SIEMENS

SIMATIC NET

Industrial Ethernet Switches SCALANCE XB-200 Web Based Management

Projektierungshandbuch

09/2015

C79000-G8900-C360-03

Rechtliche Hinweise

Warnhinweiskonzept

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

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

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

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

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

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

Qualifiziertes Personal

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

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

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

Marken

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

Haftungsausschluss

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

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

C79000-G8900-C360-03
℗ 09/2015 Änderungen vorbehalten

Inhaltsverzeichnis

Einleitung 1

Gültigkeitsbereich dieses Projektierungshandbuchs

Dieses Projektierungshandbuch behandelt folgende Produkte:

- SCALANCE XB-200

  Nachfolgend werden die Produkte auch als IE-Switches bezeichnet.

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

Das Projektierungshandbuch gilt für folgende Software-Version:

- SCALANCE XB-200 Firmware ab Version 1.2

Werkseinstellungen

EtherNet/IP-Varianten

- Industrial-Ethernet-Protokoll: EtherNet/IP
- Base Bridge Mode: 802.1Q VLAN Bridge
- Redundanzverfahren: RSTP
- Trust Mode: Trust DSCP

PROFINET-Varianten

- Industrial-Ethernet-Protokoll: PROFINET
- Base Bridge Mode: 802.1D Transparent Bridge
- Redundanzverfahren: Ringredundanz
- Trust Mode: Trust COS

Zweck dieses Projektierungshandbuchs

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

Einordnung in die Dokumentationslandschaft

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

- Projektierungshandbuch "SCALANCE XB-200 Command Line Interface"

  Dieses Dokument enthält die CLI-Befehle, die von den IE-Switches SCALANCE XB-200 unterstützt werden.

- Betriebsanleitung "SCALANCE XB-200"

  Dieses Dokument enthält Informationen zum Montieren, Anschließen und Zulassungen der Produkte.

Weiterführende Dokumentation

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

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

Sie finden die Systemhandbücher hier:

- Auf dem Datenträger, der manchen Produkten beiliegt:
  - Produkt-CD / Produkt-DVD
  - SIMATIC NET Manual Collection
- Auf den Internetseiten des Siemens Industry Online Support unter folgenden Beitrags-IDs:
  - 27069465 (http://support.automation.siemens.com/WW/view/de/27069465)
    Industrial Ethernet / PROFINET Industrial Ethernet Systemhandbuch
  - 84922825 (http://support.automation.siemens.com/WW/view/de/84922825)
    Industrial Ethernet / PROFINET Passive Netzkomponenten Systemhandbuch

SIMATIC NET-Handbücher

Sie finden die SIMATIC NET-Handbücher hier:

- Auf dem Datenträger, der manchen Produkten beiliegt:
  - Produkt-CD / Produkt-DVD
  - SIMATIC NET Manual Collection
- Auf den Internetseiten des Siemens Industry Online Support.

Siehe auch

Siemens Industry Online Support (http://support.automation.siemens.com/WW/view/de)

Link zum Bereich "Industrielle Kommunikation"
(http://support.automation.siemens.com/WW/view/de/10805878/130000)

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, Lösungen, Maschinen, Geräten und/oder Netzwerken unterstützen. Sie sind wichtige Komponenten in einem ganzheitlichen Industrial Security-Konzept. Die Produkte und Lösungen von Siemens werden unter diesem Gesichtspunkt ständig weiterentwickelt. Siemens empfiehlt, sich unbedingt regelmäßig über Produkt-Updates zu informieren.

Für den sicheren Betrieb von Produkten und Lösungen von Siemens ist es erforderlich, geeignete Schutzmaßnahmen (z. B. Zellenschutzkonzept) zu ergreifen und jede Komponente in ein ganzheitliches Industrial Security-Konzept zu integrieren, das dem aktuellen Stand der Technik entspricht. Dabei sind auch eingesetzte Produkte von anderen Herstellern zu berücksichtigen. Weitergehende Informationen über Industrial Security finden Sie unter http://www.siemens.com/industrialsecurity.

Um stets über Produkt-Updates informiert zu sein, melden Sie sich für unseren produktspezifischen Newsletter an. Weitere Informationen hierzu finden Sie unter http://support.automation.siemens.com.

Lizenzbedingungen

Hinweis

Open Source Software

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

Sie können die Lizenzbedingungen im WBM auf der Seite "System > Load&Save" herunterladen.

Marken

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

SIMATIC NET, SCALANCE, C-PLUG, OLM

Firmware

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

Beschreibung 2

2.1 Produkteigenschaften

Die IE-Switches SCALANCE XB-200 verfügen über folgende Eigenschaften:

- Die Ethernet-Schnittstellen unterstützen folgende Betriebsarten und Modi:
  - 10 MBit/s und 100 MBit/s jeweils Voll- und Halb-Duplex
  - Auto-Crossing
  - Auto-Polarity
- EtherNet/IP

  EtherNet/IP (Ethernet/Industrial Protocol) ist ein offener Industriestandard für industrielles Echtzeit-Ethernet, basierend auf TCP/IP und UDP/IP.
- PROFINET IO

  PROFINET (Process Field Network) ist ein offener Industriestandard für industrielles Echtzeit-Ethernet, basierend auf TCP/IP und IT-Standards. Über PROFINET IO (Input/Output) können dezentrale Peripheriegeräte an eine Steuerung (Controller) angebunden werden.
- Redundanzverfahren Rapid Spanning Tree Protocol (RSTP) und Spanning Tree Protocol (STP)

  Das Redundanzverfahren Spanning Tree definiert in einem Netzwerk mehrere Verbindungswege zwischen Netzteilnehmern, von denen nur einer aktiv ist. Damit werden Schleifen unterdrückt und die Pfade optimiert.
- Virtuelle Netze (VLAN)

  Zur Strukturierung von Industrial Ethernet-Netzen mit stark wachsender Teilnehmeranzahl kann ein physikalisch vorhandenes Netz in mehrere virtuelle Teilnetze unterteilt werden.
- Lastbegrenzung bei Einsatz von Multicast- und Broadcast-Protokollen, z. B. Video-Übertragung

  Durch Lernen der Multicast-Quellen und -Ziele (IGMP-Snooping, IGMP-Querier) können die IE-Switches Multicast-Datenverkehr filtern und damit die Last im Netz begrenzen. Multicast- und Broadcast-Datenverkehr können begrenzt werden.
- Uhrzeitsynchronisation

  Diagnosemeldungen (Log Table-Einträge, E-Mails) werden mit Zeitstempeln versehen. Die lokale Zeit ist durch Synchronisation mit einem SICLOCK-Uhrzeitsender oder SNTP-/NTP-Server netzweit einheitlich und erleichtert damit die Zuordnung von Diagnosemeldungen mehrerer Geräte.
- Quality of Service zur Klassifizierung des Netzwerkverkehrs nach CoS (Class of Service - IEEE 802.11Q) und DSCP (Differentiated Services Code Point - RFC 2474)

- Port Mirroring

  Mirroring ermöglicht es, den Datenverkehr eines Ports auf einen anderen Port (Monitor-Port) abzubilden. Am Monitor-Port kann dann rückwirkungsfrei der Datenverkehr analysiert werden.

- Netzzugriffsschutz nach dem Standard IEEE 802.1x

  Ports können für Endgeräte konfiguriert werden, die die Authentifizierung nach IEEE 802.1x unterstützen. Die Authentifizierung erfolgt über einen RADIUS-Server, der über das Netz erreichbar sein muss.

- Log-Tabelle

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

2.2 Voraussetzungen für Installation und Betrieb

Voraussetzungen für die Installation und den Betrieb der IE-Switches

Für die Konfiguration der IE-Switches muss ein PG/PC mit Netzwerkanschluss vorhanden sein. Dem IE-Switch muss eine IP-Adresse zugewiesen sein und er muss im Netzwerk verfügbar sein, siehe auch "Erstmalige Vergabe einer IP-Adresse (Seite 15)".

Vergabe einer IP-Adresse

3

3.1 Aufbau einer IP-Adresse

Adressklassen

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

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

XXX.XXX.XXX.XXX

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

Subnetzmaske

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

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

Beispiel für ein Klasse B-Netz:

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

Um festzustellen, ob zwei IP-Adressen zum gleichen Subnetz gehören, werden auf die beiden IP-Adressen und die Subnetzmaske eine bitweise UND-Verknüpfung angewendet.

Wenn beide Verknüpfungen das gleiche Ergebnis haben, gehören beide IP-Adressen zum gleichen Subnetz, wie z. B. 141.120.246.210 und 141.120.252.108.

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

Hinweis

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

3.2 Erstmalige Vergabe einer IP-Adresse

Konfigurationsmöglichkeiten

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

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

- **DHCP** (Default)
- **Primary Setup Tool** (PST)
  - Um dem IE-Switch mit dem PST eine IP-Adresse zuweisen zu können, muss der IE-Switch über Ethernet erreichbar sein.
  - Sie finden das PST auf den Internetseiten des Siemens Industry Online Support unter der Beitrags-ID 19440762 (http://support.automation.siemens.com/WW/view/de/19440762).
  - Beachten Sie für weitere Informationen zur Vergabe der IP-Adresse mit dem PST die Dokumentation "Primary Setup Tool (PST)".
- **STEP 7**

  Sie können in STEP 7 die Topologie, den Gerätenamen und die IP-Adresse projektieren. Wenn Sie einen unkonfigurierten IE-Switch mit dem Controller verbinden, weist der Controller dem IE-Switch den projektierten Gerätenamen und die IP-Adresse automatisch zu.
  - **STEP 7 ab V5.5 SP4**

    Beachten Sie für weitere Informationen zur Vergabe der IP-Adresse über STEP 7 die Dokumentation "Hardware konfigurieren und Verbindungen projektieren mit STEP 7", Abschnitt "Schritte zum Konfigurieren eines PROFINET IO-Systems".
  - **STEP 7 Basic ab V13 SP1** bzw. **STEP 7 Professional ab V13 SP1**

    Beachten Sie für weitere Informationen zur Vergabe der IP-Adresse über STEP 7 die Online-Hilfe "Informationssystem", Abschnitt "Adressierung von PROFINET-Geräten".
- **CLI** über die serielle Schnittstelle
  Beachten Sie für weitere Informationen zur Vergabe der IP-Adresse über das CLI die Dokumentation "SCALANCE XB-200 Command Line Interface".
- **NCM PC**

  Beachten Sie für weitere Informationen zur Vergabe der IP-Adresse über NCM PC die Dokumentation "PC-Stationen in Betrieb nehmen - Anleitung und Schnelleinstieg", Abschnitt "PROFINET IO-System anlegen".

Hinweis

DHCP ist im Auslieferungszustand und nach "Restore Factory Defaults and Restart" eingeschaltet. Wenn ein DHCP-Server im lokalen Netz verfügbar ist und dieser auf den DHCP-Request eines IE-Switches antwortet, werden beim ersten Hochlauf automatisch IP-Adresse, Subnetzmaske und Gateway zugeteilt.

3.3 Adressvergabe über DHCP

Eigenschaften von DHCP

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

- DHCP kann sowohl während des Hochlaufs eines Geräts als auch im laufenden Betrieb eingesetzt werden.
- Die vergebene IP-Adresse bleibt nur für eine begrenzte Zeitdauer (Lease Time) gültig. Nach Ablauf dieser Zeitdauer muss der Client entweder eine neue IP-Adresse anfordern oder die Gültigkeitsdauer der vorhandenen IP-Adresse verlängern.
- Normalerweise erfolgt keine feste Adresszuordnung, d. h. wenn ein Client erneut eine IP-Adresse anfordert, erhält er in der Regel eine andere Adresse als bei der vorhergehenden Anforderung. Es ist möglich, den DHCP-Server so zu konfigurieren, dass der DHCP-Client auf seine Anfrage immer dieselbe feste Adresse zugeordnet bekommt. Über welchen Parameter der DHCP-Client für die feste Adresszuordnung identifiziert wird, wird im DHCP-Client eingestellt. Die Adresse kann über die MAC-Adresse, die DHCP Client ID oder den Systemnamen zugeordnet werden. Den Parameter konfigurieren Sie unter "System > DHCP-Client".
- Folgende DHCP-Optionen werden unterstützt:
  - DHCP-Option 66: Vergabe eines dynamischen TFTP-Servernamens
  - DHCP-Option 67: Vergabe eines dynamischen Bootfile-Namens

Hinweis

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

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.

Technische Grundlagen

4

4.1 Mengengerüst

Mengengerüst des Geräts

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

Die Nutzbarkeit verschiedener Funktionen ist vom verwendeten Gerätetyp abhängig.

	konfigurierbare Funktion	maximale Anzahl
System	Syslog-Server	3
	E-Mail-Server	3
	SNMP-Trapempfänger	10
	SNTP-Server	1
	NTP-Server	1
	Agent Interfaces	1
Layer 2	Virtuelle LANs (inklusive VLAN 1)	17
	Mirroring-Sessions	1
	Unicast Filtering	128
	Multicast-Gruppen	256
	Statische MAC-Adressen in der forward database (FDB)	128
Layer 3	DHCP Relay Agent Interfaces	1
	DHCP Relay Agent Server	4
Security	IP-Adressen von RADIUS-Servern	3
	Management ACLs (Zugriffsregeln für das Management)	10

4.2 EtherNet/IP

EtherNet/IP

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

EtherNet/IP konfigurieren Sie unter "System > EtherNet/IP (Seite 126)".

Common Industrial Protocol

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

Electronic Data Sheet

Electronic Data Sheet (EDS) sind elektronische Datenblätter zur Beschreibung von Geräten.

Die für den EtherNet/IP-Betrieb benötigte EDS finden Sie unter "System > Load&Save (Seite 80)".

4.3 PROFINET

PROFINET

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

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

PROFINET konfigurieren Sie unter "System > PNIO (Seite 125)".

PROFINET IO

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

4.4 Redundanzverfahren

4.4.1 Spanning Tree

Vermeidung von Schleifenbildung bei redundanten Verbindungen

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

Definition der Netztopologie durch Konfigurationstelegramme

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

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

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

Verhalten bei Veränderungen der Netztopologie

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

Aktualität der Konfigurationsinformation

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

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

4.4.1.1 RSTP

Rapid Spanning Tree Protocol (RSTP)

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

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

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

4.4.2 HRP

HRP - High Speed Redundancy Protocol

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

Wenn die Testtelegramme des RM bei einer Unterbrechung des Rings nicht mehr am anderen Ringport ankommen, schaltet der RM seine beiden Ringports durch und informiert die Redundanz-Clients umgehend über den Wechsel. Die Rekonfigurationszeit nach Unterbrechung des Rings beträgt maximal 0,3 Sekunden.

Standby-Redundanz

Standby-Redundanz ist ein Verfahren, bei dem Ringe, die jeder für sich durch High-Speed Redundancy gesichert sind, redundant gekoppelt werden. Im Ring wird ein Master-/Slave-Gerätepaar konfiguriert, das sich gegenseitig über seine Ringports überwacht. Der Datenverkehr wird im Fehlerfall von einer Ethernet-Verbindung (Standby-Port des Master bzw. Standby-Server) zu einer anderen Ethernet-Verbindung (Standby-Port des Slave) umgeleitet.

Voraussetzungen

- HRP 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.
- 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 Web Based Management, Command Line Interface 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, Command Line Interface oder SNMP geschehen.
- Im Grundzustand sind die Betriebsarten "HRP Client" oder "Automatic Redundancy Detection" voreingestellt.

4.4.3 MRP

4.4.3.1 MRP - Media Redundancy Protocol

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

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

Die Rekonfigurationszeit nach Unterbrechung des Rings beträgt maximal 0,2 Sekunden.

Voraussetzungen

Voraussetzung für den störungsfreien Betrieb mit dem Medienredundanzverfahren MRP sind:

- MRP wird in Ringtopologien mit bis zu 50 Geräten unterstützt.

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

  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 angegeben Rekonfigurationszeit kommen.

- Bei allen Geräten im Ring muss "MRP" aktiviert sein (siehe Kapitel "Projektierung in STEP 7 (Seite 26)").

- 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.

Topologie

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

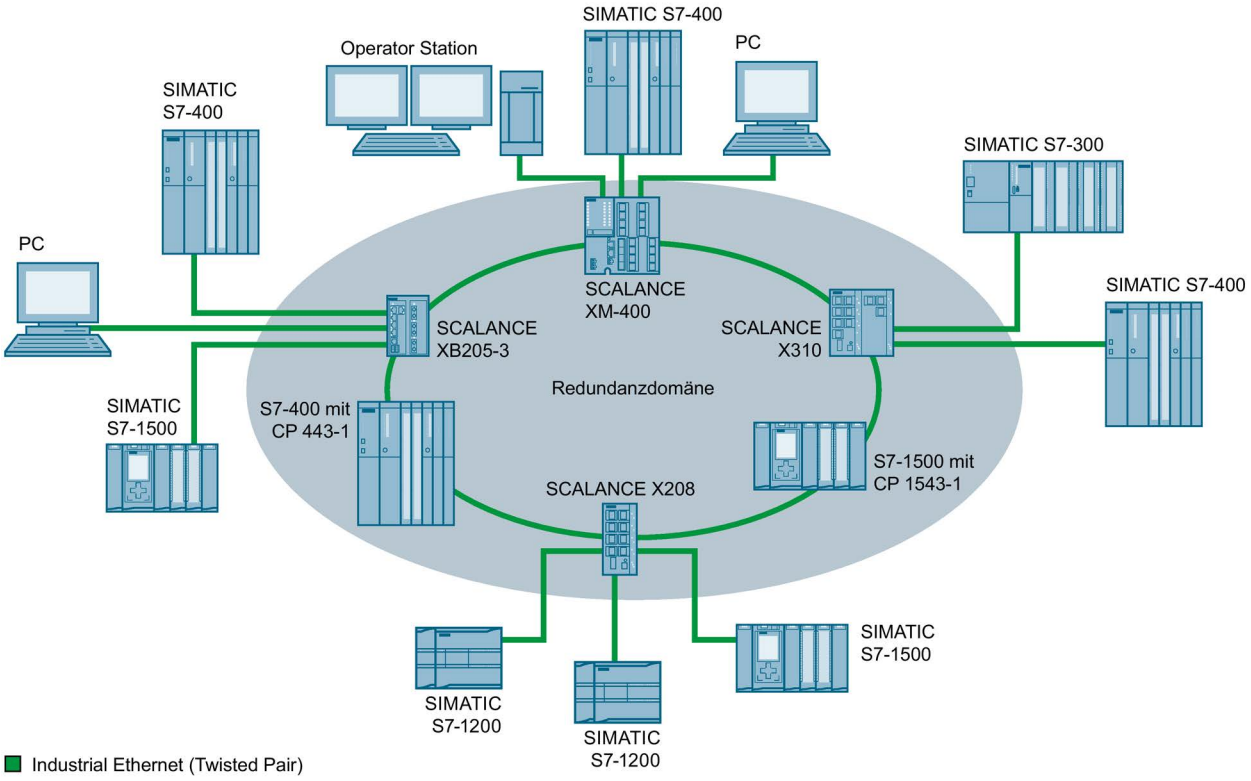


Bild 4-1 Beispiel einer Ringtopologie mit dem Medienredundanzverfahren MRP

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

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

Nicht MRP-fähige Geräte können über einen Switch SCALANCE X oder einen PC mit CP 1616 an den Ring angebunden werden.

4.4.3.2 Projektierung im WBM

Rolle

Die Auswahl der Rolle ist von den folgenden Einsatzfällen abhängig:

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

Hinweis

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

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

Hinweis

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

Projektierung

Im WBM projektieren Sie MRP auf folgenden Seiten:

- Configuration (Seite 130)
- Ring Redundancy (Seite 150)

4.4.3.3 Projektierung in STEP 7

Projektierung in STEP 7

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

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

- Domäne
- Rolle
- Ringport
- Diagnosealarme

Diese Einstellungen werden nachfolgend beschrieben.

Hinweis

Gültige MRP-Projektierung

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

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

Hinweis

Rolle ändern

Wenn Sie die MRP-Rolle ändern wollen, öffnen Sie zunächst den Ring.

Hinweis

Neustart und Wiederanlauf

Die MRP-Einstellungen sind auch nach einem Neustart des Geräts oder nach einem Spannungsausfall und Wiederanlauf noch wirksam.

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 angehören.

Wenn Sie die Einstellung von "Domäne" in der werkseitigen Vorbelegung "mrpdomain-1" belassen, dann bleiben auch die werkseitig vorbelegten Einstellungen von "Rolle" und "Ringports" aktiv.

MRP-Mehrfachringe

Wenn Sie mehrere 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.

Rolle

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 (MRP-Mehrfachringe):
  - Ordnen Sie genau dem Gerät, das die Ringe verbindet, die Rolle "Manager" zu.
  - Wählen Sie bei allen anderen Geräten der Ringtopologie die Rolle "Client".
- Sie wollen MRP in einer Ringtopologie einsetzen, die auch Nicht-Siemens-Geräte enthält, oder Sie wollen Diagnosealarme zum MRP-Zustand von einem Gerät erhalten (siehe "Diagnosealarme"):
  - Ordnen Sie genau einem Gerät im Ring die Rolle "Manager (Auto)" zu.
  - Wählen Sie bei allen anderen Geräten der Ringtopologie die Rolle "Client".

- Sie wollen MRP deaktivieren:

  Wählen Sie die Option "Nicht Teilnehmer des Rings", wenn Sie das Gerät nicht innerhalb einer Ringtopologie mit MRP betreiben wollen.

Hinweis

Rolle beim Rücksetzen auf Werkseinstellungen

Bei fabrikneuen und auf Werkseinstellungen gesetzte Siemens-Geräte ist folgende MRP-Rolle eingestellt:

- CPs:

  "Manager (Auto)"
- SCALANCE X-200, SCALANCE XB-200 (PROFINET-Varianten), SCALANCE X-300 und SCALANCE X-400:

  "Automatic Redundancy Detection"

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

Bei fabrikneuen und auf Werkseinstellungen gesetzte IE-Switches SCALANCE XB-200 (EtherNet/IP-Varianten), SCALANCE XM-400 und SCALANCE XR-500 ist MRP deaktiviert und Spanning Tree aktiviert.

Ringport 1 / Ringport 2

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

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

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

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

Diagnosealarme

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

Folgende Diagnosealarme können gebildet werden:

- Verdrahtungs- bzw. Port-Fehler

  Bei folgenden Fehlern an den Ringports werden Diagnosealarme generiert:

  – Verbindungsabbruch an einem Ringport
  – Ein Nachbar des Ringports unterstützt nicht MRP.
  – Ein Ringport ist mit einem Nicht-Ringport verbunden.
  – Ein Ringport ist mit dem Ringport einer anderen MRP-Domäne verbunden.

- Statuswechsel Aktiv/Passiv (nur Redundanzmanager)

  Wenn sich in einem Ring der Status ändert (Aktiv/Passiv), wird ein Diagnosealarm generiert.

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

Diese Option betrifft nur Switches. Wählen Sie diese Option, wenn die Eigenschaften zur Medienredundanz durch alternative Mechanismen wie Web Based Management (WBM), CLI oder SNMP parametriert werden sollen.

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

4.4.4 Standby

Allgemeines

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

Standby-Redundanz

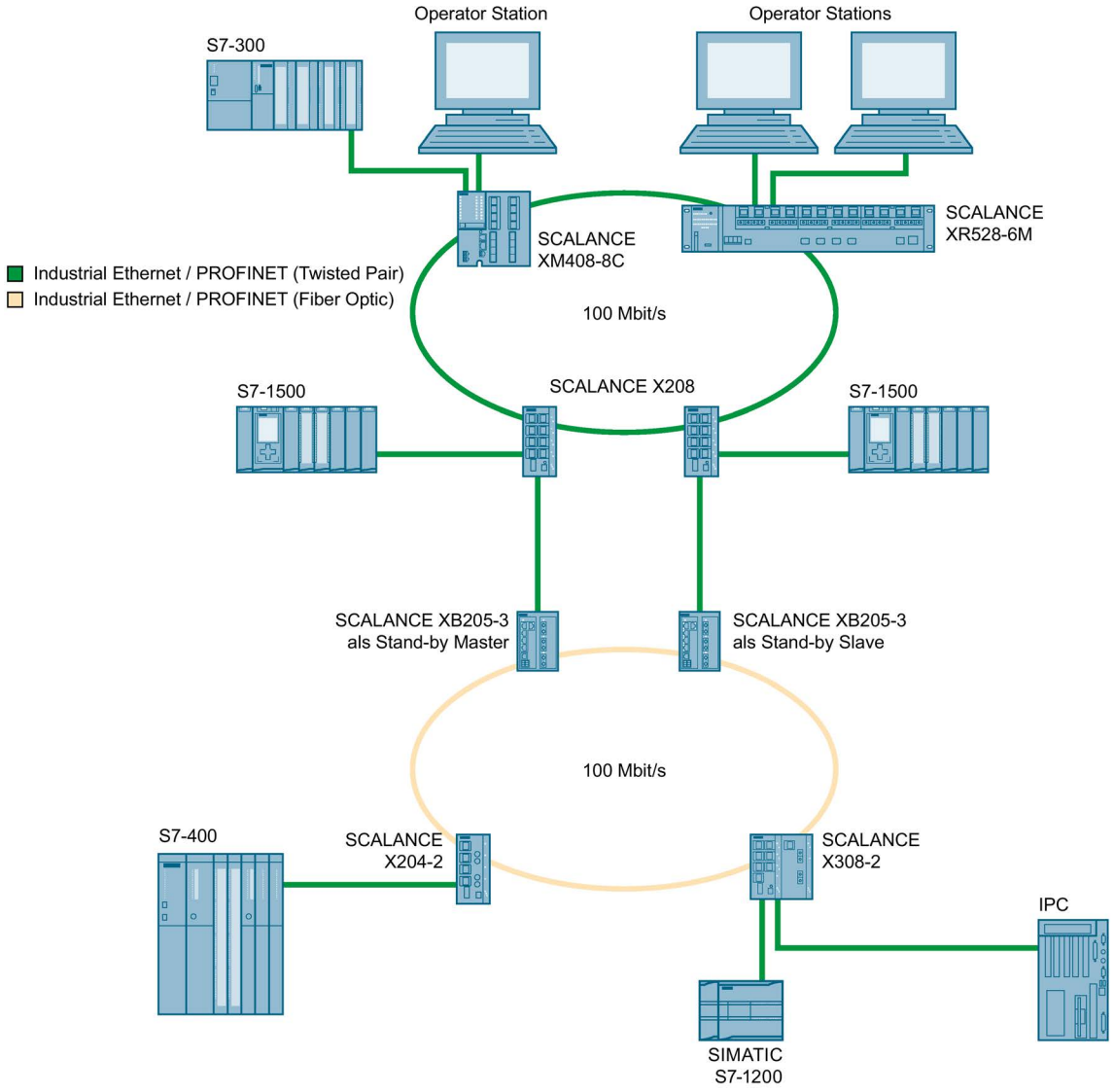


Bild 4-2 Beispiel einer redundanten Kopplung von zwei Ringen

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

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

4.5 VLAN

Netzwerkdefinition unabhängig von der räumlichen Lage der Teilnehmer

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

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

Für die Kennung, welches Paket welchem VLAN zugeordnet ist, wird das Telegramm um 4 Byte erweitert (VLAN-Tagging (Seite 31)). Diese Erweiterung enthält neben der VLAN-ID auch Prioritätsinformationen.

Möglichkeiten der VLAN-Zuordnung

Jedem Port eines Geräts wird eine VLAN-ID zugewiesen (Port-basiertes VLAN). Port-basiertes VLAN konfigurieren Sie unter "Layer 2 > VLAN > Port Based VLAN (Seite 143)".

4.6 VLAN-Tagging

Erweiterung der Ethernet-Telegramme um vier Byte

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

Hinweis

Durch das VLAN-Tag erhöht sich die zulässige Gesamtlänge des Telegramms von 1518 auf 1522 Byte. Bei den IE-Switches beträgt die Standard Telegrammgröße mindestens 1536 Byte.
Es muss geprüft werden, ob die Endteilnehmer im Netz diese Länge / diesen Telegrammtyp verarbeiten können. Ist dies nicht der Fall, dürfen an diese Teilnehmer nur Telegramme mit der Standardlänge gesendet werden.

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

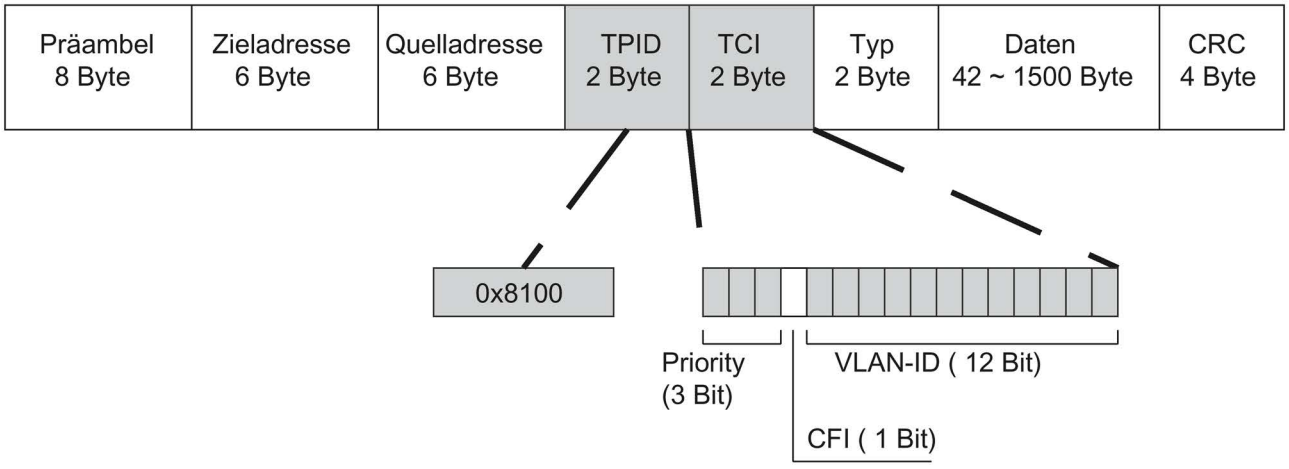


Bild 4-3 Aufbau des erweiterten Ethernet-Telegramms

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

Tag Protocol Identifier (TPID)

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

Tag Control Information (TCI)

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

CoS– Priorisierung

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

Das Gerät besitzt mehrere parallele Warteschlangen, in denen die verschieden priorisierten Telegramme abgearbeitet werden. Dabei werden zuerst die Telegramme mit der höchsten Priorität abgearbeitet ("Strict Priority"-Verfahren). Dieses Verfahren gewährleistet auch bei einem hohen Datenaufkommen, dass die Telegramme mit der höchsten Priorität auf jeden Fall gesendet werden.

Canonical Format Identifier (CFI)

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

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

VLAN-ID

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

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

4.7 SNMP

Einleitung

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

Aufgaben von SNMP:

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

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

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

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

Standardwerte der Community-Strings:

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

Hinweis

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

Weitere einfache Schutzmechanismen auf Geräteebene:

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

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

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

Die Management-Station sendet Datenpakete folgenden Typs:

- GET
  Anfordern eines Datensatzes vom Agenten
- GETNEXT
  Ruft den nächsten Datensatz auf.
- GETBULK (verfügbar ab SNMPv2)
  Fordert mehrere Datensätze auf einmal an, z. B. mehrere Zeilen einer Tabelle.
- SET
  Beinhaltet Parametrierungsdaten für das entsprechende Gerät.

Der SNMP-Agent sendet Datenpakete folgenden Typs:

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

SNMPv1/v2/v3 verwenden UDP (User Datagram Protocol) und nutzen die UDP-Ports 161 und 162. Die Beschreibung der Daten erfolgt in einer Management Information Base (MIB).

SNMPv3

SNMPv3 führt gegenüber den Vorgängerversionen SNMPv1 und SNMPv2 ein umfangreicheres Sicherheitskonzept ein.

SNMPv3 unterstützt:

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

Konfigurieren mit dem Web Based Management 5

5.1 Web Based Management

Funktionsprinzip

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

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

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

Hinweis

Sichere Verbindung

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

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

Voraussetzungen

Darstellung des WBM

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

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

- Microsoft Internet Explorer 10
- Mozilla Firefox 31 ESR
- Chrome V40

Hinweis

Kompatibilitätsansicht

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

Darstellung des WBM auf mobilen Geräten

Für mobile Geräte gelten folgende minimale Voraussetzungen:

Auflösung	Betriebssystem	Internet-Browser
960 x 640 Pixel	Android ab Version 4.2.1 iOS ab Version 6.0.2	Chrome ab Version 18 auf Android Safari ab Version 6 auf iOS

Getestet mit folgenden Internet-Browsern für mobile Geräte:

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

Hinweis

Seitendarstellung und Bedienung des WBM auf mobilen Geräten

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

5.2 Login

Verbindung zu einem Gerät herstellen

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

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

Anmeldung mit Hilfe des Internet-Browsers

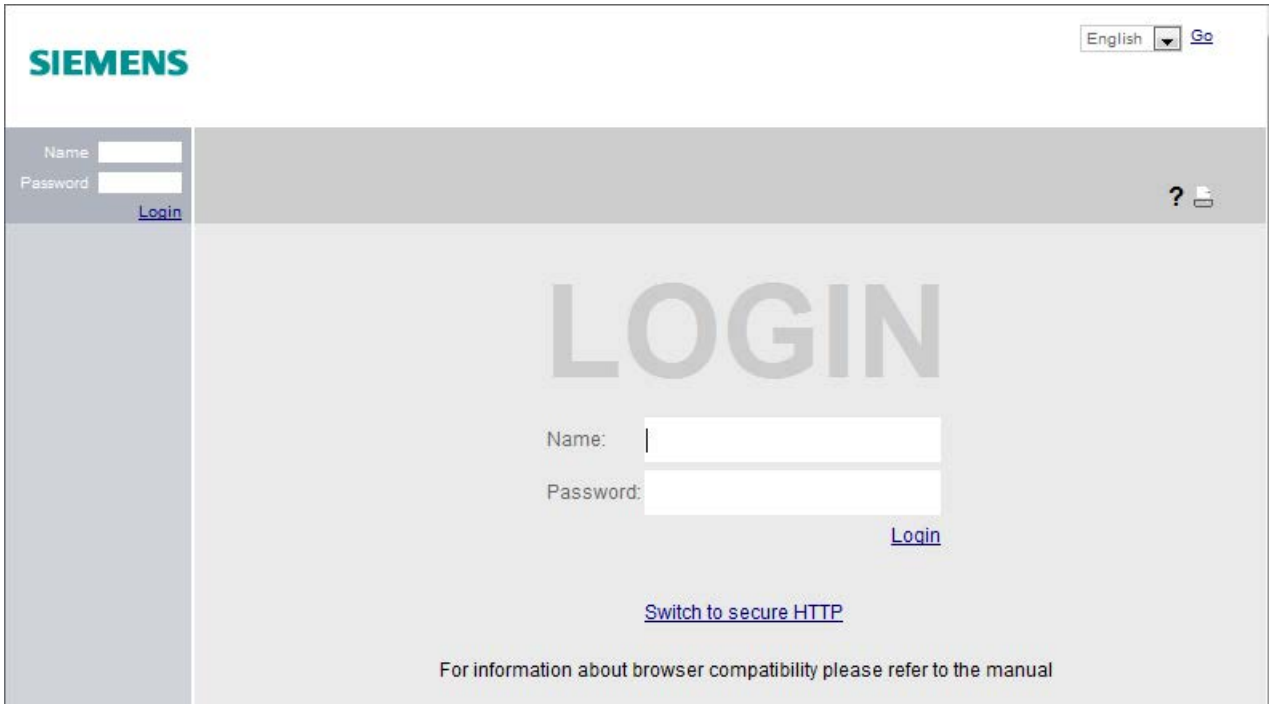
Auswahl der Sprache des WBM

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

Hinweis

Verfügbare Sprachen

In dieser Version ist nur Englisch verfügbar. Weitere Sprachen folgen in einer späteren Version.



Anmeldung über HTTP

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

Für beide Möglichkeiten gelten folgende Schritte, um sich anzumelden:

1. Tragen Sie im Eingabefeld "Name" Folgendes ein:
   - "admin": Mit diesem Benutzertyp können Sie Einstellungen des Gerätes verändern (lesender und schreibender Zugriff auf die Konfigurationsdaten).
   - "user": Mit diesem Benutzertyp können Sie keine Einstellungen des Gerätes verändern (lesender Zugriff auf die Konfigurationsdaten).
2. Tragen Sie im Eingabefeld "Password" Ihr Passwort ein.
   Wenn Sie sich das erste Mal oder nach einem "Restore Factory Defaults and Restart" anmelden, tragen Sie im Eingabefeld "Password" das Standard-Passwort ein.
   - "admin": Standard-Passwort "admin"
   - "user": Standard-Passwort "user"
3. Klicken Sie die Schaltfläche "Login" oder bestätigen Sie die Eingabe mit "Enter".
   Wenn Sie sich das erste Mal oder nach einem "Restore Factory Defaults and Restart" mit dem voreingestellten Benutzer "admin" anmelden, werden Sie aufgefordert das Passwort zu ändern. Zur Bestätigung müssen Sie das Passwort wiederholen. Beide Passworteingaben müssen übereinstimmen. Klicken Sie auf die Schaltfläche "Set Values", um den Vorgang abzuschließen und das neue Passwort zu aktivieren.

Wenn Sie sich erfolgreich angemeldet haben, erscheint die Startseite.

Anmeldung über HTTPS

Das Web Based Management bietet auch die Möglichkeit, sich über die gesicherte Verbindung des HTTPS-Protokolls mit dem Gerät zu verbinden. Gehen Sie folgendermaßen vor:

1. Klicken Sie auf den Link "Switch to secure HTTP" in der Anmeldeseite oder geben Sie im Adressfeld des Internet-Browsers "https://" und die IP-Adresse des Gerätes ein.
2. Bestätigen Sie die angezeigte Zertifikatswarnung.
   Die Anmeldeseite des Web Based Management erscheint.
3. Tragen Sie im Eingabefeld "Name" Folgendes ein:
   - "admin": Mit diesem Benutzertyp können Sie Einstellungen des Gerätes verändern (lesender und schreibender Zugriff auf die Konfigurationsdaten).
   - "user": Mit diesem Benutzertyp können Sie keine Einstellungen des Gerätes verändern (lesender Zugriff auf die Konfigurationsdaten).

4. Tragen Sie im Eingabefeld "Password" Ihr Passwort ein.
   Wenn Sie sich das erste Mal oder nach einem "Restore Factory Defaults and Restart" anmelden, tragen Sie im Eingabefeld "Password" das Standard-Passwort ein.
   - "admin": Standard-Passwort "admin"
   - "user": Standard-Passwort "user"
5. Klicken Sie die Schaltfläche "Login" oder bestätigen Sie die Eingabe mit "Enter".
   Wenn Sie sich das erste Mal oder nach einem "Restore Factory Defaults and Restart" mit dem voreingestellten Benutzer "admin" anmelden, werden Sie aufgefordert das Passwort zu ändern. Zur Bestätigung müssen Sie das Passwort wiederholen. Beide Passworteingaben müssen übereinstimmen. Klicken Sie auf die Schaltfläche "Set Values", um den Vorgang abzuschließen und das neue Passwort zu aktivieren.

Wenn Sie sich erfolgreich angemeldet haben, erscheint die Startseite.

5.3 Das Menü "Information"

5.3.1 Start Page

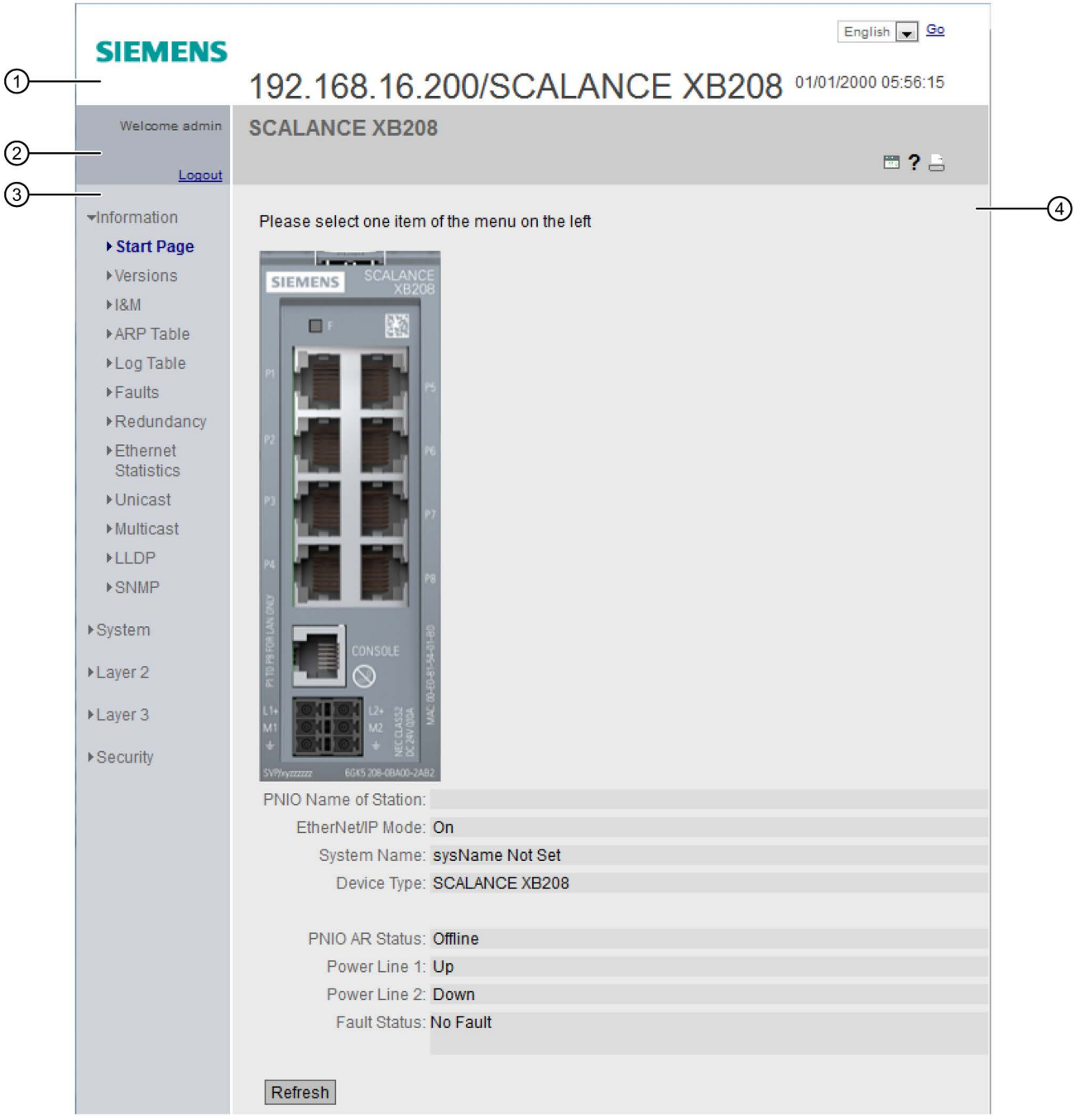
Ansicht der Startseite

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

Allgemeiner Aufbau der WBM-Seiten

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

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


1
2
3
4
SIEMENS
English
Go
192.168.16.200/SCALANCE XB208
01/01/2000 05:56:15
Welcome admin
Logout
SCALANCE XB208
Information
Start Page
Versions
I&M
ARP Table
Log Table
Faults
Redundancy
Ethernet Statistics
Unicast
Multicast
LLDP
SNMP
System
Layer 2
Layer 3
Security
Please select one item of the menu on the left
PNIO Name of Station:
EtherNet/IP Mode: On
System Name: sysName Not Set
Device Type: SCALANCE XB208
PNIO AR Status: Offline
Power Line 1: Up
Power Line 2: Down
Fault Status: No Fault
Refresh

Auswahlbereich (1)

Im Auswahlbereich wird Ihnen Folgendes angeboten:

- Logo der Siemens AG
- Anzeige von: "System Location/System Name"
  - "System Location" enthält die Ortsangabe des Geräts.
    Im Auslieferzustand wird die Agent IP-Adresse des Geräts angezeigt.
  - "System Name" ist der Gerätename.
    Im Auslieferzustand wird der Gerätetyp angezeigt.

