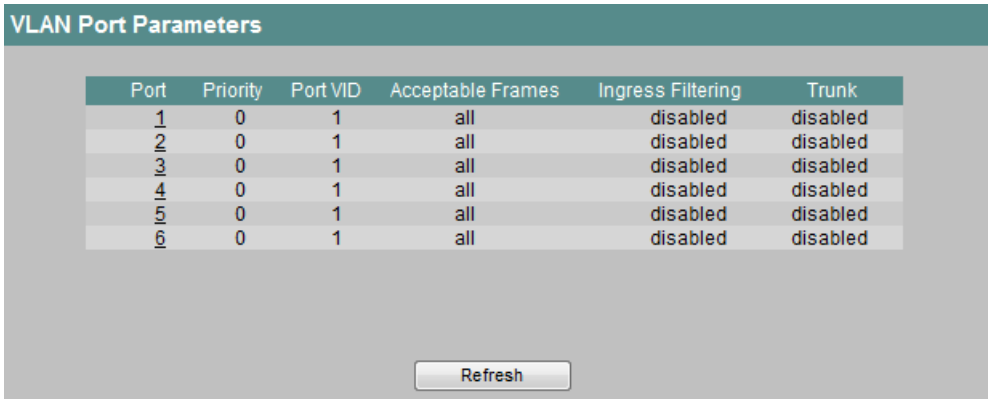


Bild 5-80 VLAN Port Parameters

Die fünf Spalten der Tabelle zeigen folgende Informationen:

Port
Hier wird der Steckplatz und der Port angegeben, auf die sich die nachfolgenden Informationen beziehen.

Priority
Die CoS-Priorität (Class of Service), die im VLAN-Tag verwendet wird. Wird ein Frame ohne Tag empfangen, kann ihm eine Priorität pro Port vergeben werden. Diese Priorität legt fest, wie dieser Frame im Vergleich zu anderen Frames weiterhin bearbeitet wird.
Es gibt insgesamt acht Prioritäten, mit den Werten 0 bis 7, wobei die 7 der höchsten Priorität entspricht (IEEE 802.1p Port Priority). Detailinformationen über das Tagging von Frames finden Sie im Anhang C.

Port VID
Hat ein empfangener Frame kein VLAN-Tag, so wird es um einen Tag mit der hier angegebenen VLAN-ID ergänzt und entsprechend den Switch-Regeln am Port ausgesendet.

Wenn die VLAN-ID des Ports dynamisch über das Authentifizierungsverfahren "MAC Authentication" oder "Guest VLAN" definiert wurde, wird die "Port VID" automatisch konfiguriert.

Acceptable Frames
Hier wird angegeben, wie mit ungetaggten Frames verfahren wird. Es gibt folgende Alternativen:

- tagged only
  Der IE-Switch verwirft alle ungetaggten Frames.
- all
  Der IE-Switch leitet alle Frames weiter.

Ingress Filtering
Hier wird angegeben, ob die VID von empfangenen Frames ausgewertet wird (Eintrag enabled) oder nicht (Eintrag disabled).

Trunk
Hier wird angegeben, ob ein Port als Trunk Port konfiguriert wurde (Eintrag enabled) oder nicht (Eintrag disabled).

Konfiguration eines Ports für VLAN

Nach dem Anklicken eines Eintrags in der Spalte Ports gelangen Sie zur Seite für die Konfiguration der Port-Eigenschaften für den Frame-Empfang:

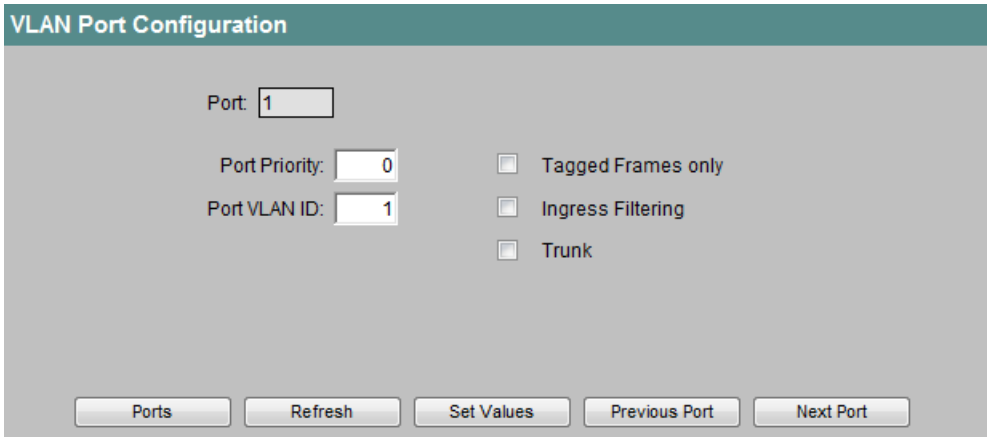


Bild 5-81 VLAN Port Configuration

Port
In diesem nur lesbaren Feld werden Steckplatz und Portnummer angegeben, auf die sich die Informationen dieser Seite beziehen.

Port Priority
Die Priorität, mit der ungetaggte Frames versehen werden.

Port VLAN ID
Die VLAN-ID, die ungetaggten Frames zugewiesen wird.
Wenn die VLAN-ID des Ports dynamisch über das Authentifizierungsverfahren "MAC Authentication" oder "Guest VLAN" definiert wurde, wird die "Port VLAN ID" automatisch konfiguriert.

Tagged Frames only
Wenn Sie diese Option aktivieren, werden ungetaggte Frames verworfen. Andernfalls gelten die Weiterleitungsregeln entsprechend der Konfiguration.

Ingress Filtering
Wenn Sie diese Option aktivieren, bestimmt die VLAN-ID empfangener Frames die Weiterleitung: Für die VLAN-ID des empfangenen Frames muss das VLAN im IE-Switch angelegt sein und der Port muss Mitglied (Member) des VLANs sein.
Frames mit der projektierten Port-VLAN-ID werden weitergeleitet, Frames mit einer davon abweichenden VLAN-ID werden beim Empfang verworfen. Frames ohne VLAN-ID werden empfangen und an die Port-VLAN-ID weitergeleitet.

Trunk
Wenn Sie diese Option aktivieren, ist der Port ein Trunk Port. Ein Trunk Port ist automatisch Mitglied in allen konfigurierten VLANs und sendet nur getaggte Frames.

Wenn Sie die Option deaktivieren, wird die VLAN-Konfiguration wiederhergestellt, die vor dem Einschalten aktiv war.

Syntax Command Line Interface

Tabelle 5-60 VLAN Port Parameters - CLI\SWITCH\VLAN\PORTS>

Befehl	Beschreibung	Kommentar
info	Zeigt eine Übersicht der Ports und der zugehörigen VLAN-Einstellungen an.	-
vid [<VLAN-ID> [ports]]	Empfangene Frames ohne VLAN-Tag bekommen an den angegebenen Ports ein VLAN-Tag mit der <VLAN-ID>.	Nur Administrator.
prio [<0...7> [ports]]	Legt die Priorität von Ports fest.	Nur Administrator.
ingress [<E|D> [ports]]	Aktiviert/Deaktiviert die Auswertung der VID von empfangenen Frames.	Nur Administrator.
untagged [<E|D> [ports]]	Legt die Verarbeitung von Frames ohne VLAN-Tag fest. Wenn aktiviert, werden auch Frames ohne VLAN-Tag akzeptiert, andernfalls nicht.	Nur Administrator.
trk [<E|D> [ports]]	Aktiviert/Deaktiviert die Trunk-Eigenschaft. Ein Trunk Port ist automatisch Mitglied in allen konfigurierten VLANs und sendet nur getaggte Frames.	Nur Administrator.

5.5.13.3 GVRP Configuration

Aktivieren der GVRP- Funktionalität

Über einen GVRP-Frame kann sich ein Endteilnehmer oder Switch an einem Port des IE-Switch für eine bestimmte VID registrieren. Auf der Seite GVRP Configuration können Sie jeden Port für die GVRP-Funktionalität freischalten.

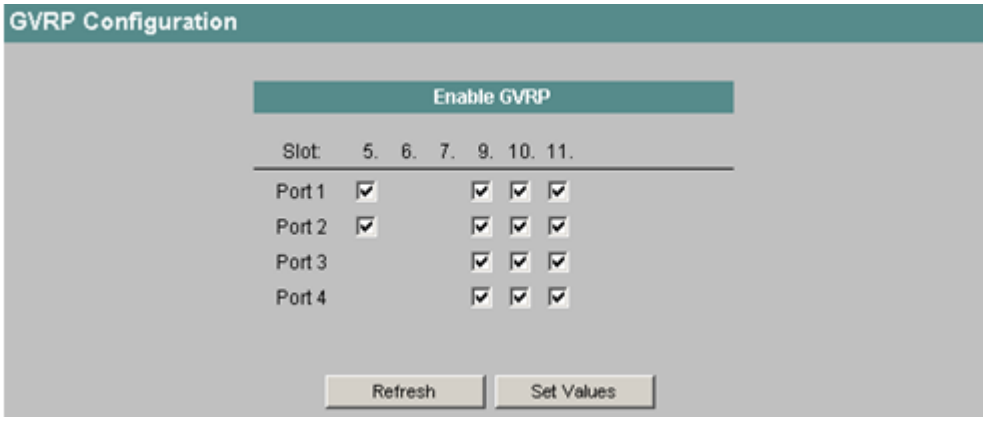


Bild 5-82 GVRP Configuration

Enable GVRP
Wenn Sie eine Option aktivieren, ermöglicht der IE-Switch das Registrieren eines VLANs über GVRP-Frames an dem entsprechenden Port. Außerdem kann der IE-Switch auch GVRP-Frames über diesen Port senden.

Syntax Command Line Interface

Tabelle 5-61 GVRP Configuration - CLI\SWITCH\VLAN>

Befehl	Beschreibung	Kommentar
gvrpport [<E|D> [ports]]	Aktiviert/Deaktiviert die dynamische Registrierung von VLANs mit GVRP für die angegebenen Ports.	Nur Administrator.

5.5.13.4 VLAN Learning

MAC-Adressen in VLANs lernen

Auf dieser Seite können Sie die Option "Learn to all VLANs" pro Port konfigurieren.

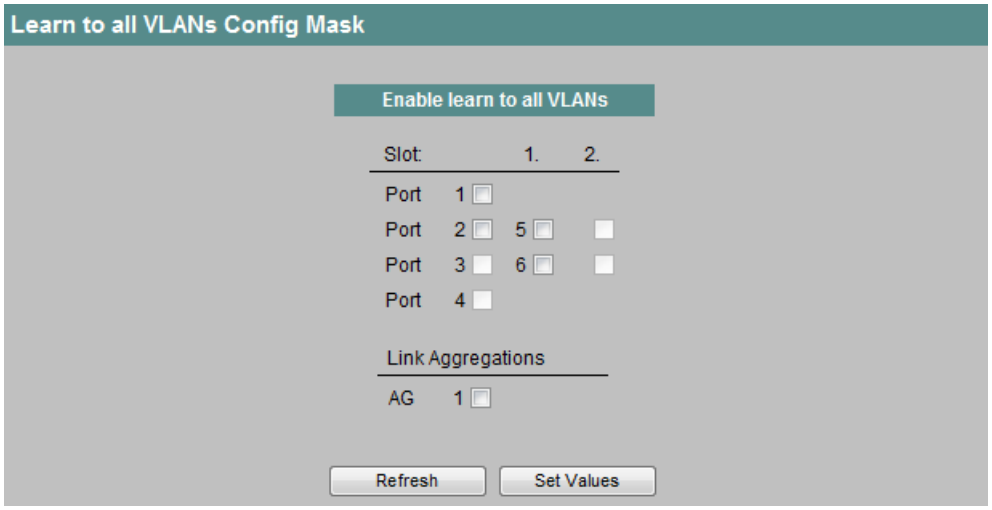


Bild 5-83 Learn to all VLANs Config Mask

Enable learn to all VLANs

Wenn Sie die Option an einem Port aktivieren, wird eine MAC-Adresse, die an dem Port empfangen wird, automatisch in allen konfigurierten VLANs gelernt.

Syntax Command Line Interface

Tabelle 5-62 Learn to all VLANs - CLI\SWITCH\VLAN>

Befehl	Beschreibung	Kommentar
lrnallv [<E|D> [Ports]]	Aktiviert/Deaktiviert das automatische Lernen einer MAC-Adresse in allen konfigurierten VLANs.	Nur Administrator.

5.5.13.5 X-300 VLAN Port Priority Mapping

VLAN Port Priority Mapping

Diese Seite zeigt an, mit welcher Priorität ein Port empfangene Frames versendet.

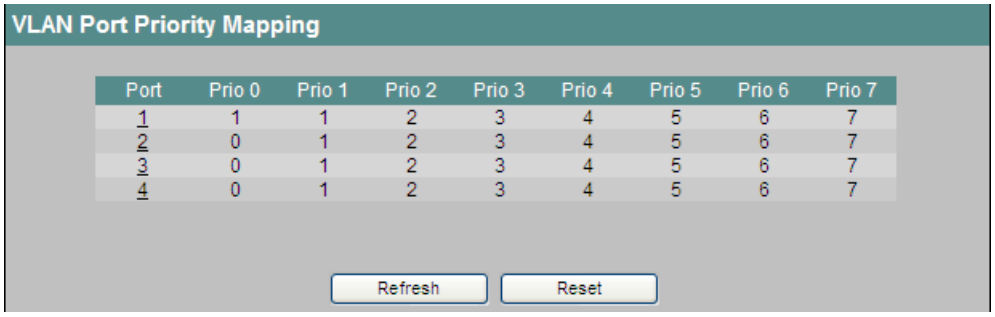


Bild 5-84 VLAN Port Priority Mapping

Port

Port, auf den sich die nachfolgenden Informationen beziehen.

Prio 0

Zeigt die Priorität, mit der Frames versendet werden, die mit der Priorität 0 empfangen werden.

Für Port 1 wurde z. B. eingestellt, dass empfangene Frames mit der Priorität 0 mit der Priorität 1 versendet werden sollen.

Die Spalten "Prio 1" bis "Prio 7" werden genauso gelesen.

VLAN Priority Remap Configuration

Die Maske "VLAN Priority Remap Configuration" erscheint, wenn Sie auf der Seite "VLAN Port Priority Mapping" einen Port angeklickt haben.

Abhängig von der Priorität beim Empfangen, können Sie für Frames die Priorität ändern, mit der sie versendet werden.

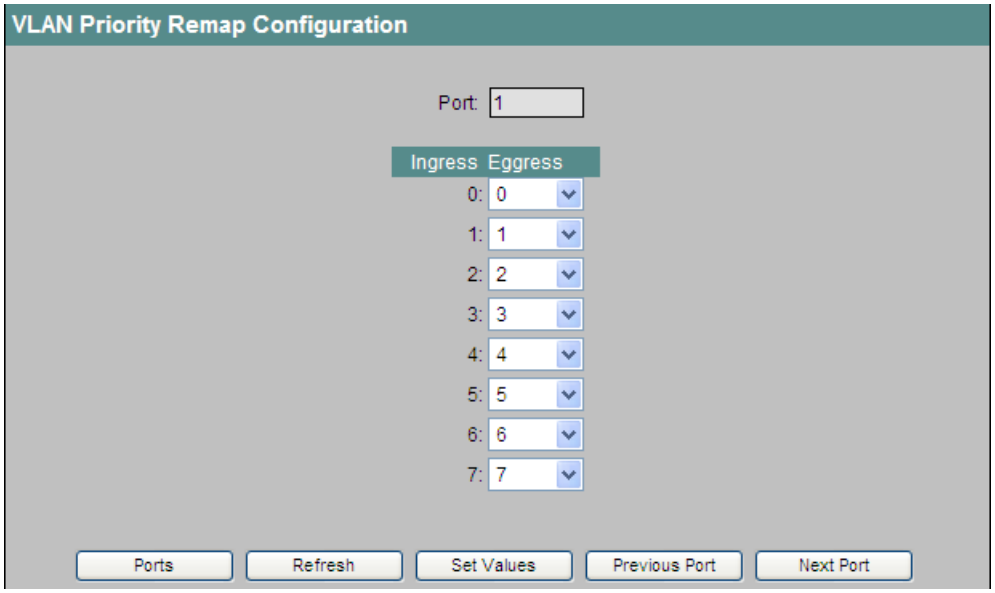


Bild 5-85 VLAN Priority Remap Configuration

Port

In diesem nur lesbaren Feld wird die Portnummer angegeben, auf die sich die Informationen dieser Seite beziehen.

Ingress

Priorität, mit der ein Frame empfangen wird.

Egress

Priorität, mit der ein Frame versendet werden soll.

Syntax Command Line Interface

Tabelle 5-63 VLAN Port Priority Mapping - CLI\SWITCH\VLAN\PRIO>

Befehl	Beschreibung	Kommentar
info	Zeigt an, mit welcher Priorität ein Port empfangene Frames versendet.	-
remap [port] [<0..7><0..7>]	Ändert die Priorität empfangener Frames für das Versenden.	Nur Administrator.

Befehl	Beschreibung	Kommentar
reset	Setzt die Priorität empfangener Frames zurück. Die Priorität beim Empfangen entspricht dann der Priorität beim Senden.	Nur Administrator.
vprio <VID> [noforce | <0-7>]	Ändert die Priorität empfangener Frames in Abhängigkeit von der VLAN-Zugehörigkeit. Die Frames werden mit dieser geänderten Priorität gesendet. Im Grundzustand "noforce" bleibt die Priorität der Frames unverändert.	Nur Administrator.

5.5.14 STP/RSTP

5.5.14.1 Spanning Tree Configuration

Vermeidung von Schleifenbildung bei redundanten Verbindungen

Das Spanning Tree Protocol (STP) ermöglicht es, Netzwerkstrukturen aufzubauen, bei denen es mehrere Verbindungen zwischen zwei Stationen gibt. STP lässt genau einen Pfad zu und deaktiviert die anderen (redundanten) Ports für den Datenverkehr. Dadurch wird verhindert, dass es zu einer Schleifenbildung im Netz kommt. Bei einer Unterbrechung wird ein alternativer Pfad ermittelt, über den die Daten gesendet werden. Die Funktionalität des Spanning Tree-Verfahrens basiert auf dem Austausch von Konfigurations- und Topologieänderungs-Frames.

Definition der Netztopologie durch Konfigurations-Frames

Die Switches tauschen zur Berechnung der Topologie untereinander Konfigurations-Frames aus, sogenannte BPDUs (Bridge Protocol Data Unit). Mit diesen Frames wird die Root Bridge ausgewählt und die Netztopologie erstellt. Die Root Bridge ist die Bridge, die das Spanning Tree-Verfahren für alle beteiligten Komponenten steuert. Darüber hinaus bewirken BPDU-Frames den Statuswechsel der Bridge-Ports.

Rapid Spanning Tree

Das Rapid Spanning Tree Protocol basiert auf dem Spanning Tree Protocol. Bei RSTP wurde die Rekonfigurationszeit optimiert, indem die Geräte bereits zum Zeitpunkt des ungestörten Betriebs Informationen über Alternativrouten sammeln. Typische Rekonfigurationszeiten bei Spanning Tree liegen zwischen 20 und 30 Sekunden. Bei Rapid Spanning Tree liegen die Rekonfigurationszeiten im Sekundenbereich. Das wird durch folgende Maßnahmen erreicht:

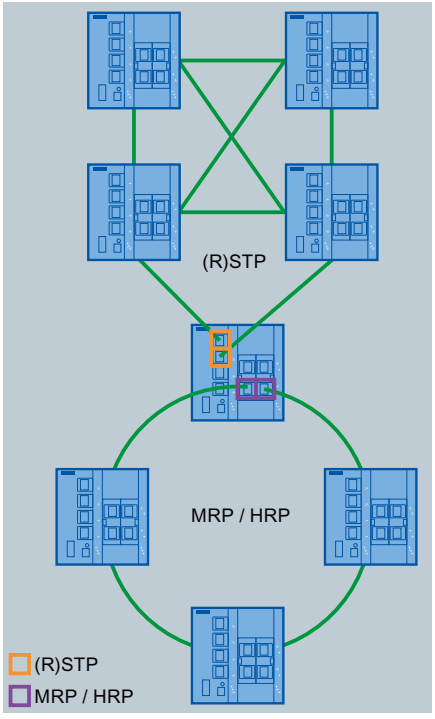
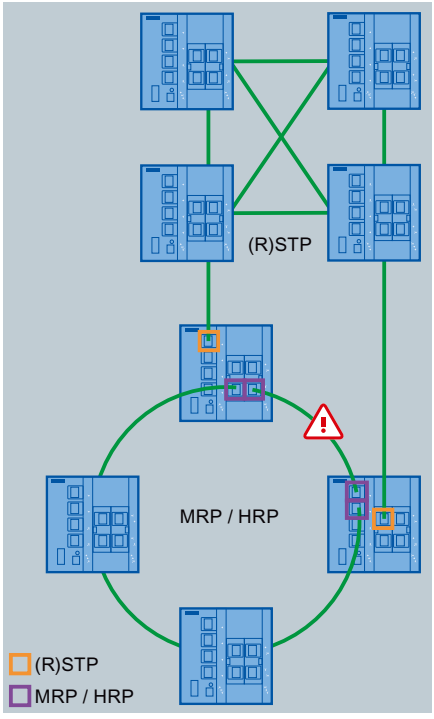
- Edge Ports (Endteilnehmer-Port)
  Ein Port, der als Edge Port definiert ist, wird direkt nach einem Link-Up aktiv geschaltet. Wenn an einem Edge Port eine Spanning Tree BPDU empfangen wird, verliert der Port die Rolle als Edge Port und nimmt wieder am (R)STP teil.
- Point to Point (direkte Kommunikation zweier benachbarter Switches)
  Durch die direkte Koppelung der Switche kann eine Zustandsänderung (Umkonfiguration der Ports) ohne Verzögerungen durchgeführt werden.
- Alternate Port (Ersatz für den Root Port)
  Ein Alternate Port dient als Ersatz für den Root Port. Bei einem Verbindungsverlust zur Root Bridge kann der IE-Switch deshalb ohne Verzögerung durch Neukonfiguration eine Verbindung über den Alternate Port aufbauen.
- Filtertabelle
  Bei Rapid Spanning Tree werden Ports, die von einer Umkonfiguration betroffen sind, sofort aus der Filtertabelle gelöscht. Im Gegensatz dazu ist bei Spanning Tree der Zeitpunkt des Eintrags in die Filtertabelle für das Löschen von Ports maßgeblich.
- Reaktion auf Ereignisse
  Rapid Spanning Tree reagiert auf Ereignisse, z. B. einen Verbindungsabbruch, ohne Verzögerung. Es müssen also keine Zeitgeber wie bei Spanning Tree abgewartet werden.

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

(Rapid) Spanning Tree, Medienredundanz und Passive Listening

Sie haben folgende Möglichkeiten, um ein (R)STP-Segment an einen MRP- bzw. HRP-Ring anzubinden:

- über (R)STP an einem Gerät im Ring
  Sie können (R)STP zeitgleich mit den Medienredundanzverfahren MRP bzw. HRP auf verschiedenen Ports eines Geräts aktivieren (vgl. Abbildung ① "Zulässige (R)STP-Anbindung an Ringredundanz").
  Eine Anbindung über (R)STP an verschiedenen Geräten eines Rings ist nicht möglich. Da die (R)STP-BPDUs nicht über einen MRP- bzw. HRP-Ring weitergeleitet werden, kommt es zu kreisenden Frames und zum Ausfall des Datenverkehrs (vgl. ② "Nicht zulässige (R)STP-Anbindung an Ringredundanz").

① Zulässige (R)STP-Anbindung an Ringredundanz	② Nicht zulässige (R)STP-Anbindung an Ringredundanz
	

- über Passive Listening an verschiedenen Geräten im Ring
  Wenn Sie ein (R)STP-Segment an verschiedenen Geräten eines MRP- bzw. HRP-Rings anbinden wollen, müssen Sie bei allen Geräten des Rings Passive Listening aktivieren und (R)STP deaktivieren. Da Passive Listening die Weiterleitung von (R)STP-BPDUs unterstützt, entstehen keine kreisenden Frames.

Hinweis

Wenn (R)STP und Passive Listening gleichzeitig über WBM oder CLI aktiviert wurden, dann ist Passive Listening nicht aktiv.

Spanning Tree-Konfiguration beim IE-Switch

Die für das Spanning Tree-Protokoll verwendeten Parameter werden im Menüpunkt "Spanning Tree Configuration" angezeigt und eingestellt:

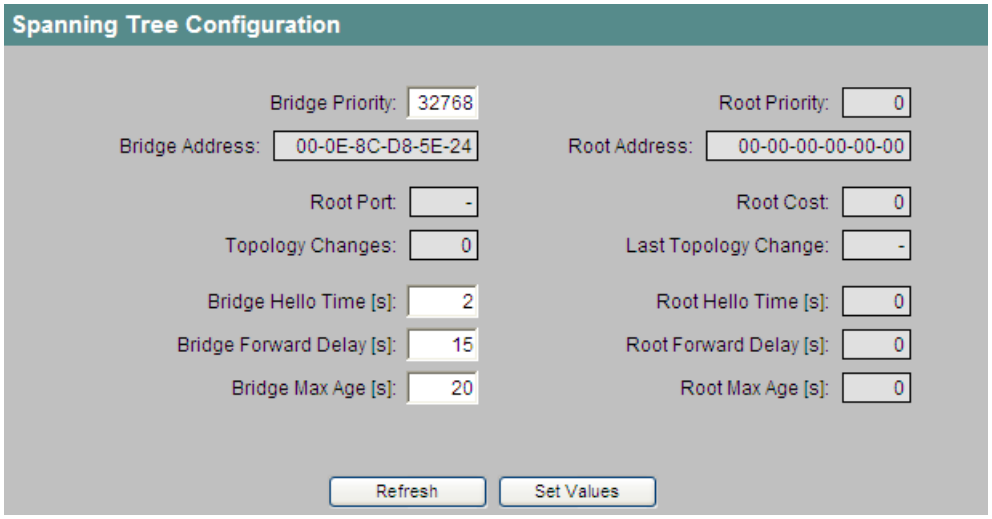


Bild 5-86 Spanning Tree Configuration

Der linke Teil der Seite zeigt die Konfiguration des IE-Switches. Der rechte Teil zeigt die Konfiguration der Root Bridge, wie sie aus Spanning Tree-Frames abgeleitet werden kann, die ein IE-Switch empfangen hat. Deshalb sind die dort angezeigten Daten nur lesbar. Wenn ein IE-Switch Root Bridge ist, stimmen die Informationen der linken und der rechten Seite überein. Die Parameter haben folgende Bedeutung:

Bridge Priority / Root Priority
Anhand der Bridge Priority wird festgelegt, welcher Switch 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 Switches die gleiche Priorität besitzen, dann wird der Switch Root Bridge, dessen MAC-Adresse den niedrigsten Zahlenwert hat. Beide Parameter, Bridge Priority und MAC-Adresse, bilden zusammen den Bridge Identifier. Da die Root Bridge alle Wegeänderungen verwaltet, sollte sie wegen der Laufzeit der Frames möglichst zentral angeordnet sein. Der Wert für die Bridge Priority ist ein ganzzahliges Vielfaches von 4096 mit einem Wertebereich von 0 bis 65.535.

Bridge Address / Root Address
Die MAC-Adresse des IE-Switch bzw. der Root Bridge.

Root Port
Der Port, über den mit der Root Bridge kommuniziert wird.

Topology Changes / Last Topology Change
Die Angabe für den IE-Switch nennt die Zahl der Umkonfigurationen aufgrund des Spanning Tree Mechanismus seit dem letzten Hochlauf. Für die Root Bridge wird die Zeitdauer in Minuten (Zusatz m hinter der Zahlenangabe) seit der letzten Umkonfiguration angezeigt.

Bridge Hello Time / Root Hello Time
Jede Bridge versendet regelmäßig Konfigurations-Frames (BPDUs). Der Zeitabstand zwischen zwei solchen Frames ist die Hello Time.

Bridge Forward Delay / Root Forward Delay
Neue Konfigurationsinformationen werden von einer Bridge 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. Der Default-Wert für diesen Parameter beträgt 15 Sekunden.

Bridge Max Age / Root Max Age
Bridge Max Age definiert das maximale "Alter" die eine empfangene BPDU haben darf um vom Switch als gültig akzeptiert zu werden. Der Default-Wert für diesen Parameter beträgt den Wert 20.

Syntax Command Line Interface

Tabelle 5-64 Spanning Tree Configuration - CLI\SWITCH\STP>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuelle Spanning Tree-Konfiguration an.	-
bprio [0...61440]	Legt die Bridgepriorität für den IE-Switch fest.	Nur Administrator.
hellotm [1 ... 10]	Legt den Zeitabstand zwischen zwei BPDU-Frames in Sekunden fest.	Nur Administrator.
fwddelay [4 ... 30]	Legt die Verzögerungszeit für die Wirksamkeit von Konfigurationsinformationen fest (Angabe in Sekunden).	Nur Administrator. Default-Wert: 15 s
maxage [6 ... 40]	Maximales Alter für Konfigurations-Informationen.	Nur Administrator. Default-Wert: 20 s

5.5.14.2 Spanning Tree Port Parameters

Portspezifische Parameter

Diese Seite zeigt die aktuellen Port-Parameter, die vom Anwender so parametriert wurden oder die über Autofunktionen vom IE-Switch so eingestellt wurden.

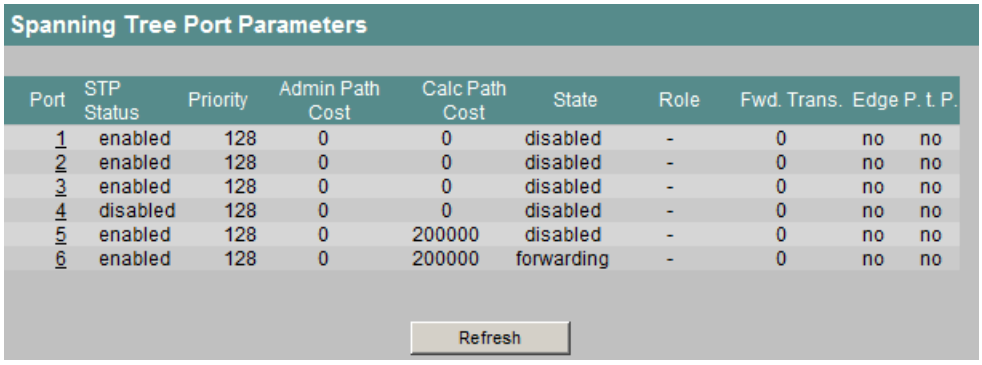


Bild 5-87 Spanning Tree Port Parameters

Die Tabelle gliedert sich in folgende Spalten:

Port
Angabe von Steckplatz und Port, auf den sich die Informationen beziehen.

STP Status
Zeigt an, ob Spanning Tree für den Port aktiviert (enabled) oder deaktiviert (disabled) ist.

Priority
Kann der von Spanning Tree ermittelte Weg alternativ über mehrere Ports eines Switch 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 255 angegeben sein, der Default-Wert ist 128.

Admin Path Cost

Zeigt den Wert für die zu verwendenden Pfadkosten an.

Calc Path Cost

Wenn der Wert für Admin Path Cost > 0 ist, wird dieser Wert als als Calculated Path Cost übernommen.
Wenn der Wert für Admin Path Cost = 0, wird der Wert für Calculated Path Cost automatisch ermittelt. Die Ermittlung der Pfadkosten richtet sich maßgeblich nach der Übertragungsgeschwindigkeit.

Je höher die erzielbare Übertragungsgeschwindigkeit ist, umso kleiner sollte der Wert für Admin Path Cost sein.

Typische Werte für Wegkosten bei Rapid Spanning Tree:

- 1000 Mbit/s = 20.000
- 100 Mbit/s = 200.000
- 10 Mbit/s = 2.000.000

State
Zeigt den momentanen Status an, in dem sich der Port befindet. Es sind folgende Stati möglich:

- disabled
  Der Port empfängt nur und nimmt nicht an der STP-Konfiguration teil.
- blocking
  Im Blocking-Modus werden BPDU-Frames empfangen.
- listening
  In diesem Status werden sowohl BPDU-Frames empfangen als auch gesendet. Der Port ist in den Spanning Tree-Algorithmus einbezogen.
- learning
  Vorstufe zum Forwarding-Status, der Port lernt wieder aktiv die Topologie (d. h. die Teilnehmeradressen).
- forwarding
  Der Port ist nach der Umkonfigurationszeit wieder aktiv im Netz, er empfängt und sendet Datenframes.

FWD Transitions
Gibt die Anzahl der Wechsel von Listening- in den Forwarding-Status an.

Edge

In dieser Spalte sind folgende Eintragungen möglich:

- yes
  An diesem Port befindet sich ein Endgerät.
- no
  An diesem Port befindet sich ein Spanning Tree- oder Rapid Spanning Tree-Gerät.

  Bei einem Endgerät kann ein IE-Switch ohne Rücksicht auf Spanning Tree-Frames schneller den Port umschalten. Wird entgegen dieser Einstellung ein Spanning Tree-Frame empfangen, dann wechselt der Port automatisch auf die Einstellung no für Switches.

P.t.P.

Eine Point to Point-Verbindung liegt dann vor, wenn zwei RSTP-fähige Netzkomponenten über diesen Port miteinander verbunden sind. Es gibt 2 mögliche Zustände:

- Yes
  Es liegt eine Point to Point-Verbindung vor.
- No
  Es liegt keine Point to Point-Verbindung vor.

Syntax Command Line Interface

Tabelle 5-65 (Rapid) Spanning Tree Port Parameters - SWITCH\STP\PORTS>

Befehl	Beschreibung	Kommentar
info	Zeigt eine Übersicht der Ports und der zugehörigen Rapid Spanning Tree-Einstellungen.	-

5.5.14.3 Spanning Tree Port Configuration

Konfiguration eines Ports für (Rapid) Spanning Tree

Hinweis

Auf den Ringports und den Standby-Ports kann (R)STP nicht aktiviert werden.

Wenn Sie auf der Seite "Spanning Tree Port Parameters" in der Spalte "Port" eine Portbezeichnung anklicken, gelangen Sie zur Seite "Spanning Tree Port Configuration":

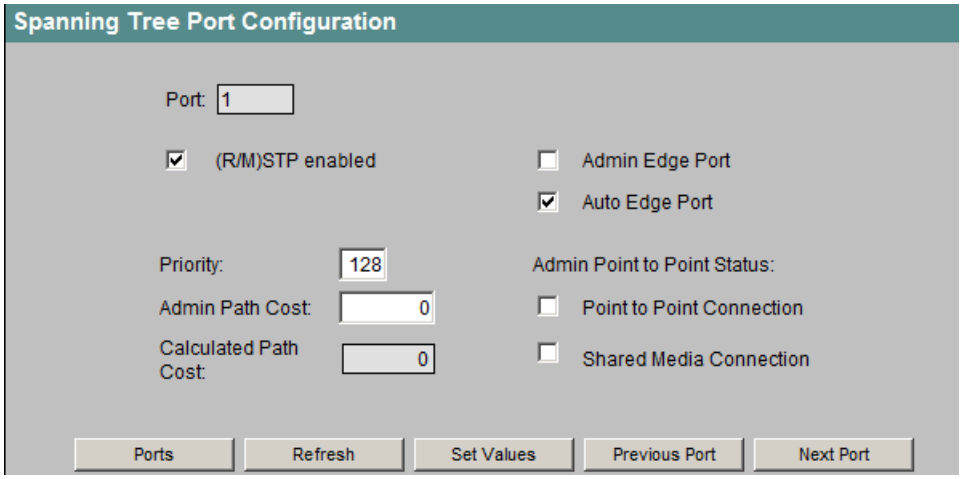


Bild 5-88 Spanning Tree Port Configuration

Port
Das Anzeigefeld "Port" zeigt den ausgewählten Port an.

(R)STP enabled
Aktivieren Sie diese Option, wenn der Port das (Rapid) Spanning Tree-Protokoll verwenden soll.

Admin Edge Port
Aktivieren Sie diese Option, wenn sich an diesem Port ein Endgerät befindet. Andernfalls wird bei jeder Linkänderung an diesem Port eine Rekonfiguration des Netzwerkes ausgelöst.

Auto Edge Port
Aktivieren Sie diese Option, wenn an diesem Port automatisch erkannt werden soll, ob ein Endgerät angeschlossen ist.
Diese Option ist sinnvoll im Zusammenhang mit Passive Listening, da dadurch bei Ausfall des Hauptlinks eine schnellere Rekonfiguration vorgenommen werden kann (siehe Betriebsanleitung des entsprechenden IE-Switches).

Priority
Tragen Sie im Eingabefeld "Priority" einen Wert für die Port-Priorität ein.
zulässige Werte: 0 bis 255

Admin Path Cost

Hier können die Werte für die zu verwendenden Pfadkosten pro Port manuell vorgegeben werden.

Calc Path Cost

Wenn der Wert für Admin Path Cost > 0 ist, wird dieser Wert als als Calculated Path Cost übernommen.
Wenn der Wert für Admin Path Cost = 0, wird der Wert für Calculated Path Cost automatisch ermittelt. Die Ermittlung der Pfadkosten richtet sich maßgeblich nach der Übertragungsgeschwindigkeit.

Je höher die erzielbare Übertragungsgeschwindigkeit ist, umso kleiner sollte der Wert für Admin Path Cost sein.

Typische Werte für Wegkosten bei Rapid Spanning Tree:

- 1000 Mbit/s = 20.000
- 100 Mbit/s = 200.000
- 10 Mbit/s = 2.000.000

Admin Point to Point Status
Hierfür gibt es drei Einstellmöglichkeiten:

- Point to Point Connection und Shared Media Connection sind nicht markiert:
  Point to Point wird automatisch ermittelt. Steht der Port auf Halbduplex, wird nicht von einer Point to Point Verbindung ausgegangen.
- Shared media Connection ist markiert:
  Auch bei einer Vollduplexverbindung wird nicht von einer Point to Point-Verbindung ausgegangen.
- Point to Point Connection ist markiert:
  Auch bei Halbduplex wird von einer Point to Point Verbindung ausgegangen.

Hinweis

Point to Point bedeutet eine direkte Verbindung zwischen zwei Switches. Shared Media Connection wäre z.B. eine Verbindung zu einem Hub.

Syntax Command Line Interface

Tabelle 5-66 (Rapid) Spanning Tree Port Configuration - SWITCH\STP\PORTS>

Befehl	Beschreibung	Kommentar
stpport [<E|D> [Ports]]	Aktiviert/Deaktiviert den Spanning Tree-Algorithmus für die angegebenen Ports.	Nur Administrator. Wenn Sie mehrere Ports als Parameter angeben wollen, können Sie die Portnummern durch Leerzeichen, Kommas oder Bindestriche trennen.
prio [<0...255> [ports]]	Legt die Priorität für den Port fest.	Nur Administrator.
pathcost [<0..200000000> [ports]]	Legt die Pfadkosten für den Port fest.	Nur Administrator.

Befehl	Beschreibung	Kommentar
admedge [<T|F> [ports]]	Gibt an, ob an diesem Port ein • T Endgerät oder ein • F Switch angeschlossen ist, welches Spanning Tree bzw. Rapid Spanning Tree unterstützt. Wird ein (Rapid) Spanning Tree-Protokoll empfangen, wird der Wert F angezeigt.	
autoedge [<T|F> [ports]]	Gibt an, ob an diesem Port automatisch erkannt werden soll, ob ein • T Endgerät oder ein • F Switch angeschlossen ist.	Nur Administrator.
ptp [<A|T|F> [ports]]	Die Point-to-Point-Verbindung stellt eine direkte Verbindung zwischen zwei Switches dar. Für diesen Fall gibt es folgende Einstellmöglichkeiten: • A Der Port erkennt anhand der Duplexität einen PtP-Port. Bei Vollduplex wird eine PtP-Verbindung angenommen, bei Halbduplex kein PtP-Verbindung (shared medium). • T Legt auch bei Halbduplex eine PtP-Verbindung fest. • F Legt fest, dass über den betreffenden Port auch bei Vollduplex keine PtP-Verbindung besteht.	-

5.5.15 MSTP (SCALANCE X-300/X408)

5.5.15.1 Multiple Spanning Tree Configuration

Multiple Spanning Tree

Das Multiple Spanning Tree Protocol (MSTP) ist eine Weiterentwicklung des Rapid Spanning Tree Protocols (RSTP).

Beim MSTP wird im Vergleich zum RSTP nicht nur ein Rapid Spanning Tree aufgebaut. Mit MSTP entstehen mehrere voneinander unabhängige Rapid Spanning Tree-Instanzen für verschiedene VLANs. So kann der Verkehr von verschiedenen logischen Netzen über unterschiedliche Wege geleitet werden.

Multiple Spanning Tree-Konfiguration beim IE-Switch

Die Maske "Multiple Spanning Tree Configuration" erscheint, wenn Sie das Ordnersymbol "MSTP" angeklickt haben.
In dieser Maske werden die Parameter für das Multiple Spanning Tree-Protokoll angezeigt und eingestellt.

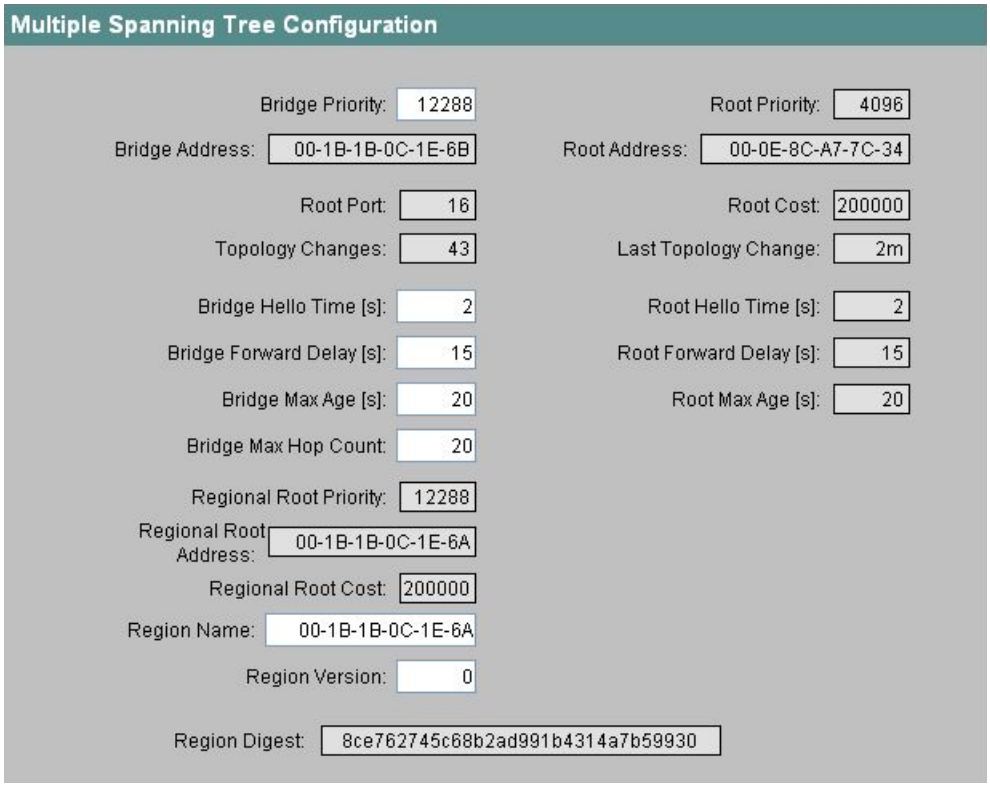


Bild 5-89 Multiple Spanning Tree Configuration

Die folgenden Felder betreffen die Konfiguration des Gerätes und der Root Bridge.
Die linke Spalte bezieht sich auf die Konfiguration des Gerätes. Die rechte Spalte zeigt die Konfiguration der Root Bridge, wie sie aus Spanning Tree-Frames abgeleitet werden kann, die

das Gerät empfangen hat. Aus diesem Grund sind die dort angezeigten Daten nur lesbar. Wenn das Gerät eine Root Bridge ist, stimmen die Informationen der linken und rechten Spalte überein.

- **Bridge Priority / Root Priority**
  Anhand der Bridge-Priorität wird festgelegt, welches Gerät die 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 mit dem niedrigsten Zahlenwert der MAC-Adresse die Root-Bridge.
  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 Frames möglichst zentral angeordnet sein.
  Tragen Sie im Eingabefeld "Bridge Priority" die Priorität des Geräts ein.
  Der Wert für die Bridge-Priorität ist ein ganzzahliges Vielfaches von 4096 mit einem Wertebereich von 0 bis 61440.
  Das Anzeigefeld "Root Priority" zeigt die Priorität der CIST Root Bridge an.
- **Bridge Address / Root Address**
  Das Anzeigefeld "Bridge Adresse" zeigt die MAC-Adresse des Geräts an.
  Das Anzeigefeld "Root Adresse" zeigt die MAC-Adresse der CIST Root Bridge an.
- **Root Port**
  Das Anzeigefeld "Root Port" zeigt den Port, über den das Gerät mit der CIST Root Bridge kommuniziert.
- **Root Cost**
  Das Anzeigefeld "Root Cost" zeigt die Pfadkosten von dem Gerät bis zur CIST Root Bridge.
- **Topologie Changes / Last Topology Change**
  Das Anzeigefeld "Topologie Changes" zeigt die Anzahl der Umkonfigurationen aufgrund des Spanning Tree-Mechanismus seit dem letzten Hochlauf.
  Das Anzeigefeld "Last Topologie Change" zeigt die Zeitdauer seit der letzten Umkonfiguration wie folgt:
  - Sekunden: Zusatz sec hinter der Zahlenangabe
  - Minuten: Zusatz min hinter der Zahlenangabe
  - Stunde: Zusatz hr hinter der Zahlenangabe
- **Bridge Hello Time [s] / Root Hello Time [s]**
  Jede Bridge versendet regelmäßig Konfigurations-Frames (BPDUs).
  Tragen Sie im Eingabefeld "Bridge Hello Time" den Zeitabstand zwischen zwei Konfigurations-Frames ein.
  Der Standardwert für diesen Parameter beträgt 2 Sekunden.
  Das Anzeigefeld "Root Hello Time" zeigt den Zeitabstand zwischen zwei Konfigurations-Frames bei der Root Bridge an.
- **Bridge Forward Delay [s] / Root Forward Delay [s]**
  Neue Konfigurationsinformationen werden von einer Bridge nicht sofort angewendet. So wird sichergestellt, dass der Betrieb entsprechend der neuen Topologie erst gestartet wird, wenn alle Bridges die notwendigen Informationen haben.
  Tragen Sie im Eingabefeld "Bridge Forward Delay" den Zeitraum bis zur Anwendung der neuen Informationen ein.
  Der Standardwert für diesen Parameter beträgt 15 Sekunden.
  Das Anzeigefeld "Root Forward Delay" zeigt den Zeitraum bis zur Anwendung der neuen Informationen bei der Root Bridge an.

- **Bridge Max Age [s] / Root Max Age [s]**
  Tragen Sie im Eingabefeld "Bridge Max Age" das maximale "Alter" ein, das eine empfangene BPDU haben darf, um vom Gerät als gültig akzeptiert zu werden.
  Der Standardwert für diesen Parameter beträgt 20 Sekunden.
  Das Anzeigefeld "Root Max Age" zeigt die Einstellung des maximalen Alters eine empfangene BPDU bei der Root Bridge an.
- **Bridge Max Hop Count**
  Das Eingabefeld "Bridge Max Hop Count" ist nur dann sichtbar, wenn auf der Seite "General" "MSTP" aktiviert und bei "Protocol Compatiblity" "MSTP" eingestellt ist..
  Tragen Sie im Eingabefeld "Bridge Max Hop Count" ein, 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.

Die folgenden Felder betreffen die Konfiguration der CIST Regional Root Bridge, wie sie aus den MSTP-Frames abgeleitet werden kann.
Die angezeigten Daten sind nur dann sichtbar, wenn auf der Seite "General" "MSTP" aktiviert und bei "Protocol Compatiblity" "MSTP" eingestellt ist.

- **Regional Root Priority**
  Das Anzeigefeld "Regional Root Priority" zeigt die Priorität der CIST Regional Root Bridge an.
- **Regional Root Address**
  Das Anzeigefeld "Regional Root Adresse" zeigt die MAC-Adresse der CIST Regional Root Bridge an.
- **Regional Root Cost**
  Das Anzeigefeld "Regional Root Cost" zeigt die Pfadkosten vom Gerät bis zur CIST Regional Root Bridge.
- **Region Name**
  Tragen Sie im Eingabefeld "Region Name" den Namen der MSTP-Region ein, zu der dieses Gerät gehört.
  Defaultmäßig ist hier die MAC-Adresse des Gerätes eingetragen.
  Dieser Wert muss auf allen Geräten, die zur selben MSTP-Region gehören, gleich sein.
- **Region Version**
  Tragen Sie im Eingabefeld "Region Version" 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.
- **Region Digest**
  Das Anzeigefeld "Region Digest" zeigt eine Prüfsumme, mit der die Konfigurationen von VLANs und MSTP-Instanzen verschiedener Geräte verglichen werden können.
  Abhängig von den Parametern, die bei einem Gerät für MSTP eingestellt werden können, entsteht eine spezielle Prüfsumme. Haben mehrere Geräte die gleiche Prüfsumme, sind die Parameter gleich eingestellt.

Hinweis

Damit Geräte zur gleichen MSTP-Region gehören, müssen "Region Name", "Region Version" und "Region Digest" gleich sein.

Syntax Command Line Interface

Tabelle 5-67 Multiple Spanning Tree Configuration - CLI\SWITCH\MSTP>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuelle Spanning Tree-Konfiguration an.	-
bprio [0...61440]	Legt die Bridgepriorität für den IE-Switch fest.	Nur Administrator.
hellotm [1 ... 10]	Legt den Zeitabstand zwischen zwei BPDU-Frames in Sekunden fest.	Nur Administrator.
fwddelay [4 ... 30]	Legt die Verzögerungszeit für die Wirksamkeit von Konfigurationsinformationen fest (Angabe in Sekunden).	Nur Administrator. Default-Wert: 15 s
maxage [6 ... 40]	Legt das maximale Alter für Konfigurations-Informationen fest.	Nur Administrator. Default-Wert: 20 s
maxhopcnt [6 ... 40]	Legt die Anzahl an MSTP-Teilnehmern fest, die eine BPDU passieren darf.	Nur Administrator.
regname	Legt den Namen der MSTP-Region fest, zu der das Gerät gehört.	Nur Administrator.
regvers	Legt die Versionsnummer der MSTP-Region ein, in der sich das Gerät befindet.	Nur Administrator.

5.5.15.2 CIST Port Parameters

Portspezifische Parameter

Die Maske "CIST Port Parameters" erscheint, wenn Sie das Untermenü "CIST Ports" angeklickt haben.

CIST (Common and Internal Spanning Tree) bezeichnet beim MSTP die intern vom Switch verwendete Instanz, die im Prinzip einem internen Rapid Spanning Tree entspricht.

Diese Maske zeigt die aktuellen Port-Parameter, die vom Anwender parametriert wurden oder die über Autofunktionen vom IE-Switch eingestellt wurden.

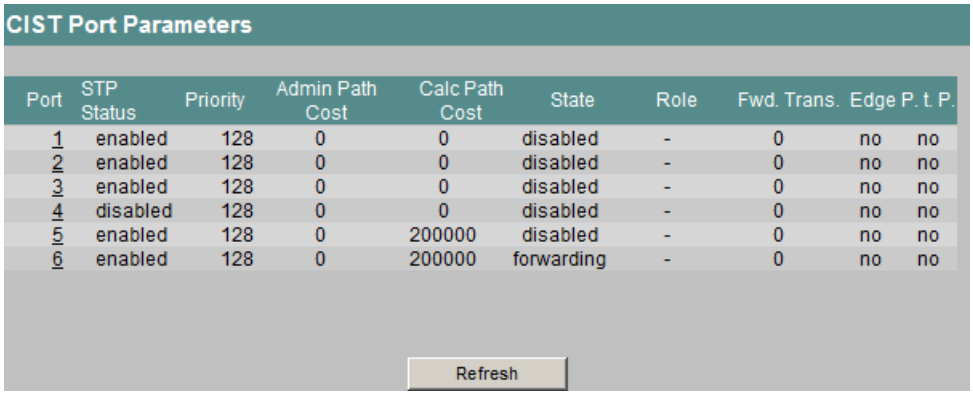


Bild 5-90 CIST Port Parameters

In der Tabelle wird beim Aufruf der Seite der aktuelle Stand der Konfiguration der Port-Parameter angezeigt.

Die Tabelle gliedert sich in folgende Spalten:

- **Port**
  Die Spalte "Port" zeigt die Ports, auf die sich die Informationen beziehen.
- **STP Status**
  Die Spalte "STP Status" zeigt an, ob Spanning Tree für den Port aktiviert (enabled) oder deaktiviert (disabled) ist.
- **Priority**
  Die Spalte "Priority" zeigt den Wert der Priorität an.
  Wenn der von MSTP ermittelte Weg alternativ über mehrere Ports eines Switch führen kann, wird der Port mit der höchsten Priorität, d. h. dem kleinsten Wert für die Priorität, ausgewählt. Für die Priorität kann ein Wert von 0 bis 255 angegeben sein. Der Default-Wert ist 128. Wenn die Prioritäten gleich sind, wird der Pfad mit den kleinsten Pfad-Kosten ausgewählt.
- **Admin Path Cost**
  Zeigt den Wert für die zu verwendenden Pfadkosten an.
- **Calc Path Cost**
  Wenn der Wert für Admin Path Cost > 0 ist, wird dieser Wert als als Calculated Path Cost übernommen.
  Wenn der Wert für Admin Path Cost = 0, wird der Wert für Calculated Path Cost automatisch ermittelt. Die Ermittlung der Pfadkosten richtet sich maßgeblich nach der Übertragungsgeschwindigkeit.
  Je höher die erzielbare Übertragungsgeschwindigkeit ist, umso kleiner sollte der Wert für Admin Path Cost sein.
  Typische Werte für Wegkosten bei Rapid Spanning Tree:
  - 1000 Mbit/s = 20.000
  - 100 Mbit/s = 200.000
  - 10 Mbit/s = 2.000.000
- **State**
  Die Spalte "State" zeigt den Zustand an, in dem sich der Port befindet.
  Folgende Zustände sind möglich:
  - disabled
    Der Port empfängt nur und nimmt nicht am STP, MSTP und RSTP teil.
  - blocking
    Der Port empfängt BPDU-Frames.
  - listening
    Der Port empfängt und sendet BPDU-Frames. Der Port ist in den Spanning Tree-Algorithmus einbezogen.
  - learning
    Vorstufe zum Forwarding-Status, der Port lernt aktiv die Topologie, d. h. die Teilnehmeradressen.
  - forwarding
    Der Port ist nach der Umkonfigurationszeit wieder aktiv im Netz, er empfängt und sendet Datenframes.

- **Role**
  Die Spalte "Role" gibt an, welche Rolle der Port einnimmt:
  - Root
    Der Port hat die niedrigsten Pfadkosten vom Gerät selbst zur CIST Regional Root Bridge.
  - Designated
    Über diesen Port erreicht ein angeschlossenes Netzsegment die CIST Regional Root Bridge mit minimalen Pfadkosten.
  - Alternate
    Der Port ist geblockt und bietet einen alternativen Weg zur CIST Regional Root Bridge.
  - Backup
    Der Port ist geblockt und bietet einen alternativen Weg zu einer Collision Domain, die bereits durch einen anderen Port angebunden ist.
- **FWD Transitions**
  Die Spalte "FWD Transitions" gibt die Anzahl der Wechsel vom Status listening zum Status forwarding an.
- **Edge**
  Die Spalte "Edge" zeigt an, ob an den Port ein Endgerät angeschlossen ist oder nicht.
  Bei einem Endgerät kann ein IE-Switch ohne Rücksicht auf Spanning Tree-Frames schneller den Port umschalten. Wird entgegen dieser Einstellung ein Spanning Tree-Frame empfangen, dann wechselt der Port automatisch in den Zustand no.
  - yes
    An diesem Port befindet sich ein Endgerät.
  - no
    An diesem Port befindet sich ein Spanning Tree- oder Rapid Spanning Tree-Gerät.
- **P.t.P.**
  Eine Point to Point-Verbindung liegt dann vor, wenn zwei RSTP-fähige Netzkomponenten über diesen Port miteinander verbunden sind.
  Folgende Zustände sind möglich:
  - Yes
    Es liegt eine Point to Point-Verbindung vor.
  - No
    Es liegt keine Point to Point-Verbindung vor.

Konfiguration eines Ports für Multiple Spanning Tree

Wenn Sie auf der Seite "CIST Port Parameters" in der Spalte "Port" eine Portbezeichnung anklicken, gelangen Sie zur Seite "Spanning Tree Port Configuration".

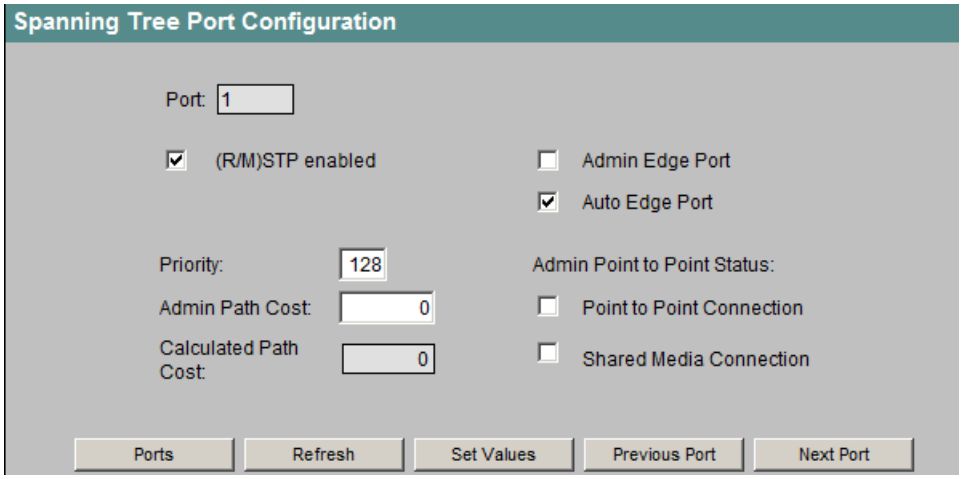


Bild 5-91 Spanning Tree Port Configuration

Die portspezifische Konfiguration der CIST-Port Parameter wird auch für STP und RSTP übernommen. Diese Konfiguration ist daher in MSTP, RSTP und STP gleich.

Die Bescheibung der einzelnen Seitenelemente und CLI-Befehle finden Sie im Kapitel Spanning Tree Port Configuration (Seite 221).

