



HIRSCHMANN

A **BELDEN** BRAND

Hirschmann Automation and Control GmbH

GRS103 HiOS-2A Rel. 09400

Referenz-Handbuch

Grafische Benutzeroberfläche

Anwender-Handbuch

Konfiguration



HIRSCHMANN

A **BELDEN** BRAND

Referenz-Handbuch

Grafische Benutzeroberfläche
GREYHOUND Switch GRS103
HiOS-2A

Die Nennung von geschützten Warenzeichen in diesem Handbuch berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

© 2023 Hirschmann Automation and Control GmbH

Handbücher sowie Software sind urheberrechtlich geschützt. Alle Rechte bleiben vorbehalten. Das Kopieren, Vervielfältigen, Übersetzen, Umsetzen in irgendein elektronisches Medium oder maschinell lesbare Form im Ganzen oder in Teilen ist nicht gestattet. Eine Ausnahme gilt für die Anfertigungen einer Sicherungskopie der Software für den eigenen Gebrauch zu Sicherungszwecken.

Die beschriebenen Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart wurden. Diese Druckschrift wurde von Hirschmann Automation and Control GmbH nach bestem Wissen erstellt. Hirschmann behält sich das Recht vor, den Inhalt dieser Druckschrift ohne Ankündigung zu ändern. Hirschmann gibt keine Garantie oder Gewährleistung hinsichtlich der Richtigkeit oder Genauigkeit der Angaben in dieser Druckschrift.

Hirschmann haftet in keinem Fall für irgendwelche Schäden, die in irgendeinem Zusammenhang mit der Nutzung der Netzkomponenten oder ihrer Betriebssoftware entstehen. Im Übrigen verweisen wir auf die im Lizenzvertrag genannten Nutzungsbedingungen.

Die aktuelle Benutzerdokumentation für Ihr Gerät finden Sie unter: doc.hirschmann.com

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Deutschland

Inhalt

	Sicherheitshinweise	7
	Über dieses Handbuch	9
	Legende	10
	Hinweise zur grafischen Benutzeroberfläche	11
	Banner	11
	Menübereich	13
	Dialogbereich	15
1	Grundeinstellungen	19
1.1	System	19
1.2	Module	24
1.3	Netz	26
1.3.1	Global	27
1.3.2	IPv4	29
1.3.3	IPv6	32
1.4	Out-of-Band via USB	35
1.5	Software	38
1.6	Laden/Speichern	41
1.7	Externer Speicher	54
1.8	Port	57
1.9	Power over Ethernet	63
1.9.1	PoE Global	65
1.9.2	PoE Port	67
1.10	Neustart	70
2	Zeit	73
2.1	Grundeinstellungen	73
2.2	SNTP	77
2.2.1	SNTP Client	78
2.2.2	SNTP Server	82
3	Gerätesicherheit	85
3.1	Benutzerverwaltung	85
3.2	Authentifizierungs-Liste	91
3.3	LDAP	94
3.3.1	LDAP Konfiguration	95
3.3.2	LDAP Rollen-Zuweisung	101
3.4	Management-Zugriff	103
3.4.1	Server	104
3.4.2	IP-Zugriffsbeschränkung	117
3.4.3	Web	120
3.4.4	Command Line Interface	121
3.4.5	SNMPv1/v2 Community	123
3.5	Pre-Login-Banner	125

4	Netzicherheit	127
4.1	Netzicherheit Übersicht	127
4.2	Port-Sicherheit	129
4.3	802.1X	134
4.3.1	802.1X Global	135
4.3.2	802.1X Port-Konfiguration	137
4.3.3	802.1X Port-Clients	143
4.3.4	802.1X EAPOL-Portstatistiken	145
4.3.5	802.1X Verlauf Port-Authentifizierung	147
4.3.6	802.1X Integrierter Authentifikations-Server (IAS)	149
4.4	RADIUS	150
4.4.1	RADIUS Global	151
4.4.2	RADIUS Authentication-Server	153
4.4.3	RADIUS Accounting-Server	155
4.4.4	RADIUS Authentication Statistiken	157
4.4.5	RADIUS Accounting-Statistiken	159
4.5	DoS	160
4.5.1	DoS Global	161
4.6	ACL	164
4.6.1	ACL IPv4-Regel	165
4.6.2	ACL MAC-Regel	169
4.6.3	ACL Zuweisung	172
5	Switching	175
5.1	Switching Global	175
5.2	Lastbegrenzer	178
5.3	Filter für MAC-Adressen	181
5.4	IGMP-Snooping	183
5.4.1	IGMP-Snooping Global	184
5.4.2	IGMP-Snooping Konfiguration	186
5.4.3	IGMP-Snooping Erweiterungen	190
5.4.4	IGMP Snooping-Querier	193
5.4.5	IGMP Snooping Multicasts	196
5.5	MRP-IEEE	197
5.5.1	MRP-IEEE Konfiguration	198
5.5.2	MRP-IEEE Multiple MAC Registration Protocol	199
5.5.3	MRP-IEEE Multiple VLAN Registration Protocol	204
5.6	GARP	207
5.6.1	GMRP	208
5.6.2	GVRP	210
5.7	QoS/Priority	211
5.7.1	QoS/Priority Global	212
5.7.2	QoS/Priorität Port-Konfiguration	213
5.7.3	802.1D/p Zuweisung	215
5.7.4	IP-DSCP-Zuweisung	216
5.7.5	Queue-Management	218
5.8	VLAN	219

5.8.1	VLAN Global	220
5.8.2	VLAN Konfiguration	221
5.8.3	VLAN Port	224
5.8.4	VLAN Voice	226
5.9	L2-Redundanz	229
5.9.1	MRP	230
5.9.2	Spanning Tree	233
5.9.2.1	Spanning Tree Global	234
5.9.2.2	Spanning Tree Port	240
5.9.3	Link-Aggregation	248
5.9.4	Link-Backup	255
5.9.5	FuseNet	258
5.9.5.1	Sub-Ring	259
6	Diagnose	265
6.1	Statuskonfiguration	265
6.1.1	Gerätestatus	266
6.1.2	Sicherheitsstatus	271
6.1.3	Signalkontakt	277
6.1.3.1	Signalkontakt 1 / Signalkontakt 2	278
6.1.4	MAC-Benachrichtigung	283
6.1.5	Alarmer (Traps)	285
6.1.5.1	Trap V3 Benutzerverwaltung	286
6.1.5.2	Trap Ziele	289
6.2	System	291
6.2.1	Systeminformationen	292
6.2.2	Hardware-Zustand	293
6.2.3	Konfigurations-Check	294
6.2.4	IP-Adressen Konflikterkennung	296
6.2.5	ARP	300
6.2.6	Selbsttest	302
6.3	E-Mail-Benachrichtigung	304
6.3.1	E-Mail-Benachrichtigung Global	305
6.3.2	E-Mail-Benachrichtigung Empfänger	310
6.3.3	E-Mail-Benachrichtigung Mail-Server	312
6.4	Syslog	314
6.5	Ports	318
6.5.1	SFP	319
6.5.2	TP-Kabeldiagnose	320
6.5.3	Port-Monitor	322
6.5.4	Auto-Disable	332
6.5.5	Port-Mirroring	336
6.6	LLDP	339
6.6.1	LLDP Konfiguration	340
6.6.2	LLDP Topologie-Erkennung	344
6.7	Loop-Schutz	348
6.8	Bericht	352

6.8.1	Bericht Global	353
6.8.2	Persistentes Ereignisprotokoll	358
6.8.3	System-Log	361
6.8.4	Audit-Trail.	362
7	Erweitert	363
7.1	DHCP-L2-Relay	363
7.1.1	DHCP-L2-Relay Konfiguration	364
7.1.2	DHCP-L2-Relay Statistiken	367
7.2	DHCP Server	368
7.2.1	DHCP-Server Global	369
7.2.2	DHCP-Server Pool	371
7.2.3	DHCP-Server Lease-Tabelle	376
7.3	DNS	377
7.3.1	DNS-Client	377
7.3.1.1	DNS-Client Global	378
7.3.1.2	DNS-Client Aktuell	379
7.3.1.3	DNS-Client Statisch	380
7.3.1.4	DNS-Client Statische Hosts	383
7.4	Industrie-Protokolle	384
7.4.1	IEC61850-MMS	385
7.4.2	Modbus TCP	388
7.4.3	OPC UA Server	390
7.5	Tracking	393
7.5.1	Tracking Konfiguration	394
7.5.2	Tracking Applikationen.	398
7.6	Command Line Interface	399
A	Stichwortverzeichnis	401
B	Weitere Unterstützung.	407
C	Leserkritik.	408

Sicherheitshinweise

WARNUNG

UNKONTROLLIERTE MASCHINENBEWEGUNGEN

Um unkontrollierte Maschinenbewegungen aufgrund von Datenverlust zu vermeiden, konfigurieren Sie alle Geräte zur Datenübertragung individuell.

Nehmen Sie eine Maschine, die mittels Datenübertragung gesteuert wird, erst in Betrieb, wenn Sie alle Geräte zur Datenübertragung vollständig konfiguriert haben.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Über dieses Handbuch

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 Industrial HiVision 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.
<i>Courier</i>	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

Voraussetzung für den Zugriff auf die grafische Benutzeroberfläche des Geräts ist ein Webbrowser mit HTML5-Unterstützung.

Die responsive grafische Benutzeroberfläche passt sich automatisch an die Größe Ihres Bildschirms an. Demzufolge können Sie auf einem großen, hochauflösenden Bildschirm mehr Details sehen als auf einem kleinen Bildschirm. Auf einem hochauflösenden Bildschirm haben die Schaltflächen zum Beispiel eine Beschriftung neben dem Symbol. Auf einem Bildschirm mit geringer Breite zeigt die grafische Benutzeroberfläche lediglich das Symbol.

Anmerkung: Auf einem konventionellen Bildschirm klicken Sie, um zu navigieren. Auf einem Gerät mit Touchscreen hingegen tippen Sie. Der Einfachheit halber verwenden wir in unseren Hilfetexten lediglich „Klicken“.

Die grafische Benutzeroberfläche ist wie folgt unterteilt:

- [Banner](#)
- [Menübereich](#)
- [Dialogbereich](#)

Banner

Das Banner zeigt die folgenden Informationen:



Blendet das Menü ein und wieder aus. Die grafische Benutzeroberfläche blendet den Menübereich aus, wenn das Fenster des Webbrowsers zu schmal ist. Das Banner zeigt stattdessen die Schaltfläche.

Hersteller-Logo

Klicken Sie das Logo, um die Website des Herstellers des Geräts in einem neuen Fenster zu öffnen.

Name des Dialogs

Zeigt den Namen des gegenwärtig im Dialogbereich angezeigten Dialogs.



Zeigt, dass der Webbrowser das Gerät nicht erreichen kann. Die Verbindung zum Gerät ist unterbrochen.



Zeigt, ob die Einstellungen im flüchtigen Speicher (*RAM*) von den Einstellungen des „ausgewählten“ Konfigurationsprofils im permanenten Speicher (*NVM*) abweichen. Das Banner zeigt das Symbol, sobald Sie die Einstellungen angewendet, diese jedoch noch nicht im permanenten Speicher (*NVM*) gespeichert haben.



Wenn Sie die Schaltfläche klicken, öffnet sich die Online-Hilfe in einem neuen Fenster.



Wenn Sie die Schaltfläche klicken, zeigt ein Tooltip die folgenden Informationen:

- Die Zusammenfassung des Rahmens *Geräte-Status*. Siehe Dialog *Grundeinstellungen > System*.
- Die Zusammenfassung des Rahmens *Sicherheits-Status*. Siehe Dialog *Grundeinstellungen > System*.


Ein roter Punkt neben dem Symbol bedeutet, dass mindestens einer der Werte größer ist als 0.



Wenn Sie die Schaltfläche klicken, öffnet sich ein Untermenü mit den folgenden Menüeinträgen:

- Name des Benutzerkontos
Kontoname des Benutzers, der gegenwärtig angemeldet ist.
- Schaltfläche *Abmelden*
Wenn Sie die Schaltfläche klicken, meldet dies den gegenwärtig angemeldeten Benutzer ab.
Danach öffnet sich der Login-Dialog.

Menübereich

Die grafische Benutzeroberfläche blendet den Menübereich aus, wenn das Fenster des Webbrowsers zu schmal ist. Um den Menübereich anzuzeigen, klicken Sie im Banner die Schaltfläche .

Der Menübereich ist wie folgt unterteilt:

- [Symbolleiste](#)
- [Menübaum](#)

Symbolleiste

Die Symbolleiste zeigt die folgenden Informationen:


Geräte-Software

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



Zeigt ein Textfeld, um nach einem Schlüsselwort zu suchen. Wenn Sie ein Zeichen oder eine Zeichenkette eingeben, zeigt der Menübaum ausschließlich für diejenigen Dialoge einen Menüeintrag an, die mit diesem Schlüsselwort in Zusammenhang stehen.



Der Menübaum zeigt ausschließlich für diejenigen Dialoge einen Menüeintrag an, in denen mindestens ein Parameter von der Voreinstellung abweicht (*Mit [Werkseinstellung vergleichen](#)*). Um den kompletten Menübaum wieder anzuzeigen, klicken Sie die Schaltfläche .



Klappt den Menübaum zu. Der Menübaum zeigt dann ausschließlich Menüeinträge der ersten Ebene.



Klappt den Menübaum auf. Der Menübaum zeigt dann jeden Menüeintrag auf jeder Ebene.

Menübaum

Der Menübaum enthält einen Eintrag für jeden Dialog in der grafischen Benutzeroberfläche. Wenn Sie einen Menüeintrag klicken, zeigt der Dialogbereich den zugehörigen Dialog. Sie können die Ansicht des Menübaums ändern, indem Sie die Schaltflächen in der Symbolleiste am oberen Rand klicken. Des Weiteren können Sie die Ansicht des Menübaums ändern, indem Sie die folgenden Schaltflächen klicken:



Klappt den aktuellen Menüeintrag auf und zeigt die Menüeinträge der nächsttieferen Ebene. Der Menübaum zeigt die Schaltfläche neben jedem zugeklappten Menüeintrag an, der Menüeinträge auf der nächsttieferen Ebene enthält.



Klappt den Menüeintrag zu und blendet die Menüeinträge der unteren Ebenen aus. Der Menübaum zeigt die Schaltfläche neben jedem aufgeklappten Menüeintrag.

Dialogbereich

Der Dialogbereich zeigt den Dialog, den Sie im Menübaum auswählen, einschließlich seiner Bedienelemente. Hier können Sie abhängig von Ihrer Zugriffsrolle die Einstellungen des Geräts überwachen und ändern.

Nachfolgend finden Sie nützliche Informationen zur Bedienung der Dialoge.

- [Bedienelemente](#)
- [Änderungsmarkierung](#)
- [Standard-Schaltflächen](#)
- [Einstellungen speichern](#)
- [Anzeige aktualisieren](#)
- [Arbeiten mit Tabellen](#)

Bedienelemente

Die Dialoge enthalten unterschiedliche Bedienelemente. Diese Bedienelemente sind abhängig vom Parameter und von Ihrer Zugriffsrolle als Benutzer schreibgeschützt oder editierbar.

Die Bedienelemente haben folgende visuelle Eigenschaften:

- Eingabefelder
 - Ein editierbares Eingabefeld hat am unteren Rand eine Linie.
 - Ein schreibgeschütztes Eingabefeld hat keine speziellen visuellen Eigenschaften.
- Kontrollkästchen
 - Ein editierbares Kontrollkästchen hat eine kräftige Farbe.
 - Ein schreibgeschütztes Kontrollkästchen hat eine graue Farbe.
- Optionsfelder
 - Ein editierbares Optionsfeld hat eine kräftige Farbe.
 - Ein schreibgeschütztes Optionsfeld hat eine graue Farbe.

Änderungsmarkierung

Wenn Sie einen Wert ändern, zeigt das betreffende Feld oder die Tabellenzelle ein rotes Dreieck in der linken oberen Ecke. Das rote Dreieck signalisiert, dass Sie die Änderung noch nicht angewendet haben. Die geänderten Einstellungen sind noch nicht wirksam.

Standard-Schaltflächen

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



Wendet die von Ihnen geänderten Einstellungen im Gerät an.

Informationen darüber, wie das Gerät die geänderten Einstellungen auch nach einem Neustart beibehält, finden Sie im Abschnitt „[Einstellungen speichern](#)“ auf Seite 16.



Verwirft nicht gespeicherte Änderungen im gegenwärtigen Dialog. Setzt die Werte in den Feldern auf die im Gerät angewendeten Einstellungen zurück.

Einstellungen speichern

Beim Anwenden der Einstellungen speichert das Gerät die geänderten Einstellungen vorläufig. Führen Sie dazu den folgenden Schritt aus:


Klicken Sie die Schaltfläche  .


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.

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 Kontrollkästchen ganz links in der Tabellenzeile des gewünschten Konfigurationsprofils.

Wenn das Kontrollkästchen in Spalte *Ausgewählt* unmarkiert ist, klicken Sie die Schaltfläche  und dann den Eintrag *Auswählen*.

Klicken Sie die Schaltfläche  , um die gegenwärtigen Änderungen zu speichern.

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.

Arbeiten mit Tabellen

Die Dialoge zeigen zahlreiche Einstellungen in tabellarischer Form. Sie haben die Möglichkeit, das Erscheinungsbild der Tabellen an Ihre Bedürfnisse anzupassen.

In den folgenden Abschnitten finden Sie nützliche Informationen zur Bedienung der Tabellen:

- [Zeilen filtern](#)
- [Zeilen sortieren](#)
- [Mehrere Tabellenzeilen auswählen](#)

Zeilen filtern

Der Filter ermöglicht Ihnen, die Anzahl der angezeigten Tabellenzeilen zu verringern.



Zeigt im Tabellenkopf eine zweite Tabellenzeile, die für jede Spalte ein Textfeld enthält. Wenn Sie in ein Feld eine Zeichenfolge einfügen, zeigt die Tabelle lediglich noch die Tabellenzeilen, welche in der betreffenden Spalte diese Zeichenfolge enthalten.

Zeilen sortieren

Die Reihenfolge der Tabellenzeilen können Sie ändern. Ein Symbol zeigt den Sortierstatus, sobald Sie den Tabellenkopf klicken.



Zeigt, dass die Zeilen der Tabelle anhand eines anderen Kriteriums sortiert sind als anhand der Werte in dieser Spalte.

Klicken Sie das Symbol, um die Zeilen der Tabelle anhand der Einträge in der betreffenden Spalte in absteigender Reihenfolge zu sortieren. Die ursprüngliche Sortierung in der Tabelle lässt sich möglicherweise erst nach dem Abmelden und erneuten Anmelden wiederherstellen.



Zeigt, dass die Zeilen der Tabelle anhand der Einträge der betreffenden Spalte in absteigender Reihenfolge sortiert sind.

Klicken Sie das Symbol, um die Zeilen der Tabelle anhand der Einträge in der betreffenden Spalte in aufsteigender Reihenfolge zu sortieren. Die ursprüngliche Sortierung in der Tabelle lässt sich möglicherweise erst nach dem Abmelden und erneuten Anmelden wiederherstellen.



Zeigt, dass die Zeilen der Tabelle anhand der Einträge der betreffenden Spalte in aufsteigender Reihenfolge sortiert sind.

Klicken Sie das Symbol, um die Zeilen der Tabelle anhand der Einträge in der betreffenden Spalte in absteigender Reihenfolge zu sortieren. Die ursprüngliche Sortierung in der Tabelle lässt sich möglicherweise erst nach dem Abmelden und erneuten Anmelden wiederherstellen.

Mehrere Tabellenzeilen auswählen

Sie haben die Möglichkeit, mehrere Tabellenzeilen auf einmal auszuwählen und eine Aktion auf die ausgewählten Tabellenzeilen anzuwenden. Dies ist nützlich, wenn Sie in der Tabelle zum Beispiel mehrere Zeilen gleichzeitig entfernen möchten.

Um in der Tabelle einzelne Zeilen auszuwählen, markieren Sie das Kontrollkästchen ganz links in der gewünschten Tabellenzeile.

Um in der Tabelle jede Zeile auszuwählen, markieren Sie das Kontrollkästchen ganz links im Tabellenkopf.

1 Grundeinstellungen

Das Menü enthält die folgenden Dialoge:

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

1.1 System

[Grundeinstellungen > System]

Dieser Dialog zeigt Informationen zum Betriebszustand des Geräts.

Geräte-Status

Geräte-Status

Zeigt den Geräte-Status und die gegenwärtig vorliegenden Alarme. Wenn mindestens 1 Alarm vorliegt, ist die Hintergrundfarbe rot. Andernfalls ist die Hintergrundfarbe grün.

Die Parameter, die das Gerät überwacht, legen Sie fest im Dialog [Diagnose > Statuskonfiguration > Gerätestatus](#). Das Gerät löst einen Alarm aus, wenn ein überwachter Parameter vom gewünschten Zustand abweicht.

Ein Tooltip zeigt die Ursache der gegenwärtig vorliegenden Alarme und den Zeitpunkt, zu dem das Gerät den Alarm ausgelöst hat. Um den Tooltip anzuzeigen, bewegen Sie den Mauszeiger über das Feld oder tippen Sie darauf. Die Registerkarte [Status](#) im Dialog [Diagnose > Statuskonfiguration > Gerätestatus](#) zeigt eine Übersicht über die Alarme.

Anmerkung: Das Gerät meldet einen Alarm, wenn Sie an ein Gerät, das 2 redundante Netzteile unterstützt, lediglich 1 Netzteil anschließen. Um einen solchen Alarm zu vermeiden, deaktivieren Sie im Dialog [Diagnose > Statuskonfiguration > Gerätestatus](#) das Überwachen fehlender Netzteile.

Sicherheits-Status



Sicherheits-Status

Zeigt den Sicherheits-Status und die gegenwärtig vorliegenden Alarmer. Wenn mindestens 1 Alarm vorliegt, ist die Hintergrundfarbe rot. Andernfalls ist die Hintergrundfarbe grün.

Die Parameter, die das Gerät überwacht, legen Sie fest im Dialog [Diagnose > Statuskonfiguration > Sicherheitsstatus](#). Das Gerät löst einen Alarm aus, wenn ein überwachter Parameter vom gewünschten Zustand abweicht.

Ein Tooltip zeigt die Ursache der gegenwärtig vorliegenden Alarmer und den Zeitpunkt, zu dem das Gerät den Alarm ausgelöst hat. Um den Tooltip anzuzeigen, bewegen Sie den Mauszeiger über das Feld oder tippen Sie darauf. Die Registerkarte [Status](#) im Dialog [Diagnose > Statuskonfiguration > Sicherheitsstatus](#) zeigt eine Übersicht über die Alarmer.

Status Signalkontakt

Das Gerät enthält möglicherweise mehrere Signalkontakte.



Status Signalkontakt

Zeigt den Signalkontakt-Status und die gegenwärtig vorliegenden Alarmer. Wenn mindestens 1 Alarm vorliegt, ist die Hintergrundfarbe rot. Andernfalls ist die Hintergrundfarbe grün.

Die Parameter, die das Gerät überwacht, legen Sie fest im Dialog [Diagnose > Statuskonfiguration > Signalkontakt > Signalkontakt 1](#)/[Diagnose > Statuskonfiguration > Signalkontakt > Signalkontakt 2](#). Das Gerät löst einen Alarm aus, wenn ein überwachter Parameter vom gewünschten Zustand abweicht.

Ein Tooltip zeigt die Ursache der gegenwärtig vorliegenden Alarmer und den Zeitpunkt, zu dem das Gerät den Alarm ausgelöst hat. Um den Tooltip anzuzeigen, bewegen Sie den Mauszeiger über das Feld oder tippen Sie darauf. Die Registerkarte [Status](#) im Dialog [Diagnose > Statuskonfiguration > Signalkontakt > Signalkontakt 1](#)/[Diagnose > Statuskonfiguration > Signalkontakt > Signalkontakt 2](#) zeigt eine Übersicht über die Alarmer.

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
Das Gerät akzeptiert die folgenden Zeichen:

- 0..9
 - a..z
 - A..Z
 - !#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~
- <Name des Gerätetyps>-<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 Fully Qualified Domain Name (FQDN). Für die Kompatibilität ist es empfehlenswert, nur Kleinbuchstaben zu verwenden, da manche Systeme zwischen Groß- und Kleinschreibung im FQDN unterscheiden. Vergewissern Sie sich, dass dieser Name im gesamten Netz eindeutig ist.

- DHCP-Client
- [Syslog](#)
- [IEC61850-MMS](#)

Standort

Legt den gegenwärtigen oder geplanten Standort 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 Grundgeräts.

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 des 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 Grenzwerte für die Temperatur aktivieren Sie im Dialog [Diagnose > Statuskonfiguration > Gerätestatus](#).

Obere Temp.-Grenze [°C]

Legt den oberen Temperaturschwellwert in °C fest.

Mögliche Werte:

-99 . . 99 (ganze Zahl)

Wenn die Temperatur im Gerät den festgelegten Wert überschreitet, dann zeigt das Gerät einen Alarm.

Untere Temp.-Grenze [°C]

Legt den unteren Temperaturschwellwert in °C fest.

Mögliche Werte:

-99 . . 99 (ganze Zahl)

Wenn die Temperatur im Gerät den festgelegten Wert unterschreitet, dann zeigt das Gerät einen Alarm.

LED-Status

Weitere Informationen zu den Gerätestatus-LEDs finden Sie im Anwender-Handbuch „Installation“.

Status



Gegenwärtig ist kein Alarm vorhanden. Der Gerätestatus ist OK.



Zum Geräte-Status liegt gegenwärtig mindestens 1 Alarm vor. Für Details siehe Rahmen [Geräte-Status](#).

Power



Gerät, das 2 redundante Netzteile unterstützt: Lediglich 1 Versorgungsspannung liegt an.



Gerät, das 1 Netzteil unterstützt: Die Versorgungsspannung liegt an.

Gerät, das 2 redundante Netzteile unterstützt: Beide Versorgungsspannungen liegen an.

ACA



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 Anzeigeaktualisierung. Den Port-Status erkennen Sie an der Markierung.

In der Grundansicht zeigt der Rahmen lediglich Ports mit aktivem Link. Wenn Sie die Schaltfläche



klicken, zeigt der Rahmen sämtliche Ports.

- Neben der Port-Nummer steht die Übertragungsrate des Ports.
- Wenn Sie den Mauszeiger über dem Port-Symbol positionieren oder darauf tippen, zeigt ein Tooltip detaillierte Informationen zum Port-Status.

Grüne Hintergrundfarbe

Port mit aktivem Link.

Graue Hintergrundfarbe

Port mit inaktivem Link.

Gelbe Hintergrundfarbe

Port, an dem das Gerät einen nicht unterstützten SFP-Transceiver oder eine nicht unterstützte Datenrate erkannt hat.

Gestrichelte Umrandung

Port ist aufgrund einer Redundanz-Funktion im Zustand *Blocking*.

1.2 Module

[Grundeinstellungen > Module]

Das Gerät ermöglicht Ihnen, die Module im laufenden Betrieb zu installieren oder zu entfernen (hot-plug).

Solange die Spalte *Status Ethernet-Modul* den Wert *configurable* zeigt, können Sie das Modul konfigurieren und seine Einstellungen speichern.

- Wenn Sie das Modul durch ein baugleiches Modul ersetzen, wendet das Gerät die bisherigen Einstellungen sofort auf das neue Modul an.
- Wenn Sie das Modul durch ein Modul anderen Typs ersetzen, wendet das Gerät die Werkseinstellungen auf das neue Modul an.
- Wenn Sie ein Modul in einen leeren Steckplatz einschieben, konfiguriert das Gerät das Modul mit seinen Voreinstellungen. Wenn der Steckplatz inaktiv ist, bleibt er solange inaktiv, bis Sie das Kontrollkästchen in Spalte *Aktiv* markieren. Nachdem die Voreinstellungen des Ports in das Modul geladen wurden, ist der Zugriff auf das Netz möglich.

Ethernet-Modul installieren

Führen Sie die folgenden Schritte aus:

Stecken Sie das Modul in den Steckplatz.

Das Gerät konfiguriert das Modul automatisch anhand der Voreinstellungen und erkennt die Modul-Parameter.

Um die grafische Benutzeroberfläche zu aktualisieren, klicken Sie die Schaltfläche .

Die Spalte *Status Ethernet-Modul* zeigt für das installierte Ethernet-Modul den Wert *physical*.

Einstellungen vorläufig anwenden. Klicken Sie dazu die Schaltfläche .

Steckplatz aktivieren/deaktivieren

Auf einem inaktiven Steckplatz erkennt das Gerät das installierte Modul und das Konfigurieren der Ports ist möglich. Das Modul stellt auf einem inaktivem Steckplatz keine Verbindungen ins Netz her.

Führen Sie die folgenden Schritte aus:

Wählen Sie die Tabellenzeile des Moduls.

Um den Steckplatz zu deaktivieren und Zugriffe auf das Netz zu unterbinden, heben Sie die Markierung des Kontrollkästchens *Aktiv* auf.

Um den Steckplatz zu aktivieren und Zugriffe auf das Netz zu erlauben, markieren Sie das Kontrollkästchen *Aktiv*.

Einstellungen vorläufig anwenden. Klicken Sie dazu die Schaltfläche .

Ethernet-Modul entfernen

Führen Sie die folgenden Schritte aus:

Entfernen Sie das Modul aus dem Steckplatz.

Um die grafische Benutzeroberfläche zu aktualisieren, klicken Sie die Schaltfläche .

Die Spalte *Status Ethernet-Modul* zeigt für das zuvor entfernte Modul den Wert *configurable*. Wählen Sie die Tabellenzeile des zuvor entfernten Moduls.

Klicken Sie die Schaltfläche .

Die Spalte *Status Ethernet-Modul* zeigt für das zuvor entfernte Modul den Wert *remove*.

Die Spalte *Typ* und einige andere Spalten zeigen den Wert *n/a*.

Das markierte Kontrollkästchen *Aktiv* weist darauf hin, dass der Steckplatz noch aktiv ist.

Einstellungen vorläufig anwenden. Klicken Sie dazu die Schaltfläche .

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Schaltflächen

 Ethernet-Modul entfernen

Entfernt das markierte Ethernet-Modul aus der Tabelle.

Ethernet-Modul

Zeigt die Nummer des Steckplatzes, auf den sich die Tabellenzeile bezieht.

Aktiv

Aktiviert/deaktiviert den Steckplatz.

Mögliche Werte:

`markiert` (Voreinstellung)

Der Steckplatz ist aktiv. Das Gerät erkennt ein in diesem Steckplatz installiertes Modul.

`unmarkiert`

Der Steckplatz ist inaktiv.

Typ

Zeigt den Zustand des installierten Moduls.

Ein Wert von `n/a` weist darauf hin, dass der Steckplatz leer ist.

Beschreibung

Legt eine Kurzbeschreibung für das installierte Modul fest.

Version

Zeigt die Versionsnummer des installierten Moduls.

Ports

Zeigt, wie viele Ports auf dem installierten Modul verfügbar sind.

Seriennummer

Zeigt die Seriennummer des installierten Moduls.

Ein Wert von `n/a` weist darauf hin, dass der Steckplatz leer ist.

Status Ethernet-Modul

Zeigt den Status des Steckplatzes.

Mögliche Werte:

physical

Im Steckplatz ist ein Modul installiert.

configurable

Der Steckplatz ist leer und für die Konfiguration verfügbar.

remove

Der Steckplatz ist leer und inaktiv.

fix

Das Modul kann nicht entfernt werden.

1.3 Netz

[Grundeinstellungen > Netz]

Das Menü enthält die folgenden Dialoge:

Global

IPv4

IPv6

1.3.1 Global

[Grundeinstellungen > Netz > Global]

Dieser Dialog ermöglicht Ihnen, die VLAN- und HiDiscovery-Einstellungen festzulegen, die für den Zugriff über das Netz auf das Management des Geräts erforderlich sind.

Management-Schnittstelle

Dieser Rahmen ermöglicht Ihnen, das VLAN festzulegen, 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 im Dialog [Switching > VLAN > Konfiguration](#) das VLAN bereits eingerichtet ist.

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.

HiDiscovery Protokoll v1/v2

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

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

Anmerkung: Mit der HiDiscovery-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 HiDiscovery im Gerät ein/aus.

Mögliche Werte:

An (Voreinstellung)

Die Funktion HiDiscovery ist eingeschaltet.

Sie haben die Möglichkeit, das Gerät mit der HiDiscovery-Software von Ihrem PC aus zu erreichen.

Aus

Die Funktion HiDiscovery ist ausgeschaltet.

Zugriff

Schaltet den Schreibzugriff auf das Gerät für die Funktion HiDiscovery ein/aus.

Mögliche Werte:

read-write (Voreinstellung)

Die Funktion HiDiscovery hat Schreibzugriff auf das Gerät. Das Gerät ermöglicht Ihnen, mit der Funktion HiDiscovery die IP-Parameter im Gerät zu ändern.

read-only

Die Funktion HiDiscovery hat lediglich Lesezugriff auf das Gerät. Das Gerät ermöglicht Ihnen, mit der Funktion HiDiscovery 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 HiDiscovery-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.

1.3.2 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 > Client > 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.

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

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.

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 Management des Geräts zugewiesen hat.

Um die Anzeige zu aktualisieren, klicken Sie die Schaltfläche .

1.3.3 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 IPv6 können im Gerät parallel betrieben werden. Das wird durch die Verwendung von Dual 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.

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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 finden Sie im Anwender-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.

Manuell

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 noch einige Konfigurationsparameter fehlen.

Anmerkung: Wenn die IPv6-Adresse manuell festgelegt wird, können Sie manuell zwischen Status *aktiv* und Status *notInService* wechseln. Wählen Sie dazu in der Dropdown-Liste in Spalte *Status* den gewünschten Status für die entsprechende Tabellenzeile.

1.4 Out-of-Band via USB

[Grundeinstellungen > Out-of-Band via USB]

Das Gerät verfügt über eine USB-Netzchnittstelle, 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-Netzchnittstelle dennoch Zugriff auf das Management des Geräts.

Das Gerät ermöglicht Ihnen über die USB-Netzchnittstelle 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-Netz Schnittstelle 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-Netz Schnittstelle bei Bedarf auszuschalten.

Funktion

Funktion

Schaltet die USB-Netz Schnittstelle ein/aus.

Mögliche Werte:

An (Voreinstellung)

Das Gerät ermöglicht Ihnen den Zugriff auf das Management des Geräts über die USB-Netz Schnittstelle.

Aus

Das Gerät unterbindet den Zugriff auf das Management des Geräts über die USB-Netz Schnittstelle.

Management-Schnittstelle

Gerät MAC-Adresse

Zeigt die MAC-Adresse der USB-Netz Schnittstelle.

Host MAC-Adresse

Zeigt die MAC-Adresse der angeschlossenen Management-Station.

IP-Parameter

Vergewissern Sie sich, dass das IP-Subnetz dieser Netzchnittstelle 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-Netzchnittstelle erreichbar ist.

Mögliche Werte:

Gültige IPv4-Adresse

(Voreinstellung: 192.168.248.100)

Das Gerät weist diese IP-Adresse, um 1 erhöht, der Management-Station zu, die mit dem Gerät verbunden ist.

Beispiel: 192.168.248.100 für die USB-Netzchnittstelle, 192.168.248.101 für die Management-Station.

Netzmaske

Legt die Netzmaske fest.

Mögliche Werte:

Gültige IPv4-Netzmaske

(Voreinstellung: 255.255.255.0)

1.5 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 Systemstart.

Ausgeführte Version

Zeigt Versionsnummer und Erstellungsdatum der Geräte-Software, die das Gerät beim letzten Systemstart 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.

Beim nächsten Systemstart lädt das Gerät die im Feld [Gespeicherte Version](#) angezeigte Geräte-Software.

Bootcode

Zeigt Versionsnummer und Erstellungsdatum des Bootcodes.

Software-Update


Alternativ dazu 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.

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

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 dazu 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 Systemstart 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 dazu legen Sie vor dem Software-Update im Dialog **Gerätesicherheit > Management-Zugriff > Web**, Feld **Webinterface-Session Timeout [min]** einen ausreichend hohen Wert fest.

Hochladen unsignierter Geräte-Software erlauben

Aktiviert/deaktiviert die Option, dass das Gerät das Hochladen einer unsignierten Gerätesoftware erlaubt. Der Zweck dieser Einstellung ist, das Hochladen einer Geräte-Software zuzulassen, die keine kryptografische Signatur hat.

Mögliche Werte:

markiert

Das Gerät erlaubt das Hochladen einer unsignierten Gerätesoftware.

