



HIRSCHMANN

A **BELDEN** BRAND

Hirschmann Automation and Control GmbH

Eagle40-6M HiSecOS Rel. 05000

Referenz-Handbuch

Grafische Benutzeroberfläche

Anwender-Handbuch

Konfiguration



HIRSCHMANN

A **BELDEN** BRAND

Referenz-Handbuch

Grafische Benutzeroberfläche

Industrial Firewall

EAGLE406M

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.

© 2024 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	Netz	23
1.2.1	Global	24
1.2.2	IPv4	26
1.3	Software	27
1.4	Laden/Speichern	30
1.5	Externer Speicher	41
1.6	Port	44
1.7	Neustart	49
2	Zeit	51
2.1	Grundeinstellungen	51
2.2	NTP	55
2.2.1	Global	56
2.2.2	Server	58
3	Gerätesicherheit	61
3.1	Benutzerverwaltung	61
3.2	Authentifizierungs-Liste	66
3.3	LDAP	69
3.3.1	LDAP Konfiguration	70
3.3.2	LDAP Rollen-Zuweisung	76
3.4	Management-Zugriff	78
3.4.1	Server	79
3.4.2	IP-Zugriffsbeschränkung	91
3.4.3	Web	95
3.4.4	Command Line Interface	96
3.4.5	SNMPv1/v2 Community	98
3.5	Pre-Login-Banner	99
4	Netzsicherheit	101
4.1	Netzsicherheit Übersicht	101
4.2	RADIUS	102
4.2.1	RADIUS Global	103
4.2.2	RADIUS Authentication-Server	104
4.2.3	RADIUS Authentication Statistiken	106

4.3	Asset	107
4.4	Protokoll	111
4.5	Paketfilter	114
4.5.1	Routed-Firewall-Modus	114
4.5.1.1	Global	116
4.5.1.2	Firewall-Lern-Modus	118
4.5.1.3	Paketfilter Regel	125
4.5.1.4	Paketfilter Zuweisung	131
4.5.1.5	Paketfilter Übersicht	134
4.5.2	Transparent-Firewall-Modus	135
4.5.2.1	Paketfilter Global	137
4.5.2.2	Paketfilter Regel	139
4.5.2.3	Paketfilter Zuweisung	147
4.5.2.4	Paketfilter Übersicht	150
4.6	Deep Packet Inspection	152
4.6.1	Deep Packet Inspection - Modbus Enforcer	153
4.6.2	Deep Packet Inspection - OPC Enforcer	159
4.6.3	Deep Packet Inspection - DNP3 Enforcer	162
4.6.3.1	DNP3-Profil	163
4.6.3.2	DNP3-Objekt	168
4.6.4	Deep Packet Inspection - IEC104 Enforcer	190
4.6.5	Deep Packet Inspection - AMP-Enforcer	197
4.6.5.1	AMP Global	198
4.6.5.2	AMP-Profil	201
4.6.6	Deep Packet Inspection - ENIP Enforcer	209
4.6.6.1	ENIP-Profil	211
4.6.6.2	ENIP-Objekt	215
4.7	DoS	244
4.7.1	DoS Global	245
4.8	Intrusion Detection System	248
5	Virtual Private Network	251
5.1	VPN Übersicht	251
5.2	VPN Zertifikate	260
5.3	VPN Verbindungen	264
6	Switching	291
6.1	Switching Global	291
6.2	Lastbegrenzer	293
6.3	Filter für MAC-Adressen	296
6.4	QoS/Priority	297
6.4.1	QoS/Priority Global	299
6.4.2	QoS/Priorität Port-Konfiguration	300
6.4.3	802.1D/p Zuweisung	301
6.5	VLAN	302
6.5.1	VLAN Global	303
6.5.2	VLAN Konfiguration	304
6.5.3	VLAN Port	306