  Den Inhalt dieser Anzeige können Sie unter "System > General > Device" ändern.
- Klappliste für die Sprachauswahl
- Systemzeit und -datum

  Der Inhalt dieser Anzeige können Sie unter "System > System Time" ändern.

Anzeigebereich (2)

Im oberen Teil des Anzeigebereichs befindet sich der vollständige Titel des aktuell gewählten Menüpunkts.

Im unteren Teil des Anzeigebereichs befindet sich Folgendes:

- **Drucken** 
  Wenn Sie diese Schaltfläche anklicken, wird ein Popup-Fenster geöffnet. Das Popup-Fenster enthält eine Ansicht des Seiteninhalts, die für Drucker optimiert ist.

  Hinweis
  Drucken großer Tabellen

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

- **Hilfe** 
  Wenn Sie diese Schaltfläche anklicken, wird die Hilfeseite des aktuell gewählten Menüpunktes in einem neuen Browser-Fenster aufgerufen.

  Auf der Hilfeseite finden Sie eine Beschreibung des Inhaltsbereichs. Unter Umständen sind Optionen beschrieben, die auf dem Gerät nicht zur Verfügung stehen.
- **Leuchtdiodensimulation** 
  Jede Komponente eines Geräts verfügt über mehrere Leuchtdioden, die Informationen über den Betriebszustand des Geräts liefern. Abhängig vom Aufstellort ist der direkte Zugang zum Gerät jedoch nicht immer möglich. Aus diesem Grund bietet das Web Based Management eine Simulationsdarstellung für die Leuchtdioden. Nicht belegte Anschlüsse werden als graue LEDs dargestellt. Die Bedeutung der Leuchtdiodenanzeigen ist in der Betriebsanleitung beschrieben.

  Wenn Sie diese Schaltfläche anklicken, rufen Sie das Fenster der Leuchtdiodensimulation auf. Sie können dieses Fenster während des Menüwechsels einblenden und beliebig verschieben. Um die Leuchtdiodensimulation zu schließen,

klicken Sie innerhalb des Fensters der Leuchtdiodensimulation auf die Schließen-Schaltfläche.

- **Abmelden**
  Sie können sich auf jeder WBM-Seite abmelden, indem Sie auf den Link "Logout" klicken.

Navigationsbereich (3)

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

Inhaltsbereich (4)

Der Inhaltsbereich enthält eine Grafik des Geräts. Die Grafik zeigt immer den SCALANCE XB-200, über den Sie das WBM aufgerufen haben.

Unter dem Gerätebild wird Folgendes angezeigt:

- **PNIO Name of Station**
  Zeigt den PROFINET IO-Gerätenamen an.
- **EtherNet/IP Mode**
  Zeigt an, ob EtherNet/IP aktiviert ("On") oder deaktiviert ("Off") ist.
- **System Name**
  Zeigt den Namen des Geräts an.
- **Device Type**
  Zeigt die Typenbezeichnung des Geräts an.
- **PNIO AR Status**
  Zeigt den PROFINET IO Application Relation Status an.
  - Online

    Zu einem PROFINET IO Controller besteht eine Verbindung. Der PROFINET IO Controller hat seine Konfigurationsdaten in das Gerät geladen. Das Gerät kann Statusdaten zum PROFINET IO Controller senden. In diesem Zustand sind die Parameter, die über den PROFINET IO Controller eingestellt werden, nicht am Gerät konfigurierbar.
  - Offline

    Zu einem PROFINET IO Controller besteht keine Verbindung.
- **Power Line 1 / Power Line 2**
  - Up
    Die Versorgungsspannung 1 bzw. 2 liegt an.
  - Down
    Die Versorgungsspannung 1 bzw. 2 liegt nicht an oder die zulässige Spannung ist unterschritten.
- **Fault Status**
  Zeigt den Fehlerstatus des Geräts an.

Häufig verwendete Schaltflächen

Die Seiten des WBM enthalten standardmäßig folgende Schaltflächen:

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

  Hinweis

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

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

  Hinweis

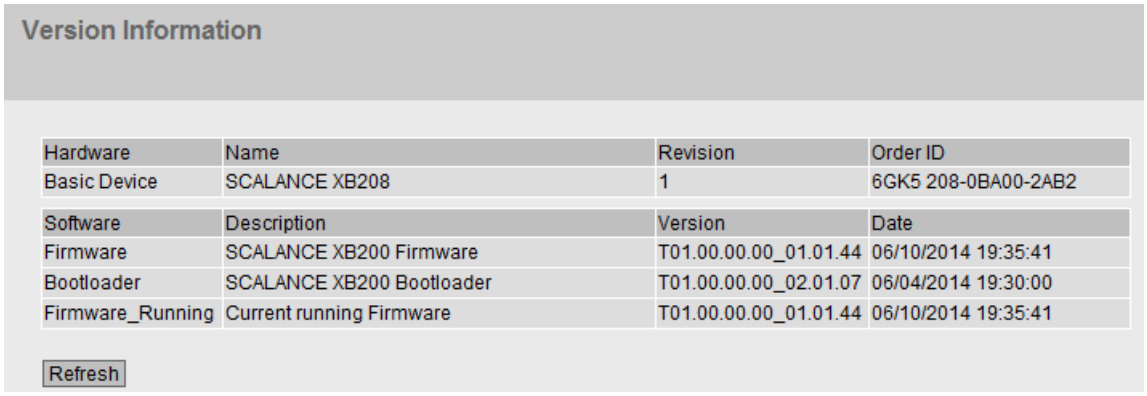
  Das Ändern der Konfigurationsdaten ist nur mit dem Login "admin" möglich.

- **Anlegen von Einträgen mit "Create"**
  Seiten, auf denen Sie neue Einträge erstellen können, haben am unteren Rand die Schaltfläche "Create". Klicken Sie auf diese Schaltfläche, um einen neuen Eintrag zu erstellen.
- **Löschen von Einträgen mit "Delete"**
  Seiten, auf denen Sie Einträge löschen können, haben am unteren Rand die Schaltfläche "Delete". Klicken Sie auf diese Schaltfläche, um die zuvor markierten Einträge aus dem Gerätespeicher zu löschen. Der Löschvorgang bewirkt auch eine Aktualisierung der Seite im WBM.
- **Vorwärts blättern mit "Next"**
  Auf Seiten mit sehr vielen Datensätzen ist die Anzahl der auf einer Seite darstellbaren Datensätze beschränkt. Klicken Sie auf die Schaltfläche "Next", um innerhalb der Datensätze vorwärts zu blättern.
- **Rückwärts blättern mit "Prev"**
  Auf Seiten mit sehr vielen Datensätzen ist die Anzahl der auf einer Seite darstellbaren Datensätze beschränkt. Klicken Sie auf die Schaltfläche "Prev", um innerhalb der Datensätze rückwärts zu blättern.

5.3.2 Versions

Versionen von Hardware und Software

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



Beschreibung der angezeigten Werte

Die Tabelle 1 gliedert sich in folgende Spalten:

- **Hardware -** Basic Device

  Zeigt das Grundgerät an.

- **Name**
  Zeigt den Namen des Geräts an.
- **Revision**
  Zeigt den Hardware-Ausgabestand des Geräts an.
- **Order ID**
  Zeigt die Bestellnummer des Geräts an.

Die Tabelle 2 gliedert sich in folgende Spalten:

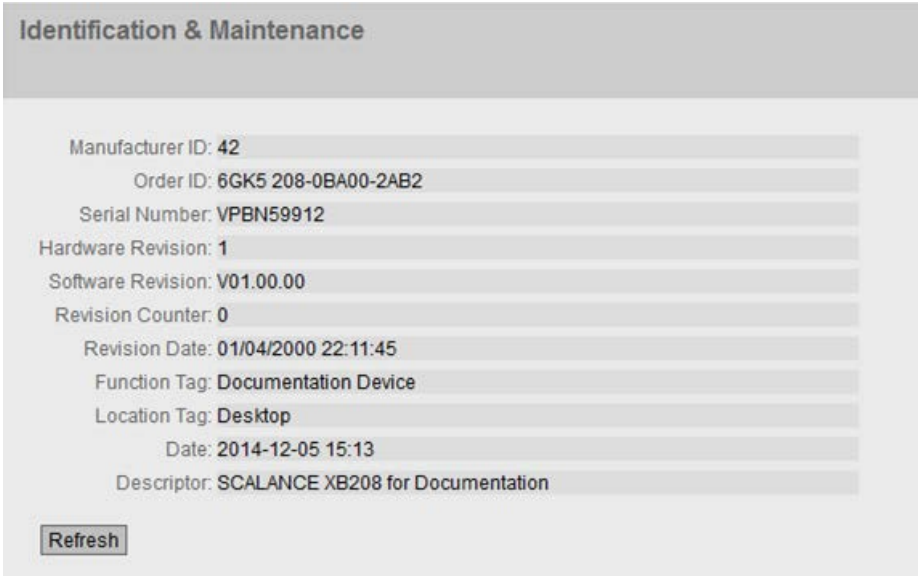
- **Software**
  - Firmware
    Zeigt die aktuelle Firmware-Version an. Wenn eine neue Firmware-Datei geladen wurde und das Gerät noch nicht neu gestartet ist, wird hier die Firmware-Version der geladenen Firmware-Datei angezeigt. Nach dem nächsten Neustart wird die geladene Firmware aktiviert und verwendet.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

- **Version**
  Zeigt die Versionsnummer des Software-Ausgabestands an.
- **Date**
  Zeigt das Erstellungsdatum des Software-Ausgabestands an.

5.3.3 I&M

Hersteller- und Wartungsdaten

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



Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Zeilen:

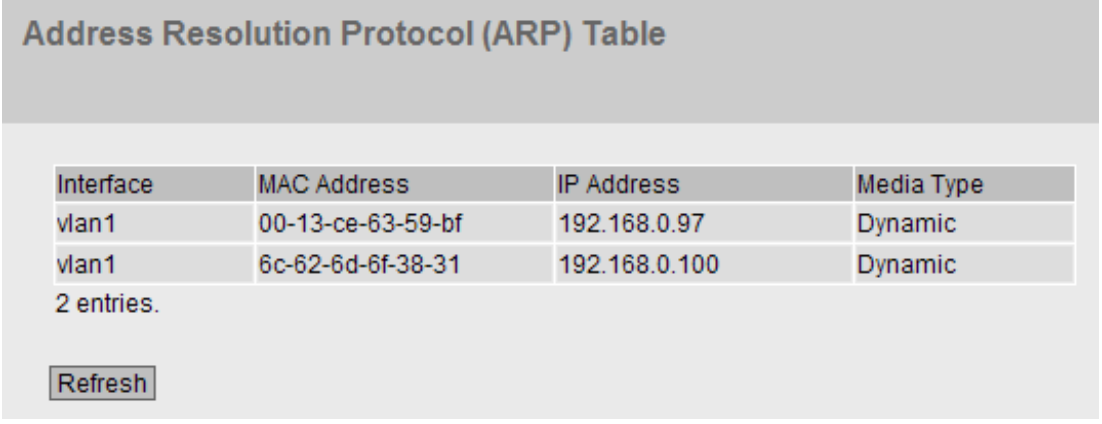
- **Manufacturer ID**
  Zeigt die Herstellerkennung an.
- **Order ID**
  Zeigt die Bestellnummer an.
- **Serial Number**
  Zeigt die Seriennummer an.
- **Hardware Revision**
  Zeigt den Hardware-Ausgabestand an.
- **Software Revision**
  Zeigt den Software-Ausgabestand an.

- **Revision Counter**
  Unabhängig von einer Versionsänderung, zeigt dieses Feld immer den Wert "0" an.
- **Revision Date**
  Datum und Uhrzeit der letzten Versionsänderung
- **Function Tag**
  Zeigt das Function Tag (Anlagenkennzeichen) des Geräts an. Das Anlagenkennzeichen (AKZ) wird bei der Projektierung des Geräts mit HWKonfig von STEP7 angelegt.
- **Location Tag**
  Zeigt das Location Tag (Ortskennzeichen) des Geräts an. Das Ortskennzeichen (OKZ) wird bei der Projektierung des Geräts mit HWKonfig von STEP7 angelegt.
- **Date**
  Zeigt das Datum, das bei der Projektierung des Geräts mit HWKonfig von STEP7 angelegt wurde.
- **Description**
  Zeigt die Beschreibung, die bei der Projektierung des Geräts mit HWKonfig von STEP7 angelegt wurde.

5.3.4 ARP Table

Zuordnung von MAC-Adresse und IP-Adresse

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



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Interface**
  Zeigt die Schnittstelle an, über die der Zeileneintrag gelernt wurde.
- **MAC Address**
  Zeigt die MAC-Adresse des Ziel- oder Quellgeräts an.
- **IP Address**
  Zeigt die IP-Adresse des Zielgeräts an.
- **Media Type**
  Zeigt die Art der Verbindung.
  - Dynamic
    Das Gerät hat die Adressdaten automatisch erkannt.
  - Static

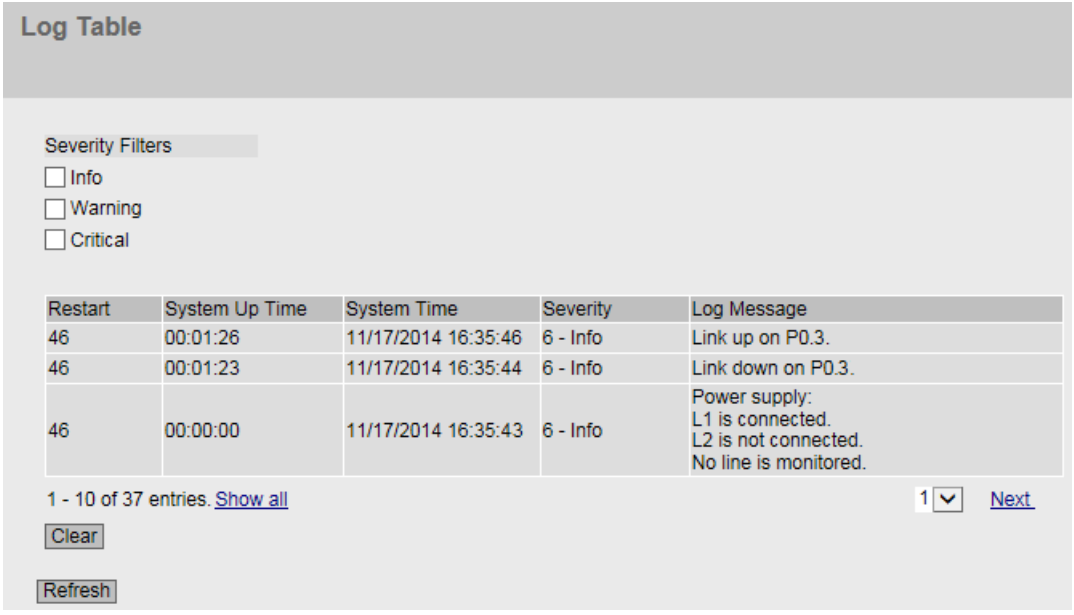
    Die Adressen wurden als statische Adressen eingetragen.

5.3.5 Log Table

Protokollierung von Ereignissen

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

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



Severity Filters

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

- **Info**
  informativ
- **Warning**
  Warnungen
- **Critical**
  kritisch

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

Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Spalten:

- **Restart**
  Zählt die Anzahl der Neustarts seit dem letzten Zurücksetzen auf Werkseinstellungen und gibt an, nach welchem Neustart des Gerätes das entsprechende Ereignis aufgetreten ist.
- **System Up Time**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an, zu der das beschriebene Ereignis aufgetreten ist.

  Wenn die Systemzeit gesetzt ist, wird auch die Zeit angezeigt, bei der das Ereignis eingetreten ist.
- **System Time**
  Zeigt das Datum und die Uhrzeit des Geräts an.
- **Severity**
  Einordnung des Eintrags in obige Kategorien.
- **Log Message**
  Zeigt eine Kurzbeschreibung des eingetretenen Ereignisses an.

Beschreibung der Schaltflächen und Eingabefelder

Schaltfläche "Clear"

Klicken Sie auf diese Schaltfläche, um den Inhalt der Ereignisprotokolldatei zu löschen. Die Anzeige wird dabei ebenfalls geleert. Erst wenn nach dem Wiederherstellen der Werkseinstellungen das Gerät neu gestartet ist, wird der Neustart-Zähler zurückgesetzt.

Hinweis

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

Schaltfläche "Show all"

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

Schaltfläche "Next"

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

Schaltfläche "Prev"

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

Klappliste für Seitenwechsel

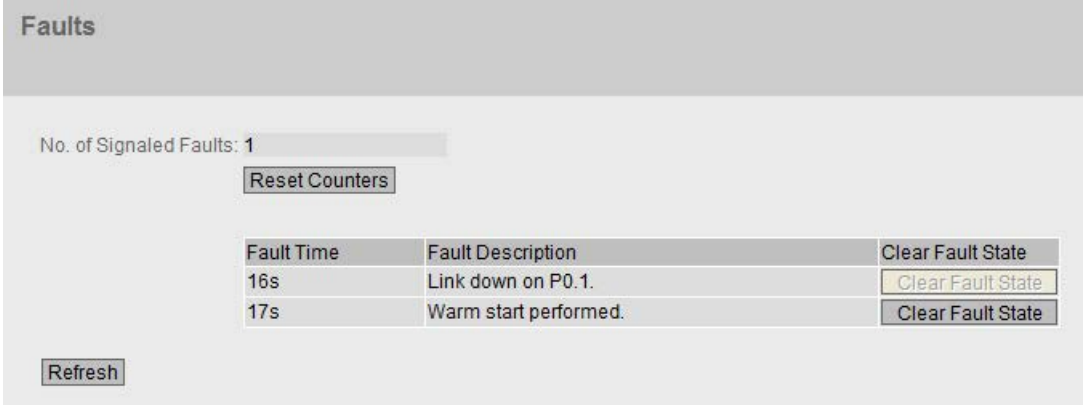
Wählen Sie aus der Klappliste die gewünschte Seite aus, um zu einer bestimmten Seite zu navigieren.

5.3.6 Faults

Fehlerstatus

Diese Seite zeigt auftretende Fehler an. Fehler des Ereignisses "Cold/Warm Start" können nach einer Bestätigung wieder gelöscht werden.
Wenn es keine weitere unbeantwortete Fehlermeldungen gibt, schaltet sich die Fehler-LED ab.

Die Zeitrechnung beginnt jeweils nach dem letzten Systemstart. Bei einem Neustart des Systems wird im Fehlerspeicher ein neuer Eintrag mit der durchgeführten Startart erzeugt.



Beschreibung der angezeigten Werte

- **No. of Signaled Faults**

  Anzahl der seit dem letzten Hochlauf angezeigten Fehler.

Die Tabelle enthält die folgenden Spalten:

- **Fault Time**
  Zeigt die Laufzeit des Geräts seit dem letzten Neustart an, zu der der beschriebene Fehler aufgetreten ist.
- **Fault Description**
  Anzeige des Fehlerstatus für das Gerät.
- **Clear Fault State**
  Wenn die Schaltfläche "Clear Fault State" aktiv ist, können Sie den Fehler löschen.

Beschreibung der Schaltfläche

Schaltfläche "Reset Counter"

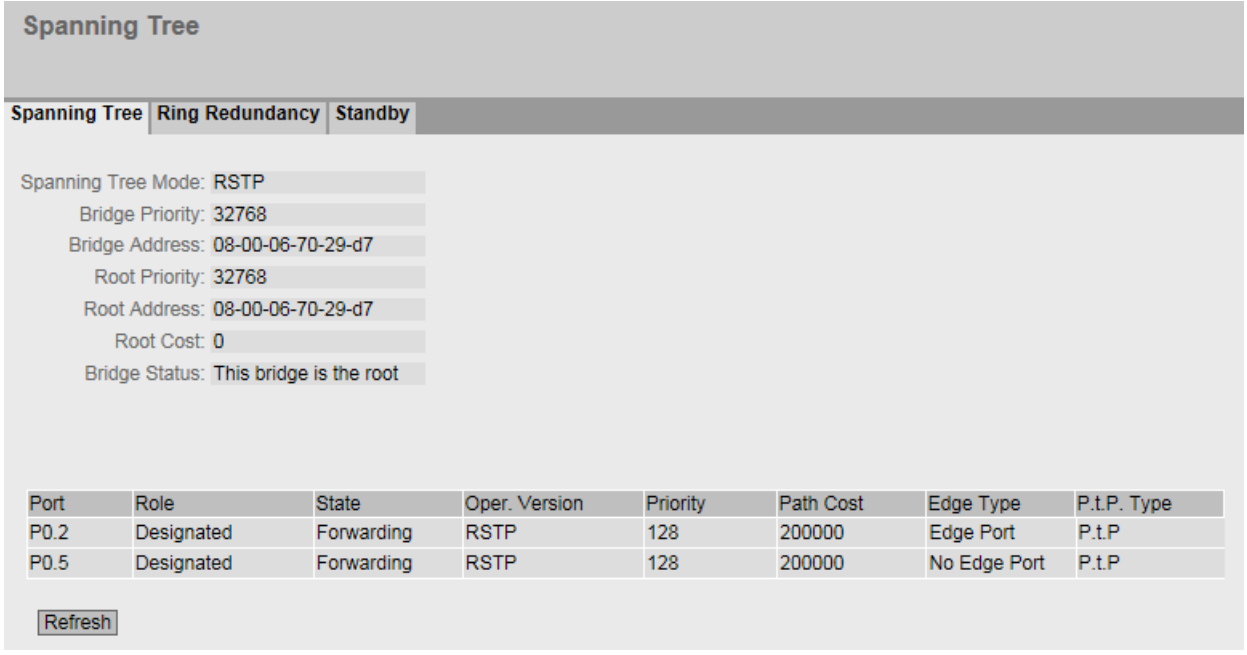
Klicken Sie auf "Reset Counter", um alle Zähler zurückzusetzen. Die Zähler werden durch einen Neustart zurückgesetzt.

5.3.7 Redundancy

5.3.7.1 Spanning Tree

Einleitung

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



Beschreibung der angezeigten Werte

Folgende Felder werden angezeigt:

- **Spanning Tree Mode**
  Zeigt den eingestellten Modus an. Den Modus legen Sie bei "Layer 2 > Configuration" und bei "Layer 2 > Spanning Tree > General" fest.
  Folgende Werte sind möglich:
  - '-'
  - STP
  - RSTP
- **Bridge Priority / Root Priority**
  Anhand der Bridge-Priorität wird festgelegt, welches Gerät Root Bridge wird. Die Bridge mit der höchsten Priorität (d. h. dem kleinsten Wert für diesen Parameter) wird Root Bridge. Wenn in einem Netz mehrere Geräte die gleiche Priorität besitzen, dann wird das Gerät Root Bridge, dessen MAC-Adresse den niedrigsten Zahlenwert hat. Beide Parameter, Bridge-Priorität und MAC-Adresse, bilden zusammen die Bridge-Kennung. Da die Root Bridge alle Wegeänderungen verwaltet, sollte sie wegen der Laufzeit der Telegramme möglichst zentral angeordnet sein. Der Wert für die Bridge-Priorität ist ein ganzzahliges Vielfaches von 4096 mit einem Wertebereich von 0 bis 32768.
- **Bridge Address / Root Address**
  Die Bridge-Adresse zeigt die MAC-Adresse des Geräts und die Root-Adresse zeigt die MAC-Adresse der Root-Switch an.
- **Root Cost**

  Zeigt die Pfadkosten von dem Gerät bis zur Root Bridge.
- **Bridge Status**

  Zeigt den Status der Bridge an, z. B. ob das Gerät die Root-Bridge ist.

Die Tabelle gliedert sich in folgende Spalten:

- Port
  Zeigt den Port an, über den das Gerät kommuniziert. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- Role
  zeigt den Status des Ports an. Folgende Werte sind möglich:
  - Disabled
    Der Port wurde manuell aus dem Spanning Tree entfernt und wird vom Spanning Tree nicht mehr berücksichtigt.
  - Designated
    Die Ports, die von der Root-Bridge wegführen.
  - Alternate
    Der Port mit einem alternativen Weg zu einem Netzwerksegment
  - Backup
    Wenn ein Switch mehrere Ports zu dem gleichen Netzwerksegment hat, wird der "schlechtere" Port zum Backup-Port.
  - Root
    Der Port, der den besten Weg zur Root Bridge bietet.
  - Master
    Dieser Port zeigt zu einer Root-Bridge, die außerhalb der MST-Region liegt.
- State
  Zeigt den momentanen Status an, in dem sich der Port befindet. Die Werte werden nur angezeigt. Der Parameter ist abhängig vom projektierten Protokoll. Folgende Status sind möglich:
  - Discarding
    Der Port empfängt BPDU-Telegramme. Andere aus- oder eingehende Telegramme werden verworfen.
  - Listening
    Der Port empfängt und sendet BPDU-Telegramme. Der Port ist in den Spanning Tree-Algorithmus einbezogen. Andere aus- und eingehende Telegramme werden verworfen.
  - Learning
    Der Port lernt aktiv die Topologie, d. h. die Teilnehmeradressen. Andere aus- und eingehende Telegramme werden verworfen.
  - Forwarding
    Der Port ist nach der Umkonfigurationszeit aktiv im Netz. Der Port empfängt und sendet Datentelegramme.
- Oper. Version
  Beschreibt die Art des Spanning Tree, in dem der Port arbeitet
- Priority
  Kann der vom Spanning-Tree ermittelte Weg alternativ über mehrere Ports eines Gerätes führen, so wird der Port mit der höchsten Priorität (d. h. dem kleinsten Wert für diesen Parameter) ausgewählt. Für die Priorität kann ein Wert von 0 bis 240 in 16er Schritte eingegeben werden. Wenn Sie einen Wert eingeben, der nicht durch 16 teilbar ist, wird der Wert automatisch angepasst. Der Standardwert ist 128.

- **Path Cost**
  Dieser Parameter dient zur Berechnung des zu wählenden Weges. Es wird die Strecke mit dem geringsten Wert als Weg ausgewählt. Haben mehrere Ports eines Gerätes den gleichen Wert, wird der Port mit der niedrigsten Portnummer ausgewählt.
  Ist der Wert im Feld "Cost Calc" "0", so wird der automatisch ermittelte Wert angezeigt. Im anderen Fall wird der Wert des Feldes "Cost Calc" angezeigt.
  Die Ermittlung der Wegekosten richtet sich maßgeblich nach der Übertragungsgeschwindigkeit. Je höher die erzielbare Übertragungsgeschwindigkeit ist, umso kleiner ist der Wert für die Wegekosten.

  Typische Werte für Wegekosten bei Rapid Spanning Tree:

  – 10.000 Mbit/s = 2.000
  – 1000 Mbit/s = 20.000
  – 100 Mbit/s = 200.000
  – 10 Mbit/s = 2.000.000

- **Edge Type**
  Zeigt den Typ der Verbindung an. Folgende Werte sind möglich:

  – Edge Port
    An diesem Port befindet sich ein Endgerät.
  – No Edge Port
    An diesem Port befindet sich ein Spanning Tree- oder Rapid Spanning Tree-Gerät.

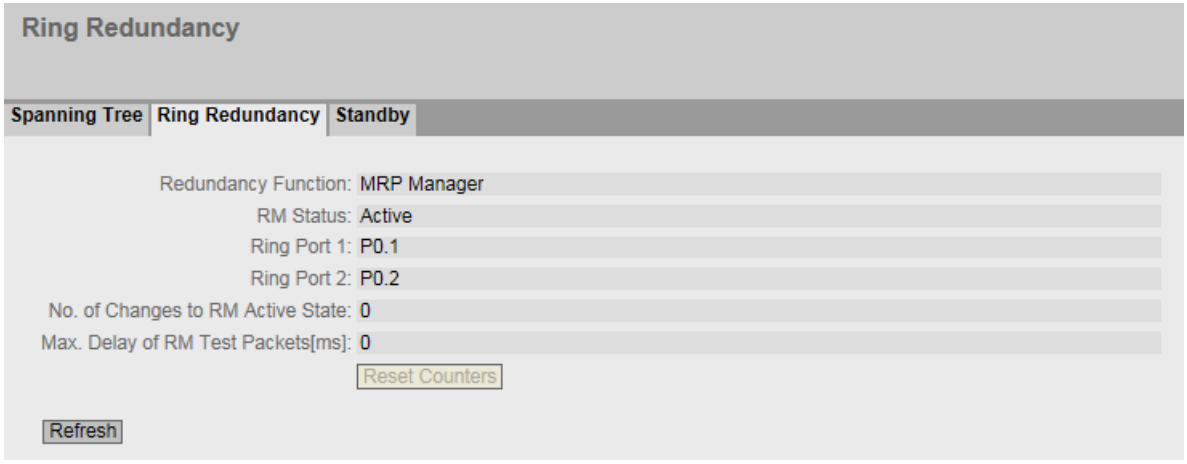
- **P.t.P. Type**
  zeigt die Art der Punkt-zu-Punkt-Verbindung an. Folgende Werte sind möglich:

  – P.t.P.
    Bei Halbduplex wird von einer Punkt-zu-Punkt-Verbindung ausgegangen.
  – Shared Media
    Bei einer Vollduplexverbindung wird nicht von einer Punkt-zu-Punkt-Verbindung ausgegangen.

5.3.7.2 Ring Redundancy

Informationen zur Ring-Redundanz

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



Beschreibung der angezeigten Werte

Folgende Felder werden angezeigt:

- **Redundancy Function**

  Das Feld "Redundancy Function" zeigt die Rolle des Geräts innerhalb des Rings an:

  – No Ring Redundancy (off)
  Der IE-Switch arbeitet ohne Redundanz-Funktion.

  – HRP Client
  Der IE-Switch arbeitet als HRP Client.

  – HRP Manager
  Der IE-Switch arbeitet als HRP Manager.

  – MRP Client
  Der IE-Switch arbeitet als MRP Client.

  – MRP Manager
  Der IE-Switch arbeitet als MRP Manager.

  Hinweis

  MRP-Projektierung in STEP 7

  Wenn Sie über STEP 7 die Rolle "Manager (Auto)" oder "Manager" für das Gerät einstellen, wird auf dieser WBM-Seite in beiden Fällen "MRP Manager" angezeigt. In der Anzeige im CLI wird zwischen den beiden Rollen unterschieden.

- **RM Status**

  Das Feld "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 die zuletzt konfigurierten Ringports angezeigt und es erscheint der Text "Ring Redundancy disabled".

- **Ring Port 1 und Ring Port 2**

  Die Felder "Ring Port 1" und "Ring Port 2" zeigen die Ports an, die als Ringports verwendet werden.

- **No. of Changes to RM Active State**

  Zeigt an, wie oft das Gerät als Redundanzmanager in den aktiven Zustand geschaltet hat, d. h. den Ring geschlossen hat.

  Wenn die Redundanzfunktion deaktiviert ist oder das Gerät "HRP-/MRP-Client" ist, dann erscheint der Text "Redundancy Manager Disabled".

- **Max. Delay of RM Test Packets[ms]**

  Zeigt die maximale Verzögerungszeit für Testtelegramme des Redundanzmanagers an.

  Wenn die Redundanzfunktion deaktiviert ist oder das Gerät "HRP-/MRP-Client" ist, dann erscheint der Text "Redundancy Manager Disabled".

Beschreibung der Schaltfläche

Schaltfläche "Reset Counter"

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

5.3.7.3 Standby

Informationen zur Standby-Redundanz

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

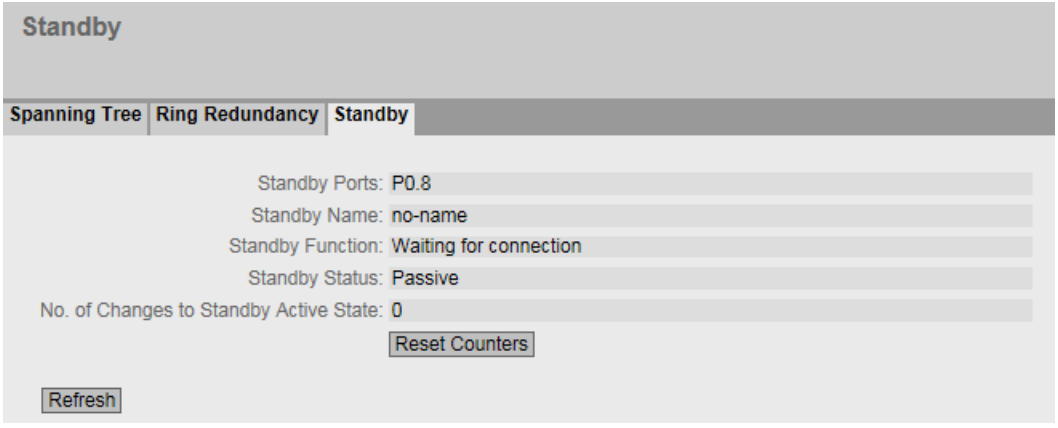
Hinweis

Gerät mit höherer MAC-Adresse wird Master

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

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

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



Beschreibung der angezeigten Werte

Folgende Felder werden angezeigt:

- **Standby Ports**

  Zeigt den Standby-Port an.

- **Standby Name**

  Name der Standby-Verbindung

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

  Das Anzeigefeld "Standby Status" zeigt den Status des Standby-Ports an:
  - Active:
    Der Standby-Port dieses Geräts ist aktiv, d. h. für den Telegrammverkehr freigeschaltet.
  - Passive:
    Der Standby-Port dieses Geräts ist inaktiv, d. h. für den Telegrammverkehr gesperrt.
  - "-":
    Die Standby-Funktion ist deaktiviert.
- **No. of Changes to Standby Active State**

  Zeigt an, wie oft der IE-Switch den Standby-Status vom Zustand "Passive" in den Zustand "Active" geändert hat. Wenn die Verbindung eines Standby-Ports beim Standby-Master ausfällt, wechselt der IE-Switch in den Zustand "Active".

  Wenn die Standby-Funktion deaktiviert ist, erscheint der Text "Standby Disabled" in diesem Feld.

Beschreibung der Schaltfläche

Schaltfläche "Reset Counter"

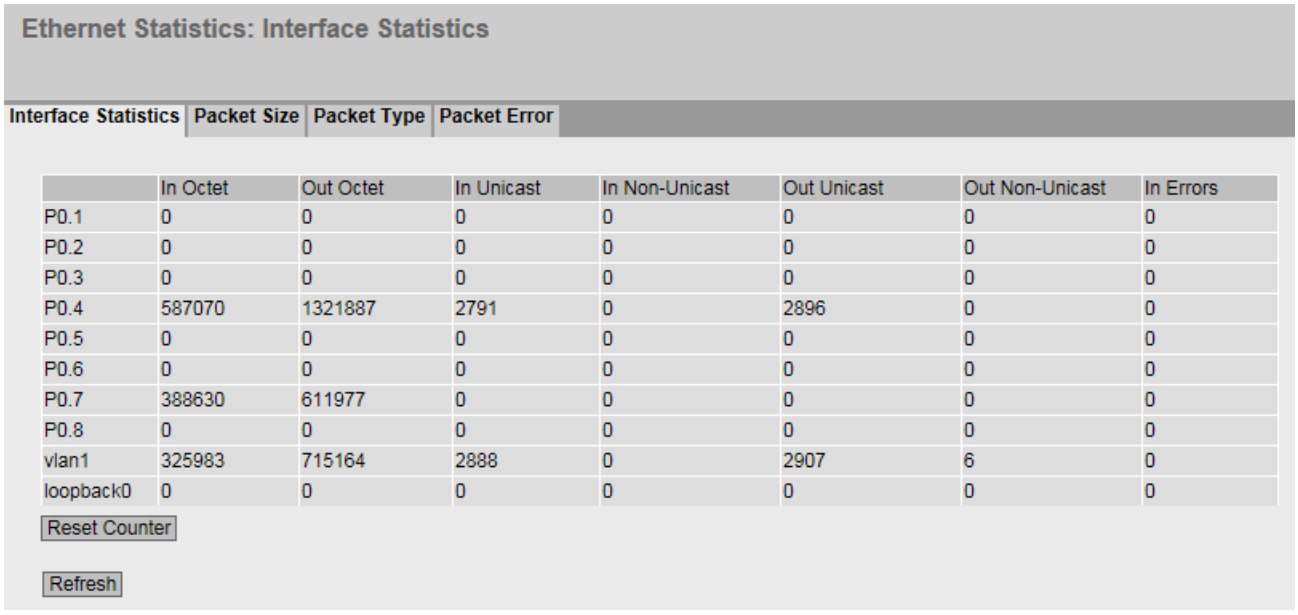
Klicken Sie auf "Reset Counter", um alle Zähler zurückzusetzen. Die Zähler werden durch einen Neustart zurückgesetzt.

5.3.8 Ethernet Statistics

5.3.8.1 Interface Statistics

Schnittstellenstatistik

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



	In Octet	Out Octet	In Unicast	In Non-Unicast	Out Unicast	Out Non-Unicast	In Errors
P0.1	0	0	0	0	0	0	0
P0.2	0	0	0	0	0	0	0
P0.3	0	0	0	0	0	0	0
P0.4	587070	1321887	2791	0	2896	0	0
P0.5	0	0	0	0	0	0	0
P0.6	0	0	0	0	0	0	0
P0.7	388630	611977	0	0	0	0	0
P0.8	0	0	0	0	0	0	0
vlan1	325983	715164	2888	0	2907	6	0
loopback0	0	0	0	0	0	0	0

Angezeigte Werte

Die Tabelle gliedert sich in folgende Spalten:

- **In Octet**

  Zeigt die Anzahl der empfangenen Bytes an.

- **Out Octet**

  Zeigt die Anzahl der gesendeten Bytes an.

- **In Unicast**

  Zeigt die Anzahl der empfangenen Unicast-Telegramme an.

- **In Non-Unicast**

  Zeigt die Anzahl der empfangenen Telegramme an, die nicht vom Telegrammtyp Unicast sind.

- **Out Unicast**

  Zeigt die Anzahl der gesendeten Unicast-Telegramme an.

- **Out Non-Unicast**

  Zeigt die Anzahl der gesendeten Telegramme an, die nicht vom Telegrammtyp Unicast sind.

- **In Errors**

  Zeigt die Anzahl aller möglichen RX-Fehler an, siehe Reiter "Packet Error".

Beschreibung der Schaltfläche

Schaltfläche "Reset Counter"

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

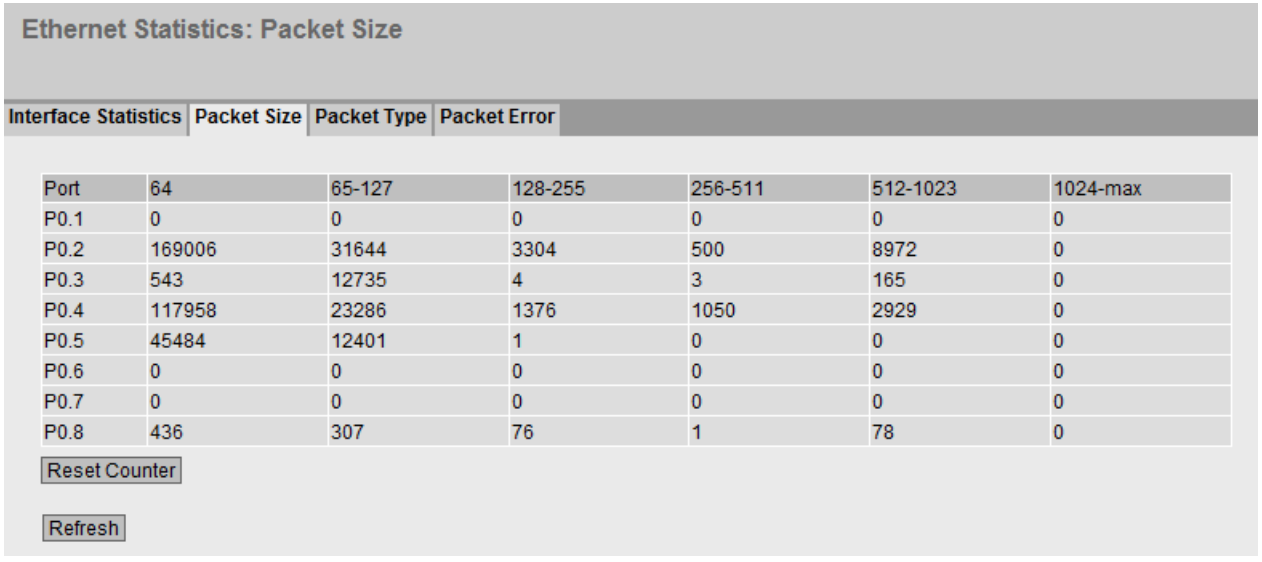
5.3.8.2 Packet Size

Telegramme sortiert nach Länge

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

Die angezeigten Werte werden durch RMON übermittelt.

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



Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Spalten:

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

  Hinweis

  Anzeige der Telegrammstatistik

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

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

Hinweis

Datenverkehr auf geblockten Ports

Aus technischen Gründen können auf geblockten Ports Datenpakete angezeigt werden.

Beschreibung der Schaltfläche

Schaltfläche "Reset Counter"

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

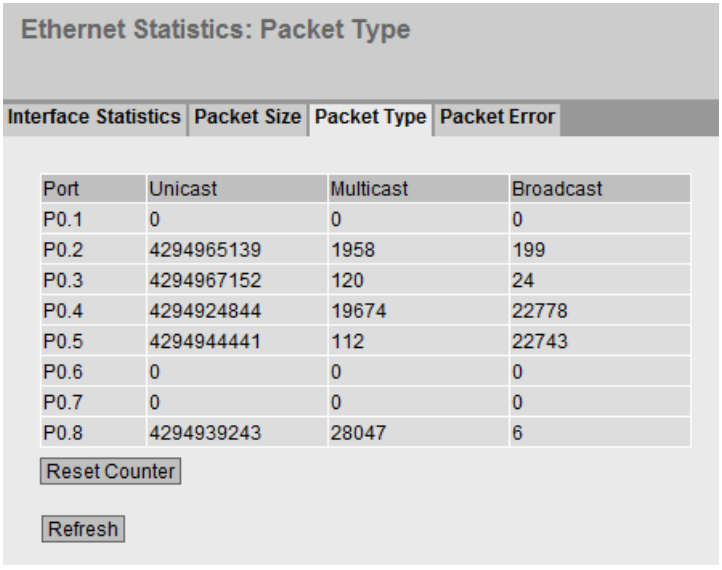
5.3.8.3 Packet Type

Empfangener Telegramme sortiert nach Telegrammtyp

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

Die angezeigten Werte werden durch RMON übermittelt.