Das Hochladen einer unsignierten Gerätesoftware kann ein Sicherheitsrisiko darstellen. Wenn Sie dem Urheber vertrauen, können Sie die unsignierte Gerätesoftware hochladen.

unmarkiert (Voreinstellung)

Das Gerät erlaubt ausschließlich das Hochladen einer signierten Gerätesoftware.

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 (ACA21/ACA22)

Index

Zeigt den Index der Geräte-Software.

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

1

Beim nächsten Systemstart lädt das Gerät diese Geräte-Software.

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.

1.6 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.

Anmerkung: Wechsel von Classic zu HiOS? Verwenden Sie unser Online-Tool, um Ihre Dateien mit der Gerätekonfiguration zu konvertieren: <https://convert.hirschmann.com>

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Schaltflächen

 Löschen

Entfernt das in der Tabelle ausgewählte 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

Speichert die vorläufig angewendeten Einstellungen in dem als „ausgewählt“ gekennzeichneten 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 Kontextmenü mit weiteren Funktionen für den betreffenden Dialog.

Speichern unter...

Öffnet das Fenster *Speichern unter...*, um das in der Tabelle ausgewählte Konfigurationsprofil zu kopieren und es mit benutzerdefiniertem Namen im permanenten Speicher (*NVM*) zu speichern.

Geben Sie im Feld *Profilname* den Namen ein, unter dem Sie das Konfigurationsprofil speichern möchten.

Um das Konfigurationsprofil unter einem neuen Namen zu speichern, klicken Sie die Schaltfläche **+**.

Um ein bestehendes Konfigurationsprofil zu überschreiben, wählen Sie in der Dropdown-Liste den zugehörigen Eintrag aus.

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“.

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.

Aktivieren

Lädt die Einstellungen des in der Tabelle ausgewählten 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 ausgewählte Konfigurationsprofil als „ausgewählt“. Anschließend ist in Spalte *Ausgewählt* das Kontrollkästchen *markiert*.

Das Gerät lädt die Einstellungen dieses Konfigurationsprofils beim Systemstart 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 dazu 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 *Speicherort* legen Sie den Speicherort für das Konfigurationsprofil fest. Voraussetzung ist, dass in der Dropdown-Liste *Select source* der Eintrag *PC/URL* ausgewählt ist.

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 Gerät Module verwendet, dann lesen Sie auch den Hilfetext zum Dialog *Grundeinstellungen > Module*.
- 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 ausgewählte 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>`


Running-Config als Skript speichern

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.

Running-Config aus Skript laden

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 dazu 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>`

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*).

Speicherort

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 Systemstart 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:

Wählen Sie die Tabellenzeile des Konfigurationsprofils.

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 im Dialog *Grundeinstellungen > Externer Speicher* das Kontrollkästchen *Sichere Konfiguration beim Speichern* markiert ist.

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. Wählen Sie dazu die Tabellenzeile eines vorhandenen Konfigurationsprofils, klicken die

Schaltfläche  und dann den Eintrag *Speichern unter...*

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...](#)


Letzte Änderung (UTC)

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

Ausgewählt

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


Das Gerät ermöglicht Ihnen, ein anderes Konfigurationsprofil als „ausgewählt“ zu kennzeichnen.

Wählen Sie dazu in der Tabelle das gewünschte Konfigurationsprofil, klicken die Schaltfläche  und dann den Eintrag [Aktivieren](#).

Mögliche Werte:

[markiert](#)

Das Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet.

- Das Gerät lädt die das Konfigurationsprofil beim Systemstart oder beim Anwenden der Funktion [Konfigurationsänderungen rückgängig machen](#) in den flüchtigen Speicher ([RAM](#)).
- Wenn Sie die Schaltfläche  klicken, speichert das Gerät die vorläufig angewendeten Einstellungen in diesem Konfigurationsprofil.

[unmarkiert](#)

Ein anderes Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet.

Verschlüsselung

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.

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.

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.

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.

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
- mit einem kleineren oder demselben Level der Geräte-Software wie HiOS-2A oder HiOS-3S auf einem Gerät, das HiOS-3S ausführt

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

Externer Speicher

Ausgewählter externer Speicher

Zeigt den Typ des externen Speichers.

Mögliche Werte:

`usb`

Externer USB-Speicher (ACA21/ACA22)

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 angeschlossen 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 *erste* 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 Eingeben 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 nächsten Systemstart 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.

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. Die gegenwärtigen Einstellungen, die lediglich zwischengespeichert 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)

Information

NVM synchron mit running-config


Zeigt, ob die Einstellungen im flüchtigen Speicher (*RAM*) von den Einstellungen des „ausgewählten“ Konfigurationsprofils im permanenten Speicher (*NVM*) abweichen.

Mögliche Werte:

markiert

Die Einstellungen stimmen überein.

unmarkiert

Die Einstellungen weichen voneinander ab. Das Banner zeigt zusätzlich das Symbol .

Externer Speicher und NVM synchron

Zeigt, ob die Einstellungen des „ausgewählten“ Konfigurationsprofils im externen Speicher (*ACA*) von den Einstellungen des „ausgewählten“ Konfigurationsprofils im permanenten Speicher (*NVM*) abweichen.

Mögliche Werte:

markiert

Die Einstellungen stimmen überein.

unmarkiert

Die Einstellungen weichen voneinander ab.

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 Eingeben 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

Das Gerät akzeptiert die folgenden Zeichen:

```
a..z  
A..Z  
0..9  
!#$%&'()*+,-./:;<=>@[\\]^_`{|}~
```

1.7 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Typ

Zeigt den Typ des externen Speichers.

Mögliche Werte:

`usb`
Externer USB-Speicher (ACA21/ACA22)

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 angeschlossen und betriebsbereit.
`outOfMemory`
Der Speicherplatz im externen Speicher ist belegt.
`genericErr`
Das Gerät hat einen Fehler erkannt.

Schreibbar

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 Systemstarts.

Mögliche Werte:

`markiert` (Voreinstellung)

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`

Keine automatische Aktualisierung der Geräte-Software während des Systemstarts.

SSH-Key automatisch uploaden

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

Mögliche Werte:

`markiert` (Voreinstellung)

Das Laden des RSA-Schlüssels ist aktiviert.

Beim Systemstart 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:

`inaktiv`

Das Gerät lädt das Konfigurationsprofil aus dem permanenten Speicher (*NVM*).

`erste`

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 *erste* 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  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 Seriennummer.

1.8 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]
- [Eingehende Netzlast]

[Konfiguration]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Port

Zeigt die Nummer des Ports.

Name

Bezeichnung des Ports.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

Das Gerät akzeptiert die folgenden Zeichen:

- <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. Wenn sich der Status des Tracking-Objekts ändert, aktiviert/deaktiviert das Gerät das mit dem Tracking-Objekt verknüpfte Interface. Sie richten das Tracking-Objekt im Dialog [Erweitert > Tracking > Konfiguration](#) ein.

Autoneg.

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 mittels Auto-Negotiation 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](#) festlegen.

Ausgegraute Darstellung

Keine automatische Auswahl des Betriebsmodus.

Manuelle Konfiguration

Legt den Betriebsmodus des Ports fest, wenn die Funktion [Autoneg.](#) ausgeschaltet ist.

Mögliche Werte:

[10M HDX](#)

Halbduplex-Verbindung

[10M FDX](#)

Vollduplex-Verbindung

[100M HDX](#)

Halbduplex-Verbindung

[100M FDX](#)

Vollduplex-Verbindung

[1G FDX](#)

Vollduplex-Verbindung

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

Link/ Aktuelle Betriebsart

Zeigt, welchen Betriebsmodus der Port gegenwärtig verwendet.

Mögliche Werte:

- Kein Kabel angesteckt, keine Verbindung.
- `10M HDX`
Halbduplex-Verbindung
- `10M FDX`
Voll duplex-Verbindung
- `100M HDX`
Halbduplex-Verbindung
- `100M FDX`
Voll duplex-Verbindung
- `1G FDX`
Voll duplex-Verbindung

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

Manuelles Cable-Crossing

Legt die Belegung der Anschlüsse eines TP-Ports fest.

Voraussetzung ist, dass die Funktion *Autoneg.* 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

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. Voraussetzung ist, dass im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.

Wenn das Gerät eine Link-Status-Änderung erkennt, sendet es einen SNMP-Trap.

`unmarkiert`

Das Senden von SNMP-Traps ist inaktiv.

Power-State

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.

Track-Name

Zeigt den Namen des Tracking-Objekts, der sich aus den in Spalte *Typ* und Spalte *Track-ID* angezeigten Werten zusammensetzt.

Energie sparen

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.

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.

[Statistiken]

Diese Registerkarte zeigt pro Port folgenden Überblick:

- Anzahl der vom Gerät empfangenen Datenpakete/Bytes
 - *Empfangene Pakete*
 - *Empfangene Oktets*
 - *Unicasts empfangen*
 - *Multicasts empfangen*
 - *Broadcasts empfangen*
- Anzahl der vom Gerät gesendeten oder vermittelten Datenpakete/Bytes
 - *Gesendete Pakete*
 - *Gesendete Oktets*
 - *Unicasts gesendet*
 - *Multicasts gesendet*
 - *Broadcasts gesendet*
- 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  .
oder

Klicken Sie im Dialog *Grundeinstellungen > Neustart* die Schaltfläche *Port-Statistiken leeren*.

[Eingehende Netzlast]

Diese Registerkarte zeigt die Eingangsnetzlast auf den einzelnen Ports.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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 Schwellenwert [%]

Legt die untere Meldeschwelle für die Netzlast fest. Wenn die Netzlast auf dem Port diesen Wert unterschreitet, dann ändert sich der Status des Kontrollkästchens in Spalte *Alarm* auf *markiert*.

Mögliche Werte:

0.00..100.00 (Voreinstellung: 0.00)

Der Wert 0 oder 0.00 deaktiviert die untere Meldeschwelle.

Oberer Schwellenwert [%]

Legt die obere Meldeschwelle für die Netzlast fest. Wenn die Netzlast auf dem Port diesen Wert überschreitet, dann ändert sich der Status des Kontrollkästchens in Spalte *Alarm* auf *markiert*.

Mögliche Werte:

0.00..100.00 (Voreinstellung: 0.00)

Der Wert 0 oder 0.00 deaktiviert die obere Meldeschwelle.

Kontroll-Intervall [s]

Legt die Zeitspanne in Sekunden fest, innerhalb der das Gerät die Netzlast ermittelt und gegebenenfalls begrenzt.

Mögliche Werte:

1..3600 (Voreinstellung: 30)

Alarm

Kennzeichnet den Alarmzustand für die Netzlast.

Mögliche Werte:

markiert

Die Netzlast auf dem Port liegt unter dem in Spalte *Unterer Schwellenwert [%]* oder über dem in Spalte *Oberer Schwellenwert [%]* festgelegten Wert. Das Gerät sendet einen SNMP-Trap. Voraussetzung ist, dass im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.

unmarkiert

Die Netzlast auf dem Port liegt zwischen der unteren und oberen Meldeschwelle.

1.9 Power over Ethernet

[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 eine 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

1.9.1 PoE Global

[Grundeinstellungen > Power over Ethernet > Global]

Anhand der in diesem Dialog festgelegten Einstellungen liefert das Gerät Strom an die Endnutzengeräte. 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.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Modul

Gerätemodule, auf die sich die Tabellenzeilen beziehen.

Budget konfigurierte Leistung [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 *Budget max. Leistung [W]*.

Budget max. Leistung [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

Schwellenwert [%]

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. Voraussetzung ist, dass im Dialog [Diagnose > Statuskonfiguration > Alarme \(Traps\)](#) die Funktion [Alarme \(Traps\)](#) eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.

Wenn der Stromverbrauch des Moduls den benutzerdefinierten Grenzwert überschreitet, sendet das Gerät einen SNMP-Trap.

`unmarkiert` (Voreinstellung)

Das Senden von SNMP-Traps ist inaktiv.

1.9.2 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 gespeiste Geräte für einen festgelegten Zeitraum aus.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

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 gespeisten 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`

Limit Leistung [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)

1.10 Neustart

[Grundeinstellungen > Neustart]

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

Neustart

Kaltstart...

Öffnet das Fenster [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 das Fenster [Warnung](#).

Um die Einstellungen permanent zu speichern, klicken Sie im Fenster [Warnung](#) die Schaltfläche [Ja](#).

Um die geänderten Einstellungen zu verwerfen, klicken Sie im Fenster [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)

Stunde:Minute:Sekunde

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.

Neustart in

Zeigt die verbleibende Zeit in Tagen, Stunden, Minuten und Sekunden bis das Gerät neu startet.

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

Abbrechen

Bricht den verzögerten Neustart ab.

Schaltflächen

MAC-Adresstabelle leeren

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 leeren

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 leeren

Entfernt die IGMP-Snooping-Einträge und setzt den Zähler im Rahmen [Information](#) auf 0.

Siehe Dialog [Switching > IGMP-Snooping > Global](#).

Log-Datei leeren

Entfernt die protokollierten Einträge aus der Log-Datei.

Siehe Dialog [Diagnose > Bericht > System-Log](#).

Persistente Log-Datei leeren

Entfernt die Log-Dateien vom externen Speicher.

Siehe Dialog [Diagnose > Bericht > Persistentes Ereignisprotokoll](#).

E-Mail-Benachrichtigung 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](#)

2.1 Grundeinstellungen

[Zeit > Grundeinstellungen]

Das Gerät ist mit einer gepufferten Hardware-Uhr ausgestattet. Diese Uhr behält die korrekte Zeit bei, wenn die Stromversorgung ausfällt oder Sie das Gerät vom Stromnetz trennen. Nach dem Systemstart steht die korrekte Uhrzeit wieder 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 und die Zeitzone fest.

Konfiguration

Systemzeit (UTC)

Zeigt Datum und Uhrzeit im Format der koordinierten Weltzeit (UTC).

Setze Zeit vom PC

Das Gerät übernimmt die Uhrzeit Ihres Computers als Systemzeit.

Systemzeit

Zeigt Datum und Uhrzeit vor Ort: $\text{Systemzeit} = \text{Systemzeit (UTC)} + \text{Lokaler Offset [min]} + \text{Sommerzeit}$

Zeitquelle

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 eingeschaltet und das Gerät ist durch einen *SNTP*-Server synchronisiert.
Siehe Dialog *Zeit > SNTP*.

Lokaler Offset [min]

Legt die Differenz in Minuten zwischen koordinierter Weltzeit (UTC) und Ortszeit fest: *Lokaler Offset [min] = Systemzeit – Systemzeit (UTC)*

Mögliche Werte:

-780..840 (Voreinstellung: 60)

[Sommerzeit]

In dieser Registerkarte schalten Sie die Funktion *Sommerzeit* ein/aus. Beginn und Ende der Sommerzeit wählen Sie anhand eines vordefinierten Profils aus. Alternativ dazu legen Sie diese Einstellungen individuell fest. Während der Sommerzeit stellt das Gerät die Ortszeit um 1 Stunde vor.

Funktion

Sommerzeit

Schaltet den *Sommerzeit*-Modus ein/aus.

Mögliche Werte:

An

Die *Sommerzeit*-Modus ist eingeschaltet.

Das Gerät stellt die Uhr automatisch auf Sommerzeit und wieder zurück.

Aus (Voreinstellung)

Die *Sommerzeit*-Modus ist ausgeschaltet.

Die Sommerzeit-Einstellungen legen Sie in den Rahmen *Sommerzeit Beginn* und *Sommerzeit Ende* fest.

Profil...

Öffnet das Fenster *Profil...*, um ein vordefiniertes Profil für Beginn und Ende der Sommerzeit auszuwählen. Das Auswählen eines Profils überschreibt die in den Rahmen *Sommerzeit Beginn* und *Sommerzeit Ende* festgelegten Einstellungen.

Mögliche Werte:

EU

Sommerzeit-Einstellungen, die in der Europäischen Union gelten.

USA

Sommerzeit-Einstellungen, die in den Vereinigten Staaten gelten.

Sommerzeit Beginn

In diesem Rahmen legen Sie den Zeitpunkt fest, zu dem das Gerät die Uhr von Normalzeit auf Sommerzeit vorstellt. In den ersten 3 Feldern legen Sie den Tag für den Beginn der Sommerzeit fest. Im letzten Feld legen Sie den Zeitpunkt fest.

Woche

Legt die Woche im gegenwärtigen Monat fest.

Mögliche Werte:

- (Voreinstellung)

erste

zweite

dritte

vierte

letzte

Tag

Legt den Wochentag fest.

Mögliche Werte:

- (Voreinstellung)

Sonntag

Montag

Dienstag

Mittwoch

Donnerstag

Freitag

Samstag

Monat

Legt den Monat fest.

Mögliche Werte:

- (Voreinstellung)

Januar

Februar

März

April

Mai

Juni

Juli

August

September

Oktober

November

Dezember

Systemzeit

Legt den Zeitpunkt fest, zu dem das Gerät die Uhr auf Sommerzeit vorstellt.

Mögliche Werte:

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

Sommerzeit Ende

In diesem Rahmen legen Sie den Zeitpunkt fest, zu dem das Gerät die Uhr von Sommerzeit auf Normalzeit zurückstellt. In den ersten 3 Feldern legen Sie den Tag für das Ende der Sommerzeit fest. Im letzten Feld legen Sie den Zeitpunkt fest.

Woche

Legt die Woche im gegenwärtigen Monat fest.

Mögliche Werte:

- (Voreinstellung)

erste

zweite

dritte

vierte

letzte

Tag

Legt den Wochentag fest.

Mögliche Werte:

- (Voreinstellung)

Sonntag

Montag

Dienstag

Mittwoch

Donnerstag

Freitag

Samstag

Monat

Legt den Monat fest.

Mögliche Werte:

- (Voreinstellung)

Januar

Februar

März

April

Mai

Juni
Juli
August
September
Oktober
November
Dezember

Systemzeit

Legt den Zeitpunkt fest, zu dem das Gerät die Uhr auf Normalzeit zurückstellt.

Mögliche Werte:

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

22 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](#)

2.21 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 *Client* des Geräts ein/aus.

Mögliche Werte:

An

Die Funktion *Client* ist eingeschaltet.
Das Gerät arbeitet als *SNTP*-Client.

Aus (Voreinstellung)

Die Funktion *Client* ist ausgeschaltet.

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.

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.

Tabelle

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Schaltflächen



Hinzufügen

Fügt eine Tabellenzeile hinzu.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Das Gerät weist den Wert automatisch zu, wenn Sie eine Tabellenzeile hinzufügen.

Wenn Sie eine Tabellenzeile löschen, bleibt eine Lücke in der Nummerierung. Wenn Sie eine neue Tabellenzeile erzeugen, schließt das Gerät die erste Lücke.

Das Gerät sendet nach dem Starten Anfragen an den [SNTP](#)-Server, der in der ersten Tabellenzeile konfiguriert ist. Bleibt die Antwort des Servers aus, sendet das Gerät seine Anfragen an den [SNTP](#)-Server, der in der nächsten Tabellenzeile 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

IP-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.

serverUnsynchronized

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.

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 örtliche 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 *Server* des Geräts ein/aus.

Mögliche Werte:

An

Die Funktion *Server* ist eingeschaltet.
Das Gerät arbeitet als *SNTP*-Server.

Aus (Voreinstellung)

Die Funktion *Server* ist ausgeschaltet.

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

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.

syncToRemoteServer

Der *SNTP*-Server ist synchronisiert auf einen *SNTP*-Server, der in einer Kaskade dem Gerät übergeordnet ist.

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.

Mögliche Werte:

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 > Global*.

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.

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.

Min. Passwort-Länge

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

Das Gerät prüft das Passwort gemäß dieser Richtlinie, unabhängig von der Einstellung des Kontrollkästchens [Richtlinien überprüfen](#).

Mögliche Werte:

1..64 (Voreinstellung: 6)

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)

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 festgelegt.

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 festgelegt.

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 festgelegt.

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 festgelegt.

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.

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Schaltflächen



Hinzufügen

Öffnet das Fenster *Erzeugen*, um eine Tabellenzeile hinzuzufügen.

- Im Feld *Benutzername* legen Sie die Bezeichnung des Benutzerkontos fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen



Löschen

Entfernt die ausgewählte Tabellenzeile.

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 Zugriffsrolle *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 *Passwort SNMP-Authentifizierung* und *Passwort SNMP-Verschlüsselung* dasselbe Passwort.

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

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 6..64 Zeichen

Das Gerät akzeptiert die folgenden Zeichen:

- 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 Zugriffsrolle 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 Zugriffsrolle ein Fehler auftritt, dann weist das Gerät dem Benutzerkonto diese Zugriffsrolle 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 Zugriffsrolle 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 mittels 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.

Passwort SNMP-Authentifizierung

Legt das Passwort fest, welches das Gerät beim Zugriff des Benutzers mittels 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.

- Für die gegenwärtige Spalte ermöglicht 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

Das Gerät akzeptiert die folgenden Zeichen:

- a..z
- A..Z
- 0..9
- !#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~

SNMP-Verschlüsselung

Legt das Verschlüsselungsprotokoll fest, welches das Gerät beim Zugriff des Benutzers mittels SNMPv3 anwendet.

Mögliche Werte:

kein

Keine Verschlüsselung.

des (Voreinstellung)

DES-Verschlüsselung

aesCfb128

AES-128-Verschlüsselung

Passwort SNMP-Verschlüsselung

Legt das Passwort fest, welches das Gerät zur Verschlüsselung beim Zugriff des Benutzers mittels 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.

- Für die gegenwärtige Spalte ermöglicht 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

Das Gerät akzeptiert die folgenden Zeichen:

- a..z
- A..Z
- 0..9
- !#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~

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 Port-basierten 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

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](#).

Schaltflächen



Hinzufügen

Öffnet das Fenster [Erzeugen](#), um eine Tabellenzeile hinzuzufügen.

- Im Feld *Name* legen Sie den Namen der Liste fest.
Mögliche Werte:
Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen



Löschen

Entfernt die ausgewählte Tabellenzeile.



Anwendungen zuordnen

Öffnet das Fenster [Anwendungen zuordnen](#). Das Fenster zeigt die Anwendungen, die Sie der ausgewählten Liste zuordnen können.

Klicken und wählen Sie einen Eintrag, um diesen der gegenwärtig ausgewählten Liste zuzuordnen.


Eine Anwendung, die bereits einer anderen Liste zugeordnet ist, ordnet das Gerät der gegenwärtig ausgewählten Liste zu, sobald Sie die Schaltfläche [Ok](#) klicken.

Klicken und wählen Sie einen Eintrag ab, um dessen Zuordnung zur gegenwärtig ausgewählten Liste rückgängig zu machen.

Wenn Sie die Anwendung [WebInterface](#) abwählen, dann bricht die Verbindung zum Gerät ab, sobald Sie auf Schaltfläche [Ok](#) klicken.

Name

Zeigt die Bezeichnung der Liste.

Um eine neue Liste anzulegen, klicken Sie die Schaltfläche .

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 Authentifizierungsliste [defaultDot1x8021AuthList](#) können Sie diesen Wert nicht zuweisen.

[radius](#)

Das Gerät authentifiziert die Benutzer mit einem RADIUS-Server im Netz. Den RADIUS-Server legen Sie im Dialog [Netzicherheit > 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 mittels 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 > IAS*. Der Authentifizierungsliste *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 *Gerätesicherheit > 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 . Das Gerät ermöglicht Ihnen, jede Anwendung genau einer Liste zuzuordnen.

Aktiv

Aktiviert/deaktiviert die Liste.

Mögliche Werte:

markiert (Voreinstellung)

Die Liste ist aktiviert. Das Gerät wendet die Richtlinien dieser Liste an, wenn Benutzer mit der betreffenden Anwendung auf das Gerät zugreifen.

unmarkiert

Die Liste ist deaktiviert.

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 Anmeldedaten flüchtig im Cache. 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 Zugriffsrolle *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

Schaltflächen



Cache leeren

Entfernt die zwischengespeicherten Anmeldeinformationen der erfolgreich angemeldeten Benutzer.

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, welches 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 eindeutigen 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 eindeutigen 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 dazu 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Schaltflächen



Hinzufügen

Fügt eine Tabellenzeile hinzu.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Das Gerät weist den Wert automatisch zu, wenn Sie eine Tabellenzeile hinzufügen.

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.

Status Server

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.

3.3.2 LDAP Rollen-Zuweisung

[Gerätesicherheit > LDAP > Rollen-Zuweisung]

Dieser Dialog ermöglicht Ihnen, bis zu 64 Mappings zu erstellen, um Benutzern eine Zugriffsrolle zuzuweisen.

In der Tabelle legen Sie fest, ob das Gerät anhand eines Attributs mit einem bestimmten Wert oder anhand der Gruppenmitgliedschaft dem Benutzer eine Zugriffsrolle 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 Zugriffsrolle mit den weitreichenderen Berechtigungen oder die 1. in der Tabelle zutreffende Zugriffsrolle.

Konfiguration

Übereinstimmende Regel

Legt fest, welche Zugriffsrolle das Gerät verwendet, wenn mehr als ein Mapping für einen Benutzer zutrifft.

Mögliche Werte:

highest (Voreinstellung)

Das Gerät verwendet die Zugriffsrolle mit den weitreichenderen Berechtigungen.

erste

Das Gerät wendet die Rolle mit dem kleineren Wert in Spalte *Index* auf den Benutzer an.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Schaltflächen



Hinzufügen

Öffnet das Fenster *Erzeugen*, um eine Tabellenzeile hinzuzufügen.

- Im Feld *Index* legen Sie die Index-Nummer fest.

Mögliche Werte:

1..64



Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Sie legen die Indexnummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Rolle

Legt die Zugriffsrolle 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 Zugriffsrolle ein Fehler erkannt wird, dann weist das Gerät dem Benutzerkonto diese Zugriffsrolle 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 festgelegt 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.

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

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.

[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`

Zugriff mittels SNMP-Version 1 ist aktiv.

- Die Community-Namen legen Sie fest im Dialog [Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community](#).
- Den Schreibzugriff für die Berechtigung *Lesen und Schreiben* aktivieren/deaktivieren Sie im Dialog [Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community](#).

`unmarkiert` (Voreinstellung)

Zugriff mittels SNMP-Version 1 ist inaktiv.

SNMPv2

Aktiviert/deaktiviert den Zugriff auf das Gerät per SNMP Version 2.

Mögliche Werte:

`markiert`

Zugriff mittels SNMP-Version 2 ist aktiv.

- Die Community-Namen legen Sie fest im Dialog [Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community](#).
- Den Schreibzugriff für die Berechtigung *Lesen und Schreiben* aktivieren/deaktivieren Sie im Dialog [Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community](#).

`unmarkiert` (Voreinstellung)

Zugriff mittels SNMP-Version 2 ist inaktiv.

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 Industrial HiVision 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 Einstellungen zu speichern.

Starten Sie das Gerät neu.

SNMPOver802

Aktiviert/deaktiviert den Zugriff auf das Gerät per SNMP over IEEE 802.

Mögliche Werte:

[markiert](#)

Zugriff ist aktiviert.

[unmarkiert](#) (Voreinstellung)

Zugriff ist deaktiviert.

[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:

[An](#) (Voreinstellung)

Der Telnet-Server ist eingeschaltet.

Der Zugriff auf das Management des Geräts ist möglich mit dem Command Line Interface über eine unverschlüsselte Telnet-Verbindung.

[Aus](#)

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)

[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. Alternativ dazu kopieren Sie eigene Schlüssel im PEM-Format in das Gerät.

Alternativ ermöglicht Ihnen das Gerät, den RSA-Schlüssel (Host Key) beim Systemstart 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)

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 dazu kopieren Sie eigene Schlüssel im PEM-Format in das Gerät. 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.

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 (Voreinstellung)

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.

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 dazu 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.

[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.

[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.

Zertifikat

Wenn das Gerät ein HTTPS-Zertifikat verwendet, das nicht von einer dem Webbrowser bekannten Zertifizierungsstelle (Certificate Authority, CA) signiert ist, dann zeigt der Webbrowser möglicherweise eine Warnung an, bevor er die grafische Benutzeroberfläche lädt.

Um diese Warnung abzustellen, haben Sie die folgenden Möglichkeiten:

- Installieren Sie auf dem Gerät ein HTTPS-Zertifikat, dessen CA Ihrem Webbrowser bekannt ist. Dies kann zusätzlich erfordern, dass Sie die CA Ihrem Webbrowser oder Betriebssystem bekannt machen.
- Als Übergangslösung können Sie auch eine Ausnahmeregel für das existierende Geräte-Zertifikat in Ihrem Webbrowser hinzufügen.

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 dazu kopieren Sie ein eigenes Zertifikat in das Gerät. 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.

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 (Voreinstellung)

Das Feld *Fingerabdruck* zeigt den SHA256-Fingerprint des Zertifikats.

Fingerabdruck

Hexadezimale Zeichenfolge des vom Server verwendeten digitalen Zertifikats.

Wenn Sie die Einstellung im Feld *Fingerabdruck Typ* ändern, klicken Sie anschließend die Schaltflächen ✓ und ↻, um die Anzeige zu aktualisieren.

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 dazu 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>[:Port]/<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>[:Port]/<Pfad>/<Dateiname>

Start

Kopiert das im Feld **URL** festgelegte Zertifikat in das Gerät.

3.4.2 IP-Zugriffsbeschränkung

[Gerätesicherheit > Management-Zugriff > IP-Zugriffsbeschränkung]

Dieser Dialog ermöglicht Ihnen, 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 eine Tabellenzeile 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 eine aktive Tabellenzeile 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 Tabellenzeilen zu definieren und separat zu aktivieren.

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Schaltflächen



Hinzufügen

Fügt eine Tabellenzeile hinzu.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Das Gerät weist den Wert automatisch zu, wenn Sie eine Tabellenzeile hinzufügen.

Wenn Sie eine Tabellenzeile löschen, bleibt eine Lücke in der Nummerierung. Wenn Sie eine neue Tabellenzeile erzeugen, schließt das Gerät die erste 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.

Aktiv

Aktiviert/deaktiviert die Tabellenzeile.

Mögliche Werte:

`markiert` (Voreinstellung)

Die Tabellenzeile ist aktiviert. Das Gerät beschränkt den Zugriff auf das Management des Geräts auf den nebenstehenden IP-Adressbereich und die ausgewählten IP-basierten Anwendungen.

`unmarkiert`

Die Tabellenzeile ist deaktiviert.

3.4.3 Web

[Gerätesicherheit > Management-Zugriff > Web]

In diesem Dialog legen Sie Einstellungen für die grafische Benutzeroberfläche fest.

Konfiguration

Webinterface-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.

3.4.4 Command Line Interface

[Gerätesicherheit > Management-Zugriff > CLI]

In diesem Dialog legen Sie Einstellungen für das Command Line Interface fest. Weitere 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: (GRS)

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*.

[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>`

3.4.5 SNMPv1/v2 Community

[Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community]

In diesem Dialog legen Sie den Community-Namen für SNMPv1/v2-Anwendungen fest und aktivieren/deaktivieren den Schreibzugriff für die Berechtigung *Lesen und Schreiben*.

Anwendungen senden Anfragen mittels SNMPv1/v2 mit einem Community-Namen im SNMP-Datenpaket-Header. Abhängig vom Community-Namen (siehe Spalte *Community*) und der Einstellung für den Schreibzugriff (siehe Kontrollkästchen in Spalte *SNMP V1/V2 read-only*) erhält die Anwendung die Berechtigung *Lesen* oder *Lesen und Schreiben*.

Den Zugriff auf das Gerät mittels SNMPv1/v2 aktivieren Sie im Dialog *Gerätesicherheit > Management-Zugriff > Server*.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

Community

Zeigt die Berechtigung für SNMPv1/v2-Anwendungen auf dem Gerät.

Mögliche Werte:

Write

Für Anfragen mit dem eingegebenen Community-Namen erhält die Anwendung die Berechtigung *Lesen und Schreiben*.

Wenn das Kontrollkästchen *SNMP V1/V2 read-only* markiert ist, erhält die Anwendung die Berechtigung *Lesen*.

Read

Für Anfragen mit dem eingegebenen Community-Namen erhält die Anwendung die Berechtigung *Lesen*.

Name

Legt den Community-Namen für die nebenstehende Berechtigung fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

private (Voreinstellung für die Berechtigung *Lesen und Schreiben*)

public (Voreinstellung für die Berechtigung *Lesen*)

Konfiguration

SNMP V1/V2 read-only

Aktiviert/deaktiviert den Schreibzugriff für die `Write-Community`.

Mögliche Werte:

`markiert`

Der Schreibzugriff für die `Write-Community` ist inaktiv.

Für Anfragen mit dem eingegebenen Community-Namen erhält die Anwendung die Berechtigung *Lesen*.

`unmarkiert` (Voreinstellung)

Der Schreibzugriff für die `Write-Community` ist aktiv.

Für Anfragen mit dem eingegebenen Community-Namen erhält die Anwendung die Berechtigung *Lesen und Schreiben*.

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>

4 Netzsicherheit

Das Menü enthält die folgenden Dialoge:

[Netzsicherheit Übersicht](#)
[Port-Sicherheit](#)
[802.1X](#)
[RADIUS](#)
[DoS](#)
[ACL](#)

4.1 Netzsicherheit Übersicht

[Netzsicherheit > Übersicht]

Dieser Dialog zeigt eine Übersicht über die im Gerät verwendeten Netzsicherheits-Regeln.

Übersicht

Die oberste Ebene zeigt:

- Die Ports, denen eine Netzsicherheits-Regel zugewiesen ist.
- Die VLANs, denen eine Netzsicherheits-Regel zugewiesen ist.

Die untergeordneten Ebenen zeigen:

- Die festgelegten [ACL](#)-Regeln.
Siehe Dialog [Netzsicherheit > ACL](#).

Schaltflächen



Zeigt ein Textfeld, um nach einem Schlüsselwort zu suchen. Wenn Sie ein Zeichen oder eine Zeichenkette eingeben, zeigt die Übersicht ausschließlich Einträge, die mit diesem Schlüsselwort in Zusammenhang stehen.



Klappt die Ebenen zu. Die Übersicht zeigt dann ausschließlich die erste Ebene der Einträge.



Klappt die Ebenen auf. Die Übersicht zeigt dann jede Ebene der Einträge.



Klappt den aktuellen Eintrag auf und zeigt die Einträge der nächsttieferen Ebene.




Klappt den Eintrag zu und blendet die Einträge der darunter liegenden Ebenen aus.

4.2 Port-Sicherheit

[Netzsicherheit > Port-Sicherheit]

Das Gerät ermöglicht Ihnen, ausschließlich Datenpakete von erwünschten Absendern auf einem Port zu vermitteln. Wenn die Funktion *Port-Sicherheit* eingeschaltet ist, prüft das Gerät die VLAN-ID und die MAC-Adresse des Absenders, bevor es ein Datenpaket vermittelt. Die Datenpakete unerwünschter Absender verwirft das Gerät und protokolliert dieses Ereignis.

In diesem Dialog unterstützt Sie ein Fenster *Wizard*, die Ports mit der Adresse eines oder mehrerer erwünschter Absender zu verknüpfen. Im Gerät heißen diese Adressen *statische Einträge*. Zum Ansehen der festgelegten statischen Adressen wählen Sie den betreffenden Port und klicken die Schaltfläche .

Um die Einrichtung zu vereinfachen, ermöglicht Ihnen das Gerät, die Adresse der erwünschten Absender automatisch zu erfassen. Das Gerät „lernt“ die Adressen durch das Bewerten der empfangenen Datenpakete. Im Gerät heißen diese Adressen *dynamische Einträge*. Wenn die benutzerdefinierte Obergrenze erreicht ist (*Dynamisches Limit*), beendet das Gerät das "Lernen" auf dem betreffenden Port. Das Gerät leitet lediglich Datenpakete weiter, deren Absender bereits auf dem Port erfasst sind. Wenn Sie die Obergrenze an die Anzahl der zu erwartenden Absender anpassen, erschweren Sie damit *MAC-Flooding*-Attacken.

Anmerkung: Beim automatischen Erfassen der *dynamischen Einträge* verwirft das Gerät stets das erste Datenpaket von unbekanntem Absendern. Anhand dieses ersten Datenpakets prüft das Gerät, ob die Obergrenze erreicht ist. Bis zum Erreichen der Obergrenze erfasst das Gerät die Adressen. Anschließend vermittelt das Gerät Datenpakete, die es auf dem betreffenden Port von diesem Absender empfängt.

Funktion

Funktion

Schaltet die Funktion *Port-Sicherheit* im Gerät 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 erwünscht sind. Damit diese Einstellung wirksam wird, aktivieren Sie zusätzlich die Funktion *Port-Sicherheit* auf den betreffenden Ports.