Syntax Command Line Interface

Tabelle 5-68 CIST Port Parameters - CLI\SWITCH\MSTP\CISTPORTS>

Befehl	Beschreibung	Kommentar
info	Zeigt eine Übersicht der Ports und der zugehörigen Rapid Spanning Tree-Einstellungen.	-
stpport [<E|D> [ports]]	Aktiviert/Deaktiviert Spanning Tree für den entsprechenden Port.	Nur Administrator.
prio [<0..255> [ports]]	Legt die Priorität für den entsprechenden Port fest.	Nur Administrator.
pathcost [<0..200000000> [ports]]	Legt die Pfadkosten für den entsprechenden Port fest.	Nur Administrator.
admedge [<T|F> [ports]]	Legt fest, ob an dem entsprechenden Port ein Endgerät oder ein Switch angeschlossen ist: • T Endgerät • F Switch	Nur Administrator.

Befehl	Beschreibung	Kommentar
autoedge [<T|F> [ports]]	Legt fest, dass automatisch erkannt werden soll, ob an dem entsprechenden Port ein Endgerät oder ein Switch angeschlossen ist: • T Endgerät • F Switch Wird ein (Rapid) Spanning Tree-Protokoll empfangen, wird der Wert "F" angezeigt.	Nur Administrator.
ptp [<A|T|F> [ports]]	Die Point-to-Point-Verbindung stellt eine direkte Verbindung zwischen zwei Switches dar. Legt fest, ob es sich bei dem entsprechenden Port um einen PtP-Port handelt: • A PtP wird automatisch ermittelt. Bei Vollduplex wird eine PtP-Verbindung angenommen, bei Halbduplex kein PtP-Verbindung. • T Legt auch bei Halbduplex eine PtP-Verbindung fest. • F Legt bei Vollduplex keine PtP-Verbindung fest.	Nur Administrator.

5.5.15.3 MSTP Instances Configuration

Multiple Spanning Tree-Konfiguration

Die Maske "MSTP Instances Configuration" erscheint, wenn Sie das Untermenü "MST Instances" angeklickt haben.
In dieser Maske können mehrere VLANs in einem LAN mit eigenen Rapid Spanning Trees verwaltet werden.

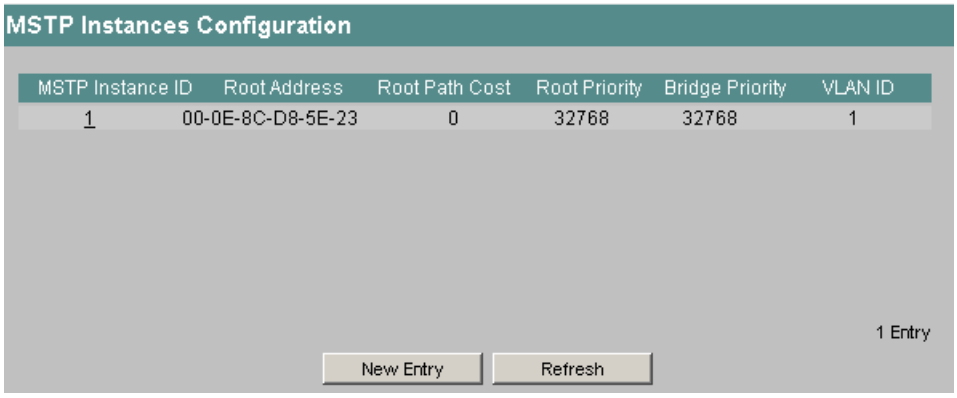


Bild 5-92 MSTP Instances Configuration

Die Tabelle gliedert sich in folgende Spalten:

- **MSTP Instance ID**
  Das Anzeigefeld "MSTP Instance ID" zeigt die Nummer der MSTP-Instanz an.
- **Root Address**
  Das Anzeigefeld "Root Address" zeigt die MAC-Adresse der MST-Instanz Regional Root-Bridge an.
- **Root Path Cost**
  Das Anzeigefeld "Root Path Cost" zeigt die Pfadkosten von dem Gerät bis zur MST-Instanz Regional Root Bridge an.
- **Root Priority**
  Das Anzeigefeld "Root Priority" zeigt die Priorität der MST-Instanz Regional Root-Bridge an.
- **Bridge Priority**
  Das Anzeigefeld "Bridge Priority" zeigt die Priorität des Geräts an.
- **VLAN ID**
  Das Anzeigefeld "VLAN ID" zeigt die Nummer des VLANs an.

Neue MSTP Instanz anlegen

1. Klicken Sie im Fenster "MSTP Instances Configuration" auf die Schaltfläche "New Entry".
   Das Fenster "MSTP Instance Configuration" erscheint.

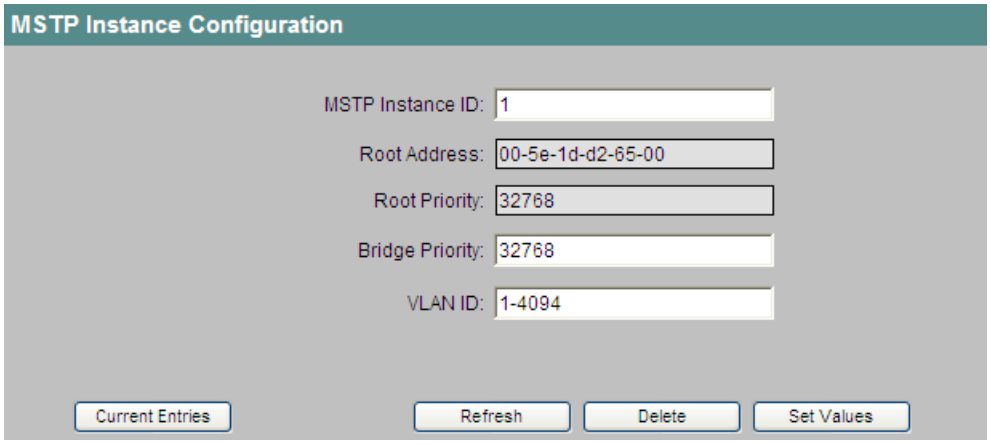


Bild 5-93 MSTP Instance Configuration

2. Tragen Sie in das Eingabefeld "MSTP Instance ID" die Nummer der MSTP-Instanz ein.
   Zulässige Werte: 1 bis 16
3. Tragen Sie in das Eingabefeld "Bridge Priority" die Bridge-Priorität ein.
   Der Wert für die Bridge-Priorität ist ein ganzzahliges Vielfaches von 4096 mit einem Wertebereich von 0 bis 61440.
4. Tragen Sie in das Eingabefeld "VLAN ID" 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 bis 4094
5. Um die Einstellungen zu speichern, klicken Sie auf die Schaltfläche "Set Values".
6. Um Current Entries zurück zur Maske "MSTP Instances Configuration" zu gelangen, klicken Sie auf die Schaltfläche "Current Entries".

MSTP Instanz löschen

1. Klicken Sie im Fenster "MSTP Instances Configuration" in der Spalte "MSTP Instance ID" auf die gewünschte ID.
   Das Fenster "ISTP Instances Configuration" erscheint.
2. Um die MSTP Instanz zu löschen, klicken Sie auf die Schaltfläche "Delete".

Syntax Command Line Interface

Tabelle 5-69 MSTP Instances Configuration - CLI\SWITCH\MSTP\MSTI>
MSTP Instance Configuration - CLI\SWITCH\MSTP\MSTI>

Befehl	Beschreibung	Kommentar
info	Zeigt Informationen zu den MSTP Instanzen an.	-
add <MST ID> <brgPrio> <vlans (1-4094)>	Erzeugt und ändert eine MSTP Instanz.	Nur Administrator.
delete <MST ID>	Löscht die MSTP Instanz.	Nur Administrator.

5.5.15.4 Multiple Spanning Tree Port Configuration

(Multiple) Spanning Tree Ports

Die Maske "MSTP Ports" erscheint, wenn Sie das Untermenü "MST Ports" angeklickt haben.
In dieser Maske stellen Sie die Parameter für die Ports der konfigurierten Multiple Spanning Tree Instanzen ein.

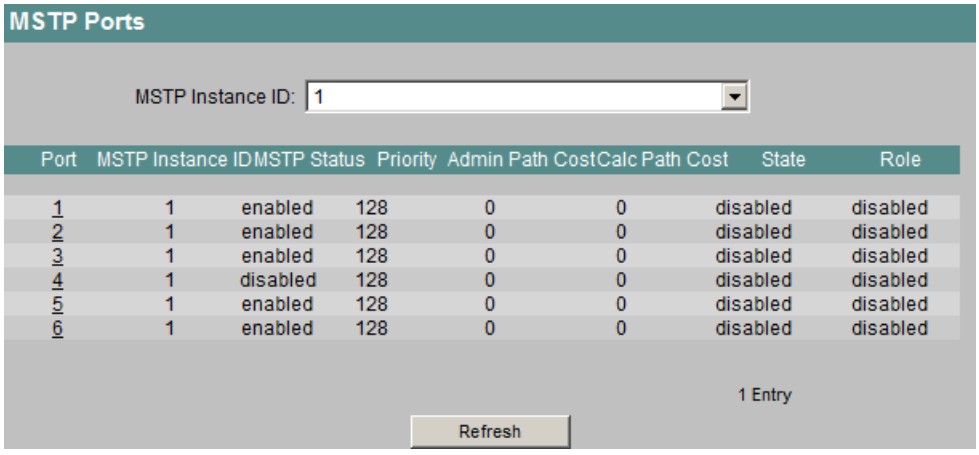


Bild 5-94 MSTP Ports

Die Seite enhält folgendes Feld:

- **MSTP Instance ID**
  Wählen Sie in der Klappliste "MSTP Instance ID" die ID der MSTP-Instanz aus.

Die Tabelle gliedert sich in folgende Spalten:

- **Port**
  Die Spalte "Port" zeigt die Ports, auf die sich die Informationen beziehen.
- **MSTP Instance ID**
  Die Spalte "MSTP Instance ID" zeigt die Nummer der MSTP-Instanz an.
- **MSTP Status**
  Die Spalte "MSTP Status" zeigt an, ob Multiple Spanning Tree für den Port aktiviert (enabled) oder deaktiviert (disabled) ist.

- **Priority**
  Die Spalte "Priority" zeigt den Wert der Priorität an.
  Wenn der von MSTP ermittelte Weg alternativ über mehrere Ports eines Switch führen kann, wird der Port mit der höchsten Priorität, d. h. dem kleinsten Wert für die Priorität, ausgewählt.
  Für die Priorität kann ein Wert von 0 bis 255 angegeben sein. Der Default-Wert ist 128.
- **Admin Path Cost**
  Die Spalte "Admin Path Cost " zeigt den Wert für die u verwendenden Pfadkosten an.
- **Calc Path Cost**
  Wenn der Wert für Admin Path Cost > 0 ist, wird dieser Wert als als Calculated Path Cost übernommen.
  Wenn der Wert für Admin Path Cost = 0, wird der Wert für Calculated Path Cost automatisch ermittelt. Die Ermittlung der Pfadkosten richtet sich maßgeblich nach der Übertragungsgeschwindigkeit.
  Je höher die erzielbare Übertragungsgeschwindigkeit ist, umso kleiner sollte der Wert für Admin Path Cost sein.
  Typische Werte für Wegkosten bei Rapid Spanning Tree:
  - 1000 Mbit/s = 20.000
  - 100 Mbit/s = 200.000
  - 10 Mbit/s = 2.000.000

- **State**
  Die Spalte "State" zeigt den Zustand an, in dem sich der Port befindet.
  Folgende Zustände sind möglich:
  - disabled
    Der Port empfängt nur und nimmt nicht am STP, MSTP und RSTP teil.
  - blocking
    Der Port empfängt BPDU-Frames.
  - listening
    Der Port empfängt und sendet BPDU-Frames. Der Port ist in den Spanning Tree-Algorithmus einbezogen.
  - learning
    Vorstufe zum Forwarding-Status, der Port lernt aktiv die Topologie, d. h. die Teilnehmeradressen.
  - forwarding
    Der Port ist nach der Umkonfigurationszeit wieder aktiv im Netz, er empfängt und sendet Datenframes.
- **Role**
  Die Spalte "Role" gibt an, welche Rolle der Port einnimmt:
  Folgende Werte sind möglich:
  - Root
    Der Port hat die niedrigsten Pfadkosten vom Gerät selbst zur Regional Root Bridge der MST-Instanz.
  - Designated
    Über diesen Port erreicht ein angeschlossenes Netzsegment die MSTI Regional Root Bridge mit minimalen Pfadkosten.
  - Alternate
    Der Port ist geblockt und bietet einen alternativen Weg zur MSTI Regional Root Bridge.
  - Backup
    Der Port ist geblockt und bietet einen alternativen Weg zu einer Collision Domain, die bereits durch einen anderen Port angebunden ist.

(Multiple) Spanning Tree Port Configuration

Wenn Sie auf der Seite "MSTP Ports" in der Spalte "Port" eine Portbezeichnung anklicken, gelangen Sie zur Seite "(Multiple) Spanning Tree Port Configuration":

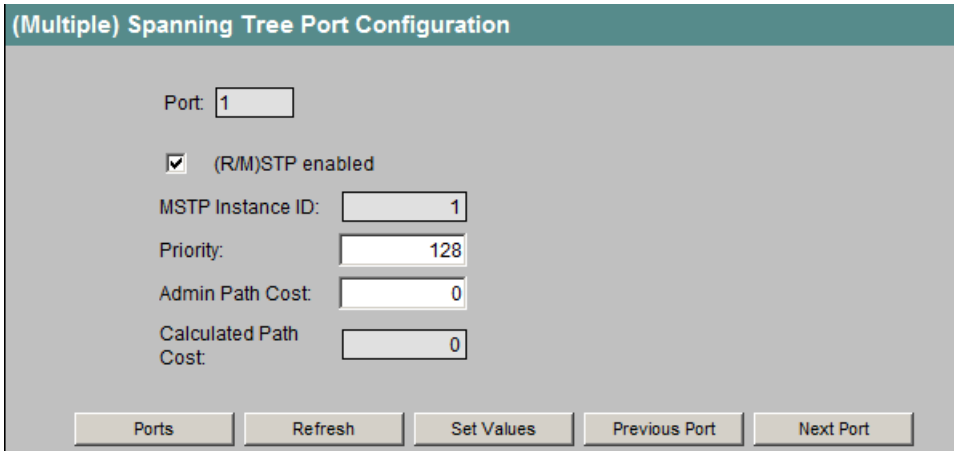


Bild 5-95 Multiple Spanning Tree Port Configuration

Port

Das Anzeigefeld "Port" zeigt den ausgewählten Port an.

(R/M)STP enabled

Aktivieren Sie diese Option, wenn der Port (Multiple) Spanning Tree-Protokoll verwenden soll.

MSTP Instance ID

Das Anzeigefeld "MSTP Instance ID" zeigt die MSTP Instances ID des ausgewählten Ports an.

Priority

Tragen Sie im Eingabefeld "Priority" einen Wert für die Port-Priorität ein.
Zulässige Werte: 0 bis 255

Admin Path Cost

Hier können die Werte für die zu verwendenden Pfadkosten pro Port und MST-Instanz manuell vorgegeben werden.

Calculated Path Cost

Wenn der Wert für Admin Path Cost > 0 ist, wird dieser Wert als als Calculated Path Cost übernommen.
Wenn der Wert für Admin Path Cost = 0, wird der Wert für Calculated Path Cost automatisch ermittelt. Die Ermittlung der Pfadkosten richtet sich maßgeblich nach der Übertragungsgeschwindigkeit.

Je höher die erzielbare Übertragungsgeschwindigkeit ist, umso kleiner sollte der Wert für Admin Path Cost sein.

Typische Werte für Wegkosten bei Rapid Spanning Tree:

- 1000 Mbit/s = 20.000
- 100 Mbit/s = 200.000
- 10 Mbit/s = 2.000.000

Syntax Command Line Interface

Tabelle 5-70 MSTP Ports/Multiple Spanning Tree Port Configuration - CLI\SWITCH\MSTP\MSTPORTS>

Befehl	Beschreibung	Kommentar
info <MST ID>	Zeigt Port-Informationen zu einer MSTP Instanzen an.	-
prio <MST ID> <0..240> <ports>	Legt die Bridgepriorität des Ports fest.	Nur Administrator.
pathcost <MST-ID> <0..200000000>	Legt die Pfadkosten des Ports in einer Instanz fest.	Nur Administrator.

5.5.16 QoS

5.5.16.1 QoS Configuration

QoS

Unterschiedliche Anwendungen haben unterschiedliche Anforderungen an Netzwerke. Für reine Dateitransfers ist der Gesamtdurchsatz entscheidend, während die individuelle Latenz und Verlustrate weniger von Bedeutung sind. Für Echtzeitkommunikation wie z.B. Voice over IP hingegen spielen die Latenz, der Jitter und die Verlustrate eine weitaus größere Rolle, weil sie maßgeblich die Sprachverständlichkeit beeinflussen.

Übertragungsprioritäten

Die IE-Switche X-300/400 unterstützen CoS to Queue sowie DSCP to Queue Mapping, wodurch Pakete unterschiedlicher Herkunft mit unterschiedlicher Priorität weitergeleitet werden können. Das DSCP Mapping ist aus Gründen der Abwärtskompatibilität zu früheren Firmwareständen per default deaktiviert.

Priorisierung von CoS- und DSCP-Informationen

Bei aktiviertem DSCP-Mapping werden CoS- und DSCP-Informationen wie folgt verarbeitet:

SCALANCE X-300 / SCALANCE X-408

- Wurde DSCP-Mapping aktiviert und enthält ein Telegramm sowohl CoS- als auch DSCP-Informationen, wird das Telegramm entsprechend der DSCP-Priorität weitergeleitet. Die CoS-Information wird ignoriert.

SCALANCE X414

- Wurde DSCP-Mapping aktiviert und enthält ein Telegramm nur DSCP-Informationen, so werden die DSCP-Prioritäten vom Switch Controller entsprechend der Einstellung "CoS to Queue Mapping" auf einen CoS-Wert abgebildet. Die Default-Werte von "CoS to Queue Mapping" können bei Bedarf geändert werden.
- Wurde DSCP-Mapping aktiviert und enthält ein Telegramm sowohl CoS- als auch DSCP-Informationen, wird das Telegramm entsprechend der DSCP-Priorität weitergeleitet. Die CoS-Information wird ignoriert.

Übersicht

Der Inhalt dieser Seite ist abhängig von Ihrem Gerät.

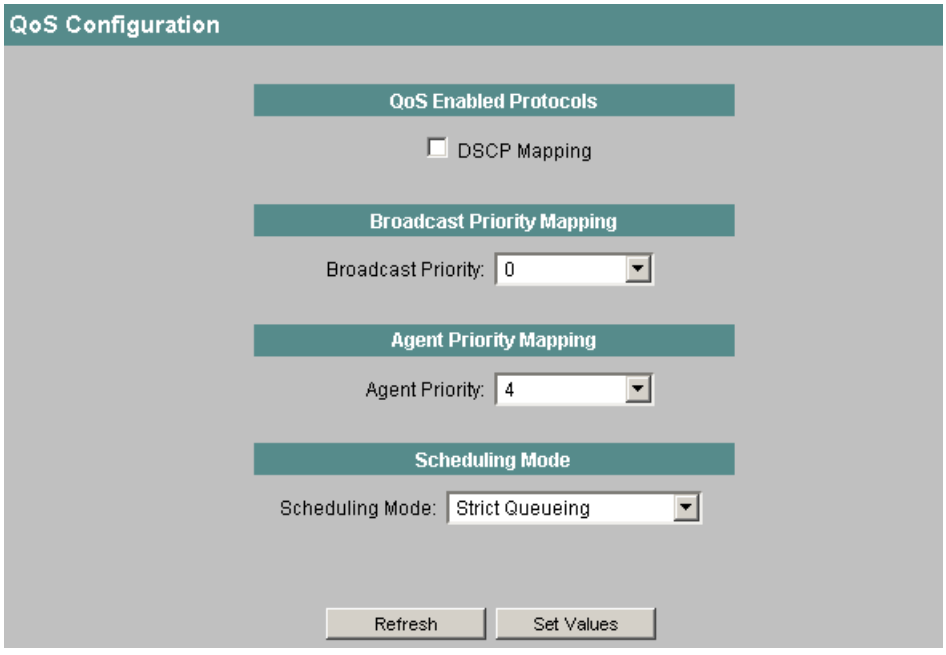


Bild 5-96 X-300 QoS Configuration

DSCP Mapping
Aktiviert/Deaktiviert das DSCP to Queue Mapping

Die folgenden Einstellungen sind nur bei IE-Switchen X-300 vorhanden:

Broadcast Priority

Legen Sie fest, mit welcher Priorität Broadcast-Frames versendet werden.

Agent Priority

Legen Sie fest, mit welcher Priorität Agent-Frames versendet werden.

Scheduling Mode

- Strict Queueing
  Solange sich Frames mit einer hohen Priorität in der Warteschlange befinden, werden nur diese hoch priorisierten Frames abgearbeitet.
- Weighted Fair Queueing (nur bei SCALANCE X-300)
  Auch wenn sich Frames mit einer hohen Priorität in der Warteschlange befinden, werden gelegentlich Frames mit einer niedrigeren Priorität abgearbeitet

Syntax Command Line Interface

Tabelle 5-71 QoS Configuration - CLI\SWITCH\QOS>

Befehl	Beschreibung	Kommentar
dscpmap [E|D]	Aktiviert/Deaktiviert DSCP to Queue Mapping.	Nur Administrator.
bcprio [noforce : <0-7>]	Legen Sie fest, mit welcher Priorität Broadcast-Frames versendet werden.	Nur Administrator.
agentprio [noforce : <0-7>]	Legen Sie fest, mit welcher Priorität Agent-Frames versendet werden.	Nur Administrator.
sched [mode]	Legt den Scheduling Mode fest.	Nur Administrator.

5.5.16.2 CoS to Queue Mapping

CoS Queue

Hier werden CoS Prioritäten bestimmten Warteschlangen (Traffic Queues) zugeordnet.

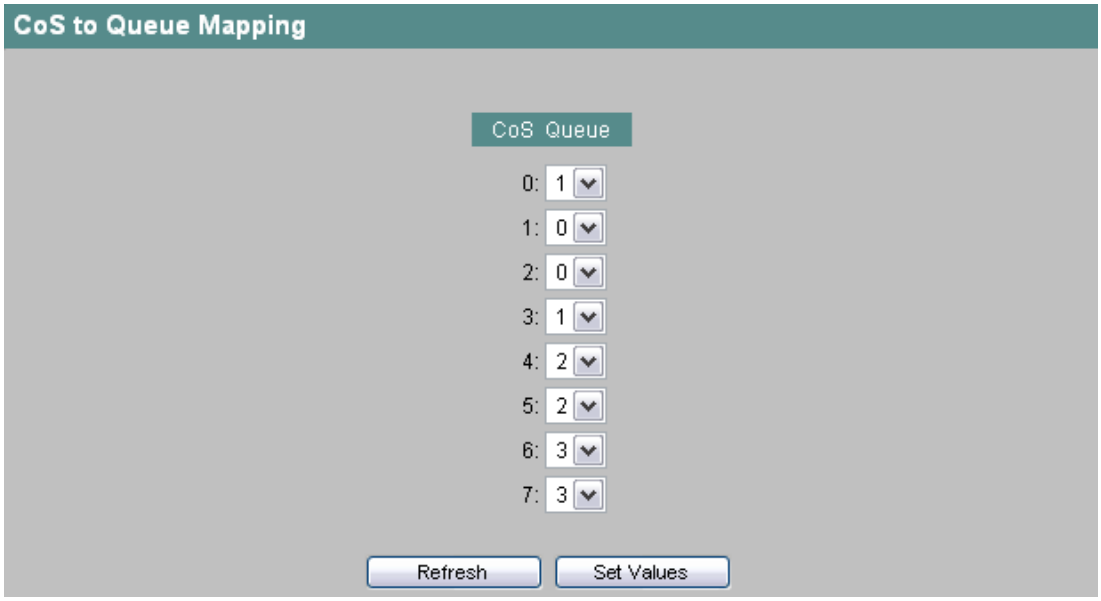


Bild 5-97 CoS to Queue Mapping

CoS
Die CoS Prioritäten-Reihenfolge der eingehenden Pakete.

Queue
Die Traffic-Forwarding-Queue (Sendepriorität) welcher die CoS-Priorität zugeordnet wird.

Syntax Command Line Interface

Tabelle 5-72 QOS Configuration - CLI\SWITCH\QOS>

Befehl	Beschreibung	Kommentar
cos [<0..3> <0..7>]	Ordnet CoS Prioritäten bestimmten Warteschlangen (Traffic Queues) zu: • Parameter 1 Queue • Parameter 2 CoS-Priorität	Nur Administrator.

5.5.16.3 DSCP to Queue Mapping

DSCP Queue

Hier werden DSCP-Einstellungen verschiedenen Warteschlangen (Traffic Queues) zugeordnet.

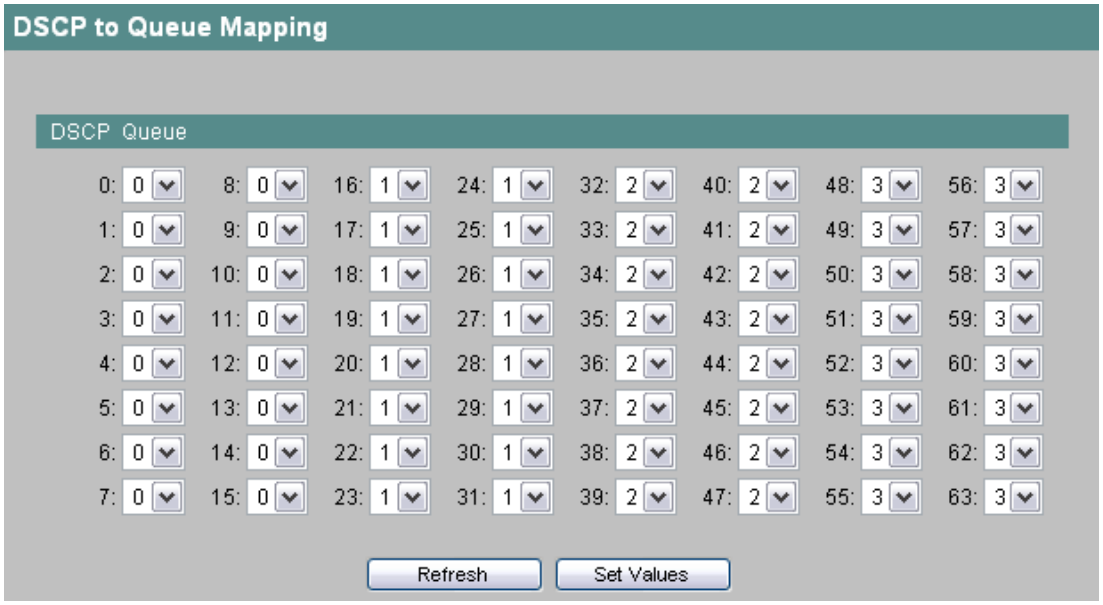


Bild 5-98 DSCP to Queue Mapping

DSCP
Der DSCP Prioritäten-Reihenfolge der eingehenden Pakte.

Queue
Die Traffic-Forwarding-Queue (Sendepriorität) welcher der DSCP Wert zugeordnet wird.

Syntax Command Line Interface

Tabelle 5-73 QoS Configuration - CLI\SWITCH\QOS>

Befehl	Beschreibung	Kommentar
dscp [<0..3> <0..63>]	Ordnet DCSP Einstellungen bestimmten Traffic Queues zu: • Parameter 1 Queue • Parameter 2 DSCP-Wert	Nur Administrator.

5.5.17 LLDP

5.5.17.1 LLDP Configuration

Anwendungen

PROFINET benutzt das LLDP Protokoll für die Topologie Diagnose. In der Werkseinstellung ist LLDP für alle Ports aktiviert, d. h. es werden LLDP-Frames auf allen Ports gesendet und empfangen. Mit dieser Funktion haben Sie die Möglichkeit das Aussenden und/oder Empfangen pro Port ein-/auszuschalten.

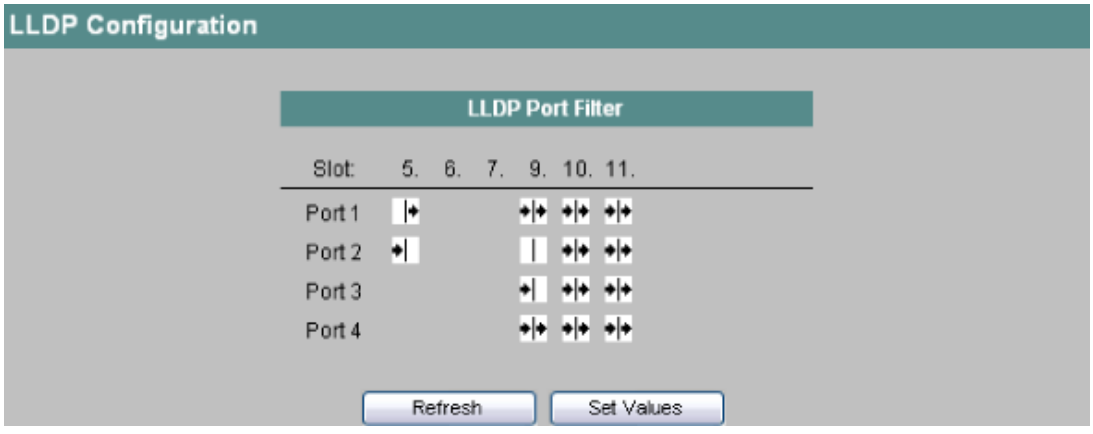


Bild 5-99 LLDP Configuration

Slot / Port

Wählen Sie hier aus, welche Ports LLDP Empfang und/oder Versand unterstützen sollen:



Rx-only: Dieser Port kann LLDP-Frames nur empfangen.



Tx-only: Dieser Port kann LLDP-Frames nur senden.



Tx and Rx: Dieser Port kann LLDP-Frames empfangen und senden.

Disabled: Dieser Port kann LLDP-Frames weder empfangen noch senden.

Syntax Command Line Interface

Tabelle 5-74 Current Multicast Groups - CLI\SWITCH\LLDP>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen LLDP-Einstellungen an.	-
lldpport <mode> [Ports]	Ändert die LLDP-Einstellungen für einen Port. Wird kein Port angegeben, werden alle Ports geändert. Der Parameter <mode> kann die folgenden Werte annehmen: • rx nur Empfang • tx nur Versand • e Empfang und Versand • d weder Empfang noch Versand	Nur Administrator.

5.5.17.2 LLDP Neighbors

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.

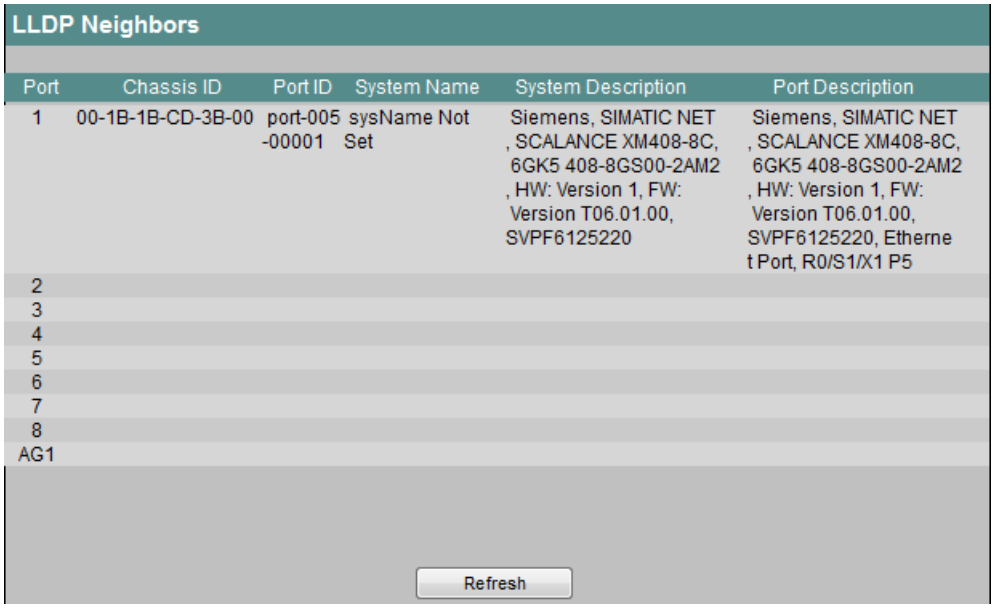


Bild 5-100 LLDP Neighbors

Port

Zeigt die verfügbaren Ports, an dem der IE-Switch die Informationen empfangen hat.

Chassis ID

Zeigt die Gerätekennung des angeschlossenen Geräts an. Die Geräte-ID entspricht dem Gerätenamen, Die Geräte-ID entspricht dem Gerätenamen, der z. B. über SINEC PNI vergeben wird. Wenn kein Gerätename vergeben ist, wird die MAC-Adresse des Geräts angezeigt.

Port ID

Zeigt den Port des angeschlossenen Geräts.

System Name

Zeigt den Systemnamen des angeschlossenen Geräts. Wenn kein Systemname vergeben ist, wird "sysName Not Set" angezeigt.

System Description

Zeigt eine Beschreibung des angeschlossenen Geräts an, z. B. Gerät, Artikelnummer und Firmware-Version.

Port Description

Zeigt eine Beschreibung des Ports an.

Syntax Command Line Interface

Tabelle 5-75 Current Multicast Groups - CLI\SWITCH\LLDP>

Befehl	Beschreibung	Kommentar
neighbors	Zeigt den aktuellen Inhalt der Nachbarschafts-tabelle an.	Nur Administrator.

5.5.18 Fiber Monitoring Protocol

Voraussetzungen

- Sie können das Fiber Monitoring Protocol (FMP) nur bei diagnosefähigen Transceivern verwenden. Geräte und Module mit diagnosefähigen Transceivern sind mit dem Zusatz "FM" gekennzeichnet.
- Um das Fiber Monitoring Protocol (FMP) nutzen zu können, aktivieren Sie LLDP. Die FMP-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 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. Unter "Agent > Event Configuration" können Sie einstellen wie der IE-Switch das Event anzeigt. Unter "X-300 > Fault Mask" können Sie außerdem einstellen, ob ein Fehler signalisiert werden soll.

Status der Ports

Diese Seite zeigt die aktuellen Port-Parameter, die vom Anwender parametriert wurden.

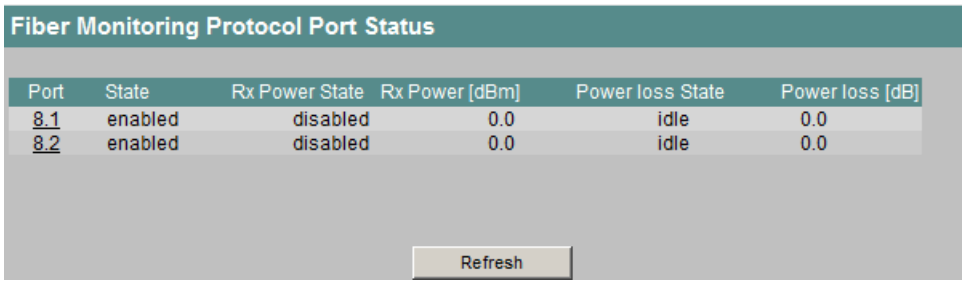


Bild 5-101 Fiber Monitoring Protocol Port Status

Port

Zeigt die verfügbaren optischen Ports an.

State

FMP ist aktiviert (enabled) oder deaktiviert (disabled)

Rx Power State

- **disabled**
  FMP ist deaktiviert.
- **ok**
  Der Wert für die Empfangsleistung der optischen Strecke ist in Ordnung.
- **maintenance required**
  Die Strecke sollte überprüft werden.
  Es wird ein Event ausgelöst.
- **maintenance demanded**
  Die Strecke muss überprüft werden.
  Es wird ein Event ausgelöst.
- **link down**
  Die Verbindung ist unterbrochen.

Rx Power [dBm]

Zeigt den aktuellen Wert der Empfangsleistung an.

Der Wert kann eine Toleranz von +/- 3 dB haben.

Power loss State

Um den Leistungsabfall der Verbindung überwachen zu können, braucht der Port eine Verbindung zu einem anderen Port mit aktiviertem FMP.

- **disabled**
  FMP ist deaktiviert.
- **ok**
  Der Wert für den Leistungsabfall der optischen Strecke ist in Ordnung.
- **maintenance required**
  Die Strecke sollte überprüft werden.
  Es wird ein Event ausgelöst.

- **maintenance demanded**
  Die Strecke muss überprüft werden.
  Es wird ein Event ausgelöst.
- **idle**
  Der Port hat keine Verbindung zu einem anderen Port mit aktiviertem FMP.
  Wenn 5 Zyklen lang keine Diagnoseinformationen empfangen wurden, gilt die Verbindung als unterbrochen. Ein Zyklus dauert 5 Sekunden.

Power loss [dB]

Zeigt den aktuellen Wert des Leistungsabfalls an.

Der Wert kann eine Toleranz von +/- 3 dB haben.

Einstellung der Leistungsgrenzen

Wenn Sie auf der Seite "Fiber Monitoring Protocol Port Status" in der Spalte "Port" eine Portbezeichnung anklicken, gelangen Sie zur Seite "FMP Port Configuration":

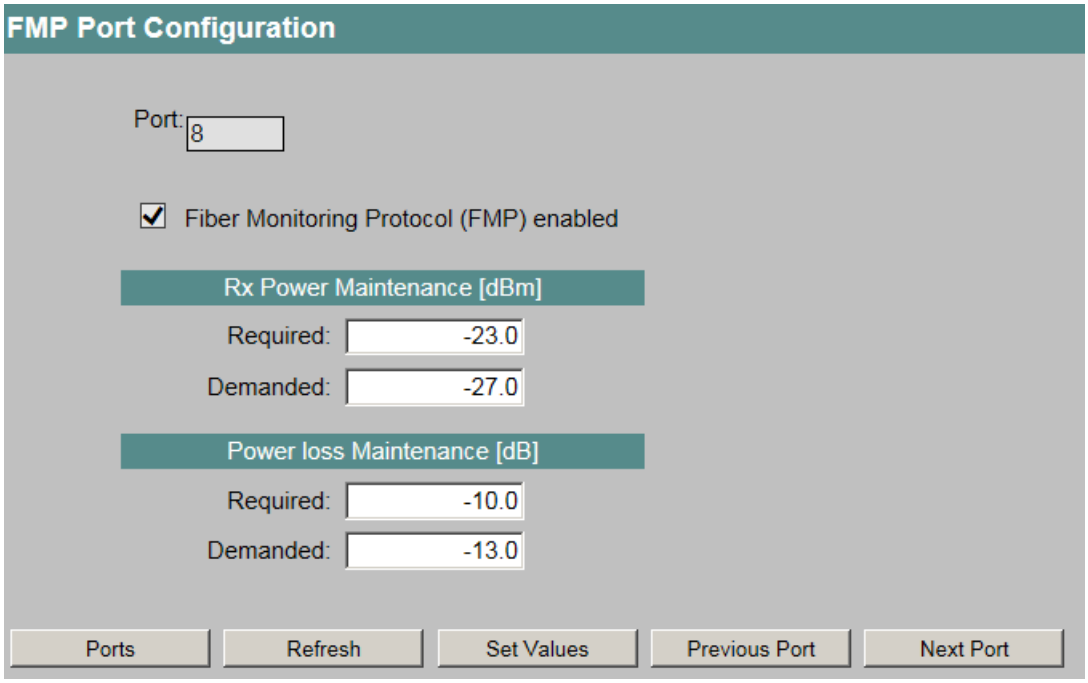


Bild 5-102 FM Port Configuration

Port

Zeigt die verfügbaren optischen Ports an.

Fiber Monitoring Protcol (FMP) enabled

Aktivieren (enabled) oder Deaktivieren (disabled) Sie FMP.

Rx Power Maintenance

- **Required**
  Tragen Sie den Wert ein, bei dem Sie zum ersten Mal über eine Verschlechterung der Empfangsleistung informiert werden wollen.
  Wenn Sie den Wert "0" eintragen, wird die Empfangsleistung nicht überwacht.
- **Demanded**
  Tragen Sie den Wert ein, bei dem Sie zum zweiten Mal über eine Verschlechterung der Empfangsleistung informiert werden wollen.
  Wenn Sie den Wert "0" eintragen, wird die Empfangsleistung nicht überwacht.

Hinweis

FMP bei SFP-Stecktransceivern

Bei SFP-Stecktransceivern können Sie die minimale Empfangsleistung auslesen, unter "Switch > Port Diagnostics > SFP Diagnostics" im Feld "RX Power (dBm)", Spalte "Low".

Es wird empfohlen, die minimale Empfangsleistung als Wert für "Rx Power Maintenance Demanded" einzustellen. Wählen Sie für "Rx Power Maintenance Required" einen höheren Wert, der z. B. 3 dBm über der minimalen Empfangsleistung liegt. Sie werden dadurch zum ersten Mal über eine Verschlechterung der Empfangsleistung informiert, bevor die minimale Empfangsleistung des SFP-Stecktransceivers unterschritten wird.

Power loss Maintenance

- **Required**
  Tragen Sie den Wert ein, bei dem Sie zum ersten Mal über den Leistungsabfall der Verbindung informiert werden wollen.
  Wenn Sie den Wert "0" eintragen, wird der Leistungsabfall nicht überwacht.
- **Demanded**
  Tragen Sie den Wert ein, bei dem Sie zum zweiten Mal über den Leistungsabfall der Verbindung informiert werden wollen.
  Wenn Sie den Wert "0" eintragen, wird der Leistungsabfall nicht überwacht.

Hinweis

FMP bei SFP-Stecktransceivern

Bei SFP-Stecktransceivern können Sie den maximal zulässigen Leistungsabfall berechnen: Differenz der minimalen Empfangsleistung und minimalen Sendeleistung der beiden verbundenen SFP-Stecktransceiver.

Sie finden die minimale Empfangsleistung unter "Switch > Port Diagnostics > SFP Diagnostics" im Feld "RX Power (dBm)", Spalte "Low".

Sie finden die minimale Sendeleistung unter "Switch > Port Diagnostics > SFP Diagnostics" im Feld "TX Power (dBm)", Spalte "Low".

Es wird empfohlen, den maximal zulässigen Leistungsabfall als Wert für "Power loss Maintenance Demanded" einzustellen. Wählen Sie für "Power loss Maintenance Required" einen niedrigeren Wert, der z. B. 3 dBm unter dem maximal zulässigen Leistungsabfall liegt. Sie werden dadurch zum ersten Mal über eine Erhöhung des Leistungsabfalls informiert, bevor der maximal zulässige Leistungsabfall des SFP-Stecktransceivers überschritten wird.

Syntax Command Line Interface

Tabelle 5-76 Fiber Monitoring Protocol - CLI\SWITCH\FMP>

Befehl	Beschreibung	Kommentar
info	Zeigt die FMP-Konfiguration an.	
limit [rx | loss] [req | dem] [<port>] [<limit>]	Legt die Grenzen für die Empfangsleistung und den Leistungsabfall pro Port fest: • rx Empfangsleistung • loss Leistungsabfall • req Erste Benachrichtigung • dem Zweite Benachrichtigung • port Port, für den die Einstellungen gelten • limit Wert für die Grenzen der Empfangsleistung bzw. des Leistungsabfalls in dBm.	Nur Administrator Wenn Sie den Wert "0" eintragen, wird die Empfangsleistung bzw. der Leistungsabfall nicht überwacht.
enable <D|E> [<Port>]	Aktiviert/deaktiviert FMP für den angegebenen Port.	Nur Administrator

Tabelle 5-77 Fiber Monitoring - CLI\SWITCH\FM>

Befehl	Beschreibung	Kommentar
info	Zeigt allgemeine Informationen zu den Transceivern, z. B. Model, Seriennummer sowie aktuelle Werte, z. B. Empfangs- und Sendeleistung.	

5.5.19 DCP Configuration

Anwendungen

Das DCP Protokoll wird von Step 7 und SINEC PNI für die Konfiguration und Diagnose der IE-Switche verwendet. In der Werkseinstellung ist DCP auf allen Ports aktiviert, d.h. empfangene DCP-Frames werden auf allen Ports weitergeleitet. Mit dieser Option haben Sie die Möglichkeit, das Aussenden der DCP-Multicast-Frames pro Port auszuschalten, um z.B. einzelne Netzbereiche von der Konfiguration mit SINEC PNI abzuschotten, bzw. um das gesamte Netz in kleinere Teilnetze für die Konfiguration und Diagnose zu unterteilen.

Hinweis

Diese Funktion hat keinen Einfluss auf dem Empfang der DCP-Frames.

Durch entsprechende Einstellungen wird das Weiterleiten der DCP-Frames allerdings nur für solche Ports verhindert, die "Untagged Member" im Management-VLAN sind. Für andere VLANs sind diese DCP-Frames "Unknown Multicast", der weitergeleitet wird.

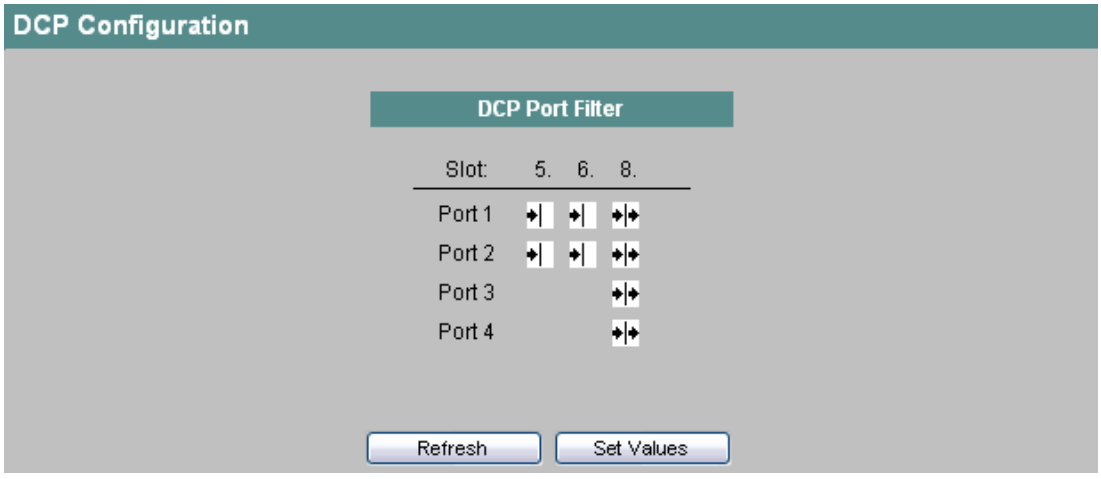


Bild 5-103 DCP Configuration

Wählen Sie hier aus, welche Ports den DCP-Versand unterstützen sollen:



Rx-only: Dieser Port sendet keine DCP-Multicast-Frames. Die DCP-Kommunikation über Unicasts wird nicht gefiltert.



Tx and Rx: Dieser Port sendet alle DCP-Frames.

Syntax Command Line Interface

Tabelle 5-78 Current Multicast Groups - CLI\SWITCH\DCP>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen DCP-Einstellungen an.	-
dcpport <mode> [Ports]	Ändert die DCP-Einstellungen für einen Port. Wird kein Port angegeben, werden alle Ports geändert. Der Parameter <mode> kann die folgenden Werte annehmen: • rx Der Port empfängt alle DCP-Frames, leitet jedoch nur DCP-Unicast-Frames weiter. • e Der Port empfängt und sendet alle DCP-Frames.	Nur Administrator.

5.5.20 DHCP Relay Agent

5.5.20.1 DHCP Relay Agent Configuration

IP-Adresse an Endgerät vergeben

Die Funktion DHCP Relay vermittelt zwischen einem DHCP-Server und einem Endgerät, das an einen bestimmten Port angeschlossen ist, um eine IP-Adresse an dieses Endgerät zu vergeben. Dazu gibt der IE-Switch die Portnummer des Endgeräts zusammen mit der DHCP-Anfrage an den DHCP-Server weiter.

Angabe von DHCP-Server IP-Adressen

Sie können für den DHCP Relay Agent bis zu 4 DHCP-Server IP-Adressen angeben, siehe auch Menüpunkt "Switch Configuration".

Für jeden DHCP-Server können Sie konfigurieren, für welche Ports und VLANs er zuständig ist, siehe "DHCP Relay Agent Port Configuration (Seite 254)".

Wenn eine DHCP-Anfrage empfangen wird, vergleicht der IE-Switch zunächst, ob die Anfrage zu der Port-/VLAN-Konfiguration von DHCP-Server 1 passt.

Wenn die Anfrage passt, leitet der IE-Switch die DHCP-Anfrage weiter und die DHCP-Server-Liste wird nicht weiter durchsucht.

Wenn die Anfrage nicht passt, vergleicht der IE-Switch die Anfrage mit den Konfigurationen von DHCP-Server 2, 3 und 4.

Wenn die eingehende DHCP-Anfrage zu keinem DHCP-Server passt, können Sie optional einstellen, dass sie als Broadcast weitergeleitet wird.

Sie können ebenfalls optional einstellen, dass der Abgleich auf erreichbare DHCP-Server beschränkt wird.

Hinweis

Der DHCP Relay Agent ist nur dann aktiv, wenn im Menüpunkt "Switch Configuration" die Option "DHCP Option 82" aktiviert ist.

Wenn sich der DHCP-Client und der DHCP-Server nicht im gleichen VLAN befinden, werden DHCP-Anfragen nur weitergeleitet, wenn im Menüpunkt "Agent Configuration" die Option "Accessible in all VLANs" aktiviert ist.

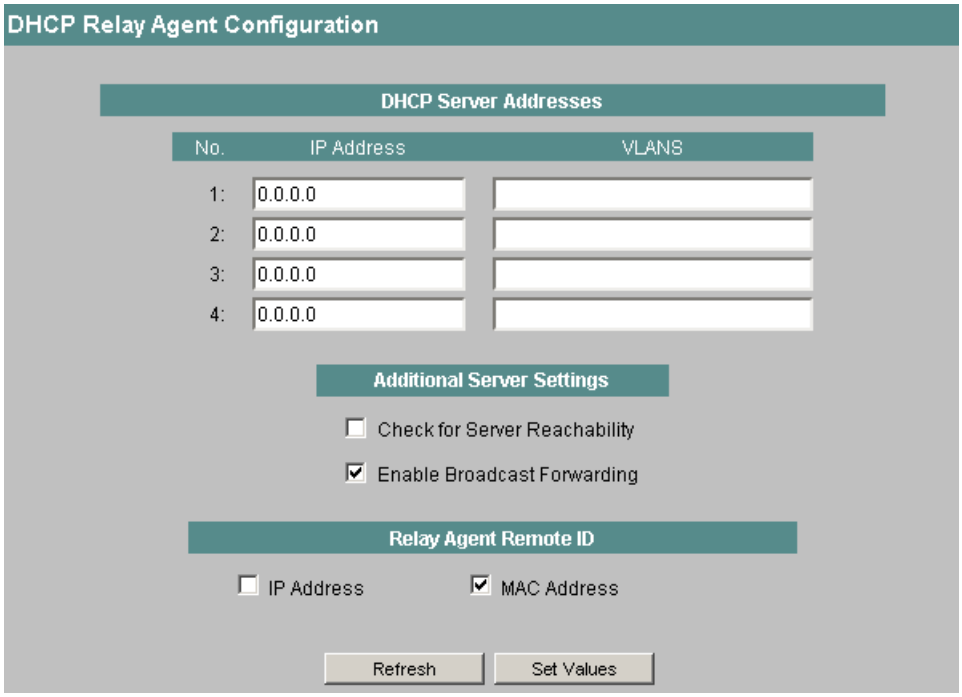


Bild 5-104 DHCP Relay Agent Configuration

IP-Address
Tragen Sie die Adressen der DHCP Server ein, an die der IE-Switch DHCP-Anfragen weiterleiten soll.

VLANs
Tragen Sie die Nummer der VLANs ein, in denen der Port Mitglied ist.
Sie können mehrere einzelne VLANs sowie VLAN-Bereiche durch Kommas getrennt eingeben, z. B. 1,5,10-12.

Relay Agent Remote ID
Sie können hier wählen, ob der Relay Agent, als Remote ID, seine IP-Adresse aus der Agent Konfiguration oder seine MAC-Adresse verwendet.

Additional Server Settings

- Check for Server Reachability
  Wenn Sie diese Option aktivieren, wird die Erreichbarkeit des DHCP-Servers alle 30s geprüft. Wenn ein Server nicht erreichbar ist, wird er beim Abarbeiten der Server-Liste nicht berücksichtigt.
- Enable Broadcast Forwarding
  Wenn Sie diese Option aktivieren, wird eine DHCP-Anfrage als Broadcast weitergeleitet, wenn es keinen passenden Eintrag in der DHCP-Server-Liste gibt.

Syntax Command Line Interface

Tabelle 5-79 DHCP Relay Agent Configuration - CLI\SWITCH\RELAGENT>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen Einstellungen des DHCP Relay Agent an.	-
server <Nummer> [IP] [VLANs]	Legt die IP-Adresse und die VLANs des DHCP Servers <Nummer> fest.	Nur Administrator. Default-Wert: 0.0.0.0
remoteid [IP|MAC]	Legt die Relay Agent Remote ID fest	Nur Administrator.
bcastfwd [E|D]	Aktiviert/deaktiviert die "Enable Broadcast Forwarding"-Funktion.	Nur Administrator.
reachchk [E|D]	Aktiviert/deaktiviert die "Check for Server Reachability"-Funktion.	Nur Administrator.

5.5.20.2 DHCP Relay Agent Port Configuration

DHCP Relay Agent Port Parameters

Diese Seite zeigt die aktuellen konfigurierten Port-spezifischen Parameter des DHCP Relay Agents.

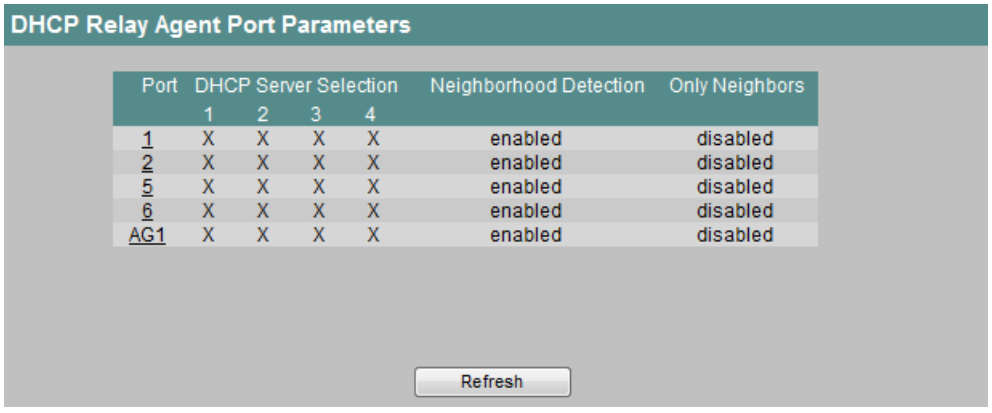


Bild 5-105 DHCP Relay Agent Port Parameters

Die drei Spalten der Porttabelle zeigen folgende Information:

Port
Angabe von Steckplatz und Port, auf den sich die Informationen beziehen. Im Falle von konfigurierten Link Aggregationen erscheint der Name der Link Aggregation.

DHCP Server Selection
Zeigt an, welche DHCP-Server für diesen Port zuständig sind.

Neighborhood Detection
Zeigt an, ob an diesem Port die Erkennung von Nachbarn eingeschaltet ist.

Only Neighbors
Zeigt an, ob der DHCP Relay Agent nur für direkte Nachbarn auf diesem Port funktionieren soll.

Konfiguration eines Ports für den DHCP Relay Agent

Wenn Sie nun in der ersten Spalte der Porttabelle eine Portbezeichnung anklicken, gelangen Sie zu der Seite "DHCP Relay Agent Port Configuration".

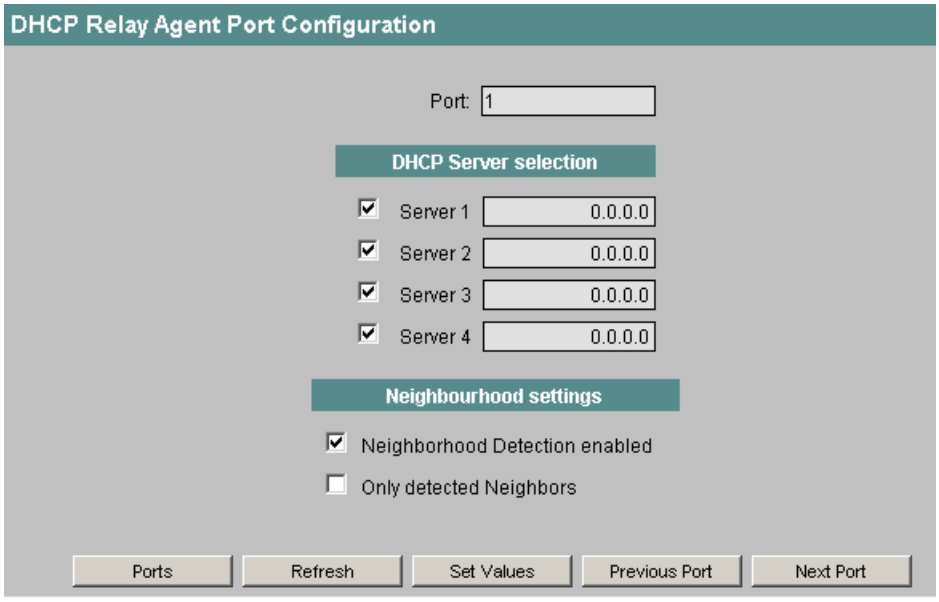


Bild 5-106 DHCP Relay Agent Configuration

Port
Angabe von Steckplatz und Port, auf den sich die Informationen beziehen. Im Falle von konfigurierten Link Aggregationen erscheint der Name der Link Aggregation.

DHCP Server Selection
Aktivieren Sie die DHCP-Server, die für den Port zuständig sein sollen.

Neighborhood Detection enabled
Aktivieren Sie diese Option, wenn versucht werden soll, DHCP requests vor dem Weiterleiten einem Nachbarn zuzuordnen.

Only detected Neighbors
Aktivieren Sie diese Option, wenn nur DHCP requests weitergeleitet werden sollen, die von erkannten Nachbarn stammen.

Syntax Command Line Interface

Tabelle 5-80 DHCP Relay Agent Port Parameters - CLI\SWITCH\RELAGENT\PORTS>

Befehl	Beschreibung	Kommentar
info	Zeigt alle Port Parameter des DHCP Relay Agent an	-
nbdetect [<E|D> [ports]]	Aktiviert/deaktiviert die "Neighborhood Detection enabled"-Funktion.	Nur Administrator.
onlynb [<E|D> [ports]]	Aktiviert/deaktiviert die "Only detected Neighbors"-Funktion.	Nur Administrator.
sel [<S1|S2|S3|S4|all> <E|D> [ports]]	S1, S2, S3, S4 Aktiviert/deaktiviert den DHCP-Server, der für den Port zuständig sein soll. all Aktiviert/deaktiviert die DHCP-Server S1 bis S4.	Nur Administrator.

