Modicon

MCSESM, MCSESM-E, MCSESP Switch mit Management
GUI Referenz-Handbuch

QGH59086.02

www.schneider-electric.com

Schneider Electric

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

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

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

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

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

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

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

Inhalt

Sicherheitshinweise

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

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

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

⚠ GEFAHR

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

⚠ WARNUNG

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

⚠ VORSICHT

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

HINWEIS

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

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

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

Über dieses Handbuch

Gültigkeitsbereich

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

Benutzerkommentare

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

Weiterführende Dokumentation

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

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

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

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

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

Legende

Die in diesem Handbuch verwendeten Auszeichnungen haben folgende Bedeutungen:

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

Auszuführen in der grafische Benutzeroberfläche

Auszuführen im Command Line Interface

Hinweise zur grafischen Benutzeroberfläche

Das Gerät unterstützt die folgenden Betriebssysteme:
- Windows 10
- Linux

Die grafische Benutzeroberfläche des Geräts ist wie folgt unterteilt:
- Navigationsbereich
- Dialogbereich
- Schaltflächen

Navigationsbereich

Der Navigationsbereich befindet sich auf der linken Seite der grafischen Benutzeroberfläche.

Der Navigationsbereich enthält die folgenden Elemente:
- Symbolleiste
- Filter
- Menü

Sie haben die Möglichkeit, den Navigationsbereich zuzuklappen, zum Beispiel wenn Sie die grafische Benutzeroberfläche auf kleinen Bildschirmen anzeigen. Zum Zu- oder Aufklappen klicken Sie den kleinen Pfeil am oberen Rand des Navigationsbereichs.

Symbolleiste

Die Symbolleiste am oberen Rand des Navigationsbereichs enthält mehrere Schaltflächen.
- Wenn Sie den Mauszeiger über einer Schaltfläche positionieren, zeigt ein Tooltip weitere Informationen.
- Wenn die Verbindung zum Gerät unterbrochen ist, dann ist die Symbolleiste ausgegraut.

Das Gerät aktualisiert die Informationen in der Symbolleiste automatisch alle 5 Sekunden.

Klicken Sie die Schaltfläche, um die Symbolleiste manuell zu aktualisieren.

Wenn Sie den Mauszeiger über der Schaltfläche positionieren, zeigt ein Tooltip die folgenden Informationen:
- *Benutzer:*
  Bezeichnung des angemeldeten Benutzers
- *Gerätename:*
  Bezeichnung des Geräts

Klicken Sie die Schaltfläche, um den Dialog *Gerätesicherheit > Benutzerverwaltung* zu öffnen.

Wenn Sie den Mauszeiger über der Schaltfläche positionieren, zeigt ein Tooltip die Zusammenfassung des Dialogs *Diagnose > System > Konfigurations-Check*.

Klicken Sie die Schaltfläche, um den Dialog *Diagnose > System > Konfigurations-Check* zu öffnen.

Klicken Sie die Schaltfläche, um den gegenwärtig angemeldeten Benutzer abzumelden und den Login-Dialog anzuzeigen.

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

- Um die Änderungen permanent zu speichern, klicken Sie im Dialog *Warnung* die Schaltfläche *Ja*.
- Um die Änderungen zu verwerfen, klicken Sie im Dialog *Warnung* die Schaltfläche *Nein*.

Zeigt die verbleibende Zeit in Sekunden, bis das Gerät einen inaktiven Benutzer automatisch abmeldet.

Klicken Sie die Schaltfläche, um den Dialog *Gerätesicherheit > Management-Zugriff > Web* zu öffnen. Dort können Sie das Timeout festlegen.

Diese Schaltfläche ist sichtbar, wenn das Konfigurationsprofil im flüchtigen Speicher (*RAM*) und das „ausgewählte“ Konfigurationsprofil im permanenten Speicher (*NVM*) sich unterscheiden. Andernfalls ist die Schaltfläche unsichtbar.

Klicken Sie die Schaltfläche, um den Dialog *Grundeinstellungen > Laden/Speichern* zu öffnen.

Mit einem Rechtsklick auf die Schaltfläche können Sie die gegenwärtigen Einstellungen im permanenten Speicher (*NVM*) speichern.

Wenn Sie den Mauszeiger über der Schaltfläche positionieren, zeigt ein Tooltip die folgenden Informationen:

- *Gerätestatus:* Dieser Abschnitt zeigt eine komprimierte Ansicht des Rahmens *Geräte-Status* im Dialog *Grundeinstellungen > System*. Der Abschnitt zeigt den zeitlich zuerst aufgetretenen, gegenwärtig noch andauernden Alarm.
- *Sicherheitsstatus:* Dieser Abschnitt zeigt eine komprimierte Ansicht des Rahmens *Sicherheits-Status* im Dialog *Grundeinstellungen > System*. Der Abschnitt zeigt den zeitlich zuerst aufgetretenen, gegenwärtig noch andauernden Alarm.
- *Boot-Parameter:* Wenn Sie geänderte Einstellungen permanent speichern und sich mindestens ein Boot-Parameter von dem beim letzten Neustart verwendeten Konfigurationsprofil unterscheidet, dann zeigt dieser Abschnitt einen Hinweis.
  Folgende Einstellungen rufen eine Änderung der Boot-Parameter hervor:
  - Dialog *Grundeinstellungen > Externer Speicher*, Parameter *Automatisches Software-Update*
  - Dialog *Grundeinstellungen > Externer Speicher*, Parameter *Konfigurations-Priorität*
  - Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SNMP*, Parameter *UDP-Port*
  - Dialog *Diagnose > System > Selbsttest*, Parameter *RAM-Test*
  - Dialog *Diagnose > System > Selbsttest*, Parameter *SysMon1 ist verfügbar*
  - Dialog *Diagnose > System > Selbsttest*, Parameter *Bei Fehler Default-Konfiguration laden*

Klicken Sie die Schaltfläche, um den Dialog *Diagnose > Statuskonfiguration > Gerätestatus* zu öffnen.

Filter

Der Filter bietet Ihnen die Möglichkeit, die Anzahl der Menüpunkte im Menü zu reduzieren. Während des Filterns zeigt das Menü ausschließlich diejenigen Menüpunkte, die den im Filterfeld eingegebenen Suchbegriff enthalten.

Menü

Das Menü zeigt die Menüpunkte.

Sie haben die Möglichkeit, die Menüpunkte zu filtern. Siehe Abschnitt „Filter”.

Um den zugehörigen Dialog im Dialogbereich anzuzeigen, klicken Sie den gewünschten Menüpunkt. Wenn der ausgewählte Menüpunkt ein Knoten ist, der untergeordnete Menüpunkte enthält, dann klappt der Knoten beim Klicken auf oder zu. Der Dialogbereich zeigt weiterhin den zuvor angezeigten Dialog.

Sie haben die Möglichkeit, jeden Knoten im Menü gleichzeitig auf- oder zuzuklappen. Wenn Sie an beliebiger Stelle im Menü rechtsklicken, zeigt ein Kontextmenü die folgenden Einträge:

- *Aufklappen*
  Klappt jeden Knoten im Menü gleichzeitig auf. Das Menü zeigt die Menüpunkte jeder Ebene.
- *Zuklappen*
  Klappt jeden Knoten im Menü gleichzeitig zu. Das Menü zeigt die Menüpunkte der obersten Ebene.

Dialogbereich

Der Dialogbereich befindet sich auf der rechten Seite der grafischen Benutzeroberfläche. Wenn Sie im Navigationsbereich einen Menüpunkt klicken, zeigt der Dialogbereich den zugehörigen Dialog.

Anzeige aktualisieren

Wenn ein Dialog über längere Zeit geöffnet ist, dann kann es vorkommen, dass sich die Werte im Gerät inzwischen geändert haben.

- ☐ Um die Anzeige im Dialog zu aktualisieren, klicken Sie die Schaltfläche  . Ungespeicherte Änderungen im Dialog gehen dabei verloren.

Einstellungen speichern

Das Speichern überträgt die geänderten Einstellungen in den flüchtigen Speicher (*RAM*) des Geräts. Führen Sie den folgenden Schritt aus:

- ☐ Klicken Sie die Schaltfläche  .

Damit die geänderten Einstellungen auch nach dem Neustart des Geräts erhalten bleiben, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- ☐ Markieren Sie in der Tabelle das gewünschte Konfigurationsprofil.
- ☐ Ist das Kontrollkästchen in Spalte *Ausgewählt* noch `unmarkiert`, klicken Sie die Schaltfläche  und dann den Eintrag *Auswählen*.
- ☐ Klicken Sie die Schaltfläche  und dann den Eintrag *Speichern*.

Anmerkung: Unbeabsichtigte Änderungen an den Einstellungen führen möglicherweise zum Verbindungsabbruch zwischen Ihrem PC und dem Gerät. Damit das Gerät erreichbar bleibt, schalten Sie die Funktion *Konfigurationsänderungen rückgängig machen* im Dialog *Grundeinstellungen > Laden/Speichern* ein, bevor Sie Einstellungen ändern. Mit der Funktion prüft das Gerät kontinuierlich, ob es von der IP-Adresse Ihres PCs erreichbar bleibt. Wenn die Verbindung abbricht, dann lädt das Gerät nach der festgelegten Zeit das im permanenten Speicher (*NVM*) gespeicherte Konfigurationsprofil. Danach ist das Gerät wieder erreichbar.

Arbeiten mit Tabellen

Die Dialoge zeigen zahlreiche Einstellungen in tabellarischer Form.

Wenn Sie eine Tabellenzelle ändern, zeigt die Tabellenzelle eine rote Markierung in der linken oberen Ecke. Die rote Markierung weist darauf hin, dass Ihre Änderungen noch nicht in den flüchtigen Speicher (*RAM*) des Geräts übertragen sind.

Sie haben die Möglichkeit, das Erscheinungsbild der Tabellen an Ihre Bedürfnisse anzupassen. Wenn Sie den Mauszeiger über einer Spaltenüberschrift positionieren, zeigt die Spaltenüberschrift die Schaltfläche einer Dropdown-Liste. Wenn Sie diese Schaltfläche klicken, zeigt die Dropdown-Liste die folgenden Einträge:

- ▶ Aufsteigend sortieren
  Sortiert die Tabelleneinträge in aufsteigender Reihenfolge basierend auf den Einträgen der ausgewählten Spalte.
  Sortierte Tabelleneinträge erkennen Sie an einem Pfeil in der Spaltenüberschrift.

- Absteigend sortieren
  Sortiert die Tabelleneinträge in absteigender Reihenfolge basierend auf den Einträgen der ausgewählten Spalte.
  Sortierte Tabelleneinträge erkennen Sie an einem Pfeil in der Spaltenüberschrift.
- Spalten
  Blendet Spalten ein oder aus.
  Ausgeblendete Spalten erkennen Sie an einem unmarkierten Kontrollkästchen in der Drop-down-Liste.
- Filter
  Die Tabelle zeigt ausschließlich die Einträge, deren Inhalt mit den festgelegten Filterkriterien der ausgewählten Spalte übereinstimmt.
  Gefilterte Tabelleneinträge erkennen Sie an einer hervorgehobenen Spaltenüberschrift.

Sie haben die Möglichkeit, mehrere Tabelleneinträge gleichzeitig zu markieren, um anschließend eine Aktion darauf anzuwenden. Dies ist nützlich, wenn Sie mehrere Tabelleneinträge gleichzeitig entfernen möchten.

- Mehrere aufeinander folgende Tabelleneinträge auswählen:
  - ☐ Klicken Sie den ersten gewünschten Tabelleneintrag, um diesen zu markieren.
  - ☐ Drücken und halten Sie die <SHIFT>-Taste.
  - ☐ Klicken Sie den letzten gewünschten Tabelleneintrag, um jeden gewünschten Tabelleneintrag zu markieren.
- Mehrere einzelne Tabelleneinträge markieren:
  - ☐ Klicken Sie den ersten gewünschten Tabelleneintrag, um diesen zu markieren.
  - ☐ Drücken und halten Sie die <STRG>-Taste.
  - ☐ Klicken Sie den nächsten gewünschten Tabelleneintrag, um diesen zu markieren. Wiederholen Sie, bis jeder gewünschte Tabelleneintrag markiert ist.

Schaltflächen

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

Überträgt die Änderungen in den flüchtigen Speicher (*RAM*) des Geräts und wendet diese an. Um die Änderungen im permanenten Speicher zu speichern, gehen Sie wie folgt vor:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- ☐ Markieren Sie in der Tabelle das gewünschte Konfigurationsprofil.
- ☐ Ist das Kontrollkästchen in Spalte *Ausgewählt* noch `unmarkiert`, klicken Sie die Schaltfläche  und dann den Eintrag *Auswählen*.
- ☐ Klicken Sie die Schaltfläche  , um die gegenwärtigen Änderungen zu speichern.

Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (*RAM*) des Geräts gespeichert sind.

Überträgt die Einstellungen aus dem flüchtigen Speicher (*RAM*) in das als „ausgewählt“ gekennzeichnete Konfigurationsprofil im permanenten Speicher (*NVM*).

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

Zeigt ein Untermenü mit den zum jeweiligen Dialog gehörenden Einträgen.

Öffnet den Dialog *Wizard*.

Fügt einen neuen Tabelleneintrag hinzu.

Entfernt den markierten Tabelleneintrag.

Öffnet die Online-Hilfe.

1 Grundeinstellungen

Das Menü enthält die folgenden Dialoge:

- System
- Netz
- Out-of-Band via USB
- Software
- Laden/Speichern
- Externer Speicher
- Port
- Power over Ethernet (MCSESP)
- Neustart

1.1 System

[Grundeinstellungen > System]

In diesem Dialog überwachen Sie einzelne Betriebszustände.

Geräte-Status

Die Felder in diesem Rahmen zeigen den Gerätestatus und informieren über aufgetretene Alarme. Der Rahmen ist hervorgehoben, wenn gegenwärtig ein Alarm vorhanden ist.

Die Parameter, die das Gerät überwacht, legen Sie fest im Dialog *Diagnose > Statuskonfiguration >* Gerätestatus.

Anmerkung: Das Gerät meldet einen Alarm, wenn Sie an ein Gerät mit mehreren Anschlüssen für die Versorgungsspannung lediglich ein Netzteil anschließen. Um diesen Alarm zu vermeiden, deaktivieren Sie im Dialog *Diagnose > Statuskonfiguration > Gerätestatus* das Überwachen der fehlenden Netzteile.

Anzahl Alarme

Zeigt die Anzahl der gegenwärtig vorhandenen Alarme.

Das Symbol ist sichtbar, wenn mindestens ein Alarm gegenwärtig vorhanden ist.

Wenn Sie den Mauszeiger über dem Symbol positionieren, zeigt ein Tooltip die Ursache der gegenwärtig vorhandenen Alarme und den Zeitpunkt, zu dem das Gerät den Alarm ausgelöst hat.

Das Gerät löst einen Alarm aus, wenn ein überwachter Parameter vom gewünschten Zustand abweicht. Der Dialog *Diagnose > Statuskonfiguration > Gerätestatus*, Registerkarte *Status* zeigt die Alarme im Überblick.

Sicherheits-Status

Die Felder in diesem Rahmen zeigen den Sicherheitsstatus und informieren über aufgetretene Alarme. Der Rahmen ist hervorgehoben, wenn gegenwärtig ein Alarm vorhanden ist.

Die Parameter, die das Gerät überwacht, legen Sie fest im Dialog *Diagnose > Statuskonfiguration >* Sicherheitsstatus.

Anzahl Alarme

Zeigt die Anzahl der gegenwärtig vorhandenen Alarme.

Das Symbol ist sichtbar, wenn mindestens ein Alarm gegenwärtig vorhanden ist.

Wenn Sie den Mauszeiger über dem Symbol positionieren, zeigt ein Tooltip die Ursache der gegenwärtig vorhandenen Alarme und den Zeitpunkt, zu dem das Gerät den Alarm ausgelöst hat.

Das Gerät löst einen Alarm aus, wenn ein überwachter Parameter vom gewünschten Zustand abweicht. Der Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus*, Registerkarte *Status* zeigt die Alarme im Überblick.

Status Signalkontakt

Die Felder in diesem Rahmen zeigen den Signalkontaktstatus und informieren über aufgetretene Alarme. Der Rahmen ist hervorgehoben, wenn gegenwärtig ein Alarm vorhanden ist.

Die Parameter, die das Gerät überwacht, legen Sie fest im Dialog *Diagnose > Statuskonfiguration >* Signalkontakt > *Signalkontakt 1*/*Signalkontakt 2*.

Anzahl Alarme

Zeigt die Anzahl der gegenwärtig vorhandenen Alarme.

Das Symbol ist sichtbar, wenn mindestens ein Alarm gegenwärtig vorhanden ist.

Wenn Sie den Mauszeiger über dem Symbol positionieren, zeigt ein Tooltip die Ursache der gegenwärtig vorhandenen Alarme und den Zeitpunkt, zu dem das Gerät den Alarm ausgelöst hat.

Das Gerät löst einen Alarm aus, wenn ein überwachter Parameter vom gewünschten Zustand abweicht. Der Dialog *Diagnose > Statuskonfiguration > Signalkontakt > Signalkontakt 1*/*Signalkontakt 2*, Registerkarte *Status* zeigt die Alarme im Überblick.

Systemdaten

Die Felder in diesem Rahmen zeigen Betriebsdaten sowie Informationen zum Standort des Geräts.

Systemname

Legt den Namen fest, unter dem das Gerät im Netz bekannt ist.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen
  Die folgenden Zeichen sind zulässig:
  - `0..9`
  - `a..z`
  - `A..Z`
  - `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`
  - `<Gerätename>-<MAC-Adresse>` (Voreinstellung)

Beim Erzeugen von HTTPS-X.509-Zertifikaten verwendet die Applikation, die das Zertifikat generiert, den festgelegten Wert als Domain-Namen und als gemeinsamen Namen.

Die folgenden Funktionen verwenden den festgelegten Wert als Hostnamen oder FQDN (Fully Qualified Domain Name). Für die Kompatibilität ist es empfehlenswert, nur Kleinbuchstaben zu verwenden, da nicht jedes System zwischen Groß- und Kleinschreibung im FQDN unterscheidet. Vergewissern Sie sich, dass dieser Name im gesamten Netz eindeutig ist.

- DHCP-Client
- *Syslog*
- *IEC61850-MMS*

Standort

Legt den Standort des Geräts fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Ansprechpartner

Legt den Ansprechpartner für dieses Gerät fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Gerätetyp

Zeigt die Produktbezeichnung des Geräts.

Netzteil 1
Netzteil 2

Zeigt den Status des Netzteils am betreffenden Spannungsversorgungs-Anschluss.

Mögliche Werte:

- *vorhanden*
- *defekt*

- *nicht vorhanden*
- *unbekannt*

Betriebszeit

Zeigt die Zeit, die seit dem letzten Neustart dieses Geräts vergangen ist.

Mögliche Werte:

- Zeit im Format `Tag(e), ...h ...m ...s`

Temperatur [°C]

Zeigt die gegenwärtige Temperatur im Gerät in °C.

Das Überwachen der Temperaturgrenzen schalten Sie ein im Dialog *Diagnose* > Statuskonfiguration > *Gerätestatus*.

Obere Temp.-Grenze [°C]

Legt die obere Temperaturgrenze in °C fest.

Mögliche Werte:

- `-99..99` (ganze Zahl)
  Wenn die Temperatur im Gerät diesen Wert überschreitet, dann generiert das Gerät einen Alarm.

Untere Temp.-Grenze [°C]

Legt die untere Temperaturgrenze in °C fest.

Mögliche Werte:

- `-99..99` (ganze Zahl)
  Wenn die Temperatur im Gerät diesen Wert unterschreitet, dann generiert das Gerät einen Alarm.

LED-Status

Dieser Rahmen zeigt die Zustände der Gerätestatus-LEDs zum Zeitpunkt der letzten Aktualisierung. Das Anwender-Handbuch „Installation“ enthält ausführliche Informationen zu den Gerätestatus-LEDs.

Parameter	Farbe	Bedeutung
Status	●	Gegenwärtig ist kein Alarm vorhanden. Der Gerätestatus ist OK.
	●	Gegenwärtig ist mindestens ein Gerätestatus-Alarm vorhanden. Siehe Rahmen *Geräte-Status* oben.
Power	●	Gerätevariante mit 2 Netzteilen: Lediglich eine Versorgungsspannung ist aktiv.
	●	Gerätevariante mit 1 Netzteil: Die Versorgungsspannung ist aktiv. Gerätevariante mit 2 Netzteilen: Beide Versorgungsspannungen sind aktiv.

Parameter	Farbe	Bedeutung
EAM	●	Kein externer Speicher angeschlossen.
	●	Der externe Speicher ist angeschlossenen, jedoch nicht betriebsbereit.
	●	Der externe Speicher ist angeschlossenen und betriebsbereit.

Status Port

Dieser Rahmen zeigt eine vereinfachte Ansicht der Ports des Geräts zum Zeitpunkt der letzten Aktualisierung.

Die Symbole stellen den Zustand der einzelnen Ports dar. In manchen Situationen überlagern sich die folgenden Symbole. Wenn Sie den Mauszeiger über dem entsprechenden Port-Symbol positionieren, zeigt ein Tooltip detaillierte Informationen zum Port-Status.

Parameter	Status	Bedeutung
`<Port-Nummer>`	●	Der Port ist inaktiv. Der Port sendet und empfängt keine Daten.
	●	Der Port ist inaktiv. Das Kabel ist verbunden. Aktiver Link.
	●	Der Port ist aktiv. Kein Kabel angesteckt oder kein aktiver Link.
	●	Der Port ist aktiv. Das Kabel ist verbunden. Verbindung in Ordnung. Aktiver Link. Vollduplex-Modus
	●	Die Halbduplex-Modus ist eingeschaltet. Prüfen Sie die Einstellungen im Dialog *Grundeinstellungen > Ports*, Registerkarte *Konfiguration*.
	●	Der Port ist aufgrund einer Redundanzfunktion im "blocking"-Zustand.
	●	Der Port arbeitet als Router-Interface.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

1.2 Netz

[Grundeinstellungen > Netz]

Das Menü enthält die folgenden Dialoge:

- Global
- IPv4
- IPv6

1.2.1 Global

[Grundeinstellungen > Netz > Global]

In diesem Dialog legen Sie die VLAN- und Ethernet Switch Configurator-Einstellungen fest, die für den Zugriff über das Netz auf das Management des Geräts erforderlich sind.

Management-Schnittstelle

In diesem Rahmen legen Sie das VLAN fest, in dem das Management des Geräts erreichbar ist.

VLAN-ID

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

Mögliche Werte:

- `1..4042` (Voreinstellung: `1`)
  Voraussetzung ist, dass das VLAN bereits eingerichtet ist. Siehe Dialog *Switching > VLAN > Konfiguration*.

Wenn Sie nach Ändern des Werts die Schaltfläche ✓ klicken, öffnet sich der Dialog *Information*. Wählen Sie den Port aus, über den Sie die Verbindung zum Gerät zukünftig herstellen. Nach Klicken der Schaltfläche *Ok* sind die Einstellungen des neuen Management-VLANs dem Port zugewiesen.

- Der Port wird Mitglied des VLANs und vermittelt die Datenpakete ohne VLAN-Tag (untagged). Siehe Dialog *Switching > VLAN > Konfiguration*.
- Das Gerät weist dem Port die Port-VLAN-ID des neuen Management-VLANs zu. Siehe Dialog *Switching > VLAN > Port*.

Nach kurzer Wartezeit ist das Gerät über den neuen Port im neuen Management-VLAN erreichbar.

MAC-Adresse

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

Ethernet Switch Configurator Protokoll v1/v2

Dieser Rahmen ermöglicht Ihnen, Einstellungen für den Zugriff auf das Gerät per Ethernet Switch Configurator-Protokoll festzulegen.

Auf einem PC zeigt die Ethernet Switch Configurator-Software im Netz erreichbare Schneider Electric-Geräte, auf denen die Funktion Ethernet Switch Configurator eingeschaltet ist. Sie erreichen die Geräte sogar dann, wenn ihnen ungültige oder keine IP-Parameter zugewiesen sind. Die Ethernet Switch Configurator-Software ermöglicht Ihnen, die IP-Parameter im Gerät zuzuweisen oder zu ändern.

Anmerkung: Mit der Ethernet Switch Configurator-Software erreichen Sie das Gerät ausschließlich über Ports, die Mitglied desselben VLANs sind wie das Management des Geräts. Welchem Port welches VLAN zugewiesen ist, legen Sie fest im Dialog *Switching > VLAN > Konfiguration*.

Funktion

Schaltet die Funktion Ethernet Switch Configurator im Gerät ein/aus.

Mögliche Werte:

- *An* (Voreinstellung)
  Ethernet Switch Configurator ist eingeschaltet.
  Sie haben die Möglichkeit, das Gerät mit der Ethernet Switch Configurator-Software von Ihrem PC aus zu erreichen.
- *Aus*
  Ethernet Switch Configurator ist ausgeschaltet.

Zugriff

Schaltet den Schreibzugriff auf das Gerät per Ethernet Switch Configurator ein/aus.

Mögliche Werte:

- *read-write* (Voreinstellung)
  Die Ethernet Switch Configurator-Software erhält Schreibzugriff auf das Gerät.
  Mit dieser Einstellung haben Sie die Möglichkeit, die IP-Parameter im Gerät zu ändern.
- *read-only*
  Die Ethernet Switch Configurator-Software erhält ausschließlich Lesezugriff auf das Gerät.
  Mit dieser Einstellung haben Sie die Möglichkeit, die IP-Parameter im Gerät anzusehen.

Empfehlung: Ändern Sie erst nach Inbetriebnahme des Geräts die Einstellung auf den Wert *read-only*.

Signal

Aktiviert/deaktiviert das Blinken der Port-LEDs wie die gleichnamige Funktion in der Ethernet Switch Configurator-Software. Diese Funktion ermöglicht Ihnen, das Gerät im Feld zu identifizieren.

Mögliche Werte:

- markiert
  Das Blinken der Port-LEDs ist aktiv.
  Die Port-LEDs blinken solange, bis Sie die Funktion wieder ausschalten.
- unmarkiert (Voreinstellung)
  Das Blinken der Port-LEDs ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

1.2.2 IPv4

[Grundeinstellungen > Netz > IPv4]

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

Management-Schnittstelle

Zuweisung IP-Adresse

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

Mögliche Werte:

- `Lokal`
  Das Gerät verwendet die IP-Parameter aus dem internen Speicher. Die Einstellungen dafür legen Sie im Rahmen *IP-Parameter* fest.
- `BOOTP`
  Das Gerät erhält seine IP-Parameter von einem BOOTP- oder DHCP-Server.
  Der Server wertet die MAC-Adresse des Geräts aus und weist daraufhin die IP-Parameter zu.
- `DHCP` (Voreinstellung)
  Das Gerät erhält seine IP-Parameter von einem DHCP-Server.
  Der Server wertet die MAC-Adresse, den DHCP-Namen oder andere Parameter des Geräts aus und weist daraufhin die IP-Parameter zu.
  Stellt der Server zusätzlich die Adressen von DNS-Servern bereit, zeigt das Gerät diese Adressen im Dialog *Erweitert > DNS > Cache > Aktuell*.

Anmerkung: Wenn die Antwort des BOOTP- oder DHCP-Servers ausbleibt, dann setzt das Gerät die IP-Adresse auf `0.0.0.0` und versucht erneut, eine gültige IP-Adresse zu erhalten.

BOOTP/DHCP

Client-ID

Zeigt die DHCP-Client-ID, die das Gerät an den BOOTP- oder DHCP-Server sendet. Wenn man eine entsprechende Konfiguration des Servers voraussetzt, dann reserviert der Server eine IP-Adresse für diese DHCP-Client-ID. Demzufolge erhält das Gerät bei jeder Anfrage dieselbe IP-Adresse vom Server.

Das Gerät sendet als DHCP-Client-ID den Gerätenamen, der im Feld *Systemname* im Dialog *Grundeinstellungen > System* festgelegt ist.

DHCP-Option 66/67/4/42

Schaltet die Funktion *DHCP-Option 66/67/4/42* im Gerät ein/aus.

Mögliche Werte:

- *An* (Voreinstellung)
  Die Funktion *DHCP-Option 66/67/4/42* ist eingeschaltet.
  Das Gerät lädt das Konfigurationsprofil und empfängt die Zeitserverinformationen mittels der folgenden DHCP-Optionen:
  - `Option 66: TFTP server name`
    `Option 67: Boot file name`
    Das Gerät lädt mittels TFTP-Protokoll das Konfigurationsprofil automatisch vom DHCP-Server in den flüchtigen Speicher (*RAM*). Das Gerät verwendet die Einstellungen des importierten Konfigurationsprofils in der `running-config`.
  - `Option 4: Time Server`
    `Option 42: Network Time Protocol Servers`
    Das Gerät empfängt die Zeitserverinformationen vom DHCP-Server.
- *Aus*
  Die Funktion *DHCP-Option 66/67/4/42* ist ausgeschaltet.
  - Das Gerät lädt kein Konfigurationsprofil mittels DHCP-Option 66/67.
  - Das Gerät empfängt keine Zeitserverinformationen mittels DHCP-Option 4/42.

IP-Parameter

Dieser Rahmen ermöglicht Ihnen, die IP-Parameter manuell zuzuweisen. Wenn Sie im Rahmen *Management-Schnittstelle*, Optionsliste *Zuweisung IP-Adresse* das Optionsfeld `Lokal` auswählen, dann sind die Felder editierbar.

IP-Adresse

Legt die IP-Adresse fest, unter der das Management des Geräts über das Netz erreichbar ist.

Mögliche Werte:

- Gültige IPv4-Adresse

Netzmaske

Legt die Netzmaske fest.

Mögliche Werte:

- Gültige IPv4-Netzmaske

Gateway-Adresse

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

Mögliche Werte:

- Gültige IPv4-Adresse

Verbleibende Lease-Time

Lease-Time [s]

Zeigt die verbleibende Zeit in Sekunden, in der die IP-Adresse noch gültig ist, die der DHCP-Server dem Managment des Geräts zugewiesen hat.

Um die Anzeige zu aktualisieren, klicken Sie die Schaltfläche  .

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

1.2.3 IPv6

[Grundeinstellungen > Netz > IPv6]

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

Funktion

Funktion

Aktiviert/deaktiviert das IPv6-Protokoll im Gerät.

IPv4 und IPv6können im Gerät parallel betrieben werden. Das wird durch die Verwendung vonDual IP Layer, auch Dual Stack genannt, ermöglicht.

Mögliche Werte:

- *An* (Voreinstellung)
  Das IPv6-Protokoll ist aktiviert.
- *Aus*
  Das IPv6-Protokoll ist deaktiviert.
  Wenn Sie ausschließlich das IPv4-Protokoll im Gerät betreiben möchten, dann deaktivieren Sie die Funktion IPv6 im Gerät.

Konfiguration

Dynamische IP-Adresszuweisung

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

Mögliche Werte:

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

DHCP

Client-ID

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

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

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

IP-Parameter

Gateway-Adresse

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

Mögliche Werte:

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

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

Erkennung doppelter Adressen

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

Anzahl der Nachbarn

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

Mögliche Werte:

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

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

Tabelle

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

Prefix

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

Prefix-Länge

Zeigt die Präfixlänge der IPv6-Adresse.

Im Gegensatz zu IPv4-Adressen verwenden IPv6-Adressen keine Subnetzmaske, um den Netzanteil einer Adresse zu bestimmen. Diese Funktion übernimmt die Präfixlänge in IPv6.

Mögliche Werte:

- `0..128`

IP-Adresse

Zeigt die gesamte IPv6-Adresse in verkürzter Schreibweise.

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

Mögliche Werte:

- Gültige IPv6-Adresse
  Für die Verwendung einer IPv6-Adresse in einer URL gilt die folgende URL-Syntax: `https://[<IPv6_Adresse>]`.

Weitere Informationen zu den Verkürzungsregeln und Adresstypen in IPv6 entnehmen Sie dem Handbuch „Konfiguration“.

EUI-Option

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

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

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

Mögliche Werte:

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

Ursprung

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

Mögliche Werte:

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

Status

Zeigt den gegenwärtigen Status der IPv6-Adresse.

Mögliche Werte:

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

Anmerkung: Wenn die IPv6-Adresse manuell festgelegt wird, können Sie manuell zwischen Status *aktiv* und Status *notInService* wechseln. Wählen Sie dafür in Spalte *Status* den entsprechenden Status in der Dropdown-Liste zu Ihrem Eintrag.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

1.3 Out-of-Band via USB

[Grundeinstellungen > Out-of-Band via USB]

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

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

- HTTP
- HTTPS

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

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

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

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

Funktion

Funktion

Schaltet die USB-Netzschnittstelle ein/aus.

Mögliche Werte:

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

Management-Schnittstelle

Device MAC-Adresse

Zeigt die MAC-Adresse der USB-Netzschnittstelle.

Host MAC-Adresse

Zeigt die MAC-Adresse der angeschlossenen Management-Station.

IP-Parameter

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

- Management-Interface

IP-Adresse

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

Mögliche Werte:

- Gültige IPv4-Adresse
  (Voreinstellung: `91.0.0.100`)
  Das Gerät weist diese IP-Adresse, um 1 erhöht, der Management-Station zu, die mit dem Gerät verbunden ist.
  Beispiel: `91.0.0.100` für die USB-Netzschnittstelle, `91.0.0.101` für die Management-Station.

Netzmaske

Legt die Netzmaske fest.

Mögliche Werte:

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

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

1.4 Software

[Grundeinstellungen > Software]

Dieser Dialog ermöglicht Ihnen, die Geräte-Software zu aktualisieren und Informationen über die Geräte-Software anzuzeigen.

Außerdem haben Sie die Möglichkeit, ein im Gerät gespeichertes Backup der Geräte-Software wiederherzustellen.

Anmerkung: Beachten Sie vor dem Aktualisieren der Geräte-Software die versionsspezifischen Hinweise in der `Liesmich`-Textdatei.

Version

Gespeicherte Version

Zeigt Versionsnummer und Erstellungsdatum der im Flash gespeicherten Geräte-Software. Das Gerät lädt die Geräte-Software beim nächsten Neustart.

Ausgeführte Version

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

Backup-Version

Zeigt Versionsnummer und Erstellungsdatum der als Backup im Flash gespeicherten Geräte-Software. Diese Geräte-Software hat das Gerät beim letzten Software-Update oder nach Klicken der Schaltfläche *Wiederherstellen* in den Backup-Bereich kopiert.

Wiederherstellen

Stellt die als Backup gespeicherte Geräte-Software wieder her. Dabei tauscht das Gerät die *Gespeicherte Version*und die *Backup-Version* der Geräte-Software.

Das Gerät lädt die *Gespeicherte Version*beim nächsten Neustart.

Bootcode

Zeigt Versionsnummer und Erstellungsdatum des Bootcodes.

Software-Update

Alternativ ermöglicht Ihnen das Gerät, die Geräte-Software durch Rechtsklicken in der Tabelle zu aktualisieren, wenn sich die Image-Datei im externen Speicher befindet.

URL

Legt Pfad und Dateiname der Image-Datei fest, mit der Sie die Geräte-Software aktualisieren.

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

- Software-Update vom PC
  Befindet sich die Datei auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie die Datei in den  -Bereich. Alternativ klicken Sie in den Bereich, um die Datei auszuwählen.
- Software-Update von einem FTP-Server
  Befindet sich die Datei auf einem FTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  `ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Dateiname>`
- Software-Update von einem TFTP-Server
  Befindet sich die Datei auf einem TFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  `tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
- Software-Update von einem SCP- oder SFTP-Server
  Befindet sich die Datei auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in einer der folgenden Formen fest:
  - `scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`
    Nach Klicken der Schaltfläche *Start* zeigt das Gerät das Fenster *Anmeldeinformationen*. Geben Sie dort *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
  - `scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>`

Start

Aktualisiert die Geräte-Software.

Das Gerät installiert die ausgewählte Datei im Flash-Speicher und ersetzt die bisher dort gespeicherte Geräte-Software. Beim nächsten Neustart lädt das Gerät die installierte Geräte-Software.

Die bisher verwendete Geräte-Software kopiert das Gerät in den Backup-Bereich.

Um während des Software-Updates im Gerät angemeldet zu bleiben, bewegen Sie gelegentlich den Mauszeiger. Alternativ legen Sie vor dem Software-Update im Dialog *Gerätesicherheit > Management-Zugriff > Web*, Feld *Web-Interface Session-Timeout [min]* einen ausreichend hohen Wert fest.

Tabelle

Datei Ort

Zeigt den Speicherort der Geräte-Software.

Mögliche Werte:

- *ram*
  Flüchtiger Speicher des Geräts

- *flash*
  Permanenter Speicher (*NVM*) des Geräts
- *usb*
  Externer USB-Speicher (EAM)

Index

Zeigt den Index der Geräte-Software.

Für die der Geräte-Software im Flash hat der Index die folgende Bedeutung:

- 1
  Diese Geräte-Software lädt das Gerät beim Neustart.
- 2
  Diese Geräte-Software hat das Gerät beim letzten Software-Update in den Backup-Bereich kopiert.

Dateiname

Zeigt den geräteinternen Dateinamen der Geräte-Software.

Firmware

Zeigt Versionsnummer und Erstellungsdatum der Geräte-Software.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

1.5 Laden/Speichern

[Grundeinstellungen > Laden/Speichern]

Dieser Dialog ermöglicht Ihnen, die Einstellungen des Geräts permanent in einem Konfigurationsprofil zu speichern.

Im Gerät können mehrere Konfigurationsprofile gespeichert sein. Wenn Sie ein alternatives Konfigurationsprofil aktivieren, schalten Sie das Gerät auf andere Einstellungen um. Sie haben die Möglichkeit, die Konfigurationsprofile auf Ihren PC oder auf einen Server zu exportieren. Außerdem haben Sie die Möglichkeit, Konfigurationsprofile von Ihrem PC oder von einem Server in das Gerät zu importieren.

In der Voreinstellung speichert das Gerät die Konfigurationsprofile unverschlüsselt. Wenn Sie ein Passwort im Rahmen *Konfigurations-Verschlüsselung* vergeben, speichert das Gerät sowohl das gegenwärtige als auch die zukünftigen Konfigurationsprofile in einem verschlüsselten Format.

Unbeabsichtigte Änderungen an den Einstellungen führen möglicherweise zum Verbindungsabbruch zwischen Ihrem PC und dem Gerät. Damit das Gerät erreichbar bleibt, schalten Sie vor dem Ändern von Einstellungen die Funktion *Konfigurationsänderungen rückgängig machen* ein. Wenn die Verbindung abbricht, dann lädt das Gerät nach der festgelegten Zeit das im permanenten Speicher (*NVM*) gespeicherte Konfigurationsprofil.

Externer Speicher

Ausgewählter externer Speicher

Zeigt den Typ des externen Speichers.

Mögliche Werte:

- *usb*
  Externer USB-Speicher (EAM)

Status

Zeigt den Betriebszustand des externen Speichers.

Mögliche Werte:

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

Konfigurations-Verschlüsselung

Aktiv

Zeigt, ob die Konfigurations-Verschlüsselung im Gerät aktiv/inaktiv ist.

Mögliche Werte:

- `markiert`
  Die Konfigurations-Verschlüsselung ist aktiv.
  Das Gerät lädt ein Konfigurationsprofil aus dem permanenten Speicher (*NVM*) ausschließlich dann, wenn dieses verschlüsselt ist und das Passwort mit dem im Gerät gespeicherten Passwort übereinstimmt.
- `unmarkiert`
  Die Konfigurations-Verschlüsselung ist inaktiv.
  Das Gerät lädt ein Konfigurationsprofil aus dem permanenten Speicher (*NVM*) ausschließlich dann, wenn dieses unverschlüsselt ist.

Wenn im Dialog *Grundeinstellungen > Externer Speicher* die Spalte *Konfigurations-Priorität* den Wert `first` hat und das Konfigurationsprofil unverschlüsselt ist, dann zeigt der Rahmen *Sicherheits-Status* im Dialog *Grundeinstellungen > System* einen Alarm.

Im Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus*, Registerkarte *Global*, Spalte *Überwachen* legen Sie fest, ob das Gerät den Parameter *Unverschlüsselte Konfiguration vom externen Speicher laden* überwacht.

Passwort setzen

Öffnet das Fenster *Passwort setzen*, das Ihnen beim Festlegen des Passworts hilft, das für die Verschlüsselung des Konfigurationsprofils erforderlich ist. Das Verschlüsseln des Konfigurationsprofils erschwert den unberechtigten Zugriff. Führen Sie dazu die folgenden Schritte aus:

- ☐ Wenn Sie ein vorhandenes Passwort ändern, geben Sie in das Feld *Altes Passwort* das bisherige Passwort ein. Um anstelle von ***** (Sternchen) das Passwort im Klartext anzuzeigen, markieren Sie das Kontrollkästchen *Passwort anzeigen*.
- ☐ Geben Sie im Feld *Neues Passwort* das Passwort ein.
  Um anstelle von ***** (Sternchen) das Passwort im Klartext anzuzeigen, markieren Sie das Kontrollkästchen *Passwort anzeigen*.
- ☐ Markieren Sie das Kontrollkästchen *Konfiguration danach speichern*, um die Verschlüsselung auf das „ausgewählte“ Konfigurationsprofil im permanenten Speicher (*NVM*) und im externen Speicher anzuwenden.

Anmerkung: Wenden Sie diese Funktion ausschließlich dann an, wenn maximal ein Konfigurationsprofil im permanenten Speicher (*NVM*) des Geräts gespeichert ist. Entscheiden Sie sich vor dem Anlegen zusätzlicher Konfigurationsprofile für oder gegen eine dauerhaft eingeschaltete Konfigurations-Verschlüsselung im Gerät. Speichern Sie zusätzliche Konfigurationsprofile entweder unverschlüsselt oder mit demselben Passwort verschlüsselt.

Wenn Sie ein Gerät mit verschlüsseltem Konfigurationsprofil ersetzen, zum Beispiel weil das Gerät nicht mehr funktioniert, dann führen Sie die folgenden Schritte aus:

- ☐ Starten Sie das neue Gerät, weisen Sie die IP-Parameter zu.
- ☐ Öffnen Sie auf dem neuen Gerät den Dialog *Grundeinstellungen > Laden/Speichern*.
- ☐ Verschlüsseln Sie im neuen Gerät das Konfigurationsprofil. Siehe oben. Geben Sie dasselbe Passwort ein, das Sie im nicht mehr funktionierenden Gerät verwendet haben.

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

Löschen

Öffnet das Fenster *Löschen*, das Ihnen beim Aufheben der Konfigurations-Verschlüsselung im Gerät hilft. Um die Konfigurations-Verschlüsselung aufzuheben, führen Sie die folgenden Schritte aus:

- ☐ Geben Sie im Feld *Altes Passwort* das bisherige Passwort ein.
  Um anstelle von ***** (Sternchen) das Passwort im Klartext anzuzeigen, markieren Sie das Kontrollkästchen *Passwort anzeigen*.
- ☐ Markieren Sie das Kontrollkästchen *Konfiguration danach speichern*, um die Verschlüsselung auch im „ausgewählten“ Konfigurationsprofil im permanenten Speicher (*NVM*) und im externen Speicher aufzuheben.

Anmerkung: Wenn Sie weitere Konfigurationsprofile verschlüsselt im Speicher vorhalten, sorgt das Gerät dafür, dass Sie diese Konfigurationsprofile nicht aktivieren oder als „ausgewählt“ kennzeichnen.

Information

NVM synchron mit running-config

Zeigt, ob das Konfigurationsprofil im flüchtigen Speicher (*RAM*) und das „ausgewählte“ Konfigurationsprofil im permanenten Speicher (*NVM*) übereinstimmen.

Mögliche Werte:

- ▶ `markiert`
  Die Konfigurationsprofile stimmen überein.
- ▶ `unmarkiert`
  Die Konfigurationsprofile unterscheiden sich.

Externer Speicher und NVM synchron

Zeigt, ob das „ausgewählte“ Konfigurationsprofil im externen Speicher und das „ausgewählte“ Konfigurationsprofil im permanenten Speicher (*NVM*) übereinstimmen.

Mögliche Werte:

- ▶ `markiert`
  Die Konfigurationsprofile stimmen überein.
- ▶ `unmarkiert`
  Die Konfigurationsprofile unterscheiden sich.
  Mögliche Ursachen:
  - An das Gerät ist kein externer Speicher angeschlossen.
  - Im Dialog *Grundeinstellungen > Externer Speicher* ist die Funktion *Sichere Konfiguration beim Speichern*ausgeschaltet.

Sichere Konfiguration auf Remote-Server beim Speichern

Funktion

Schaltet die Funktion *Sichere Konfiguration auf Remote-Server beim Speichern* ein/aus.

Mögliche Werte:

- `Eingeschaltet`
  Die Funktion *Sichere Konfiguration auf Remote-Server beim Speichern* ist eingeschaltet.
  Wenn Sie das Konfigurationsprofil im permanenten Speicher (`NVM`) speichern, sichert das Gerät das Konfigurationsprofil automatisch auf dem im Feld *URL* festgelegten Remote-Server.
- `Ausgeschaltet` (Voreinstellung)
  Die Funktion *Sichere Konfiguration auf Remote-Server beim Speichern* ist ausgeschaltet.

URL

Legt Pfad und Dateiname des zu sichernden Konfigurationsprofils auf dem Remote-Server fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen
  Beispiel: `tftp://192.9.200.1/cfg/config.xml`
  Das Gerät unterstützt die folgenden Platzhalter:
  - `%d`
    Systemdatum im Format `YYYY-mm-dd`
  - `%t`
    Systemzeit im Format `HH_MM_SS`
  - `%i`
    IP-Adresse des Geräts
  - `%m`
    MAC-Adresse des Geräts im Format `AA-BB-CC-DD-EE-FF`
  - `%p`
    Produktbezeichnung des Geräts

Zugangsdaten setzen

Öffnet das Fenster *Anmeldeinformationen*, das Ihnen beim Festlegen des Login-Passworts hilft, das für die Anmeldung auf dem Remote-Server erforderlich ist. Führen Sie dazu die folgenden Schritte aus:

- ☐ Geben Sie im Feld *Benutzername* den Benutzernamen ein.
  Um anstelle von ***** (Sternchen) den Benutzernamen im Klartext anzuzeigen, markieren Sie das Kontrollkästchen *Passwort anzeigen*.
  Mögliche Werte:
  - Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen
- ☐ Geben Sie im Feld *Passwort* das Passwort ein.
  Um anstelle von ***** (Sternchen) das Passwort im Klartext anzuzeigen, markieren Sie das Kontrollkästchen *Passwort anzeigen*.
  Mögliche Werte:
  - Alphanumerische ASCII-Zeichenfolge mit 6..64 Zeichen
    Die folgenden Zeichen sind zulässig:
    `a..z`
    `A..Z`
    `0..9`
    `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`

Konfigurationsänderungen rückgängig machen

Funktion

Schaltet die Funktion *Konfigurationsänderungen rückgängig machen* ein/aus. Mit der Funktion prüft das Gerät kontinuierlich, ob es von der IP-Adresse Ihres PCs erreichbar bleibt. Bricht die Verbindung ab, lädt das Gerät nach einer festgelegten Zeitspanne das „ausgewählte“ Konfigurationsprofil aus dem permanenten Speicher (*NVM*). Danach ist das Gerät wieder erreichbar.

Mögliche Werte:

- *An*
  Die Funktion ist eingeschaltet.
  - Die Zeitspanne zwischen Verbindungsabbruch und Laden des Konfigurationsprofils legen Sie fest im Feld *Timeout [s] für Wiederherstellung nach Verbindungsabbruch*.
  - Enthält der permanente Speicher (*NVM*) mehrere Konfigurationsprofile, lädt das Gerät das als „ausgewählt“ gekennzeichnete Konfigurationsprofil.
- *Aus* (Voreinstellung)
  Die Funktion ist ausgeschaltet.
  Schalten Sie die Funktion wieder aus, bevor Sie die grafische Benutzeroberfläche schließen. So vermeiden Sie, dass das Gerät das als „ausgewählt“ gekennzeichnete Konfigurationsprofil wiederherstellt.

Anmerkung: Bevor Sie die Funktion einschalten, speichern Sie die Einstellungen im Konfigurationsprofil. Gegenwärtige Änderungen, die lediglich flüchtig im Gerät gespeichert sind, bleiben somit erhalten.

Timeout [s] für Wiederherstellung nach Verbindungsabbruch

Legt die Zeit in Sekunden fest, nach der das Gerät das „ausgewählte“ Konfigurationsprofil aus dem permanenten Speicher (*NVM*) lädt, wenn die Verbindung abbricht.

Mögliche Werte:

- `30..600` (Voreinstellung: `600`)

Legen Sie den Wert ausreichend groß fest. Berücksichtigen Sie die Zeit, in der Sie die Dialoge der grafischen Oberfläche lediglich ansehen, ohne sie zu ändern oder zu aktualisieren.

Watchdog IP-Adresse

Zeigt die IP-Adresse des PCs, auf dem Sie die Funktion eingeschaltet haben.

Mögliche Werte:

- IPv4-Adresse (Voreinstellung: `0.0.0.0`)

Tabelle

Speicher-Typ

Zeigt den Speicherort des Konfigurationsprofils.

Mögliche Werte:

- *RAM* (flüchtiger Speicher des Geräts)
  Im flüchtigen Speicher speichert das Gerät die Einstellungen für den laufenden Betrieb.

- *NVM* (permanenter Speicher des Geräts)
  Aus dem permanenten Speicher lädt das Gerät das „ausgewählte“ Konfigurationsprofil beim Neustart oder beim Anwenden der Funktion *Konfigurationsänderungen rückgängig machen*.
  Der permanente Speicher bietet Platz für mehrere Konfigurationsprofile, abhängig von der Anzahl der im Konfigurationsprofil gespeicherten Einstellungen. Das Gerät verwaltet im permanenten Speicher maximal 20 Konfigurationsprofile.
  Sie können ein Konfigurationsprofil in den flüchtigen Speicher (*RAM*) laden. Führen Sie dazu die folgenden Schritte aus:
  - ☐ Markieren Sie in der Tabelle das Konfigurationsprofil.
  - ☐ Klicken Sie die Schaltfläche ☰ und dann den Eintrag *Aktivieren*.
- *ENVM* (externer Speicher)
  Im externen Speicher speichert das Gerät eine Sicherungskopie des „ausgewählten“ Konfigurationsprofils.
  Voraussetzung ist, dass Sie im Dialog *Grundeinstellungen > Externer Speicher* das Kontrollkästchen in Spalte *Sichere Konfiguration beim Speichern*markieren.

Profilname

Zeigt die Bezeichnung des Konfigurationsprofils.

Mögliche Werte:

- `running-config`
  Bezeichnung des Konfigurationsprofils im flüchtigen Speicher (*RAM*).
- `config`
  Bezeichnung des werksseitig vorhandenen Konfigurationsprofils im permanenten Speicher (*NVM*).
- benutzerdefinierter Name
  Das Gerät ermöglicht Ihnen, ein Konfigurationsprofil mit benutzerdefiniertem Namen zu speichern, wenn Sie ein vorhandenes Konfigurationsprofil in der Tabelle markieren, die Schaltfläche ☰ und dann den Eintrag *Speichern unter...* klicken.

Um das Konfigurationsprofil als XML-Datei auf Ihren PC zu exportieren, klicken Sie den Link. Dann wählen Sie den Speicherort und legen den Dateinamen fest.

Um die Datei auf einem Remote-Server zu speichern, klicken Sie die Schaltfläche ☰ und dann den Eintrag *Exportieren...*.

Datum der letzten Änderung (UTC)

Zeigt den Zeitpunkt (UTC), zu dem ein Benutzer das Konfigurationsprofil zuletzt gespeichert hat.

Ausgewählt

Zeigt, ob das Konfigurationsprofil als „ausgewählt“ gekennzeichnet ist.

Um ein anderes Konfigurationsprofil als „ausgewählt“ zu kennzeichnen, markieren Sie das gewünschte Konfigurationsprofil in der Tabelle, klicken die Schaltfläche ☰ und dann den Eintrag *Aktivieren*.

Mögliche Werte:

- `markiert`
  Das Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet.
  - Das Gerät lädt die das Konfigurationsprofil beim Neustart oder beim Anwenden der Funktion *Konfigurationsänderungen rückgängig machen* in den flüchtigen Speicher (`RAM`).
  - Wenn Sie die Schaltfläche  klicken, speichert das Gerät die zwischengespeicherten Einstellungen in diesem Konfigurationsprofil.
- `unmarkiert`
  Ein anderes Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet.

Verschlüsselt

Zeigt, ob das Konfigurationsprofil verschlüsselt ist.

Mögliche Werte:

- `markiert`
  Das Konfigurationsprofil ist verschlüsselt.
- `unmarkiert`
  Das Konfigurationsprofil ist unverschlüsselt.

Die Verschlüsselung des Konfigurationsprofils schalten Sie im Rahmen *Konfigurations-Verschlüsselung* ein und aus.

Verschlüsselung verifiziert

Zeigt, ob das Passwort des verschlüsselten Konfigurationsprofils mit dem im Gerät gespeicherten Passwort übereinstimmt.

Mögliche Werte:

- `markiert`
  Die Passwörter stimmen überein. Das Gerät ist imstande, das Konfigurationsprofil zu entschlüsseln.
- `unmarkiert`
  Die Passwörter unterscheiden sich. Das Gerät ist außerstande, das Konfigurationsprofil zu entschlüsseln.

Software-Version

Zeigt die Versionsnummer der Geräte-Software, die das Gerät beim Speichern des Konfigurationsprofils ausgeführt hat.

Fingerabdruck

Zeigt die im Konfigurationsprofil gespeicherte Prüfsumme.

Das Gerät berechnet die Prüfsumme beim Speichern der Einstellungen und fügt sie in das Konfigurationsprofil ein.

Fingerabdruck verifiziert

Zeigt, ob die im Konfigurationsprofil gespeicherte Prüfsumme gültig ist.

Das Gerät berechnet die Prüfsumme des als „ausgewählt“ gekennzeichneten Konfigurationsprofils und vergleicht diese mit der Prüfsumme, die in diesem Konfigurationsprofil gespeichert ist.

Mögliche Werte:

- `markiert`
  Berechnete und gespeicherte Prüfsumme stimmen überein.
  Die gespeicherten Einstellungen sind konsistent.
- `unmarkiert`
  Für das als „ausgewählt“ gekennzeichnete Konfigurationsprofil gilt:
  Berechnete und gespeicherte Prüfsumme unterscheiden sich.
  Das Konfigurationsprofil enthält geänderte Einstellungen.
  Mögliche Ursachen:
  – Die Datei ist beschädigt.
  – Das Dateisystem im externen Speicher ist inkonsistent.
  – Ein Benutzer hat das Konfigurationsprofil exportiert und die XML-Datei außerhalb des Geräts verändert.
  Für die anderen Konfigurationsprofile hat das Gerät die Prüfsumme nicht berechnet.

Das Gerät verifiziert die Prüfsumme ausschließlich dann korrekt, wenn das Konfigurationsprofil zuvor wie folgt gespeichert wurde:

- auf einem baugleichen Gerät
- mit derselben Software-Version, welche das Gerät derzeit ausführt

Anmerkung: Diese Funktion kennzeichnet Änderungen an den Einstellungen des Konfigurationsprofils. Die Funktion bietet keinen Schutz davor, das Gerät mit geänderten Einstellungen zu betreiben.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Entfernt das in der Tabelle markierte Konfigurationsprofil aus dem permanenten Speicher (*NVM*) oder vom externen Speicher.

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

Speichern unter...

Kopiert das in der Tabelle markierte Konfigurationsprofil und speichert es mit benutzerdefiniertem Namen im permanenten Speicher (*NVM*). Das Gerät kennzeichnet das neue Konfigurationsprofil als „ausgewählt“.

Anmerkung: Entscheiden Sie sich vor dem Anlegen zusätzlicher Konfigurationsprofile für oder gegen eine dauerhaft eingeschaltete Konfigurations-Verschlüsselung im Gerät. Speichern Sie zusätzliche Konfigurationsprofile entweder unverschlüsselt oder mit demselben Passwort verschlüsselt.

Wenn im Dialog *Grundeinstellungen > Externer Speicher* das Kontrollkästchen in Spalte *Sichere Konfiguration beim Speichern*markiert ist, kennzeichnet das Gerät auch das gleichnamige Konfigurationsprofil auf dem externen Speicher als „ausgewählt“.

Aktivieren

Lädt die Einstellungen des in der Tabelle markierten Konfigurationsprofils in den flüchtigen Speicher (*RAM*).

- Das Gerät trennt die Verbindung zur grafischen Benutzeroberfläche. Um wieder auf das Geräte-Management zuzugreifen, führen Sie die folgenden Schritte aus:
  - ☐ Laden Sie die grafische Benutzeroberfläche neu.
  - ☐ Melden Sie sich erneut an.
- Das Gerät verwendet die Einstellungen des Konfigurationsprofils ab sofort im laufenden Betrieb.

Schalten Sie die Funktion *Konfigurationsänderungen rückgängig machen* ein, bevor Sie ein anderes Konfigurationsprofil aktivieren. Bricht danach die Verbindung ab, lädt das Gerät das zuletzt als „ausgewählt“ gekennzeichnete Konfigurationsprofil aus dem permanenten Speicher (*NVM*). Das Gerät ist dann wieder erreichbar.

Ist die Konfigurations-Verschlüsselung inaktiv, lädt das Gerät das Konfigurationsprofil ausschließlich dann, wenn dieses unverschlüsselt ist. Ist die Konfigurations-Verschlüsselung aktiv, lädt das Gerät das Konfigurationsprofil ausschließlich dann, wenn dieses verschlüsselt ist und das Passwort mit dem im Gerät gespeicherten Passwort übereinstimmt.

Wenn Sie ein älteres Konfigurationsprofil aktivieren, übernimmt das Gerät die Einstellungen der in dieser Software-Version vorhandenen Funktionen. Das Gerät setzt die Werte der neuen Funktionen auf ihren voreingestellten Wert.

Auswählen

Kennzeichnet das in der Tabelle markierte Konfigurationsprofil als „ausgewählt“. Anschließend ist in Spalte *Ausgewählt* das Kontrollkästchen `markiert`.

Das Gerät lädt die Einstellungen dieses Konfigurationsprofils beim Neustart oder beim Anwenden der Funktion *Konfigurationsänderungen rückgängig machen* in den flüchtigen Speicher (*RAM*).

- Kennzeichnen Sie ein unverschlüsseltes Konfigurationsprofil ausschließlich dann als „ausgewählt“, wenn die Konfigurations-Verschlüsselung im Gerät ausgeschaltet ist.
- Kennzeichnen Sie ein verschlüsseltes Konfigurationsprofil ausschließlich dann als „ausgewählt“, wenn die Konfigurations-Verschlüsselung im Gerät eingeschaltet ist und das Passwort mit dem im Gerät gespeicherten Passwort übereinstimmt.

Andernfalls ist das Gerät außerstande, beim nächsten Neustart die Einstellungen des Konfigurationsprofils zu laden und zu entschlüsseln. Für diesen Fall legen Sie im Dialog *Diagnose > System > Selbsttest* fest, ob das Gerät mit Werkseinstellungen startet oder den Neustart abbricht und anhält.

Anmerkung: Als „ausgewählt“ lassen sich ausschließlich Konfigurationsprofile kennzeichnen, die im permanenten Speicher (*NVM*) gespeichert sind.

Wenn im Dialog *Grundeinstellungen > Externer Speicher* das Kontrollkästchen in Spalte *Sichere Konfiguration beim Speichern*markiert ist, kennzeichnet das Gerät auch das gleichnamige Konfigurationsprofil auf dem externen Speicher als „ausgewählt“.

Importieren...

Öffnet das Fenster *Importieren...*, um ein Konfigurationsprofile zu importieren.

Voraussetzung ist, dass Sie das Konfigurationsprofil zuvor mit der Schaltfläche *Exportieren...* oder mit dem Link in Spalte *Profilname* exportiert haben.

☐ Wählen Sie in der Dropdown-Liste *Select source* aus, woher das Gerät das Konfigurationsprofil importiert.

▶ *PC/URL*
Das Gerät importiert das Konfigurationsprofil vom lokalen PC oder von einem Remote-Server.

▶ *Externer Speicher*
Das Gerät importiert das Konfigurationsprofil vom externen Speicher.

☐ Wenn oben *PC/URL* ausgewählt ist, legen Sie im Rahmen *Import profile from PC/URL* die Datei des zu importierenden Konfigurationsprofils fest.

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

– Import von einem FTP-Server
Befindet sich die Datei auf einem FTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
`ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Dateiname>`

– Import von einem TFTP-Server
Befindet sich die Datei auf einem TFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
`tftp://<IP-Adresse>/<Pfad>/<Dateiname>`

– Import von einem SCP- oder SFTP-Server
Befindet sich die Datei auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in einer der folgenden Formen fest:
`scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`
Nach Klicken der Schaltfläche *Start* zeigt das Gerät das Fenster *Anmeldeinformationen*. Geben Sie dort *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
`scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>`

☐ Wenn oben *Externer Speicher* ausgewählt ist, legen Sie im Rahmen *Import profile from external memory* die Datei des zu importierenden Konfigurationsprofils fest.
Wählen Sie in der Dropdown-Liste *Profilname* den Namen des zu importierenden Konfigurationsprofils.

☐ Im Rahmen *Ziel* legen Sie fest, wo das Gerät das importierte Konfigurationsprofil speichert.
Im Feld *Profilname* legen Sie den Namen fest, unter dem das Gerät das Konfigurationsprofil speichert.
Im Feld *Speicher-Typ* legen Sie den Speicherort für das Konfigurationsprofil fest. Voraussetzung ist, dass Sie in der Dropdown-Liste *Select source* den Eintrag *PC/URL* auswählen.

▶ *RAM*
Das Gerät speichert das Konfigurationsprofil im flüchtigen Speicher (*RAM*) des Geräts. Dies ersetzt die `running-config`, das Gerät verwendet sofort die Einstellungen des importierten Konfigurationsprofils. Das Gerät trennt die Verbindung zur grafischen Benutzeroberfläche. Laden Sie die grafische Benutzeroberfläche neu. Melden Sie sich erneut an.

▶ *NVM*
Das Gerät speichert das Konfigurationsprofil im permanenten Speicher (*NVM*) des Geräts.

Beim Importieren eines Konfigurationsprofils übernimmt das Gerät die Einstellungen wie folgt:

- Wenn das Konfigurationsprofil von demselben Gerät oder von einem identisch ausgestatteten Gerät des gleichen Typs exportiert wurde:
  Das Gerät übernimmt die Einstellungen komplett.
- Wenn das Konfigurationsprofil von einem anderen Gerät exportiert wurde:
  Das Gerät übernimmt die Einstellungen, die es mit seiner Hardware-Ausstattung und seinem Software-Level interpretieren kann.
  Die übrigen Einstellungen übernimmt das Gerät aus seinem `running-config`-Konfigurationsprofil.

Bezüglich Verschlüsselung des Konfigurationsprofils lesen Sie auch den Hilfetext zum Rahmen *Konfigurations-Verschlüsselung*. Das Gerät importiert das Konfigurationsprofil unter den folgenden Bedingungen:

- Die Konfigurations-Verschlüsselung des Geräts ist inaktiv. Das Konfigurationsprofil ist unverschlüsselt.
- Die Konfigurations-Verschlüsselung des Geräts ist aktiv. Das Konfigurationsprofil ist mit dem gleichen Passwort verschlüsselt, welches das Gerät gegenwärtig verwendet.

Exportieren...

Exportiert das in der Tabelle markierte Konfigurationsprofil und speichert es als XML-Datei auf einem Remote-Server.

Um die Datei auf Ihrem PC zu speichern, klicken Sie den Link in Spalte *Profilname*, um den Speicherort zu wählen und den Dateinamen festzulegen.

Das Gerät bietet Ihnen folgende Möglichkeiten, ein Konfigurationsprofil zu exportieren:

- Export auf einen FTP-Server
  Um die Datei auf einem FTP-Server zu speichern, legen Sie den URL zur Datei in der folgenden Form fest:
  `ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Dateiname>`
- Export auf einen TFTP-Server
  Um die Datei auf einem TFTP-Server zu speichern, legen Sie den URL zur Datei in der folgenden Form fest:
  `tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
- Export auf einen SCP- oder SFTP-Server
  Um die Datei auf einem SCP- oder SFTP-Server zu speichern, legen Sie den URL zur Datei in einer der folgenden Formen fest:
  - `scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`
    Nach Klicken der Schaltfläche *Ok* zeigt das Gerät das Fenster *Anmeldeinformationen*. Geben Sie dort *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
  - `scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>`

Load running-config as script

Importiert eine Skript-Datei, die das gegenwärtige Konfigurationsprofil `running config` ändert.

Das Gerät bietet Ihnen folgende Möglichkeiten, eine Skript-Datei zu importieren:

- Import vom PC
  Befindet sich die Datei auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie die Datei in den  -Bereich. Alternativ klicken Sie in den Bereich, um die Datei auszuwählen.
- Import von einem FTP-Server
  Befindet sich die Datei auf einem FTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  `ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Dateiname>`

- Import von einem TFTP-Server
  Befindet sich die Datei auf einem TFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  `tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
- Import von einem SCP- oder SFTP-Server
  Befindet sich die Datei auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in einer der folgenden Formen fest:
  `scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`

Anmerkung: Das Gerät wendet Skript-Dateien zusätzlich zu den gegenwärtigen Einstellungen an. Vergewissern Sie sich, dass die Skript-Datei keine Teile enthält, die mit den gegenwärtigen Einstellungen in Konflikt stehen.

Save running-config as script

Speichert das Konfigurationsprofil `running config` als Skript-Datei auf dem lokalen PC. Dies ermöglicht Ihnen, die gegenwärtigen Einstellungen des Geräts zu sichern oder auf anderen Geräten zu verwenden.

Auf Lieferzustand zurücksetzen...

Setzt die Einstellungen im Gerät auf die voreingestellten Werte zurück.

- Das Gerät löscht die gespeicherten Konfigurationsprofile aus dem flüchtigen Speicher (*RAM*) und aus dem permanenten Speicher (*NVM*).
- Das Gerät löscht das vom Webserver im Gerät verwendete HTTPS-Zertifikat.
- Das Gerät löscht den vom SSH-Server im Gerät verwendeten RSA-Schlüssel (Host Key).
- Ist ein externer Speicher angeschlossen, löscht das Gerät die auf dem externen Speicher gespeicherten Konfigurationsprofile.
- Nach kurzer Zeit startet das Gerät neu mit den im Lieferzustand voreingestellten Werten.

Auf Default-Zustand zurücksetzen

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

1.6 Externer Speicher

[Grundeinstellungen > Externer Speicher]

Dieser Dialog ermöglicht Ihnen, Funktionen zu aktivieren, die das Gerät automatisch in Verbindung mit dem externen Speicher ausführt. Der Dialog zeigt außerdem den Betriebszustand sowie Identifizierungsmerkmale des externen Speichers.

Tabelle

Typ

Zeigt den Typ des externen Speichers.

Mögliche Werte:

- *usb*
  Externer USB-Speicher (EAM)

Status

Zeigt den Betriebszustand des externen Speichers.

Mögliche Werte:

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

Beschreibbar

Zeigt, ob das Gerät Schreibzugriff auf den externen Speicher hat.

Mögliche Werte:

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

Automatisches Software-Update

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

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die automatische Aktualisierung der Geräte-Software während des Neustarts ist aktiviert. Das Gerät aktualisiert die Geräte-Software, wenn sich folgende Dateien im externen Speicher befinden:
  - die Image-Datei der Geräte-Software
  - eine Textdatei `startup.txt` mit dem Inhalt `autoUpdate=<Name_der_Image-Datei>.bin`
- `unmarkiert`
  Die automatische Aktualisierung der Geräte-Software während des Neustarts ist deaktiviert.

SSH-Key automatisch uploaden

Aktiviert/deaktiviert das Laden des RSA-Schlüssels vom externen Speicher beim Neustart.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Laden des RSA-Schlüssels ist aktiviert.
  Beim Neustart lädt das Gerät den RSA-Schlüssel vom externen Speicher, wenn sich im externen Speicher folgende Dateien befinden:
  - SSH-RSA-Schlüssel-Datei
  - eine Textdatei `startup.txt` mit dem Inhalt
    `autoUpdateRSA=<Dateiname_des_SSH-RSA-Schlüssels>`

  Meldungen zeigt das Gerät auf der Systemkonsole der seriellen Schnittstelle.
- `unmarkiert`
  Das Laden des RSA-Schlüssels ist deaktiviert.

Anmerkung: Beim Laden des RSA-Schlüssels aus dem externen Speicher (*ENVM*) überschreibt das Gerät die im permanenten Speicher (*NVM*) vorhandenen Schlüssel.

Konfigurations-Priorität

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

Mögliche Werte:

- `disable`
  Das Gerät lädt das Konfigurationsprofil aus dem permanenten Speicher (*NVM*).
- `first`
  Das Gerät lädt das Konfigurationsprofil vom externen Speicher.
  Findet das Gerät auf dem externen Speicher kein Konfigurationsprofil, lädt es das Konfigurationsprofil aus dem permanenten Speicher (*NVM*).

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

Wenn die Spalte *Konfigurations-Priorität* den Wert `first` hat und das Konfigurationsprofil unverschlüsselt ist, dann zeigt der Rahmen *Sicherheits-Status* im Dialog *Grundeinstellungen > System* einen Alarm.

Im Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus*, Registerkarte *Global*, Spalte *Überwachen* legen Sie fest, ob das Gerät den Parameter *Unverschlüsselte Konfiguration vom externen Speicher laden* überwacht.

Sichere Konfiguration beim Speichern

Aktiviert/deaktiviert das Erzeugen einer Kopie im externen Speicher beim Speichern des Konfigurationsprofils.

Mögliche Werte:

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

Hersteller-ID

Zeigt den Namen des Speicher-Herstellers.

Revision

Zeigt die durch den Speicher-Hersteller vorgegebene Revisionsnummer.

Version

Zeigt die durch den Speicher-Hersteller vorgegebene Versionsnummer.

Name

Zeigt die durch den Speicher-Hersteller vorgegebene Produktbezeichnung.

Seriennummer

Zeigt die durch den Speicher-Hersteller vorgegebene Seriennumer.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

1.7 Port

[Grundeinstellungen > Port]

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

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

[Konfiguration]

Tabelle

Port

Zeigt die Nummer des Ports.

Name

Bezeichnung des Ports.

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

Port an

Aktiviert/deaktiviert den Port.

Mögliche Werte:
- `markiert` (Voreinstellung)
  Der Port ist aktiv.
- `unmarkiert`
  Der Port ist inaktiv. Der Port sendet und empfängt keine Daten.

Zustand

Zeigt, ob der Port gegenwärtig physikalisch eingeschaltet oder ausgeschaltet ist.

Mögliche Werte:

- `markiert`
  Der Port ist physikalisch eingeschaltet.
- `unmarkiert`
  Der Port ist physikalisch ausgeschaltet.
  Wenn die Funktion *Port an* aktiv ist, hat die Funktion *Auto-Disable* den Port ausgeschaltet.
  Die Einstellungen der Funktion *Auto-Disable* legen Sie im Dialog *Diagnose > Ports > Auto-Disable* fest.

Power-State (Port aus)

Legt fest, ob der Port physikalisch eingeschaltet oder ausgeschaltet ist, wenn Sie den Port mit der Funktion *Port an* deaktivieren.

Mögliche Werte:

- `markiert`
  Der Port bleibt physikalisch eingeschaltet. Ein angeschlossenes Gerät empfängt einen aktiven Link.
- `unmarkiert` (Voreinstellung)
  Der Port ist physikalisch ausgeschaltet.

Automatisches Ausschalten

Legt fest, wie sich der Port verhält, wenn kein Kabel angeschlossen ist.

Mögliche Werte:

- *`no-power-save`* (Voreinstellung)
  Der Port bleibt aktiviert.
- *`auto-power-down`*
  Der Port schaltet in den Energiesparmodus.
- *`unsupported`*
  Der Port unterstützt diese Funktion nicht und bleibt aktiviert.

Automatische Konfiguration

Aktiviert/deaktiviert die automatische Auswahl des Betriebsmodus für den Port.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die automatische Auswahl des Betriebsmodus ist aktiv.
  Der Port handelt den Betriebsmodus per Autonegotiation selbständig aus und erkennt die Belegung der Anschlüsse des TP-Ports automatisch (Auto Cable-Crossing). Diese Einstellung hat Vorrang vor der manuellen Einstellung des Betriebsmodus.
  Bis der Port den Betriebsmodus eingestellt hat, vergehen einige Sekunden.
- `unmarkiert`
  Die automatische Auswahl des Betriebsmodus ist inaktiv.
  Der Port arbeitet mit den Werten, die Sie in Spalte *Manuelle Konfiguration* und in Spalte *Manuelles Cable-Crossing (Auto. Konfig. aus)*festlegen.
- Ausgegraute Darstellung
  Keine automatische Auswahl des Betriebsmodus.

Manuelle Konfiguration

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

Mögliche Werte:

- `10 Mbit/s HDX`
  Halbduplex-Verbindung
- `10 Mbit/s FDX`
  Vollduplex-Verbindung
- `100 Mbit/s HDX`
  Halbduplex-Verbindung
- `100 Mbit/s FDX`
  Vollduplex-Verbindung
- `1000 Mbit/s FDX`
  Vollduplex-Verbindung
- `2500 Mbit/s FDX`
  Vollduplex-Verbindung

Anmerkung: Die tatsächlich zur Verfügung stehenden Betriebsmodi des Ports sind abhängig von der Ausstattung des Geräts.

Link/ Aktuelle Betriebsart

Zeigt, welchen Betriebsmodus der Port gegenwärtig verwendet.

Mögliche Werte:

- `-`
  Kein Kabel angesteckt, keine Verbindung.
- `10 Mbit/s HDX`
  Halbduplex-Verbindung
- `10 Mbit/s FDX`
  Vollduplex-Verbindung
- `100 Mbit/s HDX`
  Halbduplex-Verbindung
- `100 Mbit/s FDX`
  Vollduplex-Verbindung
- `1000 Mbit/s FDX`
  Vollduplex-Verbindung
- `2500 Mbit/s FDX`
  Vollduplex-Verbindung

Anmerkung: Die tatsächlich zur Verfügung stehenden Betriebsmodi des Ports sind abhängig von der Ausstattung des Geräts.

Manuelles Cable-Crossing (Auto. Konfig. aus)

Legt die Belegung der Anschlüsse eines TP-Ports fest.

Voraussetzung ist, dass die Funktion *Automatische Konfiguration* ausgeschaltet ist.

Mögliche Werte:

- *mdi*
  Das Gerät vertauscht das Sende- und Empfangsleitungspaar auf dem Port.

- `mdix` (Voreinstellung auf TP-Ports)
  Das Gerät hilft, das Vertauschen der Sende- und Empfangsleitungspaare auf dem Port zu vermeiden.
- `auto-mdix`
  Das Gerät erkennt das Sende- und Empfangsleitungspaar des angeschlossenen Geräts und stellt sich automatisch darauf ein.
  Beispiel: Wenn Sie ein Endgerät mit gekreuztem Kabel anschließen, stellt das Gerät den Port automatisch von `mdix` auf `mdi`.
- `unsupported` (Voreinstellung auf optischen Ports oder TP-SFP-Ports)
  Der Port unterstützt diese Funktion nicht.

Flusskontrolle

Aktiviert/deaktiviert die Flusskontrolle auf dem Port.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Flusskontrolle auf dem Port ist aktiv.
  Auf dem Port ist das Senden und Auswerten von Pause-Paketen (Vollduplex-Betrieb) oder Kollisionen (Halbduplex-Betrieb) aktiviert.
  - ☐ Um die Flusskontrolle im Gerät einzuschalten, aktivieren Sie zusätzlich die Funktion *Flusskontrolle* im Dialog *Switching > Global*.
  - ☐ Aktivieren Sie die Flusskontrolle außerdem auf dem Port des mit diesem Port verbundenen Geräts.

  Auf einem Uplink-Port führt das Aktivieren der Flusskontrolle möglicherweise zu unerwünschten Sendepausen im übergeordneten Netzsegment („Wandering Backpressure“).
- `unmarkiert`
  Die Flusskontrolle auf dem Port ist inaktiv.

Wenn Sie eine Redundanzfunktion einsetzen, dann deaktivieren Sie die Flusskontrolle auf den beteiligten Ports. Wenn die Flusskontrolle und die Redundanzfunktion gleichzeitig aktiv sind, arbeitet die Redundanzfunktion möglicherweise anders als beabsichtigt.

Trap senden (Link-Up/Down)

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung des Link-Status auf dem Port erkennt.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Senden von SNMP-Traps ist aktiv.
  Wenn das Gerät eine Link-Status-Änderung erkennt, sendet es einen SNMP-Trap.
- `unmarkiert`
  Das Senden von SNMP-Traps ist inaktiv.

Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* einschalten und mindestens ein Trap-Ziel festlegen.

MTU

Legt die maximal zulässige Größe der Ethernet-Pakete auf dem Port in Byte fest.

Mögliche Werte:

- `1518..9720` (Voreinstellung: `1518`)
  Mit der Einstellung `1518` vermittelt der Port die Ethernet-Pakete bis zu einschließlich folgender Größe:
  - 1518 Byte ohne VLAN-Tag
    (1514 Byte + 4 Byte CRC)
  - 1522 Byte mit VLAN-Tag
    (1518 Byte + 4 Byte CRC)

Diese Einstellung ermöglicht Ihnen, die maximal erlaubte Größe von Ethernet-Paketen zu erhöhen, die dieser Port empfangen oder senden kann.

Mögliche Anwendungsfälle sind:

- Wenn Sie das Gerät im Transfer-Netz mit Double-VLAN-Tagging einsetzen, ist möglicherweise eine um 4 Byte größere *MTU* erforderlich.

Auf anderen Interfaces legen Sie die maximal zulässige Größe der Ethernet-Pakete wie folgt fest:

- *Link-Aggregation*-Interfaces
  Dialog *Switching > L2-Redundanz > Link-Aggregation*, Spalte *MTU*

Signal

Aktiviert/deaktiviert das Blinken der Port-LED. Diese Funktion ermöglicht Ihnen, den Port im Feld zu identifizieren.

Mögliche Werte:

- `markiert`
  Das Blinken der Port-LED ist aktiv.
  Die Port-LED blinkt solange, bis Sie die Funktion wieder ausschalten.
- `unmarkiert` (Voreinstellung)
  Das Blinken der Port-LED ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Port-Statistiken leeren

Setzt die Zähler der Portstatistik auf `0`.

[Statistiken]

Diese Registerkarte zeigt pro Port folgenden Überblick:

- Anzahl der vom Gerät empfangenen Datenpakete/Bytes
  - *Empfangene Pakete*
  - *Empfangene Oktets*
  - *Empfangene Unicast-Pakete*
  - *Empfangene Multicast-Pakete*
  - *Empfangene Broadcast-Pakete*
- Anzahl der vom Gerät gesendeten Datenpakete/Bytes
  - *Gesendete Pakete*
  - *Gesendete Oktets*
  - *Gesendete Unicast-Pakete*
  - *Gesendete Multicast-Pakete*
  - *Gesendete Broadcast-Pakete*
- Anzahl der vom Gerät erkannten Fehler
  - *Empfangene Fragmente*
  - *Erkannte CRC-Fehler*
  - *Erkannte Kollisionen*
- Anzahl der vom Gerät empfangenen Datenpakete pro Größenkategorie
  - *Pakete 64 Byte*
  - *Pakete 65 bis 127 Byte*
  - *Pakete 128 bis 255 Byte*
  - *Pakete 256 bis 511 Byte*
  - *Pakete 512 bis 1023 Byte*
  - *Pakete 1024 bis 1518 Byte*
- Anzahl der vom Gerät verworfenen Datenpakete
  - *Empfangsseitig verworfene Pakete*
  - *Sendeseitig verworfene Pakete*

Um die Tabelle nach einem bestimmten Kriterium zu sortieren, klicken Sie die Überschrift der entsprechenden Spalte.

Um die Tabelle beispielsweise nach der Anzahl der empfangenen Bytes in aufsteigender Reihenfolge zu sortieren, klicken Sie 1 Mal die Überschrift der Spalte *Empfangene Oktets*. Um absteigend zu sortieren, klicken Sie die Überschrift erneut.

Um die Portstatistik-Zähler in der Tabelle auf 0 zurückzusetzen, führen Sie die folgenden Schritte aus:

- ☐ Klicken Sie im Dialog *Grundeinstellungen > Port* die Schaltfläche ☰ und dann den Eintrag *Port-Statistiken leeren*.
  oder
- ☐ Klicken Sie im Dialog *Grundeinstellungen > Neustart* die Schaltfläche *Port-Statistiken leeren*.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Port-Statistiken leeren

Setzt die Zähler der Portstatistik auf 0.

[Netzlast]

Diese Registerkarte zeigt die Auslastung (Netzlast) der einzelnen Ports.

Tabelle

Port

Zeigt die Nummer des Ports.

Netzlast [%]

Zeigt die gegenwärtige Netzlast in Prozent, bezogen auf die in Spalte *Kontroll-Intervall [s]* festgelegte Zeitspanne.

Die Netzlast ist das Verhältnis der empfangen Datenmenge zur maximal möglichen Datenmenge bei der gegenwärtig konfigurierten Datenrate.

Unterer Grenzwert [%]

Legt einen unteren Grenzwert für die Netzlast fest. Unterschreitet die Netzlast des Ports diesen Wert, zeigt Spalte *Alarm* einen Alarm.

Mögliche Werte:

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

Der Wert `0` deaktiviert den unteren Grenzwert.

Oberer Grenzwert [%]

Legt einen oberen Grenzwert für die Netzlast fest. Überschreitet die Netzlast des Ports diesen Wert, zeigt Spalte *Alarm* einen Alarm.

Mögliche Werte:

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

Der Wert `0` deaktiviert den oberen Grenzwert.

Kontroll-Intervall [s]

Legt die Zeitspanne in Sekunden fest.

Mögliche Werte:

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

Alarm

Kennzeichnet den Alarmzustand für die Netzlast.

Mögliche Werte:

- `markiert`
  Die Netzlast des Ports liegt unter dem in Spalte *Unterer Grenzwert [%]* oder über dem in Spalte *Oberer Grenzwert [%]* festgelegten Wert. Das Gerät sendet einen SNMP-Trap.
- `unmarkiert`
  Die Netzlast des Ports liegt über dem in Spalte *Unterer Grenzwert [%]* und unter dem in Spalte *Oberer Grenzwert [%]* festgelegten Wert.
  Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog *Diagnose* > Statuskonfiguration > *Alarme (Traps)* einschalten und mindestens ein Trap-Ziel festlegen.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Port-Statistiken leeren

Setzt die Zähler der Portstatistik auf `0`.

1.8 Power over Ethernet (MCSESP)

[Grundeinstellungen > Power over Ethernet]

Bei Power-over-Ethernet (PoE) versorgt das Strom liefernde Gerät (Power Source Equipment, PSE) die Stromverbraucher (Powered Devices, PD) wie IP-Telefone über das Twisted-Pair-Kabel mit Strom.

Ob Ihr Gerät *Power over Ethernet* unterstützt, können Sie anhand des Produktcodes und einer PoE-spezifischen Kennzeichnung am Gehäuse des PSE-Geräts feststellen. Die PoE-Ports des Geräts unterstützen Power over Ethernet nach IEEE 802.3at.

Das System stellt ein internes, maximales Leistungsbudget für die Ports zur Verfügung. Entsprechend der ermittelten Klasse eines angeschlossenen Stromverbrauchers reservieren die Ports Strom. Die tatsächlich abgegebene Leistung gleicht der Reserveleistung oder ist kleiner als diese.

Die Ausgangsleistung verwalten Sie mit dem Parameter *Priorität*. Wenn die Summe der für die angeschlossenen Geräte erforderlichen Leistung die verfügbare Leistung überschreitet, geht das Gerät beim Abschalten des für die Ports bereitgestellten Stroms nach der festgelegten Priorität vor. Beim Abschalten des für die Ports bereitgestellten Stroms beginnt das Gerät bei den Ports, bei denen Sie einen niedrige Priorität festgelegt haben. Wenn mehrere Ports eine niedrige Priorität aufweisen, beginnt das Gerät beim Abschalten bei den höher nummerierten Ports.

Das Menü enthält die folgenden Dialoge:

- PoE Global
- PoE Port

1.8.1 PoE Global

[Grundeinstellungen > Power over Ethernet > Global]

Anhand der in diesem Dialog festgelegten Einstellungen liefert das Gerät Strom an die Endnutzergeräte. Wenn der Stromverbrauch den benutzerdefinierten Grenzwert erreicht, sendet das Gerät einen SNMP-Trap.

Funktion

Funktion

Schaltet die Funktion *Power over Ethernet* ein/aus.

Mögliche Werte:

- `An` (Voreinstellung)
  Die Funktion *Power over Ethernet* ist eingeschaltet.
- `Aus`
  Die Funktion *Power over Ethernet* ist ausgeschaltet.

Konfiguration

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps.

Wenn der Stromverbrauch den benutzerdefinierten Grenzwert übersteigt, sendet das Gerät einen SNMP-Trap.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Gerät sendet SNMP-Traps.
- `unmarkiert`
  Das Gerät sendet keine SNMP-Traps.

Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog *Diagnose* > Statuskonfiguration > *Alarme (Traps)* einschalten und mindestens ein Trap-Ziel festlegen.

Grenzwert [%]

Legt den Grenzwert für den allgemeinen Stromverbrauch in Prozent fest.

Das Gerät misst die Gesamtausgangsleistung und sendet einen SNMP-Trap, wenn die Ausgangsleistung diesen Grenzwert überschreitet.

Mögliche Werte:

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

Systemleistung

Budget [W]

Zeigt die für das globale Leistungsbudget verfügbare Gesamtstromleistung.

Reserviert [W]

Zeigt die allgemeine Reserveleistung. Entsprechend der ermittelten Klassen von angeschlossenen Stromverbrauchern reserviert das Gerät Strom. Die Reserveleistung gleicht der tatsächlich abgegebenen Leistung oder ist kleiner als diese.

Abgegeben [W]

Zeigt die tatsächlich an die Module abgegebene Leistung in Watt.

Abgegeben [mA]

Zeigt den tatsächlich an die Module abgegebenen Strom in Milliampere.

Tabelle

Modul

Gerätemodul, auf das sich die Tabelleneinträge beziehen.

Konfiguriertes Leistungs-Budget [W]

Legt die Modul-Leistung für die Verteilung an die Ports fest.