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



Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Spalten:

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

Beschreibung der Schaltfläche

Schaltfläche "Reset Counter"

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

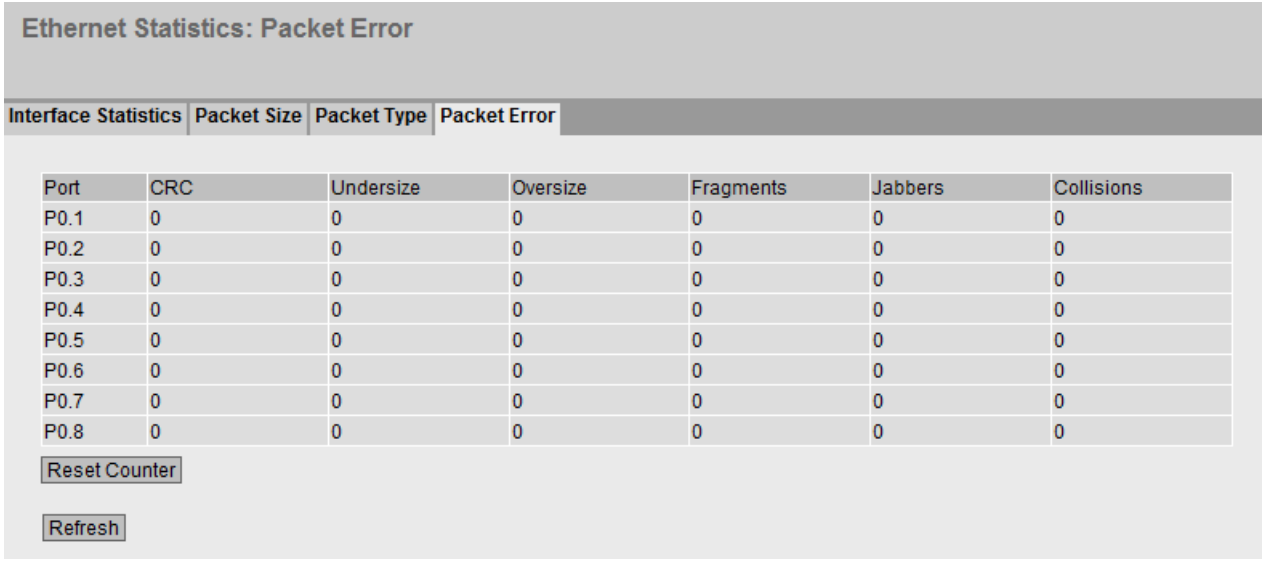
5.3.8.4 Packet Error

Fehlerhaft empfangener Telegramme

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

Die angezeigten Werte werden durch RMON übermittelt.

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



Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Fehlertypen**
  Die weiteren Spalten hinter der jeweiligen Portnummer enthalten die absoluten Zahlen der eingegangenen Telegramme entsprechend ihres Fehlertyps.

  Dabei wird in den Spalten der Tabelle nach folgenden Fehlertypen unterschieden:

  – CRC
    Pakete, deren Inhalt nicht mit der zugehörigen CRC-Prüfsumme übereinstimmt.
  – Undersize
    Pakete mit einer Länge kleiner als 64 Byte.
  – Oversize
    Pakete, die aufgrund einer zu großen Länge verworfen wurden.
  – Fragments
    Pakete mit einer Länge kleiner als 64 Byte und einer falschen CRC-Prüfsumme.
  – Jabbers
    VLAN-getaggte Pakete mit einer falschen CRC Prüfsumme, die aufgrund einer zu großen Länge verworfen wurden.
  – Collisions
    Erkannte Kollisionen.

Beschreibung der Schaltfläche

Schaltfläche "Reset Counter"

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

5.3.9 Unicast

Status der Unicast-Filtertabelle

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

Abhängigkeit vom "Base Bridge Mode"

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

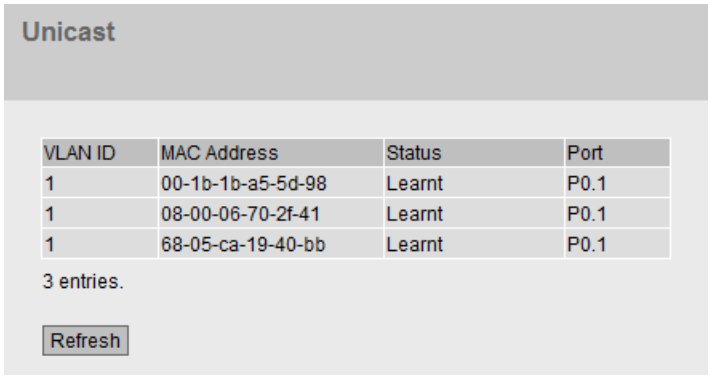


Bild 5-1 Base Bridge Mode: 802.1Q VLAN Bridge

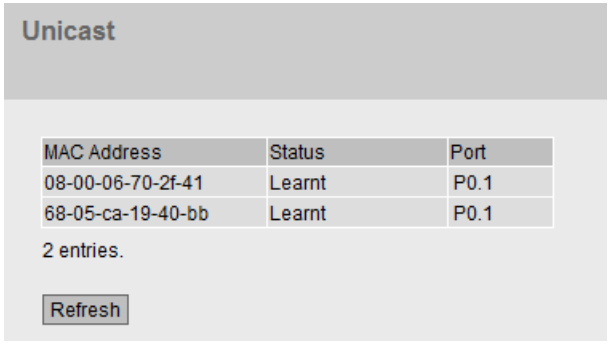


Bild 5-2 Base Bridge Mode: 802.1D Transparent Bridge

Beschreibung

Die Tabelle kann folgende Spalten enthalten:

- **VLAN ID**
  Zeigt die VLAN-ID, die dieser MAC-Adresse zugeordnet ist.
- **MAC Address**
  Zeigt die MAC-Adresse des Teilnehmers, die das Gerät gelernt hat oder die der Anwender projektiert hat.

- **Status**
  Zeigt den Status jedes Adresseintrags:
  - Learnt
    Die angegebene Adresse wurde durch Empfang eines Telegramms dieses Teilnehmers gelernt und wird nach Ablauf der Aging Time wieder gelöscht, sollten keine weiteren Pakete dieses Teilnehmers empfangen werden.

    Hinweis

    Bei einem Link-Down werden gelernte MAC-Einträge gelöscht.

  - Static
    Vom Anwender projektiert. Statische Adressen sind permanent gespeichert, d.h. sie werden nach Ablauf der Aging Time oder beim Neustart des Switchs nicht gelöscht.
- **Port**
  Zeigt an, über welchen Port der Teilnehmer mit der angegebenen Adresse erreichbar ist. Vom Gerät empfangene Telegramme, deren Zieladresse mit dieser Adresse übereinstimmt, werden an diesen Port weitergegeben.

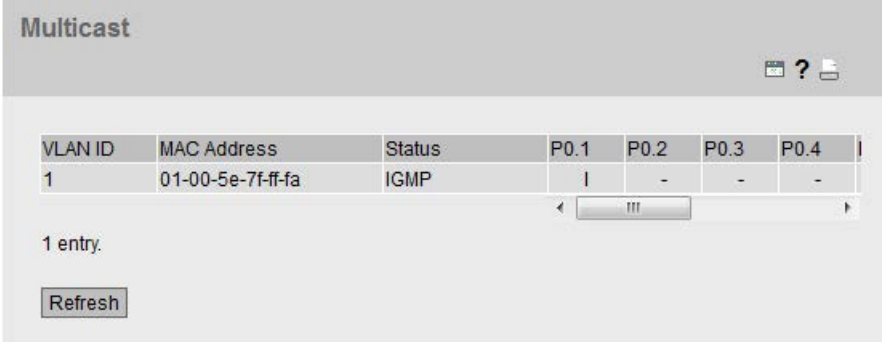
5.3.10 Multicast

Status der Multicast-Filtertabelle

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

Abhängigkeit vom "Base Bridge Mode"

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



Beschreibung

Die Tabelle kann folgende Spalten enthalten:

- **VLAN ID**

  Zeigt VLAN-ID des VLANs an, dem die MAC-Multicast-Adresse zugeordnet ist.

- **MAC Address**

  Zeigt MAC-Multicast-Adresse an, die das Gerät gelernt hat oder die der Anwender projektiert hat.

- **Status**

  Zeigt den Status jedes Adress-Eintrags. Dabei sind folgende Angaben möglich:

  – 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 Neustart des Gerätes gelöscht. Sie müssen vom Anwender gelöscht werden.

  – IGMP
  Der Zielport für diese Adresse wurde über IGMP-Konfiguration ermittelt.

- **Liste der Ports**
  Für jeden Steckplatz gibt es eine Spalte. Innerhalb einer Spalte wird für jeden Port die Zugehörigkeit zur Multicast-Gruppe angezeigt:

  – M
  (Member) Über diesen Port werden Multicast-Telegramme gesendet.

  – I
  (IGMP) Mitglied der Multicast-Gruppe, die Registrierung erfolgte über ein IGMP-Telegramm.

  – –
  Kein Mitglied der Multicast-Gruppe. Über diesen Port werden keine Multicast-Telegramme mit der definierten Multicast-MAC-Adresse gesendet.

  – F
  (Forbidden) Kein Mitglied der Multicast-Gruppe. Außerdem darf diese Adresse nicht dynamisch über IGMP gelernt werden.

5.3.11 LLDP

Status der Nachbarschaftstabelle

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

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

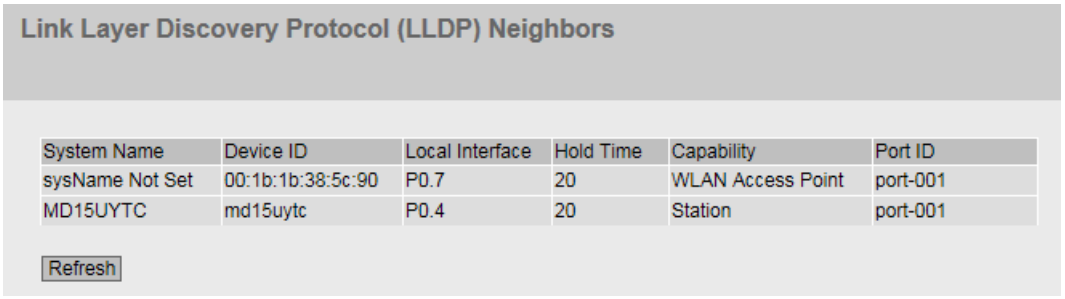


Bild 5-3 Information LLDP

Beschreibung der angezeigten Werte

Die Tabelle enthält folgende Spalten:

- **System Name**

  Systemname des angeschlossenen Geräts.

- **Device ID**

  Gerätekennung des angeschlossenen Geräts.

- **Local Interface**

  Port, an dem der IE-Switch die Informationen empfangen hat.

- **Hold Time**

  Ein Eintrag bleibt für die hier angegebene Zeit in der MIB gespeichert. Wenn der IE-Switch in dieser Zeit keine neuen Informationen von dem angeschlossenen Gerät erhält, wird der Eintrag gelöscht.

- **Capability**

  Zeigt die Eigenschaften des angeschlossenen Geräts an:

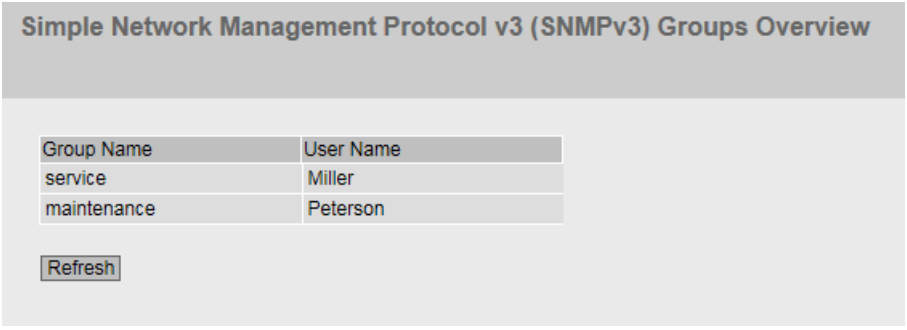
  – Router
  – Bridge
  – Telephone
  – DOCSIS Cable Device
  – WLAN Access Point
  – Repeater
  – Station
  – Other

- **Port ID**

  Port des Geräts, der mit dem IE-Switch verbunden ist.

5.3.12 SNMP

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



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Group Name**

  Zeigt den Gruppennamen an.

- **User Name**

  Zeigt den Benutzer an, welcher der Gruppe zugeordnet ist.

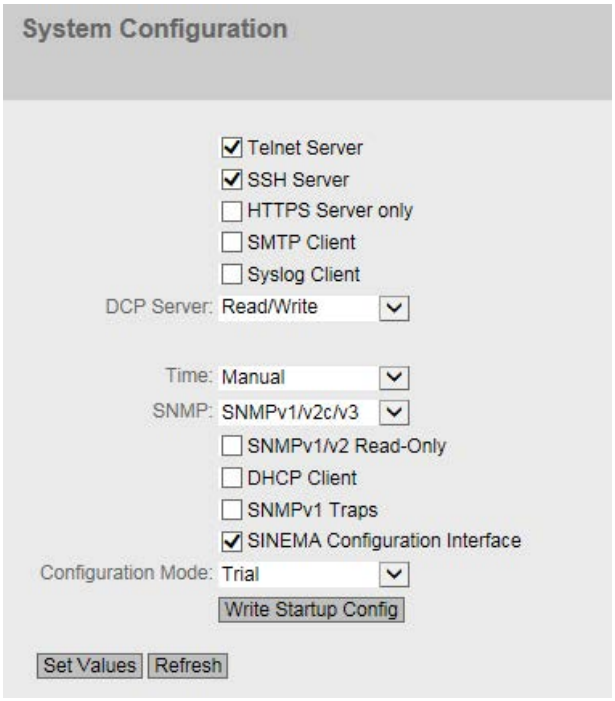
5.4 Das Menü "System"

5.4.1 Configuration

Systemkonfiguration

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

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



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Telnet Server**
  Aktivieren oder deaktivieren Sie den Dienst "Telnet Sever" für den unverschlüsselten Zugriff auf das CLI.
- **SSH Server**
  Aktivieren oder deaktivieren Sie den Dienst "SSH Server" für den verschlüsselten Zugriff auf das CLI.
- **HTTPS Server only**
  Wenn diese Funktion aktiviert ist, können Sie nur noch über HTTPS auf das Gerät zugreifen.

- **SMTP Client**
  Aktivieren oder deaktivieren Sie den SMTP-Client. Weitere Einstellungen konfigurieren Sie unter "System > SMTP Client".
- **Syslog Client**
  Aktivieren oder deaktivieren Sie den Syslog-Client. Weitere Einstellungen konfigurieren Sie unter "System > Syslog Client".
- **DCP Server**
  Legen Sie fest, ob auf das Gerät mit DCP (Discovery and Configuration Protocol) zugegriffen werden kann:
  - "-" (Deaktiviert)
    DCP ist deaktiviert. Geräteparameter können weder gelesen noch geändert werden.
  - Read/Write
    Mit DCP können Geräteparameter sowohl gelesen als auch verändert werden.
  - Read-Only
    Mit DCP können Geräteparameter zwar gelesen aber nicht verändert werden.
- **Time**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungen sind möglich:
  - Manual
    Die Systemzeit wird manuell eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > System Time > Manual Setting".
  - SIMATIC Time
    Die Systemzeit wird über einen SIMATIC Zeitgeber eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > System Time > SIMATIC Time Client".
  - SNTP Client
    Die Systemzeit wird über einen SNTP Server eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > System Time > SNTP Client".
  - NTP Client
    Die Systemzeit wird über einen NTP Server eingestellt. Weitere Einstellungen konfigurieren Sie unter "System > System Time > NTP Client".
- **SNMP**
  Wählen Sie aus der Klappliste das Protokoll. Folgende Einstellungen sind möglich:
  - "-" (SNMP deaktiviert)
    Ein Zugriff auf die Geräteparameter ist über SNMP nicht möglich.
  - SNMPv1/v2c/v3
    Ein Zugriff auf die Geräteparameter ist mit den SNMP Versionen 1, 2c oder 3 möglich. Weitere Einstellungen konfigurieren Sie unter "System > SNMP > General".
  - SNMPv3
    Ein Zugriff auf die Geräteparameter ist nur mit der SNMP Version 3 möglich. Weitere Einstellungen konfigurieren Sie unter " System > SNMP > General".
- **SNMPv1/v2 Read-Only**
  Aktivieren oder deaktivieren Sie den schreibenden Zugriff auf SNMP-Variablen bei SNMPv1/v2c.

- **DHCP Client**
  Aktivieren oder deaktivieren Sie den DHCP-Client. Weitere Einstellungen konfigurieren Sie unter "System > DHCP Client".
- **SNMPv1 Traps**
  Aktivieren oder deaktivieren Sie das Versenden von Traps (Alarmtelegramme). Weitere Einstellungen konfigurieren Sie unter "System > SNMP > Traps".
- **SINEMA Configuration Interface**
  Wenn die SINEMA-Konfigurationsschnittstelle aktiviert ist, können Sie Konfigurationen über das TIA-Portal auf den IE-Switch laden.
- **Configuration Mode**

  Wählen Sie aus der Klappliste die Betriebsart. Folgende Betriebsarten sind möglich:

  – Automatic Save
    Automatischer Sicherungsbetrieb. Ca. 1 Minute nach der letzten Parameteränderung oder beim Neustart des Geräts wird die Konfiguration automatisch abgespeichert.

  – Trial
    Trial-Modus. Im Trial-Modus werden Änderungen zwar übernommen aber nicht in der Konfigurationsdatei (Startup Configuration) gespeichert.
    Um Änderungen in der Konfigurationsdatei abzuspeichern, verwenden Sie die Schaltfläche "Write Startup Config". Die Schaltfläche "Write Startup Config" wird eingeblendet, wenn Sie den Trial-Modus einstellen. Zusätzlich wird im Anzeigebereich die Meldung "Trial Mode Active – Press "Write Startup Config" button to make your settings persistent." angezeigt sobald es ungespeicherte Änderungen gibt. Diese Meldung ist auf jeder WBM-Seite sichtbar, bis die vorgenommenen Änderungen entweder gespeichert werden oder das Gerät neu gestartet wird.

Vorgehensweise zur Konfiguration

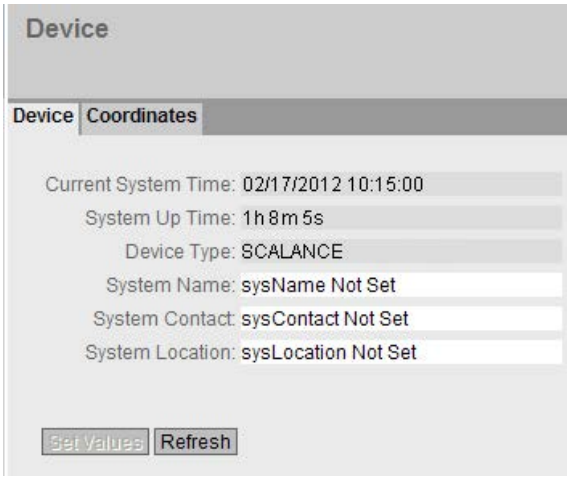
1. Um die gewünschte Funktion zu nutzen, aktivieren Sie das entsprechende Optionskästchen.
2. Wählen Sie aus den Klapplisten die gewünschten Optionen.
3. Klicken Sie auf die Schaltfläche "Set Values".

5.4.2 General

5.4.2.1 Device

Allgemeine Geräteinformationen

Diese Seite enthält die allgemeinen Geräteinformationen.



Die Felder "Current System Time", "System Up Time" und "Device Type" können nicht geändert werden.

Beschreibung

Die Seite enthält folgende Felder:

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

- **Eingabefeld "System Contact"**
  Sie können den Namen einer Kontaktperson eintragen, die für die Verwaltung des Gerätes zuständig ist. Es sind maximal 255 Zeichen möglich.
- **Eingabefeld "System Location"**
  Sie können den Montageort des Gerätes eintragen. Der eingetragene Montageort wird im Auswahlbereich angezeigt. Es sind maximal 255 Zeichen möglich.

Hinweis

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

Zu Beginn und am Ende der Felder **"System Name"**, **"System Contact"** und **"System Location"** sind die Zeichen "<", ">" und "Leer" nicht erlaubt.

Vorgehensweise

1. Tragen Sie in das Eingabefeld "System Contact" den für das Gerät zuständigen Ansprechpartner ein.
2. Tragen Sie in das Eingabefeld "System Location" die Ortsbezeichnung des Aufstellungsorts ein.
3. Tragen Sie in das Eingabefeld "System Name" den Namen des Gerätes ein.
4. Klicken Sie auf die Schaltfläche "Set Values".

5.4.2.2 Coordinates

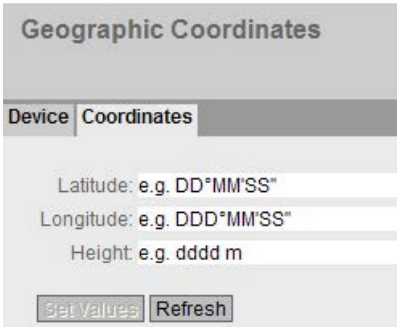
Informationen über die geografischen Koordinaten

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

Ermittlung der Koordinaten

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

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



Beschreibung

Die Seite enthält folgende Felder. Es sind reine Informationsfelder mit einer maximalen Länge von 32 Zeichen.

- **Eingabefeld "Latitude"**
  Geografische Breite: Hier wird der Wert für nördliche oder südliche Breite für den Standort des Gerätes eingegeben.

  Der Wert +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).
- **Eingabefeld "Longitude"**
  Geografische Länge: Hier wird der Wert für östliche oder westliche Länge für den Standort des Gerätes eingegeben.
  Der Wert +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).
- **Eingabefeld: "Height"**
  Geografische Höhe: Hier wird der Wert für geografische Höhe über oder unter normal Null (Meereshöhe) in Metern eingegeben.
  Z.B. 158 m bedeutet, dass sich das Gerät in einer Höhe von 158 m über normal Null befindet.
  Höhenangaben unterhalb von normal Null (z. B. am Toten Meer) werden mit einem führenden Minuszeichen dargestellt.

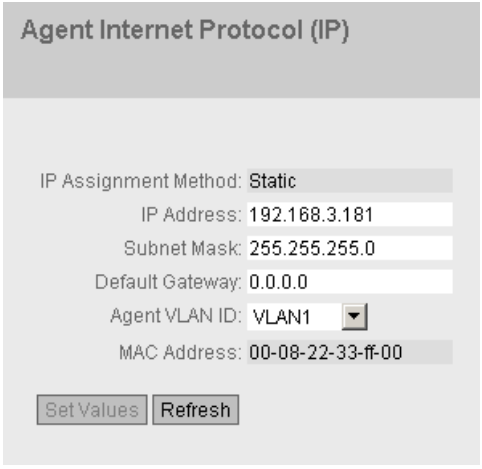
Vorgehensweise

1. Geben Sie in das Eingabefeld "Latitude" den ermittelten Breitengrad ein.
2. Geben Sie in das Eingabefeld "Longitude" den ermittelten Längengrad ein.
3. Geben Sie in das Eingabefeld "Height" die ermittelte Höhe über dem Meeresspiegel ein.
4. Klicken Sie auf die Schaltfläche "Set Values".

5.4.3 Agent IP

Konfiguration der IP-Adressen

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



Beschreibung

Die Seite enthält folgende Felder:

- **IP Assignment Method**
  Zeigt an, wie die IP-Adresse zugeordnet wird.
  - Static
    Die IP-Adresse ist statisch. Die IP-Einstellungen tragen Sie in den Eingabefeldern "IP Address" und "Subnet Mask" ein.
  - Dynamic (DHCP)
    Das Gerät bezieht eine dynamische IP-Adresse von einem DHCP-Server.
- **IP Address**
  Tragen Sie die IP-Adresse des Geräts ein.
  Nach dem Anklicken der Schaltfläche "Set Values" wird diese IP-Adresse auch in der Adresszeile des Internet-Browsers angezeigt. Sollte dies nicht automatisch erfolgen, müssen Sie die IP-Adresse manuell in die Adresszeile des Internet-Browsers eintragen.
- **Subnet Mask**
  Tragen die Subnetzmaske des Geräts ein.
- **Default Gateway**
  Tragen Sie die IP-Adresse des Standard-Gateways ein, um mit Geräten in einem anderen Subnetz zu kommunizieren, z. B. Diagnosestationen, E-Mail-Server.

- **Agent VLAN ID**

  Wählen Sie aus der Klappliste die VLAN ID. Sie können nur aus bereits konfigurierten VLANs auswählen.

  In dem Modus "802.1D Transparent Bridge" ist diese Klappliste ausgegraut, siehe auch "Layer 2 > VLAN > General".

  Hinweis
  Ändern der Agent VLAN ID

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

- **MAC Address**

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

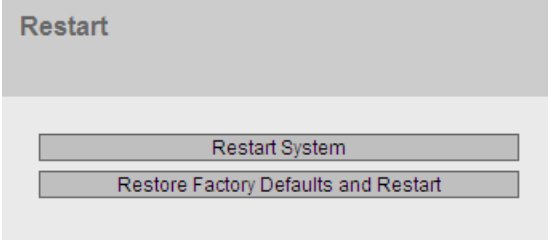
Vorgehensweise

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

5.4.4 Restart

Zurücksetzen der Voreinstellungen

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



Hinweis

Beachten Sie folgende Punkte beim Neustart eines Gerätes:

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

Beschreibung der angezeigten Felder

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

- **Schaltfläche "Restart System"**
  Klicken Sie auf diese Schaltfläche, um das System neu zu starten. Sie müssen den Neustart in einer Dialogbox bestätigen. Bei einem Neustart wird das Gerät neu initialisiert, die interne Firmware wird neu geladen und das Gerät führt einen Selbsttest durch. Die gelernten Einträge in der Adresstabelle werden gelöscht. Sie können das Browser-Fenster geöffnet lassen, während das Gerät neu startet. Sie müssen sich wieder neu anmelden.
- **Schaltfläche "Restore Factory Defaults and Restart"**
  Klicken Sie auf diese Schaltfläche, um die werkseitigen Konfigurationseinstellungen wiederherzustellen. Es werden auch die geschützten Voreinstellungen zurückgesetzt. Es wird ein automatischer Neustart ausgeführt.

ACHTUNG
Durch das Zurücksetzen aller Voreinstellungen auf die Werkseinstellungen gehen auch die IP-Adresse und die Passwörter verloren. Das Gerät ist danach nur über die serielle Schnittstelle, das Primary Setup Tool oder über DHCP ansprechbar. Bei entsprechendem Anschluss kann ein zuvor korrekt konfiguriertes Gerät kreisende Telegramme und damit den Ausfall des Datenverkehrs verursachen.

5.4.5 Load & Save

Übersicht der Dateitypen

Dateityp	Beschreibung
Config	Startkonfiguration
ConfigPack	Detaillierte Konfigurationsinformationen z. B. Startkonfiguration, Benutzer, Zertifikate
Copyright	OSS-Lizenzen
Debug	Diese Datei beinhaltet Informationen für den Siemens Support.
EDS	Electronic Data Sheet (EDS) elektronische Datenblätter zur Beschreibung von Geräten im EtherNet/IP-Betrieb
Firmware	Firmware
GSDML	Informationen über die Geräteeigenschaften
HTTPSCert	HTTPS-Zertifikat
LogFile	Datei mit Einträgen aus der Ereignisprotokolltabelle
MIB	Private MSPS MIB-Datei "scalance_x_xb200_msps.mib"
RunningCLI	Diese Datei enthält eine Übersicht der aktuellen Konfiguration in Form von CLI-Befehlen. Sie können die Textdatei herunterladen. Die Datei ist nicht dafür vorgesehen, dass Sie sie unverändert wieder hochladen.
Script	CLI-Skriptdatei
StartupInfo	Startup Logdatei
Users	Datei mit Benutzernamen und Passwörtern

5.4.5.1 HTTP

Laden und speichern von Daten über HTTP

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

Hinweis

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

Firmware

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

Hinweis

Inkompatibilität zu Firmware-Vorgängerversionen

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

Konfigurationsdateien

Hinweis

Konfigurationsdateien und Trial-Modus/Automatic Save-Modus

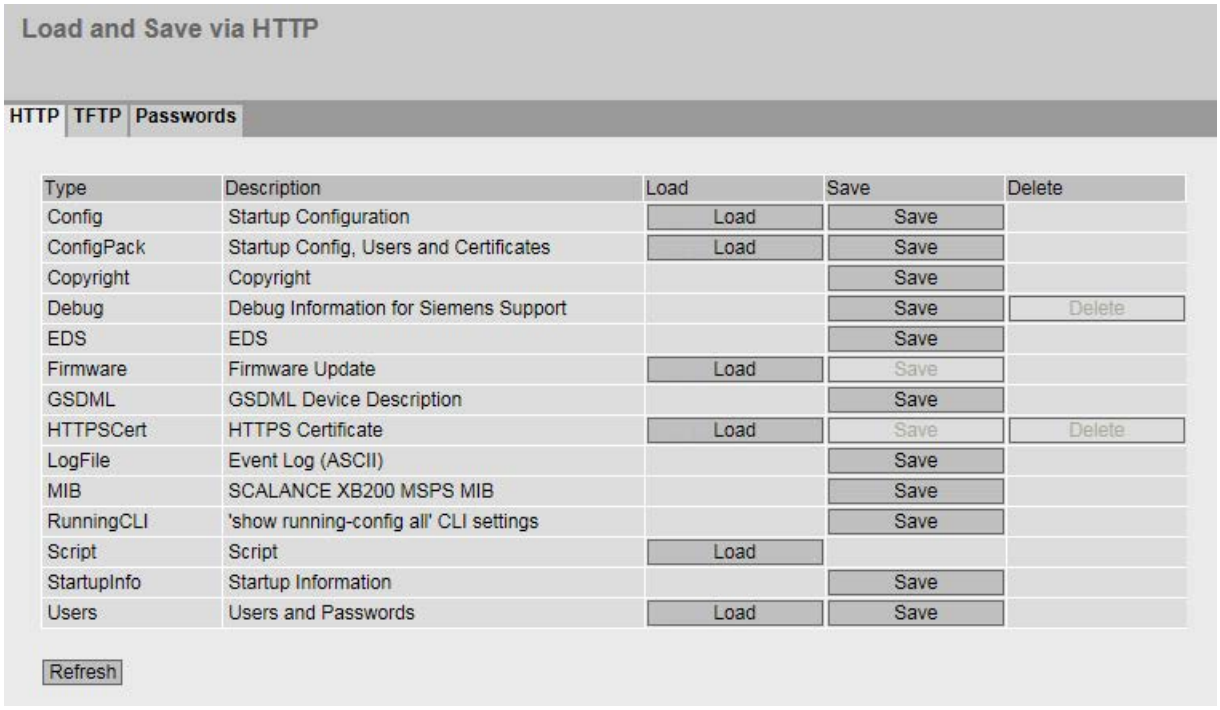
Im Automatic Save-Modus wird eine automatische Sicherung durchgeführt, bevor die Konfigurationsdateien (ConfigPack und Config) übertragen werden.
Im Trial-Modus werden Änderungen zwar übernommen aber nicht in den Konfigurationsdateien (ConfigPack und Config) gespeichert. Verwenden Sie die Schaltfläche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

CLI-Skriptdatei

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

Hinweis

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



Beschreibung der angezeigten Felder

Die Tabelle gliedert sich in folgende Spalten:

- **Type**
  Zeigt den Dateityp an.
- **Description**
  Zeigt die Kurzbeschreibung des Dateityps an.
- **Load**
  Mit dieser Schaltfläche können Sie Dateien auf das Gerät hochladen. Die Schaltfläche ist aktivierbar, wenn diese Funktion von dem Dateityp unterstützt wird.
- **Save**
  Mit dieser Schaltfläche können Sie Dateien vom Gerät herunterladen. Die Schaltfläche ist nur aktivierbar, wenn diese Funktion von dem Dateityp unterstützt wird und die Datei auf dem Gerät vorhanden ist.
- **Delete**
  Mit dieser Schaltfläche können Sie Dateien vom Gerät löschen. Die Schaltfläche ist nur aktivierbar, wenn diese Funktion von dem Dateityp unterstützt wird und die Datei auf dem Gerät vorhanden ist.

Hinweis

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

Vorgehensweise zur Konfiguration

Daten über HTTP hochladen

1. Starten Sie das Hochladen durch Anklicken einer der Schaltflächen "Load".

   Es öffnet sich ein Dialogfenster zum Hochladen einer Datei.

2. Wählen Sie die gewünschte Datei aus und bestätigen Sie das Hochladen.

   Die Datei wird hochgeladen.

3. Wenn ein Neustart notwendig ist, wird eine entsprechende Meldung ausgegeben. Klicken Sie auf die Schaltfläche "OK", um den Neustart durchzuführen. Wenn Sie auf die Schalfläche "Cancel" klicken, wird kein Neustart des Geräts durchgeführt. Erst nach einem Neustart werden die Änderungen wirksam.

Daten über HTTP herunterladen

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

   Die Datei wird heruntergeladen und gespeichert.

Daten über HTTP löschen

1. Starten Sie das Löschen durch Anklicken einer der Schaltflächen "Delete".

   Die Datei wird gelöscht.

Konfigurationsdaten wiederverwenden

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

Gehen Sie folgendermaßen vor, um Konfigurationsdaten wiederzuverwenden:

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

Hinweis

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

5.4.5.2 TFTP

Laden und speichern von Daten über einen TFTP-Server

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

Firmware

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

Hinweis

Inkompatibilität zu Firmware-Vorgängerversionen

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

Konfigurationsdateien

Hinweis

Konfigurationsdateien und Trial-Modus/Automatic Save-Modus

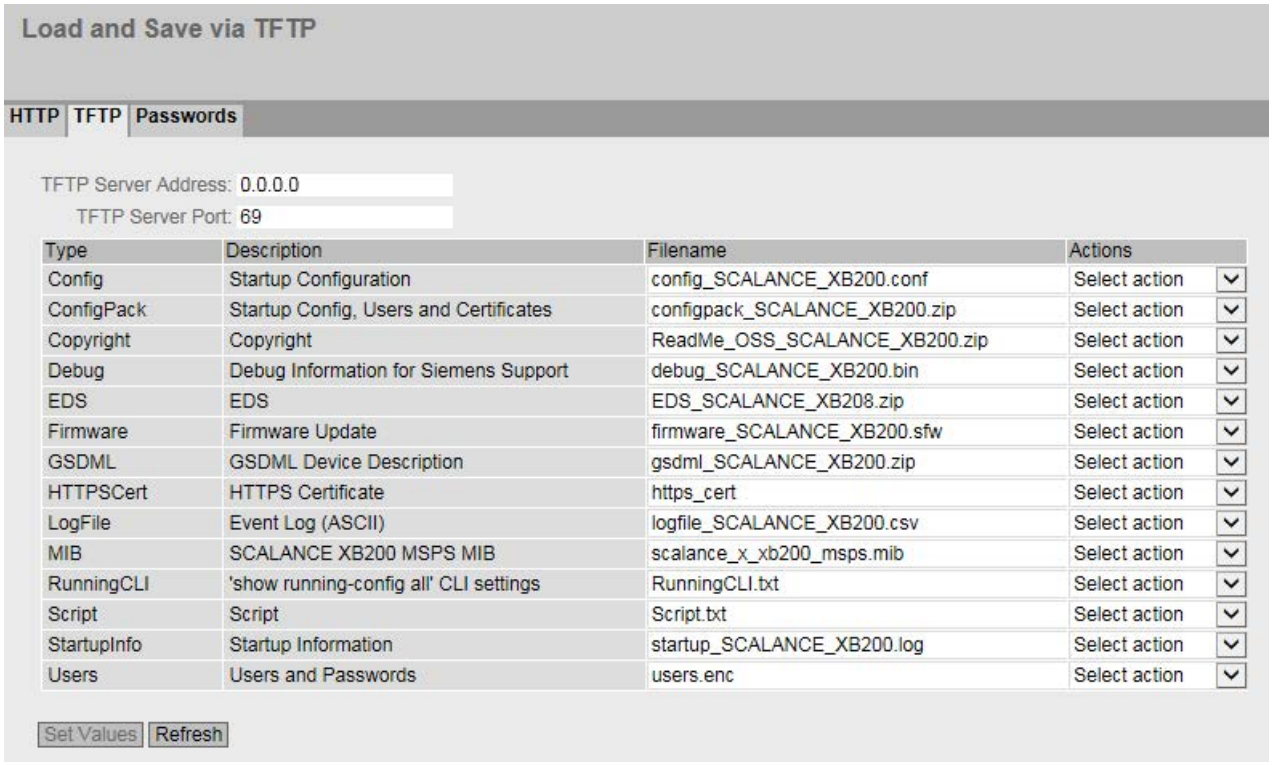
Im Automatic Save-Modus wird eine automatische Sicherung durchgeführt, bevor die Konfigurationsdateien (ConfigPack und Config) übertragen werden.
Im Trial-Modus werden Änderungen zwar übernommen aber nicht in den Konfigurationsdateien (ConfigPack und Config) gespeichert. Verwenden Sie die Schaltfläche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

CLI-Skriptdatei

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

Hinweis

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



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

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

Die Tabelle gliedert sich in folgende Spalten:

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

Hinweis

Änderung des Dateinamens

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

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

Vorgehensweise zur Konfiguration

Daten über TFTP laden bzw. speichern

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

Konfigurationsdaten wiederverwenden

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

Gehen Sie folgendermaßen vor, um Konfigurationsdaten wiederzuverwenden:

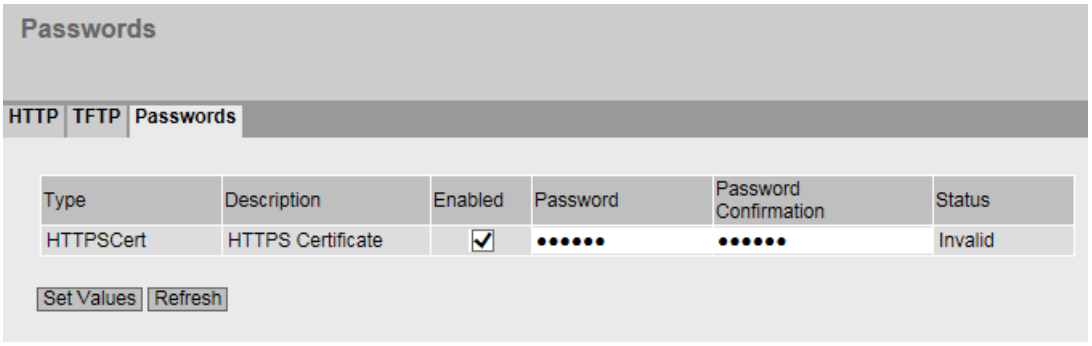
1. Speichern Sie die Konfigurationsdaten eines konfigurierten Gerätes auf Ihrem PC.
2. Laden Sie diese Konfigurationsdateien auf alle weiteren Geräte, die Sie so konfigurieren wollen.
3. Falls für einzelne Geräte individuelle Einstellungen erforderlich sind, müssen Sie diese online am betreffenden Gerät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

Hinweis

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

5.4.5.3 Passwords

Es gibt Dateien, deren Zugriff passwortgeschützt ist. Um die Datei erfolgreich ins Gerät zu laden, geben Sie auf der WBM-Seite das für die Datei festgelegte Passwort ein.



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Type**
  Zeigt den Dateityp an.
- **Description**
  Zeigt die Kurzbeschreibung des Dateityps an.
- **Enabled**
  Wenn aktiviert, wird das Passwort verwendet. Nur aktivierbar, wenn das Passwort konfiguriert ist.
- **Password**
  Geben Sie das Passwort für die Datei ein.
- **Password Confirmation**
  Bestätigen Sie das Passwort.
- **Status**
  Zeigt an, ob die aktuellen Einstellungen zur Datei auf dem Gerät passen.
  - valid
    Das Optionskästchen "Enabled" ist aktiviert und das Passwort passt zu dem Zertifikat.
  - invalid
    Das Optionskästchen "Enabled" ist aktiviert, aber das Passwort passt nicht zu dem Zertifikat oder es ist noch kein Zertifikat geladen.
  - '-'
    Das Passwort kann nicht ausgewertet werden oder wird noch nicht verwendet. Das Optionskästchen "Enabled" ist nicht aktiviert.

Vorgehensweise

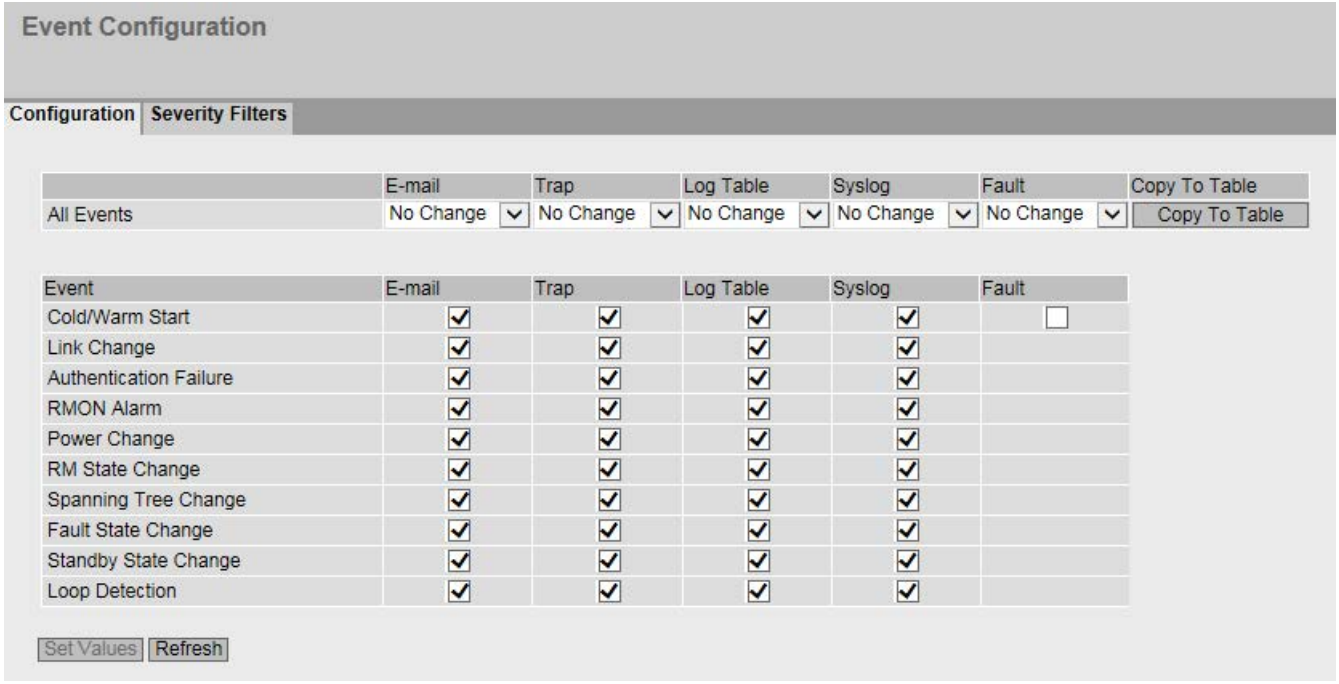
1. Tragen Sie bei "Password" das Passwort ein.
2. Um das Passwort zu bestätigen, tragen Sie bei "Password Confirmation" das Passwort nochmals ein.
3. Aktivieren Sie die Option "Enabled".
4. Klicken Sie auf die Schaltfläche "Set Values".