Aus (Voreinstellung)

Die Funktion *Port-Sicherheit* ist ausgeschaltet.

Das Gerät vermittelt jedes empfangene Datenpaket, ohne die Absenderadresse zu prüfen.

Konfiguration

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für *Port-Sicherheit* im Gerät.

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. Das Gerät schaltet den Port aus und sendet optional einen SNMP-Trap, wenn eines der folgenden Ereignisse eintritt:

- Das Gerät erfasst mindestens eine Adresse eines Absenders, der auf dem Port nicht erwünscht ist.
- Das Gerät erfasst mehr Adressen als in Spalte *Dynamisches Limit* festgelegt.

unmarkiert (Voreinstellung)

Die Funktion *Auto-Disable* für *Port-Sicherheit* ist inaktiv.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

Schaltflächen



Öffnet das Fenster *Wizard*, das Sie dabei unterstützt, die Ports mit der Adresse eines oder mehrerer erwünschter Absender zu verknüpfen. Siehe „[\[Wizard: Port-Sicherheit\]](#)“ auf [Seite 132](#).

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert die Funktion *Port-Sicherheit* auf dem Port.

Mögliche Werte:

markiert

Das Gerät prüft jedes auf dem Port empfangene Datenpaket und vermittelt es ausschließlich dann, wenn die Absenderadresse des Datenpakets erwünscht 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 betreiben, empfehlen wir, die Markierung des Kontrollkästchens für die Ring-Ports aufzuheben.

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für *Port-Sicherheit* auf dem Port.

Mögliche Werte:

markiert (Voreinstellung)

Die Funktion *Auto-Disable* ist auf dem Port aktiv.

Das Gerät schaltet den Port aus und sendet optional einen SNMP-Trap, wenn eines der folgenden Ereignisse eintritt:

- Das Gerät erfasst mindestens eine Adresse eines Absenders, der auf dem Port nicht erwünscht ist.
- Das Gerät erfasst mehr Adressen als in Spalte *Dynamisches Limit* festgelegt.

Die *Link status*-LED des Ports blinkt 3x pro Periode. Diese Begrenzung erschwert *MAC-Spoofing*-Attacken.

Voraussetzung ist, dass im Rahmen *Konfiguration* das Kontrollkästchen *Auto-Disable* markiert ist.

- Der Dialog *Diagnose > Ports > Auto-Disable* zeigt, welche Ports aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet sind.
- Nach einer Wartezeit schaltet die Funktion *Auto-Disable* 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* ist auf dem Port 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. Voraussetzung ist, dass im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.

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.

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 Adressen (*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 Adressen erfasst als hier festgelegt ist, dann 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

Keine automatische Erfassung von Adressen auf diesem Port.

1 .. 600 (Voreinstellung: 600)

Statisches Limit

Legt die Obergrenze fest für die Anzahl der Adressen, die mittels des Fensters *Wizard* mit dem Port verknüpft sind (*statische Einträge*).

Mögliche Werte:

0

Keine Verknüpfung zwischen dem Port und einem erwünschten Absender möglich. Legen Sie diesen Wert ausschließlich dann fest, wenn Sie in Spalte *Dynamisches Limit* einen Wert > 0 festlegen.

1 .. 64 (Voreinstellung: 64)

Dynamische Einträge

Zeigt, wie viele Adressen das Gerät automatisch erfasst hat.

Statische MAC Einträge

Zeigt die Anzahl der MAC-Adressen, die mit dem Port verknüpft sind.

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.

[Wizard: Port-Sicherheit]

Das Fenster *Wizard* unterstützt Sie dabei, die Ports mit der Adresse eines oder mehrerer erwünschter Absender zu verknüpfen.

Das Fenster *Wizard* führt Sie durch die folgenden Schritte:

- [Port auswählen](#)
- [MAC-Adressen](#)

Anmerkung: Das Gerät speichert die mit dem Port verknüpften Adressen so lange, bis Sie die Funktion *Port-Sicherheit* auf dem betreffenden Port deaktivieren oder die Funktion *Port-Sicherheit* im Gerät ausschalten.

Nach Schließen des Fensters *Wizard* klicken Sie die Schaltfläche ✓, um Ihre Einstellungen zu speichern.

Port auswählen

Port

Legt den Port fest, den Sie im nächsten Schritt mit der Adresse erwünschter Absender verknüpfen.

MAC-Adressen

Statische Einträge (x/y)

Zeigt, wie viele Adressen mit dem Port mittels des Fensters *Wizard* verknüpft sind sowie die Obergrenze für *statische Einträge*. Der untere Teil des Fensters *Wizard* zeigt die Einträge im Detail, sofern vorhanden.



Entfernt die Einträge im unteren Teil des Fensters *Wizard*. Das Gerät hebt die jeweilige Zuordnung zwischen einem Port und den erwünschten Absendern auf.

VLAN-ID

Legt die VLAN-ID des erwünschten Absenders fest.

Mögliche Werte:

1 . . 4042

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.

Anmerkung: Eine MAC-Adresse können Sie lediglich einem Port zuweisen.

Hinzufügen

Erzeugt einen *statischen Eintrag* basierend auf den in den Feldern *VLAN-ID* und *MAC-Adresse* festgelegten Werten. Folglich finden Sie im unteren Teil des Fensters *Wizard* einen neuen Eintrag.


Einträge im unteren Teil des Fensters

Der untere Teil des Fensters *Wizard* zeigt VLAN-ID und MAC-Adresse der an diesem Port erwünschten Absender. Im Folgenden finden Sie eine Beschreibung der Symbole, die spezifisch für diese Einträge sind.



Statischer Eintrag: Wenn Sie das Symbol klicken, entfernt das Gerät den *statischen Eintrag* und die jeweilige Zuordnung zwischen dem Port und den erwünschten Absendern.



Dynamischer Eintrag: Wenn Sie das Symbol klicken, ändert sich das Symbol zu . Das Gerät wandelt den *dynamischen Eintrag* in einen *statischen Eintrag* um, wenn Sie das *Wizard* Fenster schließen. Um diese Änderung rückgängig zu machen, klicken Sie das Symbol noch einmal, bevor Sie das Fenster *Wizard* schließen.

4.3 802.1X

[Netzsicherheit > 802.1X]

Mit der Port-basierten 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 mittels des Authentisierungsprotokolls 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 Verlauf Port-Authentifizierung
- 802.1X Integrierter Authentifikations-Server (IAS)

4.3.1 802.1X Global

[Netzsicherheit > 802.1X > Global]

Dieser Dialog ermöglicht Ihnen, grundlegende Einstellungen für die Port-basierte Zugriffskontrolle festzulegen.

Funktion

Funktion

Schaltet die Funktion [802.1X](#) ein/aus.

Mögliche Werte:

[An](#)

Die Funktion [802.1X](#) ist eingeschaltet.

Das Gerät prüft den Zugriff angeschlossener Endgeräte auf das Netz.

Die Port-basierte Zugriffskontrolle ist eingeschaltet.

[Aus](#) (Voreinstellung)

Die Funktion [802.1X](#) ist ausgeschaltet.

Die Port-basierte 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-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.

Information

Monitor-Mode Clients

Zeigt, wie vielen Endgeräten das Gerät trotz erfolgloser Anmeldung Zugriff auf das Netz gewährt hat.

Voraussetzung ist, dass im Rahmen *Konfiguration* die Funktion *Monitor-Mode* aktiv ist.

Non-Monitor-Mode Clients

Zeigt, wie vielen Endgeräten das Gerät nach erfolgreicher Anmeldung Zugriff auf das Netz gewährt hat.

Richtlinie 1

Zeigt die Methode an, die das Gerät zum Authentifizieren der Endgeräte mithilfe des Protokolls *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 Richtlinie `8021x` zu.

Um die Endgeräte über den Integrierten Authentifikationsserver (IAS) zu authentifizieren, weisen Sie der Liste `ias` die Richtlinie `8021x` zu.

4.3.2 802.1X Port-Konfiguration

[Netzsicherheit > 802.1X > Port-Konfiguration]

Dieser Dialog ermöglicht Ihnen, die Zugriffseinstellungen für jeden Port festzulegen.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Port

Zeigt die Nummer des Ports.

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.

Status Authentifizierung

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.

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 [Netzicherheit > 802.1X > Port-Clients](#).

Grund

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 [Netzicherheit > 802.1X > Port-Clients](#).

Gast VLAN-ID

Legt die ID des VLANs fest, die der Authenticator dem Port zuweist, wenn sich das Endgerät während der in Spalte *Intervall Gast-VLAN* festgelegten Zeit nicht 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 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.

1..4042

Anmerkung: Die Funktion *MAC-Authorized-Bypass* und die Funktion *Gast VLAN-ID* können nicht gleichzeitig verwendet werden.

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.

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 *Periode Reauthentifizierung [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.

Periode Reauthentifizierung [s]

Legt die Zeitspanne in Sekunden fest, nach welcher der Authenticator periodisch das Endgerät auffordert, sich erneut anzumelden.

Mögliche Werte:

1..65535 (Voreinstellung: 3600)

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)

Timeout Supplikant [s]

Legt die Zeitspanne in Sekunden fest, innerhalb welcher der Authenticator auf die Anmeldung des Endgeräts wartet.

Mögliche Werte:

1..65535 (Voreinstellung: 30)

Timeout Server [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 *Timeout Supplikant [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)

Intervall Gast-VLAN

Zeigt die Zeitspanne in Sekunden, 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.

Der Wert in dieser Spalte ist das Dreifache des in Spalte *Sendeperiode [s]* festgelegten Werts.

Status

Zeigt den gegenwärtigen Zustand des Authenticators (*Authenticator PAE state*).

Mögliche Werte:

initialize
disconnected
connecting
authenticating
authenticated
aborting
held
forceAuth
forceUnauth

Backend Status Authentifizierung

Zeigt den gegenwärtigen Zustand der Verbindung zum Authentifizierungs-Server (*Backend Authentication state*).

Mögliche Werte:

request
response
erfolgreich
fail
timeout
idle
initialize

Port initialisieren

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* 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.

Reauthentifizieren

Aktiviert/deaktiviert die einmalige Authentifizierungsanforderung.

Wenden Sie diese Funktion ausschließlich dann an, wenn für den Port in Spalte *Port-Kontrolle* der Wert *auto* 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.

4.3.3 802.1X Port-Clients

[Netzicherheit > 802.1X > Port-Clients]

Dieser Dialog zeigt Informationen über die angeschlossenen Endgeräte.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

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.

VLAN 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 [Netzicherheit > 802.1X > Port-Konfiguration](#), Spalte [Port-Kontrolle](#) der Wert `auto` 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

4.3.4 802.1X EAPOL-Portstatistiken

[Netzicherheit > 802.1X > Statistiken]

Dieser Dialog zeigt, welche EAPOL-Datenpakete das Gerät für die Authentifizierung der Endgeräte gesendet und empfangen hat.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Schaltflächen



Entfernt die ausgewählte Tabellenzeile.

Port

Zeigt die Nummer des Ports.

Empfangene

Zeigt, wie viele EAPOL-Datenpakete insgesamt das Gerät auf dem Port empfangen hat.

Gesendete

Zeigt, wie viele EAPOL-Datenpakete insgesamt das Gerät auf dem Port gesendet hat.

Start

Zeigt, wie viele EAPOL-Start-Datenpakete das Gerät auf dem Port empfangen hat.

Logoff

Zeigt, wie viele EAPOL-Logoff-Datenpakete das Gerät auf dem Port empfangen hat.

Response/ID

Zeigt, wie viele EAP-Response/Identity-Datenpakete das Gerät auf dem Port empfangen hat.

Response

Zeigt, wie viele gültige EAP-Response-Datenpakete das Gerät auf dem Port empfangen hat (ohne EAP-Response/Identity-Datenpakete).

Request/ID

Zeigt, wie viele EAP-Request/Identity-Datenpakete das Gerät auf dem Port empfangen hat.

Request

Zeigt, wie viele gültige EAP-Request-Datenpakete das Gerät auf dem Port empfangen hat (ohne EAP-Request/Identity-Datenpakete).

Invalid

Zeigt, wie viele EAPOL-Datenpakete mit unbekanntem Frame-Typ das Gerät auf dem Port empfangen hat.

Fehlerhaft Empfangene

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.

4.3.5 802.1X Verlauf Port-Authentifizierung

[Netzicherheit > 802.1X > Verlauf Port-Authentifizierung]

Das Gerät protokolliert den Authentifizierungsvorgang der Endgeräte, die an seinen Ports angeschlossen sind. Dieser Dialog zeigt die bei der Authentifizierung erfassten Informationen.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Schaltflächen



Entfernt die ausgewählte Tabellenzeile.

Port

Zeigt die Nummer des Ports.

Zeit

Zeigt den Zeitpunkt, zu dem der Authenticator das Endgerät authentifiziert hat.

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.

Status

Zeigt den Zustand der Authentifizierung auf dem Port.

Mögliche Werte:

erfolgreich

Die Authentifizierung war erfolgreich.

Fehler

Die Authentifizierung war nicht erfolgreich.

Zugriff

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.

VLAN Typ

Zeigt die Art des VLAN, das der Authenticator dem Port zugewiesen hat.

Mögliche Werte:

default

radius

unauthenticatedVlan

guestVlan

monitorVlan

notAssigned

Grund

Zeigt den Grund für die Zuweisung der VLAN-ID und des VLAN-Typs.

4.3.6 802.1X Integrierter Authentifikations-Server (IAS)

[Netzicherheit > 802.1X > IAS]

Der Integrierte Authentifikationsserver (IAS) ermöglicht Ihnen, Endgeräte mittels Protokoll [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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

Schaltflächen

 Hinzufügen

Öffnet das Fenster [Erzeugen](#), um eine Tabellenzeile hinzuzufügen.

- Im Feld [Benutzername](#) legen Sie den Namen des Benutzerkontos auf dem Endgerät fest.

 Löschen

Entfernt die ausgewählte Tabellenzeile.

Benutzername

Zeigt den Namen des Benutzerkontos auf dem Endgerät.

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 mittels Protokoll `802.1X` anzumelden.

`unmarkiert` (Voreinstellung)

Die Zugangsdaten sind inaktiv.

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. Dies ermöglicht Ihnen, 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 der Benutzer.

Den in der Antwort eines RADIUS-Servers übertragenen Service-Type weist das Gerät wie folgt einer auf dem Gerät vorhandenen Zugriffsrolle 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

[Netzicherheit > RADIUS > Global]

Dieser Dialog ermöglicht Ihnen, grundlegende Einstellungen für RADIUS festzulegen.

RADIUS-Konfiguration

Schaltflächen

 Zurücksetzen

Löscht die Statistik im Dialog [Netzicherheit > RADIUS > Authentication-Statistiken](#) und die Statistik im Dialog [Netzicherheit > RADIUS > Accounting-Statistiken](#).

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 [Netzicherheit > 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.

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

Schaltflächen



Hinzufügen

Öffnet das Fenster [Erzeugen](#), um eine Tabellenzeile hinzuzufügen.

- Im Feld [Index](#) legen Sie die Index-Nummer fest.
- Im Feld [IP-Adresse](#) legen Sie die IP-Adresse des Servers fest.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Sie legen die Indexnummer fest, wenn Sie eine Tabellenzeile hinzufügen.

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](#))

Sie können für mehrere Server den gleichen Namen festlegen. Wenn mehrere Server den gleichen Namen haben, gilt die Einstellung in Spalte [Primärer Server](#).

IP-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.

Diese Einstellung gilt ausschließlich dann, wenn mehr als ein Server in der Tabelle den gleichen Wert in Spalte *Name* hat.

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.

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 Dialog [Netzsicherheit > RADIUS > Global](#) die Funktion [Accounting](#) aktiv 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

Schaltflächen



Hinzufügen

Öffnet das Fenster [Erzeugen](#), um eine Tabellenzeile hinzuzufügen.

- Im Feld [Index](#) legen Sie die Index-Nummer fest.
- Im Feld [IP-Adresse](#) legen Sie die IP-Adresse des Servers fest.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Sie legen die Indexnummer fest, wenn Sie eine Tabellenzeile hinzufügen.

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](#))

IP-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.

4.4.4 RADIUS Authentication Statistiken

[Netzicherheit > 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 Tabellenzeile.

Um die Statistik zu löschen, klicken Sie im Dialog [Netzicherheit > RADIUS > Global](#) die Schaltfläche



Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

Name

Zeigt den Namen des Servers.

IP-Adresse

Zeigt die IP-Adresse des Servers.

Zeit Round-Trip

Zeigt das Zeitintervall in Hundertstelsekunden zwischen der zuletzt empfangenen Antwort des Servers (Access-Reply/Access-Challenge) und dem zugehörigen gesendeten Datenpaket (Access-Request).

Access-Anfragen

Zeigt, wie viele Access-Datenpakete das Gerät an den Server gesendet hat. Der Wert berücksichtigt keine Wiederholungen.

Wiederholt gesendete Access-Anfragen

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.

Verworfenen 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.

Verworfen Pakete

Zeigt, wie viele Datenpakete das Gerät auf dem Authentication-Port vom Server empfangen und anschließend verworfen hat.

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 Tabellenzeile.

Um die Statistik zu löschen, klicken Sie im Dialog [Netzsicherheit > RADIUS > Global](#) die Schaltfläche



Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Name

Zeigt den Namen des Servers.

IP-Adresse

Zeigt die IP-Adresse des Servers.

Zeit Round-Trip

Zeigt das Zeitintervall in Hundertstelsekunden zwischen der zuletzt empfangenen Antwort des Servers (Accounting-Response) und dem zugehörigen gesendeten Datenpaket (Accounting-Request).

Accounting-Anfragen

Zeigt, wie viele Accounting-Request-Datenpakete das Gerät an den Server gesendet hat. Der Wert berücksichtigt keine Wiederholungen.

Wiederholt gesendete Accounting-Anfragen

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.

Verworfen Pakete

Zeigt, wie viele Datenpakete das Gerät auf dem Accounting-Port vom Server empfangen und anschließend verworfen hat.

4.5 DoS

[Netzsicherheit > DoS]

Denial-of-Service (DoS) ist ein Cyber-Angriff, der darauf abzielt, bestimmte Dienste oder Geräte funktionsunfähig zu machen. 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.

Anmerkung: Wir empfehlen, die Filter zu aktivieren, um das Sicherheitsniveau des Geräts zu erhöhen.

TCP/UDP

Scanner nutzen Port-Scans, um Angriffe auf das Netz vorzubereiten. 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 Schutz

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 Schutz

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 Schutz

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.

Min.-Header-Size Filter

Aktiviert/deaktiviert den Minimal-Header-Filter.

Der Minimal-Header-Filter vergleicht den TCP-Header von eingehenden Datenpaketen. Wenn der mit 4 multiplizierte Daten-Offset-Wert kleiner ist als die minimale TCP-Header-Größe, dann verwirft der Filter die Datenpakete.

Mögliche Werte:

`markiert`

Der Filter ist aktiv.

`unmarkiert` (Voreinstellung)

Der Filter ist inaktiv.

Min. Größe TCP-Header

Zeigt die minimale Größe eines gültigen TCP-Headers.

IP

Land-Attack Filter

Aktiviert/deaktiviert den *Land Attack*-Filter. Bei der *Land Attack*-Methode sendet die angreifende Station Datenpakete, deren Quell- und Zieladressen identisch mit der IP-Adresse des Empfängers sind.

Mögliche Werte:

`markiert`

Der Filter ist aktiv. Das Gerät verwirft Datenpakete, deren Quell- und Zieladressen identisch sind.

`unmarkiert` (Voreinstellung)

Der Filter ist inaktiv.

ICMP

Dieser Dialog bietet Ihnen Filtermöglichkeiten für folgende ICMP-Parameter:

- Fragmentierte Datenpakete
- ICMP-Pakete ab einer bestimmten Größe

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)

4.6 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.

Wenn ein Datenpaket die Kriterien einer oder mehrerer Regeln erfüllt, dann wendet das Gerät die in der ersten zutreffenden Regel festgelegte Aktion auf den Datenstrom an. Das Gerät ignoriert die Regeln, die der ersten zutreffenden Regel folgen. 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 dieses Verhalten. An das Ende einer Access-Control-Liste fügt das Gerät eine implizite Deny-All-Regel ein. Demzufolge verwirft das Gerät Datenpakete, die mit keiner der Regel-Kriterien übereinstimmen. Wenn Sie ein anderes Verhalten wünschen, fügen Sie am Ende Ihrer Access-Control-Listen eine Permit-All-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

4.6.1 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

Schaltflächen

 Hinzufügen

Öffnet das Fenster [Erzeugen](#), um eine Tabellenzeile hinzuzufügen.

- Im Feld [Gruppenname](#) legen Sie den Namen der Access-Control-Liste fest, der die Regel angehört. Wenn Sie einen neuen Namen hinzufügen, klicken Sie das Symbol .
- 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 Indexwert zuerst an.

 Löschen

Entfernt die ausgewählte Tabellenzeile.

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. Sie legen die Indexnummer fest, wenn Sie eine Tabellenzeile hinzufügen.

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 abhängig vom Wert in den folgenden Feldern an:

- *Quelle IP-Adresse, Ziel IP-Adresse, Protokoll*
- *DSCP, TOS-Priorität, TOS-Maske*
- *Paket fragmentiert*

Quelle 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 IP-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 IP-Protokoll- oder Schicht-4-Protokoll-Typ der Datenpakete fest, auf die das Gerät die Regel anwendet. Das Gerät wendet die Regel ausschließlich auf Datenpakete an, die den festgelegten Wert im Feld *Protocol* enthalten.

Mögliche Werte:

`any` (Voreinstellung)

Das Gerät wendet die Regel auf jedes IP-Datenpaket an, ohne den Protokolltyp auszuwerten.

`icmp`

Internet Control Message Protocol (RFC 792)

`igmp`

Internet Group Management Protocol

`ip-in-ip`

IP in IP tunneling (RFC 2003)

`tcp`

Transmission Control Protocol (RFC 793)

`udp`

User Datagram Protocol (RFC 768)

`ip`

Internet Protocol

Quelle TCP/UDP-Port

Legt den Quell-Port der IP-Datenpakete fest, auf die das Gerät die Regel anwendet. Voraussetzung ist, dass in Spalte *Protokoll* der Wert `TCP` oder `UDP` festgelegt ist.

Mögliche Werte:

`any` (Voreinstellung)

Das Gerät wendet die Regel auf jedes IP-Datenpaket an, ohne den Quell-Port auszuwerten.

`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 in Spalte *Protokoll* der Wert `TCP` oder `UDP` festgelegt ist.

Mögliche Werte:

`any` (Voreinstellung)

Das Gerät wendet die Regel auf jedes IP-Datenpaket an, ohne den Ziel-Port auszuwerten.

`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.

Log

Aktiviert/deaktiviert die Protokollierung in der Log-Datei. Siehe Dialog [Diagnose > Bericht > System-Log](#).

Mögliche Werte:

`markiert`

Die Protokollierung ist aktiv.

Voraussetzung ist, dass im Dialog [Netzsicherheit > ACL > Zuweisung](#) die Access-Control-Liste einem VLAN oder Port zugewiesen ist.

Das Gerät protokolliert in der Log-Datei im Intervall von 30s, wie viele Male es eine Deny-Regel auf IP-Datenpakete angewendet hat.

`unmarkiert` (Voreinstellung)

Die Protokollierung ist inaktiv.

Das Gerät ermöglicht Ihnen, für bis zu 128 Deny-Regeln diese Funktion zu aktivieren.

4.6.2 ACL MAC-Regel

[Netzicherheit > 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 folgenden Kriterien zu filtern:

- Quell- oder Ziel-MAC-Adresse eines Datenpakets

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Schaltflächen

 Hinzufügen

Öffnet das Fenster *Erzeugen*, um eine Tabellenzeile hinzuzufügen.

- Im Feld *Gruppenname* legen Sie den Namen der Access-Control-Liste fest, der die Regel angehört. Wenn Sie einen neuen Namen hinzufügen, klicken Sie das Symbol **+**.
- 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 Indexwert zuerst an.

 Löschen

Entfernt die ausgewählte Tabellenzeile.

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. Sie legen die Indexnummer fest, wenn Sie eine Tabellenzeile hinzufügen.

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 abhängig vom Wert in den folgenden Feldern an:

- `Quelle MAC-Adresse`
- `Ziel MAC-Adresse`

Quelle 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.

Log

Aktiviert/deaktiviert die Protokollierung in der Log-Datei. Siehe Dialog [Diagnose > Bericht > System-Log](#).

Mögliche Werte:

`markiert`

Die Protokollierung ist aktiv.

Voraussetzung ist, dass im Dialog [Netzsicherheit > ACL > Zuweisung](#) die Access-Control-Liste einem VLAN oder Port zugewiesen ist.

Das Gerät protokolliert in der Log-Datei im Intervall von 30s, wie viele Male es eine Deny-Regel auf MAC-Datenpakete angewendet hat.

`unmarkiert` (Voreinstellung)

Die Protokollierung ist inaktiv.

Das Gerät ermöglicht Ihnen, für bis zu 128 Deny-Regeln diese Funktion zu aktivieren.

4.6.3 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 eine aktive Tabellenzeile 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Schaltflächen



Hinzufügen

Öffnet das Fenster *Erzeugen*, um einem Port oder einem VLAN eine Regel zuzuweisen.

- Im Feld *Port/VLAN* legen Sie die Nummer des Ports oder die VLAN-ID fest, auf welche das Gerät die Regel anwendet.
- Im Feld *Priorität* legen Sie die Reihenfolge fest, in der das Gerät die Regeln auf den Datenstrom anwendet.
- Im Feld *Richtung* legen Sie fest, ob das Gerät die Regel auf empfangene oder zu sendende Datenpakete anwendet.
- Im Feld *Gruppenname* legen Sie fest, welche Regel das Gerät dem Port oder dem VLAN zuweist.



Löschen

Entfernt die ausgewählte Tabellenzeile.

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. Das Gerät kann die Access-Control-Listen ausschließlich auf empfangene Datenpakete anwenden.

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. 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.

Mögliche Werte:

`1..4294967295`

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.

5 Switching

Das Menü enthält die folgenden Dialoge:

- Switching Global
- Lastbegrenzer
- Filter für MAC-Adressen
- IGMP-Snooping
- 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
- Funktion *VLAN-Unaware Modus* aktivieren

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 IEEE 802.3 definierte Flusskontrollmechanismus sorgt dafür, dass durch einen Pufferüberlauf auf einem Port keine Datenpakete verloren gehen. Kurz bevor der Pufferspeicher eines Ports 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 dann für die Dauer der Signalisierung keine Datenpakete. Auf Uplink-Ports führt dies möglicherweise zu unerwünschten Sendepausen im übergeordneten Netzsegment („Wandering Backpressure“). Der Flusskontrollmechanismus verringert das Netz somit auf die Bandbreite, die das langsamste Gerät im Netz verarbeiten kann.

Gemäß IEEE 802.1Q leitet das Gerät Datenpakete mit VLAN-Tag in einem VLAN 1 weiter. Einige wenige Anwendungen auf angeschlossenen Endgeräten allerdings senden oder empfangen Datenpakete mit einer VLAN-ID=0. Datenpakete mit einer VLAN-ID=0 heißen *Priority Tagged Frames*. Wenn das Gerät ein solches Datenpaket empfängt, überschreibt es vor dem Weiterleiten den ursprünglichen Wert im Datenpaket mit der VLAN-ID des empfangenden Ports.

Wenn Sie die Funktion *VLAN-Unaware Modus* aktivieren, dann deaktivieren Sie damit die VLAN-Einstellungen im Gerät. Das Gerät leitet dann die Datenpakete transparent weiter und wertet ausschließlich die im Datenpaket enthaltene Prioritätsinformation aus.

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.

VLAN-Unaware Modus

Aktiviert/deaktiviert den Modus, in dem das Gerät die VLAN-ID ignoriert und die Datenpakete unverändert vermittelt. Das Gerät wertet weiterhin die Prioritätsinformation in den Datenpaketen aus.

Auf den angeschlossenen Endgeräten erfordern lediglich einige wenige Anwendungen Empfangen von Datenpaketen mit einer VLAN-ID=0. Wenn die Anwendungen im Netz dies erfordern, dann aktivieren Sie die Funktion.

Mögliche Werte:

markiert

Das Gerät arbeitet gemäß IEEE 802.1Q im Modus *VLAN-unaware*:

- Das Gerät ignoriert die VLAN-Einstellungen im Gerät und die VLAN-ID in den Datenpaketen. Das Gerät vermittelt die Datenpakete anhand ihrer Ziel-MAC-Adresse.
- Das Gerät wertet die im VLAN-Tag der Datenpakete enthaltene Prioritätsinformation aus.
- Das Gerät ignoriert die in den Dialogen [Switching > VLAN > Konfiguration](#) und [Switching > VLAN > Port](#) festgelegten VLAN-Einstellungen.

Anmerkung: Legen Sie für jede Funktion im Gerät, die VLAN-Einstellungen nutzt, die VLAN-ID 1 fest. Dies betrifft unter anderem statische Filter, MRP und IGMP-Snooping.

[unmarkiert](#) (Voreinstellung)

Das Gerät arbeitet gemäß IEEE 802.1Q im Modus *VLAN-aware*:

- Das Gerät wertet das VLAN-Tag in den Datenpaketen aus.
- Das Gerät vermittelt die Datenpakete anhand ihrer Ziel-MAC-Adresse oder Ziel-IP-Adresse im jeweiligen VLAN.
- Das Gerät wertet die im Datenpaket enthaltene Prioritätsinformation aus.
- Wenn das Gerät ein Datenpaket mit einer VLAN-ID=0 empfängt, weist es dem Datenpaket die VLAN-ID des Ports zu. Siehe Dialog [Switching > VLAN > Port](#).

5.2 Lastbegrenzer

[Switching > Lastbegrenzer]

Das Gerät ermöglicht Ihnen, die Anzahl der Datenpakete an den Ports zu begrenzen, um auch bei hohem Datenaufkommen einen stabilen Betrieb zu ermöglichen. Wenn die Anzahl der Datenpakete auf einem Port den Schwellenwert überschreitet, dann verwirft das Gerät die überschüssigen Datenpakete 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 die Anzahl der Datenpakete auf einem Port den festgelegten Schwellenwert überschreitet, dann verwirft das Gerät die überschüssigen Datenpakete auf diesem Port.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Port

Zeigt die Nummer des Ports.

Schwellenwert

Legt den Grenzwert fest für Broadcast-, Multicast- und Unicast-Datenpakete auf diesem Port:

Mögliche Werte:

0 (Voreinstellung)

Die Funktion *Lastbegrenzer* ist auf diesem Port deaktiviert.

1..24414 bei 100 Mbit/s

1..244140 bei 1000 Mbit/s

Wenn in Spalte *Einheit* der Wert *Prozent* festgelegt ist, dann legen Sie einen prozentualen Wert zwischen 1 und 100 fest.

Wenn in Spalte *Einheit* der Wert *pps* festgelegt ist, dann legen Sie einen absoluten Wert fest. Die Lastbegrenzerfunktion berechnet den Grenzwert auf Grundlage von 512 Byte großen Datenpaketen.

Anmerkung: Die tatsächlich zur Verfügung stehenden Betriebsmodi sind abhängig von der Ausstattung des Geräts und vom verwendeten Modul.

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.

Multicast Modus

Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene Multicast-Datenpakete.

Mögliche Werte:

`markiert`

`unmarkiert` (Voreinstellung)

Bei Überschreiten des Grenzwerts verwirft das Gerät auf diesem Port die Überlast an Multicast-Datenpaketen.

Unknown unicast mode

Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene Unicast-Datenpakete mit unbekannter Zieladresse.

Mögliche Werte:

`markiert`

`unmarkiert` (Voreinstellung)

Bei Überschreiten des Grenzwerts verwirft das Gerät auf diesem Port die Überlast an Unicast-Datenpaketen.

[Ausgang]

In dieser Registerkarte legen Sie die Übertragungsrate für den Ausgang des Ports fest.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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.

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 Tabellenzeile 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 die Zieladresse eines Datenpakets enthält, dann vermittelt das Gerät das Datenpaket vom Empfangsport an den in der Tabellenzeile festgelegten 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 leeren](#).

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

Schaltflächen



Hinzufügen

Öffnet das Fenster [Erzeugen](#), um eine Tabellenzeile hinzuzufügen.

- Im Feld [MAC-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 festgelegten Ziel-MAC-Adresse.



Löschen

Entfernt die ausgewählte Tabellenzeile.



MAC-Adresstabelle leeren

Entfernt aus der Forwarding-Tabelle (FDB) die MAC-Adressen, die in Spalte [Status](#) den Wert [Learned](#) haben.

Adresse

Zeigt die Ziel-MAC-Adresse, für welche die Tabellenzeile gilt.

VLAN-ID

Zeigt die ID des VLANs, für das die Tabellenzeile 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.

Mgmt

MAC-Adresse des Geräts. Der Adressfilter ist gegen Veränderungen geschützt.

Other

Statische Adresse, hinzugefügt durch die folgende Funktion:

– *802.1X*

– *Port-Sicherheit*

Permanent

Adressfilter manuell eingerichtet. Der Adressfilter bleibt dauerhaft eingerichtet.

GMRP

Multicast-Adressfilter automatisch eingerichtet durch GMRP.

IGMP

Adressfilter automatisch eingerichtet durch IGMP-Snooping.

MRP-MMRP

Multicast-Adressfilter automatisch eingerichtet durch MMRP.

<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.

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 eine Tabellenzeile im Dialog [Switching > Filter für MAC-Adressen](#). Das Gerät entfernt die Tabellenzeile, wenn der Multicast-Empfänger die Multicast-Gruppe verlässt.

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

Schaltflächen



IGMP-Snooping Zähler zurücksetzen

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

Verarbeitete Multicast Controls

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:

$0 \dots 2^{31} - 1$

Mit der Schaltfläche *IGMP-Snooping Daten leeren* 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.

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

VLAN-ID

Zeigt die ID des VLANs, für das die Tabellenzeile gilt.

Aktiv

Aktiviert/deaktiviert die Funktion *IGMP-Snooping* für dieses VLAN.

Voraussetzung ist, dass die Funktion *IGMP-Snooping* global eingeschaltet 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-Gruppenmitglieder 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)

Admin-Modus Fast-Leave

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)

[Port]

In dieser Registerkarte konfigurieren Sie die Funktion *IGMP-Snooping* für jeden Port.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert die Funktion *IGMP-Snooping* auf dem Port.

Voraussetzung ist, dass die Funktion *IGMP-Snooping* global eingeschaltet 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-Gruppenmitglieder 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
unbegrenzt Time-Out, keine Ablaufzeit
- 1..3600 (Voreinstellung: 260)

Admin-Modus Fast-Leave

Aktiviert/deaktiviert die Fast-Leave-Funktion auf dem 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.

Statischer Query-Port

Aktiviert/deaktiviert den *Statischer Query-Port*-Modus.

Mögliche Werte:

- markiert
Der *Statischer Query-Port*-Modus ist aktiv.
Der Port ist ein statischer Query-Port in den eingerichteten VLANs.
- unmarkiert (Voreinstellung)
Der *Statischer 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 welche die Tabellenzeile gilt.

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Schaltflächen



Wizard

Öffnet das Fenster *Wizard*, das Sie beim Auswählen und Einrichten der Ports unterstützt. Siehe „[\[Wizard: IGMP-Snooping Erweiterungen\]](#)“ auf Seite 191.

VLAN-ID

Zeigt die ID des VLANs, für das die Tabellenzeile 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 auf der Seite *Konfiguration* das Kontrollkästchen *Statisch*.

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 Hirschmann-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 auf der Seite *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 auf der Seite *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.

Mögliche Werte:

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 “-”.

[Wizard: IGMP-Snooping Erweiterungen]

Das Fenster *Wizard* unterstützt Sie beim Auswählen und Konfigurieren der Ports.

Das Fenster *Wizard* führt Sie durch die folgenden Schritte:

- *Selection VLAN/Port*
- *Konfiguration*

Nach Schließen des Fensters *Wizard* klicken Sie die Schaltfläche ✓, um Ihre Einstellungen zu speichern.

Selection VLAN/Port

VLAN-ID

Auswahl der ID des VLANs.

Port

Auswahl der Ports.

Konfiguration

VLAN-ID

Zeigt die ID des ausgewählten VLANs.

Port

Zeigt die Nummer der ausgewählten Ports.

Statisch

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 Hirschmann-Geräte (*Automatic*) zu senden.