Mögliche Werte:

- `0..n` (Voreinstellung: n)
  Hierbei entspricht `n` dem Wert in Spalte *Max. Leistungs-Budget [W]*.

Max. Leistungs-Budget [W]

Zeigt die maximal verfügbare Leistung für dieses Modul.

Reservierte Leistung [W]

Zeigt die reservierte Leistung für das Modul entsprechend der ermittelten Klassen von angeschlossenen Stromverbrauchern.

Abgegebene Leistung [W]

Zeigt die tatsächliche Leistung in Watt, die das Gerät an die an den Port angeschlossenen Stromverbraucher abgibt.

Abgegebener Strom [mA]

Zeigt den tatsächlichen Strom in Milliampere, den das Gerät an die an den Port angeschlossenen Stromverbraucher abgibt.

Stromquelle

Zeigt den Stromversorger des Geräts.

Mögliche Werte:

- *intern*
  Interne Stromversorgung
- *extern*
  Externe Stromversorgung

Grenzwert [%]

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

Mögliche Werte:

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

Trap senden

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

Mögliche Werte:

- `markiert`
  Das Senden von SNMP-Traps ist aktiv.
  Wenn der Stromverbrauch des Moduls den benutzerdefinierten Grenzwert überschreitet, sendet das Gerät einen SNMP-Trap.
- `unmarkiert` (Voreinstellung)
  Das Senden von SNMP-Traps ist inaktiv.

Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog *Diagnose* > Statuskonfiguration > *Alarme (Traps)* einschalten und mindestens ein Trap-Ziel festlegen.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

1.8.2 PoE Port

[Grundeinstellungen > Power over Ethernet > Port]

Liegt die Leistungsaufnahme über der möglichen Leistung, schaltet das Gerät den Strom für Geräte im Netz gemäß den Prioritätsstufen und Port-Nummern ab. Sollten die angeschlossenen Stromverbraucher mehr Strom anfordern als das Gerät liefert, schaltet das Gerät die Funktion *Power over Ethernet* auf den Ports aus. Das Gerät schaltet die Funktion *Power over Ethernet* zuerst auf den Ports mit niedrigster Priorität aus. Wenn mehrere Ports die gleiche Priorität haben, deaktiviert das Gerät die *Power over Ethernet*-Funktion zuerst auf den Ports mit höherer Port-Nummer. Darüber hinaus schaltet das Gerät den Strom für Geräte im Netz für einen festgelegten Zeitraum ab.

Tabelle

Port

Zeigt die Nummer des Ports.

PoE an

Aktiviert/deaktiviert den für den Port bereitgestellten PoE-Strom.

Beim Aktivieren/Deaktivieren der Funktion protokolliert das Gerät ein Ereignis in der Log-Datei (System Log).

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die PoE-Stromversorgung auf dem Port ist aktiv.
- `unmarkiert`
  Die PoE-Stromversorgung auf dem Port ist inaktiv.

Fast-Startup

Aktiviert/deaktiviert die PoE-Schnellstart-Funktion des Geräts.

Voraussetzung ist, dass das Kontrollkästchen in Spalte *PoE an* markiert ist.

Mögliche Werte:

- `markiert`
  Die Schnellstart-Funktion ist aktiv. Vor dem Laden der eigenen Konfiguration versorgt das Gerät die Stromverbraucher mit Strom.
- `unmarkiert` (Voreinstellung)
  Die Schnellstart-Funktion ist inaktiv. Nach dem Laden der eigenen Konfiguration versorgt das Gerät die Stromverbraucher mit Strom.

Priorität

Legt die Port-Priorität fest.

Um Stromüberlastungen zu vermeiden, schaltet das Gerät die Ports mit niedrigerer Priorität zuerst aus. Um zu vermeiden, dass das Gerät Ports abschaltet, die wesentliche Geräte speisen, legen Sie für diese Ports eine hohe Priorität fest.

Mögliche Werte:

- *critical*
- *high*
- *low* (Voreinstellung)

Status

Zeigt den Port-Status für die Erkennung der zu speisenden Geräte.

Mögliche Werte:

- *disabled*
  Zeigt, dass sich das Zustandsdiagramm des Stromversorgers (PSE) im Zustand DISABLED befindet.
- *deliveringPower*
  Zeigt, dass das Gerät die Klasse des angeschlossenen Stromverbrauchers ermittelt hat und dass sich das Zustandsdiagramm des Stromversorgers (PSE) im Zustand POWER ON befindet.
- *fault*
  Zeigt, dass sich das Zustandsdiagramm des Stromversorgers (PSE) im Zustand TEST ERROR befindet.
- *otherFault*
  Zeigt, dass sich das Zustandsdiagramm des Stromversorgers (PSE) im Zustand IDLE befindet.
- *searching*
  Zeigt, dass sich das Zustandsdiagramm des Stromversorgers (PSE) in einem nicht gelisteten Zustand befindet.
- *test*
  Zeigt, dass sich das Zustandsdiagramm des Stromversorgers (PSE) im Zustand TEST MODE befindet.

Erkannte Klasse

Zeigt die Leistungsklasse des an den Port angeschlossenen Stromverbrauchers.

Mögliche Werte:

- *Klasse 0*
- *Klasse 1*
- *Klasse 2*
- *Klasse 3*
- *Klasse 4*

Klasse 0
Klasse 1
Klasse 2
Klasse 3
Klasse 4

Aktiviert/deaktiviert den Strom der Klassen 0 bis 4 auf dem Port.

Mögliche Werte:

- markiert (Voreinstellung)
- unmarkiert

Verbrauch [W]

Zeigt den gegenwärtigen Stromverbrauch des Ports in Watt.

Mögliche Werte:

▶ `0,0..30,0`

Verbrauch [mA]

Zeigt den am Port abgegebenen Strom in Milliampere.

Mögliche Werte:

▶ `0..600`

Leistungs-Limit [W]

Legt die maximale Leistung in Watt fest, die der Port ausgibt.

Diese Funktion ermöglicht Ihnen, das verfügbare Leistungsbudget nach Bedarf über die PoE-Ports zu verteilen.

Für ein verbundenes Gerät ohne Angabe einer „Leistungsklasse“ reserviert der Port die feste Leistung von 15,4 W (Klasse 0), selbst wenn das Gerät eine geringere Leistung benötigt. Die überschüssige Leistung steht keinem anderen Port zur Verfügung.

Indem Sie die Leistungsgrenze festlegen, reduzieren Sie die reservierte Leistung auf den tatsächlichen Bedarf des verbundenen Geräts. Die nicht genutzte Leistung steht den anderen Ports zur Verfügung.

Wenn die exakte Leistungsaufnahme des zu speisenden Geräts unbekannt ist, zeigt das Gerät den Wert in Spalte *Max. Verbrauch [W]*. Vergewissern Sie sich, dass die Leistungsgrenze größer ist als der Wert in Spalte *Max. Verbrauch [W]*.

Wenn die festgestellte maximale Leistung über der festgelegten Leistungsgrenze liegt, betrachtet das Gerät die Leistungsgrenze als ungültig. In diesem Fall zieht das Gerät die PoE-Klasse zur Berechnung heran.

Mögliche Werte:

▶ `0,0..30,0` (Voreinstellung: `0`)

Max. Verbrauch [W]

Zeigt die maximale Leistung in Milliwatt, die das Gerät bis zum betreffenden Zeitpunkt aufgenommen hat.

Den Wert setzen Sie zurück, wenn Sie PoE deaktivieren oder die Verbindung zum verbundenen Gerät trennen.

Name

Legt die Bezeichnung des Ports fest.

Legen Sie einen beliebigen Namen fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen

Strom automatisch ausschalten

Aktiviert/deaktiviert die Funktion *Strom automatisch ausschalten* gemäß Einstellung.

Mögliche Werte:

- `markiert`
- `unmarkiert` (Voreinstellung)

Strom ausschalten um [hh:mm]

Legt die Uhrzeit fest, zu der das Gerät bei Aktivierung der Funktion *Strom automatisch ausschalten* den Strom für den Port ausschaltet.

Mögliche Werte:

- `00:00..23:59` (Voreinstellung: `00:00`)

Strom wiedereinschalten um [hh:mm]

Legt die Uhrzeit fest, zu der das Gerät bei Aktivierung der Funktion *Strom automatisch ausschalten* den Strom für den Port einschaltet.

Mögliche Werte:

- `00:00..23:59` (Voreinstellung: `00:00`)

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

1.9 Neustart

[Grundeinstellungen > Neustart]

Dieser Dialog ermöglicht Ihnen, das Gerät neu zu starten, Port-Zähler und Adresstabellen zurückzusetzen sowie Log-Dateien zu löschen.

Neustart

Neustart in

Zeigt die verbleibende Zeit bis das Gerät neu startet.

Um die Anzeige der verbleibenden Zeit zu aktualisieren, klicken Sie die Schaltfläche  .

Abbrechen

Bricht den verzögerten Neustart ab.

Kaltstart...

Öffnet den Dialog *Neustart*, um einen sofortigen oder einen verzögerten Neustart des Geräts auszulösen.

Wenn sich das Konfigurationsprofil im flüchtigen Speicher (`RAM`) und das „ausgewählte“ Konfigurationsprofil im permanenten Speicher (`NVM`) unterscheiden, zeigt das Gerät den Dialog *Warnung*.

- Um die Änderungen permanent zu speichern, klicken Sie im Dialog *Warnung* die Schaltfläche *Ja*.
- Um die Änderungen zu verwerfen, klicken Sie im Dialog *Warnung* die Schaltfläche *Nein*.
- Im Feld *Neustart in* legen Sie die Verzögerungszeit für den verzögerten Neustart fest.
  Mögliche Werte:
  – `00:00:00..596:31:23` (Voreinstellung: `00:00:00`)

Nach Ablauf der Verzögerungszeit startet das Gerät neu und durchläuft folgende Phasen:

- Wenn Sie diese Funktion im Dialog *Diagnose > System > Selbsttest* aktivieren, dann führt das Gerät einen RAM-Test durch.
- Das Gerät startet die Geräte-Software, die das Feld *Gespeicherte Version* im Dialog *Grundeinstellungen > Software* anzeigt.
- Das Gerät lädt die Einstellungen aus dem „ausgewählten“ Konfigurationsprofil. Siehe Dialog *Grundeinstellungen > Laden/Speichern*.

Anmerkung: Während des Neustarts überträgt das Gerät keine Daten. Das Gerät ist während dieser Zeit für die grafische Benutzeroberfläche und andere Managementsysteme unerreichbar.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

MAC-Adresstabelle zurücksetzen

Entfernt aus der Forwarding-Tabelle (FDB) die MAC-Adressen, die im Dialog *Switching > Filter für MAC-Adressen* in Spalte *Status* den Wert `learned` haben.

ARP-Tabelle zurücksetzen

Entfernt aus der ARP-Tabelle die dynamisch eingerichteten Adressen.

Siehe Dialog *Diagnose > System > ARP*.

Port-Statistiken leeren

Setzt die Zähler der Portstatistik auf `0`.

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

Statistik zum Zugriff auf das Management leeren

Setzt die Zähler der Statistik über Zugriffe auf das Management des Geräts auf `0`.

Siehe Dialog *Diagnose > System > Systeminformationen*, Tabelle `Used Management Ports`.

IGMP-Snooping-Daten zurücksetzen

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

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

Log-Datei löschen

Entfernt die protokollierten Einträge aus der Log-Datei.

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

Persistente Log-Datei löschen

Entfernt die Log-Dateien vom externen Speicher.

Siehe Dialog *Diagnose > Bericht > Persistentes Ereignisprotokoll*.

E-Mail-Benachrichtung Statistik leeren

Setzt die Zähler im Rahmen *Information* auf `0`.

Siehe Dialog *Diagnose > E-Mail-Benachrichtigung > Global*.

2 Zeit

Das Menü enthält die folgenden Dialoge:
- Grundeinstellungen
- SNTP
- PTP
- 802.1AS

2.1 Grundeinstellungen

[Zeit > Grundeinstellungen]

Das Gerät ist mit einer gepufferten Hardware-Uhr ausgestattet. Diese führt die aktuelle Uhrzeit weiter, wenn die Stromversorgung ausfällt oder wenn Sie das Gerät von der Stromversorgung trennen. Nach dem Start des Geräts steht Ihnen die gegenwärtige Uhrzeit zur Verfügung, zum Beispiel für Log-Einträge.

Die Hardware-Uhr überbrückt einen Netzteil-Ausfall 3 Stunden lang. Voraussetzung dafür ist, dass das Netzteil das Gerät vorher mindestens 5 Minuten kontinuierlich gespeist hat.

In diesem Dialog legen Sie, unabhängig vom gewählten Zeitsynchronisationsprotokoll,zeitbezogene Einstellungen fest.

Der Dialog enthält die folgenden Registerkarten:
- [Global]
- [Sommerzeit]

[Global]

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

Konfiguration

Systemzeit (UTC)

Zeigt das gegenwärtige Datum und die gegenwärtige Uhrzeit bezogen auf die koordinierte Weltzeit UTC.

Setze Zeit vom PC

Das Gerät verwendet die Uhrzeit des PCs als Systemzeit.

Systemzeit

Zeigt das gegenwärtige Datum und die gegenwärtige Uhrzeit bezogen auf die lokale Zeit: *Systemzeit* = *Systemzeit (UTC)* +*Lokaler Offset [min]* + *Sommerzeit*

Quelle der Zeit

Zeigt die Zeitquelle, aus der das Gerät die Zeitinformation bezieht.

Das Gerät wählt automatisch die verfügbare Zeitquelle mit der höchsten Genauigkeit.

Mögliche Werte:

- *lokal*
  Systemuhr des Geräts.
- *sntp*
  Der *SNTP*-Client ist aktiviert und das Gerät ist durch einen *SNTP*-Server synchronisiert.
- *ptp*
  PTP ist aktiviert und die Uhr des Geräts ist auf eine *PTP*-Master-Uhr synchronisiert.

Lokaler Offset [min]

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

Mögliche Werte:

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

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Sommerzeit]

In dieser Registerkarte aktivieren Sie die automatische Sommerzeit-Umschaltung. Beginn und Ende der Sommerzeit wählen Sie anhand eines vordefinierten Profils oder Sie legen diese Einstellungen individuell fest. Während der Sommerzeit stellt das Gerät die lokale Zeit um 1 Stunde vor.

Funktion

Sommerzeit

Schaltet den *Sommerzeit*-Modus ein/aus.

Mögliche Werte:

- *An*
  Die *Sommerzeit*-Modus ist eingeschaltet.
  Das Gerät wechselt automatisch zwischen Sommerzeit und Winterzeit.
- *Aus* (Voreinstellung)
  Die *Sommerzeit*-Modus ist ausgeschaltet.

Die Zeitpunkte, zu denen das Gerät zwischen Sommer- und Winterzeit umschaltet, sind in den Rahmen *Sommerzeit Beginn* und *Sommerzeit Ende*festgelegt.

Profil...

Öffnet den Dialog *Profil...*. Dort wählen Sie ein vordefiniertes Profil für Beginn und Ende der Sommerzeit aus. Dieses Profil überschreibt die Einstellungen in den Rahmen *Sommerzeit Beginn* und *Sommerzeit Ende*.

Sommerzeit Beginn

In den ersten 3 Feldern legen Sie den Tag für den Beginn der Sommerzeit fest, im letzten Feld die Uhrzeit.

Wenn die Uhrzeit im Feld *Systemzeit* den hier festgelegten Wert erreicht, schaltet das Gerät auf Sommerzeit.

Woche

Legt die Woche im gegenwärtigen Monat fest.

Mögliche Werte:

- *kein* (Voreinstellung)
- *first*
- *second*
- *third*
- *fourth*
- *last*

Tag

Legt den Wochentag fest.

Mögliche Werte:

- *kein* (Voreinstellung)
- *Sunday*
- *Monday*
- *Tuesday*
- *Wednesday*
- *Thursday*
- *Friday*
- *Saturday*

Monat

Legt den Monat fest.

Mögliche Werte:

- *kein* (Voreinstellung)
- *January*
- *February*
- *March*
- *April*
- *May*

- *June*
- *July*
- *August*
- *September*
- *October*
- *November*
- *December*

Systemzeit

Legt die Uhrzeit fest.

Mögliche Werte:

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

Sommerzeit Ende

In den ersten 3 Feldern legen Sie den Tag für das Ende der Sommerzeit fest, im letzten Feld die Uhrzeit.

Wenn die Uhrzeit im Feld *Systemzeit* den hier festgelegten Wert erreicht, schaltet das Gerät auf Winterzeit.

Woche

Legt die Woche im gegenwärtigen Monat fest.

Mögliche Werte:

- *kein* (Voreinstellung)
- *first*
- *second*
- *third*
- *fourth*
- *last*

Tag

Legt den Wochentag fest.

Mögliche Werte:

- *kein* (Voreinstellung)
- *Sunday*
- *Monday*
- *Tuesday*
- *Wednesday*
- *Thursday*
- *Friday*
- *Saturday*

Monat

Legt den Monat fest.

Mögliche Werte:
- *kein* (Voreinstellung)
- *January*
- *February*
- *March*
- *April*
- *May*
- *June*
- *July*
- *August*
- *September*
- *October*
- *November*
- *December*

Systemzeit

Legt die Uhrzeit fest.

Mögliche Werte:
- <HH:MM> (Voreinstellung: 00:00)

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

2.2 SNTP

[Zeit > SNTP]

Das Simple Network Time Protocol (SNTP) ist ein im RFC 4330 beschriebenes Verfahren für die Zeitsynchronisation im Netz.

Das Gerät ermöglicht Ihnen, als *SNTP*-Client die Systemzeit im Gerät zu synchronisieren. Als *SNTP*-Server stellt das Gerät die Zeitinformation anderen Geräten zur Verfügung.

Das Menü enthält die folgenden Dialoge:
- SNTP Client
- SNTP Server

2.2.1 SNTP Client

[Zeit > SNTP > Client]

In diesem Dialog legen Sie die Einstellungen fest, mit denen das Gerät als *SNTP*-Client arbeitet.

Als *SNTP*-Client bezieht das Gerät die Zeitinformationen sowohl von *SNTP*-Servern als auch von *NTP*-Servern und synchronisiert die lokale Uhr auf die Zeit des Zeit-Servers.

Funktion

Funktion

Schaltet die Funktion *SNTP Client* des Geräts ein/aus.

Mögliche Werte:

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

Konfiguration

Modus

Legt fest, ob das Gerät die Zeitinformation aktiv bei einem im Netz bekannten und konfigurierten *SNTP*-Server anfragt (Unicast-Modus) oder passiv auf die Zeitinformation eines beliebigen *SNTP*-Servers wartet (Broadcast-Modus).

Mögliche Werte:

- `unicast` (Voreinstellung)
  Das Gerät bezieht die Zeitinformation ausschließlich vom konfigurierten *SNTP*-Server. Das Gerät sendet Unicast-Anfragen an den *SNTP*-Server und wertet dessen Antworten aus.
- `broadcast`
  Das Gerät bezieht die Zeitinformation von einem oder mehreren *SNTP*- oder *NTP*-Servern. Das Gerät wertet ausschließlich die Broadcasts oder Multicasts dieser Server aus.

Request-Intervall [s]

Legt das Intervall in Sekunden fest, in dem das Gerät Zeitinformationen beim *SNTP*-Server anfordert.

Mögliche Werte:

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

Broadcast-Recv-Timeout [s]

Legt die Zeit in Sekunden fest, die ein Client im Broadcast-Client-Modus wartet, bevor er den Wert im Feld von *`syncToRemoteServer`* zu *`notSynchronized`* ändert, wenn der Client keine Broadcast-Pakete empfängt.

Mögliche Werte:

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

Deaktiviere Client nach erfolgreicher Synchronisierung

Aktiviert/deaktiviert das Ausschalten des *SNTP*-Clients, wenn das Gerät die Zeit erfolgreich synchronisiert hat.

Mögliche Werte:

- `markiert`
  Das Ausschalten des *SNTP*-Clients ist aktiv.
  Das Gerät deaktiviert den *SNTP*-Client nach erfolgreicher Synchronisation der Zeit.
- `unmarkiert` (Voreinstellung)
  Das Ausschalten des *SNTP*-Clients ist inaktiv.
  Der *SNTP*-Client bleibt nach erfolgreicher Synchronisation der Zeit aktiv.

Zustand

Zustand

Zeigt den Zustand des *SNTP*-Clients.

Mögliche Werte:

- *`disabled`*
  Der *SNTP*-Client ist ausgeschaltet.
- *`notSynchronized`*
  Der *SNTP*-Client ist auf keinen *SNTP*- oder *NTP*-Server synchronisiert.
- *`synchronizedToRemoteServer`*
  Der *SNTP*-Client ist auf einen *SNTP*- oder *NTP*-Server synchronisiert.

Tabelle

In der Tabelle legen Sie die Einstellungen für bis zu 4 *SNTP*-Server fest.

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Mögliche Werte:

- `1..4`

Das Gerät legt diese Nummer automatisch fest.

Wenn Sie einen Tabelleneintrag löschen, bleibt eine Lücke in der Nummerierung. Wenn Sie einen neuen Tabelleneintrag erzeugen, schließt das Gerät die 1. Lücke.

Das Gerät sendet nach dem Starten Anfragen an den *SNTP*-Server, der im ersten Tabelleneintrag konfiguriert ist. Bleibt die Antwort des Servers aus, sendet das Gerät seine Anfragen an den *SNTP*-Server, der im nächsten Tabelleneintrag konfiguriert ist.

Wenn vorübergehend keiner der konfigurierten *SNTP*-Server antwortet, dann unterbricht der *SNTP*-Client seine Synchronisation. Das Gerät fragt solange zyklisch nacheinander bei jedem *SNTP*-Server an, bis ein Server eine gültige Zeit liefert. Das Gerät synchronisiert sich auf diesen *SNTP*-Server, auch wenn die anderen Server später wieder erreichbar sind.

Name

Legt den Namen des *SNTP*-Servers fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

Adresse

Legt die IP-Adresse des *SNTP*-Servers fest.

Mögliche Werte:

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

Ziel-UDP-Port

Legt den UDP-Port fest, auf dem der *SNTP*-Server die Zeitinformationen erwartet.

Mögliche Werte:

- `1..65535` (Voreinstellung: `123`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Status

Zeigt den Verbindungsstatus zwischen *SNTP*-Client und *SNTP*-Server.

Mögliche Werte:

- *`erfolgreich`*
  Das Gerät hat die Zeit erfolgreich mit dem *SNTP*-Server synchronisiert.

- *badDateEncoded*
  Die empfangene Zeitinformation enthält Protokollfehler, Synchronisation war nicht erfolgreich.
- *other*
  - Für die IP-Adresse des *SNTP*-Servers ist der Wert `0.0.0.0` eingetragen, Synchronisation war nicht erfolgreich.
    oder
  - Der *SNTP*-Client verwendet einen anderen *SNTP*-Server.
- *requestTimedOut*
  Das Gerät hat keine Antwort vom *SNTP*-Server erhalten, Synchronisation war nicht erfolgreich.
- *serverKissOfDeath*
  Der *SNTP*-Server ist überlastet. Das Gerät ist aufgefordert, sich mit einem anderen *SNTP*-Server zu synchronisieren. Steht kein anderer *SNTP*-Server zur Verfügung, fragt das Gerät in größeren Abständen als im Feld *Request-Intervall [s]* eingestellt nach, ob der Server noch überlastet ist.
- *serverUnsychronized*
  Der *SNTP*-Server ist weder auf eine lokale noch auf eine externe Referenzzeitquelle synchronisiert, Synchronisation war nicht erfolgreich.
- *versionNotSupported*
  Die *SNTP*-Versionen auf Client und Server sind zueinander inkompatibel, Synchronisation war nicht erfolgreich.

Aktiv

Aktiviert/deaktiviert die Verbindung zum *SNTP*-Server.

Mögliche Werte:

- `markiert`
  Die Verbindung zum *SNTP*-Server ist aktiviert.
  Der *SNTP*-Client hat Zugriff auf den *SNTP*-Server.
- `unmarkiert` (Voreinstellung)
  Die Verbindung zum *SNTP*-Server ist deaktiviert.
  Der *SNTP*-Client hat keinen Zugriff auf den *SNTP*-Server.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

2.2.2 SNTP Server

[Zeit > SNTP > Server]

In diesem Dialog legen Sie die Einstellungen fest, mit denen das Gerät als *SNTP*-Server arbeitet.

Der *SNTP*-Server stellt die koordinierte Weltzeit (UTC) zur Verfügung, ohne lokale Zeitverschiebungen zu berücksichtigen.

Bei entsprechender Einstellung arbeitet der *SNTP*-Server im Broadcast-Modus. Der *SNTP*-Server sendet im Broadcast-Modus automatisch Broadcast-Nachrichten oder Multicast-Nachrichten im Broadcast-Sendeintervall.

Funktion

Funktion

Schaltet die Funktion *SNTP Server* des Geräts ein/aus.

Mögliche Werte:

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

Beachten Sie die Einstellung des Kontrollkästchens *Server deaktivieren bei lokaler Zeitquelle* im Rahmen *Konfiguration*.

Konfiguration

UDP-Port

Legt die Nummer des UDP-Ports fest, auf dem der *SNTP*-Server des Geräts Anfragen anderer Clients entgegennimmt.

Mögliche Werte:

- `1..65535` (Voreinstellung: `123`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Broadcast-Admin-Modus

Aktiviert/deaktiviert den Broadcast-Modus.

- `markiert`
  Der *SNTP*-Server beantwortet Anfragen von *SNTP*-Clients im Unicast-Modus und sendet zusätzlich *SNTP*-Pakete im Broadcast-Modus als Broadcast oder Multicast.
- `unmarkiert` (Voreinstellung)
  Der *SNTP*-Server beantwortet Anfragen von *SNTP*-Clients im Unicast-Modus.

Broadcast-Ziel-Adresse

Legt die IP-Adresse fest, an die der *SNTP*-Server des Geräts die *SNTP*-Pakete im Broadcast-Modus sendet.

Mögliche Werte:

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

Broadcast- und Multicast-Adressen sind zulässig.

Broadcast-UDP-Port

Legt die Nummer des UDP-Ports fest, auf dem der *SNTP*-Server die *SNTP*-Pakete im Broadcast-Modus sendet.

Mögliche Werte:

- `1..65535` (Voreinstellung: `123`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Broadcast VLAN-ID

Legt die ID des VLANs fest, in welchem der *SNTP*-Server des Geräts die *SNTP*-Pakete im Broadcast-Modus sendet.

Mögliche Werte:

- `0`
  Der *SNTP*-Server sendet die *SNTP*-Pakete im selben VLAN, in dem der Zugriff auf das Managements des Geräts möglich ist. Siehe Dialog *Grundeinstellungen > Netz*.
- `1..4042` (Voreinstellung: `1`)

Broadcast-Sende-Intervall [s]

Legt den Zeitabstand fest, in dem der *SNTP*-Server des Geräts *SNTP*-Broadcast Pakete sendet.

Mögliche Werte:

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

Server deaktivieren bei lokaler Zeitquelle

Aktiviert/deaktiviert das Ausschalten des *SNTP*-Servers, wenn sich das Gerät auf die lokale Uhr synchronisiert hat.

Mögliche Werte:

- `markiert`
  Das Ausschalten des *SNTP*-Servers ist aktiv.
  Wenn das Gerät auf die lokale Uhr synchronisiert ist, dann deaktiviert das Gerät den *SNTP*-Server. Anfragen von *SNTP*-Clients beantwortet der *SNTP*-Server weiterhin. Im *SNTP*-Paket teilt der *SNTP*-Server den Clients mit, dass er lokal synchronisiert ist.
- `unmarkiert` (Voreinstellung)
  Das Ausschalten des *SNTP*-Servers ist inaktiv.
  Wenn das Gerät auf die lokale Uhr synchronisiert ist, bleibt der *SNTP*-Server aktiv.

Zustand

Zustand

Zeigt den Zustand des *SNTP*-Servers.

Mögliche Werte:

- `disabled`
  Der *SNTP*-Server ist ausgeschaltet.
- `notSynchronized`
  Der *SNTP*-Server ist weder auf eine lokale noch auf eine externe Referenzzeitquelle synchronisiert.
- `syncToLocal`
  Der *SNTP*-Server ist synchronisiert auf die Hardware-Uhr des Geräts.
- `syncToRefclock`
  Der *SNTP*-Server ist synchronisiert auf eine externe Referenzzeitquelle, zum Beispiel PTP.
- `syncToRemoteServer`
  Der *SNTP*-Server ist synchronisiert auf einen *SNTP*-Server, der in einer Kaskade dem Gerät übergeordnet ist.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

2.3 PTP

[Zeit > PTP]

Das Menü enthält die folgenden Dialoge:

- PTP Global
- PTP Boundary Clock
- PTP Transparent Clock

2.3.1 PTP Global

[Zeit > PTP > Global]

In diesem Dialog legen Sie grundlegende Einstellungen für das Protokoll *PTP* fest.

Das Precision Time Protocol (PTP) ist ein in der Norm IEEE 1588-2008 beschriebenes Verfahren, das die Geräte im Netz mit einer exakten Uhrzeit vorsorgt. Das Verfahren synchronisiert die Uhren im Netz mit einer Genauigkeit von wenigen 100 ns. Das Protokoll verwendet Multicast-Kommunikation, weshalb die *PTP*-Synchronisationsnachrichten das Netz kaum belasten.

PTP ist erheblich genauer als SNTP. Sind im Gerät die Funktion *SNTP* und die Funktion *PTP* gleichzeitig eingeschaltet, dann hat die Funktion *PTP* Vorrang.

Anhand des *„Best Master Clock"-Algorithmus* bestimmen die Geräte im Netzwerk, welches Gerät die genauste Zeit hat. Die Geräte verwenden das Gerät mit der genauesten Zeit als Referenzzeitquelle (*Grandmaster*). Anschließend synchronisieren sich die beteiligten Geräte auf diese Referenzzeitquelle.

Wenn Sie die PTP-Zeit präzise durch Ihr Netz transportieren möchten, dann verwenden Sie in den Transportpfaden ausschließlich Geräte mit PTP-Hardware-Unterstützung.

Das Protokoll unterscheidet zwischen den folgenden Uhren:

- *Boundary Clock (BC)*
  Diese Uhr besitzt beliebig viele PTP-Ports und arbeitet zugleich als *PTP*-Master und als *PTP*-Slave. Im jeweiligen Netzsegment verhält sich die Uhr wie eine Ordinary Clock.
  - Als *PTP*-Slave synchronisiert sich die Uhr auf einen *PTP*-Master, der in der Kaskade dem Gerät übergeordnet ist.
  - Als *PTP*-Master gibt die Uhr die Zeitinformation über das Netz an *PTP*-Slaves weiter, die in der Kaskade dem Gerät untergeordnet sind.
- *Transparent Clock (TC)*
  Diese Uhr besitzt beliebig viele PTP-Ports. Im Gegensatz zur *Boundary Clock* korrigiert die Uhr ausschließlich die Zeitinformation vor Weitergabe, ohne sich selbst zu synchronisieren.

Funktion IEEE1588/PTP

Funktion IEEE1588/PTP

Schaltet die Funktion *PTP* ein/aus.

Im Gerät kann entweder die Funktion *802.1AS* oder die Funktion *PTP* gleichzeitig eingeschaltet sein.

Mögliche Werte:

- `An`
  Die Funktion *PTP* ist eingeschaltet.
  Das Gerät synchronisiert seine Uhr mit PTP.
  Sind im Gerät die Funktion *SNTP* und die Funktion *PTP* gleichzeitig eingeschaltet, dann hat die Funktion *PTP* Vorrang.
- `Aus` (Voreinstellung)
  Die Funktion *PTP* ist ausgeschaltet.
  Das Gerät vermittelt *PTP*-Synchronisationsnachrichten ohne Korrektur auf jedem Port.

Konfiguration IEEE1588/PTP

PTP-Modus

Legt die PTP-Version und den Modus der lokalen Uhr fest.

Mögliche Werte:

- *v2-transparent-clock* (Voreinstellung)
- *v2-boundary-clock*

Untere Synchronisations-Schwelle [ns]

Legt den unteren Schwellwert in Nanosekunden fest für den Gangunterschied zwischen lokaler Uhr und Referenzzeitquelle (*Grandmaster*). Unterschreitet der Gangunterschied diesen Wert einmalig, dann gilt die lokale Uhr als synchronisiert.

Mögliche Werte:

- `0..999999999` (Voreinstellung: `30`)

Obere Synchronisations-Schwelle [ns]

Legt den oberen Schwellwert in Nanosekunden fest für den Gangunterschied zwischen lokaler Uhr und Referenzzeitquelle (*Grandmaster*). Überschreitet der Gangunterschied diesen Wert einmalig, dann gilt die lokale Uhr als unsynchronisiert.

Mögliche Werte:

- `31..1000000000` (Voreinstellung: `5000`)

PTP-Management

Aktiviert/deaktiviert das in der PTP-Norm definierte PTP-Management.

Mögliche Werte:

- `markiert`
  PTP-Management ist aktiviert.
- `unmarkiert` (Voreinstellung)
  PTP-Management ist deaktiviert.

Status

Ist synchronisiert

Zeigt, ob die lokale Uhr mit der Referenzzeitquelle (*Grandmaster*) synchronisiert ist.

Die lokale Uhr ist synchronisiert, sobald der Gangunterschied zwischen lokaler Uhr und Referenzzeitquelle (*Grandmaster*) einmalig den unteren Synchronisations-Grenzwert unterschreitet. Dieser Zustand bleibt so lange erhalten, bis der Gangunterschied den oberen Synchronisations-Grenzwert einmalig überschreitet.

Die Synchronisations-Grenzwerte legen Sie fest im Rahmen *Konfiguration IEEE1588/PTP*.

Max. Offset absolut [ns]

Zeigt den maximalen Gangunterschied in Nanosekunden, der aufgetreten ist, seitdem die lokale Uhr mit der Referenzzeitquelle (*Grandmaster*) synchronisiert ist.

PTP-Zeit

Zeigt Datum und Zeit der PTP-Zeitskala, wenn die lokale Uhr mit der Referenzzeitquelle (*Grandmaster*) synchronisiert ist. Format: `TT.MM.JJJJ hh:mm:ss`

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

2.3.2 PTP Boundary Clock

[Zeit > PTP > Boundary Clock]

Dieses Menü bietet Ihnen die Möglichkeit, die Einstellungen für den Boundary-Clock-Modus der lokalen Uhr festzulegen.

Das Menü enthält die folgenden Dialoge:
- PTP Boundary Clock Global
- PTP Boundary Clock Port

2.3.2.1 PTP Boundary Clock Global

[Zeit > PTP > Boundary Clock > Global]

In diesem Dialog legen Sie allgemeine, portübergreifende Einstellungen für den *Boundary Clock*-Modus der lokalen Uhr fest. Die *Boundary Clock (BC)* arbeitet gemäß PTP Version 2 (IEEE 1588-2008).

Die Einstellungen sind wirksam, wenn die lokale Uhr als *Boundary Clock (BC)* arbeitet. Wählen Sie dazu im Dialog *Zeit > PTP > Global* im Feld *PTP-Modus* den Wert `v2-boundary-clock`.

Funktion IEEE1588/PTPv2 BC

Priorität 1

Legt die *Priorität 1* des Geräts fest.

Mögliche Werte:

- `0..255` (Voreinstellung: `128`)

Der *„Best Master Clock“-Algorithmus* bewertet zuerst die *Priorität 1* zwischen den beteiligten Geräten, um die Referenzzeitquelle (*Grandmaster*) zu bestimmen.

Je niedriger Sie den Wert einstellen, desto wahrscheinlicher wird das Gerät Referenzzeitquelle (*Grandmaster*). Siehe Rahmen *Grandmaster*.

Priorität 2

Legt die *Priorität 2* des Geräts fest.

Mögliche Werte:

- `0..255` (Voreinstellung: `128`)

Wenn die zuvor bewerteten Kriterien bei mehreren Geräten gleich sind, bewertet der *„Best Master Clock“-Algorithmus* die *Priorität 2* der beteiligten Geräte.

Je niedriger Sie den Wert einstellen, desto wahrscheinlicher wird das Gerät Referenzzeitquelle (*Grandmaster*). Siehe Rahmen *Grandmaster*.

Domänen-Nummer

Weist das Gerät einer *PTP*-Domäne zu.

Mögliche Werte:

- `0..255` (Voreinstellung: `0`)

Das Gerät überträgt Zeitinformationen ausschließlich von und zu Geräten in derselben Domäne.

Status IEEE1588/PTPv2 BC

Two step

Zeigt, dass die Uhr im Two-Step-Modus arbeitet.

Steps removed

Zeigt die Anzahl der durchlaufenen Kommunikationspfade zwischen der lokalen Uhr des Geräts und der Referenzzeitquelle (*Grandmaster*).

Für einen *PTP*-Slave bedeutet der Wert `1`, dass die Uhr direkt über 1 Kommunikationspfad mit der Referenzzeitquelle (*Grandmaster*) verbunden ist.

Offset zum Master [ns]

Zeigt die gemessene Differenz (Offset) zwischen lokaler Uhr und Referenzzeitquelle (*Grandmaster*) in Nanosekunden. Der *PTP*-Slave berechnet den die Differenz aus den empfangenen Zeitinformationen.

Im Two-Step-Modus besteht die Zeitinformation aus je 2 *PTP*-Synchronisationsnachrichten, die der *PTP*-Master zyklisch sendet:

- Die 1. Synchronisationsnachricht (Sync Message) enthält einen geschätzten Wert des exakten Sendezeitpunktes der Nachricht.
- Die 2. Synchronisationsnachricht (Follow-Up Message) enthält den exakten Sendezeitpunkt der 1. Nachricht.

Der *PTP*-Slave berechnet aus beiden *PTP*-Synchronisationsnachrichten die Differenz (Offset) zum Master und korrigiert seine Uhr um diesen Differenz. Dabei berücksichtigt der *PTP*-Slave den *Laufzeit zum Master [ns]*-Wert.

Laufzeit zum Master [ns]

Zeigt die Laufzeit (Delay) beim Übertragen der *PTP*-Synchronisationsnachrichten vom *PTP*-Master zum *PTP*-Slave in Nanosekunden.

Der *PTP*-Slave sendet ein „Delay Request“-Paket an den *PTP*-Master und ermittelt dabei die exakte Sendezeit des Pakets. Der *PTP*-Master generiert bei Empfang des Pakets einen Zeitstempel und sendet diesen in einem „Delay Response“-Paket an den *PTP*-Slave zurück. Der *PTP*-Slave berechnet aus beiden Paketen die Laufzeit (Delay) und berücksichtigt sie ab der nächsten Offset-Messung.

Voraussetzung ist, dass für den Laufzeitmess-Mechanismus des Slave-Ports der Wert `e2e` festgelegt ist.

Grandmaster

Der Rahmen zeigt die Kriterien, die der *„Best Master Clock“-Algorithmus* beim Bestimmen der Referenzzeitquelle (*Grandmaster*) bewertet.

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

Das Gerät ermöglicht Ihnen, Einfluss darauf zu nehmen, welches Gerät im Netz Referenzzeitquelle (*Grandmaster*) wird. Passen Sie dazu im Rahmen *Priorität 1* den Wert im Feld *Priorität 2* oder im Feld *Funktion IEEE1588/PTPv2 BC* an.

Priorität 1

Zeigt die *Priorität 1* des Geräts, das gegenwärtig Referenzzeitquelle (*Grandmaster*) ist.

Uhr-Klasse

Zeigt die Klasse der Referenzzeitquelle (*Grandmaster*). Kenngröße für den *Best-Master-Clock-Algoritmus*.

Präzision

Zeigt die geschätzte Ganggenauigkeit der Referenzzeitquelle (*Grandmaster*). Kenngröße für den *Best-Master-Clock-Algoritmus*.

Uhr-Varianz

Zeigt die Varianz der Referenzzeitquelle (*Grandmaster*), auch bezeichnet als *Offset scaled log variance*. Kenngröße für den *Best-Master-Clock-Algoritmus*.

Priorität 2

Zeigt die *Priorität 2* des Geräts, das gegenwärtig Referenzzeitquelle (*Grandmaster*) ist.

Lokale Zeit-Eigenschaften

Quelle der Zeit

Legt fest, von welcher Zeitquelle die lokale Uhr ihre Zeitinformation bezieht.

Mögliche Werte:

- `atomicClock`
- `gps`
- `terrestrialRadio`
- `ptp`
- `ntp`
- `handSet`
- `other`
- `internalOscillator` (Voreinstellung)

UTC-Offset [s]

Legt die Differenz der *PTP*-Zeitskala zur UTC fest.

Siehe Kontrollkästchen *PTP-Zeitskala*.

Mögliche Werte:

- `-32768..32767`

Anmerkung: Voreingestellt ist der zum Zeitpunkt der Erstellung der Geräte-Software gültige Wert. Weitere Informationen finden Sie im „Bulletin C“ des International Earth Rotation and Reference Systems Service (IERS): http://www.iers.org/IERS/EN/Publications/Bulletins/bulletins.html

UTC-Offset gültig

Legt fest, ob der im Feld *UTC-Offset [s]* festgelegte Wert korrekt ist.

Mögliche Werte:

- `markiert`
- `unmarkiert` (Voreinstellung)

Zeit nachvollziehbar

Zeigt, ob das Gerät die Zeit von einer primären UTC-Referenz bezieht, zum Beispiel von einem NTP-Server.

Mögliche Werte:

- `markiert`
- `unmarkiert`

Frequenz nachvollziehbar

Zeigt, ob das Gerät die Frequenz von einer primären UTC-Referenz bezieht, zum Beispiel von einem NTP-Server.

Mögliche Werte:

- `markiert`
- `unmarkiert`

PTP-Zeitskala

Zeigt, ob das Gerät die PTP-Zeitskala verwendet.

Mögliche Werte:

- `markiert`
- `unmarkiert`

Die PTP-Zeitskala ist laut IEEE 1588 die Atomzeit TAI mit dem Startzeitpunkt 01.01.1970.

Im Gegensatz zu UTC kennt TAI keine Schaltsekunden.

Mit Stand vom 1. Juli 2020 geht die TAI-Zeit 37 s gegenüber der UTC-Zeit vor.

Kennungen

Das Gerät zeigt die Kennungen als Byte-Folge in Hexadezimalnotation.

Die Identifikationsnummern (UUID) setzen sich wie folgt zusammen:
- Die Geräte-Identifikationsnummer besteht aus der MAC-Adresse des Geräts, erweitert um die Werte `ff` und `fe` zwischen Byte 3 und Byte 4.
- Die Port-UUID besteht aus der Geräte-Identifikationsnummer, gefolgt von einer 16-bit-Port-ID.

Uhr-Kennung

Zeigt die eigene Identifikationsnummer (UUID) des Geräts.

Port-Kennung Parent

Zeigt die Port-Identifikationsnummer (UUID) des direkt übergeordneten Master-Geräts.

Grandmaster-Kennung

Zeigt die Identifikationsnummer (UUID) des Geräts der Referenzzeitquellen (*Grandmaster*).

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

2.3.2.2 PTP Boundary Clock Port

[Zeit > PTP > Boundary Clock > Port]

In diesem Dialog legen Sie für jeden einzelnen Port die Einstellungen der *Boundary Clock (BC)* fest.

Die Einstellungen sind wirksam, wenn die lokale Uhr als *Boundary Clock (BC)* arbeitet. Wählen Sie dazu im Dialog *Zeit > PTP > Global* im Feld *PTP-Modus* den Wert `v2-boundary-clock`.

Tabelle

Port

Zeigt die Nummer des Ports.

PTP an

Aktiviert/deaktiviert die Übertragung von *PTP*-Synchronisationsnachrichten auf dem Port.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Übertragung ist aktiviert. Der Port vermittelt und empfängt *PTP*-Synchronisationsnachrichten.
- `unmarkiert`
  Die Übertragung ist deaktiviert. Der Port blockiert *PTP*-Synchronisationsnachrichten.

PTP-Status

Zeigt den gegenwärtigen Zustand des Ports.

Mögliche Werte:

- *initializing*
  Initialisierungsphase
- *faulty*
  Faulty Modus: Fehler im PTP-Protokoll.
- *disabled*
  PTP ist auf dem Port ausgeschaltet.
- *listening*
  Port wartet auf *PTP*-Synchronisationsnachrichten.
- *pre-master*
  PTP-Pre-Master-Modus
- *master*
  PTP-Master-Modus
- *passiv*
  PTP-Passiv-Modus
- *uncalibrated*
  PTP-Unkalibriert-Modus
- *slave*
  PTP-Slave-Modus

Sync-Intervall [s]

Legt das Intervall in Sekunden fest, in welchem der Port *PTP*-Synchronisationsnachrichten überträgt.

Mögliche Werte:

- `0.25`
- `0.5`
- `1` (Voreinstellung)
- `2`

Laufzeitmess-Mechanismus

Legt den Mechanismus fest, mit dem das Gerät die Laufzeit (Delay) beim Übertragen der *PTP*-Synchronisationsnachrichten misst.

Mögliche Werte:

- *`disabled`*
  Die Messung der Laufzeit (Delay) der *PTP*-Synchronisationsnachrichten zu den angeschlossenen PTP-Geräten ist deaktiviert.
- *`e2e`* (Voreinstellung)
  End-to-End: Als *PTP*-Slave misst der Port die Laufzeit der *PTP*-Synchronisationsnachrichten zum *PTP*-Master.
  Das Gerät zeigt den Messwert im Dialog *Zeit > PTP > Boundary Clock > Global*.
- *`p2p`*
  Peer-to-Peer: Das Gerät misst die Laufzeit (Delay) der *PTP*-Synchronisationsnachrichten zu allen angeschlossenen PTP-Geräten, vorausgesetzt, diese Geräte unterstützen P2P.
  Dieser Mechanismus erspart dem Gerät im Fall einer Rekonfiguration, die Laufzeit erneut zu ermitteln.

P2P-Laufzeit

Zeigt die gemessene Peer-to-Peer-Laufzeit der *PTP*-Synchronisationsnachrichten.

Voraussetzung ist, dass Sie in Spalte *Laufzeitmess-Mechanismus* den Wert *`p2p`* festlegen.

P2P-Laufzeitmess-Intervall [s]

Legt das Intervall in Sekunden fest, in welchem der Port die Peer-to-Peer-Laufzeit misst.

Voraussetzung ist, dass Sie den Wert *`p2p`* auf diesem Port und auf dem Port der Gegenstelle eingestellt haben.

Mögliche Werte:

- `1` (Voreinstellung)
- `2`
- `4`
- `8`
- `16`
- `32`

Netz-Protokoll

Legt fest, welches Protokoll der Port für das Übertragen der *PTP*-Synchronisationsnachrichten verwendet.

Mögliche Werte:

- `IEEE 802.3` (Voreinstellung)
- `UDP/IPv4`

Announce-Intervall [s]

Legt das Intervall in Sekunden fest, in welchem der Port Nachrichten für die PTP-Topologieerkennung überträgt.

Weisen Sie jedem Gerät einer *PTP*-Domäne denselben Wert zu.

Mögliche Werte:

- `1`
- `2` (Voreinstellung)
- `4`
- `8`
- `16`

Announce-Timeout

Legt die Anzahl der Announce-Intervalle fest.

Beispiel:

In der Voreinstellung (*Announce-Intervall [s]* = `2` und *Announce-Timeout* = `3`) beträgt das Timeout 3 × 2 s = 6 s.

Mögliche Werte:

- `2..10` (Voreinstellung: `3`)
  Weisen Sie jedem Gerät einer *PTP*-Domäne denselben Wert zu.

E2E-Laufzeitmess-Intervall [s]

Zeigt das Intervall in Sekunden, in welchem der Port die End-to-End-Laufzeit misst:

- Arbeitet der Port als *PTP*-Master, weist das Gerät dem Port den Wert `8` zu.
- Arbeitet der Port als *PTP*-Slave, legt der mit dem Port verbundene *PTP*-Master den Wert fest.

V1-Hardware-Kompatibilität

Legt fest, ob der Port die Länge der *PTP*-Synchronisationsnachrichten anpasst, wenn Sie in Spalte *Netz-Protokoll* den Wert `udpIpv4` festgelegt haben.

Unter Umständen erwarten andere Geräte im Netz die *PTP*-Synchronisationsnachrichten in der Länge von PTPv1-Nachrichten.

Mögliche Werte:

- `auto` (Voreinstellung)
  Das Gerät erkennt automatisch, ob andere Geräte im Netz *PTP*-Synchronisationsnachrichten in der Länge von PTPv1-Nachrichten erwarten. Ist das der Fall, erweitert das Gerät die Länge der *PTP*-Synchronisationsnachrichten vor dem Übertragen.

- *on*
  Das Gerät erweitert die Länge der *PTP*-Synchronisationsnachrichten vor dem Übertragen.
- *off*
  Das Gerät überträgt *PTP*-Synchronisationsnachrichten und behält die Länge bei.

Asymmetrie

Korrigiert den durch asymmetrische Übertragungswege verfälschten Laufzeitmesswert.

Mögliche Werte:

- `-2000000000..2000000000` (Voreinstellung: `0`)

Der Wert repräsentiert die Laufzeitasymmetrie in Nanosekunden.

Ein Laufzeitmesswert von y ns ns entspricht einer Asymmetrie von y × 2 ns.

Der Wert ist positiv, wenn die Laufzeit vom *PTP*-Master zum *PTP*-Slave länger ist als in umgekehrter Richtung.

VLAN

Legt die VLAN-ID fest, mit der das Gerät die *PTP*-Synchronisationsnachrichten auf diesem Port markiert.

Mögliche Werte:

- *kein* (Voreinstellung)
  Das Gerät überträgt *PTP*-Synchronisationsnachrichten ohne VLAN-Tag.
- `0..4042`
  VLANs, die Sie im Gerät bereits eingerichtet haben, wählen Sie in der Liste aus.

Vergewissern Sie sich, dass der Port Mitglied des VLANs ist.

Siehe Dialog *Switching > VLAN > Konfiguration*.

VLAN-Priorität

Legt die Priorität fest, mit der das Gerät die mit VLAN-ID markierten *PTP*-Synchronisationsnachrichten überträgt (Schicht 2, IEEE 802.1D).

Mögliche Werte:

- `0..7` (Voreinstellung: `6`)

Wenn Sie in Spalte *VLAN* den Wert *kein* festgelegt haben, dann ignoriert das Gerät die VLAN-Priorität.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

2.3.3 PTP Transparent Clock

[Zeit > PTP > Transparent Clock]

Dieses Menü bietet Ihnen die Möglichkeit, die Einstellungen für den *Transparent Clock*-Modus der lokalen Uhr festzulegen.

Das Menü enthält die folgenden Dialoge:

- PTP Transparent Clock Global
- PTP Transparent Clock Port

2.3.3.1 PTP Transparent Clock Global

[Zeit > PTP > Transparent Clock > Global]

In diesem Dialog legen Sie allgemeine, portübergreifende Einstellungen für den *Transparent Clock*-Modus der lokalen Uhr fest. Die *Transparent Clock (TC)* arbeitet gemäß PTP Version 2 (IEEE 1588-2008).

Die Einstellungen sind wirksam, wenn die lokale Uhr als *Transparent Clock (TC)* arbeitet. Wählen Sie dazu im Dialog *Zeit > PTP > Global* im Feld *PTP-Modus* den Wert `v2-transparent-clock`.

Funktion IEEE1588/PTPv2 TC

Laufzeitmess-Mechanismus

Legt den Mechanismus fest, mit dem das Gerät die Laufzeit (Delay) beim Übertragen der *PTP*-Synchronisationsnachrichten misst.

Mögliche Werte:

- `e2e` (Voreinstellung)
  Als *PTP*-Slave misst der Port die Laufzeit der *PTP*-Synchronisationsnachrichten zum *PTP*-Master.
  Das Gerät zeigt den Messwert im Dialog *Zeit > PTP > Transparent Clock > Global*.
- `p2p`
  Das Gerät misst die Laufzeit (Delay) der *PTP*-Synchronisationsnachrichten zu allen angeschlossenen PTP-Geräten, vorausgesetzt, diese Geräte unterstützen P2P.
  Dieser Mechanismus erspart dem Gerät im Fall einer Rekonfiguration, die Laufzeit erneut zu ermitteln.
  Wenn Sie diesen Wert festlegen, dann ist in Spalte *Netz-Protokoll* ausschließlich der Wert `IEEE 802.3` verfügbar.
- `e2e-optimized`
  Wie `e2e`, mit folgenden Besonderheiten:
  - Delay-Anfragen der *PTP*-Slaves vermittelt das Gerät ausschließlich an den *PTP*-Master, obwohl diese Anfragen Multicast-Nachrichten sind. Das Gerät entlastet damit die anderen Geräte von unnötigen Multicast-Anfragen.
  - Wenn sich die Master-Slave-Topologie ändert, lernt das Gerät den Port zum *PTP*-Master um, sobald es eine Synchronisationsnachricht von einem anderen *PTP*-Master empfängt.
  - Wenn das Gerät keinen *PTP*-Master kennt, dann überträgt es Delay-Anfragen an die Ports.
- `disabled`
  Auf dem Port ist die Laufzeitmessung ausgeschaltet. Das Gerät verwirft Nachrichten für die Laufzeitmessung.

Primäre Domäne

Weist das Gerät einer *PTP*-Domäne zu.

Mögliche Werte:

- `0..255` (Voreinstellung: `0`)

Das Gerät überträgt Zeitinformationen ausschließlich von und zu Geräten in derselben Domäne.

Netz-Protokoll

Legt fest, welches Protokoll der Port für das Übertragen der *PTP*-Synchronisationsnachrichten verwendet.

Mögliche Werte:

- `ieee8023` (Voreinstellung)
- `udpIpv4`

Multi-Domain-Modus

Aktiviert/deaktiviert in jeder *PTP*-Domäne die Korrektur von *PTP*-Synchronisationsnachrichten.

Mögliche Werte:

- `markiert`
  Das Gerät korrigiert *PTP*-Synchronisationsnachrichten in jeder *PTP*-Domäne.
- `unmarkiert` (Voreinstellung)
  Das Gerät korrigiert *PTP*-Synchronisationsnachrichten ausschließlich in der primären *PTP*-Domäne. Siehe Feld *Primäre Domäne*.

VLAN-ID

Legt die VLAN-ID fest, mit der das Gerät die *PTP*-Synchronisationsnachrichten auf diesem Port markiert.

Mögliche Werte:

- `kein` (Voreinstellung)
  Das Gerät überträgt *PTP*-Synchronisationsnachrichten ohne VLAN-Tag.
- `0..4042`
  VLANs, die Sie im Gerät bereits eingerichtet haben, wählen Sie in der Liste aus.

VLAN-Priorität

Legt die Priorität fest, mit der das Gerät die mit VLAN-ID markierten *PTP*-Synchronisationsnachrichten überträgt (Schicht 2, IEEE 802.1D).

Mögliche Werte:

- `0..7` (Voreinstellung: `6`)

Wenn Sie im Feld *VLAN-ID* den Wert `kein` festgelegt haben, dann ignoriert das Gerät den hier eingestellten Wert.

Lokale Synchronisation

Syntonize

Aktiviert/deaktiviert die Frequenz-Synchronisation der *Transparent Clock* mit dem *PTP*-Master.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Frequenz-Synchronisation ist aktiv.
  Das Gerät synchronisiert die Frequenz.
- `unmarkiert`
  Die Frequenz-Synchronisation ist inaktiv.
  Die Frequenz bleibt konstant.

Lokale Uhr synchronisieren

Aktiviert/deaktiviert die Synchronisation der lokalen Systemzeit.

Mögliche Werte:

- `markiert`
  Die Synchronisation ist aktiv.
  Das Gerät synchronisiert die lokale Systemzeit mit der per PTP empfangenen Uhrzeit. Voraussetzung ist, dass das Kontrollkästchen *Syntonize* markiert ist.
- `unmarkiert` (Voreinstellung)
  Die Synchronisation ist inaktiv.
  Die lokale Systemzeit bleibt konstant.

Aktueller Master

Zeigt die Port-Identifikationsnummer (UUID) des direkt übergeordneten Master-Geräts, auf welches das Gerät seine Frequenz synchronisiert.

Enthält der Wert ausschließlich Nullen, hat das die folgende Ursache:

- Die Funktion *Syntonize* ist ausgeschaltet.
  oder
- Das Gerät findet keinen *PTP*-Master.

Offset zum Master [ns]

Zeigt die gemessene Differenz (Offset) zwischen lokaler Uhr und dem *PTP*-Master in Nanosekunden. Das Gerät berechnet den die Differenz aus den empfangenen Zeitinformationen.

Voraussetzung ist, dass die Funktion *Lokale Uhr synchronisieren* eingeschaltet ist.

Laufzeit zum Master [ns]

Zeigt die Laufzeit (Delay) beim Übertragen der *PTP*-Synchronisationsnachrichten vom *PTP*-Master zum *PTP*-Slave in Nanosekunden.

Voraussetzung:

- Die Funktion *Lokale Uhr synchronisieren* ist eingeschaltet.
- Im Feld *Laufzeitmess-Mechanismus* ist der Wert `e2e` ausgewählt.

Status IEEE1588/PTPv2 TC

Uhr-Kennung

Zeigt die eigene Identifikationsnummer (UUID) des Geräts.

Das Gerät zeigt die Kennungen als Byte-Folge in Hexadezimalnotation.

Die Geräte-Identifikationsnummer besteht aus der MAC-Adresse des Geräts, erweitert um die Werte `ff` und `fe` zwischen Byte 3 und Byte 4.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

2.3.3.2 PTP Transparent Clock Port

[Zeit > PTP > Transparent Clock > Port]

In diesem Dialog legen Sie für jeden einzelnen Port die Einstellungen der *Transparent Clock (TC)* fest.

Die Einstellungen sind wirksam, wenn die lokale Uhr als *Transparent Clock (TC)* arbeitet. Wählen Sie dazu im Dialog *Zeit > PTP > Global* im Feld *PTP-Modus* den Wert `v2-transparent-clock`.

Tabelle

Port

Zeigt die Nummer des Ports.

PTP an

Aktiviert/deaktiviert die Übertragung von *PTP*-Synchronisationsnachrichten auf dem Port.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Übertragung ist aktiv.
  Der Port vermittelt und empfängt *PTP*-Synchronisationsnachrichten.
- `unmarkiert`
  Die Übertragung ist inaktiv.
  Der Port blockiert *PTP*-Synchronisationsnachrichten.

P2P-Laufzeitmess-Intervall [s]

Legt das Intervall in Sekunden fest, in welchem der Port die Peer-to-Peer-Laufzeit misst.

Voraussetzung ist, dass Sie den Wert `p2p` auf diesem Port und auf dem Port der Gegenstelle festlegen. Siehe Optionsliste *Laufzeitmess-Mechanismus* im Dialog *Zeit > PTP > Transparent Clock > Global*.

Mögliche Werte:

- `1` (Voreinstellung)
- `2`
- `4`
- `8`
- `16`
- `32`

P2P-Laufzeit

Zeigt die gemessene Peer-to-Peer-Laufzeit der *PTP*-Synchronisationsnachrichten.

Voraussetzung ist, dass Sie in der Optionsliste *Laufzeitmess-Mechanismus* das Optionsfeld `p2p` auswählen. Siehe Feld *Laufzeitmess-Mechanismus* im Dialog *Zeit > PTP > Transparent Clock > Global*.

Asymmetrie

Korrigiert den durch asymmetrische Übertragungswege verfälschten Laufzeitmesswert.

Mögliche Werte:

- `-2000000000..2000000000` (Voreinstellung: `0`)

Der Wert repräsentiert die Laufzeitasymmetrie in Nanosekunden.

Ein Laufzeitmesswert von y ns ns entspricht einer Asymmetrie von y × 2 ns.

Der Wert ist positiv, wenn die Laufzeit vom *PTP*-Master zum *PTP*-Slave länger ist als in umgekehrter Richtung.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

2.4 802.1AS

[Zeit > 802.1AS]

Das Protokoll *802.1AS* ist ein in der Norm IEEE 802.1AS-2011 beschriebenes Verfahren, das definiert, wie zwischen den Geräten im Netz die Zeit präzise synchronisiert wird. Wenn Sie das Protokoll *802.1AS* im Ethernet einsetzen, können Sie das Protokoll als ein Profil der Norm IEEE 1588-2008 betrachten.

Anhand des *„Best Master Clock“-Algorithmus* bestimmen die Geräte im Netzwerk, welches Gerät die genauste Zeit hat. Die Geräte verwenden das Gerät mit der genauesten Zeit als Referenzzeitquelle (*Grandmaster*). Anschließend synchronisieren sich die beteiligten Geräte auf diese Referenzzeitquelle.

Das Protokoll *802.1AS* hat die folgenden Merkmale:

- Im Gerät kann entweder die Funktion *802.1AS* oder die Funktion *PTP* eingeschaltet sein.
- Sind im Gerät die Funktion *SNTP* und die Funktion *802.1AS* gleichzeitig eingeschaltet, dann hat die Funktion *802.1AS* Vorrang.
- Die Funktion *802.1AS* unterstützt ausschließlich eine Domain.

Das Menü enthält die folgenden Dialoge:

- 802.1AS Global
- 802.1AS Port
- 802.1AS Statistiken

2.4.1 802.1AS Global

[Zeit > 802.1AS > Global]

In diesem Dialog legen Sie grundlegende Einstellungen für das Protokoll *802.1AS* fest.

Funktion

Funktion

Schaltet die Funktion *802.1AS* ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *802.1AS* ist eingeschaltet.
  Das Gerät synchronisiert seine Uhr mit dem Protokoll *802.1AS*.
  Denken Sie daran, das Protokoll *802.1AS* auf den einzelnen Ports zu aktivieren.

- `Aus` (Voreinstellung)
  Die Funktion *802.1AS* ist ausgeschaltet.

Konfiguration

Priorität 1

Legt die *Priorität 1* des Geräts fest.

Mögliche Werte:

- `0..255` (Voreinstellung: `246`)

Der *„Best Master Clock“-Algorithmus* bewertet zuerst die *Priorität 1* zwischen den beteiligten Geräten, um die Referenzzeitquelle (*Grandmaster*) zu bestimmen.

Je niedriger Sie den Wert einstellen, desto wahrscheinlicher wird das Gerät die Referenzzeitquelle (*Grandmaster*).

Wenn Sie den Wert `255` festlegen, dann wird das Gerät nicht die Referenzzeitquelle (*Grandmaster*). Siehe Rahmen *Grandmaster*.

Priorität 2

Legt die *Priorität 2* des Geräts fest.

Mögliche Werte:

- `0..255` (Voreinstellung: `248`)

Wenn die zuvor bewerteten Kriterien bei mehreren Geräten gleich sind, bewertet der *„Best Master Clock“-Algorithmus* die *Priorität 2* der beteiligten Geräte.

Je niedriger Sie den Wert einstellen, desto wahrscheinlicher wird das Gerät die Referenzzeitquelle (*Grandmaster*). Siehe Rahmen *Grandmaster*.

Untere Synchronisations-Schwelle [ns]

Legt den unteren Schwellwert in Nanosekunden fest für den Gangunterschied zwischen lokaler Uhr und Referenzzeitquelle (*Grandmaster*). Unterschreitet der Gangunterschied diesen Wert einmalig, dann gilt die lokale Uhr als synchronisiert.

Mögliche Werte:

- `0..999999999` (Voreinstellung: `30`)

Obere Synchronisations-Schwelle [ns]

Legt den oberen Schwellwert in Nanosekunden fest für den Gangunterschied zwischen lokaler Uhr und Referenzzeitquelle (*Grandmaster*). Überschreitet der Gangunterschied diesen Wert einmalig, dann gilt die lokale Uhr als unsynchronisiert.

Mögliche Werte:

- `31..1000000000` (Voreinstellung: `5000`)

UTC-Offset [s]

Zeigt die Differenz der *802.1AS*-Zeitskala zur UTC.

UTC-Offset gültig

Zeigt, ob der im Feld *UTC-Offset [s]* angezeigte Wert korrekt ist.

Mögliche Werte:

- `markiert`
- `unmarkiert`

Status

Offset zum Master [ns]

Zeigt die gemessene Differenz (Offset) zwischen lokaler Uhr und Referenzzeitquelle (*Grandmaster*) in Nanosekunden. Das Gerät berechnet den die Differenz aus den empfangenen Zeitinformationen.

Max. Offset absolut [ns]

Zeigt den maximalen Gangunterschied in Nanosekunden, der aufgetreten ist, seitdem die lokale Uhr mit der Referenzzeitquelle (*Grandmaster*) synchronisiert ist.

Ist synchronisiert

Zeigt, ob die lokale Uhr mit der Referenzzeitquelle (*Grandmaster*) synchronisiert ist.

Die lokale Uhr ist synchronisiert, sobald der Gangunterschied zwischen lokaler Uhr und Referenzzeitquelle (*Grandmaster*) den unteren Synchronisations-Grenzwert unterschreitet. Dieser Zustand bleibt so lange erhalten, bis der Gangunterschied den oberen Synchronisations-Grenzwert überschreitet.

Die Synchronisations-Grenzwerte legen Sie fest im Rahmen *Konfiguration*.

Steps removed

Zeigt die Anzahl der durchlaufenen Kommunikationspfade zwischen der lokalen Uhr des Geräts und der Referenzzeitquelle (*Grandmaster*).

Für einen *802.1AS*-Slave bedeutet der Wert `1`, dass die Uhr direkt über 1 Kommunikationspfad mit der Referenzzeitquelle (*Grandmaster*) verbunden ist.

Uhr-Kennung

Zeigt die Uhr-Identifikationsnummer des Geräts.

Das Gerät zeigt die Identifikationsnummer als Byte-Folge in Hexadezimalnotation.

Die Geräte-Identifikationsnummer besteht aus der MAC-Adresse des Geräts, erweitert um die Werte `ff` und `fe` zwischen Byte 3 und Byte 4.

Grandmaster

Der Rahmen zeigt die Kriterien, die der *„Best Master Clock“-Algorithmus* beim Bestimmen der Referenzzeitquelle (*Grandmaster*) bewertet.

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

Das Gerät ermöglicht Ihnen, Einfluss darauf zu nehmen, welches Gerät im Netz Referenzzeitquelle (*Grandmaster*) wird. Passen Sie dazu im Rahmen *Priorität 1* den Wert im Feld *Priorität 2* oder im Feld *Konfiguration* an.

Priorität 1

Zeigt die *Priorität 1* des Geräts, das gegenwärtig Referenzzeitquelle (*Grandmaster*) ist.

Uhr-Klasse

Zeigt die Klasse der Referenzzeitquelle (*Grandmaster*). Kenngröße für den *Best-Master-Clock-Algoritmus*.

Präzision

Zeigt die geschätzte Ganggenauigkeit der Referenzzeitquelle (*Grandmaster*). Kenngröße für den *Best-Master-Clock-Algoritmus*.

Uhr-Varianz

Zeigt die Varianz der Referenzzeitquelle (*Grandmaster*), auch bezeichnet als *Offset scaled log variance*. Kenngröße für den *Best-Master-Clock-Algoritmus*.

Priorität 2

Zeigt die *Priorität 2* des Geräts, das gegenwärtig Referenzzeitquelle (*Grandmaster*) ist.

Uhr-Kennung

Zeigt die Identifikationsnummer des Geräts der Referenzzeitquellen (*Grandmaster*). Das Gerät zeigt die Identifikationsnummer als Byte-Folge in Hexadezimalnotation.

Parent

Uhr-Kennung

Zeigt die Port-Identifikationsnummer des direkt übergeordneten Master-Geräts. Das Gerät zeigt die Identifikationsnummer als Byte-Folge in Hexadezimalnotation.

Port

Zeigt die Port-Nummer des direkt übergeordneten Master-Geräts.

Kumuliertes Rate-Verhältnis [ppm]

Zeigt die gemessene Frequenz-Differenz in Parts per million zwischen lokaler Uhr und Referenzzeitquelle (*Grandmaster*).

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

2.4.2 802.1AS Port

[Zeit > 802.1AS > Port]

In diesem Dialog legen Sie für jeden einzelnen Port die *802.1AS*-Einstellungen fest.

Tabelle

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert das Protocol *802.1AS* auf dem Port.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Protokoll ist auf dem Port aktiv.
  Das Gerät synchronisiert auf dem Port seine Uhr mit dem Protokoll *802.1AS*.
- `unmarkiert`
  Das Protokoll ist auf dem Port inaktiv.

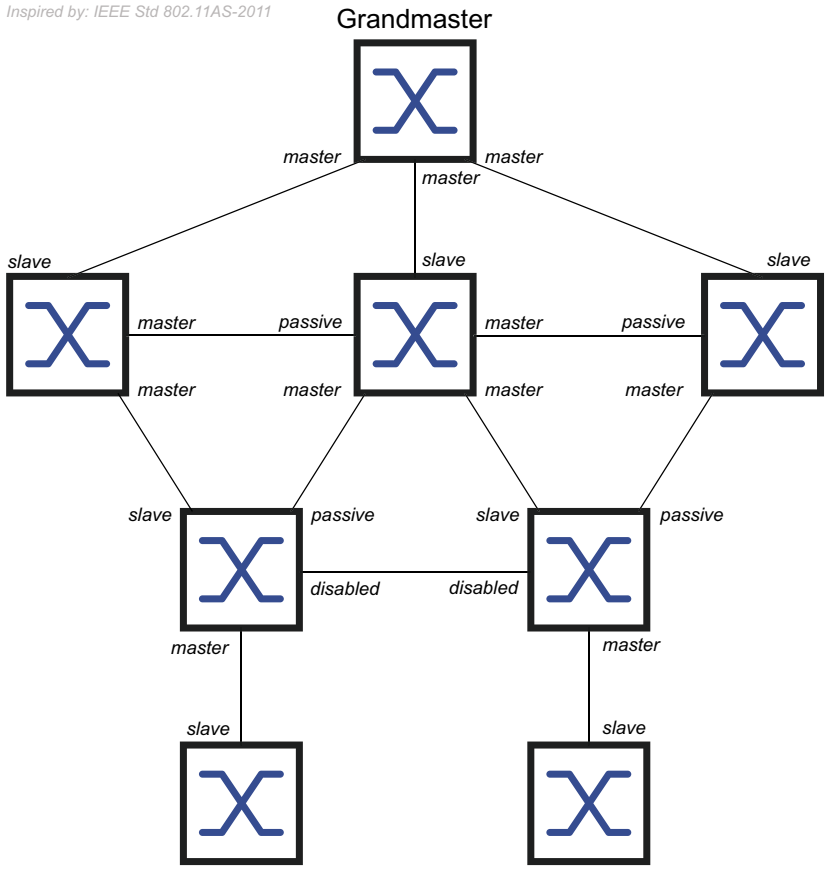
Rolle

Zeigt die gegenwärtige Rolle des Ports im Hinblick auf das Protokoll *802.1AS*.

Mögliche Werte:

- *disabled*
  Der Port arbeitet in der Rolle *Disabled Port*. Der Port ist nicht *802.1AS*-fähig.
- *master*
  Der Port arbeitet in der Rolle *Master Port*.

- `passiv`
  Der Port arbeitet in der Rolle *Passive Port*.
- `slave`
  Der Port arbeitet in der Rolle *Slave Port*.



AS capable

Zeigt, ob das Protokoll *802.1AS* auf dem Port aktiv ist.

Mögliche Werte:

- `markiert`
  Das Protokoll *802.1AS* ist auf dem Port aktiv. Die Voraussetzungen sind:
  – Der Port misst ein *Peer delay*, das Kontrollkästchen in Spalte *Measuring delay* ist markiert.
  – Der Wert in Spalte *Peer delay [ns]* ist kleiner als der Wert in Spalte *Peer delay threshold [ns]*.
- `unmarkiert`
  Das Protokoll *802.1AS* ist auf dem Port inaktiv.

Announce-Intervall [s]

Legt das Intervall in Sekunden fest, in dem der Port (in der Rolle *Master Port*) *Announce*-Nachrichten für die *802.1AS*-Topologieerkennung sendet.

Mögliche Werte:

- `1..2` (Voreinstellung: `1`)
  Weisen Sie jedem Gerät einer *802.1AS*-Domäne denselben Wert zu.
- `-`
  Der Port sendet keine *Announce*-Nachrichten.

Announce-Timeout

Legt die Anzahl *Announce-Intervall [s]* fest, die der Port (in der Rolle *Slave Port*) auf *Announce*-Nachrichten wartet.

Wenn die Anzahl der Intervalle vergeht, ohne eine *Announce*-Nachricht zu empfangen, versucht das Gerät, mit dem *„Best Master Clock“-Algorithmus* einen neuen Pfad zur Referenzzeitquelle zu finden. Wenn das Gerät eine Referenzzeitquelle (*Grandmaster*) findet, weist es dem Port zu, durch den der neue Pfad führt, die Rolle *Slave Port* zu. Andernfalls wird das Gerät selbs die Referenzzeitquelle (*Grandmaster*) und weist seinen Ports die Rolle *Master Port* zu.

Beispiel: In der Voreinstellung (`Announce-Intervall [s] = 1, Announce-Timeout = 3`) beträgt das Timeout `3 × 1 s = 3 s`.

Mögliche Werte:

- `2..10` (Voreinstellung: `3`)
  Weisen Sie jedem Port, der zur selben *802.1AS*-Domäne gehört, den gleichen Wert zu.

Sync-Intervall [s]

Legt das Intervall in Sekunden fest, in dem der Port (in der Rolle *Master Port*) *Sync*-Nachrichten für die Zeitsynchronisierung sendet.

Mögliche Werte:

- `0.125` (Voreinstellung)
- `0.250`
- `0.5`
- `1`
- `-`
  Der Port sendet keine *Sync*-Nachrichten.

Sync-Timeout

Legt die Anzahl *Sync-Intervall [s]* fest, die der Port (in der Rolle *Slave Port*) auf *Sync*-Nachrichten wartet.

Wenn die Anzahl der Intervalle vergeht, ohne eine *Sync*-Nachricht zu empfangen, versucht das Gerät, mit dem *„Best Master Clock“-Algorithmus* einen neuen Pfad zur Referenzzeitquelle zu finden. Wenn das Gerät eine Referenzzeitquelle (*Grandmaster*) findet, weist es dem Port zu, durch den der neue Pfad führt, die Rolle *Slave Port* zu. Andernfalls wird das Gerät selbs die Referenzzeitquelle (*Grandmaster*) und weist seinen Ports die Rolle *Master Port* zu.

Beispiel: In der Voreinstellung (`Sync-Intervall [s] = 0.125, Sync-Timeout = 3`) beträgt das Timeout `3 × 0.125 s = 0.375 s`.

Mögliche Werte:

- `2..10` (Voreinstellung: `3`)
  Weisen Sie jedem Port, der zur selben *802.1AS*-Domäne gehört, den gleichen Wert zu.

Peer-Delay-Intervall [s]

Legt das Intervall in Sekunden fest, in dem der Port (in der Rolle *Master Port*, *Passive Port* oder *Slave Port*) eine *Peer delay request*-Nachricht sendet, um das *Peer delay* zu messen.

Mögliche Werte:

- `1` (Voreinstellung)
- `2`
- `4`
- `8`
- `–`
  Der Port sendet keine *Peer delay request*-Nachrichten.

Peer-Delay-Timeout

Legt die Anzahl *Peer-Delay-Intervall [s]* fest, die der Port (in der Rolle *Master Port*, *Passive Port* oder *Slave Port*) auf *Delay response*-Nachrichten wartet.

Wenn die Anzahl der Intervalle vergeht, ohne eine *Delay response*-Nachricht zu empfangen, weist das Gerät dem Port die Rolle *Disabled Port* zu. Der Port ist nicht mehr *802.1AS*-fähig.

Mögliche Werte:

- `2..10` (Voreinstellung: `3`)

Peer delay threshold [ns]

Legt den oberen Schwellenwert für das *Peer delay* in Nanosekunden fest. Wenn der Wert in Spalte *Peer delay [ns]* größer ist als dieser Wert, dann weist das Gerät dem Port die Rolle *Disabled Port* zu. Der Port ist nicht mehr *802.1AS*-fähig.

Mögliche Werte:

- `0..1000000000` (Voreinstellung: `10000`)

Measuring delay

Zeigt, ob der Port ein *Peer delay* misst.

Mögliche Werte:

- `markiert`
  Der Port misst ein *Peer delay*. Die gemessenen Wert finden Sie in Spalte *Peer delay [ns]*.
- `unmarkiert`
  Der Port misst kein *Peer delay*.

Peer delay [ns]

Zeigt den gemessenen *Peer delay*-Wert in Nanosekunden. Voraussetzung ist, dass das Kontrollkästchen in Spalte *Measuring delay* markiert ist.

Neighbor rate ratio [ppm]

Zeigt die gemessene Frequenz-Differenz in Parts per million zwischen lokaler Uhr und dem benachbarten Gerät.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

2.4.3 802.1AS Statistiken

[Zeit > 802.1AS > Statistiken]

Dieser Dialog zeigt Informationen über die Anzahl der auf den Ports empfangenen, gesendeten und verworfenen Nachrichten an. Außerdem zeigt der Dialog Zähler, die sich mit jedem Auftreten eines Timeout-Ereignisses erhöhen.

Tabelle

Port

Zeigt die Nummer des Ports.

Empfangene Nachrichten

Zeigt Zähler für die auf den Ports empfangenen Nachrichten:

Sync messages

Zeigt die Anzahl der *Sync*-Nachrichten.

Sync follow-up messages

Zeigt die Anzahl der *Sync follow-up*-Nachrichten.

Delay request messages

Zeigt die Anzahl der *Peer delay request*-Nachrichten.

Delay response messages

Zeigt die Anzahl der *Peer delay response*-Nachrichten.

Delay response follow-up messages

Zeigt die Anzahl der *Peer delay response follow-up*-Nachrichten.

Announce messages

Zeigt die Anzahl der *Announce*-Nachrichten.

Discarded messages

Zeigt die Anzahl der *Sync*-Nachrichten, die das Gerät auf diesem Port verworfen hat. Das Gerät verwirft eine *Sync*-Nachricht zum Beispiel dann, wenn der Port keine *Sync follow-up*-Nachricht für die zugehörige *Sync*-Nachricht empfängt.

Sync-Timeout

Zeigt, wie oft ein *Sync-Timeout*-Ereignis auf dem Port aufgetreten ist. Siehe Spalte *Sync-Timeout* im Dialog *Zeit > 802.1AS > Port*.

Announce-Timeout

Zeigt, wie oft ein *Announce-Timeout*-Ereignis auf diesem Port aufgetreten ist. Siehe Spalte *Announce-Timeout* im Dialog *Zeit > 802.1AS > Port*.

Delay-Timeout

Zeigt, wie oft ein *Peer-Delay-Timeout*-Ereignis auf diesem Port aufgetreten ist. Siehe Spalte *Peer-Delay-Timeout* im Dialog *Zeit > 802.1AS > Port*.

Gesendete Nachrichten

Zeigt Zähler für die auf den Ports gesendeten Nachrichten:

Sync messages

Zeigt die Anzahl der *Sync*-Nachrichten.

Sync follow-up messages

Zeigt die Anzahl der *Sync follow-up*-Nachrichten.

Delay request messages

Zeigt die Anzahl der *Peer delay request*-Nachrichten.

Delay response messages

Zeigt die Anzahl der *Peer delay response*-Nachrichten.

Delay response follow-up messages

Zeigt die Anzahl der *Peer delay response follow-up*-Nachrichten.

Announce messages

Zeigt die Anzahl der *Announce*-Nachrichten.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

3 Gerätesicherheit

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

3.1 Benutzerverwaltung

[Gerätesicherheit > Benutzerverwaltung]

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

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

Die Methoden, die das Gerät für die Authentifizierung der Benutzer verwendet, legen Sie fest im Dialog *Gerätesicherheit > Authentifizierungs-Liste*.

Konfiguration

Dieser Rahmen ermöglicht Ihnen, Einstellungen für das Login festzulegen.

Login-Versuche

Legt die Anzahl der möglichen Login-Versuche fest, wenn der Benutzer auf das Management des Geräts über die grafische Benutzeroberfläche oder das Command Line Interface zugreift.

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

Mögliche Werte:
- `0..5` (Voreinstellung: `0`)

Wenn sich der Benutzer ein weiteres Mal erfolglos anmeldet, sperrt das Gerät für den Benutzer den Zugriff auf das Gerät.

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

Der Wert `0` deaktiviert die Sperre. Der Benutzer hat beliebig viele Versuche, sich anzumelden.

Zeitraum für Login-Versuche (min.)

Zeigt die Zeitspanne, nach der das Gerät den Zähler im Feld *Login-Versuche* zurücksetzt.

Mögliche Werte:

- `0..60` (Voreinstellung: `0`)

Min. Passwort-Länge

Das Gerät akzeptiert das Passwort, wenn es sich aus mindestens so vielen Zeichen zusammensetzt, wie hier angegeben.

Das Gerät prüft das Passwort gemäß dieser Richtlinie, unabhängig von der Einstellung des Kontrollkästchens *Richtlinien überprüfen*.

Mögliche Werte:

- `1..64` (Voreinstellung: `6`)

Passwort-Richtlinien

Dieser Rahmen ermöglicht Ihnen, Richtlinien für gültige Passwörter festzulegen. Das Gerät prüft jedes neue Passwort und Passwortänderungen gemäß dieser Richtlinien.

Die Einstellungen wirken auf Spalte *Passwort*. Voraussetzung ist, dass das Kontrollkästchen in Spalte *Richtlinien überprüfen* markiert ist.

Großbuchstaben (min.)

Das Gerät akzeptiert das Passwort, wenn es mindestens so viele Großbuchstaben enthält, wie hier angegeben.

Mögliche Werte:

- `0..16` (Voreinstellung: `1`)

Der Wert `0` deaktiviert diese Richtlinie.

Kleinbuchstaben (min.)

Das Gerät akzeptiert das Passwort, wenn es mindestens so viele Kleinbuchstaben enthält, wie hier angegeben.

Mögliche Werte:

- `0..16` (Voreinstellung: `1`)

Der Wert `0` deaktiviert diese Richtlinie.

Ziffern (min.)

Das Gerät akzeptiert das Passwort, wenn es mindestens so viele Ziffern enthält, wie hier angegeben.

Mögliche Werte:

- `0..16` (Voreinstellung: `1`)

Der Wert `0` deaktiviert diese Richtlinie.

Sonderzeichen (min.)

Das Gerät akzeptiert das Passwort, wenn es mindestens so viele Sonderzeichen enthält, wie hier angegeben.

Mögliche Werte:

- `0..16` (Voreinstellung: `1`)

Der Wert `0` deaktiviert diese Richtlinie.

Tabelle

Jeder Benutzer benötigt ein aktives Benutzerkonto, um Zugriff auf das Management des Geräts zu erhalten. Die Tabelle ermöglicht Ihnen, Benutzerkonten einzurichten und zu verwalten.

Um Einstellungen zu ändern, klicken Sie in der Tabelle den gewünschten Parameter und modifizieren den Wert.

Benutzername

Zeigt die Bezeichnung des Benutzerkontos.

Um ein neues Benutzerkonto anzulegen, klicken Sie die Schaltfläche  .

Aktiv

Aktiviert/deaktiviert das Benutzerkonto.

Mögliche Werte:

- `markiert`
  Das Benutzerkonto ist aktiv. Das Gerät akzeptiert die Anmeldung eines Benutzers mit diesem Benutzernamen.
- `unmarkiert` (Voreinstellung)
  Das Benutzerkonto ist inaktiv. Das Gerät verweigert die Anmeldung eines Benutzers mit diesem Benutzernamen.

Wenn ausschließlich 1 Benutzerkonto mit der Berechtigung *`administrator`* existiert, ist dieses Benutzerkonto stets aktiv.

Passwort

Legt das Passwort fest, das der Benutzer für Zugriffe auf das Management des Geräts über die grafische Benutzeroberfläche oder das Command Line Interface verwendet.

Zeigt ***** (Sternchen) anstelle des Passworts, mit dem sich der Benutzer anmeldet. Um das Passwort zu ändern, klicken Sie in das betreffende Feld.

Wenn Sie das Passwort erstmalig festlegen, verwendet das Gerät in den Spalten *SNMP-Authentifizierungspasswort* und *SNMP-Verschlüsselungspasswort* dasselbe Passwort.

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

Mögliche Werte:

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

Die Mindestlänge des Passworts ist im Rahmen *Konfiguration* festgelegt. Das Gerät unterscheidet zwischen Groß- und Kleinschreibung.

Wenn das Kontrollkästchen in Spalte *Richtlinien überprüfen* markiert ist, dann prüft das Gerät das Passwort gemäß der im Rahmen *Passwort-Richtlinien* festgelegten Richtlinien.

Das Gerät prüft stets die Mindestlänge des Passworts, auch wenn das Kontrollkästchen in Spalte *Richtlinien überprüfen*`unmarkiert` ist.

Rolle

Legt die Benutzer-Rolle fest, die den Zugriff des Benutzers auf die einzelnen Funktionen des Geräts regelt.

Mögliche Werte:

- *unauthorized*
  Der Benutzer ist gesperrt, das Gerät verweigert die Anmeldung des Benutzers.
  Weisen Sie diesen Wert zu, um das Benutzerkonto vorübergehend zu sperren. Wenn beim Zuweisen einer anderen Rolle ein Fehler auftritt, dann weist das Gerät dem Benutzerkonto diese Rolle zu.
- *guest* (Voreinstellung)
  Der Benutzer ist berechtigt, das Gerät zu überwachen.
- *auditor*
  Der Benutzer ist berechtigt, das Gerät zu überwachen und im Dialog *Diagnose > Bericht > Audit-Trail* die Protokoll-Datei zu speichern.
- *operator*
  Der Benutzer ist berechtigt, das Gerät zu überwachen und die Einstellungen zu ändern – mit Ausnahme der Sicherheitseinstellungen für den Zugriff auf das Gerät.
- *administrator*
  Der Benutzer ist berechtigt, das Gerät zu überwachen und die Einstellungen zu ändern.

Den in der Antwort eines RADIUS-Servers übertragenen Service-Type weist das Gerät wie folgt einer Benutzer-Rolle zu:

- `Administrative-User`: *administrator*
- `Login-User`: *operator*
- `NAS-Prompt-User`: *guest*

Benutzer gesperrt

Entsperrt das Benutzerkonto.

Mögliche Werte:

- `markiert`
  Das Benutzerkonto ist gesperrt. Der Benutzer hat keinen Zugriff auf das Management des Geräts.
  Das Gerät sperrt einen Benutzer automatisch, wenn dieser zu oft erfolglos versucht, sich anzumelden.
- `unmarkiert` (ausgegraut) (Voreinstellung)
  Das Benutzerkonto ist entsperrt. Der Benutzer hat Zugriff auf das Management des Geräts.