7	Routing	309
7.1	Routing Global	309
7.2	Routing-Interfaces	311
7.2.1	Routing-Interfaces Konfiguration	312
7.2.2	Routing-Interfaces Sekundäre Interface-Adressen	318
7.3	ARP	319
7.3.1	ARP Global	320
7.3.2	ARP Aktuell	322
7.3.3	ARP Statisch	324
7.4	Open Shortest Path First	326
7.4.1	OSPF Global	328
7.4.2	OSPF Areas	337
7.4.3	OSPF Stub Areas	339
7.4.4	OSPF Not So Stubby Areas	341
7.4.5	OSPF Interfaces	344
7.4.6	OSPF Virtual Links	349
7.4.7	OSPF Ranges	352
7.4.8	OSPF Diagnose	354
7.5	Routing-Tabelle	366
7.6	L3-Relay	371
7.7	Loopback-Interface	375
7.8	Multicast Routing	377
7.8.1	Multicast-Routing Global	378
7.8.2	Statisches Multicast-Routing	378
7.8.2.1	Statisches Multicast-Routing Global	379
7.8.2.2	Statische Multicast-Routing-Tabelle	380
7.9	Multicast-Routing IGMP Querier	384
7.10	L3-Redundanz	387
7.10.1	VRRP	387
7.10.1.1	VRRP Konfiguration	388
7.10.1.2	VRRP Statistiken	399
7.10.1.3	VRRP Tracking	401
7.11	NAT	402
7.11.1	NAT Global	403
7.11.2	1:1-NAT	407
7.11.2.1	1:1-NAT Regel	408
7.11.3	Destination-NAT	411
7.11.3.1	Destination-NAT Regel	413
7.11.3.2	Destination-NAT Zuweisung	418
7.11.3.3	Destination-NAT Übersicht	420
7.11.4	Masquerading-NAT	422
7.11.4.1	Masquerading-NAT Regel	423
7.11.4.2	Masquerading-NAT Zuweisung	426
7.11.4.3	Masquerading-NAT Übersicht	428
7.11.5	Double-NAT	430
7.11.5.1	Double-NAT Regel	432
7.11.5.2	Double-NAT Zuweisung	435

7.11.5.3	Double-NAT Übersicht	437
8	Diagnose	439
8.1	Statuskonfiguration	439
8.1.1	Gerätestatus	440
8.1.2	Sicherheitsstatus	444
8.1.3	Alarmer (Traps)	449
8.1.3.1	Trap Ziele	450
8.2	System	452
8.2.1	Systeminformationen	453
8.2.2	Konfigurations-Check	454
8.2.3	ARP	456
8.2.4	Selbsttest	457
8.3	Syslog	459
8.4	Ports	462
8.5	LLDP	462
8.5.1	LLDP Konfiguration	463
8.5.2	LLDP Topologie-Erkennung	467
8.6	Bericht	468
8.6.1	Bericht Global	469
8.6.2	Persistentes Ereignisprotokoll	474
8.6.3	System-Log	477
8.6.4	Audit-Trail	478
9	Erweitert	479
9.1	DNS	479
9.1.1	DNS-Client	479
9.1.1.1	DNS-Client Global	480
9.1.1.2	DNS-Client Aktuell	481
9.1.1.3	DNS-Client Statisch	482
9.1.2	DNS-Cache	483
9.1.2.1	DNS-Cache Global	484
9.2	Tracking	484
9.2.1	Tracking Konfiguration	486
9.2.2	Tracking Applikationen	492
9.3	Command Line Interface	493
A	Stichwortverzeichnis	495
B	Technische Unterstützung	499
C	Leserkritik	500

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.
<code>À<µm©*m</code>	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 () von den Einstellungen des „ausgewählten“ Konfigurationsprofils im permanenten Speicher () abweichen. Das Banner zeigt das Symbol, sobald Sie die Einstellungen angewendet, diese jedoch noch nicht im permanenten Speicher () 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 . Siehe Dialog .
- Die Zusammenfassung des Rahmens . Siehe Dialog [System](#).


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



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

- Name des Benutzerkontos
Kontoname des Benutzers, der gegenwärtig angemeldet ist.
- Schaltfläche
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 (). 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  im Dialog [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 () 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 .