Learn by LLDP

Legt den Status *Learn by LLDP* für den Port fest. Ermöglicht dem Gerät, direkt verbundene Hirschmann-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 vermittelt einen Multicast-Stream lediglich an die Ports, an denen ein Multicast-Empfänger angeschlossen ist.

Um zu erkennen, an welchen Ports Multicast-Empfänger angeschlossen sind, sendet das Gerät auf den Ports in einem bestimmten Intervall Query-Datenpakete. 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.

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

VLAN-ID

Zeigt die ID des VLANs, für das die Tabellenzeile 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.

IP-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 (Voreinstellung)
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.

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 vermittelt auch Datenpakete mit bekannten Multicast-Adressen an die Query-Ports.

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.

query ports

Das Gerät vermittelt Datenpakete mit unbekannter MAC-/IP-Multicast-Adresse an die Query-Ports.

Tabelle

In der Tabelle legen Sie die Einstellungen für bekannte Multicasts für die eingerichteten VLANs fest.

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

VLAN-ID

Zeigt die ID des VLANs, für das die Tabellenzeile 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 einer bekannten MAC-/IP-Multicast-Adresse an die Query-Ports und an registrierte Ports.

an registrierte Ports senden (Voreinstellung)

Das Gerät vermittelt Datenpakete mit einer bekannten MAC-/IP-Multicast-Adresse an registrierte Ports.

5.5 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 der IEEE-Normungsausschuss 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 beschränken. Um den Verkehr zu beschränken, 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 Datenpakete 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](#)

5.5.1 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: $(2 \times \text{JoinTime}) + 60$.
- Um das Aufkommen an wiederkehrenden Datenpaketen nach einem LeaveAll-Ereignis zu minimieren, legen Sie den Wert für den LeaveAll-Timer größer als den LeaveTime-Wert fest.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

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)

5.5.2 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 existiert 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

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.

[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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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 vermittelt die Datenpakete, welche für die im MMRP registrierten Multicast-MAC-Adressen bestimmt sind, in das VLAN. Das Gerät vermittelt die Datenpakete an Ports, die MMRP dynamisch eingerichtet hat, oder an Ports, 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 Datenpakete, 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.

[Statistiken]

Geräte in einem LAN tauschen Multiple MAC Registration Protocol Data Units (MMRPDUs) aus, um die Geräte-Status an einem aktiven MMRP-Port aufrecht zu erhalten. Diese Registerkarte ermöglicht Ihnen, für jeden Port die Statistiken der vermittelten MMRP-Datenpakete zu überwachen.

Information

Schaltflächen

 Statistiken zurücksetzen

Setzt die Zähler der Port-Statistiken und die Werte in Spalte [Letzte empfangene MAC-Adresse](#) zurück.

MMRP-PDU gesendet

Zeigt die Anzahl der an das Gerät übermittelten MMRPDUs.

MMRP-PDU empfangen

Zeigt die Anzahl der vom Gerät empfangenen MMRPDUs.

Bad-Header PDU empfangen

Zeigt die Anzahl der vom Gerät empfangenen MMRPDUs mit fehlerhaftem Header.

Bad-Format PDU empfangen

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter [„Arbeiten mit Tabellen“](#) auf Seite 16.

Port

Zeigt die Nummer des Ports.

MMRP-PDU gesendet

Zeigt die Anzahl der an den Port übermittelten MMRPDUs.

MMRP-PDU empfangen

Zeigt die Anzahl der vom Port empfangenen MMRPDUs.

Bad-Header PDU empfangen

Zeigt die Anzahl der vom Port empfangenen MMRPDUs mit fehlerhaftem Header.

Bad-Format PDU empfangen

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 MVRPDUs empfangen hat.

5.5.3 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 existiert 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

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 MVRP aus.

Eingeschränkte VLAN-Registrierung

Aktiviert/deaktiviert die Funktion *Eingeschränkte VLAN-Registrierung* 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 *Eingeschränkte VLAN-Registrierung* auf diesem Port aus.

[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 MVRP-Datenpakete zu überwachen.

Information

Schaltflächen

 Statistiken zurücksetzen

Setzt die Zähler der Port-Statistiken und die Werte in Spalte *Letzte empfangene MAC-Adresse* zurück.

MVRP-PDU gesendet

Zeigt die Anzahl der an das Gerät übermittelten MVRPDUs.

MVRP-PDU empfangen

Zeigt die Anzahl der vom Gerät empfangenen MVRPDUs.

Bad-Header PDU empfangen

Zeigt die Anzahl der vom Gerät empfangenen MVRPDUs mit fehlerhaftem Header.

Bad-Format PDU empfangen

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.

Fehler Message-Queue

Zeigt die Anzahl der vom Gerät blockierten MVRPDUs.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

Port

Zeigt die Nummer des Ports.

MVRP-PDU gesendet

Zeigt die Anzahl der an den Port übermittelten MVRPDUs.

MVRP-PDU empfangen

Zeigt die Anzahl der vom Port empfangenen MVRPDUs.

Bad-Header PDU empfangen

Zeigt die Anzahl der vom Gerät auf dem Port empfangenen MVRPDUs mit fehlerhaftem Header.

Bad-Format PDU empfangen

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.

5.6 GARP

[Switching > GARP]

Das Generic Attribute Registration Protocol (GARP) wurde durch den IEEE-Normungsausschuss definiert, um ein generisches Framework bereitzustellen, in welchem Switches Attributwerte registrieren und wieder austragen, zum Beispiel VLAN-Kennungen und Multicast-Gruppen-Mitgliedschaften.

Wird ein Attribut für einen Teilnehmer gemäß dem GARP registriert oder wieder ausgetragen, 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](#)

5.6.1 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 802.1D 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 unbekanntenen Multicast-Daten, die entweder geflutet oder verworfen werden sollen.

Mögliche Werte:

discard

Das Gerät verwirft unbekanntene Multicast-Daten.

flood (Voreinstellung)

Das Gerät vermittelt unbekanntene Multicast-Daten an jeden Port.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Port

Zeigt die Nummer des Ports.

GMRP aktiv

Aktiviert/deaktiviert die Teilnahme des Ports an *GMRP*.

Voraussetzung ist, dass die Funktion *GMRP* global eingeschaltet 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.

5.6.2 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 unbekanntes 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 ausgeschaltet ist, dann ignoriert das Gerät **GVRP**-Nachrichten.

Mögliche Werte:

An

Die Funktion **GVRP** ist eingeschaltet.

Aus (Voreinstellung)

Die Funktion **GVRP** ist ausgeschaltet.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Port

Zeigt die Nummer des Ports.

GVRP aktiv

Aktiviert/deaktiviert die Teilnahme des Ports an **GVRP**.

Voraussetzung ist, dass die Funktion **GVRP** global eingeschaltet ist.

Mögliche Werte:

markiert (Voreinstellung)

Die Teilnahme des Ports an **GVRP** ist aktiv.

unmarkiert

Die Teilnahme des Ports an **GVRP** ist inaktiv.

5.7 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](#)

5.7.1 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 (*Verkehrsklasse* nach IEEE 802.1D).

5.7.2 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

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

5.7.3 802.1D/p Zuweisung

[Switching > QoS/Priority > 802.1D/p Zuweisung]

Das Gerät vermittelt Datenpakete mit VLAN-Tag anhand der enthaltenen QoS-/Priorisierungsinformation mit höherer oder mit niedrigerer Priorität.

In diesem Dialog weisen Sie jeder VLAN-Priorität eine *Verkehrsklasse* zu. Die *Verkehrsklassen* sind den Warteschlangen der Ports (Prioritäts-Queues) fest zugewiesen.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

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*.

Werkseitige Zuweisung der VLAN-Priorität zu Verkehrsklassen

VLAN-Priorität	Verkehrsklasse	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
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

5.7.4 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

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.

Werkseitige Zuweisung der DSCP-Werte zu Verkehrsklassen

DSCP-Wert	DSCP-Name	Verkehrsklasse
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
40	CS5	5
41,42,43,44,45,47		5
46	EF	5

DSCP-Wert	DSCP-Name	Verkehrsklasse
48	CS6	6
49-55		6
56	CS7	7
57-63		7

5.7.5 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.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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%.

5.8 VLAN

[Switching > VLAN]

Mit VLAN (Virtual Local Area Network) verteilen Sie die Datenpakete im physischen Netz auf logische Teilnetze. Das bietet Ihnen folgende Vorteile:

- Hohe Flexibilität
 - Mit VLAN verteilen Sie den Datenpakete 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 der Datenpakete auf einzelne logische Netze erschwert ungewolltes Abhören und härtet das System gegen Angriffe, wie MAC-Flooding oder MAC-Spoofing.

Das Gerät unterstützt gemäß IEEE 802.1Q paketbasierte „tagged“ VLANs. Das VLAN-Tag im Datenpaket kennzeichnet, zu welchem VLAN das Datenpaket gehört.

Das Gerät vermittelt die markierten Datenpakete eines VLANs ausschließlich an 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](#)

5.8.1 VLAN Global

[Switching > VLAN > Global]

Dieser Dialog ermöglicht Ihnen, sich allgemeine VLAN-Parameter des Geräts anzusehen.

Konfiguration

Schaltflächen

 VLAN-Einstellungen zurücksetzen

Versetzt die VLAN-Einstellungen des Geräts in den Voreinstellung.

Beachten Sie, dass Sie Ihre Verbindung zum Gerät trennen, wenn Sie im Dialog [Grundeinstellungen > Netz > Global](#) die VLAN-ID für das Management des Geräts geändert haben.

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.

5.8.2 VLAN Konfiguration

[Switching > VLAN > Konfiguration]

In diesem Dialog verwalten Sie die VLANs. Um ein VLAN einzurichten, erzeugen Sie eine weitere Tabellenzeile. 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.

Anmerkung: Die Einstellungen sind ausschließlich dann wirksam, wenn die Funktion *VLAN-Unaware Modus* inaktiv ist. Siehe Dialog [Switching > Global](#).

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

Schaltflächen



Hinzufügen

Öffnet das Fenster *Erzeugen*, um eine Tabellenzeile hinzuzufügen.

Im Feld *VLAN-ID* legen Sie die ID des VLANs fest.



Löschen

Entfernt den ausgewählten Tabelleneintrag.

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*. Siehe Dialog *Netzsicherheit > 802.1X*.

permanent

VLAN eingerichtet durch den Benutzer.

oder

VLAN eingerichtet durch Funktion *MRP*. Siehe Dialog *Switching > L2-Redundanz > MRP*.

Wenn Sie die Einstellungen 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.

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.

5.8.3 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 bei inaktiver Funktion *VLAN-Unaware Modus* Datenpakete vermittelt, 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.

Anmerkung: Die Einstellungen sind ausschließlich dann wirksam, wenn die Funktion *VLAN-Unaware Modus* inaktiv ist. Siehe Dialog *Switching > Global*.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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* ist der Wert *admitAll* festgelegt.

Mögliche Werte:

- *1..4042* (Voreinstellung: *1*)
ID eines bereits eingerichteten VLANs

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 Eingangsfilerung.

Mögliche Werte:

`markiert`

Die Eingangsfilerung 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 Eingangsfilerung ist inaktiv.

Das Gerät vermittelt empfangene Datenpakete, ohne die VLAN-ID zu vergleichen. Demzufolge vermittelt das Gerät auch Datenpakete in VLANs, in denen der Port nicht Mitglied ist.

5.8.4 VLAN Voice

[Switching > VLAN > Voice]

Verwenden Sie die Voice-VLAN-Funktion, um auf einem Port die Sprach- und Datenpakete bezüglich VLAN und/oder Priorität zu trennen. Ein wesentlicher Nutzen von Voice-VLAN ist, bei hoher Auslastung des Ports 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 mittels LLDP-MED vom Gerät erhält. Infolgedessen sendet das VoIP-Telefon Sprachdatenpakete entweder mit VLAN-Tag, mit Prioritätsmarkierung oder ohne VLAN-Tag. 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 *Voice* des Geräts global ein/aus.

Mögliche Werte:

An

Aus (Voreinstellung)

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

Port

Zeigt die Nummer des Ports.

Modus Voice-VLAN

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 *Voice* für diese Tabellenzeile.

kein

Ermöglicht dem IP-Telefon, seine eigene Konfiguration zum Senden von Sprachdatenpaketen ohne VLAN-Tag 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.

Modus Data-Priority

Legt den Trust-Modus für die Datenpakete auf dem jeweiligen Port fest.

Das Gerät verwendet diesen Modus für Datenpakete im Voice-VLAN, wenn es ein VoIP-Telefon und einen PC erkennt, die das gleiche Kabel für die Datenübertragung verwenden.

Mögliche Werte:

trust (Voreinstellung)

Die Datenpakete haben normale Priorität, wenn Sprachdatenpakete auf dem Interface anliegen.

untrust

Die Datenpakete haben die Priorität 0, wenn Sprachdatenpakete auf dem Interface anliegen und in Spalte *Modus Voice-VLAN* der Wert *dot1p-priority* festgelegt ist. 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 die Tabellenzeile gilt. Um die Datenpakete an diese VLAN-ID unter Verwendung dieses Filters weiterzuleiten, legen Sie in Spalte *Modus Voice-VLAN* den Wert *vlan* fest.

Mögliche Werte:

1..4042 (Voreinstellung: *1*)

Priorität

Legt die Voice-VLAN-Priorität des Ports fest.

Voraussetzungen:

- In Spalte *Modus Voice-VLAN* ist der Wert *dot1p-priority* festgelegt.

Mögliche Werte:

0..7

kein

Deaktiviert die Voice-VLAN-Priorität des Ports.

DSCP

Legt den IP-DSCP-Wert fest.

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-Precedence-Modell.

Im Dialog *Switching > QoS/Priority > IP-DSCP-Zuweisung* weisen Sie jedem IP-DSCP-Wert eine *Verkehrsklasse* zu.

Bypass-Authentifizierung

Aktiviert den Voice-VLAN-Authentifizierungsmodus.

Wenn Sie die Funktion deaktivieren und den Wert in Spalte *Modus Voice-VLAN* auf *dot1p-priority* setzen, benötigen Sprachgeräte eine Authentifizierung.

Mögliche Werte:

markiert (Voreinstellung)

Wenn die Funktion im Dialog *Netzicherheit > 802.1X > 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 *Netzicherheit > 802.1X > Global*.

unmarkiert

5.9 L2-Redundanz

[Switching > L2-Redundanz]

Das Menü enthält die folgenden Dialoge:

- MRP
- Spanning Tree
- Link-Aggregation
- Link-Backup
- FuseNet

5.9.1 MRP

[Switching > L2-Redundanz > MRP]

Das Media Redundancy Protocol (MRP) ist ein Protokoll, das Ihnen den Aufbau hochverfügbarer, ringförmiger Netzstrukturen ermöglicht. Ein MRP-Ring mit Hirschmann-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.

Das *Ring-Manager*-Gerät 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*.

Funktion

Schaltflächen



Lösche Ring-Konfiguration

Schaltet die Redundanzfunktion aus und setzt alle Einstellungen im Dialog die voreingestellten Werte zurück.

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 das *Ring-Manager*-Gerät auf den primären Ring-Port zurück.

unmarkiert (Voreinstellung)

Die Backup-Funktion für *Ring-Port 2* ist deaktiviert. Ist der Ring geschlossen, sendet das *Ring-Manager*-Gerät 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*.

Um unerwartetes Verhalten zu vermeiden, schalten Sie die Funktion nicht auf einem Gerät ein, auf dem die Funktion *RCP* eingeschaltet ist.

Aus (Voreinstellung)

Die Funktion *Ring-Manager* ist ausgeschaltet.

Das Gerät arbeitet ausschließlich als *Ring-Client*.

Advanced-Modus

Aktiviert/deaktiviert den *Advanced-Modus* für schnelle Umschaltzeiten.

Mögliche Werte:

`markiert` (Voreinstellung)

Advanced-Modus aktiv.

MRP-fähige Hirschmann-Geräte unterstützen diesen Modus.

`unmarkiert`

Advanced-Modus inaktiv.

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.

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 eine Tabellenzeile für das VLAN und weist den Ring-Ports den Wert `Tzu`.

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.

5.9.2 Spanning Tree

[Switching > L2-Redundanz > Spanning Tree]

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 Port](#)

5.9.21 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 (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 numerischen 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 numerischen 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:

$$\text{Forward-Verzögerung [s]} = (\text{Max age}/2) + 1$$

Wenn Sie in die Felder einen Wert eingeben, 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, also 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, das 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 Kontrollkästchens *BPDU-Guard* auf.

Um den Port wieder einzuschalten, verwenden Sie die Funktion *Auto-Disable*. Alternativ dazu 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 3x pro Periode.
- Der Dialog [Diagnose > Ports > Auto-Disable](#) zeigt, welche Ports aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet sind.
- Nach einer Wartezeit schaltet die Funktion *Auto-Disable* 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

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 Verzögerungszeit 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 bereitgestellte maximal zulässige Astlänge fest, also 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`

Das Gerät übernimmt die Rolle der Root-Bridge.

`1..200000000`

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>`

5.9.2.2 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Port

Zeigt die Nummer des Ports.

STP aktiv

Aktiviert/deaktiviert die Funktion *Spanning Tree* auf dem Port.

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 abhängig von der Datenrate des Ports.

Port-Priorität

Legt die Priorität des Ports fest.

Mögliche Werte:

0..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 erkannten 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-BPDU 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 erkannten 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-BPDU 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 erkannten 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-BPDU 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 $1,5 \times \text{Hello-Time [s]}$ in den Zustand *forwarding* (in der Voreinstellung $1,5 \times 2$ 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 ermöglicht 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.

[Guards]

Diese Registerkarte ermöglicht Ihnen, an den Ports die Einstellungen für verschiedene Schutzfunktionen festzulegen.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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, das 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 $2 \times$ *Hello-Time [s]* zurück.

unmarkiert (Voreinstellung)

Überwachung auf STP-BPDUs ist inaktiv.

TCN-Guard

Aktiviert/deaktiviert die Überwachung von *Topology Change*-Meldungen auf dem Port. Mit dieser Einstellung hilft das Gerät, das Netz vor Angriffen mit STP-BPDUs zu schützen, die versuchen, die Topologie zu verändern.

Mögliche Werte:

`markiert`

Die Überwachung von *Topology Change*-Meldungen ist aktiv.

- 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)

Die Überwachung von *Topology Change*-Meldungen ist inaktiv.

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 [Switching > L2-Redundanz > Spanning Tree > 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 Kontrollkästchens [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](#).

5.9.3 Link-Aggregation

[Switching > L2-Redundanz > Link-Aggregation]

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Schaltflächen



Hinzufügen

Öffnet das Fenster *Erzeugen*, um eine Tabellenzeile für ein LAG-Interface hinzuzufügen oder um 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.



Löschen

Entfernt die ausgewählte Tabellenzeile.

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 nicht betriebsbereit.

`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.

`unmarkiert`

Das LAG-Interface ist inaktiv.

STP aktiv

Aktiviert/deaktiviert das *Spanning Tree*-Protokoll auf diesem LAG-Interface. Voraussetzung ist, dass im Dialog *Switching > L2-Redundanz > Spanning Tree > Global* die Funktion *Spanning Tree* eingeschaltet ist.

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.

Track-Name

Zeigt den Namen des Tracking-Objekts, der sich aus den in Spalte *Typ* und Spalte *Track-ID* angezeigten Werten zusammensetzt.

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:

statisch

Das LAG-Interface arbeitet mit der Funktion *Statische Link-Aggregation*.

dynamisch

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. Voraussetzung ist, dass im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.

Wenn das Gerät eine Link-Status-Änderung erkennt, sendet es einen SNMP-Trap.

unmarkiert

Das Senden von SNMP-Traps ist inaktiv.

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 des 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 LACPDU's 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 LACPDU's zyklisch, andernfalls bei Bedarf.

`STO`

(Status `LACP_Timeout`)

Wenn ausgewählt, vermittelt der Link die LACPDU's 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 IEEE 802.1AX-2014.

LACP actor oper state

Zeigt die Statuswerte des Aktors, die das LAG-Interface in den LACPDU's vermittelt.

Mögliche Werte:

`ACT`

(Status `LACP_Activity`)

Wenn sichtbar, vermittelt der Link die LACPDU's zyklisch, andernfalls bei Bedarf.

STO

(Status *LACP_Timeout*)

Wenn sichtbar, vermittelt der Link die LACPDU's 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 LACPDU's 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 IEEE 802.1AX-2014.

5.9.4 Link-Backup

[Switching > L2-Redundanz > Link-Backup]

Mit Link Backup konfigurieren Sie Paare von redundanten Links. Jedes Paar besteht aus einem primären Port und einem Backup-Port. Der primäre Port leitet die Datenpakete weiter, bis das Gerät einen Fehler ermittelt. Wenn das Gerät einen Fehler auf dem primären Port ermittelt, vermittelt die Link-Backup-Funktion die Datenpakete über den Backup-Port.

Der Dialog ermöglicht Ihnen außerdem, eine Fail-Back-Funktion einzurichten. Wenn Sie die Funktion *Fail back* aktivieren und der primäre Port in den Normalbetrieb zurückkehrt, blockiert das Gerät zunächst die Datenpakete am Backup-Port und vermittelt die Datenpakete dann an den primären Port. 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Schaltflächen

 Hinzufügen

Fügt eine Tabellenzeile hinzu.

 Löschen

Entfernt die ausgewählte Tabellenzeile.

Primärer Port

Zeigt den primären Port des Interface-Paares. Wenn Sie die Funktion Link-Backup einschalten, ist dieser Port für die Weiterleitung der Datenpakete verantwortlich.

Mögliche Werte:

Physische Ports

Backup-Port

Zeigt den Backup-Port, an den das Gerät die Datenpakete vermittelt, wenn es auf dem primären Port einen Fehler erkennt.

Mögliche Werte:

Physische 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, Weiterleitung der Datenpakete.

blocking

Der Link ist vorhanden, keine Abschaltung, keine Weiterleitung der Datenpakete.

down

Das Kabel ist ausgesteckt, der Port ist ausgeschaltet, die Verbindung auf dem Port ist unterbrochen, oder eine Funktion im Gerät hat den Port ausgeschaltet.

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, Weiterleitung der Datenpakete.

blocking

Der Link ist vorhanden, keine Abschaltung, keine Weiterleitung der Datenpakete.

down

Das Kabel ist ausgesteckt, der Port ist ausgeschaltet, die Verbindung auf dem Port ist unterbrochen, oder eine Funktion im Gerät hat den Port ausgeschaltet.

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 der 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 die Datenpakete 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 der 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 Datenpakete entsprechend der Paar-Konfiguration weiter.

`unmarkiert` (Voreinstellung)

Das Link-Backup-Paar ist deaktiviert. Die Ports leiten die Datenpakete entsprechend den Grundeinstellungen weiter.

Erzeugen

Primärer Port

Legt den primären Port des Backup-Interface-Paares fest. Im Normalbetrieb ist dieser Port verantwortlich für die Weiterleitung der Datenpakete.

Mögliche Werte:

Physische Ports

Backup-Port

Legt den Backup-Port fest, an den das Gerät die Datenpakete vermittelt, wenn es auf dem primären Port einen Fehler ermittelt.

Mögliche Werte:

Physische Ports außer dem Port, den Sie als primären Port festlegen.

5.9.5 FuseNet

[Switching > L2-Redundanz > FuseNet]

Die *FuseNet*-Protokolle ermöglichen Ihnen, Ringe zu koppeln, die mit einem der folgenden Redundanzprotokolle arbeiten:

- MRP
- RSTP

Das Menü enthält die folgenden Dialoge:

[Sub-Ring](#)

5.9.5.1 Sub-Ring

[Switching > L2-Redundanz > FuseNet > Sub-Ring]

Dieser Dialog ermöglicht Ihnen, das Gerät so einzurichten, dass es als *Sub-Ring-Manager* arbeitet.

Die Funktion *Sub-Ring* ermöglicht Ihnen eine einfache Ankopplung von Netzsegmenten an bestehende Redundanz-Ringe. Das *Sub-Ring-Manager*-Gerät koppelt einen Sub-Ring an einen vorhandenen Ring (Base-Ring).

Sie können beliebige Geräte, die MRP unterstützen, als Teilnehmer in den Sub-Ring integrieren. Diese Geräte benötigen keine Unterstützung für die Funktion *Sub-Ring*.

Berücksichtigen Sie beim Einrichten von Sub-Ringen folgende Regeln:

- Das Gerät unterstützt *Link-Aggregation* im Sub-Ring
- Kein Spanning Tree auf Sub-Ring-Ports
- Gleiche *MRP-Domäne* auf Geräten innerhalb eines Sub-Rings
- Unterschiedliche VLANs für Base-Ring und Sub-Ring

Legen Sie die VLAN-Einstellungen wie folgt fest:

- VLAN *x* für Base-Ring
 - auf den Ring-Ports der am Base-Ring teilnehmenden Geräte
 - auf den Base-Ring-Ports des *Sub-Ring-Manager*-Geräts
- VLAN *y* für Sub-Ring
 - auf den Ring-Ports der am Sub-Ring teilnehmenden Geräte
 - auf den Sub-Ring-Ports des *Sub-Ring-Manager*-Geräts

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 Sub-Ringen, die das Gerät unterstützt.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Schaltflächen



Hinzufügen

Fügt eine Tabellenzeile hinzu.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Sub-Ring-ID

Zeigt die eindeutige Kennung des Sub-Rings.

Mögliche Werte:

1..8

Name

Legt den Namen des Sub-Rings fest (optional).

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Aktiv

Aktiviert/deaktiviert den Sub-Ring.

Aktivieren Sie den Sub-Ring, wenn die Konfiguration jedes am Sub-Ring teilnehmenden Geräts abgeschlossen ist. Schließen Sie den Sub-Ring erst, nachdem Sie die Funktion [Sub-Ring](#) aktiviert haben.

Mögliche Werte:

`markiert`

Der Sub-Ring ist aktiviert.

`unmarkiert` (Voreinstellung)

Der Sub-Ring ist inaktiv.

Status

Zeigt den Betriebszustand der Sub-Ring-Konfiguration.

Mögliche Werte:

`noError`

Das Gerät erkennt eine geeignete Sub-Ring-Konfiguration.

`ringPortLinkError`

– Der Ring-Port hat keine Datenverbindung.

– Eine der Sub-Ring-Leitungen ist verbunden mit einem weiteren Anschluss des Geräts. Jedoch ist die Sub-Ring-Leitung nicht verbunden mit einem der Ringports des Geräts.

multipleSRM

Das *Sub-Ring-Manager*-Gerät empfängt Datenpakete von mehr als einem *Sub-Ring-Manager*-Gerät im Sub-Ring.

noPartnerManager

Das *Sub-Ring-Manager*-Gerät empfängt seine eigenen Datenpakete.

concurrentVLAN

Das MRP-Protokoll im Basis-Ring verwendet das VLAN der *Sub-Ring-Manager*-Domäne.

concurrentPort

Ein weiteres Redundanzprotokoll verwendet den Ring-Port der *Sub-Ring-Manager*-Domäne.

concurrentRedundancy

Die *Sub-Ring-Manager*-Domäne ist inaktiv aufgrund eines weiteren aktiven Redundanzprotokolls.

trunkMember

Der Ring-Port der *Sub-Ring-Manager*-Domäne ist Mitglied einer *Link-Aggregation*-Verbindung.

sharedVLAN

Die *Sub-Ring-Manager*-Domäne ist inaktiv, weil Shared-VLAN aktiv ist und der Hauptring außerdem das MRP-Protokoll verwendet.

Redundanz

Zeigt, ob die Redundanz verfügbar ist.

Fällt eine Komponente des Sub-Rings aus, übernimmt die redundante Strecke deren Funktion.

Mögliche Werte:

redGuaranteed

Redundanz ist verfügbar.

redNotGuaranteed

Keine Redundanz verfügbar.

Port

Legt den Port fest, der das Gerät mit dem Sub-Ring verbindet.

Mögliche Werte:

<Port-Nummer>

SRM-Modus

Legt die Betriebsart des *Sub Ring Manager*-Geräts fest.

Jeweils 2 *Sub-Ring-Manager*-Geräte verbinden den Sub-Ring mit dem Base-Ring. So lange der Sub-Ring physisch geschlossen ist, blockiert ein *Sub-Ring-Manager*-Gerät seinen Sub-Ring-Port.

Mögliche Werte:

manager (Voreinstellung)

Der Sub-Ring-Port vermittelt Datenpakete.

Wenn dieser Wert auf beiden Geräten, die den Sub-Ring an den Base-Ring koppeln, eingestellt ist, arbeitet das Gerät mit der höheren MAC-Adresse als *redundantManager*.

redundantManager

Der Sub-Ring-Port ist blockiert, so lange der Sub-Ring physisch geschlossen ist. Bei einer Unterbrechung des Sub-Rings vermittelt der Sub-Ring-Port die Datenpakete. Wenn dieser Wert auf beiden Geräten, die den Sub-Ring an den Base-Ring koppeln, eingestellt ist, arbeitet das Gerät mit der höheren MAC-Adresse als *redundantManager*.

singleManager

Verwenden Sie diesen Wert, wenn der Sub-Ring über ein einziges Gerät an den Base-Ring gekoppelt ist. Voraussetzung sind 2 Instanzen des Sub-Rings in der Tabelle. Weisen Sie diesen Wert beiden Instanzen zu. Der Sub-Ring-Port der Instanz mit der höheren Port-Nummer ist blockiert, so lange der Sub-Ring physisch geschlossen ist.

SRM-Modus

Zeigt die gegenwärtige Betriebsart des *Sub-Ring-Manager*-Geräts.

Mögliche Werte:

manager

Der Sub-Ring-Port vermittelt Datenpakete.

redundantManager

Der Sub-Ring-Port ist blockiert, so lange der Sub-Ring physisch geschlossen ist. Bei einer Unterbrechung des Sub-Rings vermittelt der Sub-Ring-Port die Datenpakete.

singleManager

Der Sub-Ring ist über ein einziges Gerät an den Base-Ring gekoppelt. Dieses Gerät blockiert seinen Sub-Ring-Port mit der höheren Port-Nummer, solange der Sub-Ring physikalisch geschlossen ist.

disabled

Der Sub-Ring ist inaktiv.

Status Port

Zeigt den Verbindungsstatus des Sub-Ring-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 Verbindung auf dem Port ist unterbrochen.

VLAN

Legt das VLAN fest, dem dieser Sub-Ring zugewiesen ist. Wenn kein VLAN mit der festgelegten VLAN-ID existiert, dann erstellt das Gerät dieses automatisch.

Mögliche Werte:

Verfügbare eingerichtete VLANs (Voreinstellung: 0)

Wenn Sie für diesen Sub-Ring kein eigenständiges VLAN benutzen möchten, dann lassen Sie den Wert auf 0.

Partner-MAC

Zeigt die MAC-Adresse des *Sub-Ring-Manager*-Geräts am anderen Ende des Sub-Rings.

MRP-Domäne

Legt die MRP-Domäne des *Sub-Ring-Manager*-Geräts fest. Weisen Sie jedem Mitglied im Sub-Ring denselben MRP-Domänen-Namen zu. Wenn Sie ausschließlich Hirschmann-Geräte verwenden, übernehmen Sie den voreingestellten Wert für die MRP-Domäne; andernfalls passen Sie diesen Wert gegebenenfalls an. Bei mehreren Sub-Ringen ermöglicht Ihnen diese Funktion, für die Sub-Ringe 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`)

Protokoll

Legt das Protokoll fest.

Mögliche Werte:

`iec-62439-mrp`

6 Diagnose

Das Menü enthält die folgenden Dialoge:

- Statuskonfiguration
- System
- E-Mail-Benachrichtigung
- Syslog
- Ports
- LLDP
- Loop-Schutz
- 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 *Geräte-Status*.

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:

ok

error

Das Gerät zeigt diesen Wert, um einen ermittelten Fehler für eine der überwachten Parameter anzuzeigen.

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. Voraussetzung ist, dass im Dialog [Diagnose > Statuskonfiguration > Alarme \(Traps\)](#) die Funktion [Alarme \(Traps\)](#) eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.

Das Gerät sendet einen SNMP-Trap, wenn es an den überwachten Funktionen eine Änderung erkennt.

`unmarkiert`

Das Senden von SNMP-Traps ist inaktiv.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

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.

Temperatur

Aktiviert/deaktiviert die Überwachung der Temperatur im Gerät.

Mögliche Werte:

`markiert` (Voreinstellung)

Die Überwachung ist aktiv.

Wenn die Temperatur die festgelegten Schwellwerte überschreitet oder unterschreitet, wechselt der Wert im Rahmen [Geräte-Status](#) auf `error`.

`unmarkiert`

Die Überwachung ist inaktiv.

Die Temperaturschwellwerte legen Sie fest im Dialog [Grundeinstellungen > System](#), Feld [Obere Temp.-Grenze \[°C\]](#) und Feld [Untere Temp.-Grenze \[°C\]](#).

Ethernet-Modul entfernen

Aktiviert/deaktiviert die Überwachung der Module.

Mögliche Werte:

`markiert`

Die Überwachung ist aktiv.

Der Wert im Rahmen *Geräte-Status* wechselt auf `error`, wenn Sie ein Modul aus dem Gerät entfernen.

Weiter unten haben Sie die Möglichkeit, die zu überwachenden Module 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.

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.

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.

Ethernet-Modul

Aktiviert/deaktiviert die Überwachung dieses Moduls.

Mögliche Werte:

`markiert`

Die Überwachung ist aktiv.

Der Wert im Rahmen *Geräte-Status* wechselt auf `error`, wenn Sie das Modul aus dem Gerät entfernen.

`unmarkiert` (Voreinstellung)

Die Überwachung ist inaktiv.

Die Einstellung ist wirksam, wenn Sie weiter oben das Kontrollkästchen *Ethernet-Modul entfernen* markieren.

[Port]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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.

[Status]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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.

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:

ok

error

Das Gerät zeigt diesen Wert, um einen ermittelten Fehler für eine der überwachten Parameter anzuzeigen.

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. Voraussetzung ist, dass im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.

Das Gerät sendet einen SNMP-Trap, wenn es an den überwachten Funktionen eine Änderung erkennt.

unmarkiert (Voreinstellung)

Das Senden von SNMP-Traps ist inaktiv.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Passwort-Voreinstellung unverändert

Aktiviert/deaktiviert die Überwachung des Passworts für das lokal eingerichtete Benutzerkonto `admin`.

Mögliche Werte:

`markiert` (Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie für das Benutzerkonto `admin` das voreingestellte Passwort unverändert verwenden.

`unmarkiert`

Die Überwachung ist inaktiv.

Das Passwort legen Sie fest im Dialog *Gerätesicherheit > Benutzerverwaltung*.

Min. Passwort-Länge kürzer als 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 aktiv ist, haben Sie die Möglichkeit, während des Systemstarts mit einer seriellen Verbindung in den System-Monitor zu wechseln.

Mögliche Werte:

`markiert`

Die Überwachung ist aktiv.

Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie den System-Monitor aktivieren.

`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 aktiv 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 HiDiscovery möglich

Aktiviert/deaktiviert die Überwachung der Funktion HiDiscovery.

Mögliche Werte:

`markiert` (Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie die Funktion HiDiscovery einschalten.

`unmarkiert`

Die Überwachung ist inaktiv.

Die Funktion HiDiscovery schalten Sie im Dialog *Grundeinstellungen > Netz > Global* 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 `erste`.

`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 *Erweitert > 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.

[Port]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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.

[Status]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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.

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 in der Dropdown-Liste *Modus* der Eintrag *Manuelle Einstellung* ausgewählt ist.

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. Voraussetzung ist, dass im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.

Das Gerät sendet einen SNMP-Trap, wenn es an den überwachten Funktionen eine Änderung erkennt.

unmarkiert (Voreinstellung)

Das Senden von SNMP-Traps ist inaktiv.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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 festgelegten Schwellwerte überschreitet oder unterschreitet.

`unmarkiert`

Die Überwachung ist inaktiv.

Die Temperaturschwellwerte 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.

Ethernet-Modul entfernen

Aktiviert/deaktiviert die Überwachung der Module.

Mögliche Werte:

`markiert`

Die Überwachung ist aktiv.

Der Signalkontakt öffnet, wenn Sie ein Modul aus dem Gerät entfernen.

Weiter unten haben Sie die Möglichkeit, die zu überwachenden Module einzeln auszuwählen.

`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 Schicht-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.

Ethernet-Modul

Aktiviert/deaktiviert die Überwachung dieses Moduls.

Mögliche Werte:

`markiert`

Die Überwachung ist aktiv.

Der Signalkontakt öffnet, wenn Sie dieses Modul aus dem Gerät entfernen.