5.4.6 Events

5.4.6.1 Configuration

Systemereignisse auswählen

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



Beschreibung der angezeigten Felder

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

- **Event**

  Zeigt an, dass die Einstellungen für alle Ereignisse der Tabelle 2 gültig sind.

- **E-mail / Trap / Log Table / Syslog / Fault**

  Aktivieren oder deaktivieren Sie die gewünschte Art der Benachrichtigung für alle Ereignisse. Wenn "No Change" ausgewählt ist, bleiben die Einträge der entsprechenden Spalte in der Tabelle 2 unverändert.

- **Copy to Table**

  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ereignisse der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Event**
  Die Spalte enthält folgende Werte:
  - Cold/Warm Start
    Das Gerät wurde eingeschaltet oder vom Anwender neu gestartet.
  - Link Change
    Dieses Ereignis tritt nur auf, wenn der Port-Status überwacht wird und sich entsprechend geändert hat, siehe "System > Fault Monitoring > Link Change".
  - Authentication Failure
    Dieses Ereignis tritt beim Versuch eines Zugriffs mit fehlerhaftem Passwort auf.
  - RMON Alarm
    Ein Alarm oder ein Ereignis ist im Zusammenhang mit der Fernüberwachung des Systems aufgetreten.
  - Power Change
    Dieses Ereignis tritt nur auf, wenn die Spannungsversorgungsleitungen 1 und 2 überwacht werden. Es zeigt an, dass ein Wechsel auf Leitung 1 bzw. auf Leitung 2 stattgefunden hat. Siehe "System > Fault Monitoring > Power Supply".
  - RM State Change
    Der Redundanzmanager hat eine Unterbrechung oder Wiederherstellung des Rings erkannt und hat die Strecke um- bzw. zurückgeschaltet.
  - Spanning Tree Change
    Die STP- bzw. RSTP-Topologie hat sich geändert.
  - Fault State Change
    Der Fehlerstatus hat sich geändert. Der Fehlerstatus kann sich auf die aktivierte Portüberwachung oder die Spannungsüberwachung beziehen.
  - 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.
  - Loop Detection

    Es wurde eine Schleife im Netzsegment erkannt.
- **E-mail**
  Das Gerät sendet eine E-Mail. Voraussetzung ist, dass der SMTP-Server eingerichtet und die Funktion "SMTP Client" aktiviert ist.
- **Trap**
  Das Gerät löst einen SNMP-Trap aus. Voraussetzung ist, dass unter "System > Configuration" "SNMPv1 Traps" aktiviert ist.
- **Log Table**
  Das Gerät schreibt einen Eintrag in die Ereignisprotokoll-Tabelle, siehe "Information > Log Table"

- **Syslog**
  Das Gerät schreibt einen Eintrag auf den Systemprotokoll-Server. Voraussetzung ist, dass der Systemprotokoll-Server eingerichtet und die Funktion "Syslog Client" aktiviert ist.
- **Fault**
  Das Gerät löst einen Fehler aus. Die Fehler-LED leuchtet auf

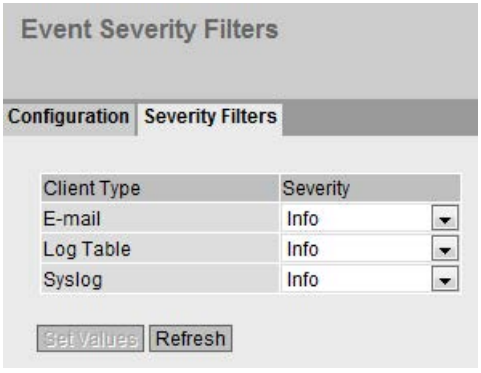
Vorgehensweise zur Konfiguration

1. Aktivieren Sie das Optionskästchen in der Zeile des gewünschten Ereignisses. Wählen Sie dabei das Ereignis in der Spalte unter den folgenden Aktionen aus:
   - E-mail
   - Trap
   - Log Table
   - Syslog
   - Fault
2. Klicken Sie auf die Schaltfläche "Set Values".

5.4.6.2 Severity Filters

Einstellung der Severity Filter

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



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

- **E-Mail**

  Versand von Systemereignismeldungen per E-Mail

- **Log Table**

  Eintragen von Systemereignissen in die Log-Tabelle

- **Syslog**

  Eintragen von Systemereignissen in die Syslog-Datei

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

Sie haben folgende Werte zur Auswahl:

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

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

Vorgehensweise

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

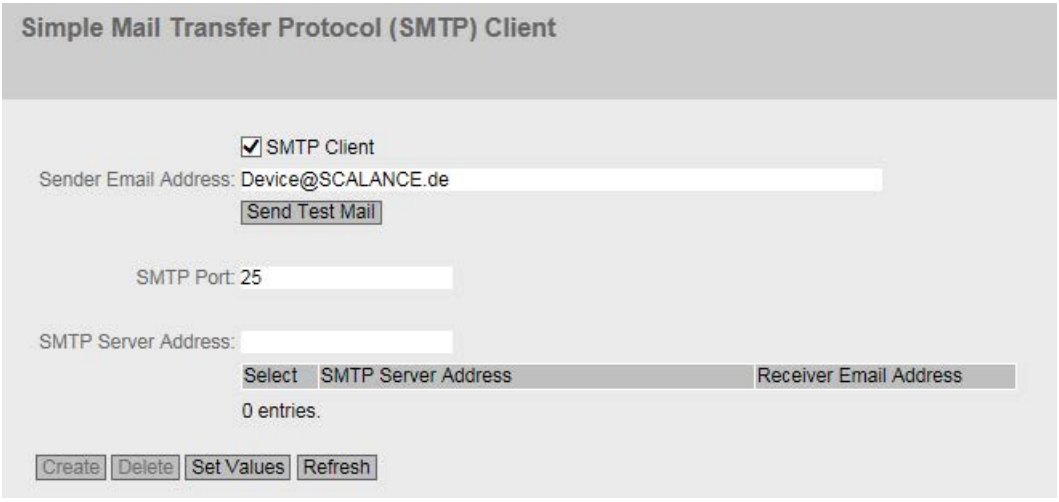
1. Wählen Sie aus den Klapplisten in der zweiten Tabellenspalte hinter den Client-Typen die gewünschten Werte aus.
2. Klicken Sie auf die Schaltfläche "Set Values".

5.4.7 SMTP Client

Netzüberwachung durch E-Mails

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

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



Beschreibung

Die Seite enthält folgende Felder:

- **SMTP Client**
  Aktivieren oder deaktivieren Sie den SMTP-Client.
- **Sender Email Address**
  Geben Sie die E-Mail-Adresse ein, die in der E-Mail angegeben werden soll.

  Diese Einstellung gilt für alle konfigurierten SMTP-Server.
- **Send Test Mail**

  Verschicken Sie eine Test-E-Mail, um Ihre Konfiguration zu prüfen.

- **SMTP Port**

  Geben Sie den Port ein, über den Ihr SMTP-Server erreichbar ist.

  Werkseinstellung: 25

  Diese Einstellung gilt für alle konfigurierten SMTP-Server.

- **SMTP Server Address**
  Geben Sie die IP-Adresse des SMTP-Servers ein.

Die Tabelle enthält folgende Spalten:

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

Vorgehensweise

1. Aktivieren Sie die Option "SMTP Client".
2. Geben Sie in das Eingabefeld "SMTP Server Address" die IP-Adresse des SMTP-Servers ein.
3. Klicken Sie auf die Schaltfläche "Create". In der Tabelle wird ein neuer Eintrag erzeugt.
4. Geben Sie in das Eingabefeld "Receiver Email Address" die E-Mail-Adresse ein, an die das Gerät im Fehlerfall eine E-Mail senden soll.
5. Klicken Sie auf die Schaltfläche "Set Values".

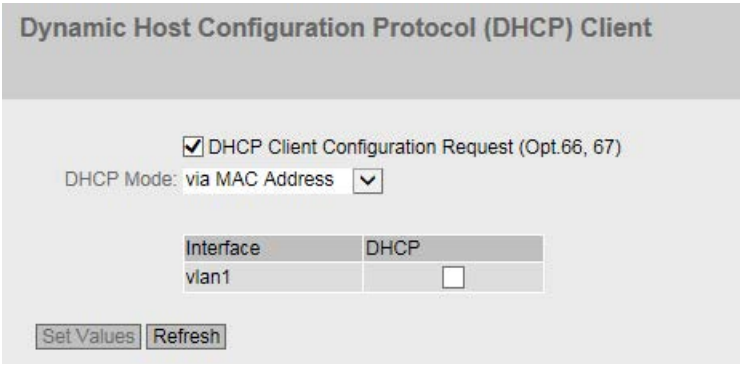
Hinweis

Je nach Eigenschaften und Konfiguration des SMTP-Servers kann es notwendig sein, das Eingabefeld "Sender Email Address" anzupassen. Informieren Sie sich beim Administrator des SMTP-Servers.

5.4.8 DHCP Client

Einstellung der DHCP-Betriebsart

Wenn die DHCP-Betriebsart aktiviert ist, startet der DHCP-Client bei einem konfigurierten DHCP-Server eine DHCP-Anfrage und erhält als Antwort eine IPv4-Adresse zugewiesen. Der Server verwaltet einen Adressbereich, aus welchem er IPv4-Adressen vergibt. Es ist auch möglich den Server so zu konfigurieren, dass der Client auf seine Anfrage immer dieselbe IPv4-Adresse zugewiesen bekommt.



Beschreibung

Die Seite enthält folgende Felder:

- **Optionskästchen "DHCP Client Configuration Request (Opt.66, 67)"**
  Aktivieren Sie diese Option, wenn der DHCP-Client die Optionen 66, und 67 dazu verwenden soll, eine Konfigurationsdatei (Config oder ConfigPack) herunterzuladen und diese dann zu aktivieren.
- **Klappliste "DHCP Mode"**
  Wählen Sie aus der Klappliste die DHCP-Betriebsart. Folgende Betriebsarten sind möglich:
  - via MAC Address
    Die Identifikation läuft über die MAC-Adresse ab.
  - via DHCP Client ID
    Die Identifikation läuft über eine frei definierte DHCP-Client-ID ab.
  - via System Name
    Die Identifikation läuft über den Systemnamen ab. Ist der Systemname 255 Zeichen lang, dann wird das letzte Zeichen nicht zur Identifikation benutzt.

Die Tabelle gliedert sich in folgende Spalten:

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

Vorgehensweise

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

1. Aktivieren Sie die Option "DHCP Client".
2. Wählen Sie aus der Klappliste "DHCP Mode" die DHCP-Betriebsart "via DHCP Client ID".
3. Geben Sie in das aktivierte Eingabefeld "DHCP Client ID" eine Zeichenkette zur Identifikation des Gerätes ein. Diese wird dann vom DHCP-Server ausgewertet.
4. Wählen Sie die Option "Client Configuration Request (Opt.66, 67)", wenn der DHCP-Client die Optionen 66 und 67 dazu verwenden soll, eine Konfigurationsdatei herunterzuladen und diese dann zu aktivieren.
5. Klicken Sie auf die Schaltfläche "Set Values".

Hinweis

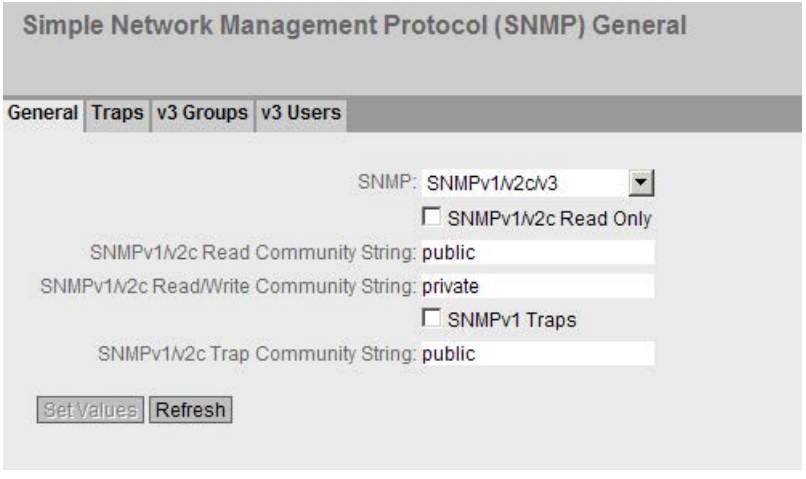
Wird eine Konfigurationsdatei heruntergeladen, so löst dies einen Neustart des Systems aus. Achten Sie darauf, dass in dieser Konfigurationsdatei die Option "Client Configuration Request (Opt.66, 67)" nicht mehr gesetzt ist.

5.4.9 SNMP

5.4.9.1 General

Konfiguration von SNMP

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



Beschreibung

Die Seite enthält folgende Felder:

- **Klappliste "SNMPv1/v2c/v3"**
  Wählen Sie aus der Klappliste das SNMP-Protokoll. Folgende Einstellungen sind möglich:
  - "-" (Deaktiviert)
    SNMP deaktiviert.
  - SNMPv1/v2c/v3
    SNMPv1/v2c/v3 wird unterstützt.
  - SNMPv3
    Nur SNMPv3 wird unterstützt.
- **Optionskästchen "SNMPv1/v2c Read Only"**
  Wenn Sie diese Option aktivieren, kann SNMPv1/v2c nur lesend auf die SNMP-Variablen zugreifen.

  Hinweis
  Community String

  Verwenden Sie aus Sicherheitsgründen nicht die Standardwerte "public" oder "private". Ändern Sie die Community Strings nach der Erst-Installation.
- **Eingabefeld "SNMPv1/v2c Read Community String"**
  Tragen Sie den Community String für den lesenden Zugriff des SNMP-Protokolls ein.
- **Eingabefeld "SNMPv1/v2c Read/Write Community String"**
  Tragen Sie den Community String für den lesenden und schreibenden Zugriff des SNMP-Protokolls ein.
- **Optionskästchen "SNMPv1 Traps"**
  Aktivieren oder deaktivieren Sie das Senden von SNMP-Traps (Alarmtelegramme). Auf dem Register "Trap" legen Sie die IP-Adressen der Geräte fest, an die SNMP Traps gesendet werden.
- **Eingabefeld "SNMPv1/v2c Trap Community String"**
  Tragen Sie den Community String für das Senden von SNMPv1/v2-Meldungen ein.

Vorgehensweise

1. Wählen Sie aus der Klappliste "SNMP" die gewünschte Option:
   - "-" (Deaktiviert)
   - SNMPv1/v2c/v3
   - SNMPv3
2. Aktivieren Sie das Optionskästchen "SNMPv1/v2c Read only", wenn Sie mit SNMPv1/v2c nur lesend auf SNMP-Variablen zugreifen wollen.
3. Tragen Sie im Eingabefeld "SNMPv1/v2c Read Community String" die gewünschte Zeichenkette ein.

4. Tragen Sie in das Eingabefeld "SNMPv1/v2c Read/Write Community String" die gewünschte Zeichenkette ein.
5. Klicken Sie auf die Schaltfläche "Set Values".

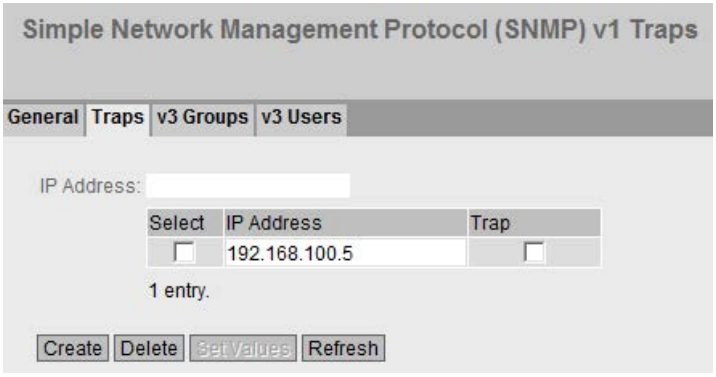
5.4.9.2 Traps

SNMP-Traps bei Alarmereignissen

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

Hinweis

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



Beschreibung

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

Die Tabelle gliedert sich in folgende Spalten:

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

Vorgehensweise

Trap-Eintrag erstellen

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

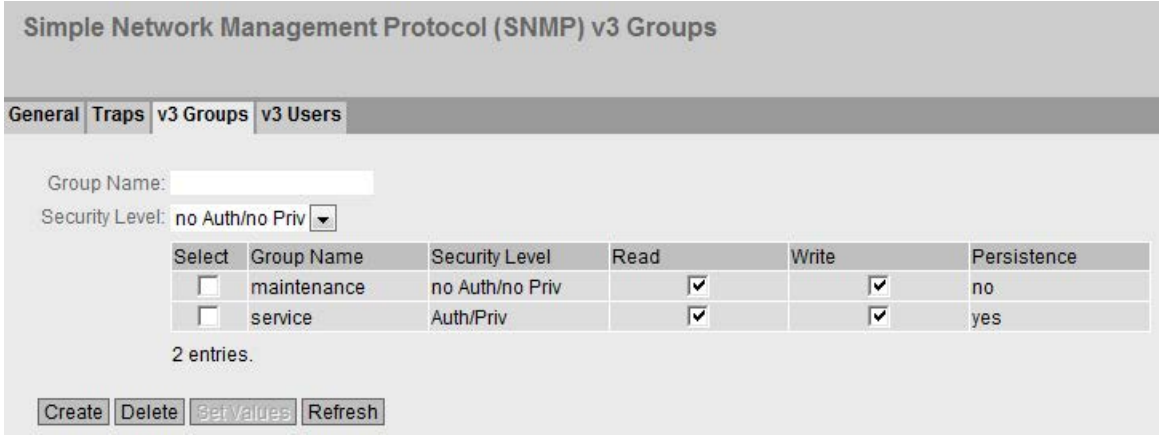
Trap-Eintrag löschen

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

5.4.9.3 Groups

Sicherheitseinstellungen und Rechtevergabe

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



Beschreibung

Die Seite enthält folgende Felder:

- **Group Name**
  Tragen Sie den Namen der Gruppe ein. Die maximale Länge beträgt 32 Zeichen.
- **Security Level**
  Wählen Sie die Sicherheitsstufe (Authentifizierung, Verschlüsselung) aus, die für die gewählte

  Gruppe gültig ist. Bei den Sicherheitsstufen die folgenden Möglichkeiten:

  – No Auth/no Priv
  Keine Authentifizierung aktiviert / keine Verschlüsselung aktiviert.

  – Auth/no Priv
  Authentifizierung aktiviert / keine Verschlüsselung aktiviert.

  – Auth/Priv
  Authentifizierung aktiviert / Verschlüsselung aktiviert.

Die Tabelle gliedert sich in folgende Spalten:

- **Select**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Group Name**
  Zeigt die definierten Gruppennamen an.
- **Security Level**
  Zeigt die konfigurierte Sicherheitsstufe an.
- **Read**
  Aktivieren oder deaktivieren Sie den Lesezugriff für die gewünschte Gruppe.
- **Write**
  Aktivieren oder deaktivieren Sie den Schreibzugriff für die gewünschte Gruppe.

  Hinweis

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

- **Persistence**
  Zeigt an, ob die Gruppe einem SNMPv3-Benutzer zugeordnet ist. Wenn die Gruppe keinem SNMPv3-Benutzer zugeordnet ist, wird kein automatisches Speichern ausgelöst und die konfigurierte Gruppe ist nach einem Neustart des Gerätes wieder verschwunden.

  – Yes

  Die Gruppe ist einem SNMPv3-Benutzer zugeordnet.

  – No

  Die Gruppe ist keinem SNMPv3-Benutzer zugeordnet.

Vorgehensweise

Anlegen einer neuen Gruppe

1. Geben Sie bei "Group Name" den gewünschten Gruppennamen ein.
2. Wählen Sie aus der Klappliste "Security Level" die gewünschte Sicherheitsstufe aus.
3. Klicken Sie auf die Schaltfläche "Create", um einen neuen Eintrag zu erzeugen.
4. Legen Sie bei "Read" die gewünschten Leserechte für die Gruppe fest.
5. Legen Sie bei "Write" die gewünschten Schreibrechte für die Gruppe fest.
6. Klicken Sie auf die Schaltfläche "Set Values".

Ändern einer Gruppe

1. Legen Sie bei "Read" die gewünschten Leserechte für die Gruppe fest.
2. Legen Sie bei "Write" die gewünschten Schreibrechte für die Gruppe fest.
3. Klicken Sie auf die Schaltfläche "Set Values".

Hinweis

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

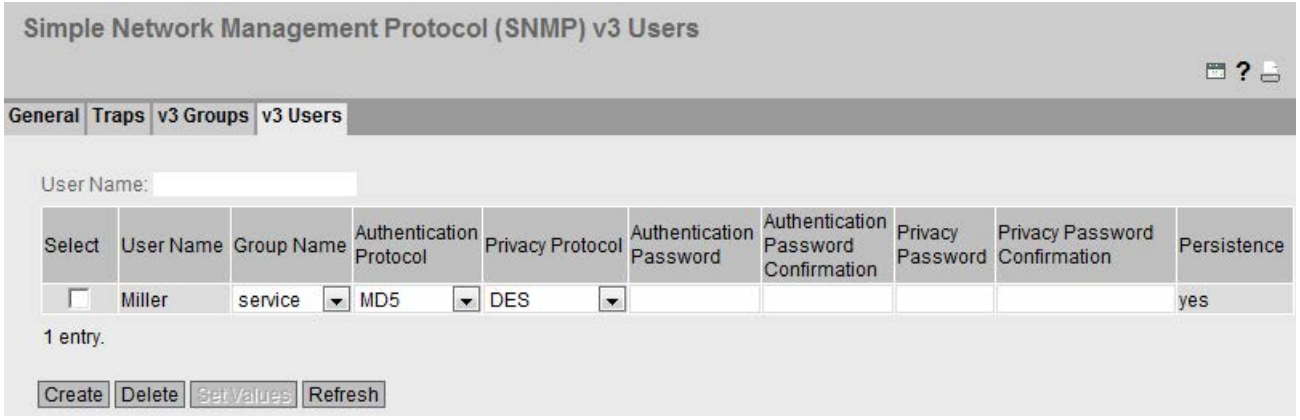
Löschen einer Gruppe

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

5.4.9.4 Users

Benutzerspezifische Sicherheitseinstellungen

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



Beschreibung

Die Seite enthält folgende Felder:

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

Die Tabelle gliedert sich in folgende Spalten:

- **Select**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **User Name**
  Zeigt die angelegten Benutzer an.
- **Group Name**
  Wählen Sie die Gruppe aus, die dem Benutzer zugeordnet wird.
- **Authentication Protocol**
  Legen Sie das Authentifizierungsprotokoll fest. Nur aktvierbar, wenn die Gruppe die Funktion unterstützt.

  Folgende Einstellungen gibt es:

  – none
  – MD5
  – SHA

- **Privacy Protocol**
  Legen Sie fest, ob der Benutzer den DES-Algorithmus verwendet. Nur aktivierbar, wenn die Gruppe diese Funktion unterstützt.
- **Authentication Password**
  Geben Sie in das erste Eingabefeld das Authentifizierungspasswort ein. Das Passwort muss mindestens 6 Zeichen lang sein, die maximale Länge beträgt 32 Zeichen.
- **Authentication Password Confirmation**
  Bestätigen Sie das Passwort durch die Wiederholung der Eingabe.
- **Privacy Password**
  Geben Sie Ihr Verschlüsselungspasswort ein. Das Passwort muss mindestens 6 Zeichen lang sein, die maximale Länge beträgt 32 Zeichen.
- **Privacy Password Confirmation**
  Bestätigen Sie das Verschlüsselungspasswort durch die Wiederholung der Eingabe.
- **Persistence**
  Zeigt an, ob der User einer SNMPv3-Gruppe zugeordnet ist. Wenn der User keiner SNMPv3-Gruppe zugeordnet ist, wird kein automatisches Speichern ausgelöst und der konfigurierte User ist nach einem Neustart des Gerätes wieder verschwunden.
  - Yes

    Der User ist einer SNMPv3-Gruppe zugeordnet.
  - No

    Der User ist keiner SNMPv3-Gruppe zugeordnet.

Vorgehensweise

Neuen Benutzer anlegen

1. Geben Sie im Eingabefeld "User Name" den Namen des neuen Benutzers ein.
2. Klicken Sie auf die Schaltfläche "Create". In der Tabelle wird ein neuer Eintrag erzeugt.
3. Wählen Sie bei "Groups" die Gruppe aus, der der neue Benutzer angehören soll.

   Wenn die Gruppe noch nicht angelegt ist, wechseln Sie auf die Seite "v3 Groups" und legen Sie die Einstellungen für diese Gruppe fest.
4. Wenn für die ausgewählte Gruppe eine Authentifizierung notwendig ist, wählen Sie bei "Authentification Protocol" den Authentifizierungsalgorithmus.
   Tragen Sie in die entsprechenden Eingabefelder das Authentifizierungspasswort sowie dessen Bestätigung ein.
5. Wenn für die Gruppe eine Verschlüsselung festgelegt wurde, wählen Sie bei "Privacy Protocol" den Algorithmus aus. Tragen Sie in die entsprechenden Eingabefelder das Verschlüsselungspasswort sowie dessen Bestätigung ein.
6. Klicken Sie auf die Schaltfläche "Set Values".

Benutzer löschen

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

Hinweis

Wenn Sie vor diesem Schritt eine andere Schaltfläche z. B. die Schaltfläche "Refresh" anklicken, wird der Löschvorgang abgebrochen. Die Daten der markierten Zeilen bleiben erhalten. Die Markierungen werden entfernt. Wenn Sie den Vorgang wiederholen wollen, dann müssen Sie die zu löschenden Datensätze neu markieren.

5.4.10 System Time

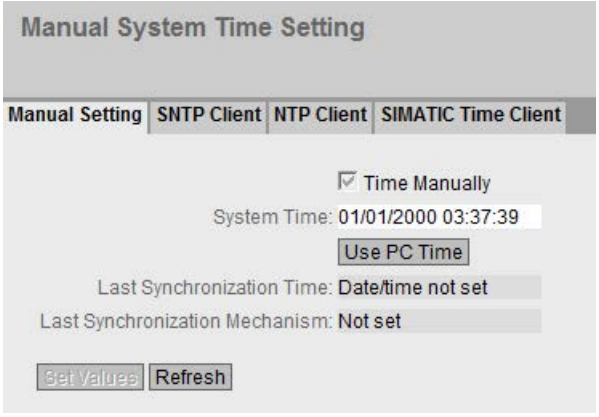
Um die Systemzeit des Geräts einzustellen, gibt es unterschiedliche Methoden. Es kann immer nur eine Methode aktiv sein.

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

5.4.10.1 Manual Setting

Manuelle Einstellung der Systemzeit

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



Beschreibung

Die Seite enthält folgende Felder:

- **Time Manually**
  Aktivieren oder deaktivieren Sie die manuelle Zeiteinstellung. Wenn Sie die Option aktivieren, wird das Eingabefeld "System Time" editierbar.
- **System Time**
  Geben Sie Datum und Uhrzeit im Format "MM/DD/YYYY HH:MM:SS" ein.

  Nach dem Neustart beginnt die Uhrzeit mit 01/01/2000 00:00:00
- **Use PC Time**
  Klicken Sie auf die Schaltfläche, um die Zeiteinstellung des PCs zu übernehmen.
- **Last Synchronization Time**
  Dieses Feld ist nur lesbar und zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat. Wenn keine Uhrzeitsynchronisation möglich war, enthält das Feld die Angabe "Date/time not set".
- **Last Synchronization Mechanism**
  Dieses Feld zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde.
  - Not set
    Die Zeit wurde nicht eingestellt.
  - Manual
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm

Vorgehensweise

1. Aktivieren Sie die Option "Time Manually".
2. Klicken Sie in das Eingabefeld "System Time".
3. Geben Sie im Eingabefeld "System Time" Datum und Uhrzeit im Format " MM/DD/YYYY HH:MM:SS" ein.
4. Klicken Sie auf die Schaltfläche "Set Values".
   Datum und Uhrzeit werden übernommen und im Feld "Last Synchronization Mechanism" wird "Manual" eingetragen.

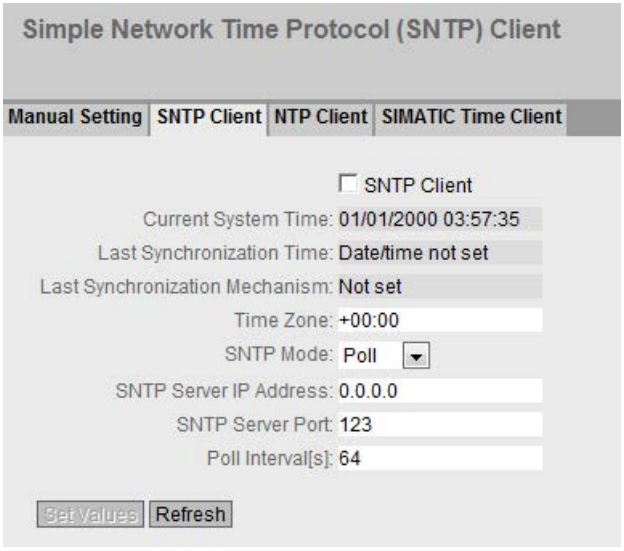
5.4.10.2 SNTP Client

Uhrzeitsynchronisation im Netzwerk

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

Hinweis

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



Beschreibung

Die Seite enthält folgende Felder:

- **SNTP Client**
  Aktivieren oder deaktivieren Sie die automatische Zeitsynchronisation über SNTP.
- **Current System Time**
  Zeigt das aktuelle Datum und die aktuelle Normalzeit an, die vom IE-Switch empfangen wurden. Wenn Sie eine Zeitzone angeben, wird die Zeitangabe entsprechend angepasst.
- **Last Synchronization Time**
  Dieses Feld ist nur lesbar und zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.

- **Last Synchronization Mechanism**
  Dieses Feld zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde. Folgende Arten gibt es:
  - Not set
    Die Zeit wurde nicht eingestellt.
  - Manual
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm
- **Time Zone**
  Geben Sie die verwendete Zeitzone im Format "+/- HH:MM" an. Die Zeitzone bezieht sich auf UTC Standard-Weltzeit.
- **SNTP Mode**
  Wählen Sie aus der Klappliste die Synchronisationsart aus. Folgende Synchronisierungsarten sind möglich:
  - Poll
    Wenn Sie diese Protokollart wählen, werden die Eingabefelder "SNTP Server IP Address", "SNTP Server Port" und "Poll Interval(s)" zur weiteren Konfiguration eingeblendet. Bei dieser Synchronisationsart ist das Gerät aktiv und sendet eine Zeitabfrage an den SNTP-Server.
  - Listen
    Bei dieser Synchronisationsart ist das Gerät passiv und "hört" auf SNTP-Telegramme, die die Uhrzeit liefern.
- **SNTP Server IP Address**
  Geben Sie die IP-Adresse des SNTP-Servers ein.
- **SNTP Server Port**
  Geben Sie den Port des SNTP-Servers ein.
  Folgende Ports sind möglich:
  - 123 (Standard-Port)
  - 1025 bis 36564
- **Poll Interval(s)**
  Geben Sie den Zeitabstand zwischen zwei Zeitanfragen ein. In diesem Feld geben Sie das Abfrageintervall in Sekunden an. Mögliche Werte sind 16 bis 16284 Sekunden.

Vorgehensweise

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

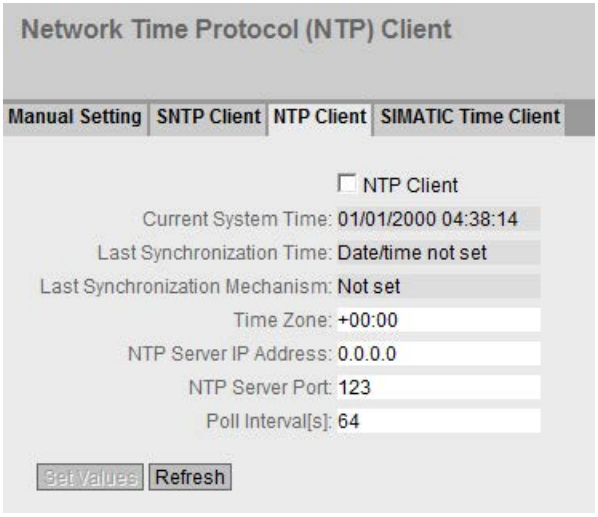
5.4.10.3 NTP Client

Automatische Zeiteinstellung über NTP

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

Hinweis

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



Beschreibung

Die Seite enthält folgende Felder:

- **NTP Client**
  Markieren Sie dieses Optionskästchen, um die automatische Zeitsynchronisation über NTP zu aktivieren.
- **Current System Time**
  Zeigt das aktuelle Datum und die aktuelle Normalzeit an, die vom IE-Switch empfangen wurden. Wenn Sie eine Zeitzone angeben, wird die Zeitangabe entsprechend angepasst.
- **Last Synchronization Time**
  Dieses Feld ist nur lesbar und zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.

- **Last Synchronization Mechanism**
  Dieses Feld zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde. Folgende Arten gibt es:
  - Not set
    Die Zeit wurde nicht eingestellt.
  - Manual
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm
- **Time Zone**
  Geben Sie in diesem Feld Ihre verwendete Zeitzone im Format "+/- HH:MM" an. Die Zeitzone bezieht sich auf UTC Standard-Weltzeit.
- **NTP Server IP Address**
  Geben Sie die IP-Adresse des NTP-Servers an.
- **NTP Server Port**
  Geben Sie den Port des NTP-Servers an.
  Folgende Ports sind möglich:
  - 123 (Standard-Port)
  - 1025 bis 36564
- **Poll Interval(s)**
  Tragen Sie hier den Zeitabstand zwischen zwei Zeitanfragen ein. In diesem Feld geben Sie das Abfrageintervall in Sekunden an. Mögliche Werte sind 64 bis 1024 Sekunden.

Vorgehensweise

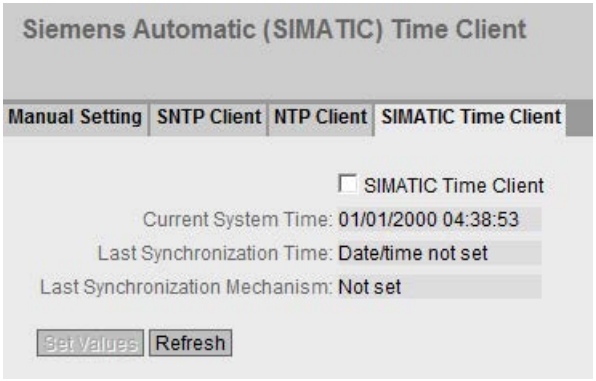
1. Klicken Sie in das Optionskästchen "NTP Client", um die automatische Zeiteinstellung über NTP zu aktivieren.
2. Tragen Sie die erforderlichen Werte in die folgenden Felder ein:
   - Zeitzone
   - NTP-Server IP-Adresse
   - NTP-Server Port
   - Abfrageintervall
3. Klicken Sie auf die Schaltfläche "Set Values".

5.4.10.4 SIMATIC Time Client

Zeiteinstellung über SIMATIC Time Client

Hinweis

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



Beschreibung

Die Seite enthält folgende Felder:

- **SIMATIC Time Client**
  Markieren Sie dieses Optionskästchen, um das Gerät als SIMATIC Time Client zu aktivieren.
- **Current System Time**
  Dieses Feld zeigt die aktuelle Systemzeit an.

- **Last Synchronization Time**
  Dieses Feld ist nur lesbar und zeigt an, wann die letzte Uhrzeitsynchronisation stattgefunden hat.
- **Last Synchronization Mechanism**
  Dieses Feld zeigt an, wie die letzte Zeitsynchronisation durchgeführt wurde. Folgende Arten gibt es:
  - Not set
    Die Zeit wurde nicht eingestellt.
  - Manual
    Manuelle Zeiteinstellung
  - SNTP
    Automatische Zeitsynchronisation über SNTP
  - NTP
    Automatische Zeitsynchronisation über NTP
  - SIMATIC
    Automatische Zeitsynchronisation über SIMATIC-Uhrzeittelegramm

Vorgehensweise

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

5.4.11 Auto Logout

Einstellung der automatischen Abmeldung

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

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

Konfiguration

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

5.4.12 Button

Beschreibung des RESET-Tasters

Der Taster "RESET" dient zum Zurücksetzen auf werkseitige Voreinstellungen.

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

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

Beschreibung der angezeigten Felder

Folgende Funktionalitäten sind möglich:

- **Optionskästchen "Restore Factory Defaults"**
  Aktivieren oder deaktivieren Sie die Funktion "Restore Factory Defaults" am Taster "RESET".

⚠ VORSICHT
Tasterfunktion "Restore Factory Defaults" beim Hochlauf aktiv Wenn Sie diese Funktion in ihrer Projektierung deaktiviert haben, ist die Deaktivierung nur im laufenden Betrieb gültig. Bei einem Hochlauf, z.B. nach "Stromaus", ist die Funktion bis zum Laden der Projektierung aktiv und das Gerät kann so auch unbeabsichtigt auf die Werkseinstellungen zurückgesetzt werden. Dies kann zu unerwünschten Störungen des Netzwerkbetriebs führen, da das Gerät nach diesem Vorfall erst neu projektiert werden muss.

Vorgehensweise zur Konfiguration

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

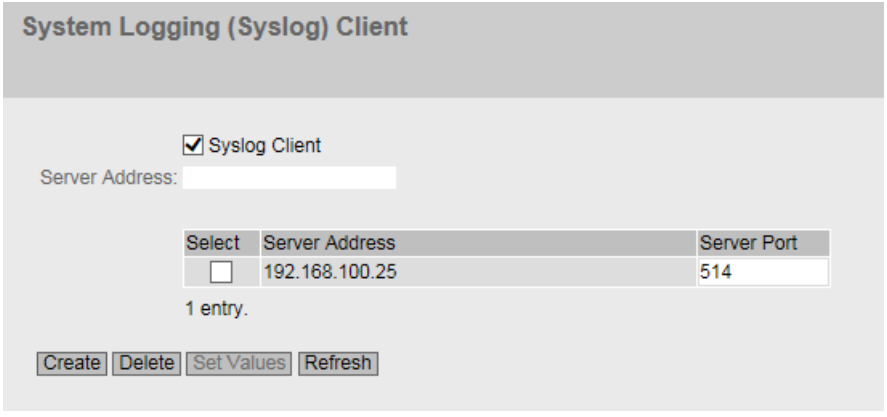
5.4.13 Syslog Client

Systemereignis-Agent

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

Voraussetzungen für das Versenden der Protokolleinträge:

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



Beschreibung

Die Seite enthält folgende Felder:

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

Die Tabelle enthält folgende Spalten

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

Vorgehensweise

Funktion aktivieren

1. Aktivieren Sie das Optionskästchen "Syslog Client".
2. Klicken Sie auf die Schaltfläche "Set Values".

Neuen Eintrag anlegen

1. Geben Sie in das Eingabefeld "Server Address" die IP-Adresse des Syslog-Servers ein, auf dem die Protokolleinträge gespeichert werden sollen.
2. Klicken Sie auf die Schaltfläche "Create". In der Tabelle wird eine neue Zeile eingefügt.
3. Geben Sie in das Eingabefeld "Server Port" die Nummer des UDP-Ports des Servers ein.
4. Klicken Sie auf die Schaltfläche "Set Values".

Hinweis

Die Standardeinstellung des Server Ports ist Port 514.

Eintrag ändern

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

Eintrag löschen

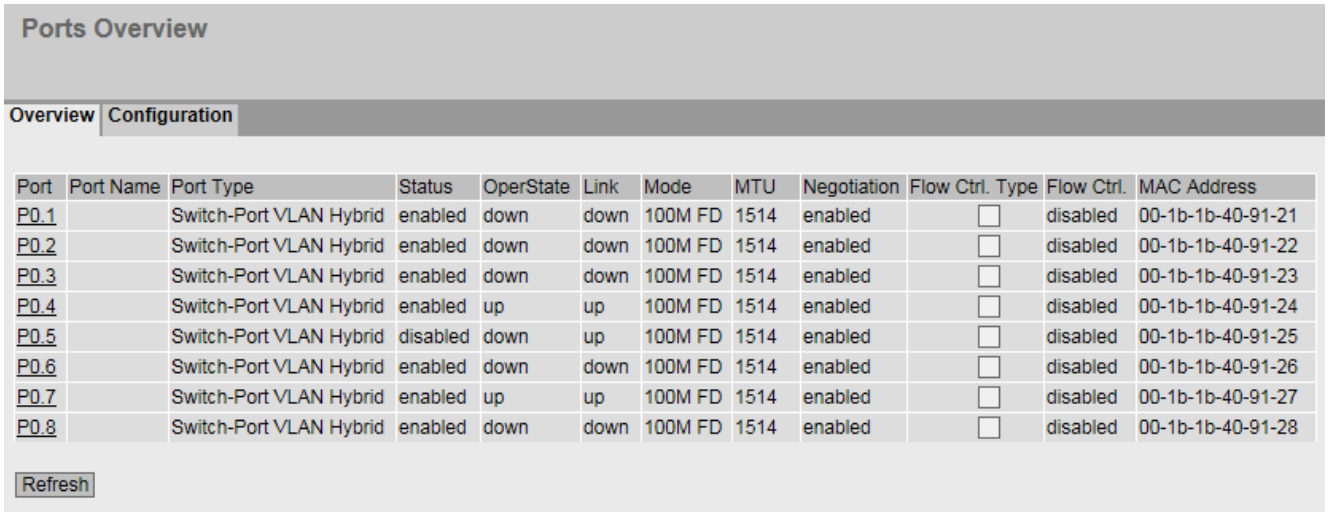
1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Delete". Alle markierten Einträge werden gelöscht und die Anzeige wird aktualisiert.