Markieren Sie in der Tabelle das Kontrollkästchen ganz links in der Tabellenzeile des gewünschten Konfigurationsprofils.

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

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
- Netz
- Software
- Laden/Speichern
- Externer Speicher
- Port
- 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 ein Alarm vorliegt, wechselt die Hintergrundfarbe zu rot. Andernfalls bleibt die Hintergrundfarbe grün.

Die Parameter, die das Gerät überwacht, legen Sie fest im Dialog [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 jeweiligen Alarm ausgelöst hat. Um den Tooltip anzuzeigen, bewegen Sie den Mauszeiger über das Feld oder tippen Sie darauf. Die Registerkarte [im Dialog Statuskonfiguration > Gerätestatus](#) zeigt eine Übersicht über die Alarme.

Anmerkung: Das Gerät löst einen Alarm aus, wenn Sie an ein Gerät, das 2 redundante Netzteile unterstützt, lediglich ein Netzteil anschließen. Um diesen Alarm zu vermeiden, deaktivieren Sie im Dialog [das Überwachen fehlender Netzteile](#).

Sicherheits-Status



Sicherheits-Status

Zeigt den Sicherheits-Status und die gegenwärtig vorliegenden Alarme. Wenn mindestens ein Alarm vorliegt, wechselt die Hintergrundfarbe zu rot. Andernfalls bleibt die Hintergrundfarbe grün.

Die Parameter, die das Gerät überwacht, legen Sie fest im Dialog [Sicherheitsstatus](#). 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 jeweiligen Alarm ausgelöst hat. Um den Tooltip anzuzeigen, bewegen Sie den Mauszeiger über das Feld oder tippen Sie darauf. Die Registerkarte [Statuskonfiguration](#) > [Sicherheitsstatus](#) zeigt eine Übersicht über die Alarme.

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:

-
-
-
-

(Voreinstellung)

Beim Generieren eines digitalen Zertifikats 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). Aus Kompatibilitätsgründen ist es empfehlenswert, ausschließlich Kleinbuchstaben zu verwenden, da manche Systeme zwischen Groß- und Kleinschreibung im FQDN unterscheiden. Vergewissern Sie sich, dass dieser Name im gesamten Netz eindeutig ist.

-

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 Geräts.

Netzteil 1 Netzteil 2

Zeigt den Status des Netzteils am betreffenden Spannungsversorgungs-Anschluss.

Mögliche Werte:

Betriebszeit

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

Mögliche Werte:

Zeit im Format

Temperatur [°C]

Zeigt die gegenwärtige Temperatur im Gerät in °C.

Das Überwachen der Schwellenwerte für die Temperatur aktivieren Sie im Dialog [Statuskonfiguration > Gerätestatus](#).

Obere Temp.-Grenze [°C]

Legt den oberen Schwellenwert für die Temperatur in °C fest.

Mögliche Werte:

(ganze Zahl)

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

Untere Temp.-Grenze [°C]

Legt den unteren Schwellenwert für die Temperatur in °C fest.

Mögliche Werte:

(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 ein Alarm vor. Für Details siehe Rahmen

Power



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



Gerät, das ein 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 angeschlossen, jedoch nicht betriebsbereit.



Der externe Speicher ist angeschlossen 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 Port-Übertragungsrate.
- 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.

1.2 Netz

[Grundeinstellungen > Netz]

Das Menü enthält die folgenden Dialoge:

[Global](#)

[IPv4](#)

1.21 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:

(Voreinstellung:)

Voraussetzung ist, dass im Dialog das VLAN bereits eingerichtet ist.

Weisen Sie ein VLAN zu, das keinem Router-Interface zugewiesen ist.

Wenn Sie nach Ändern des Werts die Schaltfläche ✓ klicken, öffnet sich der Dialog . Wählen Sie den Port aus, über den Sie die Verbindung zum Gerät zukünftig herstellen. Nach Klicken der Schaltfläche 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 .
- Das Gerät weist dem Port die Port-VLAN-ID des neuen Management-VLANs zu. Siehe Dialog .

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 .

Funktion

Schaltet die Funktion HiDiscovery im Gerät ein/aus.