Richtlinien überprüfen

Aktiviert/deaktiviert das Prüfen des Passworts.

Mögliche Werte:

- `markiert`
  Das Prüfen des Passworts ist aktiviert.
  Beim Einrichten oder Ändern des Passworts prüft das Gerät das Passwort gemäß der im Rahmen *Passwort-Richtlinien*festgelegten Richtlinien.
- `unmarkiert` (Voreinstellung)
  Das Prüfen des Passworts ist deaktiviert.

SNMP-Authentifizierung

Legt das Authentifizierungsprotokoll fest, welches das Gerät beim Zugriff des Benutzers per SNMPv3 anwendet.

Mögliche Werte:

- *hmacmd5* (Voreinstellung)
  Das Gerät verwendet für dieses Benutzerkonto das Protokoll HMAC-MD5.
- *hmacsha*
  Das Gerät verwendet für dieses Benutzerkonto das Protokoll HMAC-SHA.

SNMP-Authentifizierungspasswort

Legt das Passwort fest, welches das Gerät beim Zugriff des Benutzers per SNMPv3 anwendet.

Zeigt ***** (Sternchen) anstelle des Passworts, mit dem sich der Benutzer anmeldet. Um das Passwort zu ändern, klicken Sie in das betreffende Feld.

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

- In der gegenwärtigen Spalte erlaubt Ihnen das Gerät, ein anderes Passwort als in Spalte *Passwort* festzulegen.
- Wenn Sie das Passwort in Spalte *Passwort* ändern, dann ändert das Gerät auch das Passwort für die gegenwärtige Spalte, allerdings ausschließlich dann, wenn dieses zuvor nicht individuell angepasst wurde.

Mögliche Werte:

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

SNMP-Verschlüsselung

Legt das Verschlüsselungsprotokoll fest, welches das Gerät beim Zugriff des Benutzers per SNMPv3 anwendet.

Mögliche Werte:

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

SNMP-Verschlüsselungspasswort

Legt das Passwort fest, welches das Gerät zur Verschlüsselung beim Zugriff des Benutzers per SNMPv3 anwendet.

Zeigt ***** (Sternchen) anstelle des Passworts, mit dem sich der Benutzer anmeldet. Um das Passwort zu ändern, klicken Sie in das betreffende Feld.

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

- In der gegenwärtigen Spalte erlaubt Ihnen das Gerät, ein anderes Passwort als in Spalte *Passwort* festzulegen.
- Wenn Sie das Passwort in Spalte *Passwort* ändern, dann ändert das Gerät auch das Passwort für die gegenwärtige Spalte, allerdings ausschließlich dann, wenn dieses zuvor nicht individuell angepasst wurde.

Mögliche Werte:

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

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

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

3.2 Authentifizierungs-Liste

[Gerätesicherheit > Authentifizierungs-Liste]

In diesem Dialog verwalten Sie die Authentifizierungs-Listen. In einer Authentifizierungsliste legen Sie fest, welche Methode das Gerät für die Authentifizierung verwendet. Sie haben außerdem die Möglichkeit, den Authentifizierungslisten vordefinierte Anwendungen zuzuweisen.

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

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

In der Voreinstellung sind die folgende Authentifizierungslisten verfügbar:
- `defaultDot1x8021AuthList`
- `defaultLoginAuthList`
- `defaultV24AuthList`

Tabelle

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

Name

Zeigt die Bezeichnung der Liste.

Um eine neue Liste anzulegen, klicken Sie die Schaltfläche  .

Mögliche Werte:
- Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

Richtlinie 1
Richtlinie 2
Richtlinie 3
Richtlinie 4
Richtlinie 5

Legt die Authentifizierungsrichtlinie fest, die das Gerät beim Zugriff über die in Spalte *Zugeordnete Anwendungen* festgelegte Anwendung anwendet.

Das Gerät bietet Ihnen die Möglichkeit einer Fall-Back-Lösung. Legen Sie hierfür in den Richtlinien-Feldern jeweils eine andere Richtlinie fest. Abhängig von der Reihenfolge der in den einzelnen Richtlinien eingetragenen Werte kann das Gerät die nächste Richtlinie verwenden, wenn die Authentifizierung mit der festgelegten Richtlinie erfolglos ist.

Mögliche Werte:

- `lokal` (Voreinstellung)
  Das Gerät authentifiziert die Benutzer mittels der lokalen Benutzerverwaltung. Siehe Dialog *Gerätesicherheit > Benutzerverwaltung*.
  Der Authentifizierungliste `defaultDot1x8021AuthList` können Sie diesen Wert nicht zuweisen.
- `radius`
  Das Gerät authentifiziert die Benutzer mit einen RADIUS-Server im Netz. Den RADIUS-Server legen Sie im Dialog *Netzsicherheit > RADIUS > Authentication-Server* fest.
- `reject`
  Abhängig von der Richtlinie, die Sie zuerst anwenden, akzeptiert das Gerät die Authentifizierung oder lehnt die Authentifizierung ab. Mögliche Authentifizierungsszenarios sind:
  - Wenn die erste Richtlinie in der Authentifizierungsliste `lokal` ist und das Gerät die Anmeldedaten des Benutzers akzeptiert, meldet das Gerät den Benutzer an, ohne die anderen Authentifizierungsrichtlinien anzuwenden.
  - Wenn die erste Richtlinie in der Authentifizierungsliste `lokal` ist und das Gerät die Anmeldedaten des Benutzers ablehnt, versucht das Gerät, den Benutzer mithilfe der anderen Richtlinien in der festgelegten Reihenfolge anzumelden.
  - Wenn die erste Richtlinie in der Authentifizierungsliste `radius` oder `ldap` ist und das Gerät die Anmeldung ablehnt, wird die Anmeldung sofort verweigert, ohne dass das Gerät versucht, den Benutzer über eine andere Richtlinie anzumelden.
    Bleibt die Antwort des RADIUS- oder LDAP-Servers aus, versucht das Gerät die Authentifizierung des Benutzers mit der nächsten Richtlinie.
  - Wenn die erste Richtlinie in der Authentifizierungsliste `reject` ist, lehnen die Geräte die Benutzeranmeldung sofort ab, ohne eine andere Richtlinie anzuwenden.
  - Vergewissern Sie sich, dass die Authentifizierungsliste `defaultV24AuthList` mindestens eine Richtlinie enthält, die vom Wert `reject` abweicht.
- `ias`
  Das Gerät authentifiziert die sich per 802.1X anmeldenden Endgeräte mit dem Integrierten Authentifizierungs-Server (IAS). Der Integrierte Authentifizierungs-Server verwaltet die Zugangsdaten in einer eigenständigen Datenbank. Siehe Dialog *Netzsicherheit > 802.1X Port-Authentifizierung > Integrierter Authentifikations-Server*.
  Der Authentifizierungliste `defaultDot1x8021AuthList` können Sie ausschließlich diesen Wert zuweisen.
- `ldap`
  Das Gerät authentifiziert die Benutzer über Authentifizierungsdaten und die Zugriffsrolle, die an einem zentralen Ort gespeichert sind. Den vom Gerät verwendeten Active-Directory-Server legen Sie im Dialog *Netzsicherheit > LDAP > Konfiguration* fest.

Zugeordnete Anwendungen

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

Um der Liste eine andere Anwendung zuzuordnen oder die Zuordnung aufzuheben, klicken Sie die Schaltfläche ☰ und dann den Eintrag *Anwendungen zuordnen*. Das Gerät ermöglicht Ihnen, jede Anwendung genau einer Liste zuzuordnen.

Aktiv

Aktiviert/deaktiviert die Liste.

Mögliche Werte:

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

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Anwendungen zuordnen

Öffnet das Fenster *Anwendungen zuordnen*.

- Das linke Feld zeigt die Anwendungen, die sich der ausgewählten Liste zuordnen lassen.
- Das rechte Feld zeigt die Anwendungen, die der ausgewählten Liste zugeordnet sind.
- Schaltflächen:
  - Verschiebt jeden Eintrag in das rechte Feld.
  - Verschiebt die markierten Einträge aus dem linken Feld in das rechte Feld.
  - Verschiebt die markierten Einträge aus dem rechten Feld in das linke Feld.
  - Verschiebt jeden Eintrag in das linke Feld.

Anmerkung: Wenn Sie den Eintrag `WebInterface` in das linke Feld verschieben, bricht die Verbindung zum Gerät ab, sobald Sie die Schaltfläche *Ok* klicken.

3.3 LDAP

[Gerätesicherheit > LDAP]

Das Lightweight Directory Access Protocol (LDAP) ermöglicht Ihnen, die Benutzer an einer zentralen Stelle im Netz zu authentifizieren und zu autorisieren. Ein weit verbreiteter, mit LDAP abfragbarer Verzeichnisdienst ist Active Directory®.

Das Gerät leitet die Zugangsdaten der Benutzer mit dem LDAP-Protokoll weiter an den Authentication-Server. Der Authentication-Server entscheidet, ob die Zugangsdaten gültig sind und übermittelt dem Gerät die Berechtigungen des Benutzers.

Nach erfolgreicher Anmeldung speichert das Gerät die Anmeldeinformationen temporär zwischen. Dies beschleunigt den Anmeldevorgang, wenn sich Benutzer erneut anmelden. In diesem Fall ist keine aufwendige LDAP-Suchoperation notwendig.

Das Menü enthält die folgenden Dialoge:

- LDAP Konfiguration
- LDAP Rollen-Zuweisung

3.3.1 LDAP Konfiguration

[Gerätesicherheit > LDAP > Konfiguration]

Dieser Dialog ermöglicht Ihnen, bis zu 4 Authentication-Server festzulegen. Ein Authentication-Server authentifiziert und autorisiert die Benutzer, wenn das Gerät die Zugangsdaten an ihn weiterleitet.

Das Gerät sendet die Zugangsdaten an den ersten Authentication-Server. Bleibt dessen Antwort aus, kontaktiert das Gerät den jeweils nächsten Server in der Tabelle.

Funktion

Funktion

Schaltet den *LDAP*-Client ein/aus.

Das Gerät verwendet den *LDAP*-Client, wenn Sie im Dialog *Gerätesicherheit > Authentifizierungs-Liste* den Wert `ldap` in einer der Spalten *Richtlinie 1* bis *Richtlinie 5* festlegen. Legen Sie zuvor im Dialog *Gerätesicherheit > LDAP > Rollen-Zuweisung* mindestens ein Mapping für die Rolle `administrator` fest. Damit haben Sie nach Anmeldung über LDAP weiterhin als Administrator Zugriff auf das Gerät.

Mögliche Werte:

- `An`
  Der *LDAP*-Client ist eingeschaltet.
- `Aus` (Voreinstellung)
  Der *LDAP*-Client ist ausgeschaltet.

Konfiguration

Client-Cache-Timeout [min]

Legt fest, wie viele Minuten die Anmeldeinformation nach erfolgreicher Anmeldung eines Benutzers gültig bleibt. Wenn ein Benutzer sich innerhalb dieser Zeit erneut anmeldet, ist keine aufwendige LDAP-Suchoperation notwendig. Der Anmeldevorgang ist deutlich schneller.

Mögliche Werte:

- `1..1440` (Voreinstellung: `10`)

Bind-Benutzer

Legt die Benutzerkennung in Form des „Distinguished Name“ (DN) fest, mit der das Gerät sich am LDAP-Server anmeldet.

Diese Angabe ist erforderlich, wenn der LDAP-Server bei der Anmeldung eine Benutzerkennung in Form des „Distinguished Name“ (DN) erfordert. In Active-Directory-Umgebungen ist diese Angabe nicht erforderlich.

Das Gerät meldet sich mit dieser Benutzerkennung am LDAP-Server an, um den „Distinguished Name“ (DN) für sich anmeldende Benutzer zu finden. Das Gerät sucht gemäß den Einstellungen in den Feldern *Base DN* und *Benutzername-Attribut*.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

Bind-Benutzer Passwort

Legt das Passwort fest, das das Gerät bei der Anmeldung am LDAP-Server zusammen mit der in Feld *Bind-Benutzer* festgelegten Benutzerkennung verwendet.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

Base DN

Legt den Startpunkt in Form des „Distinguished Name“ (DN) fest für die Suche im Verzeichnisbaum.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Benutzername-Attribut

Legt das LDAP-Attribut fest, das einen eineindeutigen Benutzernamen enthält. Später verwendet der Benutzer den in diesem Attribut enthaltenen Benutzernamen, um sich anzumelden.

Häufig enthalten die LDAP-Attribute `userPrincipalName`, `mail`, `sAMAccountName` und `uid` einen eineindeutigen Benutzernamen.

Unter der folgenden Voraussetzung fügt das Gerät die im Feld *Default-Domain* festgelegte Zeichenfolge an den Benutzernamen an:

- Der im Attribut enthaltene Benutzername enthält kein @-Zeichen.
- Im Feld *Default-Domain* ist ein Domänenname festgelegt.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen
  (Voreinstellung: `userPrincipalName`)

Default-Domain

Legt die Zeichenfolge fest, mit der das Gerät den Benutzernamen sich anmeldender Benutzer ergänzt, sofern der Benutzername kein @-Zeichen enthält.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

CA certificate

URL

Legt Pfad und Dateiname des Zertifikats fest.

Zulässig sind Zertifikate mit folgenden Eigenschaften:

- X.509-Format
- `.PEM` Dateinamenserweiterung
- Base64-kodiert, umschlossen von
  `-----BEGIN CERTIFICATE-----`
  und
  `-----END CERTIFICATE-----`

Aus Sicherheitsgründen empfehlen wir, stets ein Zertifikat zu verwenden, das von einer Zertifizierungsstelle signiert ist.

Das Gerät bietet Ihnen folgende Möglichkeiten, das Zertifikat in das Gerät zu kopieren:

- Import vom PC
  Befindet sich das Zertifikat auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie das Zertifikat in den -Bereich. Alternativ klicken Sie in den Bereich, um das Zertifikat auszuwählen.
- Import von einem FTP-Server
  Befindet sich das Zertifikat auf einem FTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  `ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Pfad>/<Dateiname>`
- Import von einem TFTP-Server
  Befindet sich das Zertifikat auf einem TFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  `tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
- Import von einem SCP- oder SFTP-Server
  Befindet sich das Zertifikat auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  - `scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`
    Nach Klicken der Schaltfläche *Start* zeigt das Gerät das Fenster *Anmeldeinformationen*. Geben Sie dort *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
  - `scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>`

Start

Kopiert das im Feld *URL* festgelegte Zertifikat in das Gerät.

Tabelle

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Beschreibung

Legt die Beschreibung fest.

Wenn gewünscht, beschreiben Sie hier den Authentication-Server oder notieren zusätzliche Informationen.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Adresse

Legt IP-Adresse oder DNS-Name des Servers fest.

Mögliche Werte:

- IPv4-Adresse (Voreinstellung: `0.0.0.0`)
- IPv6-Adresse
- DNS-Name im Format `<domain>.<tld>` oder `<host>.<domain>.<tld>`
- `_ldap._tcp.<domain>.<tld>`
  Mit diesem DNS-Namen erfragt das Gerät die LDAP-Server-Liste (SRV Resource Record) beim DNS-Server.

Verwenden Sie einen DNS-Namen, wenn in Spalte *Verbindungssicherheit* ein anderer Wert als *kein* festgelegt ist und das Zertifikat ausschließlich DNS-Namen des Servers enthält. Schalten Sie die Funktion *Client* im Dialog *Erweitert > DNS > Client > Global* ein.

Ziel-TCP-Port

Legt den TCP-Port fest, auf dem der Server die Anfragen erwartet.

Wenn in Spalte *Adresse* der Wert `_ldap._tcp.domain.tld` festgelegt ist, dann ignoriert das Gerät den hier festgelegten Wert.

Mögliche Werte:

- `0..65535` (Voreinstellung: `389`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Häufig verwendete TCP-Ports:

- `LDAP: 389`
- `LDAP over SSL: 636`
- `Active Directory Global Catalogue: 3268`
- `Active Directory Global Catalogue SSL: 3269`

Verbindungssicherheit

Legt das Protokoll fest, das die Kommunikation zwischen Gerät und Authentication-Server verschlüsselt.

Mögliche Werte:

- *kein*
  Keine Verschlüsselung.
  Das Gerät baut eine LDAP-Verbindung zum Server auf und überträgt die Kommunikation inklusive Passwörter im Klartext.
- *ssl*
  Verschlüsselung mit SSL.
  Das Gerät baut eine TLS-Verbindung zum Server auf und tunnelt darüber die LDAP-Kommunikation.
- *startTLS* (Voreinstellung)
  Verschlüsselung mit startTLS-Erweiterung.
  Das Gerät baut eine LDAP-Verbindung zum Server auf und verschlüsselt die Kommunikation.

Voraussetzung für die verschlüsselte Kommunikation ist, dass das Gerät die korrekte Uhrzeit verwendet. Wenn das Zertifikat ausschließlich DNS-Namen enthält, dann legen Sie in Spalte *Adresse* den DNS-Namen des Servers fest. Schalten Sie die Funktion *Client* im Dialog *Erweitert* > DNS > *Client* > *Global* ein.

Wenn das Zertifikat im Feld “Subject Alternative Name” die IP-Adresse des Servers enthält, kann das Gerät ohne DNS-Konfiguration die Identität des Servers verifizieren.

Server-Status

Zeigt den Verbindungsstatus und die Authentifizierung mit dem Authentication-Server.

Mögliche Werte:

- *ok*
  Der Server ist erreichbar.
  Wenn in Spalte *Verbindungssicherheit* ein anderer Wert als *kein* festgelegt ist, dann hat das Gerät das Zertifikat des Servers verifiziert.
- *unreachable*
  Server ist unerreichbar.
- *other*
  Das Gerät hat noch keine Verbindung zum Server aufgebaut.

Aktiv

Aktiviert/deaktiviert die Verwendung des Servers.

Mögliche Werte:

- markiert
  Das Gerät verwendet den Server.
- unmarkiert (Voreinstellung)
  Das Gerät verwendet den Server nicht.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Cache leeren

Entfernt die zwischengespeicherten Anmeldeinformationen der erfolgreich angemeldeten Benutzer.

3.3.2 LDAP Rollen-Zuweisung

[Gerätesicherheit > LDAP > Rollen-Zuweisung]

Dieser Dialog ermöglicht Ihnen, bis zu 64 Mappings zu erstellen, um Benutzern eine Rolle zuzuweisen.

In der Tabelle legen Sie fest, ob das Gerät anhand eines Attributs mit einem bestimmten Wert oder anhand der Gruppenitgliedschaft dem Benutzer eine Rolle zuweist.
- Attribut und Attributwert sucht das Gerät innerhalb des Benutzerobjekts.
- Die Gruppenmitgliedschaft prüft das Gerät durch Auswertung des in den Member-Attributen enthaltenen „Distinguished Name“ (DN).

Wenn ein Benutzer sich anmeldet, sucht das Gerät auf dem LDAP-Server folgende Informationen:
- Im zugehörigen Benutzerobjekt sucht das Gerät die in den Mappings festgelegten Attribute.
- In den Gruppenobjekten der in den Mappings festgelegten Gruppen sucht das Gerät die Member-Attribute.

Darauf basierend prüft das Gerät jedes Mapping:
- Enthält das Benutzerobjekt das erforderliche Attribut?
  oder
- Ist der Benutzer Mitglied der Gruppe?

Wenn das Gerät keine Übereinstimmung findet, dann erhält der Benutzer keinen Zugriff auf das Gerät.

Wenn das Gerät mehr als ein zutreffendes Mapping für einen Benutzer findet, dann entscheidet die Einstellung im Feld *Übereinstimmende Regel*. Entweder erhält der Benutzer die Rolle mit den weitreichenderen Berechtigungen oder die 1. in der Tabelle zutreffende Rolle.

Konfiguration

Übereinstimmende Regel

Legt fest, welche Rolle das Gerät verwendet, wenn mehr als ein Mapping für einen Benutzer zutrifft.

Mögliche Werte:
- *highest* (Voreinstellung)
  Das Gerät verwendet die Rolle mit den weitreichenderen Berechtigungen.
- *first*
  Das Gerät wendet die Rolle mit dem kleineren Wert in Spalte *Index* auf den Benutzer an.

Tabelle

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Rolle

Legt die Benutzer-Rolle fest, die den Zugriff des Benutzers auf die einzelnen Funktionen des Geräts regelt.

Mögliche Werte:

- *unauthorized*
  Der Benutzer ist gesperrt, das Gerät verweigert die Anmeldung des Benutzers.
  Weisen Sie diesen Wert zu, um das Benutzerkonto vorübergehend zu sperren. Wenn beim Zuweisen einer anderen Rolle ein Fehler erkannt wird, dann weist das Gerät dem Benutzerkonto diese Rolle zu.
- *guest* (Voreinstellung)
  Der Benutzer ist berechtigt, das Gerät zu überwachen.
- *auditor*
  Der Benutzer ist berechtigt, das Gerät zu überwachen und im Dialog *Diagnose > Bericht > Audit-Trail* die Protokoll-Datei zu speichern.
- *operator*
  Der Benutzer ist berechtigt, das Gerät zu überwachen und die Einstellungen zu ändern – mit Ausnahme der Sicherheitseinstellungen für den Zugriff auf das Gerät.
- *administrator*
  Der Benutzer ist berechtigt, das Gerät zu überwachen und die Einstellungen zu ändern.

Typ

Legt fest, ob in Spalte *Parameter* eine Gruppe oder ein Attribut mit einem Attributwert angegeben ist.

Mögliche Werte:

- *attribute* (Voreinstellung)
  Die Spalte *Parameter* enthält ein Attribut mit einem Attributwert.
- *group*
  Die Spalte *Parameter* enthält den „Distinguished Name“ (DN) einer Gruppe.

Parameter

Legt abhängig von der Einstellung in Spalte *Typ* eine Gruppe oder ein Attribut mit einem Attributwert fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen
  Das Gerät unterscheidet zwischen Groß- und Kleinschreibung.
  - Wenn in Spalte *Typ* der Wert *attribute* festgelegt ist, dann legen Sie das Attribut in der Form `Attributname=Attributwert` fest.
    Beispiel: `l=Germany`
  - Wenn in Spalte *Typ* der Wert *group* festgelegt ist, dann legen Sie den „Distinguished Name“ (DN) einer Gruppe fest.
    Beispiel: `CN=admin-users,OU=Groups,DC=example,DC=com`

Aktiv

Aktiviert/deaktiviert das Mapping der Rolle.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Mapping der Rolle ist aktiv.
- `unmarkiert`
  Das Mapping der Rolle ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

- Im Feld *Index* legen Sie die Index-Nummer fest.
  Mögliche Werte:
  - `1..64`

3.4 Management-Zugriff

[Gerätesicherheit > Management-Zugriff]

Das Menü enthält die folgenden Dialoge:

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

3.4.1 Server

[Gerätesicherheit > Management-Zugriff > Server]

Dieser Dialog ermöglicht Ihnen, die Server-Dienste einzurichten, mit denen Benutzer oder Anwendungen Management-Zugriff auf das Gerät erhalten.

Der Dialog enthält die folgenden Registerkarten:
- [Information]
- [SNMP]
- [Telnet]
- [SSH]
- [HTTP]
- [HTTPS]

[Information]

Diese Registerkarte zeigt im Überblick, welche Server-Dienste eingeschaltet sind.

Tabelle

SNMPv1

Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit SNMP Version 1 ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte *SNMP*.

Mögliche Werte:
- `markiert`
  Server-Dienst ist aktiv.
- `unmarkiert`
  Server-Dienst ist inaktiv.

SNMPv2

Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit SNMP Version 2 ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte *SNMP*.

Mögliche Werte:
- `markiert`
  Server-Dienst ist aktiv.
- `unmarkiert`
  Server-Dienst ist inaktiv.

SNMPv3

Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit SNMP Version 3 ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte *SNMP*.

Mögliche Werte:

- `markiert`
  Server-Dienst ist aktiv.
- `unmarkiert`
  Server-Dienst ist inaktiv.

Telnet server

Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit Telnet ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte *Telnet*.

Mögliche Werte:

- `markiert`
  Server-Dienst ist aktiv.
- `unmarkiert`
  Server-Dienst ist inaktiv.

SSH-Server

Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit Secure Shell ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte *SSH*.

Mögliche Werte:

- `markiert`
  Server-Dienst ist aktiv.
- `unmarkiert`
  Server-Dienst ist inaktiv.

HTTP server

Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit der grafischen Bedienoberfläche über HTTP ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte *HTTP*.

Mögliche Werte:

- `markiert`
  Server-Dienst ist aktiv.
- `unmarkiert`
  Server-Dienst ist inaktiv.

HTTPS server

Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit der grafischen Bedienoberfläche über HTTPS ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte *HTTPS*.

Mögliche Werte:

- `markiert`
  Server-Dienst ist aktiv.
- `unmarkiert`
  Server-Dienst ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[SNMP]

Diese Registerkarte ermöglicht Ihnen, Einstellungen für den SNMP-Agenten des Geräts festzulegen und den Zugriff auf das Gerät mit unterschiedlichen SNMP-Versionen ein-/auszuschalten.

Der SNMP-Agent ermöglicht den Zugriff auf das Management des Geräts mit SNMP-basierten Anwendungen.

Konfiguration

SNMPv1

Aktiviert/deaktiviert den Zugriff auf das Gerät per SNMP Version 1.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Zugriff ist aktiviert.
- `unmarkiert`
  Zugriff ist deaktiviert.

Die Community-Namen legen Sie fest im Dialog *Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community*.

SNMPv2

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

Mögliche Werte:

- `markiert` (Voreinstellung)
  Zugriff ist aktiviert.
- `unmarkiert`
  Zugriff ist deaktiviert.

Die Community-Namen legen Sie fest im Dialog *Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community*.

SNMPv3

Aktiviert/deaktiviert den Zugriff auf das Gerät per SNMP Version 3.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Zugriff ist aktiviert.
- `unmarkiert`
  Zugriff ist deaktiviert.

Netzmanagementsysteme wie ConneXium Network Manager verwenden dieses Protokoll, um mit dem Gerät zu kommunizieren.

UDP-Port

Legt die Nummer des UDP-Ports fest, auf dem der SNMP-Agent Anfragen von Clients entgegennimmt.

Mögliche Werte:

- `1..65535` (Voreinstellung: `161`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Damit der SNMP-Agent nach einer Änderung den neuen Port verwendet, gehen Sie wie folgt vor:

- ☐ Klicken Sie die Schaltfläche ✓.
- ☐ Wählen Sie im Dialog *Grundeinstellungen > Laden/Speichern* das aktive Konfigurationsprofil.
- ☐ Klicken Sie die Schaltfläche 💾, um die gegenwärtigen Änderungen zu speichern.
- ☐ Starten Sie das Gerät neu.

SNMPover802

Aktiviert/deaktiviert den Zugriff auf das Gerät per SNMP über IEEE-802.

Mögliche Werte:

- `markiert`
  Zugriff ist aktiviert.
- `unmarkiert` (Voreinstellung)
  Zugriff ist deaktiviert.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Telnet]

Diese Registerkarte ermöglicht Ihnen, den Telnet-Server im Gerät ein-/auszuschalten und die für Telnet erforderlichen Einstellungen festzulegen.

Der Telnet-Server ermöglicht den Zugriff auf das Management des Geräts per Fernzugriff mit dem Command Line Interface. Telnet-Verbindungen sind unverschlüsselt.

Funktion

Telnet server

Schaltet den Telnet-Server ein/aus.

Mögliche Werte:

- Der Telnet-Server ist eingeschaltet.
  Der Zugriff auf das Management des Geräts ist möglich mit dem Command Line Interface über eine unverschlüsselte Telnet-Verbindung.
- Der Telnet-Server ist ausgeschaltet.

Anmerkung: Wenn der *SSH*-Server ausgeschaltet ist und Sie auch den *Telnet*-Server ausschalten, dann ist der Zugriff auf das Command Line Interface ausschließlich über die serielle Schnittstelle des Geräts möglich.

Konfiguration

TCP-Port

Legt die Nummer des TCP-Ports fest, auf dem das Gerät Telnet-Anfragen von den Clients entgegennimmt.

Mögliche Werte:

- `1..65535` (Voreinstellung: `23`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Nach Ändern des Ports startet der Server automatisch neu. Bestehende Verbindungen bleiben aufgebaut.

Verbindungen

Zeigt, wie viele Telnet-Verbindungen gegenwärtig zum Gerät aufgebaut sind.

Verbindungen (max.)

Legt fest, wie viele gleichzeitige Telnet-Verbindungen zum Gerät maximal möglich sind.

Mögliche Werte:

- `1..5` (Voreinstellung: `5`)

Session-Timeout [min]

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

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

Mögliche Werte:

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

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[SSH]

Diese Registerkarte ermöglicht Ihnen, den SSH-Server im Gerät ein-/auszuschalten und die für SSH erforderlichen Einstellungen festzulegen. Der Server arbeitet mit SSH-Version 2.

Der SSH-Server ermöglicht den Zugriff auf das Management des Geräts per Fernzugriff mit dem Command Line Interface. SSH-Verbindungen sind verschlüsselt.

Der SSH-Server identifiziert sich gegenüber den Clients mit seinem öffentlichen RSA-Schlüssel. Beim 1. Verbindungsaufbau zeigt das Client-Programm dem Benutzer den Fingerprint dieses Schlüssels. Der Fingerprint enthält eine einfach zu prüfende, Base64-kodierte Zeichenfolge. Wenn Sie den Benutzern diese Zeichenfolge über einen vertrauenswürdigen Kanal zur Verfügung stellen, haben diese die Möglichkeit, beide Fingerprints zu vergleichen. Wenn die Zeichenfolgen übereinstimmen, dann ist der Client mit dem korrekten Server verbunden.

Das Gerät ermöglicht Ihnen, die für RSA erforderlichen privaten und öffentlichen Schlüssel (Host Keys) direkt auf dem Gerät zu erzeugen. Andernfalls haben Sie die Möglichkeit, eigene Schlüssel im PEM-Format auf das Gerät zu kopieren.

Alternativ ermöglicht Ihnen das Gerät, den RSA-Schlüssel (Host Key) beim Neustart vom externen Speicher zu laden. Diese Funktion aktivieren Sie im Dialog *Grundeinstellungen > Externer Speicher*, Spalte *SSH-Key automatisch uploaden*.

Funktion

SSH-Server

Schaltet den SSH-Server ein/aus.

Mögliche Werte:

- `An` (Voreinstellung)
  Der SSH-Server ist eingeschaltet.
  Der Zugriff auf das Management des Geräts ist möglich mit dem Command Line Interface über eine verschlüsselte SSH-Verbindung.
  Der Server lässt sich ausschließlich dann starten, wenn eine RSA-Signatur im Gerät vorhanden ist.
- `Aus`
  Der SSH-Server ist ausgeschaltet.
  Wenn Sie den SSH-Server ausschalten, bleiben bestehende Verbindungen aufgebaut. Das Gerät sorgt dafür, den Aufbau neuer Verbindungen zu verhindern.

Anmerkung: Wenn der *Telnet*-Server ausgeschaltet ist und Sie auch den *SSH*-Server ausschalten, dann ist der Zugriff auf das Command Line Interface ausschließlich über die serielle Schnittstelle des Geräts möglich.

Konfiguration

TCP-Port

Legt die Nummer des TCP-Ports fest, auf dem das Gerät SSH-Anfragen von den Clients entgegennimmt.

Mögliche Werte:

- `1..65535` (Voreinstellung: `22`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Nach Ändern des Ports startet der Server automatisch neu. Bestehende Verbindungen bleiben aufgebaut.

Sessions

Zeigt, wie viele SSH-Verbindungen gegenwärtig zum Gerät aufgebaut sind.

Sitzungen (max.)

Legt fest, wie viele gleichzeitige SSH-Verbindungen zum Gerät maximal möglich sind.

Mögliche Werte:

- `1..5` (Voreinstellung: `5`)

Session-Timeout [min]

Legt die Timeout-Zeit in Minuten fest. Bei Inaktivität des angemeldeten Benutzers trennt das Gerät nach dieser Zeit die Verbindung.

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

Mögliche Werte:

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

Fingerabdruck

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

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

Fingerabdruck-Typ

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

Mögliche Werte:

- `md5`
  Das Feld *RSA-Fingerabdruck* zeigt den Fingerprint als hexadezimalen MD5-Hash.
- `sha256`
  Das Feld *RSA-Fingerabdruck* zeigt den Fingerprint als Base64-codierten SHA256-Hash.

RSA-Fingerabdruck

Zeigt den Fingerprint des öffentlichen Host-Keys des SSH-Servers.

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

Signatur

RSA vorhanden

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

Mögliche Werte:

- `markiert`
  Schlüssel vorhanden.
- `unmarkiert`
  Kein Schlüssel vorhanden.

Erzeugen

Erzeugt einen Host-Key auf dem Gerät. Voraussetzung ist, dass der *SSH*-Server ausgeschaltet ist.

Länge des erzeugten Schlüssels:

- 2048 Bit (RSA)

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

Alternativ haben Sie die Möglichkeit, einen eigenen Host-Key im PEM-Format auf das Gerät zu kopieren. Siehe Rahmen *Key-Import*.

Löschen

Entfernt den Host-Key aus dem Gerät. Voraussetzung ist, dass der SSH-Server ausgeschaltet ist.

Betriebszustand

Zeigt, ob das Gerät gegenwärtig einen Host-Key erzeugt.

Möglicherweise hat ein anderer Benutzer diese Aktion ausgelöst.

Mögliche Werte:

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

Key-Import

URL

Legt Pfad und Dateiname Ihres RSA-Host-Keys fest.

Das Gerät akzeptiert den RSA-Schlüssel, wenn dieser die folgende Schlüssellänge aufweist:

- 2048 bit (RSA)

Das Gerät bietet Ihnen folgende Möglichkeiten, den Schlüssel in das Gerät zu kopieren:

- Import vom PC
  Befindet sich der Host-Key auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie die Datei, die den Host-Key enthält, in den -Bereich. Alternativ klicken Sie in den Bereich, um die Datei auszuwählen.
- Import von einem FTP-Server
  Befindet sich der Schlüssel auf einem FTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  `ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Dateiname>`
- Import von einem TFTP-Server
  Befindet sich der Schlüssel auf einem TFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  `tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
- Import von einem SCP- oder SFTP-Server
  Befindet sich der Schlüssel auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  - `scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`
    Nach Klicken der Schaltfläche *Start* zeigt das Gerät das Fenster *Anmeldeinformationen*. Geben Sie dort *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
  - `scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>`

Start

Kopiert den im Feld *URL* festgelegten Key in das Gerät.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[HTTP]

Diese Registerkarte ermöglicht Ihnen, für den Webserver das Protokoll HTTP ein-/auszuschalten und die für HTTP erforderlichen Einstellungen festzulegen.

Der Webserver liefert die grafische Benutzeroberfläche über eine unverschlüsselte HTTP-Verbindung aus. Deaktivieren Sie aus Sicherheitsgründen das HTTP-Protokoll, verwenden Sie stattdessen das HTTPS-Protokoll.

Das Gerät unterstützt bis zu 10 gleichzeitige Verbindungen per HTTP oder HTTPS.

Anmerkung: Wenn Sie Einstellungen in dieser Registerkarte ändern und die Schaltfläche ☑ klicken, dann beendet das Gerät die Sitzung und trennt jede geöffnete Verbindung. Um wieder mit der grafischen Benutzeroberfläche zu arbeiten, melden Sie sich erneut an.

Funktion

HTTP server

Schaltet für den Webserver das Protokoll *HTTP* ein/aus.

Mögliche Werte:

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

Anmerkung: Wenn die Protokolle *HTTP* und *HTTPS* ausgeschaltet sind, können Sie das Protokoll *HTTP* mit dem Kommando `http server` im Command Line Interface einschalten, um die grafische Benutzeroberfläche zu erreichen.

Konfiguration

TCP-Port

Legt die Nummer des TCP-Ports fest, auf dem der Webserver HTTP-Anfragen von den Clients entgegennimmt.

Mögliche Werte:

- `1..65535` (Voreinstellung: `80`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[HTTPS]

Diese Registerkarte ermöglicht Ihnen, für den Webserver das Protokoll HTTPS ein-/auszuschalten und die für HTTPS erforderlichen Einstellungen festzulegen.

Der Webserver liefert die grafische Benutzeroberfläche über eine verschlüsselte HTTP-Verbindung aus.

Für die Verschlüsselung der HTTP-Verbindung ist ein digitales Zertifikat notwendig. Das Gerät ermöglicht Ihnen, dieses Zertifikat selbst zu erzeugen oder ein vorhandenes Zertifikat auf das Gerät zu laden.

Das Gerät unterstützt bis zu 10 gleichzeitige Verbindungen per HTTP oder HTTPS.

Anmerkung: Wenn Sie Einstellungen in dieser Registerkarte ändern und die Schaltfläche ✓ klicken, dann beendet das Gerät die Sitzung und trennt jede geöffnete Verbindung. Um wieder mit der grafischen Benutzeroberfläche zu arbeiten, melden Sie sich erneut an.

Funktion

HTTPS server

Schaltet für den Webserver das Protokoll *HTTPS* ein/aus.

Mögliche Werte:

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

Anmerkung: Wenn die Protokolle *HTTP* und *HTTPS* ausgeschaltet sind, können Sie das Protokoll *HTTPS* mit dem Kommando `https server` im Command Line Interface einschalten, um die grafische Benutzeroberfläche zu erreichen.

Konfiguration

TCP-Port

Legt die Nummer des TCP-Ports fest, auf dem der Webserver HTTPS-Anfragen von den Clients entgegennimmt.

Mögliche Werte:

- `1..65535` (Voreinstellung: `443`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Fingerabdruck

Der Fingerprint ist eine einfach zu prüfende, hexadezimale Ziffernfolge, die das digitale Zertifikat des HTTPS-Servers eindeutig identifiziert.

Nach dem Importieren oder Erzeugen eines neuen digitalen Zertifikats zeigt das Gerät den gegenwärtig gültigen Fingerprint so lange, bis Sie den Server neu starten.

Fingerabdruck-Typ

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

Mögliche Werte:

- *sha1*
  Das Feld *Fingerabdruck* zeigt den SHA1-Fingerprint des Zertifikats.
- *sha256*
  Das Feld *Fingerabdruck* zeigt den SHA256-Fingerprint des Zertifikats.

Fingerabdruck

Zeichenfolge des digitalen Zertifikats, das der Server verwendet.

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

Zertifikat

Anmerkung: Beim Laden der grafischen Benutzeroberfläche zeigt der Web-Browser eine Meldung, wenn das Gerät ein Zertifikat verwendet, das nicht von einer Zertifizierungsstelle signiert wurde. Um fortzufahren, fügen Sie im Web-Browser eine Ausnahmeregel für das Zertifikat hinzu.

Vorhanden

Zeigt, ob das digitale Zertifikat im Gerät vorhanden ist.

Mögliche Werte:

- `markiert`
  Das Zertifikat ist vorhanden.
- `unmarkiert`
  Das Zertifikat wurde entfernt.

Erzeugen

Generiert ein digitales Zertifikat auf dem Gerät.

Bis zum Neustart verwendet der Webserver das vorherige Zertifikat.

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

Alternativ haben Sie die Möglichkeit, ein eigenes Zertifikat in das Gerät zu kopieren. Siehe Rahmen *Zertifikat-Import*.

Löschen

Entfernt das digitale Zertifikat.

Bis zum Neustart verwendet der Webserver das vorherige Zertifikat.

Betriebszustand

Zeigt, ob das Gerät gegenwärtig ein digitales Zertifikat generiert oder löscht.

Möglicherweise hat ein anderer Benutzer die Aktion ausgelöst.

Mögliche Werte:

- *kein*
  Das Gerät generiert oder löscht gegenwärtig kein Zertifikat.
- *delete*
  Das Gerät löscht gegenwärtig ein Zertifikat.
- *generate*
  Das Gerät generiert gegenwärtig ein Zertifikat.

Zertifikat-Import

URL

Legt Pfad und Dateiname des Zertifikats fest.

Zulässig sind Zertifikate mit folgenden Eigenschaften:

- X.509-Format
- `.PEM` Dateinamenserweiterung
- Base64-kodiert, umschlossen von
  - `-----BEGIN PRIVATE KEY-----`
    und
    `-----END PRIVATE KEY-----`
    sowie
  - `-----BEGIN CERTIFICATE-----`
    und
    `-----END CERTIFICATE-----`
- RSA-Schlüssel mit 2048 bit Länge

Das Gerät bietet Ihnen folgende Möglichkeiten, das Zertifikat in das Gerät zu kopieren:

- Import vom PC
  Befindet sich das Zertifikat auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie das Zertifikat in den  -Bereich. Alternativ klicken Sie in den Bereich, um das Zertifikat auszuwählen.
- Import von einem FTP-Server
  Befindet sich das Zertifikat auf einem FTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  `ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Pfad>/<Dateiname>`
- Import von einem TFTP-Server
  Befindet sich das Zertifikat auf einem TFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  `tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
- Import von einem SCP- oder SFTP-Server
  Befindet sich das Zertifikat auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  - `scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`
    Nach Klicken der Schaltfläche *Start* zeigt das Gerät das Fenster *Anmeldeinformationen*. Geben Sie dort *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
  - `scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>`

Start

Kopiert das im Feld *URL* festgelegte Zertifikat in das Gerät.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

3.4.2 IP-Zugriffsbeschränkung

[Gerätesicherheit > Management-Zugriff > IP-Zugriffsbeschränkung]

Dieser Dialog bietet Ihnen die Möglichkeit, den Zugriff auf das Management des Geräts auf gewisse IP-Adressbereiche und ausgewählte IP-basierte Anwendungen zu beschränken.

- Bei ausgeschalteter Funktion ist der Zugriff auf das Management des Geräts von jeder beliebigen IP-Adresse und mit jeder Anwendung möglich.
- Bei eingeschalteter Funktion ist der Zugriff beschränkt. Ausschließlich unter den folgenden Voraussetzungen haben Sie Zugriff auf das Management des Geräts:
  - Mindestens ein Tabelleneintrag ist aktiviert.
    und
  - Sie verbinden sich mit einer erlaubten Anwendung aus einem zugelassenen IP-Adressbereich mit dem Gerät.

Funktion

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

Funktion

Schaltet die Funktion *IP-Zugriffsbeschränkung* ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *IP-Zugriffsbeschränkung* ist eingeschaltet.
  Der Zugriff auf das Management des Geräts ist beschränkt.
- `Aus` (Voreinstellung)
  Die Funktion *IP-Zugriffsbeschränkung* ist ausgeschaltet.

Tabelle

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

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Wenn Sie einen Tabelleneintrag löschen, bleibt eine Lücke in der Nummerierung. Wenn Sie einen neuen Tabelleneintrag erzeugen, schließt das Gerät die 1. Lücke.

Mögliche Werte:

- `1..16`

Adresse

Legt die IP-Adresse des Netzes fest, von dem aus Sie den Zugriff auf das Management des Geräts erlauben. Den Netz-Bereich legen Sie fest in Spalte *Netzmaske*.

Mögliche Werte:

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

Netzmaske

Legt den Bereich des in Spalte *Adresse* festgelegten Netzes fest.

Mögliche Werte:

- Gültige Netzmaske (Voreinstellung: `0.0.0.0`)

HTTP

Aktiviert/deaktiviert den HTTP-Zugriff.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Zugriff ist aktiviert für nebenstehenden IP-Adressbereich.
- `unmarkiert`
  Zugriff ist deaktiviert.

HTTPS

Aktiviert/deaktiviert den HTTPS-Zugriff.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Zugriff ist aktiviert für nebenstehenden IP-Adressbereich.
- `unmarkiert`
  Zugriff ist deaktiviert.

SNMP

Aktiviert/deaktiviert den SNMP-Zugriff.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Zugriff ist aktiviert für nebenstehenden IP-Adressbereich.
- `unmarkiert`
  Zugriff ist deaktiviert.

Telnet

Aktiviert/deaktiviert den Telnet-Zugriff.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Zugriff ist aktiviert für nebenstehenden IP-Adressbereich.
- `unmarkiert`
  Zugriff ist deaktiviert.

SSH

Aktiviert/deaktiviert den SSH-Zugriff.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Zugriff ist aktiviert für nebenstehenden IP-Adressbereich.
- `unmarkiert`
  Zugriff ist deaktiviert.

IEC61850-MMS

Aktiviert/deaktiviert den Zugriff auf den MMS-Server.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Zugriff ist aktiviert für nebenstehenden IP-Adressbereich.
- `unmarkiert`
  Zugriff ist deaktiviert.

Modbus TCP

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

Mögliche Werte:

- `markiert` (Voreinstellung)
  Zugriff ist aktiviert für nebenstehenden IP-Adressbereich.
- `unmarkiert`
  Zugriff ist deaktiviert.

EtherNet/IP

Aktiviert/deaktiviert den Zugriff auf den *EtherNet/IP*-Server.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Zugriff ist aktiviert für nebenstehenden IP-Adressbereich.
- `unmarkiert`
  Zugriff ist deaktiviert.

Aktiv

Aktiviert/deaktiviert den Tabelleneintrag.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Tabelleneintrag ist aktiviert. Das Gerät beschränkt den Zugriff auf das Management des Geräts auf den nebenstehenden IP-Adressbereich und die ausgewählten IP-basierten Anwendungen.
- `unmarkiert`
  Tabelleneintrag ist deaktiviert.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

3.4.3 Web

[Gerätesicherheit > Management-Zugriff > Web]

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

Konfiguration

Web-Interface Session-Timeout [min]

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

Mögliche Werte:

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

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

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

3.4.4 Command Line Interface

[Gerätesicherheit > Management-Zugriff > CLI]

In diesem Dialog legen Sie Einstellungen für das Command Line Interface fest. Detaillierte Informationen zum Command Line Interface finden Sie im Referenzhandbuch „Command Line Interface“.

Der Dialog enthält die folgenden Registerkarten:
- [Global]
- [Login-Banner]

[Global]

Diese Registerkarte ermöglicht Ihnen, den Prompt im Command Line Interface zu ändern und das automatische Beenden bei Inaktivität der Sitzung über die serielle Schnittstelle festzulegen.

Das Gerät bietet Ihnen folgende seriellen Schnittstellen:
- USB-C-Interface

Konfiguration

Login-Prompt

Legt die Zeichenfolge fest, die das Gerät im Command Line Interface am Beginn jeder Kommandozeile anzeigt.

Mögliche Werte:
- Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen (`0x20..0x7E`) inklusive Leerzeichen
  Wildcards
  - `%d` Datum
  - `%i` IP-Adresse
  - `%m` MAC-Adresse
  - `%p` Produktname
  - `%t` Uhrzeit

  Voreinstellung: `(MCSESM-E)`

Änderungen an dieser Einstellung sind in aktiven Sitzungen im Command Line Interface sofort wirksam.

Timeout serielle Schnittstelle [min]

Legt die Zeit in Minuten fest, nach der das Gerät die Sitzung eines inaktiven Benutzers automatisch beendet, der mit dem Command Line Interface über die serielle Schnittstelle angemeldet ist.

Mögliche Werte:
- `0..160` (Voreinstellung: `5`)
  Der Wert `0` deaktiviert die Funktion, der Benutzer bleibt bei Inaktivität angemeldet.

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

Für den *Telnet*-Server und den *SSH*-Server legen Sie das Timeout fest im Dialog *Gerätesicherheit* > Management-Zugriff > *Server*.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Login-Banner]

In dieser Registerkarte ersetzen Sie den Startbildschirm im Command Line Interface durch einen individuellen Text.

In der Voreinstellung zeigt der Startbildschirm Informationen über das Gerät, zum Beispiel die Software-Version und Geräte-Einstellungen. Mit der Funktion in dieser Registerkarte deaktivieren Sie diese Informationen und ersetzen sie durch einen individuell festgelegten Text.

Um vor der Anmeldung einen individuellen Text im Command Line Interface und in der grafischen Benutzeroberfläche anzuzeigen, verwenden Sie den Dialog *Gerätesicherheit > Pre-Login-Banner*.

Funktion

Funktion

Schaltet die Funktion *Login-Banner* ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *Login-Banner* ist eingeschaltet.
  Das Gerät zeigt die im Feld *Banner-Text* festgelegte Textinformation den Benutzern, die sich mit dem Command Line Interface anmelden.
- `Aus` (Voreinstellung)
  Die Funktion *Login-Banner* ist ausgeschaltet.
  Der Startbildschirm zeigt Informationen über das Gerät. Die Textinformation im Feld *Banner-Text* bleibt erhalten.

Banner-Text

Banner-Text

Legt die Textinformation fest, die das Gerät zu Beginn jeder Sitzung im Command Line Interface anzeigt.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..1024 Zeichen
  (`0x20..0x7E`) inklusive Leerzeichen

- `<Tabulator>`
- `<Zeilenumbruch>`

Verbleibende Zeichen

Zeigt, wie viele Zeichen im Feld *Banner-Text* noch für die Textinformation zur Verfügung stehen.

Mögliche Werte:

- `1024..0`

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

3.4.5 SNMPv1/v2 Community

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

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

Anwendungen senden Anfragen per SNMPv1/v2 mit einem Community-Namen im SNMP-Datenpaket-Header. Abhängig vom Community-Namen erhält die Anwendung Leserechte oder Lese- und Schreibrechte auf dem Gerät.

Den Zugriff auf das Gerät per SNMPv1/v2 aktivieren Sie im Dialog *Gerätesicherheit > Management-Zugriff > Server*.

Tabelle

Community

Zeigt die Berechtigung für SNMPv1/v2-Anwendungen auf dem Gerät:

- `Write`
  Bei Anfragen mit dem nebenstehenden Community-Namen erhält die Anwendung Lese- und Schreibrechte auf dem Gerät.
- `Read`
  Bei Anfragen mit dem nebenstehenden Community-Namen erhält die Anwendung Leserechte auf dem Gerät.

Name

Legt den Community-Namen für die nebenstehende Berechtigung fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen
  `admin` (Voreinstellung für Lese- und Schreibrechte)
  `user` (Voreinstellung für Leserechte)

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

3.5 Pre-Login-Banner

[Gerätesicherheit > Pre-Login-Banner]

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

Die Benutzer sehen den Text im Login-Dialog der grafischen Benutzeroberfläche und im Command Line Interface. Benutzer, die sich mit SSH anmelden, sehen den Text – abhängig vom verwendeten Client – vor oder während der Anmeldung.

Um den Text ausschließlich im Command Line Interface anzuzeigen, verwenden Sie die Einstellungen im Dialog *Gerätesicherheit > Management-Zugriff > CLI*.

Funktion

Funktion

Schaltet die Funktion *Pre-Login-Banner* ein/aus.

Mit der Funktion *Pre-Login-Banner* zeigt das Gerät im Login-Dialog der grafischen Benutzeroberfläche und im Command Line Interface eine Begrüßung oder einen Hinweis.

Mögliche Werte:

- *An*
  Die Funktion *Pre-Login-Banner* ist eingeschaltet.
  Das Gerät zeigt im Login-Dialog den im Feld *Banner-Text* festgelegten Text.
- *Aus* (Voreinstellung)
  Die Funktion *Pre-Login-Banner* ist ausgeschaltet.
  Das Gerät zeigt im Login-Dialog keinen Text. Haben Sie im Feld *Banner-Text* einen Text eingegeben, bleibt dieser erhalten.

Banner-Text

Banner-Text

Legt den Hinweistext fest, den das Gerät im Login-Dialog der grafischen Benutzeroberfläche und im Command Line Interface anzeigt.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..512 Zeichen
  (`0x20..0x7E`) inklusive Leerzeichen
- `<Tabulator>`
- `<Zeilenumbruch>`

Verbleibende Zeichen

Zeigt, wie viele Zeichen im Feld *Banner-Text* noch zur Verfügung stehen.

Mögliche Werte:

- 512..0

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

4 Netzsicherheit

Das Menü enthält die folgenden Dialoge:

- Netzsicherheit Übersicht
- Port-Sicherheit
- 802.1X Port-Authentifizierung
- RADIUS
- DoS
- DHCP-Snooping
- IP Source Guard
- Dynamic ARP Inspection
- ACL

4.1 Netzsicherheit Übersicht

[Netzsicherheit > Übersicht]

Dieser Dialog zeigt die im Gerät verwendeten Netzsicherheits-Regeln.

Parameter

Port/VLAN

Legt fest, ob das Gerät VLAN- und/oder portbasierte Regeln anzeigt.

Mögliche Werte:

- `Alle` (Voreinstellung)
  Das Gerät zeigt die von Ihnen festgelegten VLAN- und portbasierten Regeln.
- `Port: <Port-Nummer>`
  Das Gerät zeigt portbasierte Regeln für einen bestimmten Port. Diese Auswahl ist verfügbar, wenn Sie für diesen Port eine oder mehrere Regeln festgelegt haben.
- `VLAN: <VLAN-ID>`
  Das Gerät zeigt VLAN-basierte Regeln für ein bestimmtes VLAN. Diese Auswahl ist verfügbar, wenn Sie für dieses VLAN eine oder mehrere Regeln festgelegt haben.

ACL

Zeigt die *ACL*-Regeln in der Übersicht.

Die *ACL*-Regeln bearbeiten Sie im Dialog *Netzsicherheit > ACL*.

Alle

Markiert die nebenstehenden Kontrollkästchen. Das Gerät zeigt die zugehörigen Regeln in der Übersicht.

Kein

Hebt die Markierung der nebenstehenden Kontrollkästchen auf. Das Gerät zeigt keine Regeln in der Übersicht.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

4.2 Port-Sicherheit

[Netzsicherheit > Port-Sicherheit]

Das Gerät ermöglicht Ihnen, ausschließlich Datenpakete von erwünschten Absendern auf einem Port zu vermitteln. Wenn diese Funktion eingeschaltet ist, prüft das Gerät die VLAN-ID und die MAC-Adresse oder die VLAN-ID und die IP-Adresse des Absenders, bevor es ein Datenpaket vermittelt. Die Datenpakete anderer Absender verwirft das Gerät und protokolliert dieses Ereignis.

Das Gerät bietet auch die Funktion, die IP-Adresse des Absenders zu überprüfen, bevor es ein Datenpaket vermittelt.

Anmerkung: Wenn im Rahmen *Modus* das Optionsfeld *IP* ausgewählt ist, arbeitet die Funktion *Port-Sicherheit* indirekt auf Layer 2. Wenn Sie eine erlaubte IP-Adresse festlegen, ermittelt das Gerät die MAC-Adresse, die gegenwärtig mit der IP-Adresse verknüpft ist. Das Gerät verwendet einen ARP-Request und speichert intern die verknüpfte MAC-Adresse. Voraussetzung für das Festlegen einer erlaubten IP-Adresse ist, dass das angeschlossene Gerät erreichbar ist und auf ARP-Requests antwortet.

Wenn ein angeschlossenes Gerät Datenpakete mit einer erlaubten IP-Adresse sendet, jedoch mit einer anderen MAC-Adresse als der verknüpften MAC-Adresse, dann verwirft das Gerät die zugehörigen Datenpakete. Wenn Sie das angeschlossene Gerät ersetzen und die gleiche IP-Adresse wie zuvor verwenden, dann legen Sie die IP-Adresse erneut als zulässig fest. Nach diesem Schritt verwendet das Gerät die neue verknüpfte MAC-Adresse.

Wenn die Funktion *Auto-Disable* aktiviert ist, schaltet das Gerät den Port aus. Diese Begrenzung erschwert MAC-Spoofing-Attacken. Die Funktion *Auto-Disable* schaltet den betreffenden Port automatisch wieder ein, sofern die Überschreitung der Parameter aufgehoben ist.

In diesem Dialog unterstützt Sie ein Fenster *Wizard*, die Ports mit einem oder mehreren erwünschten Absendern zu verknüpfen. Im Gerät heißen diese Adressen *Statische Einträge (x/y)*. Zum Ansehen der festgelegten statischen Adressen markieren Sie den betreffenden Port und klicken die Schaltfläche  .

Um die Einrichtung zu vereinfachen, ermöglicht Ihnen das Gerät, die erwünschten Absender automatisch zu erfassen. Das Gerät „lernt“ die Absender durch das Bewerten der empfangenen Datenpakete. Im Gerät heißen diese Adressen *Dynamische Einträge*. Wenn der kopierte Datenstrom die Bandbreite des Ziel-Ports überschreitet (*Dynamisches Limit*), verwirft das Gerät überschüssige Datenpakete auf dem Ziel-Port. Wenn Sie die Obergrenze an die Anzahl der zu erwartenden Absender anpassen, erschweren Sie damit MAC-Flooding-Attacken.

Anmerkung: Beim automatischen Erfassen der *Dynamische Einträge* verwirft das Gerät stets das 1. Datenpaket von unbekannten Absendern. Anhand dieses 1. Datenpakets prüft das Gerät, ob die Obergrenze erreicht ist. Bis zum Erreichen der Obergrenze erfasst das Gerät den Absender. Anschließend vermittelt das Gerät Datenpakete, die es auf dem betreffenden Port von diesem Absender empfängt.

Funktion

Funktion

Schaltet die Funktion *Port-Sicherheit* ein/aus.

Mögliche Werte:

- *An*
  Die Funktion *Port-Sicherheit* ist eingeschaltet.
  Das Gerät prüft die VLAN-ID und die Absender-MAC-Adresse, bevor es ein Datenpaket vermittelt.
  Das Gerät vermittelt ein empfangenes Datenpaket ausschließlich dann, wenn die VLAN-ID und die Absender-MAC-Adresse des Datenpakets auf dem betreffenden Port erlaubt sind. Damit diese Einstellung wirksam wird, aktivieren Sie zusätzlich das Prüfen der Absenderadresse auf den betreffenden Ports.
- *Aus* (Voreinstellung)
  Die Funktion *Port-Sicherheit* ist ausgeschaltet.
  Das Gerät vermittelt jedes empfangene Datenpaket, ohne die Absenderadresse zu prüfen.

Anmerkung: Wenn im Rahmen *Modus* das Optionsfeld *MAC* ausgewählt ist, prüft das Gerät die Absender-MAC-Adresse gegen die erlaubten Absender-MAC-Adressen. Wenn das Optionsfeld *IP* ausgewählt ist, prüft das Gerät die Absender-MAC-Adresse gegen die MAC-Adressen, die mit den erlaubten Absender-IP-Adressen verknüpft sind.

Konfiguration

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für *Port-Sicherheit*.

Mögliche Werte:

- `markiert`
  Die Funktion *Auto-Disable* für *Port-Sicherheit* ist aktiv.
  Markieren Sie zusätzlich das Kontrollkästchen in Spalte *Auto-Disable* für die gewünschten Ports.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Auto-Disable* für *Port-Sicherheit* ist inaktiv.

Modus

Modus

Legt fest, ob die Funktion *Port-Sicherheit* die erlaubten MAC-Adressen oder die erlaubten IP-Adressen verwendet, um ein empfangenes Paket zu prüfen.

Mögliche Werte:

- *MAC* (Voreinstellung)
  Die Funktion *Port-Sicherheit* verwendet die erlaubten Absender-MAC-Adressen.
  Das Gerät prüft VLAN-ID und Absender-MAC-Adresse gegen die erlaubten Absender-MAC-Adressen, bevor es ein Datenpaket vermittelt.
- *IP*
  Die Funktion *Port-Sicherheit* verwendet die erlaubten Absender-IP-Adressen.
  Das Gerät prüft VLAN-ID und Absender-MAC-Adresse gegenüber den MAC-Adressen, die mit den erlaubten Absender-IP-Adressen verknüpft sind, bevor es ein Datenpaket vermittelt.

Tabelle

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert auf dem Port das Prüfen der Absenderadresse.

Mögliche Werte:

- `markiert`
  Das Gerät prüft jedes auf dem Port empfangene Datenpaket und vermittelt es ausschließlich dann, wenn die Absenderadresse des Datenpakets erlaubt ist. Schalten Sie zusätzlich im Rahmen *Funktion* die Funktion *Port-Sicherheit* ein.
- `unmarkiert` (Voreinstellung)
  Das Gerät vermittelt jedes auf dem Port empfangene Datenpaket, ohne die Absenderadresse zu prüfen.

Anmerkung: Wenn Sie das Gerät als aktiven Teilnehmer innerhalb eines *MRP*-Rings oder *HIPER-Ring*s betreiben, empfehlen wir, die Markierung des Kontrollkästchens für die Ring-Ports aufzuheben.

Anmerkung: Wenn Sie das Gerät als aktiven Teilnehmer einer *Ring-/Netzkopplung* oder *RCP* betreiben, empfehlen wir, die Markierung des Kontrollkästchens für die jeweiligen Kopplungs-Ports aufzuheben.

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für die Parameter, deren Einhaltung die Funktion *Port-Sicherheit* auf dem Port überwacht.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Funktion *Auto-Disable* ist auf dem Port aktiv.
  Voraussetzung ist, dass im Rahmen *Konfiguration* das Kontrollkästchen *Auto-Disable* markiert ist.
  - Das Gerät schaltet den Port aus, wenn der Port unerwünschte Absender oder mehr Absender erfasst als in Spalte *Dynamisches Limit* festgelegt ist. Die „Link-Status“-LED des Ports blinkt 3× pro Periode.
  - Der Dialog *Diagnose > Ports > Auto-Disable* zeigt, welche Ports aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet sind.
  - Die Funktion *Auto-Disable* schaltet den Port automatisch wieder ein. Legen Sie dazu im Dialog *Diagnose > Ports > Auto-Disable* in Spalte *Reset-Timer [s]* eine Wartezeit für den betreffenden Port fest.
- `unmarkiert`
  Die Funktion *Auto-Disable* auf dem Port ist inaktiv.

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät ein Datenpaket von einem unerwünschten Absender auf dem Port verwirft.

Mögliche Werte:

- `markiert`
  Das Senden von SNMP-Traps ist aktiv.
  Das Gerät sendet einen SNMP-Trap, wenn es auf dem Port Datenpakete von einem unerwünschten Absender verwirft.
- `unmarkiert` (Voreinstellung)
  Das Senden von SNMP-Traps ist inaktiv.

Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* einschalten und mindestens ein Trap-Ziel festlegen.

Trap-Intervall [s]

Legt die Wartezeit in Sekunden fest, die das Gerät nach Senden eines SNMP-Traps einhält, bis es den nächsten SNMP-Trap sendet.

Mögliche Werte:

- `0..3600` (Voreinstellung: `0`)

Der Wert `0` deaktiviert die Wartezeit.

Dynamisches Limit

Legt die Obergrenze fest für die Anzahl automatisch erfasster Absender (*Dynamische Einträge*). Sobald die Obergrenze erreicht ist, beendet das Gerät das „Lernen“ auf diesem Port.

Passen Sie den Wert an die Anzahl der zu erwartenden Absender an.

Wenn der Port mehr Absender erfasst als hier festgelegt ist, schaltet die Funktion *Auto-Disable* den Port aus. Voraussetzung ist, dass in Spalte *Auto-Disable* das Kontrollkästchen markiert ist und im Rahmen *Konfiguration* das Kontrollkästchen *Auto-Disable* markiert ist.

Mögliche Werte:

- `0`
  Deaktiviert das automatische Erfassen der Absender auf diesem Port.
- `1..600` (Voreinstellung: `600`)

Statisches Limit

Legt die Obergrenze fest für die Anzahl der mit dem Port verknüpften Absender (*Statische Einträge (x/y)*). Das Fenster *Wizard*, Dialog *MAC-Adressen*, unterstützt Sie dabei, den Port mit einem oder mehreren erwünschten Absendern zu verknüpfen.

Mögliche Werte:

- `0..64` (Voreinstellung: `64`)

Der Wert `0` sorgt dafür, zu verhindern, dass Sie einen Absender mit dem Port verknüpfen.

Dynamische Einträge

Zeigt, wie viele Absender das Gerät automatisch ermittelt hat.

Siehe Fenster *Wizard*, Dialog *MAC-Adressen*, Feld *Dynamische Einträge*.

Wenn Sie im Rahmen *Modus* den Wert *IP* auswählen, dann zeigt Spalte *Dynamische Einträge* den Wert `0`.

Statische MAC Einträge

Zeigt, wie viele Absender mit dem Port verknüpft sind.

Siehe Fenster *Wizard*, Dialog *MAC-Adressen*, Feld *Statische Einträge (x/y)*.

Statische IP Einträge

Zeigt die Anzahl der IP-Adressen, die auf dem Port erlaubt sind.

Siehe Fenster *Wizard*, Dialog *IP-Adressen*, Feld *Statische Einträge (x/y)*.

Last violating VLAN ID/MAC

Zeigt VLAN-ID und MAC-Adresse eines unerwünschten Absenders, dessen Datenpakete das Gerät auf diesem Port zuletzt verworfen hat.

Gesendete Traps

Zeigt die Anzahl der auf diesem Port verworfenen Datenpakete, die das Gerät zum Senden eines SNMP-Traps veranlasst haben.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Port-Sicherheit (Wizard)]

Das Fenster *Wizard* unterstützt Sie dabei, die Ports mit einem oder mehreren erwünschten Absendern zu verknüpfen. Wenn Sie die Einstellungen festgelegt haben, klicken Sie die Schaltfläche *Fertig*.

Anmerkung: Das Gerät speichert die mit dem Port verknüpften Absender so lange, bis Sie das Prüfen der Absender auf dem betreffenden Port oder im Rahmen *Funktion*deaktivieren.

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

[Port-Sicherheit (Wizard) – Port auswählen]

Port

Legt den Port fest, dem Sie im nächsten Schritt die Absender zuweisen.

[Port-Sicherheit (Wizard) – MAC-Adressen]

VLAN-ID

Legt die VLAN-ID des erwünschten Absenders fest.

Mögliche Werte:

- `1..4042`

Um VLAN-ID und MAC-Adresse in das Feld *Statische Einträge (x/y)* zu übernehmen, klicken Sie die Schaltfläche *Hinzufügen*.

MAC-Adresse

Legt die MAC-Adresse des erwünschten Absenders fest.

Mögliche Werte:

- Gültige Unicast-MAC-Adresse
  Legen Sie den Wert mit Doppelpunkt-Trennzeichen fest, zum Beispiel `00:11:22:33:44:55`.

Um VLAN-ID und MAC-Adresse in das Feld *Statische Einträge (x/y)* zu übernehmen, klicken Sie die Schaltfläche *Hinzufügen*.

Hinzufügen

Übernimmt die in den Feldern *VLAN-ID* und *MAC-Adresse* festgelegten Werte in das Feld *Statische Einträge (x/y)*.

Statische Einträge (x/y)

Zeigt VLAN-ID und MAC-Adresse der mit dem Port verknüpften, erwünschten Absender.

Über dem Feld zeigt das Gerät die Anzahl der mit dem Port verknüpften Absender sowie die Obergrenze. Die Obergrenze für die Anzahl der Einträge legen Sie fest in der Tabelle, Feld *Statisches Limit*.

Anmerkung: Eine MAC-Adresse, die sie diesem Port zuweisen, können Sie keinem weiteren Port zuweisen.

Entfernen

Entfernt die im Feld *Statische Einträge (x/y)*markierten Einträge.

Verschiebt die im Feld *Dynamische Einträge* markierten Einträge in das Feld *Statische Einträge (x/y)*.

Verschiebt jeden Eintrag aus dem Feld *Dynamische Einträge*in das Feld *Statische Einträge (x/y)*.

Enthält das Feld *Dynamische Einträge* mehr Einträge als im Feld *Statische Einträge (x/y)* erlaubt sind, verschiebt das Gerät die vorderen Einträge so lange, bis die Obergrenze erreicht ist.

Dynamische Einträge

Zeigt in aufsteigender Reihenfolge VLAN-ID und MAC-Adresse der auf diesem Port automatisch erfassten Absender. Das Gerät vermittelt Datenpakete von diesen Absendern, wenn es die Datenpakete auf diesem Port empfängt.

Voraussetzungen dafür, dass das Gerät MAC-Adressen anzeigt, sind:

- Die Funktion *Port-Sicherheit* ist eingeschaltet. Siehe Rahmen *Funktion*.
- Das Gerät prüft jedes Datenpaket, das es auf dem Port empfängt. Das Kontrollkästchen in Spalte *Aktiv* ist markiert.

Die Obergrenze für die Anzahl der Einträge legen Sie fest in der Tabelle, Feld *Dynamisches Limit*.

Die Schaltflächen und bieten Ihnen die Möglichkeit, Einträge aus diesem Feld in das Feld *Statische Einträge (x/y)* zu übernehmen. Damit verknüpfen Sie die betreffenden Absender mit dem Port.

[Port-Sicherheit (Wizard) – IP-Adressen]

VLAN-ID

Legt die VLAN-ID des erwünschten Absenders fest.

Mögliche Werte:

- `1..4042`

Anmerkung: Weisen Sie die VLAN-ID des Management-VLANs zu.

Um *VLAN-ID* und *IP-Adresse* in das Feld *Statische Einträge (x/y)* zu übernehmen, klicken Sie die Schaltfläche*Hinzufügen*.

IP-Adresse

Legt die IP-Adresse der erwünschten Quelle fest.

Mögliche Werte:

- Gültige IPv4-Adresse

Um *VLAN-ID* und *IP-Adresse* in das Feld *Statische Einträge (x/y)* zu übernehmen, klicken Sie die Schaltfläche*Hinzufügen*.

Hinzufügen

Übernimmt die in den Feldern *VLAN-ID* und *IP-Adresse* festgelegten Werte in das Feld *Statische Einträge (x/y)*.

Statische Einträge (x/y)

Zeigt VLAN-ID und IP-Adresse der mit dem Port verknüpften, erwünschten Absender.

Über dem Feld zeigt das Gerät die Anzahl der mit dem Port verknüpften Absender sowie die Obergrenze. Sie können maximal `10` IP-Adressen festlegen.

Entfernen

Entfernt die im Feld *Statische Einträge (x/y)*markierten Einträge.

4.3 802.1X Port-Authentifizierung

[Netzsicherheit > 802.1X Port-Authentifizierung]

Mit der portbasierten Zugriffskontrolle gemäß IEEE 802.1X kontrolliert das Gerät den Zugriff angeschlossener Endgeräte auf das Netz. Das Gerät (Authenticator) ermöglicht einem Endgerät (Supplicant) den Zugriff auf das Netz, wenn dieses sich mit gültigen Zugangsdaten anmeldet. Authenticator und Endgeräte kommunizieren über das Authentisierungsprotokoll EAPoL (Extensible Authentication Protocol over LANs).

Das Gerät unterstützt die folgenden Methoden, um Endgeräte zu authentifizieren:

- `radius`
  Ein RADIUS-Server im Netz authentifiziert die Endgeräte.
- `ias`
  Der im Gerät eingebaute Integrierte Authentifikationsserver (IAS) authentifiziert die Endgeräte. Im Vergleich zu RADIUS bietet der IAS lediglich grundlegende Funktionen.

Das Menü enthält die folgenden Dialoge:

- 802.1X Global
- 802.1X Port-Konfiguration
- 802.1X Port-Clients
- 802.1X EAPOL-Portstatistiken
- 802.1X Port-Authentifizierung-Historie
- 802.1X Integrierter Authentifikations-Server

4.3.1 802.1X Global

[Netzsicherheit > 802.1X Port-Authentifizierung > Global]

Dieser Dialog ermöglicht Ihnen, grundlegende Einstellungen für die portbasierte Zugriffskontrolle festzulegen.

Funktion

Funktion

Schaltet die Funktion *802.1X Port-Authentifizierung* ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *802.1X Port-Authentifizierung* ist eingeschaltet.
  Das Gerät prüft den Zugriff angeschlossener Endgeräte auf das Netz.
  Die portbasierte Zugriffskontrolle ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *802.1X Port-Authentifizierung* ist ausgeschaltet.
  Die portbasierte Zugriffskontrolle ist ausgeschaltet.

Konfiguration

VLAN zuweisen

Aktiviert/deaktiviert die Zuweisung des betreffenden Ports zu einem VLAN. Diese Funktion ermöglicht Ihnen, dem angeschlossenen Endgerät in diesem VLAN ausgewählte Dienste bereitzustellen.

Mögliche Werte:

- `markiert`
  Das Zuweisen ist aktiv.
  Wenn sich das Endgerät erfolgreich authentifiziert, weist das Gerät dem betreffenden Port die vom RADIUS-Authentication-Server übermittelte VLAN-ID zu.
- `unmarkiert` (Voreinstellung)
  Die Zuweisen ist inaktiv.
  Der betreffende Port ist dem im Dialog *Netzsicherheit > 802.1X Port-Authentifizierung > Port-Konfiguration*, Spalte *Zugewiesene VLAN-ID* festgelegten VLAN zugewiesen.

VLAN dynamisch erzeugen

Aktiviert/deaktiviert das automatische Einrichten des vom RADIUS-Authentication-Server zugewiesenen VLANs, falls dieses nicht existiert.

Mögliche Werte:

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

Monitor-Mode

Aktiviert/deaktiviert den Monitor-Modus.

Mögliche Werte:

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

Formatoptionen MAC Authentication Bypass

Gruppen-Größe

Legt die Größe der MAC-Adress-Gruppen fest. Für die Authentifizierung unterteilt das Gerät die MAC-Adresse in Gruppen. Die Größe der Gruppen ist festgelegt in Halb-Bytes, die jeweils als ein Zeichen dargestellt werden.

Mögliche Werte:

- *1*
  Das Gerät unterteilt die MAC-Adresse in 12 Gruppen mit je einem Zeichen.
  Beispiel: `A:A:B:B:C:C:D:D:E:E:F:F`
- *2*
  Das Gerät unterteilt die MAC-Adresse in 6 Gruppen mit je 2 Zeichen.
  Beispiel: `AA:BB:CC:DD:EE:FF`
- *4*
  Das Gerät unterteilt die MAC-Adresse in 3 Gruppen mit je 4 Zeichen.
  Beispiel: `AABB:CCDD:EEFF`
- *12* (Voreinstellung)
  Das Gerät formatiert die MAC-Adresse als eine Gruppe mit 12 Zeichen.
  Beispiel: `AABBCCDDEEFF`

Gruppen-Trennzeichen

Legt das Trennzeichen zwischen den Gruppen fest.

Mögliche Werte:

- *-*
  Bindestrich
- *:*
  Doppelpunkt
- *.*
  Punkt

Groß-/Kleinschreibung

Legt fest, ob das Gerät die Authentifizierungsdaten in Klein- oder Großbuchstaben formatiert.

Mögliche Werte:

- *lower-case*
- *upper-case*

Passwort

Legt für Clients, die den Authentifizierungs-Bypass verwenden, das optionale Passwort fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen
  Nach Eingabe zeigt das Feld ***** (Sternchen) anstelle des Passworts.
- `<leer>`
  Das Gerät verwendet den Benutzernamen des Clients zugleich als Passwort.

Information

Monitor-Mode-Clients

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

Voraussetzung ist, dass die Funktion *Monitor-Mode* im Gerät aktiviert ist. Siehe Rahmen *Konfiguration*.

Non-Monitor-Mode-Clients

Zeigt, wie vielen Endgeräten das Gerät nach erfolgreicher Anmeldung Zugriff auf das Netz gewährt hat.

Richtlinie 1

Zeigt die Methode, die das Gerät zum Authentifizieren der Endgeräte per IEEE 802.1X gegenwärtig anwendet.

Die anzuwendende Methode legen Sie im Dialog *Gerätesicherheit > Authentifizierungs-Liste* fest.

- ☐ Um die Endgeräte über einen RADIUS-Server zu authentifizieren, weisen Sie der Liste `radius` die Richtline `8021x` zu.
- ☐ Um die Endgeräte über den Integrierten Authentifikationsserver (IAS) zu authentifizieren, weisen Sie der Liste `ias` die Richtline `8021x` zu.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

4.3.2 802.1X Port-Konfiguration

[Netzsicherheit > 802.1X Port-Authentifizierung > Port-Konfiguration]

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

Sind mehrere Endgeräte an einem Port angeschlossen, ermöglicht Ihnen das Gerät, diese individuell zu authentifizieren (Multi-Client-Authentifizierung). In diesem Fall ermöglicht das Gerät angemeldeten Endgeräten den Zugriff auf das Netz. Dagegen sperrt das Gerät den Zugriff für unauthentifizierte Endgeräte oder für Endgeräte, deren Authentifizierung abgelaufen ist.

Tabelle

Port

Zeigt die Nummer des Ports.

Port-Initialisierung

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

Mögliche Werte:

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

Port-Reauthentifizierung

Aktiviert/deaktiviert die einmalige Authentifizierungsanforderung.

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

Das Gerät ermöglicht Ihnen außerdem, das Endgerät periodisch aufzufordern, sich erneut anzumelden. Siehe Spalte *Periodische Reauthentifizierung*.

Mögliche Werte:

- `markiert`
  Die einmalige Authentifizierungsanforderung ist aktiv.
  Das Gerät fordert das Endgerät auf, sich erneut anzumelden. Anschließend ändert das Gerät den Wert wieder auf `unmarkiert`.
- `unmarkiert` (Voreinstellung)
  Die einmalige Authentifizierungsanforderung ist inaktiv.
  Das Gerät behält die Anmeldung des Endgeräts bei.

Authentifizierungs-Vorgang

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

Mögliche Werte:

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

Authentifizierungs-Zustand Backend

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

Mögliche Werte:

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

Authentifizierungs-Zustand

Zeigt den gegenwärtigen Zustand der Authentifizierung auf dem Port (`Controlled Port Status`).

Mögliche Werte:

- *authorized*
  Das Endgerät ist erfolgreich angemeldet.
- *unauthorized*
  Das Endgerät ist nicht angemeldet.

Benutzer (max.)

Legt die Obergrenze fest für die Anzahl von Endgeräten, die das Gerät auf diesem Port gleichzeitig authentifiziert. Diese Obergrenze gilt ausschließlich dann, wenn für den Port in Spalte *Port-Kontrolle* der Wert `multiClient` festgelegt ist.

Mögliche Werte:

- `1..16` (Voreinstellung: `16`)

Port-Kontrolle

Legt fest, wie das Gerät den Zugriff auf das Netz gewährt (`Port control mode`).

Mögliche Werte:

- *forceUnauthorized*
  Das Gerät sperrt den Zugriff auf das Netz. Verwenden Sie diese Einstellung, wenn an den Port ein Endgerät angeschlossen ist, das keinen Zugriff auf das Netz erhält.
- *auto*
  Das Gerät gewährt den Zugriff auf das Netz, wenn sich das Endgerät erfolgreich angemeldet hat. Verwenden Sie diese Einstellung, wenn an den Port ein Endgerät angeschlossen ist, das sich beim Authenticator anmeldet.

Anmerkung: Wenn über denselben Port weitere Endgeräte angeschlossen sind, erhalten diese ohne zusätzliche Authentifizierung Zugriff auf das Netz.

- *forceAuthorized* (Voreinstellung)
  Wenn Endgeräte kein IEEE 802.1X unterstützen, gewährt das Gerät Zugriff auf das Netz. Verwenden Sie diese Einstellung, wenn an den Port ein Endgerät angeschlossen ist, das ohne Anmeldung Zugriff auf das Netz erhält.
- *multiClient*
  Das Gerät gewährt den Zugriff auf das Netz, wenn sich das Endgerät erfolgreich anmeldet. Wenn das Endgerät keine EAPOL-Datenpakete sendet, gewährt oder sperrt das Gerät den Zugriff auf das Netz individuell anhand der MAC-Adresse des Endgeräts. Siehe Spalte *MAC-Authorized-Bypass*.
  Verwenden Sie diese Einstellung, wenn mehrere Endgeräte an den Port angeschlossen sind oder wenn die Funktion *MAC-Authorized-Bypass* erforderlich ist.

Ruheperiode [s]

Legt die Zeitspanne in Sekunden fest, in welcher der Authenticator nach einem erfolglosen Anmeldeversuch keine erneute Anmeldung des Endgeräts akzeptiert (`Ruheperiode [s]`).

Mögliche Werte:

- `0..65535` (Voreinstellung: `60`)

Sendeperiode [s]

Legt die Zeit in Sekunden fest, nach welcher der Authenticator das Endgerät auffordert, sich erneut anzumelden. Nach dieser Wartezeit sendet das Gerät ein EAP-Request/Identity-Datenpaket an das Endgerät.

Mögliche Werte:

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

Supplikant-Timeout [s]

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

Mögliche Werte:

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

Server-Timeout [s]

Legt die Zeitspanne in Sekunden fest, innerhalb welcher der Authenticator auf die Antwort des Authentication-Servers (RADIUS oder IAS) wartet.

Mögliche Werte:

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

Requests (max.)

Legt fest, wie viele Male der Authenticator das Endgerät auffordert, sich anzumelden, bis die in Spalte *Supplikant-Timeout [s]* festgelegte Zeit erreicht ist. Das Gerät sendet sooft wie hier festgelegt ein EAP-Request/Identity-Datenpaket an das Endgerät.

Mögliche Werte:

- `0..10` (Voreinstellung: `2`)

Zugewiesene VLAN-ID

Zeigt die ID des VLANs, die der Authenticator dem Port zugewiesen hat. Dieser Wert gilt ausschließlich dann, wenn für den Port in Spalte *Port-Kontrolle* der Wert `auto` festgelegt ist.

Mögliche Werte:

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

Die VLAN-ID, die der Authenticator den Ports zugewiesen hat, finden Sie im Dialog *Netzsicherheit* > 802.1X Port-Authentifizierung > *Port-Clients*.

Wenn für den Port in Spalte *Port-Kontrolle* der Wert `multiClient`, festgelegt ist, weist das Gerät das VLAN-Tag anhand der MAC-Adresse des Endgeräts zu, wenn es Datenpakete ohne VLAN-Tag empfängt.

Zuweisungsgrund

Zeigt den Grund für die Zuweisung der VLAN-ID. Dieser Wert gilt ausschließlich dann, wenn für den Port in Spalte *Port-Kontrolle* der Wert `auto` festgelegt ist.

Mögliche Werte:

- `notAssigned` (Voreinstellung)
- `radius`
- `guestVlan`
- `unauthenticatedVlan`

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

Reauthentifizierungs-Periode [s]

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

Mögliche Werte:

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

Periodische Reauthentifizierung

Aktiviert/deaktiviert periodische Authentifizierungsanforderungen.

Mögliche Werte:

- `markiert`
  Periodische Authentifizierungsanforderungen sind aktiv.
  Das Gerät fordert das Endgerät periodisch auf, sich erneut anzumelden. Die Zeitspanne legen Sie fest in Spalte *Reauthentifizierungs-Periode [s]*.
  Diese Einstellung ist außer Kraft gesetzt, wenn der Authenticator dem Endgerät die ID eines Voice-, Unauthenticated- oder Gast-VLANs zugewiesen hat.
- `unmarkiert` (Voreinstellung)
  Periodische Authentifizierungsanforderungen sind inaktiv.
  Das Gerät behält die Anmeldung des Endgeräts bei.

Gast VLAN-ID

Legt die ID des VLANs fest, die der Authenticator dem Port zuweist, wenn sich das Endgerät während der in Spalte *Gast-VLAN-Intervall*festgelegten Zeit nicht anmeldet. Dieser Wert gilt ausschließlich dann, wenn für den Port in Spalte *Port-Kontrolle* der Wert `auto` oder `multiClient` festgelegt ist.

Diese Funktion ermöglicht Ihnen, Endgeräten ohne Unterstützung für IEEE 802.1X den Zugriff auf ausgewählte Dienste im Netz zu gewähren.

Mögliche Werte:

- `0` (Voreinstellung)
  Der Authenticator weist dem Port kein Gast-VLAN zu.
  Wenn Sie in Spalte *MAC-Authorized-Bypass* die MAC-basierte Authentifizierung einschalten, legt das Gerät automatisch den Wert `0` fest.
- `1..4042`

Anmerkung: Die Funktion *MAC-Authorized-Bypass* und die Funktion *Gast VLAN-ID* können nicht gleichzeitig verwendet werden.

Gast-VLAN-Intervall

Legt die Zeitspanne in Sekunden fest, in welcher der Authenticator nach Anschließen des Endgeräts auf EAPOL-Datenpakete wartet. Läuft diese Zeit ab, gewährt der Authenticator dem Endgerät Zugriff auf das Netz und weist den Port dem in Spalte *Gast VLAN-ID* festgelegten Gast-VLAN zu.

Mögliche Werte:

- `1..300` (Voreinstellung: `90`)

Unauthenticated-VLAN-ID

Legt die ID des VLANs fest, die der Authenticator dem Port zuweist, wenn sich das Endgerät ohne Erfolg anmeldet. Dieser Wert gilt ausschließlich dann, wenn für den Port in Spalte *Port-Kontrolle* der Wert *auto* festgelegt ist.

Diese Funktion ermöglicht Ihnen, Endgeräten ohne gültige Zugangsdaten den Zugriff auf ausgewählte Dienste im Netz zu gewähren.

Mögliche Werte:

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

Der Wert `0` bewirkt, dass der Authenticator dem Port kein Unauthenticated-VLAN zuweist.

Anmerkung: Weisen Sie dem Port ausschließlich ein im Gerät statisch eingerichtetes VLAN zu.

MAC-Authorized-Bypass

Aktiviert/deaktiviert die MAC-basierte Authentifizierung.

Diese Funktion ermöglicht Ihnen, Endgeräte ohne Unterstützung für IEEE 802.1X anhand ihrer MAC-Adresse zu authentifizieren.

Mögliche Werte:

- `markiert`
  Die MAC-basierte Authentifizierung ist aktiv.
  Das Gerät sendet die MAC-Adresse des Endgeräts an den RADIUS-Authentication-Server. Das Gerät weist den Port dem jeweiligen VLAN zu, als hätte die Authentifizierung direkt über IEEE 802.1X stattgefunden.
- `unmarkiert` (Voreinstellung)
  Die MAC-basierte Authentifizierung ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

4.3.3 802.1X Port-Clients

[Netzsicherheit > 802.1X Port-Authentifizierung > Port-Clients]

Dieser Dialog zeigt Informationen über die angeschlossenen Endgeräte.

Tabelle

Port

Zeigt die Nummer des Ports.

Benutzername

Zeigt den Benutzernamen, mit dem sich das Endgerät angemeldet hat.

MAC-Adresse

Zeigt die MAC-Adresse des Endgeräts.

Zugewiesene VLAN-ID

Zeigt die VLAN-ID, die der Authenticator dem Port nach erfolgreicher Authentifizierung des Endgeräts zugewiesen hat.

Wenn für den Port im Dialog *Netzsicherheit > 802.1X Port-Authentifizierung > Port-Konfiguration*, Spalte *Port-Kontrolle* der Wert `multiClient` festgelegt ist, dann weist das Gerät das VLAN-Tag anhand der MAC-Adresse des Endgeräts zu, wenn es Datenpakete ohne VLAN-Tag empfängt.

Zuweisungsgrund

Zeigt den Grund für die Zuweisung des VLANs.