5.4.14 Ports

5.4.14.1 Overview

Portkonfiguration im Überblick

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



Port	Port Name	Port Type	Status	OperState	Link	Mode	MTU	Negotiation	Flow Ctrl. Type	Flow Ctrl.	MAC Address
P0.1		Switch-Port VLAN Hybrid	enabled	down	down	100M FD	1514	enabled	☐	disabled	00-1b-1b-40-91-21
P0.2		Switch-Port VLAN Hybrid	enabled	down	down	100M FD	1514	enabled	☐	disabled	00-1b-1b-40-91-22
P0.3		Switch-Port VLAN Hybrid	enabled	down	down	100M FD	1514	enabled	☐	disabled	00-1b-1b-40-91-23
P0.4		Switch-Port VLAN Hybrid	enabled	up	up	100M FD	1514	enabled	☐	disabled	00-1b-1b-40-91-24
P0.5		Switch-Port VLAN Hybrid	disabled	down	up	100M FD	1514	enabled	☐	disabled	00-1b-1b-40-91-25
P0.6		Switch-Port VLAN Hybrid	enabled	down	down	100M FD	1514	enabled	☐	disabled	00-1b-1b-40-91-26
P0.7		Switch-Port VLAN Hybrid	enabled	up	up	100M FD	1514	enabled	☐	disabled	00-1b-1b-40-91-27
P0.8		Switch-Port VLAN Hybrid	enabled	down	down	100M FD	1514	enabled	☐	disabled	00-1b-1b-40-91-28

Beschreibung der angezeigten Felder

Die Tabelle gliedert sich in folgende Spalten:

- **Port**
  Zeigt die konfigurierbaren Ports an. Der Eintrag ist ein Link. Wenn Sie auf den Link klicken, wird die entsprechende Konfigurationsseite geöffnet.

  Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Port Name**
  Zeigt den Namen des Ports.
- **Port Type**
  Zeigt den Typ des Ports an: Switch-Port VLAN Hybrid. Der Port sendet getaggte und ungetaggte Telegramme. Er ist nicht automatisch Mitglied eines VLANs.
- **Status**
  Zeigt an, ob der Port ein- oder ausgeschaltet ist. Datenverkehr ist nur über einen eingeschalteten Port möglich.

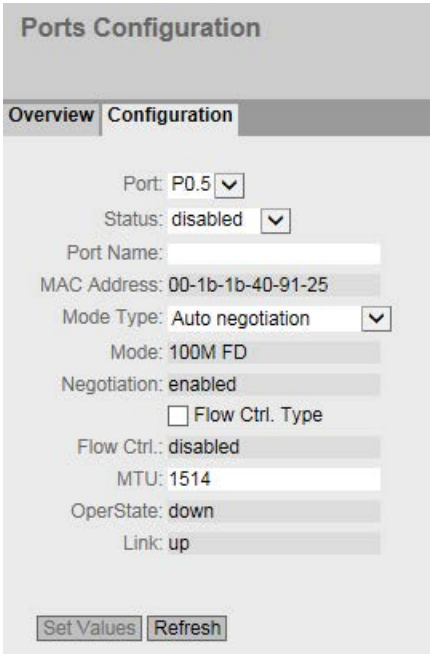
- **OperState**
  Zeigt den aktuellen Betriebszustand an. Der Betriebszustand ist vom konfigurierten "Status" und dem "Link" abhängig. Es gibt folgende Möglichkeiten:
  - Up
    Sie haben für den Port den Status "enabled" konfiguriert und der Port hat eine gültige Verbindung zum Netzwerk.
  - Down
    Sie haben für den Port den Status "disabled" oder "Link down" konfiguriert oder der Port hat keine Verbindung.
- **Link**
  Zeigt den Verbindungsstatus zum Netzwerk am. Beim Verbindungsstatus ist Folgendes möglich:
  - Up
    Der Port hat eine gültige Verbindung zum Netzwerk, es wird ein "Link Integrity Signal" empfangen.
  - Down
    Die Verbindung ist unterbrochen, weil beispielsweise das angeschlossene Gerät ausgeschaltet ist.
- **Mode**
  Zeigt die Übertragungsparameter des Ports an.
- **MTU (Maximum Transmission Unit)**
  Zeigt die Paketgröße an.
- **Negotiation**
  Zeigt an, ob die automatische Konfiguration aktiviert oder deaktiviert ist.
- **Flow Ctrl. Type**
  Gibt an, ob für den Port die Flusskontrolle aktiviert oder deaktiviert ist.
- **Flow Ctrl.**
  Gibt an, ob bei diesem Port die Flusskontrolle arbeitet.
- **MAC Address**

  Zeigt die MAC-Adresse des Ports an.

5.4.14.2 Configuration

Ports konfigurieren

Mit dieser Seite können Sie alle Ports des Geräts konfigurieren.



Beschreibung der angezeigten Felder

Die Tabelle gliedert sich in folgende Zeilen:

- **Port**
  Wählen Sie aus der Klappliste den zu konfigurierenden Port aus. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Status**
  Legen Sie fest, ob der Port ein- oder ausgeschaltet ist. Der Datenverkehr ist nur über einen eingeschalteten Port möglich.
  - enabled
    Der Port ist eingeschaltet.
  - disabled
    Der Port ist ausgeschaltet, aber die Verbindung besteht noch.
  - link down
    Der Port ist ausgeschaltet und die Verbindung zum Partnergerät ist abgebaut.

  Hinweis

  Reduzierte Stromaufnahme

  Für jeden optischen Port, den Sie auf "link down" setzen, verringert sich die Stromaufnahme des Geräts um 30 mA.

- **Port Name**
  Tragen Sie hier einen Namen für den Port ein.
- **MAC Address**
  Zeigt die MAC-Adresse des Ports an.
- **Mode Type**
  Wählen Sie aus dieser Klappliste die Übertragungsgeschwindigkeit und das Übertragungsverfahren des Ports aus. Wenn Sie die Betriebsart auf "Auto negotiation" stellen, werden diese Parameter automatisch mit dem angeschlossenen Endgerät ausgehandelt. Dieses muss sich hierzu ebenfalls in der Betriebsart "Auto negotiation" befinden.

  Hinweis

  Damit der Port und der Partner-Port miteinander kommunizieren können, müssen die Einstellungen auf beiden Seiten übereinstimmen.

  Hinweis

  Wenn die Funktion "Auto negotiation" ausgeschaltet wird, ist auch die Funktion "MDI/MDI-X Autocrossover" nicht aktiv. Verwenden Sie dann ein gekreuztes Kabel.

- **Mode**
  Zeigt die Übertragungsgeschwindigkeit und das Übertragungsverfahren des Ports an. Die Übertragungsgeschwindigkeit kann 10 Mbit/s oder 100 Mbit/s betragen. Als Übertragungsverfahren können Vollduplex (FD) oder Halbduplex (HD) konfiguriert werden.
- **Negotiation**
  Zeigt an, ob die automatische Anschlusskonfiguration zum Partner-Port aktiviert oder deaktiviert ist.

  Hinweis

  Ein-/Ausschalten der Flusskontrolle bei Auto Negotiation

  Die Flusskontrolle kann nur bei ausgeschalteter Funktion "Auto Negotiation" aktiviert oder deaktiviert werden. Die Funktion kann danach wieder aktiviert werden.

- **Flow Ctrl. Type**
  Aktivieren oder deaktivieren Sie die Flusskontrolle für den Port.
- **Flow Ctrl.**
  Zeigt an, ob bei diesem Port die Flusskontrolle arbeitet.
- **MTU**
  Tragen Sie die maximale Paketgröße ein.

- **OperState**
  Zeigt den aktuellen Betriebszustand an. Der Betriebszustand ist vom konfigurierten "Status" und dem "Link" abhängig. Es gibt folgende Möglichkeiten:
  - Up
    Sie haben für den Port den Status "enabled" konfiguriert und der Port hat eine gültige Verbindung zum Netzwerk.
  - Down
    Sie haben für den Port den Status "disabled" oder "Link down" konfiguriert oder der Port hat keine Verbindung.
- **Link**
  Zeigt den Verbindungsstatus zum Netzwerk an. Es gibt folgende Möglichkeiten:
  - Up
    Der Port hat eine gültige Verbindung zum Netzwerk, es wird ein "Link IntegritySignal" empfangen.
  - Down
    Die Verbindung ist unterbrochen, weil z. B. das angeschlossene Gerät ausgeschaltet ist.

Veränderung der Port-Konfiguration

Klicken Sie in das entsprechende Feld, um die Konfiguration zu ändern.

Hinweis

Optische Ports arbeiten immer mit dem Übertragungsverfahren Vollduplex und mit maximaler Übertragungsgeschwindigkeit. Deshalb können Sie bei optischen Ports folgende Einstellungen nicht vornehmen:

- Automatische Konfiguration
- Übertragungsgeschwindigkeit
- Übertragungsverfahren

Hinweis

Das Gerät verhindert oder reduziert bei Überlastung eines Ports durch verschiedene Automatismen die Rückwirkung auf andere Ports und Prioritätsklassen (Class of Service). Dies kann auch bei aktivierter Flusskontrolle dazu führen, dass Telegramme verworfen werden.

Port-Überlastungen treten auf, wenn das Gerät mehr Telegramme empfängt, als es senden kann, z.B. infolge unterschiedlicher Übertragungsgeschwindigkeiten.

Vorgehensweise zur Konfiguration

1. Ändern Sie die Einstellungen entsprechend Ihrer Konfiguration.
2. Klicken Sie auf die Schaltfläche "Set Values".

5.4.15 Fault Monitoring

5.4.15.1 Power Supply

Einstellungen zur Überwachung der Spannungsversorgung

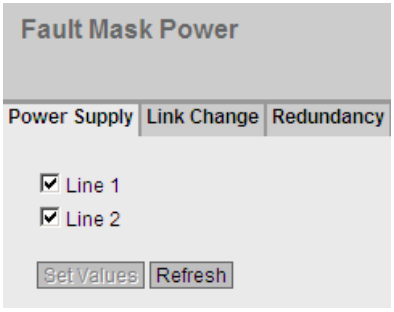
Konfigurieren Sie, ob die Spannungsversorgung durch das Meldesystem überwacht werden soll. Je nach Hardware-Variante gibt es ein oder zwei Spannungsanschlüsse (Line 1 / Line 2). Bei redundanter Spannungsversorgung konfigurieren Sie die Überwachung für jede einzelne Zuleitung getrennt.

Es wird dann ein Fehler durch das Meldesystem signalisiert, wenn an einem überwachten Anschluss (Line 1 oder Line 2) keine oder eine zu geringe Spannung anliegt.

Hinweis

Die zulässigen Betriebsspannungsgrenzen entnehmen Sie der Betriebsanleitung des Geräts.

Ein Fehler führt zum Aufleuchten der Fehler-LED am Gerät und kann abhängig von der Konfiguration einen Trap, eine E-Mail oder einen Eintrag in der Ereignisprotokoll-Tabelle auslösen.



Vorgehensweise

1. Klicken Sie in das Optionskästchen vor dem entsprechenden Anschlussnamen, den Sie überwachen wollen, um die Überwachungsfunktion ein- oder auszuschalten.
2. Klicken Sie auf die Schaltfläche "Set Values".

5.4.15.2 Link Change

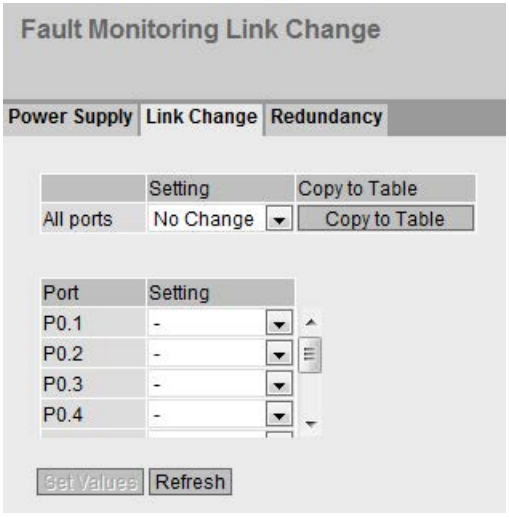
Konfiguration der Fehlerüberwachung von Zustandsänderungen bei Verbindungen

Auf dieser Seite konfigurieren Sie, ob bei einer Zustandsänderung einer Netzwerkverbindung eine Fehlermeldung ausgelöst wird.

Bei aktivierter Verbindungsüberwachung wird ein Fehler signalisiert,

- wenn an einem Port ein Link vorhanden sein soll und dieser fehlt.
- oder wenn an dem Port kein Link vorhanden sein soll und ein Link erkannt wird.

Ein Fehler führt zum Aufleuchten der Fehler-LED am Gerät und kann abhängig von der Konfiguration einen Trap, eine E-Mail oder einen Eintrag in der Ereignisprotokoll-Tabelle auslösen.



Beschreibung der angezeigten Felder

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports gültig sind.
- **Setting**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - "-" (Deaktiviert)
  - Up
  - Down
  - No Change: Einstellung in der Tabelle 2 bleibt unverändert.
- **Copy to Table**

  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

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

  Wählen Sie aus der Klappliste die Einstellung aus. Folgende Möglichkeiten haben Sie:

  – Up
  Die Fehlerbehandlung wird beim Übergang in den aktiven Zustand des Ports ausgelöst.

  (Von "Link down" nach "Link up")

  – Down
  Die Fehlerbehandlung wird beim Übergang in den inaktiven Zustand des Ports ausgelöst.

  (Von "Link up" nach "Link down")

  – "-" (Deaktiviert)
  Die Fehlerbehandlung wird nicht ausgelöst.

Vorgehensweise zur Konfiguration

Fehlerüberwachung für einen Port konfigurieren

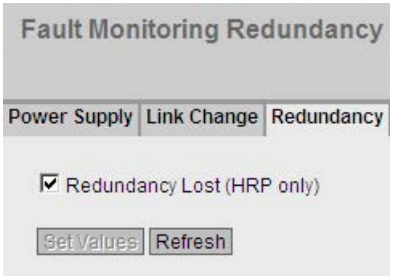
1. Wählen Sie aus der entsprechenden Klappliste die Optionen der Steckplätze/Ports, deren Verbindungsstatus Sie überwachen wollen.
2. Klicken Sie auf die Schaltfläche "Set Values".

Fehlerüberwachung für alle Ports konfigurieren

1. Wählen Sie in der Klappliste der Spalte "Setting" die gewünschte Einstellung aus.
2. Klicken Sie auf die Schaltfläche "Copy to Table". Die Einstellung wird für alle Ports der Tabelle 2 übernommen.
3. Klicken Sie auf die Schaltfläche "Set Values".

5.4.15.3 Redundancy

Auf dieser Seite konfigurieren Sie, ob bei einer Zustandsänderung einer Netzwerkverbindung eine Fehlermeldung ausgelöst wird.



Einstellung

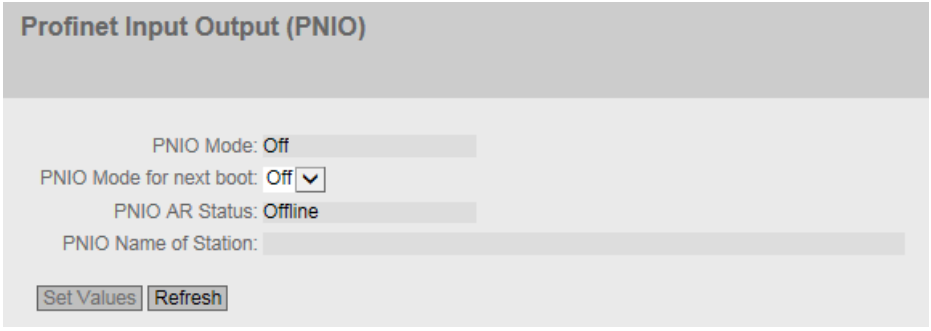
- **Redundancy Lost (HRP only)**

  Aktivieren oder deaktivieren Sie die Verbindungsüberwachung. Wenn die Redundanz der Verbindung verloren geht, wird ein Fehler signalisiert.

5.4.16 PNIO

Einstellungen für PROFINET IO

Diese Seite zeigt den PROFINET IO AR Status und den Gerätenamen an.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **PNIO Mode**

  Zeigt an, ob PNIO aktiviert ("On") oder deaktiviert ("Off") ist.

- **PNIO Mode for next boot**

  Stellen Sie ein, ob PNIO nach dem nächsten Neustart des Geräts aktiviert ("On") oder deaktiviert ("Off") sein soll.

  Hinweis

  PNIO AR Status

  Wenn eine PROFINET-Verbindung aufgebaut ist, d. h. der PNIO AR-Status "Online" ist, können Sie PNIO nicht deaktivieren.

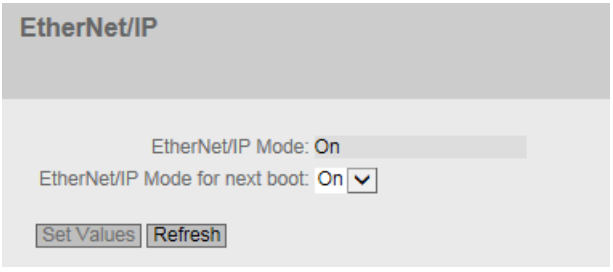
- **PNIO AR Status**
  Dieses Feld zeigt den Status des PROFINET IO-Verbindungsverhältnisses an, d.h. ob das Gerät mit einem PROFINET IO-Controller "Online" oder "Offline" verbunden ist. Online bedeutet hierbei, dass eine Verbindung zu einem PROFINET IO-Controller besteht, dass dieser seine Konfigurationsdaten auf das Gerät 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 konfigurierbar.

- **PNIO Name of Station**
  In diesem Feld erscheint der PROFINET IO-Gerätenamen gemäß der Projektierung in der HW-Konfig von STEP 7.

5.4.17 EtherNet/IP

EtherNet/IP

Auf dieser Seite konfigurieren Sie den Modus von EtherNet/IP.



Beschreibung

Die Seite enthält folgende Felder:

- **EtherNet/IP Mode**

  Zeigt an, ob EtherNet/IP aktiviert ("On") oder deaktiviert ("Off") ist.

- **EtherNet/IP Mode for next boot**

  Stellen Sie ein, ob EtherNet/IP nach dem nächsten Neustart des Geräts aktiviert ("On") oder deaktiviert ("Off") sein soll.

Hinweis

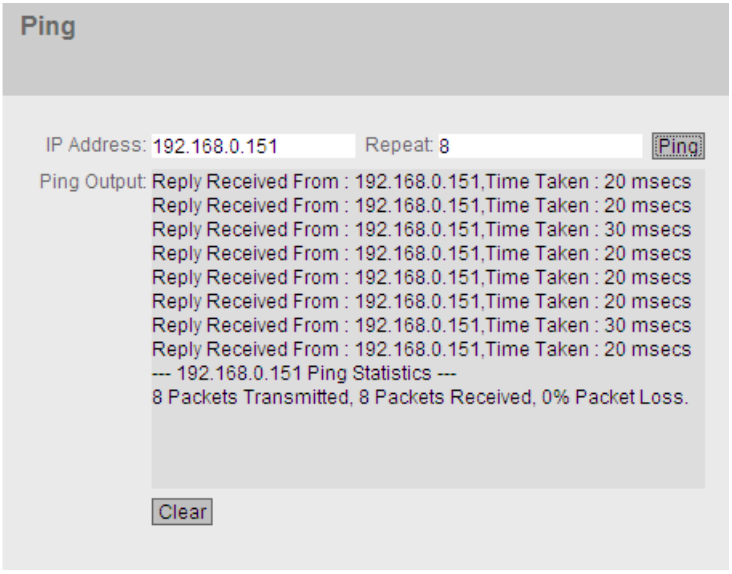
PNIO AR Status

Wenn eine PROFINET-Verbindung aufgebaut ist, d. h. der PNIO AR-Status "Online" ist, können Sie EtherNet/IP nicht aktivieren.

5.4.18 Ping

Erreichbarkeit einer Adresse in einem IP-Netzwerk

Mit der Ping-Funktion können Sie überprüfen, ob eine bestimmte IP-Adresse im Netzwerk erreichbar ist.



Beschreibung

Die Tabelle gliedert sich in folgende Spalten:

- **Eingabefeld "IP Address"**
  Tragen Sie die IP-Adresse des Geräts ein.
- **Eingabefeld "Repeat"**
  Tragen Sie die Anzahl der Ping-Anforderungen ein.
- **Schaltfläche "Ping"**
  Klicken Sie diese Schaltfläche, um die Ping-Funktion zu starten.
- **Ping Output**
  Dieses Feld zeigt die Ausgabe der Ping-Funktion an.
- **Schaltfläche "Clear"**
  Klicken Sie diese Schaltfläche, um das Feld "Ping Output" zu leeren.

5.4.19 Port Diagnostics

5.4.19.1 Cable Tester

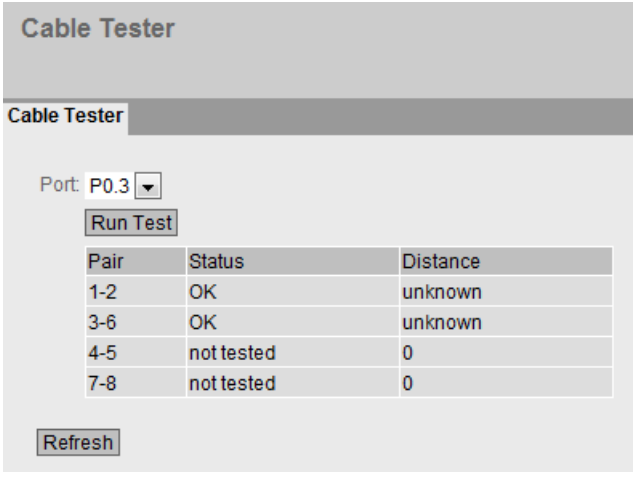
Mit dieser Seite kann jeder einzelne Ethernet-Port eine unabhängige Fehlerdiagnose am Kabel durchführen. Dieser Test wird durchgeführt, ohne dass das Kabel ausgesteckt, ein Kabeltester angeschlossen und am anderen Ende ein Loopback-Modul installiert ist. Kurzschlüsse sowie Leitungsunterbrechungen können auf wenige Meter genau lokalisiert werden.

Hinweis

Bitte beachten Sie, dass dieser Test nur zulässig ist, wenn auf dem zu testenden Port keine Datenverbindung aufgebaut ist.

Sollte dennoch auf dem zu testenden Port eine Datenverbindung bestehen, so wird diese kurzzeitig unterbrochen.

Ein automatischer Wiederaufbau der Verbindung kann scheitern und muss dann manuell erfolgen.



Beschreibung

Die Seite enthält folgende Felder:

- **Port**
  Wählen Sie aus der Klappliste den gewünschten Port aus.
- **Run Test**
  Aktiviert die Fehlerdiagnose. Das Ergebnis wird in der Tabelle dargestellt.

Die Tabelle enthält folgende Spalten:

- **Pair**
  Zeigt das Adernpaar im Kabel an.

  Hinweis

  Adernpaare

  bei 10/100 Mbit Netzwerkkabeln werden die Adernpaare 4-5 und 7-8 nicht verwendet.

  Dabei ist die Zuordnung Adernpaar - Pinbelegung wie folgt (DIN EN 50173):

  Paar 1 = Pin 1-2

  Paar 2 = Pin 3-6

  Paar 3 = Pin 4-5

  Paar 4 = Pin 7-8

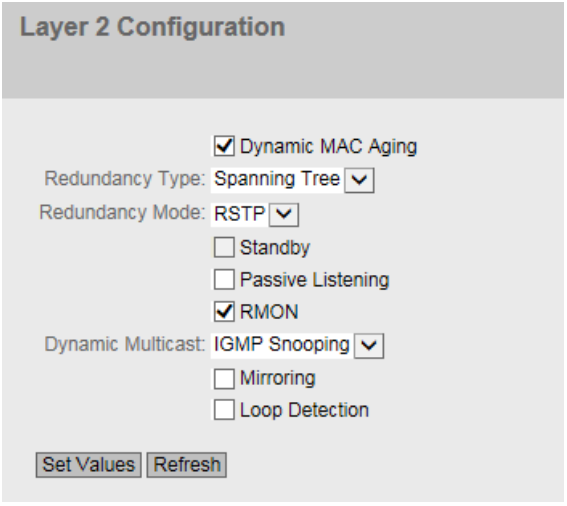
- **Status**
  Zeigt den Status der Leitung an.
- **Distance**
  Zeigt die Entfernung zum Kabelende, Kabelbruch oder zum Kurzschluss an. Der Wert für die Entfernung hat eine Toleranz von +/- 1 m.

5.5 Das Menü "Layer 2"

5.5.1 Configuration

Layer 2 konfigurieren

Auf dieser Seite nehmen Sie eine Basiskonfiguration der Funktionen von Layer 2 vor. Auf den jeweiligen Konfigurationsseiten dieser Funktionen sind detailliertere Einstellungen möglich. Auf den Konfigurationsseiten können Sie auch die Einstellungen prüfen.



Beschreibung der angezeigten Felder

- **Dynamic MAC Aging**
  Aktivieren oder deaktivieren Sie den Mechanismus "Aging". Weitere Einstellungen konfigurieren Sie unter "Layer 2 > Dynamic MAC Aging".
- **Redundancy Type**
  Folgende Einstellungen gibt es:
  - **"-" (Deaktiviert)**
    Die Redundanzfunktion ist deaktiviert.
  - **Ring**
    Wenn Sie diese Option auswählen, legen Sie in der Klappliste "Redundancy Mode" den gewünschten Redundanzmodus fest.
  - **Spanning Tree**
    Wenn Sie diese Option auswählen, legen Sie in der Klappliste "Redundancy Mode" den gewünschten Kompatibilitätsmodus fest.

- **Redundancy Mode**

  Wenn Sie in der Klappliste "Redundancy Type" "Ring" auswählen, stehen Ihnen folgende Auswahlmöglichkeiten zur Verfügung:

  – Automatic Redundancy Detection

    Wählen Sie diese Einstellung, um eine automatische Konfiguration der Redundanzbetriebsart vorzunehmen.

    Im Modus "Automatic Redundancy Detection" stellt das Gerät automatisch fest, ob sich ein Gerät mit der Rolle "HRP Manager" im Ring befindet. Ist dies der Fall, so nimmt das Gerät die Rolle "HRP Client" ein.
    Wird kein HRP Manager gefunden, so handeln alle Geräte mit der Einstellung "Automatic Redundancy Detection" oder "MRP Auto-Manager" untereinander aus, welches Gerät die Rolle "MRP Manager" einnimmt. Dabei wird immer das Gerät mit der niedrigsten MAC-Adresse zum "MRP Manager". Die übrigen Geräte stellen sich automatisch auf die Betriebsart "MRP Client" ein.

  – MRP Auto-Manager

    Im Modus "MRP Auto-Manager" handeln die Geräte untereinander aus, welches Gerät die Rolle "MRP Manager" einnimmt. Dabei wird immer das Gerät mit der niedrigsten MAC-Adresse zum "MRP Manager". Die übrigen Geräte stellen sich automatisch auf die Betriebsart "MRP Client" ein.

    Im Gegensatz zur Einstellung "Automatic Redundancy Detection" sind die Geräte nicht in der Lage zu erkennen, ob ein HRP-Manager im Ring ist.

    Hinweis

    MRP-Projektierung in STEP 7

    Wenn Sie über STEP 7 die Rolle "Manager (Auto)" oder "Manager" für das Gerät einstellen, wird auf dieser WBM-Seite in beiden Fällen "MRP Auto-Manager" angezeigt. In der Anzeige im CLI wird zwischen den beiden Rollen unterschieden.

  – MRP Client

    Das Gerät nimmt die Rolle MRP-Client ein.

  – HRP Client

    Das Gerät nimmt die Rolle HRP-Client ein.

  – HRP Manager

    Das Gerät nimmt die Rolle HRP-Manager ein.

    Bei der Projektierung eines HRP-Rings muss ein Gerät als HRP-Manager eingestellt werden. Bei allen übrigen Geräten muss "HRP Client" oder "Automatic Redundancy Detection" eingestellt sein.

  Wenn Sie in der Klappliste "Redundancy Type" "Spanning Tree" auswählen, stehen Ihnen folgende Auswahlmöglichkeiten zur Verfügung:

  – **STP**
    Aktiviert Spanning Tree Protocol. Typische Rekonfigurationszeiten bei Spanning Tree liegen zwischen 20 und 30 Sekunden.

  - **RSTP**
    Aktiviert Rapid Spanning Tree Protocol (RSTP). Wenn an einem Port ein Spanning Tree-Telegramm erkannt wird, fällt dieser Port von RSTP auf Spanning Tree zurück.

    Hinweis

    Bei RSTP (Rapid Spanning Tree-Protokoll) kann es zu kurzzeitiger Schleifenbildung mit Telegrammverdoppelung oder zu Telegrammüberholungen kommen. Wenn das in Ihrem Anwendungsfall nicht akzeptabel sein sollte, müssen Sie das langsamere Standardverfahren Spanning Tree benutzen.

  Weitere Einstellungen konfigurieren Sie unter "Layer 2 > Spanning Tree".

- **Standby**
  Aktivieren oder deaktivieren Sie die Funktion Standby Redundanz. Weitere Einstellungen finden Sie unter "Layer 2 > Ring Redundancy".
- **Passive Listening**
  Aktivieren oder deaktivieren Sie die Funktion Passive Listening.
- **RMON**
  Wenn Sie dieses Optionskästchen aktivieren, ermöglicht Remote Monitoring (RMON), Diagnosedaten im Gerät zu sammeln, aufzubereiten und über SNMP von einer Netzwerkmanagement-Station, die ebenfalls RMON unterstützt, auszulesen. Diese Diagnosedaten, wie zum Beispiel portbezogene Lastverläufe, ermöglichen es, Probleme im Netzwerk frühzeitig zu erkennen und zu beseitigen. Die "Ethernet Statistics Counter" sind zum Teil Bestandteil der RMON Funktion. Wenn Sie RMON deaktivieren, wird der "Ethernet Statistic Counter" bei "Information > Ethernet Statistics" nicht weiter aktualisiert.

  Weitere Einstellungen konfigurieren Sie unter "Layer 2 > RMON".
- **Dynamic Multicast**
  Folgende Einstellung sind möglich:
  - **"-" (Deaktiviert)**
  - **IGMP Snooping**
    Aktiviert IGMP (Internet Group Management Protocol). Weitere Einstellungen konfigurieren Sie unter "Layer 2 > Mulitcast > IGMP".

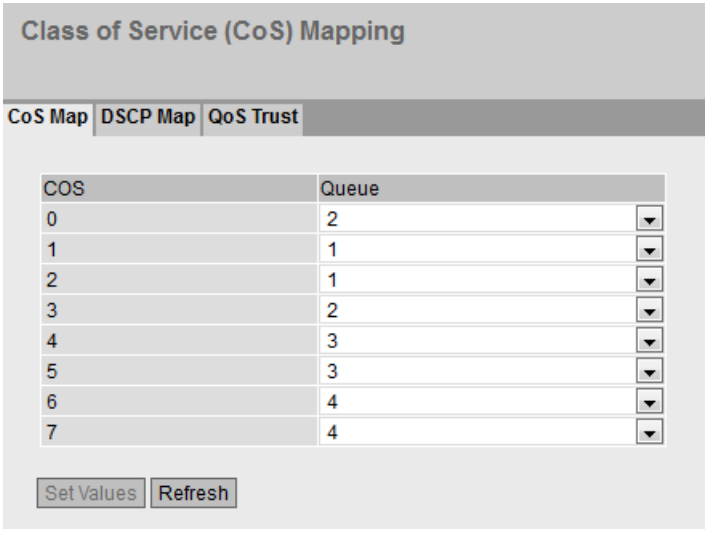
  Weitere Einstellungen konfigurieren Sie unter "Layer 2 > Multicast".
- **Mirroring**
  Aktivieren oder deaktivieren Sie die Port-Spiegelung. Weitere Einstellungen konfigurieren Sie unter "Layer 2 > Mirroring".
- **Loop Detection**
  Aktivieren oder deaktivieren Sie die Funktion Loop Detection. Damit werden Schleifen im Netzwerk erkannt. Weitere Einstellungen finden Sie unter "Layer 2 > Loop Detection"

5.5.2 Qos

5.5.2.1 CoS Queue Mapping

COS Queue Mapping

Hier werden CoS-Prioritäten bestimmten Warteschlangen (Traffic Queues) zugeordnet.



Beschreibung der angezeigten Felder

Die Tabelle gliedert sich in folgende Spalten:

- **COS**
  Zeigt CoS-Priorität der eingehenden Pakete an.
- **Queue**
  Wählen Sie aus der Klappliste die Weiterleitungs-Warteschlange (Sendepriorität) aus, welcher der COS-Priorität zugeordnet wird.
  Je höher die Nummer der Warteschlange desto höher die Sendepriorität.

Die Service-Klassen (COS) sind den Warteschlangen (Queue) wie folgt zugeordnet:

- COS 0 → Queue 2
- COS 1 → Queue 1
- COS 2 → Queue 1
- COS 3 → Queue 2
- COS 4 → Queue 3
- COS 5 → Queue 3
- COS 6 → Queue 4
- COS 7 → Queue 4

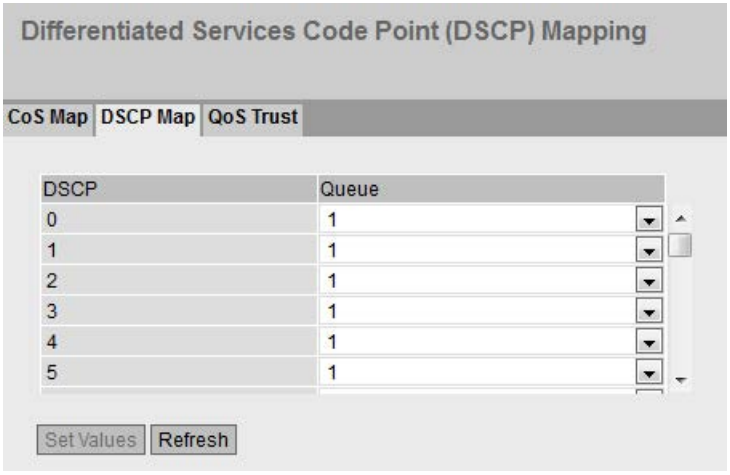
Vorgehensweise zur Konfiguration

1. Wählen Sie zu jedem Wert der Spalte "COS" mit Hilfe der Klappliste "Queue" die Weiterleitungs-Warteschlange aus.
2. Klicken Sie auf die Schaltfläche "Set Values".

5.5.2.2 DSCP Mapping

DSCP Warteschlange

Auf dieser Seite werden DSCP-Einstellungen verschiedenen Warteschlangen (Traffic Queues) zugeordnet.



Beschreibung der angezeigten Werte

Die Tabelle gliedert sich in folgende Spalten:

- **DSCP**
  Zeigt DSCP-Priorität der eingehenden Pakete an.
- **Queue**
  Wählen Sie aus der Klappliste die Weiterleitungs-Warteschlange (Sendepriorität) aus, welcher dem DSCP-Wert zugeordnet wird.
  Je höher die Queue-Nummer desto höher die Sendepriorität.

Die DSCP-Codes sind den Warteschlangen (Queue) wie folgt zugeordnet:

- DSCP-Codes 0 - 15 → Queue 1
- DSCP-Codes 16 - 31 → Queue 2
- DSCP-Codes 32 - 47 → Queue 3
- DSCP-Codes 48 - 63 → Queue 4

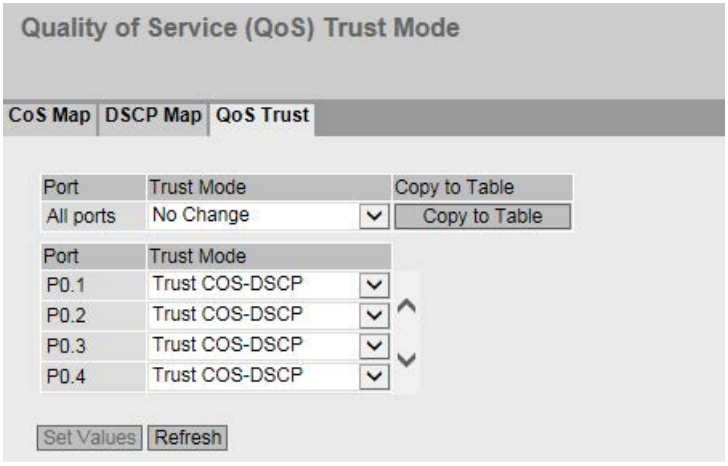
Vorgehensweise zur Konfiguration

1. Wählen Sie zu jedem Wert der Spalte "DSCP" mithilfe der Klappliste "Queue" die Weiterleitungs-Warteschlange aus.
2. Klicken Sie auf die Schaltfläche "Set Values".

5.5.2.3 QoS Trust

Festlegen der Priorität

Auf dieser Seite können Sie portgranular einstellen, nach welchem Verfahren weiterzuleitende Pakete priorisiert werden.



Beschreibung der angezeigten Werte

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**

  Zeigt an, dass die Einstellung für alle Ports der Tabelle 2 gültig ist.

- **Trust Mode**

  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellmöglichkeiten haben Sie:

  – No Trust
  – Trust COS
  – Trust DSCP
  – Trust COS-DSCP
  – No Change

    Tabelle 2 bleibt unverändert.

- **Copy to Table**

  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die konfigurierbaren Ports an.
  Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Trust Mode**
  Wählen Sie aus der Klappliste den gewünschten Modus:
  - No Trust

    Ankommende Pakete werden mit der Priorisierung des Empfangsports weitergeleitet. Wenn ein DSCP-Wert im IP-Header vorhanden ist, wird dieser nicht berücksichtigt. Wenn ein VLAN-Tag vorhanden ist, wird es durch den Prioritätswert des Eingangsports ersetzt.
  - Trust COS

    Wenn ein ankommendes Paket ein VLAN-Tag enthält, wird es mit dieser Priorisierung weitergeleitet. Wenn ein DSCP-Wert im IP-Header vorhanden ist, wird dieser nicht berücksichtigt. Wenn das Paket kein VLAN-Tag enthält, wird es mit der Priorisierung des Empfangsports weitergeleitet.
  - Trust DSCP

    Wenn ein ankommendes Paket eine DSCP-Priorisierung enthält, wird es mit dieser Priorisierung weitergeleitet. Wenn ein VLAN-Tag vorhanden ist, wird es nicht berücksichtigt. Wenn das Paket keine DSCP-Priorisierung enthält, wird es mit der Priorisierung des Empfangsports weitergeleitet.
  - Trust COS-DSCP

    Bei einem ankommenden Paket wird sequenziell geprüft, welche Priorisierung es enthält.
    Wenn es eine DSCP-Priorisierung enthält, wird es wie im Modus "Trust DSCP" behandelt.
    Wenn es keine DSCP-Priorisierung enthält, wird auf ein VLAN-Tag geprüft. Wenn es ein VLAN-Tag enthält, wird es mit dieser Priorisierung weitergeleitet. Wenn es weder eine DSCP-Priorisierung noch ein VLAN-Tag enthält, wird es mit der Priorisierung des Empfangsports weitergeleitet.

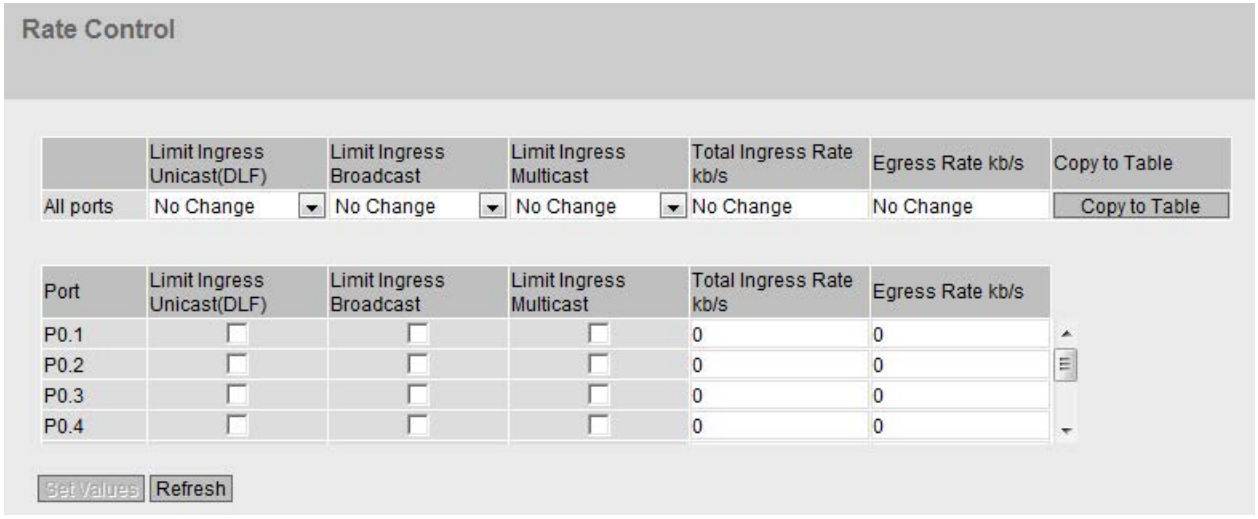
Vorgehensweise zur Konfiguration

1. Wählen Sie aus der Klappliste den gewünschten Wert aus.
2. Klicken Sie auf die Schaltfläche "Set Values".

5.5.3 Rate Control

Begrenzung der Transferrate eingehender und ausgehender Daten

Auf dieser Seite konfigurieren Sie die Lastbegrenzung (maximale Anzahl von Datenpaketen pro Sekunde) für die einzelnen Ports. Sie können festlegen, für welche Kategorie von Telegrammen diese Grenzwerte gelten sollen.



Beschreibung der angezeigten Werte

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports gültig sind.
- **Limit Ingress Unicast (DLF) / Limit Ingress Broadcast / Limit Ingress Multicast**
  Wählen Sie in der Klappliste die gewünschte Einstellung aus.
  - enabled: Aktiviert die Funktion.
  - disabled: Deaktiviert die Funktion
  - No Change: Einstellung in der Tabelle 2 bleibt unverändert
- **Total Ingress Rate kb/s**
  Legen Sie Datenrate für alle eingehenden Telegramme fest. Wenn "No Change" eingetragen ist, bleibt der Eintrag in der Tabelle unverändert.
- **Egress Rate kb/s**
  Legen Sie Datenrate für alle ausgehenden Telegramme fest. Wenn "No Change" eingetragen ist, bleibt der Eintrag in der Tabelle unverändert
- **Copy to Table**
  Wenn Sie auf die Schaltfläche klicken, werden die Einstellungen für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt den jeweiligen Steckplatz und den dazugehörigen Port an, auf die sich die weiteren Angaben beziehen. Dieses Feld ist nicht konfigurierbar. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Limit Ingress Unicast (DLF)**
  Aktivieren oder deaktivieren Sie die Datenrate zur Begrenzung der eingehenden Unicast-Telegramme mit nicht auflösbarer Adresse (Destination Lookup Failure).
- **Limit Ingress Broadcast**
  Aktivieren oder deaktivieren Sie die Datenrate zur Begrenzung der eingehenden Broadcast-Telegramme.
- **Limit Ingress Multicast**
  Aktivieren oder deaktivieren Sie die Datenrate zur Begrenzung der eingehenden Multicast-Telegramme.
- **Total Ingress Rate kb/s**
  Legen Sie Datenrate für alle eingehenden Telegramme fest.
- **Egress Rate kb/s**
  Legen Sie Datenrate für alle ausgehenden Telegramme fest.

Hinweis

Rundungen der Werte, Abweichung vom Sollwert

Beachten Sie bei der Eingabe der Rate-Werte, dass das WBM auf korrekte Werte rundet.

Sind Werte für Total Ingress Rate und Egress Rate konfiguriert, können die tatsächlichen Werte im Betrieb leicht von den eingestellten Werten abweichen.