5.5.21 Precision Time Protocol (PTP) entsprechend IEEE 1588

Einleitung

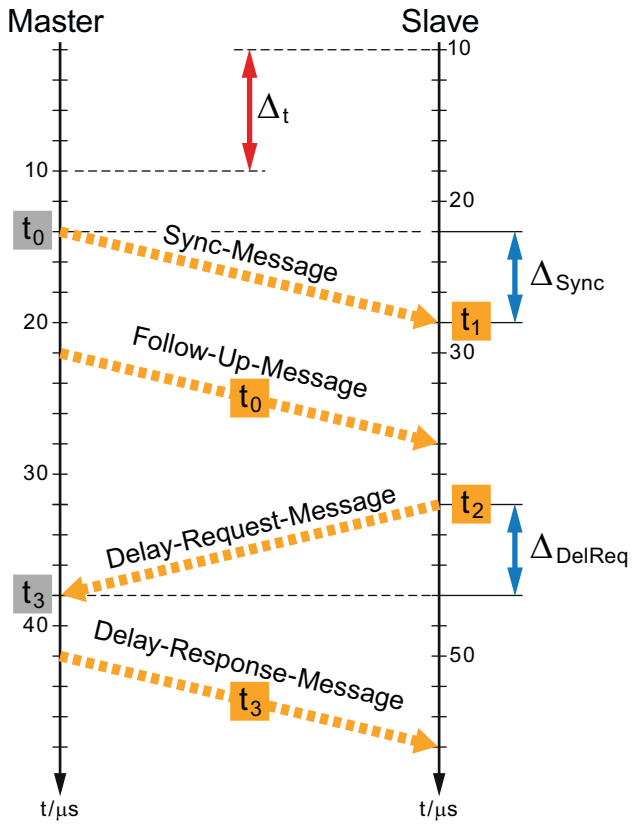
Das Precision Time Protocol (PTP) nach IEEE 1588v2 ermöglicht die Uhrzeitsynchronisation von Geräten, die an den Ports eines SCALANCE X300 angeschlossen sind. Diese Geräte leiten die Synchronisations-Frames nach dem Verfahren "Transparent Clock" (TC) durch das Netz. Es werden die Korrekturmechanismen "End-to-End" und "Peer-to-Peer" unterstützt.

Hinweis

PTP wird nur von folgenden Geräten der Produktlinie SCALANCE X300 unterstützt:

- Das Gerät X308-2M.
- Alle Geräte der Produktgruppe X300 EEC.
- Alle Geräte der Produktgruppe XR300.
- Alle Geräte der Produktgruppe XR300 EEC.

Delay-Request-Response-Mechanismus



Ein Gerät im Netzwerk übernimmt die Funktion des Uhrzeit-Masters (Best Master Clock, BMC), der die Referenz-Zeit für alle anderen Geräte vorgibt. Dazu versendet der Master zyklisch Synchronisations-Nachrichten (Sync-Message), im dargestellten Beispiel zum Zeitpunkt t_0. Der Zeitpunkt t_1 des Eintreffens dieser Nachricht wird vom Slave gespeichert. In einer zweiten Nachricht (Follow-Up-Message) liefert der Master den exakten Versendezeitpunkt t_0 der Sync-Message an den Slave.

Nur mit diesen beiden Werten kann aber weder die Abweichung der Slave-Uhr noch die Nachrichtenlaufzeit berechnet werden. Deshalb übermittelt der Slave anschließend eine sogenannte Delay-Request-Nachricht an den Master und speichert den Versendezeitpunkt t_2 dieser Nachricht. Der Master informiert den Slave mit einer Delay Response Message, zu welchem Zeitpunkt t_3 er diese Nachricht erhalten hat.

Für die folgenden Berechnungen wird angenommen, dass die Übertragung einer Nachricht vom Master zum Slave genau die gleiche Zeit in Anspruch nimmt wie die Übertragung einer Nachricht in umgekehrter Richtung. Diese Voraussetzung ist bei einer direkten Kabelverbindung erfüllt.

Die rechnerischen Werte für Δ_{Sync} und Δ_{DelReq} ergeben sich als Differenz von Empfangs- und Sendezeitpunkt:

$\Delta_{Sync} = t_1 - t_0$

$\Delta_{DelReq} = t_3 - t_2$

Wenn die Uhrzeit des Slaves um den Betrag Δ_t von der Uhrzeit des Masters abweicht, ergeben diese beiden Berechnungen jedoch noch nicht den tatsächlichen Wert für die

Nachrichtenlaufzeit Δ_D, weil den Sende- und Empfangszeiten unterschiedliche Bezugssysteme zugrunde liegen. Die Berechnung der tatsächlichen Nachrichtenlaufzeit Δ_D erfolgt am einfachsten, indem der Mittelwert gebildet wird:

$\Delta_D = (\Delta_{Sync} + \Delta_{DelReq}) / 2$

Die Abweichung der Slave-Uhr Δ_t ergibt sich, wenn Δ_{Sync} um die tatsächliche Nachrichtenlaufzeit Δ_D vermindert wird:

$\Delta_t = \Delta_{Sync} - \Delta_D$

Ist Δ_t positiv, geht die Uhr des Slaves "vor". Bei einem negativen Wert für Δ_t geht die Uhr des Slaves "nach".

Beispiel

Zum Zeitpunkt t_0 = 14 µs sendet der Master eine Sync-Message, die zum Zeitpunkt t_1 = 28 µs beim Slave eintrifft. Daraus wird der Wert für Δ_{Sync} berechnet:

$\Delta_{Sync} = t_1 - t_0 = 28\ \mu s - 14\ \mu s = 14\ \mu s$

Wenn die Uhren von Master und Slave exakt synchronisiert wären, würde die Nachrichtenlaufzeit 14 µs betragen, was jedoch aus dieser einzelnen Messung noch nicht geschlossen werden kann.

Deshalb sendet der Slave zum Zeitpunkt t_2 = 40 µs eine Delay-Request-Message, die zum Zeitpunkt t_3 = 38 µs beim Master eintrifft. Der Wert für Δ_{DelReq} ist die Differenz von Empfangs- und Sendezeitpunkt dieser Nachricht:

$\Delta_{DelReq} = t_3 - t_2 = 38\ \mu s - 40\ \mu s = -2\ \mu s$

Die tatsächliche Nachrichtenlaufzeit Δ_D ist der Mittelwert von Δ_{Sync} und Δ_{DelReq}, weil dadurch die Zeitabweichung der beiden Geräteuhren voneinander eliminiert wird:

$\Delta_D = (\Delta_{Sync} + \Delta_{DelReq}) / 2$

$\Delta_D = (14\ \mu s - 2\ \mu s) / 2 = 6\ \mu s$

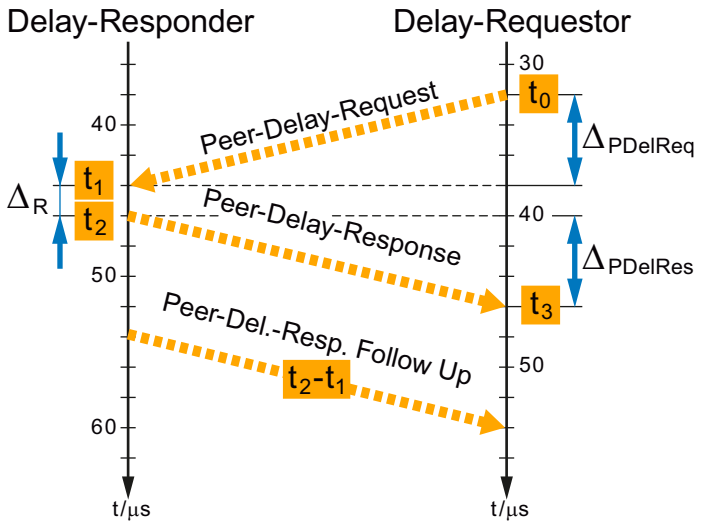
Die Abweichung der Slave-Uhr beträgt

$\Delta_t = \Delta_{Sync} - \Delta_D = 14\ \mu s - 6\ \mu s = 8\ \mu s$

Die Uhr des Slaves geht also "vor" und muss um 8 µs korrigiert werden.

Peer-Delay-Mechanismus

Der Peer-Delay-Mechanismus hat das Ziel, die Laufzeit einer Nachricht zwischen zwei Ports von PTP-fähigen Geräten zu ermitteln. Im Gegensatz zu einer Delay-Request-Response-Nachricht, die zwischen Slave und Master auch über mehrere Netzwerkknoten hinweg transportiert wird, werden Peer-Delay-Nachrichten nur mit den jeweiligen Nachbarknoten ausgetauscht, daher der Name "Peer-Delay".



Der Delay-Requestor übermittelt eine Peer-Delay-Request-Nachricht an einen Nachbarknoten, den Delay-Responder, und speichert den Versendezeitpunkt t_0 dieser Nachricht. Der Delay-Responder schickt umgehend eine Peer-Delay-Response-Nachricht zurück. In das Korrekturfeld der Peer-Delay-Response Follow-Up-Nachricht trägt er die Zeitdifferenz zwischen dem Versendezeitpunkt t_2 der Peer-Delay-Response-Nachricht und dem Empfang der Peer-Delay-Request-Nachricht t_1 ein:

$\Delta_R = t_2 - t_1$

Mit dem Empfangszeitpunkt t_3 der Peer-Delay-Respons-Nachricht hat der Delay-Requestor dann alle Daten, um die Nachrichtenlaufzeit zum Nachbarknoten zu berechnen:

$\Delta_{PDelReq} = \Delta_{PDelRes} = (t_3 - t_0 - \Delta_R) / 2$

Um die Abweichung einer Slave-Uhr zu berechnen, müssen auch beim Peer-Delay-Mechanismus Sync-Nachrichten und Follwow-Up-Nachrichten ausgewertet werden. Der Abschnitt "Peer-to-Peer- Transparent Clock" enthält eine Beschreibung des kompletten Synchronisations-Zyklus.

Synchronisation unabhängig von der Topologie des Netzwerks

Die in den vorangegangenen Abschnitten dargestellten Berechnungen gelten unter der Voraussetzung, dass der Nachrichtenaustausch über eine direkte Verbindungsleitung zwischen den beiden Kommunikationspartnern erfolgt. In der Regel bestehen Netzwerke aber aus mehreren Switches, die die Uhrzeit-Nachrichten zwischen Uhrzeit-Master und Slave transportieren müssen. Wie die Synchronisation über mehrere Switches hinweg erfolgt, hängt davon ab, welcher Geräte-Kategorie ein Switch zugeordnet wird (Boundary Clock oder Transparent Clock) und welche Methode zur Ermittlung der Nachrichtenlaufzeit eingesetzt wird (Delay-Request-Response-Mechanismus oder Peer-Delay-Mechanismus).

Für jedes Gerät muss konfiguriert werden, nach welchem Verfahren es PTP-Nachrichten behandeln soll. In einem Netzabschnitt können nicht beide Delay-Mechanismen gleichzeitig angewendet werden. Alle Geräte innerhalb eines Abschnitts müssen entweder für den Delay-Request-Response-Mechanismus oder den Peer-Delay-Mechanismus konfiguriert sein. Alle beteiligten Switches sollten PTP unterstützen, damit eine präzise Uhrzeitsynchronisation erreicht werden kann. Ein nicht PTP-fähiger Switch kann wegen Queuing keine konstanten Nachrichtenlaufzeiten zwischen Master und Slave sicherstellen.

Boundary Clock

Dieser Switch übernimmt an einem Port die Rolle des Slaves und synchronisiert sich mit einem Uhrzeit-Master. Gegenüber den anderen angeschlossenen Geräten übernimmt er die Funktion des Masters und versendet an diese Teilnehmer zyklisch Synchronisations-Nachrichten. Bei einem Netz mit mehreren Switches und Endgeräten sorgt der BMC-Algorithmus für die automatische Wahl der präzisesten Uhr im Netzwerk. Es entsteht eine Master-Slave-Hierarchie, bei der sich jeder Switch mit dem Nachbar-Switch in Richtung BMC synchronisiert.

Synchronisations-Mechanismen bei Boundary Clocks

Ist eine Boundary Clock für den Delay-Request-Response-Mechanismus konfiguriert, sendet sie Delay-Request-Nachrichten an den Uhrzeit-Master sowie Sync- und Follow-Up-Nachrichten an die Slaves.

Beim Peer-Delay-Mechanismus ermittelt die Boundary Clock für jeden Port die Nachrichtenlaufzeit zum Nachbargerät. Sie synchronisiert sich, indem sie die Sync- und Follow-Up-Nachrichten des Masters auswertet. Die Boundary Clock ermöglicht die Synchronisation der Slaves durch die Versendung von Sync- und Follow-Up-Nachrichten.

Transparent Clock

Eine Transparent Clock synchronisiert sich nicht mit einem Uhrzeit-Master, leitet aber PTP-Nachrichten zwischen Uhrzeit-Master und den zu synchronisierenden Slaves weiter. Im Vergleich zur Boundary Clock ermöglicht die Transparent Clock eine genauere Synchronisation, weil der Fehler bei der Synchronisation der Boundary Clock entfällt. Bei mehreren hintereinander liegenden Switches in einer Linien- oder Ring-Topologie ist es deshalb vorteilhaft, diese als Transparent Clock zu konfigurieren.

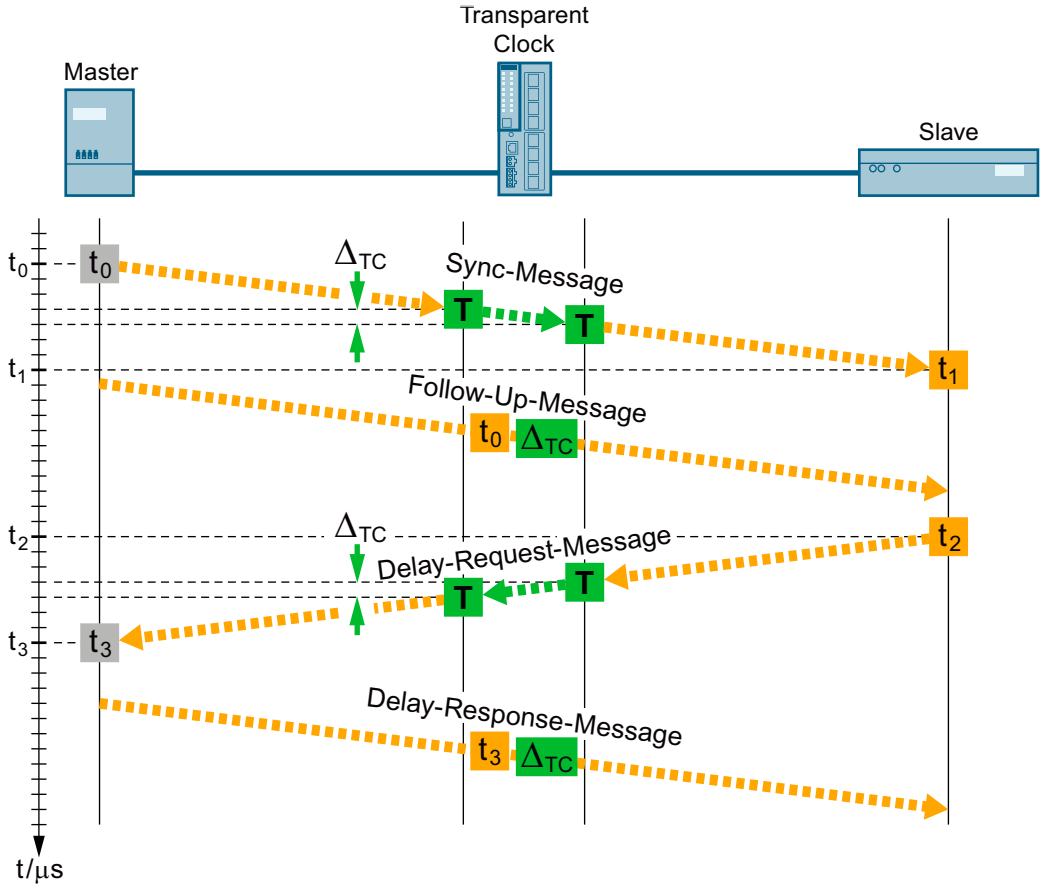
Auch bei Topologieänderungen im Netz sorgt die Transparent Clock für eine präzisere Synchronisation als die Boundary Clock. Unabhängig von ihrer Position innerhalb der Topologie, hat die Transparent Clock die Funktion Synchronisations-Frames weiterzuleiten. Bei einer Boundary Clock ändern sich die Zuordnungen von Master und Slave zu den einzelnen Ports und somit die gesamte Synchronisations-Hierarchie. Es kann mehrere Sekunden dauern bis sich dann alle Geräte wieder auf den Uhrzeit-Master synchronisiert haben.

Synchronisations-Mechanismen bei Transparent Clocks

Bei der Ermittlung der tatsächlichen Nachrichtenlaufzeiten über mehrere Netzknoten hinweg müssen auch die Zeiten berücksichtigt werden, die für die Verarbeitung einer Nachricht in einer Transparent Clock notwendig sind. Eine Transparent Clock muss also die Zeitdauer vom Empfang einer Nachricht am Eingangsport bis zur Versendung am Ausgangsport ermitteln und diesen Wert an den Slave weiterleiten. Zu diesem Zweck gibt es in PTP-Nachrichten ein Korrekturfeld, in dem die Switches entsprechende Eintragungen machen. Der Slave berücksichtigt diese Information bei der Berechnung der Nachrichtenlaufzeit.

Wie eine Transparent Clock diese Korrekturinformationen handhabt, hängt davon ab, welcher Delay-Mechanismus konfiguriert wurde. Beim Delay-Request-Response-Mechanismus spricht man von einer End-to-End Transparent Clock, beim Peer-Delay-Mechanismus von einer Peer-to-Peer Transparent Clock.

End-to-End Transparent Clock

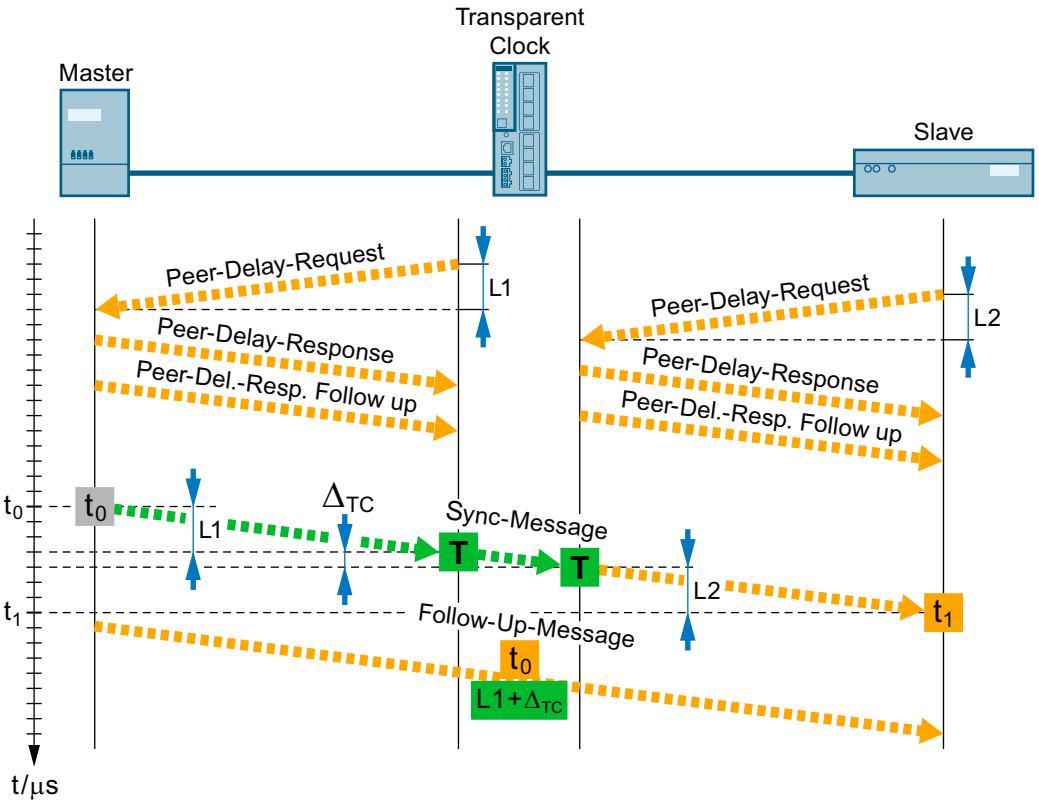


Im dargestellten Beispiel versendet der Uhrzeit-Master eine Synchronisations-Nachricht. Die Zeitdauer Δ_{TC} vom Empfang dieser Nachricht am Eingangsport bis zur Versendung am Ausgangsport trägt die Transparent Clock in das Korrekturfeld der Follow-Up-Nachricht ein. Den Versendezeitpunkt t_0 erhält der Slave ebenfalls mit der Follow-Up-Nachricht und kann damit, wie bereits beschrieben, die notwendigen Berechnungen durchführen.

Wenn eine Nachricht auf dem Weg zum Slave noch von weiteren Transparent Clocks weitergeleitet wird, addiert jedes Gerät seine Zeitdauer Δ_{TC} zum Inhalt des Korrekturfeldes der Follow-Up-Nachricht. Wenn die Synchronisations-Nachricht beim Slave eintrifft, enthält das Korrekturfeld die Summe aller Zeiten, die für die Verarbeitung der Nachrichten in den Transparent Clocks notwendig war. Ebenso geht das Gerät auch mit Delay-Request-Messages um.

Der Slave korrigiert die Nachrichtenlaufzeit um den Wert Δ_{TC} bzw. bei mehreren Transparent Clocks um die Summe aller Werte Δ_{TC} und kann seine Uhrzeit wie im Abschnitt Delay-Request-Response-Mechanismus beschrieben synchronisieren.

Peer-to-Peer Transparent Clock



Jedes Gerät ermittelt mit dem Peer-Delay-Mechanismus für seine Ports die Laufzeit einer Nachricht bis zum Nachbargerät. So erhält die Transparent Clock die Nachrichtenlaufzeit L1 zum Master, der Slave erhält den Wert L2 für die Nachrichtenlaufzeit zur Transparent Clock.

Die Verarbeitung der Synchronisations-Nachricht durch die Transparent Clock nimmt die Zeitdauer Δ_{TC} in Anspruch. Die Transparent Clock trägt die Summe von L1 und Δ_{TC} in das Korrekturfeld der Follow-Up-Nachricht ein. Der Slave addiert dann den Inhalt des Korrekturfeldes mit der Nachrichtenlaufzeit L2 für den Eingangsport, über den die Synchronisations-Nachricht empfangen wurde. So erhält er die Laufzeit einer Nachricht zwischen Master und Slave.

Wird eine Nachricht auf dem Weg zum Slave von mehreren Transparent Clocks weitergeleitet, verändert jede Transparent Clock den Inhalt des Korrekturfeldes der Follow-Up-Nachricht: Die Nachrichtenlaufzeit zum Nachbarn, über den die Synchronisations-Nachricht empfangen

wurde, sowie die Zeit Δ_{TC} für die Verarbeitung der Nachricht werden zum Inhalt des Korrekturfeldes addiert.

Ein besonderer Vorteil der Peer-to-Peer Transparent Clock besteht darin, dass auch für geblockte Ports die Nachrichtenlaufzeiten zum Nachbargerät berechnet werden. Bei einer Umkonfiguration des Netzwerks stehen dem Slave sehr schnell wieder korrekte Laufzeitinformationen zur Verfügung.

5.5.22 Konfiguration des Precision Time Protocols mit dem WBM

IEEE 1588 bei SCALANCE-Geräten

Hinweis

Der Menüpunkt IEEE 1588 ist bei den folgenden Geräten ab Firmwarestand 3.5.0 verfügbar:

- SCALANCE X308-2M
- SCALANCE X308-2M PoE
- SCALANCE X302-7EEC
- SCALANCE X307-2EEC
- SCALANCE XR324-12M
- SCALANCE XR324-4M PoE
- SCALANCE XR324-4M EEC

Die Synchronisations-Frames werden nach dem Verfahren "Transparent Clock" durch das Netz geleitet, wobei die Korrekturmechanismen "End-to-End" und "Peer-to-Peer" unterstützt werden.

Die SCALANCE-Geräte arbeiten als Two-Step-Clock. Sie unterstützen die Verwendung sowohl von One-Step Clocks als auch von Two-Step Clocks im Netz.

Die Norm IEEE 1588v2 definiert Mechanismen, mit denen eine hochpräzise Synchronisation der Uhrzeit von Geräten in einem Netzwerk erreicht wird. Die aufgeführten SCALANCE-Geräte unterstützen die Zeitsynchronisation nach IEEE 1588v2 auch durch eine entsprechende Hardware-Ausstattung. Die IEEE1588v2-Funktionalität ist bei diesen Geräten im Auslieferungszustand und nach einem "Reset to factory default" abgeschaltet. Um IEEE 1588v2 nutzen zu können, müssen Sie diese Funktion aktivieren und jeden Port, der im Synchronisationspfad liegt, sowie Ports, die durch Redundanzmechanismen geblockt sind, konfigurieren. IEEE 1588v2 ist auch nutzbar bei Redundanzmechanismen im Ring wie HRP, Standby-Kopplung von Ringen, MRP und RSTP. Die folgenden Abschnitte beschreiben die Konfigurationsmöglichkeiten des Web Based Managements.

1588 Configuration

Auf dieser Seite legen Sie fest, wie das Gerät PTP-Nachrichten verarbeiten soll.

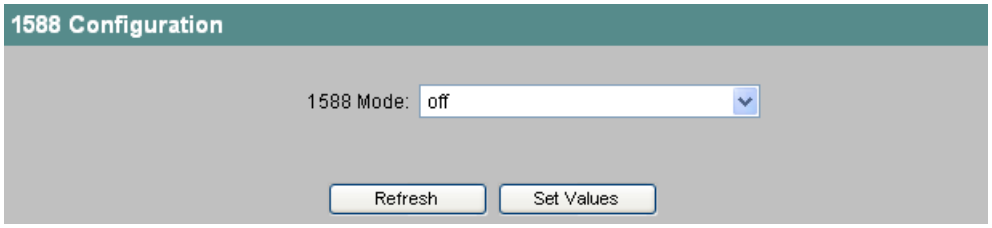


Bild 5-107 1588 Configuration

1588 Mode
Es gibt die folgenden Einstellmöglichkeiten:

- **off**
  Das Gerät verarbeitet keine PTP-Nachrichten. PTP-Nachrichten werden aber nach den Regeln des Switchs weitergeleitet.
- **Transparent Clock**
  Das Gerät übernimmt die Funktion einer Transparent Clock und leitet PTP-Nachrichten an andere Teilnehmer weiter, wobei es Eintragungen in das Korrekturfeld der PTP-Nachricht vornimmt.

1588 Transparent Clock Configuration

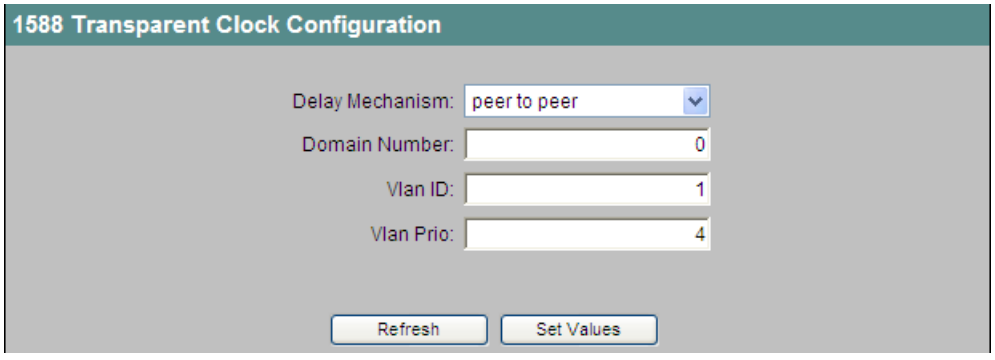


Bild 5-108 1588 Transparent Clock

Delay Mechanism
Legen Sie fest, mit welchem Delay-Mechanismus das Gerät arbeiten soll:

- End to End (Delay-Request-Response-Mechanismus wird verwendet)
- Peer to Peer (Peer-Delay-Mechanismus wird verwendet)

Domain Number
Tragen Sie hier die Domain-Nummer für das Gerät ein. Das Gerät ignoriert PTP-Nachrichten mit einer abweichenden Domain-Nummer. Ein SCALANCE-Gerät kann nur einer Synchronisations-Domäne zugeordnet sein.

Vlan ID
Tragen Sie hier die Vlan ID des Geräts mit der Funktion "Transparent Clock" ein.

Vlan Prio
Tragen Sie hier die Priorität des Vlans ein.

1588 Transparent Clock Port Parameters

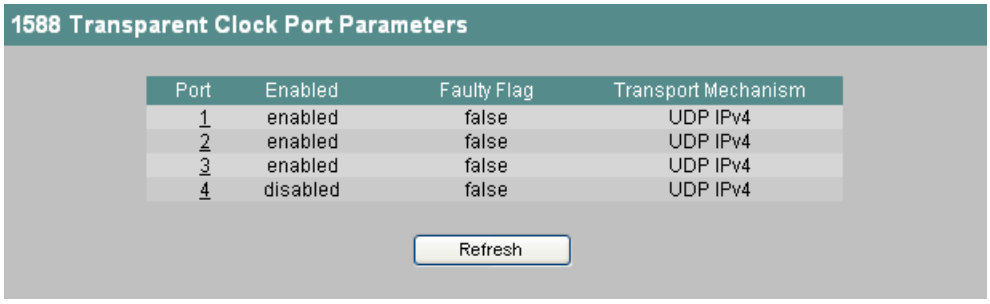


Bild 5-109 1588 Transparent Clock Port Parameters

Die Tabelle zeigt Detailinformationen zu den einzelnen Ports:

Port
Die Portnummer. Bei modularen Geräten werden Steckplatznummer und Portnummer durch einen Punkt getrennt angezeigt. Wenn Sie eine Portnummer anklicken, wird die zugehörige Seite "1588 Transparent Clock Port Configuration" angezeigt.

Enabled
Der Port-Status. Folgende Angaben sind möglich:

- **disabled**
  Der Port beteiligt sich nicht am PTP.
- **enabled**
  Der Port verarbeitet PTP-Nachrichten.

Faulty Flag
Der Fehlerstatus im Bezug auf PTP.

- **true**
  Es ist ein Fehler aufgetreten.
- **false**
  An diesem Port sind keine Fehler aufgetreten.

Transport Mechanism
Entweder "Ethernet" oder "UDP IPv4".

1588 Transparent Clock Port Configuration

Sie gelangen zu dieser Seite, wenn Sie eine Portnummer in der Tabelle auf der Seite "Transparent Clock Port Parameters" anklicken.

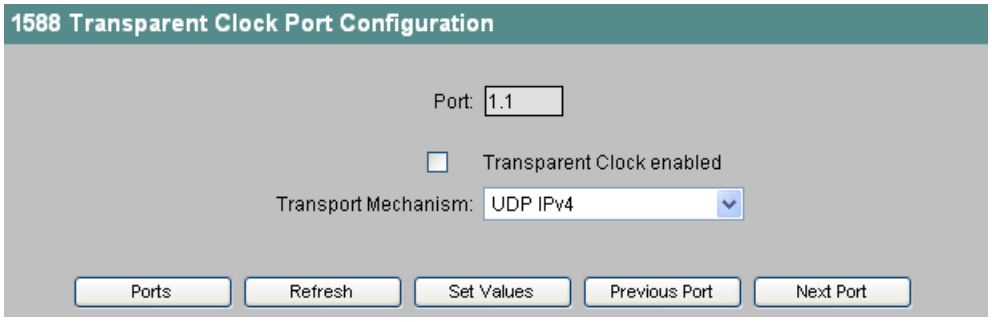


Bild 5-110 1588 Transparent Clock Port Configuration

Port
Die Portnummer. Bei modularen Geräten werden Steckplatznummer und Portnummer durch einen Punkt getrennt angezeigt.

Transparent Clock enabled
Markieren Sie diese Optionskästchen, wenn das Gerät PTP-Nachrichten über diesen Port verarbeiten soll.

Transport Mechanism
Wählen Sie aus, wie dieser Port den Datenverkehr von PTP-Nachrichten abwickeln soll. Sie können für die Ports eines Geräts unterschiedliche Einstellungen vornehmen, allerdings muss der entsprechende Kommunikationspartner den gewählten Transportmechanismus unterstützen. Es gibt folgende Einstellmöglichkeiten:

- Ethernet
- UDP IPv4

Ports
Durch Anklicken dieser Schaltflächen wechseln Sie zur Seite "Transparent Clock Port Parameters".

Previous Port und Next Port
Durch Anklicken dieser Schaltflächen wechseln Sie direkt zur Konfigurationsseite des vorhergehenden bzw. des nächsten Ports, ohne erst die Seite "Transparent Clock Port Parameters aufrufen zu müssen.

5.5.23 Konfiguration des Precision Time Protocols mit dem CLI

CLI\SWITCH\1588>

Befehl	Beschreibung		Kommentar
mode [off|TC]	Aktiviert/Deaktiviert das Precision Time Protocol für das Gerät und legt fest, wie sich das Gerät im Bezug auf das PTP verhalten soll:		Nur Administrator.
	off	Das Gerät verarbeitet keine PTP-Nachrichten.	
	TC	Transparent Clock	
TC	Öffnet das Menü zum Konfigurieren eines Geräts als Transparent Clock.		Nur Administrator.

CLI\SWITCH\1588\TC>

Befehl	Beschreibung		Kommentar
delaymec [E2E|P2P]	Legt den Delay-Mechanismus für das Gerät fest:		Nur Administrator.
	E2E	End-to-End (Delay-Request-Response-Mechanismus wird verwendet).	
	P2P	Peer-to-Peer (Peer-Delay-Mechanismus wird verwendet).	
domainnb [number]	Legt die Identifikations-Nummer für die Uhrzeitdomäne fest. Die Synchronisation erfolgt nur für die Geräte innerhalb der Domäne, PTP-Nachrichten mit einer abweichenden Domain-Nummer werden verworfen.		Nur Administrator.
vlanid [VID]	Legt die Vlan ID fest.		Nur Administrator.
vlanprio [<0..7>]	Legt die Vlan Priorität fest.		Nur Administrator.
PORTS	Öffnet das Menü PORTS.		Nur Administrator.

CLI\SWITCH\1588\TC\PORTS>

Befehl	Beschreibung		Kommentar
tcport <E|D> [ports]	Aktiviert/Deaktiviert die angegebenen Ports. Ein Bereich von Ports wird mit Bindestrich angegeben. Mehreren Ports werden durch Leerzeichen oder Komma getrennt.		Nur Administrator.
transmec <IPv4|ETH> [ports]	Legt das Protokoll für die Übertragung der PTP-Nachrichten fest. Dieses Protokoll muss vom jeweiligen Kommunikationspartner des Ports unterstützt werden.		Nur Administrator.
	IPv4	Internet Protocol (Layer 3)	
	ETH	Ethernet (Layer 2)	

5.5.24 Port Diagnostics

5.5.24.1 Cable Tester (SCALANCE X-300/X408-2)

Switch Cable Tester

Mit dieser Maske kann jeder einzelne Ethernet-Port eine unabhängige Fehlerdiagnose am Kabel durchführen. Hierbei können Kurzschlüsse sowie Leitungsunterbrechungen lokalisiert werden.

Hinweis

Dieser Test ist nur zulässig, wenn auf dem zu testenden Port keine Datenverbindung aufgebaut ist.

Vor dem Starten der Funktion "Cable Tester" müssen Sie zusätzlich die Funktion "Link Check" auf allen Ringports des Geräts deaktivieren.

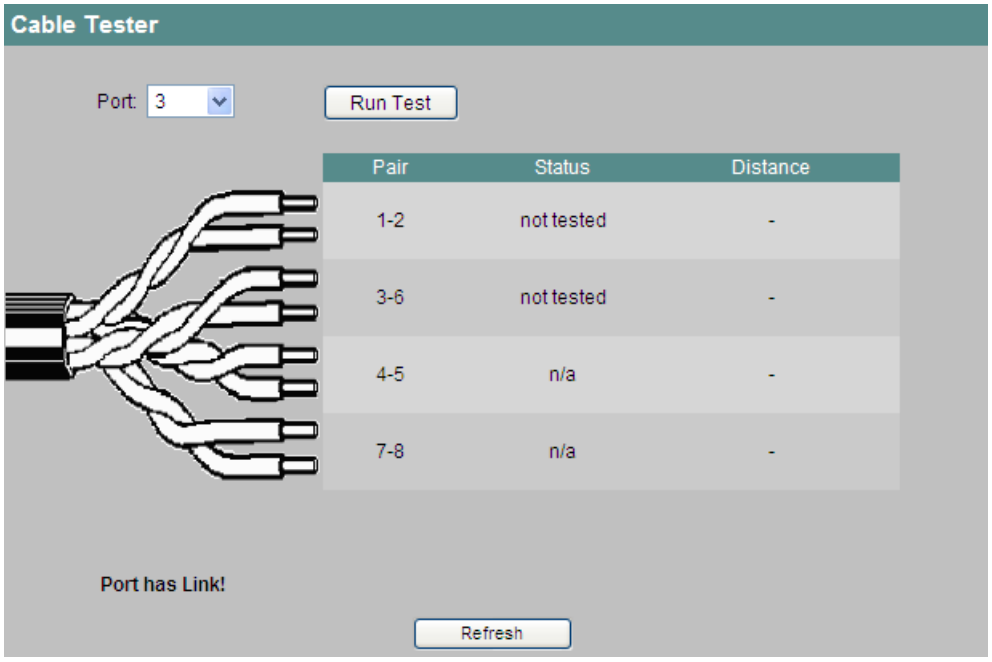


Bild 5-111 Cable Tester

Port

Hier wird der zu testende Port angegeben.

Run Test

Mit dieser Schaltfläche aktivieren Sie den Test.

Pair

Zeigt das Adernpaar im Kabel an.
Die Paare 4-5 und 7-8 werden bei Fast Ethernet nicht verwendet.

Status

Zeigt den Status der Leitung an.

Distance

Zeigt die Entfernung zum Kabelende, Kabelbruch oder zum Kurzschluss an.

Syntax Command Line Interface

Tabelle 5-81 Cable Tester - CLI\SWITCH\PORTDIAG\CABLETESTER>

Befehl	Beschreibung	Kommentar
runtest [Ports]	Testet die angegebenen Ports. Wird kein Port angegeben, werden alle getestet.	Nur Administrator.

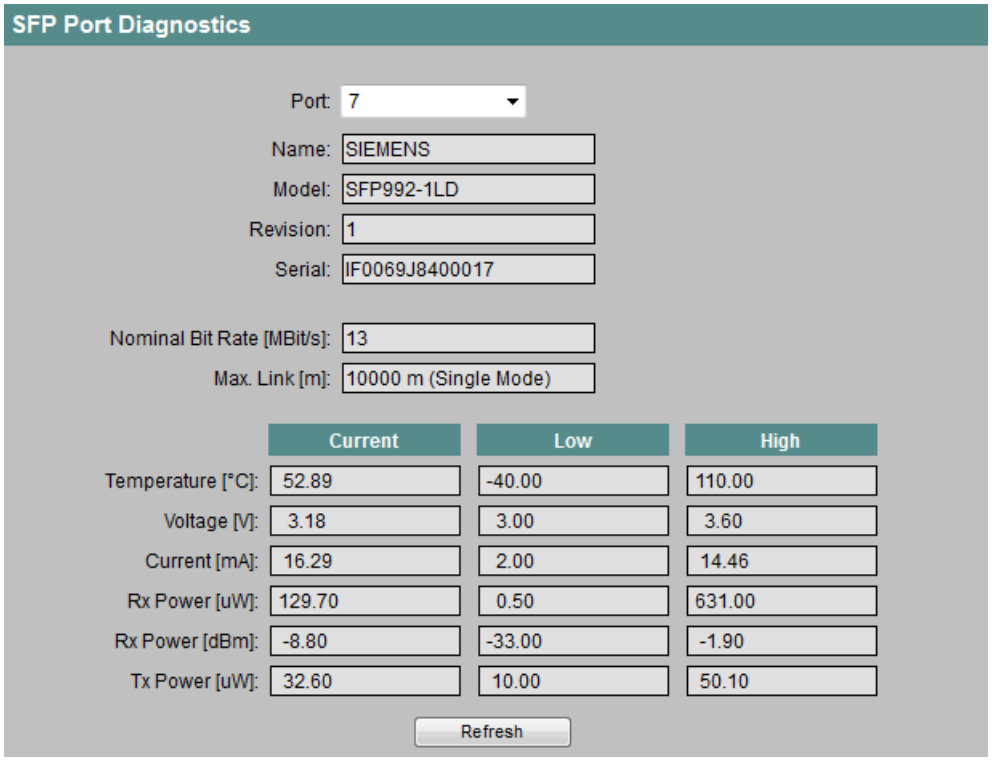
5.5.24.2 SFP Diagnostics

Voraussetzung

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.

Sie können SFP Diagnostics nur bei Stecktransreceivern SFP verwenden.

SFP Port Diagnostics



Port
Hier wird der zu testende SFP-Port angegeben.

Entsprechend der Auswahl wird Folgendes angezeigt:

- Name (nur lesbar)
  Der Name des SFP-Ports
- Model (nur lesbar)
  Der eingesetzte Stecktransreceivers SFP
- Revision (nur lesbar)
  Der Hardware Ausgabestand des Stecktransreceivern SFP
- Serial (nur lesbar)
  Die Seriennummer des Stecktransreceivers SFP
- Nominal Bit Rate (nur lesbar)
  Die Nenn-Bitrate des SFP-Ports
- Max. Link (nur lesbar)
  Die maximale Distanz in Metern, die mit diesem Medium möglich ist.

Die Tabelle ist so aufgebaut, dass zu den folgenden Parametern immer der aktuellste (Current), der niedrigste (Low) und der höchste (High) Wert angezeigt wird.

Temperature (nur lesbar)

Die Temperatur des Ports.

Voltage (nur lesbar)

Die Spannung, die am Port anliegt.

Current (nur lesbar)

Der Strom, mit dem ein Gerät an diesem Port versorgt wird.

Rx Power (nur lesbar)

Die Empfangsleistung des Ports.

Tx Power (nur lesbar)

Die Sendeleistung des Ports.

Syntax Command Line Interface

Tabelle 5-82 SFPDIAGNOSTIC - CLI\SWITCH\PORTDIAG\SFPDIAG>

Befehl	Beschreibung	Kommentar
details [Port]	Testet den angegebenen SFP-Port.	Nur Administrator.

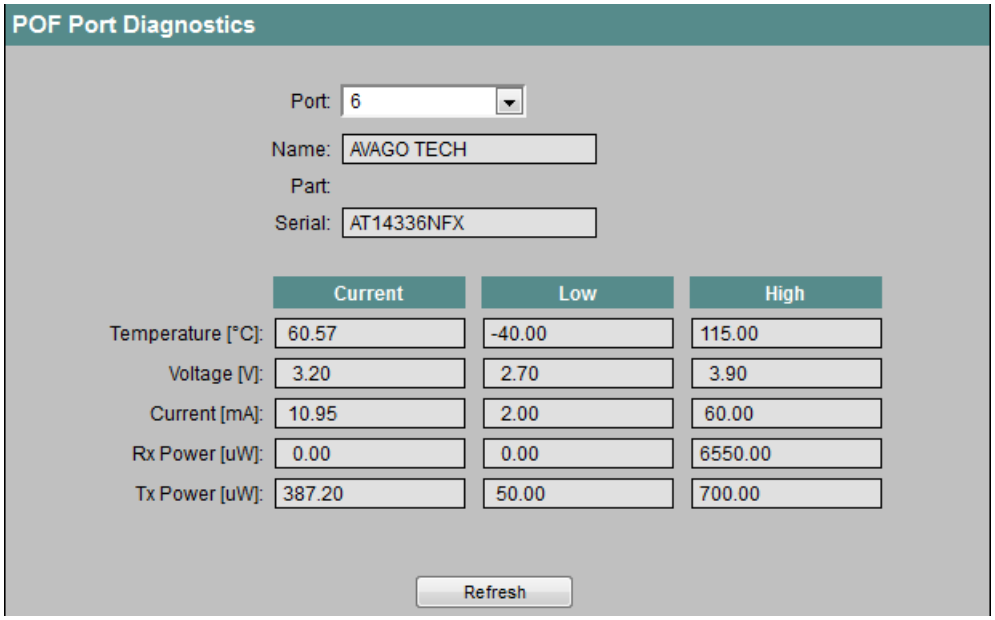
5.5.24.3 POF Diagnostics

Voraussetzung

Mit dieser Seite führen Sie für jeden einzelnen POF-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.

Sie können POF Diagnostics nur bei diagnosefähigen Transceivern verwenden. Geräte und Module mit diagnosefähigen Transceivern sind mit dem Zusatz "P" gekennzeichnet.

POF Port Diagnostics



Port
Hier wird der zu testende POF-Port angegeben.

Entsprechend der Auswahl wird Folgendes angezeigt:

- Name (nur lesbar)
  Der Name des POF-Ports
- Model (nur lesbar)
  Das eingesetzte POF-Modul
- Serial (nur lesbar)
  Die Seriennummer des POF-Moduls

Die Tabelle ist so aufgebaut, dass zu den folgenden Parametern immer der aktuellste (Current), der niedrigste (Low) und der höchste (High) Wert angezeigt wird.

Temperature (nur lesbar)

Die Temperatur des Ports.

Voltage (nur lesbar)

Die Spannung, die am Port anliegt.

Current (nur lesbar)

Der Strom, mit dem ein Gerät an diesem Port versorgt wird.

Rx Power (nur lesbar)

Die Empfangsleistung des Ports.

Tx Power (nur lesbar)

Die Sendeleistung des Ports.

Syntax Command Line Interface

Tabelle 5-83 SFPDIAGNOSTIC - CLI\SWITCH\PORTDIAG\POFDIAG>

Befehl	Beschreibung	Kommentar
details [Port]	Testet den angegebenen POF-Port.	Nur Administrator.

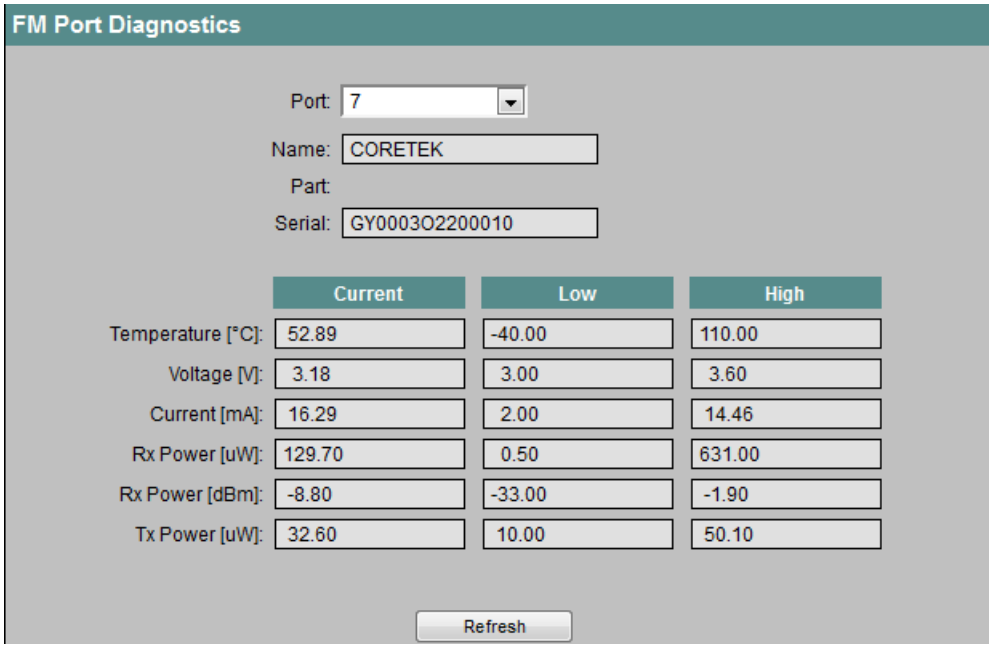
5.5.24.4 FM Diagnostics

Voraussetzung

Mit dieser Seite führen Sie für jeden einzelnen 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.

Sie können FMP Diagnostics nur bei diagnosefähigen Transceivern verwenden. Geräte und Module mit diagnosefähigen Transceivern sind mit dem Zusatz "FM" gekennzeichnet.

FM Port Diagnostics



Port
Hier wird der zu testende Port angegeben.

Entsprechend der Auswahl wird Folgendes angezeigt:

- Name (nur lesbar)
  Der Name des Ports
- Model (nur lesbar)
  Der eingesetzte FM-Transceiver
- Serial (nur lesbar)
  Die Seriennummer des FM-Transceivers

Die Tabelle ist so aufgebaut, dass zu den folgenden Parametern immer der aktuellste (Current), der niedrigste (Low) und der höchste (High) Wert angezeigt wird.

Temperature (nur lesbar)

Die Temperatur des Ports.

Voltage (nur lesbar)

Die Spannung, die am Port anliegt.

Current (nur lesbar)

Der Strom, mit dem ein Gerät an diesem Port versorgt wird.

Rx Power (nur lesbar)

Die Empfangsleistung des Ports.

Tx Power (nur lesbar)

Die Sendeleistung des Ports.

Syntax Command Line Interface

Tabelle 5-84 SFPDIAGNOSTIC - CLI\SWITCH\PORTDIAG\FMDIAG>

Befehl	Beschreibung	Kommentar
details [Port]	Testet den angegebenen Port.	Nur Administrator.

5.5.24.5 POF-Ports

Voraussetzung

Die Seite zur Diagnose der Lichtwellenleiter zeigt nur dann korrekte Dämpfungsbudgets an, wenn Plastic Optical Fiber (POF) verwendet wird. Bei Verwendung von Polymer Cladded Fiber (PCF) ist keine Diagnose möglich.

Sie können POF Diagnositics nur bei diagnosefähigen Transceivern verwenden. Geräte und Module mit diagnosefähigen Transceivern sind mit dem Zusatz "P" gekennzeichnet.

Plastic Optical Fiber Management

Auf dieser Seite finden Sie Diagnosedaten für Schnittstellen mit Plastik-Lichtwellenleiter.

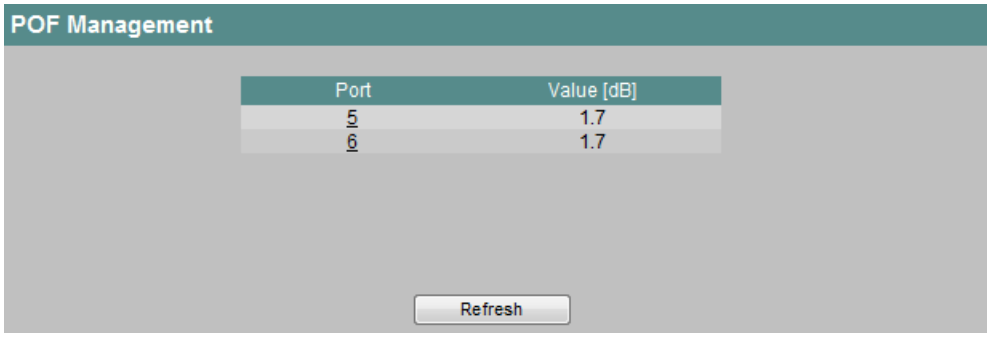


Bild 5-112 POF Management

Hier ist für jeden POF-Port das aktuell verfügbare Dämpfungsbudget als Zahlenwert dargestellt.

Das Dämpfungsbudget ist eine Maß dafür, welche Dämpfung auf der Verbindung zwischen Sender und Empfänger noch überbrückt werden kann. Je höher das Budget ist, desto größer ist die überbrückbare Dämpfung der Strecke. Sinkt das Dämpfungsbudget, so hat sich die Dämpfung der Übertragungsstrecke erhöht, was zum Beispiel durch Alterung oder einen Defekt verursacht werden kann. Je länger das verwendete Kabel ist, desto geringer ist das zur Verfügung stehende Dämpfungsbudget.

Die nachfolgend abgebildete Diagnose-Seite erscheint, wenn Sie einen der angezeigten Ports anklicken. Sie zeigt Informationen über den zeitlichen Verlauf des verfügbaren Dämpfungsbudgets.

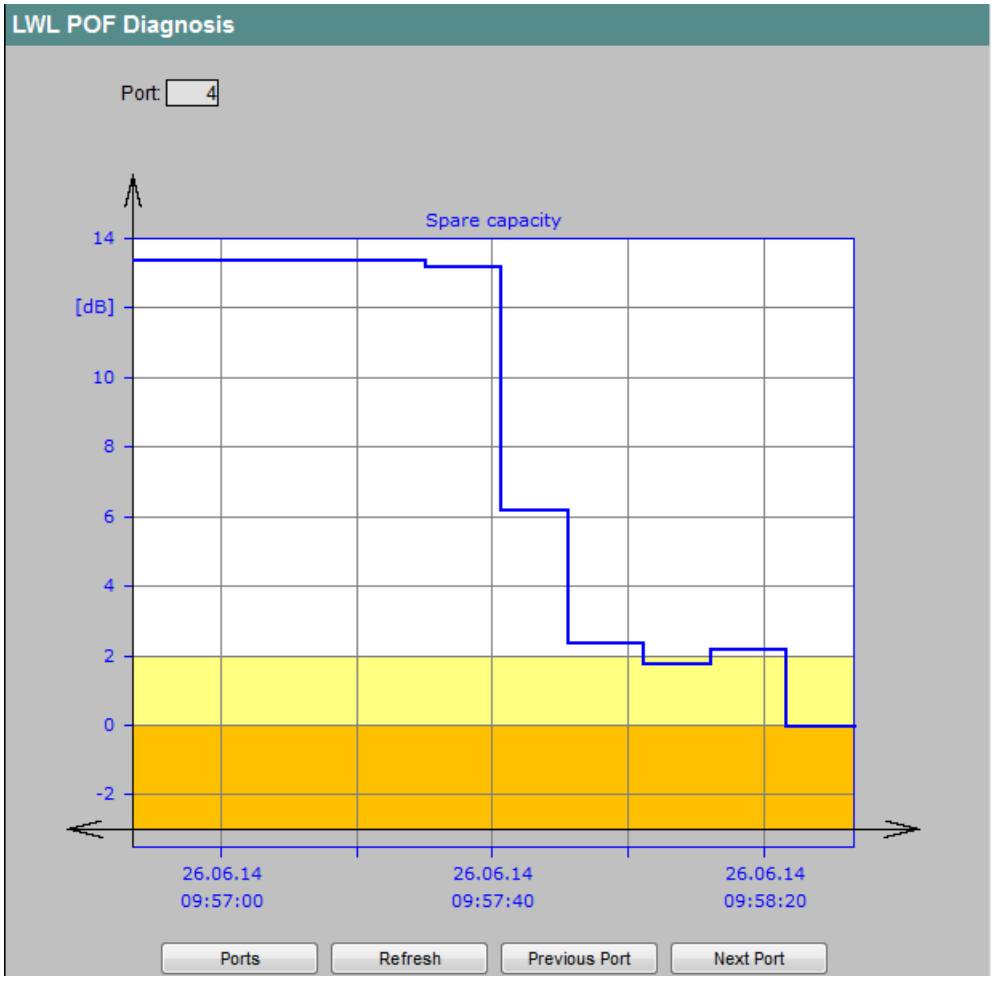


Bild 5-113 LWL POF Diagnose

Die vertikale Achse zeigt das verfügbare Dämpfungsbudget in dB. Nur im Bereich von 0 dB bis 6 dB haben die Messwerte die erforderliche Genauigkeit, um das vorhandene Dämpfungsbudget korrekt anzuzeigen.

Die horizontale Achse zeigt die Zeit ab dem Hochlauf des IE-Switch, bezogen auf die aktuelle Uhrzeit und das aktuelle Datum. Datums- und Uhrzeitinformationen werden von dem PC übernommen, auf dem der verwendete Web-Browser läuft.

Das Diagramm ist in folgende Bereiche unterteilt:

- **Weiß**
  Es ist ausreichend Dämpfungsbudget für einen fehlerfreien Betrieb vorhanden. Bei der Installation und Montage eines IE-Switch X-200 sollte das Budget in diesem Bereich liegen.
- **Gelb**
  Der Eintritt des Dämpfungsbudgets in den gelben Bereich zeigt Wartungsbedarf an. Die Grenze zum gelben Bereich liegt bei einem Budget von 2 dB. Um eine langfristige Funktion der Anlage sicherzustellen, sollte die Wartung durchgeführt werden. Befindet sich das Dämpfungsbudget im gelben Bereich, wird ein Event ausgelöst.
- **Orange**
  Der Eintritt des Dämpfungsbudgets in den orangenen Bereich zeigt dringenden Wartungsbedarf an. Die Grenze zum orangenen Bereich liegt bei einem Budget von 0 dB. Befindet sich das Dämpfungsbudget im orangenen Bereich, wird ein Event ausgelöst und die LWL-LED des betroffenen Ports leuchtet gelb.

5.5.25 Loop Detection

Funktionsweise

Wenn für einen Port die Funktion "Loop Detection" (Schleifenerkennung) eingestellt ist, sendet der Port spezielle Test-Frames, die Loop-Detection-Frames. Wenn diese Frames wieder zum Gerät zurückgesendet werden, dann liegt eine Schleife ("Loop") vor.

Wenn das Gerät die gesendeten Frames an einem anderen Port wieder empfängt, ist ein "Local Loop" aufgetreten. Das Gerät ist selbst ein Teil der Schleife.

Wenn das Gerät die gesendeten Frames am gleichen Port wieder empfängt, ist bei anderen Netzkomponenten eine Schleife aufgetreten, ein "Remote Loop".

Schleifen im Netzwerk

Eine Schleife kann z. B. durch eine Fehlkonfiguration oder durch falsches Stecken eines Kabels verursacht werden. Außerdem kann eine mechanische Beschädigung an Kabeln zu Kurzschlüssen führen und damit ebenfalls Schleifen verursachen.

Eine Schleife ist ein Fehler im Netzaufbau, der beseitigt werden muss. Die Schleifenerkennung kann helfen den Fehler zu finden, behebt ihn jedoch nicht. Die Schleifenerkennung ist nicht dazu geeignet, die Netzwerkverfügbarkeit durch den gezielten Einbau von Schleifen zu erhöhen.

Aktivierung der Funktion

Hinweis

Die Schleifenerkennung ist nur auf Ports möglich, die nicht als Ring-Port oder Standby-Port konfiguriert sind.

Funktion für das Gerät aktivieren

Um die Funktion "Loop Detection" generell für das Gerät zu aktivieren, aktivieren Sie die Option "Loop Detection Enabled" auf der Seite "Loop Detection Config". Auf dieser Seite können Sie Grundeinstellungen vornehmen, die für alle Ports gelten, siehe Abschnitt "Loop Detection Configuration".

Mit dieser Einstellung ist die Funktion nicht für alle Ports aktiviert. Sie müssen die Ports einzeln konfigurieren.