Mögliche Werte:

- `default`
- `radius`
- `unauthenticatedVlan`
- `guestVlan`
- `monitorVlan`
- `invalid`

Das Feld zeigt ausschließlich dann einen gültigen Wert, solange der Client authentifiziert ist.

Session-Timeout

Zeigt die verbleibende Zeit in Sekunden, bis die Anmeldung des Endgeräts abläuft. Dieser Wert gilt ausschließlich dann, wenn für den Port im Dialog *Netzsicherheit > 802.1X Port-Authentifizierung > Port-Konfiguration*, Spalte *Port-Kontrolle* der Wert `auto` oder `multiClient` festgelegt ist.

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

Aktion beim Beenden

Zeigt die Aktion, die das Gerät bei Ablauf der Anmeldung ausführt.

Mögliche Werte:

- *default*
- *reauthenticate*

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

4.3.4 802.1X EAPOL-Portstatistiken

[Netzsicherheit > 802.1X Port-Authentifizierung > Statistiken]

Dieser Dialog zeigt, welche EAPOL-Datenpakete das Gerät für die Authentifizierung der Endgeräte gesendet und empfangen hat.

Tabelle

Port

Zeigt die Nummer des Ports.

Empfangene Pakete

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

Gesendete Pakete

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

Start-Pakete

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

Abmelde-Pakete

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

Response/ID packets

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

Antwort-Pakete

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

Request/ID-Pakete

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

Request-Pakete

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

Ungültige Pakete

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

Empfangene Error-Pakete

Zeigt, wie viele EAPOL-Datenpakete mit ungültigem Packet-Body-Length-Feld das Gerät auf dem Port empfangen hat.

Paket-Version

Zeigt die Protokoll-Versionsnummer des EAPOL-Datenpakets, welches das Gerät auf dem Port zuletzt empfangen hat.

Quelle des zuletzt empfangenen Pakets

Zeigt die Absender-MAC-Adresse des EAPOL-Datenpakets, welches das Gerät auf dem Port zuletzt empfangen hat.

Der Wert `00:00:00:00:00:00` bedeutet, dass der Port noch kein EAPOL-Datenpaket empfangen hat.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

4.3.5 802.1X Port-Authentifizierung-Historie

[Netzsicherheit > 802.1X Port-Authentifizierung > Port-Authentifizierung-Historie]

Das Gerät protokolliert den Authentifizierungsvorgang der Endgeräte, die an seinen Ports angeschlossen sind. Dieser Dialog zeigt die bei der Authentifizierung erfassten Informationen.

Tabelle

Port

Zeigt die Nummer des Ports.

Authentifizierungs-Zeitpunkt

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

Eintrag vorhanden seit

Zeigt, seit wann dieser Eintrag in der Tabelle eingetragen ist.

MAC-Adresse

Zeigt die MAC-Adresse des Endgeräts.

VLAN-ID

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

Authentifizierungs-Status

Zeigt den Zustand der Authentifizierung auf dem Port.

Mögliche Werte:

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

Zugriffs-Status

Zeigt, ob das Gerät dem Endgerät Zugriff auf das Netz gewährt.

Mögliche Werte:

- *granted*
  Das Gerät gewährt dem Endgerät den Zugriff auf das Netz.
- *denied*
  Das Gerät sperrt dem Endgerät den Zugriff auf das Netz.

Zugewiesene VLAN-ID

Zeigt die ID des VLANs, die der Authenticator dem Port zugewiesen hat.

Zuweisungs-Typ

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

Mögliche Werte:

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

Zuweisungsgrund

Zeigt den Grund für die Zuweisung der VLAN-ID und des VLAN-Typs.

802.1X Port-Authentifizierung-Historie

Port

Vereinfacht die Anzeige und zeigt in der Tabelle ausschließlich die Einträge, die den hier ausgewählten Port betreffen. Dies erleichtert Ihnen, die Tabelle zu erfassen und nach Ihren Wünschen zu sortieren.

Mögliche Werte:

- `all`
  Die Tabelle zeigt die Einträge für jeden Port.
- `<Port-Nummer>`
  Die Tabelle zeigt die Einträge, die ausschließlich den hier ausgewählten Port betreffen.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

4.3.6 802.1X Integrierter Authentifikations-Server

Der Integrierte Authentifikationsserver (IAS) ermöglicht Ihnen, Endgeräte per IEEE 802.1X zu authentifizieren. Im Vergleich zu RADIUS hat der IAS einen sehr eingeschränkten Funktionsumfang. Die Authentifizierung erfolgt ausschließlich anhand von Benutzername und Passwort.

In diesem Dialog verwalten Sie die Zugangsdaten der Endgeräte. Das Gerät ermöglicht Ihnen, bis zu 100 Zugangsdaten einzurichten.

Um die Endgeräte über den Integrierten Authentifikationsserver zu authentifizieren, weisen Sie im Dialog *Gerätesicherheit > Authentifizierungs-Liste* der Liste 8021x die Richtlinie `ias` zu.

Tabelle

Benutzername

Zeigt den Benutzernamen des Endgeräts.

Um einen neuen Benutzer anzulegen, klicken Sie die Schaltfläche .

Passwort

Legt das Passwort fest, mit dem sich der Benutzer authentifiziert.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

Das Gerät unterscheidet zwischen Groß- und Kleinschreibung.

Aktiv

Aktiviert/deaktiviert die Zugangsdaten.

Mögliche Werte:

- `markiert`
  Die Zugangsdaten sind aktiv. Ein Endgerät hat die Möglichkeit, sich mit diesen Zugangsdaten per IEEE 802.1X anzumelden.
- `unmarkiert` (Voreinstellung)
  Die Zugangsdaten sind inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

4.4 RADIUS

[Netzsicherheit > RADIUS]

Das Gerät ist ab Werk so eingestellt, dass es Benutzer anhand der lokalen Benutzerverwaltung authentifiziert. Mit zunehmender Größe eines Netzes jedoch steigt der Aufwand, die Zugangsdaten der Benutzer über Geräte hinweg konsistent zu halten.

RADIUS (Remote Authentication Dial-In User Service) ermöglicht Ihnen, die Benutzer an zentraler Stelle im Netz zu authentifizieren und zu autorisieren. Ein RADIUS-Server erledigt dabei folgende Aufgaben:

- Authentifizierung
  Der Authentication-Server authentifiziert die Benutzer, wenn der RADIUS-Client im Zugangspunkt die Zugangsdaten der Benutzer an ihn weiterleitet.
- Autorisierung
  Der Authentication-Server autorisiert angemeldete Benutzer für ausgewählte Dienste, indem er dem RADIUS-Client im Zugangspunkt diverse Parameter für das betreffende Endgerät zuweist.
- Abrechnung
  Der Accounting-Server erfasst die während der Port-Authentifizierung gemäß IEEE 802.1X angefallenen Verkehrsdaten. Damit lässt sich nachträglich feststellen, welche Dienste die Benutzer in welchem Umfang genutzt haben.

Das Gerät arbeitet in der Rolle des RADIUS-Clients, wenn Sie im Dialog `radius` einer Anwendung die Richtlinie *Gerätesicherheit > Authentifizierungs-Liste* zuweisen. Das Gerät leitet die Zugangsdaten der Benutzer weiter an den primären Authentication-Server. Der Authentication-Server entscheidet, ob die Zugangsdaten gültig sind und übermittelt dem Gerät die Berechtigungen des Benutzers.

Den in der Antwort eines RADIUS-Servers übertragenen Service-Type weist das Gerät wie folgt einer auf dem Gerät vorhandenen Benutzer-Rolle zu:

- `Administrative-User`: *administrator*
- `Login-User`: *operator*
- `NAS-Prompt-User`: *guest*

Das Gerät ermöglicht Ihnen außerdem, Endgeräte per IEEE 802.1X über einen Authentication-Server zu authentifizieren. Hierzu weisen Sie im Dialog `radius` der Liste `8021x` die Richtlinie *Gerätesicherheit > Authentifizierungs-Liste* zu.

Das Menü enthält die folgenden Dialoge:

- RADIUS Global
- RADIUS Authentication-Server
- RADIUS Accounting-Server
- RADIUS Authentication Statistiken
- RADIUS Accounting-Statistiken

4.4.1 RADIUS Global

[Netzsicherheit > RADIUS > Global]

Dieser Dialog ermöglicht Ihnen, grundlegende Einstellungen für RADIUS festzulegen.

RADIUS-Konfiguration

Anfragen (max.)

Legt fest, wie viele Male das Gerät eine unbeantwortete Anfrage an den Authentication-Server wiederholt, bevor es die Anfrage an einen anderen Authentication-Server sendet.

Mögliche Werte:

- `1..15` (Voreinstellung: `4`)

Timeout [s]

Legt fest, wie viele Sekunden das Gerät nach einer Anfrage an den Authentication-Server auf Antwort wartet, bevor es die Anfrage erneut sendet.

Mögliche Werte:

- `1..30` (Voreinstellung: `5`)

Accounting

Aktiviert/deaktiviert das Accounting.

Mögliche Werte:

- `markiert`
  Accounting ist aktiv.
  Das Gerät sendet die Verkehrsdaten an einen im Dialog *Netzsicherheit > RADIUS > Accounting-Server* festgelegten Accounting-Server.
- `unmarkiert` (Voreinstellung)
  Accounting ist inaktiv.

NAS-IP-Adresse (Attribut 4)

Legt die IP-Adresse fest, die das Gerät als Attribut 4 an den Authentication-Server überträgt. Legen Sie die IP-Adresse des Geräts oder eine andere, frei wählbare Adresse fest.

Anmerkung: Das Gerät sendet das Attribut 4 ausschließlich dann mit, wenn das Paket durch die *802.1X*-Authentifizierungsanfrage eines Endgeräts (Supplicant) ausgelöst wurde.

Mögliche Werte:

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

In vielen Fällen befindet sich zwischen Gerät und Authentication-Server eine Firewall. Bei der Network Address Translation (NAT) in der Firewall ändert sich die ursprüngliche IP-Adresse, der Authentication-Server empfängt die übersetzte IP-Adresse des Geräts.

Die IP-Adresse in diesem Feld überträgt das Gerät unverändert über Network Address Translation (NAT) hinweg.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Zurücksetzen

Löscht die Statistik im Dialog *Netzsicherheit > RADIUS > Authentication-Statistiken* und die Statistik im Dialog *Netzsicherheit > RADIUS > Accounting-Statistiken*.

4.4.2 RADIUS Authentication-Server

[Netzsicherheit > RADIUS > Authentication-Server]

Dieser Dialog ermöglicht Ihnen, bis zu 8 Authentication-Server festzulegen. Ein Authentication-Server authentifiziert und autorisiert die Benutzer, wenn das Gerät die Zugangsdaten an ihn weiterleitet.

Das Gerät sendet die Zugangsdaten an den als primär gekennzeichneten Authentication-Server. Bleibt dessen Antwort aus, kontaktiert das Gerät den obersten in der Tabelle festgelegten Authentication-Server. Bleibt auch dessen Antwort aus, kontaktiert das Gerät den jeweils nächsten Server in der Tabelle.

Tabelle

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Name

Zeigt den Namen des Servers.

Um den Wert zu ändern, klicken Sie in das betreffende Feld.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen
  (Voreinstellung: `Default-RADIUS-Server`)

Adresse

Legt die IP-Adresse des Servers fest.

Mögliche Werte:

- Gültige IPv4-Adresse

Ziel-UDP-Port

Legt die Nummer des UDP-Ports fest, auf dem der Server Anfragen entgegennimmt.

Mögliche Werte:

- `0..65535` (Voreinstellung: `1812`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Secret

Zeigt ****** (Sternchen), wenn ein Passwort festgelegt ist, mit dem sich das Gerät beim Server anmeldet. Um das Passwort zu ändern, klicken Sie in das betreffende Feld.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..64 Zeichen

Das Passwort erfahren Sie vom Administrator des Authentication-Servers.

Primärer Server

Kennzeichnet den Authentication-Server als primär oder sekundär.

Mögliche Werte:

- `markiert`
  Der Server ist als primärer Authentication-Server gekennzeichnet. Das Gerät sendet die Zugangsdaten zum Authentifizieren der Benutzer an diesen Authentication-Server.
  Wenn Sie mehrere Server markieren, kennzeichnet das Gerät den zuletzt markierten Server als primären Authentication-Server.
- `unmarkiert` (Voreinstellung)
  Der Server ist als sekundärer Authentication-Server gekennzeichnet. Das Gerät sendet die Zugangsdaten an den sekundären Authentication-Server, wenn es vom primären Authentication-Server keine Antwort erhält.

Aktiv

Aktiviert/deaktiviert die Verbindung zum Server.

Das Gerät verwendet den Server, wenn Sie im Dialog *Gerätesicherheit > Authentifizierungs-Liste* den Wert `radius` in einer der Spalten *Richtlinie 1* bis *Richtlinie 5* festlegen.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Verbindung ist aktiv. Das Gerät sendet die Zugangsdaten zum Authentifizieren der Benutzer an diesen Server, wenn die obengenannten Voraussetzungen erfüllt sind.
- `unmarkiert`
  Die Verbindung ist inaktiv. Das Gerät sendet keine Zugangsdaten an diesen Server.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

- Im Feld *Index* legen Sie die Index-Nummer fest.
- Im Feld *Adresse*legen Sie die IP-Adresse des Servers fest.

4.4.3 RADIUS Accounting-Server

[Netzsicherheit > RADIUS > Accounting-Server]

Dieser Dialog ermöglicht Ihnen, bis zu 8 Accounting-Server festzulegen. Ein Accounting-Server erfasst die während der Port-Authentifizierung gemäß IEEE 802.1X angefallenen Verkehrsdaten. Voraussetzung ist, dass im Menü *Netzsicherheit > RADIUS > Global* die Funktion *Accounting* eingeschaltet ist.

Das Gerät sendet die Verkehrsdaten an den ersten erreichbaren Accounting-Server. Wenn der Accounting-Server nicht antwortet, kontaktiert das Gerät den jeweils nächsten Server aus der Tabelle.

Tabelle

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Mögliche Werte:

- `1..8`

Name

Zeigt den Namen des Servers.

Um den Wert zu ändern, klicken Sie in das betreffende Feld.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen
  (Voreinstellung: `Default-RADIUS-Server`)

Adresse

Legt die IP-Adresse des Servers fest.

Mögliche Werte:

- Gültige IPv4-Adresse

Ziel-UDP-Port

Legt die Nummer des UDP-Ports fest, auf dem der Server Anfragen entgegennimmt.

Mögliche Werte:

- `0..65535` (Voreinstellung: `1813`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Secret

Zeigt ****** (Sternchen), wenn ein Passwort festgelegt ist, mit dem sich das Gerät beim Server anmeldet. Um das Passwort zu ändern, klicken Sie in das betreffende Feld.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..16 Zeichen

Das Passwort erfahren Sie vom Administrator des Authentication-Servers.

Aktiv

Aktiviert/deaktiviert die Verbindung zum Server.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Verbindung ist aktiv. Das Gerät sendet Verkehrsdaten an diesen Server, wenn die obengenannten Voraussetzungen erfüllt sind.
- `unmarkiert`
  Die Verbindung ist inaktiv. Das Gerät sendet keine Verkehrsdaten an diesen Server.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

- Im Feld *Index* legen Sie die Index-Nummer fest.
- Im Feld *Adresse*legen Sie die IP-Adresse des Servers fest.

4.4.4 RADIUS Authentication Statistiken

[Netzsicherheit > RADIUS > Authentication-Statistiken]

Dieser Dialog zeigt Informationen über die Kommunikation zwischen dem Gerät und dem Authentication-Server. Die Tabelle zeigt die Informationen für jeden Server in einer separaten Zeile.

Um die Statistik zu löschen, klicken Sie im Dialog *Netzsicherheit > RADIUS > Global* die Schaltfläche ☰ und dann den Eintrag *Zurücksetzen*.

Tabelle

Name

Zeigt den Namen des Servers.

Adresse

Zeigt die IP-Adresse des Servers.

Round-Trip-Time

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

Zugriffsanforderungen

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

Neu gesendete Access-Request-Pakete

Zeigt, wie viele Access-Datenpakete das Gerät wiederholt an den Server gesendet hat.

Akzeptierte Anfragen

Zeigt, wie viele Access-Accept-Datenpakete das Gerät vom Server empfangen hat.

Verworfene Anfragen

Zeigt, wie viele Access-Reject-Datenpakete das Gerät vom Server empfangen hat.

Access challenges

Zeigt, wie viele Access-Challenge-Datenpakete das Gerät vom Server empfangen hat.

Fehlerhafte Access-Antworten

Zeigt, wie viele fehlerhafte Access-Response-Datenpakete das Gerät vom Server empfangen hat (einschließlich Datenpakete mit ungültiger Länge).

Fehlerhafter Authentifikator

Zeigt, wie viele Access-Response-Datenpakete mit ungültigem Authentifikator das Gerät vom Server empfangen hat.

Offene Anfragen

Zeigt, wie viele Access-Request-Datenpakete das Gerät an den Server gesendet hat, auf die es noch keine Antwort vom Server empfangen hat.

Timeouts

Zeigt, wie viele Male die Antwort des Servers vor Ablauf der voreingestellten Wartezeit ausgeblieben ist.

Unbekannte Pakete

Zeigt, wie viele Datenpakete mit unbekanntem Datentyp das Gerät auf dem Authentication-Port vom Server empfangen hat.

Verworfene Pakete

Zeigt, wie viele Datenpakete das Gerät auf dem Authentication-Port vom Server empfangen und anschließend verworfen hat.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

4.4.5 RADIUS Accounting-Statistiken

[Netzsicherheit > RADIUS > Accounting-Statistiken]

Dieser Dialog zeigt Informationen über die Kommunikation zwischen dem Gerät und dem Accounting-Server. Die Tabelle zeigt die Informationen für jeden Server in einer separaten Zeile.

Um die Statistik zu löschen, klicken Sie im Dialog *Netzsicherheit > RADIUS > Global* die Schaltfläche ☰ und dann den Eintrag *Zurücksetzen*.

Tabelle

Name

Zeigt den Namen des Servers.

Adresse

Zeigt die IP-Adresse des Servers.

Round-Trip-Time

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

Accounting-Request-Pakete

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

Neu gesendete Accounting-Request-Pakete

Zeigt, wie viele Accounting-Request-Datenpakete das Gerät wiederholt an den Server gesendet hat.

Empfangene Pakete

Zeigt, wie viele Accounting-Response-Datenpakete das Gerät vom Server empfangen hat.

Fehlerhafte Pakete

Zeigt, wie viele fehlerhafte Accounting-Response-Datenpakete das Gerät vom Server empfangen hat (einschließlich Datenpakete mit ungültiger Länge).

Fehlerhafter Authentifikator

Zeigt, wie viele Accounting-Response-Datenpakete mit ungültigem Authentifikator das Gerät vom Server empfangen hat.

Offene Anfragen

Zeigt, wie viele Accounting-Request-Datenpakete das Gerät an den Server gesendet hat, auf die es noch keine Antwort vom Server empfangen hat.

Timeouts

Zeigt, wie viele Male die Antwort des Servers vor Ablauf der voreingestellten Wartezeit ausgeblieben ist.

Unbekannte Pakete

Zeigt, wie viele Datenpakete mit unbekanntem Datentyp das Gerät auf dem Accounting-Port vom Server empfangen hat.

Verworfene Pakete

Zeigt, wie viele Datenpakete das Gerät auf dem Accounting-Port vom Server empfangen und anschließend verworfen hat.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

4.5 DoS

[Netzsicherheit > DoS]

Denial-of-Service (DoS) ist ein Cyber-Angriff, der darauf abzielt, den Betrieb bestimmter Dienste oder Geräte zu stören. In diesem Menü können Sie mehrere Filter einrichten, um das Gerät selbst und andere Geräte im Netz vor DoS-Angriffen zu schützen.

Das Menü enthält die folgenden Dialoge:
- DoS Global

4.5.1 DoS Global

[Netzsicherheit > DoS > Global]

In diesem Dialog legen Sie die DoS-Einstellungen für die Protokolle TCP/UDP, IP und ICMP fest.

TCP/UDP

Scanner nutzen Port-Scans, um Angriffe auf das Netz vorzubreiten. Der Scanner verwendet unterschiedliche Techniken, um aktive Geräte und offene Ports zu ermitteln. Dieser Rahmen ermöglicht Ihnen, Filter für bestimmte Scan-Techniken zu aktivieren.

Das Gerät unterstützt die Erkennung der folgenden Scan-Typen:
- Null-Scans
- Xmas-Scans
- SYN/FIN-Scans
- TCP-Offset-Angriffe
- TCP-SYN-Angriffe
- L4-Port-Angriffe
- Minimal-Header-Scans

Null-Scan-Filter

Aktiviert/deaktiviert den Null-Scan-Filter.

Das Gerät erkennt und verwirft eingehende TCP-Datenpakete mit den folgenden Eigenschaften:
- Keine TCP-Flags sind gesetzt.
- Die TCP-Sequenznummer ist 0.

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

Xmas-Filter

Aktiviert/deaktiviert den Xmas-Filter.

Das Gerät erkennt und verwirft eingehende TCP-Datenpakete mit den folgenden Eigenschaften:
- Die TCP-Flags *FIN*, *URG* und *PSH* sind gleichzeitig gesetzt.
- Die TCP-Sequenznummer ist 0.

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

SYN/FIN-Filter

Aktiviert/deaktiviert den SYN/FIN-Filter.

Das Gerät erkennt eingehende Datenpakete mit gleichzeitig gesetzten TCP-Flags *SYN* und *FIN* und verwirft diese.

Mögliche Werte:

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

TCP-Offset-Protection

Aktiviert/deaktiviert den TCP-Offset-Schutz.

Der TCP-Offset-Schutz erkennt eingehende TCP-Datenpakete, deren Fragment-Offset-Feld des IP-Headers gleich 1 ist und verwirft diese.

Der TCP-Offset-Schutz akzeptiert UDP- und ICMP-Pakete mit Fragment-Offset-Feld des IP-Headers gleich 1.

Mögliche Werte:

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

TCP-SYN-Protection

Aktiviert/deaktiviert den TCP-SYN-Schutz.

Der TCP-SYN-Schutz erkennt eingehende Datenpakete mit gesetztem TCP-Flag SYN und L4-Quell-Port <1024 und verwirft diese.

Mögliche Werte:

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

L4-Port-Protection

Aktiviert/deaktiviert den L4-Port-Schutz.

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

Mögliche Werte:

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

IP

Dieser Rahmen ermöglicht Ihnen, den Land-Attack-Filter zu aktivieren und zu deaktivieren. Bei der Land-Attack-Methode sendet die angreifende Station Datenpakete, deren Quell- und Zieladresse identisch mit denen des Empfängers ist. Wenn Sie diesen Filter aktivieren, erkennt das Gerät Datenpakete mit identischer Quell- und Zieladresse und verwirft diese.

Land-Attack-Filter

Aktiviert/deaktiviert den Land-Attack-Filter.

Der Land-Attack-Filter erkennt eingehende IP-Datenpakete, deren Quell- und Ziel-IP-Adresse identisch ist, und verwirft diese.

Mögliche Werte:

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

ICMP

Dieser Dialog bietet Ihnen Filtermöglichkeiten für folgende ICMP-Parameter:

- Fragmentierte Datenpakete
- ICMP-Pakete ab einer bestimmten Größe
- Broadcast-Pings

Fragmentierte Pakete filtern

Aktiviert/deaktiviert den Filter für fragmentierte ICMP-Pakete.

Der Filter erkennt fragmentierte ICMP-Pakete und verwirft diese.

Mögliche Werte:

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

Anhand Paket-Größe verwerfen

Aktiviert/deaktiviert den Filter für eingehende ICMP-Pakete.

Der Filter erkennt ICMP-Pakete, deren Payload-Größe die im Feld *Erlaubte Payload-Größe [Byte]* festgelegte Größe überschreitet und verwirft diese.

Mögliche Werte:

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

Erlaubte Payload-Größe [Byte]

Legt die maximal erlaubte Payload-Größe von ICMP-Paketen in Byte fest.

Markieren Sie das Kontrollkästchen *Anhand Paket-Größe verwerfen*, wenn Sie eingehende Datenpakete verwerfen möchten, deren Payload-Größe die maximal erlaubte Größe von ICMP-Paketen überschreitet.

Mögliche Werte:

- `0..1472` (Voreinstellung: `512`)

Broadcast-Ping verwerfen

Aktiviert/deaktiviert den Filter für Broadcast-Pings. Broadcast Pings sind ein bekanntes Indiz für Smurf-Angriffe.

Mögliche Werte:

- `markiert`
  Der Filter ist aktiv.
  Das Gerät erkennt Broadcast-Pings und verwirft diese.
- `unmarkiert` (Voreinstellung)
  Der Filter ist inaktiv.

Information

Verworfene Pakete

Zeigt, wie viele Datenpakete das Gerät verworfen hat.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

4.6 DHCP-Snooping

[Netzsicherheit > DHCP-Snooping]

DHCP Snooping ist eine Funktion zur Unterstützung der Netzsicherheit. DHCP Snooping überwacht DHCP-Pakete zwischen DHCP-Client und DHCP-Server und verhält sich zwischen den ungesicherten Hosts und den gesicherten DHCP-Servern wie eine Firewall.

In diesem Dialog konfigurieren und überwachen Sie die folgenden Geräteeigenschaften:

- DHCP-Pakete aus nicht vertrauenswürdigen Quellen validieren und ungültige Pakete herausfiltern.
- DHCP-Datenverkehr aus vertrauenswürdigen und nicht vertrauenswürdigen Quellen limitieren.

- Die DHCP-Snooping Binding-Datenbasis aufbauen und aktualisieren. Diese Datenbasis enthält MAC-Adresse, IP-Adresse, VLAN und Port von DHCP-Clients an nicht vertrauenswürdigen Ports.
- Folgeanfragen von nicht vertrauenswürdigen Hosts auf Basis der DHCP-Snooping Binding-Datenbasis validieren.

Sie können DHCP-Snooping global und für ein bestimmtes VLAN einschalten. Den Sicherheitsstatus (vertrauenswürdig oder nicht vertrauenswürdig) können Sie an einzelnen Ports festlegen. Vergewissern Sie sich, dass der DHCP-Server über vertrauenswürdige Ports erreichbar ist. Für DHCP-Snooping konfigurieren Sie typischerweise die Benutzer-/Client-Ports als nicht vertrauenswürdig und die Uplink-Ports als vertrauenswürdig.

Das Menü enthält die folgenden Dialoge:

- DHCP-Snooping Global
- DHCP-Snooping Konfiguration
- DHCP-Snooping Statistiken
- DHCP-Snooping Bindings

4.6.1 DHCP-Snooping Global

[Netzsicherheit > DHCP-Snooping > Global]

Dieser Dialog ermöglicht Ihnen, die globalen DHCP-Snooping-Parameter Ihres Geräts zu konfigurieren:

- *DHCP-Snooping* global ein-/ausschalten.
- *Auto-Disable* global ein-/ausschalten.
- Das Prüfen der MAC-Quelladresse ein-/ausschalten.
- Name, Ablageort und Speicherintervall für die Binding-Datenbasis konfigurieren.

Funktion

Funktion

Bei eingeschalteter Funktion ist DHCP-Snooping global eingeschaltet.

Mögliche Werte:

- `An`
- `Aus` (Voreinstellung)

Konfiguration

MAC verifizieren

Aktiviert/deaktiviert die Verifizierung der Quell-MAC-Adresse im Ethernet-Paket.

Mögliche Werte:

- `markiert`
  Die Verifizierung der Quell-MAC-Adresse ist aktiv.
  Das Gerät vergleicht die Quell-MAC-Adresse mit der MAC-Adresse des Clients im empfangenen DHCP-Paket.
- `unmarkiert` (Voreinstellung)
  Die Verifizierung der Quell-MAC-Adresse ist inaktiv.

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für *DHCP-Snooping*.

Mögliche Werte:

- `markiert`
  Die Funktion *Auto-Disable* für *DHCP-Snooping* ist aktiv.
  Markieren Sie zusätzlich im Dialog *Netzsicherheit > DHCP-Snooping > Konfiguration*, Registerkarte *Auto-Disable* das Kontrollkästchen in Spalte *Port* für die gewünschten Ports.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Auto-Disable* für *DHCP-Snooping* ist inaktiv.

Binding-Datenbank

Remote Datei-Name

Legt den Namen der Datei fest, in der das Gerät die DHCP-Snooping Binding-Datenbasis speichert.

Anmerkung:

Das Gerät speichert ausschließlich dynamische Bindungen in der persistenten Binding-Datenbasis. Statische Bindungen speichert das Gerät im Konfigurationsprofil.

Remote IP-Adresse

Legt die Remote-IP-Adresse fest, unter der das Gerät die persistente DHCP-Snooping-Binding-Datenbasis speichert. Mit dem Wert `0.0.0.0` speichert das Gerät die Binding-Datenbasis lokal.

Mögliche Werte:

- Gültige IPv4-Adresse
- `0.0.0.0` (Voreinstellung)
  Das Gerät speichert die DHCP-Snooping Binding-Datenbasis lokal.

Speicher-Intervall [s]

Legt die Zeitverzögerung in Sekunden fest, nach der das Gerät die DHCP-Snooping-Binding-Datenbasis speichert, wenn es eine Veränderung in der Datenbasis ermittelt hat.

Mögliche Werte:

- `15..86400` (Voreinstellung: `300`)

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

4.6.2 DHCP-Snooping Konfiguration

[Netzsicherheit > DHCP-Snooping > Konfiguration]

Dieser Dialog ermöglicht Ihnen, DHCP-Snooping für einzelne Ports und für einzelne VLANs zu konfigurieren.

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

[Port]

In dieser Registerkarte konfigurieren Sie die Funktion *DHCP-Snooping* für einzelne Ports.
- Einen Port als vertrauenswürdig / nicht vertrauenswürdig konfigurieren.
- Die Protokollierung ungültiger Pakete für einzelne Ports ein-/ausschalten.
- Die Anzahl von DHCP-Paketen begrenzen.
- Einen Port automatisch abschalten, falls der DHCP-Datenverkehr das festgelegte Limit überschreitet.

Tabelle

Port

Zeigt die Nummer des Ports.

Vertraue

Legt den Sicherheitsstatus (trusted, untrusted) des Ports fest.

Bei eingeschalteter Funktion ist der Port als vertrauenswürdig konfiguriert. Typischerweise haben Sie den vertrauenswürdigen Port an einen DHCP-Server angeschlossen.

Bei ausgeschalteter Funktion ist der Port als nicht vertrauenswürdig konfiguriert.

Mögliche Werte:
- `markiert`
  Der Port ist als vertrauenswürdig (trusted) konfiguriert. Über vertrauenswürdige Ports leitet DHCP-Snooping zulässige Client-Pakete weiter.
- `unmarkiert` (Voreinstellung)
  Der Port ist als nicht vertrauenswürdig (untrusted) konfiguriert. An nicht vertrauenswürdigen Ports vergleicht das Gerät in der Binding-Databasis den Empfänger-Port mit dem Client-Port.

Protokolliere

Aktiviert/deaktiviert die Protokollierung von ungültigen Paketen, die das Gerät auf diesem Port ermittelt.

Mögliche Werte:

- `markiert`
  Die Protokollierung ungültiger Pakete ist aktiv.
- `unmarkiert` (Voreinstellung)
  Die Protokollierung ungültiger Pakete ist inaktiv.

Lastbegrenzung

Legt die maximale Anzahl von DHCP-Paketen pro Burst-Intervall für diesen Port fest. Wenn die Anzahl der eingehenden DHCP-Pakete das festgelegte Limit in einem Burst-Intervall gegenwärtig überschreitet, dann verwirft das Gerät weitere eingehende DHCP-Pakete.

Mögliche Werte:

- `-1` (Voreinstellung)
  Hebt die Limitierung der Anzahl von DHCP-Paketen pro Burst-Intervall auf diesem Port auf.
- `0..150` Pakete pro Intervall
  Begrenzt die maximale Anzahl von DHCP-Paketen pro Burst-Intervall auf diesem Port.

Das Burst-Intervall legen Sie in Spalte *Burst-Intervall* fest.

Wenn Sie die Auto-Disable-Funktion aktiviert haben, schaltet das Gerät zusätzlich den Port aus. Die Auto-Disable-Funktion finden Sie in Spalte *Auto-Disable*.

Burst-Intervall

Legt die Länge des Burst-Intervalls in Sekunden auf diesem Port fest. Das Burst-Intervall ist für die Rate-Limiting-Funktion relevant.

Die maximale Anzahl von DHCP-Paketen pro Burst-Intervall legen Sie in Spalte *Lastbegrenzung* fest.

Mögliche Werte:

- `1..15` (Voreinstellung: `1`)

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für die Parameter, deren Einhaltung die Funktion *DHCP-Snooping* auf dem Port überwacht.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Funktion *Auto-Disable* ist auf dem Port aktiv.
  Voraussetzung ist, dass im Dialog *Netzsicherheit > DHCP-Snooping > Global*, Rahmen *Konfiguration* das Kontrollkästchen *Auto-Disable* markiert ist.
  - Das Gerät schaltet den Port aus, wenn der Port während der in Spalte *Burst-Intervall* festgelegten Zeit mehr DHCP-Pakete empfängt als im Feld *Lastbegrenzung* festgelegt ist. Die „Link-Status“-LED des Ports blinkt 3× pro Periode.
  - Der Dialog *Diagnose > Ports > Auto-Disable* zeigt, welche Ports aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet sind.
  - Die Funktion *Auto-Disable* schaltet den Port automatisch wieder ein. Legen Sie dazu im Dialog *Diagnose > Ports > Auto-Disable* in Spalte *Reset-Timer [s]* eine Wartezeit für den betreffenden Port fest.
- `unmarkiert`
  Die Funktion *Auto-Disable* auf dem Port ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[VLAN-ID]

In dieser Registerkarte konfigurieren Sie die Funktion *DHCP-Snooping* für einzelne VLANs.

Tabelle

VLAN-ID

Zeigt die VLAN-ID, auf die sich der Tabelleneintrag bezieht.

Aktiv

Aktiviert/deaktiviert die Funktion *DHCP-Snooping* in diesem VLAN.

Die Funktion *DHCP-Snooping* leitet gültige DHCP-Client-Nachrichten weiter an den vertrauenswürdigen Ports in VLANs ohne Funktion *Routing*.

Mögliche Werte:

- `markiert`
  Die Funktion *DHCP-Snooping* ist in diesem VLAN aktiv.
- `unmarkiert` (Voreinstellung)
  Die Funktion *DHCP-Snooping* ist in diesem VLAN inaktiv.
  Das Gerät leitet DHCP-Pakete entsprechend der Switching-Einstellungen weiter, ohne die Pakete zu überwachen. Die Binding-Datenbasis bleibt unverändert.

Anmerkung: Um DHCP-Snooping für einen Port einzuschalten, schalten Sie im Dialog *Netzsicherheit > DHCP-Snooping > Global* die Funktion *DHCP-Snooping* global ein. Vergewissern Sie sich, dass der Port einem VLAN zugewiesen ist, in dem DHCP-Snooping eingeschaltet ist.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

4.6.3 DHCP-Snooping Statistiken

[Netzsicherheit > DHCP-Snooping > Statistiken]

Das Gerät protokolliert beim DHCP-Snooping erkannte Fehler und erstellt Statistiken. In diesem Dialog überwachen Sie die DHCP-Snooping-Statistiken für jeden Port.

Das Gerät protokolliert folgendes:
- Erkannte Fehler bei der Prüfung der MAC-Adresse des DHCP-Clients
- DHCP-Client-Nachrichten mit erkanntem fehlerhaftem Port
- DHCP-Server-Nachrichten an nicht vertrauenswürdigen Ports

Tabelle

Port

Zeigt die Nummer des Ports.

Fehler bei MAC-Prüfung

Zeigt die Anzahl der Diskrepanzen zwischen der MAC-Adresse des DHCP-Clients im Feld 'chaddr' des DHCP-Datenpaketes und der Quelladresse im Ethernet-Paket.

Ungültige Client-Nachrichten

Zeigt die Anzahl der auf dem Port eingegangenen DHCP-Client-Meldungen, bei denen das Gerät gemäß DHCP-Snooping Binding-Datenbasis den Client auf einem anderen Port erwartet.

Ungültige Server-Nachrichten

Zeigt die Anzahl der DHCP-Server-Meldungen, die das Gerät auf dem nicht-vertrauenswürdigen Port empfangen hat.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Zurücksetzen

Setzt die gesamte Tabelle zurück.

4.6.4 DHCP-Snooping Bindings

[Netzsicherheit > DHCP-Snooping > Bindings]

DHCP-Snooping verwendet DHCP-Nachrichten, um die Binding-Datenbasis aufzubauen und zu aktualisieren.

- Statische Bindungen
  Das Gerät ermöglicht Ihnen, bis zu 256 statische DHCP-Snooping-Bindungen in die Datenbasis einzutragen.
- Dynamische Bindungen
  Die dynamische Binding-Datenbasis enthält ausschließlich Daten für Clients an nicht vertrauenswürdigen Ports.

Dieses Menü ermöglicht Ihnen, die Einstellungen für statische und für dynamische Bindungen festzulegen.

- Neue statische Bindungen einrichten und aktiv/inaktiv setzen.
- Eingerichtete statische Bindungen anzeigen, aktivieren/deaktivieren oder löschen.

Tabelle

MAC-Adresse

Legt die MAC-Adresse im Tabelleneintrag fest, die Sie an eine *IP-Adresse* und eine *VLAN-ID* binden.

Mögliche Werte:

- Gültige Unicast-MAC-Adresse
  Legen Sie den Wert mit Doppelpunkt-Trennzeichen fest, zum Beispiel `00:11:22:33:44:55`.

IP-Adresse

Legt die IP-Adresse für die statische Bindung von DHCP-Snooping fest.

Mögliche Werte:

- Gültige Unicast-IPv4-Adresse kleiner als `224.x.x.x` und außerhalb des Bereiches `127.0.0.0/8` (Voreinstellung: `0.0.0.0`)

VLAN-ID

Legt die ID des VLANs fest, für das der Tabelleneintrag gilt.

Mögliche Werte:

- `<ID der VLANs, die eingerichtet sind>`

Port

Legt den Port für die statische DHCP-Snooping-Bindung fest.

Mögliche Werte:

- Verfügbare Ports

Verbleibende Binding-Zeit

Zeigt die Restlaufzeit der dynamischen DHCP-Snooping-Bindung.

Aktiv

Aktiviert/deaktiviert die konfigurierte statische DHCP-Snooping-Bindung.

Mögliche Werte:

- `markiert`
  Die statische DHCP-Snooping-Bindung ist aktiv.
- `unmarkiert` (Voreinstellung)
  Die statische DHCP-Snooping-Bindung ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

Im Feld *MAC-Adresse* legen Sie die MAC-Adresse fest, die Sie an eine IP-Adresse und VLAN-ID binden.

Entfernt den markierten Tabelleneintrag.

Voraussetzung ist, dass das Kontrollkästchen in Spalte *Aktiv* unmarkiert ist.

Außerdem entfernt das Gerät die mit der Funktion *IP Source Guard* erzeugten dynamischen Bindungen dieses Ports.

4.7 IP Source Guard

[Netzsicherheit > IP Source Guard]

IP Source Guard (IPSG) ist eine Funktion zur Unterstützung der Netzsicherheit. Die Funktion filtert IP-Datenpakete basierend auf der Source-ID (Quell-IP-Adresse oder die Quell-MAC-Adresse) des Teilnehmers. IPSG unterstützt Sie beim Schutz des Netzes vor Angriffen über IP-/MAC-Adress-Spoofing.

IPSG und DHCP-Snooping
IP Source Guard arbeitet mit der Funktion *DHCP-Snooping*zusammen.

DHCP-Snooping verwirft IP-Datenpakete an nicht vertrauenswürdigen Ports mit Ausnahme von DHCP-Nachrichten. Wenn das Gerät DHCP-Antworten empfängt und die DHCP-Snooping Binding-Datenbasis eingerichtet ist, erstellt das Gerät pro Port eine VLAN Access Control List (VACL), welche die Source-IDs der Teilnehmer enthält.

Die Parameter der Funktion *DHCP-Snooping* für einzelne Ports und für einzelne VLANs konfigurieren Sie im Dialog *Netzsicherheit > DHCP-Snooping > Konfiguration*.

IPSG und Portsicherheit
IP Source Guard arbeitet mit der Funktion *Port-Sicherheit* zusammen. Siehe Dialog *Netzsicherheit > Port-Sicherheit*. IPSG teilt der Funktion *Port-Sicherheit* auf Anfrage mit, ob eine neu gelernte MAC-Adresse zu einer gültigen Bindung gehört.

- Wenn Sie IPSG am Ingress-Port deaktiviert haben, bezeichnet IPSG das Datenpaket als gültig.
- Wenn Sie IPSG am Ingress-Port aktiviert haben, prüft IPSG die MAC-Adresse anhand der Bindings-Datenbasis. Wenn die MAC-Adresse in der Bindings-Datenbasis eingetragen ist, bezeichnet IPSG das Datenpaket als gültig, andernfalls als ungültig.

Die Funktion *Port-Sicherheit*übernimmt die weitere Behandlung von ungültigen Datenpaketen. Die Einstellungen der Funktion *Port-Sicherheit* legen Sie im Dialog *Netzsicherheit > Port-Sicherheit* fest.

Anmerkung: Damit das Gerät die IP-Adresse und die MAC-Adresse der auf dem Port empfangenen Datenpakete prüft, schalten Sie die Funktion *MAC verifizieren* ein.

Damit das Gerät vor Weiterleiten des Datenpakets die VLAN-ID und MAC-Adresse des Absenders prüft, schalten Sie zusätzlich die Funktion *Port-Sicherheit* ein. Siehe Dialog *Netzsicherheit > Port-Sicherheit*.

Das Menü enthält die folgenden Dialoge:

- IP Source Guard Port
- IP Source Guard Bindings

4.7.1 IP Source Guard Port

[Netzsicherheit > IP Source Guard > Port]

Dieser Dialog ermöglicht Ihnen, die folgenden Geräteeigenschaften pro Port anzuzeigen und zu konfigurieren:

- Quell-MAC-Adressen für die Filterung ein-/ausschließen
- Die Funktion *IP Source Guard* aktivieren/deaktivieren.

Tabelle

Port

Zeigt die Nummer des Ports.

MAC verifizieren

Aktiviert/deaktiviert bei aktiver Funktion *IP Source Guard* die Filterung nach der Quell-MAC-Adresse. Das Gerät führt diese Filterung zusätzlich zur Filterung nach der Quell-IP-Adresse durch.

Mögliche Werte:

- `markiert`
  Die Filterung nach der Quell-MAC-Adresse ist aktiv.
  Um die Funktion zu aktivieren, markieren Sie das Kontrollkästchen *Aktiv*.
- `unmarkiert` (Voreinstellung)
  Die Filterung nach der Quell-MAC-Adresse ist inaktiv.
  Um die Funktion zu deaktivieren, heben Sie die Markierung des Kontrollkästchens *Aktiv* auf.

Aktiv

Aktiviert/deaktiviert die Funktion *IP Source Guard* auf dem Port.

Mögliche Werte:

- `markiert`
  Die Funktion *IP Source Guard* ist aktiv.
  Schalten Sie zusätzlich im Dialog *Netzsicherheit > DHCP-Snooping > Global* die Funktion *DHCP-Snooping* ein.
- `unmarkiert` (Voreinstellung)
  Die Funktion *IP Source Guard* ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

4.7.2 IP Source Guard Bindings

[Netzsicherheit > IP Source Guard > Bindings]

Dieser Dialog zeigt statische und dynamische IP Source Guard-Bindungen.

- Dynamische Bindungen lernt das Gerät mit DHCP-Snooping. Siehe Dialog *Netzsicherheit > DHCP-Snooping > Konfiguration*.
- Statische Bindungen sind manuell durch Benutzer eingerichtete IP-Source-Guard-Bindungen. Der Dialog ermöglicht Ihnen, statische Bindungen zu bearbeiten.

Tabelle

MAC-Adresse

Zeigt die MAC-Adresse der Bindung.

IP-Adresse

Zeigt die IP-Adresse der Bindung.

VLAN-ID

Zeigt die VLAN-ID der Bindung.

Port

Zeigt die Nummer des Ports der Bindung.

Hardware-Status

Zeigt den Hardware-Status der Bindung.

Das Gerät wendet die Bindung ausschließlich dann auf die Hardware an, wenn die Einstellungen korrekt sind. Bevor das Gerät die statische IPSG-Bindung auf die Hardware anwendet, prüft es die Voraussetzungen:

- Das Kontrollkästchen *Aktiv* ist markiert.
- Die Funktion *IP Source Guard* auf dem Port ist eingeschaltet, im Dialog *Netzsicherheit > IP Source Guard > Port* ist das Kontrollkästchen *Aktiv* markiert.

Mögliche Werte:

- `markiert`
  Die Bindung ist aktiv, das Gerät wendet die Bindung auf die Hardware an.
- `unmarkiert`
  Die Bindung ist inaktiv.

Aktiv

Aktiviert/deaktiviert die konfigurierte statische IPSG-Bindung zwischen der festgelegten MAC-Adresse und der festgelegten IP-Adresse, für das festgelegte VLAN auf dem festgelegten Port.

Mögliche Werte:

- `markiert`
  Die statische IPSG-Bindung ist aktiv.
- `unmarkiert` (Voreinstellung)
  Die statische IPSG-Bindung ist inaktiv.

Anmerkung: Damit die statische Bindung wirksam wird, schalten Sie die Funktion *IP Source Guard* auf dem zugehörigen Port ein. Markieren Sie im Dialog *Netzsicherheit > IP Source Guard > Port* das Kontrollkästchen *Aktiv*.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

- Im Feld *MAC-Adresse* legen Sie die MAC-Adresse für die statische Bindung fest.
- Im Feld *IP-Adresse* legen Sie die IP-Adresse für die statische Bindung fest.
- Im Feld *VLAN-ID*legen Sie die VLAN-ID fest.
- Im Feld *Port* legen Sie die ID des VLANs fest.

Entfernt den markierten Tabelleneintrag.

Voraussetzung ist, dass das Kontrollkästchen in Spalte *Aktiv* unmarkiert ist.

4.8 Dynamic ARP Inspection

[Netzsicherheit > Dynamic ARP Inspection]

Dynamic ARP Inspection ist eine Funktion zur Unterstützung der Netzsicherheit. Diese Funktion analysiert ARP-Pakete, protokolliert sie und weist ungültige und feindliche ARP-Pakete zurück.

Die Funktion *Dynamic ARP Inspection* hilft, eine Reihe von Man-in-the-Middle-Angriffen zu verhindern. Bei dieser Art von Angriffen hört eine bösartige Station den Datenverkehr von anderen Teilnehmern ab, wobei sie in den ARP-Cache ihrer arglosen Nachbarn eingreift. Die bösartige Station sendet ARP-Anfragen und ARP-Antworten und trägt in der IP-zu-MAC Adress-Beziehung (Binding) bei ihrer eigenen MAC-Adresse die IP-Adresse eines anderen Teilnehmers ein.

Die Funktion *Dynamic ARP Inspection* hilft, durch folgende Maßnahmen sicherzustellen, dass das Gerät ausschließlich gültige ARP-Anfragen und ARP-Antworten weiterleitet.

- Abhören von ARP-Anfragen und ARP-Antworten an nicht vertrauenswürdigen Ports.
- Vergewissern, dass die ermittelten Pakete eine gültige IP-zu-MAC-Adress-Beziehung (Binding) haben, bevor das Gerät den lokalen ARP-Cache aktualisiert und bevor das Gerät die Pakete an die zugehörige Zieladresse weiterleitet.
- Verwerfen von ungültigen ARP-Paketen.

Das Gerät ermöglicht Ihnen, bis zu 100 aktive ARP-ACLs (Zugriffslisten) zu definieren. Pro ARP-ACL können Sie bis zu 20 Regeln aktivieren.

Das Menü enthält die folgenden Dialoge:

- Dynamic-ARP-Inspection Global
- Dynamic-ARP-Inspection Konfiguration
- Dynamic-ARP-Inspection ARP-Regeln
- Dynamic-ARP-Inspection Statistiken

4.8.1 Dynamic-ARP-Inspection Global

[Netzsicherheit > Dynamic ARP Inspection > Global]

Konfiguration

Quell-MAC verifizieren

Aktiviert/deaktiviert die Verifizierung der Quell-MAC-Adresse. Das Gerät führt die Prüfung sowohl in ARP-Anfragen als auch in ARP-Antworten durch.

Mögliche Werte:

- `markiert`
  Die Verifizierung der Quell-MAC-Adresse ist aktiv.
  Das Gerät prüft die Quell-MAC-Adresse empfangener ARP-Pakete.
  - ARP-Pakete mit gültiger Quell-MAC-Adresse vermittelt das Gerät an die zugehörige Zieladresse und aktualisiert den lokalen ARP-Cache.
  - ARP-Pakete mit ungültiger Quell-MAC-Adresse verwirft das Gerät.
- `unmarkiert` (Voreinstellung)
  Die Verifizierung der Quell-MAC-Adresse ist inaktiv.

Destination-MAC verifizieren

Aktiviert/deaktiviert die Verifizierung der Ziel-MAC-Adresse. Das Gerät führt die Prüfung in ARP-Antworten durch.

Mögliche Werte:

- `markiert`
  Die Verifizierung der Ziel-MAC-Adresse ist aktiv.
  Das Gerät prüft die Ziel-MAC-Adresse der eingehenden ARP-Pakete.
  - ARP-Pakete mit gültiger Ziel-MAC-Adresse leitet das Gerät an die zugehörige Zieladresse weiter und aktualisiert den lokalen ARP-Cache.
  - ARP-Pakete mit ungültiger Ziel-MAC-Adresse verwirft das Gerät.
- `unmarkiert` (Voreinstellung)
  Das Prüfen der Ziel-MAC-Adresse der eingehenden ARP-Pakete ist deaktiviert.

IP-Adresse verifizieren

Aktiviert/deaktiviert die Verifizierung der IP-Adresse.

In ARP-Anfragen prüft das Gerät die Quell-IP-Adresse. In ARP-Antworten prüft das Gerät die Ziel- und die Quell-IP-Adresse.

Das Gerät betrachtet die folgenden IP-Adressen als ungültig:

- `0.0.0.0`
- Broadcast-Adressen `255.255.255.255`
- Multicast-Adressen `224.0.0.0/4` (Class D)
- Class-E-Adressen `240.0.0.0/4` (reserviert für spätere Zwecke)
- Loopback-Adressen im Bereich `127.0.0.0/8`.

Mögliche Werte:

- `markiert`
  Die Verifizierung der IP-Adresse ist aktiv.
  Das Gerät prüft die IP-Adresse der eingehenden ARP-Pakete. ARP-Pakete mit gültiger IP-Adresse leitet das Gerät an die zugehörige Zieladresse weiter und aktualisiert den lokalen ARP-Cache. ARP-Pakete mit ungültiger IP-Adresse verwirft das Gerät.
- `unmarkiert` (Voreinstellung)
  Die Verifizierung der IP-Adresse ist inaktiv.

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für *Dynamic ARP Inspection*.

Mögliche Werte:

- `markiert`
  Die Funktion *Auto-Disable* für *Dynamic ARP Inspection* ist aktiv.
  Markieren Sie zusätzlich im Dialog *Netzsicherheit > Dynamic ARP Inspection > Konfiguration*, Registerkarte *Port* das Kontrollkästchen in Spalte *Auto-Disable* für die gewünschten Ports.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Auto-Disable* für *Dynamic ARP Inspection* ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

4.8.2 Dynamic-ARP-Inspection Konfiguration

[Netzsicherheit > Dynamic ARP Inspection > Konfiguration]

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

[Port]

Tabelle

Port

Zeigt die Nummer des Ports.

Vertraue

Aktiviert/deaktiviert die Überwachung von ARP-Paketen auf nicht-vertrauenswürdigen Ports.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Das Gerät überwacht ARP-Pakete auf nicht-vertrauenswürdigen Ports.
  ARP-Pakete auf vertrauenswürdigen Ports leitet das Gerät direkt weiter.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Lastbegrenzung

Legt die maximale Anzahl von ARP-Paketen pro Intervall auf diesem Port fest. Wenn die Rate der eingehenden ARP-Pakete das festgelegte Limit in einem Burst-Intervall gegenwärtig überschreitet, verwirft das Gerät weitere eingehende ARP-Pakete. Das Burst-Intervall legen Sie in Spalte *Burst-Intervall* fest.

Optional schaltet das Gerät zusätzlich den Port aus, wenn Sie die Auto-Disable Funktion aktiviert haben. Die Funktion *Auto-Disable* schalten Sie in Spalte *Auto-Disable* ein/aus.

Mögliche Werte:

- `-1` (Voreinstellung)
  Hebt die Limitierung der Anzahl von ARP-Paketen pro Burst-Intervall auf diesem Port auf.
- `0..300` Pakete pro Intervall
  Begrenzt die maximale Anzahl von ARP-Paketen pro Burst-Intervall auf diesem Port.

Burst-Intervall

Legt die Länge des Burst-Intervalls in Sekunden auf diesem Port fest. Das Burst-Intervall ist für die Rate-Limiting-Funktion relevant.

Die maximale Anzahl von ARP-Paketen pro Burst-Intervall legen Sie in Spalte *Lastbegrenzung* fest.

Mögliche Werte:

- `1..15` (Voreinstellung: `1`)

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für die Parameter, deren Einhaltung die Funktion *Dynamic ARP Inspection* auf dem Port überwacht.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Funktion *Auto-Disable* ist auf dem Port aktiv.
  Voraussetzung ist, dass im Dialog *Netzsicherheit > Dynamic ARP Inspection > Global*, Rahmen *Konfiguration* das Kontrollkästchen *Auto-Disable* markiert ist.
  - Das Gerät schaltet den Port aus, wenn der Port während der in Spalte *Burst-Intervall* festgelegten Zeit mehr ARP-Pakete empfängt als im Feld *Lastbegrenzung* festgelegt ist. Die „Link-Status“-LED des Ports blinkt 3× pro Periode.
  - Der Dialog *Diagnose > Ports > Auto-Disable* zeigt, welche Ports aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet sind.
  - Die Funktion *Auto-Disable* schaltet den Port automatisch wieder ein. Legen Sie dazu im Dialog *Diagnose > Ports > Auto-Disable* in Spalte *Reset-Timer [s]* eine Wartezeit für den betreffenden Port fest.
- `unmarkiert`
  Die Funktion *Auto-Disable* auf dem Port ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[VLAN-ID]

Tabelle

VLAN-ID

Zeigt die VLAN-ID, auf die sich der Tabelleneintrag bezieht.

Protokolliere

Aktiviert/deaktiviert die Protokollierung von ungültigen ARP-Paketen, die das Gerät in diesem VLAN ermittelt. Das Gerät behandelt ein ARP-Paket als ungültig, wenn es bei der Prüfung von IP-Adresse, Quell-MAC-Adresse, Ziel-MAC-Adresse oder bei der Prüfung der IP-zu-MAC-Adress-Beziehung (Binding) einen Fehler erkennt.

Mögliche Werte:

- `markiert`
  Die Protokollierung ungültiger Pakete ist aktiv.
  Das Gerät protokolliert ungültige ARP-Pakete.
- `unmarkiert` (Voreinstellung)
  Die Protokollierung ungültiger Pakete ist inaktiv.

Binding check

Aktiviert/deaktiviert das Prüfen eingehender ARP-Pakete, die das Gerät an nicht-vertrauenswürdigen Ports und an VLANs mit aktiver Funktion *Dynamic ARP Inspection* empfängt. Das Gerät prüft bei diesen ARP-Paketen die ARP- ACL und die DHCP-Snooping-Beziehung (Binding).

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Beziehungs(Binding)-Prüfung von ARP-Paketen ist aktiviert.
- `unmarkiert`
  Die Beziehungs(Binding)-Prüfung von ARP-Paketen ist deaktiviert.

ACL strict

Aktiviert/deaktiviert die strikte Prüfung von eingehenden ARP-Paketen anhand der festgelegten ARP-ACL-Regeln.

Mögliche Werte:

- `markiert`
  Die strikte Prüfung ist aktiv.
  Das Gerät prüft eingehende ARP-Pakete anhand der in Spalte *ARP ACL* festgelegten ARP-ACL-Regeln.
- `unmarkiert` (Voreinstellung)
  Die strikte Prüfung ist inaktiv.
  Das Gerät prüft eingehende ARP-Pakete anhand der in Spalte *ARP ACL* festgelegten ARP-ACL-Regeln und anschließend anhand der Einträge in der DHCP-Snooping-Datenbank.

ARP ACL

Legt die ARP-ACL fest, die das Gerät verwendet.

Mögliche Werte:

- `<Name der Regel>`
  Die Regeln erzeugen und bearbeiten Sie im Dialog *Netzsicherheit > Dynamic ARP Inspection > ARP Regeln*.

Aktiv

Aktiviert/deaktiviert die Funktion *Dynamic ARP Inspection* in diesem VLAN.

Mögliche Werte:

- `markiert`
  Die Funktion *Dynamic ARP Inspection* ist in diesem VLAN aktiv.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Dynamic ARP Inspection* ist in diesem VLAN inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

4.8.3 Dynamic-ARP-Inspection ARP-Regeln

[Netzsicherheit > Dynamic ARP Inspection > ARP Regeln]

Dieser Dialog ermöglicht Ihnen, Regeln zur Prüfung und Filterung von ARP-Paketen zu definieren.

Tabelle

Name

Zeigt den Namen der ARP-Regel.

Quell-IP-Adresse

Legt die Quelladresse der IP-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

- Gültige IPv4-Adresse
  Das Gerät wendet die Regel auf IP-Datenpakete mit der festgelegten Quelladresse an.

Quell-MAC-Adresse

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

Mögliche Werte:

- Gültige MAC-Adresse
  Das Gerät wendet die Regel auf MAC-Datenpakete mit der festgelegten Quelladresse an.

Aktiv

Aktiviert/deaktiviert die *ARP*-Regel.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Regel ist aktiv.
- `unmarkiert`
  Die Regel ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

- Im Feld *Name* legen Sie den Namen der ARP-Regel fest.
- Im Feld *Quell-IP-Adresse* legen Sie die Quell-IP-Adresse der ARP-Regel fest.
- Im Feld *Quell-MAC-Adresse* legen Sie die Quell-MAC-Adresse der ARP-Regel fest.

4.8.4 Dynamic-ARP-Inspection Statistiken

[Netzsicherheit > Dynamic ARP Inspection > Statistiken]

Dieses Fenster zeigt die Anzahl verworfener und weitergeleiteter ARP-Pakete in einer Übersicht.

Tabelle

VLAN-ID

Zeigt die VLAN-ID, auf die sich der Tabelleneintrag bezieht.

Weitergeleitete Pakete

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung durch die Funktion *Dynamic ARP Inspection* weitergeleitet hat.

Verworfene Pakete

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung durch die Funktion *Dynamic ARP Inspection* verworfen hat.

DHCP drops

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung der DHCP-Snooping-Beziehung (Binding) verworfen hat.

DHCP permits

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung der DHCP-Snooping-Beziehung (Binding) weitergeleitet hat.

ACL drops

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung anhand der ARP-ACL-Regeln verworfen hat.

ACL permits

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung anhand der ARP-ACL-Regeln weitergeleitet hat.

Ungültige Quell-MAC

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung durch die Funktion *Dynamic ARP Inspection* aufgrund eines erkannten Fehlers in der Quell-MAC-Adresse verworfen hat.

Ungültige Ziel-MAC

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung durch die Funktion *Dynamic ARP Inspection* aufgrund eines erkannten Fehlers in der Ziel-MAC-Adresse verworfen hat.

Ungültige IP-Adresse

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung durch die Funktion *Dynamic ARP Inspection* aufgrund eines erkannten Fehlers in der IP-Adresse verworfen hat.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Zurücksetzen

Setzt die gesamte Tabelle zurück.

4.9 ACL

[Netzsicherheit > ACL]

In diesem Menü legen Sie die Einstellungen für Access-Control-Listen (ACL) fest. Access-Control-Listen enthalten Regeln, die das Gerät nacheinander auf den Datenstrom an seinen Ports oder VLANs anwendet.

Erfüllt ein Datenpaket die Kriterien einer oder mehrerer Regeln, wendet das Gerät die in der 1. zutreffenden Regel festgelegte Aktion auf das Datenpaket an. Die noch folgenden Regeln ignoriert das Gerät. Mögliche Aktionen sind:
- `permit`: Das Gerät vermittelt das Datenpaket an einen Port oder an ein VLAN.
- `deny`: Das Gerät verwirft das Datenpaket.

In der Voreinstellung vermittelt das Gerät jedes Datenpaket. Sobald Sie einem Port oder VLAN eine Access-Control-Liste zuweisen, ändert sich dort dieses Verhalten. An das Ende einer Access-Control-Liste fügt das Gerät eine implizite Deny-All-Regel ein. Demzufolge verwirft das Gerät Datenpakete, die keines der Regel-Kriterien erfüllen. Wenn Sie ein anderes Verhalten wünschen, fügen Sie am Ende Ihrer Access-Control-Listen eine „permit“-Regel ein.

Gehen Sie wie folgt vor, um Access-Control-Listen und Regeln einzurichten:
- ☐ Erzeugen Sie eine Regel und legen Sie die Einstellungen der Regel fest. Siehe Dialog *Netzsicherheit > ACL > IPv4-Regel* oder Dialog *Netzsicherheit > ACL > MAC-Regel*.
- ☐ Weisen Sie die Access-Control-Liste den Ports und VLANs des Geräts zu. Siehe Dialog *Netzsicherheit > ACL > Zuweisung*.

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

4.9.1 ACL IPv4-Regel

[Netzsicherheit > ACL > IPv4-Regel]

In diesem Dialog legen Sie die Regeln fest, die das Gerät auf IP-Datenpakete anwendet.

Eine Access-Control-Liste (Gruppe) enthält eine oder mehrere Regeln. Das Gerät wendet die Regeln einer Access-Control-Liste nacheinander an, zuerst die Regel mit dem kleinsten Wert in Spalte *Index*.

Das Gerät ermöglicht Ihnen, nach folgenden Kriterien zu filtern:
- Quell- oder Ziel-IP-Adresse eines Datenpakets
- Typ des übertragenden Protokolls
- Quell- oder Ziel-Port eines Datenpakets

Tabelle

Gruppenname

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

Index

Zeigt die Nummer der Regel innerhalb der Access-Control-Liste.

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

Alle Pakete filtern

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

Mögliche Werte:
- `markiert` (Voreinstellung)
  Das Gerät wendet die Regel auf jedes IP-Datenpaket an.
- `unmarkiert`
  Das Gerät wendet die Regel auf IP-Datenpakete an, abhängig vom Wert in den Feldern *Quell-IP-Adresse*,*Ziel-IP-Adresse*und *Protokoll*.

Quell-IP-Adresse

Legt die Quelladresse der IP-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:
- `?.?.?.?` (Voreinstellung)
  Das Gerät wendet die Regel auf IP-Datenpakete mit beliebiger Quelladresse an.

- Gültige IPv4-Adresse
  Das Gerät wendet die Regel auf IP-Datenpakete mit der festgelegten Quelladresse an. Verwenden Sie das Zeichen `?` als Platzhalter.
  Beispiel `192.?.?.32`: Das Gerät wendet die Regel auf IP-Datenpakete an, deren Quelladresse mit `192.` beginnt und mit `.32` endet.
- Gültige IPv4-Adresse/Bitmaske
  Das Gerät wendet die Regel auf IP-Datenpakete mit der festgelegten Quelladresse an. Die inverse Bitmaske ermöglicht Ihnen, den Adressbereich bitgenau festzulegen.
  Beispiel `192.168.1.0/0.0.0.127`: Das Gerät wendet die Regel auf IP-Datenpakete mit einer Quelladresse im Bereich von `192.168.1.0` bis `….127` an.

Ziel-IP-Adresse

Legt die Zieladresse der IP-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

- `?.?.?.?` (Voreinstellung)
  Das Gerät wendet die Regel auf Datenpakete mit beliebiger Zieladresse an.
- Gültige IPv4-Adresse
  Das Gerät wendet die Regel auf Datenpakete mit der festgelegten Zieladresse an. Verwenden Sie das Zeichen `?` als Platzhalter.
  Beispiel `192.?.?.32`: Das Gerät wendet die Regel auf IP-Datenpakete an, deren Quelladresse mit `192.` beginnt und mit `.32` endet.
- Gültige IPv4-Adresse/Bitmaske
  Das Gerät wendet die Regel auf Datenpakete mit der festgelegten Zieladresse an. Die inverse Bitmaske ermöglicht Ihnen, den Adressbereich bitgenau festzulegen.
  Beispiel `192.168.1.0/0.0.0.127`: Das Gerät wendet die Regel auf IP-Datenpakete mit einer Zieladresse im Bereich von `192.168.1.0` bis `….127` an.

Protokoll

Legt den Protokolltyp der IP-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

- `any` (Voreinstellung)
  Das Gerät wendet die Regel auf jedes IP-Datenpaket an, ohne den Protokolltyp zu berücksichtigen.
- `icmp`
- `igmp`
- `ip-in-ip`
- `tcp`
- `udp`
- `ip`

Quell-TCP/UDP-Port

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

Mögliche Werte:

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

Ziel-TCP/UDP-Port

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

Mögliche Werte:

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

Aktion

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

Mögliche Werte:

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

Protokolliere

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

Mögliche Werte:

- `markiert`
  Die Protokollierung ist aktiviert.
  Voraussetzung ist, dass Sie die Access-Control-Liste im Dialog *Netzsicherheit > ACL > Zuweisung* einem VLAN oder einem Port zuweisen.
  Das Gerät protokolliert in der Log-Datei im Intervall von 30 s, wie viele Male es eine Deny-Regel auf IP-Datenpakete angewendet hat.
- `unmarkiert` (Voreinstellung)
  Die Protokollierung ist deaktiviert.

Das Gerät ermöglicht Ihnen, für bis zu 128 Deny-Regeln diese Funktion zu aktivieren.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

- Im Feld *Gruppenname* legen Sie den Namen der Access-Control-Liste fest, der die Regel angehört.
- Im Feld *Index* legen Sie die Nummer der Regel innerhalb der Access-Control-Liste fest. Enthält die Access-Control-Liste mehrere Regeln, wendet das Gerät die Regel mit dem kleinsten Wert zuerst an.

4.9.2 ACL MAC-Regel

[Netzsicherheit > ACL > MAC-Regel]

In diesem Dialog legen Sie die Regeln fest, die das Gerät auf MAC-Datenpakete anwendet.

Eine Access-Control-Liste (Gruppe) enthält eine oder mehrere Regeln. Das Gerät wendet die Regeln einer Access-Control-Liste nacheinander an, zuerst die Regel mit dem kleinsten Wert in Spalte *Index*.

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

Tabelle

Gruppenname

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

Index

Zeigt die Nummer der Regel innerhalb der Access-Control-Liste.

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

Alle Pakete filtern

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

Mögliche Werte:

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

Quell-MAC-Adresse

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

Mögliche Werte:

- `??:??:??:??:??:??` (Voreinstellung)
  Das Gerät wendet die Regel auf MAC-Datenpakete mit beliebiger Quelladresse an.
- Gültige MAC-Adresse
  Das Gerät wendet die Regel auf MAC-Datenpakete mit der festgelegten Quelladresse an.
  Verwenden Sie das Zeichen `?` als Platzhalter.
  Beispiel `00:11:??:??:??:??`: Das Gerät wendet die Regel auf MAC-Datenpakete an, deren Quelladresse mit `00:11` beginnt.
- Gültige MAC-Adresse/Bitmaske
  Das Gerät wendet die Regel auf MAC-Datenpakete mit der festgelegten Quelladresse an. Die Bitmaske ermöglicht Ihnen, den Adressbereich bitgenau festzulegen.
  Beispiel `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`: Das Gerät wendet die Regel auf MAC-Datenpakete mit einer Quelladresse im Bereich von `00:11:22:33:44:54` bis `…:57` an.

Ziel-MAC-Adresse

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

Mögliche Werte:

- `??:??:??:??:??:??` (Voreinstellung)
  Das Gerät wendet die Regel auf MAC-Datenpakete mit beliebiger Zieladresse an.
- Gültige MAC-Adresse
  Das Gerät wendet die Regel auf MAC-Datenpakete mit der festgelegten Zieladresse an.
  Verwenden Sie das Zeichen `?` als Platzhalter.
  Beispiel `00:11:??:??:??:??`: Das Gerät wendet die Regel auf MAC-Datenpakete an, deren Zieladresse mit `00:11` beginnt.
- Gültige MAC-Adresse/Bitmaske
  Das Gerät wendet die Regel auf MAC-Datenpakete mit der festgelegten Quelladresse an. Die Bitmaske ermöglicht Ihnen, den Adressbereich bitgenau festzulegen.
  Beispiel `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`: Das Gerät wendet die Regel auf MAC-Datenpakete mit einer Zieladresse im Bereich von `00:11:22:33:44:54` bis `…:57` an.

Aktion

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

Mögliche Werte:

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

Protokolliere

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

Mögliche Werte:

- `markiert`
  Die Protokollierung ist aktiviert.
  Voraussetzung ist, dass Sie die Access-Control-Liste im Dialog *Netzsicherheit > ACL > Zuweisung* einem VLAN oder einem Port zuweisen.
  Das Gerät protokolliert in der Log-Datei im Intervall von 30 s, wie viele Male es eine Deny-Regel auf MAC-Datenpakete angewendet hat.
- `unmarkiert` (Voreinstellung)
  Die Protokollierung ist deaktiviert.

Das Gerät ermöglicht Ihnen, für bis zu 128 Deny-Regeln diese Funktion zu aktivieren.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

- Im Feld *Gruppenname* legen Sie den Namen der Access-Control-Liste fest, der die Regel angehört.
- Im Feld *Index* legen Sie die Nummer der Regel innerhalb der Access-Control-Liste fest. Enthält die Access-Control-Liste mehrere Regeln, wendet das Gerät die Regel mit dem kleinsten Wert zuerst an.

4.9.3 ACL Zuweisung

[Netzsicherheit > ACL > Zuweisung]

Dieser Dialog ermöglicht Ihnen, den Ports und VLANs des Geräts eine oder mehrere Access-Control-Listen zuzuweisen. Mit dem Zuweisen einer Priorität legen Sie die Reihenfolge der Abarbeitung fest, sofern Sie einem Port oder VLAN mehrere Access-Control-Listen zugewiesen haben.

Das Gerät wendet die Regeln nacheinander an, und zwar in der durch den Regelindex vorgegebenen Reihenfolge. Die Priorität einer Gruppe legen Sie in Spalte *Priorität*fest. Je kleiner die Zahl, desto höher die Priorität. Während der Bearbeitung wendet das Gerät die Regeln mit hoher Priorität vor Regeln mit niedriger Priorität an.

Beim Zuweisen der Access-Control-Listen zu Ports und VLANs ergeben sich folgende unterschiedliche ACL-Typen:
- Port-basierte IPv4-ACLs
- Port-basierte MAC-ACLs
- VLAN-basierte IPv4-ACLs
- VLAN-basierte MAC-ACLs

Das Gerät ermöglicht Ihnen, die Access-Control-Listen auf empfangene (`inbound`) Datenpakete anzuwenden.

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

Tabelle

Gruppenname

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

Typ

Zeigt, ob die Access-Control-Liste MAC-Regeln oder IPv4-Regeln enthält.

Mögliche Werte:

- *mac*
  Die Access-Control-Liste enthält MAC-Regeln.
- *ip*
  Die Access-Control-Liste enthält IPv4-Regeln.

Access-Control-Listen mit IPv4-Regeln bearbeiten Sie im Dialog *Netzsicherheit > ACL > IPv4-Regel*.
Access-Control-Listen mit MAC-Regeln bearbeiten Sie im Dialog *Netzsicherheit > ACL > MAC-Regel*.

Port

Zeigt den Port, dem die Access-Control-Liste zugewiesen ist. Das Feld bleibt leer, wenn die Access-Control-Liste einem VLAN zugewiesen ist.

VLAN-ID

Zeigt das VLAN, dem die Access-Control-Liste zugewiesen ist. Das Feld bleibt leer, wenn die Access-Control-Liste einem Port zugewiesen ist.

Richtung

Zeigt, dass das Gerät die Access-Control-Liste auf empfangene Datenpakete anwendet.

Priorität

Zeigt die Priorität der Access-Control-Liste.

Anhand der Priorität legen Sie die Reihenfolge fest, in welcher das Gerät die Regeln der Access-Control-Listen auf den Datenstrom anwendet. Das Gerät wendet die Regeln beginnend mit Priorität `1` in aufsteigender Reihenfolge an.

Mögliche Werte:

- `1..4294967295`

Wenn eine Access-Control-Liste mit derselben Priorität einem Port und einem VLAN zugewiesen ist, wendet das Gerät die Regeln zuerst auf dem Port an.

Aktiv

Zeigt, ob die Access-Control-Liste auf dem Port oder im VLAN aktiv ist.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Access-Control-Liste ist aktiv.
- `unmarkiert`
  Die Access-Control-Liste ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Öffnet den Dialog *Erzeugen*, um einem Port oder einem VLAN eine Regel zuzuweisen.

- Im Feld *Port/VLAN* legen Sie den Port oder die VLAN-ID fest.
- Im Feld *Priorität* legen Sie die Quell-MAC-Adresse der ARP-Regel fest.
- Im Feld *Richtung*legen Sie fest, auf welche Datenpakete das Gerät die Regel anwendet.
- Im Feld *Gruppenname* legen Sie fest, welche Regel das Gerät dem Port oder dem VLAN zuweist.

5 Switching

Das Menü enthält die folgenden Dialoge:
- Switching Global
- Lastbegrenzer
- Filter für MAC-Adressen
- IGMP-Snooping
- Time-Sensitive Networking
- MRP-IEEE
- GARP
- QoS/Priority
- VLAN
- L2-Redundanz

5.1 Switching Global

[Switching > Global]

Dieser Dialog ermöglicht Ihnen, folgende Einstellungen festzulegen:
- Aging-Time der Adresstabelle ändern
- Flusskontrolle im Gerät einschalten

Wenn in der Warteschlange eines Ports sehr viele Datenpakete gleichzeitig eintreffen, dann führt dies möglicherweise zum Überlaufen des Port-Speichers. Beispielsweise passiert dies dann, wenn das Gerät Daten auf einem Gigabit-Port empfängt und diese an einen Port mit niedrigerer Bandbreite weiterleitet. Das Gerät verwirft überschüssige Datenpakete.

Der in der Norm IEEE 802.3 beschriebene Flusskontrollmechanismus sorgt dafür, dass keine Datenpakete durch Überlaufen eines Portspeichers verloren gehen. Kurz bevor ein Portspeicher vollständig gefüllt ist, signalisiert das Gerät den angeschlossenen Geräten, dass es keine Datenpakete von ihnen mehr annimmt.
- Im Vollduplex-Betrieb sendet das Gerät ein Pause-Datenpaket.
- Im Halbduplex-Betrieb simuliert das Gerät eine Kollision.

Die angeschlossenen Geräte senden daraufhin so lange keine Datenpakete mehr, wie die Signalisierung andauert. Auf Uplink-Ports führt dies möglicherweise zu unerwünschten Sendepausen im übergeordneten Netzsegment („Wandering Backpressure“).

Konfiguration

MAC-Adresse

Zeigt die MAC-Adresse des Geräts.

Aging-Time [s]

Legt die Aging-Zeit in Sekunden fest.

Mögliche Werte:

- `10..500000` (Voreinstellung: `30`)

Das Gerät überwacht das Alter der gelernten Unicast-MAC-Adressen. Adresseinträge, die ein bestimmtes Alter (Aging-Zeit) überschreiten, löscht das Gerät aus seiner Adresstabelle.

Die Adresstabelle finden Sie im Dialog *Switching > Filter für MAC-Adressen*.

Flusskontrolle

Aktiviert/deaktiviert die Flusskontrolle im Gerät.

Mögliche Werte:

- `markiert`
  Die Flusskontrolle ist im Gerät aktiviert.
  Aktivieren Sie die Flusskontrolle zusätzlich auf den erforderlichen Ports. Siehe Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*, Kontrollkästchen in Spalte *Flusskontrolle*.
- `unmarkiert` (Voreinstellung)
  Die Flusskontrolle ist im Gerät deaktiviert.

Wenn Sie eine Redundanzfunktion einsetzen, dann deaktivieren Sie die Flusskontrolle auf den beteiligten Ports. Wenn die Flusskontrolle und die Redundanzfunktion gleichzeitig aktiv sind, arbeitet die Redundanzfunktion möglicherweise anders als beabsichtigt.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.2 Lastbegrenzer

[Switching > Lastbegrenzer]

Das Gerät ermöglicht Ihnen, den Datenverkehr an den Ports zu begrenzen, um auch bei hohem Datenverkehr einen stabilen Betrieb zu ermöglichen. Wenn der Verkehr an einem Port den eingegebenen Grenzwert überschreitet, dann verwirft das Gerät die Überlast auf diesem Port.

Die Lastbegrenzerfunktion arbeitet ausschließlich auf Schicht 2 und dient dem Zweck, Stürme von Datenpaketen, die das Gerät flutet, in ihrer Auswirkung zu begrenzen (typischerweise Broadcasts).

Die Lastbegrenzerfunktion ignoriert die Protokollinformationen höherer Schichten wie IP oder TCP.

Der Dialog enthält die folgenden Registerkarten:
- [Eingang]
- [Ausgang]

[Eingang]

In dieser Registerkarte schalten Sie die Funktion *Lastbegrenzer* ein. Der Grenzwert legt fest, welchen maximalen Verkehr der Port eingangsseitig vermittelt. Wenn der Verkehr auf dem Port den Grenzwert überschreitet, dann verwirft das Gerät die Überlast auf diesem Port.

Tabelle

Port

Zeigt die Nummer des Ports.

Grenzwert Einheit

Legt die Einheit für den Grenzwert fest:

Mögliche Werte:
- *Prozent* (Voreinstellung)
  Der Grenzwert ist festgelegt in Prozent der Datenrate des Ports.
- *pps*
  Der Grenzwert ist festgelegt in Datenpaketen pro Sekunde.

Broadcast-Modus

Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene Broadcast-Datenpakete.

Mögliche Werte:
- markiert
- unmarkiert (Voreinstellung)

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

Broadcast-Grenzwert

Legt den Grenzwert für empfangene Broadcasts auf diesem Port fest.

Mögliche Werte:

- `0..14880000` (Voreinstellung: `0`)
  Der Wert `0` deaktiviert die Lastbegrenzerfunktion auf diesem Port.
  - Wenn Sie in Spalte *Grenzwert Einheit* den Wert `Prozent` auswählen, dann geben Sie einen Prozentwert zwischen `1` und `100` ein.
  - Wenn Sie in Spalte *Grenzwert Einheit* den Wert `pps` auswählen, dann geben Sie einen Absolutwert für die Datenrate ein.

Modus f. Multicasts m. bekannter Zieladresse

Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene bekannte Multicast-Datenpakete.

Mögliche Werte:

- `markiert`
- `unmarkiert` (Voreinstellung)

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

Grenzwert f. Multicasts m. bekannter Zieladresse

Legt den Grenzwert für empfangene Multicasts auf diesem Port fest.

Mögliche Werte:

- `0..14880000` (Voreinstellung: `0`)
  Der Wert `0` deaktiviert die Lastbegrenzerfunktion auf diesem Port.
  - Wenn Sie in Spalte *Grenzwert Einheit* den Wert `Prozent` auswählen, dann geben Sie einen Prozentwert zwischen `0` und `100` ein.
  - Wenn Sie in Spalte *Grenzwert Einheit* den Wert `pps` auswählen, dann geben Sie einen Absolutwert für die Datenrate ein.

Modus f. Pakete m. unbekannter Zieladresse

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

Mögliche Werte:

- `markiert`
- `unmarkiert` (Voreinstellung)

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

Grenzwert f. Pakete m. unbekannter Zieladresse

Legt den Grenzwert für empfangene Unicasts mit unbekannter Zieladresse auf diesem Port fest.

Mögliche Werte:

- `0..14880000` (Voreinstellung: `0`)
  Der Wert `0` deaktiviert die Lastbegrenzerfunktion auf diesem Port.
  - Wenn Sie in Spalte *Grenzwert Einheit* den Wert `Prozent` auswählen, dann geben Sie einen Prozentwert zwischen `0` und `100` ein.
  - Wenn Sie in Spalte *Grenzwert Einheit* den Wert `pps` auswählen, dann geben Sie einen Absolutwert für die Datenrate ein.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Ausgang]

In dieser Registerkarte legen Sie die Übertragungsrate für den Ausgang des Ports fest.

Tabelle

Port

Zeigt die Nummer des Ports.

Bandbreite [%]

Legt die Ausgangs-Übertragungsrate fest.

Mögliche Werte:

- `0` (Voreinstellung)
  Die Bandbreitenbegrenzung ist ausgeschaltet.
- `1..100`
  Die Bandbreitenbegrenzung ist eingeschaltet.
  Der Wert legt die Prozentzahl der Gesamt-Verbindungsgeschwindigkeit für den Port in 1-%-Schritten fest.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.3 Filter für MAC-Adressen

[Switching > Filter für MAC-Adressen]

Dieser Dialog ermöglicht Ihnen, Adressfilter für die Adresstabelle anzuzeigen und zu bearbeiten. Adressfilter legen die Vermittlungsweise der Datenpakete im Gerät anhand der Ziel-MAC-Adresse fest.

Jede Zeile in der Tabelle stellt einen Filter dar. Das Gerät richtet die Filter automatisch ein. Das Gerät ermöglicht Ihnen, von Hand weitere Filter einzurichten.

Das Gerät vermittelt die Datenpakete wie folgt:

- Wenn die Tabelle einen Eintrag für die Zieladresse eines Datenpakets enthält, dann vermittelt das Gerät das Datenpaket vom Empfangsport an den im Tabelleneintrag angegebenen Port.
- Existiert kein Tabelleneintrag für die Zieladresse, vermittelt das Gerät das Datenpaket vom Empfangsport an jeden anderen Port.

Tabelle

Um die gelernten MAC-Adressen aus der Adresstabelle zu entfernen, klicken Sie im Dialog *Grundeinstellungen > Neustart* die Schaltfläche *MAC-Adresstabelle zurücksetzen*.

Adresse

Zeigt die Ziel-MAC-Adresse, für die der Tabelleneintrag gilt.

VLAN-ID

Zeigt die ID des VLANs, für das der Tabelleneintrag gilt.

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

Status

Zeigt, auf welche Weise das Gerät den Adressfilter eingerichtet hat.

Mögliche Werte:

- *learned*
  Adressfilter automatisch durch das Gerät eingerichtet anhand empfangener Datenpakete.
- *permanent*
  Adressfilter manuell eingerichtet. Der Adressfilter bleibt dauerhaft eingerichtet.
- *IGMP*
  Adressfilter automatisch eingerichtet durch IGMP-Snooping.
- *mgmt*
  MAC-Adresse des Geräts. Der Adressfilter ist gegen Veränderungen geschützt.
- *MRP-MMRP*
  Multicast-Adressfilter automatisch eingerichtet durch MMRP.
- *GMRP*
  Multicast-Adressfilter automatisch eingerichtet durch GMRP.

<Port-Nummer>

Zeigt, wie der betreffende Port Datenpakete vermittelt, die an nebenstehende Zieladresse adressiert sind.

Mögliche Werte:

- `-`
  Der Port vermittelt keine Datenpakete an die Zieladresse.
- `learned`
  Der Port vermittelt Datenpakete an die Zieladresse. Das Gerät hat den Filter anhand empfangener Datenpakete automatisch eingerichtet.
- `IGMP learned`
  Der Port vermittelt Datenpakete an die Zieladresse. Das Gerät hat den Filter anhand von IGMP automatisch eingerichtet.
- `unicast static`
  Der Port vermittelt Datenpakete an die Zieladresse. Ein Benutzer hat den Filter erzeugt.
- `multicast static`
  Der Port vermittelt Datenpakete an die Zieladresse. Ein Benutzer hat den Filter erzeugt.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

- Im Feld *Adresse* legen Sie die Ziel-MAC-Adresse fest.
- Im Feld *VLAN-ID* legen Sie die ID des VLANs fest.
- Im Feld *Port* legen Sie den Port fest.
  - Wählen Sie einen Port aus, wenn die Ziel-MAC-Adresse eine Unicast-Adresse ist.
  - Wählen Sie einen oder mehrere Ports aus, wenn die Ziel-MAC-Adresse eine Multicast-Adresse ist.
  - Wählen Sie keinen Port aus, um einen Discard-Filter einzurichten. Das Gerät verwirft Datenpakete mit der im Tabelleneintrag angegebenen Ziel-MAC-Adresse.

MAC-Adresstabelle zurücksetzen

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

5.4 IGMP-Snooping

[Switching > IGMP-Snooping]

Das Internet Group Management Protocol (IGMP) ist ein Protokoll für das dynamische Verwalten von Multicast-Gruppen. Das Protokoll beschreibt das Vermitteln von Multicast-Datenpaketen zwischen Routern und Endgeräten auf Schicht 3.

Das Gerät ermöglicht Ihnen, mit der IGMP-Snooping-Funktion die IGMP-Mechanismen auch auf Schicht 2 zu nutzen:

- Ohne IGMP-Snooping vermittelt das Gerät die Multicast-Datenpakete an jeden Port.
- Mit aktivierter IGMP-Snooping-Funktion vermittelt das Gerät die Multicast-Datenpakete ausschließlich an Ports, an denen Multicast-Empfänger angeschlossen sind. Dies reduziert die Netzlast. Das Gerät wertet die auf Schicht 3 übertragenen IGMP-Datenpakete aus und wendet die Informationen auf Schicht 2 an.

Aktivieren Sie die IGMP-Snooping-Funktion erst, wenn folgende Voraussetzungen erfüllt sind:

- Im Netz ist ein Multicast-Router vorhanden, der IGMP-Queries (periodische Anfragen) erzeugt.
- Die am IGMP-Snooping beteiligten Geräte im Netz leiten die IGMP-Queries weiter.

Das Gerät verknüpft die IGMP-Reports mit den Einträgen in seiner Adresstabelle. Tritt ein Multicast-Empfänger einer Multicast-Gruppe bei, erzeugt das Gerät für diesen Port einen Tabelleneintrag im Dialog *Switching > Filter für MAC-Adressen*. Verlässt der Multicast-Empfänger die Multicast-Gruppe, entfernt das Gerät den Tabelleneintrag wieder.