Vorgehensweise zur Konfiguration

1. Tragen Sie in der Zeile des zu konfigurierenden Ports die entsprechenden Werte in die Spalten "Total Ingress Rate" und "Egress Rate" ein.
2. Um die Begrenzung für die eingehenden Telegramme zu verwenden, aktivieren Sie in der Zeile die Optionskästchen. Für die ausgehenden Telegramme wird der Wert in der Spalte "Egress Rate" verwendet.
3. Klicken Sie auf die Schaltfläche "Set Values".

5.5.4 VLAN

5.5.4.1 General

VLAN-Konfigurationsseite

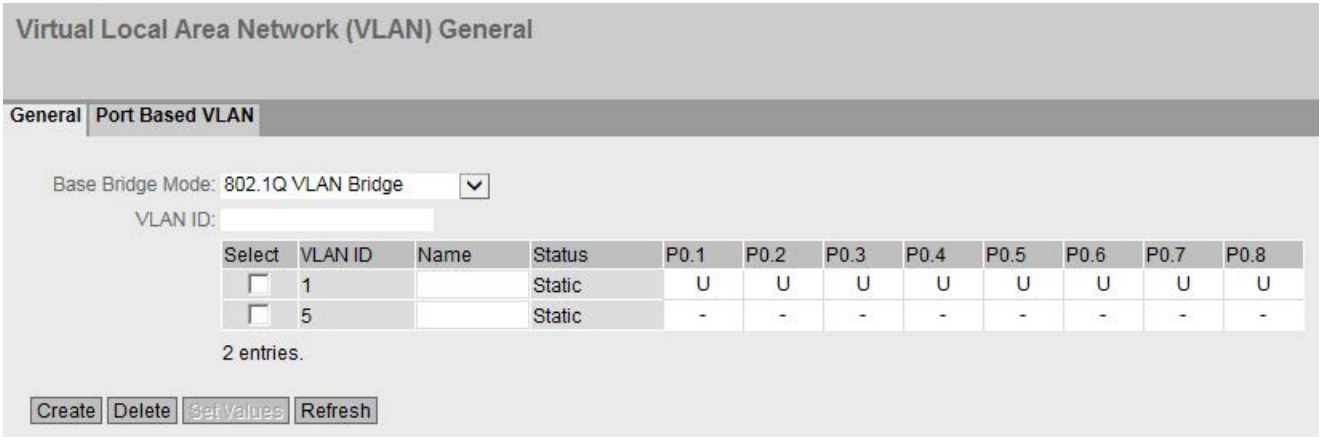
Auf dieser Seite legen Sie fest, ob das Gerät Telegramme mit VLAN-Tags transparent weiterleitet (IEEE 802.1D/VLAN-unaware-Modus) oder VLAN-Informationen berücksichtigt (IEEE 802.1Q/VLAN-aware-Modus). Wenn sich das Gerät im Modus "802.1Q VLAN Bridge" befindet, können Sie VLANs definieren und die Verwendung der Ports festlegen.

Die Einstellmöglichkeiten auf dieser Seite sind abhängig davon, was Sie im Feld "Base Bridge Mode" auswählen.

Hinweis

Ändern der Agent VLAN ID

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



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Base Bridge Mode**
  Wählen Sie aus der Klappliste den Modus. Folgende Modi sind möglich:

  Hinweis

  Base Bridge Mode wechseln

  Beachten Sie den Abschnitt "Base Bridge Mode wechseln". In diesem Abschnitt ist beschrieben, wie sich ein Wechsel auf die bestehende Konfiguration auswirkt.

  – 802.1Q VLAN Bridge

    Stellt bei dem Gerät den Modus "VLAN-aware" ein. In diesem Modus werden VLAN-Informationen berücksichtigt.

    Default-Einstellung bei EtherNet/IP-Varianten

  – 802.1D Transparent Bridge

    Stellt bei dem Gerät den Modus "VLAN-unaware" ein. In diesem Modus werden VLAN-Tags nicht berücksichtigt bzw. verändert, sondern transparent weitergeleitet. Sie können in diesem Modus keine VLANs anlegen. Es ist nur ein Management-VLAN verfügbar: VLAN 1.

    Default-Einstellung bei PROFINET-Varianten

- **VLAN ID**
  Tragen Sie im Eingabefeld "VLAN ID" die VLAN ID ein.
  Wertebereich: 1 ... 4094

Die Tabelle gliedert sich in folgende Spalten:

- **Select**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **VLAN ID**
  Zeigt die VLAN ID an. Die VLAN ID (eine Zahl zwischen 1 und 4094) kann nur beim Anlegen eines neuen Datensatzes einmalig vergeben werden und ist danach nicht mehr änderbar. Zur Änderung muss der gesamte Datensatz gelöscht und neu angelegt werden. Das Gerät unterstützt bis zu 17 VLANs.
- **Name**
  Tragen Sie einen Namen für das VLAN ein. Der Name hat nur informativen Charakter und keine Auswirkungen auf die Konfiguration. Die Länge ist max. 32 Zeichen.

- **Status**
  Zeigt die Statusart des Eintrags in der internen Portfiltertabelle an. Dabei bedeutet statisch, dass die Adresse vom Anwender statisch eingetragen wurde.
- **Liste der Ports**
  Legen Sie die Verwendung des Ports fest. Folgende Möglichkeiten gibt es:
  - "-"
    Der Port ist kein Mitglied des angegebenen VLANs.
    Bei der Neudefinition sind alle Ports mit der Kennung "-" belegt.
  - M
    Der Port ist Mitglied des VLANs. In diesem VLAN gesendete Telegramme werden mit dem entsprechenden VLAN-Tag weitergeleitet.
  - U (Großbuchstabe)
    Der Port ist ungetaggtes Mitglied des VLANs. In diesem VLAN gesendete Telegramme werden ohne VLAN-Tag weitergeleitet. Von diesem Port werden Telegramme ohne VLAN-Tag gesendet.
  - u (Kleinbuchstabe)
    Der Port ist ungetaggtes Mitglied des VLANs, jedoch ist das VLAN nicht als Port-VLAN konfiguriert. In diesem VLAN gesendete Telegramme werden ohne VLAN-Tag weitergeleitet.
  - F
    Der Port ist kein Mitglied des angegebenen VLANs und kann kein Mitglied dieses VLAN werden, auch dann nicht, wenn er als Trunk-Port konfiguriert wird.

Base Bridge Mode wechseln

VLAN-unaware (802.1D Transparent Bridge) → VLAN-aware (802.1Q VLAN Bridge)

Wenn Sie den Base Bridge Mode von VLAN-unaware in VLAN-aware ändern, hat dies folgende Auswirkungen:

- Alle statischen und dynamischen Unicast-Einträge werden gelöscht.
- Alle statischen und dynamischen Multicast-Einträge werden gelöscht.

VLAN-aware (802.1Q VLAN Bridge) → VLAN-unaware (802.1D Transparent Bridge)

Wenn Sie den Base Bridge Mode von VLAN-aware in VLAN-unaware ändern, hat dies folgende Auswirkungen:

- Alle VLAN-Konfigurationen werden gelöscht.
- Es wird ein Management-VLAN angelegt: VLAN 1.
- Alle statischen und dynamischen Unicast-Einträge werden gelöscht.
- Alle statischen und dynamischen Multicast-Einträge werden gelöscht.

802.1Q VLAN Bridge: Wichtige Regeln für VLANs

Berücksichtigen Sie bei der Konfiguration und beim Betrieb Ihrer VLANs folgende Regeln:

- Telegramme mit der VLAN ID "0" werden wie ungetaggte Telegramme behandelt, behalten jedoch ihren Prioritätswert.
- Alle Ports am Gerät senden standardmäßig Telegramme ohne VLAN-Tag, um sicher zu gehen, dass der Endteilnehmer diese Telegramme empfangen kann.
- Bei SCALANCE X-Geräten ist an allen Ports die VLAN ID "1" voreingestellt.
- Wenn an einem Port ein Endteilnehmer angebunden ist, dann sollen ausgehende Telegramme ohne Tag versendet werden (statischer Zugriffs-Port). Wenn sich an dem Port ein weiterer Switch befindet, so ist das Telegramm mit einem Tag zu versehen (Trunk Port).

Vorgehensweise zur Konfiguration

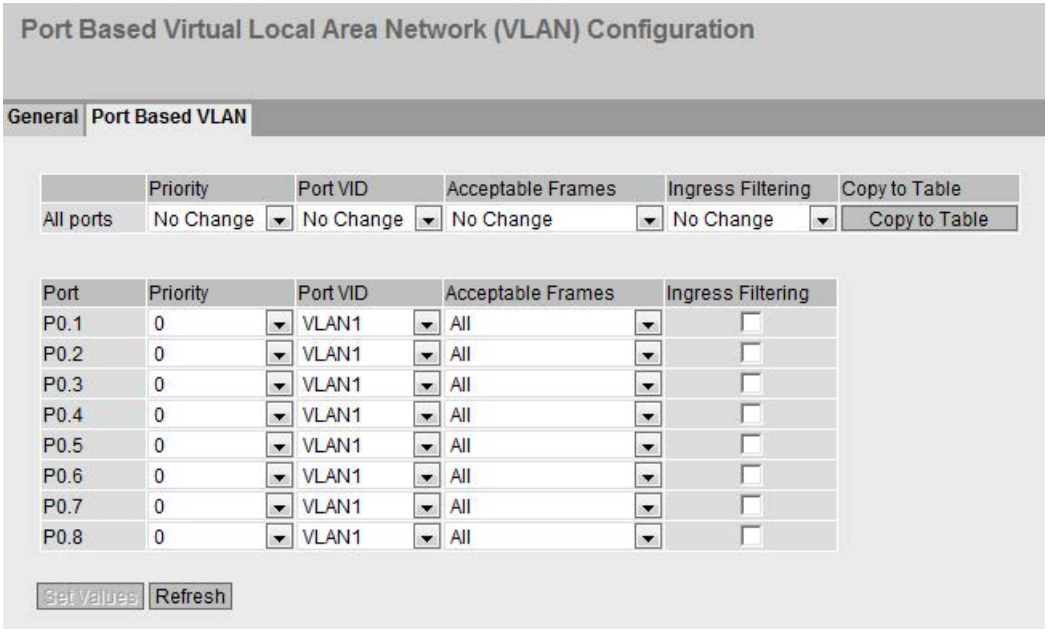
1. Wenn "802.1Q VLAN Bridge" nicht eingestellt ist, wählen Sie in der Klappliste "Base Bridge Mode" den Eintrag "802.1Q VLAN Bridge" aus. Klicken Sie auf die Schaltfläche "Set Values".
2. Tragen Sie im Eingabefeld "VLAN ID" eine ID ein.
3. Klicken Sie auf die Schaltfläche "Create". In der Tabelle wird ein neuer Eintrag erzeugt. Die Felder sind standardmäßig mit "-" belegt.
4. Tragen Sie bei Name einen Namen für das VLAN ein.
5. Legen Sie die Verwendung der Ports in dem VLAN fest. Wenn Sie z. B. M auswählen, ist der Port Mitglied des VLANs. Das in diesem VLAN gesendete Telegramm wird mit dem entsprechenden VLAN-Tag weitergeleitet.
6. Klicken Sie auf die Schaltfläche "Set Values".

5.5.4.2 Port-based VLAN

Verarbeitung empfangener Telegramme

Auf dieser Seite legen Sie die Konfiguration der Port-Eigenschaften für den Telegrammempfang fest.

Sie können die Einstellungen auf dieser Seite nur dann konfigurieren, wenn Sie auf dem Reiter "General" zuvor den "Base Bridge Mode" "802.1Q VLAN Bridge" ausgewählt haben.



Beschreibung der angezeigten Felder

Die Tabelle 1 gliedert sich in folgende Spalten:

- **All ports**
  Zeigt an, dass die Einstellungen für alle Ports gültig sind.
- **Priority / Port VID / Acceptable Frames / Ingress Filtering**
  Wählen Sie in der Klappliste die Einstellung aus. Wenn "No Change" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **Copy to Table**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Priority**
  Wählen Sie aus der Klappliste die Priorität aus, mit der ungetaggte Telegramme versehen werden.

  Die CoS-Priorität (Class of Service), die im VLAN-Tag verwendet wird. Wird ein Telegramm ohne Tag empfangen, wird ihm diese Priorität zugeordnet. Diese Priorität legt fest, wie dieses Telegramm im Vergleich zu anderen Telegrammen weiterhin bearbeitet wird.
  Es gibt insgesamt acht Prioritäten, mit den Werten 0 bis 7, wobei 7 der höchsten Priorität entspricht (IEEE 802.1p Port Priority).
- **Port VID**
  Wählen Sie aus der Klappliste die VLAN ID aus. Nur die VLAN IDs sind wählbar, die Sie auf der Seite "VLAN > General" definiert haben.
  Wenn ein empfangenes Telegramm kein VLAN-Tag hat, so wird es um ein Tag mit der hier angegebenen VLAN ID ergänzt und entsprechend den Regeln am Port gesendet.
- **Acceptable Frames**
  Legen Sie fest, welche Arten von Telegrammen akzeptiert werden. Es gibt folgende Alternativen:
  - Tagged Frames Only
    Das Gerät verwirft alle ungetaggten Telegramme. Andernfalls gelten die Weiterleitungsregeln entsprechend der Konfiguration.
  - All
    Das Gerät leitet alle Telegramme weiter.
- **Ingress Filtering**
  Legen Sie fest, ob die VID von empfangenen Telegrammen ausgewertet wird.
  Sie haben folgende Möglichkeiten:
  - Aktiviert
    Die VLAN ID empfangener Telegramme bestimmt die Weiterleitung: Für die Weiterleitung eines VLAN-getaggten Telegramms muss der Empfangsport Mitglied im selben VLAN sein. Am Empfangsport werdenTelegramme aus unbekannten VLANs verworfen.
  - Deaktiviert
    Alle Telegramme werden weitergeleitet.

Vorgehensweise zur Konfiguration

1. Klicken Sie in der Zeile des zu konfigurierenden Ports in das entsprechende Feld der Tabelle, um es zu konfigurieren.
2. Tragen Sie in die Eingabefelder die einzustellenden Werte ein.
3. Wählen Sie aus den Klapplisten die einzustellenden Werte aus.
4. Klicken Sie auf die Schaltfläche "Set Values".

5.5.5 Mirroring

Mirroring

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

Ports spiegeln

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

Wird am Monitor-Port ein Protokollanalysator angeschlossen, kann damit der Datenverkehr am gespiegelten Port aufgezeichnet werden, ohne dass die Verbindung dort unterbrochen wird. Dadurch ist eine rückwirkungsfreie Untersuchung des Datenverkehrs möglich. Voraussetzung hierfür ist, dass am Gerät ein freier Port als Monitor-Port zur Verfügung steht.

5.5.5.1 General

Mirroring General

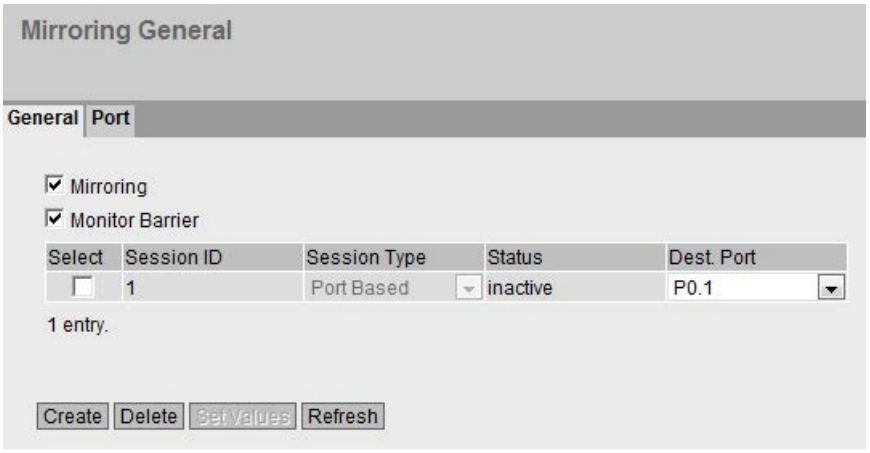
Auf dieser Seite können Sie die Funktion Mirroring ein- bzw. ausschalten und die Basiseinstellungen vornehmen.

Hinweis

Wenn die maximale Datenrate des gespiegelten Ports höher ist als die des Monitor-Ports, kann es zu Datenverlusten kommen und der Monitor-Port gibt nicht mehr die Abläufe am gespiegelten Port wieder. Auf einem Monitor-Port können mehrere Ports gleichzeitig gespiegelt werden.

Sie müssen die Portspiegelung ausschalten, wenn Sie an den Monitor-Port ein normales Endgerät anschließen.

Einstellungen



Die Seite enthält folgende Felder:

- **Mirroring**

  Klicken Sie in dieses Optionskästchen, um das Mirroring zu aktivieren bzw. zu deaktivieren

- **Monitor Barrier**

  Klicken Sie in dieses Optionskästchen, um Monitor Barrier zu aktivieren bzw. zu deaktivieren

---

Hinweis

Auswirkungen von Monitor Barrier

Wenn Sie diese Option einschalten, ist das Management des Switches über den Monitor-Port nicht mehr erreichbar. Folgende portspezifische Funktionen werden geändert:

- DCP forwarding wird ausgeschaltet
- LLDP wird ausgeschaltet
- Unicast- Multicast- und Broadcast-Blocking werden eingeschaltet

Die vorherigen Zustände dieser Funktionen werden nach Beendigung von Monitor Barrier nicht wieder hergestellt. Sie werden auf die Default-Werte zurückgesetzt und müssen eventuell neu konfiguriert werden.

Sie können diese Funktionen manuell konfigurieren, auch wenn Monitor Barrier eingeschaltet ist. Sie erlauben damit aber auch wieder den entsprechenden Datenverkehr auf den Monitor-Port. Wenn Sie dies nicht wünschen, achten Sie darauf, dass nur der zu beobachtende Datenverkehr auf die Schnittstelle geleitet wird.

Wird Mirroring ausgeschaltet, dann werden die genannten portspezifischen Funktionen auf die Default-Werte zurückgesetzt. Das Zurücksetzen erfolgt unabhängig davon, ob die Funktionen manuell oder automatisch durch das Einschalten von Monitor Barrier konfiguriert wurde.

Die Tabelle für die Basiseinstellungen enthält folgende Felder:

- **Select**

  Wählen Sie die Zeile, die Sie löschen wollen.

- **Session ID**

  Die Session ID wird automatisch vergeben, wenn ein neuer Eintrag angelegt wird. Sie können genau eine Session anlegen.

- **Session Type**

  Zeigt die Art der Mirroring-Session an.

- **Status**

  Zeigt an, ob Mirroring aktiv ist.

- **Dest. Port**

  Wählen Sie aus der Klappliste den Ausgangsport aus, auf den in dieser Session gespiegelt werden soll.

Vorgehensweise

1. Klicken Sie auf die Schaltfläche "Create", um in der Tabelle einen Eintrag anzulegen.

   Die Session ID wird dabei automatisch vergeben.

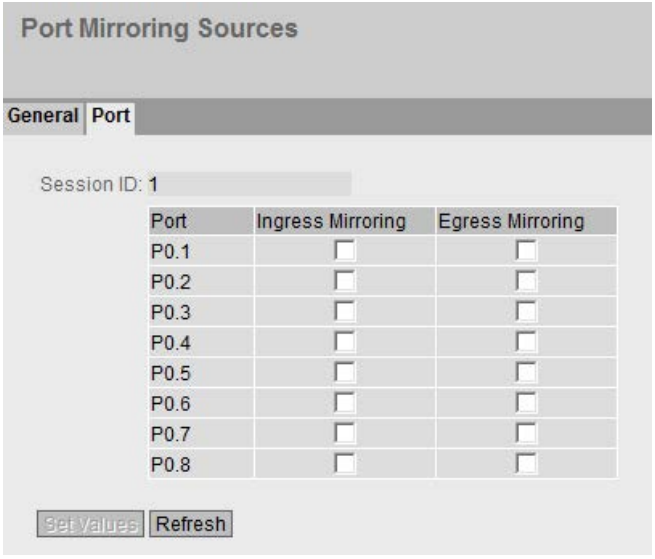
2. Wählen Sie ihre Einstellungen aus.
3. Klicken Sie auf die Schaltfläche "Set Values", um die gewählten Einstellungen zu speichern und zu aktivieren.
4. Wechseln Sie zu dem folgenden Reiter, um zu der Session-ID weitere Detaileinstellungen vorzunehmen.
5. Klicken Sie in der ersten Spalte in das Optionskästchen, um die Zeile zu markieren.

   Klicken Sie auf die Schaltfläche "Delete", um die so markierte Zeile zu löschen.

5.5.5.2 Port

Ports spiegeln

Sie können die Einstellungen auf dieser Seite nur dann konfigurieren, wenn unter dem Reiter "General" zuvor eine Session ID mit dem Session Type "Port Based" erzeugt wurde.



Beschreibung der angezeigten Felder

- **Session ID**
  Zeigt die Session an.
- **Ingress Mirroring**
  Aktiviert oder deaktivieren Sie am gewünschten Port das Mithören der eingehenden Pakete.
- **Egress Mirroring**
  Aktiviert oder deaktivieren Sie am gewünschten Port das Mithören der ausgehenden Pakete.

Hinweis

Mirroring bei Ring-Ports

Wenn Sie bei einem Ring-Port die Funktion Mirroring aktivieren, sendet der Ring-Port Testframes, selbst wenn er sich im Zustand "link down" befindet.

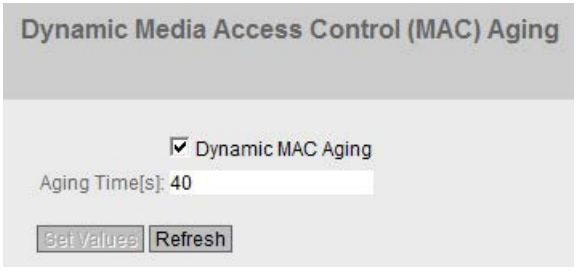
Vorgehensweise zur Konfiguration

1. Klicken Sie in der Tabelle in die Optionskästchen der Zeile hinter dem zu spiegelnden Port.
   Wählen Sie dabei aus, ob Sie eingehende oder ausgehende Pakete mithören wollen. Zum Mithören des gesamten Datenverkehrs eines Ports müssen Sie beide Optionskästchen markieren.
2. Klicken Sie auf die Schaltfläche "Set Values".

5.5.6 Dynamic MAC Aging

Protokolleinstellungen und Switch-Funktionalität

Das Gerät lernt automatisch die Quelladressen der angeschlossenen Teilnehmer. Diese Information wird dazu benutzt, um Datentelegramme gezielt an die betroffenen Teilnehmer weiterzuleiten. Dadurch wird die Netzlast für die anderen Teilnehmer reduziert.
Erhält ein Gerät innerhalb einer bestimmten Zeitspanne kein Telegramm, dessen Quelladresse mit einer gelernten Adresse übereinstimmt, dann löscht es die gelernte Adresse. Dieser Mechanismus wird als "Aging" bezeichnet. Durch Aging wird verhindert, dass Telegramme fehlgeleitet werden, wenn z.B. ein Endgerät (beispielsweise ein Programmiergerät) an einen anderen Port angeschlossen wird.
Wenn die Option nicht aktiviert ist, löscht ein Gerät gelernte Adressen nicht automatisch.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Dynamic MAC Aging**
  Aktivieren oder deaktivieren Sie die Funktion zum automatischen Aging von gelernten MAC-Adressen:
- **Aging Time [s]**
  Tragen Sie die Zeitspanne in Sekunden ein. Nach dieser Zeitspanne wird eine gelernte Adresse gelöscht, wenn das Gerät keine weiteren Telegramme von dieser Absenderadresse mehr empfängt. Der Wertebereich ist von 10 Sekunden bis 630 Sekunden

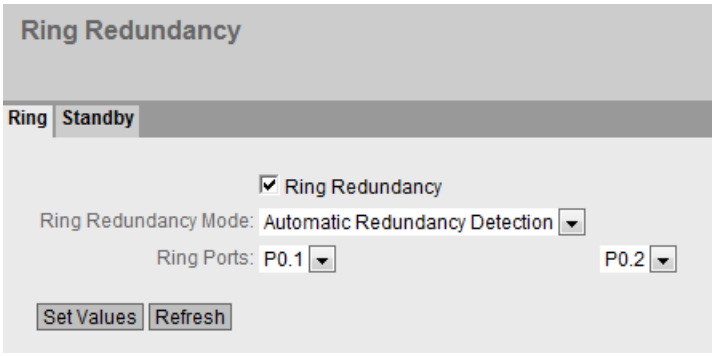
Vorgehensweise zur Konfiguration

1. Aktivieren Sie das Optionskästchen "Dynamic MAC Aging".
2. Tragen Sie in das Eingabefeld "Aging Time [s]" die Zeitspanne in Sekunden ein.
3. Klicken Sie auf die Schaltfläche "Set Values".

5.5.7 Ring Redundancy

5.5.7.1 Ring Redundancy

Konfiguration der Ringredundanz



- **Ring Redundancy**
  Wenn Sie das Optionskästchen "Ring Redundancy" aktivieren, schalten Sie die Ringredundanz ein. Es werden die auf dieser Seite eingestellten Ring-Ports verwendet.
- **Ring Redundancy Mode**

  Hier stellen Sie die Betriebsart der Ringredundanz ein.

  Folgende Betriebsarten stehen zur Verfügung:

  – Automatic Redundancy Detection

    Wählen Sie diese Einstellung, um eine automatische Konfiguration der Redundanzbetriebsart vorzunehmen.

    Im Modus "Automatic Redundancy Detection" stellt das Gerät automatisch fest, ob sich ein Gerät mit der Rolle "HRP Manager" im Ring befindet. Ist dies der Fall, so nimmt das Gerät die Rolle "HRP Client" ein.
    Wird kein HRP Manager gefunden, so handeln alle Geräte mit der Einstellung "Automatic Redundancy Detection" oder "MRP Auto-Manager" untereinander aus, welches Gerät die Rolle "MRP Manager" einnimmt. Dabei wird immer das Gerät mit der niedrigsten MAC-Adresse zum "MRP Manager". Die übrigen Geräte stellen sich automatisch auf die Betriebsart "MRP Client" ein.

– MRP Auto-Manager

Im Modus "MRP Auto-Manager" handeln die Geräte untereinander aus, welches Gerät die Rolle "MRP Manager" einnimmt. Dabei wird immer das Gerät mit der niedrigsten MAC-Adresse zum "MRP Manager". Die übrigen Geräte stellen sich automatisch auf die Betriebsart "MRP Client" ein.

Im Gegensatz zur Einstellung "Automatic Redundancy Detection" sind die Geräte nicht in der Lage zu erkennen, ob ein HRP-Manager im Ring ist.

Hinweis

MRP-Projektierung in STEP 7

Wenn Sie über STEP 7 die Rolle "Manager (Auto)" oder "Manager" für das Gerät einstellen, wird auf dieser WBM-Seite in beiden Fällen "MRP Auto-Manager" angezeigt. In der Anzeige im CLI wird zwischen den beiden Rollen unterschieden.

– MRP Client

Das Gerät nimmt die Rolle MRP-Client ein.

– HRP Client

Das Gerät nimmt die Rolle HRP-Client ein.

– HRP Manager

Das Gerät nimmt die Rolle HRP-Manager ein.

Bei der Projektierung eines HRP-Rings muss ein Gerät als HRP-Manager eingestellt werden. Bei allen übrigen Geräten muss "HRP Client" oder "Automatic Redundancy Detection" eingestellt sein.

- **Ring Ports**

  Hier stellen Sie die Ports ein, die bei der Ringredundanz als Ring-Ports verwendet werden sollen.

  Der Ring-Port, den Sie im linken Drop-down-Menü auswählen, ist bei HRP der "Isolated Port".

  Die Werkseinstellung definiert folgende Ring-Ports:

Geräte	Werkseinstellung Ring-Ports
SCALANCE XB208 und XB216	P0.1 und P0.2
SCALANCE XB205-3	P0.7 und P0.8
SCALANCE XB213-3	P0.15 und P0.16

Vorgehensweise zur Konfiguration

1. Aktivieren Sie das Optionskästchen "Ring Redundancy".
2. Wählen Sie die Redundanzbetriebsart aus.
3. Legen Sie die Ring-Ports fest.
4. Klicken Sie auf die Schaltfläche "Set Values".

Werkseinstellungen wiederherstellen

EtherNet/IP-Varianten

Wenn Sie die Werkseinstellungen (Restore Factory Defaults) wiederherstellen, dann ist die Ringredundanz deaktiviert und die Ringport-Einstellungen sind zurückgesetzt. RSTP ist aktiviert.

PROFINET-Varianten

Wenn Sie die Werkseinstellungen (Restore Factory Defaults) wiederherstellen, dann ist die Ringredundanz aktiviert. Mit dem Zurücksetzen auf Werkseinstellungen werden auch die Ringport-Einstellungen zurückgesetzt. Wenn Sie vor dem Zurücksetzen andere Ports als Ringports verwendet haben, dann kann ein zuvor korrekt konfiguriertes Gerät kreisende Telegramme und damit den Ausfall des Datenverkehrs verursachen.

Zustand der Ring-Ports beim Redundanzmanager tauschen (HRP)

Wenn Sie einen Redundanzmanager konfigurieren, stellen Sie den Zustand der Ring-Ports fest ein. Der erste Ring-Port geht in den Zustand "blocking" und der zweite Ring-Port in den Zustand "forwarding". Bei aktivierter Ringredundanz können Sie den Zustand dieser Ring-Ports tauschen.

Hinweis

Achten Sie darauf, dass Sie zunächst den Ring öffnen, damit es nicht zu kreisenden Telegrammen kommt.

Ring-Ports ändern

Um die Ring-Ports zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie den Ring.
2. Wählen Sie die neuen Ring-Ports aus.
3. Stecken Sie die Kabel um.
4. Schließen Sie den Ring.

5.5.7.2 Standby

Redundante Kopplung von Ringen

Die Standby-Redundanz erlaubt die redundante Kopplung von HRP-Ringen.

Um eine Standby-Verbindung zu etablieren, konfigurieren Sie innerhalb eines Rings zwei benachbarte Geräte als Standby-Master bzw. Standby-Slave. Der Standby-Master und der Standby-Slave müssen über parallele Leitungen mit zwei Geräten in einem anderen Ring verbunden werden.

Im ungestörten Zustand laufen Nachrichten zwischen den beiden Ringen über den Master. Wenn die Leitung des Masters gestört wird, übernimmt der Slave die Weiterleitung von Nachrichten zwischen beiden Ringen.

Aktivieren sie die Standby-Redundanz für beide Standby-Partner und wählen Sie, über welche Ports das Gerät mit den zu koppelnden Ringen verbunden ist.

Als "Standby Connection Name" muss für beide Partner ein eindeutiger Name im Ring vergeben werden, mit dem die beiden zusammengehörenden Geräte als Standby-Partner identifiziert werden.

Hinweis

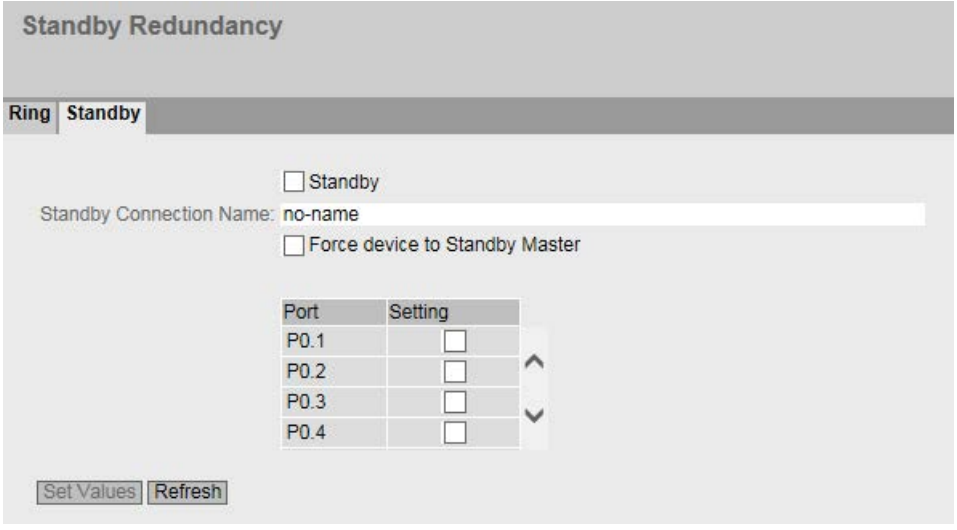
Um die Funktion nutzen zu können, muss HRP aktiviert sein.

Der Standby Manager erfordert immer einen aktivierten HRP-Client oder HRP-Manager.

Hinweis

Standby-Master-Kopplung mit optischer 100 MBit/s-Verbindung

Während der Koppelpartner eines Standby-Masters mit einer optischen 100 MBit/s-Verbindung wieder anläuft, trennen Sie die Verbindung zwischen dem Standby-Master und seinem Koppelpartner physikalisch.



Beschreibung der angezeigten Felder

- **Standby**
  Klicken Sie auf das Optionskästchen, um die Funktion ein- bzw. auszuschalten.
- **Standby Connection Name**
  Durch diesen Namen wird das Master-/Slave-Gerätepaar definiert. Beide Geräte müssen im gleichen Ring liegen.

  Tragen Sie hier den Namen für die Standby-Verbindung ein. Dieser muss identisch sein mit dem beim Standby-Partner eingetragenen Namen. Der Name kann frei gewählt werden, darf im ganzen Netz jedoch nur für ein Gerätepaar verwendet werden.
- **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, für die der Standby-Manager eingeschaltet ist, dieses Optionskästchen markiert ist, dann übernimmt im fehlerfreien Zustand das Gerät mit der höheren MAC-Adresse die Funktion des Standby-Masters.
  - Wenn diese Option bei beiden Geräten ausgewählt ist, oder wenn die Eigenschaft "Force device to Standby Master" nur von einem Gerät unterstützt wird, dann wird der Standby-Master ebenfalls anhand der MAC-Adresse ausgewählt.

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

  Hinweis

  Sind zwei Geräte über Standby-Funktion gekoppelt, muss die Funktion "Standby" an beiden Geräten aktiviert sein.

- **Standby Port**
  Wählen Sie aus, welcher Port Standby-Port ist. Über den Standby-Port erfolgt die Kopplung zum anderen Ring.

  Der Standby-Port ist an der Umleitung des Datenverkehrs beteiligt. Im ungestörten Fall ist nur der Standby-Port des Master aktiv und übernimmt den Datenverkehr in den angeschlossenen HRP-Ring bzw. HRP-Linie.

  Wenn der Master oder die Ethernet-Verbindung (Link) eines Standby-Port des Master ausfällt, dann wird der Standby-Port des Master abgeschaltet und der Standby-Port des Slave aktiviert. Damit wird wieder eine funktionierende Ethernet-Verbindung in das angeschlossene Netzsegment (HRP-Ring bzw. HRP-Linie) hergestellt.

5.5.8 Spanning Tree

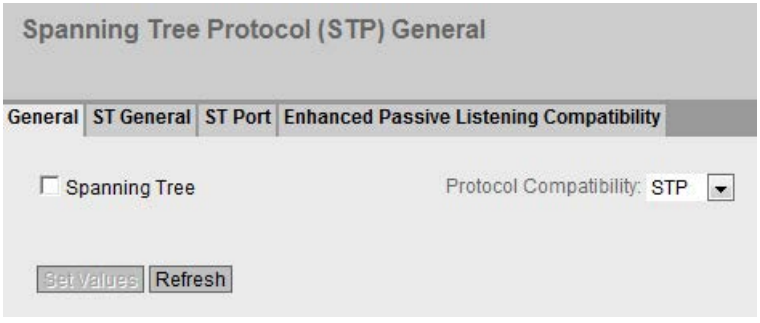
5.5.8.1 General

Allgemeine Einstellungen von STP

Dies ist die Basisseite zu Spanning Tree. Wählen Sie aus der Klappliste den Kompatibilitätsmodus aus. Standardmäßig ist Rapid Spanning Tree aktiviert.

In der jeweiligen Konfigurationsseite der Funktionen sind weitere Einstellungen möglich.

Je nach Kompatibilitätsmodus können Sie in der jeweiligen Konfigurationsseite die entsprechende Funktion konfigurieren.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Spanning Tree**
  Aktivieren oder deaktivieren Sie Spanning Tree.
- **Protocol Compatibility**
  Wählen Sie den Kompatibiltätsmodus von STP aus.

  Folgende Einstellungen gibt es:

  – STP

  – RSTP

Vorgehensweise zur Konfiguration

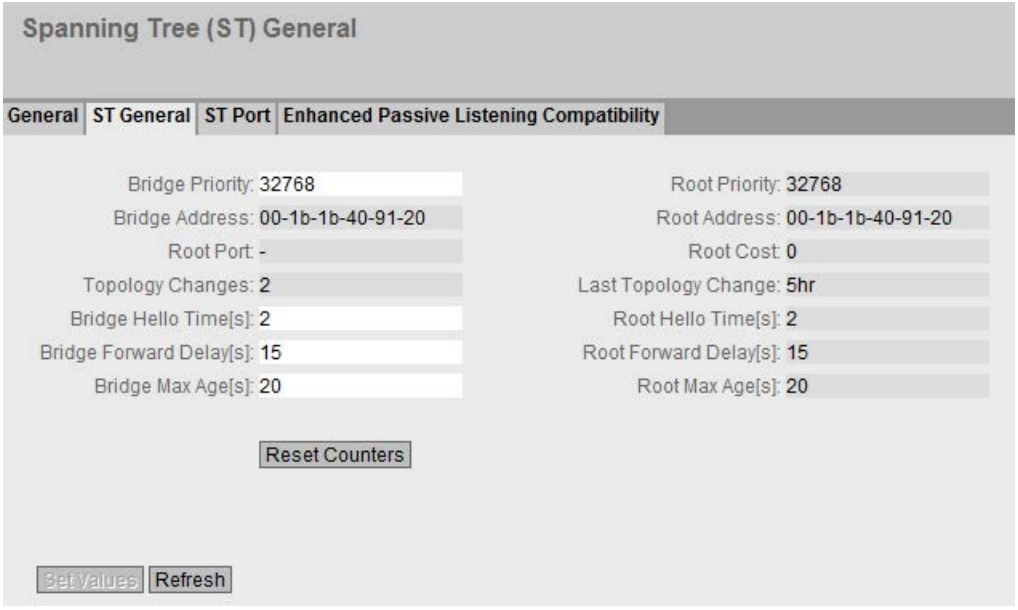
1. Aktivieren Sie das Optionskästchen "Spanning Tree".
2. Wählen Sie aus der Klappliste "Protocol Compatibility" die Kompatibilitätsart aus.
3. Klicken Sie auf die Schaltfläche "Set Values".

5.5.8.2 ST General

Konfiguration von Spanning Tree

Die Seite besteht aus folgenden Teilen.

- Der linke Teil der Seite zeigt die Konfiguration des Geräts.
- Der mittlere Teil zeigt die Konfiguration der Root-Bridge, wie sie aus Spanning Tree-Telegrammen abgeleitet werden kann, die ein Gerät empfangen hat.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Bridge Priority / Root Priority**
  Anhand der Bridge Priority wird festgelegt, welches Gerät Root Bridge wird. Die Bridge mit der höchsten Priorität wird Root Bridge. Je kleiner der Wert, desto höher die Priorität. Wenn in einem Netz mehrere Geräte die gleiche Priorität besitzen, wird das Gerät Root-Bridge, dessen MAC-Adresse den niedrigsten Zahlenwert hat. Beide Parameter, Bridge Priority und MAC-Adresse, bilden zusammen die Bridge-Kennung. Da die Root Bridge alle Wegeänderungen verwaltet, sollte sie wegen der Laufzeit der Telegramme möglichst zentral angeordnet sein. Der Wert für die Bridge Priority ist ein ganzzahliges Vielfaches von 4096 mit einem Wertebereich von 0 bis 61440.
- **Bridge Adresse / Root Adresse**
  Die Bridge Adresse zeigt die MAC-Adresse des Geräts und die Root-Adresse zeigt die MAC-Adresse der Root-Bridge an.
- **Root Port**
  Zeigt den Port an, über den der Switch mit der Root-Bridge kommuniziert.
- **Root Cost**
  Die Pfadkosten von diesem Gerät bis zur Root-Bridge.

- **Topologie Changes / Last Topology Change**
  Die Angabe für das Gerät nennt die Zahl der Umkonfigurationen aufgrund des Spanning Tree-Mechanismus seit dem letzten Hochlauf. Für die Root-Bridge wird die Zeitdauer seit der letzten Umkonfiguration wie folgt angezeigt:
  - 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 Konfigurationstelegramme (BPDUs). Der Zeitabstand zwischen zwei solchen Telegrammen ist die Hello-Time. Der Standardwert für diesen Parameter beträgt 2 Sekunden.
- **Bridge Forward Delay[s] / Root Forward Delay[s]**
  Neue Konfigurationsinformationen werden von einer Bridge nicht sofort, sondern erst nach dem im Parameter Weiterleitungsverzögerung festgelegten Zeitraum angewendet. So wird sichergestellt, dass der Betrieb entsprechend der neuen Topologie erst gestartet wird, wenn alle Bridges die notwendigen Informationen haben. Der Standardwert 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 Standardwert für diesen Parameter beträgt 20.
- **Reset Counters**

  Klicken Sie auf diese Schaltfläche, um die Zähler auf dieser Seite zurückzusetzen.

Vorgehensweise zur Konfiguration

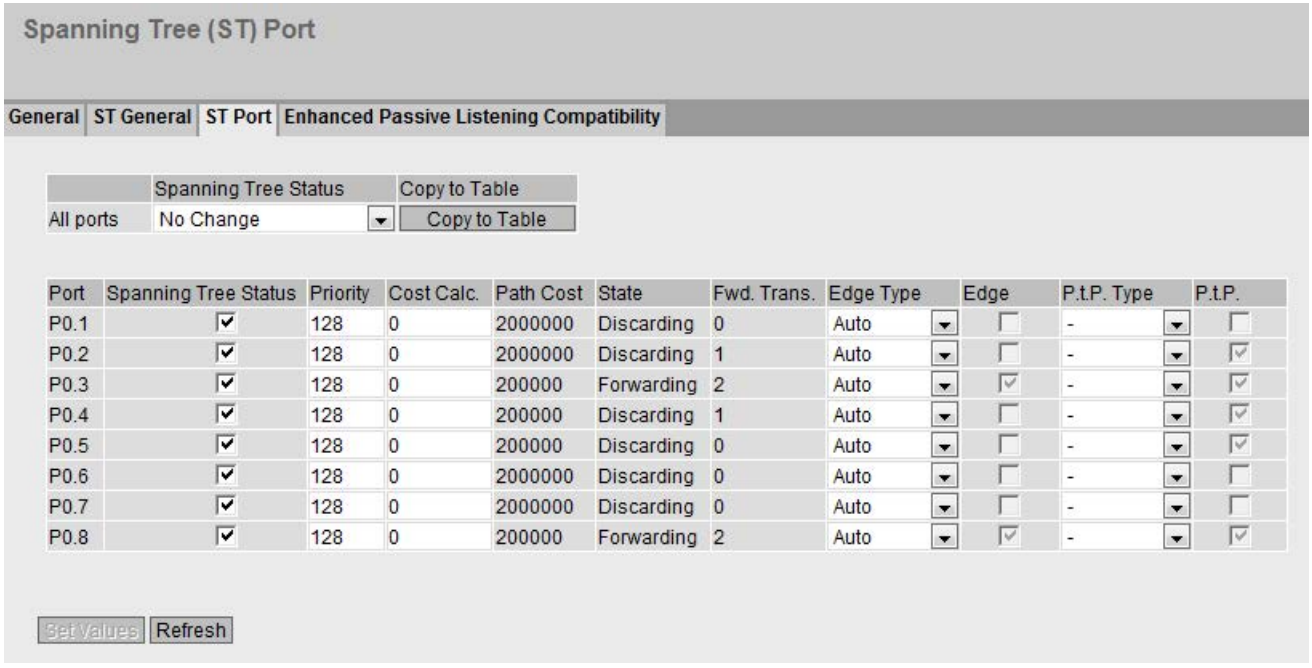
1. Tragen Sie in die Eingabefelder die für die Konfiguration benötigten Daten ein.
2. Klicken Sie auf die Schaltfläche "Set Values".