`unmarkiert` (Voreinstellung)

Die Überwachung ist inaktiv.

Die Einstellung ist wirksam, wenn Sie weiter oben das Kontrollkästchen [Ethernet-Modul entfernen](#) markieren.

[Port]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

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.

[Status]**Tabelle**

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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.

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: 1)

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

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.

Voraussetzung ist, dass im Dialog [Diagnose > Statuskonfiguration > Alarme \(Traps\)](#) die Funktion [Alarme \(Traps\)](#) eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.

[unmarkiert](#) (Voreinstellung)

Die Funktion [MAC-Benachrichtigung](#) ist auf dem Port inaktiv.

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

Status letzte MAC

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.

6.1.5 Alarme (Traps)

[Diagnose > Statuskonfiguration > Alarme (Traps)]

Das Gerät ermöglicht Ihnen das Senden eines SNMP-Traps als Reaktion auf bestimmte Ereignisse.

Die Ereignisse, bei denen das Gerät einen SNMP-Trap auslöst, legen Sie in den folgenden Dialogen fest:

- [Diagnose > Statuskonfiguration > Gerätestatus](#)
- [Diagnose > Statuskonfiguration > Sicherheitsstatus](#)
- [Diagnose > Statuskonfiguration > MAC-Benachrichtigung](#)

Das Menü enthält die folgenden Dialoge:

[Trap V3 Benutzerverwaltung](#)

[Trap Ziele](#)

6.1.5.1 Trap V3 Benutzerverwaltung

[Diagnose > Statuskonfiguration > Alarmer (Traps) > Trap V3 Benutzerverwaltung]

In diesem Dialog legen Sie die SNMPv3-Trap-Benutzer fest, welche SNMP-Traps an das/die Trap-Ziel(e) senden können. Das Gerät unterstützt verschlüsselte SNMPv3-Traps sowie Authentifizierung für das Senden.

SNMPv3-Trap-Benutzer haben die Berechtigung, SNMPv3-Traps an die festgelegten SNMPv3-Trap-Destinations zu senden.

SNMPv3-Trap-Benutzer sind ausschließlich für das Senden von SNMPv3-Traps an SNMPv3-Trap-Destinations bestimmt. Die SNMPv3-Trap-Benutzer unterscheiden sich von den im Gerät eingerichteten Benutzerkonten. Verwechseln Sie diese nicht. Siehe Dialog [Gerätesicherheit > Benutzerverwaltung](#).

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Schaltflächen



Hinzufügen

Öffnet das Fenster [Erzeugen](#), um eine Tabellenzeile hinzuzufügen. Das Gerät legt einen SNMPv3-Trap-Benutzer mit den Parametern an, die Sie in diesem Fenster festlegen.

- In der Dropdown-Liste [Zu klonender Benutzer](#) wählen Sie das Benutzerkonto, von dem das Gerät die Authentifizierungseinstellungen kloniert.
Wählen Sie obligatorisch eines der im Gerät eingerichteten Benutzerkonten aus. Benutzerkonten für das Gerät richten Sie im Dialog [Gerätesicherheit > Benutzerverwaltung](#) ein.
- Im Feld [Trap Benutzer Name](#) legen Sie den Namen für den SNMPv3-Trap-Benutzer fest.
Mögliche Werte:
Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen
- In der Dropdown-Liste [Trap Benutzer Auth Protokoll](#) wählen Sie das Protokoll für das Senden von SNMPv3-Traps mit Authentifizierung.
Mögliche Werte:
[kein](#)
Das Gerät sendet SNMPv3-Traps unverschlüsselt ohne Authentifizierung.
[hmacmd5](#)
Das Gerät sendet SNMPv3-Traps mittels des Protokolls Message-Digest Algorithm 5 (HMACMD5).
Verfügbar, wenn dieses Protokoll bereits für den zu klonenden Benutzer festgelegt ist.
[hmacsha](#)
Das Gerät sendet SNMPv3-Traps mittels des Protokolls Secure Hash Algorithm (HMACSHA).
Verfügbar, wenn dieses Protokoll bereits für den zu klonenden Benutzer festgelegt ist.
- Im Feld [Trap Benutzer Auth Passwort](#) legen Sie das Passwort fest, mit dem sich der SNMPv3-Trap-Benutzer vor dem Senden authentifiziert.
Mögliche Werte:
Alphanumerische ASCII-Zeichenfolge mit 8..64 Zeichen
Voraussetzung ist, dass in der Dropdown-Liste [Trap Benutzer Auth Protokoll](#) ein anderer Eintrag als [kein](#) ausgewählt ist.

- In der Dropdown-Liste *Trap Benutzer Priv Protokoll* wählen Sie das Protokoll, welches das Gerät für diesen Benutzer zur Verschlüsselung der SNMPv3-Traps verwendet.
Mögliche Werte:
 - kein* (Voreinstellung)
Keine Verschlüsselung.
 - des*
Data Encryption Standard (DES).
Verfügbar, wenn dieses Protokoll bereits für den zu klonenden Benutzer festgelegt ist.
 - aesCfb128*
Advanced Encryption Standard (AES).
Verfügbar, wenn dieses Protokoll bereits für den zu klonenden Benutzer festgelegt ist.
- Im Feld *Trap Benutzer Priv Passwort* legen Sie das Passwort fest, mit dem sich der SNMPv3-Trap-Benutzer vor dem Senden authentifiziert.
Mögliche Werte:
 - Alphanumerische ASCII-Zeichenfolge mit 8..64 Zeichen
 Voraussetzung ist, dass in der Dropdown-Liste *Trap Benutzer Auth Protokoll* ein anderer Eintrag als *kein* ausgewählt ist.

Wenn Sie die Schaltfläche *Ok* klicken, erzeugt das Gerät eine Tabellenzeile für den SNMPv3 trap-Benutzer. Wenn Sie in der Dropdown-Liste *Trap Benutzer Auth Protokoll* oder *Trap Benutzer Priv Protokoll* einen anderen Eintrag als *kein* gewählt haben, öffnet sich zunächst das Fenster *Anmeldeinformationen*. Dann geben Sie das/die erforderliche(n) Passwort(e) ein. Auch wenn Sie ein falsches Passwort eingeben, erzeugt das Gerät den SNMPv3-Trap-Benutzer. Wenn das Gerät SNMPv3-Traps sendet, kann das Trap-Ziel diese jedoch nicht entschlüsseln.



Löschen

Entfernt die ausgewählte Tabellenzeile.

SNMPv3 Notification Benutzer

Zeigt den Namen des SNMPv3-Trap-Benutzers.

Authentifizierung

Zeigt das Protokoll für das Senden von SNMPv3-Traps mit Authentifizierung im Kontext des SNMPv3-Trap-Benutzers.

Auth Passwort

Zeigt ***** (Sternchen) anstelle des Authentifizierungspassworts des SNMPv3 trap-Benutzers an.

Um das Passwort zu ändern, erzeugen Sie einen weiteren SNMPv3-Trap-Benutzer und löschen dann den bestehenden.

Privacy

Zeigt das Protokoll, welches das Gerät für diesen Benutzer zur Verschlüsselung der SNMPv3-Traps verwendet.

Priv Passwort

Zeigt ***** (Sternchen) anstelle des Passworts an, das der SNMPv3-Trap-Benutzer zur Authentifizierung vor dem Senden verwendet.

Um das Passwort zu ändern, erzeugen Sie einen weiteren SNMPv3-Trap-Benutzer und löschen dann den bestehenden.

Status Benutzer

Zeigt den Status des SNMPv3-Trap-Benutzers.

Mögliche Werte:

`markiert` (Voreinstellung)

Der SNMPv3-Trap-Benutzer ist aktiv.

`unmarkiert`

Der SNMPv3-Trap-Benutzer ist inaktiv.

6.1.5.2 Trap Ziele

[Diagnose > Statuskonfiguration > Alarme (Traps) > Trap Ziele]

In diesem Dialog legen Sie die Trap-Ziele fest, an die das Gerät SNMP-Traps sendet.

Für SNMPv3 gelten die folgenden Kriterien:

Das Gerät sendet SNMPv3-Traps an das für den betreffenden SNMPv3-Trap-Benutzer festgelegte Trap-Ziel.

Das Gerät unterstützt maximal 10 Trap-Ziele für SNMPv3.

Funktion

Funktion

Schaltet das Senden von SNMP-Traps ein/aus.

Mögliche Werte:

[An](#) (Voreinstellung)

Das Senden von SNMP-Traps ist eingeschaltet.

[Aus](#)

Das Senden von SNMP-Traps ist ausgeschaltet.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

Schaltflächen



Hinzufügen

Öffnet das Fenster [Erzeugen](#), um eine Tabellenzeile hinzuzufügen. Damit richten Sie ein Trap-Ziel auf dem Gerät ein.

- Im Feld [Name](#) legen Sie einen Namen für das Trap-Ziel fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

- In der Dropdown-Liste [Typ](#) wählen Sie die SNMP-Version, die das Gerät zum Senden von SNMP-Traps an das Trap-Ziel verwendet.

Mögliche Werte:

[V1](#)

SNMP Version 1

Aus Sicherheitsgründen empfehlen wir, diese Einstellung nicht zu verwenden.

[V3](#)

SNMP Version 3

- Im Feld [Adresse](#) legen Sie IP-Adresse und Port des Trap-Ziels fest.

Mögliche Werte:

[<IPv4-Adresse>:<Port>](#)

Wenn Sie keinen Port festlegen, fügt das Gerät automatisch den Port [162](#) dem Trap-Ziel hinzu.

- In der Dropdown-Liste [SNMPv3 Trap Benutzer](#) wählen Sie den SNMPv3-Trap-Benutzer, in dessen Kontext das Gerät SNMPv3-Traps an das Trap-Ziel sendet.
Voraussetzung ist, dass Sie in der Dropdown-Liste [Typ](#) den Eintrag [v3](#) wählen.
Sie wählen einen der Benutzer, die Sie im Dialog [Diagnose > Statuskonfiguration > Alarmer \(Traps\) > Trap V3 Benutzerverwaltung](#) eingerichtet haben.
- In der Dropdown-Liste [Sicherheitsstufe](#) wählen Sie, ob das Gerät die SNMPv3-Traps verschlüsselt sendet und ob vor dem Senden eine Authentifizierung erforderlich ist.
Voraussetzung ist, dass Sie in der Dropdown-Liste [Typ](#) den Eintrag [v3](#) wählen.
Mögliche Werte:
 - [noAuthNoPriv](#)
Das Gerät sendet SNMPv3-Traps unverschlüsselt ohne Authentifizierung.
Aus Sicherheitsgründen empfehlen wir, diese Einstellung nicht zu verwenden.
 - [authNoPriv](#)
Das Gerät sendet SNMPv3-Traps unverschlüsselt.
Der Benutzer muss sich vor dem Senden von SNMPv3-Traps authentifizieren.
 - [authPriv](#)
Das Gerät sendet SNMPv3-Traps verschlüsselt.
Der Benutzer muss sich vor dem Senden von SNMPv3-Traps authentifizieren.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Name

Zeigt den Namen, den Sie für das SNMPv3-Trap-Ziel (Trap-Host) festgelegt haben.

SNMP Protokoll

Zeigt die SNMP-Version, die das Gerät verwendet, um SNMP-Traps an das Trap-Ziel zu senden.

Adresse

Legt IP-Adresse und Port des Trap-Ziels (Trap-Host) fest.

Mögliche Werte:

[<IPv4-Adresse> : <Port>](#)Wenn Sie keinen Port festlegen, fügt das Gerät automatisch den Port [162](#) dem Trap-Ziel hinzu.

SNMPv3 Trap Benutzer

Legt den SNMPv3-Trap-Benutzer fest, den das Gerät verwendet, um SNMPv3-Traps an das Trap-Ziel zu senden.

Sie wählen einen der SNMPv3-Trap-Benutzer, die Sie im Dialog [Diagnose > Statuskonfiguration > Alarmer \(Traps\) > Trap V3 Benutzerverwaltung](#) eingerichtet haben.

Sicherheitsstufe

Legt fest, ob das Gerät die SNMPv3-Traps verschlüsselt sendet und ob vor dem Senden eine Authentifizierung erforderlich ist.

Mögliche Werte:

[noAuthNoPriv](#)

Das Gerät sendet SNMPv3-Traps unverschlüsselt ohne Authentifizierung.
Aus Sicherheitsgründen empfehlen wir, diese Einstellung nicht zu verwenden.

[authNoPriv](#)

Das Gerät sendet SNMPv3-Traps unverschlüsselt.
Der Benutzer muss sich vor dem Senden von SNMPv3-Traps authentifizieren.

[authPriv](#)

Das Gerät sendet SNMPv3-Traps verschlüsselt.
Der Benutzer muss sich vor dem Senden von SNMPv3-Traps authentifizieren.

Typ

Zeigt den Typ der Benachrichtigung.

Aktiv

Aktiviert/deaktiviert das Senden von SNMP-Traps an das Trap-Ziel.

Mögliche Werte:

[markiert](#) (Voreinstellung)

Das Senden von SNMP-Traps an das Trap-Ziel ist aktiv.

[unmarkiert](#)

Das Senden von SNMP-Traps an dieses Trap-Ziel ist inaktiv.

6.2 System

[Diagnose > System]

Das Menü enthält die folgenden Dialoge:

[Systeminformationen](#)

[Hardware-Zustand](#)

[Konfigurations-Check](#)

[IP-Adressen Konflikterkennung](#)

[ARP](#)

[Selbsttest](#)

6.21 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



Systeminformationen speichern

Öffnet die HTML-Seite in einem neuen Webbrowser-Fenster oder -Tab. Sie können die HTML-Seite mit dem entsprechenden Webbrowser-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

Betriebsstunden

Zeigt die Gesamtbetriebszeit des Geräts seit Lieferung.

Mögliche Werte:

`..d ..h ..m ..s`

Tag(e) Stunde(n) Minute(n) Sekunde(n)

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Flash-Region

Zeigt den Namen des Parameters, zum Beispiel für den betreffenden Speicherbereich.

Beschreibung

Zeigt eine Beschreibung für den Parameter.

Flash-Sektoren

Zeigt, wie viele Sektoren dem Speicherbereich zugewiesen sind.

Lösch-Vorgänge

Zeigt, wie viele Male das Gerät die Sektoren des Speicherbereichs überschrieben hat.

6.23 Konfigurations-Check

[Diagnose > System > Konfigurations-Check]

Das Gerät ermöglicht Ihnen, die Einstellungen im Gerät mit den Einstellungen seiner Nachbargeräte zu vergleichen. Dazu verwendet das Gerät die Informationen, die es mittels Topologie-Erkennung (LLDP) von seinen Nachbargeräten empfangen hat.

Der Dialog listet die erkannten Abweichungen auf, welche die Leistungsfähigkeit der Kommunikation zwischen dem Gerät und den erkannten Nachbargeräten beeinflussen.

Anmerkung: Ein Nachbargerät ohne LLDP-Unterstützung, das LLDP-Pakete weiterleitet, kann im Dialog mehrdeutige Meldungen verursachen. Dies tritt auf, wenn das Nachbargerät ein Hub oder ein Switch ohne Management ist, der IEEE 802.1D-2004 ignoriert. Der Dialog stellt in dem Fall die am Nachbargerät angeschlossenen und erkannten Geräte als direkt mit dem Gerät verbunden dar, obwohl diese am Nachbargerät angeschlossen sind.

Konfiguration

Starte Konfigurations-Check...

Startet die Prüfung und aktualisiert den Inhalt der Tabelle.

Bleibt die Tabelle leer, war der Konfigurations-Check erfolgreich und die Einstellungen im Gerät sind kompatibel zu den Einstellungen in den erkannten Nachbargeräten.

Information



Fehler

Zeigt, wie viele Abweichungen des Levels **ERROR** das Gerät beim Konfigurations-Check erkannt hat.



Warnung

Zeigt, wie viele Abweichungen des Levels **WARNING** das Gerät beim Konfigurations-Check erkannt hat.

Wenn im Gerät mehr als 39 VLANs eingerichtet sind, dann zeigt der Dialog fortwährend eine Warnung. Der Grund ist die begrenzte Anzahl der möglichen VLAN-Informationen in LLDP-Paketen mit begrenzter Länge. Das Gerät vergleicht die ersten 39 VLANs automatisch. Wenn im Gerät 40 oder mehr VLANs eingerichtet sind, dann prüfen Sie die Übereinstimmung der weiteren VLANs gegebenenfalls manuell.




Information

Zeigt, wie viele Abweichungen des Levels **INFORMATION** das Gerät beim Konfigurations-Check erkannt hat.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.



Zeigt detaillierte Informationen über die erkannten Abweichungen im Bereich unterhalb der Tabellenzeile. Um die detaillierten Informationen wieder auszublenden, klicken Sie die Schaltfläche . Wenn Sie das Symbol in der Kopfzeile der Tabelle klicken, blenden Sie die detaillierten Informationen für jede Tabellenzeile ein oder aus.

ID

Zeigt die Regel-ID der aufgetretenen Abweichungen. Der Dialog fasst mehrere Abweichungen mit der gleichen Regel-ID unter einer Regel-ID zusammen.

Level

Zeigt den Grad der Abweichung zwischen den Einstellungen dieses Geräts und den Einstellungen der erkannten Nachbargeräte.

Das Gerät unterscheidet die folgenden Zustände:

- **INFORMATION**
Die Leistungsfähigkeit der Kommunikation zwischen den beiden Geräten ist nicht beeinträchtigt.
- **WARNING**
Die Leistungsfähigkeit der Kommunikation zwischen den beiden Geräten kann beeinträchtigt sein.
- **ERROR**
Die Kommunikation zwischen den beiden Geräten ist beeinträchtigt.

Nachricht

Zeigt eine Zusammenfassung der erkannten Abweichungen.

6.24 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.

Information

Konflikt erkannt

Zeigt, ob gegenwärtig ein Adresskonflikt besteht.

Mögliche Werte:

markiert

Das Gerät erkennt einen Adresskonflikt.

unmarkiert

Das Gerät erkennt keinen Adresskonflikt.

Konfiguration

Erkennung 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 *Erkennung Verzögerung [ms]* festgelegten zeitlichen Abstand. Empfängt das Gerät auf diese Datenpakete eine Antwort, liegt ein Adresskonflikt 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 Datenstrom 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-Protection* 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 *Erkennung 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.

Erkennung 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: 1)

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..10000 (Voreinstellung: 10000)

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät einen Adresskonflikt erkennt.

Mögliche Werte:

`markiert` (Voreinstellung)

Das Senden von SNMP-Traps ist aktiv. Voraussetzung ist, dass im Dialog [Diagnose > Statuskonfiguration > Alarme \(Traps\)](#) die Funktion [Alarme \(Traps\)](#) eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.

Das Gerät sendet einen SNMP-Trap, wenn es einen Adresskonflikt erkennt.

`unmarkiert`

Das Senden von SNMP-Traps ist inaktiv.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter [„Arbeiten mit Tabellen“ auf Seite 16](#).

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.

6.25 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Schaltflächen

 ARP-Tabelle leeren

Entfernt aus der ARP-Tabelle die dynamisch eingerichteten Adressen.

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:

statisch

Statischer Eintrag. Der statische Eintrag bleibt nach dem Löschen der ARP-Tabelle erhalten.

dynamisch

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.

lokal

IP- und MAC-Adresse des Geräte-Managements.

Aktiv

Zeigt, dass die ARP-Tabelle die IP/MAC-Adresszuweisung als aktiven Eintrag enthält.

6.26 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 sperrern 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 Systemstarts.

Mögliche Werte:

markiert (Voreinstellung)

Der RAM-Speicher-Test ist aktiviert. Während des Systemstarts testet das Gerät den RAM-Speicher.

unmarkiert

Der RAM-Speicher-Test ist deaktiviert. Dies verkürzt die Startzeit des Geräts.

SysMon1 ist verfügbar

Aktiviert/deaktiviert die Möglichkeit, während des Systemstarts in den System-Monitor zu wechseln.

Mögliche Werte:

markiert (Voreinstellung)

Das Gerät ermöglicht Ihnen, während des Systemstarts 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 während des Systemstarts.

Tabelle

In dieser Tabelle legen Sie fest, wie sich das Gerät verhält, wenn es einen Fehler erkennt.

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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:

`logOnly`

Das Gerät protokolliert den Fehler in der Log-Datei. Siehe Dialog [Diagnose > Bericht > System-Log](#).

`sendTrap`

Das Gerät sendet einen SNMP-Trap.

Voraussetzung ist, dass im Dialog [Diagnose > Statuskonfiguration > Alarme \(Traps\)](#) die Funktion [Alarme \(Traps\)](#) eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.

`reboot` (Voreinstellung)

Das Gerät löst einen Neustart aus.

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 E-Mails ist eingeschaltet.

Aus (Voreinstellung)

Das Senden von E-Mails ist ausgeschaltet.

Information

Schaltflächen



E-Mail-Benachrichtigung Statistik leeren

Setzt die Zähler im Rahmen *Information* auf 0.

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.

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 (Certificate Authority, CA) 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 dazu 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

E-Mail-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
(Voreinstellung: switch@hirschmann.com)

Benachrichtigung 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

Benachrichtigung 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.

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Schaltflächen



Fügt eine Tabellenzeile hinzu.



Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Das Gerät weist den Wert automatisch zu, wenn Sie eine Tabellenzeile hinzufügen.

Benachrichtigung Typ

Legt fest, ob das Gerät die E-Mails sofort oder in regelmäßigen Abständen an diesen Empfänger 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.

E-Mail-Adresse

Legt die E-Mail-Adresse des Empfängers fest.

Mögliche Werte:

Gültige E-Mail-Adresse mit bis zu 255 Zeichen

Aktiv

Aktiviert/deaktiviert das Benachrichtigen des Empfängers.

Mögliche Werte:

`markiert`

Das Benachrichtigen des Empfängers ist aktiv.

`unmarkiert` (Voreinstellung)

Das Benachrichtigen des Empfängers ist inaktiv.

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Schaltflächen



Hinzufügen

Fügt eine Tabellenzeile hinzu.



Löschen

Entfernt die ausgewählte Tabellenzeile.



Verbindung testen

Öffnet das Fenster [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.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Das Gerät weist den Wert automatisch zu, wenn Sie eine Tabellenzeile hinzufügen.

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 festlegen, 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:

`kein` (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, welches 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, welches 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.

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 (Certificate Authority, CA) 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: Damit die Änderungen nach dem Laden eines neuen Zertifikates wirksam werden, 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 dazu 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Schaltflächen



Hinzufügen

Fügt eine Tabellenzeile hinzu.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Das Gerät weist den Wert automatisch zu, wenn Sie eine Tabellenzeile hinzufügen.

Wenn Sie eine Tabellenzeile löschen, bleibt eine Lücke in der Nummerierung. Wenn Sie eine Tabellenzeile erzeugen, schließt das Gerät die erste 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` (default setting)

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.

Mögliche Werte:

`markiert`

Das Gerät sendet Ereignisse zum Syslog-Server.

`unmarkiert` (Voreinstellung)

Die Übermittlung der Ereignisse zum Syslog-Server ist deaktiviert.

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.

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

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.

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 feststellt, zeigt es auch die geschätzte Entfernung zu der Stelle, an der es das Problem erkannt hat.

Um verlässliche Ergebnisse zu erhalten, verwenden Sie die Funktion *TP-Kabeldiagnose* für Twisted-Pair-Kabel, die mindestens 10 Meter lang sind.

Anmerkung: Dieser Test unterbricht den Datenstrom vorübergehend auf dem betreffenden Port.

Information

Port

Zeigt die Nummer des Ports.

Starte Kabeldiagnose...

Öffnet das Fenster *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*.

Status

Status des virtuellen Kabeltesters.

Mögliche Werte:

aktiv

Der Kabeltest ist im Gange.

Um den Test zu starten, klicken Sie die Schaltfläche *Starte Kabeldiagnose...* Diese Aktion öffnet das Fenster *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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Kabelpaar

Zeigt das Kabelpaar, auf das sich diese Tabellenzeile 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 inaktiv 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.

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Schaltflächen

 Zurücksetzen

Öffnet das Fenster *Welche Statistik soll gelöscht werden?*. Das Fenster zeigt die Ports, die Sie wieder einschalten und die zugehörigen Zähler auf 0 zurücksetzen können. Klicken und wählen Sie eine Tabellenzeile, um den zugehörigen Port wieder einzuschalten.

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*

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, wählen Sie die Tabellenzeile des Ports, klicken die Schaltfläche .
- 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 ist, dass im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.

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.
- Nach einer Wartezeit schaltet die Funktion *Auto-Disable* 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.

[Auto-Disable]

In dieser Registerkarte aktivieren Sie die Funktion *Auto-Disable* für die von der Funktion *Port-Monitor* überwachten Parameter.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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.

[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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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.

[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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

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.

[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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Port

Zeigt die Nummer des Ports.

Typ

Legt den Typ der Datenpakete fest, den das Gerät beim Überwachen der Last auf dem Port berücksichtigt.

Mögliche Werte:

alle

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.

Einheit

Legt die Einheit der Datenrate fest.

Mögliche Werte:

pps (Voreinstellung)

Pakete pro Sekunde

kbps

Kbit pro Sekunde

Voraussetzung ist, dass in Spalte *Typ* der Wert *all* festgelegt ist.

Unterer Schwellenwert

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 Schwellenwert

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.

[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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Port

Zeigt die Nummer des Ports.

10M 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.

10M 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.

100M 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.

100M 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.

1G 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.

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Schaltflächen



Zurücksetzen

Öffnet das Fenster *Welche Statistik soll gelöscht werden?*. Das Fenster zeigt die Ports, die Sie wieder einschalten und die zugehörigen Zähler auf 0 zurücksetzen können. Klicken und wählen Sie eine Tabellenzeile, um den zugehörigen Port wieder einzuschalten.

Davon betroffen sind die Zähler in den folgenden Dialogen:

- Dialog *Diagnose > Ports > Auto-Disable*
- Dialog *Diagnose > Ports > Port-Monitor*
 - Registerkarte *Link-Änderungen*
 - Registerkarte *CRC/Fragmente*
 - Registerkarte *Überlast-Erkennung*

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*.

DOT1S

BPDUGuard

Siehe Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.

Grund

Zeigt den überwachten Parameter, der zum Ausschalten des Ports geführt hat.

Mögliche Werte:

kein

Kein überwachter Parameter.

Der Port ist eingeschaltet.

Link-Änderungen

Zu viele Linkänderungen. Siehe Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *Link-Änderungen*.

CRC-/Fragment Fehler

Zu viele CRC-/Fragmentfehler erkannt. Siehe Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *CRC/Fragmente*.

Duplex-Mismatch Erkennung

Duplex-Mismatch erkannt. Siehe Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *Global*.

BPDURate

STP-BPDUs empfangen. Siehe Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.

MAC-basierte Port-Sicherheit

Zu viele Datenpakete von unerwünschten Absendern. Siehe Dialog *Netzsicherheit > Port-Sicherheit*.

Überlast-Erkennung

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-Schutz

Schicht-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.

[Status]

Diese Registerkarte zeigt, für welche überwachten Parameter die Funktion [Auto-Disable](#) aktiv ist.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

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 Dialog [Diagnose > Ports > Port-Monitor](#).

network security

Der Parameter gehört zu den Funktionen im Dialog [Netzsicherheit](#).

l2 redundancy

Der Parameter gehört zu den Funktionen im Dialog [Switching > L2-Redundanz](#) oder zur Funktion [Loop-Schutz](#), siehe Dialog [Diagnose > Loop-Schutz](#).

Auto-Disable

Zeigt, ob die Funktion *Auto-Disable* für den nebenstehenden Parameter aktiv/inaktiv 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.

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 Start*.

Funktion

Schaltflächen



Konfiguration zurücksetzen

Setzt die Einstellungen im Dialog auf die Voreinstellung zurück und stellt die zuvor angewendeten Einstellungen wieder her.

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 Start

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:

- (Voreinstellung)

Kein Ziel-Port ausgewählt.

<Port-Nummer>

Nummer des Ziel-Ports. Das Gerät kopiert die Datenpakete von den Quell-Ports auf diesen Port.

Auf dem Ziel-Port fügt das Gerät den Datenpaketen, die der Quell-Port sendet, ein VLAN-Tag hinzu. Datenpakete, die der Quell-Port empfängt, sendet der Ziel-Port ohne Änderungen.

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:

- (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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Quelle Port

Zeigt die Nummer des Ports.

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.

Auf dem Ziel-Port fügt das Gerät den Datenpaketen, die der Quell-Port sendet, ein VLAN-Tag hinzu. Datenpakete, die der Quell-Port empfängt, sendet der Ziel-Port ohne Änderungen.

Mögliche Werte:

`kein` (Voreinstellung)

Keine Datenpakete.

`tx`

Datenpakete, die der Quell-Port sendet.

`rx`

Datenpakete, die der Quell-Port empfängt.

`txrx`

Datenpakete, die der Quell-Port sendet.

Anmerkung: Mit der Einstellung `txrx` kopiert das Gerät jedes übertragene Datenpaket. 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.

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.

6.6 LLDP

[Diagnose > LLDP]

Das Gerät ermöglicht Ihnen, Informationen über benachbarte Geräte zu sammeln. Dazu nutzt das Gerät Link Layer Discovery Protocol (LLDP). Diese Informationen ermöglichen einer Netzmanagement-Station, die Struktur des 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter [„Arbeiten mit Tabellen“](#) auf Seite 16.

Port

Zeigt die Nummer des Ports.

Funktion

Legt fest, ob der Port LLDP-Datenpakete überträgt.

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.

Benachrichtigung

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)

Modus FDB

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.

`beide`

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`.

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 gesendeten 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. Diese Informationen ermöglichen einer Netzmanagement-Station, die Struktur des 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 angeschlossene Gerät je eine Zeile.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

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`

Das angeschlossene Gerät unterstützt aktiv LLDP.

Nachbar-Adresse

Zeigt die IPv4-Adresse oder den Hostnamen, mit der/dem der Zugriff auf das Management des Nachbargeräts möglich ist.

Nachbar IPv6-Adresse

Zeigt die IPv6-Adresse, mit welcher 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 aktiv ist.

Unterstützt PoE

Zeigt, ob der Port des Nachbargeräts Power over Ethernet (PoE) unterstützt.

PoE eingeschaltet

Zeigt, ob Power over Ethernet (PoE) auf dem Port des Nachbargeräts aktiv ist.

[LLDP-IVED]

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter [„Arbeiten mit Tabellen“ auf Seite 16](#).

Port

Zeigt die Nummer des Ports.

Geräteklasse

Zeigt die Geräteklasse des über Fernverbindung angeschlossenen Geräts.

Mögliche Werte:

notDefined

Das Gerät weist Funktionsmerkmale auf, welche durch keine der *LLDP-MED*-Klassen abgedeckt sind.

endpointClass1

Das Gerät weist die Funktionsmerkmale *endpointClass1* auf.

endpointClass2

Das Gerät weist die Funktionsmerkmale *endpointClass2* auf.

endpointClass3

Das Gerät weist die Funktionsmerkmale *endpointClass3* auf.

networkConnectivity

Das Gerät verfügt über Anschlussmöglichkeiten für das Netz.

VLAN-ID

Zeigt die Erweiterung für die VLAN-Kennung des entfernten Systems, welches an diesen Port angeschlossen ist (gemäß IEEE 802.3).

0

Pakete mit Prioritäts-Tag

Ausschließlich die 802.1D-Priorität ist von Bedeutung und das Gerät verwendet die voreingestellte VLAN-Kennung des Eingangs-Ports.

1..4042

gültige Port-VLAN-ID

Priorität

Zeigt den Wert der *802.1D Priority*, welche dem an diesen Port angeschlossenen entfernten System zugeordnet ist.

DSCP

Zeigt den Wert der *Differentiated Service Code Point (DSCP)*, welche dem an diesen Port angeschlossenen entfernten System zugeordnet ist.

Status Unknown-Bit

Zeigt den *Unknown Bit Status* des eingehenden Verkehrs.

Mögliche Werte:

true

Die Netz-Richtlinie für den festgelegten Anwendungstyp ist gegenwärtig unbekannt. In diesem Fall ignoriert die VLAN-ID die Schicht-2-Priorität und den Wert des Feldes *DSCP*.

false

Kennzeichnet eine festgelegte Netz-Richtlinie.

Status Tagged-Bit

Zeigt den sog. „Tagged Bit Status“.

Mögliche Werte:

true

Die Anwendung verwendet ein markiertes VLAN.

false

Das Gerät greift für die spezifische Anwendung auf unmarkierten VLAN-Betrieb zurück. 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.

6.7 Loop-Schutz

[Diagnose > Loop-Schutz]

Die Funktion *Loop-Schutz* unterstützt beim Schutz vor Schicht-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 Schicht-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 Signalkontakt 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.

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* der Wert *auto-disable* oder *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 Spalte *Reset-Timer [s]* die Wartezeit fest.

unmarkiert (Voreinstellung)

Die Funktion *Auto-Disable* für *Loop-Schutz* ist inaktiv.

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

Schwellenwert Empfang

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

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Schaltflächen



Port-Statistiken leeren

Setzt die Werte in den folgenden Spalten zurück:

- *Loops*
- *Gesendete Pakete*
- *Empfangene Pakete*

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 (Voreinstellung)

Das Gerät wertet empfangene *Loop-Detection*-Pakete aus.

Aktion

Legt die Aktion fest, die das Gerät ausführt, wenn es einen Schicht-2-Loop an diesem Port erkennt.

Mögliche Werte:

trap

Das Gerät sendet einen Trap.

auto-disable (Voreinstellung)

Das Gerät schaltet den Port mit der Funktion *Auto-Disable* aus.

Voraussetzung für das Abschalten des Ports ist, dass im Rahmen *Konfiguration* das Kontrollkästchen *Auto-Disable* 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 im Rahmen *Konfiguration* das Kontrollkästchen *Auto-Disable* 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 im Dialog [Switching > VLAN > Port](#) das VLAN bereits eingerichtet ist und dass der Port Mitglied des VLANs ist.

Loop erkannt

Zeigt, ob das Gerät einen Schicht-2-Loop auf dem Port erkannt hat.

Mögliche Werte:

`ja`

Das Gerät hat einen Schicht-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 Schicht-2-Loop auf dem Port erkannt.

Loops

Zeigt die Anzahl der Loops, die das Gerät auf dem Port seit dem letzten Zurücksetzen der Portstatistik oder seit dem letzten Systemstart erkannt hat.

Zeit letzter Loop

Zeigt den Zeitpunkt, an dem das Gerät den letzten Loop auf dem Port erkannt hat.

Voraussetzung für die korrekte Ermittlung des Werts ist, dass im Dialog [Zeit > Grundeinstellungen](#) die Systemzeit des Geräts mit der entsprechenden Referenzzeit synchronisiert ist.

Gesendete Pakete

Zeigt die Anzahl der *Loop-Detection* an, die seit dem letzten Zurücksetzen der Portstatistik oder seit dem letzten Systemstart 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 Systemstart.

Verworfen 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 ausgeschaltet ist.

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 detaillierten Informationen zum Gerät für Supportzwecke auf Ihrem PC zu speichern.

Console-Logging

Schaltflächen

 Support-Informationen herunterladen

Erzeugt ein ZIP-Archiv, das Sie mit dem Webbrowser vom Gerät herunterladen können.

Das ZIP-Archiv enthält Dateien mit detaillierten Informationen zum Gerät für Supportzwecke. Weitere Informationen finden Sie unter „[Support-Informationen: Dateien im ZIP-Archiv](#)“ auf [Seite 356](#).

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. Weitere Informationen finden Sie unter „[Bedeutung der Ereignis-Schweregrade](#)“ auf [Seite 356](#).

Das Gerät gibt die Meldungen auf der seriellen Schnittstelle aus.

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.

Logge SNMP Get-Requests

Schaltet die Protokollierung von *SNMP Get*-Anfragen 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.

Logge SNMP Set-Requests

Schaltet die Protokollierung von *SNMP Set*-Anfragen 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*-Anfragen protokolliert. Weitere Informationen finden Sie unter „[Bedeutung der Ereignis-Schweregrade](#)“ auf [Seite 356](#).

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*-Anfragen protokolliert. Weitere Informationen finden Sie unter „[Bedeutung der Ereignis-Schweregrade](#)“ auf [Seite 356](#).

Mögliche Werte:

emergency
alert
critical
error
warning
notice (Voreinstellung)
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. Weitere Informationen finden Sie unter „[Bedeutung der Ereignis-Schweregrade](#)“ auf [Seite 356](#).

Mögliche Werte:

emergency
alert
critical

`error`
`warning` (Voreinstellung)
`notice`
`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.