Ports aktivieren

Für die einzelnen Ports können Sie die Funktion "Loop Detection" auf der Seite "Loop Detection Port Configuration" einstellen, siehe Abschnitt "Loop Detection Port Configuration".

Nur wenn ein Port als "Sender" konfiguriert ist, kann der Port im Fehlerfall geblockt werden und somit eine Schleife verhindern.

Anwendungsbeispiel

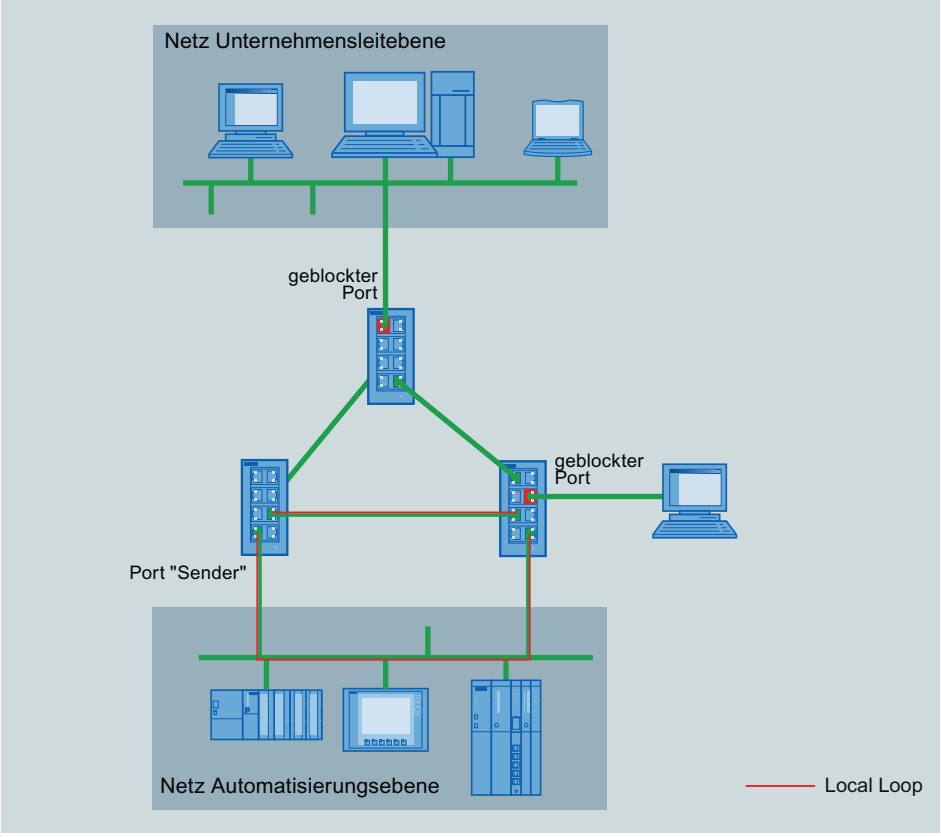


Bild 5-114 Schleifenerkennung mit projektiertem Sender

Die Abbildung oben zeigt die Vernetzung von Unternehmensleitebene und Automatisierungsebene über einen MRP/HRP-Ring. Die rot markierten, geblockten Ports wurden auf "Disable port" gesetzt.

Wenn eine Schleife im Netz auf Automatisierungsebene auftritt, wird die Schleife als "Remote Loop" erkannt. Durch die geblockten Ports werden keine Loop-Detection-Frames an das Netz auf Unternehmensleitebene oder an das Endgerät weitergeleitet.

Wenn ein "Local Loop" eintritt, wird der Port nach einer festgelegten Anzahl von Loop-Detection-Frames automatisch geblockt.

Die Einstellungen für die Schleifenerkennung werden in den folgenden Abschnitten anhand der WBM-Seiten erläutert.

Loop Detection Configuration

Nehmen Sie auf dieser Seite die Einstellungen zur Schleifenerkennung vor, die grundsätzlich für alle Ports gelten.

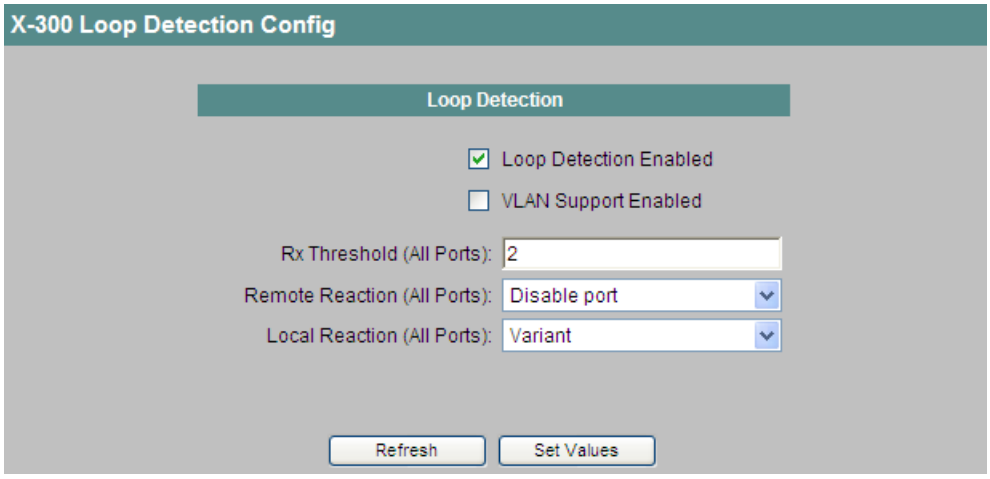


Bild 5-115 Konfiguration für Loop Detection

Hinweis

Schleifen können nur zwischen Geräten erkannt werden, die Loop-Detection-Frames weiterleiten. Schleifen über Netzkomponenten, deren Ports geblockt wurden, werden nicht erkannt.

Loop Detection Enabled

Schalten Sie die Schleifenerkennung durch Klicken auf das Optionskästchen ein bzw. aus.
Bei abgeschalteter Schleifenerkennung werden die Loop-Detection-Frames anderer Geräte weitergeleitet.

VLAN Support Enabled

Legen Sie durch Klicken auf das Optionskästchen für alle Ports fest, ob Loop-Detection-Frames für alle auf den jeweiligen Ports konfigurierten VLANs ausgesendet werden.
Bei ausgeschaltetem VLAN Support werden nur Loop-Detection-Frames ohne VLAN Tag gesendet.

Rx Threshold (All Ports)

Legen Sie durch Eingabe einer Zahl fest, nach wie vielen empfangenen Loop-Detection-Frames von einer Schleife ausgegangen wird.
Falls eine portspezifische Einstellung vorgenommen wurde, siehe unten, wird "Variant" angezeigt.

Remote Reaction (All Ports)

Legen Sie fest, wie das Gerät reagiert, wenn ein Remote Loop auftritt. Wählen Sie aus der Klappliste eine der beiden Optionen:

- No reaction:
  Eine Schleife hat keine Auswirkungen auf den Port, an dem die Schleife auftritt.
- Disable port:
  Der Port, an dem die Schleife auftritt, wird geblockt.

Wenn Sie eine portspezifische Einstellung vorgenommen haben, siehe unten, wird "Variant" angezeigt.

Local Reaction (All Ports):

Legen Sie fest, wie das Gerät reagiert, wenn ein Local Loop auftritt. Wählen Sie aus der Klappliste eine der beiden Optionen:

- No reaction:
  Eine Schleife hat keine Auswirkungen auf den Port, an dem die Schleife auftritt.
- Disable port:
  Der Port wird geblockt.

Wenn Sie eine portspezifische Einstellung vorgenommen haben, siehe unten, wird "Variant" angezeigt.

Loop Detection Port Control

Auf dieser Seite sehen Sie die spezifischen Einstellungen der einzelnen Ports.

Loop Detection Port Control

Port	Setting	Rx Threshold	Remote Loop Reaction	Local Loop Reaction	Reaction Timeout	State	Source Port	Source VLAN
1	Forwarder	2	Disable	Disable	0	deactivated	-	-
2	Forwarder	2	Disable	Disable	0	deactivated	-	-
4	Forwarder	2	Disable	Disable	0	deactivated	-	-
5	Forwarder	2	Disable	Disable	0	deactivated	-	-
6	Forwarder	2	Disable	Disable	0	deactivated	-	-
7	Forwarder	2	Disable	Disable	0	deactivated	-	-
8	Forwarder	2	Disable	Disable	0	deactivated	-	-
AG1	Forwarder	2	Disable	Disable	0	deactivated	-	-

Refresh

Bild 5-116 Loop Detection Port Control

Um einen Port zu konfigurieren, klicken Sie in der Spalte "Port" auf die entsprechende Portnummer. Die Seite "Loop Detection Port Configuration" erscheint.

Loop Detection Port Configuration

Nehmen Sie auf dieser Seite die spezifischen Einstellungen für einzelne Ports vor.

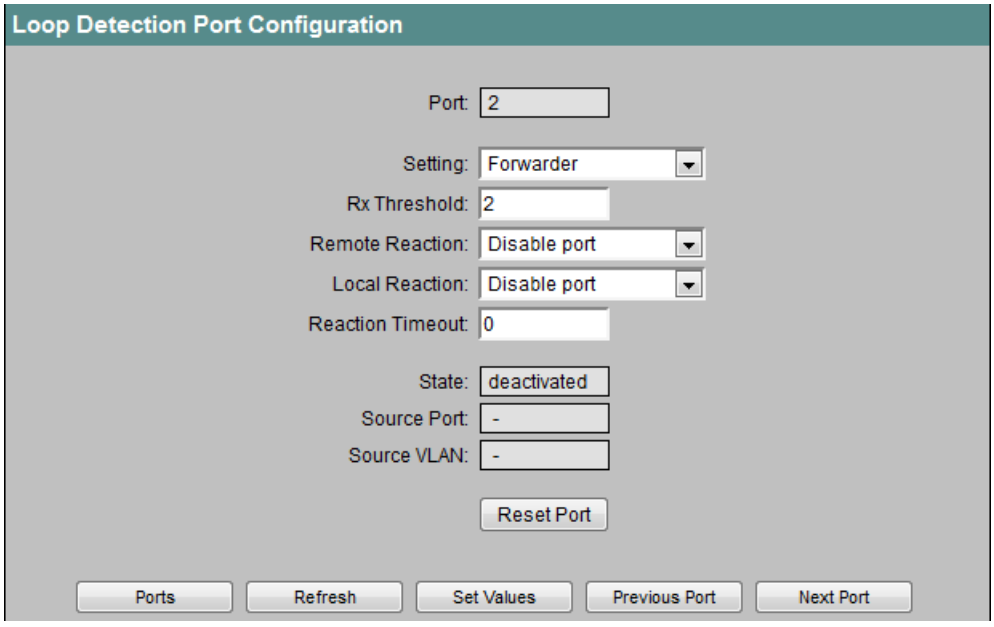


Bild 5-117 Loop Detection Port Configuration

Hinweis

Durch die Test-Frames entsteht zusätzliche Netzlast. Wir empfehlen, nur einzelne Switches, z. B. an den Abzweigungen vom Ring, als "Sender" zu konfigurieren und die anderen als "Forwarder".

Port

Dieses Feld zeigt die Nummer des ausgewählten Ports an.

Setting

Legen Sie fest, wie der Port mit Loop-Detection-Frames verfahren soll. Wählen Sie aus der Klappliste eine der folgenden Optionen:

- Sender
  Loop-Detection-Frames werden ausgesendet und weitergeleitet.
- Forwarder
  Loop-Detection-Frames von anderen Geräten werden weitergeleitet.
- Blocked
  Die Weiterleitung der Loop-Detection-Frames wird blockiert.

Rx Threshold

Legen Sie durch Eingabe einer Zahl fest, nach wie vielen empfangenen Loop-Detection-Frames von einer Schleife ausgegangen wird.

Wenn der Port mehr Loop-Detection-Frames empfängt, als festgelegt wurde, leitet der Port die Loop-Detection-Frames nicht mehr weiter.

Remote Reaction

Legen Sie fest, wie der Port reagiert, wenn ein Remote Loop auftritt. Wählen Sie aus der Klappliste eine der beiden Optionen:

- No reaction:
  Eine Schleife hat keine Auswirkungen auf den Port.
- Disable port:
  Der Port wird geblockt.

Local Reaction

Legen Sie fest, wie der Port reagiert, wenn ein Local Loop auftritt. Wählen Sie aus der Klappliste eine der beiden Optionen:

- No reaction
  Eine Schleife hat keine Auswirkungen auf den Port.
- Disable port
  Der Port wird geblockt.

Reaction Timeout

Legt 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 "Reset Port".

State

Dieses Feld zeigt an, ob die Schleifenerkennung für diesen Port ein- oder ausgeschaltet ist.

Source Port

Dieses Feld zeigt den Empfänger-Port des Loop-Detection-Frames an, das die letzte Reaktion ausgelöst hat.

Source VLAN

Dieses Feld zeigt die VLAN-ID des Loop-Detection-Frames an, das die letzte Reaktion ausgelöst hat.
Voraussetzung dafür ist, dass Sie die Option "VLAN Support Enabled" auf der Seite "Loop Detection Configuration" aktiviert haben.

Schaltfläche "Reset Port"

Nachdem eine Schleife im Netzwerk beseitigt wurde, klicken Sie auf diese Schaltfläche, um den Port zurücksetzen.

Fehlermeldungen

Wenn die Funktion "Loop Detection" eine Schleife erkennt, wird dies über die Fehler-LED, den Meldekontakt und entsprechende Meldetexte signalisiert. Die Meldetexte werden über den Meldeweg angezeigt, den Sie für das Alarmereignis "Loop Detection State Change" konfiguriert haben, siehe Kapitel "Agent Event Configuration (Seite 119)".

Mögliche Meldewege sind E-Mail, Trap, Eintrag in der Log-Datei bzw. auf dem Syslog-Server.

Die Auflistung der Meldetexte finden Sie im Anhang D "Fehlermeldungen des SCALANCE X300 / X400 (Seite 403)".

Fehler-LED und Meldekontakt

Wenn eine Schleife erkannt wird, leuchtet die Fehler-LED des Geräts und der Meldekontakt öffnet. Wenn der Fehlerzustand nicht mehr besteht, erlischt die Fehler-LED und der Meldekontakt schließt.

Zustandsmeldungen

Folgende Zustandsmeldungen können auftreten:

- "Local Loop detected on <Portnummer>. Port disabled."
  Das Gerät hat einen Local Loop erkannt. Der betroffene Port wird abgeschaltet (disabled). Ein angeschlossener Partner sieht weiterhin den Zustand "Link up".
- "Local Loop detected on <Portnummer>. Port disabled for <Wartezeit> seconds."
  Das Gerät hat einen Local Loop erkannt. Der betroffene Port wird für eine bestimmte Zeit abgeschaltet (disabled). Ein angeschlossener Partner sieht weiterhin den Zustand "Link up".
- "Remote Loop detected on <Portnummer>. Port disabled."
  Das Gerät hat einen Remote Loop erkannt. Der betroffene Port wird abgeschaltet (disabled). Ein angeschlossener Partner sieht weiterhin den Zustand "Link up".
- "Remote Loop detected on <Portnummer>. Port disabled for <Wartezeit> seconds."
  Das Gerät hat einen Remote Loop erkannt. Der betroffene Port wird für eine bestimmte Zeit abgeschaltet (disabled). Ein angeschlossener Partner sieht weiterhin den Zustand "Link up".
- "Local Loop detected on <Portnummer>."
  Das Gerät hat einen Local Loop erkannt.
- "Remote Loop detected on <Portnummer>."
  Das Gerät hat einen Remote Loop erkannt.
- "<Portnummer> is enabled again for loop detecion."
  Die Funktion "Loop Detection" wurde für den Port wieder aktiviert.
- "<Portnummer> is enabled again after being disabled by loop detecion."
  Ein Port, der wegen eines Loops abgeschaltet (disabled) war, wurde wieder eingeschaltet (enabled).

Syntax Command Line Interface

Tabelle 5-85 Loop Detection Configuration – CLI\SWITCH\LOOPD >

Befehl	Beschreibung	Kommentar
info	Zeigt Informationen über die "Loop Detection Configuration" an.	
loopd [E | D]	Aktiviert / Deaktiviert die Schleifenerkennung.	Nur Administrator.
vlansupp [E | D]	Aktiviert / Deaktiviert VLAN Support.	Nur Administrator.

Tabelle 5-86 Loop Detection Configuration – CLI\SWITCH\LOOPD\PORTS >

Befehl	Beschreibung	Kommentar
info	Zeigt Informationen über die "Loop Detection Port Configuration" an.	
local <N | D> [ports]	Legt die Reaktion auf einen Local Loop fest.	Nur Administrator.
loopd <B | F | S> [ports]	Legt das Verhalten eines Ports für die Schleifenerkennung fest: • "Blocked," • "Forwarder" • "Sender"	Nur Administrator.
remote <N | D> [ports]	Legt die Reaktion auf einen Remote Loop fest.	Nur Administrator.
reset [ports]	Reaktiviert den Port, falls er wegen einer erkannten Schleife deaktiviert wurde.	Nur Administrator.
rxthres <count> [ports]	Legt fest, nach wie vielen empfangenen Loop-Detection-Frames von einer Schleife ausgegangen wird.	Nur Administrator.
timeout [<0..86400> [ports]]	Legt 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 dem Befehl "reset".	Nur Administrator.

5.5.26 NAT - Network Address Translation

Hinweis

Die Funktion NAT ist nur beim SCALANCE X300 und SCALANCE X408 verfügbar.

Unter Network Address Translation (NAT) versteht man das Umschreiben einer Netzwerkadresse in einem Router bezogen auf einen Datenstrom. Damit ist nicht unbedingt nur die IP-Adresse gemeint. Wenn Knoten mit lokalen Adressen Serverfunktionen für außen übernehmen, dann werden neben den IP-Adressen auch Port-Nummern im Router ersetzt.

Der häufigste Grund für den Einsatz von NAT ist, dass die IP-Adressen der Geräte im lokalen Netz nach außen nicht sichtbar werden sollen.

Traditional NAT

Beim Traditional NAT sind Verbindungen nur in eine Richtung erlaubt, und zwar vom lokalen Netzwerk aus. Traditional NAT unterscheidet die Verfahren Basic NAT und NAPT (Network Address Port Translation).

Bei Basic NAT wird ein Pool von globalen/externen Adressen für die Umschreibung bereit gehalten und jede interne Adresse wird in eine externe Adresse umgewandelt.

Bei NAPT wird der Transport Identifier, z. B. Port-Nummern, in die Umsetzung mit einbezogen. Daher reicht bei diesem Verfahren eine einzige externe Adresse zum Umschreiben aus.

1:1-NAT bei SCALANCE X300/X400

Eine besondere Variante des NAT, die beim SCALANCE X300/X400 zum Einsatz kommt, ist 1:1-NAT, auch Bi-directional NAT genannt. Diese Variante erlaubt den Verbindungsaufbau in beide Richtungen, also auch vom externen Netzwerk in das lokale Netz. Das Umschreiben der Netzwerkadressen erfolgt über eine statische Tabelle. In dieser Tabelle legen Sie 1:1 fest, in welche globale IP-Adresse eine lokale IP-Adresse übersetzt werden soll und umgekehrt.

NAT-Konfiguration

Hinweis

Die Funktion NAT beansprucht viel Rechenkapazität. Schalten Sie daher möglichst viele der anderen Funktionen und Protokolle (RSTP, HRP/MRP, PTP, etc.) ab, wenn Sie den Switch als NAT-Gerät benutzen. Dadurch ist ein höherer Datendurchsatz für die NAT-Pakete möglich.

Klicken Sie im Menübaum auf den Ordner "NAT", um zum Fenster "Network Address Translation" zu gelangen. Dieses Fenster zeigt die aktuellen NAT-Einstellungen an.

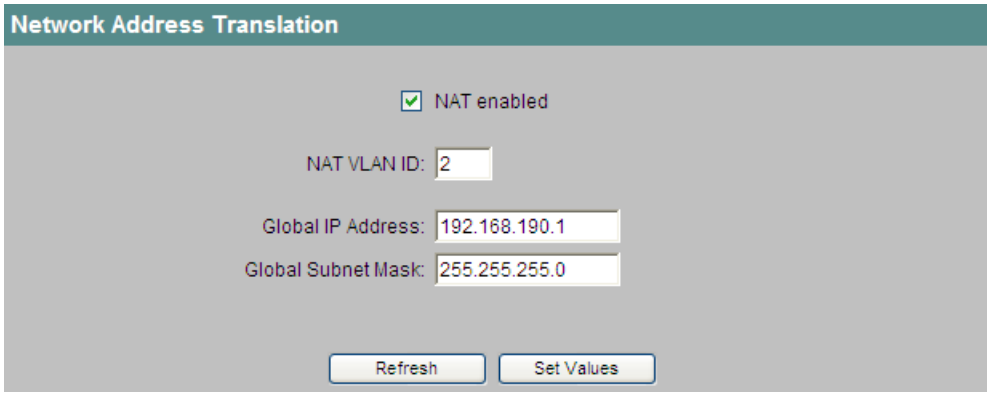


Bild 5-118 Network Address Translation

NAT enabled

Aktivieren oder deaktivieren Sie die NAT-Funktion durch Klicken auf das Optionskästchen.

NAT VLAN ID:

Geben Sie in das Eingabefeld die Kennung von einem konfigurierten virtuellen LAN für die globale Netzwerkanbindung ein.

Global IP Address:

Geben Sie in das Eingabefeld die globale IP-Adresse für die dynamische Adressumschreibung ein.

Global Subnet Mask:

Geben Sie in das Eingabefeld die globale Subnetzmaske ein. Die Subnetzmaske muss eine Class-C Adresse der Form 255.255.255.0 sein.

Statische NAT-Tabelle

Im Menübaum befindet sich im Ordner "NAT" der Unterpunkt "Basic NAT". Klicken Sie auf diesen Unterpunkt, um zur statischen Adress-Tabelle zu gelangen.

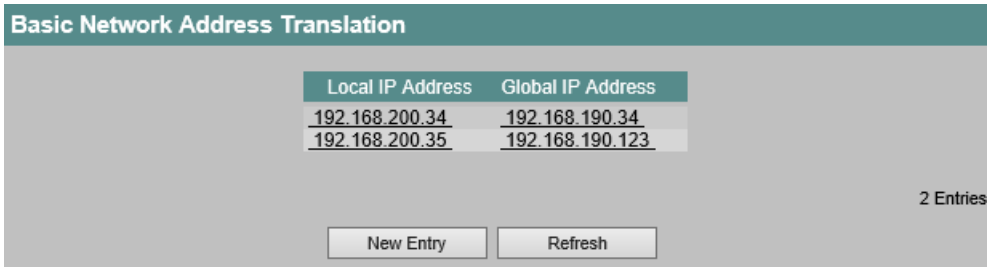


Bild 5-119 Statische NAT-Tabelle

Einen neuen Eintrag anlegen

1. Klicken Sie auf die Schaltfläche "New Entry".
   Das Fenster "Basic Network Address Translation Entry" erscheint.
2. Tragen Sie in das Feld "Local IP" die zu übersetzende lokale IP-Adresse ein.
3. Tragen Sie in das Feld "Global IP" die entsprechende globale IP-Adresse ein.
4. Klicken Sie auf die Schaltfläche "Set Values", um die Einstellungen zu speichern.

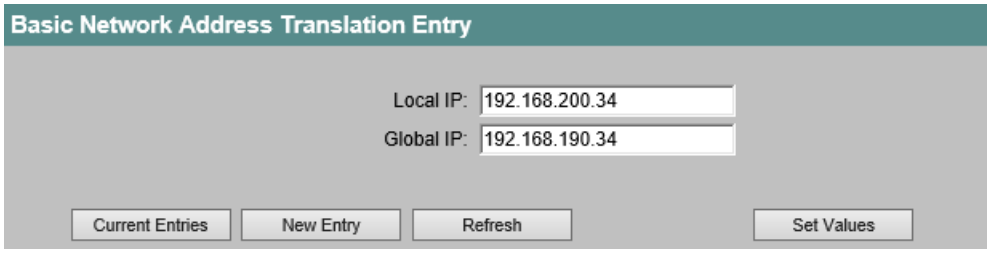


Bild 5-120 NAT-Eintrag erstellen

Einen vorhandenen Eintrag löschen

1. Klicken Sie im Fenster "Basic Network Address Translation" auf eine vorhandene IP-Adresse.
   Das Fenster "Basic Network Address Translation Entry" erscheint.
2. Klicken Sie auf die Schaltfläche "Delete", um diesen Eintrag zu löschen.

Syntax Command Line Interface

NAT - Network Address Translation

Tabelle 5-87 **CLI\SWITCH\NAT>**

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen NAT-Einstellungen an.	
nat [<E|D]	Aktiviert/Deaktiviert die NAT-Funktion.	Nur Administrator.

Befehl	Beschreibung	Kommentar
config <VID> <IP> <subnet>	Legt die NAT-Einstellungen VLAN-ID, IP-Adresse und Subnetzmaske fest.	Nur Administrator.
BASIC	Öffnet den Menüpunkt "Basic NAT".	Nur Administrator.

Tabelle 5-88 **CLI\SWITCH\NAT\BASIC>**

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen NAT-Einträge an.	
add <local IP> <global IP>	Legt einen neuen NAT-Eintrag an.	Nur Administrator.
delete <local IP> <global IP>	Löscht einen vorhandenen NAT-Eintrag.	Nur Administrator.

5.5.27 Statistics

Zählen und Auswerten empfangener Frames

Ein IE-Switch führt interne Statistikzähler, mit denen er für jeden Port die Anzahl der empfangenen Frames nach folgenden Kriterien zählt:

- Framelänge
- Frametyp
- Fehlerhafte Frames

Diese Informationen geben Ihnen einen Überblick über den Datenverkehr sowie über eventuell aufgetretene Netzprobleme.

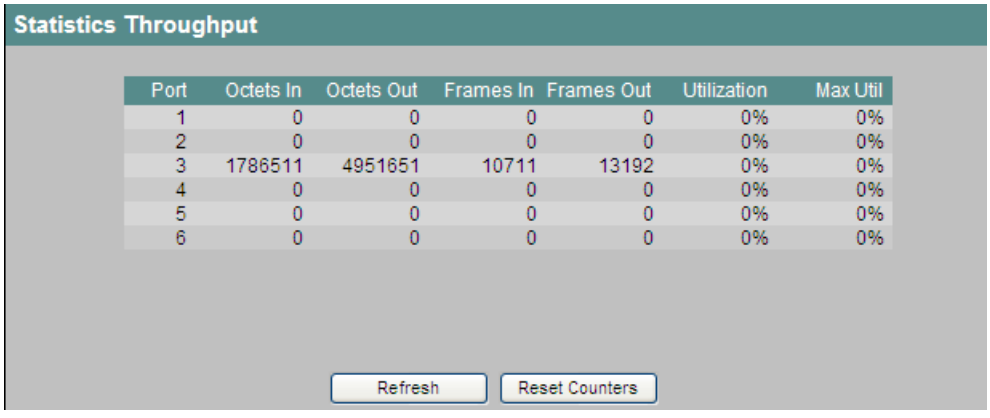


Bild 5-121 Statistics Throughput

Octets In

Zeigt die Anzahl der empfangenen Bytes an.

Octets Out

Zeigt die Anzahl der gesendeten Bytes an.

Frames In

Zeigt die Anzahl der empfangenen Blöcke an.

Frames Out

Zeigt die Anzahl der gesendeten Blöcke an.

Utilization

Zeigt die aktuelle Portauslastung in Prozent (%) an. Wenn die Busauslastung < 1% ist, erfolgt keine Anzeige. Die Anzeige kann je nach Framelänge (systembedingt) um bis zu 20% abweichen, da bei kurzen Frames der Anteil der Pausen zwischen den Frames steigt. Der Wert für die Utilization wird alle 5 Sekunden ermittelt.

Max. Utilization

Zeigt den Spitzenwert der Portauslastung in Prozent (%) an.

Hinweis

Beim X300 errechnet sich der Wert Utilization aus den eingehenden Frames. Dabei sind nur korrekte Frames relevant.

Beim X414 errechnet sich der Wert Utilization aus den eingehenden und ausgehenden Frames. Bei den eingehenden Frames sind sowohl korrekte als auch fehlerhafte Frames relevant. Bei den ausgehenden Frames sind nur korrekte Frames relevant.

Syntax Command Line Interface

Tabelle 5-89 Statistics Throughput - CLI\SWITCH\STATS>

Befehl	Beschreibung	Kommentar
info	Zeigt Statistikinformationen über gesendete und empfangene Frames an.	Nur Administrator.
size [ports]	Zeigt Informationen zur Länge der gesendeten und empfangenen Frames an.	Nur Administrator.
type [ports]	Zeigt Informationen zum Typ der gesendeten und empfangenen Frames an.	Nur Administrator.
error [ports]	Zeigt Informationen zu fehlerhaft gesendeten und empfangenen Frames an.	Nur Administrator.
clear	Setzt die Zählerstände zurück.	Nur Administrator.

5.5.27.1 Packet Size Statistic

Empfangene Frames sortiert nach Länge

Die Seite "Packet Size Statistic" zeigt, wie viele Frames welcher Größe an jedem Port empfangen wurden.

Durch Anklicken der Schaltfläche "Reset Counters" setzen Sie diesen Zähler für alle Ports zurück.

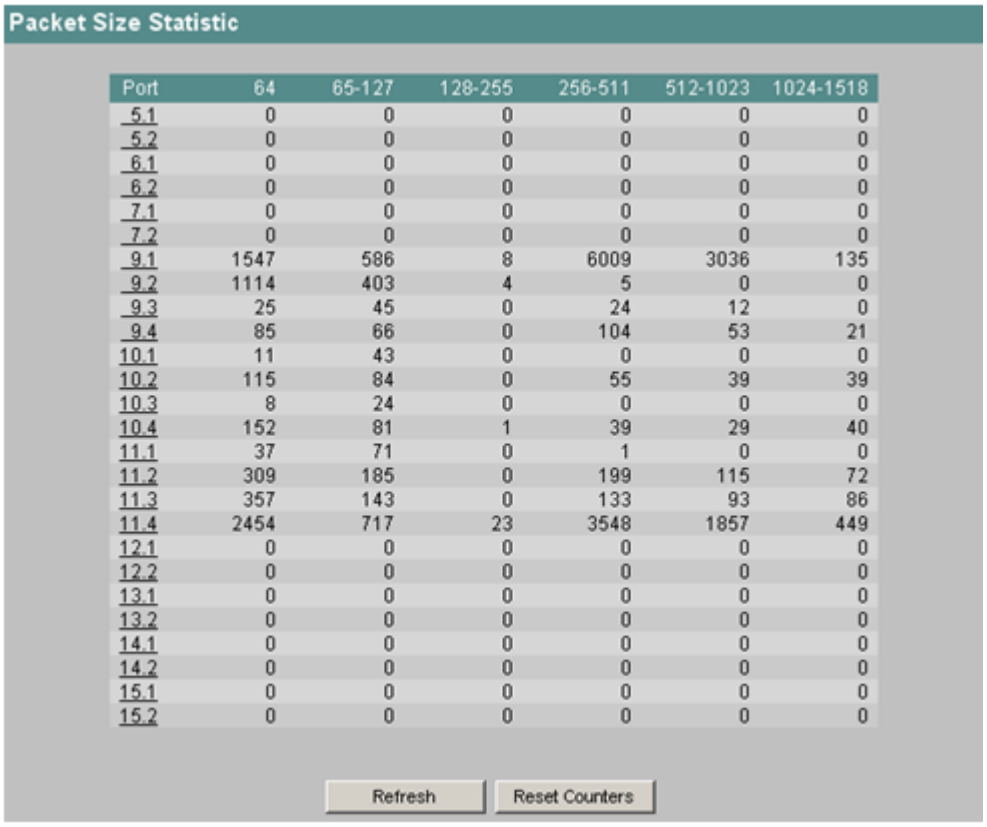


Bild 5-122 Packet Size Statistic

Wenn Sie einen Eintrag in der Spalte Port anklicken, wird die Seite "Packet Size Statistic Graphic" für den ausgewählten Port angezeigt. Dort gibt es eine konfigurierbare grafische Darstellung des Zählerstandes.

Grafische Darstellung der Statistik

Diese Seite stellt die Anzahl der an einem Port empfangenen Frames grafisch dar. Dabei erfolgt die Darstellung abhängig von der Framelänge. Für jeden der folgenden Bereiche gibt es ein eigenes Element in der Grafik:

- 64 Byte
- 65 - 127 Byte
- 128 - 255 Byte
- 256 - 511 Byte

- 512 - 1023 Byte
- 1024 - 1518 Byte

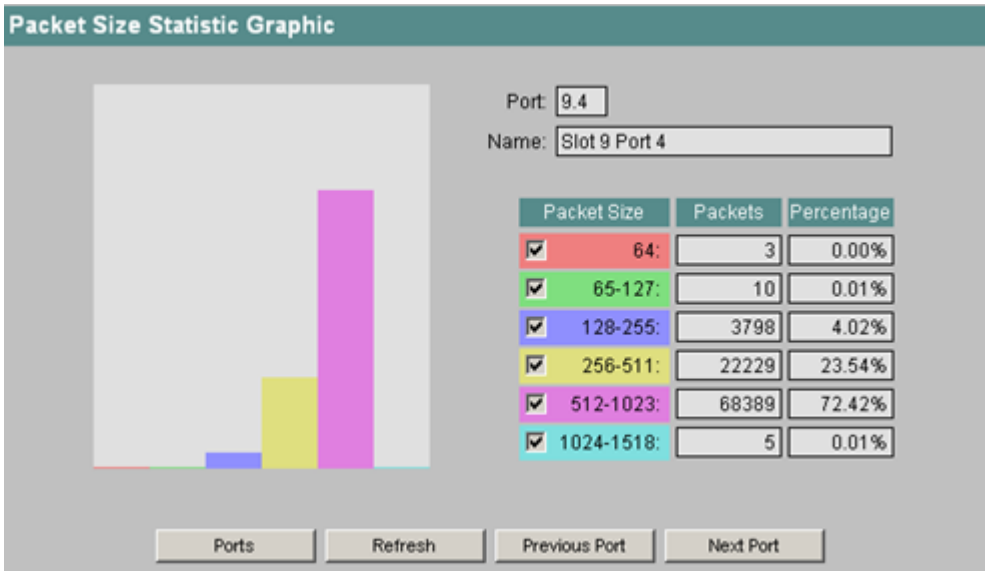


Bild 5-123 Packet Size Statistic Graphics

Mit den Optionskästchen in der Spalte "Packet Size" bestimmen Sie den Inhalt der Grafik. In der Grafik wird der Wert in der Spalte "Packets" für einen bestimmten Größenbereich nur dann dargestellt, wenn die entsprechende Option aktiviert ist. Die Spalte "Percentage" gibt den prozentualen Anteil der Pakete in einem bestimmten Längenbereich an der Gesamtmenge der Pakete für diesen Port an. Bei der Berechnung des prozentualen Anteils werden nur die Größenbereiche einbezogen, deren Option aktiviert ist.

Mit den Schaltflächen "Previous Port" und "Next Port" können Sie zur Darstellung des vorangegangenen bzw. des nächsten Ports wechseln.

Syntax Command Line Interface

Tabelle 5-90 Statistics - CLI\ SWITCH\STATS>

Befehl	Beschreibung	Kommentar
size [ports]	Zeigt die Anzahl der empfangenen Frames, geordnet nach Framelänge. Es können auch mehrere Ports angegeben werden. Beispiel: • size 5.1, 6.1-7.2 Zeigt die Längen der an den Ports 5.1 sowie 6.1 bis 7.2 empfangenen Frames.	-

5.5.27.2 Packet Type Statistic

Empfangene Frames sortiert nach Typ

Die Seite "Packet Type Statistic" zeigt, wie viele Frames des Typs "Unicast", "Multicast" und "Broadcast" an jedem Port empfangen wurden.

Durch Anklicken der Schaltfläche "Reset Counters" setzen Sie diesen Zähler für alle Ports zurück.

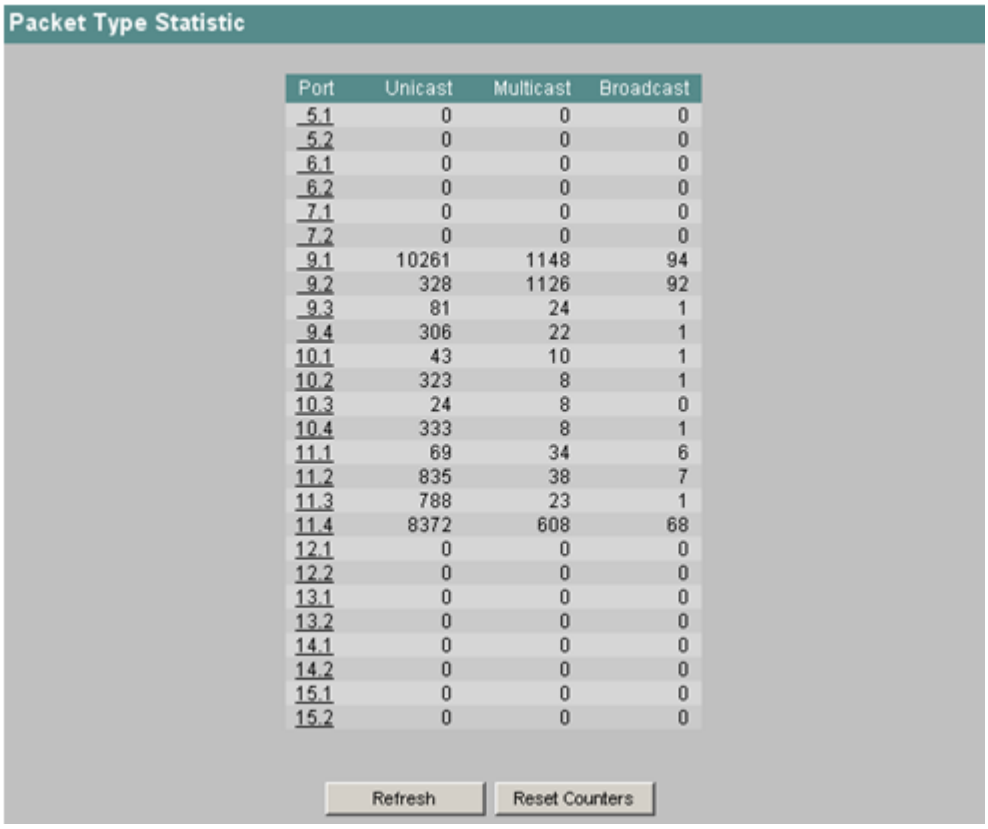


Bild 5-124 Packet Type Statistc

Wenn Sie einen Eintrag in der Spalte Port anklicken, wird die Seite "Packet Type Statistic Graphic" für den ausgewählten Port angezeigt. Dort gibt es eine konfigurierbare grafische Darstellung des Zählerstandes.

Grafische Darstellung der Statistik

Diese Seite stellt die Anzahl der an einem Port empfangenen Frames grafisch dar. Dabei erfolgt die Darstellung abhängig vom Frametyp. Für jeden der folgenden Bereiche gibt es ein eigenes Element in der Grafik:

- Unicast
- Multicast
- Broadcast

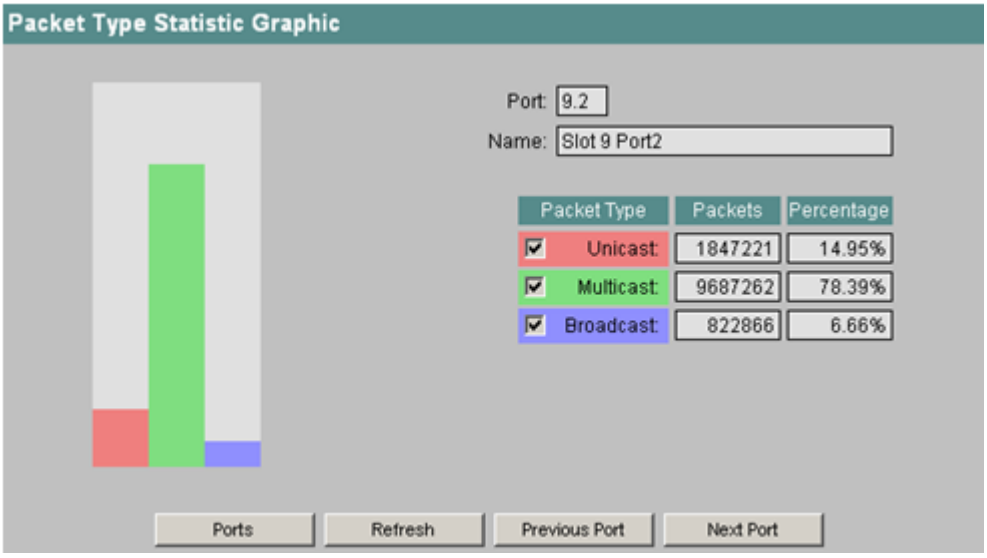


Bild 5-125 Packet Type Statistic Graphic

Mit den Optionskästchen in der Spalte "Packet Type" bestimmen Sie den Inhalt der Grafik. In der Grafik wird der Wert in der Spalte "Packets" für einen bestimmten Frametyp nur dann dargestellt, wenn die entsprechende Option aktiviert ist. Die Spalte "Percentage" gibt den prozentualen Anteil der Pakete eines bestimmten Typs an der Gesamtmenge der Pakete für diesen Port an. Bei der Berechnung des prozentualen Anteils werden nur die Frametypen einbezogen, deren Option aktiviert ist.

Mit den Schaltflächen "Previous Port" und "Next Port" können Sie zur Darstellung des vorangegangenen bzw. des nächsten Ports wechseln.

Syntax Command Line Interface

Tabelle 5-91 Statistics - CLI\SWITCH\STATS>

Befehl	Beschreibung	Kommentar
type [ports]	Zeigt die Anzahl der empfangenen Frames, geordnet nach Frametyp. Es können auch mehrere Ports angegeben werden. Beispiel: • type 5.1, 6.1-7.2 Zeigt die Typen der an den Ports 5.1 sowie 6.1 bis 7.2 empfangenen Frames.	-

5.5.27.3 Error Statistic

Fehler in empfangenen Frames

Die Seite "Packet Error Statistic" zeigt, wie viele fehlerhafte Frames pro Port empfangen wurden. Dabei wird nach folgenden Fehlertypen unterschieden:

- CRC
  Pakete, deren Inhalt nicht mit der zugehörigen CRC-Prüfsumme übereinstimmte.
- Undersize
  Pakete mit einer Länge kleiner als 64 Byte.
- Oversize
  Pakete mit einer Länge größer als 1518 bzw. 1522 Byte bei Frames mit VLAN-Tag.
- Fragments
  Pakete mit einer Länge kleiner als 64 Byte und einer falschen CRC-Prüfsumme.
- Jabbers
  Pakete mit einer Länge größer als 1518 bzw. 1522 Byte bei Frames mit VLAN-Tag und einer falschen CRC-Prüfsumme.

  Hinweis

  Der SCALANCE X414-3E zählt auch solche Frames als Jabber, die länger als 1518 Byte bzw. 1522 Byte sind und ein korrekte CRC-Prüfsumme haben.

- Collisions
  Erkannte Kollisionen.

Durch Anklicken der Schaltfläche "Reset Counters" setzen Sie diesen Zähler für alle Ports zurück.

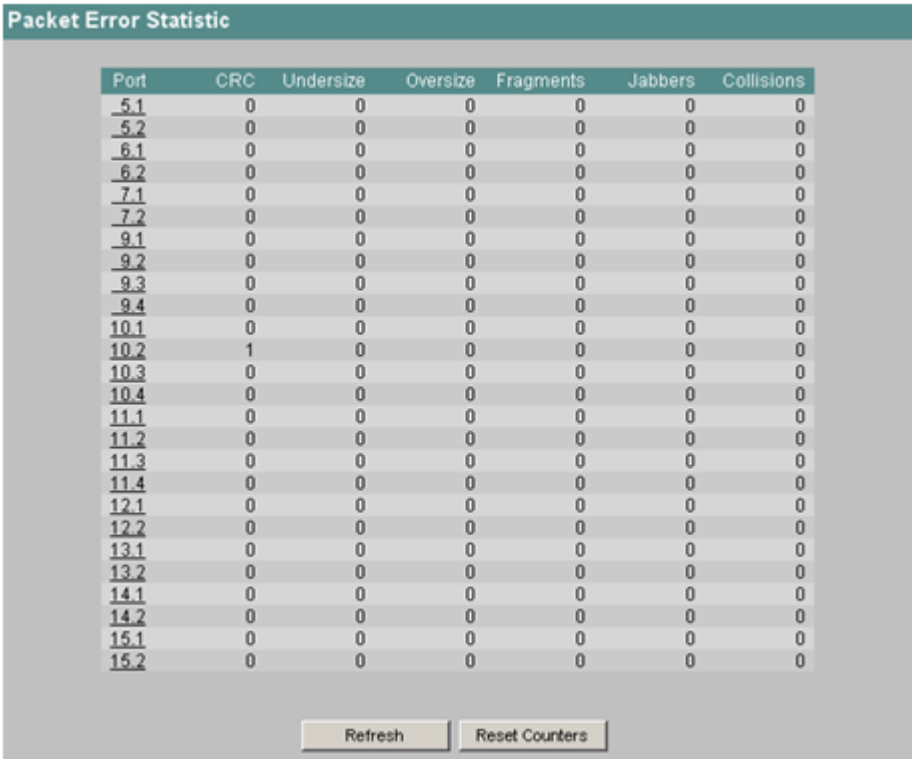


Bild 5-126 Packet Error Statistic

Wenn Sie einen Eintrag in der Spalte Port anklicken, wird die Seite "Packet Error Statistic Graphic" für den ausgewählten Port angezeigt. Dort gibt es eine konfigurierbare grafische Darstellung des Zählerstandes.

Grafische Darstellung der Statistik

Diese Seite stellt die Anzahl der fehlerhaften Frames grafisch dar. Dabei erfolgt die Darstellung abhängig von der Fehlerursache. Für jede der folgenden Fehlerursachen gibt es ein eigenes Element in der Grafik:

- CRC
- Undersize
- Oversize

- Jabbers
- Collisions

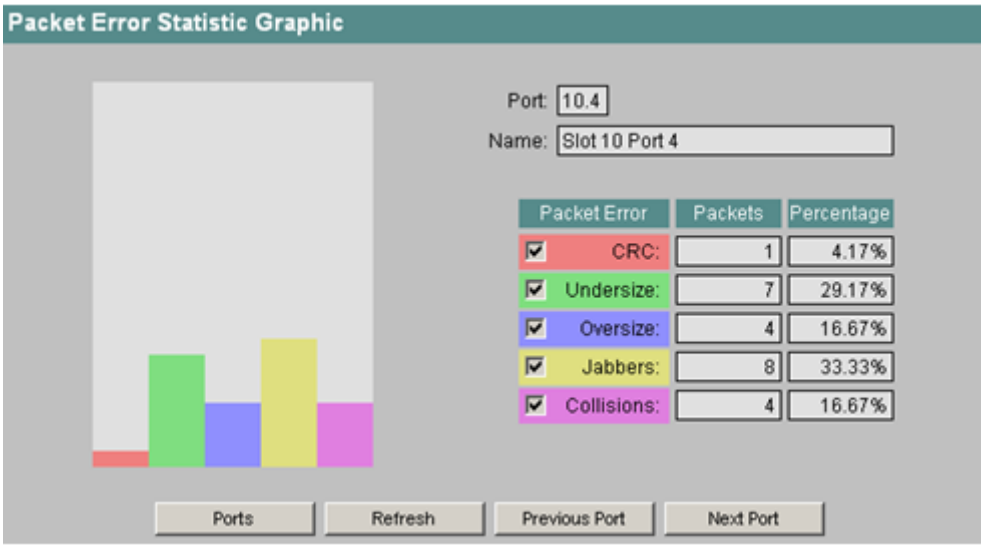


Bild 5-127 Packet Error Statistic Graphic

Mit den Optionskästchen in der Spalte "Packet Error" bestimmen Sie den Inhalt der Grafik. In der Grafik wird der Wert in der Spalte "Packets" für einen bestimmten Frametyp nur dann dargestellt, wenn die entsprechende Option aktiviert ist. Die Spalte "Percentage" gibt den prozentualen Anteil der Fehler eines bestimmten Typs an der Gesamtmenge der Fehler für diesen Port an. Bei der Berechnung des prozentualen Anteils werden nur die Fehlertypen einbezogen, deren Option aktiviert ist.

Mit den Schaltflächen "Previous Port" und "Next Port" können Sie zur Darstellung des vorangegangenen bzw. des nächsten Ports wechseln.

Syntax Command Line Interface

Tabelle 5-92 Statistics - CLI\SWITCH\STATS>

Befehl	Beschreibung	Kommentar
error [ports]	Zeigt die Anzahl der empfangenen Frames, geordnet nach Frame-Fehlern. Es können auch mehrere Ports angegeben werden. Beispiel: • error 5.1, 6.1-7.2 Zeigt die fehlerhaften Frames die an den Ports 5.1 sowie 6.1 bis 7.2 empfangen wurden.	-

5.6 Der Menüpunkt PoE

Einstellungen für Power over Ethernet

SCALANCE-Geräte in der Ausführung "PoE" können andere PoE-fähige Geräte über eine Ethernet-Leitung mit Spannung versorgen. 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.

Die Übersichtsseite zeigt Informationen über die vom SCALANCE-Gerät über PoE gelieferte Leistung sowie Detailinformationen zu jedem einzelnen PoE-Port.

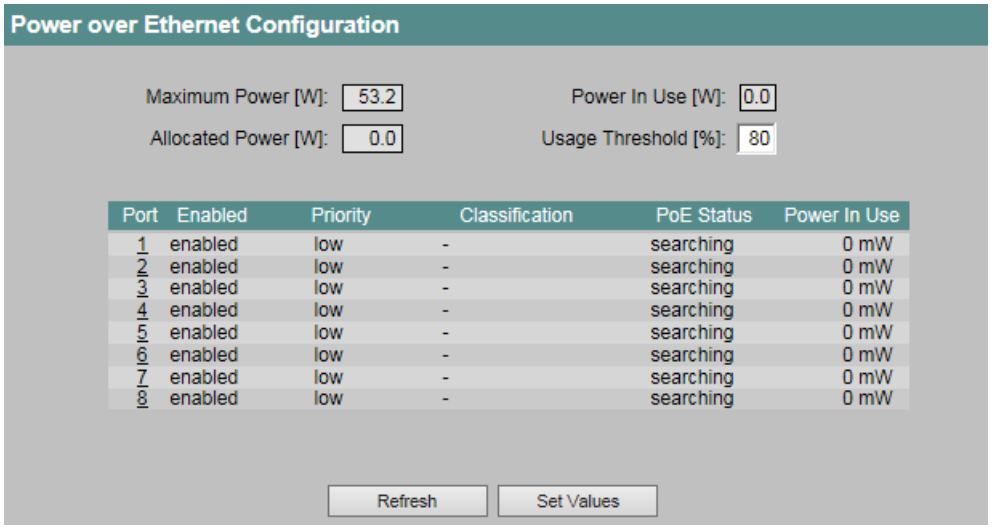


Bild 5-128 Informationen zur PoE-Konfiguration des SCALANCE

Die folgenden Felder zeigen Informationen zu der Leistung, die der IE-Switch über PoE liefert.

- **Maximum Power [W]** (nur lesbar)
  Maximale Leistung, die der SCALANCE für die Versorgung von PoE-Geräten zur Verfügung stellt.
- **Allocated Power [W]** (nur lesbar)
  Summe der durch die PoE-Geräte reservierte Leistung.
- **Power in Use [W]** (nur lesbar)
  Summe der von den Engeräten verbrauchten Leistung.
- **Usage Threshold** [%]
  Sobald die von den angeschlossenen Geräten verbrauchte Leistung größer ist als dieser Prozentanteil der maximalen Leistung, wird ein Event ausgelöst.

Die Tabelle zeigt folgende Informationen an.

- **Port**
  Zeigt die konfigurierbaren PoE-Ports an.
- **Enabled**
  Zeigt ob die PoE-Spannungsversorgung für diesen Port aktiviert oder deaktiviert ist.

- **Priority**
  Zeigt mit welcher Priorität dieser Port bei der Spannungsversorgung berücksichtigt wird.
- **Classification**
  Die Classification gibt die Klasse des Geräts an. Daran kann man die maximale Leistung des Geräts ablesen.
- **PoE Status**
  Zeigt an, in welchem Zustand sich der Port befindet. Es gibt folgende Zustände:
  - disabled
    Die PoE-Spannungsversorgung für diesen Port ist deaktiviert.
  - delivering Power
    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.
- **Power in Use**
  Zeigt die Leistung an, die der SCALANCE an diesem Port liefert.

Einstellungen für einen Port vornehmen

Klicken Sie auf eine Nummer in der Spalte "Port", um die Seite "PoE Port Configuration" zu öffnen.

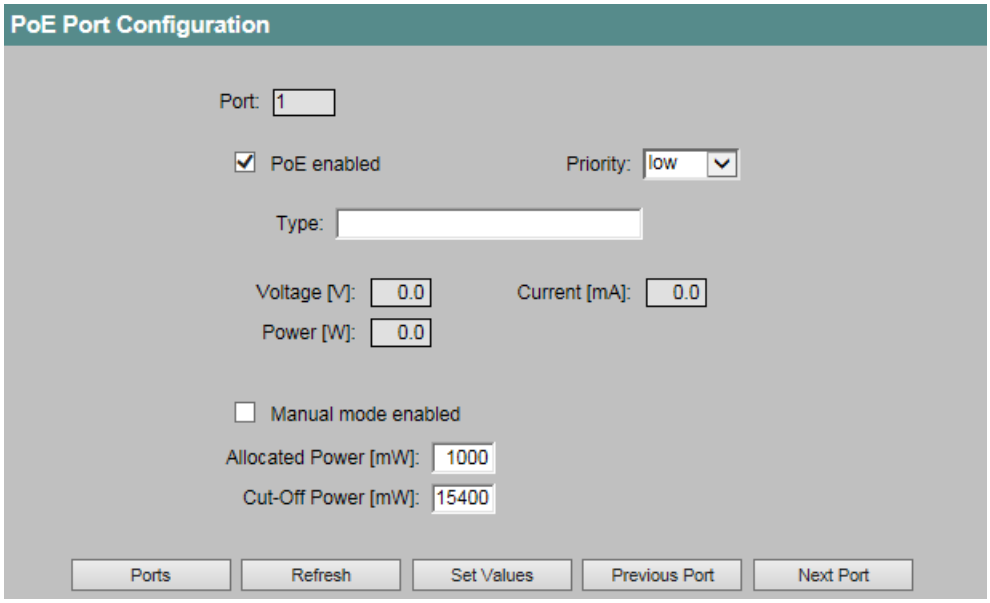


Bild 5-129 Detailinformationen über die Spannungsversorgung eines Ports

PoE enabled
Bei markiertem Kontrollkästchen ist die PoE-Spannungsversorgung für diesen Port aktiviert.

Priority
Legt fest, mit welcher Priorität dieser Port bei der Spannungsversorgung berücksichtigt wird. Es gibt folgende Einstellmöglichkeiten:

- low
- high
- critical

Ist für zwei Ports die gleiche Priorität vorgegeben, wird im Bedarfsfall der Port mit der niedrigeren Nummer bevorzugt.

Type
Hier können Sie eine Zeichenkette eingeben, die das angeschlossene Gerät näher beschreibt. Die maximale Länge beträgt 64 Zeichen.

Voltage [V] (nur lesbar)
Die Spannung, die an diesem Port anliegt.

Power [W] (nur lesbar)
Dies Leistung, die der SCALANCE an diesem Port abgibt.

Current [mA] (nur lesbar)
Der Strom, mit dem ein Gerät an diesem Port versorgt wird.

Manual mode enabled
Aktiviert/Deaktiviert den manuellen Modus für PoE.
Wenn der manuelle Modus aktiviert ist, können Sie die Leistungswerte für die PoE-Ports manuell vorgeben.

Allocated Power [mW]
Weist einem Port eine bestimmte Leistung in mW zu ("Allocated Power").
Wertebereich: 1000 mW - 20000 mW

Cut-Off Power [mW]
Legt die Cut-off Leistung für einen Port in mW fest. Wenn die Cut-off Leistung überschritten wird, wird der Port abgeschaltet.
Wertebereich: 1000 mW - 20000 mW

Syntax Command Line Interface

Tabelle 5-93 CLI\POE>

Befehl	Beschreibung	Kommentar
info [ports]	Zeigt für den entsprechende Port Informationen über PoE an.	-
pseusage [percent]	Setzt einen Wert (in Prozent) für den Parameter Usage Threshold. Sobald die von den angeschlossenen Geräten verbrauchte Leistung größer ist als dieser Prozentanteil der maximalen Leistung, wird ein Event ausgelöst. Wenn Sie diesen Befehl ohne Parameter aufrufen, wird der aktuelle Wert angezeigt.	Nur Administrator.

Befehl	Beschreibung	Kommentar
status [<E|D> [ports]]	Aktiviert/Deaktiviert die PoE-Spannungsversorgung für den angegebenen Port.	Nur Administrator.
prio [<LOW|HIGH|CRITICAL> [ports]]	Legt die Priorität für die Spannungsversorgung für den angegebenen Port fest. Wird kein Port angegeben, gilt der Wert für alle Ports.	Nur Administrator.
type <port> [string]	Legt eine Zeichenkette fest, die das angeschlossene Gerät näher beschreibt. Die maximale Länge beträgt 64 Zeichen.	Nur Administrator.
manmode [<E|D>]	Aktiviert/Deaktiviert den "Manual Power Allocation Mode" für einen Port. Wenn der "Manual Power Allocation Mode" aktiviert ist, können Sie die Leistungswerte für die PoE-Ports manuell vorgeben.	Nur Administrator.
apower [<power> [ports]]	Weist einem Port eine bestimmte Leistung in mW zu ("Allocated Power"). Wertebereich: 1000 mW - 20000 mW	Nur Administrator.
copower [<power> [ports]]	Legt die Cut-off Leistung für einen Port in mW fest. Wenn die Cut-off Leistung überschritten wird, wird der Port abgeschaltet. Wertebereich: 1000 mW - 20000 mW	Nur Administrator.
assign [<port>]	Die Leistung, die ein Port aktuell verbraucht, wird dem Port fest zugewiesen, als "Allocated Power".	Nur Administrator.

5.7 Das Menü Router (SCALANCE X414-3E)

Hinweis

Die Routing-Funktion ist nur beim SCALANCE X414-3E verfügbar.

Grundsätzliches zur Vorgehensweise

Um einen SCALANCE X414-3E als Router einzurichten, legen Sie zunächst mindestens zwei Subnetze an und ordnen jedes Subnetz einem vorher definierten VLAN zu. Dann können Sie statische Routen eintragen oder/und die Router Protokolle RIP oder OSPF aktivieren.