5.5.8.3 ST Port

Konfiguration der STP-Ports

In der Tabelle wird beim Aufruf der Seite der aktuelle Stand der Konfiguration der Port-Parameter angezeigt.

Klicken Sie zur Konfiguration in die entsprechenden Felder der Port-Tabelle.



Beschreibung der angezeigten Felder

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Spanning Tree Status**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - enabled
    Port ist im Spanning-Tree integriert.
  - disabled
    Port ist im Spanning-Tree nicht integriert.
  - No Change
    Tabelle 2 bleibt unverändert.
- **Copy to Table**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt alle verfügbaren Ports an.
- **Spanning Tree Status**
  Legen Sie fest, ob der Port im Spanning-Tree integriert ist oder nicht.

  Hinweis

  Wenn Sie die Option "Spanning Tree Status" für einen Port deaktivieren, kann es zur Schleifenbildung kommen. Die Topologie muss beachtet werden.

- **Priority**
  Tragen Sie die Priorität des Ports ein. Die Priorität wird nur ausgewertet, wenn die Pfadkosten gleich sind.
  Der Wert muss durch 16 teilbar sein. Wenn der Wert nicht durch 16 teilbar ist, wird der Wert automatisch angepasst.
  Wertebereich: 0 - 240.
  Der Standardwert ist 128.
- **Cost Calc.**
  Tragen Sie die Wegekostenberechnung ein. Wenn Sie den Wert "0" eintragen, wird im Feld "Path Cost" der automatisch ermittelte Wert angezeigt.
- **Path Cost**
  Dieser Parameter dient zur Berechnung des zu wählenden Weges. Die Strecke mit dem geringsten Wert wird als Weg ausgewählt. Haben mehrere Ports eines Geräts den gleichen Wert bei gleichen Pfadkosten, wird der Port mit der niedrigsten Portnummer ausgewählt.
  Wenn im Feld "Cost Calc" der Wert "0" ist, so wird der automatisch ermittelte Wert angezeigt.
  Im anderen Fall wird der Wert des Feldes "Cost Calc" angezeigt.
  Die Ermittlung der Wegekosten richtet sich maßgeblich nach der Übertragungsgeschwindigkeit. Je höher die erzielbare Übertragungsgeschwindigkeit ist, umso kleiner ist der Wert für die Wegekosten.

  Typische Werte für Wegekosten bei Rapid Spanning Tree:

  – 10.000 Mbit/s = 2.000
  – 1000 Mbit/s = 20.000
  – 100 Mbit/s = 200.000
  – 10 Mbit/s = 2.000.000

  Die Werte können aber auch individuell parametriert werden.

- **State**
  Zeigt den momentanen Status an, in dem sich der Port befindet. Die Werte werden nur angezeigt und können nicht parametriert werden. Der Parameter "Status" ist abhängig von dem projektierten Protokoll. Beim Status ist Folgendes möglich:
  - Disabled
    Der Port empfängt nur und nimmt nicht am STP und RSTP teil.
  - Discarding
    In der Betriebsart "Discarding" werden BPDU-Telegramme empfangen. Andere aus- oder eingehende Telegramme werden verworfen.
  - Listening
    In diesem Status werden sowohl BPDU-Telegramme empfangen als auch gesendet. Der Port ist in den Spanning Tree-Algorithmus einbezogen.
  - Learning
    Vorstufe zum Weiterleitungsstatus, der Port lernt aktiv die Topologie (d. h. die Teilnehmeradressen).
  - Forwarding
    Der Port ist nach der Umkonfigurationszeit aktiv im Netz, er empfängt und sendet Datentelegramme.
- **Fwd. Trans**
  Gibt die Anzahl der Wechsel vom Status "Discarding" zum Status "Forwarding" an.
- **Edge Type**
  Legen Sie die Art des Edge Port fest. Sie haben folgende Möglichkeiten:
  - "-"
    Edge Port ist deaktiviert. Der Port wird wie ein "no EdgePort" behandelt.
  - Admin
    Wählen Sie diese Option, wenn sich an diesem Port ein immer Endgerät befindet. Sonst wird bei jeder Verbindungsänderung eine Rekonfiguration des Netzwerks ausgelöst.
  - Auto
    Wählen Sie diese Option, wenn an diesem Port automatisch erkannt werden soll, ob ein Endgerät angeschlossen ist. Beim ersten Verbindungsaufbau wird der Port wie ein "no Edge Port" behandelt.
  - Admin/Auto
    Wählen Sie diese Optionen, wenn Sie an diesem Port eine Kombination aus beiden betreiben. Beim ersten Verbindungsaufbau wird der Port als Edge Port behandelt.
- **Edge**
  Zeigt an, in welchem Status der Port ist.
  - Aktiviert
    An diesem Port befindet sich ein Endgerät.
  - Deaktiviert
    An diesem Port befindet sich ein Spanning Tree- oder Rapid Spanning Tree-Gerät.

  Bei einem Endgerät kann ein Switch ohne Rücksicht auf Spanning Tree-Telegramme schneller den Port umschalten. Wird entgegen dieser Einstellung ein Spanning Tree-Telegramm empfangen, wechselt der Port automatisch auf die Einstellung "Deaktiviert" für Switches.

- **P.t.P. Type**
  Wählen Sie in der Klappliste die gewünschte Option aus. Die Auswahl ist abhängig vom eingestellten Port.
  - "-"
    Punkt zu Punkt wird automatisch ermittelt. Steht der Port auf Halbduplex, wird nicht von einer Punkt zu Punkt-Verbindung ausgegangen.
  - P.t.P.
    Auch bei Halbduplex wird von einer Punkt zu Punkt-Verbindung ausgegangen.
  - Shared Media
    Auch bei einer Vollduplexverbindung wird nicht von einer Punkt zu Punkt-Verbindung ausgegangen.

  Hinweis

  Punkt zu Punkt-Verbindung bedeutet eine direkte Verbindung zwischen zwei Geräten. Eine Shared Media-Verbindung ist z.B. eine Verbindung zu einem Hub.

- **P.t.P.**
  Aktivieren oder deaktivieren Sie P.t.P.

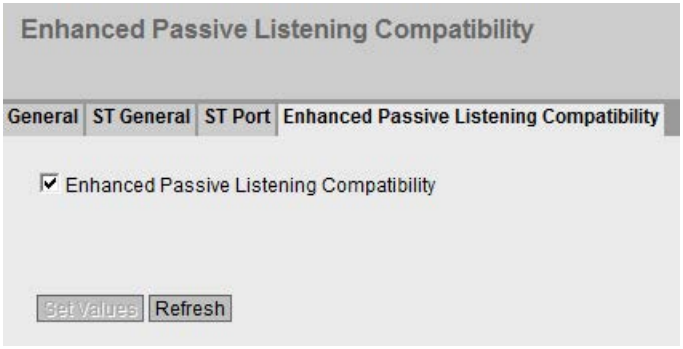
Vorgehensweise zur Konfiguration

1. Tragen Sie in den Eingabefeldern der Tabellenzeile des zu konfigurierenden Ports die Werte ein.
2. Wählen Sie aus den Klapplisten der Felder der Tabellenzeile des zu konfigurierenden Ports die Werte aus.
3. Klicken Sie auf die Schaltfläche "Set Values".

5.5.8.4 Enhanced Passive Listening Compatibility

Aktivieren der Funktion

Auf dieser Seite können Sie die Funktion Enhanced Passive Listening Compatibility aktivieren.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

- **Enhanced Passive Listening Compatibility**
  Aktivieren oder deaktivieren Sie diese Funktion für das gesamte Gerät.

Vorgehensweise zur Konfiguration

1. Aktivieren oder deaktivieren Sie "Enhanced Passive Listening Compatibility"
2. Klicken sie auf die Schaltfläche "Set Values"

5.5.9 Loop Detection

Mit der Funktion "Loop Detection" legen Sie fest, für welche Ports Schleifenerkennung aktiviert werden soll. Von den betreffenden Ports werden spezielle Testtelegramme, die Loop-Detection-Telegramme gesendet. Wenn diese Telegramme wieder zum Gerät zurück gesendet werden, dann liegt eine Schleife ("Loop") vor.

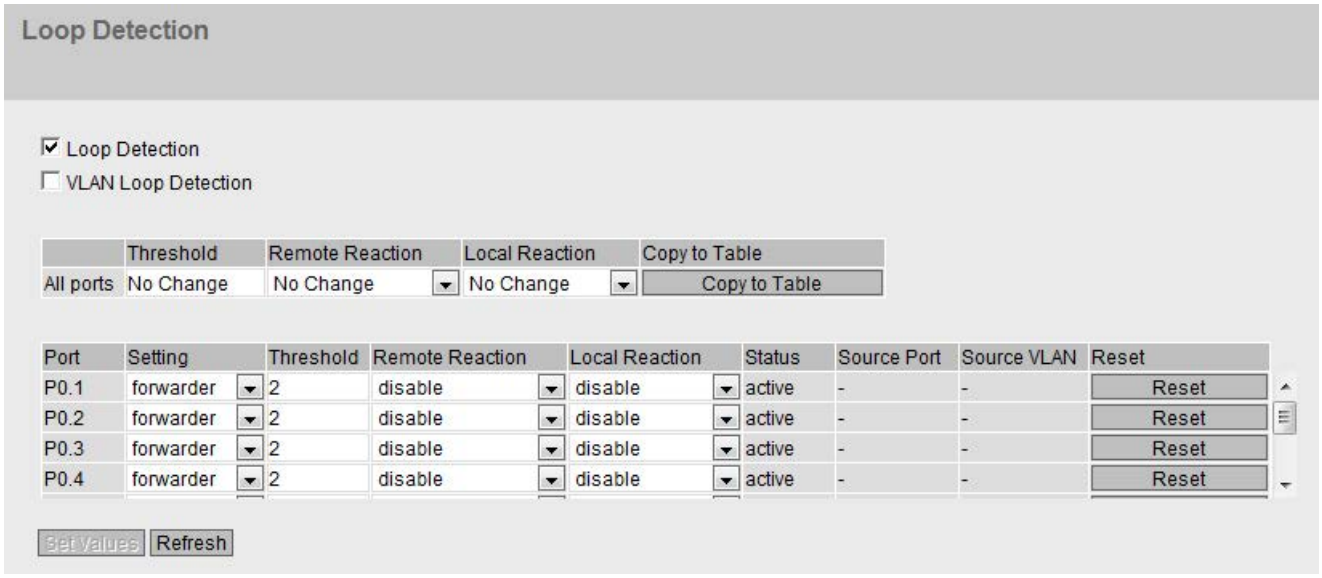
Von einem "Local Loop" unter Beteiligung dieses Gerätes spricht man, wenn die Telegramme an einem anderen Port desselben Gerätes wieder empfangen werden. Wenn die ausgesendeten Telegramme wieder am gleichen Port empfangen werden, ist eine Schleife "Remote Loop" an anderen Netzkomponenten aufgetreten.

Hinweis

Eine Schleife ist ein Fehler im Netzaufbau, der beseitigt werden muss. Die Schleifenerkennung kann helfen, den Fehler schneller zu finden, behebt ihn jedoch nicht. Die Schleifenerkennung ist nicht dazu geeignet, die Netzwerkverfügbarkeit durch den gezielten Einbau von Schleifen zu erhöhen.

Hinweis

Beachten Sie, dass die Schleifenerkennung nur auf Ports möglich ist, die nicht als Ring-Port oder Standby-Port konfiguriert wurden.



Beschreibung

- **Loop Detection**
  Aktivieren oder deaktivieren Sie die Schleifenerkennung.
- **VLAN Loop Detection**
  Aktivieren oder deaktivieren Sie die Schleifenerkennung bei VLAN.

Die Tabelle 1 enthält folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind
- **Threshold / Remote Reaction / Local Reaction**
  Legen Sie die gewünschten Einstellungen fest.
- **Copy to table**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen

Die Tabelle 2 enthält folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an.
- **Setting**
  Legen Sie fest, wie der Port mit Loop-Detection-Telegrammen verfahren soll. Wählen Sie aus der Klappliste eine der folgenden Optionen:

  Hinweis

  Durch die Testtelegramme entsteht zusätzliche Netzlast. Wir empfehlen, nur einzelne Switches, z. B. an den Abzweigungen vom Ring, als "Sender" zu konfigurieren und die anderen als "Forwarder".

  – sender
    Loop-Detection-Telegramme werden ausgesendet und weitergeleitet.
  – forwarder
    Loop-Detection-Telegramme von anderen Geräten werden weitergeleitet.
  – blocked
    Die Weiterleitung der Loop-Detection-Telegramme wird blockiert.
- **Threshold**
  Legen Sie durch Eingabe einer Zahl fest, nach wie vielen empfangenen Loop-Detection-Telegrammen von einer Schleife ausgegangen wird.
- **Remote Reaction**
  Legen Sie fest, wie der Port bei Auftreten einer Remote-Loop reagieren soll. Wählen Sie aus der Klappliste eine der beiden Optionen:
  – keine Aktion: Eine Schleife hat keine Auswirkungen auf den Port.
  – deaktivieren: Der Port wird geblockt.
- **Local Reaction**
  Legen Sie fest, wie der Port bei Auftreten eines Local Loop reagieren soll. Wählen Sie aus der Klappliste eine der beiden Optionen:
  – keine Aktion: Eine Schleife hat keine Auswirkungen auf den Port.
  – deaktivieren: Der Port wird geblockt
- **Status**
  Zeigt an, ob die Schleifenerkennung für diesen Port ein- oder ausgeschaltet ist.
- **Source-Port**
  Zeigt den Empfänger-Port des Loop-Detection-Telegramms an, das die letzte Reaktion ausgelöst hat.
- **Source-VLAN**
  Dieses Feld zeigt die VLAN-ID des Loop-Detection-Telegramms an, das die letzte Reaktion ausgelöst hat.
  Voraussetzung dafür ist, dass zuvor "VLAN Support Enabled" auf der Seite "Loop Detection Configuration" aktiviert wurde.
- **Reset**
  Nachdem eine Schleife im Netzwerk beseitigt wurde, klicken Sie auf diese Schaltfläche "Zähler zurücksetzen", um den Port wieder zurückzusetzen.

Änderung des konfigurierten Port-Status durch Loop Detection

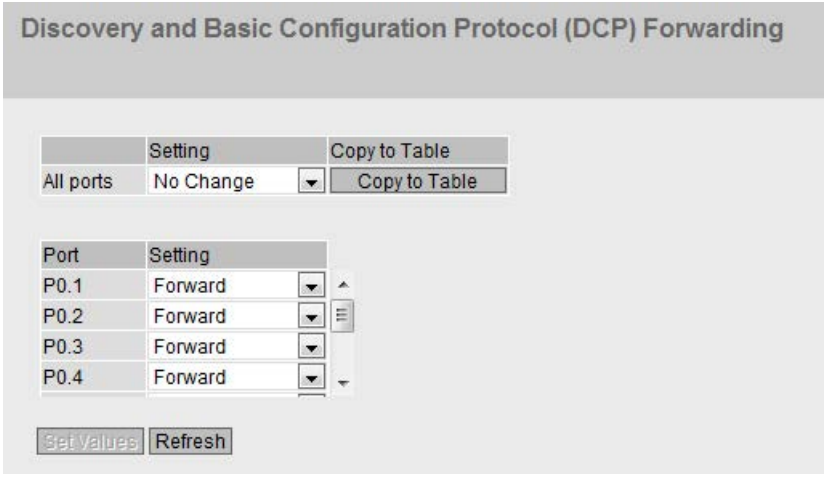
Die Konfiguration des Port-Status kann durch die Funktion "Loop Detection" verändert werden. Wenn der Administrator z. B. einen Port deaktiviert hat (disabled), kann der Port nach einem Geräteneustart durch „Loop Detection“ wieder aktiviert werden (enabled). Der Port-Status „Link-down“ wird durch „Loop Detection“ nicht verändert.

5.5.10 DCP Forwarding

Anwendungen

Das DCP-Protokoll wird von STEP 7 und dem PST-Tool für die Konfiguration und Diagnose verwendet. In der Werkseinstellung ist DCP auf allen Ports aktiviert, d.h. empfangene DCP-Telegramme werden auf allen Ports weitergeleitet. Mit dieser Option haben Sie die Möglichkeit das Aussenden der Telegramme für einzelne Ports auszuschalten, um z.B. einzelne Netzbereiche von der Konfiguration per PST-Tool abzuschotten, bzw. um das gesamte Netz in kleinere Teilnetze für die Konfiguration und Diagnose zu unterteilen.

Auf dieser Seite werden alle Ports des Gerätes angezeigt. Hinter jedem angezeigten Port befindet sich eine Klappliste zur Funktionsauswahl.



Beschreibung der angezeigten Werte

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Setting**
  Wählen Sie aus der Klappliste die Einstellung. Wenn "No Change" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **Copy to Table**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeigt die verfügbaren Ports an. Der Port setzt sich aus der Modulnummer und der Portnummer zusammen, z. B. Port 0.1 ist Modul 0, Port 1.
- **Setting**
  Wählen Sie aus der Klappliste aus, ob der Port DCP-Telegramme ausgangsseitig blocken oder weiterleiten soll. Sie haben die folgenden Möglichkeiten zur Auswahl:
  - **Forward**
    An diesem Port werden DCP-Telegramme weitergeleitet.
  - **Block**
    An diesem Port werden ausgangsseitig keine DCP-Telegramme weitergeleitet. Ein Empfangen ist jedoch über diesen Port weiterhin möglich.

Vorgehensweise zur Konfiguration

1. Wählen Sie aus den Optionen der Klappliste in der Zeile hinter der Portnummer aus, welche Ports den DCP-Versand unterstützen sollen.
2. Klicken Sie auf die Schaltfläche "Set Values".

5.5.11 LLDP

Bestimmung der Netzwerktopologie

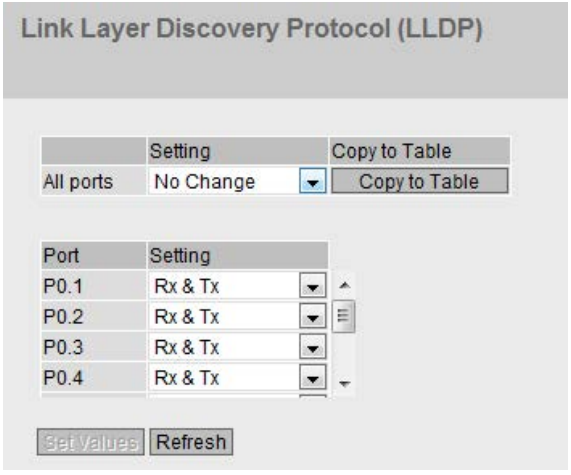
LLDP (Link Layer Discovery Protocol) ist im Standard IEEE 802.AB definiert.

LLDP ist ein Verfahren zur Bestimmung der Netzwerktopologie. Netzwerkkomponenten tauschen über LLDP Informationen mit ihren Nachbargeräten aus.

Netzwerkkomponenten, die LLDP unterstützen, verfügen über einen LLDP-Agenten. Der LLDP-Agent versendet in periodischen Abständen Informationen über sich selbst und empfängt Informationen von angeschlossenen Geräten. Die empfangenen Informationen werden in der MIB gespeichert.

Anwendungen

PROFINET benutzt LLDP für die Topologie-Diagnose. In der Werkseinstellung ist LLDP für alle Ports aktiviert, d. h. es werden LLDP-Telegramme auf allen Ports gesendet und empfangen. Mit dieser Funktion haben Sie die Möglichkeit das Aussenden und/oder Empfangen pro Port ein- oder auszuschalten.



Beschreibung der angezeigten Felder

Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports gültig sind.
- **Setting**
  Wählen Sie aus der Klappliste die Einstellung. Wenn "No Change" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.
- **Copy to Table**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Zeig den Port an.
- **Setting**
  Wählen Sie aus der Klappliste aus, ob der Port LLDP-Telegramme senden oder empfangen soll. Sie haben die folgenden Möglichkeiten zur Auswahl:
  - Rx
    Dieser Port kann LLDP-Telegramme nur empfangen.
  - Tx
    Dieser Port kann LLDP-Telegramme nur senden.
  - Rx & Tx
    Dieser Port kann LLDP-Telegramme empfangen und senden.
  - "-" (Deaktiviert)
    Dieser Port kann LLDP-Telegramme weder empfangen noch senden.

Vorgehensweise zur Konfiguration

1. Wählen Sie aus der Klappliste der Zeile des Ports, den Sie konfigurieren wollen die LLDP-Funktionalität aus.
2. Klicken Sie auf die Schaltfläche "Set Values".

5.5.12 Unicast

5.5.12.1 Filtering

Adressfilterung

Diese Tabelle zeigt die Quelladressen von Unicast-Adresstelegrammen, die statisch durch Parametrierung des Anwenders eingetragen wurden.

Auf dieser Seite definieren Sie auch die statischen Unicast-Filter.

Abhängigkeit vom "Base Bridge Mode"

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

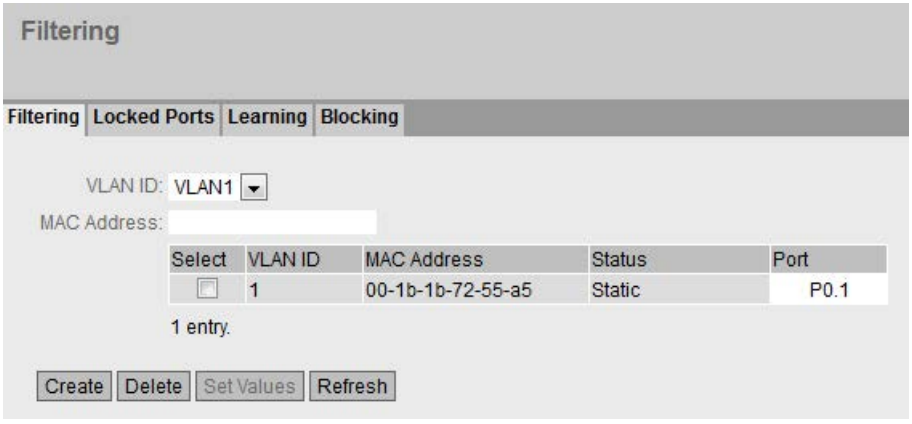


Bild 5-4 Base Bridge Mode: 802.1Q VLAN Bridge

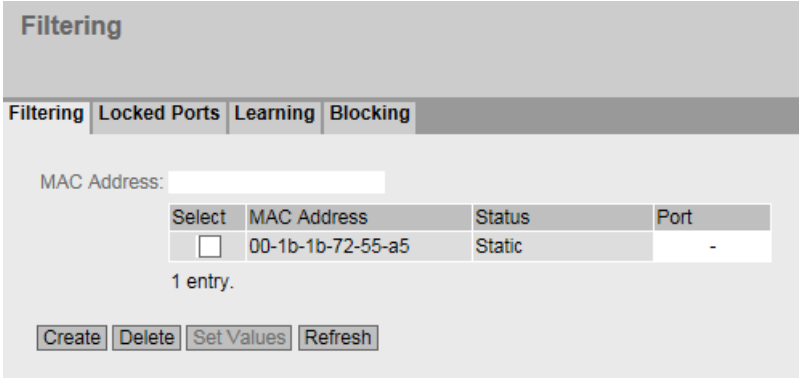


Bild 5-5 Base Bridge Mode: 802.1D Transparent Bridge

Beschreibung der angezeigten Felder

Die Seite kann folgende Felder enthalten:

- **VLAN ID**

  Wählen Sie die VLAN ID aus, in dem Sie eine neue MAC-Adresse statisch konfigurieren. Wenn nichts vorgegeben wird, ist "VLAN1" als Grundeinstellung parametriert.

- **MAC Address**
  Tragen Sie hier die MAC-Adresse ein.

Die Tabelle enthält folgende Spalten:

- **Select**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **VLAN ID**
  Zeigt die VLAN ID, die dieser MAC-Adresse zugeordnet ist.
- **MAC Address**
  Zeigt die MAC-Adresse des Teilnehmers, die das Gerät gelernt hat oder die der Anwender projektiert hat.
- **Status** - Static
  Zeigt den Status jedes Adress-Eintrags. Die Adresse wurde vom Anwender statisch eingetragen. Statische Adressen sind permanent gespeichert, d.h. sie werden nicht nach Ablauf der Aging-Time oder beim Neustart des Geräts gelöscht. Sie müssen vom Anwender gelöscht werden.
- **Port**

  Zeigt an, über welchen Port der Teilnehmer mit der angegebenen Adresse erreichbar ist. Vom Gerät empfangene Telegramme, deren Zieladresse mit dieser Adresse übereinstimmen, werden an diesen Port weitergegeben.

  Hinweis

  Für Unicast-Adressen können Sie nur **einen** Port angeben.

Vorgehensweise zur Konfiguration

Zur Bearbeitung der Einträge gehen Sie folgendermaßen vor.

Neuen Eintrag erstellen

1. Wählen Sie im "Base Bridge Mode: 802.1Q VLAN Bridge" die entsprechende VLAN ID aus.
2. Geben Sie die MAC-Adresse in das Eingabefeld "MAC Address" ein.
3. Klicken Sie auf die Schaltfläche "Create", um einen neuen Eintrag in der Tabelle zu erstellen.
4. Klicken Sie auf die Schaltfläche "Refresh".
5. Wählen Sie aus der Klappliste den entsprechenden Port aus.
6. Klicken Sie auf die Schaltfläche "Set Values".

Eintrag ändern

1. Wählen Sie den entsprechenden Port aus.
2. Klicken Sie auf die Schaltfläche "Set Values".

Eintrag Löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
   Wiederholen Sie den Vorgang für alle Einträge, die Sie löschen wollen.
2. Um die selektierten Einträge aus der Filtertabelle zu löschen, klicken Sie auf die Schaltfläche "Delete".
3. Klicken Sie auf die Schaltfläche "Refresh".

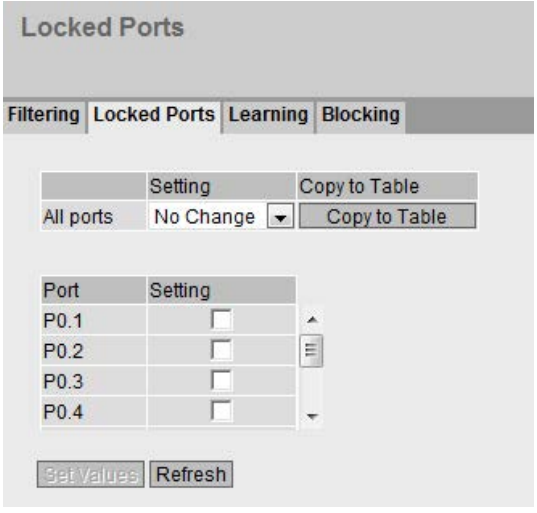
5.5.12.2 Locked Ports

Aktivierung der Zugangskontrolle

Auf dieser Seite können Sie einzelne Ports für unbekannte Teilnehmer sperren.

Wenn die Port Lock-Funktion aktiviert ist, werden Pakete an diesem Port, die von unbekannten MAC-Adressen kommen, sofort verworfen. Die Pakete von bekannten Teilnehmern werden vom Port angenommen.
Da Ports mit aktivierter Port Lock-Funktion auch keine MAC-Adressen lernen, werden gelernte Adressen auf diesen Ports nach Aktivieren der Port Lock-Funktion automatisch ausgetragen.
Der Port akzeptiert nur statische MAC-Adressen, die vorher entweder manuell oder mit der "Start Learning"-Funktion und der "Stop learning"-Funktion erstellt wurden.

Um alle angeschlossenen Teilnehmer automatisch einzutragen, gibt es eine Funktion zum automatischen Lernen (siehe " Layer 2 > Unicast > Learning").



Beschreibung der angezeigten Felder

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Setting**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - enabled
    Aktiviert die Port Lock-Funktion.
  - disabled
    Deaktiviert die Port Lock-Funktion.
  - No Change
    Tabelle 2 bleibt unverändert.
- **Copy to Table**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  In dieser Spalte werden alle in diesem Gerät verfügbaren Ports aufgeführt.
- **Optionskästchen "Setting"**
  Aktivieren oder deaktivieren Sie die Zugriffsteuerung für den Port.

Vorgehensweise zur Konfiguration

Zugriffssteuerung für einen einzelnen Port aktivieren

1. Aktivieren Sie in der Tabelle 2 in der entsprechenden Zeile das Optionskästchen.
2. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Set Values".

Zugriffssteuerung für alle Ports aktivieren

1. Wählen in der Klappliste "Setting" den Eintrag "enabled".
2. Klicken Sie auf die Schaltfläche "Copy to Table". In der Tabelle 2 wird bei allen Ports das Optionskästchen aktiviert.
3. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Set Values".

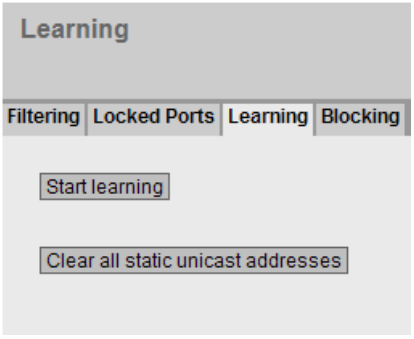
5.5.12.3 Learning

Lernen starten/stoppen

Mit Hilfe des Automatischen Lernens können alle angeschlossenen Geräte automatisch in die Unicast Filter Tabelle eingetragen werden. Solange die "Start learning"-Funktion aktiviert ist, werden alle gelernten Unicast-Adressen sofort als statische Unicast-Einträge angelegt. Der Lernvorgang wird erst wieder durch Klicken auf die Schaltfläche "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 des Lernens Pakete senden.
Durch anschließendes Aktivieren der Port Lock-Funktion werden auf den entsprechenden Ports nur noch Pakete von den nach Beendigung des Lernvorgangs bekannten Teilnehmern (statische Unicast-Einträge) angenommen.

Hinweis

Ist die Port Lock-Funktion auf einzelnen Ports bereits vor dem automatischen Lernen aktiv, werden auf diesen Ports keine Adressen gelernt. Auf diese Weise ist es möglich nur auf bestimmten Ports zu lernen. Aktivieren Sie hierzu vorher die Port Lock-Funktion auf den Ports, die keine Adressen lernen sollen.



Vorgehensweise zur Konfiguration

Adressen lernen

1. Klicken Sie auf die Schaltfläche "Start learning", um den Lernvorgang zu starten.
   Nach dem Starten des Lernvorgangs wird die Schaltfläche "Start learning" durch die Schaltfläche "Stop learning" ersetzt.
   Das Gerät trägt nun solange die Adressen angeschlossener Geräte ein, bis Sie den Vorgang anhalten.
2. Klicken Sie auf die Schaltfläche "Stop learning", um den Lernvorgang anzuhalten.
   Die Schaltfläche wird wieder durch die Schaltfläche "Start learning " ersetzt. Die gelernten Einträge werden gespeichert.

Alle statischen Unicast-Adressen löschen

1. Klicken Sie auf die Schaltfläche "Clear all static unicast addresses", um alle statischen Einträge zu löschen.
   In großen Netzen mit sehr vielen Teilnehmern kann das automatische Lernen eventuell zu vielen unerwünschten statischen Einträgen führen. Um diese nicht einzeln löschen zu müssen, gibt es über diese Schaltfläche die Möglichkeit, alle statischen Einträge zu löschen. Diese Funktion ist während des automatischen Lernens deaktiviert.

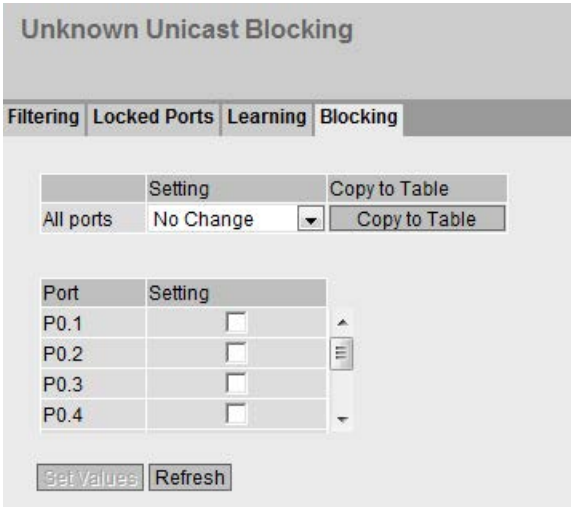
Hinweis

Das Löschen kann je nach Anzahl der Einträge einige Zeit in Anspruch nehmen.

5.5.12.4 Unicast Blocking

Weiterleitung von unbekannten Unicast-Telegrammen sperren

Auf der Seite wird das Weiterleiten von unbekannten Unicast-Telegrammen für einzelne Ports gesperrt.



Beschreibung der angezeigten Werte

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Setting**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - enabled
    Blocken von Unicast-Telegrammen ist aktiviert.
  - disabled
    Blocken von Unicast-Telegrammen ist deaktiviert.
  - No Change
    Tabelle 2 bleibt unverändert.
- **Copy to Table**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Alle verfügbaren Ports werden in dieser Spalte aufgeführt. Nicht verfügbare Ports werden nicht angezeigt.

  Hinweis

  Ringredundanz / Standby

  Wenn Ringredundanz oder Standby aktiviert sind, werden die hierfür konfigurierten Ports vom Unicast Blocking ausgenommen.

- **Setting**
  Aktivieren oder deaktivieren Sie das Sperren von Unicast-Telegrammen.

Vorgehensweise zu Konfiguration

Das Blocken für einen einzelnen Port aktivieren

1. Aktivieren Sie in der Tabelle 2 in der entsprechenden Zeile das Optionskästchen.
2. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Set Values".

Das Blocken für alle Ports aktivieren

1. Wählen in der Klappliste "Setting" den Eintrag "enabled".
2. Klicken Sie auf die Schaltfläche "Copy to Table". In der Tabelle 2 wird bei allen Ports das Optionskästchen aktiviert.
3. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Set Values".

5.5.13 Multicast

5.5.13.1 Groups

Multicast-Anwendungen

In der Mehrzahl der Fälle wird ein Telegramm mit einer Unicast-Adresse an einen bestimmten Empfänger gesendet. Wenn eine Anwendung die gleichen Daten an mehrere Empfänger senden soll, kann das zu sendende Datenvolumen reduziert werden, indem die Daten über eine Multicast-Adresse an alle gesendet werden. Für manche Anwendungen gibt es feste Multicast-Adressen (NTP, IETF1-Audio, IETF1-Video usw.).

Reduzierung der Netzlast

Im Gegensatz zu Unicast-Telegrammen bewirken Multicast-Telegramme eine höhere Last für das Gerät. Denn generell werden Multicast-Telegramme an allen Ports versendet. Es gibt folgende Möglichkeiten, die Last durch Multicast-Telegramme zu reduzieren:

- Statischer Eintrag der Adressen in die Multicast-Filtertabelle.
- Dynamischer Eintrag der Adressen durch Mithören von IGMP-Parametriertelegrammen (IGMP-Konfiguration).

Alle genannten Verfahren haben zur Folge, dass Multicast-Telegramme nur an solche Ports versendet werden, für die eine entsprechende Adresse eingetragen ist.

Der Menüpunkt "Multicast " zeigt die aktuell in der Filtertabelle eingetragenen Multicast-Telegramme mit ihren Zielports, die der Anwender parametriert hat (statisch).

Abhängigkeit vom "Base Bridge Mode"

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

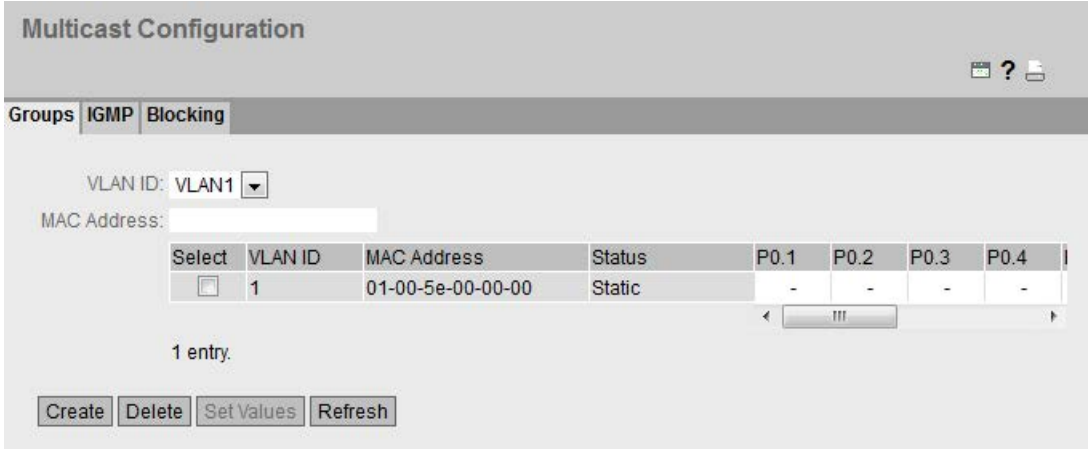


Bild 5-6 Base Bridge Mode: 802.1Q VLAN Bridge

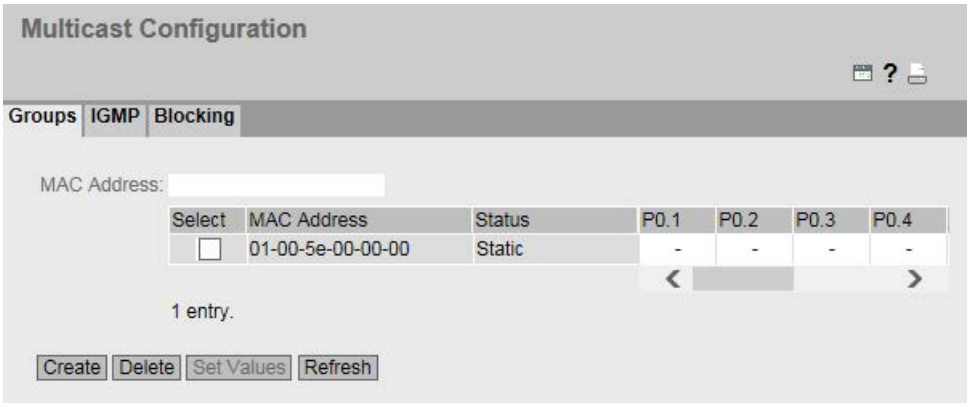


Bild 5-7 Base Bridge Mode: 802.1D Transparent Bridge

Beschreibung der angezeigten Felder

Die Seite kann folgende Felder enthalten:

- **VLAN ID**
  Wenn Sie auf dieses Textfeld klicken, wird Ihnen eine Klappliste angeboten. Hier können Sie die VLAN ID einer neu zu projektierenden MAC-Adresse auswählen.
- **MAC Address**
  Hier geben Sie eine neu zu projektierende MAC-Multicast-Adresse ein.

Die Tabelle gliedert sich in folgende Spalten:

- **Select**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **VLAN ID**
  Hier wird die VLAN ID des VLANs angezeigt, dem die MAC-Multicast-Adresse dieser Zeile zugeordnet ist.
- **MAC Address**
  Hier wird die MAC-Multicast-Adresse angezeigt, die das Gerät gelernt hat oder die der Anwender projektiert hat.

- **Status -** Static
  Zeigt den Status jedes Adress-Eintrags. Die Adresse wurde vom Anwender statisch eingetragen. Statische Adressen sind permanent gespeichert, d.h. sie werden nicht nach Ablauf der Aging-Time oder beim Neustart des Geräts gelöscht. Sie müssen vom Anwender gelöscht werden.
- **Liste der Ports**
  Für jeden Steckplatz gibt es eine Spalte. Innerhalb einer Spalte wird für jeden Port die Zugehörigkeit zur Multicast-Gruppe angegeben. Folgende Werte sind möglich:
  - M
    (Member) Über diesen Port werden Multicast-Telegramme gesendet.
  - F
    (Forbidden) Kein Mitglied der Multicast-Gruppe. Außerdem darf diese Adresse nicht dynamisch über IGMP gelernt werden.
  - I

    (IGMP) Mitglied der Multicast-Gruppe, die Registrierung erfolgte über ein IGMP-Telegramm. Dieser Wert wird nur dynamisch vergeben.
  - –
    Kein Mitglied der Multicast-Gruppe. Über diesen Port werden keine Multicast-Telegramme mit der definierten Multicast-MAC-Adresse gesendet.

Vorgehensweise zur Konfiguration

Neuen Eintrag erstellen

1. Wählen Sie im "Base Bridge Mode: 802.1Q VLAN Bridge" aus der Klappliste "VLAN ID" die gewünschte ID aus.
2. Tragen Sie in das Eingabefeld "MAC Address" die MAC-Adresse ein
3. Klicken Sie die Schaltfläche "Create". In der Tabelle wird ein neuer Eintrag erzeugt.
4. Weisen Sie der MAC-Adresse die entsprechenden Ports zu.
5. Klicken Sie auf die Schaltfläche "Set Values".

Eintrag löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Klicken Sie auf die Schaltfläche "Delete".
   Die Zeile wird aus der Anzeige und aus dem Speicher des Geräts gelöscht.

5.5.13.2 IGMP

Funktion

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

IGMP Snooping Aging Time

Mit diesem Menü können Sie die Aging-Time für die IGMP-Konfiguration festlegen. Nach Ablauf dieser Zeit werden durch IGMP erzeugte Einträge aus der Adresstabelle gelöscht, wenn diese nicht durch ein neues IGMP-Telegramm aktualisiert werden.

Die Festlegung gilt für alle Ports, eine portspezifische Konfiguration ist nicht möglich.