Mögliche Werte:

(Voreinstellung)

Die Funktion HiDiscovery ist eingeschaltet.

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

Die Funktion HiDiscovery ist ausgeschaltet.

Zugriff

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

Mögliche Werte:

(Voreinstellung)

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

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

.

1.22 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.

IP-Parameter

Dieser Rahmen ermöglicht Ihnen, die IP-Parameter manuell zuzuweisen. Wenn Sie im Rahmen , Optionsliste das Optionsfeld 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

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

- Router-Interface
- Loopback-Interface

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

Wenn das Gerät das festgelegte Gateway nicht verwendet, dann prüfen Sie, ob ein anderes Stand-
festgelegt ist. Die Einstellung im folgenden Dialog hat Vorrang:

- Dialog , Spalte , wenn der Wert in Spalte
und in Spalte gleich ist.

1.3 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: Bevor Sie die Geräte-Software aktualisieren, beachten Sie die versionsspezifischen Hinweise in der -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 in den Backup-Bereich kopiert.

Wiederherstellen

Das Gerät vertauscht die Software-Images und dementsprechend die in den Feldern und angezeigten Werte.

Beim nächsten Systemstart lädt das Gerät die im Feld angezeigte Geräte-Software.

Bootcode

Zeigt Versionsnummer und Erstellungsdatum des Bootcodes.

Software-Update

Das Gerät ermöglicht Ihnen, die Geräte-Software mittels der Felder in diesem Rahmen zu aktualisieren. 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 dazu 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

Ziehen Sie die Datei von Ihrem PC oder Netzlaufwerk in den -Bereich. Alternativ dazu klicken Sie in den Bereich, um die Datei auszuwählen.

Außerdem können Sie die Datei von Ihrem PC mittels SFTP oder SCP zum Gerät übertragen. Führen Sie die folgenden Schritte aus:

Öffnen Sie auf Ihrem PC einen SFTP- oder SCP-Client, zum Beispiel WinSCP.

Öffnen Sie mit dem SFTP- oder SCP-Client eine Verbindung zum Gerät.

Übertragen Sie die Datei auf das Gerät in das Verzeichnis

Sobald die Datei vollständig übertragen ist, beginnt das Gerät, die Geräte-Software zu aktualisieren. Wenn die Aktualisierung erfolgreich war, dann generiert das Gerät eine Datei im Verzeichnis und löscht die übertragene Datei.

Das Gerät lädt die Geräte-Software beim nächsten Systemstart.

- Software-Update von einem SCP- oder SFTP-Server

Wenn sich die Datei auf einem SCP- oder SFTP-Server befindet, dann legen Sie den URL in einer der folgenden Formen fest:

oder `--\)0 Åhm• • 0-°h Å°-©|°k•`

Klicken Sie die Schaltfläche , um das Fenster zu öffnen. In diesem Fenster geben Sie und ein, um sich am Server anzumelden.

oder `--\ "•|µ-#•ml°k• 0° n<m-)0 Åhm• • 0-°h Å°-©|°k•`

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.

Das Gerät kopiert die bisher verwendete Geräte-Software in den Backup-Bereich.

Um während des Software-Updates beim Management des Geräts angemeldet zu bleiben, bewegen Sie gelegentlich den Mauszeiger. Alternativ dazu legen Sie vor dem Software-Update im Dialog , Feld einen ausreichend hohen Wert fest.

Tabelle

Datei Ort

Zeigt den Speicherort der Geräte-Software.

Mögliche Werte:

Flüchtiger Speicher des Geräts

Permanenter Speicher () des Geräts

Externer USB-Speicher (ACA21/ACA22)

Index

Zeigt den Index der Geräte-Software.

Die Index-Nummer der Geräte-Software im Flash-Speicher hat die folgende Bedeutung:

Beim nächsten Systemstart lädt das Gerät diese Geräte-Software.

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.