Informationen zur Konfiguration von VLANs finden Sie in Kapitel "Menüpunkt Current VLAN Configuration".

5.7.1 Router Configuration

Einleitung

Die Maske "Router Configuration" erscheint, wenn Sie das Ordnersymbol *Router* angeklickt haben. In dieser Maske können Sie den SCALANCE X414-3E als IPv4 Router parametrieren.

Um die Routing-Information im Netzwerk zu verteilen, stehen die Protokolle RIPv2 und OSPFv2 zur Verfügung, die Sie hier auswählen können. Die Detail-Parametrierung der Protokolle nehmen Sie in den jeweiligen Untermenüs vor.

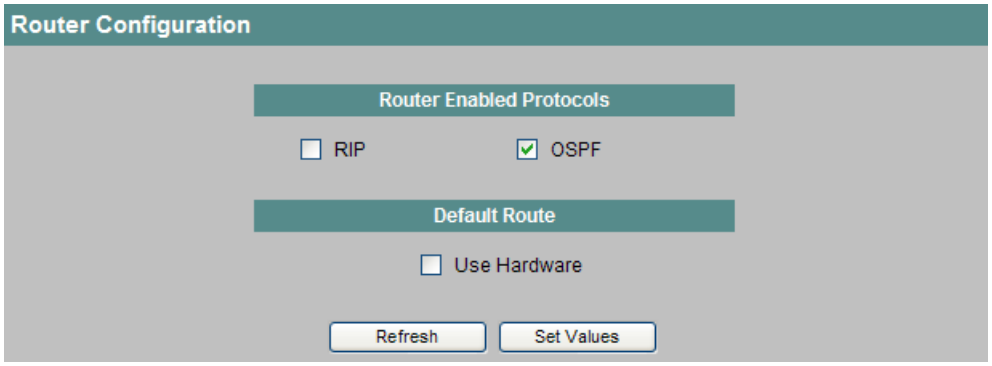


Bild 5-130 Router Configuration

Einstellungen für den SCALANCE X-400

RIP
Aktiviert die Option "Routing Information Protocol version 2" (RIP).

Hinweis

Der Router nimmt am RIP-Protokoll teil, sobald mindestens ein Interface für RIP konfiguriert wurde.

OSPF
Aktiviert die Option "Open Shortest Path First protocol version 2" (OSPF).

Hinweis

Der Router nimmt am OSPF-Protokoll teil, sobald mindestens ein Interface für OSPF konfiguriert und eine Router ID festgelegt wurde.

Use Hardware
Der SCALANCE X-414 bietet die Möglichkeit, ein performantes Hardware-Routing

durchzuführen. Markieren Sie diese Kontrollkästchen, wenn Sie Hardware-Routing für die Default-Adressen aktivieren wollen.

Hinweis

Wird die Default Route in die Hardware eingetragen, reduziert sich die Anzahl der über Routing erreichbaren Subnetze auf 14.

Bei dynamisch gelernten Routen (RIP oder OSPF) entfernt der Routing-Mechanismus die Default-Routen bei Bedarf automatisch aus der Hardware.

Syntax Command Line Interface

Tabelle 5-94 Router Configuration - CLI\ROUTER>

Befehl	Beschreibung	Kommentar
setrip <E|D>	Aktiviert/Deaktiviert RIP	Nur Administrator.
setospf <E|D>	Aktiviert/Deaktiviert OSPF	Nur Administrator.
defrthw <E|D>	Aktiviert/Deaktiviert Hardware-Routing für Default-Adressen.	Nur Administrator.

5.7.2 Router Subnets

Erstellung von Subnetzen

Um den SCALANCE X414-3E als IPv4 Router zu betreiben, müssen Sie mehrere (mindestens 2) Subnetze anlegen.

Dem ersten Subnetz entspricht die Agent Configuration (siehe Kapitel "Menü Agent"). Die Daten können nur dort geändert werden.

Alle weiteren Subnetze können hier angelegt werden (Schaltfläche "New Entry"). Ein Subnetz bezieht sich dabei immer auf eine VLAN ID, die vorher im VLAN Menü angelegt worden sein muss.

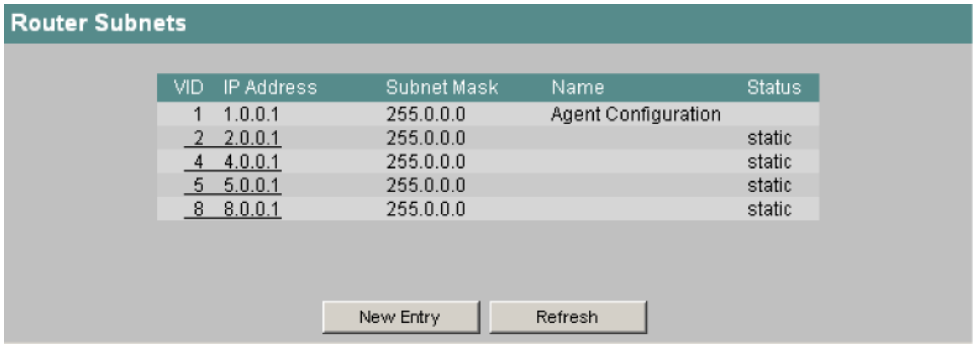


Bild 5-131 Router Subnets

VID
VLAN ID des IP-Subnetzes.

IP Address
IP-Adresse des Subnetzes (muss eindeutig sein).

Subnet Mask
Subnetz-Maske des IP-Subnetzes. Die in der Bit-Darstellung der Subnetz-Maske linksbündig zu setzenden "Einsen" spezifizieren den Netzanteil der IP-Adresse.

Name
Frei wählbarer Name des Subnetzes. Der vordefinierte Name des ersten Subnetzes, das der Agent Configuration entsprechen muss, lautet "Agent Configuration".

Status
Status des Subnetzes. Es gibt folgende Zustände:

- static
- invalid
  Ein Subnetz mit dem Status "invalid" weist auf eine Fehlkonfiguration hin, die behoben werden muss.
- RIP
- OSPF

Anlegen eines neuen IP Subnetzes

Ein neues Subnetz können Sie durch Betätigen der Schaltfläche "New Entry" im Menü "Router Subnets" anlegen. Die Parametrierung des Subnetzes erfolgt im Menü "Router Subnet Configuration".

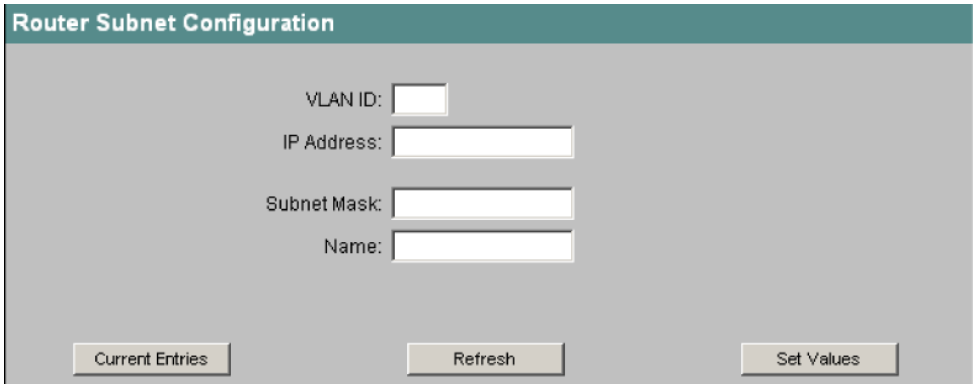


Bild 5-132 Router Subnets Configuration

VLAN ID
Geben Sie hier die ID des VLAN ein (VID siehe Kapitel "Menüpunkt Current VLAN

Configuration"), über das Pakete dieses IP Subnetzes übertragen werden sollen (Wertebereich der ID: 1 bis 4094).

Hinweis

Die Agent VLAN ID darf nicht noch einmal verwendet werden. Alle anderen IDs können mehrfach verwendet werden.

IP Address
Geben Sie hier die IP-Adresse des IP Subnetzes ein. IP-Adressen dürfen nicht mehrfach verwendet werden.

Hinweis

Durch anhängen des Zeichens "/" und einer Zahl zwischen 1 und 30 kann die Subnetzmaske gleich mit definiert werden.

Subnet Mask
Geben Sie hier die Subnetzmaske des zu erstellenden IP Subnetzes ein. Die Subnetzmaske muss aus einem linksbündigen Bitfeld aus Einsen bestehen.

Name
Geben Sie hier den Namen des Subnetzes ein (hat für die Funktionalität keine Bedeutung).

Syntax Command Line Interface

Tabelle 5-95 Subnets - CLI\ROUTER\SUBNETS>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen Subnetze an.	Nur Administrator.
add <VID> <IP> <Subnet> [name]	Fügt ein neues Subnetz ein. Der Parameter Subnet bezeichnet die Subnetzmaske.	Nur Administrator.
edit <VID> <IP> [Subnet] [name]	Ändert ein Subnetz. Der Parameter Subnet bezeichnet die Subnetzmaske.	Nur Administrator.
delete <VID> <IP>	Löscht ein Subnetz.	Nur Administrator.

Der CLI-Befehl "info" gibt eine Tabelle aus (analog zur Tabelle im Web Interface). Die Spalte "Status" ist hier jedoch auf zwei Zeichen beschränkt (St).

Es gibt die folgenden Status (siehe auch Web Interface):

- RI (RIP)
- OS (OSPF)
- st (static)
- ?? (invalid)

5.7.3 Current Routes

Routing-Tabelle

In diesem Menü wird die Routing-Tabelle angezeigt. Auch statische Routing-Tabelleneinträge können hier erzeugt werden.

Eine Routing-Tabelle ist im allgemeinen eine Liste von Regeln, nach denen empfangene Pakete weitergeleitet werden sollen. Steht ein Paket für das Routing an, so wird seine Zieladresse mit den Adressen in der Routing-Tabelle verglichen. Der Eintrag dessen Adresse verbunden mit der Subnetzmaske am besten passt (nach dem Longest Prefix Match-Verfahren), beschreibt dann, wie das Paket weiterzuleiten ist.

Einträge in der Routing-Tabelle mit dem Status "local" bezeichnen die projektierten Subnetze.

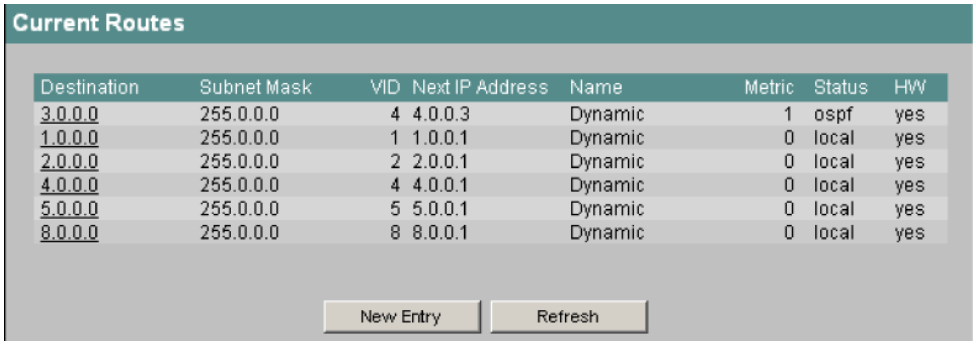


Bild 5-133 Current Routes

Destination
Destination Adresse dieser Route.

Subnet Mask
Bezeichnet die gültigen Bits der Spalte Destination. Sie muss aus linksbündigen Einsen bestehen.

VID
Die VID bezeichnet diejenige VLAN ID, über deren IP-Subnetz ein Paket weiterzuleiten ist, wenn die Regel verwendet wird.

Next IP Address
Die Next IP Address bezeichnet die IP-Adresse des Geräts, das als nächstes anzusteuern ist.

Name
Der Name beeinflusst den Routing Prozess nicht.
Bei statischen Routen kann ein Name eingetragen werden.
Bei dynamischen Routen wird der Name auf "Dynamic" gesetzt.

Metric
In der Spalte Metric wird die Entfernung zwischen Router und Ziel angezeigt.

Status
Mit dem Status einer Route wird angezeigt, ob diese vom OSPF- oder vom RIP-Protokoll als statische Route (static) oder lokal (local) erzeugt wurde.
Statische Routen werden manuell über die Schaltfläche "New Entry" angelegt.
Lokale Routen werden beim Anlegen eines Subnetzes automatisch angelegt.

HW
Die Spalte HW (Hardware) kennzeichnet die Zuordnung der Route zur Hardware. Es gibt folgende Möglichkeiten:

- Yes:
  Darf in der HW gespeichert werden
- In use:
  Ist bereits in der HW gespeichert
- No:
  Darf nicht in der HW gespeichert werden
  Bei statischen Routen kann "Yes" oder "No" vorgegeben werden. Erst beim tatsächlichen Gebrauch werden die Routen in der HW gespeichert und als "In use" gekennzeichnet.

Anlegen einer neuen statischen Route

Über die Schaltfläche "New Entry" im Menü "Current Routes" kann eine neue Route angelegt werden. Diese administrativ erstellten Routen sind immer statisch.

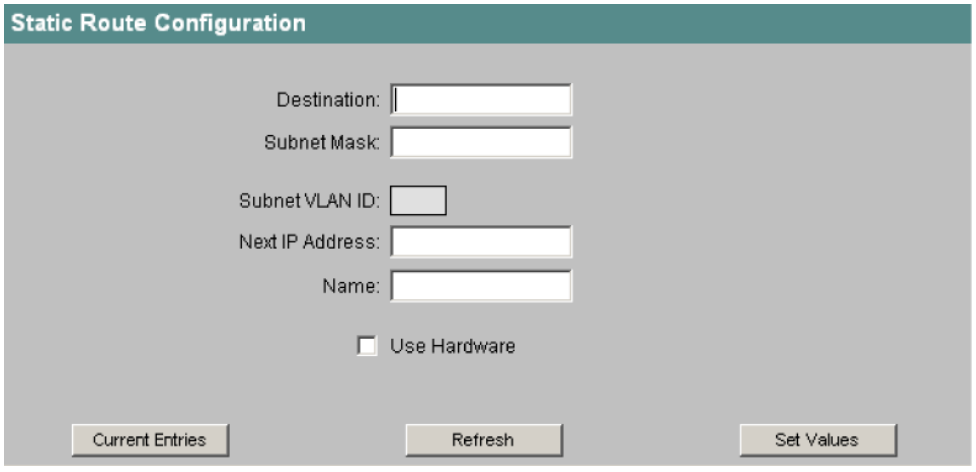


Bild 5-134 Static Route Configuration

Destination
Geben Sie hier eine IP-Adresse ein, auf die sich der Routing-Tabelleneintrag beziehen soll.

Subnet Mask
Geben Sie hier die Subnetz Maske des Routing Eintrags an. Sie zeigt an, welche Bits der Adresse für den Routing-Vergleich gültig sind.

Subnet VLAN ID
Die Subnet VLAN ID wird aus der nächsten IP-Adresse automatisch berechnet und ist bei neuen Anlagen leer.

Next IP Address
Geben Sie hier die Adresse des nächsten Routers ein, an den die Pakete dieser Route geschickt werden sollen. Der Router muss sich in einem angeschlossenen Subnetz befinden.

Name
Geben Sie hier den Namen der Route ein (hat für die Funktionalität keine Bedeutung).

Use Hardware
Aktivieren Sie diese Option, wenn die Route in die Hardware geschrieben werden soll. Ist die Option aktiviert, so wird nach dem ersten erfolgreichen Weiterleiten die Route in die Hardware geschrieben und kann damit schneller verwendet werden.

Hinweis

Die Route kann nur dann in die Hardware geschrieben werden, wenn dort noch genügend Speicherplatz zur Verfügung steht.

Syntax Command Line Interface

Tabelle 5-96 Current Routes - CLI\ROUTER\ROUTES>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen Routen an.	Nur Administrator
add <IP> <Subnet> <NextIP> [E|D] [name]	Fügt eine neue Route ein. Parameter E|D für Aktivieren/ Deaktivieren von "Use Hardware".	Nur Administrator
edit <IP> [NextIP] [E|D] [name]	Ändert eine Route. Parameter E|D für Aktivieren/ Deaktivieren von "Use Hardware".	Nur Administrator
delete <IP>	Löscht eine Route.	Nur Administrator

Der CLI-Befehl "info" gibt eine Tabelle aus (analog zur Tabelle im Web Interface). Die Spalten "Metric" und "Status" sind hier jedoch auf zwei Zeichen beschränkt (Me; St).
Es gibt die folgenden Stati:

- OS (OSPF)
- RI (RIP)
- st (static)
- lo (local)
- ot (other)
- ?? (invalid)

In der Spalte "Hardware" (HW) gibt es folgende Möglichkeiten (siehe auch Web Interface):

- Yes: X (großes X)
- In use: * (Stern)
- No: - (Minuszeichen)

5.7.4 RIPv2 Configuration

Einleitung

Im Menü "RIPv2 Configuration" können Sie allgemeine Parameter des RIP-Protokolls einstellen sowie einige grundlegende Statistikzähler anschauen.

Hinweis

Damit die hier getroffenen Einstellungen wirksam werden, muss im Menü "Router Configuration", RIP aktiviert sein.

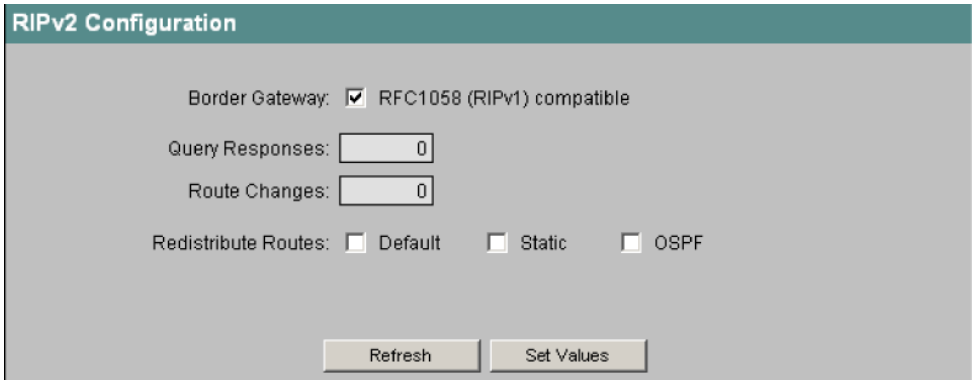


Bild 5-135 RIPv2 Configuration

Border Gateway
Aktivieren Sie diese Option nur, wenn Sie den Router zusammen mit Original RIPv1 Routern betreiben. In dem Fall werden Subnetzrouten Class-spezifisch zusammengefasst und sogenannte Supernets nicht propagiert. Damit erreichen Sie die größtmögliche Kompatibilität mit RIPv1 Routern.

Query Responses
Anzahl der beantworteten speziellen Routing-Anfragen.

Route Changes
Anzahl der in der Routing-Tabelle durchgeführten Änderungen.

Redistribute Routes (Default/Static/OSPF)
Mit dieser Option geben Sie an, welche bekannten Routen über RIP weitergegeben werden sollen. Sie können unterschiedliche Entscheidungen für die Route-Typen Default, Static und OSPF treffen.

Hinweis

Aktivieren Sie diese Option bitte nur an Übergängen zwischen unterschiedlichen Netzwerken (Border Gateways). Besonders die Aktivierung der Optionen Default und Static kann zu Problemen (z.B. erhöhte Verkehrslast in Forwarding Loops) führen, wenn sie an zu vielen Stellen im Netz aktiviert werden.

Syntax Command Line Interface

Tabelle 5-97 RIPv2 Configuration - CLI\ROUTER\RIP>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuelle RIP Konfiguration an.	-
rfc1058 <E|D>	Setzt die RFC1058 (RIPv1)-Kompatibilität.	Nur Administrator.
redistr <E|D> <E|D> <E|D>	Aktiviert/Deaktiviert "redistribute routes". • Parameter 1 default routes • Parameter 2 static routes • Parameter 3 OSPF routes	Nur Administrator.

5.7.5 RIPv2 Interfaces

Einleitung

Im Menü "RIPv2 Interfaces" wird eine Übersicht über alle IP Subnetze angezeigt, die am RIP-Protokoll teilnehmen.

Über die Schaltfläche "New Entry" können neue Subnetze für RIP angemeldet werden.

Hinweis

Damit ein Subnetz für RIP angemeldet werden kann, muss es zunächst im Menü "Router Subnets" angelegt werden.

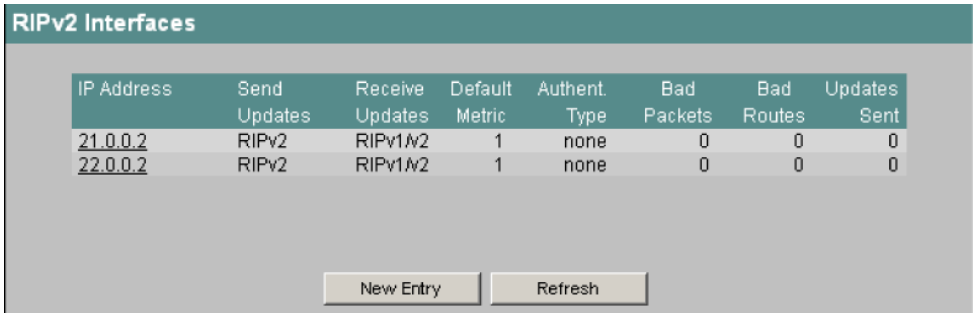


Bild 5-136 RIPv2 Interfaces

IP Address
IP-Adresse des RIP-fähigen Subnetzes (alleiniger Identifikator für diese Tabelle). Alle anderen

Subnetzparameter (wie beispielsweise die Subnetzmaske) findet man im Menü "Router Subnets".

Send Updates
In dieser Spalte wird angezeigt, auf welche Weise Updates gesendet werden sollen. Zur Auswahl stehen:

- no send:
  Es werden keine Updates versendet
- RIPv1:
  Versenden von RIPv1 Updates nach RFC 1058
- RIPv1-compat:
  Versenden von RIPv2 Updates nach den Regeln von RFC 1058 als Broadcasts
- RIPv2:
  Versenden von RIPv2 Updates als multicast
- RIPv1 demand und RIPv2 demand:
  RIP Pakete werden nur als Antworten auf explizites Nachfragen versendet.
  Verwenden Sie diese Option nur, wenn ihr Router mit einem anderen Router über eine WAN Schnittstelle kommunizieren muss.

Receive Updates
In dieser Spalte wird angezeigt, in welcher Form empfangenen RIP Pakete akzeptiert werden. Zur Auswahl stehen:

- no receive:
  Es werden keine Pakete akzeptiert.
- RIPv1:
  Es werden nur Pakete von RIPv1 Routern akzeptiert.
- RIPv2:
  Es werden nur Pakete von RIPv2 Routern empfangen und bearbeitet.
- RIPv1/v2:
  Alle Varianten des RIP Protokolls werden auf diesem Interface akzeptiert.

Default Metric
In dieser Spalte wird angezeigt, welche Metrik der Default Route auf diesem Interface zugeordnet wird.
Der Wert 0 gibt an, dass keine Default Route propagiert wird.
Ansonsten sind die Werte 1..15 gültig.

Authent. Type
In dieser Spalte wird der Authentifizierungstyp angezeigt. Dies kann sein:

- keine Authentifizierung
- simple password
- MD5 Authentifizierung.

Bad Packets
Zähler für empfangen RIP Pakete, die gelöscht und deswegen nicht beachtet wurden.

Bad Routes
Anzahl der Routen gültiger RIP Pakete, die nicht berücksichtigt werden konnten.

Updates Sent
Anzahl der "Triggered Updates" für dieses Interface

Anlegen eines neuen RIPv2 Interfaces

Ein neues Interface können Sie durch Betätigen der Schaltfläche "New Entry" im Menü "RIP Interfaces" anlegen. Damit gelangen Sie in folgendes Menü.

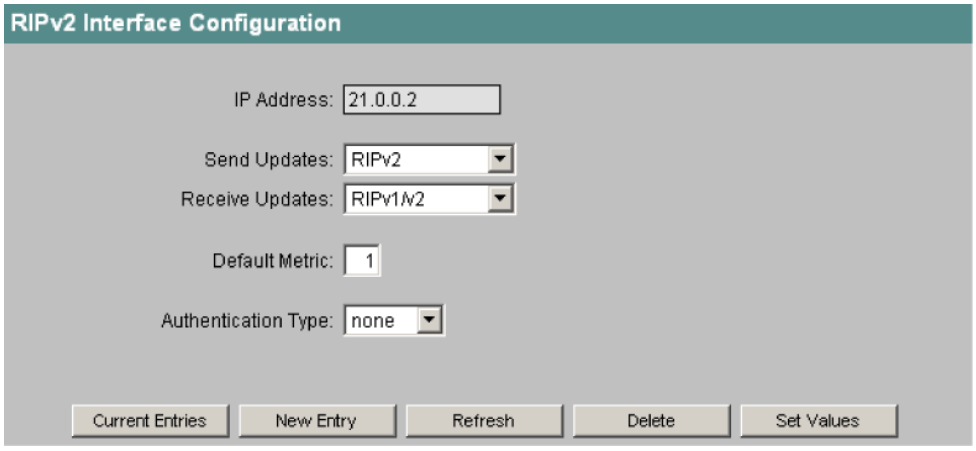


Bild 5-137 RIPv2 Interface Configuration

IP Address
Geben Sie hier die IP-Adresse des Interfaces ein, auf das RIP konfiguriert werden soll. Diese IP-Adresse muss bereits als IP Subnetz konfiguriert worden sein.

Send-Updates
Wählen Sie hier aus, wie RIP Updates gesendet werden sollen. Die Update Pakete enthalten die Routing-Tabelle des lokalen Systems. Zur Auswahl stehen:

- no send:
  keine Updates versenden
- RIPv1:
  RIPv1 Updates nach den Regeln von RFC 1058 versenden
- RIPv1-compat:
  RIPv2 Updates nach den Regeln von RFC 1058 als Broadcasts versenden
- RIPv2:
  RIPv2 updates als multicast versenden
- Die Werte "RIPv1 demand" und "RIPv2 demand" werden nur bei WAN-Schnittstellen benötigt. Hierbei werden RIP Pakete nur als Antwort auf explizites Nachfragen versendet.

Hinweis

Sind keinerlei RIPv1 Geräte in Ihrem Netzwerk vorhanden, sollten Sie "RIPv2" einstellen.

Receive-Updates
Wählen Sie hier aus, nach welchen Regeln empfangene Pakete akzeptiert werden sollen. Zur Auswahl stehen:

- no receive:
  keine Updates empfangen
- RIPv1:
  RIPv1 Updates empfangen
- RIPv2:
  RIPv2 Updates empfangen
- RIPv1/v2:
  RIPv1 und RIPv2 Updates empfangen

Default Metric
Geben Sie hier an, mit welcher Metrik die Default-Route auf diesem Interface propagiert wird. RIP verwendet im die Hop-Metrik, bei der Distanzen in "Anzahl benutzter Router" angegeben werden (Wertebereich: 1-15 (0 schaltet die Default-Route aus)).
Es gilt: Je größer der Wert, desto länger benötigen Pakete zu Ihrem Ziel.

Authentication Type

Wählen Sie hier die Authentifizierungsmethode der RIP Pakete aus. Zur Auswahl stehen

- none: Keine Authentifizierung (default)
- simple: Authentifizierung über Passwort und Bestätigung
- MD5: Authentifizierung über das Keyed MD5 Verfahren (Passwort, Bestätigung und Key ID)
- Diese Methoden dienen lediglich dazu, die Authentizität eines Pakets zu bestimmen; sie verschlüsseln keine Daten.

Key ID

Hinweis

Das Textfeld "Key ID" wird nur eingeblendet, wenn die Authentifizierungsmethode auf MD5 eingestellt wurde.

Geben Sie hier die Key ID ein, unter der das Passwort als Schlüssel verwendet wird. Da die Key ID mit dem Protokoll übertragen wird, muss bei allen benachbarten Routern der gleiche Schlüssel unter der gleichen Key ID gespeichert werden.

Password/Confirmation

Hinweis

Das Textfeld "Password/Confirmation" wird nur eingeblendet, wenn die Authentifizierungsmethode auf MD5 oder simple eingestellt wurde.

Bei Authentifizierung über Passwort und über MD5 wird ein Key benötigt, der hier eingegeben werden kann.

Syntax Command Line Interface

Tabelle 5-98 RIPv2 Interfaces - CLI\ROUTER\RIP\RIP\IFACE>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen Interfaces an.	-
add <IP> [SendUpd] [RecvUpd] [Metric]	Fügt ein neues Interface ein. Mögliche Parameter für SendUpd: • SV1 RIPv1 • SV1C RIPv1 Comp. • SV1D RIPv1 Dem. • SV2 RIPv2 • SV2D RIPv2 Dem. • SNO No Send Mögliche Parameter für RecvUpd: • RV1 RIPv1 • RV2 RIPv2 • RV1V2 RIPv1/v2 • RNO No Receive	Nur Administrator.
edit <IP> [SendUpd] [RecvUpd] [Metric]	Ändert ein Interface. Mögliche Parameter für SendUpd und RecvUpd wie bei Befehl add.	Nur Administrator.
auth <IP> <authtype> [password] [key-id]	Ändert die Authentifizierung eines Interfaces. Mögliche Typen: • None • Simple • MD5 (nur hier wird der "Key-Id" benötigt)	Nur Administrator.
delete <IP>	Löscht ein Interface.	Nur Administrator.

5.7.6 OSPFv2 Configuration

Einleitung

Im Menü "OSPFv2 Configuration" und dessen Untermenüs können Sie die Einstellung der OSPF-Parameter vornehmen.

OSPFv2 unterteilt das administrierte IPv4 Netzwerk (Autonomous System) in verschiedene Bereiche (Areas). Innerhalb dieser Areas, werden die Link Stati aller Router ausgetauscht, so dass jeder Router eine komplette Netzsicht hat. Diese Sicht wird in der Link State Database (LSDB) festgehalten. Jeder Router kann damit nach dem Dijkstra Algorithmus selbst alle Routen innerhalb der Area ermitteln.

Zwischen den Areas gibt es keine einheitliche Sicht. Man beschränkt sich deshalb auf den Austausch von gesammelten Routen, die nach dem distant vector Algorithmus bestimmt werden können.

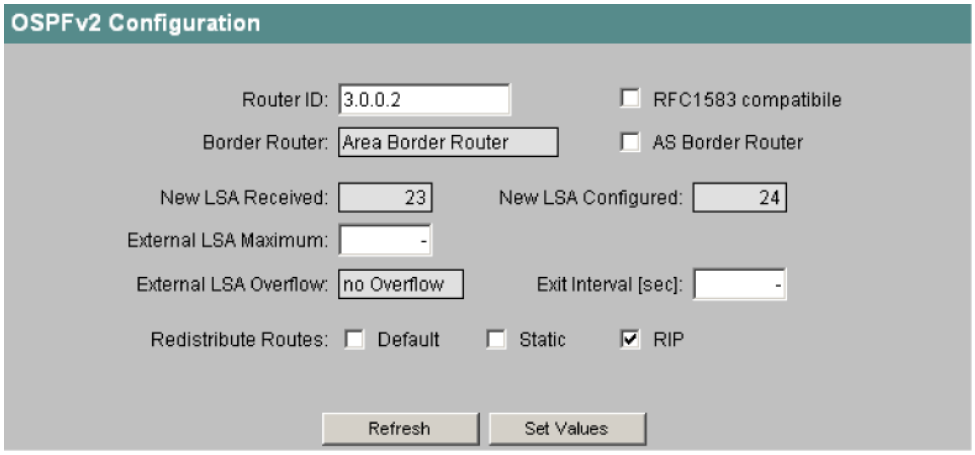


Bild 5-138 OSPFv2 Configuration

Router ID
Stellen Sie hier die Adresse eines der OSPF Interfaces ein. Die IP-Adresse muss eindeutig sein.

RFC 1583 compatible
Diese Option benötigen Sie nur, wenn sich noch alte OSPFv2 Router in Betrieb haben, die nicht zu RFC 2328 kompatibel sind.

Border Router
Anzeige des Border Router Status. Ist das lokale System aktives Mitglied in mindestens 2 Areas, so handelt es sich um einen Area Border Router.

AS Border Router
Aktivieren Sie diese Option, wenn dieser Router als AS Border Router fungieren, d. h. zwischen mehreren Protokollwelten vermitteln soll (wenn Sie z.B. noch ein zusätzliches RIP Netzwerk betreiben).

New LSA received
Anzahl der Link State Advertisements, die empfangen wurden. Updates und eigene LSAs werden nicht gezählt.

New LSA configured
Anzahl der unterschiedlichen LSAs, die von diesem lokalen System versendet wurden.

External LSA Maximum
Geben Sie hier die maximale Anzahl der External LSAs an, wenn sie die External LSDB begrenzen wollen.

External LSA Overflow
Zeigt an, ob die maximale Anzahl der External LSAs überschritten wurde.

Exit Intervall (sec)
Geben Sie hier, die Zeit in Sekunden an, nach der der OSPF Router wieder versuchen soll aus dem Overflow-Status herauszukommen. Eine 0 bedeutet, dass der OSPF Router erst nach einem Hochlauf (ausgelöst durch ein Disable und Enable im Hauptmenü des Routers) wieder versucht den Overflow Status zu verlassen.

Redistribute Routes (Default/Static/RIP)
Mit dieser Option geben Sie an, welche bekannten Routen über OSPF weitergegeben werden sollen. Sie können unterschiedliche Entscheidungen für die Route-Typen Default, Static und RIP treffen.

Hinweis

Aktivieren Sie diese Option bitte nur an Übergängen zwischen unterschiedlichen Netzwerken (Border Gateways). Besonders die Aktivierung der Optionen Default und Static kann zu Problemen (z.B. Forwarding Loops) führen, wenn sie an zu vielen Stellen im Netz aktiviert werden.

Syntax Command Line Interface

Tabelle 5-99 OSPFv2 Configuration - CLI\ROUTER\OSPF>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuelle OSPF Konfiguration an.	-
id <IP>	Setzt die Router-ID (IP-Adresse).	Nur Administrator.
rfc1583 <E|D>	Setzt die RFC1583-Kompatibilität.	Nur Administrator.
asbr <E|D>	Aktiviert/deaktiviert AS border router.	Nur Administrator.
lsamax <number>	Setzt das externe LSA Maximum.	Nur Administrator.
exitint <sec>	Setzt das externe Exit interval.	Nur Administrator.

Befehl	Beschreibung	Kommentar
redistr <E|D> <E|D> <E|D>	Aktiviert/Deaktiviert "Redistribute routes". • Parameter 1 default routes • Parameter 2 static routes • Parameter 3 RIP routes	Nur Administrator.
ospfdbg [E|D] [debugtype]	Aktiviert/deaktiviert OSPF-Debug-Funktionen. Geben Sie "ospfdbg ?" ein, um Hilfe zu erhalten.	Nur Administrator.

5.7.7 OSPFv2 Areas

Übersicht

Ein autonomes Netzwerk (Autonomous System) kann in kleinere Bereiche (Areas) unterteilt werden (siehe Kapitel Menüpunkt OSPFv2 Configuration).

In diesem Menü können Sie die OSPF Areas des Routers überwachen. Neben den Konfigurationsparametern können auch statistische Werte eingesehen werden.

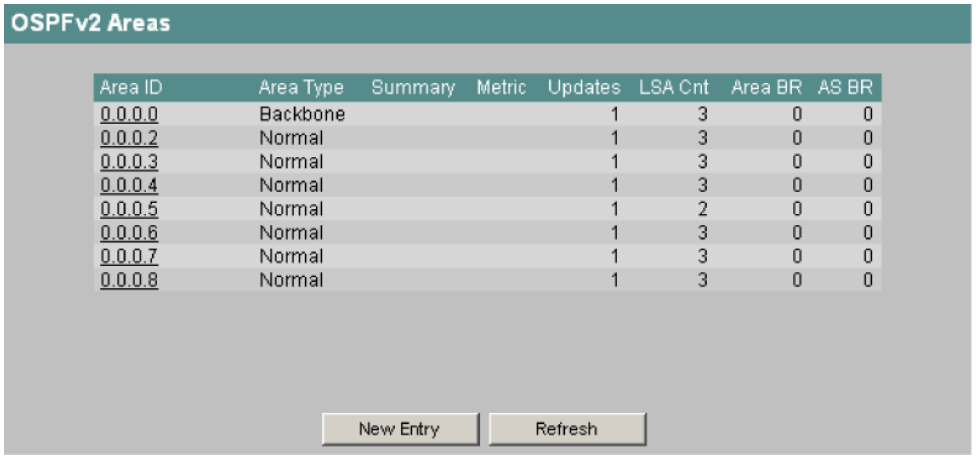


Bild 5-139 OSPFv2 Areas

Area ID
Zeigt die ID dieser Area an. Eine Area ID besteht aus 4 Zahlen jeweils zwischen 0 und 255 und muss eindeutig vergeben sein.
Die Area 0.0.0.0 wird Backbone Area genannt.
Für alle Router in einer Area wird die LSDB dieser Area synchronisiert.

Area Type
Zeigt den Typ der Area an. Es gibt folgende Area Typen:

- Normal
- Stub
- NSSA
- Backbone: Die Backbone Area wird hier besonders gekennzeichnet.

Summary
Zeigt an, ob für diese Area summary LSA erzeugt werden. Diese Spalte ist nur für Stub Areas bedeutsam. Folgende Anzeigen sind möglich:

- import: Summary LSAs werden in diese Area verschickt
- disregard: summary LSAs werden nicht in diese Area verschickt

Metric
Zeigt die Metric der propagierten Default Route der Stub Areas an. Für alle anderen Areas wird nichts angezeigt.

Updates
Anzahl der Routing Tabellen-Berechnungen

LSA Cnt
Anzahl der LSA in der LSDB dieser Area

Area BR
Anzahl der erreichbaren Area Border Router (ABR) innerhalb dieser Area

ASBR
Anzahl der erreichbaren Autonomous System Border Router (ASBR) in dieser Area.

Anlegen einer neuen OSPFv2 Area

Über die Schaltfläche "New Entry" im Menü "OSPFv2 Areas" kann eine neue Area angelegt werden.

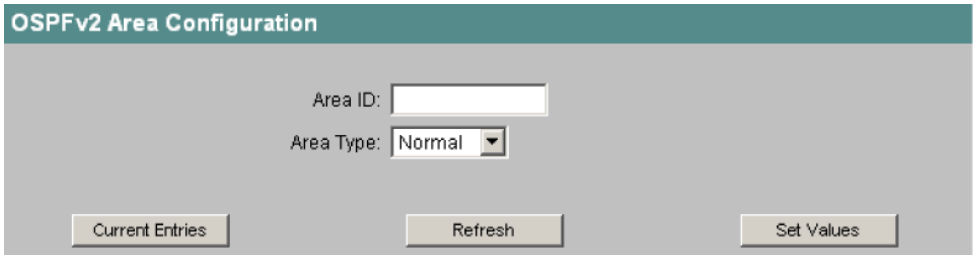


Bild 5-140 OSPFv2 Area Configuration

Area ID
Geben Sie hier die ID der Area an.

Area Type
Es gibt folgende Area Typen:

- Normal
- Stub
- NSSA

Hinweis

Für die Backbone Area muss der Area Typ "Normal" und die Area ID 0.0.0.0 gewählt werden.

Import Summary

Hinweis

Das Optionskästchen "Import Summary" wird nur eingeblendet, wenn der Area Typ "Stub" eingestellt wurde.

Aktivieren Sie diese Option, um die Summary LSAs in dieser Area zu erzeugen und zu propagieren. In diesem Fall ist für die Kommunikation innerhalb des gesamten Netzwerks keine Default Route notwendig.

Hinweis

Bei nur einem Border Router in dieser Stub Area, brauchen Sie diese Option nicht zu aktivieren.

Default Metric

Hinweis

Das Textfeld "Default Metric" wird nur eingeblendet, wenn der Area Typ "Stub" eingestellt wurde.

Geben Sie hier die Metrik Ihrer Default Route an, die in der Stub Area propagiert werden soll.

Syntax Command Line Interface

Tabelle 5-100 OSPFv2 Areas - CLI\ROUTER\OSPF\AREAS>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen Areas an.	-
add <AreaID> <Type> [E|D] [Metric]	Fügt eine neue Area ein. Mögliche Typen: • Normal • Stub • NSSA Die Parameter [E|D] und Metric sind nur bei einer Stub-Area möglich. • E Enable Importing Summary • D Disable Importing Summary	Nur Administrator.
edit <AreaID> [Type] [E|D] [Metric]	Ändert eine Area. Mögliche Typen: • Normal • Stub • NSSA Die Parameter [E|D] und Metric sind nur bei einer Stub-Area möglich. • E Enable Importing Summary • D Disable Importing Summary	Nur Administrator.
delete <AreaID>	Löscht eine Area	Nur Administrator.

Beispiel

Der Befehl

```
add 0.0.0.3 Stub d 2
```

erzeugt eine Stub-Area "0.0.0.3", für die keine Summary LSAs erzeugt werden. Die Default Route wird mit der Metrik "2" belegt.

5.7.8 OSPFv2 Area Ranges

Übersicht

Im Menü "Area Ranges" können Adressbereiche angelegt werden, die es erlauben, beim Propagieren verschiedene Adressbereiche zusammenzufassen. Dadurch kann die Anzahl der Summary LSAs in den Areas verringert werden.

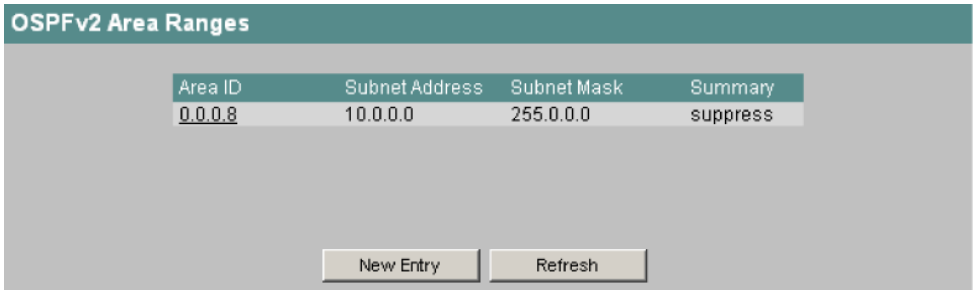


Bild 5-141 OSPFv2 Area Ranges

Area ID
Area ID auf die sich der Adressbereich bezieht.

Subnet Address
Adresse des Netzwerkbereichs, der zusammengefasst werden soll.

Subnet Mask
Subnetzmaske des zusammengefassten Netzwerkbereichs.

Summary
Zeigt an, ob der zusammengefasste Adressbereich nach außen bekannt gemacht wird ("advertise") oder nicht ("suppress").

Anlegen einer neuen OSPFv2 Area Range

Über die Schaltfläche "New Entry" im Menü "OSPFv2 Area Ranges" können bis zu vier Area Ranges für eine Area neu angelegt werden.

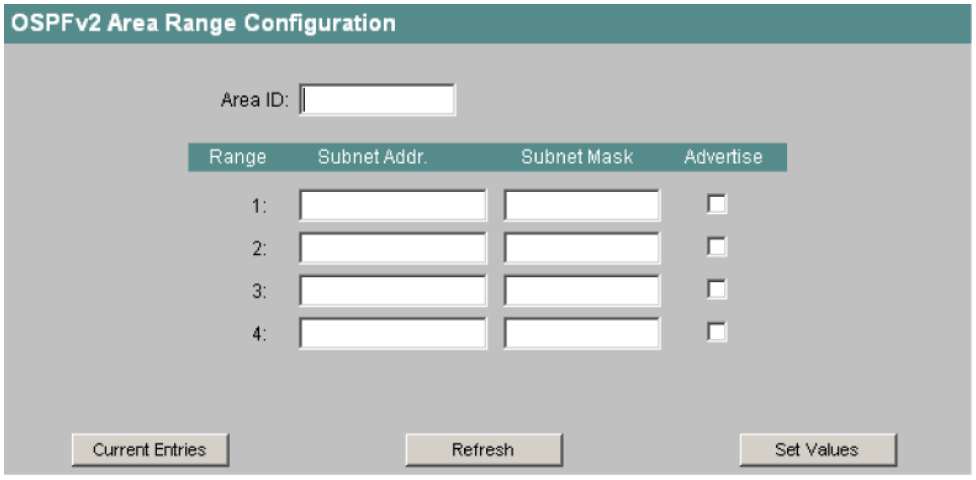


Bild 5-142 OSPFv2 Area Range Configuration

Area ID
Geben Sie hier die ID derjenigen Area ein, für die Sie einen Adressbereich anlegen wollen.

Subnet Addr.
Geben Sie hier die Adresse des Netzwerks ein, das zusammengefasst werden soll.

Subnet Mask
Geben Sie hier die Subnetzmaske des Netzwerks ein, das zusammengefasst werden soll.

Advertise
Aktivieren Sie diese Option, um das zusammengefasste Netzwerk zu propagieren.

Syntax Command Line Interface

Tabelle 5-101 OSPFv2 Area Ranges - CLI\ROUTER\OSPF\AREAS\RANGES>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen Area-Ranges an.	-
add <AreaID> <SNAddr> <SNMask> [E|D]	Fügt eine neuen Area-Range ein. • E Aktiviert Advertising Summary • D Deaktiviert Advertising Summary	Nur Administrator.
edit <AreaID> <SNAddr> <SNMask> <E|D>	Ändert eine Area-Range.	Nur Administrator.
delete <AreaID> <SNAddr> <SNMask>	Löscht eine Area-Range.	Nur Administrator.

5.7.9 OSPFv2 Interfaces

Übersicht

In diesem Menü können Sie sämtliche für OSPF konfigurierte IP Interfaces überwachen. Neben den Konfigurationsparametern können auch einige Statistikwerte in der doppelseitigen Anzeige überwacht werden.

Wählen Sie die Schaltflächen ">>" bzw. "<<", um zwischen den Seiten hin und her zu schalten.

OSPFv2 Interfaces: 1. Seite

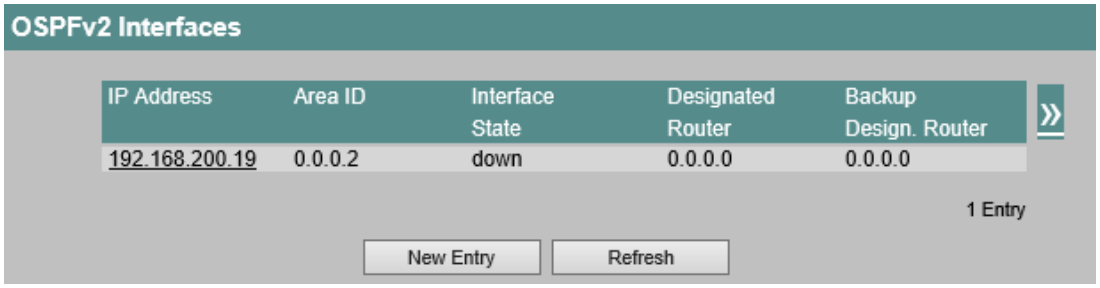


Bild 5-143 OSPFv2 Interfaces 1.Seite

IP Address
IP-Adresse des konfigurierten OSPF-Interfaces.

Area ID
Gibt die Area an, zu der dieses Interface gehört.

Interface State
Zeigt an, in welchem Status das Interface sich befindet. Dies kann sein:

- Down: Am Interface ist nichts angeschlossen
- Waiting: Hochfahren und Aushandeln des Interface
- Designated Router: Der Router ist für dieses Netzwerk hauptverantwortlich und das Network LSA wird dafür erzeugt
- Backup D. Router: Der Router ist Backup für den Designated Router
- Other: Das Interface ist hochgefahren und der Router ist weder designated noch Backup designated Router.

Designated Router
IP-Adresse des Designated Router für dieses Interface.

Backup Designated Router
IP-Adresse des Backup Designated Router für dieses Interface.

OSPFv2 Interfaces: 2. Seite

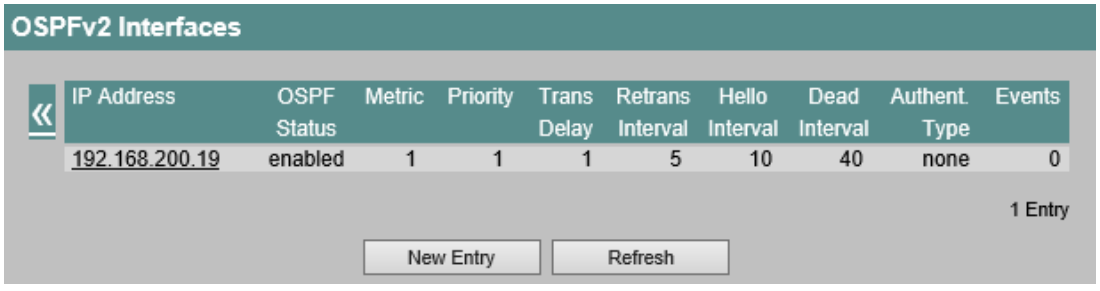


Bild 5-144 OSPFv2 Interfaces 2.Seite

IP Address:
IP-Adresse des Interfaces.

OSPF Status
OSPF Status dieses Interface. Folgende Stati sind möglich:

- Enabled: Das Interface steht für OSPF zur Verfügung.
- Disabled: Interface steht für OSPF nicht zur Verfügung.

Metric
Pfadkosten des Routers auf diesem Interface.

Priority
Priorität des Routers auf diesem Interface. Die Priorität spielt eine Rolle bei der Auswahl des Designated Router auf dem Netzwerk. Je größer die Zahl desto höher die Priorität.

Trans Delay
Geschätzte Zeit (Sekunden), die ein Link State Update Paket zur Übertragung benötigt. Bei LANs ist dieser Parameter gewöhnlich 1.

Retrans Interval
Gibt das Intervall an, nach dem Pakete, deren Empfang bei der Datenbasissynchronisation nicht bestätigt wurde, erneut übertragen werden.

Hello Interval
Gibt das Intervall an, in dem Hello Pakete gesendet werden.

Dead Interval
Gibt das Intervall an, nach dem ein Router als "nicht mehr vorhanden" klassifiziert wird, wenn keine Hello Pakete mehr von ihm empfangen wurden.

Authent. Type
Auf diesem Interface gewähltes Authentifizierungsverfahren. Zur Auswahl stehen:

- none: Keine Authentifizierung
- simple: Authentifizierung über ein Passwort
- MD5: Authentifizierung über das Keyed MD5 Verfahren

Events
Anzahl der Änderungen des Interface Status.

Anlegen eines neuen OSPFv2 Interfaces

Über die Schaltflächen "New Entry" im Menü "OSPFv2 Interfaces" kann ein neues IP Interface für OSPF konfiguriert werden.

Hinweis

Damit ein Interface als OSPF Interface angelegt werden kann, muss es vorher bereits als IP Subnetz angelegt worden sein.

Hinweis

Gehen Sie bei der Auswahl der Parameter besonders sorgfältig vor. Nur wenn auf allen Routern eines IP Subnetzes die identischen Parameter konfiguriert werden, entsteht eine korrekte Nachbarschaftsbeziehung. Andernfalls sieht es so aus, als sähen sich die Router gegenseitig nicht.

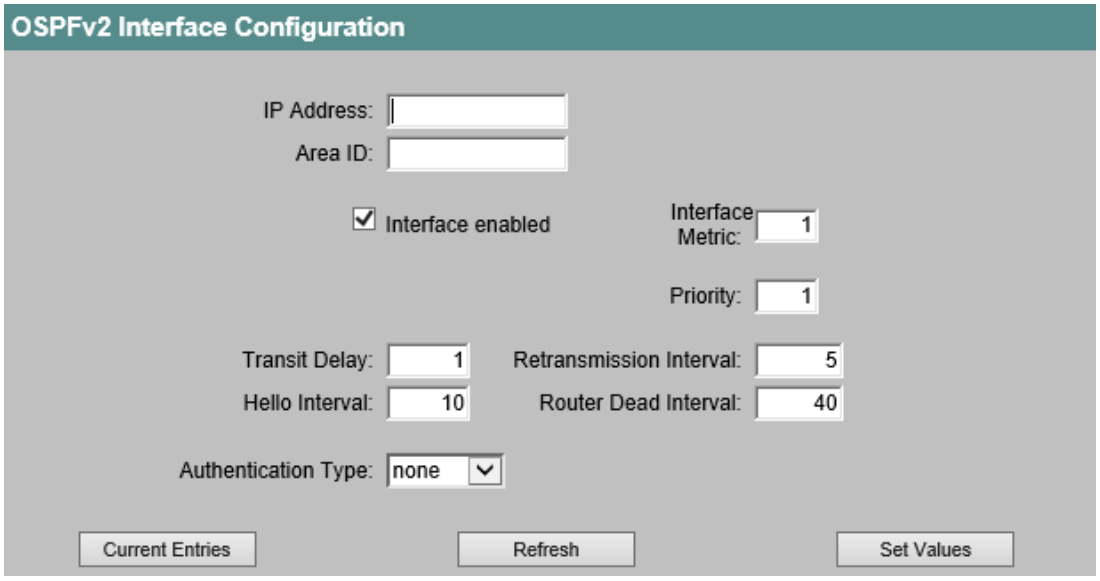


Bild 5-145 OSPFv2 Interface Configuration

IP Address
Geben Sie hier die IP-Adresse des Interface ein, das Sie konfigurieren möchten.

Area ID
Geben Sie hier die Area ID ein, zu der dieses Interface gehören soll.

Interface enabled
Aktivieren Sie diese Option, wenn Sie möchten, dass dieses Interface am OSPF Verkehr teilnimmt.

Metric
Pfadkosten des Routers auf diesem Interface. Standard ist 1. Tragen Sie hier für langsamere Netzwerke höhere Werte ein.

Priority
Geben Sie hier die Router Priorität ein. Sie spielt nur bei der Auswahl des Designated Router eine Rolle. Dieser Parameter kann auf Routern des gleichen IP Subnetzes unterschiedlich gewählt werden.

Transit Delay
Geben Sie hier die erwartete Verzögerung (Sekunden) bei dem Versenden eines Link Update Pakets an. Bei lokalen Netzwerken wird hier typischerweise 1 gewählt (Wertebereich: 1 bis 3600).

Retransmission Interval
Geben Sie hier die Zeit (Sekunden) ein, nach der ein Paket erneut übertragen wird, wenn keine Bestätigung empfangen wurde. Typischerweise wird im LAN 5 gewählt.

Hello Interval
Geben Sie hier den Abstand (Sekunden) zwischen zwei Hello Paketen an (Wertebereich: 1 bis 65.535).

Router Dead Interval
Geben Sie hier ein Intervall (Sekunden) an, nach dem ein Router als "ausgefallen" markiert wird, wenn in dieser Zeit keine Hello Pakete mehr von ihm empfangen werden.

Authentication Type
Wählen Sie hier die Authentifizierungsmethode dieses Interfaces aus. Sie können wählen zwischen:

- none: Keine Authentifizierung
- simple: Authentifizierung über ein Passwort
- MD5: Authentifizierung über das Keyed MD5 Verfahren

Key ID

Hinweis

Das Textfeld "Key ID" wird nur eingeblendet, wenn die Authentifizierungsmethode auf MD5 eingestellt wurde. Nur dort können mehrere Keys verwendet werden.

Geben Sie hier die Key ID ein, unter der das Passwort als Schlüssel verwendet wird. Da die Key ID mit dem Protokoll übertragen wird, muss bei allen benachbarten Routern der gleiche Schlüssel unter der gleichen Key ID gespeichert werden.

Passwort/Confirmation
Bei Authentifizierung über Passwort und über MD5 wird ein Key benötigt, der hier eingegeben werden kann.

Syntax Command Line Interface

Tabelle 5-102 OSPFv2 Interfaces - CLI\ROUTER\OSPF\AREAS\IFACE>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen Interfaces an.	-
add <IP> <AreaID> [E|D] [priority]	Fügt ein neues Interface ein. • E Enable Interface • D Disable Interface	Nur Administrator.
edit <IP> [AreaID] [E|D] [priority]	Ändert ein Interface. • E Enable Interface • D Disable Interface	Nur Administrator.

Befehl	Beschreibung	Kommentar
timing <IP> [<setting=value>]	Ändert die Timing-Einstellungen eines Interface. Mögliche Settings: • TD Trans. Delay • RI Retrans Interval • HI Hello Interval • DI Dead Interval	Nur Administrator.
auth <IP> <authtype> [password]	Ändert die Authentifizierung eines Interfaces Mögliche Typen: • None • Simple • MD5	Nur Administrator.
metric <IP> <metric>	Ändert die Pfadkosten eines Interfaces	Nur Administrator.
delete <IP>	Löscht ein Interface.	Nur Administrator.

5.7.10 OSPFv2 Virtual Links

Übersicht

Jeder Area Border Router (jeder Router, der in 2 oder mehr Areas angeschlossen ist), muss aus protokolltechnischen Gründen Zugang zu der Backbone Area erhalten. Ist ein solcher Router nicht direkt an der Backbone Area angeschlossen, so wird ein virtueller Link dorthin eingerichtet.

Hinweis

Virtuelle Links sind nur möglich, wenn beide Partner direkt über ein IP-Netzwerk verbunden sind und innerhalb eines Subnetzes liegen. Befindet sich ein Router zwischen den Partnern, können keine virtuellen Links angelegt werden.

In diesem Menü können die virtuellen Links überwacht werden.

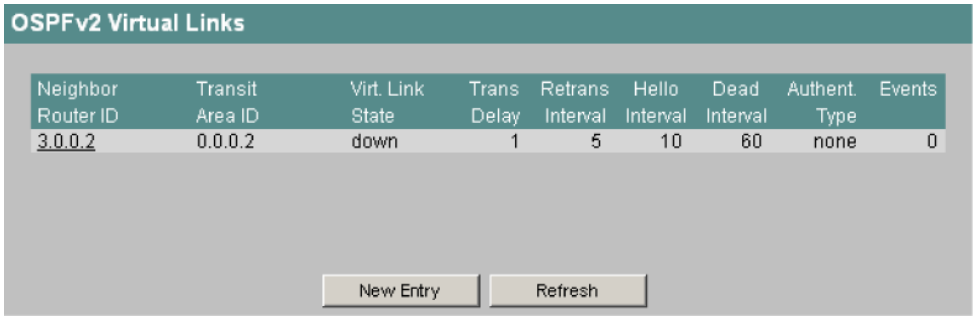


Bild 5-146 OSPFv2 Virtual Links

Neighbor Router ID
Router ID des konfigurierten Nachbarn.

Transit Area ID
Area ID derjenigen Area, über die der Router mit dem Nachbarn in virtueller Verbindung stehen soll.

Virt. Link State
Zustand in dem sich der virtuelle Link befindet. Folgende Zustände sind möglich:

- down: Der virtuelle Link kann nicht benutzt werden
- point-to-point: Der virtuelle Link kann benutzt werden

Trans Delay
Geschätzte Zeit (Sekunden), die ein Link State Update Paket zur Übertragung über den virtuelle Link benötigt.

Retrans Interval
Intervall (Sekunden), nach dem Pakete, deren Empfang nicht bestätigt wurde, erneut übertragen werden.