IGMP Snooping Aging Time in Anhängigkeit des Queriers

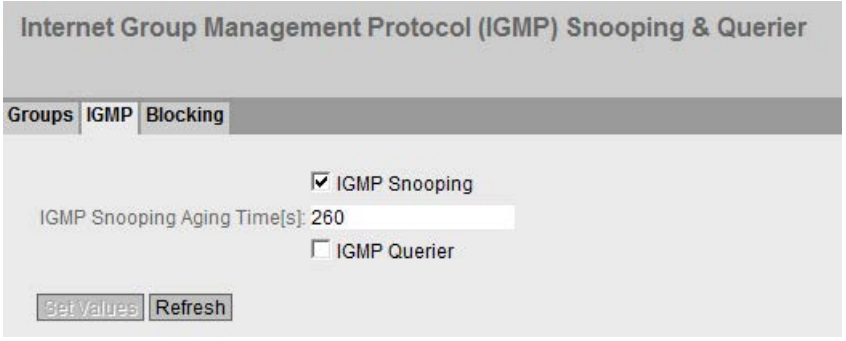
SCALANCE XB-200 als IGMP-Querier

Wenn ein SCALANCE XB-200 als IGMP-Querier verwendet wird, beträgt das Query-Intervall 125 Sekunden. Stellen Sie bei der "IGMP Snooping Aging Time" mindestens 250 Sekunden ein.

Andere IGMP-Querier

Wenn ein anderer IGMP-Querier verwendet wird, sollte der Wert der "IGMP Snooping Aging Time" mindestens doppelt so groß sein wie das Query-Intervall.

Beschreibung der angezeigten Felder



Die Seite enthält folgende Felder:

- **IGMP Snooping**
  Aktivieren oder deaktivieren Sie IGMP (Internet Group Management Protocol). Die Funktion ermöglicht die Zuordnung von IP-Adressen zu Multicast-Gruppen. Wenn die Option aktiviert ist, werden IGMP-Einträge in die Tabelle aufgenommen und IGMP-Telegramme weitergeleitet.
- **IGMP Snooping Aging Time**
  Tragen Sie in dieses Feld den Wert für die Aging Time in Sekunden ein. Standardmäßig sind 260 Sekunden eingestellt
  Gültige Werte: 130 - 300 Sekunden
- **IGMP Querier**
  Aktivieren oder deaktivieren Sie "IGMP Querier". Das Gerät verschickt IGMP-Anfragen.

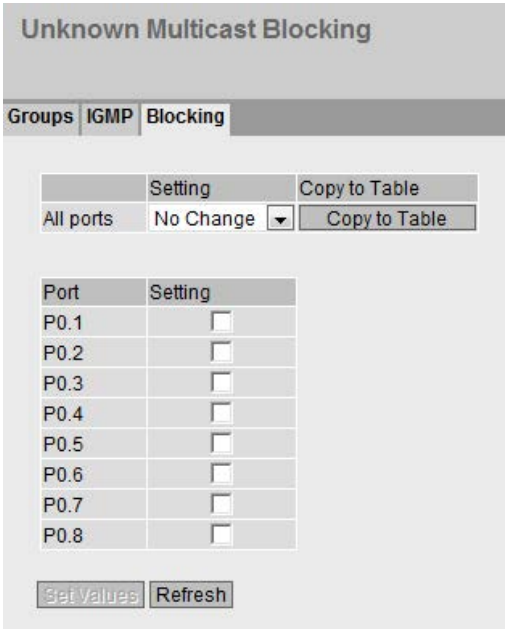
Vorgehensweise zur Konfiguration

1. Aktivieren Sie das Optionskästchen "IGMP Snooping".
2. Tragen Sie in das Feld "IGMP Snooping Aging Time" den Wert für die Aging-Time in Sekunden ein.
3. Aktivieren Sie das Optionskästchen "IGMP Querier".
4. Klicken Sie auf die Schaltfläche "Set Values".

5.5.13.3 Multicast Blocking

Sperrung der Weiterleitung von unbekannten Multicast-Telegrammen

Auf der Seite wird das Weiterleiten von unbekannten Multicast-Telegrammen für einzelne Ports gesperrt.



Beschreibung der angezeigten Werte

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Setting**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - enabled
    Blocken von Multicast-Telegrammen ist aktiviert.
  - disabled
    Blocken von Multicast-Telegrammen ist deaktiviert.
  - No Change
    Tabelle 2 bleibt unverändert.
- **Copy to Table**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Alle verfügbaren Ports werden in dieser Spalte aufgeführt. Nicht verfügbare Ports werden nicht angezeigt.
- **Setting**
  Aktivieren oder deaktivieren Sie das Blocken von Multicast-Telegrammen.

Vorgehensweise zu Konfiguration

Das Blocken für einen einzelnen Port aktivieren

1. Aktivieren Sie in der Tabelle 2 in der entsprechenden Zeile das Optionskästchen.
2. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Set Values".

Das Blocken für alle Ports aktivieren

1. Wählen in der Klappliste "Setting" den Eintrag "enabled".
2. Klicken Sie auf die Schaltfläche "Copy to Table". In der Tabelle 2 wird bei allen Ports das Optionskästchen aktiviert.
3. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Set Values".

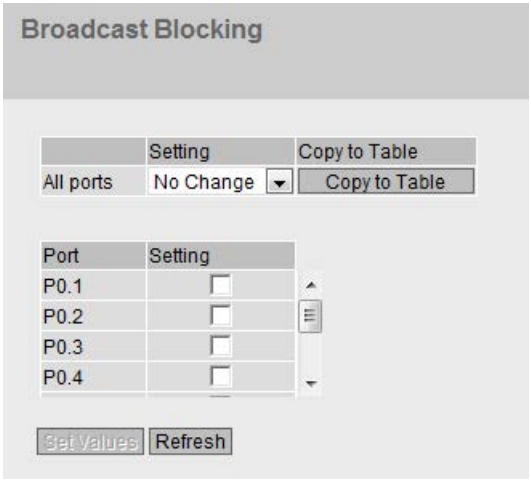
5.5.14 Broadcast

Sperrung der Weiterleitung von Broadcast-Telegrammen

Auf dieser Seite kann das Weiterleiten von Broadcast-Telegrammen für einzelne Ports gesperrt werden.

Hinweis

Einige Kommunikationsprotokolle funktionieren nur mit Unterstützung von Broadcast. In diesen Fällen kann das Sperren zum Ausfall der Datenkommunikation führen. Sperren Sie Broadcast nur, wenn Sie sicher sind, dass Sie auf darauf verzichten können.



Beschreibung der angezeigten Felder

Die Tabelle 1 gliedert sich in folgende Spalten:

- **1. Spalte**
  Zeigt an, dass die Einstellungen für alle Ports der Tabelle 2 gültig sind.
- **Setting**
  Wählen Sie aus der Klappliste die Einstellung. Folgende Einstellungsmöglichkeiten haben Sie:
  - enabled
    Das Blocken von Broadcast-Telegrammen ist aktiviert.
  - disabled
    Das Blocken von Broadcast-Telegrammen ist deaktiviert.
  - No Change
    Tabelle 2 bleibt unverändert.
- **Copy to Table**
  Wenn Sie auf die Schaltfläche klicken, wird die Einstellung für alle Ports der Tabelle 2 übernommen,

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**
  Alle verfügbaren Ports werden angezeigt.
- **Setting**
  Aktivieren oder deaktivieren Sie das Blocken von Broadcast-Telegrammen.

Vorgehensweise zur Konfiguration

Das Blocken von Broadcast-Telegrammen für einen einzelnen Port aktivieren

1. Aktivieren Sie in der Tabelle 2 in der entsprechenden Zeile das Optionskästchen.
2. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Set Values".

Das Blocken von Broadcast-Telegrammen für alle Ports aktivieren

1. Wählen in der Klappliste "Setting" den Eintrag "enabled".
2. Klicken Sie auf die Schaltfläche "Copy to Table". In der Tabelle 2 wird bei allen Ports das Optionskästchen aktiviert.
3. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche "Set Values".

5.5.15 RMON

5.5.15.1 Statistics

Statistik

Auf dieser Seite können Sie festlegen, für welche Ports RMON-Statistiken angezeigt werden.

Die RMON-Statistiken werden auf der Seite "Information > Ethernet Statistics" in den Reitern "Packet Size", "Packet Type" und "Packet Error" angezeigt.

Einstellungen

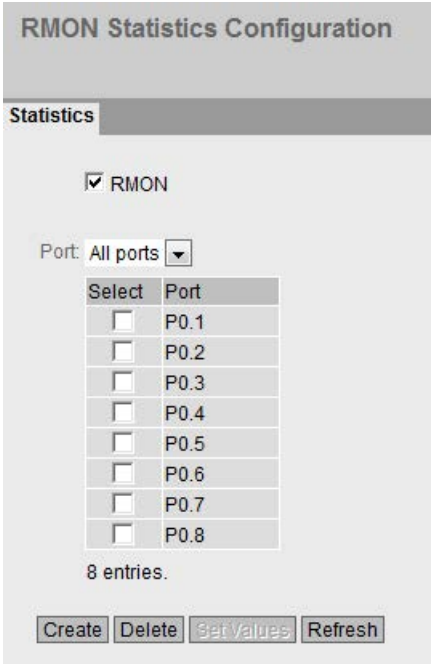


Bild 5-8 RMON Statistics

- **RMON**

  Wenn Sie dieses Optionskästchen aktivieren, ermöglicht Remote Monitoring (RMON), Diagnosedaten im Gerät zu sammeln, aufzubereiten und über SNMP von einer Netzwerkmanagement-Station, die ebenfalls RMON unterstützt, auszulesen. Diese Diagnosedaten, wie zum Beispiel portbezogene Lastverläufe, ermöglichen es, Probleme im Netzwerk frühzeitig zu erkennen und zu beseitigen.

  Hinweis

  Wenn Sie RMON deaktivieren, werden die Statistiken nicht gelöscht, sondern sie bleiben auf dem letzten Stand stehen.

- **Port**

  Wählen Sie die Ports aus, für die Statistiken angezeigt werden sollen.

Die Tabelle gliedert sich in folgende Spalten:

- **Select**

  Wählen Sie die Zeile, die Sie löschen wollen.

- **Port**

  Zeigt die Ports an, für die Statistiken angezeigt werden.

Vorgehensweise zur Konfiguration

Funktion aktivieren

1. Aktivieren Sie das Optionskästchen "RMON".
2. Klicken Sie auf die Schaltfläche "Set Values".

   Die Funktion "RMON" ist aktiviert.

RMON-Statistiken für Ports aktivieren

Hinweis

Voraussetzung

Damit RMON-Statistiken für einen Port angezeigt werden können, muss die Funktion "RMON" aktiviert sein.

1. Wählen Sie aus der Klappliste "Port" den gewünschten Port oder alle Ports "All Ports" aus.
2. Klicken Sie auf die Schaltfläche "Create".

   Für den gewählten Port bzw. alle Ports können RMON-Statistiken angezeigt werden.

RMON-Statistiken für Ports deaktivieren

1. Aktivieren Sie in der Spalte "Select" die Zeile, die Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Delete".

   Für den gewählten Port werden keine RMON-Statistiken angezeigt.

5.6 Das Menü "Layer 3"

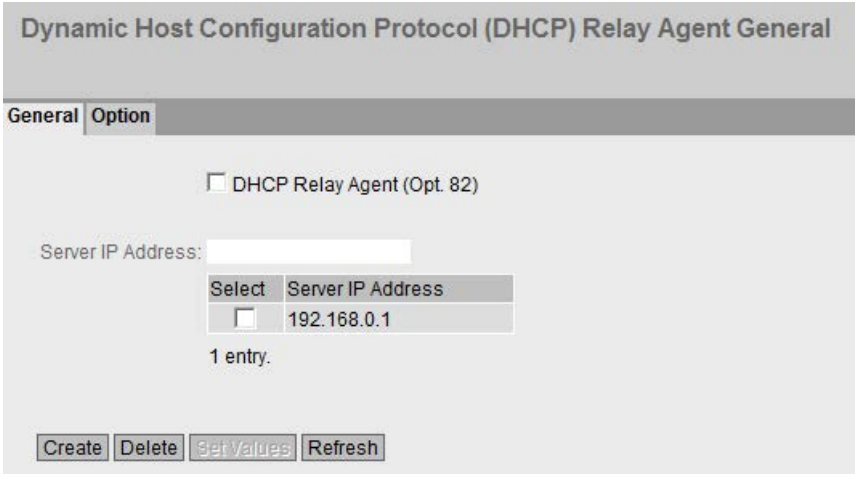
5.6.1 DHCP Relay Agent

5.6.1.1 General

DHCP Relay Agent

Wenn sich der DHCP-Server in einem anderen Netz befindet, kann das Gerät den DHCP-Server nicht erreichen. Der DHCP Relay Agent vermittelt zwischen einem DHCP-Server und dem Gerät. Dazu gibt der DHCP Relay Agent die Portnummer des Geräts zusammen mit der DHCP-Anfrage an den DHCP-Server weiter.

Sie können für den DHCP Relay Agent bis zu 4 DHCP Server IP-Adressen angeben. Wenn ein DHCP-Server nicht erreichbar ist, kann das Gerät auf einen anderen DHCP-Server ausweichen.



Beschreibung der angezeigten Werte

Die Seite enthält folgende Felder:

- **DHCP Relay Agent (Opt. 82)**
  Aktivieren oder deaktivieren Sie den DHCP Relay Agent.
- **Server IP Address**
  Tragen Sie die IP-Adresse des DHCP-Servers ein.

Die Tabelle gliedert sich in folgende Spalten:

- **Select**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Server IP Address**
  Zeigt die IP-Adresse des DHCP-Servers an.

Vorgehensweise zur Konfiguration

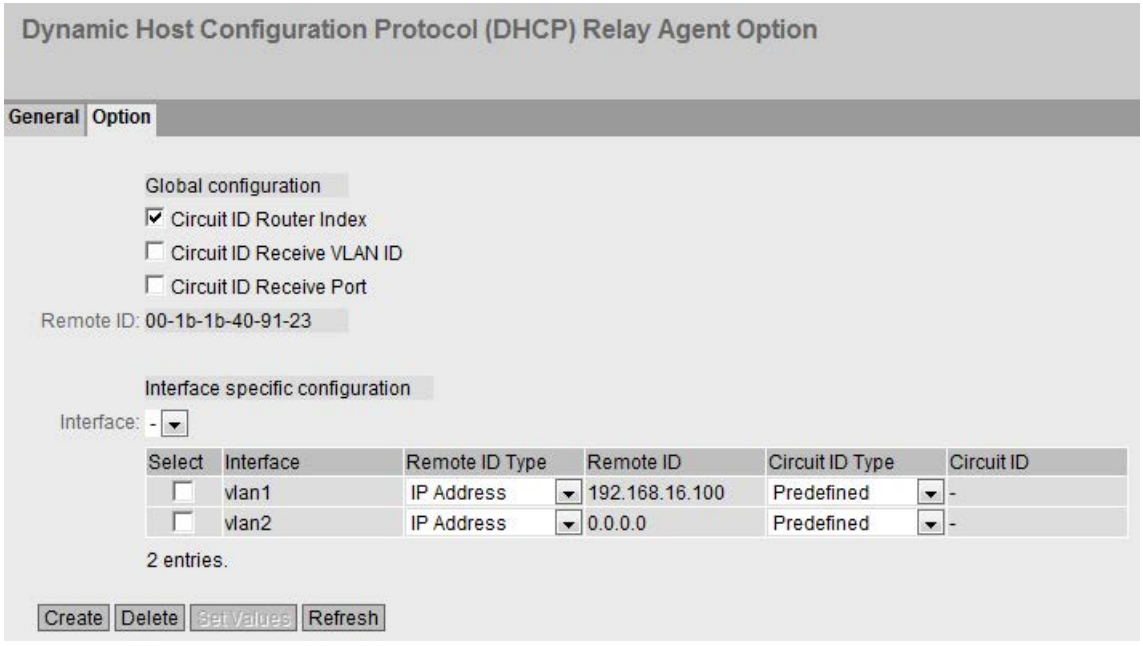
1. Tragen Sie in das Eingabefeld "Server IP Address" die IP-Adresse des DHCP-Servers an.
2. Klicken Sie auf die Schaltfläche "Create". In der Tabelle wird ein neuer Eintrag erzeugt.
3. Aktivieren Sie das Optionskästchen "DHCP Relay Agent (Opt. 82)".
4. Klicken Sie auf die Schaltfläche "Set Values".

5.6.1.2 Option

Parameter des DHCP Relay Agent

Auf dieser Seite können Sie Parameter für den DHCP-Server festlegen, z. B. die Circuit ID. Die Circuit ID beschreibt die Herkunft der DHCP-Anfrage, z. B. welcher Port die DHCP-Anfrage empfangen hat.

Die DHCP-Server legen Sie auf dem Register "General" fest.



Beschreibung der angezeigten Werte

Die Seite enthält folgende Felder:

- **Circuit ID Router Index**
  Aktivieren oder deaktivieren Sie das Optionskästchen. Wenn Sie das Optionskästchen aktivieren, wird der erzeugten Circuit ID der Router Index hinzugefügt.
- **Circuit ID Receive VLAN ID**
  Aktivieren oder deaktivieren Sie das Optionskästchen. Wenn Sie das Optionskästchen aktivieren, wird der erzeugten Circuit ID die VLAN ID hinzugefügt.

- **Circuit ID Receive Port**
  Aktivieren oder deaktivieren Sie das Optionskästchen. Wenn Sie das Optionskästchen aktivieren, wird der erzeugten Circuit ID der Empfangsport hinzugefügt.

Hinweis

Sie müssen mindestens eine Option auswählen.

- **Remote ID**
  Zeigt die Gerätekennung an.
- **Interface**
  Wählen Sie aus der Klappliste die Schnittstelle.

Die Tabelle gliedert sich in folgende Spalten:

- **Select**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Interface**
  Zeigt die Schnittstelle an.
- **Remote ID Type**
  Wählen Sie aus der Klappliste die Art der Gerätekennung aus. Sie haben folgende Möglichkeiten:
  - IP Address
    Als Gerätekennung wird die IP-Adresse des Geräts verwendet.
  - MAC Address
    Als Gerätekennung wird die MAC-Adresse des Geräts verwendet.
  - Free Text
    Wenn Sie "Free Text" verwenden, können Sie bei "Remote ID" den Gerätenamen als Gerätekennung eintragen.
- **Remote ID**
  Tragen Sie den Gerätenamen ein. Das Feld ist nur editierbar, wenn Sie bei "Remote ID Type" den Eintrag "Free Text" auswählen.
- **Circuit ID Type**
  Wählen Sie aus der Klappliste die Art der Circuit ID aus. Sie haben folgende Möglichkeiten:
  - Predefined
    Die Circuit ID wird automatisch erstellt, basierend auf Router Index, VLAN ID oder Port.
  - Free Number
    Wenn Sie "Free Number" verwenden, können Sie bei "Circuit ID" die ID eingeben.
- **Circuit ID**
  Tragen Sie die Circuit ID ein. Das Feld ist nur editierbar, wenn Sie bei "Circuit ID Type" den Eintrag "Free Number" auswählen.
  Wertebereich: 1- 188

Vorgehensweise zur Konfiguration

Gehen Sie folgendermaßen vor, um die automatische Vergabe der Parameter festzulegen:

1. Aktivieren Sie das Optionskästchen "Circuit ID Router Index".
2. Wählen Sie in der Klappliste "Interface" die Schnittstelle aus.
3. Klicken Sie auf die Schaltfläche "Create". In der Tabelle wird eine neue Zeile eingefügt
4. Wählen Sie in der Klappliste "Remote ID Type" den Eintrag "IP Address" aus. Zur Gerätekennung wird die IP-Adresse verwendet.
5. Wählen Sie in der Klappliste "Circuit ID Type" den Eintrag "Predefined" aus. Der erzeugten Circuit ID wird der Router Index hinzugefügt.
6. Klicken Sie auf die Schaltfläche "Set Values".

Gehen Sie folgendermaßen vor, um die Parameter manuell festzulegen:

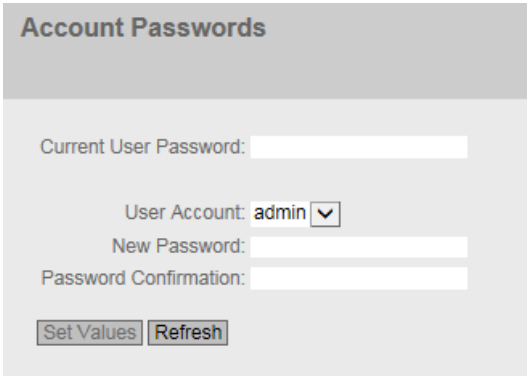
1. Aktivieren Sie das Optionskästchen "Circuit ID Router Index".
2. Wählen Sie in der Klappliste "Interface" die Schnittstelle aus.
3. Klicken Sie auf die Schaltfläche "Create". In der Tabelle wird eine neue Zeile eingefügt
4. Wählen Sie in der Klappliste "Remote ID Type" den Eintrag "Free Text" aus. Tragen Sie bei "Remote ID" die Gerätekennung ein.
5. Wählen Sie in der Klappliste "Circuit ID Type" den Eintrag "Free Number" aus. Tragen Sie bei "Circuit ID" die ID ein.
6. Klicken Sie auf die Schaltfläche "Set Values".

5.7 Das Menü "Security"

5.7.1 Passwords

Konfiguration der Geräte-Passwörter

Auf dieser Seite können Sie Passwörter ändern. Wenn Sie mit der Rolle "admin" angemeldet sind, können Sie die Passwörter für alle Benutzeraccounts ändern. Wenn Sie mit der Rolle "user" angemeldet sind, können Sie nur ihr eigenes Passwort ändern.



Beschreibung der angezeigten Werte

Die Seite enthält folgende Felder:

- **Current User Password**

  Geben Sie das Passwort des aktuell angemeldeten Benutzers ein.

- **User Account**

  Wählen Sie den Benutzeraccount, dessen Passwort Sie ändern möchten.

- **New Password**

  Geben Sie das neue Passwort ein.

- **Password Confirmation**

  Geben Sie das neue Passwort erneut ein, um es zu bestätigen.

Vorgehensweise

1. Geben Sie in das Eingabefeld "Current User Password" das gültige Passwort des aktuell angemeldeten Benutzers ein.
2. Wählen Sie aus der Klappliste "User Account" den Benutzer aus, für den das Passwort geändert wird.
   Wählen Sie aus zwischen "admin" und "user".

3. Geben Sie in das Eingabefeld "New Password" das neue Passwort für den ausgewählten Benutzer ein.
4. Wiederholen Sie das neue Passwort im Eingabefeld "Password Confirmation".
5. Klicken Sie auf die Schaltfläche "Set Values".

Hinweis

Werksseitig sind die Passwörter bei Auslieferung des Geräts wie folgt eingestellt:

- admin: admin
- user: user

Wenn Sie sich das erste Mal oder nach einem "Restore Factory Defaults and Restart" mit dem voreingestellten Benutzer "admin" anmelden, werden Sie aufgefordert das Passwort zu ändern.

Hinweis

Passwort ändern im Trial-Modus

Auch wenn Sie im Trial-Modus das Passwort ändern, wird diese Änderung sofort gespeichert.

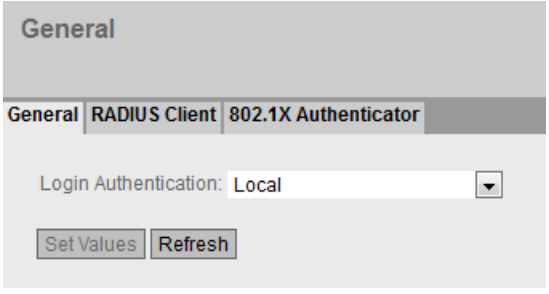
5.7.2 AAA

5.7.2.1 General

Anmeldung von Netzteilnehmern

Die verwendete Bezeichnung "AAA" steht für "Authentication, Authorization, Accounting". Dieses Feature dient dazu, Netzteilnehmer zu identifizieren und zuzulassen, ihnen die entsprechenden Dienste bereitzustellen und den Nutzungsumfang festzustellen.

Auf dieser Seite konfigurieren Sie die Anmeldung.



Beschreibung der angezeigten Felder

Die Seite enthält folgende Felder:

Hinweis

Um den Login-Authentifizierung "RADIUS", "Local and RADIUS" oder "RADIUS and fallback Local" nutzen zu können, muss ein RADIUS-Server hinterlegt und für die Benutzerauthentifizierung konfiguriert sein.

- **Login Authentication**
  Legen Sie fest, wie die Anmeldung erfolgt:
  - Local

    Die Authentifizierung muss lokal auf dem Gerät erfolgen.
  - RADIUS

    Die Authentifizierung muss über einen RADIUS-Server erfolgen.
  - Local and RADIUS

    Die Authentifizierung kann sowohl über die im Gerät vorhandenen Benutzer (Benutzername und Passwort) als auch über einen RADIUS-Server erfolgen.

    Es wird zuerst in der lokalen Datenbank nach dem Benutzer gesucht. Wenn der Benutzer dort nicht vorhanden ist oder das Passwort nicht übereinstimmt, wird eine RADIUS-Anfrage geschickt.
  - RADIUS and fallback Local

    Die Authentifizierung muss über einen RADIUS-Server erfolgen.

    Nur wenn der RADIUS-Server im Netz nicht erreichbar ist, wird eine lokale Authetifizierung durchgeführt.

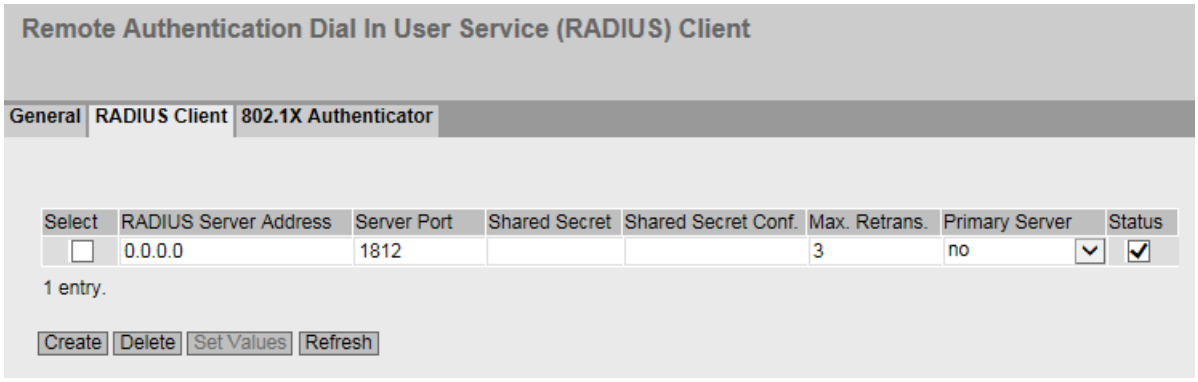
5.7.2.2 RADIUS Client

Anmeldung über einen externen Server

Das Konzept von RADIUS basiert auf einem externen Authentifizierungsserver. Für ein Endgerät ist der Zugang zum Netzwerk erst möglich, nachdem das Gerät die Anmeldedaten beim Authentifizierungsserver verifiziert hat. Sowohl das Endgerät als auch der Authentifizierungsserver müssen das EAP-Protokoll (Extensive Authentication Protocol) unterstützen.

Jede Spalte der Tabelle enthält die Zugangsdaten für je einen Server. In der Suchreihenfolge wird der primäre Server zuerst angefragt. Ist der primäre Server nicht erreichbar, werden in der eingetragenen Reihenfolge sekundäre Server angefragt.

Wenn keiner der Server antwortet, findet keine Authentifizierung statt. Der Client erhält keinen Zugriff auf das Netzwerk, obwohl ein Link am Port angezeigt wird.



Beschreibung der angezeigten Felder

Die Tabelle gliedert sich in folgende Spalten:

- **Select**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Server IP Address**
  Tragen Sie hier die IP-Adresse des Servers ein.
- **Server Port**
  Tragen Sie hier den Eingangs-Port auf dem RADIUS-Server ein. Standardmäßig ist der Eingangs-Port 1812 eingestellt. Der Wertebereich ist 1...65535.
- **Shared Secret**
  Geben Sie hier Ihre Zugangskennung an.
- **Shared Secret Conf.**
  Geben Sie die Zugangskennung zur Bestätigung erneut ein.
- **Max. Retrans.**

  Geben Sie hier die maximale Anzahl der Anfrageversuche ein, bevor ein anderer konfigurierter RADIUS-Server angefragt wird oder die Anmeldung für gescheitert erklärt wird. Standardmäßig ist 3 eingestellt. Der Wertebereich ist 1...254.
- **Primary Server**
  Legen Sie mit Hilfe der Optionen der Klappliste fest, ob dieser Server der primäre Server ist. Sie können aus den Optionen "yes" oder "no" auswählen.
- **Status**
  Mit diesem Optionskästchen können Sie den RADIUS-Servers aktivieren oder deaktivieren.

Hinweis

Sie können auf dieser Seite maximal zwei Server konfigurieren.

Vorgehensweise zur Konfiguration

Neuen Server eintragen

1. Klicken Sie auf die Schaltfläche "Create". In der Tabelle wird ein neuer Eintrag erzeugt. Folgende Standardwerte werden in die Tabelle eingetragen:
   - Server IP-Adresse: 0.0.0.0
   - Portnummer: 1812
   - Maximale Anzahl der Übertragungsversuche: 3
   - Primärer Server: Nein
2. Tragen Sie in der jeweiligen Zeile die folgenden Daten in die Eingabefelder ein:
   - Server IP-Adresse
   - Portnummer des Ziels
   - Geheime Zugangskennung
   - Wiederholung der geheimen Zugangskennung
   - Maximale Anzahl der Übertragungsversuche
   - Primärer Server
3. Klicken Sie auf die Schaltfläche "Set Values".

Wiederholen Sie den Vorgang für alle Server, die Sie eintragen wollen.

Server ändern

1. Tragen Sie in der jeweiligen Zeile die folgenden Daten in die Eingabefelder ein:
   - Server IP-Adresse
   - Portnummer des Ziels
   - Geheime Zugangskennung
   - Wiederholung der geheimen Zugangskennung
   - Maximale Anzahl der Übertragungsversuche
   - Primärer Server
2. Klicken Sie auf die Schaltfläche "Set Values".

Wiederholen sie den Vorgang bei allen Servern, deren Eintrag Sie ändern wollen

Server löschen

1. Klicken Sie in das Optionskästchen in der ersten Spalte vor der zu löschenden Zeile, um den Eintrag zum Löschen zu markieren.
   Wiederholen Sie den Vorgang für jeden Eintrag, den Sie löschen wollen.
2. Klicken Sie auf die Schaltfläche "Delete". Die Daten werden aus dem Speicher des Gerätes gelöscht und die Seite wird aktualisiert.

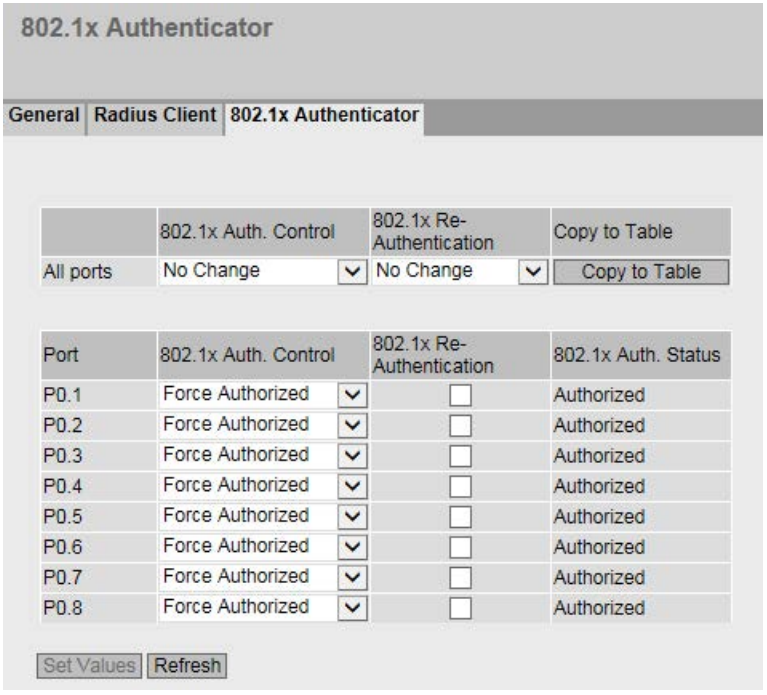
Hinweis

Wenn Sie auf die Schaltfläche "Refresh" klicken, bevor Sie Ihre Konfigurationsänderungen mit Hilfe der Schaltflächen "Set Values" oder "Delete" übertragen haben, dann werden Ihre Änderungen aufgehoben und die weiterhin bestehende bisherige Konfiguration wird aus dem Speicher des Gerätes geladen und angezeigt.

5.7.2.3 802.1x Authenticator

Aktivierung der Authentifizierung für einzelne Ports

Durch Aktivieren der entsprechenden Optionen legen Sie individuell für jeden Port fest, ob der Netzzugriffsschutz nach IEEE 802.1x auf diesem Port aktiviert ist.



Beschreibung der angezeigten Felder

Die Tabelle 1 gliedert sich in folgende Spalten:

- **802.1x Auth. Control**

  Wählen Sie die gewünschte Einstellung.
  Wenn "No Change" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.

- **802.1x Re-Authentication**

  Wählen Sie die gewünschte Einstellung.
  Wenn "No Change" ausgewählt ist, bleibt der Eintrag in der Tabelle 2 unverändert.

- **Copy to Table**
  Wenn Sie auf die Schaltfläche klicken, werden die Einstellungen für alle Ports der Tabelle 2 übernommen.

Die Tabelle 2 gliedert sich in folgende Spalten:

- **Port**

  In dieser Spalte werden alle in diesem Gerät verfügbaren Ports aufgeführt.

- **802.1x Auth. Control**

  Legen Sie die Authentifizierung des Ports fest:

  – Force Unauthorized

    Der Datenverkehr über den Port ist gesperrt.

  – Force Authorized

    Der Datenverkehr über den Port ist ohne Einschränkung erlaubt.

    Defaulteinstellung

  – Auto

    Endgeräte werden an dem Port mit dem Verfahren "802.1x" authentifiziert.

    Der Datenverkehr über den Port wird entsprechend des Authentifizierungsergebnisses erlaubt oder gesperrt.

- **802.1x Re-Authentication**

  Aktivieren Sie diese Option, wenn für ein bereits authentifiziertes Endgerät zyklisch eine Reauthentifizierung durchführt werden soll.

- **802.1x Auth. Status**

  Zeigt den Status der Authentifizierung des Ports an:

  – Unauthorized

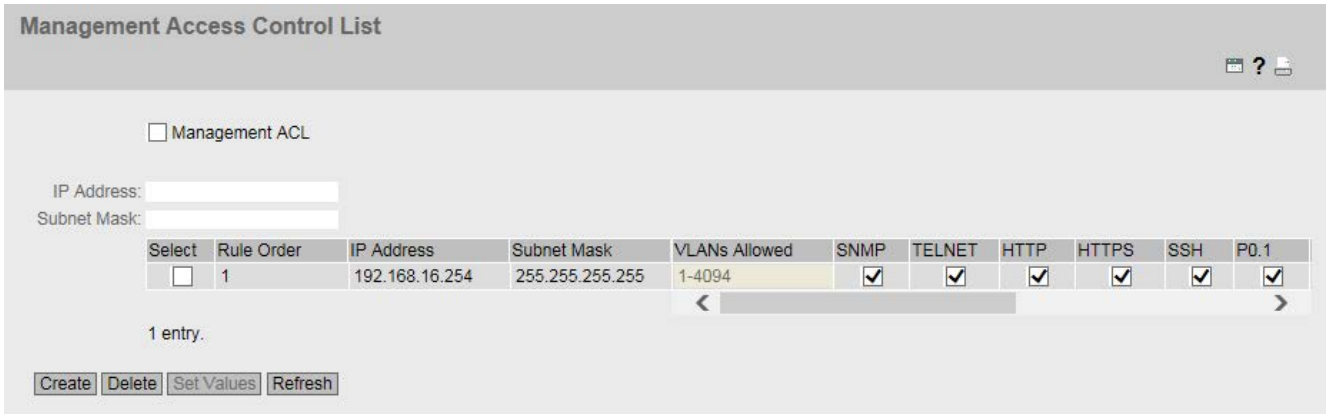
  – Authorized

5.7.3 Management ACL

Konfigurationsbeschreibung

Auf dieser Seite können Sie die Sicherheit Ihres Geräts erhöhen. Um festzulegen, welche Station mit welcher IP-Adresse auf Ihr Gerät zugreifen darf, konfigurieren Sie die IP-Adresse oder auch ein ganzes Adress-Band.

Sie können einstellen, mit welchen Protokollen und über welche Ports die Station auf das Gerät zugreifen darf.



Beschreibung der angezeigten Felder

Hinweis

Bevor Sie diese Funktion aktivieren, beachten Sie Folgendes

Eine fehlerhafte Projektierung auf der Seite "Management Access Control List" 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.

Die Seite enthält folgende Felder:

- **Management ACL**
  Aktivieren oder deaktivieren Sie die Zugriffskontrolle auf das Management des IE-Switches.

  Im Auslieferzustand ist die Funktion deaktiviert.

  Hinweis

  Wenn die Funktion deaktiviert ist, dann besteht uneingeschränkter Zugriff auf das Management des IE-Switches. Erst wenn die Funktion aktiviert ist, werden die projektierten Zugriffsregeln berücksichtigt.

- **IP Address**
  Tragen Sie die IP-Adresse oder die Netzadresse 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 Subnetzmaske ein.
  Die Subnetzmaske 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.

Die Tabelle gliedert sich in folgende Spalten:

- **Select**
  Wählen Sie die Zeile, die Sie löschen wollen.
- **Rule Order**
  Zeigt die Reihenfolge an, in der die ACL-Regeln geprüft werden. Sobald eine Regel passt, wird diese angewendet. Die folgenden Regeln werden nicht betrachtet.
- **IP Address**
  Zeigt die IP-Adresse an.
- **Subnet Mask**
  Zeigt die Subnetzmaske an.
- **VLANs Allowed**
  Sie können bezüglich VLANs keine Zugriffsregeln definieren. Die Regeln gelten für alle VLANs.

Hinweis

Kompatibilität mit älteren Firmware-Versionen

Falls Sie mit einer Firmware-Version < 1.2 bestimmte VLANs definiert haben, wird die Konfiguration der VLANs bei einem Firmware-Update durch den Default-Wert "1-4094" ersetzt.

- **SNMP**
  Legen Sie fest, ob die Station (bzw. die IP-Adresse) über das Protokoll SNMP das Gerät zugreifen darf.
- **TELNET**
  Legen Sie fest, ob die Station (bzw. die IP-Adresse) über das Protokoll TELNET auf das Gerät zugreifen darf.
- **HTTP**
  Legen Sie fest, ob die Station (bzw. die IP-Adresse) über das Protokoll HTTP auf das Gerät zugreifen darf.
- **HTTPS**
  Legen Sie fest, ob die Station (bzw. die IP-Adresse) über das Protokoll HTTPS auf den Switch zugreifen darf.

- **SSH**
  Legen Sie fest, ob die Station (bzw. die IP-Adresse) über das Protokoll SSH auf den Switch zugreifen darf.
- **Px.y**
  LegenSie fest, ob die Station (bzw. die IP-Adresse) über diesen Port auf dieses Gerät zugreifen darf.

Vorgehensweise zur Konfiguration

Hinweis

Bevor Sie diese Funktion aktivieren, beachten Sie Folgendes

Eine fehlerhafte Projektierung kann dazu führen, dass Sie nicht mehr auf das Gerät zugreifen können. Projektieren Sie daher eine Zugriffsregel, die Ihnen den Zugriff auf das Management erlaubt, bevor Sie die Funktion aktivieren.

Abhilfe erhalten Sie dann nur durch ein Rücksetzen des Geräts auf die Werkseinstellungen und anschließende Rekonfiguration.

Hinweis

Reihenfolge beachten

Die Reihenfolge, in der Sie die ACL-Regeln anlegen, entspricht der Reihenfolge, in der die Regeln geprüft werden. Sobald eine Regel passt, wird diese angewendet. Die folgenden Regeln werden nicht betrachtet.

Neue Regel anlegen

1. Tragen Sie in das Eingabefeld "IP Address" die IP-Adresse ein.
2. Tragen Sie in das Eingabefeld "Subnet Mask" die Subnetzmaske ein.
3. Klicken Sie auf die Schaltfläche "Create", um eine neue Zeile in der Tabelle anzulegen.
4. Konfigurieren Sie die Einträge der neuen Zeile.
5. Klicken Sie auf die Schaltfläche "Set Values", um die neue Regel in das Gerät zu übertragen.

Funktion aktivieren

1. Aktivieren Sie das Optionskästchen "Management ACL".
2. Klicken Sie auf die Schaltfläche "Set Values", um die projektierten Zugriffsregeln zu aktivieren.

Regel ändern

1. Konfigurieren Sie die Daten der Regel, die Sie ändern wollen.
2. Klicken Sie auf die Schaltfläche "Set Values", um die Änderungen in das Gerät zu übertragen.

Regel löschen

1. Aktivieren Sie in der zu löschenden Zeile das Optionskästchen.
2. Wiederholen Sie den Vorgang für jeden Eintrag, den Sie löschen wollen.
3. Klicken Sie auf die Schaltfläche "Delete". Die Regeln werden gelöscht und die Seite wird aktualisiert.

Troubleshooting/FAQ

6

6.1 Laden einer neuen Firmware über TFTP ohne WBM und CLI

Firmware

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

Betätigung des Tasters "RESET"

Um eine neue Firmware zu laden, benötigen Sie den Taster "RESET". Beachten Sie zur Betätigung des Tasters unbeding die Hinweise in der Betriebsanleitung (Seite 7).

Vorgehensweise unter Microsoft Windows

Über TFTP können Sie ein Gerät mit einer neuen Firmware versehen, selbst dann, wenn es nicht über das WBM oder CLI erreichbar ist. In diesem Kapitel wird die Vorgehensweise exemplarisch für Microsoft Windows erklärt.

Um eine neue Firmware über TFTP zu laden, gehen Sie wie folgt vor:

1. Schalten Sie das Gerät spannungslos.
2. Drücken Sie mit geringem Kraftaufwand den Taster "RESET" und schließen Sie das Gerät mit gedrücktem Taster wieder an die Spannungsversorgung an.
3. Halten Sie den Taster so lange gedrückt, bis die rote Fehler-LED "F" anfängt zu blinken.
4. Lassen Sie den Taster los, solange die rote Fehler-LED noch blinkt.

   Hinweis

   Dieses Zeitintervall dauert nur einige Sekunden.

   Der Bootloader des Geräts wartet in diesem Zustand auf eine neue Firmware-Datei, die Sie per TFTP laden können.
5. Verbinden Sie einen PC über ein Ethernet-Kabel mit dem Port 0.1.
6. Vergeben Sie über DHCP oder mit dem Primary Setup Tool eine IP-Adresse für das Gerät.

7. Wechseln Sie in einer Windows-Eingabeaufforderung in das Verzeichnis, in dem sich die Datei mit der neuen Firmware befindet und rufen Sie das folgende Kommando auf:
   ```
   tftp -i <IP-Adresse> put <Firmwaredatei>
   ```

   Hinweis

   Sie können TFTP unter Microsoft Windows wie folgt aktivieren:

   "Systemsteuerung" > "Programme und Funktionen" > "Windows-Funktionen aktivieren und deaktivieren" > "TFTP-Client"

8. Nachdem die Firmware komplett auf das Gerät übertragen und validiert wurde, erfolgt ein automatischer Neustart des Geräts. Dieser Vorgang kann einige Minuten in Anspruch nehmen.

Index

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z