Das Menü enthält die folgenden Dialoge:

- IGMP-Snooping Global
- IGMP-Snooping Konfiguration
- IGMP-Snooping Erweiterungen
- IGMP Snooping-Querier
- IGMP Snooping Multicasts

5.4.1 IGMP-Snooping Global

[Switching > IGMP-Snooping > Global]

Dieser Dialog ermöglicht Ihnen, das *IGMP-Snooping*-Protokoll im Gerät einzuschalten sowie pro Port und pro VLAN zu konfigurieren.

Funktion

Funktion

Schaltet die Funktion *IGMP-Snooping* im Gerät ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *IGMP-Snooping* ist im Gerät eingeschaltet gemäß RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) und Multicast Listener Discovery (MLD) Snooping Switches).
- `Aus` (Voreinstellung)
  Die Funktion *IGMP-Snooping* ist im Gerät ausgeschaltet.
  Das Gerät vermittelt empfangene Query-, Report- und Leave-Datenpakete, ohne sie auszuwerten. Empfangene Datenpakete mit Multicast-Zieladresse vermittelt das Gerät an jeden Port.

Information

Verarbeitete Multicast-Control-Pakete

Zeigt die Anzahl der verarbeiteten Multicast-Kontroll-Datenpakete.

Diese Statistik umfasst folgende Paketarten:

- IGMP-Reports
- IGMP-Queries Version V1
- IGMP-Queries Version V2
- IGMP-Queries Version V3
- IGMP-Queries mit falscher Version
- PIM- oder DVMRP-Pakete

Das Gerät verwendet die Multicast-Kontroll-Datenpakete für die Erstellung der Adresstabelle zur Vermittlung der Multicast-Datenpakete.

Mögliche Werte:

- `0..2^31-1`

Mit der Schaltfläche *IGMP-Snooping-Daten zurücksetzen* im Dialog *Grundeinstellungen > Neustart* oder mit dem Kommando `clear igmp-snooping` im Command Line Interface setzen Sie die IGMP-Snooping-Einträge zurück, inklusive des Zählers für die verarbeiteten Multicast-Kontroll-Datenpakete.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

IGMP-Snooping-Zähler zurücksetzen

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

5.4.2 IGMP-Snooping Konfiguration

[Switching > IGMP-Snooping > Konfiguration]

Dieser Dialog ermöglicht Ihnen, die Funktion *IGMP-Snooping* im Gerät einzuschalten sowie pro Port und pro VLAN zu konfigurieren.

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

[VLAN-ID]

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

Tabelle

VLAN-ID

Zeigt die ID des VLANs, für das der Tabelleneintrag gilt.

Aktiv

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

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

Mögliche Werte:

- `markiert`
  IGMP-Snooping ist für dieses VLAN aktiviert. Das VLAN ist am Multicast-Datenstrom angemeldet.
- `unmarkiert` (Voreinstellung)
  IGMP-Snooping ist für dieses VLAN deaktiviert. Das VLAN ist vom Multicast-Datenstrom abgemeldet.

Group-Membership-Intervall

Legt die Zeit in Sekunden fest, in der ein VLAN aus einer dynamischen Multicast-Gruppe in der Adresstabelle eingetragen bleibt, wenn das Gerät keine Report-Datenpakete mehr von dem VLAN empfängt.

Legen Sie den Wert größer fest als den Wert in Spalte *Max. Antwortzeit*.

Mögliche Werte:

- `2..3600` (Voreinstellung: `260`)

Max. Antwortzeit

Legt die Zeit in Sekunden fest, in der die Mitglieder einer Multicast-Gruppe auf ein Query-Datenpaket antworten. Die Mitglieder wählen für ihre Antwort einen zufälligen Zeitpunkt innerhalb der Antwortzeit (Response Time) aus. Damit helfen Sie, zu verhindern, dass die Multicast-Gruppen-Mitglieder gleichzeitig auf den Query antworten.

Legen Sie den Wert kleiner fest als den Wert in Spalte *Group-Membership-Intervall*.

Mögliche Werte:

- `1..25` (Voreinstellung: `10`)

Fast-Leave-Admin-Modus

Aktiviert/deaktiviert die Fast-Leave-Funktion für dieses VLAN.

Mögliche Werte:

- `markiert`
  Wenn die Fast-Leave-Funktion eingeschaltet ist und das Gerät eine IGMP-Leave-Nachricht aus einer Multicast-Gruppe erhält, entfernt es sofort den Eintrag aus seiner Adresstabelle.
- `unmarkiert` (Voreinstellung)
  Bei ausgeschalteter Fast-Leave-Funktion sendet das Gerät zuerst MAC-basierte Queries an die Mitglieder der Multicast-Gruppe und entfernt einen Eintrag erst dann, wenn ein VLAN keine Report-Nachrichten mehr sendet.

MRP-Ablaufzeit

Multicast-Router-Present-Ablaufzeit. Legt die Zeit in Sekunden fest, in der das Gerät auf einen Query auf diesem Port, der einem VLAN angehört, wartet. Empfängt der Port kein Query-Datenpaket, entfernt das Gerät den Port aus der Liste der Ports mit angeschlossenen Multicast-Routern.

Den Parameter können Sie ausschließlich dann konfigurieren, wenn der Port einem bestehenden VLAN angehört.

Mögliche Werte:

- `0`
  unbegrenztes Time-Out, keine Ablaufzeit
- `1..3600` (Voreinstellung: `260`)

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Port]

In dieser Registerkarte konfigurieren Sie die Funktion *IGMP-Snooping* für jeden Port.

Tabelle

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert die Funktion *IGMP-Snooping* für diesen Port.

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

Mögliche Werte:

- `markiert`
  IGMP-Snooping ist auf diesem Port eingeschaltet. Der Port ist für den Multicast-Datenstrom angemeldet.
- `unmarkiert` (Voreinstellung)
  IGMP-Snooping ist auf diesem Port ausgeschaltet. Der Port ist vom Multicast-Datenstrom abgemeldet.

Group-Membership-Intervall

Legt die Zeit in Sekunden fest, in der ein Port aus einer dynamischen Multicast-Gruppe in der Adresstabelle eingetragen bleibt, wenn das Gerät keine Report-Datenpakete mehr von dem Port empfängt.

Mögliche Werte:

- `2..3600` (Voreinstellung: `260`)

Wählen Sie den Wert im größer als den Wert in Spalte *Max. Antwortzeit*.

Max. Antwortzeit

Legt die Zeit in Sekunden fest, in der die Mitglieder einer Multicast-Gruppe auf ein Query-Datenpaket antworten. Die Mitglieder wählen für ihre Antwort einen zufälligen Zeitpunkt innerhalb der Antwortzeit (Response Time) aus. Damit helfen Sie, zu verhindern, dass die Multicast-Gruppen-Mitglieder gleichzeitig auf den Query antworten.

Mögliche Werte:

- `1..25` (Voreinstellung: `10`)

Wählen Sie den Wert kleiner als den Wert in Spalte *Group-Membership-Intervall*.

MRP-Ablaufzeit

Legt die Multicast-Router-Present-Ablaufzeit fest. Die MRP-Ablaufzeit ist die Zeit in Sekunden, in der das Gerät auf ein Query-Datenpaket auf diesem Port wartet. Empfängt der Port kein Query-Datenpaket, entfernt das Gerät den Port aus der Liste der Ports mit angeschlossenen Multicast-Routern.

Mögliche Werte:

- `0`
  unbegrenztes Time-Out, keine Ablaufzeit
- `1..3600` (Voreinstellung: `260`)

Fast-Leave-Admin-Modus

Aktiviert/deaktiviert die Fast-Leave-Funktion für diesen Port.

Mögliche Werte:

- `markiert`
  Wenn die Fast-Leave-Funktion eingeschaltet ist und das Gerät eine IGMP-Leave-Nachricht aus einer Multicast-Gruppe erhält, entfernt es sofort den Eintrag aus seiner Adresstabelle.
- `unmarkiert` (Voreinstellung)
  Bei ausgeschalteter Fast-Leave-Funktion sendet das Gerät zuerst MAC-basierte Queries an die Mitglieder der Multicast-Gruppe und entfernt einen Eintrag dann, wenn ein Port keine Report-Nachrichten mehr sendet.

Static-Query-Port

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

Mögliche Werte:

- `markiert`
  Der *Static-Query-Port*-Modus ist aktiv.
  Der Port ist ein statischer Query-Port in den eingerichteten VLANs.
  Wenn Sie die Funktion *Redundant Coupling Protocol* verwenden und das Gerät als Slave arbeitet, dann verwenden Sie nicht den *Static-Query-Port*-Modus für die Ports am sekundären Ring/Netz.
- `unmarkiert` (Voreinstellung)
  Der *Static-Query-Port*-Modus ist inaktiv.
  Der Port ist kein statischer Query-Port. Das Gerät vermittelt IGMP-Report-Nachrichten ausschließlich dann an den Port, wenn es IGMP-Queries empfängt.

VLAN-IDs

Zeigt die ID der VLANs, für die der Tabelleneintrag gilt.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.4.3 IGMP-Snooping Erweiterungen

[Switching > IGMP-Snooping > Snooping Erweiterungen]

Dieser Dialog ermöglicht Ihnen, für eine VLAN-ID einen Port auszuwählen und den Port zu konfigurieren.

Tabelle

VLAN-ID

Zeigt die ID des VLANs, für das der Tabelleneintrag gilt.

<Port-Nummer>

Zeigt für jedes im Gerät eingerichtete VLAN, ob der betreffende Port ein Query-Port ist. Außerdem zeigt das Feld, ob das Gerät jeden Multicast-Stream im VLAN an diesen Port vermittelt.

Mögliche Werte:

- `-`
  Der Port ist in diesem VLAN kein Query-Port.
- `L`= Learned
  Das Gerät hat den Port als Query-Port erkannt, weil der Port IGMP-Queries in diesem VLAN empfangen hat. Der Port ist kein statisch konfigurierter Query-Port.
- `A`= Automatic
  Das Gerät hat den Port als Query-Port erkannt. Voraussetzung ist, dass der Port als *`Learn by LLDP`*konfiguriert ist.
- `S`= Static (einstellbar)
  Ein Benutzer hat den Port als statischen Query-Port konfiguriert. Das Gerät vermittelt IGMP-Reports ausschließlich an Ports, an denen es zuvor IGMP-Queries empfangen hat – und an statisch konfigurierte Query-Ports.
  Um diesen Wert zuzuweisen, führen Sie die folgenden Schritte aus:
  - ☐ Öffnen Sie das Fenster *Wizard*.
  - ☐ Markieren Sie im Dialog *Konfiguration* das Kontrollkästchen *`Static`*.
- `P`= Learn by LLDP (einstellbar)
  Ein Benutzer hat den Port als *`Learn by LLDP`*konfiguriert.
  Mit dem Link Layer Discovery Protocol (LLDP) erkennt das Gerät direkt an den Port angeschlossene Schneider Electric-Geräte. Erkannte Query-Ports kennzeichnet das Gerät mit `A`.
  Um diesen Wert zuzuweisen, führen Sie die folgenden Schritte aus:
  - ☐ Öffnen Sie das Fenster *Wizard*.
  - ☐ Markieren Sie im Dialog *Konfiguration* das Kontrollkästchen *`Learn by LLDP`*.
- `F`= Forward All (einstellbar)
  Ein Benutzer hat den Port so konfiguriert, dass das Gerät sämtliche empfangene Multicast-Streams in diesem VLAN an diesen Port vermittelt. Diese Einstellung ist zum Beispiel für Diagnosezwecke geeignet.
  Um diesen Wert zuzuweisen, führen Sie die folgenden Schritte aus:
  - ☐ Öffnen Sie das Fenster *Wizard*.
  - ☐ Markieren Sie im Dialog *Konfiguration* das Kontrollkästchen *`Forward all`*.

Display categories

Erhöht die Übersichtlichkeit der Anzeige. Die Tabelle hebt Zellen hervor, die den ausgewählten Wert enthalten. Dies erleichtert das bedarfsgerechte Analysieren und Sortieren der Tabelle.

- *Learned (L)*
  Die Tabelle zeigt Zellen, die den Wert `L` und gegebenenfalls weitere mögliche Werte enthalten. Zellen, die ausschließlich andere Werte als `L` enthalten, zeigt die Tabelle mit dem Zeichen "`-`".
- *Static (S)*
  Die Tabelle zeigt Zellen, die den Wert `S` und gegebenenfalls weitere mögliche Werte enthalten. Zellen, die ausschließlich andere Werte als `S` enthalten, zeigt die Tabelle mit dem Zeichen "`-`".
- *Automatic (A)*
  Die Tabelle zeigt Zellen, die den Wert `A` und gegebenenfalls weitere mögliche Werte enthalten. Zellen, die ausschließlich andere Werte als `A` enthalten, zeigt die Tabelle mit dem Zeichen "`-`".
- *Learned by LLDP (P)*
  Die Tabelle zeigt Zellen, die den Wert `P` und gegebenenfalls weitere mögliche Werte enthalten. Zellen, die ausschließlich andere Werte als `P` enthalten, zeigt die Tabelle mit dem Zeichen "`-`".
- *Forward all (F)*
  Die Tabelle zeigt Zellen, die den Wert `F` und gegebenenfalls weitere mögliche Werte enthalten. Zellen, die ausschließlich andere Werte als `F` enthalten, zeigt die Tabelle mit dem Zeichen "`-`".

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen" auf Seite 17.

Öffnet das Fenster *Wizard*, das Ihnen beim Auswählen und Einstellen der Ports hilft.

[Selection VLAN/Port (Wizard)]

Im Dialog *Selection VLAN/Port* weisen Sie einem Port eine VLAN-ID zu.

Im Dialog *Konfiguration* legen Sie die Einstellungen des Ports fest.

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

[Selection VLAN/Port (Wizard) – Selection VLAN/Port]

VLAN-ID

Auswahl der ID des VLANs.

Mögliche Werte:

- `1..4042`

Port

Auswahl des Ports.

Mögliche Werte:

- `<Port-Nummer>`

[Selection VLAN/Port (Wizard) – Konfiguration]

VLAN-ID

Zeigt die ID des ausgewählten VLANs.

Port

Zeigt die Nummer des ausgewählten Ports.

Static

Legt den Port als statischen Query-Port in den eingerichteten VLANs fest. Das Gerät überträgt IGMP-Benachrichtigungen ausschließlich an die Ports, an denen es IGMP-Queries empfängt. Dies ermöglicht Ihnen, IGMP-Benachrichtigungen auch an andere ausgewählte Ports oder angeschlossene Schneider Electric-Geräte (`Automatic`) zu senden.

Learn by LLDP

Legt den Status *`Learn by LLDP`* für den Port fest. Ermöglicht dem Gerät, direkt verbundene Schneider Electric-Geräte mit LLDP zu erkennen und die betreffenden Ports als Query-Port zu lernen.

Forward all

Legt den Status *`Forward all`* für den Port fest. Mit der Einstellung *`Forward all`* sendet das Gerät auf diesem Port jedes Datenpaket mit einer Multicast-Adresse im Zieladressfeld.

5.4.4 IGMP Snooping-Querier

[Switching > IGMP-Snooping > Querier]

Das Gerät ermöglicht Ihnen, einen Multicast-Stream ausschließlich an die Ports zu vermitteln, an denen ein Multicast-Empfänger angeschlossen ist.

Um zu ermitteln, an welchen Ports Multicast-Empfänger angeschlossen sind, sendet das Gerät in einem einstellbaren Intervall Query-Datenpakete an die Ports. Ist ein Multicast-Empfänger angeschlossen, meldet er sich für den Multicast-Stream an, indem er dem Gerät mit einem Report-Datenpaket antwortet.

Dieser Dialog ermöglicht Ihnen, die Snooping-Querier-Einstellungen global und für die eingerichteten VLANs zu konfigurieren.

Funktion

Funktion

Schaltet die IGMP-Querier-Funktion im Gerät global ein/aus.

Mögliche Werte:

- *An*
- *Aus* (Voreinstellung)

Konfiguration

In diesem Rahmen legen Sie die IGMP-Snooping-Querier-Einstellungen für die General-Query-Datenpakete fest.

Protokoll-Version

Legt die IGMP-Version der General-Query-Datenpakete fest.

Mögliche Werte:

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

Query-Intervall [s]

Legt die Zeitspanne in Sekunden fest, nach der das Gerät selbst General-Query-Datenpakete generiert, wenn es Query-Datenpakete vom Multicast-Router empfangen hat.

Mögliche Werte:

- `1..1800` (Voreinstellung: `60`)

Ablauf-Intervall [s]

Legt die Zeitspanne in Sekunden fest, nach der ein aktiver Querier aus dem Passivzustand wieder in den Aktivzustand wechselt, wenn er länger als hier festgelegt keine Query-Pakete empfängt.

Mögliche Werte:

- `60..300` (Voreinstellung: `125`)

Tabelle

In der Tabelle legen Sie die Snooping-Querier-Einstellungen für die eingerichteten VLANs fest.

VLAN-ID

Zeigt die ID des VLANs, für das der Tabelleneintrag gilt.

Aktiv

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

Mögliche Werte:

- `markiert`
  Die IGMP-Snooping-Querier-Funktion ist für dieses VLAN aktiv.
- `unmarkiert` (Voreinstellung)
  Die IGMP-Snooping-Querier-Funktion ist für dieses VLAN deaktiviert.

Momentaner Zustand

Zeigt, ob der Snooping-Querier in diesem VLAN aktiv ist.

Mögliche Werte:

- `markiert`
  Der Snooping-Querier ist in diesem VLAN aktiv.
- `unmarkiert`
  Der Snooping-Querier ist in diesem VLAN inaktiv.

Adresse

Legt die IP-Adresse fest, die das Gerät als Absenderadresse in generierte Datenpakete mit allgemeinen Abfragen einfügt. Verwenden Sie die Adresse des Multicast-Routers.

Mögliche Werte:

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

Protokoll-Version

Zeigt die IGMP-Protokoll-Version der General-Query-Datenpakete.

Mögliche Werte:

- `1`
  IGMP v1
- `2`
  IGMP v2
- `3`
  IGMP v3

Max. Antwortzeit

Zeigt die Zeit in Sekunden, in der die Mitglieder einer Multicast-Gruppe auf ein Query-Datenpaket antworten. Die Mitglieder wählen für ihre Antwort einen zufälligen Zeitpunkt innerhalb der Antwortzeit (Response Time) aus. Dies hilft, zu vermeiden, dass jedes Multicast-Gruppen-Mitglied gleichzeitig auf den Query antwortet.

Letzte Querier-Adresse

Zeigt die IP-Adresse des Multicast-Routers, von dem die letzte eingegangene IGMP-Abfrage (Querier) ausging.

Letzte Querier-Version

Zeigt die IGMP-Version, die der Multicast-Router beim Aussenden der letzten in diesem VLAN eingegangenen IGMP-Abfrage (Querier) verwendete.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.4.5 IGMP Snooping Multicasts

[Switching > IGMP-Snooping > Multicasts]

Das Gerät ermöglicht Ihnen, festzulegen, wie es Datenpakete unbekannter Multicast-Adressen vermittelt: Entweder verwirft das Gerät diese Datenpakete, flutet sie an jeden Port oder vermittelt sie ausschließlich an die Ports, die zuvor Query-Pakete empfangen haben.

Das Gerät ermöglicht Ihnen außerdem, die Datenpakete bekannter Multicast-Adressen an die Query-Ports zu vermitteln.

Konfiguration

Unbekannte Multicasts

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

Mögliche Werte:

- *discard*
  Das Gerät verwirft Datenpakete mit unbekannter MAC-/IP-Multicast-Adresse.
- *flood* (Voreinstellung)
  Das Gerät vermittelt Datenpakete mit unbekannter MAC-/IP-Multicast-Adresse an jeden Port.

Tabelle

In der Tabelle legen Sie die Einstellungen für bekannte Multicasts für die eingerichteten VLANs fest.

VLAN-ID

Zeigt die ID des VLANs, für das der Tabelleneintrag gilt.

Bekannte Multicasts

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

Mögliche Werte:

- *an Query- und registrierte Ports senden*
  Das Gerät vermittelt Datenpakete mit unbekannter MAC-/IP-Multicast-Adresse an die Query-Ports und an registrierte Ports.
- *an registrierte Ports senden* (Voreinstellung)
  Das Gerät vermittelt Datenpakete mit unbekannter MAC-/IP-Multicast-Adresse an registrierte Ports.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.5 Time-Sensitive Networking

[Switching > TSN]

Das Menü enthält die folgenden Dialoge:

- TSN Konfiguration
- TSN Gate Control List

5.5.1 TSN Konfiguration

[Switching > TSN > Konfiguration]

In diesem Dialog schalten Sie die Funktion *TSN* ein-/aus und legen die Zeit-Einstellungen fest.

Das Gerät unterstützt das in IEEE 802.1 Qbv definierte Time-aware Queuing. Diese Funktion *TSN* ermöglicht den TSN-fähigen Ports, die Datenpakete jeder Verkehrsklasse planmäßig zu übertragen – relativ zu einem definierten Zyklus in der Gate-Control-Liste. Das VLAN-Tag eines Ethernet-Pakets – oder die Port-Priorität bei einem unmarkierten Paket – enthält die Priorität.

Diese Funktion hilft, Latenzzeiten und Stauverluste für reservierte Datenströme zu vermeiden. Die präzise Synchronisation der Zyklen und Gate-Zustände mittels IEEE1588 (PTP) ermöglicht eine staufreie, latenzarme Kommunikation. Voraussetzung ist, dass jedes Gerät im Netz IEEE 802.1 Qbv unterstützt.

Anmerkung: Im Gegensatz zum Command Line Interface wenden Sie die Einstellungen sofort an, sobald Sie die Schaltfläche ✓ klicken.

Funktion

Funktion

Schaltet die Funktion *TSN* im Gerät ein/aus.

Mögliche Werte:

- *An*
  Die Funktion *TSN* ist global eingeschaltet.
  Das Gerät verarbeitet Link-Local-Frames auf den TSN-fähigen Ports mit der Priorität der Verkehrsklasse`6`. Infolgedessen konkurrieren die Link-Local-Frames beim Weiterleiten mit anderen Datenpaketen, die dieselbe oder eine höhere Priorität haben. Dies betrifft die folgenden Frame-Typen:
  - RSTP
  - LLDP
  - IEEE 802.1AS
  - PTP Peer Delay
- *Aus* (Voreinstellung)
  Die Funktion *TSN* ist global ausgeschaltet.
  Wenn die Funktion *TSN* an einem Port aktiv ist, verwendet der Port die geöffneten Gates `0,1,2,3,4,5,6,7`. Diese Einstellung ist vom Hersteller voreingestellt.

Basiszeit

Datum
Zeit
[ns]

Legt den Zeitpunkt bezogen auf die UTC-Zeit fest, zu dem der Zyklus beginnt.

Das Gerät rechnet den Wert direkt in die PTP-Zeitskala um, ohne die Schaltsekunden zu berücksichtigen.

Mögliche Werte:

- `TT.MM.JJ`
  Tag.Monat.Jahr
  (abhängig von den Spracheinstellungen Ihres Web-Browsers)
- `hh:mm:ss`
  Stunde:Minute:Sekunde
- `0..999999999`
  Legt den zeitlichen Versatz in Nanosekunden fest.

Anmerkung: Wenn Sie die Basiszeit in der Zukunft festlegen, beginnt der Zyklus um so viele Sekunden früher wie im Feld *UTC-Offset [s]* festgelegt ist. Siehe Dialog *Zeit > PTP > Boundary Clock > Global*.

Konfiguration

Zyklus-Zeit [ns]

Legt die Dauer eines Zyklus in Nanosekunden fest.

Mögliche Werte:

- `50000..10000000` (Voreinstellung: `1000000`)
  50 µs .. 10 ms

Tabelle

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert die Funktion *TSN* auf dem Port.

Mögliche Werte:

- `markiert`
  Die Funktion *TSN* ist auf dem Port aktiv.
  Wenn Sie die Basiszeit in der Zukunft festlegen, beginnt der Zyklus zu dem im Rahmen *Basiszeit* festgelegten Zeitpunkt.
  Voraussetzung ist, dass die Funktion *PTP* eingeschaltet und das Gerät synchronisiert ist.
  Wenn die Funktion *TSN* global eingeschaltet ist, verwendet der Port den im Dialog *Switching > TSN > Gate Control List > Konfiguriert* festgelegten Zyklus.
- `unmarkiert` (Voreinstellung)
  Die Funktion *TSN* ist auf dem Port inaktiv.
  Wenn die Funktion *TSN* global eingeschaltet ist, verwendet der Port die geöffneten Gates `0,1,2,3,4,5,6,7`.

Port-Zustand

Zeigt den Zustand des Zyklus auf dem Port.

Mögliche Werte:

- *running*
  Der Zyklus wird ausgeführt.
  Der Port wendet den im Dialog *Switching > TSN > Gate Control List > Konfiguriert* festgelegten Zyklus an.
- *waitForTimeSync*
  Der Zyklus hat noch nicht begonnen.
  Die Uhr des Geräts ist nicht synchronisiert.
  Prüfen Sie die *PTP*-Einstellungen.
- *pending*
  Der Zyklus hat noch nicht begonnen.
  Die Basiszeit ist in der Zukunft festgelegt.
- *disabled*
  Der Zyklus wird nicht ausgeführt.
  Die Funktion *TSN* ist auf dem Port inaktiv.
  – Prüfen Sie die Einstellungen im Rahmen *Funktion*.
  – Prüfen Sie die Einstellungen in Spalte *Aktiv*.
  Der Port wendet die in Spalte *Standard-Gate-Zustände* festgelegten Gate-Zustände an.
- *error*
  Der Zyklus wird nicht ausgeführt.
  Ein Fehler wurde erkannt.

Letzter Aktivierungszeitpunkt

Zeigt den Zeitpunkt (Datum und Uhrzeit), zu dem die Zeiteinstellungen zum letzten Mal aktiv wurden.

Dieser Wert bezieht sich auf die PTP-Zeit.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.5.2 TSN Gate Control List

[Switching > TSN > Gate Control List]

Das Menü enthält die folgenden Dialoge:

- TSN Konfigurierte Gate Control List
- TSN Aktuelle Gate Control List

5.5.2.1 TSN Konfigurierte Gate Control List

[Switching > TSN > Gate Control List > Konfiguriert]

In diesem Dialog legen Sie für die TSN-fähigen Ports die Zeitschlitze des Zyklus fest. Mit Hinzufügen eines Tabelleneintrags legen Sie die geöffneten Gates und die Dauer des Zeitschlitzes fest.

Anmerkung: Im Gegensatz zum Command Line Interface wenden Sie die Einstellungen sofort an, sobald Sie die Schaltfläche ✓ klicken.

Der Dialog enthält die folgenden Registerkarten:

- Eine Registerkarte für jeden TSN-fähigen Port.
  Die Anzahl der TSN-fähigen Ports ist geräteabhängig.

[<Port-Nummer>]

Konfiguration

Status

Zeigt das Template, das der Gate-Control-Liste zugewiesen ist.

Mögliche Werte:

- `-`
  Kein Template. Der Gate-Control-Liste sind keine Einträge zugewiesen.
- *`default 2 time slots`*
  Template mit 3 Einträgen:
  - Erster Eintrag ist die Verkehrsklasse `7`.
  - Zweiter Eintrag ist die Verkehrsklasse `6` bis `0`.
  - Dritter Eintrag ist ein Schutzband.
- *`default 3 time slots`*
  Template mit 5 Einträgen:
  - Erster Eintrag ist die Verkehrsklasse `7`.
  - Zweiter Eintrag ist ein Schutzband.
  - Dritter Eintrag ist die Verkehrsklasse `6`.
  - Vierter Eintrag ist die Verkehrsklasse `5` bis `0`.
  - Fünfter Eintrag ist ein Schutzband.
- <`any other template name`>
  Das Template wurde mittels Command Line Interface zugewiesen.

Template

Öffnet das Fenster *Template*, um der Gate-Control-Liste ein anderes Template zuzuweisen. Wenn Sie ein anderes Template auswählen und die Schaltfläche *Ok* klicken, ersetzt das Gerät die Einträge in der Tabelle.

In der Dropdown-Liste wählen Sie eines der folgenden Templates aus:

- *`default 2 time slots`*
- *`default 3 time slots`*

Das Gerät ermöglicht, zusätzliche Templates mittels Command Line Interface zuzuweisen.

Löschen

Entfernt das Template, das der Gate-Control-Liste zugewiesen ist. Danach sind der Gate-Control-Liste keine Einträge mehr zugeordnet.

Tabelle

Index

Zeigt die Positionsnummer des Eintrags in der Gate-Control-Liste, welche die chronologische Reihenfolge der Zeitschlitze festlegt.

Gate-Zustände

Legt die geöffneten Gates für den Fall fest, dass die Funktion *TSN* auf dem Port aktiv ist.

- Für die Übertragung ausgewählt sind diejenigen Datenpakete, deren Verkehrsklasse einem ausgewählten Gate zugewiesen ist – Gate-Zustand OPEN.
- Nicht für die Übertragung ausgewählt sind diejenigen Datenpakete, deren Verkehrsklasse einem nicht-ausgewählten Gate zugewiesen ist – Gate-Zustand CLOSED.

Mögliche Werte:

▶ `-` (Voreinstellung)
Kein Gate ausgewählt.
Das Gerät öffnet während der Abarbeitung des Zeitschlitzes kein Gate auf dem Port. Heben Sie in der Dropdown-Liste für jedes Gate die Markierung auf.

▶ `0..7`
Das Gerät öffnet während der Abarbeitung des Zeitschlitzes die ausgewählten Gates auf dem Port. Wählen Sie in der Dropdown-Liste ein oder mehrere Gates.
Die VLAN-Prioritäten weisen Sie im Dialog *Switching > QoS/Priority > 802.1D/p Zuweisung* einer Verkehrsklasse zu.

Intervall [ns]

Legt die Dauer des Zeitschlitzes in Nanosekunden fest.

Mögliche Werte:

▶ `1000..10000000`

Beachten Sie beim Festlegen der Dauer der Zeitschlitze folgende Rahmenbedingungen:

- Einzelner Zeitschlitz
  - Vergewissern Sie sich, dass ein Zeitschlitz mindestens so lang ist, dass der Port das längste zu erwartende Datenpaket übertragen kann.
  - Vergewissern Sie sich, dass ein Zeitschlitz kürzer oder gleich der Zyklus-Dauer ist.
- Summe der festgelegten Zeitschlitze
  - Wir empfehlen, dass die Summe der Zeitschlitze gleich der Zyklus-Dauer ist.
  - Wenn die Summe die Zyklus-Dauer überschreitet, dann werden die überlappenden Zeitschlitze verworfen und der Zyklus startet neu.
  - Wenn die Summe kleiner als die Zyklus-Dauer ist, dann wird das Intervall des letzten Zeitschlitzes verlängert, um es in den Zyklus einzupassen.

Anmerkung: Abweichungen zwischen den festgelegten Zeitschlitzen und der Zyklus-Dauer sind im Dialog *Switching > TSN > Gate Control List > Aktuell* nicht hervorgehoben.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.5.2.2 TSN Aktuelle Gate Control List

[Switching > TSN > Gate Control List > Aktuell]

In diesem Dialog überwachen Sie die gegenwärtigen Einstellungen des Zyklus für die TSN-fähigen Ports. Jeder Tabelleneintrag repräsentiert einen festgelegten Zeitschlitz.

Wenn der Zeitpunkt des Zyklus-Beginns (*Basiszeit*) in der Zukunft liegt, unterscheiden sich die angezeigten Werte von den im Dialog *Switching > TSN > Gate Control List > Konfiguriert* festgelegten Werten.

Im Dialog *Switching > TSN > Konfiguration* zeigt die Spalte *Port-Zustand*, ob der Zyklus auf einem Port aktiv ist.

Der Dialog enthält die folgenden Registerkarten:
- Eine Registerkarte für jeden TSN-fähigen Port.
  Die Anzahl der TSN-fähigen Ports ist geräteabhängig.

[<Port-Nummer>]

Tabelle

Index

Zeigt die Positionsnummer des Eintrags in der Gate-Control-Liste, welche die chronologische Reihenfolge der Zeitschlitze festlegt.

Gate-Zustände

Zeigt die geöffneten Gates für den Fall, dass die Funktion *TSN* auf dem Port aktiv ist.

Intervall [ns]

Zeigt die Dauer des Zeitschlitzes in Nanosekunden.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.6 MRP-IEEE

[Switching > MRP-IEEE]

Die Erweiterung IEEE 802.1ak der Norm IEEE 802.1Q führte das Multiple Registration Protocol (MRP) als Ersatz für das Generic Attribute Registration Protocol (GARP) ein. Zudem änderte und ersetzte das IEEE die GARP-Anwendungen, das GARP Multicast Registration Protocol (GMRP) und das GARP VLAN Registration Protocol (GVRP). Das Multiple MAC Registration Protocol (MMRP) und das Multiple VLAN Registration Protocol (MVRP) ersetzen diese Protokolle.

MRP-IEEE hilft, den Verkehr auf die erforderlichen Bereiche des LANs zu begrenzen. Um den Verkehr zu begrenzen, verteilen die MRP-IEEE-Anwendungen Attribut-Werte an teilnehmende MRP-IEEE-Geräte innerhalb eines LANs, wobei sie Multicast-Gruppen-Mitgliedschaften und VLAN-Kennungen registrieren und deregistrieren.

Die Registrierung von Gruppen-Teilnehmern ermöglicht Ihnen, Ressourcen für bestimmte Daten im LAN zu reservieren. Die Festlegung der Ressourcen-Anforderungen reguliert den Grad des Verkehrs und ermöglicht den Geräten, die erforderlichen Ressourcen zu ermitteln und für die dynamische Verwaltung der zugeordneten Ressourcen bereitzustellen.

Das Menü enthält die folgenden Dialoge:

- MRP-IEEE Konfiguration
- MRP-IEEE Multiple MAC Registration Protocol
- MRP-IEEE Multiple VLAN Registration Protocol

5.6.1 MRP-IEEE Konfiguration

[Switching > MRP-IEEE > Konfiguration]

Dieser Dialog ermöglicht Ihnen, die verschiedenen MRP-Timer einzurichten. Mit der Aufrechterhaltung einer Beziehung zwischen den verschiedenen Timer-Werten arbeitet das Protokoll effizient bei geringerer Wahrscheinlichkeit von unnötigen Attributrücknahmen und erneuten Registrierungen. Die voreingestellten Timer-Werte erhalten wirksam diese Beziehungen.

Erhalten Sie folgende Beziehungen aufrecht, wenn Sie die Timer neu konfigurieren:
- Für eine erneute Registrierung nach einem Leave- oder LeaveAll-Ereignis legen Sie – auch im Fall einer verlorenen Nachricht – den Wert für LeaveTime fest auf: `≥ (2x JoinTime) + 60`.
- Um das Volumen des nach einem LeaveAll-Ereignis neu hinzukommenden Verkehrs zu minimieren, legen Sie für den LeaveAll-Timer einen Wert fest, der höher ist als der LeaveTime-Wert.

Tabelle

Port

Zeigt die Nummer des Ports.

Join-Time [1/100s]

Legt den Join-Timer fest, der den Intervall zwischen den Vermittlungsmöglichkeiten überwacht, die auf die Applicant-State-Machine angewendet werden.

Mögliche Werte:
- `10..100` (Voreinstellung: `20`)

Leave-Time [1/100s]

Legt den Leave-Timer fest, der die Zeitspanne überwacht, in der die Registrar-State-Machine im Leave(LV)-Zustand bleibt, bevor er in den Empty(MT)-Zustand wechselt.

Mögliche Werte:
- `20..600` (Voreinstellung: `60`)

Leave-all-Time [1/100s]

Legt den LeaveAll-Timer fest, der die Frequenz überwacht, mit welcher die LeaveAll-State-Machine LeaveAll-PDUs erzeugt.

Mögliche Werte:
- `200..6000` (Voreinstellung: `1000`)

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.6.2 MRP-IEEE Multiple MAC Registration Protocol

[Switching > MRP-IEEE > MMRP]

Das Multiple MAC Registration Protocol (MMRP) ermöglicht Endgeräten und MAC-Switches das Registrieren und Deregistrieren von Gruppen-Mitgliedschaften und individuellen MAC-Adressen-Informationen in Switches, die sich im selben LAN befinden. Die Switches im LAN verteilen die Information über Switches, die erweiterte Filter-Dienste unterstützen. MMRP ermöglicht Ihnen, mit Hilfe der MAC-Adressen-Informationen den Multicast-Verkehr auf die erforderlichen Bereiche des Schicht-2-Netzes zu begrenzen.

Die Arbeitsweise von MMRP verdeutlicht das Beispiel einer Sicherheitskamera, die von einem Mast aus ein Gebäude überwacht. Die Kamera sendet Multicast-Pakete an ein LAN. Für die Überwachung haben Sie 2 Endgeräte an unterschiedlichen Orten installiert. Sie melden die MAC-Adressen der Kamera und die 2 Endgeräte in derselben Multicast-Gruppe an. Dann legen Sie die MMRP-Einstellungen an den Ports zum Senden der Multicast-Gruppen-Pakete an die 2 Endgeräte fest.

Der Dialog enthält die folgenden Registerkarten:
- [Konfiguration]
- [Service-Requirement]
- [Statistiken]

[Konfiguration]

In dieser Registerkarte wählen Sie aktive MMRP-Port-Teilnehmer und stellen das Gerät so ein, dass es periodische Ereignisse überträgt. Der Dialog ermöglicht Ihnen außerdem, das Broadcasting der im VLAN registrierten MAC-Adressen einzuschalten.

Für jeden Port exisitert eine Periodic-State-Machine, die regelmäßig periodische Ereignisse an die mit aktiven Ports verbundenen Applicant-State-Machines überträgt. Periodische Ereignisse enthalten Informationen, die über den Status der mit dem aktiven Port verbundenen Geräte informieren.

Funktion

Funktion

Aktiviert/deaktiviert die globale Funktion *MMRP* des Geräts. Das Gerät nimmt am Austausch von MMRP-Nachrichten teil.

Mögliche Werte:

- *An*
  Das Gerät ist normaler Teilnehmer beim Austausch von MMRP-Nachrichten.
- *Aus* (Voreinstellung)
  Das Gerät ignoriert MMRP-Nachrichten.

Konfiguration

Periodische State-Machine

Schaltet die globale Periodic-State-Machine im Gerät ein/aus.

Mögliche Werte:

- *An*
  Bei global eingeschalteter MMRP-*Funktion* überträgt das Gerät MMRP-Nachrichten im Intervall von 1 Sekunde an die an MMRP teilnehmenden Ports.
- *Aus* (Voreinstellung)
  Deaktiviert die Periodic-State-Machine im Gerät.

Tabelle

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert die Teilnahme des Ports an MMRP.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Bei global und auf diesem Port eingeschaltetem MMRP sendet und empfängt das Gerät MMRP-Nachrichten auf diesem Port.
- `unmarkiert`
  Deaktiviert die Teilnahme des Ports an MMRP.

Eingeschränkte Gruppen-Registrierung

Aktiviert/deaktiviert die Begrenzung der dynamischen Registrierung von MAC-Adressen mittels MMRP an dem Port.

Mögliche Werte:

- `markiert`
  Wenn die Funktion eingeschaltet ist und im VLAN ein statischer Filtereintrag für die MAC-Adresse vorhanden ist, ermöglicht das Gerät, die MAC-Adressattribute dynamisch zu registrieren.
- `unmarkiert` (Voreinstellung)
  Aktiviert/deaktiviert die Begrenzung der dynamischen Registrierung von MAC-Adressen mittels MMRP an dem Port.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Service-Requirement]

Diese Registerkarte enthält für jedes aktive VLAN Weiterleitungsparameter die festlegen, für welche Ports die Multicast-Weiterleitung zutrifft. Das Gerät ermöglicht Ihnen, VLAN-Ports als *Forward all* oder Forbidden statisch einzurichten. Den Wert Forbidden für ein MMRP-Service-Requirement legen Sie ausschließlich statisch über die grafische Benutzeroberfläche oder das Command Line Interface fest.

Ein Port ist ausschließlich als ForwardAll oder Forbidden eingerichtet.

Tabelle

VLAN-ID

Zeigt die ID des VLANs.

<Port-Nummer>

Legt die Verarbeitung der Service-Requirements für den Port fest.

Mögliche Werte:

- FA
  Legt die Einstellung ForwardAll auf dem Port fest. Das Gerät leitet die an MMRP-registrierte Multicast-MAC-Adressen gerichteten Daten ans VLAN weiter. Das Gerät leitet die Daten an Ports weiter, die MMRP dynamisch eingerichtet hat oder die der Administrator statisch als ForwardAll-Ports eingerichtet hat.
- F
  Legt die Einstellung Forbidden auf dem Port fest. Das Gerät blockiert die dynamischen MMRP-Service-Requirements für ForwardAll. Bei auf diesem Port in diesem VLAN blockierten ForwardAll-Anfragen blockiert das Gerät auf diesem Port auch Daten, die an MMRP-registrierte Multicast-MAC-Adressen gerichtet sind. Außerdem blockiert das Gerät MMRP-Service-Anfragen, diesen Wert auf diesem Port zu ändern.
- \- (Voreinstellung)
  Schaltet auf diesem Port die Weiterleitungsfunktionen aus.
- Learned
  Zeigt die durch MMRP-Service-Anfragen eingesetzten Werte.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Statistiken]

Geräte in einem LAN tauschen Multiple MAC Registration Protocol Data Units (MMRPDU) aus, um die Geräte-Status an einem aktiven MMRP-Port aufrecht zu erhalten. Diese Registerkarte ermöglicht Ihnen, die Statistiken des MMRP-Verkehrs für jeden Port zu überwachen.

Information

Gesendete MMRP-PDU

Zeigt die Anzahl der an das Gerät übermittelten MMRPDUs.

Empfangene MMRP-PDU

Zeigt die Anzahl der vom Gerät empfangenen MMRPDUs.

Empfangene Bad-Header-PDU

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

Empfangene Bad-Format-PDU

Zeigt die Anzahl der nicht an das Gerät übermittelten MMRPDUs mit fehlerhaftem Datenfeld.

Senden fehlgeschlagen

Zeigt die Anzahl der nicht an das Gerät übermittelten MMRPDUs.

Tabelle

Port

Zeigt die Nummer des Ports.

Gesendete MMRP-PDU

Zeigt die Anzahl der an den Port übermittelten MMRPDUs.

Empfangene MMRP-PDU

Zeigt die Anzahl der vom Port empfangenen MMRPDUs.

Empfangene Bad-Header-PDU

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

Empfangene Bad-Format-PDU

Zeigt die Anzahl der nicht an den Port übermittelten MMRPDUs mit fehlerhaftem Datenfeld.

Senden fehlgeschlagen

Zeigt die Anzahl der nicht an den Port übermittelten MMRPDUs.

Letzte empfangene MAC-Adresse

Zeigt die letzte MAC-Adresse, von welcher der Port MMRPDUs empfangen hat.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Zurücksetzen

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

5.6.3 MRP-IEEE Multiple VLAN Registration Protocol

[Switching > MRP-IEEE > MVRP]

Das Multiple VLAN Registration Protocol (MVRP) besitzt einen Mechanismus, der Ihnen das Verteilen von VLAN-Informationen und das dynamische Konfigurieren von VLANs ermöglicht. Wenn Sie zum Beispiel ein VLAN an einem aktiven MVRP-Port konfigurieren, verteilt das Gerät die VLAN-Informationen an andere Geräte mit eingeschaltetem MVRP. Anhand der erhaltenen Informationen erzeugt ein Gerät mit aktiviertem MVRP dynamisch nach Bedarf VLAN-Trunks in anderen Geräten mit aktiviertem MVRP.

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

[Konfiguration]

In dieser Registerkarte wählen Sie aktive MVRP-Port-Teilnehmer und stellen das Gerät so ein, dass es periodische Ereignisse überträgt.

Für jeden Port exisitert eine Periodic-State-Machine, die regelmäßig periodische Ereignisse an die mit aktiven Ports verbundenen Applicant-State-Machines überträgt. Periodische Ereignisse enthalten eine Information, die über den Status der mit dem aktiven Port verbundenen VLANs informiert. Mit periodischen Ereignissen erhalten Switches mit eingeschaltetem MVRP dynamisch die VLANs aufrecht.

Funktion

Funktion

Schaltet die globale Applicant-Administrative-Überwachung ein/aus, welche festlegt, ob die Applicant-State-Machine am Austausch von MMRP-Nachrichten teilnimmt.

Mögliche Werte:

- *An*
  Normaler Teilnehmer. Die Applicant-State-Machine nimmt am Austausch von MMRP-Nachrichten teil.
- *Aus* (Voreinstellung)
  Kein Teilnehmer. Die Applicant-State-Machine ignoriert MMRP-Nachrichten.

Konfiguration

Periodische State-Machine

Schaltet die Periodic-State-Machine im Gerät ein/aus.

Mögliche Werte:

- *An*
  Die Periodic-State-Machine ist eingeschaltet.
  Bei global eingeschalteter MVRP-*Funktion* überträgt das Gerät periodische MVRP-Nachrichten im Intervall von 1 Sekunde an die an MVRP teilnehmenden Ports.
- *Aus* (Voreinstellung)
  Die Periodic-State-Machine ist ausgeschaltet.
  Deaktiviert die Periodic-State-Machine im Gerät.

Tabelle

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert die Teilnahme des Ports an MVRP.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Bei global und auf diesem Port eingeschaltetem MVRP verteilt das Gerät Informationen zur VLAN-Mitgliedschaft an MVRP-fähige Geräte, die an diesen Port angeschlossen sind.
- `unmarkiert`
  Schaltet die Teilnahme des Ports an MMRP aus.

Restricted VLAN registration

Aktiviert/deaktiviert die Funktion *Restricted VLAN registration* auf diesem Port.

Mögliche Werte:

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

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Statistiken]

Geräte in einem LAN tauschen Multiple VLAN Registration Protocol Data Units (MVRPDU) aus, um die Status von VLANs an einem aktiven Port aufrecht zu erhalten. Diese Registerkarte ermöglicht Ihnen, die Statistiken des MVRP-Verkehrs zu überwachen.

Information

Gesendete MVRP-PDU

Zeigt die Anzahl der an das Gerät übermittelten MVRPDUs.

Empfangene MVRP-PDU

Zeigt die Anzahl der vom Gerät empfangenen MVRPDUs.

Empfangene Bad-Header-PDU

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

Empfangene Bad-Format-PDU

Zeigt die Anzahl der vom Gerät blockierten MVRPDUs mit fehlerhaftem Datenfeld.

Senden fehlgeschlagen

Zeigt die Anzahl der Fehler beim Hinzufügen einer Nachricht zur MVRP-Warteschlange.

Message-Queue-Fehler

Zeigt die Anzahl der vom Gerät blockierten MVRPDUs.

Tabelle

Port

Zeigt die Nummer des Ports.

Gesendete MVRP-PDU

Zeigt die Anzahl der an den Port übermittelten MVRPDUs.

Empfangene MVRP-PDU

Zeigt die Anzahl der vom Port empfangenen MVRPDUs.

Empfangene Bad-Header-PDU

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

Empfangene Bad-Format-PDU

Zeigt die Anzahl der vom Gerät auf dem Port blockierten MVRPDUs mit fehlerhaftem Datenfeld.

Senden fehlgeschlagen

Zeigt die Anzahl der vom Gerät auf dem Port blockierten MVRPDUs.

Registrierungen fehlgeschlagen

Zeigt die Anzahl der erfolglosen Registrierungsversuche auf dem Port.

Letzte empfangene MAC-Adresse

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

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Zurücksetzen

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

5.7 GARP

[Switching > GARP]

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

Wird ein Attribut für einen Teilnehmer gemäß dem GARP registriert oder deregistriert, wird der Teilnehmer auf der Grundlage spezifischer Regeln geändert. Bei den Teilnehmern handelt es sich um eine Reihe erreichbarer Endgeräte und Geräte im Netz. Der definierte Satz von Teilnehmern zu einem bestimmten Zeitpunkt zusammen mit den zugehörigen Attributen stellt den Erreichbarkeitsbaum für die Teilmenge der Netztopologie dar. Das Gerät leitet die Datenpakete ausschließlich an die registrierten Endgeräte weiter. Durch die Registrierung von Stationen wird vermieden, dass versucht wird, Daten an nicht erreichbare Endgeräte zu senden.

Anmerkung: Vergewissern Sie sich vor dem Einschalten der Funktion *GMRP*, dass die Funktion *MMRP* ausgeschaltet ist.

Das Menü enthält die folgenden Dialoge:

- GMRP
- GVRP

5.7.1 GMRP

[Switching > GARP > GMRP]

Das GARP Multicast Registration Protocol (GMRP) ist ein Generic Attribute Registration Protocol (GARP), das einen Mechanismus für die dynamische Registrierung von Gruppenmitgliedschaften durch Geräte im Netz und Endgeräte bereitstellt. Die Geräte registrieren Informationen zur Gruppenmitgliedschaft mit den Geräten, die mit demselben LAN-Segment verbunden sind. GARP ermöglicht den Geräten außerdem, Informationen über Geräte hinweg, die erweiterte Filterdienste unterstützen, im Netz zu verteilen.

GMRP und GARP sind durch IEEE 802.1P definierte Industriestandardprotokolle.

Funktion

Funktion

Aktiviert/deaktiviert die globale Funktion *GMRP* des Geräts. Das Gerät nimmt am Austausch von GMRP-Nachrichten teil.

Mögliche Werte:

- *An*
  GMRP ist aktiviert.
- *Aus* (Voreinstellung)
  Das Gerät ignoriert GMRP-Nachrichten.

Multicasts

Unbekannte Multicasts

Aktiviert/deaktiviert die unbekannten Multicast-Daten, die entweder geflutet oder verworfen werden sollen.

Mögliche Werte:

- *discard*
  Das Gerät verwirft unbekannte Multicast-Daten.
- *flood* (Voreinstellung)
  Das Gerät vermittelt unbekannte Multicast-Daten an jeden Port.

Tabelle

Port

Zeigt die Nummer des Ports.

GMRP aktiv

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

Voraussetzung ist, dass die Funktion *GMRP* global aktiviert ist.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Teilnahme des Ports an *GMRP* ist aktiv.
- `unmarkiert`
  Die Teilnahme des Ports an *GMRP* ist inaktiv.

Service-Requirement

Legt die Ports fest, für welche die Multicast-Weiterleitung gilt.

Mögliche Werte:

- *`Alle unregistrierten Gruppen weiterleiten`* (Voreinstellung)
  Das Gerät leitet die an *GMRP*-registrierte Multicast-MAC-Adressen gerichteten Daten an das VLAN weiter. Das Gerät leitet Daten an nicht registrierte Gruppen weiter.
- *`Alle Gruppen weiterleiten`*
  Das Gerät leitet an jede Gruppe gerichtete Daten weiter, unabhängig davon, ob es sich dabei um registrierte oder nicht registrierte Gruppen handelt.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.7.2 GVRP

[Switching > GARP > GVRP]

Das GARP VLAN Registration Protocol (GVRP) oder Generic VLAN Registration Protocol ist ein Protokoll zur Steuerung von Virtual Local Area Networks (VLANs) innerhalb eines größeren Netzes. GVRP ist ein Schicht-2-Netzprotokoll, das für die automatische Konfiguration von Geräten in einem VLAN-Netz verwendet wird.

GVRP ist eine GARP-Anwendung, die IEEE-802.1Q-konformes VLAN-Pruning bereitstellt und dynamische VLANs an 802.1Q-Trunk-Ports erstellt. Mit GVRP tauscht das Gerät Informationen zur VLAN-Konfiguration mit anderen GVRP-Geräten aus. Auf diese Weise reduziert das Gerät unnötigen Broadcast- und unbekannten Unicast-Verkehr. Das Austauschen der VLAN-Konfigurationsinformationen ermöglicht Ihnen außerdem, die über 802.1Q-Trunk-Ports verbundenen VLANs dynamisch zu erzeugen und zu verwalten.

Funktion

Funktion

Aktiviert/deaktiviert die Funktion *GVRP* global im Gerät. Das Gerät nimmt am Austausch von *GVRP*-Nachrichten teil. Wenn die Funktion deaktiviert ist, dann ignoriert das Gerät *GVRP*-Nachrichten.

Mögliche Werte:

- `An`
  Die Funktion *GVRP* ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *GVRP* ist ausgeschaltet.

Tabelle

Port

Zeigt die Nummer des Ports.

GVRP aktiv

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

Voraussetzung ist, dass die Funktion *GVRP* global aktiviert ist.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Teilnahme des Ports an *GVRP* ist aktiv.
- `unmarkiert`
  Die Teilnahme des Ports an *GVRP* ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.8 QoS/Priority

[Switching > QoS/Priority]

Kommunikationsnetze übertragen gleichzeitig eine Vielzahl von Anwendungen, die jeweils unterschiedliche Anforderungen an Verfügbarkeit, Bandbreite und Latenzzeiten haben.

QoS (Quality of Service) ist ein in der Norm IEEE 802.1D beschriebenes Verfahren. Damit verteilen Sie die Ressourcen im Netz. Sie haben damit die Möglichkeit, wesentlichen Anwendungen eine Mindestbandbreite zur Verfügung zu stellen. Voraussetzung ist, dass die Endgeräte und die Geräte im Netz die priorisierte Datenübertragung unterstützen. Hochpriorisierte Datenpakete vermitteln die Geräte im Netz bevorzugt. Datenpakete mit niedriger Priorität vermitteln sie, wenn keine höher priorisierten Datenpakete zu vermitteln sind.

Das Gerät bietet Ihnen folgende Einstellmöglichkeiten:
- Für eingehende Datenpakete legen Sie fest, wie das Gerät die QoS-/Priorisierungs-Information auswertet.
- Für ausgehende Datenpakete legen Sie fest, welche QoS-/Priorisierungs-Information das Gerät in das Datenpaket schreibt (zum Beispiel Priorität für Management-Pakete, Portpriorität).

Anmerkung: Wenn Sie die Funktionen in diesem Menü nutzen, dann schalten Sie die Flusskontrolle aus. Die Flusskontrolle ist ausgeschaltet, wenn im Dialog *Switching > Global*, Rahmen *Konfiguration*, das Kontrollkästchen *Flusskontrolle*`unmarkiert` ist.

Das Menü enthält die folgenden Dialoge:
- QoS/Priority Global
- QoS/Priorität Port-Konfiguration
- 802.1D/p Zuweisung
- IP-DSCP-Zuweisung
- Queue-Management

5.8.1 QoS/Priority Global

[Switching > QoS/Priority > Global]

Das Gerät ermöglicht Ihnen, auch in Situationen mit großer Netzlast Zugriff auf das Management des Geräts zu behalten. In diesem Dialog legen Sie die dazu notwendigen QoS-/Priorisierungseinstellungen fest.

Konfiguration

VLAN-Priorität für Management-Pakete

Legt die VLAN-Priorität für zu sendende Management-Datenpakete fest. Abhängig von der VLAN-Priorität weist das Gerät das Datenpaket einer bestimmten Verkehrsklasse zu und dementsprechend einer bestimmten Warteschlange des Ports.

Mögliche Werte:

- `0..7` (Voreinstellung: `0`)

Im Dialog *Switching > QoS/Priority > 802.1D/p Zuweisung* weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu.

IP-DSCP-Wert für Management-Pakete

Legt den IP-DSCP-Wert für zu sendende Management-Datenpakete fest. Abhängig vom IP-DSCP-Wert weist das Gerät das Datenpaket einer bestimmten Verkehrsklasse zu und dementsprechend einer bestimmten Warteschlange des Ports.

Mögliche Werte:

- `0 (be/cs0)..63` (Voreinstellung: `0 (be/cs0)`)

Einige Werte in der Liste haben zusätzlich ein DSCP-Schlüsselwort, zum Beispiel `0 (be/cs0)`, `10 (af11)` und `46 (ef)`. Diese Werte sind kompatibel zum IP-Precendence-Modell.

Im Dialog *Switching > QoS/Priority > IP-DSCP-Zuweisung* weisen Sie jedem IP-DSCP-Wert eine Verkehrsklasse zu.

Queues je Port

Zeigt die Anzahl der Warteschlangen pro Port.

Das Gerät verfügt über 8 Warteschlangen pro Port. Jede Warteschlange ist einer bestimmten Verkehrsklasse zugewiesen (Traffic Class nach IEEE 802.1D).

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.8.2 QoS/Priorität Port-Konfiguration

[Switching > QoS/Priority > Port-Konfiguration]

In diesem Dialog legen Sie für jeden Port fest, wie das Gerät empfangene Datenpakete anhand ihrer QoS-/Prioritätsinformation verarbeitet.

Tabelle

Port

Zeigt die Nummer des Ports.

Port-Priorität

Legt fest, welche VLAN-Prioritätsinformation das Gerät in ein Datenpaket schreibt, wenn das Datenpaket keine Prioritätsinformation enthält. Das Gerät vermittelt das Datenpaket anschließend abhängig vom festgelegten Wert in Spalte *Trust-Mode*.

Mögliche Werte:

- `0..7` (Voreinstellung: `0`)

Trust-Mode

Legt fest, wie das Gerät ein empfangenes Datenpaket behandelt, wenn das Datenpaket eine Prioritätsinformation enthält.

Mögliche Werte:

- *untrusted*
  Das Gerät vermittelt das Datenpaket gemäß der in Spalte *Port-Priorität*festgelegten Priorität. Das Gerät ignoriert die im Datenpaket enthaltene Prioritätsinformation.
  Im Dialog *Switching > QoS/Priority > 802.1D/p Zuweisung* weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu.
- *trustDot1p* (Voreinstellung)
  Das Gerät vermittelt das Datenpaket gemäß der Prioritätsinformation im VLAN-Tag.
  Im Dialog *Switching > QoS/Priority > 802.1D/p Zuweisung* weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu.
- *trustIpDscp*
  - Wenn das Datenpaket ein IP-Paket ist:
    Das Gerät vermittelt das Datenpaket gemäß des im Datenpaket enthaltenen IP-DSCP-Werts.
    Im Dialog *Switching > QoS/Priority > IP-DSCP-Zuweisung* weisen Sie jedem IP-DSCP-Wert eine Verkehrsklasse zu.
  - Wenn das Datenpaket kein IP-Paket ist:
    Das Gerät vermittelt das Datenpaket gemäß der in Spalte *Port-Priorität*festgelegten Priorität.
    Im Dialog *Switching > QoS/Priority > 802.1D/p Zuweisung* weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu.

Untrusted-Traffic-Klasse

Zeigt die Verkehrsklasse, welche der in Spalte *Port-Priorität*festgelegten VLAN-Prioritätsinformation zugewiesen ist. Im Dialog *Switching > QoS/Priority > 802.1D/p Zuweisung* weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu.

Mögliche Werte:

- `0..7`

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.8.3 802.1D/p Zuweisung

[Switching > QoS/Priority > 802.1D/p Zuweisung]

Das Gerät vermittelt Datenpakete mit VLAN-Tag anhand der enthaltenen QoS-/Priorisierungsinformation mit hoher oder mit niedriger Priorität.

In diesem Dialog weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu. Die Verkehrsklassen sind den Warteschlangen der Ports (Prioritäts-Queues) fest zugewiesen.

Tabelle

VLAN-Priorität

Zeigt die VLAN-Priorität.

Traffic-Klasse

Legt die Verkehrsklasse fest, die der VLAN-Priorität zugewiesen ist.

Mögliche Werte:

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

Anmerkung: Unter anderem Redundanzmechanismen nutzen die höchste Verkehrsklasse. Wählen Sie deshalb für Anwendungsdaten eine andere Verkehrsklasse.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Werksseitige Zuweisung der VLAN-Priorität zu Verkehrsklassen

VLAN-Priorität	Traffic Class	Inhaltskennzeichnung gemäß IEEE 802.1D
`0`	2	`Best Effort` Normale Daten ohne Priorisierung
`1`	0	`Background` Zeitunkritische Daten und Hintergrunddienste
`2`	1	`Standard` Normale Daten
`3`	3	`Excellent Effort` Wichtige Daten
`4`	4	`Controlled Load` Zeitkritische Daten mit hoher Priorität

VLAN-Priorität	Traffic Class	Inhaltskennzeichnung gemäß IEEE 802.1D
5	5	Video Bildübertragung mit Verzögerungen und Jitter < 100 ms
6	6	Voice Sprachübertragung mit Verzögerungen und Jitter < 10 ms
7	7	Network Control Daten für Netzmanagement und Redundanzmechanismen

5.8.4 IP-DSCP-Zuweisung

[Switching > QoS/Priority > IP-DSCP-Zuweisung]

Das Gerät vermittelt IP-Datenpakete anhand des im Datenpaket enthaltenen DSCP-Werts mit hoher oder mit niedriger Priorität.

In diesem Dialog weisen Sie jedem DSCP-Wert eine Verkehrsklasse zu. Die Verkehrsklassen sind den Warteschlangen der Ports (Prioritäts-Queues) fest zugewiesen.

Tabelle

DSCP Wert

Zeigt den DSCP-Wert.

Traffic-Klasse

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

Mögliche Werte:

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

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Werksseitige Zuweisung der DSCP-Werte zu Verkehrsklassen

DSCP-Wert	DSCP-Name	Traffic Class
0	Best Effort /CS0	2
1-7		2
8	CS1	0
9,11,13,15		0
10,12,14	AF11,AF12,AF13	0
16	CS2	1
17,19,21,23		1
18,20,22	AF21,AF22,AF23	1
24	CS3	3
25,27,29,31		3
26,28,30	AF31,AF32,AF33	3
32	CS4	4
33,35,37,39		4
34,36,38	AF41,AF42,AF43	4

DSCP-Wert	DSCP-Name	Traffic Class
40	CS5	5
41,42,43,44,45,47		5
46	EF	5
48	CS6	6
49-55		6
56	CS7	7
57-63		7

5.8.5 Queue-Management

[Switching > QoS/Priority > Queue-Management]

Dieser Dialog ermöglicht Ihnen, für die Verkehrsklassen die Funktion *Strict priority* ein- und auszuschalten. Bei ausgeschalteter Funktion *Strict priority* arbeitet das Gerät die Warteschlangen der Ports mit „Weighted Fair Queuing“ ab.

Außerdem haben Sie die Möglichkeit, jeder Verkehrsklasse eine Mindestbandbreite zuzuweisen, mit der das Gerät die Warteschlangen mit „Weighted Fair Queuing“ abarbeitet.

Tabelle

Traffic-Klasse

Zeigt die Verkehrsklasse.

Strict priority

Aktiviert/deaktiviert für diese Verkehrsklasse die Abarbeitung der Port-Warteschlange mit *Strict priority*.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Abarbeitung der Port-Warteschlange mit *Strict priority* ist aktiv.
  - Der Port vermittelt ausschließlich Datenpakete, die sich in der Warteschlange mit der höchsten Priorität befinden. Ist diese Warteschlange leer, sendet der Port Datenpakete, die sich in der Warteschlange mit der nächstniedrigeren Priorität befinden.
  - Datenpakete mit niedriger Verkehrsklasse vermittelt der Port erst, wenn die Warteschlangen mit höherer Priorität leer sind. In ungünstigen Fällen sendet der Port diese Datenpakete nicht.
  - Wenn Sie diese Einstellung für eine Verkehrsklasse festlegen, schaltet das Gerät die Funktion auch bei Verkehrsklassen mit höherer Priorität ein.
  - Verwenden Sie diese Einstellung für Anwendungen wie VoIP oder Video, die möglichst verzögerungsfrei arbeiten sollen.
- `unmarkiert`
  Die Abarbeitung der Port-Warteschlange mit *Strict priority* ist inaktiv. Das Gerät verwendet „Weighted Fair Queuing“/“Weighted Round Robin“ (WRR), um die Port-Warteschlange abzuarbeiten.
  - Das Gerät weist jeder Verkehrsklasse eine Mindestbandbreite zu.
  - Der Port sendet auch bei hoher Netzlast Datenpakete mit niedriger Verkehrsklasse.
  - Wenn Sie diese Einstellung für eine Verkehrsklasse festlegen, schaltet das Gerät die Funktion auch bei Verkehrsklassen mit niedrigerer Priorität aus.

Min. Bandbreite [%]

Legt die Mindestbandbreite für diese Verkehrsklasse fest, wenn das Gerät die Warteschlangen der Ports mit „Weighted Fair Queuing“ abarbeitet.

Mögliche Werte:

- `0..100` (Voreinstellung: `0` = das Gerät reserviert für diese Verkehrsklasse keine Bandbreite)

Der festgelegte Wert in Prozent bezieht sich auf die auf dem Port verfügbare Bandbreite. Wenn Sie für jede Verkehrsklasse die Funktion *Strict priority* ausschalten, steht auf dem Port die maximale Bandbreite für „Weighted Fair Queuing“ zur Verfügung.

Die Summe der zugewiesenen Bandbreiten ist höchstens 100 %.

Max. Bandbreite [%]

Legt die Shaping-Rate fest, mit der eine Verkehrsklasse Pakete vermittelt (Queue-Shaping).

Mögliche Werte:

- `0` (Voreinstellung)
  Das Gerät reserviert für diese Verkehrsklasse keine Bandbreite.
- `1..100`
  Das Gerät reserviert für diese Verkehrsklasse die festgelegte Bandbreite. Der festgelegte Wert in Prozent bezieht sich auf die maximal verfügbare Bandbreite auf dem Port.

Queue-Shaping ermöglicht Ihnen zum Beispiel, die Rate einer hochprioren Warteschlange zu beschränken. Die Beschränkung einer hochprioren Warteschlange ermöglicht dem Gerät außerdem, niederpriore Warteschlangen abzuarbeiten. Um Queue-Shaping zu verwenden, legen Sie die maximale Bandbreite für eine bestimmte Warteschlange fest.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.9 VLAN

[Switching > VLAN]

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

- Hohe Flexibilität
  - Mit VLAN verteilen Sie den Datenverkehr auf logische Netze in der vorhandenen Infrastruktur. Ohne VLAN wären dazu weitere Geräte und eine aufwendigere Verkabelung notwendig.
  - Mit VLAN definieren Sie Netzsegmente unabhängig vom Standort der einzelnen Endgeräte.

- Verbesserter Durchsatz
  - Datenpakete lassen sich in VLANs priorisiert übertragen.
    Bei höherer Priorisierung überträgt das Gerät die Daten eines VLANs bevorzugt, zum Beispiel mit zeitkritischen Anwendungen wie VoIP-Telefonaten.
  - Die Netzlast reduziert sich erheblich, wenn sich Datenpakete und Broadcasts in kleinen Netzsegmenten anstatt im gesamten Netz ausbreiten.
- Höhere Sicherheit
  Das Verteilen des Datenverkehrs auf einzelne logische Netze erschwert ungewolltes Abhören und härtet das System gegen Angriffe, wie MAC-Flooding oder MAC-Spoofing.

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

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

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

Das Gerät priorisiert den empfangenen Datenstrom in folgender Reihenfolge:
- Voice-VLAN
- Port-basiertes VLAN

Das Menü enthält die folgenden Dialoge:
- VLAN Global
- VLAN Konfiguration
- VLAN Port
- VLAN Voice

5.9.1 VLAN Global

[Switching > VLAN > Global]

Dieser Dialog ermöglicht Ihnen, sich allgemeine VLAN-Parameter des Geräts anzusehen.

Konfiguration

Größte VLAN-ID

Größtmögliche ID, die Sie einem VLAN zuweisen können.

Siehe Dialog *Switching > VLAN > Konfiguration*.

VLANs (max.)

Zeigt die maximale Anzahl der im Gerät einrichtbaren VLANs.

Siehe Dialog *Switching > VLAN > Konfiguration*.

VLANs

Anzahl der VLANs, die im Gerät gegenwärtig eingerichtet sind.

Siehe Dialog *Switching > VLAN > Konfiguration*.

Das VLAN mit der ID 1 ist stets im Gerät eingerichtet.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Leeren...

Versetzt die VLAN-Einstellungen des Geräts in den Voreinstellung.

Beachten Sie, dass Sie Ihre Verbindung zum Gerät trennen, wenn Sie im Dialog *Grundeinstellungen > Netz* die VLAN-ID für das Management des Geräts geändert haben.

5.9.2 VLAN Konfiguration

[Switching > VLAN > Konfiguration]

In diesem Dialog verwalten Sie die VLANs. Um ein VLAN einzurichten, erzeugen Sie in der Tabelle eine weitere Zeile. Dort legen Sie für jeden Port fest, ob er Datenpakete des betreffenden VLANs vermittelt und ob die Datenpakete ein VLAN-Tag enthalten.

Man unterscheidet zwischen folgenden VLANs:
- Statische VLANs sind durch den Benutzer eingerichtet.
- Dynamische VLANs richtet das Gerät automatisch ein und entfernt sie wieder, sobald die Voraussetzungen entfallen.
  Für folgende Funktionen erzeugt das Gerät dynamische VLANs:
  - *MRP*: Wenn Sie den Ring-Ports ein noch nicht eingerichtetes VLAN zuweisen, dann erzeugt das Gerät dieses VLAN.
  - *MVRP*: Das Gerät erzeugt ein VLAN auf Grundlage der Meldungen benachbarter Geräte.

Tabelle

VLAN-ID

ID des VLANs.

Das Gerät unterstützt bis zu 128 gleichzeitig eingerichtete VLANs.

Mögliche Werte:
- `1..4042`

Status

Zeigt, auf welche Weise das VLAN eingerichtet ist.

Mögliche Werte:
- *other*
  VLAN `1`
  oder
  VLAN eingerichtet durch Funktion *802.1X Port-Authentifizierung*. Siehe Dialog *Netzsicherheit* > 802.1X Port-Authentifizierung.
- *permanent*
  VLAN eingerichtet durch den Benutzer.
  oder
  VLAN eingerichtet durch Funktion *MRP*. Siehe Dialog *Switching > L2-Redundanz > MRP*.
  Wenn Sie die Änderungen im permanenten Speicher speichern, dann bleiben die VLANs mit dieser Einstellung nach einem Neustart eingerichtet.
- *dynamicMvrp*
  VLAN eingerichtet durch Funktion *MVRP*. Siehe Dialog *Switching > MRP-IEEE > MVRP*.
  VLANs mit dieser Einstellung sind schreibgeschützt. Das Gerät entfernt ein VLAN aus der Tabelle, sobald der letzte Port das VLAN verlässt.

Erstellungszeit

Zeigt, seit wann das VLAN eingerichtet ist.

Das Feld zeigt den Zeitstempel der Betriebszeit (System Uptime).

Name

Legt die Bezeichnung des VLANs fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

<Port-Nummer>

Legt fest, ob der betreffende Port Datenpakete des VLANs vermittelt und ob die Datenpakete ein VLAN-Tag enthalten.

Mögliche Werte:

- `-` (Voreinstellung)
  Der Port ist kein Mitglied des VLANs und vermittelt keine Datenpakete des VLANs.
- `T` = Tagged
  Der Port ist Mitglied des VLANs und vermittelt die Datenpakete mit VLAN-Tag. Verwenden Sie diese Einstellung zum Beispiel auf Uplink-Ports.
- `LT` = Tagged Learned
  Der Port ist Mitglied des VLANs und vermittelt die Datenpakete mit VLAN-Tag.
  Das Gerät hat den Eintrag mit der Funktion *GVRP* oder *MVRP* automatisch eingerichtet.
- `F` = Forbidden
  Der Port ist kein Mitglied des VLANs und vermittelt keine Datenpakete dieses VLANs.
  Das Gerät sorgt zudem dafür, zu vermeiden, dass der Port durch die Funktion *MVRP*Mitglied eines VLANs wird.
- `U` = Untagged (Voreinstellung für VLAN 1)
  Der Port ist Mitglied des VLANs und vermittelt die Datenpakete ohne VLAN-Tag. Verwenden Sie diese Einstellung, wenn das angeschlossene Gerät kein VLAN-Tag auswertet, zum Beispiel auf EndPorts.
- `LU` = Untagged Learned
  Der Port ist Mitglied des VLANs und vermittelt die Datenpakete ohne VLAN-Tag.
  Das Gerät hat den Eintrag mit der Funktion *GVRP* oder *MVRP* automatisch eingerichtet.

Anmerkung: Vergewissern Sie sich, dass der Port, an dem die Netzmanagement-Station angeschlossen ist, Mitglied des VLANs ist, in welchem das Gerät die Management-Daten vermittelt. In der Voreinstellung vermittelt das Gerät die Management-Daten im VLAN 1. Sonst bricht die Verbindung zum Gerät ab, sobald Sie die Änderungen an das Gerät übertragen. Der Zugriff auf das Management des Geräts ist ausschließlich mit dem Command Line Interface über die serielle Schnittstelle möglich.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

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

5.9.3 VLAN Port

[Switching > VLAN > Port]

In diesem Dialog legen Sie fest, wie das Gerät empfangene Datenpakete behandelt, die kein VLAN-Tag haben oder deren VLAN-Tag von der VLAN-ID des Ports abweicht.

Dieser Dialog ermöglicht Ihnen, den Ports ein VLAN zuzuweisen und damit die Port-VLAN-ID festzulegen.

Außerdem legen Sie für jeden Port fest, wie das Gerät Datenpakete überträgt, wenn eine der folgenden Situationen eintritt:
- Der Port empfängt Datenpakete ohne VLAN-Tag.
- Der Port empfängt Datenpakete mit VLAN-Prioritätsinformation (VLAN-ID `0`, priority tagged).
- Das VLAN-Tag des Datenpaketes weicht ab von der VLAN-ID des Ports.

Tabelle

Port

Zeigt die Nummer des Ports.

Port-VLAN-ID

Legt die ID des VLANs fest, die das Gerät Datenpaketen ohne eigenes VLAN-Tag zuweist.

Voraussetzungen:
- In Spalte *Akzeptierte Datenpakete* legen Sie den Wert `admitAll` fest.

Mögliche Werte:
- ID eines bereits eingerichteten VLANs (Voreinstellung: `1`)

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

Akzeptierte Datenpakete

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

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

Ingress-Filtering

Aktiviert/deaktiviert die Eingangsfilterung.

Mögliche Werte:

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

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.9.4 VLAN Voice

[Switching > VLAN > Voice]

Verwenden Sie die Voice-VLAN-Funktion, um den Sprach- und Datenverkehr an einem Port nach VLAN und/oder Priorität zu trennen. Ein wesentlicher Nutzen von Voice-VLAN liegt darin, in Zeiten mit erhöhtem Datenverkehrsaufkommen die Qualität des Sprachverkehrs sicherzustellen.

Das Gerät erkennt VoIP Telefone, die Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) verwenden. Dann fügt das Gerät den entsprechenden Switch-Port zur Mitgliedergruppe des konfigurierten Voice-VLANs hinzu. Die Mitgliedergruppe enthält entweder „getaggte“ oder „ungetaggte“ Mitglieder. Die Markierung ist abhängig vom Voice-VLAN-Interface-Modus (VLAN ID, Dot1p, None, Untagged).

Ein weiterer Nutzen der Voice-VLAN-Funktion liegt darin, dass das VoIP-Telefon Informationen zu VLAN-Kennung und Priorität via LLDP-Med vom Gerät erhält. Infolgedessen sendet das VoIP-Telefon die Sprachdaten entweder mit Prioritätsmarkierung oder unmarkiert. Dies ist abhängig vom festgelegten Interface-Modus des Voice-VLANs. Die Voice-VLAN-Funktion aktivieren Sie auf dem Port, an dem Sie das VoIP-Telefon anschließen.

Funktion

Funktion

Schaltet die Funktion *VLAN Voice* des Geräts global ein/aus.

Mögliche Werte:

- *An*
- *Aus* (Voreinstellung)

Tabelle

Port

Zeigt die Nummer des Ports.

Voice-VLAN-Modus

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

Mögliche Werte:

- *disabled* (Voreinstellung)
  Deaktiviert die Funktion *VLAN Voice* für diesen Tabelleneintrag.
- *kein*
  Ermöglicht es dem IP-Telefon, seine eigene Konfiguration beim Senden von unmarkiertem Sprachverkehr zu verwenden.
- *vlan/dot1p-priority*
  Der Port filtert Datenpakete des Voice-VLANs anhand der vlan- und dot1p-Prioritätsmarkierungen.

- *untagged*
  Der Port filtert Datenpakete ohne Voice-VLAN-Tag.
- *vlan*
  Der Port filtert Datenpakete des Voice-VLANs anhand des VLAN-Tags.
- *dot1p-priority*
  Der Port filtert Datenpakete des Voice-VLANs anhand der dot1p-Prioritätsmarkierungen. Wenn Sie diesen Wert auswählen, dann legen Sie zusätzlich in Spalte *Priorität* einen geeigneten Wert fest.

Data-Priority-Modus

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

Das Gerät setzt diesen Modus für Datenverkehr auf dem Voice-VLAN ein, wenn es zugleich ein VoIP-Telefon wie auch einen PC ermittelt und diese Geräte dasselbe Kabel für die Datenübertragung verwenden.

Mögliche Werte:

- *trust* (Voreinstellung)
  Mittels dieser Einstellung kann der Datenverkehr mit normaler Priorität ablaufen, wenn auf dem Interface Sprachverkehr anliegt.
- *untrust*
  Wenn Sprachverkehr anliegt und der *Voice-VLAN-Modus* auf *dot1p-priority* gesetzt ist, verwendet der Datenverkehr die Priorität 0. Wenn das Interface ausschließlich Datenverkehr vermittelt, verwendet der Datenverkehr die normale Priorität.

Status

Zeigt den Status des Voice-VLANs auf dem betreffenden Port.

Mögliche Werte:

- markiert
  Das Voice-VLAN ist eingeschaltet.
- unmarkiert
  Das Voice-VLAN ist ausgeschaltet.

VLAN-ID

Legt die ID des VLANs fest, für das der Tabelleneintrag gilt.

Um den Datenverkehr an diese VLAN-ID unter Verwendung dieses Filters weiterzuleiten, legen Sie in Spalte *Voice-VLAN-Modus* den Wert *vlan*fest.

Mögliche Werte:

- `0..4042`

Priorität

Legt die Voice-VLAN-Priorität des Ports fest.

Voraussetzungen:

- In Spalte *Voice-VLAN-Modus* legen Sie den Wert `dot1p-priority` fest.

Mögliche Werte:

- `0..7`
- `kein`
  Deaktiviert die Voice-VLAN-Priorität des Ports.

Bypass-Authentifizierung

Aktiviert den Voice-VLAN-Authentifizierungsmodus.

Wenn Sie die Funktion deaktivieren und den Wert in Spalte *Voice-VLAN-Modus* auf `dot1p-priority` setzen, benötigen Sprachgeräte eine Authentifizierung.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Wenn die Funktion im Dialog *Netzsicherheit > 802.1X Port-Authentifizierung > Global* eingeschaltet ist, dann stellen Sie den Parameter *Port-Kontrolle* für diesen Port auf den Wert `multiClient`, bevor Sie diese Funktion aktivieren. Den Parameter *Port-Kontrolle* finden Sie im Dialog *Netzsicherheit > 802.1X Port-Authentifizierung > Global*.
- `unmarkiert`

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.10 L2-Redundanz

[Switching > L2-Redundanz]

Das Menü enthält die folgenden Dialoge:

- MRP
- HIPER-Ring
- Spanning Tree
- Link-Aggregation
- Link-Backup
- FuseNet

5.10.1 MRP

[Switching > L2-Redundanz > MRP]

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *MRP*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der Ring-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Das Media Redundancy Protocol (MRP) ist ein Protokoll, das Ihnen den Aufbau hochverfügbarer, ringförmiger Netzstrukturen ermöglicht. Ein MRP-Ring mit Schneider Electric-Geräten besteht aus bis zu 100 Geräten, die das MRP-Protokoll gemäß IEC 62439 unterstützen.

Die Ringstruktur eines MRP-Rings wandelt sich zurück in eine Linienstruktur, wenn eine Teilstrecke nicht in Betrieb ist. Die maximale Umschaltzeit ist konfigurierbar.

Die Ring-Manager-Funktion des Geräts schließt die Enden eines Backbones in Linienstruktur zu einem redundanten Ring.

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

Wenn Sie mit übergroßen Ethernet-Paketen arbeiten (für diesen Port ist der Wert in Spalte *MTU* > `1518`, siehe Dialog *Grundeinstellungen > Port*), ist die Umschaltzeit bei der Rekonfiguration des MRP-Rings abhängig von folgenden Parametern:

- Bandbreite der Ring-Leitung
- Größe der Ethernet-Pakete
- Anzahl der Geräte im Ring

Legen Sie die Umschaltzeit ausreichend groß fest, um Verzögerungen der MRP-Pakete aufgrund von Latenzen in den Geräten zu vermeiden. Die Formel zum Berechnen der Umschaltzeit finden Sie in IEC 62439-2, Kapitel 9.5.

Funktion

Funktion

Schaltet die Funktion *MRP* ein/aus.

Wenn alle Parameter für den MRP-Ring konfiguriert sind, schalten Sie hier die Funktion ein.

Mögliche Werte:

- *An*
  Die Funktion *MRP* ist eingeschaltet.
  Sind alle Geräte im MRP-Ring konfiguriert, ist die Redundanz aktiv.
- *Aus* (Voreinstellung)
  Die Funktion *MRP* ist ausgeschaltet.

Ring-Port 1/Ring-Port 2

Port

Legt die Nummer des Ports fest, der als Ring-Port arbeitet.

Mögliche Werte:

- <Port-Nummer>
  Nummer des Ring-Ports

Funktion

Zeigt den Betriebszustand des Ring-Ports.

Mögliche Werte:

- *forwarding*
  Der Port ist eingeschaltet, Verbindung vorhanden.
- *blocked*
  Der Port ist blockiert, Verbindung vorhanden.
- *disabled*
  Der Port ist ausgeschaltet.
- *nicht verbunden*
  Keine Verbindung vorhanden.

Fixed backup

Aktiviert/deaktiviert die Backup-Port-Funktion für den *Ring-Port 2*.

Anmerkung: Bei der Umschaltung auf den primären Port wird ggf. die maximal zulässige Ring-Wiederherstellungszeit überschritten.

Mögliche Werte:

- markiert
  Die Backup-Funktion für *Ring-Port 2* ist aktiviert. Ist der Ring geschlossen, schaltet der Ring-Manager auf den primären Ring-Port zurück.
- unmarkiert (Voreinstellung)
  Die Backup-Funktion für *Ring-Port 2* ist deaktiviert. Ist der Ring geschlossen, sendet der Ring-Manager weiterhin Daten an den sekundären Ring-Port.

Konfiguration

Ring-Manager

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

Aktivieren Sie diese Funktion bei genau einem Gerät an den Enden der Linie.

Mögliche Werte:

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

Advanced mode

Aktiviert/deaktiviert den Advanced-Modus für schnelle Umschaltzeiten.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Advanced Mode eingeschaltet.
  MRP-fähige Schneider Electric-Geräte unterstützen diesen Modus.
- `unmarkiert`
  Advanced Mode ausgeschaltet.
  Wählen Sie diese Einstellung, wenn ein anderes Gerät im Ring keine Unterstützung für diesen Modus bietet.

Ring-Rekonfiguration

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

Mögliche Werte:

- `500ms`
- `200ms` (Voreinstellung)

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

Wenn Sie mit übergroßen Ethernet-Paketen arbeiten, ist die Anzahl der Geräte im Ring begrenzt. Beachten Sie, dass die Umschaltzeit von mehreren Parametern abhängig ist. Siehe Beschreibung oben.

VLAN-ID

Legt die ID des VLANs fest, das den Ring-Ports zugewiesen ist.

Mögliche Werte:

- `0` (Voreinstellung)
  Kein VLAN zugewiesen.
  Weisen Sie im Dialog *Switching > VLAN > Konfiguration*. den Ring-Ports für VLAN `1` den Wert `U` zu.
- `1..4042`
  VLAN zugewiesen.
  Wenn Sie den Ring-Ports ein noch nicht eingerichtetes VLAN zuweisen, dann erzeugt das Gerät dieses VLAN. Im Dialog *Switching > VLAN > Konfiguration* erzeugt das Gerät in der Tabelle einen Eintrag für das VLAN und weist den Ring-Ports den Wert `T`zu.

Information

Information

Zeigt Meldungen zur Redundanzkonfiguration und mögliche Ursachen für erkannte Fehler.

Wenn das Gerät als Ring-Client oder als Ring-Manager arbeitet, sind folgende Meldungen möglich:

- *Redundanz verfügbar*
  Die Redundanz ist eingerichtet. Fällt eine Komponente des Rings aus, übernimmt die redundante Strecke deren Funktion.
- *Konfigurationsfehler: Ring-Port-Verbindung fehlerhaft*
  In der Verkabelung der Ring-Ports wurde ein Fehler erkannt.

Wenn das Gerät als Ring-Manager arbeitet, sind folgende Meldungen möglich:

- *Konfigurationsfehler: Pakete eines anderen Ring-Managers empfangen*
  Im Ring existiert ein weiteres Gerät, das als Ring-Manager arbeitet.
  Schalten Sie die Funktion *Ring-Manager* bei genau einem Gerät im Ring ein.
- *Konfigurationsfehler: Verbindung im Ring ist mit falschem Port verbunden*
  Eine Leitung des Rings ist anstatt mit einem Ring-Port mit einem anderen Port verbunden. Das Gerät empfängt Test-Datenpakete ausschließlich auf einem Ring-Port.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Lösche Ring-Konfiguration

Schaltet die Redundanzfunktion aus und setzt alle Einstellungen im Dialog die voreingestellten Werte zurück.

5.10.2 HIPER-Ring

[Switching > L2-Redundanz > HIPER-Ring]

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *HIPER-Ring*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der Ring-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Das Konzept der Ring-Redundanz ermöglicht den Aufbau hochverfügbarer, ringförmiger Netze. Dieses Gerät stellt einen HIPER-Ring-Client bereit. Diese Funktion ermöglicht Ihnen, einen vorhandenen HIPER-Ring zu erweitern oder ein Gerät zu ersetzen, das bereits als Client in einem HIPER-Ring aktiv ist.

Ein HIPER-Ring enthält einen Ring-Manager (RM), der den Ring kontrolliert. Der Ring-Manager sendet sowohl auf dem primären als auch auf dem sekundären Port Watchdog-Pakete in den Ring. Wenn der Ring-Manager die Watchdog-Pakete auf beiden Ports empfängt, verbleibt der primäre Port im Forwarding-Status und der sekundäre Port im Discarding-Status.

Das Gerät arbeitet ausschließlich im Ring-Client-Modus. Das bedeutet, dass das Gerät in der Lage ist, an den Ring-Ports Watchdog-Pakete zu erkennen und weiterzuleiten sowie die Änderung des Link-Status an den Ring-Manager zu senden, zum Beispiel LinkDown- und LinkUp-Pakete.

Als Ring-Ports unterstützt das Gerät ausschließlich Fast-Ethernet-Ports und Gigabit-Ethernet-Ports. Des Weiteren unterstützt das Gerät ausschließlich HIPER-Ring in VLAN `1`.