Hello Interval
Intervall (Sekunden), in dem Hello Pakete über den virtuellen Link gesendet werden.

Dead Interval
Intervall (Sekunden), nach dem der Nachbar-Router als "ausgefallen" klassifiziert wird, wenn von ihm keine Hello Pakete mehr empfangen wurden.

Authent. Type
Authentifizierungsmethode des virtuellen Links. Zur Auswahl stehen:

- none: Keine Authentifizierung
- simple: Authentifizierung über ein Passwort
- MD5: Authentifizierung über das Keyed MD5 Verfahren

Events
Anzahl der Änderungen des Interface Status.

Anlegen eines neuen virtuellen Links

Über die Schaltflächen "New Entry" im Menü " OSPFv2 Virtual Links " kann ein neuer virtueller Link angelegt werden.

Hinweis

Beachten Sie, dass beim Anlegen eines virtuellen Links sowohl die Transit Area als auch die Backbone Area bereits konfiguriert sein müssen.

Ein virtueller Link muss auf beiden Seiten gleich konfiguriert werden.

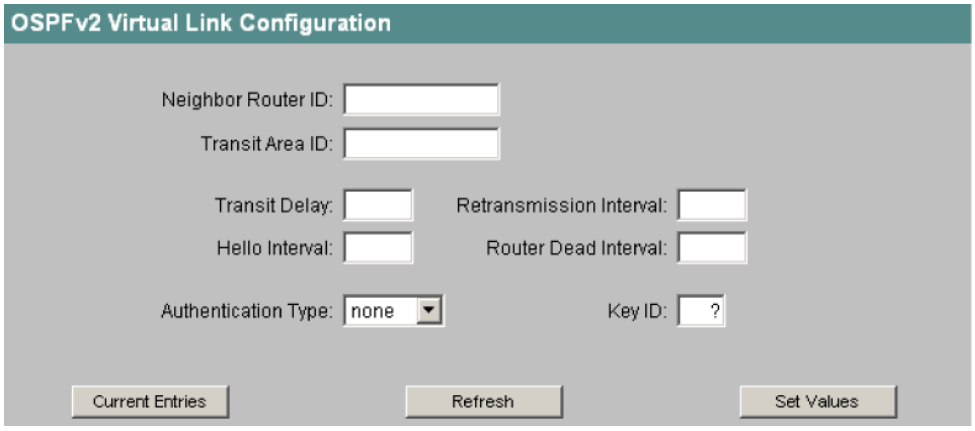


Bild 5-147 OSPFv2 Virtual Link Configuration

Neighbor Router ID
Geben Sie hier die Router ID des Partnergeräts auf der anderen Seite des virtuellen Links an.

Transit Area ID
Geben Sie hier die Area ID an, über die die beiden Partner verbunden sind.

Transit Delay
Geben Sie hier die erwartete Verzögerung (Sekunden) bei dem Versenden eines Link Update Pakets an (Wertebereich: 1 bis 3600).

Retransmission Interval
Geben Sie hier die Zeit (Sekunden) ein, nach der ein Paket erneut übertragen wird, wenn keine Bestätigung empfangen wurde (Wertebereich: 1 bis 3600).

Hello Interval
Geben Sie hier den Abstand (Sekunden) zwischen zwei Hello Paketen an (Wertebereich: 1 bis 65.535).

Router Dead Interval
Geben Sie hier ein Intervall (Sekunden) an, nach dem der Nachbar-Router als "ausgefallen" markiert wird, wenn in dieser Zeit keine Hello Pakete mehr von ihm empfangen wurden.

Authentication Type
Wählen Sie hier die Authentifizierungsmethode des virtuellen Links aus. Sie können wählen zwischen

- none: Keine Authentifizierung
- simple: Authentifizierung über ein Passwort
- MD5: Authentifizierung über das Keyed MD5 Verfahren

Key ID

Hinweis

Das Textfeld "Key ID" wird nur eingeblendet, wenn die Authentifizierungsmethode auf MD5 eingestellt wurde. Nur dort können mehrere Keys verwendet werden.

Geben Sie hier die Key ID ein, unter der das Passwort als Schlüssel verwendet wird. Da die Key ID mit dem Protokoll übertragen wird, muss bei allen benachbarten Routern der gleiche Schlüssel unter der gleichen Key ID gespeichert werden.

Passwort/Confirmation
Bei Authentifizierung über Passwort und über MD5 wird ein Key benötigt, der hier eingegeben werden kann.

Syntax Command Line Interface

Tabelle 5-103 OSPFv2 Virtual Links - CLI\ROUTER\OSPF\AREAS\VLINKS>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen virtuellen Links an.	-
add<RtrID> <AreaID> [<setting=value>]	Fügt einen neuen virtuellen Link ein. Mögliche Settings: • TD Trans. Delay • RI Retrans Interval • HI Hello Interval • DI Dead Interval	-

Befehl	Beschreibung	Kommentar
edit <RtrID> <AreaID> [<setting=value>]	Ändert einen virtuellen Link. Mögliche Settings: • TD Trans. Delay • RI Retrans Interval • HI Hello Interval • DI Dead Interval	-
auth <RtrID> <AreaID> <authtype> [password]	Ändert die Authentifizierung eines virtuellen Link. Mögliche Typen: • None • Simple • MD5	-
Delete <RtrID> <AreaID>	Löscht einen virtuellen Link.	-

Beispiel

Der Befehl

```
add 1.1.1.51 0.0.0.2
```

erstellt einen virtuellen Link zu dem Router mit der ID "1.1.1.51" über die Transit Area "0.0.0.2". Die restlichen Parameter werden auf Default-Werte eingestellt.

5.7.11 OSPFv2 Neighbors

Übersicht

Im diesem Menü können Sie die OSPF Nachbarn überwachen. Dazu gehören die dynamisch erfassten Nachbarn an den jeweiligen Netzwerken, und die konfigurierten virtuellen Nachbarn.

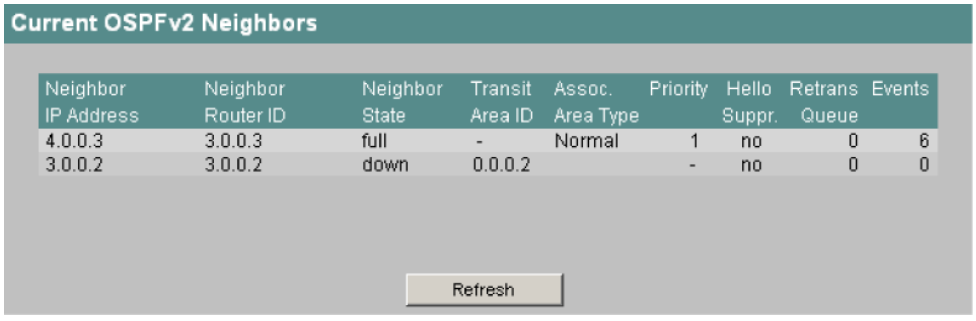


Bild 5-148 Current OSPFv2 Neighbors

Neighbor IP Address
IP-Adresse des Nachbarn auf diesem Netzwerk.

Neighbor Router ID
Router ID des Nachbarn. Beide Adressen können übereinstimmen.

Neighbor State
Status des Nachbarn. Der Status kann folgende Werte annehmen:

- down: Der Nachbar ist nicht erreichbar
- attempt und init: Kurzlebige Stati während der Initialisierung
- two-way: Beiderseitiger Empfang von Hello Paketen
- exchangestart, exchange und loading: Stati während des Austausches der Link State Database
- full: Zustand, wenn die Datenbasen synchron sind.

Hinweis

Der Status "full" ist der Normalzustand mit einem stabilen Nachbarn, wenn einer der Partner ein Designated Router oder ein Backup Designated Router ist. Andernfalls ist der Zustand "two-way" der stabile Normalzustand.

Transit Area ID
Transit Area ID des Nachbarn, sofern dieser virtuell ist.

Assoc. Area Type
Status der Area über die die Nachbarschaftsbeziehung besteht. Es gibt folgende Area Typen:

- Normal
- Stub
- NSSA

Priority
Router Priorität des Nachbarn. Diese ist nur während der Auswahl des Designated Router auf einem Netzwerk von Bedeutung. Bei virtuellen Nachbarn ist diese Angabe nicht relevant.

Hello Suppr.
Anzeige unterdrückter Hello Pakete zum Nachbarn. Dieses Feld steht normalerweise auf "no".

Retrans Queue
Länge der Warteschlange mit den noch zu übertragenden Paketen.

Events
Anzahl der Statusänderungen.

Hinweis

Der Status "full" ist der Normalzustand mit einem stabilen Nachbarn, wenn einer der Partner ein Designated Router oder ein Backup Designated Router ist. Andernfalls ist der Zustand "two-way" der stabile Normalzustand.

Syntax Command Line Interface

Tabelle 5-104 OSPFv2 Neighbors - CLI\ROUTER\OSPF>

Befehl	Beschreibung	Kommentar
neighbrs	Zeigt die aktuellen Nachbarn an.	-

5.7.12 OSPFv2 State Database

Übersicht

Die Link State Database ist die zentrale Datenbank zur Verwaltung aller Links innerhalb einer Area. Sie besteht aus den sogenannten Link State Advertisements (LSAs). Die wichtigsten Daten dieser LSAs werden in diesem Menü angezeigt.

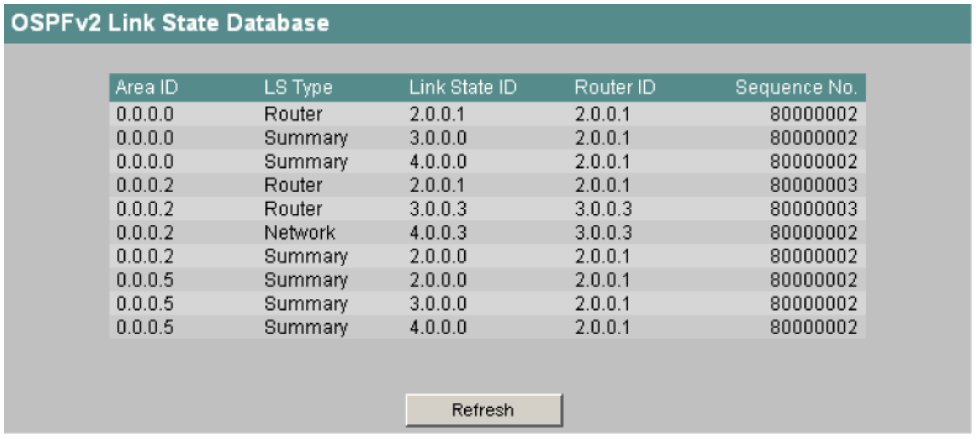


Bild 5-149 OSPFv2 Link State Database

Area ID
Area ID zu der dieses Link State Advertisement (LSA) gehört.

LS Type
Typ des LSA. Dieser kann sein:

- Router
- Network
- Summary
- ASBR (Autonomous System Border Router).

Link State ID
Eindeutige ID des LSA.

Router ID
Router der dieses LSA erzeugt hat.

Sequence No.
Sequenznummer des LSA. Mit jeder Erneuerung eines LSA wird diese Sequenz-Nummer um eins hoch gezählt.

Syntax Command Line Interface

Tabelle 5-105 OSPFv2 State Database - CLI\ROUTER\OSPF>

Befehl	Beschreibung	Kommentar
lnkstate	Zeigt die aktuelle Links State Tabelle an.	-

Hinweis

Weitere Informationen zu den LSAs finden Sie im Kapitel Konfiguration und Diagnose über SNMP.

5.7.13 VRRP

Einleitung

In den Untermenüs des Menüs "VRRP" können Sie Einstellungen der VRRP-Parameter vornehmen.

Das VRRP führt Redundanz in das IPv4-Netzwerk ein. Hierbei können verschiedene IP Router die Routing Funktionalität eines anderen übernehmen, wenn der eigentliche Router ausfällt. Dazu werden mehrere Router auf einem IP Subnetz zu einem virtuellen Router zusammengefasst. Diesem virtuellen Router wird eine Liste von IPv4 Adressen zugeordnet, für die der jeweilige Master die Routing-Funktionalität übernimmt.

5.7.14 VRRP Virtual Routers

Einleitung

In diesem Menü können Sie die virtuellen Router dieses Systems überwachen.

Über die Schaltfläche "New Entry" können Sie neue virtuelle Router angelegen.
Maximal sind 32 Virtuelle Router konfigurierbar.

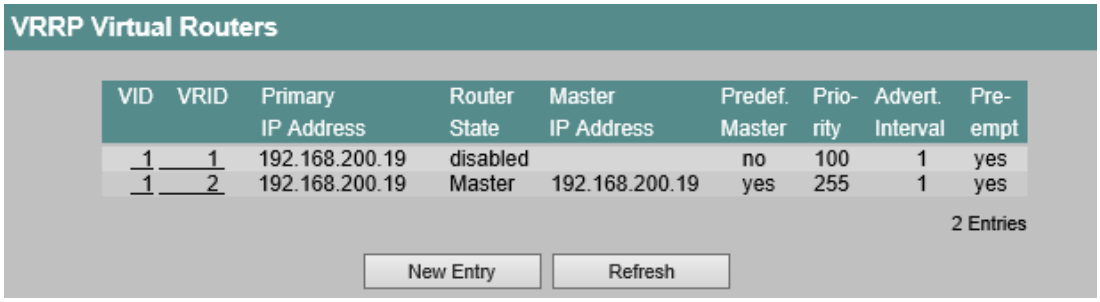


Bild 5-150 VRRP Virtual Routers

VID
VLAN ID des Subnetzes. Die hierfür eingerichteten IP-Adressen mit allen Subnetzparametern findet man im Menü "Router Subnets"

VRID
In dieser Spalte wird die ID des virtuellen Routers angezeigt. Diese ID muss für dieses VLAN eindeutig vergeben sein. Gültige Werte sind 1..255.

Primary IP Address
In dieser Spalte wird die vorrangige IP-Adresse auf diesem VLAN angezeigt. Der Eintrag 0.0.0.0 bedeutet, dass die kleinste Adresse auf diesem VLAN verwendet wird. Ansonsten sind alle IP-Adressen, die auf diesem VLAN in dem Menü "Router Subnets" konfiguriert wurden, gültige Werte.

Router State
In dieser Spalte wird der derzeitige Zustand des virtuellen Routers angezeigt. Mögliche Werte sind:

- Master: Dieser Router übernimmt die Routingfunktionalität für alle zugeordneten IP-Adressen.
- Backup: Derzeit übernimmt ein anderer Router die Routing Funktionalität und ist im Zustand "Master". Der angezeigte Router übernimmt die Redundanzfunktion und ist bereit beim Ausfall des Masters zu übernehmen.
- Disabled: Dieser Router wurde vom Administrator ausgeschaltet. Er übernimmt keine Routerredundanz mehr.
- Initialize: Der virtuelle Router wurde soeben eingeschaltet. In kurzer Zeit wird er in den Zustand "Master" oder "Backup" wechseln.
- Invalid: Die Konfiguration dieses virtuellen Routers ist ungültig. Bitte überprüfen Sie die Konfiguration.

Master IP Address
In dieser Spalte wird die IP-Adresse des Routers angezeigt, der derzeitig die Routingfunktionalität übernimmt.

Predef. Master
In dieser Spalte wird angezeigt, ob mindestens eine redundante Router Adresse diesem IE-Switch X-400 gehört. In diesem Fall ist die Priorität mit 255 vorgeschrieben und der IE-Switch X-400 geht beim Einschalten sofort in den Zustand "Master" über.

Priority
In dieser Spalte wird die Priorität des virtuellen Routers angegeben. Gültige Werte sind 1.255. Die 255 ist für den Eigentümer der redundanten Router Adressen vorgesehen. Alle anderen

Prioritäten können frei auf die redundanten Router verteilt werden. Je größer eine Priorität ist, desto eher wird der Router zum "Master".

Advert. Interval
In dieser Spalte wird der Abstand angezeigt, in dem der Master Router seine Advertisement Pakete verschickt.

Preempt
Diese Spalte gibt an, ob ein Router mit höherer Priorität einen anderen Router mit niedriger Priorität unterbrechen soll.

Anlegen oder Ändern eines virtuellen Routers

Über die Schaltfläche "New Entry" im Menüpunkt "VRRP Virtual Routers" können Sie einen neuen virtuellen Router angelegen.

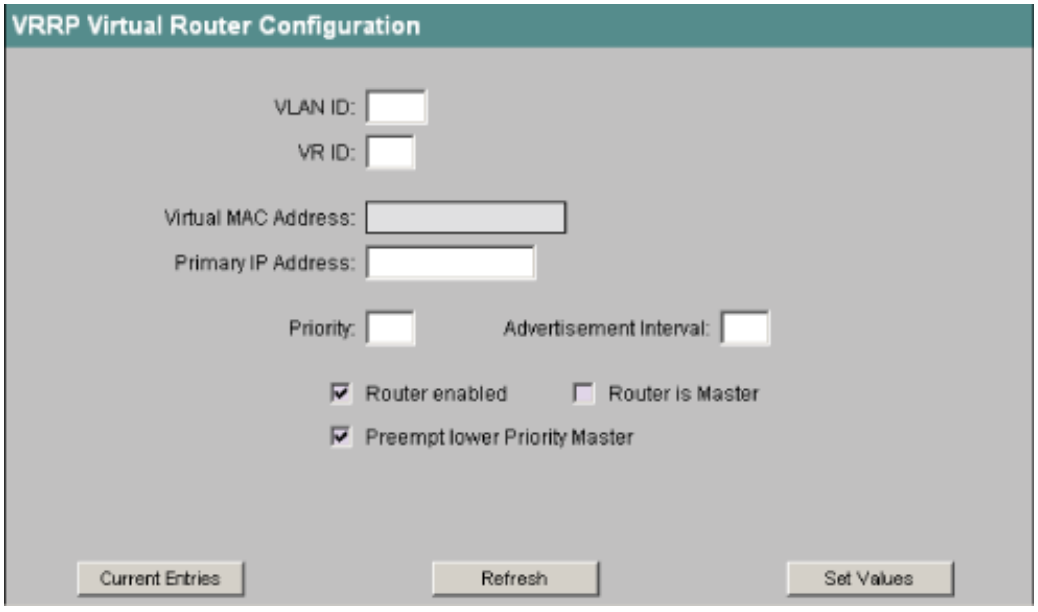


Bild 5-151 VRRP Virtual Router Configuration

VLAN ID
Tragen Sie hier das VLAN ein, auf dem der virtuelle Router agieren soll. Gültige Werte sind alle ID von VLANs, die über mindestens ein konfiguriertes IP-Subnetz verfügen.

VR ID
Tragen Sie hier die ID des virtuellen Routers ein. Sie muss auf dem angeschlossenen LAN eindeutig vergeben sein.

Virtual MAC Address
Aus der ID des virtuellen Routers und einem festen Prefix ermittelt sich die virtuelle MAC-Adresse automatisch.

Primary IP Address
Tragen Sie hier die Adresse ein, die als IP Quell-Adresse verwendet werden soll, sobald dieser virtuelle Router in den Zustand "Master" übergeht.

Hinweis

Haben Sie auf diesem VLAN nur ein IP-Subnetz konfiguriert ist keine Angabe erforderlich (Eintrag 0.0.0.0). Haben Sie aber mehrere IP-Subnetze auf diesem VLAN konfiguriert und Sie möchten, dass eine bestimmte Adresse als Quelladresse für VRRP Pakete genutzt wird, sollten Sie dies hier eintragen. Ansonsten wird die numerisch kleinste IP-Adresse verwendet.

Priority
Tragen Sie hier die Priorität dieses virtuellen Routers ein. Gültige Werte sind 1..255. Die 255 ist für den Eigentümer der Router Adressen vorgesehen. Alle anderen Prioritäten können frei auf die redundanten Router verteilt werden. Je größer eine Priorität ist, desto eher wird der Router zum "Master".

Advertisement Interval
Tragen Sie hier das Zeitintervall in Sekunden ein, nach welchem ein Router im Zustand "Master" erneut ein Advertisement Paket verschickt.

Router enabled
Tragen Sie hier ein, ob der Router am VRRP Protokoll teilnehmen soll.

Router is Master
Tragen Sie hier ein, ob der Router von vorneherein im Zustand "Master" sein soll. In diesem Fall wird die Primary IP-Adresse gleich zu den Router Adressen hinzugefügt.

Prempt lower Priority Master
Tragen Sie hier ein, ob dieser Router einen anderen mit niedrigerer Priorität unterbrechen darf.

Syntax Command Line Interface

VRRP - CLI\VRRP\ROUTERS>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuellen virtuellen Router an.	-
add <VID> <VRID>	Fügt einen neuen virtuellen Router ein.	Nur Administrator.
status <VID> <VRID> <E|D>	Aktiviert/Deaktiviert einen virtuellen Router	Nur Administrator.
master <VID> <VRID> <E|D>	Legt fest, ob der virtuellen Router Master ist.	Nur Administrator.
preempt <VID> <VRID> <E|D>	Legt fest, ob höherpriore Router unterbrechen dürfen.	Nur Administrator.
primip <VID> <VRID> <IP>	Ändert die primäre IP-Adresse eines virtuellen Routers.	Nur Administrator.
priority <VID> <VRID> <0..255>	Ändert die Priorität eines virtuellen Routers.	Nur Administrator.

Befehl	Beschreibung	Kommentar
advint <VID> <VRID> <0..255>	Ändert das Zeitintervall für den Versand von Advertisement Paketen eines virtuellen Routers.	Nur Administrator.
delete <VID> <VRID>	Löscht einen virtuellen Router.	Nur Administrator.

5.7.15 VRRP Associated IP Adresses

Einleitung

In diesem Menüpunkt können Sie die redundanten IP Adressen der virtuellen Router einsehen.

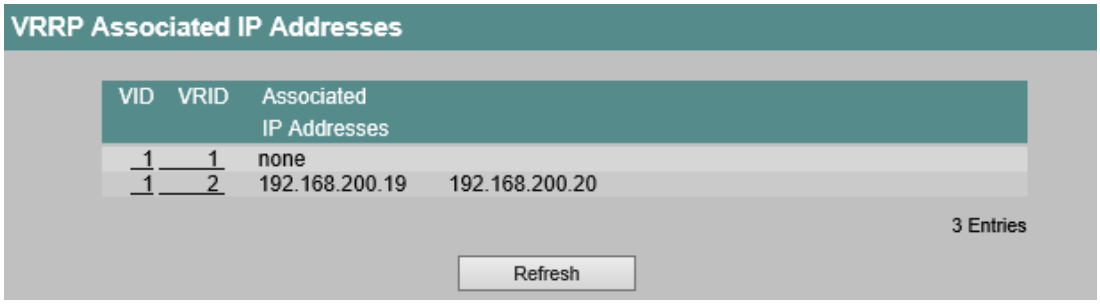


Bild 5-152 VRRP Associated IP Addresses

VID
VLAN ID des Subnetzes. Die hierfür eingerichteten IP-Adressen mit allen Subnetzparametern findet man im Menü "Router Subnets"

VRID
In dieser Spalte wird die ID des virtuellen Routers angezeigt. Diese ID muss für dieses VLAN eindeutig vergeben sein. Gültige Werte sind 1..255.

Associated IP Addresses
In dieser Spalte werden die Router IP Adressen angezeigt, die durch diesen virtuellen Router überwacht werden. Wenn ein Router die Rolle des Masters übernimmt, wird die Routing Funktion all dieser IP-Adressen durch diesen Router übernommen.

Anlegen oder ändern der überwachten IP Adressen

Über den hinterlegten Link der beiden ersten Spalten können Sie IP-Adressen, die überwacht werden sollen hinzufügen, ändern oder löschen.

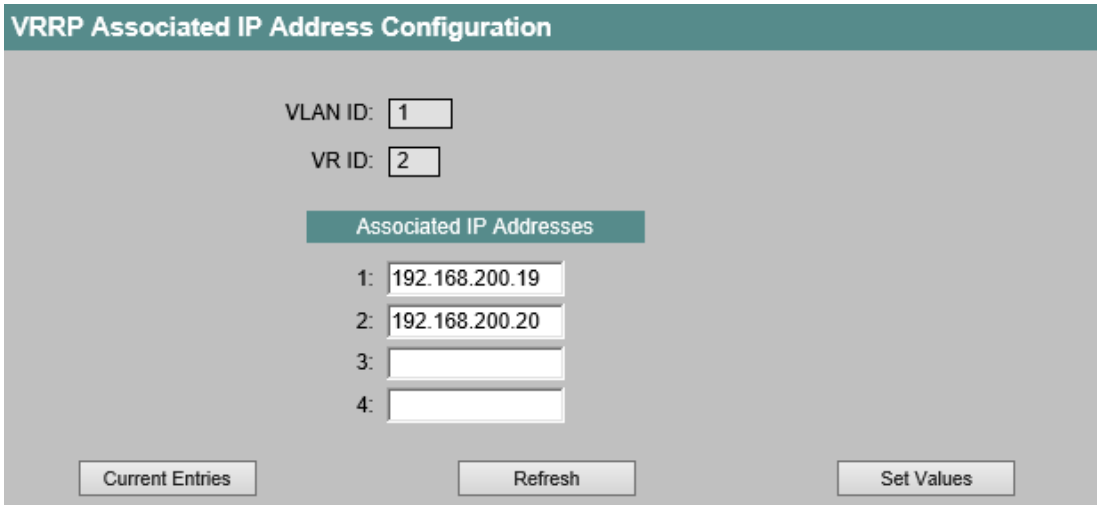


Bild 5-153 VRRP Associated IP Address Configuration

VLAN ID
Zeigt das VLAN an auf dem sich der konfigurierte virtuelle Router befindet.

VR ID
Zeigt die ID dieses virtuellen Routers an.

Textfeld 1:, Textfeld 2:, Textfeld 3: Textfeld 4:
Tragen Sie hier die redundanten IP Adressen ein, die dieser virtuelle Router überwachen soll.

Syntax Command Line Interface

VRRP - CLI\ROUTER\VRRP\ADDR>

Befehl	Beschreibung	Kommentar
info	Zeigt die aktuell überwachten IP-Adressen an.	-
add <VID> <VRID> <IP>	Fügt eine neue zu überwachende IP-Adresse ein.	Nur Administrator.
delete <VID> <VRID> <IP>	Löscht eine überwachte IP-Adresse.	Nur Administrator.

5.7.16 VRRP Statistics

Einleitung

In diesem Menüpunkt können Sie die Statistiken des VRRP Protokolls und aller konfigurierten virtuellen Router einsehen.

Über die Schaltfläche "Reset Counters" können die Statistiken auf 0 zurückgesetzt werden.

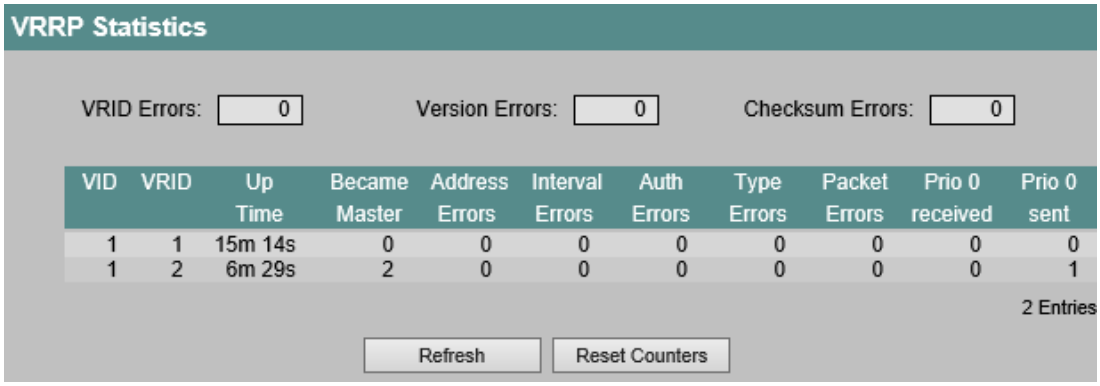


Bild 5-154 VRRP Statistics

VRID Errors
Zeigt die Anzahl der empfangenen VRRP Pakete an, die eine nicht unterstütze VRID enthalten haben.

Version Errors
Zeigt die Anzahl der empfangenen VRRP Pakete an, die eine ungültige Versionsnummer enthalten haben.

Checksum Errors
Zeigt die Anzahl der empfangenen VRRP Pakete an, die eine ungültige Prüfsumme enthalten haben.

VID
VLAN ID des Subnetzes. Die hierfür eingerichteten IP-Adressen mit allen Subnetzparametern findet man im Menü "Router Subnets"

VRID
In dieser Spalte wird die ID des virtuellen Routers angezeigt. Diese ID muss für dieses VLAN eindeutig vergeben sein. Gültige Werte sind 1..255.

Up Time
Diese Spalte gibt an, zu welchem Zeitpunkt der virtuelle Router in Betrieb genommen wurde.

Hinweis

Das MIB Objekt "vrrpOperVirtualRouterUpTime" stellt den Zeitpunkt dar, zu dem der virtuelle Router eingeschaltet wurde. Der Übersichtlichkeit halber zeigt die Spalte "Up Time" an, wie lange der virtuelle Router bereits eingeschaltet ist.
Genauer gesagt wird in der Spalte "Up Time" die Differenz aus der derzeitigen sysUpTime und dem MIB Objekt angezeigt.

Became Master
Gibt an, wie häufig diese virtuelle Router in den Zustand "Master" ging.

Address Errors
Gibt an, wie häufig eine Paket empfangen wurde, das eine falsche Adressliste enthalten hat.

Interval Errors
In dieser Spalte wird die Anzahl der fehlerhaft empfangenen Pakete angezeigt, deren Advertisement Intervall nicht mit dem lokal gesetzten Wert übereinstimmt.

Auth Errors
In dieser Spalte wird die Anzahl der fehlerhaft empfangenen Pakete angezeigt, deren Authentifizierungstyp nicht Typ 0 war. Typ 0 ist der einzige akzeptable Typ und bedeutet "keine Authentifizierung"

Hinweis

Die Spalte "Auth Errors" ist die Summe der MIB Objekte "vrrpStatsInvalidAthType" und "vrrpStatsAuthTypeMismatch."

Type Errors
In dieser Spalte wird die Anzahl der fehlerhaft empfangenen Pakete angezeigt, deren VRRP Typ nicht korrekt gesetzt war.

Packet Errors
In dieser Spalte wird die Anzahl der fehlerhaft empfangenen Pakete angezeigt. Hierbei werden sowohl Pakete gezählt, deren Länge nicht korrekt war als auch Pakete, deren TTL Wert im IP Header nicht stimmte.

Hinweis

Die Spalte "Packet Errors" ist die Summe der MIB Objekte "vrrpStatsPacketLengthErrors" und "vrrpStatsIpTtlErrors."

Prio 0 received
Gibt an, wie viele Pakete mit der Priorität 0 empfangen wurden. Pakete mit der Priorität 0 werden versendet, wenn ein Master Router heruntergefahren wird. Diese Pakete ermöglichen dann eine schnelle Übergabe an den entsprechenden Backup Router.

Prio 0 sent
Gibt an, wie viele Pakete mit der Priorität 0 versendet wurden. Pakete mit der Priorität 0 werden versendet, wenn ein Master Router heruntergefahren wird. Diese Pakete ermöglichen dann eine schnelle Übergabe an den entsprechenden Backup Router.

Syntax Command Line Interface

VRRP - CLI\ROUTER\VRRP\STAT

Befehl	Beschreibung	Kommentar
Info	Zeigt die VRRP-Statistiken an.	-
resetc	Setzt die Statistiken auf 0 zurück.	Nur Administrator.

Konfiguration und Diagnose über SNMP

6

Konfiguration eines IE-Switches über SNMP

Über SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) kann eine Netzwerkmanagementstation SNMP-fähige Teilnehmer wie z.B. einen IE-Switch konfigurieren und überwachen. Hierzu ist im Teilnehmer ein Management-Agent installiert, mit dem die Managementstation über sogenannte Get- und Set-Requests Daten austauscht. Die IE-Switch unterstützt SNMPvV1, SNMPv2 und SNMPv3.

Die konfigurierbaren Daten sind im IE-Switch in einer Datenbasis, der sogenannten MIB (**M**anagement **I**nformation **B**ase) abgelegt, auf die die Management-Station oder das Web Based Management zugreifen.

Hinweis

Nur die über WBM und CLI möglichen Einstellungen sind freigegeben

Im Gegensatz zur Konfiguration über WBM oder CLI findet bei der Konfiguration über SNMP keine oder nur eine eingeschränkte Plausibilitäts- und Konsistenzüberprüfung der Gerätekonfiguration statt. Eine fehlerhafte Gerätekonfiguration kann zu Datenverlust und einer Beeinträchtigung des gesamten Netzwerks führen.

Getestet und freigegeben sind nur solche Konfigurationseinstellungen, die Sie über WBM oder CLI vornehmen können.

SIMATIC NET SNMP OPC Server

Der SNMP OPC-Server stellt die SNMP-Informationen von TCP/IP-Netzwerken mit SNMP (Simple Network Management Protocol) auf der OPC Schnittstelle zur Verfügung. Mit Hilfe des SNMP OPC-Server können beliebigen OPC-Client-Systeme (wie z.B. WinCC) nun auf Diagnose- und Parameterdaten SNMP-fähiger Komponenten zugreifen.

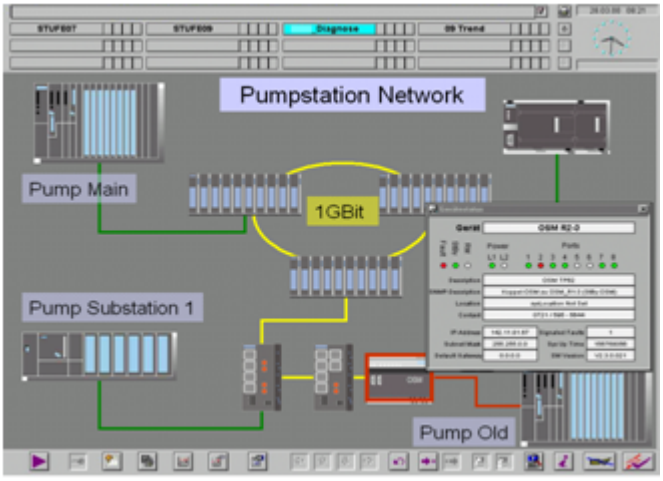


Bild 6-1 WinCC-Beispiel für Netzwerkdiagnose mit dem SIMATIC NET SNMP-OPC Server

Zusätzlich können auch Komponenten ohne SNMP-Fähigkeit über ihre IP-Adresse in die Anlagenvisualisierung aufgenommen werden. Es lassen sich dadurch z.B. neben einfacher Gerätediagnose auch Detailinformationen wie redundante Netzstrukturen oder Netzlastverteilungen kompletter TCP/IP-Netzwerke darstellen. Durch die zusätzliche Überwachung dieser Daten können Geräteausfälle schnell erkannt und lokalisiert werden. Dies erhöht die Betriebssicherheit und verbessert die Anlagenverfügbarkeit. Sie projektieren mit STEP 7 (alternativ NCM PC), welche Geräte der SNMP OPC-Server überwacht.

Weitere Informationen zum SNMP OPC-Server von SIMATIC NET stehen unter folgendem Link zur Verfügung:

SNMP OPC Server (http://www.automation.siemens.com/mcms/industrial-communication/de/ie/software/netzwerkmanagement/snmp-opc-server/Seiten/snmp-opc-server.aspx)

SNMP OPC MIB-Compiler und Profildateien

Der Umfang der Information, die von den jeweiligen Geräten mit dem SNMP OPC-Server überwacht werden, bestimmt das jeweilige Geräteprofil. Durch den integrierten MIB-Compiler können vorhandene Profile geändert bzw. neue Geräteprofile für beliebige SNMP fähige Geräte erzeugt werden.

Der MIB-Compiler des SNMP-OPC-Servers benötigt MIB Dateien nach dem SMIv1-Standard. Sie benötigen deshalb eine geänderte Version der privaten SMIv2 MIB-Datei des IE-Switches. Die SMIv1 MIB des IE-Switches sowie ein fertiges Geräteprofil steht Ihnen unter folgendem Link zum Download zur Verfügung:

Private MIBs (http://support.automation.siemens.com/WW/view/de/22015045) (Beitrags-ID: 22015045)

Standard MIBs

Bei MIBs wird zwischen standardisierten MIBs, die in sogenannten RFCs definiert sind, und privaten MIBs unterschieden. Private MIBs enthalten produktspezifische Erweiterungen, die in Standard MIBs nicht erfasst sind.

Ein IE-Switch unterstützt folgende MIBs:

- RFC 1213: MIB II (Alle Gruppen außer egp and transmission)
- RFC 2233: Interface MIB (Conformance Group 4, 5, 6, 7, 10, 11, 13)
- RFC 1286, RFC 1493: Bridge-MIB (dot1dBase und dot1dStp)
- RFC 1724: RIP Version 2 MIB Extension (SCALANCE X414-3E)
- RFC 1757: RMON-MIB (statistics, history, alarm, event)
- RFC 1850: OSPF Version 2 Management Information Base (SCALANCE X414-3E)
- RFC 2665: EtherLike-MIB (dot3StatsTable für SMIv2)
- RFC 2674p: P-BRIDGE-MIB (Conformance Group 1, 2, 3, 4, 6, 8, 9)
- RFC 2674q: Q-BRIDGE-MIB (Conformance Group 1, 3, 4, 6, 7, 8, 5 teilweise)
- RFC 1907: SNMPv2-MIB (Conformance Group 5, 6, 7, 8, 9)
- RFC 2571: SNMP-FRAMEWORK-MIB (SNMPv3 MIB: Conformance Group 1)
- RFC 2572: SNMP-MPD-MIB (SNMPv3 MIB: Conformance Group 1)
- RFC 2573: SNMP-NOTIFICATION-MIB
  (SNMPv3 MIB: Conformance Group 1, 2)
- RFC 2573: SNMP-PROXY-MIB
- RFC 2573: SNMP-TARGET-MIB (SNMPv3 MIB: Conformance Group 1, 2, 3)
- RFC 2574: SNMP-USER-BASED-SM-MIB
  (SNMPv3 MIB: Conformance Group 1)
- RFC 2575: SNMP-VIEW-BASED-ACM-MIB
  (SNMPv3 MIB: Conformance Group 1)
- RFC 2787: VRRP-MIB (Virtual Router Redundancy Protocol; nur SCLANCE X414-3E)

Private MIB

Informationen über die Private MIB des IE-Switches finden Sie im Anhang B dieses Handbuchs.

Zugriff auf die Private MIB-Datei eines IE-Switch

Führen Sie folgende Schritte durch, um auf die Private MIB-Datei eines IE-Switches zuzugreifen.

1. Öffnen Sie das Web Based Management.
2. Wählen Sie den Menüpunkt "System -> Save & Load HTTP"
3. Klicken Sie auf den Button "Save Private MIB".
4. Sie werden aufgefordert einen Speicherort und einen Namen für die Datei zu wählen bzw. den vorgeschlagenen Dateinamen zu übernehmen.

PROFINET IO-Funktionalität 7

7.1 Projektieren mit PROFINET IO

Einsatz von PROFINET IO

Eine Möglichkeit der Diagnose, Parametrierung und Generierung von Alarmmeldungen der angeschlossenen IE-Switches ist der Einsatz von PROFINET IO.

Hier wird gezeigt, wie die Möglichkeiten von PROFINET IO für einen angeschlossenen IE-Switch genutzt werden können.

Im folgenden Beispiel wird davon ausgegangen, dass bereits ein PROFNET IO-Controller V2 mit PROFINET IO-Strang projektiert ist (siehe auch PROFINET IO-Systemhandbuch).

Hinweis

Es wird Step 7 V5.4 SP5 oder eine neuer Version benötigt.

Im Folgenden wird am SCALANCE X-400 exemplarisch eine Hardwarekonfiguration mit PROFINET IO-Strang dargestellt.

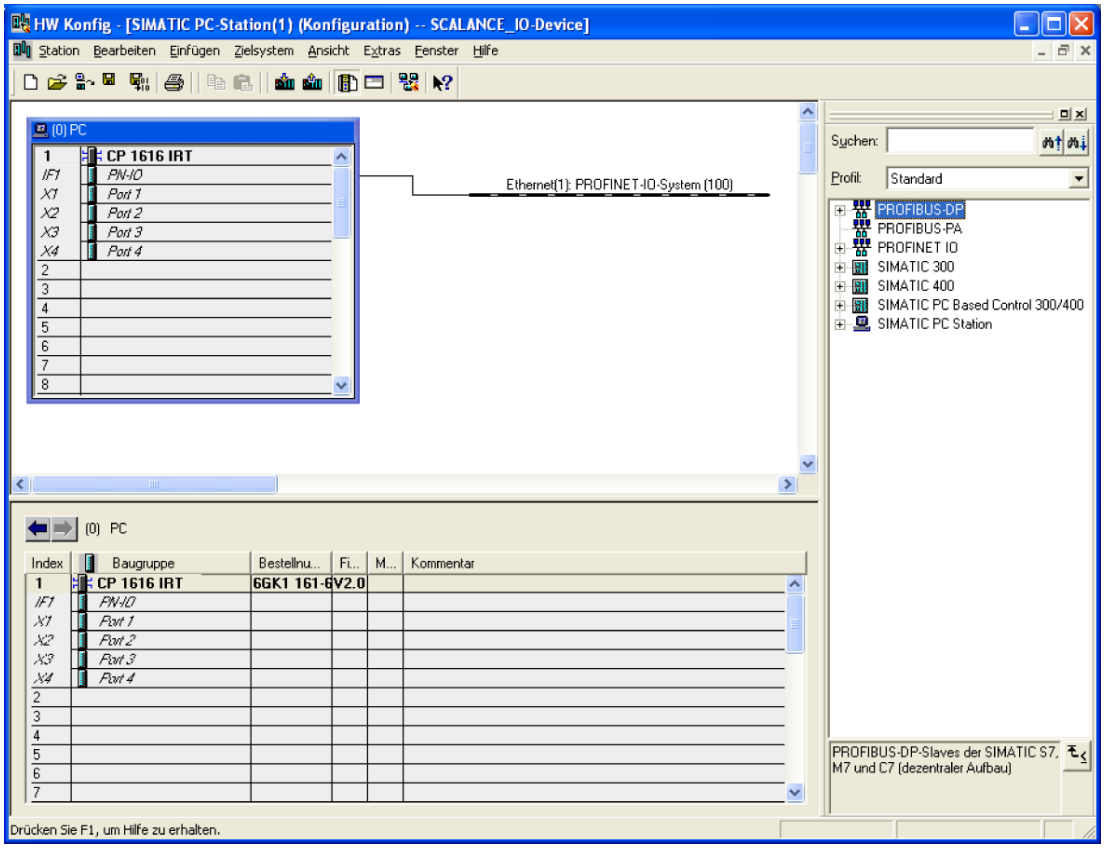


Bild 7-1 HW-Konfig PROFNET IO, Aufbau der Station

Anbindung der IE-Switches

Um die einzelnen IE-Switches als PN IO Device anzubinden, ist es erforderlich, dass die IE-Switches im Baugruppenkatalog unter PROFINET IO vorhanden sind.

Vorgehen

Sollten die Geräte in STEP 7 noch nicht aufgenommen sein, gehen Sie wie folgt vor:

1. Wählen Sie in der Maske HW Konfig > Extras "GSD Dateien installieren".
   Folgende Maske erscheint:

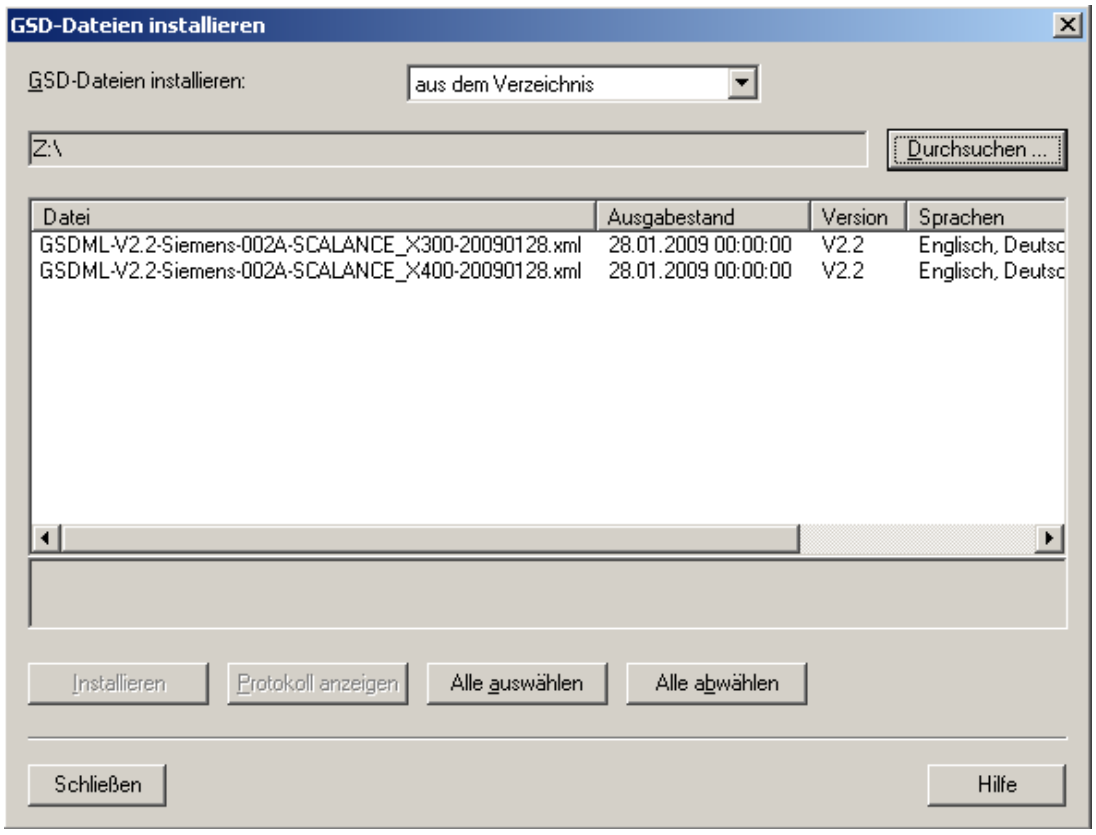


Bild 7-2 GSD-Dateien installieren

2. Navigieren Sie über "Durchsuchen" zu der mitgelieferten xml Datei (z. B. GSDML-Vx.x-Siemens-002A-SCALANCE_X400-JJJJMMTT.xml - J, M und T stehen für das Ausgabedatum der Datei).

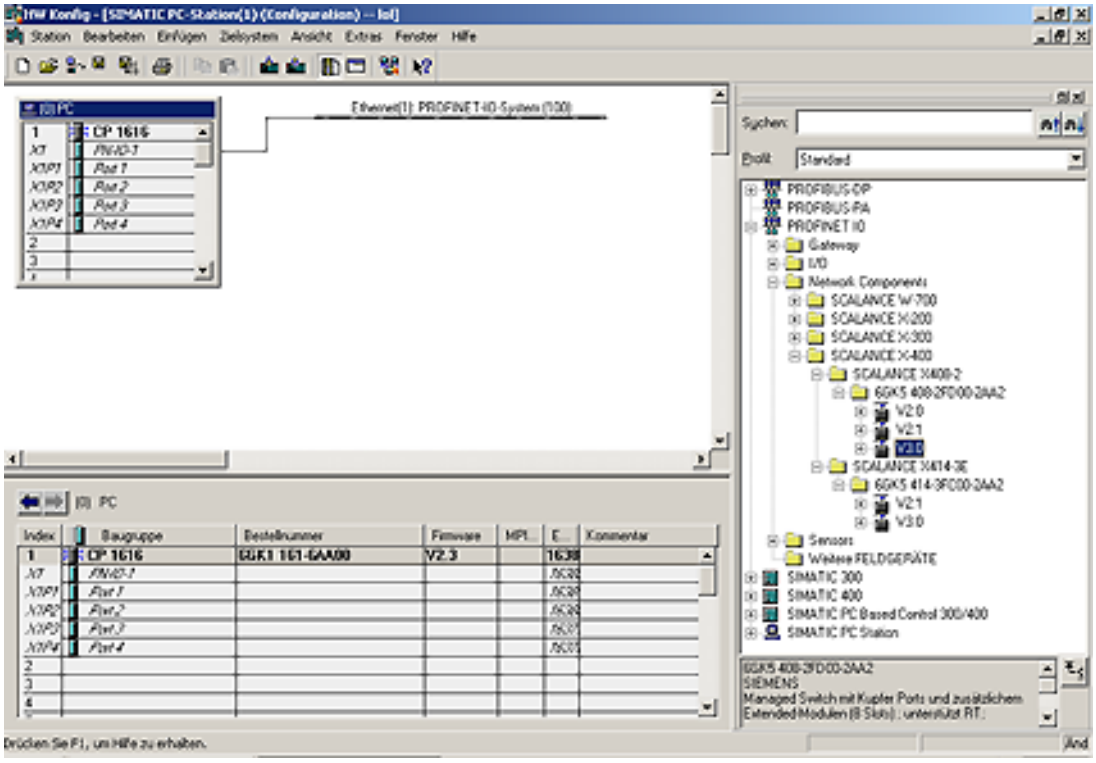


Bild 7-3 HW Konfig PROFINET IO SCALANCE Switch einfügen

3. Übernehmen Sie anschließend die Datei mit "Installieren".
   Damit sind die IE-Switches im Baugruppenkatalog aufgenommen (siehe Baugruppenkatalog im folgenden Bild).

4. Entnehmen Sie dem HW Katalog den gewünschten IE-Switch – hier beispielhaft SCALANCE X408-2 (PROFINET IO > Network Components > SCALANCE X-400 Switches > SCALANCE X408-2). Fügen Sie den selektierten SCALANCE per Drag&Drop in das PROFINET IO System ein.

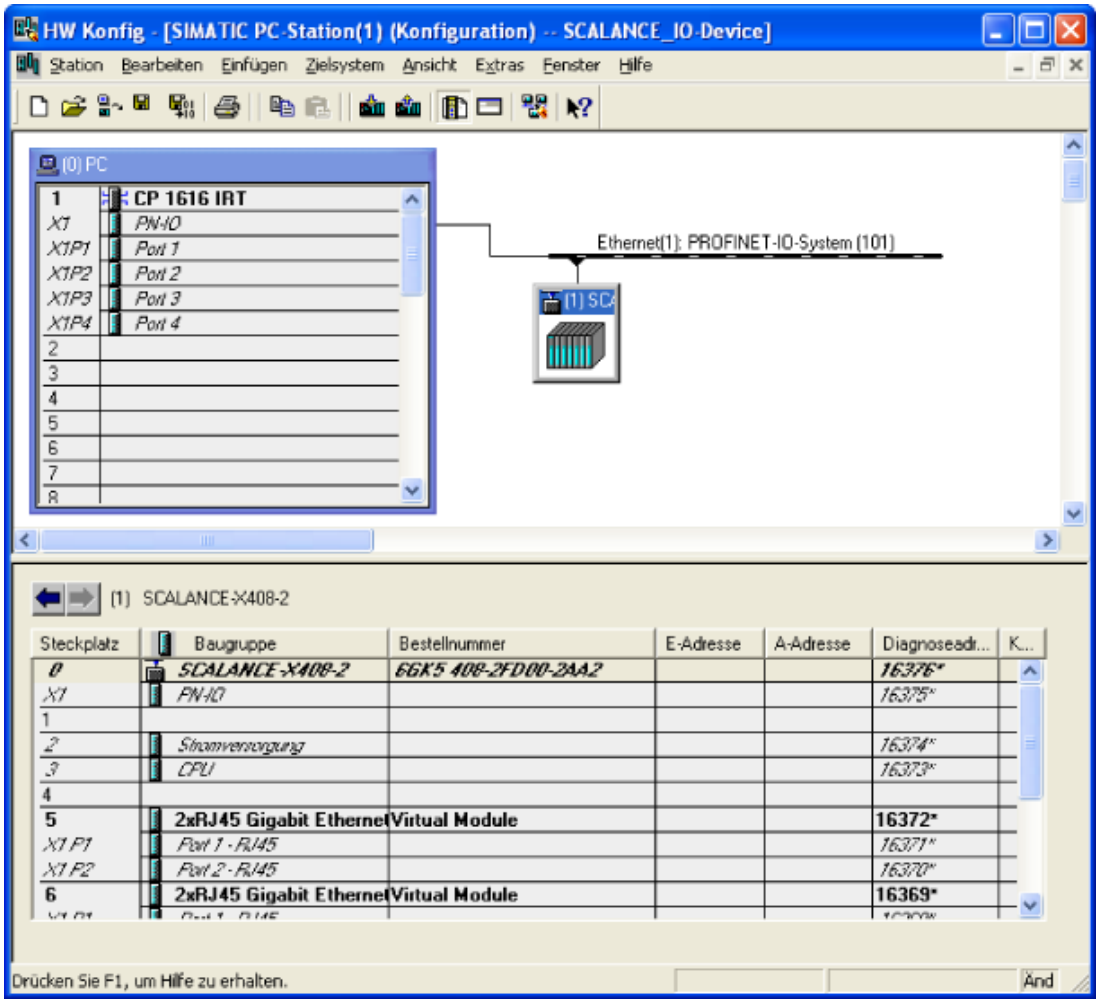


Bild 7-4 HW Konfig PROFINET IO Einstellung globaler Parameter

5. Klicken Sie auf das Icon "(1)SCALANCE", so dass im unteren Bildteil die Steckplätze des IE-Switches dargestellt werden. Durch einen Doppelklick auf den Steckplatz 0 können die globalen Parameter des IE-Switches (Stellvertretermodul) eingestellt werden (siehe Bild).
6. Mit einem Doppelklick auf einen Steckplatz, können Sie die dazugehörigen Eigenschaften aufrufen und einstellen.

7. Klicken Sie auf die Steckplätze der Ports, um die portspezifischen Parameter einzustellen.

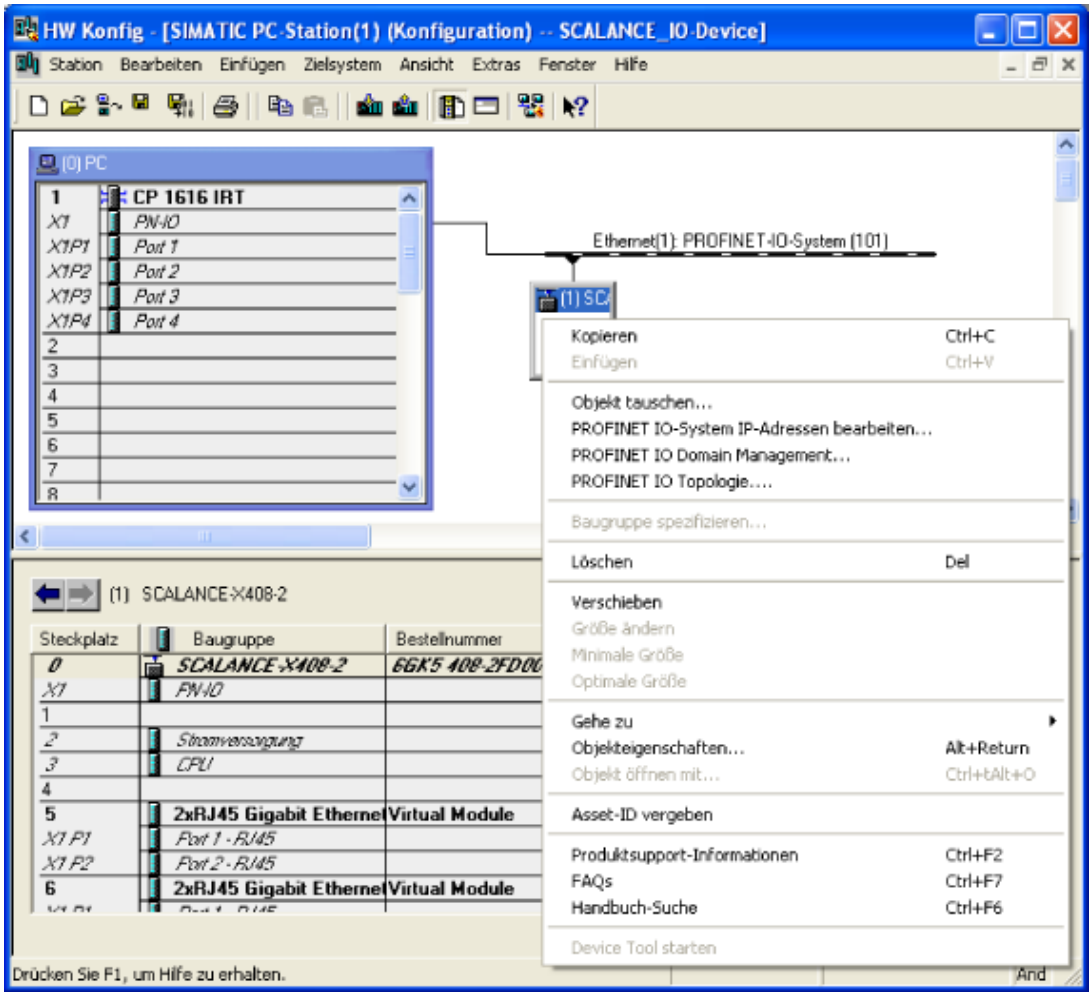


Bild 7-5 HW Konfig

8. Öffnen Sie in HW Konfig den Dialog "Objekteigenschaften des SCALANCE X408-2" (Klick mit rechter Maustaste auf das Icon -> Objekteigenschaften) und tragen Sie dort den Gerätenamen für das PROFINET IO Device ein. Beenden Sie den Dialog mit OK.

9. Wählen Sie den Menübefehl Station > Speichern und Übersetzen.
10. Vernetzen Sie die Geräte miteinander und schalten Sie die Spannungsversorgungen der vernetzten Geräte ein.