Support-Informationen: Dateien im ZIP-Archiv

Dateiname	Format	Bemerkungen
<code>audittrail.html</code>	HTML	Enthält die im <i>Audit Trail</i> -Protokoll chronologisch aufgezeichneten Systemereignisse und gespeicherten Änderungen durch die Benutzer.
<code>config.xml</code>	XML	Enthält die im „ausgewählten“ Konfigurationsprofil gespeicherten Einstellungen des Geräts.
<code>defaultconfig.xml</code>	XML	Enthält die Voreinstellungen des Geräts.
<code>script</code>	TEXT	Enthält die Ausgaben des Kommandos <code>show running-config script</code> .
<code>runningconfig.xml</code>	XML	Enthält die gegenwärtigen Betriebseinstellungen des Geräts.
<code>supportinfo.html</code>	HTML	Enthält geräteinterne Service-Information.
<code>systeminfo.html</code>	HTML	Enthält Information über die gegenwärtigen Einstellungen und Betriebsparameter.
<code>systemlog.html</code>	HTML	Enthält die in der Log-Datei protokollierten Ereignisse. Siehe Dialog Diagnose > Bericht > System-Log .

Bedeutung der Ereignis-Schweregrade

Schweregrad	Bedeutung
<code>emergency</code>	Gerät nicht betriebsbereit
<code>alert</code>	Sofortiger Bedieneringriff erforderlich
<code>critical</code>	Kritischer Zustand
<code>error</code>	Fehlerhafter Zustand
<code>warning</code>	Warnung

Schweregrad	Bedeutung
<code>notice</code>	Signifikanter, normaler Zustand
<code>informational</code>	Informelle Nachricht
<code>debug</code>	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 in 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 in 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 (ACA21/ACA22)

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Schaltflächen



Persistente Log-Datei leeren

Entfernt die Log-Dateien vom externen Speicher.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile 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.

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 Webbrowsers.

Die Log-Datei bleibt bis zu einem Neustart des Geräts erhalten. Nach dem Neustart erstellt das Gerät die Datei neu.

Schaltflächen



Log-Datei speichern

Öffnet die HTML-Seite in einem neuen Webbrowser-Fenster oder -Tab. Sie können die HTML-Seite mit dem entsprechenden Webbrowser-Befehl auf Ihrem PC speichern.



Log-Datei leeren

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 Webbrowsers.

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 Zugriffsrolle `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 das 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 mittels HiDiscovery
- 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.

Anmerkung: In der Voreinstellung des Geräts ist der Zugriff auf den System-Monitor während des Systemstarts 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. 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](#).

Schaltflächen



Audit-Trail Datei speichern

Öffnet die HTML-Seite in einem neuen Webbrowser-Fenster oder -Tab. Sie können die HTML-Seite mit dem entsprechenden Webbrowser-Befehl auf Ihrem PC speichern.

7 Erweitert

Das Menü enthält die folgenden Dialoge:

- [DHCP-L2-Relay](#)
- [DHCP Server](#)
- [DNS](#)
- [Industrie-Protokolle](#)
- [Tracking](#)
- [Command Line Interface](#)

7.1 DHCP-L2-Relay

[Erweitert > DHCP-L2-Relay]

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 Längensfeld sowie entweder einer MAC-Adresse, einer IP-Adresse, einer Client-ID oder einer benutzerdefinierten Gerätebeschreibung. Bei einer Client-ID 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

[Erweitert > 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

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.

[VLAN-ID]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

VLAN-ID

VLAN, auf das sich die Tabellenzeile 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. Das Feld *Remote-ID* zeigt die Zeichenfolge, die das Gerät als *Remote-ID* verwendet.

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 Eintrag wählen, geben Sie in Spalte *Remote-ID* eine beliebige Zeichenfolge ein.

Remote-ID


Zeigt die *Remote-ID*, welche das Gerät für dieses VLAN verwendet. Geben Sie eine beliebige Zeichenfolge ein, wenn in der Dropdown-Liste *Remote-ID Typ* der Eintrag `other` ausgewählt ist.

Mögliche Werte:


Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

Das Gerät schreibt ASCII-Code-Werte in das Paket. Wenn in der Dropdown-Liste *Remote-ID Typ* der Eintrag `client-id` oder `other` ausgewählt ist, dann verarbeitet das Gerät den ASCII-Code der Zeichen. Wenn Sie zum Beispiel die Zeichenfolge `abc` eingeben, schreibt das Gerät den Wert `616263` in das Paket.

Wenn das Gerät die eingegebene Zeichenfolge nicht akzeptiert, führen Sie die folgenden Schritte aus:

Klicken Sie die Schaltfläche , um die nicht gespeicherten Änderungen im gegenwärtigen Dialog zu verwerfen.

Wählen Sie in der Dropdown-Liste *Remote-ID Typ* den Eintrag `other`.

Klicken Sie die Schaltfläche , ohne die Zeichenfolge zu ändern.

Geben Sie die beliebige Zeichenfolge ein.

7.1.2 DHCP-L2-Relay Statistiken

[Erweitert > DHCP-L2-Relay > Statistiken]

Das Gerät überwacht den Datenstrom auf den Ports und zeigt die Ergebnisse in tabellarischer Form.

Die Tabelle ist in unterschiedliche Kategorien unterteilt, um Sie bei der Analyse des Datenstroms zu unterstützen.

Die DHCPv6-Relay-Optionen werden in der Statistik-Tabelle nicht angezeigt.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

Schaltflächen



Setzt die Zähler der Statistik auf 0.

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.

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 eingeschaltet, weist der DHCP-Server dem Client auch die entsprechenden Konfigurationsdaten zu. Die Konfigurationsdaten legen beispielsweise fest, welche IP-Adresse, welchen DNS-Server und welche Standard-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](#)

7.21 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-Überprüfung

Aktiviert/deaktiviert das Prüfen auf eindeutige IP-Adressen. Vor dem Zuweisen einer IP-Adresse sendet der Server ein *ICMP echo request*-Paket, um zu prüfen, ob diese IP-Adresse bereits im Netz verwendet wird.

Mögliche Werte:

`markiert` (Voreinstellung)

Die Funktion *IP-Überprüfung* ist aktiv.

`unmarkiert`

Die Funktion *IP-Überprüfung* ist inaktiv.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

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.

7.2.2 DHCP-Server Pool

[Erweitert > DHCP Server > Pool]


In diesem Dialog legen Sie die Einstellungen fest, um DHCP-Clients, von denen das Gerät einen DHCP-Request empfängt, eine spezifische IP-Adresse zuzuordnen. Abhängig davon, ob ein anfragendes Gerät mit einem physischen Port verbunden oder ein Mitglied in einem VLAN ist, weist der DHCP-Server eine IP-Adresse aus einem spezifischen Pool (Adressbereich) zu.

Das Gerät stellt maximal 128 Pools bereit, mit insgesamt maximal 1000 Einträgen. Der DHCP-Server bietet die folgenden Arten der IP-Adress-Zuordnung an:

- **Statisch**
 Das Gerät ordnet einen statischen Eintrag zu, basierend auf einem Pool, der 1 IP-Adresse enthält (IP-Adresse = letzte IP-Adresse). Dies ist nützlich, um die selbe IP-Adresse einem spezifischen Gerät zuzuordnen, zum Beispiel einem Server, NAS oder Drucker. Das Gerät ordnet die Adresse zu, basierend auf:
 - der MAC-Adresse des Clients
 - dem physischen Port, an dem der Client angeschlossen ist
 - dem VLAN, in dem der Client Mitglied ist
- **Dynamisch**
 Das Gerät ordnet einen dynamischen Eintrag zu, basierend auf einem Pool, der mehr als 1 IP-Adresse enthält. Dies ist nützlich, um eine IP-Adresse aus einem bestimmten Adressbereich zum Beispiel solchen Clients zuzuordnen, die Mitglied in einem bestimmten VLAN sind.

Wenn gewünscht, verarbeitet das Gerät außerdem weitere Informationen aus der DHCP-Anfrage, um dem Client eine IP-Adresse aus einem bestimmten Pool zuzuweisen. Diese weiteren Informationen können zum Beispiel eine *Client-ID*, eine *Remote-ID* oder eine *Circuit-ID* sein.

Sie können für jeden Pool individuelle Parameter (DHCP-Optionen) festlegen. Das Gerät sendet diese Parameter zusammen mit der IP-Adresse an die Clients. Die Bereitstellung von DHCP-Optionen ist ein intelligenter Weg, um Netzwerk-Clients in der frühen Phase der Bereitstellung des Netzzugangs einzurichten.

Dieser Dialog zeigt die unterschiedlichen Informationen, die zur Vergabe einer IP-Adresse an einen Client an einem Port oder in einem VLAN erforderlich sind. Verwenden Sie die Schaltfläche , um eine Tabellenzeile hinzuzufügen.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Schaltflächen



Hinzufügen

Fügt eine Tabellenzeile hinzu.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Das Gerät weist den Wert automatisch zu, wenn Sie eine Tabellenzeile hinzufügen.

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 (Voreinstellung: `0.0.0.0`)

Letzte IP-Adresse

Wenn Sie die dynamische IP-Adresszuweisung verwenden, definiert dieser Wert das Ende des IP-Adressraums.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung: `0.0.0.0`)

Port

Legt die Nummer des Ports fest.

Mögliche Werte:

`Alle` (Voreinstellung)

Das Gerät weist einem Client-Gerät eine IP-Adresse zu, unabhängig davon, an welchem Port das lokale Gerät die DHCP-Anfrage empfängt.

`<Port-Nummer>`

Das Gerät weist einem Client-Gerät nur dann eine IP-Adresse zu, wenn das lokale Gerät die DHCP-Anfrage auf dem festgelegten Port empfängt.

VLAN-ID

Legt das VLAN fest, auf das sich die Tabellenzeile bezieht.

Der Wert `1` entspricht dem Standard-VLAN für das Management des Geräts.

Mögliche Werte:

- (Voreinstellung)

`1..4042`

MAC-Adresse

Legt die MAC-Adresse des Geräts fest, welches die IP-Adresse vergibt.

Mögliche Werte:

- (Voreinstellung)

Bei der IP-Adresszuweisung ignoriert der Server diese Variable.

Gültige Unicast-MAC-Adresse

Legen Sie den Wert mit Doppelpunkt-Trennzeichen fest, zum Beispiel `00:11:22:33:44:55`.

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:

- (Voreinstellung)

Kein DHCP-Relay festgelegt.

Gültige IPv4-Adresse

IP-Adresse des DHCP-Relays.

Client-ID

Legt den benutzerdefinierten Bezeichner für den Client anstelle der MAC-Adresse fest.

Mögliche Werte:

- (Voreinstellung)

Das Gerät ignoriert den Parameter während der Zuweisung einer IP-Adresse aus dem Pool.

Folge von hexadezimalen Zeichenpaaren mit 1..254 Paaren, getrennt durch ein Leerzeichen.

Beispiel: `41 42 43 44 4F`

Anmerkung: Wenn Sie hohe Sicherheitsanforderungen haben und den Clients nicht bedingungslos vertrauen möchten, ziehen Sie in Betracht, die *Remote-ID* oder die *Circuit-ID* statt der *Client-ID* zu benutzen. Die *Remote-ID* und die *Circuit-ID* werden von einem DHCP-Relay eingefügt und sind dadurch schwerer zu fälschen.

Remote-ID

Legt die *Remote-ID* fest. Das DHCP-Relay fügt die *Remote-ID* in die DHCP-Anfrage ein.

Mögliche Werte:

- (Voreinstellung)

Das Gerät ignoriert den Parameter während der Zuweisung einer IP-Adresse aus dem Pool.

Folge von hexadezimalen Zeichenpaaren mit 1..254 Paaren, getrennt durch ein Leerzeichen.

Beispiel: `41 42 43 44 4F`

Circuit-ID

Legt die *Circuit-ID* fest. Das DHCP-Relay fügt die *Circuit-ID* in die DHCP-Anfrage ein.

Mögliche Werte:

- (Voreinstellung)

Das Gerät ignoriert den Parameter während der Zuweisung einer IP-Adresse aus dem Pool.

Folge von hexadezimalen Zeichenpaaren mit 1..254 Paaren, getrennt durch ein Leerzeichen.

Beispiel: `41 42 43 44 4F`

Hirschmann-Gerät

Aktiviert/deaktiviert die Hirschmann-Multicasts. Wenn das Gerät in diesem IP-Adressbereich nur Hirschmann-Clients bedient, dann aktivieren Sie diese Funktion.

Mögliche Werte:

`markiert`

In diesem IP-Adressbereich bedient das Gerät ausschließlich Hirschmann-Clients. Die Hirschmann-Multicasts sind aktiviert.

`unmarkiert` (Voreinstellung)

In diesem IP-Adressbereich bedient das Gerät die Clients verschiedener Hersteller. Die Hirschmann-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 mittels 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 (Voreinstellung: `0.0.0.0`)

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 (Voreinstellung: 255.255.255.0)

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 (Voreinstellung: 0.0.0.0)

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 (Voreinstellung: 0.0.0.0)

Hostname

Legt den Hostnamen 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

7.23 DHCP-Server Lease-Tabelle

[Erweitert > DHCP Server > Lease-Tabelle]

Dieser Dialog zeigt den Status der IP-Adressvergabe auf den einzelnen Ports.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Port

Zeigt die Nummer des Ports, an welchen die Adresse gegenwärtig vergeben ist.

IP-Adresse

Zeigt die vergabene 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 bietet IP-Adresse an), Request (Client fordert IP-Adresse an) sowie Acknowledgement (Server bestätigt IP-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-ID* des Geräts, welches die IP-Adresse least.

Remote-ID

Zeigt die *Remote-ID* des Geräts, welches die IP-Adresse least.

Circuit-ID

Zeigt die *Circuit-ID* des Geräts, welches die IP-Adresse least.

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.

Mittels der Funktion [Client](#) sendet das Gerät Anfragen zur Auflösung von Hostnamen in IP-Adressen an einen DNS-Server.

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

Schaltflächen



Cache leeren

Entfernt jeden Eintrag aus dem DNS-Cache.

Cache

Schaltet die Funktion *Cache* ein/aus.

Mögliche Werte:

An (Voreinstellung)

Die Funktion *Cache* ist eingeschaltet.

Das Gerät speichert bis zu 128 DNS-Server-Antworten (Hostname und zugehörige IP-Adresse) flüchtig im Cache. 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.

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

Index

Zeigt die fortlaufende Nummer des DNS-Servers.

IP-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.

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

Quelle

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 im Feld `Request Timeout [s]` ein Wert >0 festgelegt ist.

Mögliche Werte:

0..100 (Voreinstellung: 2)

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Schaltflächen

 Hinzufügen

Öffnet das Fenster *Erzeugen*, um eine Tabellenzeile hinzuzufügen.

Im Feld *Index* legen Sie die Index-Nummer fest.

Mögliche Werte:

– 1..4

Das Gerät ermöglicht Ihnen, bis zu 4 externe DNS-Server festzulegen.

Im Feld *IP-Adresse* legen Sie die IP-Adresse des DNS-Servers fest.

Mögliche Werte:

- Gültige IPv4-Adresse
- Gültige IPv6-Adresse

 Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die fortlaufende Nummer des DNS-Servers. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

IP-Adresse

Legt die IP-Adresse des DNS-Servers fest.

Mögliche Werte:

Gültige IPv4-Adresse

Gültige IPv6-Adresse

Aktiv

Aktiviert/deaktiviert die Tabellenzeile.

Voraussetzungen:

- Im Dialog *Erweitert > DNS > Client > Global* ist die Funktion *DNS client* eingeschaltet.
- Im Rahmen *Konfiguration* ist in der Dropdown-Liste *Quelle* der Eintrag `user` ausgewählt.

Mögliche Werte:

`markiert` (Voreinstellung)

Die Tabellenzeile ist aktiv.

Das Gerät sendet Anfragen an den in der ersten aktiven Tabellenzeile festgelegten DNS-Server. Erhält das Gerät von diesem Server keine Antwort, sendet es Anfragen an den in der nächsten aktiven Tabellenzeile festgelegten DNS-Server. Das entsprechende Timeout legen Sie im Rahmen *Konfiguration*, Feld *Request Timeout [s]* fest.

`unmarkiert`

Die Tabellenzeile ist inaktiv.

Das Gerät sendet keine Anfragen an diesen DNS-Server.

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf Seite 16.

Schaltflächen

 Hinzufügen

Öffnet das Fenster *Erzeugen*, um eine Tabellenzeile hinzuzufügen.

Im Feld *Index* legen Sie die Index-Nummer fest.

Mögliche Werte:

- 1..64

Das Gerät ermöglicht Ihnen, bis zu 64 statische Hosts festzulegen.

Im Feld *Name* legen Sie den Hostnamen des zugehörigen Geräts fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..255 Zeichen

Im Feld *IP-Adresse* legen Sie die IP-Adresse des zugehörigen Geräts fest.

Mögliche Werte:

- Gültige IPv4-Adresse
- Gültige IPv6-Adresse

 Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Name

Legt den Hostnamen fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..255 Zeichen

IP-Adresse

Legt die IP-Adresse fest, mit welcher der Host erreichbar ist.

Mögliche Werte:

Gültige IPv4-Adresse

Gültige IPv6-Adresse

Aktiv

Aktiviert/deaktiviert die Tabellenzeile.

Mögliche Werte:

`markiert` (Voreinstellung)

Die Tabellenzeile ist aktiv.

Wenn das Gerät eine Anfrage für diesen Hostnamen empfängt, weist es dem anfragenden Gerät die verknüpfte IP-Adresse zu.

`unmarkiert`

Die Tabellenzeile ist inaktiv.

Wenn das Gerät eine Anfrage für diesen Hostnamen empfängt, leitet es die Anfrage an einen im Dialog *Erweitert > DNS > Client > Statisch* festgelegten DNS-Server weiter.

7.4 Industrie-Protokolle

[Erweitert > Industrie-Protokolle]

Das Menü enthält die folgenden Dialoge:

[IEC61850-MMS](#)

[Modbus TCP](#)

[OPC UA Server](#)

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 kann zu fehlerhaften Einstellungen im Gerät führen und möglicherweise Unterbrechungen im Netz zur Folge haben.

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.

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.

Konfiguration

Schaltflächen

 ICD-Datei herunterladen

Kopiert die ICD-Datei auf Ihren PC.

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 Lesezugriff 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

Das Gerät akzeptiert die folgenden Zeichen:

- `-`
- `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)

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)

7.4.3 OPC UA Server

[Erweitert > Industrie-Protokolle > OPC UA Server]

Das Protokoll *OPC UA* ist ein standardisiertes Protokoll für die industrielle Kommunikation, das in der Norm IEC 62541 definiert ist. Die Funktion *OPC UA Server* überwacht die *OPC UA*-Informationsmodell-Daten von Geräten für die industrielle Automatisierung wie speicherprogrammierbare Steuerungen (SPS), Sensoren und Messgeräte.

Um die *OPC UA*-Informationsmodell-Daten der angeschlossenen Endgeräte zu überwachen, verwenden Sie eine *OPC UA*-Client-Anwendung.

In diesem Dialog schalten Sie die Funktion *OPC UA Server* ein und legen die erforderlichen Einstellungen fest. Darüber hinaus können Sie in diesem Dialog die Anzahl der Sitzungen festlegen, die zeitgleich geöffnet sein dürfen. Der Dialog ermöglicht Ihnen die Verwaltung der *OPC UA*-Benutzerkonten, die erforderlich sind, um mit einer *OPC UA*-Client-Anwendung auf das Gerät zuzugreifen. Jeder *OPC UA*-Benutzer benötigt ein aktives *OPC UA*-Benutzerkonto, um Zugriff auf den *OPC UA*-Server des Geräts zu erhalten.

Funktion

Funktion

Schaltet die Funktion *OPC UA Server* im Gerät ein/aus.

Mögliche Werte:

An

Die Funktion *OPC UA Server* ist eingeschaltet.

Aus (Voreinstellung)

Die Funktion *OPC UA Server* ist ausgeschaltet.

Konfiguration

Listening-Port

Legt die TCP-Port-Nummer fest, die der *OPC UA Server*-Server für die Kommunikation verwendet.

Mögliche Werte:

1..65535 (Voreinstellung: 4840)

Ausnahme: Port 2222 ist für interne Funktionen reserviert.

Sitzungen (max.)

Legt fest, wie viele gleichzeitige *OPC UA*-Verbindungen zum Gerät maximal möglich sind. Jede zugreifende *OPC UA*-Client-Anwendung stellt eine separate *OPC UA*-Verbindung zum Gerät her.

Mögliche Werte:

1..5 (Voreinstellung: 5)

Security-Policy

Legt das Authentifizierungsprotokoll fest, welches das Gerät für den *OPC UA*-Benutzer anwendet.

Mögliche Werte:

kein (Voreinstellung)

Der *OPC UA*-Benutzer benötigt keine Authentifizierung.

basic128Rsa15

Der *OPC UA*-Benutzer authentifiziert sich mit dem Protokoll *Basic128Rsa15*.

basic256

Der *OPC UA*-Benutzer authentifiziert sich mit dem Protokoll *Basic256*.

basic256Sha256

Der *OPC UA*-Benutzer authentifiziert sich mit dem Protokoll *Basic256Sha256*.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Schaltflächen

 Hinzufügen

Öffnet das Fenster *Erzeugen*, um eine Tabellenzeile hinzuzufügen. Das Gerät ermöglicht Ihnen, bis zu 4 *OPC UA*-Benutzerkonten festzulegen.

- Im Feld *Benutzername* legen Sie die Bezeichnung des *OPC UA*-Benutzerkontos fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

Das Gerät akzeptiert die folgenden Zeichen:

a..z

A..Z

0..9

<Leerzeichen>

-

 Löschen

Entfernt die ausgewählte Tabellenzeile.

Benutzername

Zeigt den Namen des *OPC UA*-Benutzers, der Zugriff auf das Gerät mit einer *OPC UA*-Client-Anwendung hat.

Passwort

Legt das Passwort fest, das der Benutzer für den Zugriff auf das Gerät mit einer *OPC UA* Client-Anwendung verwendet.

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

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 6..64 Zeichen

Das Gerät akzeptiert die folgenden Zeichen:

- a..z
- A..Z
- 0..9
- !#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~

Rolle

Legt die Rolle fest, die den Zugriff des *OPC UA*-Benutzers mit einer *OPC UA*-Client-Anwendung regelt.

Mögliche Werte:

`read-only` (Voreinstellung)

Das Benutzerkonto *OPC UA* hat Lesezugriff auf das Gerät. Der *OPC UA*-Benutzer kann die *OPC UA*-Informationsmodell-Daten der angeschlossenen Endgeräte ansehen.

Aktiv

Aktiviert/deaktiviert das *OPC UA*-Benutzerkonto im Gerät.

Mögliche Werte:

`markiert`

Das *OPC UA*-Benutzerkonto ist aktiv. Das Gerät akzeptiert die Anmeldung eines *OPC UA*-Benutzers mit diesem Benutzernamen.

`unmarkiert` (Voreinstellung)

Das *OPC UA*-Benutzerkonto ist inaktiv. Das Gerät verweigert die Anmeldung eines *OPC UA*-Benutzers mit diesem Benutzernamen.

7.5 Tracking


[Erweitert > Tracking]

Die Tracking-Funktion ermöglicht Ihnen, sogenannte Tracking-Objekte zu überwachen. Überwachte Tracking-Objekte sind beispielsweise der Link-Status eines Interfaces oder die Erreichbarkeit eines entfernten Routers oder Endgeräts.

Das Gerät leitet Zustandsänderungen der Tracking-Objekte an die registrierten Applikationen weiter, zum Beispiel an die Routing-Tabelle oder an eine VRRP-Instanz. Die Applikationen reagieren daraufhin auf die Zustandsänderungen:

- Das Gerät aktiviert/deaktiviert in der Routing-Tabelle die mit dem Tracking-Objekt verknüpfte Route.
- Die mit dem Tracking-Objekt verknüpfte VRRP-Instanz reduziert die Priorität des virtuellen Routers, so dass ein Backup-Router die Rolle des Masters übernimmt.
- Wenn sich der Status des Tracking-Objekts ändert, aktiviert/deaktiviert das Gerät das mit dem Tracking-Objekt verknüpfte Interface. Das Gerät zeigt die zugehörige Anwendung im Dialog [Erweitert > Tracking > Applikationen](#).

Sobald Sie die Tracking-Objekte im Dialog [Erweitert > Tracking > Konfiguration](#) eingerichtet haben, können Sie Applikationen mit den Tracking-Objekten verknüpfen:

- Statische Routen verknüpfen Sie mit einem Tracking-Objekt im Dialog [Routing > Routing-Tabelle](#), Spalte [Track-Name](#).
- Virtuelle Router verknüpfen Sie mit einem Tracking-Objekt im Dialog [Routing > L3-Redundanz > VRRP > Tracking](#). Klicken Sie die Schaltfläche , um das Fenster [Erzeugen](#) zu öffnen und in der Dropdown-Liste [Track-Name](#) das Tracking-Objekt auszuwählen.
- Sie verknüpfen den Interface-Status mit einem Tracking-Objekt im Dialog [Grundeinstellungen > Port](#), Spalte [Track-Name](#).

Das Menü enthält die folgenden Dialoge:

[Tracking Konfiguration](#)
[Tracking Applikationen](#)

7.5.1 Tracking Konfiguration

[Erweitert > Tracking > Konfiguration]

In diesem Dialog richten Sie die Tracking-Objekte ein.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen“ auf Seite 16.

Schaltflächen



Hinzufügen

Öffnet das Fenster *Erzeugen*, um eine Tabellenzeile hinzuzufügen.

- Im Feld *Typ* legen Sie den Typ des Tracking-Objekts fest.
Mögliche Werte:
 - interface*
Das Gerät überwacht den Link-Status seiner physischen Ports, Link-Aggregation-, LRE- oder VLAN-Router-Interfaces.
 - logical*
Das Gerät überwacht logisch miteinander verknüpfte Tracking-Objekte und ermöglicht somit komplexe Überwachungsaufgaben.
- Im Feld *Track-ID* legen Sie die Identifikationsnummer des Tracking-Objektes fest.
Mögliche Werte:
 - 1..256



Löschen

Entfernt die ausgewählte Tabellenzeile.

Typ

Legt den Typ des Tracking-Objekts fest.

Mögliche Werte:

interface

Das Gerät überwacht den Link-Status seiner physischen Ports, Link-Aggregation-, LRE- oder VLAN-Router-Interfaces.

logical

Das Gerät überwacht logisch miteinander verknüpfte Tracking-Objekte und ermöglicht somit komplexe Überwachungsaufgaben.

Track-ID

Legt die Identifikationsnummer des Tracking-Objektes fest.

Mögliche Werte:

1..256

Dieser Bereich steht jedem Typ (*interface*, *ping* und *logical*) zur Verfügung.

Track-Name

Zeigt den Namen des Tracking-Objekts, der sich aus den in Spalte *Typ* und Spalte *Track-ID* angezeigten Werten zusammensetzt.

Aktiv

Aktiviert/deaktiviert die Überwachung des Tracking-Objekts.

Mögliche Werte:

markiert

Die Überwachung ist aktiv. Das Gerät überwacht das Tracking-Objekt.

unmarkiert (Voreinstellung)

Die Überwachung ist inaktiv.

Beschreibung

Legt die Beschreibung fest.

Beschreiben Sie hier, wofür das Gerät das Tracking-Objekt verwendet.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Status

Zeigt das Überwachungsergebnis des Tracking-Objekts.

Mögliche Werte:

up

Das Überwachungsergebnis ist positiv:

- Der Link-Status ist aktiv.
- oder
- Der entfernte Router oder das Endgerät ist erreichbar.
- oder
- Das Ergebnis der logischen Verknüpfung ist *WAHR*.

down

Das Überwachungsergebnis ist negativ:

- Der Link-Status ist inaktiv.
- oder
- Der entfernte Router oder das Endgerät ist unerreichbar.
- oder
- Das Ergebnis der logischen Verknüpfung ist *FALSCH*.

notReady

Die Überwachung des Tracking-Objekts ist inaktiv. Sie aktivieren die Überwachung in Spalte *Aktiv*.

Änderungen

Zeigt die Anzahl der Zustandsänderungen, seitdem das Tracking-Objekt aktiv ist.

Letzte Änderung

Zeigt den Zeitpunkt der letzten Zustandsänderung.

Trap senden

Aktiviert/deaktiviert das Senden eines SNMP-Traps, wenn jemand das Tracking-Objekt aktiviert oder deaktiviert.

Mögliche Werte:

`markiert`

Das Gerät sendet einen SNMP-Trap, wenn jemand das Tracking-Objekt in Spalte *Aktiv* aktiviert oder deaktiviert.

`unmarkiert` (Voreinstellung)

Das Gerät sendet keinen SNMP-Trap.

Port

Legt für Tracking-Objekte des Typs *interface* das zu überwachende Interface fest.

Mögliche Werte:

`<Interface-Nummer>`

Nummer des physischen Ports, des Link-Aggregation-, LRE- oder VLAN-Router-Interfaces.

`no Port`

Kein Tracking-Objekt des Typs *interface*.

Link-Up Verzögerung [s]

Legt die Zeit in Sekunden fest, nach der das Gerät das Überwachungsergebnis als positiv erkennt. Wenn der Link auf dem Interface länger als die hier festgelegte Zeit aktiv ist, zeigt Spalte *Status* den Wert *up*.

Mögliche Werte:

`0..255`

`-`

Kein Tracking-Objekt des Typs *logical*.

Link-Down Verzögerung [s]

Legt die Zeit in Sekunden fest, nach der das Gerät das Überwachungsergebnis als negativ erkennt. Wenn der Link auf dem Interface länger als die hier festgelegte Zeit inaktiv ist, zeigt Spalte *Status* den Wert *down*.

Mögliche Werte:

`0..255`

`-`

Kein Tracking-Objekt des Typs *interface*.

Link-Aggregation-, LRE- und VLAN-Router-Interfaces haben ein negatives Überwachungsergebnis, wenn die Verbindung jedes aggregierten Ports unterbrochen ist.

Ein VLAN-Router-Interface hat ein negatives Überwachungsergebnis, wenn die Verbindung zu jedem physischen Port und Link-Aggregation-Interface, das Mitglied im VLAN ist, unterbrochen ist.

Logischer Operand A

Legt für Tracking-Objekte des Typs *logical* den ersten Operanden der logischen Verknüpfung fest.

Mögliche Werte:

Eingerichtete Tracking-Objekte

–

Kein Tracking-Objekt des Typs *logical*.

Logischer Operand B

Legt für Tracking-Objekte des Typs *logical* den zweiten Operanden der logischen Verknüpfung fest.

Mögliche Werte:

Eingerichtete Tracking-Objekte

–

Kein Tracking-Objekt des Typs *logical*.

Operator

Verknüpft die in den Feldern *Logischer Operand A* und *Logischer Operand B* festgelegten Tracking-Objekte.

Mögliche Werte:

and

Logische UND-Verknüpfung

or

Logische ODER-Verknüpfung

–


Kein Tracking-Objekt des Typs *logical*.

7.5.2 Tracking Applikationen

[Erweitert > Tracking > Applikationen]

In diesem Dialog sehen Sie, welche Applikationen mit den Tracking-Objekten verknüpft sind.

Die folgenden Applikationen lassen sich mit Tracking-Objekten verknüpfen:

- Statische Routen verknüpfen Sie mit einem Tracking-Objekt im Dialog [Routing > Routing-Tabelle](#), Spalte [Track-Name](#).
- Virtuelle Router verknüpfen Sie mit einem Tracking-Objekt im Dialog [Routing > L3-Redundanz > VRRP > Tracking](#). Klicken Sie die Schaltfläche , um das Fenster [Erzeugen](#) zu öffnen und in der Dropdown-Liste [Track-Name](#) das Tracking-Objekt auszuwählen.
- Sie verknüpfen den Interface-Status mit einem Tracking-Objekt im Dialog [Grundeinstellungen > Port](#), Spalte [Track-Name](#).

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „[Arbeiten mit Tabellen](#)“ auf [Seite 16](#).

Typ

Zeigt den Typ des Tracking-Objekts.

Track-ID

Zeigt die Identifikationsnummer des Tracking-Objektes.

Applikation

Zeigt den Namen der Applikation, die mit dem Tracking-Objekte verknüpft ist.

Mögliche Werte:

Tracking-Objekte des Typs *logical*
 Statische Routen
 Virtuelle Router einer VRRP-Instanz
 Interface-Status

Track-Name

Zeigt den Namen des Tracking-Objekts, der sich aus den in Spalte [Typ](#) und Spalte [Track-ID](#) angezeigten Werten zusammensetzt.

7.6 Command Line Interface

[Erweitert > CLI]

Dieser Dialog ermöglicht Ihnen, mit dem Command Line Interface auf das Gerät zuzugreifen.

Voraussetzungen:

- Im Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH* ist der SSH-Server eingeschaltet.
- Installieren Sie auf Ihrer Workstation eine SSH-fähige Client-Anwendung, die in Ihrem Betriebssystem einen Handler für URLs registriert, die mit `ssh://` beginnen.

Schaltflächen

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 Webbrowser eine SSH-fähige Client-Anwendung findet, dann stellt der SSH-fähige Client eine Verbindung mit dem SSH-Protokoll zum Gerät her.

A Stichwortverzeichnis

0-9	
802.1D/p-Mapping	215
802.1X	91, 134
A	
Access-Control-Listen	164
ACL	164
Adresskonflikt-Erkennung	296
Aging-Time	175
Alarm	286, 289
Anforderungsintervall	79
ARP	296
ARP-Tabelle	71, 300
Audit-Trail	362
Ausgangs-Lastbegrenzer	178
Authentifizierungs-Historie	147
Authentifizierungs-Liste	91
Auto-Disable	130, 131, 237, 325, 326, 332, 349
B	
Benutzerverwaltung	85
Betriebszeit	21, 293
Bridge	234
C	
CLI	121
Command Line Interface	121
Community-Namen	123
D	
DHCP-L2-Relay	363
DHCP-Server	368
DHCPv6-L2-Relay	363
DNS	377
DNS-Cache	378
DNS-Client	378
Domain Name System	377
DoS	160
DSCP	216
Duplicate Address Detection	33
E	
EAPOL	145
Eingangs-Lastbegrenzer	178
Einstellungen	41
E-Mail-Benachrichtigung	72, 304
ENVM	40, 46, 49, 54, 268, 274, 281, 359
Ereignis-Schweregrad	309, 356
Externer Speicher	22, 40, 46, 49, 54, 359
F	
FDB	181
Fingerprint	111, 115
Flash-Speicher	40, 293
Flusskontrolle	175
Forwarding-Tabelle	181

G	
GARP	207
Geräte-Software	38
Geräte-Software Backup	38
Gerätestatus	19, 266
GMRP	208
Grenzwerte Netzlast	178
Guards	245
GVRP	210
H	
Hardware-Uhr	73
Hardware-Zustand	293
Häufig gestellte Fragen	407
HiDiscovery	27, 275, 362
Host-Key	111
HTML	292, 361
HTTP	112
HTTPS	113
HTTP-Server	273
I	
IAS	91, 149
IEC61850 MMS	276, 385
IEEE 802.1X	91
IGMP-Snooping	72, 183
Industrial HiVision	9, 106
Ingress Filtering	225
Integrierter Authentifikations-Server	91, 149
IP-Adressen Konflikterkennung	296
IP-DSCP-Mapping	216
IPv4-Regel	165
IP-Zugriffsbeschränkung	117
K	
Kabeldiagnose	320
Konfigurations-Check	294
Konfigurationsprofil	16, 41
L	
L2-Relay	363
Laden/Speichern	41
Lastbegrenzer	178
LDAP	91
Link-Aggregation	248
Link-Backup	255
LLDP	339
Logdatei	70, 72, 361
Login-Banner	122, 125
Loops	233
Loop-Schutz	281

M	
MAC-Adress-Filter	181
MAC-Adress-Tabelle	71, 181
MAC-Flooding	129
MAC-Regel	169
MAC-Spoofing	131
Management-VLAN	27
Management-Zugriff	27, 32, 117
Manufacturing Message Specification	385
Media Redundancy Protocol	230
MMRP	199
MMS	385
Modbus TCP	276, 388
Module	268, 281
MRP	230
MRP-IEEE	197
MVRP	204
N	
Netzlast	62
Netzteil	21, 269, 282
Neustart	70
NVM	16, 40, 46
O	
Out-of-Band-Management-Port	36
P	
Passwort	86, 272
Passwort-Länge	86, 272
Persistente Log-Datei	72
Persistentes Ereignisprotokoll	358
PoE	63
Port-basierte Zugriffskontrolle	134
Port-Clients	143
Port-Konfiguration	137, 213
Port-Mirroring	336
Port-Monitor	332
Port-Priorität	213
Portsicherheit	129
Port-Statistiken	72, 145
Port-VLAN	224
Power over Ethernet	63
Pre-Login-Banner	125
Q	
Queue-Management	218
Queues	212
R	
RADIUS	91, 150
RAM	46
RAM-Test	302
Relay	363
Ringstruktur	230
Root-Bridge	234
RSTP	233, 234

S	
Schulungsangebote	407
Schweregrad	309, 356
Secure Shell	108
Selbsttest	302
Serielle Schnittstelle	274
SFP-Modul	319
Sicherheitsstatus	20, 271
Signalkontakt	20, 277
SNMP-Server	106, 274
SNMP-Traps	60, 66, 131, 234, 251, 267, 271, 279, 286, 289, 298, 325, 396
SNMPv1/v2	123
SNTP	77
SNTP-Client	78
SNTP-Server	82
Software-Backup	38
Software-Update	38
Sommerzeit	74
Spanning Tree Protocol	233
SSH-Server	108
Statistik Zugriffe auf Management	72
Sub-Ring	259
Support-Informationen	353
Support-Informationen (ZIP-Archiv)	356
Syslog	314
System Log	361
Systeminformationen	292
System-Monitor	302
Systemzeit	73
T	
Technische Fragen	407
Telnet-Server	107, 273
Temperatur	21, 267, 280
Topologie-Erkennung	344
Tracking	393
Traps	60, 66, 131, 234, 251, 267, 271, 279, 286, 289, 298, 325, 396
Trap-Ziel	286, 289
Trust Modus	213
Twisted-Pair	320
U	
Unaware-Modus	175
Unsignierte Gerätesoftware (Hochladen zulassen)	40
USB-Netzanschluss	36
V	
Verschlüsselung	41
Virtual Local Area Network	219
VLAN	27, 219, 351
VLAN Konfiguration	221
VLAN-Ports	224
VLAN-Unaware-Modus	175
W	
Warteschlange (Queue)	212
Watchdog	41, 51
Webserver	112, 113

Z

Zähler-Reset	70
Zertifikat	21, 46, 97, 114, 115, 276, 306, 315
ZIP-Archiv mit Support-Informationen	356
Zugriffsbeschränkung	117
Zugriffskontrolle	134

B Weitere Unterstützung

Technische Fragen

Bei technischen Fragen wenden Sie sich bitte an den Hirschmann-Vertragspartner in Ihrer Nähe oder direkt an Hirschmann.