1.4 Laden/Speichern

[Grundeinstellungen > Laden/Speichern]

Dieser Dialog ermöglicht Ihnen, die Einstellungen des Geräts dauerhaft 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 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 ein. Wenn die Verbindung abbricht, dann lädt das Gerät nach der festgelegten Zeit das im permanenten Speicher () gespeicherte Konfigurationsprofil.

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 () 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 ().

Wenn im Dialog das Kontrollkästchen in Spalte markiert ist, dann speichert das Gerät eine Kopie des Konfigurationsprofils im externen Speicher.



Zeigt ein Kontextmenü mit weiteren Funktionen für den betreffenden Dialog.

Speichern unter...

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

Geben Sie im Feld 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 das Kontrollkästchen in Spalte - markiert ist, kennzeichnet das Gerät auch das gleichnamige Konfigurationsprofil auf dem externen Speicher als „ausgewählt“.

Anmerkung: Entscheiden Sie sich vor dem Hinzufügen 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 () .

- 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 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 () . 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.

Wenn oben ausgewählt ist, legen Sie im Rahmen die Datei des zu importierenden Konfigurationsprofils fest.
 Wählen Sie in der Dropdown-Liste den Namen des zu importierenden Konfigurationsprofils.
 Im Rahmen legen Sie fest, wo das Gerät das importierte Konfigurationsprofil speichert.
 Im Feld legen Sie den Namen fest, unter dem das Gerät das Konfigurationsprofil speichert.
 Im Feld legen Sie den Speicherort für das Konfigurationsprofil fest. Voraussetzung ist, dass in der Dropdown-Liste der Eintrag ausgewählt ist.

Das Gerät speichert das Konfigurationsprofil im flüchtigen Speicher () des Geräts. Dies ersetzt die , 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.

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

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

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

Bezüglich Verschlüsselung des Konfigurationsprofils lesen Sie auch den Hilfetext zum Rahmen . 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 , um den Speicherort zu wählen und den Dateinamen festzulegen.

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

- 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:
 oder)0 Åhm• • 0-°h Å°-•©l°k•
 Klicken Sie die Schaltfläche , um das Fenster zu öffnen. In diesem Fenster geben Sie und ein, um sich am Server anzumelden.
 oder "•lµ-#•ml°k• 0° n<m-)0 Åhm• • 0-°h Å°-•©l°k•

Auf Lieferzustand zurücksetzen...

Setzt die Einstellungen im Gerät auf die voreingestellten Werte zurück.

- Das Gerät löscht die gespeicherten Konfigurationsprofile aus dem flüchtigen Speicher () und aus dem permanenten Speicher ().
- Das Gerät löscht das vom Webserver im Gerät verwendete digitale 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 und verwendet dann die Werkseinstellungen.

Auf Default-Zustand zurücksetzen

Löscht die gegenwärtigen Betriebseinstellungen () aus dem flüchtigen Speicher ().

Speicherort

Zeigt den Speicherort des Konfigurationsprofils.

Mögliche Werte:

(flüchtiger Speicher des Geräts)

Im flüchtigen Speicher speichert das Gerät die Einstellungen für den laufenden Betrieb.

(permanenter Speicher des Geräts)

Aus dem permanenten Speicher lädt das Gerät das „ausgewählte“ Konfigurationsprofil beim Systemstart oder beim Anwenden der Funktion .

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 () laden. Führen Sie dazu die folgenden Schritte aus:

Wählen Sie die Tabellenzeile des Konfigurationsprofils.

Klicken Sie die Schaltfläche  und dann den Eintrag .

(externer Speicher)

Im externen Speicher speichert das Gerät eine Sicherungskopie des „ausgewählten“ Konfigurationsprofils.

Voraussetzung ist, dass im Dialog  das Kontrollkästchen  markiert ist.

Profilname

Zeigt die Bezeichnung des Konfigurationsprofils.

Mögliche Werte:

Bezeichnung des Konfigurationsprofils im flüchtigen Speicher ().



Bezeichnung des werksseitig vorhandenen Konfigurationsprofils im permanenten Speicher ().

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 .

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 .



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 .

Mögliche Werte:

Das Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet.

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

Ein anderes Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet.