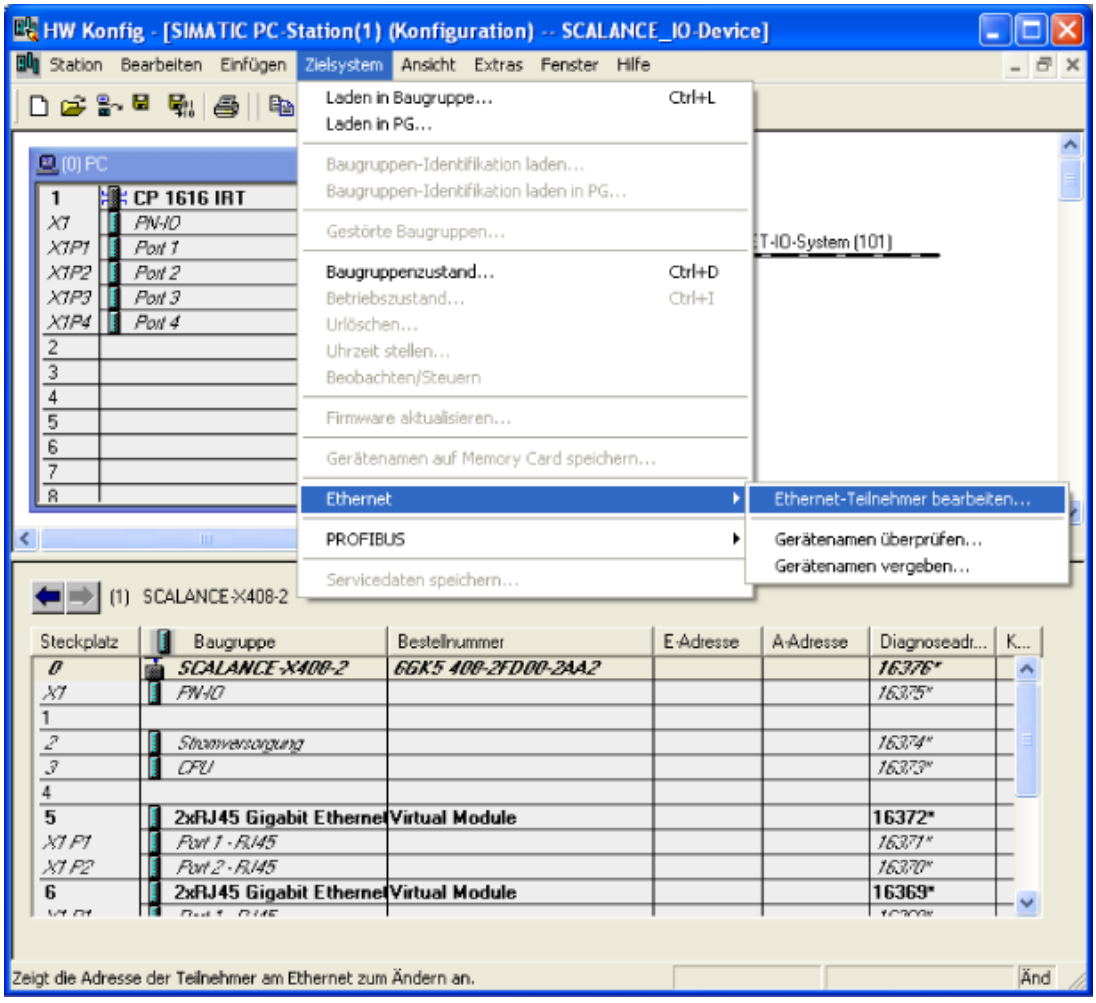


Bild 7-6 HW Konfig PROFINET IO Gerätenamen vergeben

Für die Namensübergabe zum SCALANCE X408-2 ist eine Online Verbindung vom PG zum PROFINET IO Device notwendig.

1. Über "Zielsystem > Ethernet > Gerätenamen vergeben" übergeben Sie den Gerätenamen an den SCALANCE X408-2.

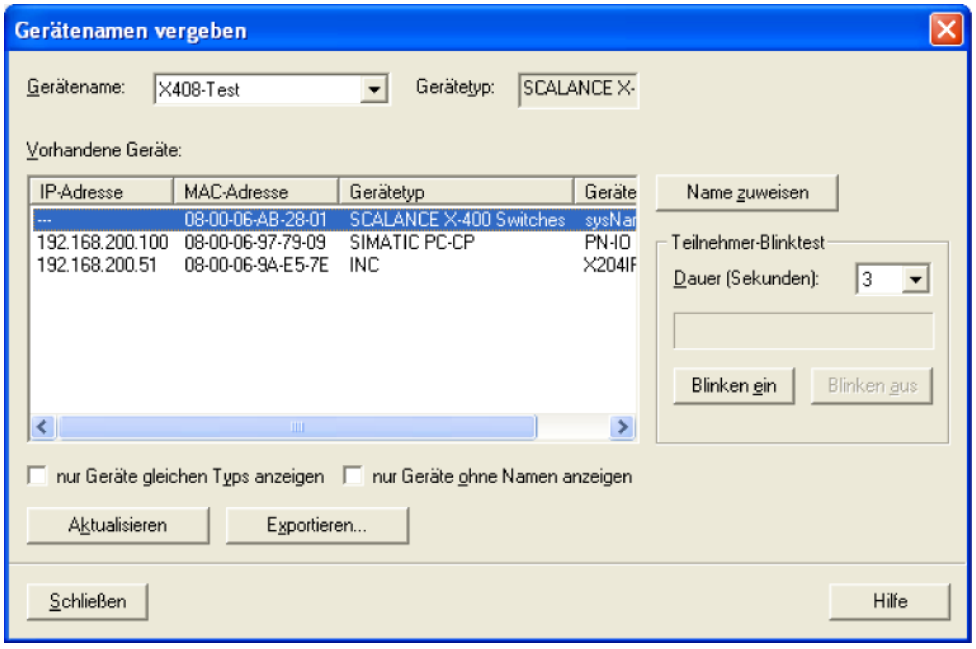


Bild 7-7 Gerätenamen vergeben

Wenn Sie mehrere PROFINET IO Devices einsetzen, werden im Dialogfeld "Gerätenamen vergeben" auch mehrere PROFINET IO Devices angezeigt. Vergleichen Sie in diesem Fall die MAC-Adresse des Gerätes mit der angezeigten MAC-Adresse und wählen Sie dann das richtige IO Device aus. Sie können auch über den Schaltknopf "Blinken ein/aus" die Gerätezuordnung visuell prüfen (beim ausgewählten IE-Switch blinken alle LEDs).

1. Klicken Sie im Dialogfeld "Gerätenamen vergeben" auf die Schaltfläche "Name zuweisen". Im IE-Switch wird der Gerätename remanent gespeichert. Nach der Zuweisung des Namens wird im Dialogfeld der von Ihnen vergebene Gerätename angezeigt.
2. Laden Sie die Hardware Konfiguration in den Controller (hier im Beispiel die CP1616). Wählen Sie Zielsystem > Laden in Baugruppe

7.2 Einstellungen in HW Konfig

Hinweis

Bei den IE-Switches X-400 sind die Stromversorgung und die C-PLUG-Alarmeinstellungen unterteilt in zwei Masken "Stromversorgung" und "CPU". Bei den IE-Switches X-300 sind diese in einer Maske vereint.

Stromversorgungsüberwachung

Hier stellen Sie die Parameter des IE-Switches ein, die für die Stromversorgung relevant sind.

Redundante Stromversorgung

- Nicht überwacht
  Der Ausfall einer der beiden Spannungsquellen löst keinen Alarm aus.
- Überwacht
  Der Ausfall einer der beiden Spannungsquellen löst einen Alarm aus.

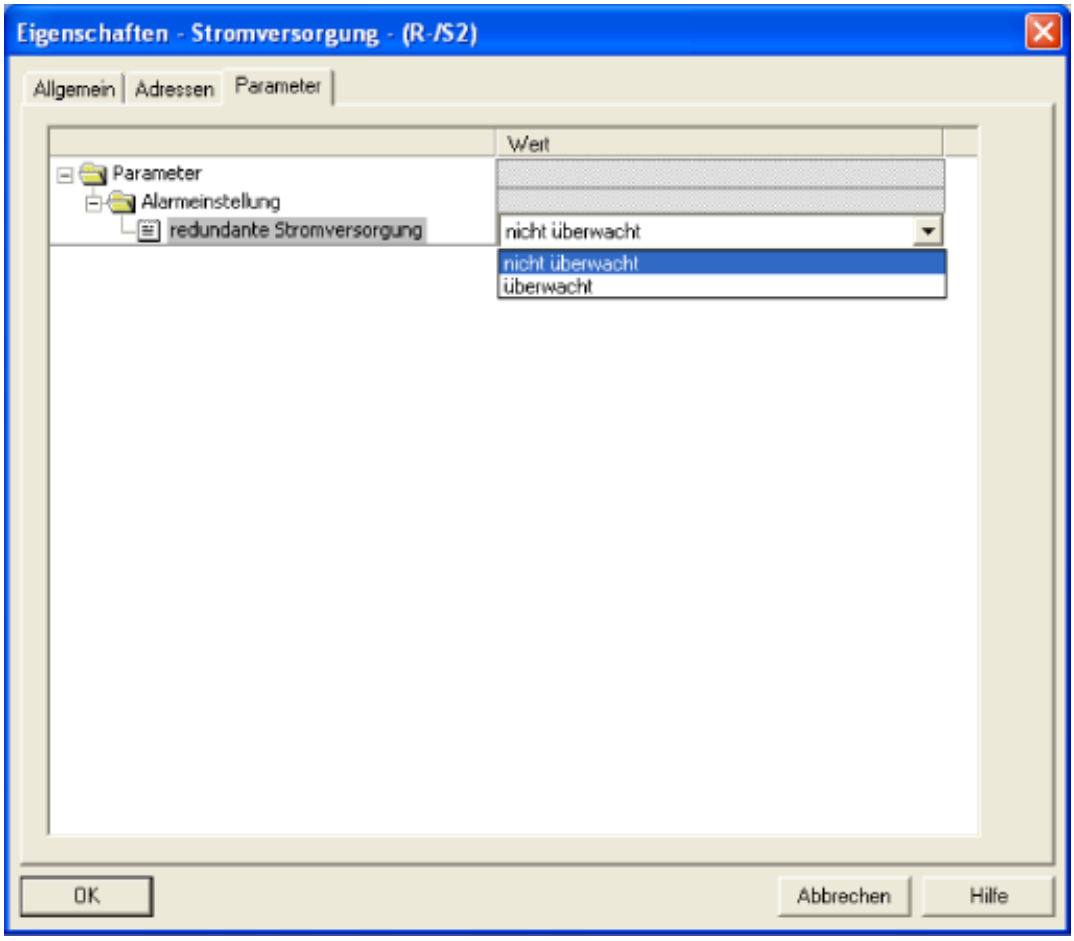


Bild 7-8 Eigenschaften - Stromversorgung beim IE-Switch X-400

CPU-Überwachung

Hier stellen Sie die Parameter des IE-Switches ein, die für das CPU-Modul relevant sind.

C-PLUG

- Nicht überwacht
  Der C-PLUG wird nicht überwacht.
- Überwacht
  Ein C-PLUG Fehler führt zu einem Alarm.

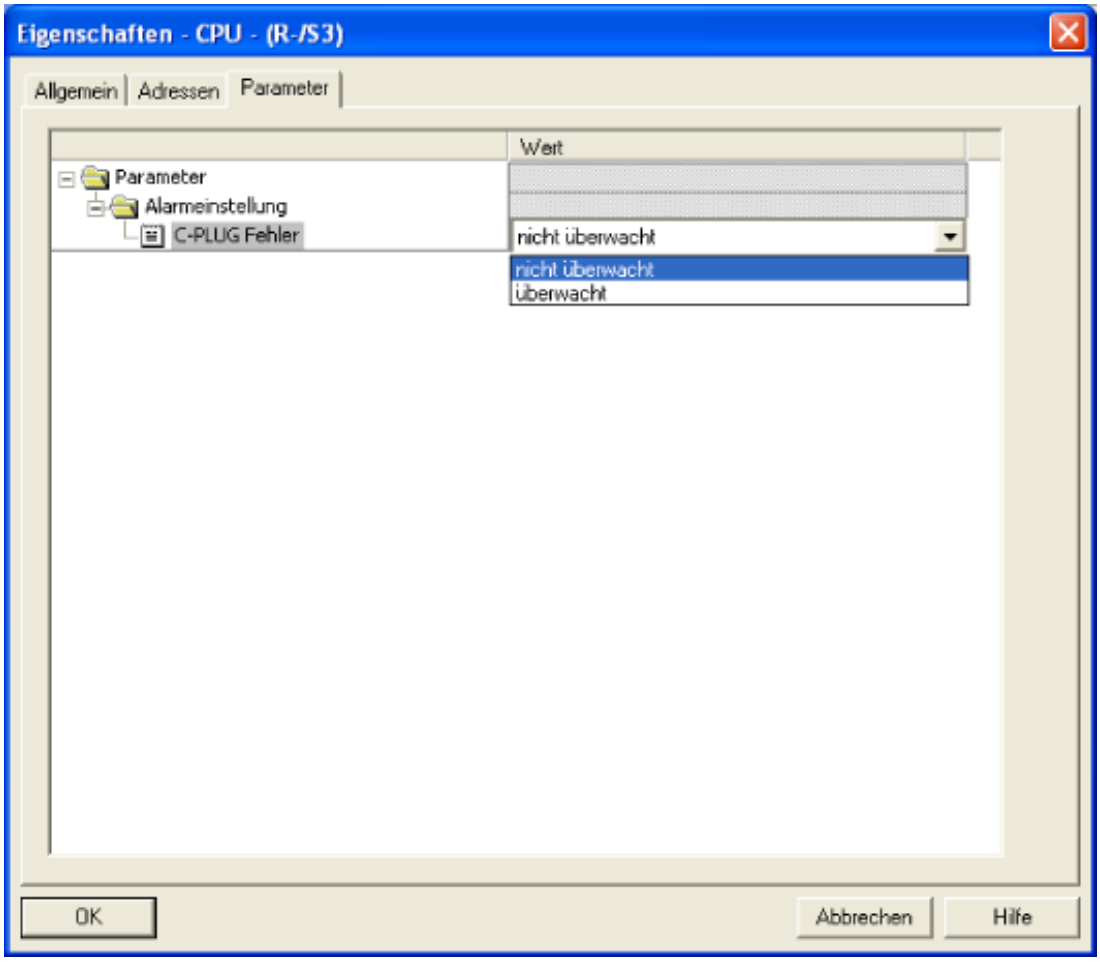


Bild 7-9 Eigenschaften - CPU beim IE-Switch X-400

Stromversorgungsüberwachung und CPU-Überwachung beim IE-Switch X-300

Die Einstellungen erfolgen hier mit den gleichen Möglichkeiten, wie bereits im vorherigen Teil des Kapitels beschrieben.

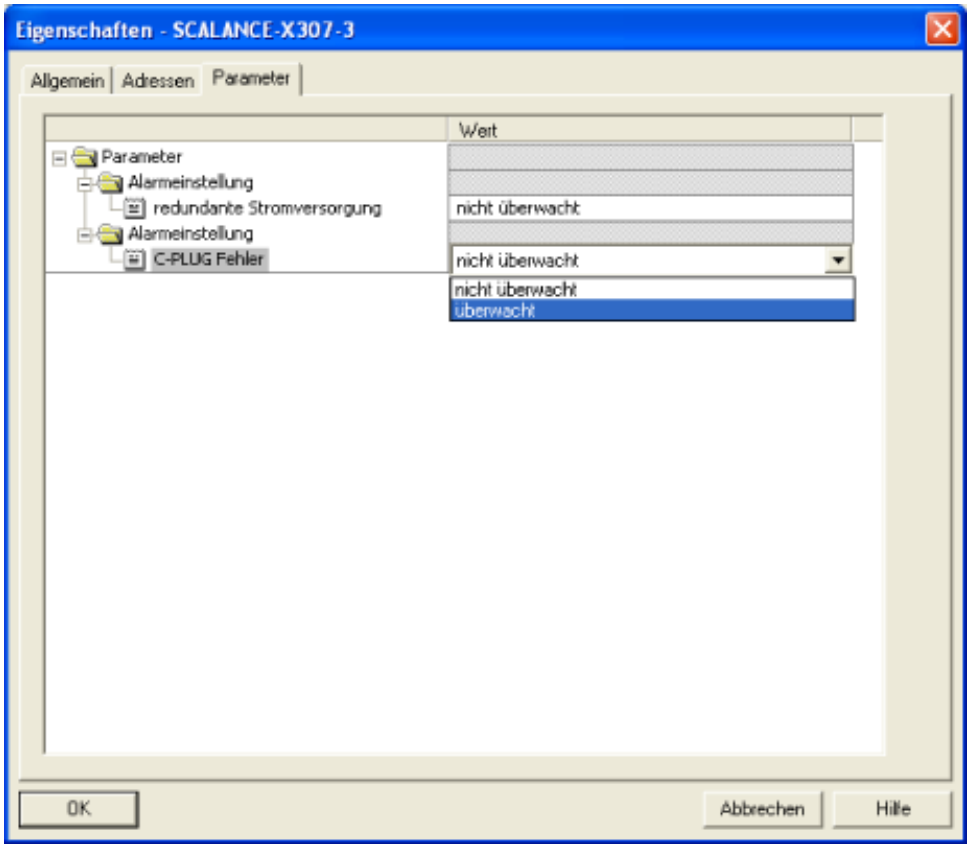


Bild 7-10 Eigenschaften - Stromversorgung und CPU beim IE-Switch X-300

Portspezifische Einstellungen

Hier können Sie Einstellungen zu den einzelnen Ports der IE-Switches vornehmen.
In der folgenden Maske wird dies am Beispiel eines SCALANCE X408-2 durchgeführt.

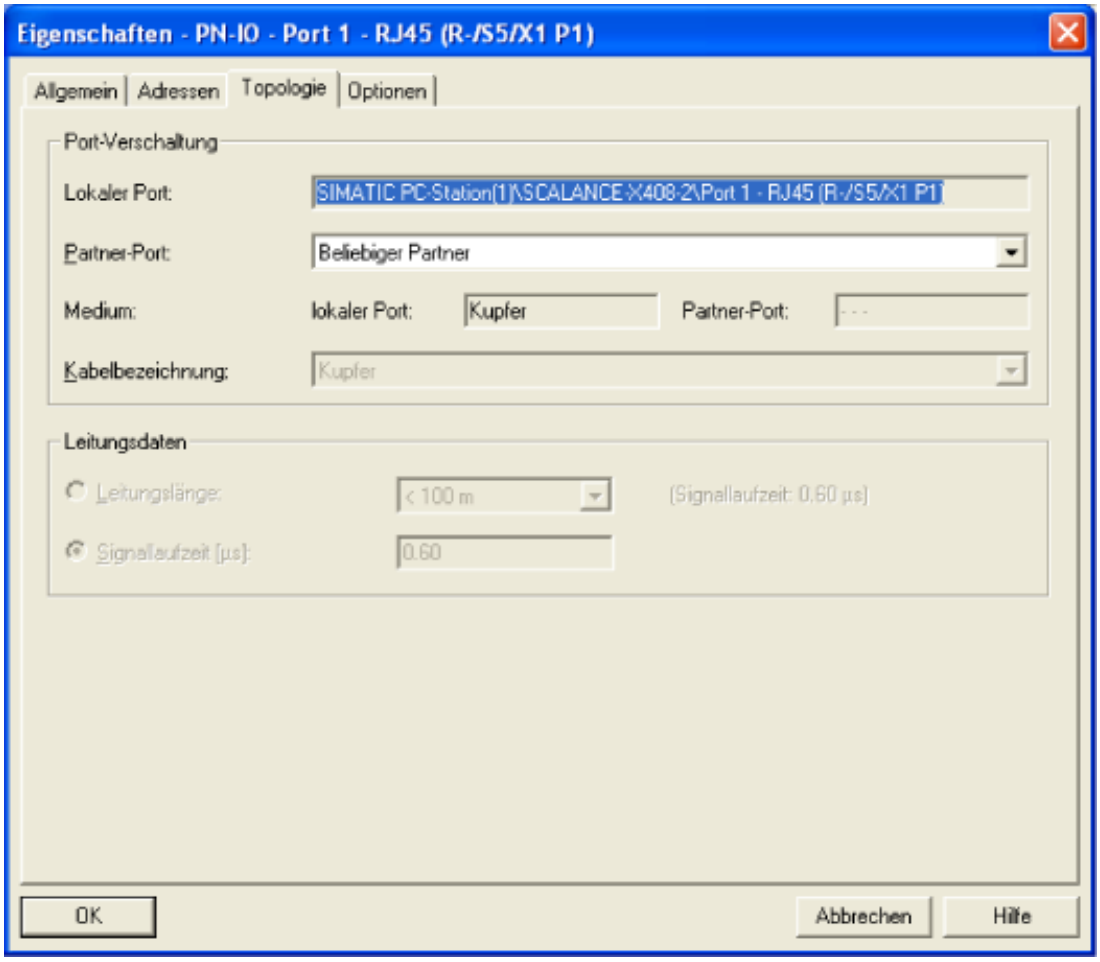


Bild 7-11 Eigenschaften - RJ45 Gigabit Ethernet

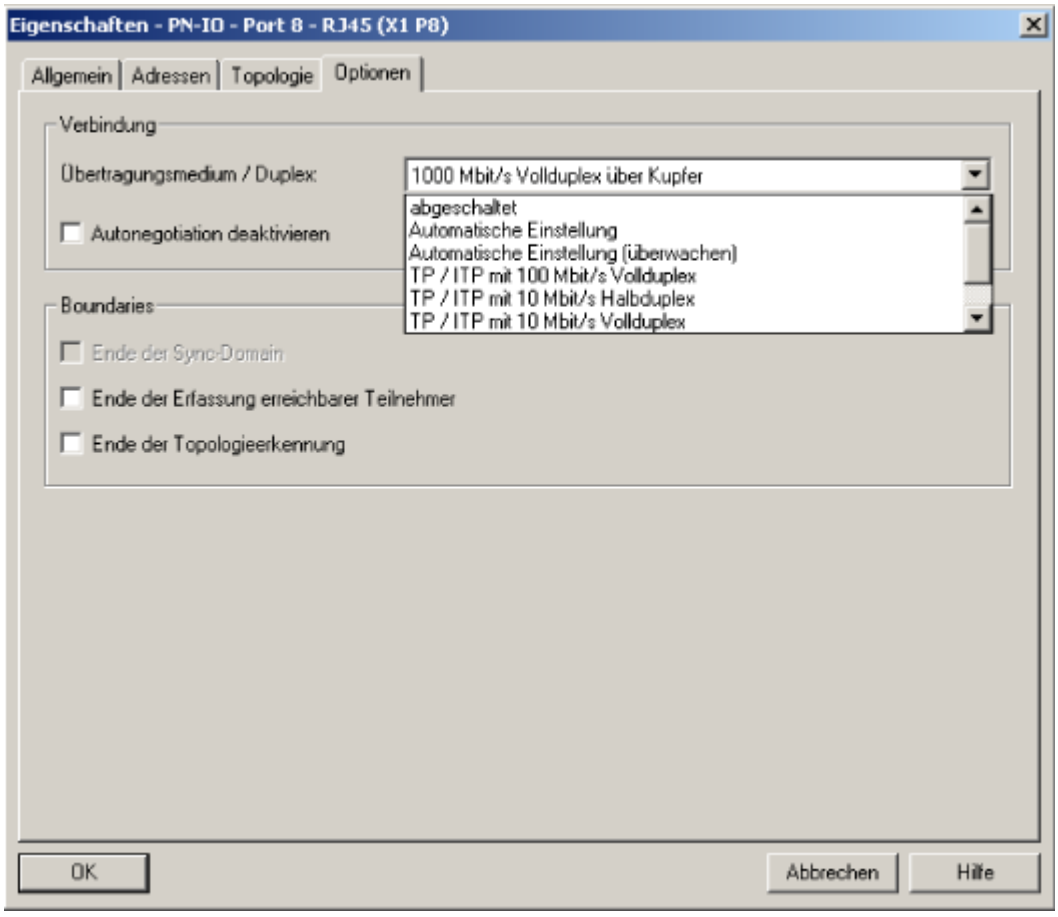


Bild 7-12 Eigenschaften - RJ45 Gigabit Ethernet Port Optionen

Sollvorgabe über Projektierung

Die Übertragungsrate des Ports kann auf Autonegotiation oder z.B. fest auf 100 Mbit Vollduplex eingestellt werden.

Hinweis

Wenn Sie eine feste Geschwindigkeit und Duplexität auswählen, müssen Sie das Häkchen bei "Autonegotiation deaktivieren" setzen.

7.3 Zugriffsmöglichkeiten über PROFINET IO

Hinweis

Die Tabelle Slot-Funktionen X-300 gilt für alle IE-Switches X-300 mit Ausnahme von folgenden Geräten, für die es eigene Tabellen gibt:

- Slot-Funktionen X308-2M
- Slot-Funktionen XR-324-12M
- Slot-Funktionen X302-7EEC und X307-2EEC
- Slot-Funktionen XR324-4M EEC

Slot-Funktionen X-300

Die IE-Switches X-300 haben pro Switch Port einen Subslot im Slot 0.
Funktionen, die nicht eindeutig einem Port zugeordnet werden können, sind dem Device Access Point (Slot 0) zugeordnet.

Slot 0	Subslot 1	• Alarme • Datensätze (4,5)	Device Access Point (DAP) • Kopfbaugruppe • C-PLUG • Redundante Stromversorgung
	Subslot 8001 - 8010 **SCALANCE X304-2FE:** Subslot 8001 - 8006 **SCALANCE X306-1LD FE:** Subslot 8001 - 8007 **SCALANCE X320-1FE:** Subslot 8001 - 8021 **SCALANCE X320-3LD:** Subslot 8001 - 8023	• Alarme (IEC) • Datensätze (IEC)	Switchport 1 - 10 (bzw. 1 - 6, 1 - 7, 1 - 21, 1 - 23) • Alarmverhalten • Port Zustand

Slot-Funktionen X308-2M

Der IE-Switch X308-2M hat 3 Slots. Die fest verbauten Ports sind dem Slot 0 zugeordnet. Die weiteren Steckplätze mit jeweils 2 Ports, sind Slot 1 und Slot 2 zugeordnet.
Funktionen die nicht eindeutig einem Port zugeordnet werden können, sind dem Device Access Point (Slot 0) zugeordnet.

Slot 0	Subslot 1	• Alarme • Datensätze (4,5)	Device Access Point (DAP) • Kopfbaugruppe • C-PLUG • Redundante Stromversorgung
	Subslot 8001 - 8004	• Alarme (IEC) • Datensätze (IEC)	Switchport 1 - 4 • Alarmverhalten • Port Zustand
Slot 1; Slot 2	Subslot 8001 - 8002	• Alarme (IEC) • Datensätze (IEC)	Switchport 5 - 6; Switchport 7 - 8 • Alarmverhalten • Port Zustand

Slot-Funktionen XR324-12M

Die IE-Switches XR324-12M haben mehrere Slots (Slot1-Slot12) mit jeweils 2 Ports.
Funktionen die nicht eindeutig einem Port zugeordnet werden können, sind dem Device Access Point (Slot 0) zugeordnet.

Slot 0	Subslot 1	• Alarme • Datensätze (4,5)	Device Access Point (DAP) • Kopfbaugruppe • C-PLUG • Redundante Stromversorgung
Slot 1 bis Slot 12	Subslot 8001 - 8002	• Alarme (IEC) • Datensätze (IEC)	Switchport 1.1 - 12.2 • Alarmverhalten • Port Zustand

Slot-Funktionen X302-7EEC und X307-2EEC

Die IE-Switches X302-7EEC und X307-2EEC haben pro Switch einen Subslot im Slot 0.
Funktionen die nicht eindeutig einem Port zugeordnet werden können, sind dem Device Access Point (Slot 0) zugeordnet.

Slot 0	Subslot 1	• Alarme • Datensätze (4,5)	Device Access Point (DAP) • Kopfbaugruppe • C-PLUG • Redundante Stromversorgung
	Subslot 8001 - 8009	• Alarme (IEC) • Datensätze (IEC)	Switchport 1 - 9 • Alarmverhalten • Port Zustand

Slot-Funktionen XR324-4M EEC

Die IE-Switches XR324-4M EEC haben mehrere Slots. Die fest verbauten Ports sind dem Slot 0 zugeordnet. Die weiteren Steckplätze sind mit jeweils 2 Ports Slot 1 bis Slot 4 zugeordnet. Funktionen die nicht eindeutig einem Port zugeordnet werden können, sind dem Device Access Point (Slot 0) zugeordnet.

Slot 0	Subslot 1	• Alarme • Datensätze (4,5)	Device Access Point (DAP) • Kopfbaugruppe • C-PLUG • Redundante Stromversorgung
	Subslot 8001-8016	• Alarme (IEC) • Datensätze (IEC)	Switchport 1-16 • Alarmverhalten • Port Zustand
Slot 1 bis Slot 4	Subslot 8001 - 8002	• Alarme (IEC) • Datensätze (IEC)	Switchport 1.1 - 4.2 • Alarmverhalten • Port Zustand

Slot-Funktionen X-400

Die IE-Switches X-400 haben mehrere Slots mit jeweils bis zu 4 Ports. Funktionen, die nicht eindeutig einem Port/Slot zugeordnet werden können, sind dem Device Access Point (Slot 0) bzw. den anderen übergeordneten Modulen (CPU und Power Modul) zugeordnet.

Slot 0	Subslot 1	• Alarme (IEC) • Datensätze (IEC)	Device Access Point (DAP) • Kopfbaugruppe
Slot 2	Subslot 1	• Alarme 0x200 • Datensätze 10,12	Power Module • Redundante Stromversorgung
Slot 3 (X408) Slot 4 (X414)	Subslot 1	• Alarme 0x201, 0x202, 0x203, 0x204 • Datensätze 11,13	CPU-Modul • C-PLUG
Slot 5, 6 u. 8 (X408) Slot 5-7, 9-15 (X414)	Subslot 8001-800n	• Alarme (IEC) • Datensätze (IEC)	Switchport 5.1-8.4 (X408) Switchport 5.1-15.2 (X414) • Alarmverhalten • Port Zustand

Die Alarmgenerierung

Der Anwender projektiert exakt die Belegung und die Solleigenschaften seiner Anschlüsse. Dadurch ist eine Abstimmung zwischen Projektierung und Installation erforderlich. Besagt die Einstellung in STEP 7, dass Port 3 verlinkt ist, müssen Sie dies bei der Montage berücksichtigen. Die von STEP 7 vorgegebene Power Meldemaske wird im Gerät remanent gespeichert und die Port-Meldemaske zurückgesetzt. Wenn Sie DataEX beenden, bleiben die von STEP 7 vorgegebenen Einstellungen der Meldemaske vorhanden und gelten weiterhin auch ohne PROFINET-Betrieb.

- Einfluss des SELECT/SET-Tasters während DataEX.
  Eine Betätigung des Knopfes zum Setzen der Meldemaske hat keinen Einfluss. Ein entsprechendes Blinken der Port-LEDs signalisiert dem Anwender, dass keine Änderung der Meldemaske stattgefunden hat.
- Einfluss weiterer Meldemechanismen während DataEX.
  Die Meldemaske wird wie von STEP 7 vorgegeben sowohl im Web-Interface als auch im CLI angezeigt. Änderungen sind nicht möglich. Es erscheint sinngemäß der Meldetext "Wegen PROFINET IO ist keine Einstellung möglich".

Aufbau der Datensätze

Hinweis

Die Datensätze 4 und 5 beziehen sich auf die IE-Switches X-300, die Datensätze 10 bis 13 auf die IE-Switches X-400.

Datensatz 4:

Zugriff: Read-Write,

Struktur:

typedef struct {

Word BlockType;

Word BlockLength;

Byte BlockVersionHigh:

Byte BlockVersionLow:

DWord Alarm_enable; };

BlockType:

1: Konstante

BlockLength:

6: Konstante in GSD, Bezeichnet die Länge ohne Type+ Length

BlockVersionHigh:

1: Konstante in GSD, Bezeichnet die Major Version

BlockVersionLow:

1: Konstante in GSD, Bezeichnet die Minor Version

Alarme_enable:

Diese Bitliste stellt ein, was überwacht werden soll. Ist ein Bit gesetzt, wird diese Alarmquelle freigeschaltet.

Reserved **Bit 2 - 31**	**C-PLUG** **Bit 1**	**Red_power** **Bit 0**
0	0: Keine CPLUG überwachung	0: Keine Überwachung der redundanten Spannungsversorgung
	1: Fehlender oder falscher CPLUG erzeugt Alarm	1: Überwachung der redundanten Spannungsversorgung

Datensatz 5:

Er liefert die aktuelle Alarmeinstellung bezüglich dieses Ports

Zugriff: Read-Only

typedef struct {

Word BlockType;

Word BlockLength;

Byte BlockVersionHigh;

Byte BlockVersionLow;

DWord status; };

BlockType:

1: Konstante

BlockLength:

6: Konstante in GSD, bezeichnet die Länge ohne Type+ Length

BlockVersionHigh:

1: Konstante in GSD, bezeichnet die Major Version

BlockVersionLow:

1: Konstante in GSD, bezeichnet die Minor Version

Status:

Reserved Bit 8-31	C-PLUG_status Bit 4-7	Reserved Bit 2-3	Fault_line_status Bit 1	Power Line Redundanz Bit 0
0	Information über den Configuration-Plug der Netzkomponente 0: C-PLUG gesteckt und ok 1:C-PLUG nicht gesteckt 2: C-PLUG gesteckt aber nicht ok (Falscher Typ) 3: C-PLUG gesteckt aber nicht ok (Check-summ-fehler)		Information über den aktuellen Zustand des Meldekontakt 0: Fault line passiv 1: Fault line aktiv	Dieses Bit liefert Informationen über die redundante Stromversorgung 0: nicht redundant 1: redundant

Datensatz 10 (Stromversorgung, Parametrierung)

Zugriff: Read Write,

Struktur:

typedef struct {

Word BlockType;

Word BlockLength;

Byte BlockVersionHigh:

Byte BlockVersionLow:

DWord Alarm_enable; };

BlockType

1: Konstante

BlockLength

6: Konstante in GSD, Bezeichnet die Länge ohne Type+ Length

BlockVersionHigh

1: Konstante in GSD, Bezeichnet die Major Version

BlockVersionLow

1: Konstante in GSD, Bezeichnet die Minor Version

Alarme_enable

Reserved **Bit 1-31**	**Red_power** **Bit 0**
0	0: Keine Überwachung der redundanten Spannungsversorgung
	1: Überwachung der redundanten Spannungsversorgung

Datensatz 11 (CPU, Parametrierung)

Struktur

typedef struct {
Word BlockType;
Word BlockLength;
Byte BlockVersionHigh:
Byte BlockVersionLow:
Word Alarm_Mode;
DWord Alarm_Parameter; };

BlockType

1: Konstante

BlockLength

6: Konstante in GSD, bezeichnet die Länge ohne Type+ Length

BlockVersionHigh

1: Konstante in GSD, bezeichnet die Major Version

BlockVersionLow

1: Konstante in GSD, bezeichnet die Minor Version

Alarm_Mode

Reserved Bit 2-31	Enhanced_Alarm_Mode Bit 1	Show_C-PLUG_Error Bit 0
0	Keine Funktion	0: Keine Überwachung des C-PLUGs
		1: Fehlender oder nicht richtiger C-PLUG erzeugt einen Alarm.

Datensatz 12 (Stromversorgung, Baugruppenzustand)

Er liefert die aktuelle Alarmeinstellung bezüglich dieses Ports

Zugriff: Read Only

typedef struct {

Word BlockType;

Word BlockLength;

Byte BlockVersionHigh;

Byte BlockVersionLow;

DWord status; };

BlockType

1: Konstante

BlockLength

6: Konstante in GSD, bezeichnet die Länge ohne Type+ Length

BlockVersionHigh

1: Konstante in GSD, bezeichnet die Major Version

BlockVersionLow

1: Konstante in GSD, bezeichnet die Minor Version

Status

Reserved Bit 2-31	Fault_line_status Bit 1	Power Line Redundanz Bit 0
0	Information über den aktuellen Zustand des Meldekontakt 0: Fault line passiv 1: Fault line aktiv	Dieses Bit liefert Informationen über die redundante Stromversorgung 0: nicht redundant 1: redundant

Datensatz 13 (CPU, Baugruppenzustand)

Struktur

```
typedef struct {
Word BlockType;
Word BlockLength;
Byte BlockVersionHigh;
Byte BlockVersionLow;
DWord PortState;
byte PortType;
byte reserved; };
```

BlockType

1: Konstante

BlockLength

6: Konstante in GSD, bezeichnet die Länge ohne Type+ Length

BlockVersionHigh

1: Konstante in GSD, bezeichnet die Major Version

BlockVersionLow

1: Konstante in GSD, bezeichnet die Minor Version

Status

Reserved **Bit 2-31**	**C-PLUG_status** **Bit 0-1**
0	Informationen über den C-PLUG der Netzkomponente 0: C-PLUG gesteckt und OK 1: C-PLUG nicht gesteckt 2: C-PLUG gesteckt aber nicht OK (Falscher Typ) 3: C-PLUG gesteckt aber nicht OK (Checksummfehler)

7.4 Datensatz 0x802A (PDPortDataReal)

Struktur

```
typdef struct{
Word BlockType;
Word BlockLength;
Byte BlockVersionHigh;
Byte BlockVersionLow;
Word Padding;
Word SlotNumber;
Word SubslotNumber;
Byte LengthOwnPortID;
8 Byte OwnPortID;
Byte NumberOfPeers;
Word Padding;
Byte LengthPeerPortID;
8 Byte PeerPortID;
Byte LengthPeerChassisID;
8 Byte PeerChassisID;
Word Padding;
DWord LineDelay;
6 Byte PeerMACAddress;
Word Padding;
Word MAUType;
Word Padding;
DWord DomainBoundary;
DWord MulticastBoundary;
Word LinkState;
Word Padding;
DWord MediaType;};
```

BlockType

Konstante = 0x020F

BlockLength

Konstante, bezeichnet die Länge des Datensatzes ohne die Felder BlockType und BlockLength.

BlockVersionHigh

Konstante = 1, bezeichnet die Major Version.

BlockVersionLow

Konstante = 0, bezeichnet die Minor Version.

SlotNumber

Slotbezeichnung, siehe Kapitel "Zugriffsmöglichkeiten über PROFINET IO"

SubslotNumber

Subslotbezeichnung, siehe Kapitel "Zugriffsmöglichkeiten über PROFINET IO"

LengthOwnPortID

Länge des Feldes OwnPortID in Byte.

OwnPortID

Bezeichnung des verwendeten Ports.

NumberOfPeers

Anzahl der Nachbarports.

LengthPeerPortID

Länge des Feldes PeerPortID in Byte.

PeerPortID

Bezeichnung des Nachbarports.

LengthPeerChassisID

Länge des Feldes PeerChassisID in Byte.

PeerChassisID

Bezeichnung des Nachbargeräts.

LineDelay

LineDelay.FormatIndicator = 0

Wert (hexadezimal)	Bedeutung
0x00000000	Line Delay und Cable Delay unbekannt.
0x00000001 – 0x7FFFFFFF	Line Delay in Nanosekunden.

LineDelay.FormatIndicator = 1

Wert (hexadezimal)	Bedeutung
0x00000000	Reserviert
0x00000001 – 0x7FFFFFFF	Cable Delay in Nanosekunden.

PeerMACAddress

MAC-Adresse des Nachbargeräts.

MAUType

Wert (hexadezimal)	Bedeutung
0x0000 – 0x0004	Reserviert
0x0005	10BASET
0x0006-0x0009	Reserviert
0x000A	10BASETXHD
0x000B	10BASETXFD
0x000C	10BASEFLHD
0x000D	10BASEFLFD
0x000F	100BASETXHD
0x0010	100BASETXFD (Default)
0x0011	100BASEFXHD
0x0012	100BASEFXFD
0x0013 – 0x0014	Reserviert
0x0015	1000BASEXHD
0x0016	1000BASEXFD
0x0017	1000BASELXHD
0x0018	1000BASELXFD
0x0019	1000BASESXHD
0x001A	1000BASESXFD
0x001B – 0x001C	Reserviert
0x001D	1000BASETHD
0x001E	1000BASETFD
0x001F	10GigBASEFX
0x0020 – 0x002D	Reserviert
0x002E	100BASELX10
0x002F – 0x0035	Reserviert
0x0036	100BASEPXFD
0x0037 – 0xFFFF	Reserviert

DomainBoundary

Legt fest, welche Multicast-Adressen geblockt werden.

MulticastBoundary

Mit den einzelnen Bits der DWord-Variablen wird festgelegt, welche der 32 ersten RT_CLASS_2 Multicast-Adressen (von 01-0E-CF-00-02-00 bis 01-0E-CF-00-02-1F) geblockt wird.

Bit	Wert	Bedeutung
0	1	Die Multicast MAC-Adresse 01-0E-CF-00-02-00 wird geblockt.
	0	Die Multicast MAC-Adresse 01-0E-CF-00-02-00 wird nicht geblockt.
...	1	Die Multicast MAC-Adresse 01-0E-CF-00-02-xx wird geblockt.
	0	Die Multicast MAC-Adresse 01-0E-CF-00-02-xx wird nicht geblockt.
31	1	Die Multicast MAC-Adresse 01-0E-CF-00-02-1F wird geblockt.
	0	Die Multicast MAC-Adresse 01-0E-CF-00-02-1F wird nicht geblockt.

LinkState

LinkState.Link

Wert (hexadezimal)	Bedeutung
0x00	Reserved
0x01	Up (Bereit zum Pakete versenden)
0x02	Down
0x03	Testing (Es werden keine Nutzdaten transportiert)
0x04	Unknown (Status kann nicht ermittelt werden)
0x05	Dormant (Wartet auf externe Aktion)
0x06	Not present
0x07	LowerLayerDown
0x08 - 0xFF	Reserved

LinkState.Port

Wert (hexadezimal)	Bedeutung
0x00	Unbekannt
0x01	Deaktiviert / Verworfen
0x02	Geblockt
0x03	Port-Listening aktiviert
0x04	Lernen
0x05	Weiterleiten
0x06	Unterbrochen
0x07 – 0xFF	Reserviert

MediaType

Wert (hexadezimal)	Bedeutung
0x00	Unbekannt
0x01	Kupfer-Leitung

Wert (hexadezimal)	Bedeutung
0x02	Fiberoptik-Leitung
0x00	Funk-Kommunikation
0x04 – 0xFFFFFFFF	Reserviert

Hinweis

Weitere Informationen zu den IEC-Datensätzen finden Sie in der IEC 61158.

7.5 MRP-Projektierung

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. Es ist auch möglich, nur für die Ringports Spanning Tree zu deaktivieren.

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

Mit der Funktion MRP-Mehrfachringe ist es möglich, mehrere MRP-Ringe mit einem zentralen Redundanzmanager zu steuern. 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 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 X408-2 ab Firmware-Version V4.0
- SCALANCE X414-3E ab Firmware-Version V3.10
- SCALANCE XB-200 ab Firmware-Version V4.3
- SCALANCE XC-200 ab Firmware-Version V4.3
- SCALANCE XP-200 ab Firmware-Version V4.3
- SCALANCE XR-300WG ab Firmware-Version V4.3
- SCALANCE XM-400 ab Firmware-Version V6.4
- SCALANCE XR-500 ab Firmware-Version V6.4

Hinweis

Geeignete Geräte für MRP-Interconnection

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

- SCALANCE XB-200 ab Firmware-Version V4.3
- SCALANCE XC-200 ab Firmware-Version V4.2
- SCALANCE XF-200BA ab Firmware-Version V4.2
- SCALANCE XP-200 ab Firmware-Version V4.2
- SCALANCE XR-300WG ab Firmware-Version V4.3
- SCALANCE XM-400 ab Firmware-Version V6.3 bzw. ab Firmware-Version V6.2 für homogene Netze
- SCALANCE XR-500 ab Firmware-Version V6.3 bzw. ab Firmware-Version V6.2 für homogene Netze

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. Das Gerät mit niedrigsten MAC-Adresse wird Manager.
  - 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

Öffnen Sie den Ring, bevor Sie ein Gerät in diesem Ring auf Werkseinstellungen zurücksetzen.

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

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.

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 STEP7 vorgegeben (Alternative Redundanz)

Diese Option betrifft alle SCALANCE X-Switches. Wählen Sie diese Option bei der Projektierung in STEP7, 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.

Hinweis

Wenn für ein Gerät im Ring die Option "Alternative Redundanz" aktiviert ist und die Topologie durch STEP7 (Controller) überwacht wird, müssen Sie auch für die restlichen Geräte im Ring die Option "Alternative Redundanz" aktivieren.

Besonderheiten beim XR-324-12M

Hinweis

PROFINET IO-Betrieb des SCALANCE XR-324-12M

Der PROFINET IO-Betrieb des SCALANCE XR-324-12M ist nur möglich, wenn ein Medienmodul gesteckt ist. Die Werkseinstellungen für "mrpdomain-1" sehen für MRP die Ports 1 und 2 vor, daher müssen diese beiden Ports im Switch durch ein gestecktes Medienmodul zur Verfügung gestellt werden.

⚠ VORSICHT

Vorbelegung der Ringports beim XR-324-12M im STEP 7-Projekt

Beim SCALANCE XR-324-12M werden bei der STEP 7-Projektierung von MRP und der Auswahl "mrpdomain-1" automatisch die Ringports auf die ersten projektierten Ports gelegt.

Kontrollieren Sie deshalb, ob die projektierten Ringports mit den beschalteten Ringports übereinstimmen.

C-PLUG

8

Anwendungsbereich

Der C-PLUG ist ein Wechselmedium zur Sicherung der Konfigurationsdaten des modularen Switches und ist im Lieferumfang enthalten. Dadurch stehen die Konfigurationsdaten bei einem Austausch des Grundgerätes weiterhin zur Verfügung.

Hinweis

Der C-PLUG darf nur im stromlosen Zustand des Gerätes gezogen oder gesteckt werden.

Funktionsprinzip

Die Energie-Versorgung erfolgt durch das Grundgerät. Der C-PLUG behält in stromlosem Zustand alle Daten dauerhaft.

Auf einem unbeschriebenen C-PLUG (Werkzustand oder mit Clean-Funktion gelöscht) werden beim Geräteanlauf automatisch alle Konfigurationsdaten eines IE-Switches gesichert. Änderungen der Konfiguration im laufenden Betrieb ohne Bedienereingriff werden auf dem C-PLUG gesichert, wenn dieser sich im Zustand *ACCEPTED* befindet.

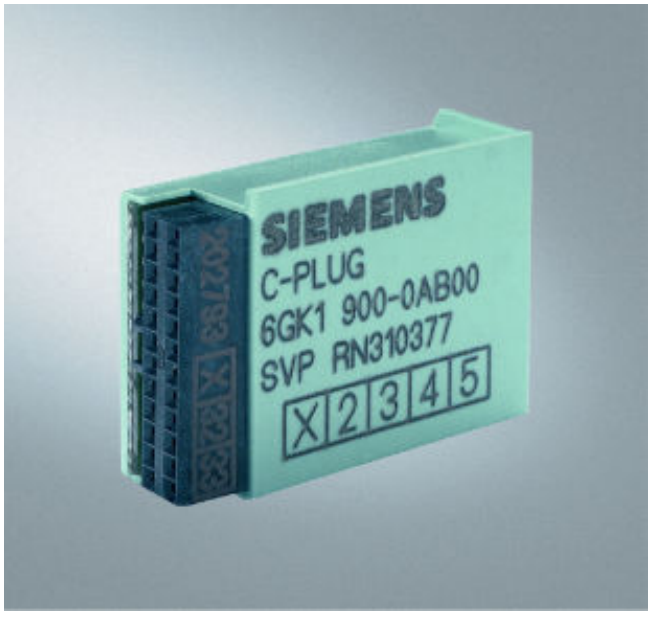


Bild 8-1 C-PLUG

Ein IE-Switch mit gestecktem und akzeptiertem (Zustand ACCEPTED) C-PLUG verwendet beim Anlauf automatisch dessen Konfigurationsdaten. Voraussetzung für die Akzeptanz ist u.a., dass die Daten von einem kompatiblen Gerätetyp geschrieben wurden.

Hinweis

Ist ein C-PLUG gesteckt, werden alle Konfigurationsänderungen sowohl im C-PLUG als auch im internen Speicher des Geräts abgelegt.

Somit wird im Austausch / Ersatzteil-Fall ein schneller und einfacher Wechsel des Grundgerätes ermöglicht. Der C-PLUG wird aus der ausgefallenen Komponente entnommen und in das Ersatzteil gesteckt. Das Ersatzgerät verfügt nach Erstanlauf automatisch über die gleiche Gerätekonfiguration wie das ausgefallene Gerät, außer der vom Hersteller festgelegten gerätespezifischen MAC-Adresse.

Hinweis

Wird ein Gerät mit aktueller Firmware und C-PLUG durch ein Gerät mit einem älteren Firmwarestand ersetzt, wird beim Umstecken des C-PLUG die aktuelle C-PLUG-Konfiguration nicht übernommen. Um die Konfiguration des C-PLUG zu nutzen, muss das Ersatzgerät mindestens über den Firmwarestand des zu ersetzenden Geräts verfügen.

Berücksichtigen Sie deshalb bei einem Firmwareupdate immer auch eventuell vorhandene Ersatzgeräte.

Hinweis

Im Austauschfall des IE-Switches ist die Bestückung durch Medienmodule, beim Einsatz eines SCALANCE X414-3E zusätzlich die Schalterstellungen der DIP-Schalter auf der Switch CPU und die optionale Bestückung der Extender-Module, zu übernehmen.

Diagnose

Das Stecken eines C-PLUGs, der die Konfiguration eines nicht kompatiblen Gerätetyps enthält, das unbeabsichtigte Entfernen des C-PLUGs oder allgemeine Fehlfunktionen des C-PLUGs werden über die Diagnosemechanismen des Gerätes (LEDs, WEB-Based-Management, SNMP und CLI) signalisiert.

Anlaufverhalten

Wird der C-PLUG zwischen Geräten mit gleichem Firmwarestand getauscht, so läuft das Gerät mit der auf dem C-PLUG gespeicherten Konfiguration hoch. Die C-PLUG-Konfiguration wird erst dann in den Konfigurationsspeicher des Gerätes übernommen, wenn entweder ein Konfigurationsparameter geändert und abgespeichert wurde oder das Gerät per CLI/WBM-Befehl neu gestartet wurde. Wenn keine Konfigurationsänderung erfolgt und der C-PLUG nach dem Ausschalten wieder entnommen wird, so startet das Gerät bei einem erneuten Anlauf wieder mit der unverändert auf dem Gerät vorhandenen Konfiguration.

Wird ein C-PLUG von einem Gerät mit einem älteren Firmwarestand in ein Gerät mit einem neueren Firmwarestand gesteckt, wird der interne Speicher schon während des Neustarts durch

die Konfiguration des C-PLUG überschrieben. Auch ohne Konfigurationsänderung startet das Gerät nach dem Entnehmen des C-PLUG mit der vom C-PLUG übernommenen Konfiguration.

	C-PLUG	Anlauf IE-Switch
1	nicht vorhanden	mit interner Konfiguration (sofern vorhanden) oder mit Factory default.
2	leer	mit interner Konfiguration, kopiert diese sofort automatisch auf den C-PLUG
3	mit eigenen Konfigurationsdaten beschrieben	mit C-PLUG Konfiguration
4	mit fremden Konfigurationsdaten beschrieben	mit fremder C-PLUG Konfiguration
5	mit Konfigurationsdaten eines anderen Gerätetyps beschrieben	mit interner Konfiguration, rote LED auf Power Module und Log-Eintrag
6	defekt	mit interner Konfiguration, rote LED auf Power Module und Log-Eintrag
7	mit Konfigurationsdaten, die mit einer älteren Firmware-Version erstellt wurde, als aktuell auf dem IE- Switch vorhanden	mit C-PLUG Konfiguration

In den Fällen 2 und 3 sind die Konfigurationsdaten auf der Switch CPU und dem C-PLUG identisch.

In den Fällen 4 und 5 sind die Konfigurationsdaten unterschiedlich und können manuell angeglichen werden.

Im Fall 6 können Sie mittels der Clean-Funktion versuchen, den C-PLUG neu zu formatieren. Im erneuten Fehlerfall ist der C-PLUG auszutauschen.

Hinweis

Im Fall 4 (Austauschfall) eines SCALANCE X414-3E werden die Schalterstellungen der DIP-Schalter vom C-PLUG und nicht die tatsächlich vorhandenen Schalterstellungen übernommen. Eine Abweichung wird über die Diagnosemöglichkeiten signalisiert.

Speicherung von Konfigurationsdaten

Wird ein Gerät mit einem C-PLUG gestartet, der mit einer älteren Firmware-Version erstellt wurde als die, die auf dem IE-Switch vorhanden ist, wird die "interne" Konfiguration des Gerätes während des Neustarts durch die Konfigurationsdaten des C-PLUG überschrieben. Auch nach dem Ziehen des C-PLUG sind im Gerät nur die vom C-PLUG übernommenen Konfigurationsdaten vorhanden.

Wird ein C-PLUG mit Konfigurationsdaten gesteckt, die mit der identischen Firmware-Version erstellt wurden, die auch aktuell auf dem IE- Switch vorhanden ist, so ist Folgendes zu beachten: Die auf dem C-PLUG enthaltene Konfiguration wird erst dann in den Gerätespeicher übernommen, wenn

- eine Konfigurationsänderung mit "Set Values" geschrieben wird oder
- ein "Save (Restart)" durchgeführt wird.

Ohne Konfigurationsänderung oder "Save (Restart)" würde ein erneuter Start des Geräts ohne C-PLUG (nach dem Abschalten der Spannungsversorgung entnommen) mit den vorherigen internen Konfigurationsdaten erfolgen.

Hinweis

Änderungen der Konfigurationsdaten werden spätestens 90 Sekunden nach Eingabe eines CLI-Befehls oder nach Anklicken der Schaltfläche "Set Values" im Web Based Management in den nichtflüchtigen Gerätespeicher übernommen.

Wird über die Schaltfläche "Restart System" im Menü "System Restart & Defaults" des Web Based Management oder mit dem Befehl "restart" des CLI ein Neustart durchgeführt, so werden alle durchgeführten Konfigurationsänderungen ebenfalls in den nichtflüchtigen Gerätespeicher übernommen.

Firmwareupdate

9

9.1 Firmwareupdate bei funktionsfähiger Firmware

9.1.1 Firmwareupdate über HTTP/HTTPS

Web Based Management oder Command Line Interface

Informationen zum Firmwareupdate über HTTP/HTTPS finden Sie im Kapitel "Menüpunkt System Save & Load".

9.1.2 Firmwareupdate über TFTP

Web Based Management oder Command Line Interface

Informationen zum Firmwareupdate über TFTP finden Sie im Kapitel "Menüpunkt System Save & Load".

9.1.3 Firmwareupdate über FTP

Zugang über Konsole

Wenn ein IE-Switch über eine IP-Adresse verfügt und eine Ethernet-Verbindung zu einem PC bzw. PG besteht, müssen Sie folgende Schritte durchführen, um ein Firmwareupdate durchzuführen:

1. Öffnen Sie ein Konsolen-Fenster und geben Sie den Befehl ftp gefolgt von der IP-Adresse des IE-Switches ein.
   Beispiel:
   ftp 192.168.20.54
2. Geben Sie für Login und Passwort die gleichen Werte ein, das Sie auch für WBM und CLI verwenden.
3. Geben Sie den Befehl "put" gefolgt vom Namen der Firmwaredatei ein.
   Beispiel:
   put v100031.lad
4. Nach dem Abschluss des Ladevorgangs beendet der IE-Switch die FTP-Verbindung und führt einen Neustart durch.

9.2 Firmwareupdate über die Boot-Software beim IE-Switch X-400/ XR-300

Notwendigkeit für einen Update über die Boot-Software

Ein Firmwareupdate über die Boot-Software ist dann notwendig, wenn das Update nicht über die Firmware durchgeführt werden kann. Mögliche Gründe dafür sind eine fehlerhafte Firmware oder eine Stromunterbrechung während des Flash-Vorgangs.

ACHTUNG
FPGA nicht über Boot-Software mit XMODEM laden und aktualisieren
Laden und aktualisieren Sie kein FPGA über die Boot-Software, wenn Sie XMODEM verwenden.

So gelangen Sie in den Bootloader-Modus

Voraussetzung ist, dass ein PC oder PG an der seriellen Schnittstelle des IE-Switches X-400/ XR-300 angeschlossen ist. Führen Sie folgende Schritte durch, um in den Bootloader-Modus zu gelangen:

1. Starten Sie den IE-Switch neu, indem Sie z. B. die Spannungsversorgung trennen und wieder verbinden.
2. Betätigen Sie während des Hochlaufs eine beliebige Taste auf der Tastatur des PC bzw. PG.

Wenn im IE-Switch X-400/XR-300 keine funktionsfähige Firmware vorhanden ist, startet der IE-Switch X-400/XR-300 automatisch in einer Betriebsart, in der mit dem integrierten FTP-Server kommuniziert werden kann. Voraussetzung ist allerdings, dass der IE-Switch X-400/XR-300 über eine IP-Adresse verfügt.