Die Adressen unserer Vertragspartner finden Sie im Internet unter www.hirschmann.com.

Eine Liste von Telefonnummern und E-Mail-Adressen für direkten technischen Support durch Hirschmann finden Sie unter hirschmann-support.belden.com. Sie finden auf dieser Website außerdem eine kostenfreie Wissensdatenbank sowie einen Download-Bereich für Software.

Technische Unterlagen

Die aktuellen Handbücher und Bedienungsanleitungen für Hirschmann-Produkte finden Sie unter doc.hirschmann.com.

Customer Innovation Center

Das Customer Innovation Center mit dem kompletten Spektrum innovativer Dienstleistungen hat vor den Wettbewerbern gleich dreifach die Nase vorn:

Das Consulting umfasst die gesamte technische Beratung von der Systembewertung über die Netzplanung bis hin zur Projektierung.

Das Training bietet Grundlagenvermittlung, Produkteinweisung und Anwenderschulung mit Zertifizierung.

Das aktuelle Schulungsangebot zu Technologie und Produkten finden Sie unter www.belden.com/solutions/customer-innovation-center.

Der Support reicht von der Inbetriebnahme über den Bereitschaftsservice bis zu Wartungskonzepten.

Mit dem Customer Innovation Center entscheiden Sie sich in jedem Fall gegen jeglichen Kompromiss. Das kundenindividuelle Angebot lässt Ihnen die Wahl, welche Komponenten Sie in Anspruch nehmen.

C Leserkritik

Wie denken Sie über dieses Handbuch? Wir sind stets bemüht, in unseren Handbüchern das betreffende Produkt vollständig zu beschreiben und wichtiges Hintergrundwissen zu vermitteln, um Sie beim Einsatz dieses Produkts zu unterstützen. Ihre Kommentare und Anregungen unterstützen uns, die Qualität und den Informationsgrad dieser Dokumentation noch zu steigern.

Ihre Beurteilung für dieses Handbuch:

	sehr gut	gut	befriedigend	mäßig	schlecht
Exakte Beschreibung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lesbarkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Verständlichkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Beispiele	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Aufbau	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vollständigkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Grafiken	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Zeichnungen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tabellen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Haben Sie in diesem Handbuch Fehler entdeckt?
 Wenn ja, welche auf welcher Seite?

Anregungen, Verbesserungsvorschläge, Ergänzungsvorschläge:

Allgemeine Kommentare:

Absender:

Firma / Abteilung:

Name / Telefonnummer:

Straße:

PLZ / Ort:

E-Mail:

Datum / Unterschrift:

Sehr geehrter Anwender,

bitte schicken Sie dieses Blatt ausgefüllt zurück
als Fax an die Nummer +49 (0)7127 14-1600 oder
per Post an
Hirschmann Automation and Control GmbH
Abteilung 01RD-NT
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Deutschland



HIRSCHMANN

A **BELDEN** BRAND



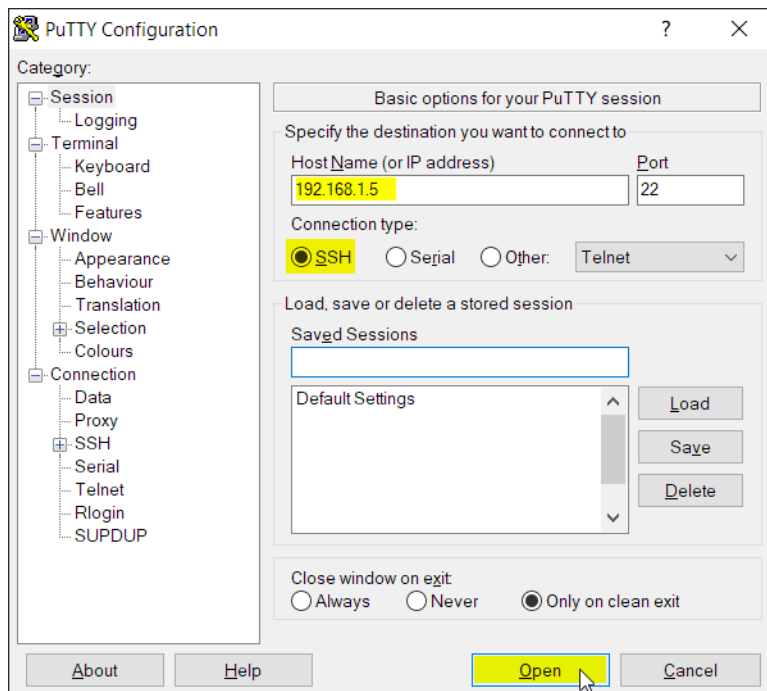
HIRSCHMANN

A **BELDEN** BRAND

[Grid of empty boxes for text input]








[Progress bar]

[Progress bar]

[Progress bar]

PuTTY Security Alert [X]

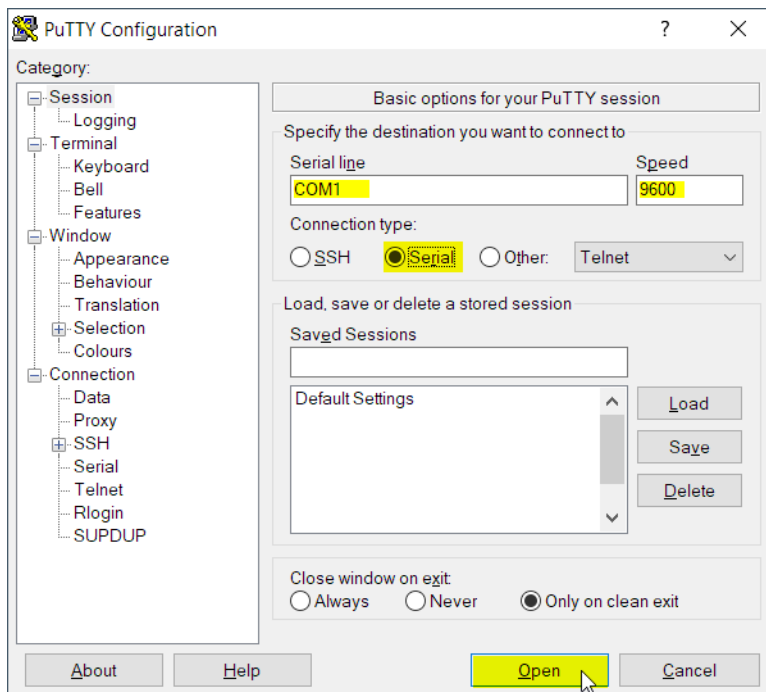
 The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.

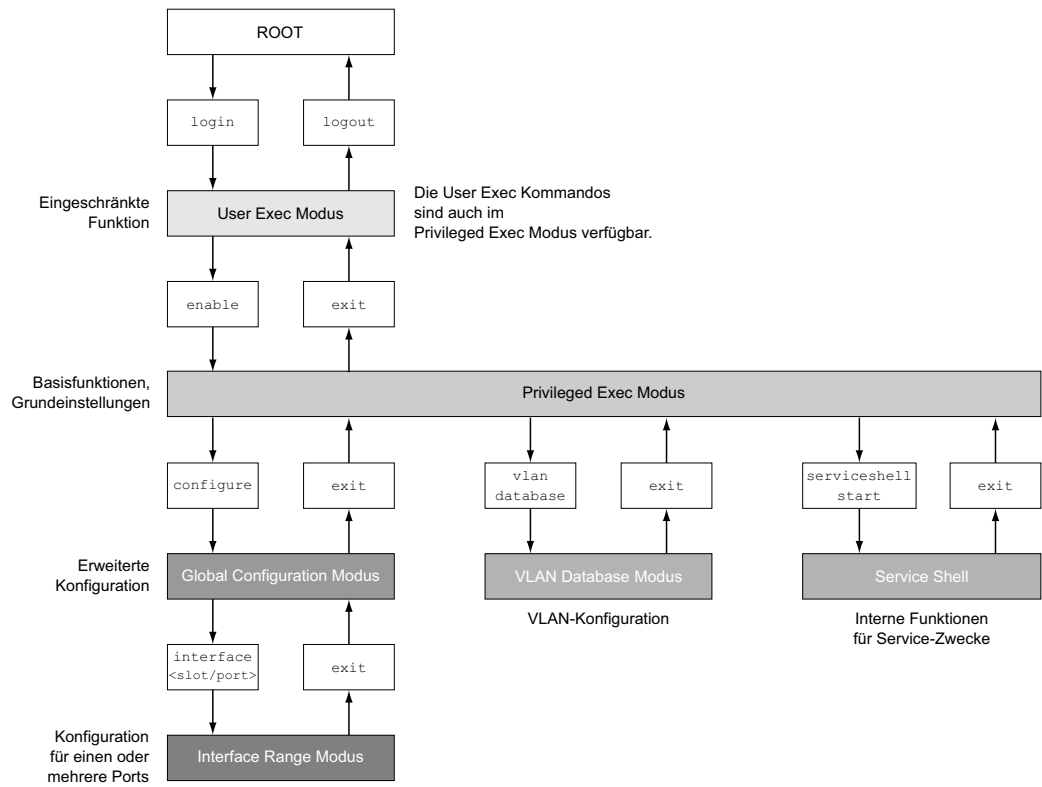
The server's rsa2 key fingerprint is:
ssh-rsa 2048 SHA256:1GepSdba8L0wRvKRLvDJ9iVeNEpFOu4sDCWXdyGK14Y

If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting.

If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".

If you do not trust this host, press "Cancel" to abandon the connection.







.....
.....
.....

.....

.....
.....

.....
.....
.....
.....

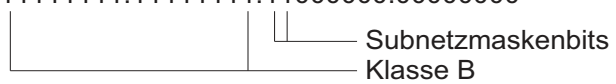
.....
.....

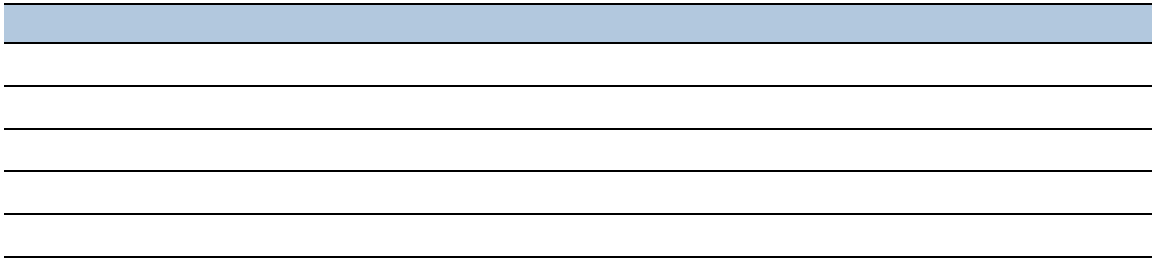
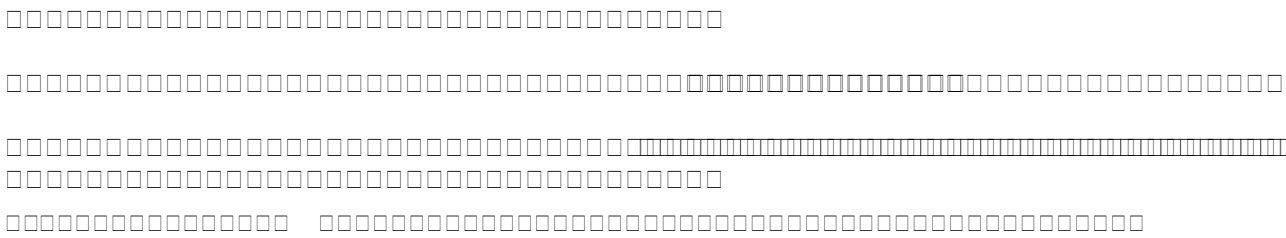
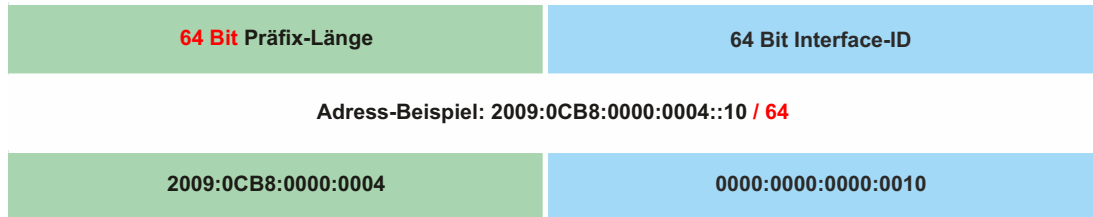
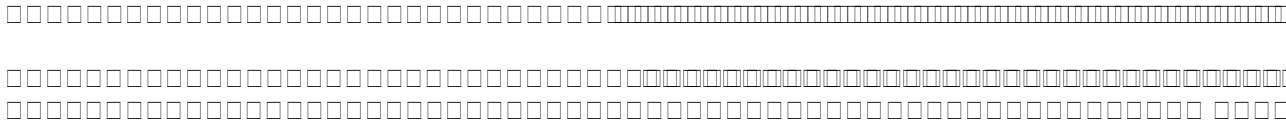
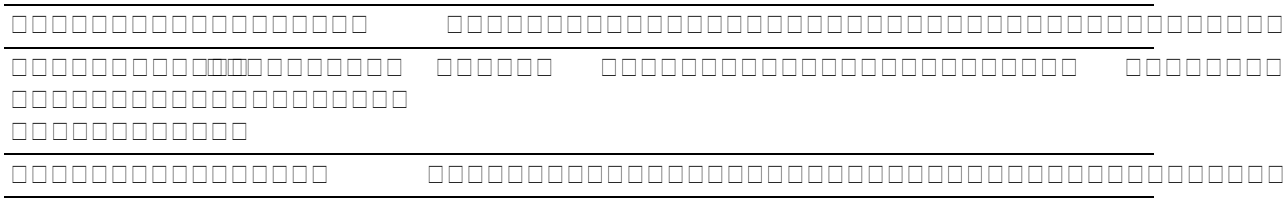


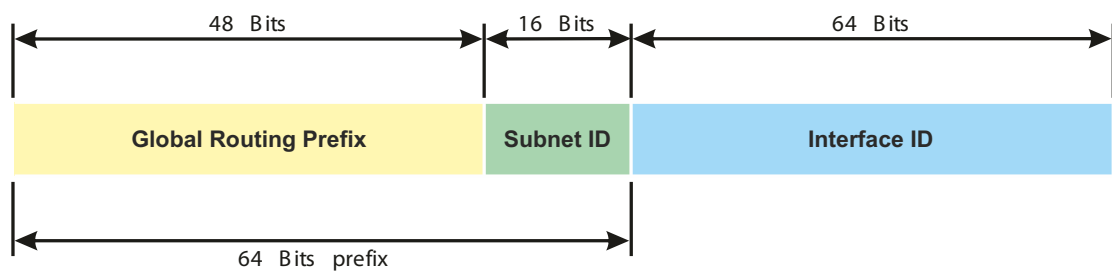
0	Net ID - 7 bits	Host ID - 24 bits	Klasse A
1 0	Net ID - 14 bits	Host ID - 16 bits	Klasse B
1 1 0	Net ID - 21 bits	Host ID - 8 bits	Klasse C
1 1 1 0	Multicast Group ID - 28 bits		Klasse D
1 1 1 1	reserved for future use - 28 bits		Klasse E

Dezimale Darstellung
255.255.192.0

Binäre Darstellung
11111111.11111111.11000000.00000000







|
|
|



|
|
|

```
NOTE: Enter '?' for Command Help. Command help displays all opt  
that are valid for the particular mode.  
For the syntax of a particular command form, please  
consult the documentation.  
!  
! ( ) >
```




[A light blue shaded rectangular box]

.....

.....

.....

.....

.....

.....

.....

.....

.....
.....
.....

.....
.....

.....

.....
.....
.....
.....
.....
.....

.....
.....
.....
.....
.....
.....
.....
.....

.....
.....

.....



□□□□□□□□□□



-

Form with 1 blue header bar and 8 horizontal lines.

Row of 30 small square boxes



Row of 25 small square boxes

Row of 8 small square boxes



Row of 30 small square boxes



□□
 □□
 □□

□□



□□

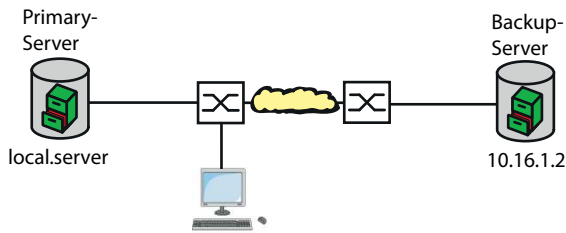


□□



.....
.....
.....

.....
.....
.....
.....



.....

.....



.....
.....

.....
.....



.....



.....
.....



□□□□□□□□□□□□□□

-







□□

-





□□□□□□□□□□

-

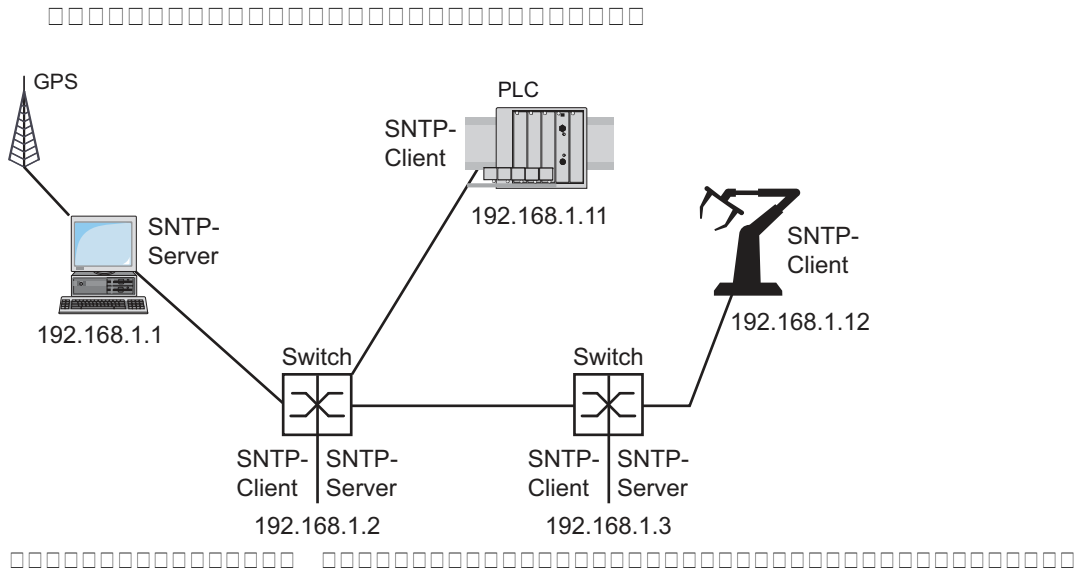


□□□□□□□□□□

-







□□□□□□□□□□□□□□□□□□□□□□

田+

✓



Form section 1: A light blue header bar followed by three horizontal lines.



Form section 2: A light blue header bar followed by four horizontal lines.



□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□











□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

-



□□□□□□□□□□□□□□□□□□□□

-



□□□□□□□□□□□□□□□□

-

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

-

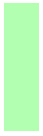
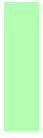


□□□□□□□□□□

□□□□□□□□□□



-
-





□□□□□□□□

-



□□□□□□□□

-



□□□□□□□□

-







-



-

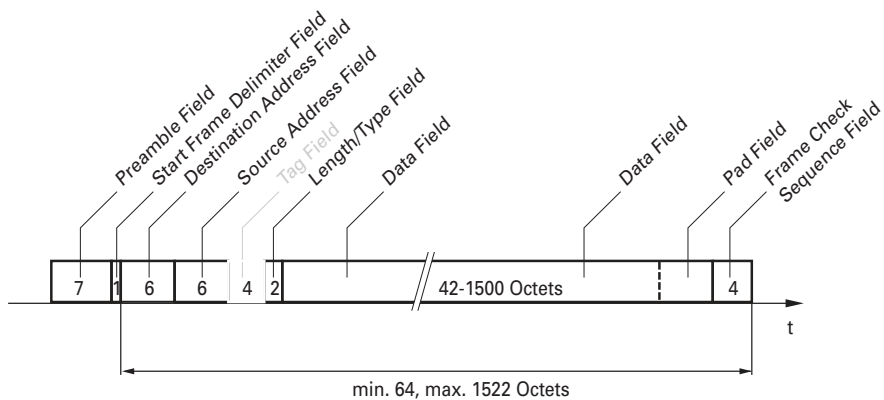
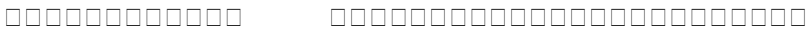
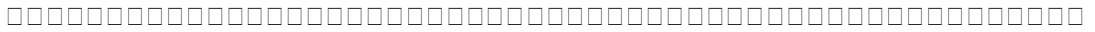
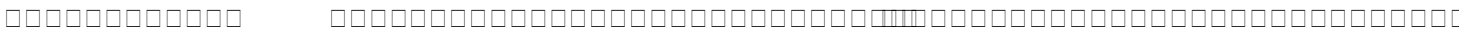
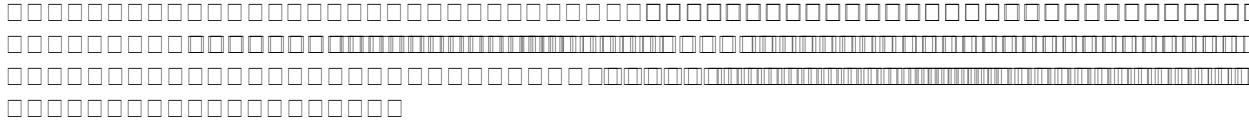


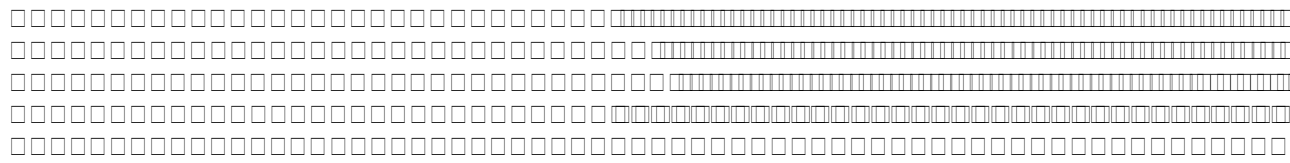
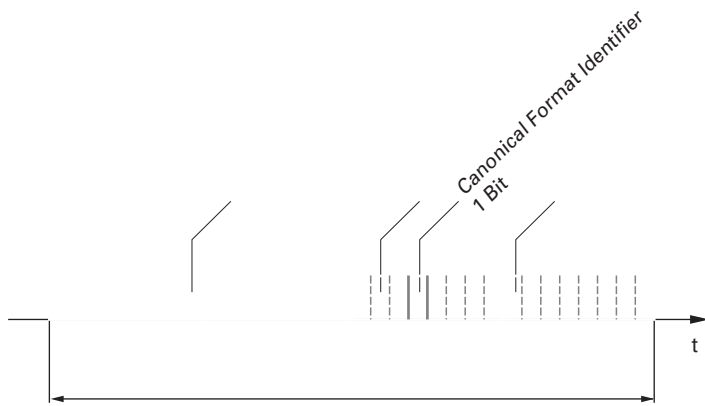


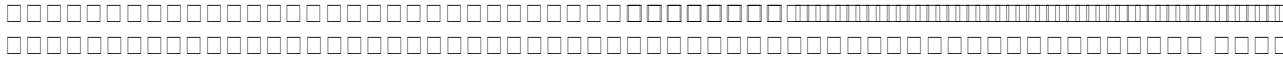
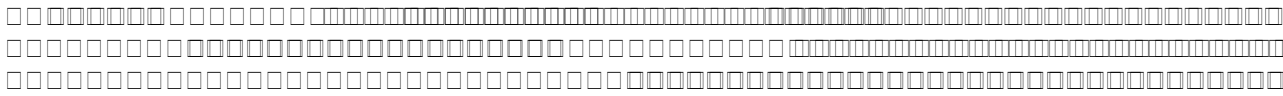
□□□□□□□□□□□□□□

-













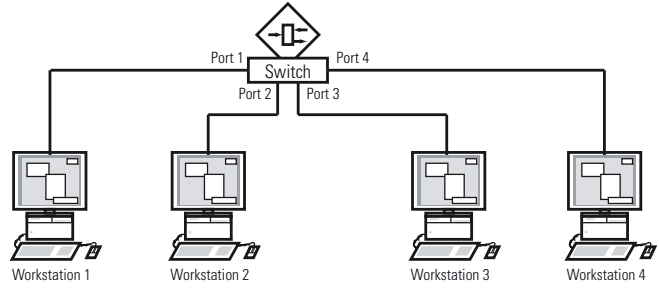
□□□□□□□□

-



.....

.....



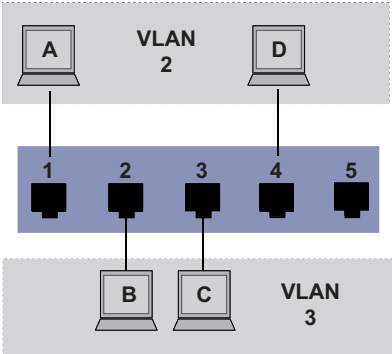
.....

.....

.....

.....







⌘
+



-□□□□□

-□□□□□





□□□□□□□□□□

-□□□□□□

-

□□□□□□□□□□

-□□□□□□

-

□□□□□□□□□□

-□□□□□□

-

□□□□□□□□□□

-□□□□□□

-

[Blue bar]

[Horizontal lines]

[Blue bar]

[Horizontal lines]

[Blue bar]

[Horizontal lines]

[Barcode]

[Barcode]



田
+

[Barcode]



-□□□□□

-□□□□□





□□□□□□□□□□



□□□□□□□□□□

-□□□□□□

□□□□□□□□□□

-□□□□□□

□□□□□□□□□□

-□□□□□□

□□□□□□□□□□

-□□□□□□

□□□□□□□□□□

-□□□□□□



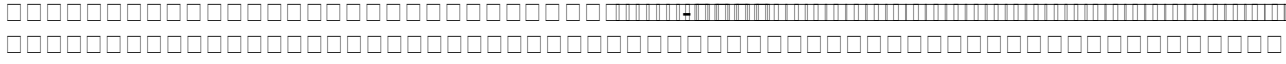


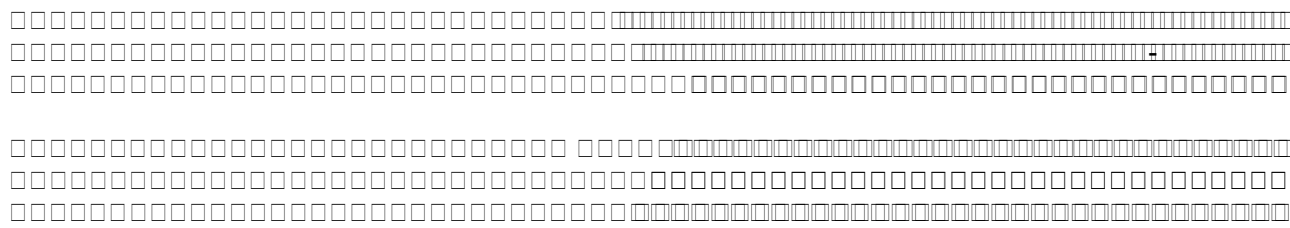
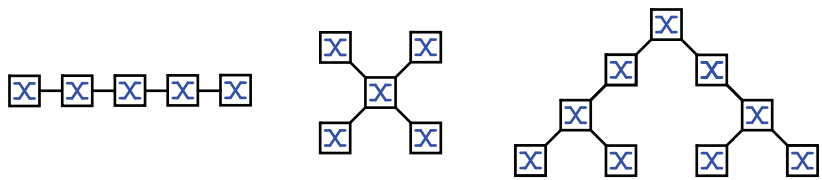
□□□□□□□□

-

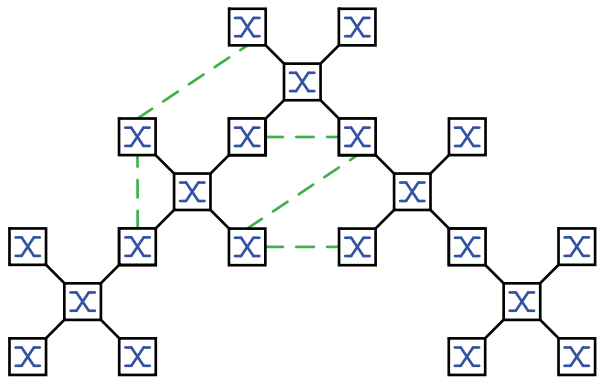
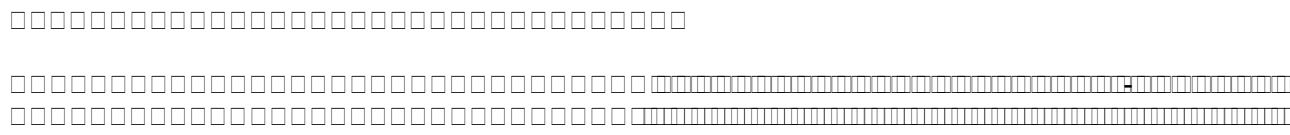


-

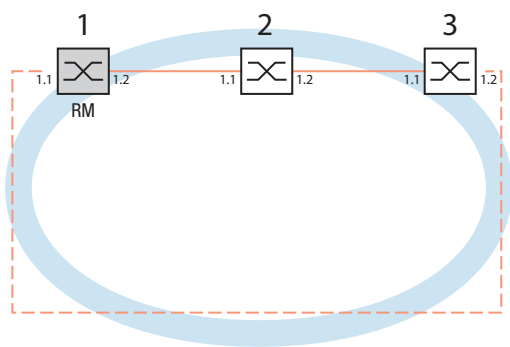


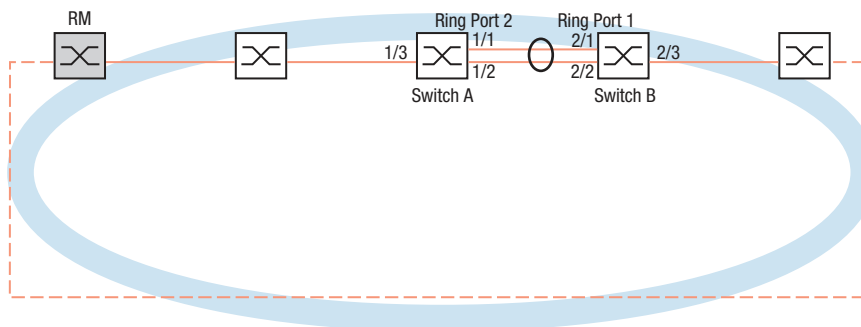
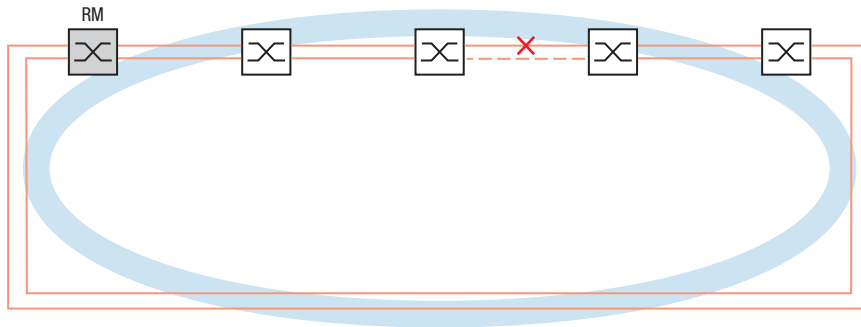


□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□



□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□





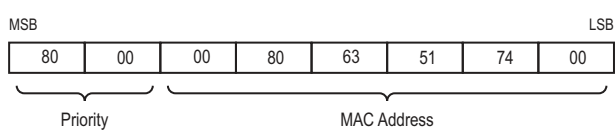
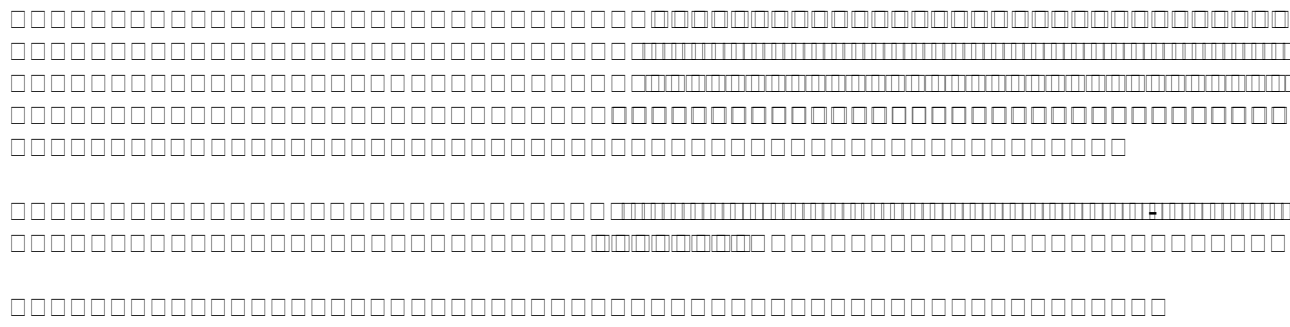


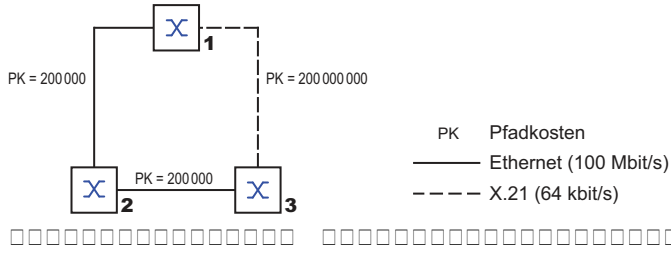
..... -
.....