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

Anmerkung: Konfigurieren Sie die Geräte des HIPER-Rings individuell. Bevor Sie die Redundanzverbindung herstellen, konfigurieren Sie jedes Gerät im HIPER-Ring vollständig. So vermeiden Sie Loops während der Konfigurationsphase.

Funktion

Funktion

Schaltet den *HIPER-Ring*-Client ein/aus.

Mögliche Werte:

- `An`
  Der *HIPER-Ring*-Client ist eingeschaltet.
- `Aus` (Voreinstellung)
  Der *HIPER-Ring*-Client ist ausgeschaltet.

Ring-Port 1/Ring-Port 2

Port

Legt die Port-Nummer für den primären/sekundären Ring-Port fest.

Mögliche Werte:

- `-` (Voreinstellung)
  Kein primärer/sekundärer Ring-Port ausgewählt.
- `<Port-Nummer>`
  Nummer des Ring-Ports

Zustand

Zeigt den Status des primären/sekundären Ring-Ports.

Mögliche Werte:

- *`not-available`*
  Der *HIPER-Ring*-Client ist ausgeschaltet.
  oder
  Kein primärer oder sekundärer Ring-Port ausgewählt.
- *`aktiv`*
  Der Ring-Port ist eingeschaltet, der Link ist vorhanden.
- *`inaktiv`*
  Kein Link auf dem Ring-Port vorhanden.
  Sobald der Link an einem Ring-Port abbricht, sendet das Gerät auf dem anderen Ring-Port ein LinkDown-Paket an den Ring-Manager.

Information

Modus

Zeigt, dass das Gerät ausschließlich im Ring-Client-Modus arbeitet.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.10.3 Spanning Tree

[Switching > L2-Redundanz > Spanning Tree]

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *Spanning Tree*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der *Spanning Tree*-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Das Spanning Tree Protocol (STP) ist ein Protokoll, das redundante Pfade eines Netzes deaktiviert, um Loops zu vermeiden. Falls auf der Strecke eine Netzkomponente ausfällt, berechnet das Gerät die neue Topologie und aktiviert diese Pfade wieder.

Das Rapid Spanning Tree Protocol (RSTP) ermöglicht schnelles Umschalten auf eine neu berechnete Topologie, ohne dabei bestehende Verbindungen zu unterbrechen. RSTP erreicht durchschnittliche Rekonfigurationszeiten von unter einer Sekunde. Wenn Sie RSTP in einem Ring mit 10 bis 20 Geräten einsetzen, erreichen Sie Rekonfigurationszeiten im Millisekundenbereich.

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

Das Menü enthält die folgenden Dialoge:

- Spanning Tree Global
- Spanning Tree Dual RSTP (MCSESM-E)
- Spanning Tree Port

5.10.3.1 Spanning Tree Global

[Switching > L2-Redundanz > Spanning Tree > Global]

In diesem Dialog schalten Sie die Funktion *Spanning Tree* ein-/aus und legen die Bridge-Einstellungen fest.

Funktion

Funktion

Schaltet die Spanning-Tree-Funktion im Gerät ein/aus.

Mögliche Werte:

- `An` (Voreinstellung)
- `Aus`
  Das Gerät verhält sich transparent. Empfangene Spanning-Tree-Datenpakete flutet das Gerät wie Multicast-Datenpakete an den Ports.

Variante

Variante

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

Mögliche Werte:

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

Traps

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps für die folgenden Ereignisse:

- Eine andere Bridge übernimmt die Rolle der Root-Bridge.
- Die Topologie ändert sich. Ein Port ändert *Port-Zustand* von *forwarding* zu *discarding* oder von *discarding* zu *forwarding*.

Mögliche Werte:

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

Bridge-Konfiguration

Bridge-ID

Zeigt die Bridge-ID des Geräts.

Das Gerät mit dem kleinsten nummerischen Bridge-ID-Wert übernimmt die Rolle der Root-Bridge im Netz.

Mögliche Werte:

- `<Bridge-Priorität> / <MAC-Adresse>`
  Wert im Feld *Priorität* / MAC-Adresse des Geräts

Priorität

Legt die Bridge-Priorität des Geräts fest.

Mögliche Werte:

- `0..61440` in 4096er-Schritten (Voreinstellung: `32768`)

Um das Gerät zur Root-Bridge zu machen, weisen Sie dem Gerät den kleinsten nummerischen Wert für die Priorität im Netz zu.

Hello-Time [s]

Legt die Zeit in Sekunden fest zwischen dem Senden zweier Konfigurationsmeldungen (Hello-Datenpakete).

Mögliche Werte:

- `1..2` (Voreinstellung: `2`)

Wenn das Gerät die Rolle der Root-Bridge übernimmt, dann verwenden die anderen Geräte im Netz den hier festgelegten Wert.

Andernfalls verwendet das Gerät den von der Root-Bridge vorgegebenen Wert. Siehe Rahmen *Root-Information*.

Aufgrund der Wechselwirkung mit dem Parameter *Tx holds* empfehlen wir, den voreinstellten Wert beizubehalten.

Forward-Verzögerung [s]

Legt die Verzögerungszeit für Zustandswechsel in Sekunden fest.

Mögliche Werte:

- `4..30` (Voreinstellung: `15`)

Wenn das Gerät die Rolle der Root-Bridge übernimmt, dann verwenden die anderen Geräte im Netz den hier festgelegten Wert.

Andernfalls verwendet das Gerät den von der Root-Bridge vorgegebenen Wert. Siehe Rahmen *Root-Information*.

Im Protokoll RSTP handeln die Bridges Zustandswechsel ohne vorgegebene Verzögerung aus.

Das *Spanning Tree*-Protokoll verwendet den Parameter, um den Wechsel zwischen den Zuständen *disabled*, *discarding*, *learning*, *forwarding* zu verzögern.

Die Parameter *Forward-Verzögerung [s]* und *Max age* stehen in folgender Beziehung zueinander:

Forward-Verzögerung [s] ≥ (*Max age*/2) + 1

Wenn Sie in die Felder einen Wert einfügen, der dieser Beziehung widerspricht, dann ersetzt das Gerät diese Werte mit den zuletzt gültigen Werten oder mit der Voreinstellung.

Max age

Legt die maximal zulässige Astlänge fest, d. h. die Anzahl der Geräte bis zur Root-Bridge.

Mögliche Werte:

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

Wenn das Gerät die Rolle der Root-Bridge übernimmt, dann verwenden die anderen Geräte im Netz den hier festgelegten Wert.

Andernfalls verwendet das Gerät den von der Root-Bridge vorgegebenen Wert. Siehe Rahmen *Root-Information*.

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

Tx holds

Begrenzt die maximale Übertragungsrate für das Senden von BPDUs.

Mögliche Werte:

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

Sendet das Gerät eine BPDU, inkrementiert das Gerät auf diesem Port einen Zähler.

Erreicht der Zähler den hier festgelegten Wert, stellt der Port das Senden weiterer BPDUs ein. Dies reduziert einerseits die durch RSTP erzeugte Last, andererseits kann es zur Unterbrechung der Kommunikation kommen, wenn das Gerät keine BPDUs empfängt.

Das Gerät dekrementiert den Zähler jede Sekunde um `1`. In der folgenden Sekunde sendet das Gerät maximal `1` neue BPDU.

BPDU-Guard

Schaltet die BPDU-Guard-Funktion im Gerät ein/aus.

Mit dieser Funktion hilft das Gerät, Ihr Netz vor Fehlkonfigurationen, Angriffen mit STP-BPDUs und unerwünschten Topologieänderungen zu schützen.

Mögliche Werte:

- `markiert`
  Der *BPDU-Guard* ist aktiv.
  - Das Gerät wendet die Funktion auf manuell festgelegte Edge-Ports an. Bei diesen Ports ist im Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Registerkarte *CIST*, das Kontrollkästchen in Spalte *Admin-Edge-Port* markiert.
  - Wenn ein Edge-Port eine STP-BPDU empfängt, dann schaltet das Gerät den Port aus. Im Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration* ist bei diesem Port das Kontrollkästchen in Spalte *Port an*`unmarkiert`.
- `unmarkiert` (Voreinstellung)
  Der *BPDU-Guard* ist inaktiv.

Um den Status des Ports wieder auf den Wert *forwarding* zu setzen, gehen Sie wie folgt vor:

- Wenn der Port weiterhin BPDUs empfängt:
  - Heben Sie im Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Registerkarte *CIST*, die Markierung des Kontrollkästchens in Spalte *Admin-Edge-Port* auf.
    oder
  - Heben Sie im Dialog *Switching > L2-Redundanz > Spanning Tree > Global* die Markierung des Kontrollkästchen *BPDU-Guard* auf.
- Um den Port wieder einzuschalten, verwenden Sie die Funktion *Auto-Disable*. Alternativ gehen Sie wie folgt vor:
  - Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
  - Markieren Sie das Kontrollkästchen in Spalte *Port an*.

BPDU-Filter (alle Admin-Edge-Ports)

Aktiviert/deaktiviert den STP-BPDU-Filter auf jedem manuell festgelegten Edge-Port. Bei diesen Ports ist im Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Registerkarte *CIST*, das Kontrollkästchen in Spalte *Admin-Edge-Port* markiert.

Mögliche Werte:

- `markiert`
  Der BPDU-Filter ist auf jedem Edge-Port aktiv.
  Die Funktion verwendet diese Ports nicht im *Spanning Tree*-Betrieb.
  - Das Gerät sendet keine STP-BPDUs auf diesen Ports.
  - Das Gerät verwirft jede STP-BPDU, die es auf diesen Ports empfängt.
- `unmarkiert` (Voreinstellung)
  Der globale BPDU-Filter ist inaktiv.
  Sie haben die Möglichkeit, den BPDU-Filter für einzelne Ports explizit zu aktivieren. Siehe Spalte *BPDU-Filter Port* im Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für die Parameter, deren Einhaltung der *BPDU-Guard* auf dem Port überwacht.

Mögliche Werte:

- `markiert`
  Die Funktion *Auto-Disable* für den *BPDU-Guard* ist aktiv.
  - Wenn der Port eine STP-BPDU empfängt, schaltet das Gerät einen Edge-Port aus. Die „Link-Status“-LED des Ports blinkt 3× pro Periode.
  - Der Dialog *Diagnose > Ports > Auto-Disable* zeigt, welche Ports aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet sind.
  - Die Funktion *Auto-Disable* schaltet den Port automatisch wieder ein. Legen Sie dazu im Dialog *Diagnose > Ports > Auto-Disable* in Spalte *Reset-Timer [s]* eine Wartezeit für den betreffenden Port fest.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Auto-Disable* für den *BPDU-Guard* ist inaktiv.

Root-Information

Bridge-ID

Zeigt die Bridge-ID der gegenwärtigen Root-Bridge.

Mögliche Werte:

- `<Bridge-Priorität> / <MAC-Adresse>`

Priorität

Zeigt die Bridge-Priorität der gegenwärtigen Root-Bridge.

Mögliche Werte:

- `0..61440` in 4096er-Schritten

Hello-Time [s]

Zeigt die von der Root-Bridge vorgegebene Zeit in Sekunden zwischen dem Senden zweier Konfigurationsmeldungen (Hello-Datenpakete).

Mögliche Werte:

- `1..2`

Das Gerät verwendet diesen vorgegebenen Wert. Siehe Rahmen *Bridge-Konfiguration*.

Forward-Verzögerung [s]

Zeigt die von der Root-Bridge vorgegebene Verzögerungzeit für Zustandswechsel in Sekunden.

Mögliche Werte:

- `4..30`

Das Gerät verwendet diesen vorgegebenen Wert. Siehe Rahmen *Bridge-Konfiguration*.

Im Protokoll RSTP handeln die Bridges Zustandswechsel ohne vorgegebene Verzögerung aus.

Das *Spanning Tree*-Protokoll verwendet den Parameter, um den Wechsel zwischen den Zuständen *disabled*, *discarding*, *learning*, *forwarding* zu verzögern.

Max age

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

Mögliche Werte:

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

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

Topologie-Information

Bridge ist Root

Zeigt, ob das Gerät gegenwärtig die Rolle der Root-Bridge übernimmt.

Mögliche Werte:

- `markiert`
  Das Gerät übernimmt gegenwärtig die Rolle der Root-Bridge.
- `unmarkiert`
  Gegenwärtig übernimmt ein anderes Gerät die Rolle der Root-Bridge.

Root-Port

Zeigt die Nummer des Ports, von dem der gegenwärtige Pfad zur Root-Bridge führt.

Übernimmt das Gerät die Rolle der Root-Bridge, dann zeigt das Feld den Wert `no Port`.

Root-Pfadkosten

Zeigt die Pfadkosten für den Pfad, der vom Root-Port des Geräts zur Root-Bridge des Schicht-2-Netzes führt.

Mögliche Werte:

- `0..200000000`
  Wenn der Wert `0` festgelegt ist, dann übernimmt das Gerät die Rolle der Root-Bridge.

Topologie-Änderungen

Zeigt, wie viele Male seit dem Start der *Spanning Tree*-Instanz das Gerät einen Port durch die Funktion *Spanning Tree* in den Zustand *forwarding* gesetzt hat.

Zeit seit letzter Änderung

Zeigt die Zeit seit der letzten Topologieänderung.

Mögliche Werte:

- `<Tage, Stunden:Minuten:Sekunden>`

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.10.3.2 Spanning Tree Dual RSTP (MCSESM-E)

[Switching > L2-Redundanz > Spanning Tree > Dual RSTP]

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *RCP*- und *Dual RSTP*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der Ring-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

In diesem Dialog legen Sie die Bridge-Einstellungen für die zweite *Spanning Tree*-Instanz fest.

Die Funktion *Dual RSTP* wird zusammen mit der Funktion *RCP* verwendet. Mit der Funktion *RCP* haben Sie die Möglichkeit, einen oder mehrere RSTP-Ringe mit der RSTP-Instanz an einen Primär-Ring zu koppeln. Beim Koppeln von 2 *Spanning Tree*-Segmenten repräsentiert der Sekundär-Ring eine separate RSTP-Instanz, für welche die Einstellungen der Funktion *Dual RSTP* gelten. Diese *Dual RSTP*-Instanz arbeitet unabhängig von der RSTP-Instanz Primär-Rings und der anderen Sekundär-Ringe. Ist RSTP in ausschließlich einem der zu koppelnden Ringe das verwendete Protokoll, benötigen Sie die Funktion *Dual RSTP* nicht.

Die Einstellungen der Funktion *RCP* legen Sie im Dialog *Switching > L2-Redundanz > FuseNet > RCP* fest.

Funktion

Funktion

Zeigt, ob die Funktion *Dual RSTP* im Gerät eingeschaltet ist.

Mögliche Werte:

- *An*
  Die Funktion *Dual RSTP* ist im Gerät eingeschaltet.
  Das Gerät schaltet die *Dual RSTP* Funktion selbständig ein, wenn folgende Voraussetzungen erfüllt sind:
  - Im Dialog *Switching > L2-Redundanz > FuseNet > RCP* haben Sie die Ports für die Einstellungen *Primärer Ring/Netzwerk* und *Sekundärer Ring/Netzwerk* festgelegt.
  - Im Dialog *Switching > L2-Redundanz > FuseNet > RCP*, Rahmen *Funktion* haben Sie die Funktion *RCP* eingeschaltet.
  - Im Dialog *Spanning Tree Global*, Rahmen *Funktion* haben Sie die Funktion *Spanning Tree* eingeschaltet.
  - Im Sekundär-Ring ist kein Redundanzprotokoll konfiguriert.
- *Aus* (Voreinstellung)
  Die Funktion *Dual RSTP* ist im Gerät ausgeschaltet.

Traps

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps für die folgenden Ereignisse:

- Eine andere Bridge übernimmt die Rolle der Root-Bridge.
- Die Topologie ändert sich. Ein Port ändert den *Port-Zustand* von *forwarding* zu *discarding* oder von *discarding* zu *forwarding*.

Mögliche Werte:

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

Bridge-Konfiguration

Bridge-ID

Zeigt die Bridge-ID des Geräts.

Das Gerät mit dem kleinsten nummerischen Bridge-ID-Wert übernimmt die Rolle der Root-Bridge im Netz.

Mögliche Werte:

- `<Bridge-Priorität> / <MAC-Adresse>`
  Wert im Feld *Priorität* / MAC-Adresse des Geräts

Priorität

Legt die Bridge-Priorität des Geräts fest.

Mögliche Werte:

- `0..61440` in 4096er-Schritten (Voreinstellung: `32768`)

Um das Gerät zur Root-Bridge zu machen, weisen Sie dem Gerät den kleinsten nummerischen Wert für die Priorität im Netz zu.

Hello-Time [s]

Legt die Zeit in Sekunden fest zwischen dem Senden zweier Konfigurationsmeldungen (Hello-Datenpakete).

Mögliche Werte:

- `1..2` (Voreinstellung: `2`)

Wenn das Gerät die Rolle der Root-Bridge übernimmt, dann verwenden die anderen Geräte im Netz den hier festgelegten Wert.

Andernfalls verwendet das Gerät den von der Root-Bridge vorgegebenen Wert. Siehe Rahmen *Root-Information*.

Aufgrund der Wechselwirkung mit dem Parameter *Tx holds* empfehlen wir, den voreinstellten Wert beizubehalten.

Forward-Verzögerung [s]

Legt die Verzögerungszeit für Zustandswechsel in Sekunden fest.

Mögliche Werte:

- `4..30` (Voreinstellung: `15`)

Wenn das Gerät die Rolle der Root-Bridge übernimmt, dann verwenden die anderen Geräte im Netz den hier festgelegten Wert. Andernfalls verwendet das Gerät den von der Root-Bridge vorgegebenen Wert. Siehe Rahmen *Root-Information*.

Im Protokoll RSTP handeln die Bridges Zustandswechsel ohne vorgegebene Verzögerung aus.

Das *Spanning Tree*-Protokoll verwendet den Parameter, um den Wechsel zwischen den Zuständen `disabled`, `discarding`, `learning`, `forwarding` zu verzögern.

Die Parameter *Forward-Verzögerung [s]* und *Max age* stehen in folgender Beziehung zueinander:

Forward-Verzögerung [s] ≥ (*Max age*/2) + 1

Max age

Legt fest, wie viele Geräte auf dem Pfad zur Root-Bridge maximal zulässig sind.

Mögliche Werte:

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

Wenn das Gerät die Rolle der Root-Bridge übernimmt, dann verwenden die anderen Geräte im Netz den hier festgelegten Wert. Andernfalls verwendet das Gerät den von der Root-Bridge vorgegebenen Wert. Siehe Rahmen *Root-Information*.

Tx holds

Begrenzt die maximale Übertragungsrate für das Senden von BPDUs.

Mögliche Werte:

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

Sendet das Gerät eine BPDU, inkrementiert das Gerät auf diesem Port einen Zähler.

Erreicht der Zähler den hier festgelegten Wert, stellt der Port das Senden weiterer BPDUs ein. Dies reduziert einerseits die durch RSTP erzeugte Last, andererseits kann es zur Unterbrechung der Kommunikation kommen, wenn das Gerät keine BPDUs empfängt.

Das Gerät dekrementiert den Zähler jede Sekunde um `1`. In der folgenden Sekunde sendet das Gerät maximal `1` neue BPDU.

BPDU-Guard

Schaltet die BPDU-Guard-Funktion im Gerät ein/aus.

Mit dieser Funktion hilft das Gerät, Ihr Netz vor Fehlkonfigurationen, Angriffen mit STP-BPDUs und unerwünschten Topologieänderungen zu schützen.

Mögliche Werte:

- `markiert`
  Der *BPDU-Guard* ist aktiv.
  - Das Gerät wendet die Funktion auf manuell festgelegte Edge-Ports an. Bei diesen Ports ist im Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Registerkarte *CIST*, das Kontrollkästchen in Spalte *Admin-Edge-Port* markiert.
  - Wenn ein Edge-Port eine STP-BPDU empfängt, dann schaltet das Gerät den Port aus. Im Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration* ist bei diesem Port das Kontrollkästchen in Spalte *Port an*`unmarkiert`.
- `unmarkiert` (Voreinstellung)
  Der *BPDU-Guard* ist inaktiv.

Um den Status des Ports wieder auf den Wert `forwarding` zu setzen, gehen Sie wie folgt vor:

- ☐ Wenn der Port weiterhin BPDUs empfängt:
  - Heben Sie im Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Registerkarte *CIST*, die Markierung des Kontrollkästchens in Spalte *Admin-Edge-Port* auf.
    oder
  - Heben Sie im Dialog *Switching > L2-Redundanz > Spanning Tree > Dual RSTP* die Markierung des Kontrollkästchen *BPDU-Guard* auf.
- ☐ Um den Port wieder einzuschalten, gehen Sie wie folgt vor:
  - Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
  - Markieren Sie das Kontrollkästchen in Spalte *Port an*.

BPDU-Filter (alle Admin-Edge-Ports)

Aktiviert/deaktiviert den STP-BPDU-Filter auf jedem manuell festgelegten Edge-Port. Bei diesen Ports ist im Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Registerkarte *CIST*, das Kontrollkästchen in Spalte *Admin-Edge-Port* markiert.

Mögliche Werte:

- `markiert`
  Der BPDU-Filter ist auf jedem Edge-Port aktiv.
  Die Funktion verwendet diese Ports nicht im *Spanning Tree*-Betrieb.
  - Das Gerät sendet keine STP-BPDUs auf diesen Ports.
  - Das Gerät verwirft jede STP-BPDU, die es auf diesen Ports empfängt.
- `unmarkiert` (Voreinstellung)
  Der globale BPDU-Filter ist inaktiv.
  Sie haben die Möglichkeit, den BPDU-Filter für einzelne Ports explizit zu aktivieren. Siehe Spalte *BPDU-Filter Port* im Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.

Root-Information

Root-ID

Zeigt die Bridge-ID der gegenwärtigen Root-Bridge.

Mögliche Werte:

- `<Bridge-Priorität> / <MAC-Adresse>`

Priorität

Zeigt die Bridge-Priorität der gegenwärtigen Root-Bridge.

Mögliche Werte:

- `0..61440` in 4096er-Schritten

Hello-Time [s]

Zeigt die von der Root-Bridge vorgegebene Zeit in Sekunden zwischen dem Senden zweier Konfigurationsmeldungen (Hello-Datenpakete).

Mögliche Werte:

- `1..2`

Das Gerät verwendet diesen vorgegebenen Wert. Siehe Rahmen *Bridge-Konfiguration*.

Forward-Verzögerung [s]

Zeigt die von der Root-Bridge vorgegebene Verzögerungzeit für Zustandswechsel in Sekunden.

Mögliche Werte:

- `4..30`

Das Gerät verwendet diesen vorgegebenen Wert. Siehe Rahmen *Bridge-Konfiguration*.

Im Protokoll RSTP handeln die Bridges Zustandswechsel ohne vorgegebene Verzögerung aus.

Das *Spanning Tree*-Protokoll verwendet den Parameter, um den Wechsel zwischen den Zuständen *disabled*, *discarding*, *learning*, *forwarding* zu verzögern.

Max age

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

Mögliche Werte:

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

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

Topologie-Information

Bridge ist Root

Zeigt, ob das Gerät gegenwärtig die Rolle der Root-Bridge übernimmt.

Mögliche Werte:

- `markiert`
  Das Gerät übernimmt gegenwärtig die Rolle der Root-Bridge.
- `unmarkiert`
  Gegenwärtig übernimmt ein anderes Gerät die Rolle der Root-Bridge.

Root-Port

Zeigt die Nummer des Ports, von dem der gegenwärtige Pfad zur Root-Bridge führt.

Übernimmt das Gerät die Rolle der Root-Bridge, dann zeigt das Feld den Wert `no Port`.

Root-Pfadkosten

Zeigt die Pfadkosten für den Pfad, der vom Root-Port des Geräts zur Root-Bridge des Schicht-2-Netzes führt.

Mögliche Werte:

- `0..200000000`
  Wenn der Wert `0` festgelegt ist, dann übernimmt das Gerät die Rolle der Root-Bridge.

Topologie-Änderungen

Zeigt, wie viele Male seit dem Start der *Spanning Tree*-Instanz das Gerät einen Port durch die Funktion *Spanning Tree* in den Zustand *forwarding* gesetzt hat.

Zeit seit letzter Änderung

Zeigt die Zeit seit der letzten Topologieänderung.

Mögliche Werte:

- `<Tage, Stunden:Minuten:Sekunden>`

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.10.3.3 Spanning Tree Port

[Switching > L2-Redundanz > Spanning Tree > Port]

In diesem Dialog aktivieren Sie die Spanning-Tree-Funktion auf den Ports, legen Edge-Ports sowie die Einstellungen für verschiedene Schutzfunktionen fest.

Der Dialog enthält die folgenden Registerkarten:
- [CIST]
- [Guards]

[CIST]

In dieser Registerkarte haben Sie die Möglichkeit, an den Ports die Spanning-Tree-Funktion einzeln zu aktivieren, die Einstellungen für Edge-Ports festzulegen sowie gegenwärtige Werte anzusehen. Die Abkürzung CIST steht für „Common and Internal Spanning Tree“.

Anmerkung: Deaktivieren Sie die Funktion *Spanning Tree* auf den Ports, die an anderen Schicht-2-Redundanzprotokollen beteiligt sind. Andernfalls arbeiten die Redundanz-Protokolle möglicherweise anders als vorgesehen. Dies kann zu Loops führen.

Tabelle

Port

Zeigt die Nummer des Ports.

STP aktiv

Schaltet die Spanning-Tree-Funktion auf dem Port ein/aus.

Mögliche Werte:
- `markiert` (Voreinstellung)
  Die Funktion *Spanning Tree* ist auf dem Port aktiv.
- `unmarkiert`
  Die Funktion *Spanning Tree* ist auf dem Port inaktiv.
  Wenn die Funktion *Spanning Tree* im Gerät eingeschaltet und auf dem Port inaktiv ist, dann sendet der Port keine STP-BPDUs und verwirft empfangene STP-BPDUs.

Port-Zustand

Zeigt den Vermittlungsstatus des Ports.

Mögliche Werte:
- *discarding*
  Der Port ist blockiert und leitet ausschließlich STP-BPDUs weiter.
- *learning*
  Der Port ist blockiert, lernt jedoch die MAC-Adressen empfangener Datenpakete.
- *forwarding*
  Der Port leitet Datenpakete weiter.

- *disabled*
  Der Port ist inaktiv. Siehe Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
- *manualFwd*
  Die Funktion *Spanning Tree* ist auf dem Port ausgeschaltet. Der Port leitet STP-BPDUs weiter.
- *notParticipate*
  Der Port nimmt nicht an STP teil.

Port-Rolle

Zeigt die gegenwärtige Rolle des Ports im CIST.

Mögliche Werte:

- *root*
  Port mit dem günstigsten Pfad zur Root-Bridge.
- *alternate*
  Port mit dem alternativen Pfad zur Root-Bridge (gegenwärtig blockierend).
- *designated*
  Port zur von der Root-Bridge abgewandten Seite des Baums (gegenwärtig blockierend).
- *backup*
  Port empfängt STP-BPDUs des eigenen Geräts.
- *disabled*
  Der Port ist inaktiv. Siehe Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.

Port-Pfadkosten

Legt die Pfadkosten des Ports fest.

Mögliche Werte:

- `0..200000000` (Voreinstellung: `0`)

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

Port-Priorität

Legt die Priorität des Ports fest.

Mögliche Werte:

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

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

Empfangene Bridge-ID

Zeigt die Bridge-ID des Geräts, von dem dieser Port zuletzt eine STP-BPDU empfangen hat.

Mögliche Werte:

- Für Ports mit der Rolle *designated* zeigt das Gerät die Information der STP-BPDU, die der Port zuletzt empfangen hat. Dies erleichtert die Diagnose von möglichen STP-Problemen im Netz.
- Für die Port-Rollen *alternate*, *backup*, *master* und *root* sind diese Informationen im stationären Zustand (statische Topologie) identisch mit den Informationen der Port-Rolle *designated*.
- Hat ein Port keine Verbindung oder hat er noch keine STP-BDPU empfangen, zeigt das Gerät die Werte, die der Port mit der Rolle *designated* senden würde.

Empfangene Port-ID

Zeigt die Port-ID des Geräts, von dem dieser Port zuletzt eine STP-BPDU empfangen hat.

Mögliche Werte:

- Für Ports mit der Rolle `designated` zeigt das Gerät die Information der STP-BPDU, die der Port zuletzt empfangen hat. Dies erleichtert die Diagnose von möglichen STP-Problemen im Netz.
- Für die Port-Rollen `alternate`, `backup`, `master` und `root` sind diese Informationen im stationären Zustand (statische Topologie) identisch mit den Informationen der Port-Rolle `designated`.
- Hat ein Port keine Verbindung oder hat er noch keine STP-BDPU empfangen, zeigt das Gerät die Werte, die der Port mit der Rolle `designated` senden würde.

Empfangene Port-Pfadkosten

Zeigt die Pfadkosten, welche die übergeordnete Bridge von ihrem Root-Port zur Root-Bridge hat.

Mögliche Werte:

- Für Ports mit der Rolle `designated` zeigt das Gerät die Information der STP-BPDU, die der Port zuletzt empfangen hat. Dies erleichtert die Diagnose von möglichen STP-Problemen im Netz.
- Für die Port-Rollen `alternate`, `backup`, `master` und `root` sind diese Informationen im stationären Zustand (statische Topologie) identisch mit den Informationen der Port-Rolle `designated`.
- Hat ein Port keine Verbindung oder hat er noch keine STP-BDPU empfangen, zeigt das Gerät die Werte, die der Port mit der Rolle `designated` senden würde.

Admin-Edge-Port

Aktiviert/deaktiviert den *Admin-Edge-Port*-Modus. Wenn ein Endgerät an den Port angeschlossen ist, dann verwenden Sie den *Admin-Edge-Port*-Modus. Diese Einstellung ermöglicht dem Edge-Port, nach dem LinkUp schneller in den Zustand 'forwarding' zu schalten und damit das Endgerät schneller erreichbar zu machen.

Mögliche Werte:

- `markiert`
  Der *Admin-Edge-Port*-Modus ist aktiv.
  Der Port ist mit einem Endgerät verbunden.
  - Nach Aufbau der Verbindung wechselt der Port in den Zustand `forwarding`, ohne zuvor in den Zustand `learning` zu wechseln.
  - Empfängt der Port eine STP-BPDU, deaktiviert das Gerät den Port, falls die BPDU-Guard-Funktion aktiv ist. Siehe Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- `unmarkiert` (Voreinstellung)
  Der *Admin-Edge-Port*-Modus ist inaktiv.
  Der Port ist mit einer anderen STP-Bridge verbunden.
  Nach Aufbau der Verbindung wechselt der Port in den Zustand `learning`, bevor er ggf. in den Zustand `forwarding` wechselt.

Auto-Edge-Port

Aktiviert/deaktiviert die automatische Erkennung, ob an den Port ein Endgerät angeschlossen ist. Voraussetzung ist, dass das Kontrollkästchen in Spalte *Admin-Edge-Port*`unmarkiert` ist.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die automatische Erkennung ist aktiv.
  Nach Aufbau der Verbindung setzt das Gerät den Port nach 1,5 × *Hello-Time [s]* in den Zustand *`forwarding`* (in der Voreinstellung 1,5 × 2 s), falls der Port währenddessen keine STP-BPDU empfängt.
- `unmarkiert`
  Die automatische Erkennung ist inaktiv.
  Nach Aufbau der Verbindung setzt das Gerät den Port nach *Max age* in den Zustand *`forwarding`*.
  (Voreinstellung: 20 s)

Oper-Edge-Port

Zeigt, ob an den Port ein Endgerät oder eine STP-Bridge angeschlossen ist.

Mögliche Werte:

- `markiert`
  An den Port ist ein Endgerät angeschlossen. Der Port empfängt keine STP-BPDUs.
- `unmarkiert`
  An den Port ist eine STP-Bridge angeschlossen. Der Port empfängt STP-BPDUs.

Oper PointToPoint

Zeigt, ob der Port über eine direkte Vollduplex-Verbindung mit einem STP-Gerät verbunden ist.

Mögliche Werte:

- `markiert`
  Der Port ist über eine Vollduplex-Verbindung direkt mit einem STP-Gerät verbunden. Die direkte, dezentrale Kommunikation zwischen 2 Bridges bewirkt kurze Rekonfigurationszeiten
- `unmarkiert`
  Der Port ist auf andere Weise verbunden, zum Beispiel über eine Halbduplex-Verbindung oder über einen Hub.

BPDU-Filter Port

Aktiviert/deaktiviert die Filterung von STP-BPDUs explizit auf diesem Port.

Voraussetzung ist, dass der Port ein manuell festgelegter Edge-Port ist. Bei diesen Ports ist das Kontrollkästchen in Spalte *Admin-Edge-Port* markiert.

Mögliche Werte:

- `markiert`
  Der BPDU-Filter ist auf dem Port aktiv.
  Die Funktion schließt den Port von *Spanning Tree*-Operationen aus.
  - Das Gerät sendet keine STP-BPDUs auf dem Port.
  - Das Gerät verwirft jede STP-BPDU, die es auf dem Port empfängt.
- `unmarkiert` (Voreinstellung)
  Der BPDU-Filter ist auf dem Port inaktiv.
  Sie haben die Möglichkeit, den BPDU-Filter global für jeden manuell festgelegten Edge-Port zu aktivieren. Siehe Dialog *Switching > L2-Redundanz > Spanning Tree > Global*, Rahmen *Bridge-Konfiguration*.
  Wenn das Kontrollkästchen *BPDU-Filter (alle Admin-Edge-Ports)* markiert ist, dann ist der BPDU-Filter auf dem Port noch aktiv.

Status BPDU-Filter

Zeigt, ob der BPDU-Filter auf dem Port aktiv ist.

Mögliche Werte:

- `markiert`
  Der BPDU-Filter ist auf dem Port aktiv aufgrund der folgenden Einstellungen:
  - Das Kontrollkästchen in Spalte *BPDU-Filter Port* ist markiert.
    und/oder
  - Das Kontrollkästchen in Spalte *BPDU-Filter (alle Admin-Edge-Ports)* ist markiert. Siehe Dialog *Switching > L2-Redundanz > Spanning Tree > Global*, Rahmen *Bridge-Konfiguration*.
- `unmarkiert`
  Der BPDU-Filter ist auf dem Port inaktiv.

BPDU flood

Aktiviert/deaktiviert den *BPDU flood*-Modus auf dem Port, auch wenn die Funktion *Spanning Tree* auf dem Port inaktiv ist. Das Gerät flutet auf dem Port empfangene STP-BPDUs auf denjenigen Ports, für welche die Funktion *Spanning Tree* inaktiv und der *BPDU flood*-Modus zugleich aktiv ist.

Mögliche Werte:

- `markiert`
  Der *BPDU flood*-Modus ist aktiv.

- `unmarkiert` (Voreinstellung)
  Der *BPDU flood*-Modus ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Guards]

Diese Registerkarte ermöglicht Ihnen, an den Ports die Einstellungen für verschiedene Schutzfunktionen festzulegen.

Tabelle

Port

Zeigt die Nummer des Ports.

Root-Guard

Schaltet die Überwachung auf STP-BPDUs auf dem Port ein/aus. Voraussetzung ist, dass die Funktion *Loop-Guard* inaktiv ist.

Mit dieser Einstellung hilft das Gerät, Ihr Netz vor Fehlkonfigurationen und Angriffen mit STP-BPDUs zu schützen, welche die Topologie zu verändern versuchen. Diese Einstellung gilt ausschließlich für Ports mit der STP-Rolle `designated`.

Mögliche Werte:

- `markiert`
  Überwachung auf STP-BPDUs ist eingeschaltet.
  - Empfängt der Port eine STP-BPDU mit besserer Pfadinformation zur Root-Bridge, verwirft das Gerät die STP-BPDU und setzt den Zustand des Ports auf den Wert `discarding` anstatt auf `root`.
  - Bleiben STP-BPDUs mit besserer Pfadinformation zur Root-Bridge aus, setzt das Gerät den Zustand des Ports nach 2 × *Hello-Time [s]* zurück.
- `unmarkiert` (Voreinstellung)
  Überwachung auf STP-BPDUs ist inaktiv.

TCN-Guard

Schaltet die Überwachung auf „Topology Change Notifications“ auf dem Port ein/aus. Mit dieser Einstellung hilft das Gerät, Ihr Netz vor Angriffen mit STP-BPDUs zu schützen, welche die Topologie zu verändern versuchen.

Mögliche Werte:

- `markiert`
  Überwachung auf ‚Topology Change Notifications‘ ist eingeschaltet.
  - Der Port ignoriert das Topology-Change-Flag in empfangenen STP-BPDUs.
  - Enthält die empfangene BPDU weitere Informationen, die eine Topologieänderung bewirken, verarbeitet das Gerät diese auch bei eingeschaltetem TCN-Guard.
    Beispiel: Das Gerät empfängt eine bessere Pfadinformation zur Root-Bridge.
- `unmarkiert` (Voreinstellung)
  Überwachung auf ‚Topology Change Notifications‘ ist ausgeschaltet.
  Empfängt das Gerät STP-BPDUs mit Topology-Change-Flag, löscht es die Adresstabelle des Ports und leitet die Topology Change Notifications weiter.

Loop-Guard

Schaltet die Überwachung auf Loops auf dem Port ein/aus. Voraussetzung ist, dass die Funktion *Root-Guard* inaktiv ist.

Mit dieser Einstellung sorgt das Gerät dafür, Loops zu vermeiden, falls der Port keine STP-BPDUs mehr empfängt. Verwenden Sie diese Einstellung ausschließlich für Ports mit der STP-Rolle `alternate`, `backup` und `root`.

Mögliche Werte:

- `markiert`
  Überwachung auf Loops ist eingeschaltet. Dies sorgt dafür, Loops zu vermeiden, zum Beispiel wenn Sie die Spanning-Tree-Funktion auf dem entfernten Gerät ausschalten oder wenn die Verbindung lediglich in der Empfangsrichtung unterbrochen ist.
  - Empfängt der Port eine Zeitlang keine STP-BPDUs, setzt das Gerät den Zustand des Ports auf den Wert *`discarding`* und markiert das Kontrollkästchen in Spalte *Loop-Zustand*.
  - Empfängt der Port anschließend wieder STP-BPDUs, setzt das Gerät den Zustand des Ports auf einen Wert gemäß *Port-Rolle* und hebt die Markierung des Kontrollkästchens in Spalte *Loop-Zustand* auf.
- `unmarkiert` (Voreinstellung)
  Überwachung auf Loops ist ausgeschaltet.
  Empfängt der Port eine Zeitlang keine STP-BPDUs, setzt das Gerät den Zustand des Ports auf den Wert *`forwarding`*.

Loop-Zustand

Zeigt, ob der Loop-Zustand des Ports inkonsistent ist.

Mögliche Werte:

- `markiert`
  Der Loop-Status des Ports ist inkonsistent:
  - Der Port empfängt keine STP-BPDUs und die Funktion *Loop-Guard* ist eingeschaltet.
  - Das Gerät setzt den Status des Ports auf den Wert *`discarding`*. Damit sorgt das Gerät dafür, mögliche Loops zu vermeiden.
- `unmarkiert`
  Der Loop-Status des Ports ist konsistent. Der Port empfängt STP-BPDUs.

Übergänge in Loop-Zustand

Zeigt, wie viele Male der Loop-Zustand inkonsistent geworden ist (markiertes Kontrollkästchen in Spalte *Loop-Zustand*).

Übergänge aus Loop-Zustand

Zeigt, wie viele Male der Loop-Zustand konsistent geworden ist (unmarkiertes Kontrollkästchen in Spalte *Loop-Zustand*).

BPDU guard effect

Zeigt, ob der Port als Edge-Port eine STP-BPDU empfangen hat.

Voraussetzung:

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

Mögliche Werte:

- `markiert`
  Der Port ist Edge-Port und hat eine STP-BPDU empfangen.
  Das Gerät deaktiviert den Port. Im Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration* ist bei diesem Port das Kontrollkästchen in Spalte *Port an*`unmarkiert`.
- `unmarkiert`
  Der Port ist Edge-Port und hat keine STP-BPDU empfangen oder der Port ist kein Edge-Port.

Um den Status des Ports wieder auf den Wert *forwarding* zu setzen, gehen Sie wie folgt vor:

- ☐ Wenn der Port weiterhin BPDUs empfängt:
  - Heben Sie in der Registerkarte *CIST* die Markierung des Kontrollkästchens in Spalte *Admin-Edge-Port* auf.
    oder
  - Heben Sie im Dialog *Switching > L2-Redundanz > Spanning Tree > Global* die Markierung des Kontrollkästchen *BPDU-Guard* auf.
- ☐ Um den Port zu aktivieren, gehen Sie wie folgt vor:
  - Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
  - Markieren Sie das Kontrollkästchen in Spalte *Port an*.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.10.4 Link-Aggregation

[Switching > L2-Redundanz > Link-Aggregation]

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *Link-Aggregation*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der *Link-Aggregation*-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Die Funktion *Link-Aggregation* ermöglicht Ihnen, mehrere parallele Links zu bündeln. Voraussetzung ist, dass die Links mit gleicher Geschwindigkeit und im Vollduplex-Modus arbeiten. Die Vorteile gegenüber herkömmlichen Verbindungen über eine Leitung sind die höhere Verfügbarkeit und eine höhere Übertragungsbandbreite.

Das Link Aggregation Control Protocol (LACP) ermöglicht, den paketbasierten kontinuierlichen Link-Status auf den physischen Ports zu überwachen. LACP sorgt außerdem dafür, dass die Link-Partner die Voraussetzungen zum Bündeln erfüllen.

Wenn die Gegenstelle kein Link Aggregation Control Protocol (LACP) unterstützt, können Sie die Funktion *Statische Link-Aggregation* verwenden. In diesem Fall bündelt das Gerät die Links basierend auf Betriebsbereitschaft des Links, Verbindungsgeschwindigkeit und Duplexeinstellung.

Tabelle

Trunk-Port

Zeigt die Nummer des LAG-Interfaces.

Name

Legt den Namen des LAG-Interfaces fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..15 Zeichen

Link/Status

Zeigt den gegenwärtigen Betriebszustand des LAG-Interfaces und der physischen Ports.

Mögliche Werte:

- *up* (Zeile `lag/…`)
  Das LAG-Interface ist in Betrieb.
  Die Voraussetzungen sind:
  - Die Funktion *Statische Link-Aggregation* ist auf diesem LAG-Interface aktiv.
    oder
  - LACP ist auf den physischen Ports aktiv, die dem LAG-Interface zugewiesen sind, siehe Spalte *LACP Aktiv*.
    und
    Der in Spalte *LACP admin key* festgelegte Schlüssel für das LAG-Interface ist identisch mit den in Spalte *LACP port actor admin key* festgelegten Schlüsseln für die physischen Ports.
    und
    Die Anzahl der sich in Betrieb befindenden physischen Ports, die dem LAG-Interface zugewiesen sind, ist größer oder gleich dem in Spalte *Aktive Ports (min.)* festgelegten Wert.
- *up*
  Der physische Port ist in Betrieb.
- *down* (Zeile `lag/…`)
  Das LAG-Interface ist außer Betrieb.
- *down*
  Der physische Port ist ausgeschaltet.
  oder
  Kein Kabel angesteckt oder kein aktiver Link.

Aktiv

Aktiviert/deaktiviert das LAG-Interface.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das LAG-Interface ist aktiv.
  Berücksichtigen Sie, dass auf den physischen Ports die folgenden Protokolle nicht ordnungsgemäß funktionieren, wenn Sie das LAG-Interface aktivieren.
  - *PTP*
  - *802.1AS*
- `unmarkiert`
  Das LAG-Interface ist inaktiv.

STP aktiv

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

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

Mögliche Werte:

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

Statische Link-Aggregation

Aktiviert/deaktiviert die Funktion *Statische Link-Aggregation* auf dem LAG-Interface. Das Gerät bindet die zugewiesenen physischen Ports in das LAG-Interface ein, auch wenn die Gegenstelle LACP nicht unterstützt.

Mögliche Werte:

- `markiert`
  Die Funktion *Statische Link-Aggregation* ist auf diesem LAG-Interface aktiv. Das Gerät bindet einen zugewiesenen physischen Port in das LAG-Interface ein, sobald der physische Port einen Link aufbaut. Das Gerät sendet keine LACPDUs und verwirft empfangene LACPDUs.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Statische Link-Aggregation* ist auf diesem LAG-Interface inaktiv. Wenn die Verbindung zuvor erfolgreich mit LACP ausgehandelt wurde, bindet das Gerät einen zugewiesenen physischen Port in das LAG-Interface ein.

MTU

Legt die auf dem LAG-Interface maximal zulässige Größe der Ethernet-Pakete in Byte fest. Ein vorhandenes VLAN-Tag wird nicht berücksichtigt.

Diese Einstellung ermöglicht Ihnen, für bestimmte Anwendungen die Ethernet-Pakete zu erhöhen.

Mögliche Werte:

- `1518..9720` (Voreinstellung: `1518`)
  Mit dem Wert `1518` überträgt das LAG-Interface Ethernet-Pakete bis einschließlich folgender Größe:
  - 1518 Byte ohne VLAN-Tag
    (1514 Byte + 4 Byte CRC)
  - 1522 Byte mit VLAN-Tag
    (1518 Byte + 4 Byte CRC)

Aktive Ports (min.)

Legt fest, wie viele physische Ports mindestens aktiv sein müssen, damit das LAG-Interface aktiv ist. Wenn die Anzahl der aktiven physischen Ports kleiner ist als der festgelegte Wert, dann deaktiviert das Gerät das LAG-Interface.

Mit dieser Funktion erzwingen Sie, dass das Gerät automatisch auf die redundante Leitung umschaltet, wenn im Gerät eine Redundanzfunktion wie *Spanning Tree* oder *MRP* over LAG aktiv ist.

Mögliche Werte:

- `1` (Voreinstellung)
- `2`
- Abhängig von der Hardware:
  `4`
  `8`
  `32`

Typ

Zeigt, ob das LAG-Interface mit der Funktion *Statische Link-Aggregation* oder mit LACP arbeitet.

Mögliche Werte:

- *`static`*
  Das LAG-Interface arbeitet mit der Funktion *Statische Link-Aggregation*.
- *`dynamic`*
  Das LAG-Interface arbeitet mit der Funktion LACP.

Trap senden (Link-Up/Down)

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung des Link-Status auf diesem Interface erkennt.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Senden von SNMP-Traps ist aktiv.
  Wenn das Gerät eine Link-Status-Änderung erkennt, sendet es einen SNMP-Trap.
- `unmarkiert`
  Das Senden von SNMP-Traps ist inaktiv.

Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog *Diagnose* > Statuskonfiguration > *Alarme (Traps)* einschalten und mindestens ein Trap-Ziel festlegen.

LACP admin key

Legt den Schlüssel des LAG-Interfaces fest. Das Gerät verwendet den Schlüssel, um diejenigen Ports zu identifizieren, die es in das LAG-Interface einbinden darf.

Mögliche Werte:

- `0..65535`
  Den korrespondierenden Wert für die physischen Ports legen Sie in Spalte *LACP port actor admin key* fest.

Port

Zeigt die Nummer der physischen Ports, die dem LAG-Interface zugewiesen sind.

Aggregation Port Status

Zeigt, ob das LAG-Interface den physischen Port eingebunden hat.

Mögliche Werte:

- *aktiv*
  Das LAG-Interface hat den physischen Port eingebunden.
- *inaktiv*
  Das LAG-Interface hat den physischen Port nicht eingebunden.

LACP Aktiv

Aktiviert/deaktiviert LACP auf dem physischen Port.

Mögliche Werte:

- `markiert` (Voreinstellung)
  LACP ist auf dem physischen Port aktiv.
- `unmarkiert`
  LACP ist auf dem physischen Port inaktiv.

LACP port actor admin key

Legt den Schlüssel des physischen Ports fest. Das Gerät verwendet den Schlüssel, um diejenigen Ports zu identifizieren, die es in das LAG-Interface einbinden darf.

Mögliche Werte:

- `0`
  Das Gerät ignoriert den Schlüssel auf diesem physischen Port bei der Entscheidung, den Port in das LAG-Interface einzubinden.
- `1..65535`
  Das Gerät bindet diesen physischen Port ausschließlich dann in das LAG-Interface ein, wenn der Wert mit dem in Spalte *LACP admin key* für das LAG-Interface festgelegten Wert übereinstimmt.

LACP actor admin state

Legt die Statuswerte des Aktors fest, die das LAG-Interface in den LACPDUs vermittelt. Dies ermöglicht Ihnen, die LACPDU-Parameter zu verwalten.

Das Gerät ermöglicht Ihnen, die Werte zu kombinieren. Wählen Sie in der Dropdown-Liste einen oder mehrere Werte.

Mögliche Werte:

- *ACT*
  (Status `LACP_Activity`)
  Wenn ausgewählt, vermittelt der Link die LACPDUs zyklisch, andernfalls bei Bedarf.
- *STO*
  (Status `LACP_Timeout`)
  Wenn ausgewählt, vermittelt der Link die LACPDUs zyklisch mit kurzem Timeout, andernfalls mit langem Timeout.
- *AGG*
  (Status `Aggregation`)
  Wenn ausgewählt, wertet das Gerät den Link als einbindbar, andernfalls als einzelnen Link.

Für weitere Informationen zu den Werten siehe Norm IEEE 802.1AX-2014.

LACP actor oper state

Zeigt die Statuswerte des Aktors, die das LAG-Interface in den LACPDUs vermittelt.

Mögliche Werte:

- *ACT*
  (Status `LACP_Activity`)
  Wenn sichtbar, vermittelt der Link die LACPDUs zyklisch, andernfalls bei Bedarf.
- *STO*
  (Status `LACP_Timeout`)
  Wenn sichtbar, vermittelt der Link die LACPDUs zyklisch mit kurzem Timeout, andernfalls mit langem Timeout.
- *AGG*
  (Status `Aggregation`)
  Wenn sichtbar, wertet das Gerät den Link als einbindbar, andernfalls als einzelnen Link.
- *SYN*
  (Status `Synchronization`)
  Wenn sichtbar, wertet das Gerät den Link als `IN_SYNC`, andernfalls als `OUT_OF_SYNC`.
- *COL*
  (Status `Collecting`)
  Wenn sichtbar, ist das Erfassen ankommender Frames auf diesem Link eingeschaltet, andernfalls ausgeschaltet.
- *DST*
  (Status `Distributing`)
  Wenn sichtbar, ist das Verteilen der zu sendenden Frames auf diesem Link eingeschaltet, andernfalls ausgeschaltet.
- *DFT*
  (Status `Defaulted`)
  Wenn sichtbar, verwendet der Link voreingestellte Informationen für den Betrieb, die administrativ für den Partner festgelegt sind. Andernfalls verwendet der Link die in einer LACPDU empfangenen Informationen für den Betrieb.
- *EXP*
  (Status `Expired`)
  Wenn sichtbar, befindet sich der Link-Empfänger im Zustand `EXPIRED`.

LACP partner oper SysID

Zeigt die MAC-Adresse des entfernten Geräts, das mit diesem physischen Port verbunden ist.

Das LAG-Interface hat diese Informationen in einer LACPDU vom Partner empfangen.

LACP partner oper port

Zeigt die Port-Nummer des entfernten Geräts, das mit diesem physischen Port verbunden ist.

Das LAG-Interface hat diese Informationen in einer LACPDU vom Partner empfangen.

LACP partner oper port state

Zeigt die Statuswerte des Partners, die das LAG-Interface in den LACPDUs empfängt.

Mögliche Werte:

- *ACT*
- *STO*
- *AGG*
- *SYN*

- *COL*
- *DST*
- *DFT*
- *EXP*

Für weitere Informationen zu den Werten siehe Beschreibung der Spalte *LACP actor oper state* und Norm IEEE 802.1AX-2014.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Öffnet das Fenster *Erzeugen*, um ein LAG-Interface hinzuzufügen oder einem LAG-Interface einen physischen Port zuzuweisen.

- In der Dropdown-Liste *Trunk-Port* wählen Sie die Nummer des LAG-Interfaces.
- In der Dropdown-Liste *Port* wählen Sie die Nummer des physischen Ports, den Sie dem LAG-Interface zuweisen möchten.

Nach Erzeugen eines LAG-Interfaces fügt das Gerät das LAG-Interface der Tabelle im Dialog *Grundeinstellungen > Port*, Registerkarte *Statistiken* hinzu.

5.10.5 Link-Backup

[Switching > L2-Redundanz > Link-Backup]

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *Link-Backup*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der *Link-Backup*-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Mit Link Backup konfigurieren Sie Paare von redundanten Links. Jedes Paar besteht aus einem primären Port und einem Backup-Port. Der primäre Port leitet Daten weiter, bis das Gerät einen Fehler ermittelt. Wenn das Gerät einen Fehler auf dem primären Port ermittelt, nutzt die Link-Backup-Funktion den Backup-Port zur Vermittlung der Daten.

Der Dialog ermöglicht Ihnen außerdem, eine Fail-Back-Funktion einzurichten. Wenn Sie die Fail-Back-Funktion einrichten und der primäre Port in den Normalbetrieb zurückkehrt, blockiert das Gerät zuerst Daten auf dem Backup-Port und leitet dann Daten an den primären Port weiter. Dieses Verfahren hilft zu verhindern, dass das Gerät Loops im Netz verursacht.

Funktion

Funktion

Schaltet die Link-Backup-Funktion global im Gerät ein/aus.

Mögliche Werte:

- *An*
  Schaltet die Link-Backup-Funktion ein.
- *Aus* (Voreinstellung)
  Schaltet die Link-Backup-Funktion aus.

Tabelle

Primärer Port

Zeigt den primären Port des Interface-Paares. Wenn Sie die Funktion Link-Backup einschalten, ist dieser Port für die Weiterleitung der Daten verantwortlich.

Mögliche Werte:

- Physikalische Ports

Backup-Port

Zeigt den Backup-Port, an den das Gerät die Daten vermittelt, wenn es auf dem primären Port einen Fehler ermittelt hat.

Mögliche Werte:

- Physikalische Ports außer dem Port, den Sie als primären Port festlegen.

Beschreibung

Legt das Link-Backup-Paar fest. Geben Sie einen Namen ein, der das Backup-Paar identifiziert.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Status Primärer Port

Zeigt den Status des primären Ports für dieses Link-Backup-Paar.

Mögliche Werte:

- *forwarding*
  Der Link ist vorhanden, keine Abschaltung, Datenweiterleitung
- *blocking*
  Der Link ist vorhanden, keine Abschaltung, Blockierung der Daten
- *down*
  Auf dem Port ist entweder der Link ausgefallen oder in der Software ausgeschaltet oder das Kabel ist entfernt, Abschaltung.
- *unbekannt*
  Die Link-Backup-Funktion ist global ausgeschaltet, oder das Port-Paar ist deaktiviert. Daher ignoriert das Gerät die Einstellungen für das Port-Paar.

Status Backup-Port

Zeigt den Status des Backup-Ports für dieses Link-Backup-Paar.

Mögliche Werte:

- *forwarding*
  Der Link ist vorhanden, keine Abschaltung, Datenweiterleitung
- *blocking*
  Der Link ist vorhanden, keine Abschaltung, Blockierung der Daten

- *down*
  Auf dem Port ist entweder der Link ausgefallen oder in der Software ausgeschaltet oder das Kabel ist entfernt, Abschaltung.
- *unbekannt*
  Die Link-Backup-Funktion ist global ausgeschaltet, oder das Port-Paar ist deaktiviert. Daher ignoriert das Gerät die Einstellungen für das Port-Paar.

Fail back

Aktiviert/deaktiviert die automatische Fail-Back-Funktion.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die automatische Fail-Back-Funktion ist aktiv.
  Nach Ablauf des Verzögerungszeit wechselt der Backup-Port zu *blocking* und der primäre Port wechselt zu *forwarding*.
- `unmarkiert`
  Die automatische Fail-Back-Funktion ist inaktiv.
  Der Backup-Port leitet Daten auch weiter, nachdem der primäre Port einen Link wiederherstellt oder Sie den Admin-Status des primären Ports manuell von `shutdown` zu `no shutdown` geändert haben.

Fail-Back-Verzögerung [s]

Legt die Wartezeit in Sekunden fest, die das Gerät wartet, nachdem der primäre Port einen Link wiederhergestellt hat. Zudem wird der Timer aktiv, wenn Sie den Admin-Status des primären Ports manuell von `shutdown` zu `no shutdown`ändern. Nach Ablauf des Verzögerungszeit wechselt der Backup-Port zu *blocking* und der primäre Port wechselt zu *forwarding*.

Mögliche Werte:

- `0..3600` (Voreinstellung: `30`)
  Bei `0` wechselt der Backup-Port unmittelbar nachdem der primäre Port einen Link wiederhergestellt hat, zu *blocking* und der primäre Port wechselt zu *forwarding*. Unmittelbar nachdem Sie den Port-Status manuell von `shutdown` zu `no shutdown` ändern, wechselt der Backup-Port zu *blocking* und der primäre Port zu *forwarding*.

Aktiv

Aktiviert/deaktiviert die Konfiguration für das Link-Backup-Paar.

Mögliche Werte:

- `markiert`
  Das Link-Backup-Paar ist aktiviert. Das Gerät ermittelt den Link- und Administration-Status und leitet die Daten entsprechend der Paar-Konfiguration weiter.
- `unmarkiert` (Voreinstellung)
  Das Link-Backup-Paar ist deaktiviert. Die Ports leiten die Daten entsprechend den Grundeinstellungen weiter.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Erzeugen

Primärer Port

Legt den primären Port des Backup-Interface-Paares fest. Im Normalbetrieb ist dieser Port verantwortlich für die Weiterleitung der Daten.

Mögliche Werte:

- Physikalische Ports

Backup-Port

Legt den Backup-Port fest, an den das Gerät die Daten vermittelt, wenn es auf dem primären Port einen Fehler ermittelt.

Mögliche Werte:

- Physikalische Ports außer dem Port, den Sie als primären Port festlegen.

5.10.6 FuseNet

[Switching > L2-Redundanz > FuseNet]

Die *FuseNet*-Protokolle ermöglichen Ihnen, Ringe zu koppeln, die mit einem der folgenden Redundanzprotokolle arbeiten:

- MRP
- HIPER Ring
- RSTP

Anmerkung: Wenn Sie das Protokoll *Ring-/Netzkopplung* verwenden, um Netze zu koppeln, dann vergewissern Sie sich, dass die Netze ausschließlich Schneider Electric-Geräte enthalten.

Verwenden Sie die folgende Tabelle, um das *FuseNet*-Kopplungs-Protokoll auszuwählen, das in Ihrem Netz zum Einsatz kommt:

Haupt-Ring	**Verbundenes Netz**		
	MRP	**HIPER-Ring**	**RSTP**
MRP	*Sub Ring*[1)]	*Redundant Coupling Protocol* *Ring-/Netzkopplung*	*Redundant Coupling Protocol* *Ring-/Netzkopplung*
HIPER-Ring	*Sub Ring*	*Ring-/Netzkopplung*	*Redundant Coupling Protocol* *Ring-/Netzkopplung*
RSTP	*Redundant Coupling Protocol*	*Redundant Coupling Protocol*	*Dual RSTP*

– kein geeignetes Kopplungs-Protokoll

1) mit *MRP* eingerichtet an unterschiedlichen VLANs

Das Menü enthält die folgenden Dialoge:

- Sub Ring
- Ring-/Netzkopplung
- Redundant Coupling Protocol (MCSESM-E)

5.10.6.1 Sub Ring

[Switching > L2-Redundanz > FuseNet > Sub Ring]

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *Sub Ring*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der Ring-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Dieser Dialog ermöglicht Ihnen, das Gerät als Subring-Manager einzurichten.

Die Funktion *Sub Ring* ermöglicht Ihnen eine einfache Ankopplung von Netzsegmenten an bestehende Redundanz-Ringe. Der Subring-Manager (SRM) koppelt einen Subring an einen vorhandenen Ring (Base-Ring).

Im Subring können Sie beliebige Geräte, die MRP unterstützen, als Ring-Teilnehmer verwenden. Diese Geräte benötigen keine Subring-Manager-Funktion.

Berücksichtigen Sie beim Einrichten von Subringen folgende Regeln:
- Das Gerät unterstützt *Link-Aggregation* im Subring
- Kein Spanning Tree auf Subring-Ports
- Gleiche *MRP-Domäne* auf Geräten innerhalb eines Subrings
- Unterschiedliche VLANs für Base-Ring und Subring

Legen Sie die VLAN-Einstellungen wie folgt fest:
- VLAN `X` für Base-Ring
  - auf den Ring-Ports der Base-Ring-Teilnehmer
  - auf den Base-Ring-Ports des Subring-Managers
- VLAN `Y` für Subring
  - auf den Ring-Ports der Subring-Teilnehmer
  - auf den Subring-Ports des Subring-Managers

Anmerkung: Um Loops zu vermeiden, schließen Sie die redundante Strecke erst dann, wenn in jedem am Ring beteiligten Gerät die Einstellungen festgelegt sind.

Funktion

Funktion

Schaltet die Funktion *Sub Ring* ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *Sub Ring* ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *Sub Ring* ist ausgeschaltet.

Information

Tabelleneinträge (max.)

Zeigt die maximale Anzahl an Subringen, die das Gerät unterstützt.

Tabelle

Sub-Ring-ID

Zeigt die eindeutige Kennung des Subrings.

Mögliche Werte:

- `1..8`

Name

Legt den Namen des Subringes fest (optional).

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Aktiv

Aktiviert/deaktiviert den Subring.

Aktivieren Sie den Subring, wenn die Konfiguration jedes Geräts des Subringes abgeschlossen ist. Schließen Sie den Subring erst, nachdem Sie die Funktion *Sub Ring* aktiviert haben.

Mögliche Werte:

- `markiert`
  Der Subring ist aktiviert.
- `unmarkiert` (Voreinstellung)
  Der Subring ist inaktiv.

Konfigurations-Status

Zeigt den Betriebszustand der Subring-Konfiguration.

Mögliche Werte:

- *noError*
  Das Gerät erkennt eine geeignete Subring-Konfiguration.
- *ringPortLinkError*
  - Der Ring-Port hat keine Datenverbindung.
  - Eine der Subring-Leitungen ist verbunden mit einem weiteren Anschluss des Geräts. Jedoch ist die Subring-Leitung nicht verbunden mit einem der Ringports des Geräts.
- *multipleSRM*
  Der Subring-Manager empfängt Datenpakete von mehr als einem Subring-Manager im Subring.
- *noPartnerManager*
  Der Subring-Manager empfängt seine eigenen Datenpakete.
- *concurrentVLAN*
  Das MRP-Protokoll im Basis-Ring verwendet das VLAN der Subring-Manager-Domäne.

- *concurrentPort*
  Ein weiteres Redundanzprotokoll verwendet den Ring-Port der Subring-Manager-Domäne.
- *concurrentRedundancy*
  Die Subring-Manager-Domäne ist inaktiv aufgrund eines weiteren aktiven Redundanzprotokolls.
- *trunkMember*
  Der Ring-Port der Subring-Manager-Domäne ist Mitglied einer *Link-Aggregation*-Verbindung.
- *sharedVLAN*
  Die Subring-Manager-Domäne ist inaktiv, weil Shared-VLAN aktiv ist und der Hauptring außerdem das MRP-Protokoll verwendet.

Redundanz verfügbar

Zeigt den Betriebszustand der Ring-Redundanz im Subring.

Mögliche Werte:

- *redGuaranteed*
  Die Redundanz-Reserve ist verfügbar.
- *redNotGuaranteed*
  Verlust der Redundanz-Reserve.

Port

Legt den Port fest, der das Gerät mit dem Subring verbindet.

Mögliche Werte:

- <Port-Nummer>

SRM-Modus

Legt den Modus des Subring-Managers fest.

Ein Subring hat 2 Manager gleichzeitig, die den Subring an den Base-Ring koppeln. So lange der Subring physikalisch geschlossen ist, blockiert ein Manager seinen Subring-Port.

Mögliche Werte:

- *manager* (Voreinstellung)
  Der Subring-Port vermittelt Datenpakete.
  Wenn dieser Wert auf beiden Geräten, die den Subring an den Base-Ring koppeln, eingestellt ist, arbeitet das Gerät mit der höheren MAC-Adresse als *redundantManager*.
- *redundantManager*
  Der Subring-Port ist blockiert, so lange der Subring physikalisch geschlossen ist. Bei einer Unterbrechung des Subrings vermittelt der Subring-Port die Datenpakete.
  Wenn dieser Wert auf beiden Geräten, die den Subring an den Base-Ring koppeln, eingestellt ist, arbeitet das Gerät mit der höheren MAC-Adresse als *redundantManager*.
- *singleManager*
  Verwenden Sie diesen Wert, wenn der Subring über ein einziges Gerät an den Base-Ring gekoppelt ist. Voraussetzung sind 2 Instanzen des Subrings in der Tabelle. Weisen Sie diesen Wert beiden Instanzen zu. Der Subring-Port der Instanz mit der höheren Port-Nummer ist blockiert, so lange der Subring physikalisch geschlossen ist.

SRM-Status

Zeigt den gegenwärtigen Modus des Subring-Managers.

Mögliche Werte:

- *manager*
  Der Subring-Port vermittelt Datenpakete.
- *redundantManager*
  Der Subring-Port ist blockiert, so lange der Subring physikalisch geschlossen ist. Bei einer Unterbrechung des Subrings vermittelt der Subring-Port die Datenpakete.
- *singleManager*
  Der Subring ist über ein einziges Gerät an den Base-Ring gekoppelt. Der Subring-Port der Instanz mit der höheren Port-Nummer ist blockiert, so lange der Subring physikalisch geschlossen ist.
- *disabled*
  Der Subring ist inaktiv.

Status Port

Zeigt den Verbindungsstatus des Subring-Ports.

Mögliche Werte:

- *forwarding*
  Der Port leitet Datenpakete gemäß IEEE 802.1D weiter.
- *disabled*
  Der Port verwirft jedes Datenpaket.
- *blocked*
  Der Port verwirft jedes Datenpaket außer in den folgenden Fällen.
  - Der Port leitet Datenpakete weiter, die vom festgelegten Ring-Protokoll verwendet werden und für die das Passieren von blockierten Ports zugelassen ist.
  - Der Port leitet Datenpakete von anderen Protokollen weiter, für die das Passieren von blockierten Ports zugelassen ist.
- *nicht verbunden*
  Die Datenverbindung auf dem Port ist unterbrochen.

VLAN

Legt das VLAN fest, dem dieser Subring zugewiesen ist. Wenn unter der angegebenen VLAN-ID noch kein VLAN existiert, erstellt das Gerät dieses automatisch.

Mögliche Werte:

- Verfügbare eingerichtete VLANs (Voreinstellung: `0`)
  Wenn Sie für diesen Subring kein eigenständiges VLAN benutzen möchten, dann lassen Sie den Eintrag auf „0“.

Partner-MAC

Zeigt die MAC-Adresse des Subring-Managers am anderen Ende des Subringes.

MRP-Domäne

Legt die MRP-Domäne des Subring-Managers fest. Weisen Sie jedem Mitglied im Subring denselben MRP-Domänen-Namen zu. Wenn Sie ausschließlich Schneider Electric-Geräte verwenden, übernehmen Sie den voreingestellten Wert für die MRP-Domäne; andernfalls passen Sie diesen Wert gegebenenfalls an. Bei mehreren Subringen ermöglicht Ihnen diese Funktion, für die Subringe dieselbe MRP-Domänen-Bezeichnung zu verwenden.

Mögliche Werte:

- Erlaubte MRP-Domänen-Bezeichnungen (Voreinstellung: `255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255`)

Protokoll

Legt das Protokoll fest.

Mögliche Werte:

- *`iec-62439-mrp`*

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

5.10.6.2 Ring-/Netzkopplung

[Switching > L2-Redundanz > FuseNet > Ring-/Netzkopplung]

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *Ring-/Netzkopplung*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der Ring-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Verwenden Sie die Funktion *Ring-/Netzkopplung*, um einen vorhandenen HIPER-, MRP- oder Fast HIPER-Ring an ein weiteres Netz oder an einen Ring redundant zu koppeln. Vergewissern Sie sich, dass die Kopplungspartner Schneider Electric-Geräte sind.

Anmerkung: Vergewissern Sie sich bei der 2-Switch-Kopplung vor der Konfiguration der *Ring-/Netzkopplung*, dass Sie einen HIPER-Ring, einen MRP-Ring oder einen Fast-HIPER-Ring konfiguriert haben.

Im Dialog *Ring-/Netzkopplung* können Sie die folgenden Aufgaben ausführen:
- Übersicht über die bestehende *Ring-/Netzkopplung*anzeigen
- *Ring-/Netzkopplung*konfigurieren
- neue *Ring-/Netzkopplung*erzeugen.
- *Ring-/Netzkopplung*löschen
- *Ring-/Netzkopplung*aktivieren/deaktivieren

Legen Sie bei der Konfiguration der Kopplungsports die folgenden Einstellungen im Dialog *Grundeinstellungen > Port* fest.

Port-Typ	Bitrate	Port an	Automatische Konfiguration	Manuelle Konfiguration
TX	100 Mbit/s	markiert	unmarkiert	*100 Mbit/s FDX*
TX	1 Gbit/s	markiert	markiert	–
Optical	100 Mbit/s	markiert	unmarkiert	*100 Mbit/s FDX*
Optical	1 Gbit/s	markiert	markiert	–
Optisch	2.5 Gbit/s	markiert	–	*2,5 Gbit/s FDX*

Anmerkung: Die tatsächlich zur Verfügung stehenden Betriebsmodi des Ports sind abhängig von der Ausstattung des Geräts.

Haben Sie VLANs konfiguriert, beachten Sie die VLAN-Konfiguration der Kopplungs- und Partner-Kopplungsports. In der *Ring-/Netzkopplung*-Konfiguration wählen Sie für Kopplungs- und Partner-Kopplungsports die folgenden Werte:
- VLAN ID 1 und *Ingress-Filtering* in der Port-Tabelle deaktiviert
- VLAN-Mitgliedschaft T in der Tabelle *VLAN Konfiguration*

Unabhängig von den VLAN-Einstellungen sendet das Gerät die Ring-Kopplungs-Frames mit `VLAN ID 1` und Priorität `7`. Vergewissern Sie sich, dass das Gerät VLAN-1-Datenpakete im lokalen Ring und im angeschlossenen Netz mit einem VLAN-Tag markiert vermittelt. Durch das Tagging der VLAN- Datenpakete bleibt die Priorität der Ring-Kopplungs-Frames erhalten.

Die Funktion *Ring-/Netzkopplung* arbeitet mit Test-Datenpaketen. Die Geräte senden ihre Test-Datenpakete mit VLAN-Tag, einschließlich VLAN-ID `1` und der höchsten VLAN-Priorität `7`. Wenn der weiterleitende Port Mitglied in VLAN `1` ist und die Datenpakete ohne VLAN-Tag vermittelt, dann sendet das Gerät ebenfalls Test-Pakete.

Funktion

Funktion

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

Mögliche Werte:

- *An*
  Die Funktion *Ring-/Netzkopplung* ist eingeschaltet.
- *Aus* (Voreinstellung)
  Die Funktion *Ring-/Netzkopplung* ist ausgeschaltet.

Modus

Typ

Legt die für die Kopplung von Netzen verwendete Methode fest.

Mögliche Werte:

- *Ein-Switch-Kopplung*
  Ermöglicht Ihnen, die Port-Einstellungen in den Rahmen *Kopplungs-Port* und *Partner-Kopplungs-Port* festzulegen.
- *Zwei-Switch-Kopplung, Master*
  Ermöglicht Ihnen, die Port-Einstellungen im Rahmen *Kopplungs-Port* festzulegen.
- *Zwei-Switch-Kopplung, Slave*
  Ermöglicht Ihnen, die Port-Einstellungen im Rahmen *Kopplungs-Port* festzulegen.
- *Zwei-Switch-Kopplung mit Steuer-Leitung, Master*
  Ermöglicht Ihnen, die Port-Einstellungen in den Rahmen *Kopplungs-Port* und *Steuer-Port* festzulegen.
- *Zwei-Switch-Kopplung mit Steuer-Leitung, Slave*
  Ermöglicht Ihnen, die Port-Einstellungen in den Rahmen *Kopplungs-Port* und *Steuer-Port* festzulegen.

Kopplungs-Port

Port

Legt den Port fest, über den Sie die Redundanzverbindung herstellen.

Mögliche Werte:

- `-`
  Kein Port ausgewählt.
- `<Port-Nummer>`

Wenn Sie auch Ring-Ports konfiguriert haben, dann verwenden Sie für Kopplungs- und Ring-Ports unterschiedliche Ports.

Um Loops zu vermeiden, schaltet das Gerät den Kopplungs-Ports in den folgenden Fällen aus:

- bei Deaktivierung der Funktion
- bei Änderung der Konfiguration, während die Datenverbindungen an den Ports aktiv sind

Wenn das Gerät den Kopplungs-Port deaktiviert hat, ist im Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration* das Kontrollkästchen *Port an* unmarkiert.

Zustand

Zeigt den Status des ausgewählten Ports.

Mögliche Werte:

- *aktiv*
  Der Port ist aktiv.
- *standby*
  Der Port befindet sich im Standby-Modus.
- *nicht verbunden*
  Der Port ist nicht verbunden.
- *unzutreffend*
  Der Port ist mit dem konfigurierten Steuerungsmodus inkompatibel.

Partner-Kopplungs-Port

Port

Legt den Port fest, mit dem Sie den Partner-Port verbinden.

Mögliche Werte:

- `-`
  Kein Port ausgewählt.
- `<Port-Nummer>`

Wenn Sie auch Ring-Ports konfiguriert haben, dann verwenden Sie für Kopplungs- und Ring-Ports unterschiedliche Ports.

Zustand

Zeigt den Status des ausgewählten Ports.

Mögliche Werte:

- *aktiv*
  Der Port ist aktiv.
- *standby*
  Der Port befindet sich im Standby-Modus.
- *nicht verbunden*
  Der Port ist nicht verbunden.
- *unzutreffend*
  Der Port ist mit dem konfigurierten Steuerungsmodus inkompatibel.

IP-Adresse

Zeigt die IP-Adresse des Partnergeräts, wenn die Geräte verbunden sind.

Voraussetzung ist, dass Sie eine 2-Switch-Kopplungs-Methode auswählen und den Partner im Netz einschalten.

Steuer-Port

Port

Zeigt den Port, an dem Sie die Steuer-Leitung anschließen.

Mögliche Werte:

- `-`
  Kein Port ausgewählt.
- `<Port-Nummer>`

Zustand

Zeigt den Status des ausgewählten Ports.

Mögliche Werte:

- *aktiv*
  Der Port ist aktiv.
- *standby*
  Der Port befindet sich im Standby-Modus.
- *nicht verbunden*
  Der Port ist nicht verbunden.
- *unzutreffend*
  Der Port ist mit dem konfigurierten Steuerungsmodus inkompatibel.

Konfiguration

Redundanz-Modus

Legt fest, ob das Gerät auf einen erkannten Fehler im entfernten Ring oder Netz reagiert.

Mögliche Werte:

- *Redundante Ring-/Netz-Kopplung*
  Entweder die Hauptleitung oder die redundante Leitung ist aktiv. Niemals sind beide Leitungen gleichzeitig aktiv. Wenn das Gerät erkennt, dass zwischen den Geräten im angeschlossenen Netz keine Verbindung besteht, behält das Standby-Gerät den Standby-Modus des redundanten Ports bei.
- *Erweiterte Redundanz*
  Die Hauptleitung und die redundante Leitung sind gleichzeitig aktiv. Erkennt das Gerät ein Problem in Bezug auf die Datenverbindung zwischen den Geräten im angeschlossenen Netz, leitet das Standby-Gerät die Daten auf dem redundanten Port weiter. Mit dieser Einstellung können Sie die Kontinuität im Remote-Netz sicherstellen.

Anmerkung: Während der Rekonfigurationszeit können Datenpaket-Doppelungen auftreten. Daher können Sie diese Einstellung auswählen, wenn Ihre Anwendung in der Lage ist, Datenpaket-Dopplungen zu erkennen.

Kopplungs-Modus

Legt die Methode zum Koppeln eines spezifischen Netztyps fest.

Mögliche Werte:

- *Ring-Kopplung*
  Das Gerät koppelt redundante Ringe. Das Gerät ermöglicht Ihnen, Ringe zu koppeln, welche die folgenden Redundanzprotokolle verwenden:
  - HIPER-Ring
  - Fast HIPER-Ring
  - MRP-Ring
- *Netz-Kopplung*
  Das Gerät koppelt Netzsegmente. Die Funktion ermöglicht Ihnen, Mesh- und Bus-Netze miteinander zu koppeln.

Information

Redundanz verfügbar

Zeigt, ob die Redundanz verfügbar ist.

Fällt eine Komponente des Rings aus, übernimmt die redundante Strecke deren Funktion.

Mögliche Werte:

- *redGuaranteed*
  Redundanz ist verfügbar.
- *redNotGuaranteed*
  Keine Redundanz verfügbar.

Konfigurationsfehler

Sie haben die Funktion falsch konfiguriert oder die Ring-Port-Verbindung ist nicht vorhanden.

Mögliche Werte:

- *noError*
- *slaveCouplingLinkError*
  Die Kopplungs-Leitung ist nicht verbunden mit dem Kopplungs-Port des Slave-Geräts. Stattdessen ist die Kopplungs-Leitung mit einem anderen Port des Slave-Geräts verbunden.
- *slaveControlLinkError*
  Der Steuer-Port des Slave-Geräts hat keine Datenverbindung.
- *masterControlLinkError*
  Die Steuer-Leitung ist nicht verbunden mit dem Steuer-Port des Master-Geräts. Stattdessen ist die Steuer-Leitung mit einem anderen Port des Master-Geräts verbunden.
- *twoSlaves*
  Die Steuer-Leitung verbindet zwei Slave-Geräte.
- *localPartnerLinkError*
  Die Partner-Kopplungs-Leitung ist nicht verbunden mit dem Partner-Kopplungs-Port des Slave-Geräts. Stattdessen ist die Partner-Kopplungs-Leitung im *Ein-Switch-Kopplung*-Modus mit einem anderen Port des Slave-Geräts verbunden.
- *localInvalidCouplingPort*
  Im *Ein-Switch-Kopplung*-Modus ist die Kopplungs-Leitung nicht mit dem selben Gerät verbunden wie die Partner-Leitung. Stattdessen ist die Kopplungs-Leitung mit einem anderen Gerät verbunden.
- *couplingPortNotAvailable*
  Der Kopplungs-Port ist nicht verfügbar, da das Modul nicht verfügbar ist, zu welchem der Port gehört, oder der Port auf diesem Modul nicht vorhanden ist.
- *controlPortNotAvailable*
  Der Steuer-Port ist nicht verfügbar, da das Modul nicht verfügbar ist, zu welchem der Port gehört, oder der Port auf diesem Modul nicht vorhanden ist.
- *partnerPortNotAvailable*
  Der Partner-Kopplungs-Port ist nicht verfügbar, da das Modul nicht verfügbar ist, zu welchem der Port gehört, oder der Port auf diesem Modul nicht vorhanden ist.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Zurücksetzen

Deaktiviert die Redundanzfunktion und setzt die Parameter im Dialog auf die voreingestellten Werte zurück.

5.10.6.3 Redundant Coupling Protocol (MCSESM-E)

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *RCP*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der Ring-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

⚠ WARNUNG

LOOP-GEFAHR

- Konfigurieren Sie jedes Gerät der *RCP*- und *Dual RSTP*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der Ring-Konfiguration abgeschlossen haben.
- Konfigurieren Sie den Timeout in der *RCP*-Kopplungskonfiguration länger als die längste anzunehmende Unterbrechungszeit der schnelleren Instanz des Redundanzprotokolls.
- Konfigurieren Sie in einer Topologie mit 2 Kopplungs-Bridges die Kopplungs-Rollen der beiden Geräte ausschließlich als `master`, `slave` oder `auto`.
- Koppeln Sie die primäre Instanz und die sekundäre Instanz ausschließlich über 1 *RCP*-Bridge (bei einer Topologie mit *RCP*-Bridge) oder 2 *RCP*-Bridges (bei einer Topologie mit 2 *RCP*-Bridges). Halten Sie die Ports der primären Instanz getrennt von den Ports der einzelnen sekundären Instanzen.
- Aktivieren Sie die *Admin-Edge-Port*-Einstellung auf einem Port ausschließlich dann, wenn ein Endgerät an den Port angeschlossen ist.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Eine Ringtopologie bietet kurze Übergangszeiten bei minimalem Ressourceneinsatz. Allerdings ist es eine Herausforderung, die Ringe redundant an ein übergeordnetes Netz zu koppeln.

Wenn Sie ein Standardprotokoll, zum Beispiel MRP für die Ringredundanz und RSTP zum Koppeln der Ringe verwenden möchten, bietet Ihnen das *Redundant Coupling Protocol* die entsprechenden Optionen.

Verwenden Sie keines der folgenden Redundanzprotokolle auf den Ports des *RCP*-Primär-Rings und der *RCP*-Sekundär-Ringe:

- *Sub Ring*
- *Ring-/Netzkopplung*

Wenn Sie RSTP für den Primär-Ring und für den Sekundär-Ring verwenden möchten, dann ordnet die Funktion *RCP* die Ports des Sekundär-Rings der *Dual RSTP*-Instanz zu. Dadurch entstehen zwei unabhängige RSTP-Netze, die mit *RCP* gekoppelt sind. Die Einstellungen der Funktion *Dual RSTP* legen Sie im Dialog *Switching > L2-Redundanz* fest.

Wenn Sie die Funktion *RCP* in einem Netz konfigurieren und die Konfiguration noch unvollständig ist, ist es möglich, dass die Geräte die Verbindung zwischen dem Primär-Ring und dem Sekundär-Ring vorübergehend trennen. In diesem Fall ist das Management der *RCP*-Bridges aus dem Sekundär-Ring unerreichbar. Schließen Sie während dieser Konfigurationsphase Ihre Management-Station an den Primär-Ring an.

Funktion

Funktion

Schaltet die Funktion *RCP* ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *RCP* ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *RCP* ist ausgeschaltet.

Primärer Ring/Netzwerk / Sekundärer Ring/Netzwerk

Wenn das Gerät als Slave arbeitet (Wert im *Rolle*-Feld ist `slave`), dann aktivieren Sie nicht den *Static-Query-Port*-Modus für die Ports im Sekundär-Ring/Netz.

Innerer Port

Legt die Nummer des inneren Ports im Primär-/Sekundär-Ring fest. Dieser Port ist direkt mit der Partner-Bridge verbunden.

Mögliche Werte:

- `-` (Voreinstellung)
  Kein Port ausgewählt.
- `<Port-Nummer>`

Äußerer Port

Legt die Nummer des äußeren Ports im Primär-/Sekundär-Ring fest.

Mögliche Werte:

- `-` (Voreinstellung)
  Kein Port ausgewählt.
- `<Port-Nummer>`

Protokoll Primärer Ring/Protokoll Sekundärer Ring

Zeigt das Protokoll, das auf dem redundanten Kopplungs-Port in den Geräten im primären/sekundären Ring aktiv ist.

Koppler-Konfiguration

Rolle

Legt die Rolle des lokalen Geräts fest.

Mögliche Werte:

- `master`
  Das Gerät arbeitet als Master.
- `slave`
  Das Gerät arbeitet als Slave.
- `single`
  Das Gerät koppelt mit einer *Dual RSTP*-Instanz 2 RSTP-Netze über eine Bridge.
- `auto` (Voreinstellung)
  Das Gerät wählt automatisch seine Rolle als *master* oder *slave*.

Momentane Rolle

Zeigt die gegenwärtige Rolle des lokalen Geräts. Der Wert kann von der konfigurierten Rolle abweichen:

- Haben Sie beide Partner-Bridges als `auto` konfiguriert, übernimmt die Partner-Bridge, die gegenwärtig die Instanzen koppelt, die `master`-Rolle. Die andere Partner-Bridge übernimmt die `slave`-Rolle.
- Sind beide Partner-Bridges als `master` oder beide als `slave` konfiguriert, übernimmt die Partner-Bridge mit der kleineren Basis-MAC-Adresse die `master`-Rolle.
  Die andere Partner-Bridge übernimmt die `slave`-Rolle.
- Ist beim Aktivieren des Protokolls auf einer Bridge in der konfigurierten Rolle `master`, `slave` oder `auto` deren Partner-Bridge unauffindbar, setzt die Bridge ihre eigene Rolle auf `listening`.
- Wenn das Gerät ein Konfigurationsproblem feststellt, zum Beispiel wenn die inneren Ring-Ports über Kreuz verbunden sind, dann setzt das Gerät seine Rolle auf `error`.

Timeout [ms]

Legt die maximale Zeit in Millisekunden fest, während der das Slave-Gerät auf den äußeren Ports auf Testpakete vom Master-Gerät wartet, bevor das Slave-Gerät die Kopplung übernimmt. Dies gilt lediglich in dem Zustand, in dem beide inneren Ports des Slave-Geräts die Datenverbindung zum Master-Gerät verloren haben.

Konfigurieren Sie den Timeout länger als die längste anzunehmende Unterbrechungszeit des Redundanzprotokolls der schnelleren Instanz. Andernfalls können Loops auftreten.

Mögliche Werte:

- `5..60000` (Voreinstellung: `45`)

Partner MAC-Adresse

Zeigt die Basis-MAC-Adresse des Partnergeräts.

Partner IP-Adresse

Zeigt die IP-Adresse des Partnergeräts.

Kopplungs-Zustand

Zeigt den Koppungsstatus des lokalen Geräts.

Mögliche Werte:

- *forwarding*
  Der Port befindet sich im Kopplungsstatus „weiterleitend“.
- *blocking*
  Der Port befindet sich im Kopplungsstatus „blocking“.

Redundanz-Zustand

Zeigt, ob die Redundanz verfügbar ist.

Bei einer Master-Slave-Konfiguration zeigen beide Bridges diese Information an.

Mögliche Werte:

- *redAvailable*
  Redundanz ist verfügbar.
- *redNotAvailable*
  Keine Redundanz verfügbar.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

6 Diagnose

Das Menü enthält die folgenden Dialoge:

- Statuskonfiguration
- System
- E-Mail-Benachrichtigung
- Syslog
- Ports
- Loop-Schutz
- LLDP
- Bericht

6.1 Statuskonfiguration

[Diagnose > Statuskonfiguration]

Das Menü enthält die folgenden Dialoge:

- Gerätestatus
- Sicherheitsstatus
- Signalkontakt
- MAC-Benachrichtigung
- Alarme (Traps)

6.1.1 Gerätestatus

[Diagnose > Statuskonfiguration > Gerätestatus]

Der Gerätestatus gibt einen Überblick über den Gesamtzustand des Geräts. Viele Prozessvisualisierungssysteme erfassen den Gerätestatus eines Geräts, um dessen Zustand grafisch darzustellen.