9.2.1 Firmwareupdate über die serielle Schnittstelle

Vorgehensweise

Führen Sie folgende Schritte durch, um Firmware über die serielle Schnittstelle des IE-Switches X-400/XR-300 zu laden:

1. Schließen Sie einen PC mit einem Terminalprogramm (z. B. HyperTerminal) an die serielle Schnittstelle des IE-Switches X-400/XR-300 an und starten Sie das Terminalprogramm. Zusatzinformationen zu diesem Thema finden Sie im Anhang A.
2. Setzen Sie den IE-Switch X-400/XR-300 zurück. Schalten Sie in den Display Mode A oder in den Display Mode D (es wird automatisch in den Display Mode A umgeschaltet, wenn der Taster SET/SEL länger als eine Minute nicht betätigt wird). Drücken Sie den Taster SET/SEL länger als 12 Sekunden. Betätigen Sie eine beliebige Taste, um den Bootloader während des Hochlaufs anzuhalten. HyperTerminal zeigt folgende Meldung:

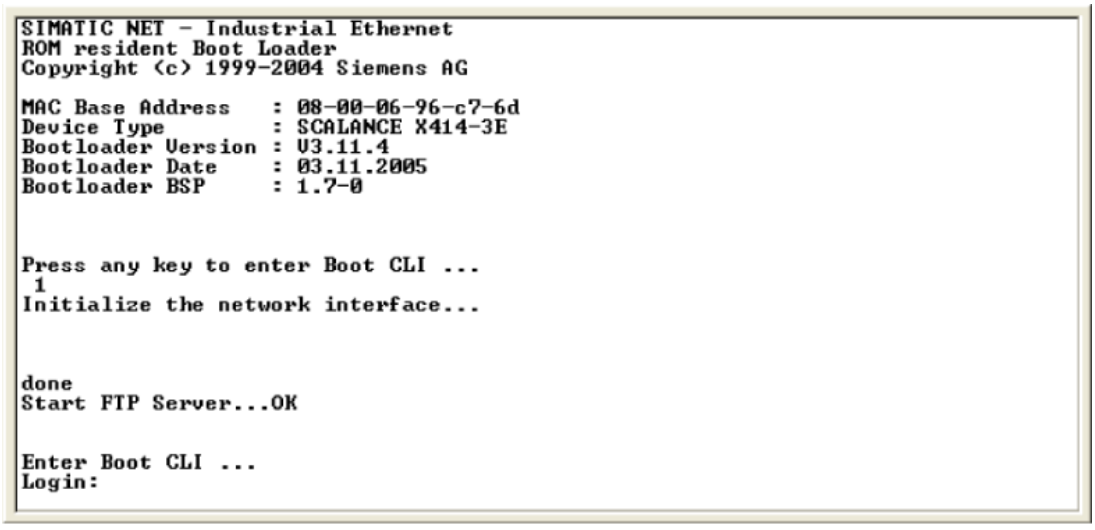


Bild 9-1 HyperTerminal

3. Loggen Sie sich in das Command Line Interface des Bootloaders mit folgenden Angaben ein:
   Login: siemens
   Password: siemens
4. Geben Sie den Befehl ldimage ein. Hyperterminal gibt daraufhin folgende Meldung aus:
   XMODEM .... waiting for file
   ATTENTION: do not switch off till the COMPLETED or FAILED message appears
   ... CCCCCCC

5. Wählen Sie das Menü Übertragung > Datei senden. HyperTerminal öffnet das folgende Dialogfenster:

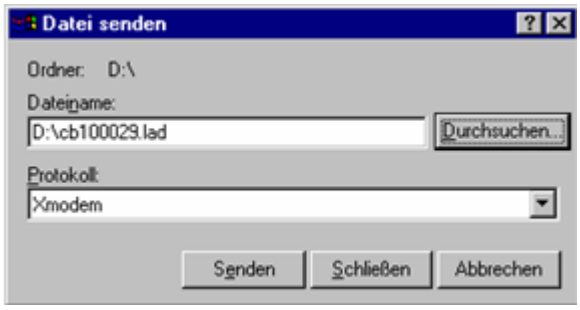


Bild 9-2 Dialogfenster - Datei senden

6. Geben Sie den Namen der zu ladenden Datei ein und wählen Sie als Protokoll Xmodem aus. Klicken Sie auf die Schaltfläche Senden, um den Uploadvorgang zu starten. Anschließend erscheint ein Dialogfeld, das den Fortschritt des Ladevorganges anzeigt:

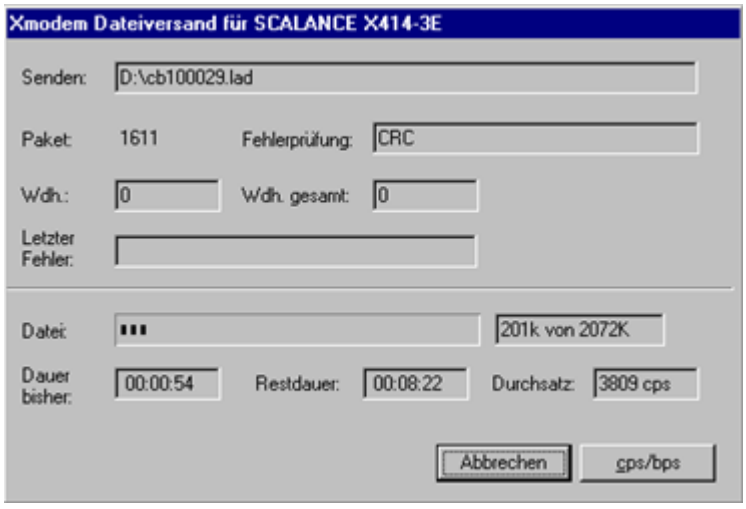


Bild 9-3 Xmodem Dateiversand

7. Nach dem Abschluss des Ladevorgangs zeigt Hyperterminal folgende Meldung an:

   FlashWrite .....COMPLETED

   Starten Sie das Gerät neu.

Hinweis

Unterbrechen Sie während des Ladens nicht die Verbindung zwischen PC und IE-Switch X-400/XR-300 oder die Versorgungsspannung zum IE-Switch X-400/XR-300.

Wird der Ladevorgang durch eine Signalleitungsstörung unterbrochen, läuft das Gerät beim nächsten Start mit der alten Firmware hoch. Sie müssen dann das Firmwareladen erneut durchführen.

Wenn die Firmware wegen eines Spannungsabfalls nicht vollständig im IE-Switch X-400/XR-300 abgespeichert werden konnte, dann erfolgt nach dem Hochlauf die Meldung "Can't load image from flash -> wrong crc". Auch in diesem Fall müssen Sie das Firmwareladen erneut durchführen.

9.2.2 Firmwareupdate über eine Ethernet-Schnittstelle und FTP

Durchführung

Wenn die Bootfunktion des IE-Switches über eine IP-Adresse verfügt und eine Ethernet-Verbindung zu einem PC bzw. PG besteht, müssen Sie folgende Schritte durchführen, um einen Firmwareupdate durchzuführen:

Hinweis

Befindet sich ein Gerät im Bootloader-Modus, so muss die Ethernet-Verbindung über Port 1 des Geräts hergestellt werden.

1. Öffnen Sie ein Konsolen-Fenster und geben Sie den Befehl ftp gefolgt von der IP-Adresse des IE-Switches ein. Beispiel:
   ftp 192.168.20.54
2. Geben Sie für Login und Passwort jeweils *siemens* ein.
3. Geben Sie den Befehl put gefolgt vom Namen der Firmwaredatei ein. Beispiel:
   put V211005.lad
4. Nach dem Abschluss des Ladevorgangs beendet der IE-Switch die FTP-Verbindung und führt einen Neustart durch. Warten Sie unbedingt bis der automatische Neustart erfolgt ist.

9.3 Firmware-Downgrade

Situation ab Firmware-Version V3.9.0 bis Firmware-Version V4.0.2

Ab der Firmware-Version V3.9.0 ist ein Downgrade der Firmware möglich, wenn das Gerät zu einem früheren Zeitpunkt mit der Ziel-Firmware ausgeliefert wurde.

ACHTUNG
Zurücksetzen auf Werkseinstellungen nach dem Firmware-Downgrade
Wenn Sie eine Firmware laden, die älter ist als die im Gerät vorhandene Firmware, dann müssen Sie das Gerät nach dem Laden der Firmware auf Werkseinstellungen zurücksetzen ("Reset to Factory Defaults").
Verwenden Sie für das Zurücksetzen des Geräts auf Werkseinstellungen den Taster SET/SELECT. Ein Zurücksetzen auf Werkseinstellungen über das WBM-Menü "System > Restart & Defaults" ist nach einem Firmware-Downgrade für die genannten Firmwareversionen nicht möglich.
Vor dem Zurücksetzen des Gerätes befindet sich die Konfiguration in einem inkonsistenten Zustand und darf keinesfalls gespeichert oder auf ein anderes Gerät übertragen werden!

Situation ab Firmware-Version V4.0.3

Ab der Firmware-Version V4.0.3 wird ein Firmware-Downgrade, das von einer höheren Firmware-Version als V4.0.3 aus stattfindet, erkannt. Beispiel: Downgrade von V4.0.4 auf V4.0.3. In einem solchen Fall wird das Gerät nach dem Firmware-Downgrade automatisch auf die Werkseinstellungen zurückgesetzt ("Reset to Factory Defaults").

Anhang A

A

A.1 PC-Anschluss an die serielle Schnittstelle eines SCALANCE X400

HyperTerminal

Das Programm HyperTerminal ist bei den Betriebssystemen Windows 95 / 98 / NT / 2000 / XP im Menü "Start > Programme > Zubehör" verfügbar. Sie können dieses Programm für folgende Aufgaben nutzen:

- Firmware Laden über die serielle Schnittstelle des IE-Switches X-400.
- Eingabe von Befehlen über das Command Line Interface

Vorgehensweise

Führen Sie folgende Schritte durch, um einen PC an den IE-Switch X-400 anzuschließen:

1. Verbinden Sie die serielle Schnittstelle des PCs mit der seriellen Schnittstelle des IE-Switches X-400 über ein handelsübliches Nullmodemkabel.
2. Wählen Sie im Programm HyperTerminal das Menü Datei > Neu. Es öffnet sich das Fenster Eigenschaften für eine Verbindung.
3. Stellen Sie die folgenden Parameter für die Verbindung ein:
   Bits pro Sekunde: 115200
   Datenbits 8
   Parität: Keine
   Stopbits: 1
   Protokoll: Kein

Pinbelegung X-400 (Nullmodemkabel)

Ein Nullmodemkabel hat für den Anschluss an den PC entweder eine 9-polige oder eine 24-polige Sub-D-Buchse und am anderen Ende eine 9-polige Sub-D-Buchse. Die folgende Tabelle zeigt die Pinbelegung für beide Kabelvarianten:

	PC-Anschluss			**SCALANCE X-400 Anschluss**
Signalname	25- pol. Buchse Pin	9 - pol. Buchse Pin	Verbunden mit	9 - pol. Buchse Pin
TD (Transmit Data)	2	3		3
RD (Receive Data)	3	2		2
RTS (Request to Send)	4	7		7
CTS (Clear to Send)	5	8		8
SG (Signal Ground)	7	5		5
DSR (Data Set Ready)	6	6		6
DTR (Data Terminal Ready)	20	4		4

Bild A-1 Tabelle Pinbelegung

Hinweis

Bei SIMATIC Programmiergeräten kann die serielle Schnittstelle als 25-polige Buchse ausgeführt sein. Verwenden Sie in einem solchen Fall einen sogenannten Gender Changer (25-polige Stiftleiste auf 25-polige Stiftleiste), der im PC-Fachhandel erhältlich ist.

A.2 PC-Anschluss an die serielle Schnittstelle eines SCALANCE XR300

HyperTerminal

Das Programm HyperTerminal ist bei den Betriebssystemen Windows 95 / 98 / NT / 2000 / XP im Menü "Start > Programme > Zubehör" verfügbar. Sie können dieses Programm für folgende Aufgaben nutzen:

- Firmware Laden über die serielle Schnittstelle des IE-Switches XR-300.
- Eingabe von Befehlen über das Command Line Interface

Vorgehensweise

Führen Sie folgende Schritte durch, um einen PC an den IE-Switch XR-300 anzuschließen:

1. Verbinden Sie die serielle Schnittstelle des PCs mit der seriellen Schnittstelle des IE-Switches XR-300 über das mitgelieferter Anschlusskabel für den Diagnoseport.
2. Wählen Sie im Programm HyperTerminal das Menü Datei > Neu. Es öffnet sich das Fenster Eigenschaften für eine Verbindung.
3. Stellen Sie die folgenden Parameter für die Verbindung ein:
   Bits pro Sekunde: 115200
   Datenbits 8
   Parität: Keine
   Stopbits: 1
   Protokoll: Kein

Pinbelegung XR-300 (Anschlusskabel Diagnoseport)

Hinweis

Bei Rack-Geräten (R) ist das Anschlusskabel für den Diagnoseport Teil des Lieferumfangs.

Ein Anschlusskabel Diagnoseport hat für den Anschluss an den PC eine 9-polige Sub-D-Buchse und am anderen Ende einen RJ11-Stecker. Die folgende Tabelle zeigt die Pinbelegung.

RJ11-Stecker		**SUB-D (9-polig, weiblich)**	
Pinnummer	**Belegung**	**Pinnummer**	**Belegung**
1	n.c.	1	n.c.
2	n.c.	2	RD (Receive Data)
3	TD (Transmit Data)	3	TD (Transmit Data)
4	SG (Signal Ground)	4	n.c.
5	RD (Receive Data)	5	SG (Signal Ground)
6	n.c.	6	n.c.
		7	n.c.
		8	n.c.
		9	n.c.

Anhang B

B

B.1 MIB-Variablen eines SCALANCE X300/X400

Wichtige Variablen im MIB-II-Standard

Im Folgenden sind einige SNMP-Variablen aus dem MIB II-Umfang zur Überwachung des Gerätestatus aufgelistet. MIB II beschreibt den Umfang an SNMP Variablen, die in der Regel von allen SNMP fähigen Geräten unterstützt wird.

Variablen im Verzeichnis System

Tabelle B-1 Variablen im Verzeichnis System

Variable	Zugriffsrechte	Beschreibung
sysDescr	Nur lesen	Es wird ein String bis zu 256 Zeichen verwendet. Dieser Wert enthält eine herstellerspezifische Identifikation des Gerätes.
sysObjectID	Nur lesen	Hier wird die Adresse (Objekt-Identifier) ausgegeben, unter der gerätespezifische SNMP-Variablen zu erreichen sind: **1.3.6.1.4.1.4196.1.1.5.4** Sind noch keine privaten OIDs deklariert, lautet der Objekt-Identifier [0,0]. Hier ist der Wert 0 vorgegeben.
sysUpTime	Nur lesen	Zeit nach dem letzten Rücksetzen (z.B. nach Power-Up). Die Angabe erfolgt in Hundertstelsekunden.
sysContact	Lesen und schreiben	Hier kann eine Kontaktperson eingetragen werden. (Default: Leerstring). Der mögliche Wert ist ein String mit maximal 255 Zeichen.
sysName	Lesen und schreiben	Hier kann ein Name für das Gerät eingetragen werden. (Default: Leerstring) Der mögliche Wert ist ein String mit maximal 255 Zeichen.

Variable	Zugriffsrechte	Beschreibung
sysLocation	Lesen und schreiben	Hier kann der Standortort des Gerätes eingetragen werden (Default: Leerstring). Der mögliche Wert ist ein String mit maximal 255 Zeichen.
sysService	Nur lesen	Zeigt die Funktionen (Services), die gemäß ISO/OSI-Modell durch die Komponente geleistet werden. Ebenenfunktionalität: • physical (z.B. Repeater) • datalink/subnetwork (z.B. Bridges , Switches) • internet (z.B. IP Gateways, router) • end to end (z.B. IP Hosts) • applications (z.B. E Mail Server) Datentyp: 32 Bit-Integer.

Variablen im Verzeichnis Interface

Tabelle B-2 Variablen im Verzeichnis Interface

Variable	Zugriffsrechte	Beschreibung
ifNumber	Nur lesen.	Die Anzahl der unterschiedlichen Interfaces, die in der Komponente verfügbar sind. Bei einem SCALANCE X414-3E wird für diese Variable der Wert 68 ausgegeben (26 physikalische Ports, 42 interne (virtuelle) Ports. Bei einem SCALANCE X408-2 wird für diese Variable der Wert 17 ausgegeben (8 physikalische Ports, 9 interne (virtuelle) Ports. Bei einem SCALANCE X-300 wird für diese Variable der Wert 21 ausgegeben (10 physikalische Ports, 11 interne (virtuelle) Ports. Datentyp: 32 Bit-Integer
ifDescr	Nur lesen.	Eine Beschreibung und gegebenenfalls zusätzliche Informationen für einen Port. Der mögliche Wert ist ein String mit maximal 255 Zeichen.
ifType	Nur lesen.	Bei IE-Switches ist der Wert ethernet-csmacd(6), gigabitEthernet(117) oder fastEther(62) eingetragen. Datentyp: Integer
ifSpeed	Nur lesen.	Datentransferrate des Ethernetports in Bits pro Sekunde. Bei IE-Switches wird entweder 10 Mbit/s, 100 Mbit/s oder 1000 Mbit/s angezeigt. Datentyp: Gauge.

Variable	Zugriffsrechte	Beschreibung
ifOperStatus	Nur lesen.	Der aktuelle Betriebszustand des Ethernetports. Es sind folgende Werte möglich: • up(1) • down(2) • testing(3) • unknown(4) • dormant(5) [Wartet auf externe Aktion] • notPresent(6) • lowerLayerDown(7) Der Zustand testing(3) zeigt an, dass keine Nutzdaten transportiert werden. Datentyp: Integer
ifLastChange	Nur lesen.	Zeit, seit der der ausgewählte Port in seinem aktuellen Arbeitszustand ist. Die Angabe erfolgt in Hundertstelsekunden. Datentyp: TimeTicks
ifInErrors	Nur lesen.	Anzahl der empfangenen Pakete, die wegen erkannter Fehler nicht an höhere Protokollschichten weitergegebenen wurden. Datentyp: Counter
ifOutErrors	Nur lesen.	Anzahl der Pakete, die wegen eines Fehlers nicht gesendet wurden. Datentyp: Counter

Portindizes

Bei SNMP können Sie Portbezeichnungen nicht in der Form "Slot.Port" angeben. SNMP adressiert die Ports mit Interface-Indizes. Um die Einstellungen eines Ports über SNMP zu ändern, verwenden Sie den AG-Index. Änderungen die über CLI oder WBM gemacht werden, sind über SNMP nur in den AG-Interfaces zu sehen. Werden Traps verwendet, ist zu beachten, dass in den SNMP-Bindings von z.B. Link Up Traps architekturbedingt die AP-Interfaces angegeben werden. Die folgenden Tabellen zeigen die Zuordnung von Interface-Index und Port.

Porttabellen für SCALANCE X-300, X408-2 und X414-3E

- Beispiel Porttabelle (gilt für SCALANCE X 300 / X408-2 / X-414-3E):
  Die Variable "ifOperStatus.51380225" ermittelt den Betriebszustand (up, down usw.) von Port 1 des IE-Switches.

Hinweis

Verfügbare Portanzahl wird durch Geräteausführung definiert

Je nach Geräteausführung sind entsprechende Ports verfügbar, z.B. sind bei der Geräteausführung X-306-1LD FE nur 7 Ports verfügbar.

Tabelle B-3 Porttabelle für SCALANCE X-300

Interface-Index AG / AP	Port	Portbezeichnung							
		X306-1LD FE	X307-3, X307-3LD, X308-2, X308-2LD, X308-2LH, X308-2LH+, X310, X310FE	X302-7 EEC, X307-2 EEC	X308-2M	X320-1 FE	X320-3LD FE	XR324-4M	XR324-12M
34603009/ 51380225	Port 1	1	1	1	1	1	1	1	1.1
34603010/ 51380226	Port 2	2	2	2	2	2	2	2	1.2
34603011/ 51380227	Port 3	3	3	3	3	3	3	3	2.1
34603012/ 51380228	Port 4	4	4	4	4	4	4	4	2.2
34603013/ 51380229	Port 5	5	5	5	5 / 1.1	5	5	5	3.1
34603014/ 51380230	Port 6	6	6	6	6 / 1.2	6	6	6	3.2
34603015/ 51380231	Port 7	7	7	7	7 / 2.1	7	7	7	4.1
34603016/ 51380232	Port 8	-	8	8	8 / 2.2	8	8	8	4.2
34603017/ 51380233	Port 9	-	9	9	-	9	9	9	5.1
34603018/ 51380234	Port 10	-	10	-	-	10	10	10	5.2
34603019/ 51380235	Port 11	-	-	-	-	11	11	11	6.1
34603020/ 51380236	Port 12	-	-	-	-	12	12	12	6.2
34603021/ 51380237	Port 13	-	-	-	-	13	13	13	7.1
34603022/ 51380238	Port 14	-	-	-	-	14	14	14	7.2
34603023/ 51380239	Port 15	-	-	-	-	15	15	15	8.1
34603024/ 51380240	Port 16	-	-	-	-	16	16	16	8.2
34603025/ 51380241	Port 17	-	-	-	-	17	17	1.1	9.1
34603026/ 51380242	Port 18	-	-	-	-	18	18	1.2	9.2
34603027/ 51380243	Port 19	-	-	-	-	19	19	2.1	10.1

Interface-Index AG / AP	Port	Portbezeichnung							
		X306-1LD FE	X307-3, X307-3LD, X308-2, X308-2LD, X308-2LH, X308-2LH+, X310, X310FE	X302-7 EEC, X307-2 EEC	X308-2M	X320-1 FE	X320-3LD FE	XR324-4M	XR324-12M
34603028/ 51380244	Port 20	-	-	-	-	20	20	2.2	10.2
34603029/ 51380245	Port 21	-	-	-	-	21	21	3.1	11.1
34603030/ 51380246	Port 22	-	-	-	-	-	22	3.2	11.2
34603031/ 51380247	Port 23	-	-	-	-	-	23	4.1	12.1
34603032/ 51380248	Port 24	-	-	-	-	-	-	4.2	12.2

Tabelle B-4 Porttabelle für SCALANCE X408-2 und X414-3E

Interface-Index AG / AP	Port	Portbezeichnung			
		X408-2	X414-3E		
			ohne Extender	mit elektrischem Extender	mit optischem Extender
34603009 / 51380225	Port 1	5.1	5.1	5.1	5.1
34603010 / 51380226	Port 2	5.2	5.2	5.2	5.2
34603011 / 51380227	Port 3	6.1	6.1	6.1	6.1
34603012 / 51380228	Port 4	6.2	6.2	6.2	6.2
34603013 / 51380229	Port 5	8.1	7.1	7.1	7.1
34603014 / 51380230	Port 6	8.2	7.2	7.2	7.2
34603015 / 51380231	Port 7	8.3	9.1	9.1	9.1
34603016 / 51380232	Port 8	8.4	9.2	9.2	9.2
34603017 / 51380233	Port 9	-	9.3	9.3	9.3
34603018 / 51380234	Port 10	-	9.4	9.4	9.4
34603019 / 51380235	Port 11	-	10.1	10.1	10.1
34603020 / 51380236	Port 12	-	10.2	10.2	10.2
34603021 / 51380237	Port 13	-	10.3	10.3	10.3
34603022 / 51380238	Port 14	-	10.4	10.4	10.4
34603023 / 51380239	Port 15	-	11.1	11.1	11.1
34603024 / 51380240	Port 16	-	11.2	11.2	11.2
34603025 / 51380241	Port 17	-	11.3	11.3	11.3
34603026 / 51380242	Port 18	-	11.4	11.4	11.4

Interface-Index AG / AP	Port	Portbezeichnung			
		X408-2	X414-3E		
			ohne Extender	mit elektrischem Extender	mit optischem Extender
34603027 / 51380243	Port 19	-	-	12.1	12.1
34603028 / 51380244	Port 20	-	-	12.2	12.2
34603029 / 51380245	Port 21	-	-	12.3	13.1
34603030 / 51380246	Port 22	-	-	12.4	13.2
34603031 / 51380247	Port 23	-	-	13.1	14.1
34603032 / 51380248	Port 24	-	-	13.2	14.2
34603033 / 51380249	Port 25	-	-	13.3	15.1
34603034 / 51380250	Port 26	-	-	13.4	15.2

Wichtige Private-MIB-Variablen eines IE-Switches

OID

Die Private MIB-Variablen des IE-Switches haben folgenden Object Identifier:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).ad(4196).adProductMibs(1).simaticNet(1).iScalanceX(5).iScalanceX300X400(4)

Tabelle B-5 Private-MIB-Variablen eines IE Switches

Variable	Zugriffsrechte	Beschreibung
snX300X400FaultState	Nur lesen	Zeigt den Status des Meldekontakts an. Mögliche Werte: • 1 kein Fehler • 2 Fehler. Datentyp: Integer
snX300X400ReportFaultIndex	Nur lesen	Fehler bekommen in der Reihenfolge ihres Auftretens einen aufsteigenden Index. Diese 4 Byte große Variable gibt den Index an.
snX300X400ReportFaultState	Nur lesen	Beinhaltet die zu einem Index gehörende Fehlermeldung.
snX300X400RmMode	Nur lesen	Der Redundanzmanager-Modus: • Der IE-Switch ist Redundanzmanager. • Der IE-Switch ist kein Redundanzmanager.

Variable	Zugriffsrechte	Beschreibung
snX300X400RmState	Nur lesen	Zeigt an, ob der Redundanzmanager aktiv oder passiv ist. Mögliche Werte: • Der Redundanzmangager ist passiv. Der IE-Switch arbeitet als Redundanzmanager und hat den Ring geöffnet, d.h. die an ihn angeschlossene Linie von IE-Switches arbeitet fehlerfrei. Der Zustand "Passiv" wird auch angezeigt, wenn der Redundanzmanager-Mode disabled ist. • Der Redundanzmangager ist aktiv. Der IE-Switch arbeitet als Redundanzmanager und hat den Ring geschlossen, d.h. die an ihn angeschlossene Linie von IE-Switches ist unterbrochen (Fehlerfall). Der Redundanzmanager schaltet die Verbindung zwischen den Ringports durch und stellt dadurch wieder eine funktionierende Linienkonfiguration her. Datentyp: Integer
snX300X400RmStateChanges	Nur lesen	Zeigt an, wie oft der Redundanzmanager aktiv geschaltet wurde. Datentyp: Counter
snX300X400StandbyMode	Nur lesen	Der Standby-Funktions-Modus: • Die Standby-Funktion ist aktiviert. • Die Standby-Funktion ist deaktiviert.
snX300X400StandbyState	Nur lesen	Zeigt den Standby Status an: • 1 Gerät ist Master und passiv. • 3 Gerät ist Slave und passiv • 5 Gerät ist Master und aktiv • 7 Gerät ist Slave und aktiv • 257 Gerät sucht Partner für Standby Verbindung • 300 Standby-Funktion ist inaktiv • Datentyp: Integer
snX300X400StandbyStateChanges	Nur lesen	Zeigt an, wie oft der Standby Status aktiv geschaltet wurde. Datentyp: Counter
snBootStrapVersion	Nur lesen	Die Firmwareversion des Bootloaders im Format *major.minor*.
snHwVersion	Nur lesen	Die Hardwareversion des Systems im Format *major.minor*.

Variable	Zugriffsrechte	Beschreibung
snSwVersion	Nur lesen	Die Software-Version des Systems.
snInfoSerialNr	Nur lesen	Die Seriennummer des Produkts.
snMacAddressBase	Nur lesen	Die Base-MAC-Adresse des IE-Switches.
snX300X400ModuleIdentMLFB	Nur lesen	Die MLFB-Nummer des Moduls.
snX300X400PowerSupply1State	Nur lesen	Der Zustand des Spannungseingangs 1.
snX300X400PowerSupply2State	Nur lesen	Der Zustand des Spannungseingangs 2.
snX300X400ReportDigitalInState	Nur lesen	Zum digitalen Eingang gehörender Status. (SCALANCE X414-3E)

Anhang C

C

C.1 Tagging von Frames

Erweiterung der Ethernet-Frames um vier Byte

Für die Funktionen CoS (Class of Service, Frame-Priorisierung) und portbasiertes VLAN (Virtuelles Netzwerk) wurde in der Norm IEEE 802.1 Q die Erweiterung der Ethernet-Frames um den sogenannten VLAN-Tag festgelegt.

Hinweis

Durch den VLAN-Tag erhöht sich die zulässige Gesamtlänge eines Ethernet-Frames von 1518 auf 1522 Bytes. Es muss geprüft werden, ob die Endteilnehmer am Netz diese Länge / diesen Frametyp verarbeiten können. Ist dies nicht der Fall, dürfen an diese Teilnehmer nur Frames mit der Standardlänge gesendet werden.

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

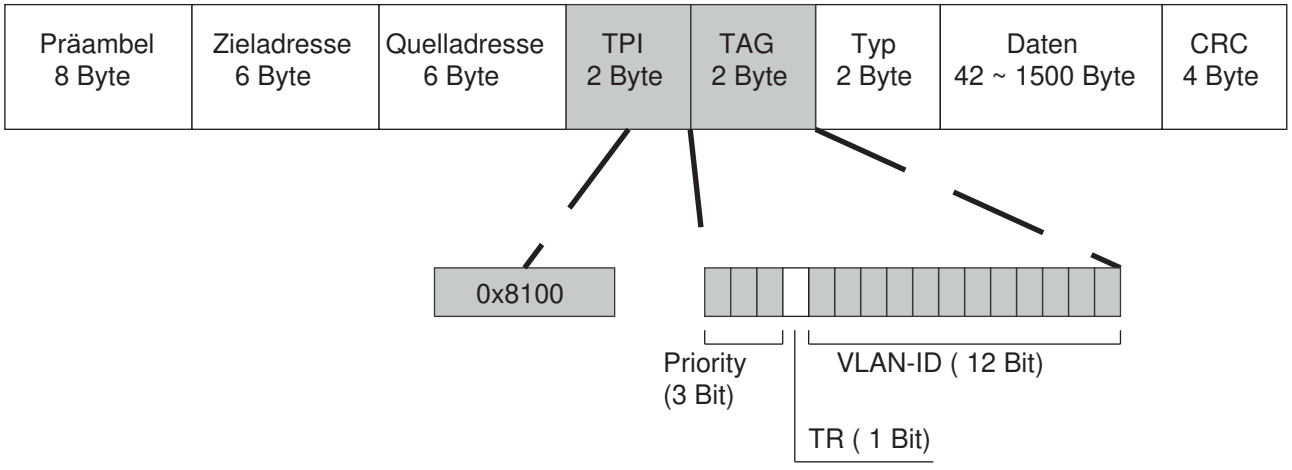


Bild C-1 Aufbau eines getaggten Frames

Die zusätzlichen Bytes beinhalten das Tag Protocol Identifier-Field und das Tag Control Information Field.

Tag Protocol Identifier Field

Die ersten 2 Bytes bilden das sogenannte **T**ag **P**rotocol **I**dentifier-Field (TPI) und sind fest mit 0x8100 belegt ist. Dieser Wert gibt an, dass das Datenpaket VLAN-Informationen oder Prioritätenangabe beinhaltet.

Tag Control Information Field

Die 2 Byte des Tag Control Information Field (TCI) beinhalten folgende Informationen:

CoS– Priorisierung

In dem getaggten Frame gibt es 3 Bits für die Priorität., die auch als **C**lass **o**f **S**ervice (CoS) bezeichnet werden. Die Priorisierung nach IEEE 802.1p lautet wie folgt:

CoS-Bits	Typ der Daten
000	Zeitunkritischer Datenverkehr (less then best effort [Grundeinstellung])
001	Normaler Datenverkehr (best effort [Hintergrund])
010	Reserviert (Standard)
011	Reserviert (excellent effort)
100	Datenübertragung mit max. 100ms Verzögerung
101	Garantierter Service, interaktives Multimedia
110	Garantierter Service, interaktives Sprachübertragung
111	Reserviert

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

Ein IE-Switch besitzt vier parallele Warteschlangen, in denen die verschieden priorisierten Frames abgearbeitet werden. Dabei werden zuerst die Frames mit der höchsten Priorität ("Strict Priority"-Verfahren) abgearbeitet. Dieses Verfahren gewährleistet auch bei einem hohen Datenaufkommen, dass die Frames mit der höchsten Priorität auf jeden Fall gesendet werden.

Canonical Format Identifier

Das TR-Bit dient als Kennung für einen **T**oken **R**ing Encapsulation Process.

VLAN–ID

Mit den restlichen 12 Bits können bis zu 4095 VLAN-IDs gebildet werden (VLAN ID 4095 ist unzulässig). Dabei gelten folgende Festlegungen:

VLAN-ID	Bedeutung
0	Der Frame beinhaltet nur Prioritätsinformation (Priority Tagged Frames) und keine gültige VLAN Kennung.
1 - 4094	Gültige VLAN-Kennung, der Frame ist einem VLAN zugeordnet, es kann zusätzlich auch Prioritätsinformationen besitzen.

Anhang D

D

D.1 Fehlermeldungen des SCALANCE X300 / X400

Hinweis

Bei aktivierter Link Aggregation kann anstelle einer Portnummer auch die Nummer der Aggregation angegeben werden (z. B. AG1).

Meldungen beim Auftreten und nach der Behebung eines Fehlers

Tabelle D-1 Fehlermeldungen, die einem Fehlerzustand (Fehler-LED) zugeordnet sind

Meldungen beim Auftreten eines Fehlers	Meldungen nach der Behebung eines Fehlers
Link down on <Portnummer>.	Link up on <Portnummer>.
Non-recoverable ring error on <Portnummer>.	Ring error on <Portnummer> gone.
Other redundancy manager detected ... MAC <MAC-Adresse> on <Portnummer>.	Other redundancy manager gone ... MAC <MAC-Adresse> on <Portnummer>.
<HRP> ring manager activated.	<HRP> ring manager falls back to client.
<HRP> ring manager enters active state.	<HRP> ring manager falls back to passive state.
Standby device enters active state.	Standby device enters passive state.
Standby is waiting for <master | slave>.	Standby connection established to <master | slave> <MAC-Adresse> on <Portnummer>.
Standby <partner | observer> lost connection to <master | slave> <MAC-Adresse> on <Portnummer>.	Standby <partner | observer> reconnected to <master | slave> <MAC-Adresse> on <Portnummer>.
Unsupported version <Versionsnummer> for standby protocol detected.	Unsupported version <Versionsnummer> for standby protocol gone.
Second observer detected. MAC <MAC-Adresse> at <Portnummer>.	Second observer gone. MAC <MAC-Adresse> at <Portnummer>.
Observer: RM switches frames on isolated port.	Observer: RM stopped switching on isolated port.
Unexpected traffic received on observer <Portnummer>.	Unexpected traffic on observer <Portnummer> gone.
Observer: Timeout for test frames detected on port <Portnummer> while RM signals "passive".	Observer: Timeout for test frames on port <Portnummer> is gone.
Observer: RM signals active but RM test frames are received on both ring ports.	Observer: RM signals right state.
Observer: RM runs incompatible software version <Versionsnummer>.	Observer: RM's incompatible software version <Versionsnummer> gone.
Observer: RM test frame timeout on both ring ports.	Observer: RM test frames received.

Meldungen beim Auftreten eines Fehlers	Meldungen nach der Behebung eines Fehlers
Observer stopped recovering because of to many (<Fehlerzahl>) repeated errors. (Observer needs to be restarted (WBM/CLI) manually).	Observer restarted because of user command.
Power down on line <ID der Spannungsversorgung>.	Power up on line <ID der Spannungsversorgung>.
Internal error: <Spannung> V power down.	Internal error gone: <Spannung> V power is back.
Wrong module <Modulname> on slot <Slotnummer> (ID: <Modul-ID>).	Wrong module <Modulname> on slot <Slotnummer> removed.
C-PLUG not accepted. See System C-PLUG mask for details.	C-PLUG accepted.
C-PLUG interface unmounted. Restart required.	C-PLUG interface mounted.
C-PLUG missing.	C-PLUG detected.
Media module for ring <Portnummer> missing.	Media module for ring <Portnummer> detected.
DIP switch <Name des Schalters> changed. Restart required.	DIP switch <Name des Schalters> set back to original state.
DIP switch <Name des Schalters> differs from C-PLUG. Restart required.	DIP switch <Name des Schalters> set back to state saved on C-PLUG.
Internal error(s) and/or exception(s) occurred.	Internal error(s) and/or exception(s) confirmed.
Device boot up incomplete.	Device boot up complete.
RM <MAC-Adresse> lost.	RM <MAC-Adresse> detected.
Media module for standby <Portnummer> missing.	Media module for standby <Portnummer> detected.
PNIO fault - please use STEP 7 for diagnostics.	PNIO fault - gone.
PNIO connection established.	PNIO connection terminated.
Severe module change detected. Restart required.	Severe module change reverted.
DIP switch settings manipulated ... → Redundancy will be started after next restart.	DIP switch settings reset ... → Redundancy mode will not change after next restart.
Authentication status on <Portnummer>: FAILED! Reason: %s.	Authentication status on <Portnummer>: OK. Reason: %s.
Standby <observer | partner> freezes current state <active | passive> because <master | slave> <MAC-Adresse> gone.	Unfreeze standby state <active | passive> because partner <MAC-Adresse> became visible.
Default route is stored in hardware.	Default route no longer in hardware.
Non-recoverable error on ring %u: RM receives test frames from only one ring port.	Non-recoverable error gone on ring %u: RM receives test frames from both ring ports.
Non-recoverable error on ring %u: Another redundancy manager detected.	Non-recoverable error gone on ring %u: Other redundancy manager gone.
Last MRP manager in ring %d won't stop on ring ports <Portnummer> and <Portnummer> (danger of network loops).	MRP ring %d manager may stop now (no danger of network loops anymore).
Redundancy mode transition not completed !\nis: \"%s\", should: \"%s\".	Redundancy mode transition to \"%s\" completed.
Erroneous connected ring line on <Portnummer> (should <Portnummer>).	Erroneous connected ring line removed on <Portnummer>.
Main power usage threshold exceeded.	Main power usage below threshold again.

Meldungen beim Auftreten eines Fehlers	Meldungen nach der Behebung eines Fehlers
Unexpected port assembly. Change device name to %s.	Port assembly known.
Unknown SFP module on <Portnummer> (vendor: \"%$str\").	Unknown SFP module on <Portnummer> removed.
SFP module on <Portnummer> is not supported and remains deactivated.	Not supported SFP module on <Portnummer> removed.
Signaling contact controlled by user configuration.	Signaling contact controlled by error state.
Local loop detected on <Portnummer>. Port disabled.	<Portnummer> is enabled again after being disabled by loop detecion.
Local loop detected on <Portnummer>. Port disabled for <Anzahl> seconds.	<Portnummer> is enabled again after being disabled by loop detecion.
Remote loop detected on <Portnummer>. Port disabled.	<Portnummer> is enabled again after being disabled by loop detecion.
Remote loop detected on <Portnummer>. Port disabled for <Anzahl> seconds.	<Portnummer> is enabled again after being disabled by loop detecion.
Local loop detected on <Portnummer>.	<Portnummer> is enabled again for loop detecion.
Remote loop detected on <Portnummer>.	<Portnummer> is enabled again for loop detecion.
Standby <partner | observer> conflicts with <active | passive> state.	Standby <partner | observer>'s state conflict resolved.
Standby <partner | observer> conflicts with observer <on | off> configuration.	Standby <partner | observer>'s observer configuration conflict resolved.
Standby <partner | observer> conflicts with <master | slave> role.	Standby <partner | observer>'s role conflict resolved.
Standby slave: At least one port has no link.	Standby slave: All ports linked up.
FMP-Port <Portnummer>: Maintenance required, Rx-Power: <empfangene Leistung> [dBm], Power Loss: <Verlustleistung> [dB]	FMP-Port <Portnummer>: OK
FMP-Port <Portnummer>: Maintenance demanded, Rx-Power: <empfangene Leistung> [dBm], Power Loss: <Verlustleistung> [dB]	FMP-Port <Portnummer>: OK
POF-Port <Portnummer>: Maintenance required, Rx-Power: <empfangene Leistung> [dBm], Power Margin: <Leistungsreserve> [dB]	POF-Port <Portnummer>: OK
POF-Port <Portnummer>: Maintenance demanded, Rx-Power: <empfangene Leistung> [dBm], Power Margin: <Leistungsreserve> [dB]	POF-Port <Portnummer>: OK
Link Check: Broken link on <Portnummer> indicated by <Fehlerbeschreibung>. Port disabled.	Link Check: Link on <Portnummer> OK. Port enabled.
Link Check: Multiple partners detected on <Portnummer>.	Link Check: Partner detection reset on <Portnummer>.
Link Check: Unapproved configuration. Disable Link Check on <Portnummer>.	Link Check: Unapproved configuration resolved on <Portnummer>.

Meldungen zur Information über ein auftretendes Ereignis

Die nachfolgenden Meldungen dienen Ihnen zur Information über Ereignisse, die nicht in direktem Zusammenhang zu einem Fehlerzustand (Fehler-LED) stehen:

- User entry: <Benutzereingabe>
- Unknown command <Befehl> for <Protokollname> protocol received.
- Device is configured to ring <off | ARD | HRP client | MRP client | HRP manager | MRP manager>.
- Standby function <Master | Slave>.
- Observer started.
- Observer stopped.
- Observer contacted Redundancy Manager <MAC-Adresse>.
- Standby is waiting for <partner | observer>.
- Standby <partner | observer> connected to <master | slave> <MAC-Adresse> <Portnummer>.
- Standby <partner | observer> lost connection to <master | slave> <MAC-Adresse> <Portnummer>.
- Port <Portnummer> is isolated ring port.
- Port <Portnummer> is static ring port.
- No SMTP connection to mail server.
  Server IP address <IP-Adresse> TCP port <TCP-Portnummer>.
- No SMTP application found.
  Server IP address <IP-Adresse> TCP port <TCP-Portnummer>.
- SMTP (E-Mail) connection aborted. Server IP address <IP-Adresse>.
- Unable to send message to syslog server. Please check syslog socket configuration.
- Connected to syslog server.
- SNMP: Authentification failure.
- R)STP: new root bridge detected.
- (R)STP: topology change detected.
- Unable to send E-Mail(s). Please check IP configuration.
- Unable to send trap(s). Please check IP configuration.
- Failure reply code <Fehlercode> from SMTP server.
- Restart requested.
- No C-PLUG found. Internal flash memory used.
- An empty C-PLUG was found.
- C-PLUG format request.
- A filled C-PLUG was found.
- A corrupted C-PLUG was found.
- C-PLUG removed at runtime.

- C-PLUG plugged in at runtime.
- RMON rising alarm occurred.
- RMON falling alarm occurred.
- Ring redundancy enabled.
- Ring redundancy disabled.
- (R)STP protocol enabled.
- (R)STP protocol disabled.
- Disabled (R)STP because ring redundancy is enabled.
- DIP settings taken from C-PLUG.
  RM=<ON|OFF>, STBY=<ON|OFF>, R1=<ON|OFF>, R2=<ON|OFF>
- (R)STP topology change detected while (R)STP is off. Aging time will be reduced to <Zeit in s> sec for at least <Zeit in s> sec.
- Set aging time back to original value <Zeit in s> sec.
- No connection to SNTP server. Server IP address <IP-Adresse>.
- Connected to SNTP server. Server IP address <IP-Adresse>.
- Enabled link status monitoring on ring ports.
- Changed port VLAN ID of the ring ports to 1.
- Disabled GVRP because ring redundancy is enabled.
- Disabled GMRP because ring redundancy is enabled.
- Disabled mirroring because monitor port is ring port.
- (Re)enabled ring ports (because disabled by user).
- Disabled port lock on ring ports.
- Warning: ring ports have different static VLAN configuration.
- Warning: ring ports have different VLAN port configuration.
- Warning: ring ports have different static multicast configuration.
- Warning: ring ports have different load limits configuration.
- Enter fault state: port <Portnummer> enabled for link status monitoring and link down.
- Leave fault state: port <Portnummer> disabled for link status monitoring.
- Enter fault state: power line <ID der Spannungsversorgung> enabled for power monitoring and power down.
- Leave fault state: power line <ID der Spannungsversorgung> disabled for power monitoring.
- <CLI | WBM | SSH>: Authentication failure.
- Warning: OSPF consumed too much memory and is shut down.
- Duplicate IP address <IP-Adresse> sent from <MAC-Adresse>
- IN <Nummer des digitale Eingangs> (<Name des Eingangs>) <high | low>

- VRRP: Virtual Router <Nummer des Routers> on VLAN <VLAN-ID> transitioned to <Master | Backup | Disabled | Initialize | Invalid> state.
- PNIO configuration invalid, conflict with standby.
- PNIO configuration invalid, conflict with HRP.
- PNIO configuration invalid, conflict in MRP ring ports: <Konfliktursache>
- PNIO configuration invalid, conflict in alternative redundancy configuration.
- PNIO configuration invalid, conflict detected: <Beschreibung des Konfigurationskonflikts>
- Standby observer function <started | stopped>
- Standby: Take on the <master | slave> role
- Authentication success, Port: <Portnummer> VLAN: <VLAN-ID> MAC: <MAC-Adresse>
- Authentication failed, Port: <Portnummer> VLAN: <VLAN-ID> MAC: <MAC-Adresse>
- Authentication for Guest-VLAN, Port: <Portnummer> VLAN: <VLAN-ID> MAC: <MAC-Adresse>
- PoE Port: <Portnummer> power up, Class: <Leistungsklasse>, allocated power: <reservierte Leistung> mW
- PoE Port: <Portnummer> power down
- PoE Port: <Portnummer> enabled
- PoE Port: <Portnummer> disabled due to <Begründung für die Abschaltung>

Anhang E

E

E.1 Gleiche Konfiguration auf mehreren IE-Switches verwenden

Die folgende Liste zeigt, auf welchen IE-Switches Sie die gleiche Konfiguration verwenden können.

Sie können Ihr Gerät über die Artikelnummer identifizieren.

Gerät	Ladbare Konfigurationen
6GK5 307-3BL00-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 307-3BM00-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3

Gerät	Ladbare Konfigurationen
6GK5 308-2FL00-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 308-2FM00-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 308-2FN00-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3

Gerät	Ladbare Konfigurationen
6GK5 308-2FP00-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 310-0BA00-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 310-0FA00-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3

Gerät	Ladbare Konfigurationen
6GK5 307-3BL10-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 307-3BM10-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 308-2FL10-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3

Gerät	Ladbare Konfigurationen
6GK5 308-2FM10-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 308-2FN10-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 308-2FP10-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3

Gerät	Ladbare Konfigurationen
6GK5 310-0BA10-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 310-0FA10-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 308-2GG00-2AA2	6GK5 308-2GG00-2AA2 6GK5 308-2GG00-2CA2
6GK5 308-2GG00-2CA2	6GK5 308-2GG00-2AA2 6GK5 308-2GG00-2CA2
6GK5 308-2QG00-2AA2	6GK5 308-2GG00-2AA2 6GK5 308-2GG00-2CA2 6GK5 308-2QG00-2AA2
6GK5 302-7GD00-1EA3	6GK5 302-7GD00-1EA3 6GK5 302-7GD00-2EA3 6GK5 302-7GD00-1GA3 6GK5 302-7GD00-2GA3 6GK5 302-7GD00-3EA3 6GK5 302-7GD00-4EA3 6GK5 302-7GD00-3GA3 6GK5 302-7GD00-4GA3

Gerät	Ladbare Konfigurationen
6GK5 302-7GD00-2EA3	6GK5 302-7GD00-1EA3 6GK5 302-7GD00-2EA3 6GK5 302-7GD00-1GA3 6GK5 302-7GD00-2GA3 6GK5 302-7GD00-3EA3 6GK5 302-7GD00-4EA3 6GK5 302-7GD00-3GA3 6GK5 302-7GD00-4GA3
6GK5 302-7GD00-1GA3	6GK5 302-7GD00-1EA3 6GK5 302-7GD00-2EA3 6GK5 302-7GD00-1GA3 6GK5 302-7GD00-2GA3 6GK5 302-7GD00-3EA3 6GK5 302-7GD00-4EA3 6GK5 302-7GD00-3GA3 6GK5 302-7GD00-4GA3
6GK5 302-7GD00-2GA3	6GK5 302-7GD00-1EA3 6GK5 302-7GD00-2EA3 6GK5 302-7GD00-1GA3 6GK5 302-7GD00-2GA3 6GK5 302-7GD00-3EA3 6GK5 302-7GD00-4EA3 6GK5 302-7GD00-3GA3 6GK5 302-7GD00-4GA3
6GK5 302-7GD00-3EA3	6GK5 302-7GD00-1EA3 6GK5 302-7GD00-2EA3 6GK5 302-7GD00-1GA3 6GK5 302-7GD00-2GA3 6GK5 302-7GD00-3EA3 6GK5 302-7GD00-4EA3 6GK5 302-7GD00-3GA3 6GK5 302-7GD00-4GA3
6GK5 302-7GD00-4EA3	6GK5 302-7GD00-1EA3 6GK5 302-7GD00-2EA3 6GK5 302-7GD00-1GA3 6GK5 302-7GD00-2GA3 6GK5 302-7GD00-3EA3 6GK5 302-7GD00-4EA3 6GK5 302-7GD00-3GA3 6GK5 302-7GD00-4GA3
6GK5 302-7GD00-3GA3	6GK5 302-7GD00-1EA3 6GK5 302-7GD00-2EA3 6GK5 302-7GD00-1GA3 6GK5 302-7GD00-2GA3 6GK5 302-7GD00-3EA3 6GK5 302-7GD00-4EA3 6GK5 302-7GD00-3GA3 6GK5 302-7GD00-4GA3

Gerät	Ladbare Konfigurationen
6GK5 302-7GD00-4GA3	6GK5 302-7GD00-1EA3 6GK5 302-7GD00-2EA3 6GK5 302-7GD00-1GA3 6GK5 302-7GD00-2GA3 6GK5 302-7GD00-3EA3 6GK5 302-7GD00-4EA3 6GK5 302-7GD00-3GA3 6GK5 302-7GD00-4GA3
6GK5 307-2FD00-1EA3	6GK5 307-2FD00-1EA3 6GK5 307-2FD00-2EA3 6GK5 307-2FD00-1GA3 6GK5 307-2FD00-2GA3 6GK5 307-2FD00-3EA3 6GK5 307-2FD00-4EA3 6GK5 307-2FD00-3GA3 6GK5 307-2FD00-4GA3
6GK5 307-2FD00-2EA3	6GK5 307-2FD00-1EA3 6GK5 307-2FD00-2EA3 6GK5 307-2FD00-1GA3 6GK5 307-2FD00-2GA3 6GK5 307-2FD00-3EA3 6GK5 307-2FD00-4EA3 6GK5 307-2FD00-3GA3 6GK5 307-2FD00-4GA3
6GK5 307-2FD00-1GA3	6GK5 307-2FD00-1EA3 6GK5 307-2FD00-2EA3 6GK5 307-2FD00-1GA3 6GK5 307-2FD00-2GA3 6GK5 307-2FD00-3EA3 6GK5 307-2FD00-4EA3 6GK5 307-2FD00-3GA3 6GK5 307-2FD00-4GA3
6GK5 307-2FD00-2GA3	6GK5 307-2FD00-1EA3 6GK5 307-2FD00-2EA3 6GK5 307-2FD00-1GA3 6GK5 307-2FD00-2GA3 6GK5 307-2FD00-3EA3 6GK5 307-2FD00-4EA3 6GK5 307-2FD00-3GA3 6GK5 307-2FD00-4GA3
6GK5 307-2FD00-3EA3	6GK5 307-2FD00-1EA3 6GK5 307-2FD00-2EA3 6GK5 307-2FD00-1GA3 6GK5 307-2FD00-2GA3 6GK5 307-2FD00-3EA3 6GK5 307-2FD00-4EA3 6GK5 307-2FD00-3GA3 6GK5 307-2FD00-4GA3

Gerät	Ladbare Konfigurationen
6GK5 307-2FD00-4EA3	6GK5 307-2FD00-1EA3 6GK5 307-2FD00-2EA3 6GK5 307-2FD00-1GA3 6GK5 307-2FD00-2GA3 6GK5 307-2FD00-3EA3 6GK5 307-2FD00-4EA3 6GK5 307-2FD00-3GA3 6GK5 307-2FD00-4GA3
6GK5 307-2FD00-3GA3	6GK5 307-2FD00-1EA3 6GK5 307-2FD00-2EA3 6GK5 307-2FD00-1GA3 6GK5 307-2FD00-2GA3 6GK5 307-2FD00-3EA3 6GK5 307-2FD00-4EA3 6GK5 307-2FD00-3GA3 6GK5 307-2FD00-4GA3
6GK5 307-2FD00-4GA3	6GK5 307-2FD00-1EA3 6GK5 307-2FD00-2EA3 6GK5 307-2FD00-1GA3 6GK5 307-2FD00-2GA3 6GK5 307-2FD00-3EA3 6GK5 307-2FD00-4EA3 6GK5 307-2FD00-3GA3 6GK5 307-2FD00-4GA3
6GK5 324-*	6GK5 324-* Sie können auf allen SCALANCE XR324-Geräten, inkl. EEC und PoE, die gleiche Konfiguration verwenden.
6GK5 414-3FC00-2AA2	6GK5 414-3FC10-2AA2
6GK5 414-3FC10-2AA2	6GK5 414-3FC00-2AA2

Verwendete Verschlüsselungsverfahren (Ciphers)

F

In den nachfolgenden Tabellen sind die Verschlüsselungsverfahren (Ciphers) aufgelistet, die SCALANCE X-300/X-400 verwendet.

SSL

Kategorie	IANA-Name	Hexadezimalwert	Standardmäßig aktiviert
Verschlüsselungssuite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	C023	✓
Verschlüsselungssuite	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	C0AC	✓
Verschlüsselungssuite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	C02B	✓
Verschlüsselungssuite	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	C024	✓
Verschlüsselungssuite	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	C0AD	✓
Verschlüsselungssuite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	C02C	✓
Protokollversion	TLSv1.2	-	✓

SSH

Kategorie	IANA-Name	Hexadezimalwert	Standardmäßig aktiviert
Verschlüsselungsverfahren (enc)	aes128-ctr	-	✓
Verschlüsselungsverfahren (enc)	aes192-ctr	-	✓
Verschlüsselungsverfahren (enc)	aes256-ctr	-	✓
Host-Schlüssel (key)	ecdsa-sha2-nistp256	-	✓
Schlüsselaustausch (kex)	ecdh-sha2-nistp256	-	✓
Schlüsselaustausch (kex)	ecdh-sha2-nistp384	-	✓
Schlüsselaustausch (kex)	ecdh-sha2-nistp521	-	✓
MAC	hmac-sha2-256	-	✓
MAC	hmac-sha2-512	-	✓
Protokollversion	SSHv2.0	-	✓

RADIUS

Kategorie	Verfahren	Hexadezimal-wert	Standardmäßig aktiviert
Integritätsalgorithmus	MD5	-	✓

Index

A

Access-Control, 25
ACL, 178
Adressfilterung, 178
Aging, 146
Aging Time, 147, 192
Alarmereignisse, 126
Anschlusskabel Diagnoseport
    Pinbelegung, 391
Authentifizierung, 170, 173
    802.1x, 174
    Authentifizierungsserver, 170
    Guest VLAN, 174
    MAC Authentication, 174
    Re-Authentication, 174
Auto-Crossover, 22
Autonegotiation, 152, 357

B

BA - Betriebsanleitung, 20
BAK - Kompaktbetriebsanleitung, 20
Betriebsart
    Halbduplexbetrieb, 22, 25
    Vollduplexbetrieb, 22, 25
BOOTP, 26, 36, 39, 102
BPDU (Bridge Protocol Data Unit), 215

C

CIST Port Parameters, 228
CLI-Befehl, 45
    Symbolik Darstellung, 47
    Verkürzte Befehlseingabe, 46
Collisions, 293
CoS (Class of Service), 402
C-PLUG, 24
CRC, 293

D

Datenrate, 22
DCP, 102
DCP Read Only, 102
Default Gateway, 53, 102
DHCP, 26, 36, 39, 102
DHCP Option 82, 27
Digitaler Eingang, 124
DLF (Destination Lookup Failure, 196
DSCP, 239

E

E-Mail-Funktion, 25, 100, 126
    Alarmereignisse, 126
    Netzüberwachung, 126
Enhanced Passive Listening Compatibility, 150
Ethernet-Schnittstelle, 21
Event Log Tabelle, 25

F

Filter
    Adressfilterung, 178
    Filterkonfiguration, 180
    Filtertabelle, 179
Firmware-Downgrade, 387
Firmwareupdate, 383
Flusskontrolle, 25
FMP-Diagnose, 273
Forward Delay, 219
Fragments, 293

G

Gigabit Ethernet-Port, 22
Glossar, 3
GMRP, 148, 191
Guest VLAN, 174
GVRP, 149, 211, 218

H

HRP, 34
HTTP, 55
HyperTerminal, 38, 389, 390

I

IEEE 1588 Uhrzeitsynchronisation (PTP), 256
IEEE 802.1x, 174
IEEE 802.1X, 170

IGMP, 148
IGMP Configuration, 27
IGMP Query, 27
In-Band-Port, 37
IP-Adresse, 35, 36, 98
    Konfigurationsmöglichkeiten, 36

J

Jabbers, 293

L

LACP, 170
Layer-3-Funktionalität
    Routing, 27
    Routing-Funktion, 37
Leuchtdiodensimulation, 44
Link Check, 159
Link Check Configuration, 160
Link Check Status, 159
LLDP, 243
LLDP Neighbors, 245
Login, 38, 64
Loop Detection, 277

M

MAC Authentication, 174
MAC-Adresstabelle, 24
MD5, 311
Medienredundanzverfahren, 34
Meldemaske, 93
MIB, 341
    MIB-Variable, 393, 398
    Private MIB, 343
    Standard MIB, 343
Mirrored Port, 147
Mirroring, 25, 147
    Mirrored Port, 147
    Monitor Port, 147
Monitor Port, 147
MSTP, 150, 225
    Portparameter, 235
MSTP (Multiple Spanning Tree Protocol), 233
MSTP-Instanz, 235
Multicast, 186
Multiple Spanning Tree, 225
Multiple Spanning Tree Protocol, 150

N

Nachbarschaftstabelle, 245
NCM PC, 37
Netzüberwachung, 126
NTP, 186
NTP (Network Time Protocol), 134
Nullmodemkabel, 21, 38
    Pinbelegung, 390

O

Observer, 85
Out-Band-Port, 21, 37
Oversize, 293
Oversize Mode, 148

P

Passive Listening, 147
PH - Projektierungshandbuch, 20
Pinbelegung
    Anschlusskabel Diagnoseport, 391
    Nullmodemkabel, 390
POF-Diagnose, 271
Point to Point, 216
Port
    In-Band-Port, 37
    Link Check, 159
    Out-Band-Port, 37
    Portkonfiguration, 152, 154
Port-Diagnose
    FMP-Diagnose, 273
    POF Ports, 274
    POF-Diagnose, 271
    SFP-Diagnose, 269
Portkonfiguration, 154
Priority, 220
PROFINET IO, 345
PTP (Precision Time Protocol), 256

Q

QoS, 239

R

RADIUS-Server, 170
Rapid Spanning Tree, 149

Redundanz
Redundante Kopplung, 23
Refresh, 46
Restart, 53
RFC
RFC 1213, 343
RFC 1286, 343
RFC 1518, 35
RFC 1519, 35
RFC 1724, 343
RFC 1757, 343
RFC 1850, 343
RFC 1907, 343
RFC 2233, 343
RFC 2571, 343
RFC 2572, 343
RFC 2573, 343
RFC 2574, 343
RFC 2575, 343
RFC 2665, 343
RFC 2674p, 343
RFC 2674q, 343
RMON, 100
Routing
Layer-3-Funktionalität, 27
Routing-Funktion, 37
RSTP, 149
RSTP Big Network Support, 150

S

Schnittstelle
Ethernet-Schnittstelle, 21
Fast Ethernet-Schnittstelle, 21
Gigabit Ethernet-Port, 22
Out-Band-Port, 21
RS 232-Schnittstelle, 21
Serielle Schnittstelle, 21, 389, 390
Set Value, 46
SFP-Diagnose, 269
SHA-Algorithmus, 112
SICLOCK, 101
SICLOCK-Uhrzeitsender, 25
SIMATIC NET-Glossar, 3
Slot-Funktion, 358, 359, 360
SMTP-Server, 127
SNMP, 106, 341
SNMP-Trap, 110
SNMPv1, 341
SNMPv2, 341
SNMPv3, 27, 341
SNMPv3-Benutzer, 115
SNTP (Simple Network Time Protocol), 132
Spanning Tree, 24, 149
Multiple Spanning Tree, 24, 225, 233
Rapid Spanning Tree, 24, 216
SSH Public Key Authentifizierung, 56, 64
Standby-Observer, 90
Statistik, 287
STEP 7, 37
Store-and-Forward, 23
STP, 149
Stromversorgungsüberwachung, 353
Subnetz-Maske, 36, 98
SysLog, 27

T

TELNET, 100
TFTP-Server, 60

U

Uhrzeit
NTP (Network Time Protocol), 134
SICLOCK, 25, 101
SNTP (Simple Network Time Protocol), 132
Systemzeit, 131
Uhrzeitsynchronisation, 25, 131
UTC-Zeit, 132
Zeitzone, 132
Uhrzeitsynchronisation, 25
Undersize, 293
Unicast Filter, 178
UTC-Zeit, 132

V

VLAN, 23, 202
VLAN-ID, 402
VLAN-Tag, 401

W

Web Based Management, 42, 383

Z

Zeitzone, 132
Zurücksetzen auf Werkseinstellungen, 387