-

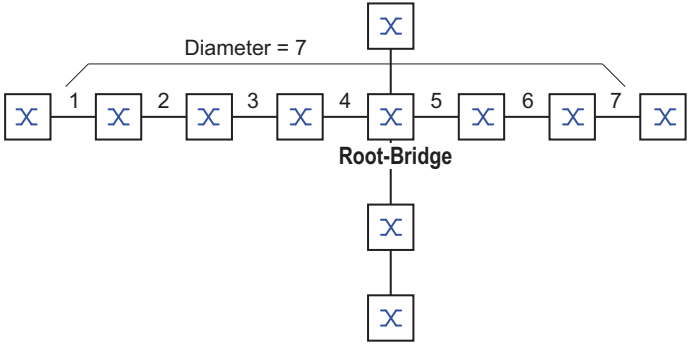
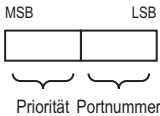
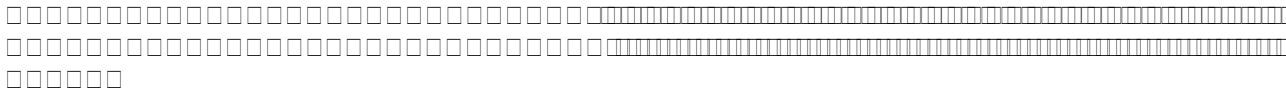
-

-

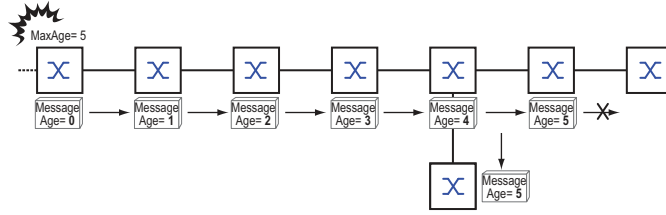


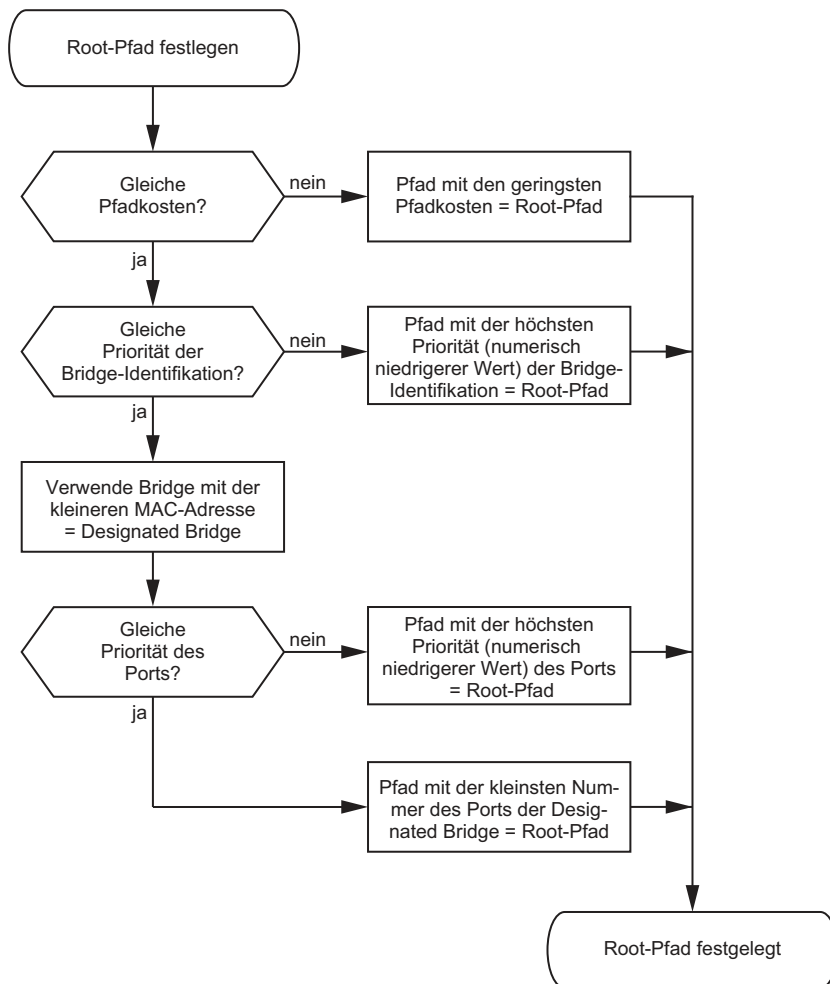


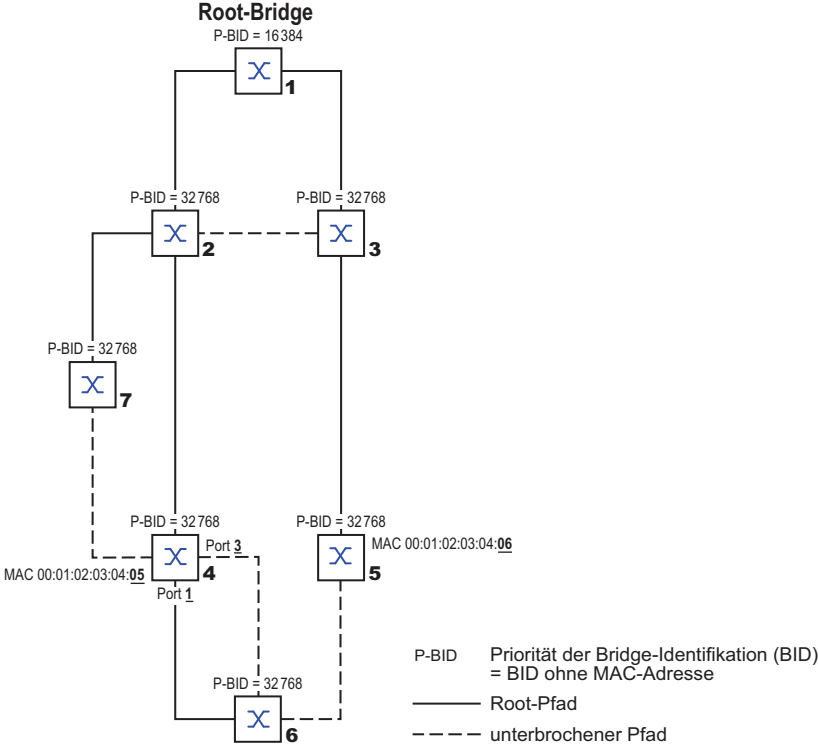
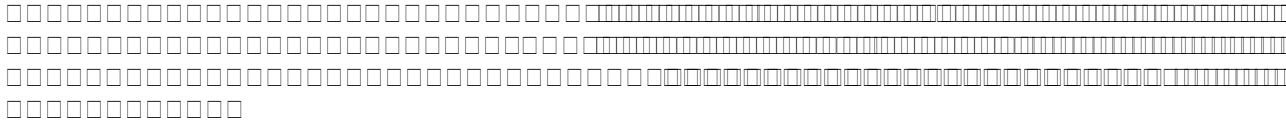
	PK	Bandwidth
Link 1 (X2 to X1)	200 000	Ethernet (100 Mbit/s)
Link 2 (X1 to X3)	200 000 000	X.21 (64 kbit/s)
Link 3 (X2 to X3)	200 000	Ethernet (100 Mbit/s)

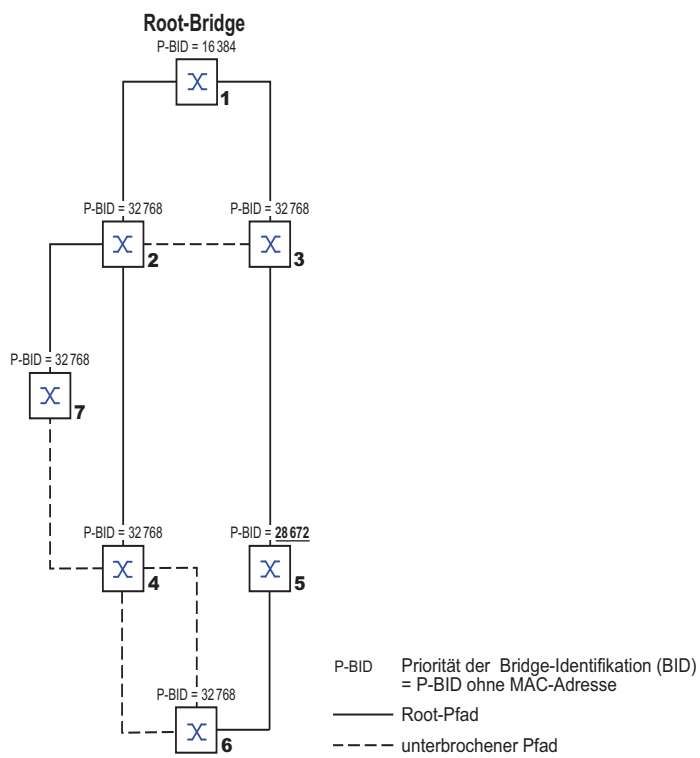


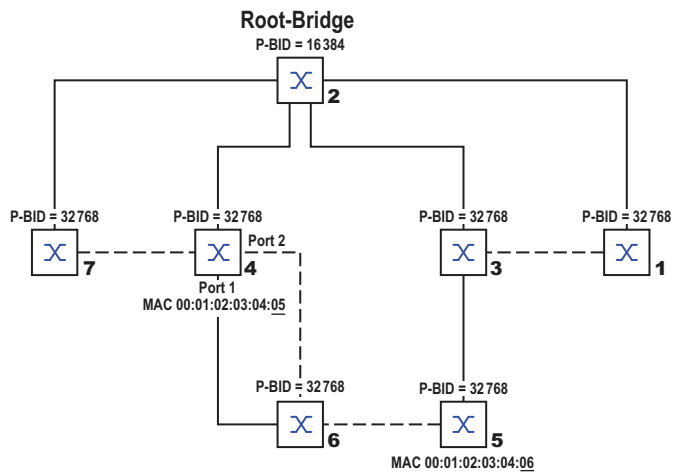
Root-Bridge







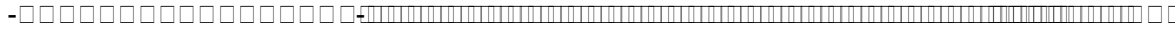




P-BID Priorität der Bridge-Identifikation (BID)
 = P-BID ohne MAC-Adresse

———— Root-Pfad

- - - - - unterbrochener Pfad





□□□□□□□□

□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□



□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□





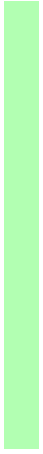
□□□□□□□□

-



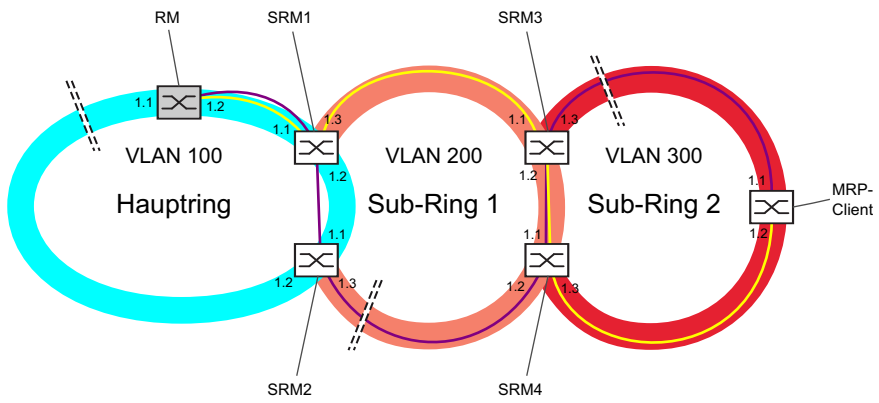
⌘
+

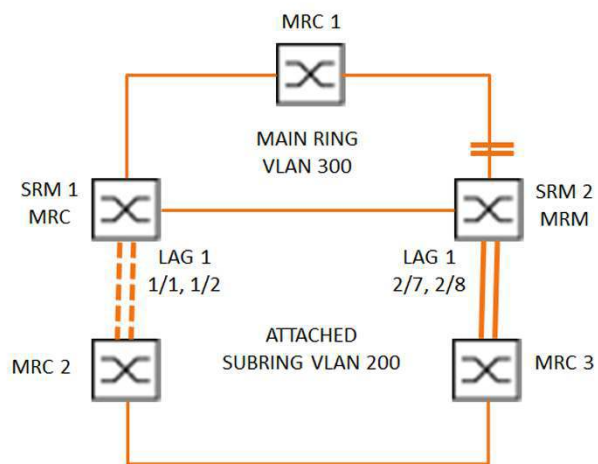






□□□□□□□□□□□□□□□□





□□□□□□□□ -



1

2

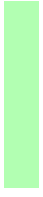
3

4



□□□□□□□□

-







□□□□□□□□

-



□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□

-
-



B
+

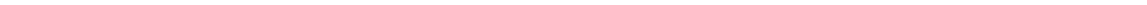






□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□



□□□□□□□□□□



□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□



□□□□□□□□□□□□□□□□□□□□
□□□

□□□



□□□





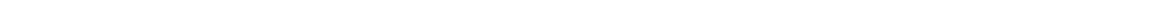
□□□□□□□□

□□□□□□□□



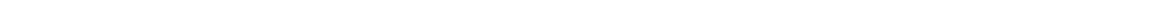
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

-



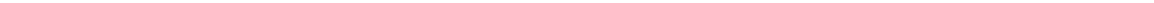
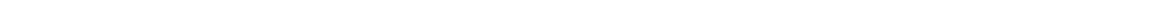
□□□□□□□□□□□□□□□□□□□□□□□□□□□□

-



□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

-

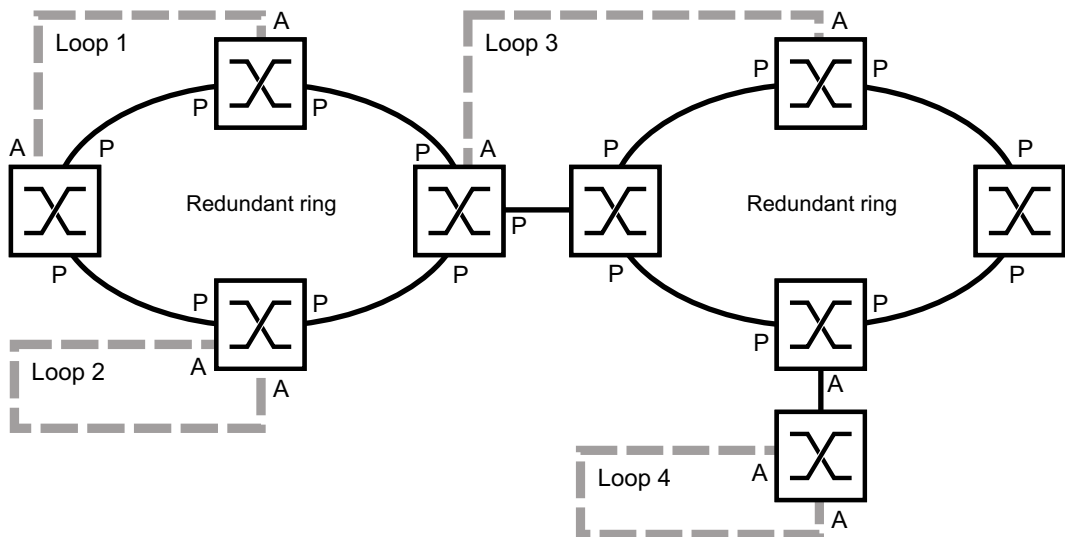
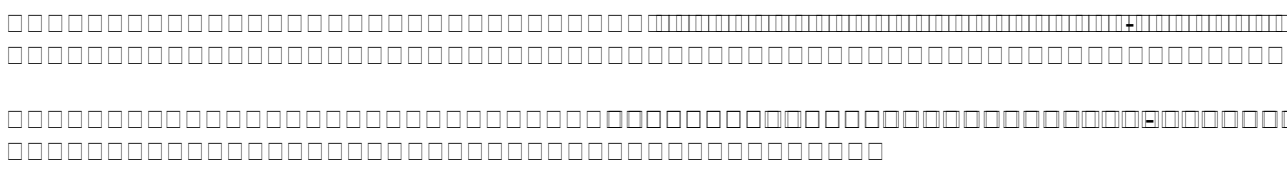




□□□□□□□□

-



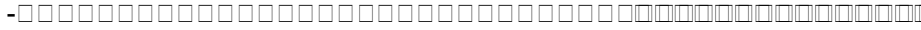
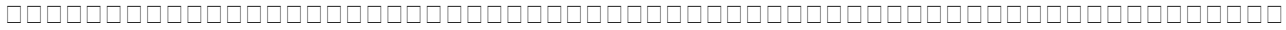
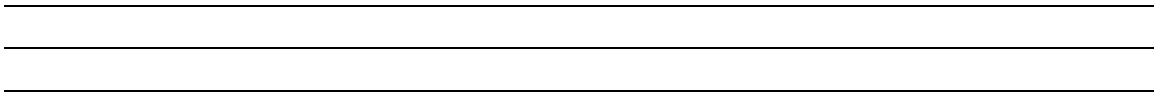




□□□□□□□□□□









Two rows of empty checkboxes



Two rows of empty checkboxes





B+







-





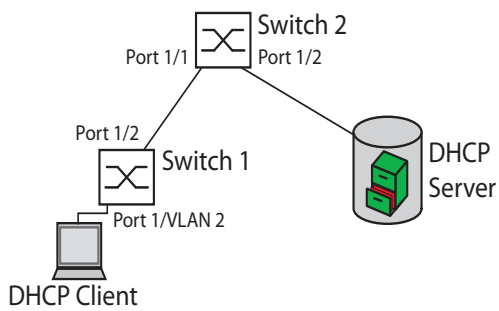
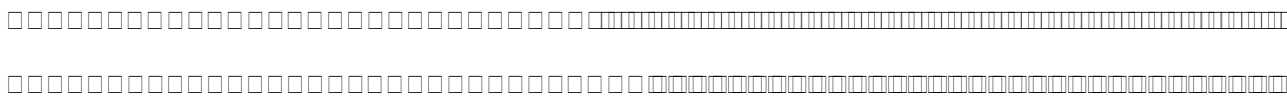


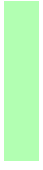
B+



□□□□□□□□

-









-□□□□□□□□□□□□□□□□

-□□□□□□□□□□□□□□□□

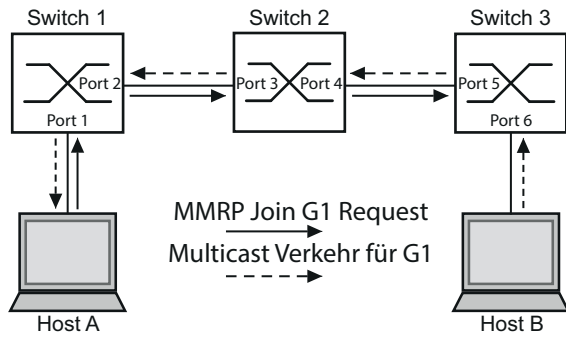


□□□□□□□□□□□□

⌘
+

-





□□□□□□□□□□

□□□□□□□□□□

-

-



□□□□□□□□

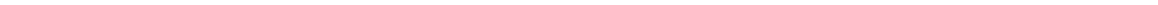
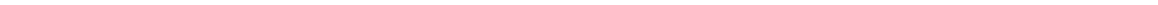
-

□□□□□□□□

-



□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□



[Blue shaded header bar]

[Lined writing area]

[Blue shaded header bar]

[Lined writing area]



A series of horizontal lines for writing, consisting of 27 evenly spaced black lines that fill the remaining page area.

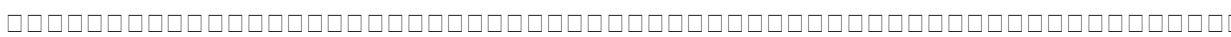




田+

✓

✓



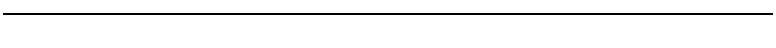
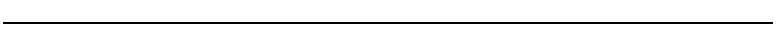
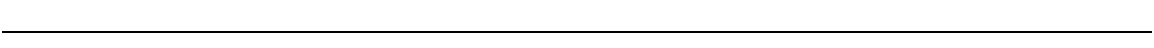
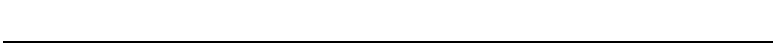
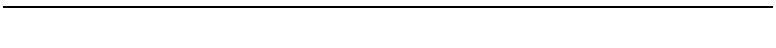
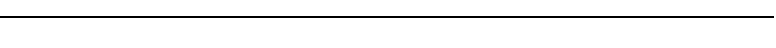
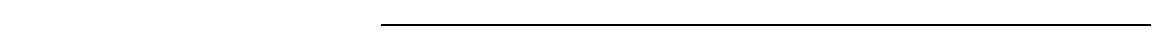
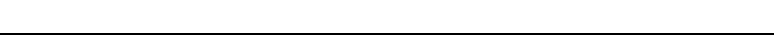
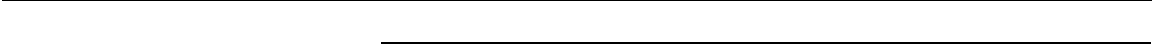
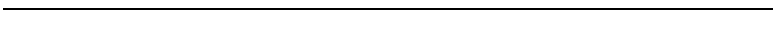
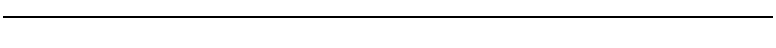
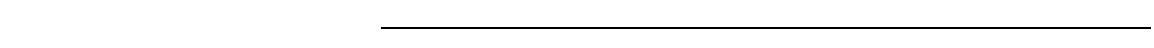
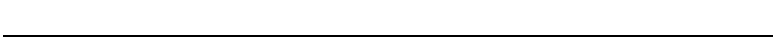
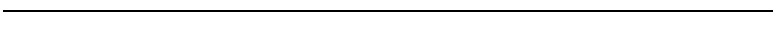
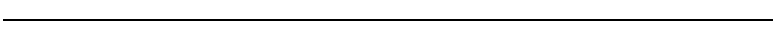
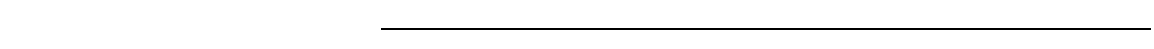
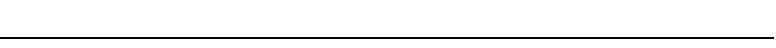
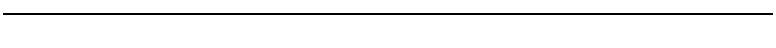
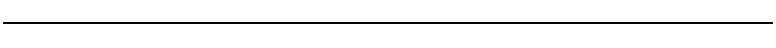
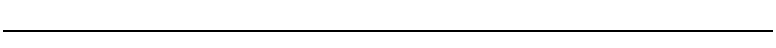
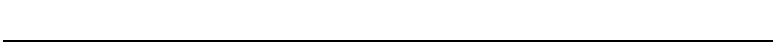
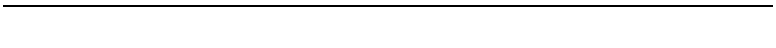
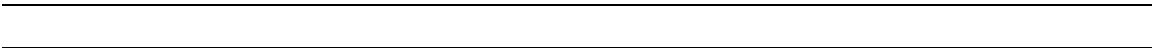
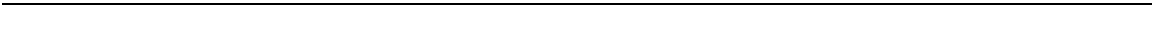




□□□□□□□□□□□□□□□□□□□□□□□□□□□□



□□□
□□□□□□□□□□□□





Handwriting practice lines consisting of a series of horizontal lines. Each line is preceded by a vertical line on the left, creating a grid-like structure for writing practice.

Handwriting practice row 1: A series of small squares followed by a series of small rectangles.

Handwriting practice row 2: A series of small squares followed by a series of small rectangles.

Handwriting practice row 3: A series of small squares followed by a series of small rectangles.

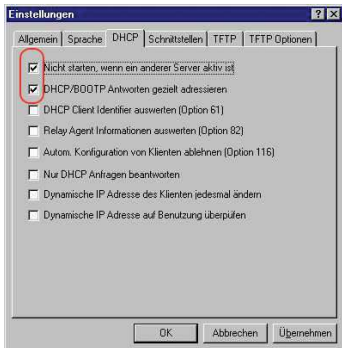
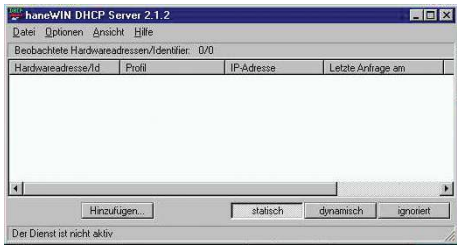
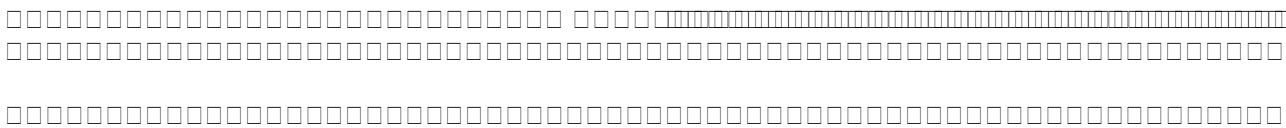


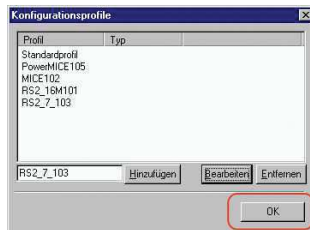
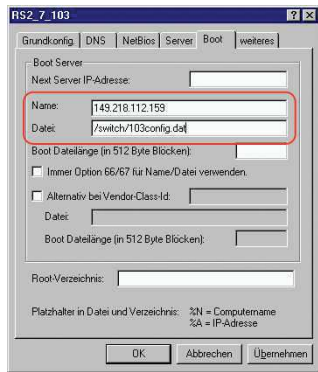
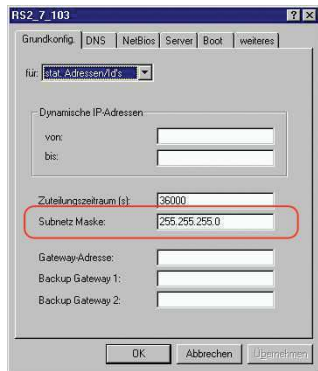
B+

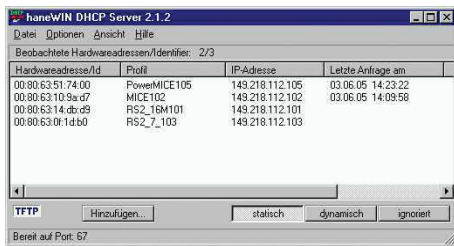
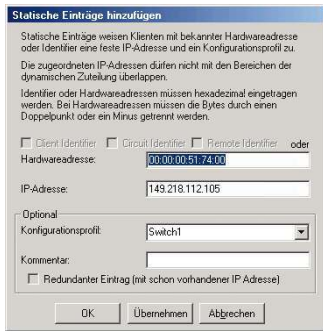
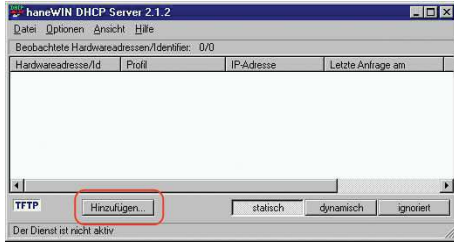
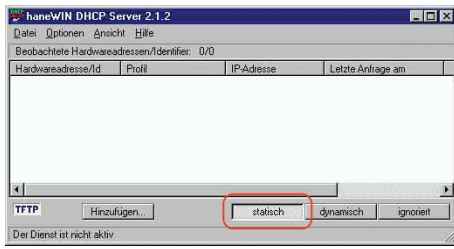


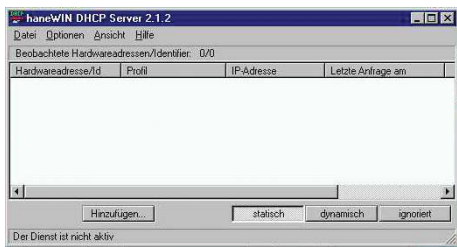
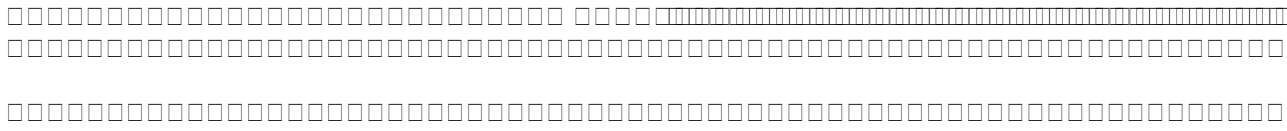


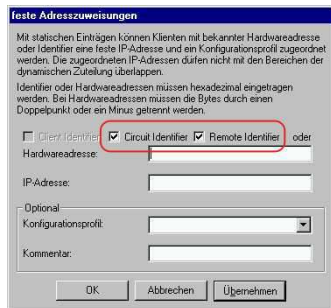
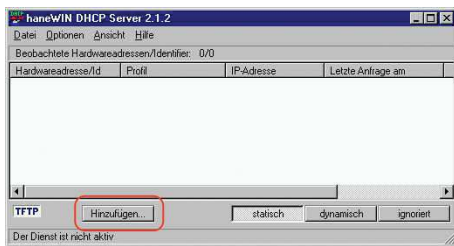
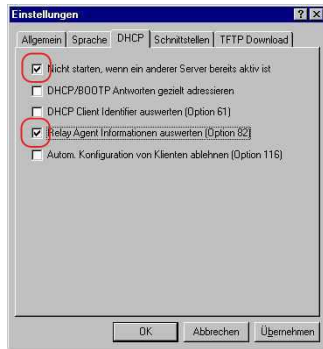














feste Adresszuweisungen

Mit statischen Einträgen können Klienten mit bekannter Hardwareadresse oder Identifier eine feste IP-Adresse und ein Konfigurationsprofil zugeordnet werden. Die zugeordneten IP-Adressen dürfen nicht mit den Bereichen der dynamischen Zuteilung überlappen.

Identifier oder Hardwareadressen müssen hexadezimal eingetragen werden. Bei Hardwareadressen müssen die Bytes durch einen Doppelpunkt oder ein Minus getrennt werden.

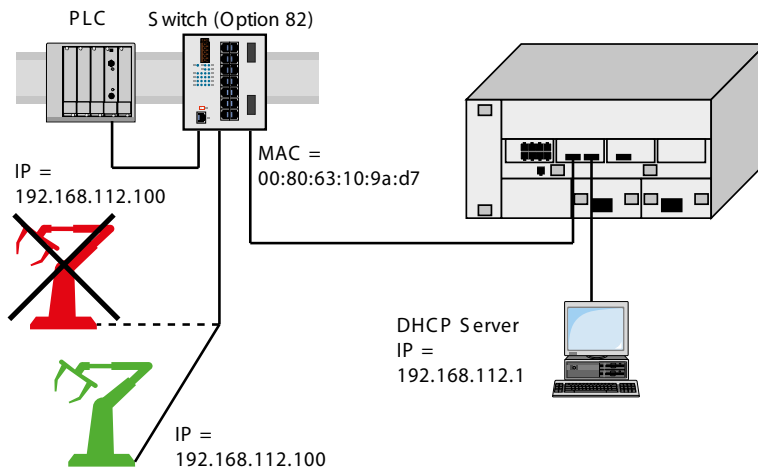
Client Identifier Circuit Identifier Remote Identifier oder Hardwareadresse:

IP-Adresse:

Optional:
Konfigurationsprofil:

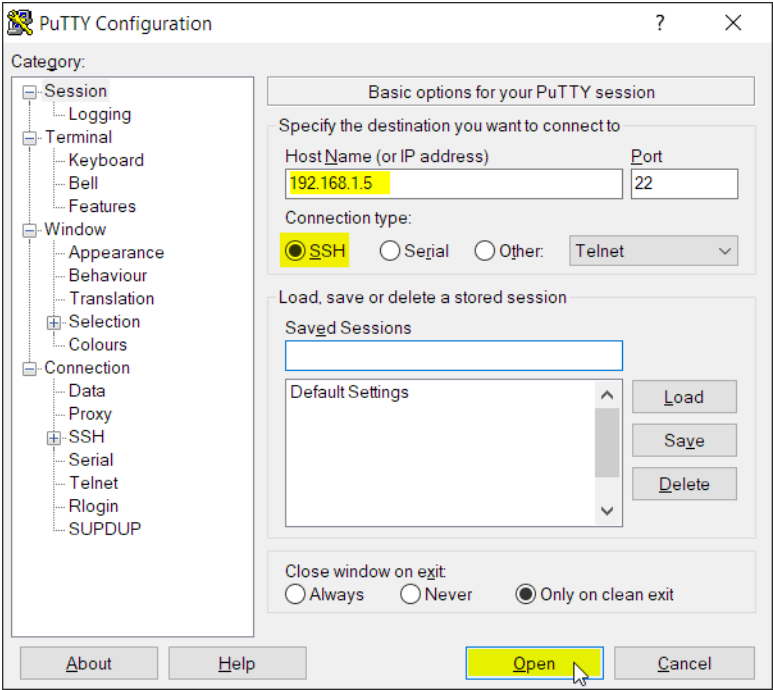
Kommentar:

OK Abbrechen Übernehmen

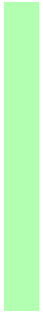
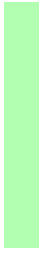




|
|
|



|
|
|

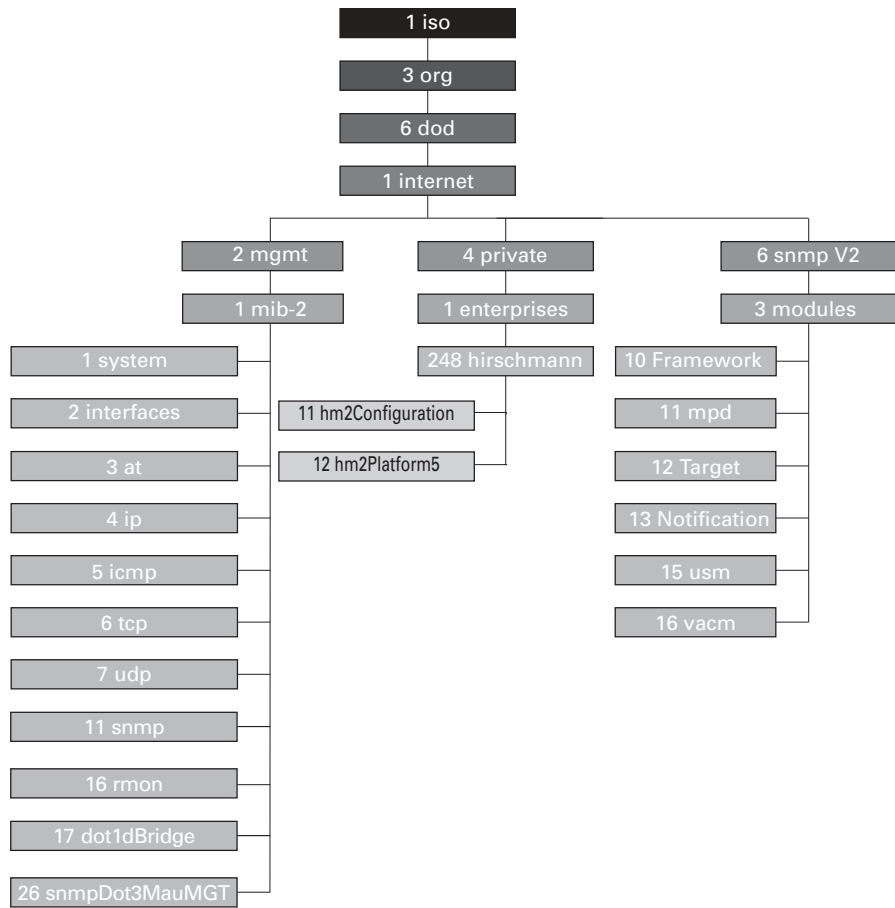






□□□□□□□□□□□□□□□□

-





A series of horizontal lines for writing, consisting of 34 lines.





A series of 25 horizontal black lines, evenly spaced, providing a template for writing or drawing.









A series of 20 horizontal black lines, evenly spaced, providing a template for text entry.



HIRSCHMANN

A **BELDEN** BRAND