Das Gerät zeigt seinen gegenwärtigen Status als `error` oder `ok` im Rahmen *Geräte-Status*. Das Gerät bestimmt diesen Status anhand der einzelnen Überwachungsergebnisse.

Das Gerät zeigt ermittelte Fehler in der Registerkarte *Status* und zusätzlich im Dialog *Grundeinstellungen > System*, Rahmen *Gerätestatus*.

Der Dialog enthält die folgenden Registerkarten:
- [Global]
- [Port]
- [Status]

[Global]

Geräte-Status

Geräte-Status

Zeigt den gegenwärtigen Status des Geräts. Das Gerät bestimmt den Status aus den einzelnen überwachten Parametern.

Mögliche Werte:

- `error`
  Das Gerät zeigt diesen Wert, um einen ermittelten Fehler für eine der überwachten Parameter anzuzeigen.
- `ok`

Traps

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung an einer überwachten Funktion erkennt.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Senden von SNMP-Traps ist aktiv.
  Das Gerät sendet einen SNMP-Trap, wenn es an den überwachten Funktionen eine Änderung erkennt.
- `unmarkiert`
  Das Senden von SNMP-Traps ist inaktiv.

Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog *Diagnose* > Statuskonfiguration > *Alarme (Traps)* einschalten und mindestens ein Trap-Ziel festlegen.

Tabelle

Temperatur

Aktiviert/deaktiviert die Überwachung der Temperatur im Gerät.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Geräte-Status* wechselt auf `error`, wenn die Temperatur die festgelegten Grenzwerte überschreitet oder unterschreitet.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Temperaturgrenzen legen Sie fest im Dialog *Grundeinstellungen > System*, Feld *Obere Temp.-Grenze [°C]* und Feld *Untere Temp.-Grenze [°C]*.

Ring-Redundanz

Aktiviert/deaktiviert die Überwachung der Ring-Redundanz.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  In folgenden Situationen wechselt der Wert im Rahmen *Geräte-Status* auf `error`:
  - Die Redundanz-Funktion schaltet sich ein (Wegfall der Redundanz-Reserve).
  - Das Gerät ist normaler Ring-Teilnehmer und erkennt Fehler in seinen Einstellungen.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Verbindungsfehler

Aktiviert/deaktiviert die Überwachung des Linkstatus auf dem Port/Interface.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Geräte-Status* wechselt auf `error`, wenn der Link auf einem überwachten Port/Interface abbricht.
  In der Registerkarte *Port* haben Sie die Möglichkeit, die zu überwachenden Ports/Interfaces einzeln auszuwählen.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Externen Speicher entfernen

Aktiviert/deaktiviert die Überwachung des aktiven externen Speichers.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Geräte-Status* wechselt auf `error`, wenn Sie den aktiven externen Speicher aus dem Gerät entfernen.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Externer Speicher nicht synchron

Aktiviert/deaktiviert die Überwachung der Konfigurationsprofile im Gerät und im externen Speicher.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  In folgenden Situationen wechselt der Wert im Rahmen *Geräte-Status* auf `error`:
  - Das Konfigurationsprofil existiert ausschließlich im Gerät.
  - Das Konfigurationsprofil im Gerät unterscheidet sich vom Konfigurationsprofil im externen Speicher.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Netzteil

Aktiviert/deaktiviert die Überwachung des Netzteils.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Geräte-Status* wechselt auf `error`, wenn das Gerät einen Fehler am Netzteil feststellt.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Port]

Tabelle

Port

Zeigt die Nummer des Ports.

Verbindungsfehler melden

Aktiviert/deaktiviert die Überwachung des Links auf dem Port/Interface.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Geräte-Status* wechselt auf `error`, wenn der Link auf dem ausgewählten Port/Interface abbricht.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Die Einstellung ist wirksam, wenn Sie in der Registerkarte *Global* das Kontrollkästchen *Verbindungsfehler* markieren.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Status]

Tabelle

Zeitstempel

Zeigt das Datum und die Uhrzeit des Ereignisses im Format `Tag.Monat.Jahr hh:mm:ss`.

Ursache

Zeigt das Ereignis, das den SNMP-Trap ausgelöst hat.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

6.1.2 Sicherheitsstatus

[Diagnose > Statuskonfiguration > Sicherheitsstatus]

Dieser Dialog gibt einen Überblick über den Zustand der sicherheitsrelevanten Einstellungen im Gerät.

Das Gerät zeigt seinen gegenwärtigen Status als *error* oder *ok* im Rahmen *Sicherheits-Status*. Das Gerät bestimmt diesen Status anhand der einzelnen Überwachungsergebnisse.

Das Gerät zeigt ermittelte Fehler in der Registerkarte *Status* und zusätzlich im Dialog *Grundeinstellungen > System*, Rahmen *Sicherheits-Status*.

Der Dialog enthält die folgenden Registerkarten:
- [Global]
- [Port]
- [Status]

[Global]

Sicherheits-Status

Sicherheits-Status

Zeigt den gegenwärtigen Status der sicherheitsrelevanten Einstellungen im Gerät. Das Gerät bestimmt den Status aus den einzelnen überwachten Parametern.

Mögliche Werte:

- *error*
  Das Gerät zeigt diesen Wert, um einen ermittelten Fehler für eine der überwachten Parameter anzuzeigen.
- *ok*

Traps

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung an einer überwachten Funktion erkennt.

Mögliche Werte:

- `markiert`
  Das Senden von SNMP-Traps ist aktiv.
  Das Gerät sendet einen SNMP-Trap, wenn es an den überwachten Funktionen eine Änderung erkennt.
- `unmarkiert` (Voreinstellung)
  Das Senden von SNMP-Traps ist inaktiv.

Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* einschalten und mindestens ein Trap-Ziel festlegen.

Tabelle

Passwort-Voreinstellung unverändert

Aktiviert/deaktiviert die Überwachung des Passworts für die lokal eingerichteten Benutzerkonten `user` und `admin`.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie für die Benutzerkonten `user` oder `admin` das voreingestellte Passwort unverändert verwenden.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Das Passwort legen Sie fest im Dialog *Gerätesicherheit > Benutzerverwaltung*.

Min. Passwort-Länge < 8

Aktiviert/deaktiviert die Überwachung der Richtlinie *Min. Passwort-Länge*.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn für die Richtlinie *Min. Passwort-Länge* ein Wert kleiner als `8` festgelegt ist.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Richtlinie für die *Min. Passwort-Länge* legen Sie fest im Dialog *Gerätesicherheit > Benutzerverwaltung*, Rahmen *Konfiguration*.

Passwort-Richtlinien deaktiviert

Aktiviert/deaktiviert die Überwachung der Passwort-Richtlinien-Einstellungen.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn für mindestens eine der folgenden Richtlinien ein Wert kleiner als `1` festgelegt ist.
  - *Großbuchstaben (min.)*
  - *Kleinbuchstaben (min.)*
  - *Ziffern (min.)*
  - *Sonderzeichen (min.)*
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Einstellungen für die Richtlinie legen Sie fest im Dialog *Gerätesicherheit > Benutzerverwaltung*, Rahmen *Passwort-Richtlinien*.

Prüfen der Passwort-Richtlinien im Benutzerkonto deaktiviert

Aktiviert/deaktiviert die Überwachung der Funktion *Richtlinien überprüfen*.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn die Funktion *Richtlinien überprüfen* bei mindestens ein Benutzerkonto inaktiv ist.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Die Funktion *Richtlinien überprüfen* aktivieren Sie im Dialog *Gerätesicherheit > Benutzerverwaltung*.

Telnet-Server aktiv

Aktiviert/deaktiviert die Überwachung des Telnet-Servers.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie den Telnet-Server einschalten.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Den Telnet-Server schalten Sie ein/aus im Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *Telnet*.

HTTP-Server aktiv

Aktiviert/deaktiviert die Überwachung des HTTP-Servers.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie den HTTP-Server einschalten.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Den HTTP-Server schalten Sie ein/aus im Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *HTTP*.

SNMP unverschlüsselt

Aktiviert/deaktiviert die Überwachung des SNMP-Servers.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn mindestens eine der folgenden Bedingungen zutrifft:
  - Die Funktion *SNMPv1* ist eingeschaltet.
  - Die Funktion *SNMPv2* ist eingeschaltet.
  - Die Verschlüsselung für SNMPv3 ist ausgeschaltet.
    Die Verschlüsselung schalten Sie ein im Dialog *Gerätesicherheit > Benutzerverwaltung*, Spalte *SNMP-Verschlüsselung*.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Einstellungen für den SNMP-Agenten legen Sie fest im Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SNMP*.

Zugriff auf System-Monitor mit serieller Schnittstelle möglich

Aktiviert/deaktiviert die Überwachung des System-Monitors.

Wenn der System-Monitor aktiviert ist, haben Sie die Möglichkeit, während des Starts des Geräts über eine serielle Verbindung in den System-Monitor zu wechseln.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn der System-Monitor aktiviert ist.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Den System-Monitor aktivieren/deaktivieren Sie im Dialog *Diagnose > System > Selbsttest*.

Speichern des Konfigurationsprofils auf dem externen Speicher möglich

Aktiviert/deaktiviert die Überwachung des Konfigurationsprofils im externen Speicher.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn das Speichern des Konfigurationsprofils auf dem externen Speicher aktiviert ist.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Das Speichern des Konfigurationsprofils im externen Speicher aktivieren/deaktivieren Sie im Dialog *Grundeinstellungen > Externer Speicher*.

Verbindungsabbruch auf eingeschalteten Ports

Aktiviert/deaktiviert die Überwachung des Links auf den aktiven Ports.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn der Link auf einem aktiven Port abbricht. In der Registerkarte *Port* haben Sie die Möglichkeit, die zu überwachenden Ports einzeln auszuwählen.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Zugriff mit Ethernet Switch Configurator möglich

Aktiviert/deaktiviert die Überwachung der Funktion Ethernet Switch Configurator.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie die Funktion Ethernet Switch Configurator einschalten.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Funktion Ethernet Switch Configurator schalten Sie im Dialog *Grundeinstellungen > Netz* ein/aus.

Unverschlüsselte Konfiguration vom externen Speicher laden

Aktiviert/deaktiviert die Überwachung des Ladens unverschlüsselter Konfigurationsprofile vom externen Speicher.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn die Einstellungen dem Gerät ermöglichen, ein unverschlüsseltes Konfigurationsprofil vom externen Speicher zu laden.
  Der Rahmen *Sicherheits-Status* im Dialog *Grundeinstellungen > System* zeigt einen Alarm, wenn folgende Voraussetzungen erfüllt sind:
  - Das im externen Speicher gespeicherte Konfigurationsprofil ist unverschlüsselt.
    und
  - Die Spalte *Konfigurations-Priorität* im Dialog *Grundeinstellungen > Externer Speicher* hat den Wert `first`.
- `unmarkiert`
  Die Überwachung ist inaktiv.

IEC61850-MMS aktiv

Aktiviert/deaktiviert die Überwachung der Funktion *IEC61850-MMS*.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie die Funktion *IEC61850-MMS* einschalten.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Funktion *IEC61850-MMS* schalten Sie im Dialog *Industrie-Protokolle > IEC61850-MMS*, Rahmen *Funktion*ein/aus.

Self-signed HTTPS-Zertifikat vorhanden

Aktiviert/deaktiviert die Überwachung des HTTPS-Zertifikats.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn der HTTPS-Server ein selbst erzeugtes digitales Zertifikat verwendet.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Modbus TCP aktiv

Aktiviert/deaktiviert die Überwachung der Funktion *Modbus TCP*.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie die Funktion *Modbus TCP* einschalten.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Funktion *Modbus TCP* schalten Sie im Dialog *Erweitert > Industrie-Protokolle > Modbus TCP*, Rahmen *Funktion*ein/aus.

EtherNet/IP aktiv

Aktiviert/deaktiviert die Überwachung der Funktion *EtherNet/IP*.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie die Funktion *EtherNet/IP* einschalten.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Funktion *EtherNet/IP* schalten Sie im Dialog *Erweitert > Industrie-Protokolle > EtherNet/IP*, Rahmen *Funktion*ein/aus.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Port]

Tabelle

Port

Zeigt die Nummer des Ports.

Verbindungsabbruch auf eingeschalteten Ports

Aktiviert/deaktiviert die Überwachung des Links auf den aktiven Ports.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn der Port eingeschaltet ist (Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*, Kontrollkästchen *Port an* ist `markiert`) und wenn der Link auf dem Port abbricht.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Diese Einstellung ist wirksam, wenn Sie im Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus*, Registerkarte *Global*, das Kontrollkästchen *Verbindungsabbruch auf eingeschalteten Ports* markieren.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Status]

Tabelle

Zeitstempel

Zeigt das Datum und die Uhrzeit des Ereignisses im Format `Tag.Monat.Jahr hh:mm:ss`.

Ursache

Zeigt das Ereignis, das den SNMP-Trap ausgelöst hat.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

6.1.3 Signalkontakt

[Diagnose > Statuskonfiguration > Signalkontakt]

Der Signalkontakt ist ein potentialfreier Relaiskontakt. Das Gerät ermöglicht Ihnen damit eine Ferndiagnose. Über den Signalkontakt signalisiert das Gerät das Eintreten von Ereignissen, indem es den Relaiskontakt öffnet und den Ruhestromkreis unterbricht.

Anmerkung: Das Gerät enthält möglicherweise mehrere Signalkontakte. Hierbei enthält jeder einzelne Signalkontakt dieselben Überwachungsfunktionen. Mehrere Signalkontakte bieten Ihnen die Möglichkeit, unterschiedliche Funktionen zu gruppieren, was die Systemüberwachung flexibel macht.

Das Menü enthält die folgenden Dialoge:

- Signalkontakt 1 / Signalkontakt 2

6.1.3.1 Signalkontakt 1 / Signalkontakt 2

[Diagnose > Statuskonfiguration > Signalkontakt > Signalkontakt 1]

In diesem Dialog legen Sie die Auslösebedingungen für den Signalkontakt fest.

Der Signalkontakt bietet Ihnen folgende Möglichkeiten:
- Funktionsüberwachung des Geräts.
- Signalisierung des Gerätestatus des Geräts.
- Signalisierung des Sicherheitsstatus des Geräts.
- Steuerung externer Geräte bei manueller Einstellung des Signalkontakts.

Das Gerät zeigt ermittelte Fehler in der Registerkarte *Status* und zusätzlich im Dialog *Grundeinstellungen > System*, Rahmen *Status Signalkontakt*.

Der Dialog enthält die folgenden Registerkarten:
- [Global]
- [Port]
- [Status]

[Global]

Konfiguration

Modus

Legt fest, welche Ereignisse der Signalkontakt signalisiert.

Mögliche Werte:

- `Manuelle Einstellung` (Voreinstellung für *Signalkontakt 2*, falls vorhanden)
  Mit dieser Einstellung schalten Sie den Signalkontakt von Hand, um zum Beispiel ein entferntes Gerät ein- oder auszuschalten. Siehe Optionsfeld *Kontakt*.
- `Funktionsüberwachung` (Voreinstellung)
  Mit dieser Einstellung signalisiert der Signalkontakt den Zustand der in der Tabelle unten festgelegten Parameter.
- `Geräte-Status`
  Mit dieser Einstellung signalisiert der Signalkontakt den Zustand der im Dialog *Diagnose* > Statuskonfiguration > *Gerätestatus* überwachten Parameter. Zusätzlich ist der Zustand im Rahmen *Signalkontakt-Status* ablesbar.
- `Sicherheits-Status`
  Mit dieser Einstellung signalisiert der Signalkontakt den Zustand der im Dialog *Diagnose* > Statuskonfiguration > *Sicherheitsstatus* überwachten Parameter. Zusätzlich ist der Zustand im Rahmen *Signalkontakt-Status* ablesbar.
- `Geräte-/Sicherheits-Status`
  Mit dieser Einstellung signalisiert der Signalkontakt den Zustand der im Dialog *Diagnose* > Statuskonfiguration > *Gerätestatus* und im Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus* überwachten Parameter. Zusätzlich ist der Zustand im Rahmen *Signalkontakt-Status* ablesbar.

Kontakt

Schaltet den Signalkontakt von Hand. Voraussetzung ist, dass Sie in der Dropdown-Liste *Modus* den Eintrag `Manuelle Einstellung` auswählen.

Mögliche Werte:

- `offen`
  Der Signalkontakt ist geöffnet.
- `geschlossen`
  Der Signalkontakt ist geschlossen.

Signalkontakt-Status

Signalkontakt-Status

Zeigt den gegenwärtigen Zustand des Signalkontakts.

Mögliche Werte:

- `Offen (Fehler)`
  Der Signalkontakt ist geöffnet. Der Ruhestromkreis ist unterbrochen.
- `Geschlossen (Ok)`
  Der Signalkontakt ist geschlossen. Der Ruhestromkreis ist geschlossen.

Trap-Konfiguration

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung an einer überwachten Funktion erkennt.

Mögliche Werte:

- `markiert`
  Das Senden von SNMP-Traps ist aktiv.
  Das Gerät sendet einen SNMP-Trap, wenn es an den überwachten Funktionen eine Änderung erkennt.
- `unmarkiert` (Voreinstellung)
  Das Senden von SNMP-Traps ist inaktiv.

Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* einschalten und mindestens ein Trap-Ziel festlegen.

Funktionsüberwachung

In dieser Tabelle legen Sie die Parameter fest, die das Gerät überwacht. Das Eintreten eines Ereignisses meldet das Gerät durch Öffnen des Signalkontakts.

Verbindungsfehler

Aktiviert/deaktiviert die Überwachung des Linkstatus auf dem Port/Interface.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Signalkontakt öffnet, wenn der Link auf einem überwachten Port/Interface abbricht.
  In der Registerkarte *Port* haben Sie die Möglichkeit, die zu überwachenden Ports/Interfaces einzeln auszuwählen.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Temperatur

Aktiviert/deaktiviert die Überwachung der Temperatur im Gerät.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Signalkontakt öffnet, wenn die Temperatur die Temperaturgrenzen überschreitet oder unterschreitet.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Temperaturgrenzen legen Sie fest im Dialog *Grundeinstellungen > System*, Feld *Obere Temp.-Grenze [°C]* und Feld *Untere Temp.-Grenze [°C]*.

Ring-Redundanz

Aktiviert/deaktiviert die Überwachung der Ring-Redundanz.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  In folgenden Situationen öffnet der Signalkontakt:
  - Die Redundanz-Funktion schaltet sich ein (Wegfall der Redundanz-Reserve).
  - Das Gerät ist normaler Ring-Teilnehmer und erkennt Fehler in seinen Einstellungen.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Externer Speicher wurde entfernt

Aktiviert/deaktiviert die Überwachung des aktiven externen Speichers.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Signalkontakt öffnet, wenn Sie den aktiven externen Speicher aus dem Gerät entfernen.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Externer Speicher und NVM nicht synchron

Aktiviert/deaktiviert die Überwachung der Konfigurationsprofile im Gerät und im externen Speicher.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  In folgenden Situationen öffnet der Signalkontakt:
  - Das Konfigurationsprofil existiert ausschließlich im Gerät.
  - Das Konfigurationsprofil im Gerät unterscheidet sich vom Konfigurationsprofil im externen Speicher.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Ethernet-Loops

Aktiviert/deaktiviert die Überwachung von Layer-2-Ethernet-Loops. Die Einstellungen der Funktion *Loop-Schutz* legen Sie im Dialog *Diagnose > Loop-Schutz* fest.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Signalkontakt öffnet, wenn das Gerät einen Ethernet-Loop feststellt.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Netzteil

Aktiviert/deaktiviert die Überwachung des Netzteils.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Signalkontakt öffnet, wenn das Gerät einen Fehler an diesem Netzteil feststellt.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Port]

Tabelle

Port

Zeigt die Nummer des Ports.

Verbindungsfehler melden

Aktiviert/deaktiviert die Überwachung des Links auf dem Port/Interface.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Signalkontakt öffnet, wenn der Link auf dem ausgewählten Port/Interface abbricht.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Die Einstellung ist wirksam, wenn Sie in der Registerkarte *Global* das Kontrollkästchen *Verbindungsfehler* markieren.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Status]

Tabelle

Zeitstempel

Zeigt das Datum und die Uhrzeit des Ereignisses im Format `Tag.Monat.Jahr hh:mm:ss`.

Ursache

Zeigt das Ereignis, das den SNMP-Trap ausgelöst hat.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

6.1.4 MAC-Benachrichtigung

[Diagnose > Statuskonfiguration > MAC-Benachrichtigung]

Das Gerät ermöglicht Ihnen, Änderungen im Netz anhand der MAC-Adresse der Geräte zu verfolgen. Das Gerät speichert die Kombination aus Port und MAC-Adresse in seiner MAC-Adresstabelle. Wenn das Gerät die MAC-Adresse eines (nicht mehr) angeschlossenen Geräts (ver-)lernt, sendet das Gerät einen SNMP-Trap.

Diese Funktion ist für Ports gedacht, an die Sie Endgeräte anschließen und an denen sich folglich die MAC-Adresse selten ändert.

Funktion

Funktion

Schaltet die Funktion *MAC-Benachrichtigung* im Gerät ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *MAC-Benachrichtigung* ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *MAC-Benachrichtigung* ist ausgeschaltet.

Konfiguration

Intervall [s]

Legt das Sendeintervall in Sekunden fest. Wenn das Gerät die MAC-Adresse eines (nicht mehr) angeschlossenen Geräts (ver-)lernt, sendet das Gerät nach dieser Zeit einen SNMP-Trap.

Mögliche Werte:

- `0..2147483647` (Voreinstellung: `30`)

Das Gerät erfasst vor dem Senden eines SNMP-Trap bis zu 20 MAC-Adressen. Wenn das Gerät sehr viele Änderungen erkennt, dann sendet es den SNMP-Trap bereits vor Ablauf des Sendeintervalls.

Tabelle

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert die Funktion *MAC-Benachrichtigung* auf dem Port.

Mögliche Werte:

- `markiert`
  Die Funktion *MAC-Benachrichtigung* ist auf dem Port aktiv.
  Das Gerät sendet einen SNMP-Trap, wenn eines der folgenden Ereignisse eintritt:
  - Das Gerät lernt die MAC-Adresse eines neu angeschlossenen Geräts.
  - Das Gerät verlernt die MAC-Adresse eines nicht mehr angeschlossenen Geräts.
- `unmarkiert` (Voreinstellung)
  Die Funktion *MAC-Benachrichtigung* ist auf dem Port inaktiv.

Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog *Diagnose* > Statuskonfiguration > *Alarme (Traps)* einschalten und mindestens ein Trap-Ziel festlegen.

Letzte MAC-Adresse

Zeigt die MAC-Adresse des Geräts, das zuletzt an den Port angeschlossen oder vom Port getrennt wurde.

Das Gerät erkennt die MAC-Adressen von Geräten, die wie folgt angeschlossen sind:

- direkt an den Port angeschlossen
- über andere Geräte im Netz mit dem Port verbunden

Letzter MAC-Status

Zeigt den Zustand des Werts *Letzte MAC-Adresse* auf dem Port.

Mögliche Werte:

- `added`
  Das Gerät hat erkannt, dass ein anderes Gerät an den Port angeschlossen wurde.
- `removed`
  Das Gerät hat erkannt, dass das angeschlossene Gerät vom Port entfernt wurde.
- `other`
  Das Gerät hat keinen Status erkannt.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

6.1.5 Alarme (Traps)

[Diagnose > Statuskonfiguration > Alarme (Traps)]

Das Gerät ermöglicht Ihnen, als Reaktion auf bestimmte Ereignisse einen SNMP-Trap zu senden. In diesem Dialog legen Sie die Trap-Ziele fest, an die das Gerät die SNMP-Traps sendet.

Die Ereignisse, bei denen das Gerät einen SNMP-Trap auslöst, legen Sie zum Beispiel in den folgenden Dialogen fest:
- im Dialog *Diagnose > Statuskonfiguration > Gerätestatus*
- im Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus*
- im Dialog *Diagnose > Statuskonfiguration > MAC-Benachrichtigung*

Funktion

Funktion

Schaltet das Senden von SNMP-Traps an die Trap-Ziele ein/aus.

Mögliche Werte:
- *An* (Voreinstellung)
  Das Senden von SNMP-Traps ist eingeschaltet.
- *Aus*
  Das Senden von SNMP-Traps ist ausgeschaltet.

Tabelle

Name

Legt die Bezeichnung des Trap-Ziels fest.

Mögliche Werte:
- Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

Adresse

Legt die IP-Adresse und die Port-Nummer des Trap-Ziels fest.

Mögliche Werte:
- `<Gültige IPv4-Adresse>:<Port-Nummer>`

Aktiv

Aktiviert/deaktiviert das Senden von SNMP-Traps an dieses Trap-Ziel.

Mögliche Werte:
- `markiert` (Voreinstellung)
  Das Senden von SNMP-Traps an das Trap-Ziel ist aktiv.
- `unmarkiert`
  Das Senden von SNMP-Traps an das Trap-Ziel ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

- Im Feld *Name* legen Sie eine Bezeichnung für das Trap-Ziel fest.
- Im Feld *Adresse*legen Sie die IP-Adresse und die Port-Nummer des Trap-Ziels fest.
  Wenn Sie auf die Eingabe der Port-Nummer verzichten, fügt das Gerät automatisch die Port-Nummer `162` hinzu.

6.2 System

[Diagnose > System]

Das Menü enthält die folgenden Dialoge:

- Systeminformationen
- Hardware-Zustand
- IP-Adressen Konflikterkennung
- ARP
- Selbsttest

6.2.1 Systeminformationen

[Diagnose > System > Systeminformationen]

Dieser Dialog zeigt den gegenwärtigen Betriebszustand einzelner Komponenten im Gerät. Die angezeigten Werte sind ein Schnappschuss, sie repräsentieren den Betriebszustand zum Zeitpunkt, zu dem der Dialog die Seite geladen hat.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Systeminformationen speichern

Öffnet die HTML-Seite in einem neuen Web-Browser-Fenster oder -Tab. Sie können die HTML-Seite mit dem entsprechenden Web-Browser-Befehl auf Ihrem PC speichern.

6.2.2 Hardware-Zustand

[Diagnose > System > Hardware-Zustand]

Dieser Dialog gibt Auskunft über Aufteilung und Zustand des Flash-Speichers des Geräts.

Information

Betriebszeit

Zeigt die Gesamtbetriebszeit des Geräts seit Lieferung.

Mögliche Werte:

- `..d ..h ..m ..s`
  Tag(e) Stunde(n) Minute(n) Sekunde(n)

Tabelle

Flash-Region

Zeigt die Bezeichnung des jeweiligen Speicherbereichs.

Beschreibung

Zeigt eine Beschreibung, wofür das Gerät den Speicherbereich verwendet.

Flash-Sektoren

Zeigt, wie viele Sektoren dem Speicherbereich zugewiesen sind.

Lösch-Vorgänge

Zeigt, wie viele Male das Gerät die Sektoren des Speicherbereichs überschrieben hat.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

6.2.3 IP-Adressen Konflikterkennung

[Diagnose > System > IP-Adressen Konflikterkennung]

Mit der Funktion *IP-Adressen Konflikterkennung* prüft das Gerät, ob ein weiteres Gerät im Netz die eigene IP-Adresse verwendet. Zu diesem Zweck analysiert das Gerät empfangene ARP-Pakete.

In diesem Dialog legen Sie das Verfahren fest, mit dem das Gerät Adresskonflikte erkennt und legen die erforderlichen Einstellungen dafür fest.

Das Gerät zeigt erkannte Adresskonflikte in der Tabelle.

Wenn das Gerät einen Adresskonflikt erkennt, blinkt die Status-LED des Geräts 4-mal rot.

Funktion

Funktion

Schaltet die Funktion *IP-Adressen Konflikterkennung* ein/aus.

Mögliche Werte:

- `An` (Voreinstellung)
  Die Funktion *IP-Adressen Konflikterkennung* ist eingeschaltet.
  Das Gerät prüft, ob ein weiteres Gerät im Netz die eigene IP-Adresse verwendet.
- `Aus`
  Die Funktion *IP-Adressen Konflikterkennung* ist ausgeschaltet.

Konfiguration

Erkennungs-Modus

Legt das Verfahren fest, mit dem das Gerät Adresskonflikte erkennt.

Mögliche Werte:

- `aktiv und passiv` (Voreinstellung)
  Das Gerät verwendet aktive und passive Adresskonflikt-Erkennung.

- *aktiv*
  Aktive Adresskonflikt-Erkennung. Das Gerät vermeidet aktiv, dass es mit einer bereits im Netz vorhandenen IP-Adresse kommuniziert. Die Adresskonflikt-Erkennung beginnt, sobald Sie das Gerät ans Netz anschließen oder seine IP-Parameter ändern.
  - Das Gerät sendet 4 ARP-Probe-Datenpakete mit dem im Feld *Erkennungs-Verzögerung [ms]* festgelegten zeitlichen Abstand. Empfängt das Gerät auf diese Datenpakete eine Antwort, liegt ein Addresskonflikt vor.
  - Erkennt das Gerät keinen Adresskonflikt, sendet es 2 Gratuitous-ARP-Datenpakete als Announcement. Diese Datenpakete sendet das Gerät auch dann, wenn die Adresskonflikt-Erkennung ausgeschaltet ist.
  - Ist die IP-Adresse bereits im Netz vorhanden, wechselt das Gerät zurück zu den zuvor verwendeten IP-Parametern (falls möglich).
    Erhält das Gerät seine IP-Parameter von einem DHCP-Server, sendet es eine DHCPDECLINE-Nachricht an den DHCP-Server zurück.
  - Das Gerät prüft jeweils nach der im Feld *Rückfallverzögerung [s]* festgelegten Zeit, ob der Adresskonflikt weiterhin besteht. Erkennt das Gerät 10 Adresskonflikte nacheinander, verlängert es die Wartezeit bis zur nächsten Prüfung auf 60 s.
  - Sobald das Gerät den Adresskonflikt behebt, geht das Management des Geräts wieder ans Netz.
- *passiv*
  Passive Adresskonflikt-Erkennung. Das Gerät analysiert den Datenverkehr im Netz. Wenn ein weiteres Gerät im Netz die eigene IP-Adresse verwendet, „verteidigt“ das Gerät seine IP-Adresse zunächst. Das Gerät hört auf zu senden, wenn anschließend das andere Gerät weiter mit derselben IP-Adresse sendet.
  - Zur „Verteidigung“ sendet das Gerät Gratuitous-ARP-Datenpakete. Diesen Vorgang wiederholt das Gerät sooft wie im Feld *Address-Protections*festgelegt.
  - Sendet das andere Gerät weiter mit derselben IP-Adresse, prüft das Gerät zyklisch jeweils nach der im Feld *Rückfallverzögerung [s]* festgelegten Zeit, ob der Adresskonflikt weiterhin besteht.
  - Sobald das Gerät den Adresskonflikt behebt, geht das Management des Geräts wieder ans Netz.

Periodische ARP-Überprüfung senden

Schaltet die periodische Adresskonflikt-Erkennung ein/aus.

Mögliche Werte:

- markiert (Voreinstellung)
  Die periodische Adresskonflikt-Erkennung ist eingeschaltet.
  - Das Gerät sendet jeweils nach 90 bis 150 Sekunden ein ARP-Probe-Datenpaket und wartet solange wie im Feld *Erkennungs-Verzögerung [ms]* festgelegt auf Antwort.
  - Erkennt das Gerät einen Adresskonflikt, wendet es die Funktionen des passiven Erkennungsmodus an. Wenn die Funktion *Trap senden* eingeschaltet ist, sendet das Gerät einen SNMP-Trap.
- unmarkiert
  Die periodische Adresskonflikt-Erkennung ist ausgeschaltet.

Erkennungs-Verzögerung [ms]

Legt die Zeitspanne in Millisekunden fest, in der das Gerät nach dem Senden eines ARP-Datenpakets auf Antwort wartet.

Mögliche Werte:

- `20..500` (Voreinstellung: `200`)

Rückfallverzögerung [s]

Legt die Zeit in Sekunden fest, nach der das Gerät erneut prüft, ob der Adresskonflikt weiterhin besteht.

Mögliche Werte:

- `3..3600` (Voreinstellung: `15`)

Address-Protections

Legt fest, wie viele Male das Gerät im passiven Erkennungsmodus zum „Verteidigen“ seiner IP-Adresse Gratuitous-ARP-Datenpakete sendet.

Mögliche Werte:

- `0..100` (Voreinstellung: `3`)

Protektions-Intervall [ms]

Legt die Zeit in Millisekunden fest, nach der das Gerät im passiven Erkennungsmodus zum „Verteidigen“ seiner IP-Adresse erneut Gratuitous-ARP-Datenpakete sendet.

Mögliche Werte:

- `20..5000` (Voreinstellung: `200`)

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät einen Adresskonflikt erkennt.

Mögliche Werte:

- `markiert`
  Das Senden von SNMP-Traps ist aktiv.
  Das Gerät sendet einen SNMP-Trap, wenn es einen Adresskonflikt erkennt.
- `unmarkiert` (Voreinstellung)
  Das Senden von SNMP-Traps ist inaktiv.

Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog *Diagnose* > Statuskonfiguration > *Alarme (Traps)* einschalten und mindestens ein Trap-Ziel festlegen.

Information

Konflikt erkannt

Zeigt, ob gegenwärtig ein Adresskonflikt besteht.

Mögliche Werte:

- `markiert`
  Das Gerät erkennt einen Adresskonflikt.
- `unmarkiert`
  Das Gerät erkennt keinen Adresskonflikt.

Tabelle

Zeitstempel

Zeigt den Zeitpunkt, zu dem das Gerät einen Adresskonflikt erkannt hat.

Port

Zeigt die Nummer des Ports, an dem das Gerät den Adresskonflikt erkannt hat.

IP-Adresse

Zeigt die IP-Adresse, die den Adresskonflikt hervorruft.

MAC-Adresse

Zeigt die MAC-Adresse des Geräts, mit dem der Adresskonflikt besteht.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

6.2.4 ARP

[Diagnose > System > ARP]

Dieser Dialog zeigt die MAC- und IP-Adressen der Nachbargeräte, die mit dem Management des Geräts verbunden sind.

Das Gerät kann IPv4- und IPv6-Adressen anzeigen. Im IPv6-Protokoll werden die Adressen benachbarter Geräte mithilfe des Neighbor Discovery Protocol (NDP) ermittelt.

Tabelle

Port

Zeigt die Nummer des Ports.

IP-Adresse

Zeigt die IPv4-Adresse oder die IPv6-Adresse eines benachbarten Geräts.

MAC-Adresse

Zeigt die MAC-Adresse eines benachbarten Geräts.

Letztes Update

Zeigt die Zeit in Sekunden, seit der die gegenwärtigen Einstellungen des Eintrags in der ARP-Tabelle eingetragen sind.

Typ

Zeigt die Art des Eintrags.

Mögliche Werte:

- `static`
  Statischer Eintrag. Der statische Eintrag bleibt nach dem Löschen der ARP-Tabelle erhalten.
- `dynamic`
  Dynamischer Eintrag. Das Gerät löscht den dynamischen Eintrag nach Überschreiten der *Aging-Time [s]*, falls das Gerät während dieser Zeit keine Daten von diesem Gerät empfängt.
- `local`
  IP- und MAC-Adresse des Geräte-Managements.

Aktiv

Zeigt, dass die ARP-Tabelle die IP/MAC-Adresszuweisung als aktiven Eintrag enthält.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

ARP-Tabelle zurücksetzen

Entfernt aus der ARP-Tabelle die dynamisch eingerichteten Adressen.

6.2.5 Selbsttest

[Diagnose > System > Selbsttest]

Dieser Dialog ermöglicht Ihnen, Folgendes zu tun:
- RAM-Test während des Starts des Geräts aktivieren/deaktivieren.
- Während des Systemstarts das Wechseln in den System-Monitor ermöglichen/unterbinden.
- Festlegen, wie sich das Gerät im verhält, wenn es einen Fehler erkennt.

Konfiguration

Die folgenden Einstellungen sperren Ihnen dauerhaft den Zugang zum Gerät, wenn das Gerät beim Neustart kein lesbares Konfigurationsprofil findet.
- Kontrollkästchen *SysMon1 ist verfügbar* ist `unmarkiert`.
- Kontrollkästchen *Bei Fehler Default-Konfiguration laden* ist `unmarkiert`.

Dies ist zum Beispiel dann der Fall, wenn sich das Passwort des zu ladenden Konfigurationsprofils von dem im Gerät festgelegten Passwort unterscheidet. Um das Gerät wieder entsperren zu lassen, wenden Sie sich an Ihren Vertriebspartner.

RAM-Test

Aktiviert/deaktiviert den RAM-Speicher-Test während des Neustarts.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Der RAM-Speicher-Test ist aktiviert. Während des Neustarts testet das Gerät den RAM-Speicher.
- `unmarkiert`
  Der RAM-Speicher-Test ist deaktiviert. Dies verkürzt die Startzeit des Geräts.

SysMon1 ist verfügbar

Aktiviert/deaktiviert den Zugang zum System-Monitor während des Neustarts.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Gerät ermöglicht Ihnen, während des Neustarts in den System-Monitor zu wechseln.
- `unmarkiert`
  Das Gerät startet ohne die Möglichkeit, in den System-Monitor zu wechseln.

Der System-Monitor ermöglicht Ihnen u. a., die Gerätesoftware zu aktualisieren und gespeicherte Konfigurationsprofile zu löschen.

Bei Fehler Default-Konfiguration laden

Aktiviert/deaktiviert das Laden der Werkseinstellungen, falls das Gerät beim Neustart kein lesbares Konfigurationsprofil findet.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Gerät lädt die Werkseinstellungen.
- `unmarkiert`
  Das Gerät bricht den Neustart ab und hält an. Der Zugriff auf das Management des Geräts ist ausschließlich mit dem Command Line Interface über die serielle Schnittstelle möglich.
  Um das Gerät wieder über das Netz erreichbar zu machen, wechseln Sie in den System-Monitor und setzen die Einstellungen zurück. Das Gerät lädt die Werkseinstellungen beim nächsten Neustart.

Tabelle

In dieser Tabelle legen Sie fest, wie sich das Gerät verhält, wenn es einen Fehler erkennt.

Ursache

Ursachen erkannter Fehler, auf die das Gerät reagiert.

Mögliche Werte:

- `task`
  Das Gerät erkennt Fehler in ausgeführten Anwendungen, zum Beispiel wenn eine Task abbricht oder nicht verfügbar ist.
- `resource`
  Das Gerät erkennt Fehler in den verfügbaren Ressourcen, zum Beispiel bei knapp werdendem Speicher.
- `software`
  Das Gerät erkennt Software-Fehler, zum Beispiel Fehler beim Konsistenz-Check.
- `hardware`
  Das Gerät erkennt Hardware-Fehler, zum Beispiel im Chipsatz.

Aktion

Legt das Verhalten des Geräts fest, wenn das nebenstehende Ereignis eintritt.

Mögliche Werte:

- `reboot` (Voreinstellung)
  Das Gerät löst einen Neustart aus.
- `logOnly`
  Das Gerät protokolliert den Fehler in der Log-Datei. Siehe Dialog *Diagnose > Bericht > System-Log*.
- `sendTrap`
  Das Gerät sendet einen SNMP-Trap.
  Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* einschalten und mindestens ein Trap-Ziel festlegen.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

6.3 E-Mail-Benachrichtigung

[Diagnose > E-Mail-Benachrichtigung]

Das Gerät ermöglicht Ihnen, mehrere Empfänger per E-Mail über aufgetretene Ereignisse zu benachrichtigen.

Das Gerät sendet die E-Mails sofort oder in regelmäßigen Abständen, abhängig vom Schweregrad des Ereignisses. Üblicherweise legen Sie fest, dass Ereignisse mit hohem Schweregrad sofort gemeldet werden.

Sie können jeweils mehrere Empfänger festlegen, an die das Gerät die E-Mails entweder sofort oder in regelmäßigen Abständen sendet.

Das Menü enthält die folgenden Dialoge:
- E-Mail-Benachrichtigung Global
- E-Mail-Benachrichtigung Empfänger
- E-Mail-Benachrichtigung Mail-Server

6.3.1 E-Mail-Benachrichtigung Global

[Diagnose > E-Mail-Benachrichtigung > Global]

In diesem Dialog legen Sie die Absender-Einstellungen fest. Außerdem legen Sie fest, für welche Ereignis-Schweregrade das Gerät die E-Mails sofort und für welche in regelmäßigen Abständen sendet.

Funktion

Funktion

Schaltet das Senden von E-Mails ein/aus.

Mögliche Werte:

- *An*
  Das Senden von von E-Mails ist eingeschaltet.
- *Aus* (Voreinstellung)
  Das Senden von von E-Mails ist ausgeschaltet.

Zertifikat

Das Gerät kann Nachrichten über ungesicherte Netze an einen Server senden. Um einen „Man in the Middle“-Angriff zu unterbinden, fordern Sie die Erstellung eines Zertifikates für den Server durch die Zertifizierungsstelle an. Konfigurieren Sie den Server, so dass er das Zertifikat verwendet. Übertragen Sie das Zertifikat auf das Gerät.

Für das Festlegen der Mail-Server-Einstellungen verwenden Sie die IP-Adresse oder den DNS-Namen, welche(r) im Zertifikat als `Common Name` oder `Subject Alternative Name` angegeben ist. Andernfalls wird die Validierung des Zertifikats erfolglos sein.

URL

Legt Pfad und Dateiname des Zertifikats fest.

Zulässig sind Zertifikate mit folgenden Eigenschaften:

- X.509-Format
- `.PEM` Dateinamenserweiterung
- Base64-kodiert, umschlossen von
  `-----BEGIN CERTIFICATE-----`
  und
  `-----END CERTIFICATE-----`

Aus Sicherheitsgründen empfehlen wir, stets ein Zertifikat zu verwenden, das von einer Zertifizierungsstelle signiert ist.

Das Gerät bietet Ihnen folgende Möglichkeiten, das Zertifikat in das Gerät zu kopieren:

- Import vom PC
  Befindet sich das Zertifikat auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie das Zertifikat in den -Bereich. Alternativ klicken Sie in den Bereich, um das Zertifikat auszuwählen.

- Import von einem FTP-Server
  Befindet sich das Zertifikat auf einem FTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  `ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Pfad>/<Dateiname>`
- Import von einem TFTP-Server
  Befindet sich das Zertifikat auf einem TFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  `tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
- Import von einem SCP- oder SFTP-Server
  Befindet sich das Zertifikat auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  - `scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`
    Nach Klicken der Schaltfläche *Start* zeigt das Gerät das Fenster *Anmeldeinformationen*. Geben Sie dort *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
  - `scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>`

Start

Kopiert das im Feld *URL* festgelegte Zertifikat in das Gerät.

Absender

Adresse

Legt die E-Mail-Adresse des Geräts fest.

Das Gerät sendet die E-Mails mit dieser E-Mail-Adresse als Absender.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Benachrichtung sofort

Hier legen Sie die Einstellungen für E-Mails fest, die das Gerät sofort sendet.

Schweregrad

Legt den Mindest-Schweregrad der Ereignisse fest, für die das Gerät die E-Mail sofort sendet. Wenn ein Ereignis mit diesem Schweregrad oder mit einem dringenderen Schweregrad auftritt, dann sendet das Gerät eine E-Mail an die Empfänger.

Mögliche Werte:

- *emergency*
- *alert* (Voreinstellung)
- *critical*
- *error*
- *warning*
- *notice*
- *informational*
- *debug*

Betreff

Legt den Betreff der E-Mail fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Benachrichtung periodisch

Hier legen Sie die Einstellungen für E-Mails fest, die das Gerät in regelmäßigen Abständen sendet.

Schweregrad

Legt den Mindest-Schweregrad der Ereignisse fest, für die das Gerät die E-Mail in regelmäßigen Abständen sendet. Wenn ein Ereignis mit diesem Schweregrad oder mit einem dringenderen Schweregrad auftritt, dann puffert das Gerät das Ereignis. Das Gerät sendet den Pufferinhalt in regelmäßigen Abständen oder wenn der Puffer überläuft.

Ereignisse mit weniger dringendem Schweregrad puffert das Gerät nicht.

Mögliche Werte:

- *emergency*
- *alert*
- *critical*
- *error*
- *warning* (Voreinstellung)
- *notice*
- *informational*
- *debug*

Betreff

Legt den Betreff der E-Mail fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Sende-Intervall [min]

Legt das Sendeintervall in Minuten fest.

Wenn das Gerät mindestens ein Ereignis gepuffert hat, dann sendet es nach dieser Zeit eine E-Mail mit dem Pufferinhalt.

Mögliche Werte:

- `30..1440` (Voreinstellung: `30`)

Senden

Sendet sofort eine E-Mail mit dem Pufferinhalt und leert den Puffer.

Information

Gesendete Nachrichten

Zeigt, wie viele Male das Gerät erfolgreich E-Mails an den Mail-Server gesendet hat.

Unzustellbare Nachrichten

Zeigt, wie viele Male das Gerät erfolglos versucht hat, E-Mails an den Mail-Server zu senden.

Zeitpunkt der letzten Nachricht

Zeigt den Zeitpunkt (Datum und Uhrzeit), zu dem das Gerät zuletzt eine E-Mail an den Mail-Server gesendet hat.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

E-Mail-Benachrichtung Statistik leeren

Setzt die Zähler im Rahmen *Information* auf `0`.

Bedeutung der Ereignis-Schweregrade

Schweregrad	Bedeutung
`emergency`	Gerät nicht betriebsbereit
`alert`	Sofortiger Bedienereingriff erforderlich
`critical`	Kritischer Zustand
`error`	Fehlerhafter Zustand
`warning`	Warnung
`notice`	Signifikanter, normaler Zustand
`informational`	Informelle Nachricht
`debug`	Debug-Nachricht

6.3.2 E-Mail-Benachrichtigung Empfänger

[Diagnose > E-Mail-Benachrichtigung > Empfänger]

In diesem Dialog legen Sie die Empfänger fest, an die das Gerät E-Mails sendet. Das Gerät ermöglicht Ihnen, bis zu 10 Empfänger festzulegen.

Tabelle

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Benachrichtungs-Typ

Legt fest, ob das Gerät die E-Mails an diesen Empfänger sofort oder in regelmäßigen Abständen sendet.

Mögliche Werte:

- *sofort*
  Das Gerät sendet die E-Mails an diesen Empfänger sofort.
- *periodisch*
  Das Gerät sendet die E-Mails an diesen Empfänger in regelmäßigen Abständen.

Adresse

Legt die E-Mail-Adresse des Empfängers fest.

Mögliche Werte:

- Gültige E-Mail-Adresse mit bis zu 255 Zeichen

Aktiv

Aktiviert/deaktivert das Benachrichtigen des Empfängers.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Benachrichtigen des Empfängers ist aktiv.
- `unmarkiert`
  Das Benachrichtigen des Empfängers ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

6.3.3 E-Mail-Benachrichtigung Mail-Server

[Diagnose > E-Mail-Benachrichtigung > Mail-Server]

In diesem Dialog legen Sie die Einstellungen für die Mail-Server fest. Das Gerät unterstützt verschlüsselte und unverschlüsselte Verbindungen zum Mail-Server.

Tabelle

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Beschreibung

Legt den Namen des Servers fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

IP-Adresse

Legt IP-Adresse oder DNS-Name des Servers fest.

Mögliche Werte:

- Gültige IPv4-Adresse (Voreinstellung: `0.0.0.0`)
- DNS-Name im Format `domain.tld` oder `host.domain.tld`
  Wenn Sie einen DNS-Namen fetlegen, dann schalten Sie außerdem die Funktion *Client* im Dialog *Erweitert > DNS > Client > Global* ein.
  Wenn Sie verschlüsselte Verbindungen herstellen und dafür das Zertifikat verwenden, dann vergewissern Sie sich, dass der DNS-Name und der im Zertifikat angegebene DNS-Name des Servers gleich sind.

Ziel-TCP-Port

Legt den TCP-Port des Servers fest.

Mögliche Werte:

- `1..65535` (Voreinstellung: `25`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Häufig verwendete TCP-Ports:

- SMTP `25`
- Message Submission `587`

Verschlüsselung

Legt das Protokoll fest, das die Verbindung zwischen Gerät und Mail-Server verschlüsselt.

Mögliche Werte:

- `none` (Voreinstellung)
  Das Gerät baut eine unverschlüsselte Verbindung zum Server auf.
- `tlsv1`
  Das Gerät baut eine verschlüsselte Verbindung zum Server auf und verwendet die startTLS-Erweiterung.

Benutzername

Legt den Benutzernamen für das Konto fest, das das Gerät verwendet, um sich beim Mail-Server anzumelden.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Passwort

Legt das Passwort für das Konto fest, das das Gerät verwendet, um sich beim Mail-Server anzumelden.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Timeout [s]

Legt fest, nach welcher Zeit in Sekunden das Gerät eine E-Mail noch einmal sendet. Voraussetzung ist, dass das Gerät aufgrund eines Verbindungsfehlers die E-Mail unvollständig gesendet hat.

Mögliche Werte:

- `1..15` (Voreinstellung: `3`)

Aktiv

Aktiviert/deaktiviert die Verwendung des Mail-Servers.

Mögliche Werte:

- `markiert`
  Der Mail-Server ist aktiv.
  Das Gerät sendet E-Mails an diesen Mail-Server.
- `unmarkiert` (Voreinstellung)
  Der Mail-Server ist inaktiv.
  Das Gerät sendet keine E-Mails an diesen Mail-Server.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Verbindung testen

Öffnet den Dialog *Verbindung testen*, um eine Test-E-Mail zu senden.

Wenn die Mail-Server-Einstellungen korrekt sind, dann erhalten die ausgewählten Empfänger eine Test-E-Mail.

- Im Feld *Empfänger* legen Sie fest, an welche Empfänger das Gerät die E-Mail sendet:
  - *sofort*
    Das Gerät sendet die Test-E-Mail an diejenigen Empfänger, an die das Gerät die E-Mails sofort sendet.
  - *periodisch*
    Das Gerät sendet die Test-E-Mail an diejenigen Empfänger, an die das Gerät die E-Mails in regelmäßigen Abständen sendet.
- Im Feld *Nachrichtentext* legen Sie den Text der E-Mail fest.

6.4 Syslog

[Diagnose > Syslog]

Das Gerät ermöglicht Ihnen, ausgewählte Ereignisse abhängig vom Schweregrad des Ereignisses an unterschiedliche Syslog-Server zu melden. In diesem Dialog legen Sie die Einstellungen dafür fest und verwalten bis zu 8 Syslog-Server.

Funktion

Funktion

Schaltet das Senden von Ereignissen an die Syslog-Server ein/aus.

Mögliche Werte:

- `An`
  Das Senden von Ereignissen ist eingeschaltet.
  Das Gerät sendet die in der Tabelle festgelegten Ereignisse zum jeweils festgelegten Syslog-Server.
- `Aus` (Voreinstellung)
  Das Senden von Ereignissen ist ausgeschaltet.

Zertifikat

Das Gerät kann Nachrichten über ungesicherte Netze an einen Server senden. Um einen „Man in the Middle“-Angriff zu unterbinden, fordern Sie die Erstellung eines Zertifikates für den Server durch die Zertifizierungsstelle an. Konfigurieren Sie den Server, so dass er das Zertifikat verwendet. Übertragen Sie das Zertifikat auf das Gerät.

Vergewissern Sie sich, dass Sie beim Festlegen der Parameter auf dem Server die IP-Adresse und den DNS-Namen festlegen, die im Zertifikat als `Common Name` oder `Subject Alternative Name` festgelegt sind. Andernfalls wird die Validierung des Zertifikats erfolglos sein.

Anmerkung: Um die Änderungen nach dem Laden eines neuen Zertifikates zu übernehmen, starten Sie die Funktion *Syslog* neu.

URL

Legt Pfad und Dateiname des Zertifikats fest.

Zulässig sind Zertifikate mit folgenden Eigenschaften:

- X.509-Format
- `.PEM` Dateinamenserweiterung
- Base64-kodiert, umschlossen von
  `-----BEGIN CERTIFICATE-----`
  und
  `-----END CERTIFICATE-----`

Aus Sicherheitsgründen empfehlen wir, stets ein Zertifikat zu verwenden, das von einer Zertifizierungsstelle signiert ist.

Das Gerät bietet Ihnen folgende Möglichkeiten, das Zertifikat in das Gerät zu kopieren:

- Import vom PC
  Befindet sich das Zertifikat auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie das Zertifikat in den  -Bereich. Alternativ klicken Sie in den Bereich, um das Zertifikat auszuwählen.
- Import von einem FTP-Server
  Befindet sich das Zertifikat auf einem FTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  `ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Pfad>/<Dateiname>`
- Import von einem TFTP-Server
  Befindet sich das Zertifikat auf einem TFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  `tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
- Import von einem SCP- oder SFTP-Server
  Befindet sich das Zertifikat auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  - `scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`
    Nach Klicken der Schaltfläche *Start* zeigt das Gerät das Fenster *Anmeldeinformationen*. Geben Sie dort *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
  - `scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>`

Start

Kopiert das im Feld *URL* festgelegte Zertifikat in das Gerät.

Tabelle

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Wenn Sie einen Tabelleneintrag löschen, bleibt eine Lücke in der Nummerierung. Wenn Sie einen neuen Tabelleneintrag erzeugen, schließt das Gerät die 1. Lücke.

Mögliche Werte:

- `1..8`

IP-Adresse

Legt die IP-Adresse des Syslog-Servers fest.

Mögliche Werte:

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

Ziel-UDP-Port

Legt den TCP- oder UDP-Port fest, auf dem der Syslog-Server die Log-Einträge erwartet.

Mögliche Werte:

- `1..65535` (Voreinstellung: `514`)

Transport-Typ

Legt den Transporttyp fest, den das Gerät verwendet, um Ereignisse an den Syslog-Server zu senden.

Mögliche Werte:

- `udp` (Voreinstellung)
  Das Gerät sendet die Ereignisse über den in Spalte *Ziel-UDP-Port* festgelegten UDP-Port.
- `tls`
  Das Gerät sendet die Ereignisse mit TLS über den in Spalte *Ziel-UDP-Port* festgelegten TCP-Port.

Min. Schweregrad

Legt den Mindest-Schweregrad der Ereignisse fest. Das Gerät sendet einen Log-Eintrag für Ereignisse mit diesem Schweregrad und mit dringlicheren Schweregraden an den Syslog-Server.

Mögliche Werte:

- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (Voreinstellung)
- `notice`
- `informational`
- `debug`

Typ

Legt den Typ des Log-Eintrags fest, den das Gerät übermittelt.

Mögliche Werte:

- `systemlog` (Voreinstellung)
- `audittrail`

Aktiv

Aktiviert bzw. deaktiviert die Übermittlung der Ereignisse zum Syslog-Server:

- `markiert`
  Das Gerät sendet Ereignisse zum Syslog-Server.
- `unmarkiert` (Voreinstellung)
  Die Übermittlung der Ereignisse zum Syslog-Server ist deaktiviert.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

6.5 Ports

[Diagnose > Ports]

Das Menü enthält die folgenden Dialoge:

- SFP
- TP-Kabeldiagnose
- Port-Monitor
- Auto-Disable
- Port-Mirroring

6.5.1 SFP

[Diagnose > Ports > SFP]

Dieser Dialog ermöglicht Ihnen, die gegenwärtige Bestückung des Geräts mit SFP-Transceivern und deren Eigenschaften einzusehen.

Tabelle

Die Tabelle zeigt ausschließlich dann gültige Werte, wenn das Gerät mit SFP-Transceivern bestückt ist.

Port

Zeigt die Nummer des Ports.

Modultyp

Typ des SFP-Transceivers, zum Beispiel M-SFP-SX/LC.

Seriennummer

Zeigt die Seriennummer des SFP-Transceivers.

Steckverbinder-Typ

Zeigt die Bauart des Steckverbinders.

Unterstützt

Zeigt, ob das Gerät den SFP-Transceiver unterstützt.

Temperatur [°C]

Betriebstemperatur des SFP-Transceivers in °Celsius.

Sendeleistung [mW]

Sendeleistung des SFP-Transceivers in mW.

Empfangsleistung [mW]

Empfangsleistung des SFP-Transceivers in mW.

Sendeleistung [dBm]

Sendeleistung des SFP-Transceivers in dBm.

Empfangsleistung [dBm]

Empfangsleistung des SFP-Transceivers in dBm.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

6.5.2 TP-Kabeldiagnose

[Diagnose > Ports > TP-Kabeldiagnose]

Diese Funktion testet ein an das Interface angeschlossene Kabel auf einen Kurzschluss oder eine Unterbrechung. Die Tabelle zeigt den Kabelstatus und die geschätzte Länge. Das Gerät zeigt auch die einzelnen, an den Port angeschlossenen Kabelpaare. Wenn das Gerät einen Kurzschluss oder eine Unterbrechung im Kabel ermittelt, zeigt es auch die geschätzte Entfernung zu dem Problem.

Um verlässliche Ergebnisse zu erhalten, verwenden Sie die Funktion *TP-Kabeldiagnose* für Twisted-Pair-Kabel, die mindestens 3 Meter lang sind.

Anmerkung: Dieser Test unterbricht den Datenverkehr auf dem betreffenden Port.

Information

Port

Zeigt die Nummer des Ports.

Status

Status des virtuellen Kabeltesters.

Mögliche Werte:

- *aktiv*
  Der Kabeltest ist im Gange.
  Um den Test zu starten, klicken Sie die Schaltfläche ☰ und dann den Eintrag *Starte Kabeldiagnose...*. Diese Aktion öffnet den Dialog *Port auswählen*.
- *erfolgreich*
  Das Gerät zeigt diesen Eintrag nach einem erfolgreichen Test.
- *Fehler*
  Das Gerät zeigt diesen Eintrag nach einer Unterbrechung des Tests.
- *nicht initialisiert*
  Das Gerät zeigt diesen Eintrag, während es sich im Standby befindet.

Tabelle

Kabelpaar

Zeigt das Kabelpaar, auf das sich dieser Eintrag bezieht. Das Gerät verwendet das erste unterstützte PHY-Register, um die Werte anzuzeigen.

Ergebnis

Zeigt das Ergebnis des Kabeltests.

Mögliche Werte:

- *normal*
  Das Kabel funktioniert ordnungsgemäß.

- *offen*
  Ein Bruch im Kabel verursacht eine Unterbrechung.
- *Kurzschluss*
  Einzelne Adern des Kabels berühren sich und verursachen einen Kurzschluss.
- *unbekannt*
  Das Gerät zeigt diesen Wert bei ungetesteten Kabelpaaren.

In den folgenden Fällen zeigt das Gerät andere Werte als erwartet:

- Wenn kein Kabel an den Port angeschlossen ist, zeigt das Gerät den Wert *unbekannt* anstatt *offen*.
- Wenn der Port deaktiviert ist, zeigt das Gerät den Wert *Kurzschluss*.

Min. Länge

Zeigt die minimale geschätzte Länge des Kabels in Metern.

Das Gerät zeigt den Wert 0, wenn die Kabellänge unbekannt ist oder wenn das Feld *Status* im Rahmen *Information* den Wert *aktiv*, *Fehler* oder *nicht initialisiert* zeigt.

Max. Länge

Zeigt die maximale geschätzte Länge des Kabels in Metern.

Das Gerät zeigt den Wert 0, wenn die Kabellänge unbekannt ist oder wenn das Feld *Status* im Rahmen *Information* den Wert *aktiv*, *Fehler* oder *nicht initialisiert* zeigt.

Distanz [m]

Zeigt die geschätzte Entfernung in Metern von einem Kabelende zum anderen oder zu einer Unterbrechung des Kabels.

Das Gerät zeigt den Wert 0, wenn die Kabellänge unbekannt ist oder wenn das Feld *Status* im Rahmen *Information* den Wert *aktiv*, *Fehler* oder *nicht initialisiert* zeigt.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Starte Kabeldiagnose...

Öffnet den Dialog *Port auswählen*.

In der Dropdown-Liste *Port* wählen Sie den zu testenden Port. Wenden Sie den Test ausschließlich für drahtgebundene Ports an.

Um den Kabeltest auf dem ausgewählten Port auszuführen, klicken Sie die Schaltfläche *Ok*.

6.5.3 Port-Monitor

[Diagnose > Ports > Port-Monitor]

Die Funktion *Port-Monitor* überwacht auf den Ports die Einhaltung festgelegter Parameter. Wenn die Funktion *Port-Monitor* eine Überschreitung der Parameter erkennt, dann führt das Gerät eine Aktion aus.

Um die *Port-Monitor*-Funktion anzuwenden, führen Sie die folgenden Schritte aus:
- Registerkarte *Global*
  - Schalten Sie im Rahmen *Funktion* die Funktion *Port-Monitor* ein.
  - Aktivieren Sie für jeden Port diejenigen Parameter, deren Einhaltung die Funktion *Port-Monitor* überwachen soll.
- Registerkarten *Link-Änderungen*, *CRC/Fragmente* und *Überlast-Erkennung*
  - Legen Sie für jeden Port die Schwellenwerte der Parameter fest.
- Registerkarte *Link-Speed-/Duplex-Mode-Erkennung*
  - Aktivieren Sie für jeden Port die erlaubten Kombinationen von Geschwindigkeit und Duplex-Modus.
- Registerkarte *Global*
  - Legen Sie für jeden Port eine Aktion fest, die das Gerät ausführt, wenn die Funktion *Port-Monitor* eine Überschreitung der Parameter erkennt.
- Registerkarte *Auto-Disable*
  - Markieren Sie für die überwachten Parameter das Kontrollkästchen *Auto-Disable*, wenn Sie die Aktion `auto-disable` mindestens einmal festgelegt haben.

Der Dialog enthält die folgenden Registerkarten:
- [Global]
- [Auto-Disable]
- [Link-Änderungen]
- [CRC/Fragmente]
- [Überlast-Erkennung]
- [Link-Speed-/Duplex-Mode-Erkennung]

[Global]

In dieser Registerkarte schalten Sie die Funktion *Port-Monitor* ein und legen die Parameter fest, deren Einhaltung die Funktion *Port-Monitor* überwacht. Außerdem legen Sie die Aktion fest, die das Gerät ausführt, wenn die Funktion *Port-Monitor* eine Überschreitung der Parameter erkennt.

Funktion

Funktion

Schaltet die Funktion *Port-Monitor* global ein/aus.

Mögliche Werte:
- `An`
  Die Funktion *Port-Monitor* ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *Port-Monitor* ist ausgeschaltet.

Tabelle

Port

Zeigt die Nummer des Ports.

Link-Änderungen an

Aktiviert/deaktiviert auf dem Port die Überwachung von Linkänderungen.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  - Die Funktion *Port-Monitor* überwacht Linkänderungen auf dem Port.
  - Wenn das Gerät zu viele Linkänderungen erkennt, dann führt es die in Spalte *Aktion* festgelegte Aktion aus.
  - In der Registerkarte *Link-Änderungen* legen Sie die zu überwachenden Parameter fest.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

CRC/Fragmente an

Aktiviert/deaktiviert die Überwachung von auf dem Port erkannten CRC-/Fragmentfehlern.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  - Die Funktion *Port-Monitor* überwacht CRC-/Fragmentfehler auf dem Port.
  - Wenn das Gerät zu viele CRC-/Fragmentfehler erkennt, dann führt es die in Spalte *Aktion* festgelegte Aktion aus.
  - In der Registerkarte *CRC/Fragmente* legen Sie die zu überwachenden Parameter fest.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Duplex-Mismatch-Erkennung an

Aktiviert/deaktiviert auf dem Port die Überwachung von Duplex-Mismatches.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  - Die Funktion *Port-Monitor* überwacht Duplex-Mismatches auf dem Port.
  - Wenn das Gerät einen Duplex-Mismatch erkennt, dann führt es die in Spalte *Aktion* festgelegte Aktion aus.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Überlast-Erkennung an

Aktiviert/deaktiviert auf dem Port die Überlast-Erkennung.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  - Die Funktion *Port-Monitor* überwacht die Last auf dem Port.
  - Wenn das Gerät Überlast auf dem Port erkennt, führt das Gerät die in Spalte *Aktion* festgelegte Aktion aus.
  - In der Registerkarte *Überlast-Erkennung* legen Sie die zu überwachenden Parameter fest.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Link-Speed-/Duplex-Mode-Erkennung an

Aktiviert/deaktiviert auf dem Port die Überwachung von Verbindungsgeschwindigkeit und Duplex-Modus.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  - Die Funktion *Port-Monitor* überwacht Verbindungsgeschwindigkeit und Duplex-Modus auf dem Port.
  - Wenn das Gerät eine unzulässige Kombination von Verbindungsgeschwindigkeit und Duplex-Modus feststellt, dann führt das Gerät die in Spalte *Aktion* festgelegte Aktion aus.
  - In der Registerkarte *Link-Speed-/Duplex-Mode-Erkennung* legen Sie die zu überwachenden Parameter fest.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Aktive Bedingung

Zeigt den überwachten Parameter, der zur Aktion auf dem Port geführt hat.

Mögliche Werte:

- `-`
  Kein überwachter Parameter.
  Das Gerät führt keine Aktion aus.
- *`Link-Änderungen`*
  Zu viele Linkänderungen im betrachteten Zeitraum.
- *`CRC/Fragmente`*
  Zu viele erkannte CRC-/Fragmentfehler im betrachteten Zeitraum.
- *`Duplex-Mismatch-Erkennung`*
  Duplex-Mismatch erkannt.
- *`Überlast-Erkennung`*
  Überlast erkannt im betrachteten Zeitraum.
- *`Link-Speed-/Duplex-Mode-Erkennung`*
  Unerlaubte Kombination von Geschwindigkeit und Duplex-Modus erkannt.

Aktion

Legt die Aktion fest, die das Gerät ausführt, wenn die Funktion *Port-Monitor* eine Überschreitung der Parameter erkennt.

Mögliche Werte:

- `disable port`
  Das Gerät schaltet den Port aus und sendet einen SNMP-Trap.
  Die „Link-Status“-LED des Ports blinkt 3× pro Periode.
  - Um den Port wieder einzuschalten, markieren Sie den Port und klicken die Schaltfläche und dann den Eintrag *Zurücksetzen*.
  - Wenn die Überschreitung der Parameter aufgehoben ist, dann schaltet die Funktion *Auto-Disable* den betreffenden Port nach der festzulegenden Wartezeit wieder ein. Voraussetzung ist, dass in der Registerkarte *Auto-Disable* das Kontrollkästchen für den überwachten Parameter markiert ist.
- `send trap`
  Das Gerät sendet einen SNMP-Trap.
  Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* einschalten und mindestens ein Trap-Ziel festlegen.
- `auto-disable` (Voreinstellung)
  Das Gerät schaltet den Port aus und sendet einen SNMP-Trap.
  Die „Link-Status“-LED des Ports blinkt 3× pro Periode.
  Voraussetzung ist, dass in der Registerkarte *Auto-Disable* das Kontrollkästchen für den überwachten Parameter markiert ist.
  - Der Dialog *Diagnose > Ports > Auto-Disable* zeigt, welche Ports aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet sind.
  - Die Funktion *Auto-Disable* schaltet den Port automatisch wieder ein. Legen Sie dazu im Dialog *Diagnose > Ports > Auto-Disable* in Spalte *Reset-Timer [s]* eine Wartezeit für den betreffenden Port fest.

Status Port

Zeigt den Betriebszustand des Ports.

Mögliche Werte:

- `up`
  Der Port ist eingeschaltet.
- `down`
  Der Port ist ausgeschaltet.
- `notPresent`
  Kein physischer Port vorhanden.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Zurücksetzen

Schaltet den in der Tabelle markierten Port wieder ein und setzt dessen Zähler zurück auf `0`. Davon betroffen sind die Zähler in den folgenden Dialogen:

- Dialog *Diagnose > Ports > Port-Monitor*
  - Registerkarte *Link-Änderungen*
  - Registerkarte *CRC/Fragmente*
  - Registerkarte *Überlast-Erkennung*
- Dialog *Diagnose > Ports > Auto-Disable*

[Auto-Disable]

In dieser Registerkarte aktivieren Sie die Funktion *Auto-Disable* für die von der Funktion *Port-Monitor* überwachten Parameter.

Tabelle

Grund

Zeigt die von der Funktion *Port-Monitor* überwachten Parameter.

Markieren Sie das nebenstehende Kontrollkästchen, damit die Funktion *Port-Monitor* bei Erkennen einer Überschreitung der überwachten Parameter die Aktion `auto-disable` ausführt.

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für nebenstehende Parameter.

Mögliche Werte:

- `markiert`
  Die Funktion *Auto-Disable* für nebenstehende Parameter ist aktiv.
  Bei Überschreiten der nebenstehenden Parameter führt das Gerät die Funktion *Auto-Disable* aus, wenn in Spalte *Aktion* der Wert `auto-disable` festgelegt ist.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Auto-Disable* für nebenstehende Parameter ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Zurücksetzen

Schaltet den in der Tabelle markierten Port wieder ein und setzt dessen Zähler zurück auf `0`. Davon betroffen sind die Zähler in den folgenden Dialogen:

- Dialog *Diagnose > Ports > Port-Monitor*
  - Registerkarte *Link-Änderungen*
  - Registerkarte *CRC/Fragmente*
  - Registerkarte *Überlast-Erkennung*
- Dialog *Diagnose > Ports > Auto-Disable*

[Link-Änderungen]

In dieser Registerkarte legen Sie für jeden Port die folgenden Einstellungen fest:

- Anzahl der Linkänderungen.
- Zeitraum, in welchem die Funktion *Port-Monitor* einen Parameter überwacht, um Abweichungen zu erkennen.

Außerdem sehen Sie, wie viele Linkänderungen die Funktion *Port-Monitor* bisher erkannt hat.

Die Funktion *Port-Monitor* überwacht diejenigen Ports, für die in der Registerkarte *Global* das Kontrollkästchen in Spalte *Link-Änderungen an* markiert ist.

Tabelle

Port

Zeigt die Nummer des Ports.

Abtast-Intervall [s]

Legt den Zeitraum in Sekunden fest, in welchem die Funktion *Port-Monitor* einen Parameter überwacht, um Abweichungen zu erkennen.

Mögliche Werte:

- `1..180` (Voreinstellung: `10`)

Link-Änderungen

Legt die Anzahl der Linkänderungen fest.

Wenn die Funktion *Port-Monitor* diese Anzahl an Linkänderungen im überwachten Zeitraum erkennt, dann führt das Gerät die festgelegte Aktion aus.

Mögliche Werte:

- `1..100` (Voreinstellung: `5`)

Letztes Abtast-Intervall

Zeigt die Anzahl der Linkänderungen, die das Gerät im zurückliegenden Zeitraum erkannt hat.

Gesamt

Zeigt die Gesamtzahl der Linkänderungen, die das Gerät seit dem Einschalten des Ports erkannt hat.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Zurücksetzen

Schaltet den in der Tabelle markierten Port wieder ein und setzt dessen Zähler zurück auf `0`. Davon betroffen sind die Zähler in den folgenden Dialogen:

- Dialog *Diagnose > Ports > Port-Monitor*
  - Registerkarte *Link-Änderungen*
  - Registerkarte *CRC/Fragmente*
  - Registerkarte *Überlast-Erkennung*
- Dialog *Diagnose > Ports > Auto-Disable*

[CRC/Fragmente]

In dieser Registerkarte legen Sie für jeden Port die folgenden Einstellungen fest:

- Die Rate erkannter Fragmentfehler.
- Zeitraum, in welchem die Funktion *Port-Monitor* einen Parameter überwacht, um Abweichungen zu erkennen.

Außerdem sehen Sie die Fragmentfehlerrate, die das Gerät bisher erkannt hat.

Die Funktion *Port-Monitor* überwacht diejenigen Ports, für die in der Registerkarte *Global* das Kontrollkästchen in Spalte *CRC/Fragmente an* markiert ist.

Tabelle

Port

Zeigt die Nummer des Ports.

Abtast-Intervall [s]

Legt den Zeitraum in Sekunden fest, in welchem die Funktion *Port-Monitor* einen Parameter überwacht, um Abweichungen zu erkennen.

Mögliche Werte:

- `5..180` (Voreinstellung: `10`)

CRC-/Fragment-Fehlerrate [ppm]

Legt die Rate erkannter Fragmentfehler (in parts per million) fest.

Wenn die Funktion *Port-Monitor* diese Fragmentfehlerrate im überwachten Zeitraum erkennt, dann führt das Gerät die festgelegte Aktion aus.

Mögliche Werte:

- `1..1000000` (Voreinstellung: `1000`)

Letztes aktives Intervall [ppm]

Zeigt die Fragmentfehlerrate, die das Gerät im zurückliegenden Zeitraum erkannt hat.

Gesamt [ppm]

Zeigt die Fragmentfehlerrate, die das Gerät seit dem Einschalten des Ports erkannt hat.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Zurücksetzen

Schaltet den in der Tabelle markierten Port wieder ein und setzt dessen Zähler zurück auf `0`. Davon betroffen sind die Zähler in den folgenden Dialogen:

- Dialog *Diagnose > Ports > Port-Monitor*
  - Registerkarte *Link-Änderungen*
  - Registerkarte *CRC/Fragmente*
  - Registerkarte *Überlast-Erkennung*
- Dialog *Diagnose > Ports > Auto-Disable*

[Überlast-Erkennung]

In dieser Registerkarte legen Sie für jeden Port die folgenden Einstellungen fest:

- Last-Grenzwerte.
- Zeitraum, in welchem die Funktion *Port-Monitor* einen Parameter überwacht, um Abweichungen zu erkennen.

Außerdem sehen Sie die Anzahl an Datenpaketen, die das Gerät bisher erkannt hat.

Die Funktion *Port-Monitor* überwacht diejenigen Ports, für die in der Registerkarte *Global* das Kontrollkästchen in Spalte *Überlast-Erkennung an* markiert ist.

Die Funktion *Port-Monitor* überwacht keine Ports, die Mitglied einer Link-Aggregation-Gruppe sind.

Tabelle

Port

Zeigt die Nummer des Ports.

Traffic-Typ

Legt den Typ der Datenpakete fest, die das Gerät beim Überwachen der Last auf dem Port berücksichtigt.

Mögliche Werte:

- `all`
  Die Funktion *Port-Monitor* überwacht Broadcast-, Multicast- und Unicast-Pakete.
- `bc` (Voreinstellung)
  Die Funktion *Port-Monitor* überwacht ausschließlich Broadcast-Pakete.
- `bc-mc`
  Die Funktion *Port-Monitor* überwacht ausschließlich Broadcast- und Multicast-Pakete.

Grenzwert-Typ

Legt die Einheit der Datenrate fest.

Mögliche Werte:

- `pps` (Voreinstellung)
  Pakete pro Sekunde
- `kbps`
  Kbit pro Sekunde
  Voraussetzung ist, dass der Wert in Spalte *Traffic-Typ* = `all` ist.

Unterer Grenzwert

Legt den unteren Schwellenwert für die Datenrate fest.

Die Funktion *Auto-Disable* schaltet den Port erst dann wieder ein, wenn die Last auf dem Port niedriger ist als der hier festgelegte Wert.

Mögliche Werte:

- `0..10000000` (Voreinstellung: `0`)

Oberer Grenzwert

Legt den oberen Schwellenwert für die Datenrate fest.

Wenn die Funktion *Port-Monitor* diese Last im überwachten Zeitraum erkennt, dann führt das Gerät die festgelegte Aktion aus.

Mögliche Werte:

- `0..10000000` (Voreinstellung: `0`)

Intervall [s]

Legt den Zeitraum in Sekunden fest, den die Funktion *Port-Monitor* für das Erkennen einer Überschreitung betrachtet.

Mögliche Werte:

- `1..20` (Voreinstellung: `1`)

Pakete

Zeigt die Anzahl an Broadcast-, Multicast- und Unicast-Paketen, die das Gerät im zurückliegenden Zeitraum erkannt hat.

Broadcast-Pakete

Zeigt die Anzahl an Broadcast-Paketen, die das Gerät im zurückliegenden Zeitraum erkannt hat.

Multicast-Pakete

Zeigt die Anzahl an Multicast-Paketen, die das Gerät im zurückliegenden Zeitraum erkannt hat.

Kbit/s

Zeigt die Datenrate in Kbit pro Sekunde, die das Gerät im zurückliegenden Zeitraum erkannt hat.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Zurücksetzen

Schaltet den in der Tabelle markierten Port wieder ein und setzt dessen Zähler zurück auf `0`. Davon betroffen sind die Zähler in den folgenden Dialogen:

- Dialog *Diagnose > Ports > Port-Monitor*
  - Registerkarte *Link-Änderungen*
  - Registerkarte *CRC/Fragmente*
  - Registerkarte *Überlast-Erkennung*
- Dialog *Diagnose > Ports > Auto-Disable*

[Link-Speed-/Duplex-Mode-Erkennung]

In dieser Registerkarte aktivieren Sie für jeden Port die erlaubten Kombinationen von Geschwindigkeit und Duplex-Modus.

Die Funktion *Port-Monitor* überwacht diejenigen Ports, für die in der Registerkarte *Global* das Kontrollkästchen in Spalte *Link-Speed-/Duplex-Mode-Erkennung an* markiert ist.

Die Funktion *Port-Monitor* überwacht ausschließlich eingeschaltete physische Ports.

Tabelle

Port

Zeigt die Nummer des Ports.

10 Mbit/s HDX

Aktiviert/deaktiviert das Akzeptieren der Kombination von 10 Mbit/s und Halbduplex auf dem Port durch den Port-Monitor.

Mögliche Werte:

- `markiert`
  Der Port-Monitor berücksichtigt die Kombinationen aus Geschwindigkeit und Duplex-Modus.
- `unmarkiert`
  Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte *Global* festgelegte Aktion aus.

10 Mbit/s FDX

Aktiviert/deaktiviert das Akzeptieren der Kombination von 10 Mbit/s und Vollduplex auf dem Port durch den Port-Monitor.

Mögliche Werte:

- `markiert`
  Der Port-Monitor berücksichtigt die Kombinationen aus Geschwindigkeit und Duplex-Modus.
- `unmarkiert`
  Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte *Global* festgelegte Aktion aus.

100 Mbit/s HDX

Aktiviert/deaktiviert das Akzeptieren der Kombination von 100 Mbit/s und Halbduplex auf dem Port durch den Port-Monitor.

Mögliche Werte:

- `markiert`
  Der Port-Monitor berücksichtigt die Kombinationen aus Geschwindigkeit und Duplex-Modus.
- `unmarkiert`
  Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte *Global* festgelegte Aktion aus.

100 Mbit/s FDX

Aktiviert/deaktiviert das Akzeptieren der Kombination von 100 Mbit/s und Vollduplex auf dem Port durch den Port-Monitor.

Mögliche Werte:

- `markiert`
  Der Port-Monitor berücksichtigt die Kombinationen aus Geschwindigkeit und Duplex-Modus.
- `unmarkiert`
  Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte *Global* festgelegte Aktion aus.

1.000 Mbit/s FDX

Aktiviert/deaktiviert das Akzeptieren der Kombination von 1 Gbit/s und Vollduplex auf dem Port durch den Port-Monitor.

Mögliche Werte:

- `markiert`
  Der Port-Monitor berücksichtigt die Kombinationen aus Geschwindigkeit und Duplex-Modus.
- `unmarkiert`
  Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte *Global* festgelegte Aktion aus.

2,5 Gbit/s FDX

Aktiviert/deaktiviert das Akzeptieren der Kombination von 2,5 Gbit/s und Vollduplex auf dem Port durch den Port-Monitor.

Mögliche Werte:

- `markiert`
  Der Port-Monitor berücksichtigt die Kombinationen aus Geschwindigkeit und Duplex-Modus.
- `unmarkiert`
  Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte *Global* festgelegte Aktion aus.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Zurücksetzen

Schaltet den in der Tabelle markierten Port wieder ein und setzt dessen Zähler zurück auf `0`. Davon betroffen sind die Zähler in den folgenden Dialogen:

- Dialog *Diagnose > Ports > Port-Monitor*
  - Registerkarte *Link-Änderungen*
  - Registerkarte *CRC/Fragmente*
  - Registerkarte *Überlast-Erkennung*
- Dialog *Diagnose > Ports > Auto-Disable*

6.5.4 Auto-Disable

[Diagnose > Ports > Auto-Disable]

Die Funktion *Auto-Disable* ermöglicht Ihnen, überwachte Ports automatisch auszuschalten und auf Wunsch wieder einzuschalten.

Beispielsweise die Funktion *Port-Monitor* und ausgewählte Funktionen im Menü *Netzsicherheit* verwenden die Funktion *Auto-Disable*, um Ports bei Überschreiten überwachter Parameter auszuschalten.

Wenn die Überschreitung der Parameter aufgehoben ist, dann schaltet die Funktion *Auto-Disable* den betreffenden Port nach der festzulegenden Wartezeit wieder ein.

Der Dialog enthält die folgenden Registerkarten:
- [Port]
- [Status]

[Port]

Diese Registerkarte zeigt, welche Ports aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet sind. Wenn Sie in Spalte *Reset-Timer [s]* eine Wartezeit festlegen, schaltet die Funktion *Auto-Disable* den betreffenden Port automatisch wieder ein, sofern die Überschreitung der Parameter aufgehoben ist.

Tabelle

Port

Zeigt die Nummer des Ports.

Reset-Timer [s]

Legt die Wartezeit in Sekunden fest, nach der die Funktion *Auto-Disable* den Port wieder einschaltet.

Mögliche Werte:
- `0` (Voreinstellung)
  Der Timer ist inaktiv. Der Port bleibt ausgeschaltet.
- `30..4294967295`
  Wenn die Überschreitung der Parameter aufgehoben ist, dann schaltet die Funktion *Auto-Disable* den betreffenden Port nach der hier festgelegten Wartezeit wieder ein.

Zeitpunkt des Fehlers

Zeigt, wann das Gerät aufgrund einer Überschreitung der Parameter den Port ausgeschaltet hat.

Verbleibende Zeit [s]

Zeigt die verbleibende Zeit in Sekunden, bis die Funktion *Auto-Disable* den Port wieder einschaltet.

Komponente

Zeigt, welche Software-Komponente im Gerät das Ausschalten des Ports veranlasst hat.

Mögliche Werte:

- `PORT_MON`
  Port-Monitor
  Siehe Dialog *Diagnose > Ports > Port-Monitor*.
- `PORT_ML`
  Port-Sicherheit
  Siehe Dialog *Netzsicherheit > Port-Sicherheit*.
- `DHCP_SNP`
  DHCP-Snooping
  Siehe Dialog *Netzsicherheit > DHCP-Snooping*.
- `DOT1S`
  BPDU-Guard
  Siehe Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- `DAI`
  Dynamic ARP Inspection
  Siehe Dialog *Netzsicherheit > Dynamic ARP Inspection*.

Grund

Zeigt den überwachten Parameter, der zum Ausschalten des Ports geführt hat.

Mögliche Werte:

- `none`
  Kein überwachter Parameter.
  Der Port ist eingeschaltet.
- `link-flap`
  Zu viele Linkänderungen. Siehe Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *Link-Änderungen*.
- `crc-error`
  Zu viele CRC-/Fragmentfehler erkannt. Siehe Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *CRC/Fragmente*.
- `duplex-mismatch`
  Duplex-Mismatch erkannt. Siehe Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *Global*.
- `dhcp-snooping`
  Zu viele DHCP-Pakete aus nicht-vertrauenswürdigen Quellen. Siehe Dialog *Netzsicherheit >* DHCP-Snooping *> Konfiguration*, Registerkarte *Port*.
- `arp-rate`
  Zu viele ARP-Pakete aus nicht-vertrauenswürdigen Quellen. Siehe Dialog *Netzsicherheit >* Dynamic ARP Inspection *> Konfiguration*, Registerkarte *Port*.
- `bpdu-rate`
  STP-BPDUs empfangen. Siehe Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- `mac-based-port-security`
  Zu viele Datenpakete von unerwünschten Absendern. Siehe Dialog *Netzsicherheit > Port-Sicherheit*.
- `overload-detection`
  Überlast. Siehe Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *Überlast-Erkennung*.
- `speed-duplex`
  Unerlaubte Kombination von Geschwindigkeit und Duplex-Modus erkannt. Siehe Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *Link-Speed-/Duplex-Mode-Erkennung*.
- `Loop protection`
  Layer-2-Loop auf dem Port erkannt. Siehe Dialog *Diagnose > Loop-Schutz*, Spalte *Loop erkannt*.

Aktiv

Zeigt, ob der Port aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet ist.

Mögliche Werte:

- `markiert`
  Der Port ist gegenwärtig ausgeschaltet.
- `unmarkiert`
  Der Port ist eingeschaltet.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[Status]

Diese Registerkarte zeigt, für welche überwachten Parameter die Funktion *Auto-Disable* aktiviert ist.

Tabelle

Grund

Zeigt die Parameter, die das Gerät überwacht.

Markieren Sie das nebenstehende Kontrollkästchen, damit die Funktion *Auto-Disable* bei Überschreiten der überwachten Parameter den Port ausschaltet und ggf. wieder einschaltet.

Kategorie

Zeigt, zu welcher Funktion der nebenstehende Parameter gehört.

Mögliche Werte:

- `port-monitor`
  Der Parameter gehört zu den Funktionen im Menü *Diagnose > Port > Port-Monitor*.
- `network-security`
  Der Parameter gehört zu den Funktionen im Menü *Netzsicherheit*.
- `l2-redundancy`
  Der Parameter gehört zu den Funktionen im Menü *Switching > L2-Redundanz*.

Auto-Disable

Zeigt, ob die Funktion *Auto-Disable* für den nebenstehenden Parameter aktiviert/deaktiviert ist.

Mögliche Werte:

- `markiert`
  Die Funktion *Auto-Disable* für nebenstehende Parameter ist aktiv.
  Die Funktion *Auto-Disable* schaltet bei Überschreiten der überwachten Parameter den betreffenden Port aus und ggf. wieder ein.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Auto-Disable* für nebenstehende Parameter ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Zurücksetzen

Schaltet den in der Tabelle markierten Port wieder ein und setzt dessen Zähler zurück auf `0`. Davon betroffen sind die Zähler in den folgenden Dialogen:

- Dialog *Diagnose > Ports > Port-Monitor*
  - Registerkarte *Link-Änderungen*
  - Registerkarte *CRC/Fragmente*
  - Registerkarte *Überlast-Erkennung*
- Dialog *Diagnose > Ports > Auto-Disable*

6.5.5 Port-Mirroring

[Diagnose > Ports > Port-Mirroring]

Die Funktion *Port-Mirroring* ermöglicht Ihnen, die empfangenen und gesendeten Datenpakete von ausgewählten Ports auf einen Ziel-Port zu kopieren. Mit einem Analyzer oder einer RMON-Probe, am Ziel-Port angeschlossen, lässt sich der Datenstrom beobachten und auswerten. Am Quell-Port bleiben die Datenpakete unverändert.

Anmerkung: Um den Zugriff über den Ziel-Port auf das Management des Geräts einzuschalten, markieren Sie vor Einschalten der Funktion *Port-Mirroring* das Kontrollkästchen *Management erlauben* im Rahmen *Ziel-Port*.

Funktion

Funktion

Schaltet die Funktion *Port-Mirroring* ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *Port-Mirroring* ist eingeschaltet.
  Das Gerät kopiert die Datenpakete von den ausgewählten Quell-Ports auf den Ziel-Port.
- `Aus` (Voreinstellung)
  Die Funktion *Port-Mirroring* ist ausgeschaltet.

Ziel-Port

Primärer Port

Legt den Ziel-Port fest.

Als Ziel-Port eignen sich Ports, die nicht für folgende Zwecke verwendet werden:

- Quell-Port
- L2-Redundanz-Protokolle

Mögliche Werte:

- `no Port` (Voreinstellung)
  Kein Ziel-Port ausgewählt.
- `<Port-Nummer>`
  Nummer des Ziel-Ports. Das Gerät kopiert die Datenpakete von den Quell-Ports auf diesen Port.

Das Gerät fügt den Datenpaketen, die der Quell-Port sendet, am Ziel-Port ein VLAN-Tag hinzu. Datenpakete, die der Quell-Port empfängt, sendet der Ziel-Port unmodifiziert.

Anmerkung: Der Ziel-Port benötigt ausreichend Bandbreite, um den Datenstrom aufzunehmen. Wenn der kopierte Datenstrom die Bandbreite des Ziel-Ports überschreitet, dann verwirft das Gerät überschüssige Datenpakete auf dem Ziel-Port.

Sekundärer Port

Legt einen zweiten Ziel-Port fest. Voraussetzung ist, dass Sie einen ersten Ziel-Port festgelegt haben.

Mögliche Werte:

- `no Port` (Voreinstellung)
  Kein Ziel-Port ausgewählt.
- `<Port-Nummer>`
  Nummer des Ziel-Ports. Das Gerät kopiert die Datenpakete von den Quell-Ports auf diesen Port.

Management erlauben

Aktiviert/deaktiviert den Zugriff auf das Management des Geräts über den Ziel-Port.

Mögliche Werte:

- `markiert`
  Der Zugriff über den Ziel-Port auf das Management des Geräts ist aktiv.
  Das Gerät ermöglicht den Benutzern über den Ziel-Port Zugriff auf das Management, ohne die aktive *Port-Mirroring*-Sitzung zu unterbrechen.
  - Das Gerät dupliziert auf dem Ziel-Port Multicasts, Broadcasts und unbekannte Unicasts.
  - Die VLAN-Einstellungen auf dem Ziel-Port bleiben unverändert. Voraussetzung für den Zugriff über den Ziel-Port auf das Management des Gerätes ist, dass der Ziel-Port Mitglied im Geräte-Management-VLAN ist.
- `unmarkiert` (Voreinstellung)
  Der Zugriff über den Ziel-Port auf das Management des Geräts ist inaktiv.
  Das Gerät unterbindet den Zugriff auf das Management des Geräts über den Ziel-Port.

Tabelle

Quell-Port

Legt die Nummer des Ports fest.

Mögliche Werte:

- `<Port-Nummer>`

Eingeschaltet

Aktiviert/deaktiviert das Kopieren der Datenpakete von diesem Quell-Port auf den Ziel-Port.

Mögliche Werte:

- `markiert`
  Das Kopieren der Datenpakete ist aktiv.
  Der Port ist als Quell-Port festgelegt.
- `unmarkiert` (Voreinstellung)
  Das Kopieren der Datenpakete ist inaktiv.
- (Ausgegraute Darstellung)
  Das Kopieren der Datenpakete dieses Ports ist nicht möglich.
  Mögliche Ursachen:
  - Der Port ist bereits als Ziel-Port festgelegt.
  - Der Port ist ein logischer Port, kein physischer Port.

Anmerkung: Das Gerät ermöglicht Ihnen, abzüglich des Ziel-Ports jeden physischen Port als Quell-Port festzulegen.

Typ

Legt fest, welche Datenpakete das Gerät auf den Ziel-Port kopiert.

Das Gerät fügt den Datenpaketen, die der Quell-Port sendet, am Ziel-Port ein VLAN-Tag hinzu. Datenpakete, die der Quell-Port empfängt, sendet der Ziel-Port unmodifiziert.

Mögliche Werte:

- `none` (Voreinstellung)
  Keine Datenpakete.
- `tx`
  Datenpakete, die der Quell-Port sendet.
- `rx`
  Datenpakete, die der Quell-Port empfängt.
- `txrx`
  Datenpakete, die der Quell-Port sendet und empfängt.

Anmerkung: Mit der Einstellung `txrx` kopiert das Gerät gesendete und empfangene Datenpakete. Der Ziel-Port benötigt mindestens eine Bandbreite, die der Summe aus Sende- und Empfangskanal der Quell-Ports entspricht. Beispielsweise ist bei gleichartigen Ports der Ziel-Port bereits zu 100 % ausgelastet, wenn Sende- und Empfangskanal eines Quell-Ports zu jeweils 50 % ausgelastet sind.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Konfiguration zurücksetzen

Setzt die Einstellungen des Dialogs auf die voreingestellten Werte zurück und überträgt die Änderungen in den flüchtigen Speicher des Geräts (*RAM*).

6.6 LLDP

[Diagnose > LLDP]

Das Gerät ermöglicht Ihnen, Informationen über benachbarte Geräte zu sammeln. Dazu nutzt das Gerät Link Layer Discovery Protocol (LLDP). Mit diesen Informationen ist eine Netzmanagement-Station in der Lage, die Struktur Ihres Netzes darzustellen.

Dieses Menü ermöglicht Ihnen, die Topologie-Erkennung zu konfigurieren und die empfangenen Informationen in Tabellenform anzuzeigen.

Das Menü enthält die folgenden Dialoge:

- LLDP Konfiguration
- LLDP Topologie-Erkennung

6.6.1 LLDP Konfiguration

[Diagnose > LLDP > Konfiguration]

Dieser Dialog ermöglicht Ihnen, die Topologie-Erkennung für jeden Port zu konfigurieren.

Funktion

Funktion

Schaltet die Funktion *LLDP* ein/aus.

Mögliche Werte:

- `An` (Voreinstellung)
  Die Funktion *LLDP* ist eingeschaltet.
  Die Topologie-Erkennung mit LLDP ist auf dem Gerät aktiv.
- `Aus`
  Die Funktion *LLDP* ist ausgeschaltet.

Konfiguration

Sende-Intervall [s]

Legt das Intervall in Sekunden fest, in dem das Gerät LLDP-Datenpakete sendet.

Mögliche Werte:

- `5..32768` (Voreinstellung: `30`)

Sende-Intervall Multiplikator

Legt den Faktor zur Bestimmung des Time-to-live-Werts für die LLDP-Datenpakete fest.

Mögliche Werte:

- `2..10` (Voreinstellung: `4`)

Der im LLDP-Header kodierte Time-to-live-Wert ergibt sich aus der Multiplikation dieses Wertes mit dem Wert im Feld *Sende-Intervall [s]*.

Reinitialisierungs-Verzögerung [s]

Legt die Verzögerung in Sekunden für die Re-Initialisierung eines Ports fest.

Mögliche Werte:

- `1..10` (Voreinstellung: `2`)

Wenn in Spalte *Funktion* der Wert `Aus` festgelegt ist, dann versucht das Gerät nach Ablauf der hier festgelegten Zeit den Port erneut zu initialisieren.

Sende-Verzögerung [s]

Legt die Verzögerung in Sekunden für die Übertragung von aufeinanderfolgenden LLDP-Datenpaketen fest, nachdem Konfigurationsänderungen im Gerät wirksam geworden sind.

Mögliche Werte:

- `1..8192` (Voreinstellung: `2`)

Der empfohlene Wert liegt zwischen einem Minimum von `1` und einem Maximum, das einem Viertel des Werts im Feld *Sende-Intervall [s]* entspricht.

Benachrichtigungs-Intervall [s]

Legt das Intervall in Sekunden für das Senden von LLDP-Benachrichtigungen fest.

Mögliche Werte:

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

Nach Senden eines Benachrichtigungs-Traps wartet das Gerät mindestens die hier festgelegte Zeit, bis es den nächsten Benachrichtigungs-Trap sendet.

Tabelle

Port

Zeigt die Nummer des Ports.

Funktion

Legt fest, ob der Port LLDP-Datenpakete sendet und empfängt.

Mögliche Werte:

- *transmit*
  Der Port sendet LLDP-Datenpakete, speichert jedoch keine Informationen über benachbarte Geräte.
- *receive*
  Der Port empfängt LLDP-Datenpakete, sendet jedoch keine Informationen an benachbarte Geräte.
- *receive and transmit* (Voreinstellung)
  Der Port sendet LLDP-Datenpakete und speichert Informationen über benachbarte Geräte.
- *disabled*
  Der Port sendet keine LLDP-Datenpakete und speichert keine Informationen über benachbarte Geräte.

Benachrichtung

Aktiviert/deaktiviert LLDP-Benachrichtigungen auf dem Port.

Mögliche Werte:

- `markiert`
  LLDP-Benachrichtigungen auf dem Port sind aktiv.
- `unmarkiert` (Voreinstellung)
  LLDP-Benachrichtigungen auf dem Port sind inaktiv.

Port-Beschreibung senden

Aktiviert/deaktiviert das Senden des TLV (Type-Length-Value) mit der Port-Beschreibung.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Senden des TLV ist aktiv.
  Das Gerät sendet den TLV mit der Port-Beschreibung.
- `unmarkiert`
  Das Senden des TLV ist inaktiv.
  Das Gerät sendet keinen TLV mit der Port-Beschreibung.

Systemname senden

Aktiviert/deaktiviert das Senden des TLV (Type-Length-Value) mit dem Gerätenamen.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Senden des TLV ist aktiv.
  Das Gerät sendet den TLV mit dem Gerätenamen.
- `unmarkiert`
  Das Senden des TLV ist inaktiv.
  Das Gerät sendet keinen TLV mit dem Gerätenamen.

Systembeschreibung senden

Aktiviert/deaktiviert das Senden des TLV (Type-Length-Value) mit der Systembeschreibung.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Senden des TLV ist aktiv.
  Das Gerät sendet den TLV mit der Systembeschreibung.
- `unmarkiert`
  Das Senden des TLV ist inaktiv.
  Das Gerät sendet keinen TLV mit der Systembeschreibung.

System-Ressourcen senden

Aktiviert/deaktiviert das Senden des TLV (Type-Length-Value) mit den System-Ressourcen (Leistungsfähigkeitsdaten).

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Senden des TLV ist aktiv.
  Das Gerät sendet den TLV mit den System-Ressourcen.
- `unmarkiert`
  Das Senden des TLV ist inaktiv.
  Das Gerät sendet keinen TLV mit den System-Ressourcen.

Nachbarn (max.)

Begrenzt für diesen Port die Anzahl der zu erfassenden benachbarten Geräte.

Mögliche Werte:

- `1..50` (Voreinstellung: `10`)

FDB-Modus

Legt fest, welche Funktion das Gerät verwendet, um benachbarte Geräte auf diesem Port zu erfassen.

Mögliche Werte:

- `lldpOnly`
  Das Gerät verwendet ausschließlich LLDP-Datenpakete, um benachbarte Geräte auf diesem Port zu erfassen.
- `macOnly`
  Das Gerät verwendet gelernte MAC-Adressen, um benachbarte Geräte auf diesem Port zu erfassen. Das Gerät verwendet die MAC-Adresse ausschließlich dann, wenn kein weiterer Eintrag in der Adresstabelle (FDB, Forwarding Database) für diesen Port vorhanden ist.
- `both`
  Das Gerät verwendet LLDP-Datenpakete und gelernte MAC-Adressen, um benachbarte Geräte auf diesem Port zu erfassen.
- `autoDetect` (Voreinstellung)
  Wenn das Gerät auf diesem Port LLDP-Datenpakete empfängt, dann arbeitet das Gerät wie mit der Einstellung `lldpOnly`. Andernfalls arbeitet das Gerät wie mit der Einstellung `macOnly`.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

6.6.2 LLDP Topologie-Erkennung

[Diagnose > LLDP > Topologie-Erkennung]

Geräte in Netzen senden Mitteilungen in Form von Paketen, welche auch unter dem Namen „LLDPDU“ (LLDP-Dateneinheit) bekannt sind. Die über LLDPDUs sendeten und empfangenen Daten sind aus vielen Gründen nützlich. So erkennt das Gerät etwa, bei welchen Geräten innerhalb des Netzes es sich um Nachbarn handelt und über welche Ports diese miteinander verbunden sind.

Der Dialog ermöglicht Ihnen, das Netz darzustellen und die angeschlossenen Geräte mitsamt ihren Funktionsmerkmalen zu ermitteln.

Der Dialog enthält die folgenden Registerkarten:
- [LLDP]
- [LLDP-MED]

[LLDP]

Diese Registerkarte zeigt die gesammelten LLDP-Informationen zu den Nachbargeräten an. Mit diesen Informationen ist eine Netzmanagement-Station in der Lage, die Struktur Ihres Netzes darzustellen.

Wenn an einem Port sowohl Geräte mit als auch ohne aktive Topologie-Erkennungs-Funktion angeschlossen sind, dann blendet die Topologie-Tabelle die Geräte ohne aktive Topologie-Erkennung aus.

Wenn ausschließlich Geräte ohne aktive Topologieerkennung an einen Port angeschlossen sind, enthält die Tabelle eine Zeile für diesen Port, um jedes Gerät zu repräsentieren. Diese Zeile enthält die Anzahl der angeschlossenen Geräte.

Die Weiterleitungstabelle (FDB) enthält MAC-Adressen von Geräten, welche die Topologietabelle aus Gründen der Übersicht ausblendet.

Wenn Sie an einen Port mehrere Geräte anschließen (zum Beispiel über einen Hub), zeigt die Tabelle für jedes angeschlossenes Gerät je eine Zeile.

Tabelle

Port

Zeigt die Nummer des Ports.

Nachbar-Bezeichner

Zeigt die Chassis-ID des Nachbargeräts. Dies kann zum Beispiel die Basis-MAC-Adresse des Nachbargeräts sein.

FDB

Zeigt, ob das angeschlossene Gerät LLDP aktiv unterstützt.

Mögliche Werte:

- `markiert`
  Das angeschlossene Gerät unterstützt kein LLDP.
  Das Gerät verwendet Informationen aus seiner Adresstabelle (FDB, Forwarding Database).
- `unmarkiert` (Voreinstellung)
  Das angeschlossene Gerät unterstützt aktiv LLDP.

Nachbar-IP-Adresse

Zeigt die IP-Adresse, mit der der Zugriff auf das Management des Nachbargeräts möglich ist.

Nachbar-Port-Beschreibung

Zeigt eine Beschreibung für den Port des Nachbargeräts.

Nachbar-Systemname

Zeigt den Gerätenamen des Nachbargeräts.

Nachbar-Systembeschreibung

Zeigt eine Beschreibung für das Nachbargerät.

Port-ID

Zeigt die ID des Ports, über den das Nachbargerät mit dem Gerät verbunden ist.

Autonegotiation-Unterstützung

Zeigt, ob der Port des Nachbargeräts Auto-Negotiation unterstützt.

Autonegotiation

Zeigt, ob Auto-Negotiation auf dem Port des Nachbargeräts aktiviert ist.

Unterstützt PoE

Zeigt, ob der Port des Nachbargeräts Pover over Ethernet (PoE) unterstützt.

PoE eingeschaltet

Zeigt, ob Power over Ethernet (PoE) auf dem Port des Nachbargeräts aktiviert ist.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[LLDP-MED]

Bei „LLDP for Media Endpoint Devices“ (LLDP-MED) handelt es sich um eine Erweiterung von LLDP, welche zwischen Endgeräten und Geräten im Netz arbeitet. Sie bietet insbesondere Unterstützung für VoIP-Anwendungen. Diese unterstützende Richtlinie bietet einen zusätzlichen Satz gebräuchlicher Mitteilungen (d. h. Nachrichten des Typs „Type Length Value“, TLV). Das Gerät nutzt die TLVs, um Funktionsmerkmale wie Netz-Richtlinien, PoE (Power over Ethernet), Bestandsverwaltung und Standortdaten zu ermitteln.

Tabelle

Port

Zeigt die Nummer des Ports.

Geräteklasse

Zeigt die Geräteklasse des über Fernverbindung angeschlossen Geräts.

- Der Wert `notDefined` zeigt, dass das Gerät Funktionsmerkmale aufweist, welche durch keine der *LLDP-MED*-Klassen abgedeckt sind.
- Der Wert `endpointClass1..3` zeigt, dass das Gerät die Funktionsmerkmale „EndPoint-Klasse 1..3“ aufweist.
- Der Wert `networkConnectivity` zeigt, dass das Gerät die Funktionsmerkmale eines Netzwerkverbindungsgeräts aufweist.

VLAN-ID

Zeigt die Erweiterung für die VLAN-Kennung des entfernten Systems, welches an diesen Port angeschlossen ist (gemäß IEEE 802.3).

- Das Gerät verwendet die Werte `1` bis `4042`, um eine gültige Port-VLAN-Kennung zu definieren.
- Das Gerät zeigt den Wert `0` für Pakete mit Prioritätsmarkierung. Dies bedeutet, dass ausschließlich die 802.1D-Priorität von Bedeutung ist und das Gerät die voreingestellte VLAN-Kennung des Eingangs-Ports verwendet.

Priorität

Zeigt den Wert der 802.1D-Priorität, welche dem an diesen Port angeschlossenen entfernten System zugeordnet ist.

DSCP

Zeigt den Wert für den „Differentiated Service Code Point“, welcher dem an diesen Port angeschlossenen entfernten System zugeordnet ist.

Status Unknown-Bit

Zeigt den sog. „Unknown Bit Status“ des eingehenden Verkehrs.

- Der Wert `true` zeigt, dass die Netz-Richtlinie für den angegebenen Anwendungstyp gegenwärtig unbekannt ist. In diesem Fall ignoriert die VLAN-ID die Schicht-2-Priorität und den Wert des Feldes *DSCP*.
- Der Wert `false` zeigt eine definierte Netz-Richtlinie.

Status Tagged-Bit

Zeigt den sog. „Tagged Bit Status“.

- Der Wert `true` zeigt, dass die Anwendung ein markiertes VLAN verwendet.
- Der Wert `false` zeigt, dass das Gerät für die spezifische Anwendung auf einen unmarkierten VLAN-Betrieb zurückgreift. In diesem Fall ignoriert das Gerät sowohl die VLAN-ID wie auch die Schicht-2-Prioritätsfelder. Der DSCP-Wert hingegen ist relevant.

Hardware-Revision

Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Hardware-Revisionskennung.

Firmware-Revision

Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Firmware-Revisionskennung.

Software-Revision

Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Software-Revisionskennung.

Seriennummer

Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Seriennummer.

Herstellername

Zeigt den vom entfernten Endpunkt mitgeteilten spezifischen Herstellernamen.

Modellname

Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Modellbezeichnung.

Asset-ID

Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Kennung zur Produktverfolgung.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

6.7 Loop-Schutz

[Diagnose > Loop-Schutz]

Die Funktion *Loop-Schutz* unterstützt beim Schutz vor Layer-2-Loops.

Ein Loop im Netz kann zu einem Stillstand des Netzes aufgrund von Überlastung führen. Eine mögliche Ursache ist das ständige Duplizieren von Datenpaketen aufgrund einer Fehlkonfiguration. Die Ursache kann zum Beispiel ein unsachgemäß angeschlossenes Kabel oder inkorrekte Einstellungen im Gerät sein.

Ein Layer-2-Loop im Netz entsteht zum Beispiel in den folgenden Fällen, wenn keine Redundanzprotokolle aktiv sind:

- Zwei Ports desselben Geräts sind direkt miteinander verbunden.
- Zwischen zwei Geräten ist mehr als eine aktive Verbindung eingerichtet.

In redundanten Netztopologien sind typischerweise verschiedene Redundanzprotokolle aktiv. In der Regel deaktivieren Sie die *Spanning Tree*-Funktion auf Ports, die an anderen Redundanzprotokollen beteiligt sind. Die Redundanzprotokolle unterstützen bereits beim Vermeiden von Loops.

Funktion

Funktion

Schaltet die Funktion *Loop-Schutz* ein/aus.

Mögliche Werte:

▶ `An`
Die Funktion *Loop-Schutz* ist eingeschaltet.
– An aktiven und passiven Ports wertet das Gerät empfangene *Loop-Detection*-Pakete aus. An aktiven Ports sendet das Gerät *Loop-Detection*-Pakete in regelmäßigen Abständen, wie im Feld *Sende-Intervall* angegeben.
Voraussetzung ist, dass die Funktion *Loop-Schutz* auf dem Port aktiv ist.
– Das Gerät ermöglicht Ihnen, Ethernet-Loops mit dem Meldekontakt zu überwachen. Siehe Dialog *Diagnose > Statuskonfiguration > Signalkontakt > Signalkontakt 1*, Kontrollkästchen für den Parameter *Ethernet-Loops*.

▶ `Aus` (Voreinstellung)
Die Funktion *Loop-Schutz* ist ausgeschaltet.
Das Gerät sendet weder *Loop-Detection*-Pakete noch wertet es empfangene *Loop-Detection*-Pakete aus.

Global

Sende-Intervall

Legt das Intervall in Sekunden fest, in dem das Gerät *Loop-Detection*-Pakete sendet, wenn die Funktion *Loop-Schutz* auf dem Port aktiv ist.

Mögliche Werte:

- `1..10`

Empfang-Grenzwert

Legt den Schwellenwert für die Anzahl der nacheinander empfangenen *Loop-Detection*-Pakete fest. Wenn die Anzahl diesen Schwellenwert erreicht oder überschreitet, dann führt das Gerät die in Spalte *Aktion* festgelegte Aktion aus.

Mögliche Werte:

- `1..50`

Konfiguration

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für *Loop-Schutz*.

Mögliche Werte:

- `markiert`
  Die Funktion *Auto-Disable* für *Loop-Schutz* ist aktiv.
  Voraussetzung für das Abschalten des Ports ist, dass in Spalte *Aktion* die Aktion *auto-disable* oder die Aktion *alle* festgelegt ist.
  Das Gerät ermöglicht Ihnen, die Wartezeit in Sekunden festzulegen, nach der die Funktion *Auto-Disable* den Port wieder einschaltet. Legen Sie dazu im Dialog *Diagnose > Ports > Auto-Disable* in der Spalte *Reset-Timer [s]* die Wartezeit fest.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Auto-Disable* für *Loop-Schutz* ist inaktiv.

Tabelle

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert die Funktion *Loop-Schutz* auf dem Port.

Mögliche Werte:

- `markiert`
  Die Funktion *Loop-Schutz* ist auf dem Port aktiv.
  Aktivieren Sie die Funktion ausschließlich auf Ports, die nicht Teil eines redundanten Netzpfads sind. Dies hilft, ein versehentliches Abschalten auf redundanten Netzpfaden zu vermeiden.
  Wenn das Gerät auf diesem Port ein *Loop-Detection*-Paket empfängt, das von einem anderen Port desselben Geräts gesendet wurde, dann führt das Gerät die in Spalte *Aktion* festgelegte Aktion aus.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Loop-Schutz* ist auf dem Port inaktiv. Der Port sendet weder *Loop-Detection*-Pakete noch wertet er empfangene *Loop-Detection*-Pakete aus.

Modus

Legt das Verhalten der Funktion *Loop-Schutz* auf dem Port fest.

Mögliche Werte:

- *aktiv*
  Das Gerät sendet *Loop-Detection*-Pakete und wertet empfangene *Loop-Detection*-Pakete aus.
- *passiv*
  Das Gerät wertet empfangene *Loop-Detection*-Pakete aus.

Aktion

Legt die Aktion fest, die das Gerät ausführt, wenn es einen Layer-2-Loop an diesem Port erkennt.

Mögliche Werte:

- *trap*
  Das Gerät sendet einen Trap.
- *auto-disable*
  Das Gerät schaltet den Port mit der Funktion *Auto-Disable* aus.
  Voraussetzung für das Abschalten des Ports ist, dass das Kontrollkästchen *Auto-Disable* im Rahmen *Konfiguration* markiert ist.
- *alle*
  Das Gerät sendet einen Trap. Dann schaltet das Gerät den Port mit der Funktion *Auto-Disable* aus.
  Voraussetzung für das Abschalten des Ports ist, dass das Kontrollkästchen *Auto-Disable* im Rahmen *Konfiguration* markiert ist.

VLAN-ID

Legt das VLAN fest, in welchem das Gerät die *Loop-Detection*-Pakete sendet.

Mögliche Werte:

- `0` (Voreinstellung)
  Das Gerät sendet die *Loop-Detection*-Pakete ohne VLAN-Tag.
- `1..4042`
  Das Gerät sendet die *Loop-Detection*-Pakete im festgelegten VLAN. Voraussetzung ist, dass das VLAN bereits eingerichtet ist und dass der Port ein Mitglied des VLANs ist. Siehe Dialog *Switching > VLAN > Port*.

Loop erkannt

Zeigt, ob das Gerät einen Layer-2-Loop auf dem Port erkannt hat.

Mögliche Werte:

- *ja*
  Das Gerät hat einen Layer-2-Loop auf dem Port erkannt.
  Nachdem der Loop aufgehoben und der Port wieder freigegeben ist, setzt das Gerät den Wert auf *nein* zurück.
- *nein*
  Das Gerät hat keinen Layer-2-Loop auf dem Port erkannt.

Loop-Anzahl

Zeigt die Anzahl der Loops, die das Gerät auf dem Port seit dem letzten Zurücksetzen der Portstatistik oder seit dem letzten Neustart des Geräts erkannt hat.

Letzter Loop-Zeitpunkt

Zeigt den Zeitpunkt, an dem das Gerät den letzten Loop auf dem Port erkannt hat.

Voraussetzung für die korrekte Ermittlung des Werts ist, dass Sie die Systemzeit des Gerätes mit der entsprechenden Referenzzeit synchronisieren. Siehe Dialog *Zeit > Grundeinstellungen*.

Gesendete Pakete

Zeigt die Anzahl der *Loop-Detection* an, die seit dem letzten Zurücksetzen der Portstatistik oder seit dem letzten Neustart des Geräts auf dem Port gesendet wurden.

Empfangene Pakete

Zeigt die Anzahl der gesendeten und wieder empfangenen *Loop-Detection*-Pakete auf dem Port seit dem letzten Zurücksetzen der Portstatistik oder seit dem letzten Neustart des Geräts.

Verworfene Pakete

Zeigt die Anzahl der verworfenen *Loop-Detection*-Pakete auf dem Port.

Beispiele für Gründe für verworfene Pakete:

- Das Gerät erkennt Pakete mit einem falschen Format.
- Das Gerät erkennt Pakete mit abgelaufenen Zeitstempeln (Pakete, die das Gerät mehr als 5 Sekunden nach dem Senden empfängt).
- Das Gerät hat ein Datenpaket mit einer nicht vorgesehenen VLAN-Information empfangen.
- Das Gerät erkennt empfangene Pakete an einem Port, der deaktiviert ist.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Port-Statistiken leeren

Setzt die Werte in den folgenden Spalten zurück:

- *Loop-Anzahl*
- *Gesendete Pakete*
- *Empfangene Pakete*

6.8 Bericht

[Diagnose > Bericht]

Das Menü enthält die folgenden Dialoge:

- Bericht Global
- Persistentes Ereignisprotokoll
- System-Log
- Audit-Trail

6.8.1 Bericht Global

[Diagnose > Bericht > Global]

Das Gerät ermöglicht Ihnen, über die folgenden Ausgaben bestimmte Ereignisse zu protokollieren:
- auf der Konsole
- auf einen oder mehreren Syslog-Servern
- auf einer per SSH aufgebauten Verbindung zum Command Line Interface
- auf einer per Telnet aufgebauten Verbindung zum Command Line Interface

In diesem Dialog legen Sie die erforderlichen Einstellungen fest. Durch Zuweisen eines Schweregrads legen Sie fest, welche Ereignisse das Gerät protokolliert.

Der Dialog ermöglicht Ihnen, ein ZIP-Archiv mit System-Informationen auf Ihrem PC zu speichern.

Console-Logging

Funktion

Schaltet die Funktion *Console-Logging* ein/aus.

Mögliche Werte:
- *An*
  Die Funktion *Console-Logging* ist eingeschaltet.
  Das Gerät protokolliert die Ereignisse auf der Konsole.
- *Aus* (Voreinstellung)
  Die Funktion *Console-Logging* ist ausgeschaltet.

Schweregrad

Legt den Mindest-Schweregrad für die Ereignisse fest. Das Gerät protokolliert Ereignisse mit diesem Schweregrad und mit dringlicheren Schweregraden.

Das Gerät gibt die Meldungen auf der seriellen Schnittstelle aus.

Mögliche Werte:
- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (Voreinstellung)
- `notice`
- `informational`
- `debug`

Buffered-Logging

Das Gerät puffert protokollierte Ereignisse in 2 getrennten Speicherbereichen, damit die Log-Einträge für dringliche Ereignisse erhalten bleiben.

Dieser Rahmen ermöglicht Ihnen, den Mindest-Schweregrad für Ereignisse festzulegen, die das Gerät im höher priorisierten Speicherbereich puffert.

Schweregrad

Legt den Mindest-Schweregrad für die Ereignisse fest. Das Gerät puffert Log-Einträge für Ereignisse mit diesem Schweregrad und mit dringlicheren Schweregraden im höher priorisierten Speicherbereich.

Mögliche Werte:

- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (Voreinstellung)
- `notice`
- `informational`
- `debug`

SNMP-Logging

Wenn Sie die Protokollierung von SNMP-Anfragen einschalten, sendet das Gerät diese als Ereignisse mit dem voreingestellten Schweregrad `notice` an die Liste der Syslog-Server. Der voreingestellte Mindest-Schweregrad für einen Syslog-Server-Eintrag ist `critical`.

Um SNMP-Anfragen an einen Syslog-Server zu senden, haben Sie mehrere Möglichkeiten, die Voreinstellungen zu ändern. Wählen Sie diejenige, die am besten zu Ihren Anforderungen passt.

- ☐ Setzen Sie den Schweregrad, mit dem das Gerät SNMP-Anfragen als Ereignisse erzeugt, auf `warning` oder `error`. Ändern Sie den Mindest-Schweregrad für einen Syslog-Eintrag bei einem oder mehreren Syslog-Servern auf den gleichen Wert.
  Sie haben auch die Möglichkeit, dafür einen eigenen Syslog-Server-Eintrag zu erzeugen.
- ☐ Setzen Sie ausschließlich den Schweregrad der SNMP-Anfragen auf `critical` oder höher. Das Gerät sendet dann SNMP-Anfragen als Ereignisse mit dem Schweregrad `critical` oder schwerer an die Syslog-Server.
- ☐ Setzen Sie ausschließlich den Mindest-Schweregrad bei einem oder mehreren Syslog-Server-Einträgen auf `notice` oder niedriger. Das Gerät sendet dann u. U. sehr viele Ereignisse an die Syslog-Server.

Protokolliere SNMP-Get-Requests

Schaltet die Protokollierung von SNMP Get requests ein/aus.

Mögliche Werte:

- *An*
  Die Protokollierung ist eingeschaltet.
  Das Gerät protokolliert SNMP Get requests als Ereignis im Syslog.
  Den Schweregrad für dieses Ereignis wählen Sie in der Dropdown-Liste *Schweregrad Get-Request* aus.
- *Aus* (Voreinstellung)
  Die Protokollierung ist ausgeschaltet.

Protokolliere SNMP-Set-Requests

Schaltet die Protokollierung von SNMP Set requests ein/aus.

Mögliche Werte:

- *An*
  Die Protokollierung ist eingeschaltet.
  Das Gerät protokolliert SNMP Set requests als Ereignis im Syslog.
  Den Schweregrad für dieses Ereignis wählen Sie in der Dropdown-Liste *Schweregrad Set-Request* aus.
- *Aus* (Voreinstellung)
  Die Protokollierung ist ausgeschaltet.

Schweregrad Get-Request

Legt den Schweregrad des Ereignisses fest, welches das Gerät bei SNMP Get requests protokolliert.

Mögliche Werte:

- `emergency`
- `alert`
- `critical`
- `error`
- `warning`
- `notice` (Voreinstellung)
- `informational`
- `debug`

Schweregrad Set-Request

Legt den Schweregrad des Ereignisses fest, welches das Gerät bei SNMP Set requests protokolliert.

Mögliche Werte:

- `emergency`
- `alert`
- `critical`
- `error`
- `warning`
- `notice` (Voreinstellung)

- informational
- debug

CLI-Logging

Funktion

Schaltet die Funktion *CLI-Logging* ein/aus.

Mögliche Werte:

- *An*
  Die Funktion *CLI-Logging* ist eingeschaltet.
  Das Gerät protokolliert jeden Befehl, den es über das Command Line Interface empfängt.
- *Aus* (Voreinstellung)
  Die Funktion *CLI-Logging* ist ausgeschaltet.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Support-Informationen herunterladen

Erzeugt ein ZIP-Archiv, das Sie mit dem Web-Browser vom Gerät herunterladen können.

Das ZIP-Archiv enthält Systeminformationen über das Gerät. Eine Erläuterung zu den im ZIP-Archiv enthaltenen Dateien finden Sie im folgenden Abschnitt.

Support Informationen: Im ZIP-Archiv enthaltene Dateien

Dateiname	Format	Bemerkungen
`audittrail.html`	HTML	Enthält die im Audit Trail chronologisch aufgezeichneten Systemereignisse und gespeicherten Änderungen durch die Benutzer.
`defaultconfig.xml`	XML	Enthält das Konfigurationsprofil mit den Werkseinstellungen.
`script`	TEXT	Enthält die Ausgaben des Kommandos `show running-config script`.
`runningconfig.xml`	XML	Enthält das Konfigurationsprofil mit den gegenwärtigen Betriebseinstellungen.
`supportinfo.html`	TEXT	Enthält geräteinterne Service-Information.
`systeminfo.html`	HTML	Enthält Information über die gegenwärtigen Einstellungen und Betriebsparameter.
`systemlog.html`	HTML	Enthält die in der Log-Datei protokollierten Ereignisse. Siehe Dialog *Diagnose > Bericht > System-Log*.

Bedeutung der Ereignis-Schweregrade

Schweregrad	Bedeutung
`emergency`	Gerät nicht betriebsbereit
`alert`	Sofortiger Bedienereingriff erforderlich
`critical`	Kritischer Zustand
`error`	Fehlerhafter Zustand
`warning`	Warnung
`notice`	Signifikanter, normaler Zustand
`informational`	Informelle Nachricht
`debug`	Debug-Nachricht

6.8.2 Persistentes Ereignisprotokoll

[Diagnose > Bericht > Persistentes Ereignisprotokoll]

Das Gerät ermöglicht Ihnen, die Log-Einträge in einer Datei im externen Speicher permanent zu speichern. Somit haben Sie auch nach einem Neustart des Geräts Zugriff auf die Log-Einträge.

In diesem Dialog begrenzen Sie die Größe der Log-Datei und legen den Mindest-Schweregrad für zu speichernde Ereignisse fest. Wenn die Log-Datei die festgelegte Größe erreicht, archiviert das Gerät diese Datei und speichert die folgenden Log-Einträge ein einer neu erstellten Datei.

In der Tabelle zeigt das Gerät die im externen Speicher vorgehaltenen Log-Dateien. Sobald die festgelegte maximale Anzahl an Dateien erreicht ist, löscht das Gerät die älteste Datei und benennt die verbleibenden Dateien um. Damit bleibt im externen Speicher ausreichend Speicherplatz verfügbar.

Anmerkung: Vergewissern Sie sich, dass ein externer Speicher angeschlossen ist. Um festzustellen, ob ein externer Speicher angeschlossen ist, siehe Spalte *Status* im Dialog *Grundeinstellungen > Externer Speicher*. Wir empfehlen, die Verbindung des externen Speichers mit der Funktion *Gerätestatus* zu überwachen, siehe Parameter *Externen Speicher entfernen* im Dialog *Diagnose > Statuskonfiguration > Gerätestatus*.

Funktion

Funktion

Schaltet die Funktion *Persistentes Ereignisprotokoll* ein/aus.

Aktivieren Sie die Funktion ausschließlich dann, wenn der externe Speicher im Gerät verfügbar ist.

Mögliche Werte:

- *An* (Voreinstellung)
  Die Funktion *Persistentes Ereignisprotokoll* ist eingeschaltet.
  Das Gerät speichert die Log-Einträge in einer Datei im externen Speicher.
- *Aus*
  Die Funktion *Persistentes Ereignisprotokoll* ist ausgeschaltet.

Konfiguration

Max. Datei-Größe [kByte]

Legt die maximale Größe der Log-Datei in KBytes fest. Wenn die Log-Datei die festgelegte Größe erreicht, archiviert das Gerät diese Datei und speichert die folgenden Log-Einträge ein einer neu erstellten Datei.

Mögliche Werte:

- `0..4096` (Voreinstellung: `1024`)

Der Wert `0` deaktiviert das Speichern der Log-Einträge in der Log-Datei.

Dateien (max.)

Legt die Anzahl an Log-Dateien fest, die das Gerät im externen Speicher vorhält.

Sobald die festgelegte maximale Anzahl an Dateien erreicht ist, löscht das Gerät die älteste Datei und benennt die verbleibenden Dateien um.

Mögliche Werte:

- `0..25` (Voreinstellung: `4`)

Der Wert `0` deaktiviert das Speichern der Log-Einträge in der Log-Datei.

Schweregrad

Legt den Mindest-Schweregrad der Ereignisse fest. Das Gerät speichert den Log-Eintrag für Ereignisse mit diesem Schweregrad und mit dringlicheren Schweregraden in der Log-Datei im externen Speicher.

Mögliche Werte:

- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (Voreinstellung)
- `notice`
- `informational`
- `debug`

Ziel der Log-Datei

Legt den Typ des externen Speichers für die Protokollierung fest.

Mögliche Werte:

- `usb`
  Externer USB-Speicher (EAM)

Tabelle

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Mögliche Werte:

- `1..25`

Das Gerät legt diese Nummer automatisch fest.

Dateiname

Zeigt den Dateinamen der Log-Datei im externen Speicher.

Mögliche Werte:

- `messages`
- `messages.X`

Datei-Größe [Byte]

Zeigt die Größe der Log-Datei im externen Speicher in Bytes.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Persistente Log-Datei löschen

Entfernt die Log-Dateien vom externen Speicher.

6.8.3 System-Log

[Diagnose > Bericht > System-Log]

Das Gerät protokolliert geräteinterne Ereignisse in einer Log-Datei (System Log).

Dieser Dialog zeigt die Log-Datei (System Log). Der Dialog ermöglicht Ihnen, die Log-Datei im HTML-Format auf Ihrem PC zu speichern.

Um die Log-Datei nach Suchbegriffen zu durchsuchen, verwenden Sie die Suchfunktion Ihres Web-Browsers.

Die Log-Datei bleibt bis zu einem Neustart des Geräts erhalten. Nach dem Neustart erstellt das Gerät die Datei neu.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Log-Datei speichern

Öffnet die HTML-Seite in einem neuen Web-Browser-Fenster oder -Tab. Sie können die HTML-Seite mit dem entsprechenden Web-Browser-Befehl auf Ihrem PC speichern.

Log-Datei löschen

Entfernt die protokollierten Einträge aus der Log-Datei.

6.8.4 Audit-Trail

[Diagnose > Bericht > Audit-Trail]

Dieser Dialog zeigt die Log-Datei (Audit Trail). Der Dialog ermöglicht Ihnen, die Log-Datei als HTML-Datei auf Ihrem PC zu speichern.

Um die Log-Datei nach Suchbegriffen zu durchsuchen, verwenden Sie die Suchfunktion Ihres Web-Browsers.

Das Gerät protokolliert Systemereignisse und schreibende Benutzeraktionen auf dem Gerät. Dies ermöglicht Ihnen, nachzuvollziehen, WER WANN WAS auf dem Gerät ändert. Voraussetzung ist, dass Ihrem Benutzerkonto die Benutzer-Rolle `auditor` oder `administrator` zugewiesen ist.

Unter anderem protokolliert das Gerät die folgenden Benutzeraktionen:
- Anmeldung eines Benutzers mit dem Command Line Interface (lokal oder remote)
- Manuelle Abmeldung eines Benutzers
- Automatische Abmeldung eines Benutzers im Command Line Interface nach vorgegebener Zeit der Inaktivität
- Neustart des Geräts
- Sperrung eines Benutzerkontos aufgrund erfolgloser Anmeldeversuche
- Sperrung des Zugriffs auf des Management des Geräts aufgrund erfolgloser Anmeldeversuche
- Im Command Line Interface ausgeführte Befehle, außer `show`-Befehle
- Änderungen an Konfigurationsvariablen
- Änderungen der Systemzeit
- Datei-Transfer-Operationen einschließlich Firmware-Updates
- Konfigurationsänderungen per Ethernet Switch Configurator
- Firmware-Updates und Automatisches Konfigurieren des Geräts über den externen Speicher
- Öffnen und Schließen von SNMP über einen HTTPS-Tunnel

Das Gerät protokolliert keine Passwörter. Die protokollierten Einträge sind schreibgeschützt und bleiben nach einem Neustart im Gerät gespeichert.

In der Voreinstellung des Geräts ist der Zugang zum System-Monitor während des Neustarts möglich. Ein Angreifer, der sich physisch Zugriff auf das Gerät verschafft, kann mit dem System-Monitor die Einstellungen im Gerät auf die voreingestellten Werte zurücksetzen. Anschließend ist der Zugriff auf das Gerät mit dem Standard-Passwort möglich, auch auf die Protokoll-Datei.

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Treffen Sie entsprechende Maßnahmen, um den physischen Zugriff auf das Gerät zu beschränken. Andernfalls deaktivieren Sie den Zugang zum System-Monitor. Siehe Dialog *Diagnose > System > Selbsttest*, Kontrollkästchen *SysMon1 ist verfügbar*.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Audit-Trail-Datei speichern

Öffnet die HTML-Seite in einem neuen Web-Browser-Fenster oder -Tab. Sie können die HTML-Seite mit dem entsprechenden Web-Browser-Befehl auf Ihrem PC speichern.

7 Erweitert

Das Menü enthält die folgenden Dialoge:

- DHCP-L2-Relay
- DHCP Server
- DNS
- Industrie-Protokolle
- Digital-IO Modul
- Command Line Interface

7.1 DHCP-L2-Relay

[Erweitert > DHCP-L2-Relay]

Auf der Frontblende des Gerätes finden Sie folgenden Gefahrenhinweis:

⚠ WARNUNG

UNBEABSICHTIGTER VORGANG

Ändern Sie die Kabelpositionen nicht, wenn DHCP Option 82 eingeschaltet ist. Lesen Sie vor der Wartung das Anwender-Handbuch.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Ein Netzadministrator verwendet den DHCP-L2-*Relay-Agenten*, um DHCP-Client-Informationen hinzuzufügen. L3-*Relay-Agenten* und DHCP-Server benötigen die DHCP-Client-Informationen, um den Clients eine IP-Adresse und eine Konfiguration zuzuweisen.

Sofern aktiv, fügt das Relay den Paketen die in diesem Dialog konfigurierten *Option 82*-Informationen hinzu, bevor es die DHCP-Anforderungen von den Clients an die Server übermittelt. Die *Option 82*-Felder zeigen eindeutige Informationen über den Client und das Relay an. Diese eindeutige Kennung besteht aus einer *Circuit-ID* für den Client und einer *Remote-ID* für das Relay.

Zusätzlich zu den Typ-, Längen- und Multicast-Feldern beinhaltet die *Circuit-ID* die VLAN-ID, die Gerätenummer, die Steckplatznummer sowie die Port-Nummer für den angeschlossenen Client.

Die *Remote-ID* besteht aus einem Typ- und einem Längenfeld sowie entweder einer MAC-Adresse, einer IP-Adresse, einer Client-Kennung oder einer benutzerdefinierten Gerätebeschreibung. Bei einer Client-Kennung handelt es sich um einen benutzerdefinierten Systemnamen für das Gerät.

Das DHCPv6-Protokoll verwendet einen *Relay-Agenten*, um *Relay-Agent*-Optionen zu DHCPv6-Paketen hinzuzufügen, die zwischen einem Client und einem DHCPv6-Server ausgetauscht werden. Der Lightweight-DHCPv6-Relay-Agent (LDRA) wird im RFC 6221 beschrieben.

Der LDRA verarbeitet 2 Arten von Nachrichten:

- *Relay-Forward*-Nachrichten
  Der *Relay-Agent* leitet *Relay-Forward*-Nachrichten weiter, die eindeutige Informationen über den Client enthalten. Die Informationen über den Client beinhalten die Peer-Adresse, also die IPv6-Link-Local-Adresse des Client und die *Interface-ID*-Information. Die *Interface-ID*-Information, auch *Option 18* genannt, stellt Informationen zur Verfügung, die das Interface identifizieren, über das die Client-Anfrage gesendet wurde.
- *Relay-Reply*-Nachrichten
  Der DHCPv6-Server sendet *Relay-Reply*-Nachrichten. Der *Relay-Agent* überprüft die Nachrichten, um die Informationen aus der ursprünglichen *Relay-Forward*-Nachricht aufzunehmen. Wenn die Informationen gültig sind, dann leitet der *Relay-Agent* das Paket an den Client weiter.

Das Menü enthält die folgenden Dialoge:

- DHCP-L2-Relay Konfiguration
- DHCP-L2-Relay Statistiken

7.1.1 DHCP-L2-Relay Konfiguration

Dieser Dialog ermöglicht Ihnen, die Relais-Funktion an einem Port und an einem VLAN zu aktivieren. Wenn Sie diese Funktion an einem Port aktivieren, leitet das Gerät die *Option 82*-Informationen entweder weiter oder verwirft diese Informationen an nicht vertrauenswürdigen Ports. Zudem ermöglicht Ihnen das Gerät, die Remote-Kennung festzulegen.

Die *Option 82*-Informationen sind auf die DHCPv4-L2-Relay-Funktion beschränkt. Die DHCPv6-L2-Relay-Funktion verwendet *Option 18*-Informationen für den Paketaustausch zwischen dem Client und dem DHCPv6-Server. Das Gerät verwirft DHCPv6-Pakete, die an einem Port empfangen werden, der keine *Option 18*-Informationen enthält.

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

Funktion

Funktion

Schaltet die DHCP-L2-Relay-Funktion des Geräts global ein oder aus.

Wenn diese Funktion eingeschaltet ist, können DHCPv4-L2-Relay-Funktionen und DHCPv6-L2-Relay-Funktionen gleichzeitig im Gerät betrieben werden.

Mögliche Werte:

- `An`
  Schaltet die Funktion *DHCP-L2-Relay* im Gerät ein.
- `Aus` (Voreinstellung)
  Schaltet die Funktion *DHCP-L2-Relay* im Gerät aus.

[Interface]

Tabelle

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert die Funktion *DHCP-L2-Relay* auf dem Port.

Voraussetzung ist, dass Sie die Funktion global aktivieren.

Mögliche Werte:

- `markiert`
  Die Funktion *DHCP-L2-Relay* ist aktiv.
- `unmarkiert` (Voreinstellung)
  Die Funktion *DHCP-L2-Relay* ist inaktiv.

Gesicherter Port

Aktiviert/deaktiviert den gesicherten *DHCP-L2-Relay*-Modus für den betreffenden Port.

Mögliche Werte:

- `markiert`
  Das Gerät akzeptiert DHCPv4-Pakete mit *Option 82*-Informationen.
  Das Gerät akzeptiert DHCPv6-Pakete mit *Option 18*-Informationen.
- `unmarkiert` (Voreinstellung)
  Das Gerät verwirft DHCPv4-Pakete, die an einem ungesicherten Port empfangen werden, der *Option 82*-Informationen enthält.
  Das Gerät verwirft DHCPv6-Pakete, die an einem Port empfangen werden, der keine *Option 18*-Informationen enthält.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

[VLAN-ID]

Tabelle

VLAN-ID

VLAN, auf das sich der Tabelleneintrag bezieht.

Aktiv

Aktiviert/deaktiviert die Funktion *DHCP-L2-Relay* in diesem VLAN.

Voraussetzung ist, dass Sie die Funktion global aktivieren.

Mögliche Werte:

- `markiert`
  Die Funktion *DHCP-L2-Relay* ist aktiv.
- `unmarkiert` (Voreinstellung)
  Die Funktion *DHCP-L2-Relay* ist inaktiv.

Circuit-ID

Aktiviert oder deaktiviert das Hinzufügen der *Circuit-ID* zu den *Option 82*-Informationen.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Aktiviert das gemeinsame Senden von *Circuit-ID* und *Remote-ID*.
- `unmarkiert`
  Das Gerät sendet ausschließlich die *Remote-ID*.

Remote-ID-Typ

Legt die Komponenten der *Remote-ID* für dieses VLAN fest.

Mögliche Werte:

- `ip`
  Legt die IP-Adresse des Geräts als *Remote-ID* fest.
- `mac` (Voreinstellung)
  Legt die MAC-Adresse des Geräts als *Remote-ID* fest.
- `client-id`
  Legt den Systemnamen des Geräts als *Remote-ID* fest.
- `other`
  Wenn Sie diesen Wert verwenden, geben Sie benutzerdefinierte Informationen in Spalte *Remote-ID* ein.

Remote-ID

Zeigt die *Remote-ID* für das VLAN.

Legen Sie die ID fest, wenn Sie in Spalte *Remote-ID-Typ* den Wert `other` festlegen.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

7.1.2 DHCP-L2-Relay Statistiken

[Erweitert > DHCP-L2-Relay > Statistiken]

Das Gerät überwacht den Verkehr auf den Ports und zeigt die Ergebnisse in tabellarischer Form.

Die Tabelle ist in unterschiedliche Kategorien unterteilt, um Sie bei der Analyse zu unterstützen.

Die DHCPv6-Relay-Optionen werden in der Statistik-Tabelle nicht angezeigt.

Tabelle

Port

Zeigt die Nummer des Ports.

Ungesicherte Server-Nachrichten mit Option 82

Zeigt die Anzahl der Nachrichten vom DHCP-Server, die mit *Option 82*-Informationen auf dem nicht vertrauenswürdigen Interface eingegangen sind.

Ungesicherte Client-Nachrichten mit Option 82

Zeigt die Anzahl der Nachrichten vom DHCP-Client, die mit *Option 82*-Informationen auf dem nicht vertrauenswürdigen Interface eingegangen sind.

Gesicherte Server-Nachrichten ohne Option 82

Zeigt die Anzahl der Nachrichten vom DHCP-Server, die ohne *Option 82*-Informationen auf dem vertrauenswürdigen Port eingegangen sind.

Gesicherte Client-Nachrichten ohne Option 82

Zeigt die Anzahl der Nachrichten des DHCP-Client, die ohne *Option 82*-Informationen auf dem vertrauenswürdigen Interface eingegangen sind.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Zurücksetzen

Setzt die gesamte Tabelle zurück.

7.2 DHCP Server

[Erweitert > DHCP Server]

Mit Hilfe des DHCP-Servers verwalten Sie eine Datenbank, welche die verfügbaren IP-Adressen sowie Konfigurationsdaten enthält. Wenn das Gerät eine Anfrage von einem Client erhält, prüft der DHCP-Server das Netz des DHCP-Clients und vergibt anschließend eine IP-Adresse. Sofern aktiviert, weist der DHCP-Server dem Client auch die entsprechenden Konfigurationsdaten zu. Die Konfigurationsdaten legen beispielsweise fest, welche IP-Adresse, welchen DNS-Server und welche Default-Route ein Client verwendet.

Der DHCP-Server weist einem Client für einen benutzerdefinierten Zeitraum eine bestimmte IP-Adresse zu. Der DHCP-Client ist verantwortlich dafür, die IP-Adresse vor Ablauf des Zeitraums zu verlängern. Ist der DHCP-Client außerstande, die Adresse zu verlängern, geht die Adresse für eine anderweitige Zuteilung in den Pool zurück.

Das Menü enthält die folgenden Dialoge:
- DHCP-Server Global
- DHCP-Server Pool
- DHCP-Server Lease-Tabelle

7.2.1 DHCP-Server Global

[Erweitert > DHCP Server > Global]

Aktivieren Sie die Funktion entsprechend Ihren Anforderungen entweder global oder pro Port.

Funktion

Funktion

Schaltet die DHCP-Server-Funktion des Geräts global ein oder aus.

Mögliche Werte:

- *An*
- *Aus* (Voreinstellung)

Konfiguration

IP-\u00dcberpr\u00fcfung

Aktiviert/deaktiviert das Prüfen auf eindeutige IP-Adressen. Vor dem Zuweisen einer IP-Adresse prüft der Server mit einer *ICMP Echo*-Abfrage, ob diese IP-Adresse bereits im Netz verwendet wird.

Mögliche Werte:

- markiert (Voreinstellung)
  Die Funktion *IP-\u00dcberpr\u00fcfung* ist aktiv.
- unmarkiert
  Die Funktion *IP-\u00dcberpr\u00fcfung* ist inaktiv.

Tabelle

Port

Zeigt die Nummer des Ports.

DHCP-Server aktiv

Aktiviert/deaktiviert die DHCP-Server-Funktion auf diesem Port.

Voraussetzung ist, dass Sie die Funktion global aktivieren.

Mögliche Werte:

- markiert (Voreinstellung)
  Die DHCP-Server-Funktion ist aktiv.
- unmarkiert
  Die DHCP-Server-Funktion ist inaktiv.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

7.2.2 DHCP-Server Pool

[Erweitert > DHCP Server > Pool]

Weisen Sie dem mit einem Port verbundenen Endgerät oder Switch eine IP-Adresse zu.

Der DHCP-Server stellt IP-Adress-Pools bereit, aus denen er den Clients IP-Adressen zuweist. Ein Pool besteht aus einer Liste mit Einträgen. Sie können einen Eintrag als statisch definieren, d. h. zu einer bestimmten IP-Adresse gehörend, oder als dynamisch, d. h. zu einem IP-Adressbereich gehörend. Das Gerät nimmt maximal 128 Pools auf. Die Pools zusammen nehmen maximal 1000 Einträge auf.

Bei statischer Zuteilung weist der DHCP-Server einem einzelnen Client eine bestimmte IP-Adresse zu. Der DHCP-Server identifiziert den Client über eine eindeutige Hardware-ID. Ein statischer Adresseintrag enthält eine IP-Adresse. Diese IP-Adresse wenden Sie entweder auf jeden Port oder auf einen bestimmten Port des Geräts an. Für eine statische Zuteilung geben Sie im Feld *IP-Adresse* eine zuzuweisende IP-Adresse ein und lassen Spalte *Letzte IP-Adresse* frei. Geben Sie eine Hardware-Kennung an, mit welcher der DHCP-Server den Client eindeutig identifiziert. Bei dieser Kennung kann es sich um eine MAC-Adresse, eine Client-ID, eine Remote-ID oder eine Circuit-ID handeln. Kontaktiert ein Client mit einer bekannten Hardware-Kennung das Gerät, weist der DHCP-Server die statische IP-Adresse zu.

Kontaktiert ein DHCP-Client bei dynamischer Zuweisung einen Port, weist der DHCP-Server eine noch freie IP-Adresse aus einem Pool für diesen Port zu. Für eine dynamische Zuteilung erstellen Sie einen Pool für die Ports, indem Sie einen IP-Adressbereich zuweisen. Legen Sie die erste und die letzte IP-Adresse des IP-Adressbereiches fest. Lassen Sie die Felder *MAC-Adresse*, *Client-ID*, *Remote-ID* und *Circuit-ID* frei. Sie haben die Möglichkeit, mehrere Pool-Einträge zu erzeugen. Dies ermöglicht Ihnen, einen IP-Adressbereich zu erzeugen, der Lücken enthält.

Dieser Dialog zeigt die unterschiedlichen Informationen, die zur Vergabe einer IP-Adresse für einen Port oder ein VLAN erforderlich sind. Verwenden Sie die Schaltfläche  , um einen Eintrag hinzuzufügen. Das Gerät fügt einen schreib- und lesbaren Eintrag hinzu.

Tabelle

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Aktiv

Aktiviert/deaktiviert die DHCP-Server-Funktion auf diesem Port.

Mögliche Werte:

- `markiert`
  Die DHCP-Server-Funktion ist aktiv.
- `unmarkiert` (Voreinstellung)
  Die DHCP-Server-Funktion ist inaktiv.

IP-Adresse

Legt die IP-Adresse für die statische IP-Adresszuweisung fest. Wenn Sie die dynamische IP-Adresszuweisung verwenden, definiert dieser Wert den Beginn des IP-Adressraums.

Mögliche Werte:

- Gültige IPv4-Adresse

Letzte IP-Adresse

Wenn Sie die dynamische IP-Adresszuweisung verwenden, definiert dieser Wert das Ende des IP-Adressraums.

Mögliche Werte:

- Gültige IPv4-Adresse

Port

Zeigt die Nummer des Ports.

VLAN-ID

Zeigt das VLAN, auf das sich der Tabelleneintrag bezieht.

Der Wert `1` entspricht dem Standard-VLAN für das Management des Geräts.

Mögliche Werte:

- `1..4042`

MAC-Adresse

Legt die MAC-Adresse des Geräts fest, welches die IP-Adresse vergibt.

Mögliche Werte:

- Gültige Unicast-MAC-Adresse
  Legen Sie den Wert mit Doppelpunkt-Trennzeichen fest, zum Beispiel `00:11:22:33:44:55`.
- `-`
  Bei der IP-Adresszuweisung ignoriert der Server diese Variable.

DHCP-Relay

Legt die IP-Adresse des DHCP-Relays fest, über das Clients ihre Anfrage an den DHCP-Server senden. Empfängt der DHCP-Server die Anfrage eines Clients über ein anderes DHCP-Relay, ignoriert er diese Anfrage.

Mögliche Werte:

- Gültige IPv4-Adresse
  IP-Adresse des DHCP-Relays.
- `-`
  Zwischen Client und DHCP-Server befindet sich kein DHCP-Relay.

Client-ID

Legt die Kennzeichnung des Client-Geräts fest, welches die IP-Adresse vergibt.

Mögliche Werte:

- 1..80 Bytes (Format `XX XX .. XX`)
- `-`
  Bei der IP-Adresszuweisung ignoriert der Server diese Variable.

Remote-ID

Legt die Kennzeichnung des entfernten Geräts fest, welches die IP-Adresse vergibt.

Mögliche Werte:

- 1..80 Bytes (Format `XX XX .. XX`)
- `-`
  Bei der IP-Adresszuweisung ignoriert der Server diese Variable.

Circuit-ID

Legt die Circuit-ID des Geräts fest, welches die IP-Adresse vergibt.

Mögliche Werte:

- 1..80 Bytes (Format `XX XX .. XX`)
- `-`
  Bei der IP-Adresszuweisung ignoriert der Server diese Variable.

Schneider Electric-Gerät

Aktiviert/deaktiviert Schneider Electric-Multicasts.

Aktivieren Sie diese Funktion, wenn das Gerät in diesem IP-Adressbereich ausschließlich Schneider Electric-Geräte bedient.

Mögliche Werte:

- `markiert`
  Das Gerät bedient in diesem IP-Adressbereich ausschließlich Schneider Electric-Geräte. Schneider Electric-Multicasts sind aktiviert.
- `unmarkiert` (Voreinstellung)
  Das Gerät bedient in diesem IP-Adressbereich Geräte unterschiedlicher Hersteller. Schneider Electric-Multicasts sind deaktiviert.

Konfigurations-URL

Legt das verwendete Protokoll sowie den Namen und den Pfad zur Konfigurationsdatei fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..70 Zeichen
  Beispiel: `tftp://192.9.200.1/cfg/config.xml`

Wenn Sie dieses Feld leer lassen, lässt das Gerät dieses Optionsfeld in der DHCP-Nachricht leer.

Lease-Time [s]

Legt die Vergabezeit in Sekunden fest.

Mögliche Werte:

- `60..220752000` (Voreinstellung: `86400`)
- `4294967295`
  Verwenden Sie diesen Wert für zeitlich unbegrenzte Vergaben oder für Vergaben über BOOTP.

Default-Gateway

Legt die IP-Adresse des Standard-Gateways fest.

Steht hier der Wert `0.0.0.0`, wird der DHCP-Nachricht kein Optionsfeld hinzugefügt.

Mögliche Werte:

- Gültige IPv4-Adresse

Netzmaske

Legt die Maske des Netzes fest, zu welcher der Client gehört.

Steht hier der Wert `0.0.0.0`, wird der DHCP-Nachricht kein Optionsfeld hinzugefügt.

Mögliche Werte:

- Gültige IPv4-Netzmaske

WINS-Server

Legt die IP-Adresse des Windows Internet Name Servers fest, welcher NetBIOS-Namen konvertiert.

Steht hier der Wert `0.0.0.0`, wird der DHCP-Nachricht kein Optionsfeld hinzugefügt.

Mögliche Werte:

- Gültige IPv4-Adresse

DNS-Server

Legt die IP-Adresse des DNS-Servers fest.

Steht hier der Wert `0.0.0.0`, wird der DHCP-Nachricht kein Optionsfeld hinzugefügt.

Mögliche Werte:

- Gültige IPv4-Adresse

Hostname

Legt den Host-Namen fest.

Wenn Sie dieses Feld leer lassen, lässt das Gerät dieses Optionsfeld in der DHCP-Nachricht leer.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

7.2.3 DHCP-Server Lease-Tabelle

[Erweitert > DHCP Server > Lease-Tabelle]

Dieser Dialog zeigt den Status der IP-Adressvergabe auf den einzelnen Ports.

Tabelle

Port

Zeigt die Nummer des Ports, an welchen die Adresse gegenwärtig vergeben ist.

IP-Adresse

Zeigt die vergebene IP-Adresse, auf die sich der Eintrag bezieht.

Status

Zeigt die Phase der Vergabe.

Gemäß DHCP-Standard läuft die Vergabe von IP-Adressen in 4 Schritten ab: Discovery (Client sendet Anfrage an Server), Offer (Server bieten IP-Adresse an), Request (Client fordert IP-Adresse an) sowie Acknowledgement (Server bestätigt Adresse).

Mögliche Werte:

- `bootp`
  Ein DHCP-Client versucht gerade, einen DHCP-Server für die IP-Adresszuweisung zu ermitteln.
- `offering`
  Der DHCP-Server prüft gerade, ob die IP-Adresse für den Client geeignet ist.
- `requesting`
  Ein DHCP-Client bezieht gerade die angebotene IP-Adresse.
- `bound`
  Der DHCP-Server vergibt die IP-Adresse an einen Client.
- `renewing`
  Der DHCP-Client fordert eine Verlängerung der Adressvergabe an.
- `rebinding`
  Nach einer erfolgreichen Verlängerung vergibt der DHCP-Server die IP-Adresse an den Client.
- `declined`
  Der DHCP-Server hat die Anfrage nach der IP-Adresse abgelehnt.
- `released`
  Die IP-Adresse steht für andere Clients zur Verfügung.

Verbleibende Lifetime

Zeigt die verbleibende Zeit für die Vergabe der IP-Adresse.

Vergeben an MAC-Adresse

Zeigt die MAC-Adresse des Geräts, welches die IP-Adresse vergibt.

Gateway

Zeigt die Gateway-IP-Adresse des Geräts, welches die IP-Adresse vergibt.

Client-ID

Zeigt die Client-Kennung des Geräts, welches die IP-Adresse vergibt.

Remote-ID

Zeigt die Remote-Kennung des Geräts, welches die IP-Adresse vergibt.

Circuit-ID

Zeigt die Circuit-ID des Geräts, welches die IP-Adresse vergibt.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

7.3 DNS

[Erweitert > DNS]

Das Menü enthält die folgenden Dialoge:
- DNS-Client

7.3.1 DNS-Client

[Erweitert > DNS > Client]

DNS (Domain Name System) ist ein Dienst im Netz, der Hostnamen in IP-Adressen übersetzt. Diese Namensauflösung ermöglicht Ihnen, andere Geräte mit ihrem Hostnamen anstatt mit ihrer IP-Adresse zu erreichen.

Die Funktion *Client* befähigt das Gerät, Anfragen zur Auflösung von Hostnamen in IP-Adressen an einen DNS-Server zu senden.

Das Menü enthält die folgenden Dialoge:
- DNS-Client Global
- DNS-Client Aktuell
- DNS-Client Statisch
- DNS-Client Statische Hosts

7.3.1.1 DNS-Client Global

[Erweitert > DNS > Client > Global]

In diesem Dialog schalten Sie die Funktion *Client* und die Funktion *Cache* ein.

Funktion

Funktion

Schaltet die Funktion *Client* ein/aus.

Mögliche Werte:

- *An*
  Die Funktion *Client* ist eingeschaltet.
  Das Gerät sendet Anfragen zur Auflösung von Hostnamen in IP-Adressen an einen DNS-Server.
- *Aus* (Voreinstellung)
  Die Funktion *Client* ist ausgeschaltet.

Cache

Cache

Schaltet die Funktion *Cache* ein/aus.

Mögliche Werte:

- *An* (Voreinstellung)
  Die Funktion *Cache* ist eingeschaltet.
  Das Gerät speichert flüchtig im Cache bis zu 128 DNS-Server-Antworten (Hostname und zugehörige IP-Adresse). Bei einer erneuten Anfrage löst das Gerät den Hostnamen selbst auf, wenn der Cache einen passenden Eintrag enthält. Die erneute Anfrage bei einem DNS-Server ist damit unnötig.
- *Aus*
  Die Funktion *Cache* ist ausgeschaltet.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

Cache leeren

Entfernt jeden Eintrag aus dem DNS-Cache.

7.3.1.2 DNS-Client Aktuell

[Erweitert > DNS > Client > Aktuell]

Dieser Dialog zeigt, an welche DNS-Server das Gerät Anfragen zur Auflösung von Hostnamen in IP-Adressen weiterleitet.

Tabelle

Index

Zeigt die fortlaufende Nummer des DNS-Servers.

Adresse

Zeigt die IP-Adresse des DNS-Servers. Das Gerät leitet Anfragen zur Auflösung von Hostnamen in IP-Adressen an den DNS-Server mit dieser IP-Adresse weiter.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

7.3.1.3 DNS-Client Statisch

[Erweitert > DNS > Client > Statisch]

In diesem Dialog legen Sie die DNS-Server fest, an die das Gerät Anfragen zur Auflösung von Hostnamen in IP-Adressen weiterleitet.

Das Gerät ermöglicht Ihnen, selbst bis zu 4 IP-Adressen festzulegen oder die IP-Adressen von einem DHCP-Server zu beziehen.

Konfiguration

Konfigurationsquelle

Legt die Quelle fest, aus der das Gerät die IP-Adresse anzufragender DNS-Server bezieht.

Mögliche Werte:

- `user`
  Das Gerät verwendet die in der Tabelle festgelegten IP-Adressen.
- `mgmt-dhcp` (Voreinstellung)
  Das Gerät verwendet die IP-Adressen, die der DHCP-Server dem Gerät übergibt.

Domänen-Name

Legt den Domain-Namen gemäß RFC 1034 fest, den das Gerät an Hostnamen ohne Domain-Suffix anfügt.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Request-Timeout [s]

Legt den Zeitabstand in Sekunden für das erneute Senden einer Anfrage an den Server fest.

Mögliche Werte:

- `0`
  Deaktiviert die Funktion. Das Gerät sendet keine erneute Anfrage an den Server.
- `1..3600` (Voreinstellung: `3`)

Request-Wiederholungen

Legt fest, wie viele Male das Gerät das Senden einer Anfrage wiederholt.

Voraussetzung ist, dass Sie im Feld *Request-Timeout [s]* einen Wert >`0`festlegen.

Mögliche Werte:

- `0..100` (Voreinstellung: `2`)

Tabelle

Index

Zeigt die fortlaufende Nummer des DNS-Servers.

Das Gerät ermöglicht Ihnen, bis zu 4 DNS-Server festzulegen.

Adresse

Legt die IP-Adresse des DNS-Servers fest.

Mögliche Werte:

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

Aktiv

Aktiviert/deaktiviert den Tabelleneintrag.

Das Gerät sendet Anfragen an den im ersten aktiven Tabelleneintrag konfigurierten DNS-Server. Erhält das Gerät von diesem Server keine Antwort, sendet es Anfragen an den im nächsten aktiven Tabelleneintrag konfigurierten DNS-Server.

Mögliche Werte:

- `markiert`
  Der DNS-Client sendet Anfragen an diesen DNS-Server.
  Voraussetzungen:
  - ☐ Schalten Sie im Dialog *Erweitert > DNS > Global* die DNS-Client-Funktion ein.
  - ☐ Legen Sie im Rahmen *Konfiguration*, Dropdown-Liste *Konfigurationsquelle* den Wert `user` fest.
- `unmarkiert` (Voreinstellung)
  Das Gerät sendet keine Anfragen an diesen DNS-Server.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

7.3.1.4 DNS-Client Statische Hosts

[Erweitert > DNS > Client > Statische Hosts]

Dieser Dialog ermöglicht Ihnen, bis zu 64 Hostnamen festzulegen, die mit jeweils einer IP-Adresse verknüpft sind. Bei Anfragen zur Auflösung von Hostnamen in IP-Adressen sucht das Gerät in dieser Tabelle nach einem passenden Eintrag. Findet das Gerät keinen passenden Eintrag, leitet es die Anfrage weiter.

Tabelle

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Mögliche Werte:

- `1..64`

Name

Legt den Host-Namen fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

IP-Adresse

Legt die IP-Adresse fest, mit der der Host erreichbar ist.

Mögliche Werte:

- Gültige IPv4-Adresse

Aktiv

Aktiviert/deaktiviert den Tabelleneintrag.

Mögliche Werte:

- `markiert`
  Das Gerät löst eine Anfrage nach dem Host-Namen für diesen Eintrag auf.
- `unmarkiert`
  Nachdem das Gerät eine Anforderung für diesen Host-Namen empfangen hat, sendet es eine Anforderung zur Auflösung an einen der konfigurierten Namens-Server.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

7.4 Industrie-Protokolle

[Erweitert > Industrie-Protokolle]

Das Menü enthält die folgenden Dialoge:

- IEC61850-MMS
- Modbus TCP
- EtherNet/IP

7.4.1 IEC61850-MMS

[Erweitert > Industrie-Protokolle > IEC61850-MMS]

IEC61850 MMS ist ein von der International Electrotechnical Commission (IEC) standardisiertes industrielles Kommunikationsprotokoll. Switches verwenden beispielsweise dieses Protokoll, wenn sie mit Anlagenkomponenten kommunizieren.

Das Paket-orientierte Protokoll definiert eine einheitliche Kommunikationssprache auf Grundlage des Transport-Protokolls TCP/IP. Das Protokoll verwendet einen Manufacturing-Message-Specification(MMS)-Server für die Kommunikation der Client-Server. Das Protokoll beinhaltet Funktionen für SCADA, Intelligent Electronic Device (IED) und die Netzüberwachungssysteme.

Anmerkung: IEC61850/MMS bietet keine Authentifizierungsmechanismen. Wenn der Schreibzugriff für IEC61850/MMS eingeschaltet ist, dann ist jeder Client, der das Gerät per TCP/IP erreicht, in der Lage, die Einstellungen des Geräts ändern. Dies wiederum führt möglicherweise zur Fehlkonfiguration des Geräts und zu möglichen Problemen im Netz.

Schalten Sie den Schreibzugriff ausschließlich dann ein, wenn Sie zusätzliche Maßnahmen (zum Beispiel Firewall, VPN etc.) getroffen haben, um die Möglichkeit eines unbefugten Zugriffs zu verringern.

Dieser Dialog ermöglicht Ihnen, folgende Server-Einstellungen für MMS festzulegen:
- Aktiviert/deaktiviert den MMS-Server.
- Aktiviert/deaktiviert den Schreibzugriff auf den MMS-Server
- TCP-Port des MMS-Servers.
- Die maximale Anzahl an MMS-Server-Sitzungen.

Funktion

Funktion

Schaltet den *IEC61850-MMS*-Server ein/aus.

Mögliche Werte:

- *An*
  Der *IEC61850-MMS*-Server ist eingeschaltet.
- *Aus* (Voreinstellung)
  Der *IEC61850-MMS*-Server ist ausgeschaltet.
  Die IEC61850 MIBs bleiben zugänglich.

Konfiguration

Schreibzugriff

Aktiviert/deaktiviert den Schreibzugriff auf den MMS-Server

Mögliche Werte:

- `markiert`
  Der Schreibzugriff auf den MMS-Server ist aktiviert. Diese Einstellung ermöglicht Ihnen, die Geräte-Einstellungen über das Protokoll IEC 61850 MMS zu ändern.
- `unmarkiert` (Voreinstellung)
  Der Schreibzugriff auf den MMS-Server ist deaktiviert. Der MMS-Server ist mit Lese-Zugriff erreichbar.

Technical-Key

Legt den IED-Namen fest.

Der IED-Name ist unabhängig vom System-Namen einstellbar.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen
  Die folgenden Zeichen sind zulässig:
  - _
  - `_`
  - `0..9`
  - `a..z`
  - `A..Z` (Voreinstellung: `KEY`)

Damit der MMS-Server den IED-Namen verwendet, klicken Sie die Schaltfläche ☑ und starten Sie den MMS-Server neu. Dabei bricht die Verbindung zu verbundenen Clients ab.

TCP-Port

Legt den TCP-Port für den Zugriff auf den MMS-Server fest.

Mögliche Werte:

- `1..65535` (Voreinstellung: `102`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Anmerkung: Nachdem Sie den Port geändert haben, startet der Server automatisch neu. Offene Verbindungen zum Server beendet das Gerät dabei.

Sitzungen (max.)

Legt die maximale Anzahl an MMS-Server-Verbindungen fest.

Mögliche Werte:

- `1..15` (Voreinstellung: `5`)

Information

Status

Zeigt den gegenwärtigen Status des *IEC61850-MMS*-Servers.

Mögliche Werte:

- *unavailable*
- *starting*
- *running*
- *stopping*
- *halted*
- *error*

Aktive Verbindungen

Zeigt die Anzahl der aktiven MMS-Server-Verbindungen.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

ICD-Datei herunterladen

Kopiert die ICD-Datei auf Ihren PC.

7.4.2 Modbus TCP

[Erweitert > Industrie-Protokolle > Modbus TCP]

Modbus TCP ist ein Protokoll für die SCADA-Systemintegration (Supervisory Control and Data Acquisition). *Modbus TCP* ist ein herstellerunabhängiges Protokoll, das für die Überwachung und Steuerung von Automatisierungstechnik im Industriebereich eingesetzt wird, zum Beispiel für speicherprogrammierbare Steuerungen (SPS), Sensoren und Messgeräte.

Dieser Dialog ermöglicht Ihnen, die Parameter des Protokolls festzulegen. Um die Parameter des Geräts zu überwachen und zu steuern, benötigen Sie Mensch-Maschine-Schnittstellen(HMI)-Software sowie die Speicherzuordnungstabelle. Die unterstützten Objekte und die Speicherzuordnung finden Sie in den Tabellen im Anwender-Handbuch „Konfiguration“.

Der Dialog ermöglicht Ihnen, die Funktion sowie den Schreibzugriff zu aktivieren und zu steuern, welchen TCP-Port die Mensch-Maschine-Schnittstelle (Human Machine Interface, HMI) nach Daten abfragt. Darüber hinaus können Sie in diesem Dialog die Anzahl der Sitzungen festlegen, die zeitgleich geöffnet sein dürfen.

Anmerkung: Das Aktivieren des *Modbus TCP*-Schreibzugriffs stellt möglicherweise ein unvermeidbares Sicherheitsrisiko dar, da das Protokoll keine Benutzerzugriffe authentifiziert.

Um das unvermeidbare Sicherheitsrisiko zu verringern, legen Sie im Dialog *Gerätesicherheit* > Management-Zugriff den IP-Adressbereich fest. Bevor Sie die Funktion einschalten, geben Sie ausschließlich die IP-Adressen ein, die Ihren Geräten zugewiesen sind. Darüber hinaus ist die Voreinstellung für das Aktivieren der Überwachungsfunktion im Dialog *Diagnose* > Statuskonfiguration > *Sicherheitsstatus*, Registerkarte *Global* aktiv.

Funktion

Funktion

Schaltet den *Modbus TCP*-Server im Gerät ein/aus.

Mögliche Werte:

- *An*
  Der *Modbus TCP*-Server ist eingeschaltet.
- *Aus* (Voreinstellung)
  Der *Modbus TCP*-Server ist ausgeschaltet.

Konfiguration

Schreibzugriff

Aktiviert/deaktiviert den Schreibzugriff auf die *Modbus TCP* parameter.

Anmerkung: Das Aktivieren des *Modbus TCP*-Schreibzugriffs stellt möglicherweise ein unvermeidbares Sicherheitsrisiko dar, da das Protokoll keine Benutzerzugriffe authentifiziert.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Der Lese-/Schreibzugriff für den *Modbus TCP*-Server ist aktiv. Dies ermöglicht Ihnen, die Geräte-Konfiguration über das *Modbus TCP*-Protokoll zu ändern.
- `unmarkiert`
  Der Lesezugriff für den *Modbus TCP*-Server ist aktiv.

TCP-Port

Legt die TCP-Port-Nummer fest, die der *Modbus TCP*-Server für die Kommunikation verwendet.

Mögliche Werte:

- `<TCP-Port-Nummer>` (Voreinstellung: `502`)
  Das Festlegen von `0` ist unzulässig.

Sitzungen (max.)

Legt die maximale Anzahl von gleichzeitigen Sitzungen fest, die der *Modbus TCP*-Server aufrechterhält.

Mögliche Werte:

- `1..5` (Voreinstellung: `5`)

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

7.4.3 EtherNet/IP

[Erweitert > Industrie-Protokolle > EtherNet/IP]

Dieser Dialog ermöglicht Ihnen, die *EtherNet/IP*-Einstellungen festzulegen. Sie haben die folgenden Möglichkeiten:

- Die Funktion *EtherNet/IP* im Gerät ein-/ausschalten.
- Ein VLAN festlegen, das ausschließlich die *EtherNet/IP*-Pakete weiterleitet.
- Die Lese-/Schreibfähigkeit des Protokolls *EtherNet/IP* aktivieren/deaktivieren.
- Das Elektronische Datenblatt (EDS) vom Gerät herunterladen.

Funktion

Funktion

Schaltet die Funktion *EtherNet/IP* im Gerät ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *EtherNet/IP* ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *EtherNet/IP* ist ausgeschaltet.

VLAN Konfiguration

Vorteile durch Einrichten eines VLANs:

- Reduziertes Fluten der *EtherNet/IP*-Pakete. Das Gerät leitet die *EtherNet/IP*-Pakete im von Ihnen zugewiesenen VLAN weiter.
- Verbesserte Sicherheit und Datenschutz im Netz.

VLAN-ID

Legt ein VLAN fest, in welchem das Gerät die *EtherNet/IP*-Pakete weiterleitet.

Mögliche Werte:

- `mgmt` (Voreinstellung)
  Das Gerät leitet die *EtherNet/IP*-Pakete in dem VLAN weiter, in welchem das Management des Geräts über das Netz erreichbar ist. Dieses VLAN legen Sie fest im Dialog *Grundeinstellungen > Netz > Global*, Feld *VLAN-ID* im Rahmen *Management-Schnittstelle*.
- `1..4042`
  Wählen Sie in der Dropdown-Liste einen Eintrag. Das Gerät leitet die *EtherNet/IP* Pakete in diesem VLAN weiter.
  Voraussetzungen:
  - Das VLAN ist im Gerät bereits eingerichtet.
    Siehe Dialog *Switching > VLAN > Konfiguration*.
  - Der Port, über den das Gerät die *EtherNet/IP*-Pakete weiterleitet, ist Mitglied des von Ihnen zugewiesenen VLANs und vermittelt die Datenpakete mit VLAN-Tag.
    Siehe Dialog *Switching > VLAN > Konfiguration*.
  - Die Funktion *IP-Zugriffsbeschränkung* ist eingeschaltet.
    Siehe Dialog *Gerätesicherheit > Management-Zugriff > IP-Zugriffsbeschränkung*.

Konfiguration

Schreibzugriff

Aktiviert/deaktiviert den Lese-/Schreibzugriff des Protokolls *EtherNet/IP*.

Mögliche Werte:

- `markiert`
  Das Protokoll *EtherNet/IP* akzeptiert GET- und SET-Requests.
- `unmarkiert` (Voreinstellung)
  Das Protokoll *EtherNet/IP* akzeptiert ausschließlich GET-Requests.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

EDS-Datei herunterladen

Kopiert die folgenden Informationen in eine Zip-Datei auf Ihren PC:

- Elektronisches Datenblatt (EDS) mit gerätebezogenen Informationen
- Gerätsymbol

7.5 Digital-IO Modul

[Erweitert > Digital-IO Modul]

Die digitalen Eingänge bieten Ihnen die Möglichkeit, Signale von digitalen Sensoren zu erfassen und weiterzuleiten. Die digitalen Ausgänge bieten Ihnen die Möglichkeit, das von den Eingängen übermittelte Signal auf die Aktoren anzuwenden. Die Ausgangsspannung von 24 VDC ermöglicht Ihnen den Betrieb von Aktoren, wie beispielsweise Kontrollleuchten.

Das Gerät überträgt Sensor-Signale in das gesamte Netz und aktiviert auf diese Weise die entsprechenden Aktoren. Über die Eingangsanschlüsse erfasst das Modul die Signale und leitet sie an die Ausgänge weiter. Abhängig von der Position der Aktoren leitet das Gerät die Signale an Ausgänge weiter, die entweder auf demselben Modul, auf einem anderen Moduls desselben Geräts oder auf einem anderen Gerät installiert sind.

Bildet das Gerät die digitalen Eingänge auf die digitalen Ausgänge ab, besteht eine 1:N-Beziehung. Das Gerät spiegelt den Datenstrom eines digitalen Eingangs an eine beliebige Anzahl von digitalen Ausgängen.

Bildet das Gerät die digitalen Ausgänge auf die digitalen Eingänge ab, besteht eine 1:1-Beziehung. Ein digitaler Ausgang spiegelt den Datenstrom eines digitalen Eingangs.

Der Dialog enthält die folgenden Registerkarten:
- [IO-Eingang]

[IO-Eingang]

Diese Registerkarte bietet Ihnen folgende Möglichkeiten:
- die Abfrage der digitalen Eingänge global aktivieren oder deaktivieren
- den Zeitabstand konfigurieren, in dem das Gerät die Werte der digitalen Eingänge abfragt
- die Protokollierung von Ereignissen aktivieren oder deaktivieren
- das Senden von SNMP-Traps aktivieren oder deaktivieren

Funktion

Funktion

Schaltet die zyklische Abfrage der digitalen Eingänge ein oder aus.

Mögliche Werte:
- *An*
  Ermöglicht das Abfragen der Eingangswerte.
- *Aus* (Voreinstellung)

Konfiguration

Aktualisierungs-Intervall [ms]

Legt den Zeitabstand in Millisekunden fest, in dem das Gerät die Werte der digitalen Eingänge abfragt.

Mögliche Werte:

- `1000..10000` (Voreinstellung: `1000`)

Tabelle

Input-ID

Zeigt die Steckplatznummer des Moduls (x) und die Nummer des digitalen Eingangs (o), für den dieser Eintrag gilt.

Schreibweise: `x.i`

Mögliche Werte:

- x =`0..7`
  Der Wert `0` entspricht der Haupteinheit (MU).
- i =`1..4`

Wert

Legt den digitalen Eingangspegel fest.

Mögliche Werte:

- `low`
  Die Eingangsspannung am digitalen Eingang beträgt 0 V.
- `high`
  Die Eingangsspannung am digitalen Eingang beträgt +24 VDC.
- `not-available`
  Die Eingangsspannung am digitalen Eingang hat einen anderen Wert als 0 V oder +24 VDC. Vergewissern Sie sich, dass das Modul vorhanden und ordnungsgemäß befestigt ist.

Ereignis protokollieren

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

Mögliche Werte:

- `markiert`
  Die Protokollierung ist aktiviert.
  Das Gerät prüft den Status der digitalen Eingänge im Intervall, das im Rahmen *Konfiguration*, Feld *Aktualisierungs-Intervall [ms]* festgelegt ist.
  Treten Änderungen an den digitalen Eingängen auf, protokolliert das Gerät ein Ereignis in der Log-Datei (System Log).
- `unmarkiert` (Voreinstellung)
  Die Protokollierung ist deaktiviert.

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung an den digitalen Eingängen erkennt.

Das Gerät prüft den Status der digitalen Eingänge im Intervall, das im Rahmen *Konfiguration*, Feld *Aktualisierungs-Intervall [ms]* festgelegt ist.

Mögliche Werte:

- `markiert`
  Das Senden von SNMP-Traps ist aktiv.
  Das Gerät sendet einen SNMP-Trap, wenn es Änderungen an den digitalen Eingängen erkennt.
- `unmarkiert` (Voreinstellung)
  Das Senden von SNMP-Traps ist inaktiv.

Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog *Diagnose* > Statuskonfiguration > *Alarme (Traps)* einschalten und mindestens ein Trap-Ziel festlegen.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

7.6 Command Line Interface

[Erweitert > CLI]

Dieser Dialog ermöglicht Ihnen, mit dem Command Line Interface auf das Gerät zuzugreifen.

Die Voraussetzungen sind:
- ☐ Schalten Sie im Gerät den SSH-Server ein, siehe Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH*.
- ☐ Installieren Sie auf Ihrer Workstation eine SSH-fähige Client-Anwendung, die in Ihrem Betriebssystem einen Handler für URLs registriert, die mit `ssh://` beginnen.

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen” auf Seite 17.

SSH-Verbindung starten

Öffnet die SSH-fähige Client-Anwendung.

Wenn Sie die Schaltfläche klicken, übergibt die Web-Anwendung den URL des Geräts beginnend mit `ssh://` und den Benutzernamen des gegenwärtig angemeldeten Benutzers.

Wenn der Web-Browser eine SSH-fähige Client-Anwendung findet, dann stellt der SSH-fähige Client eine Verbindung mit dem SSH-Protokoll zum Gerät her.

A Index

U

V

W

Z