Verschlüsselung

Zeigt, ob das Konfigurationsprofil verschlüsselt ist.

Mögliche Werte:

Das Konfigurationsprofil ist verschlüsselt.

Das Konfigurationsprofil ist unverschlüsselt.

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

Verifiziert

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

Mögliche Werte:

Die Passwörter stimmen überein. Das Gerät ist imstande, das Konfigurationsprofil zu entschlüsseln.

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:

Berechnete und gespeicherte Prüfsumme stimmen überein.
Die gespeicherten Einstellungen sind konsistent.

Für das als „ausgewählt“ gekennzeichnete Konfigurationsprofil gilt:
Berechnete und gespeicherte Prüfsumme unterscheiden sich.
Das Konfigurationsprofil enthält geänderte Einstellungen.

Mögliche Ursachen:

- Die Datei ist beschädigt.
- Das Dateisystem im externen Speicher ist inkonsistent.
- Ein Benutzer hat das Konfigurationsprofil exportiert und die XML-Datei außerhalb des Geräts verändert.

Für die anderen Konfigurationsprofile hat das Gerät die Prüfsumme nicht berechnet.

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

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

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

Externer Speicher

Ausgewählter externer Speicher

Zeigt den Typ des externen Speichers.

Mögliche Werte:

Externer USB-Speicher (ACA21/ACA22)

Status

Zeigt den Betriebszustand des externen Speichers.

Mögliche Werte:

Kein externer Speicher angeschlossen.

Jemand hat den externen Speicher während des Betriebs aus dem Gerät entfernt.

Der externe Speicher ist angeschlossen und betriebsbereit.

Der Speicherplatz im externen Speicher ist belegt.

Das Gerät hat einen Fehler erkannt.

Konfigurations-Verschlüsselung

Aktiv

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

Mögliche Werte:

Die Konfigurations-Verschlüsselung ist aktiv.

Das Gerät lädt ein Konfigurationsprofil aus dem permanenten Speicher () ausschließlich dann, wenn dieses verschlüsselt ist und das Passwort mit dem im Gerät gespeicherten Passwort übereinstimmt.

Die Konfigurations-Verschlüsselung ist inaktiv.

Das Gerät lädt ein Konfigurationsprofil aus dem permanenten Speicher () ausschließlich dann, wenn dieses unverschlüsselt ist.

Wenn im Dialog die Spalte den Wert hat und das Konfigurationsprofil unverschlüsselt ist, dann zeigt der Rahmen im Dialog einen Alarm.

Im Dialog , Registerkarte , Spalte legen Sie fest, ob das Gerät den Parameter überwacht.

Passwort setzen

Öffnet das Fenster , 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 das bisherige Passwort ein. Um anstelle von ***** (Sternchen) das Passwort im Klartext anzuzeigen, markieren Sie das Kontrollkästchen .

Geben Sie im Feld das Passwort ein. Um anstelle von ***** (Sternchen) das Passwort im Klartext anzuzeigen, markieren Sie das Kontrollkästchen .

Markieren Sie das Kontrollkästchen , um die Verschlüsselung auf das „ausgewählte“ Konfigurationsprofil im permanenten Speicher () und im externen Speicher anzuwenden.

Anmerkung: Wenden Sie diese Funktion ausschließlich dann an, wenn maximal ein Konfigurationsprofil im permanenten Speicher () des Geräts gespeichert ist. Entscheiden Sie sich vor dem Hinzufügen 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 .

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 () und in den permanenten Speicher ().

Löschen

Öffnet das Fenster , 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 das bisherige Passwort ein.

Um anstelle von ***** (Sternchen) das Passwort im Klartext anzuzeigen, markieren Sie das Kontrollkästchen .

Markieren Sie das Kontrollkästchen , um die Verschlüsselung auch im „ausgewählten“ Konfigurationsprofil im permanenten Speicher () 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 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 (). Danach ist das Gerät wieder erreichbar.

Mögliche Werte:

Die Funktion ist eingeschaltet.

- Die Zeitspanne zwischen Verbindungsabbruch und Laden des Konfigurationsprofils legen Sie fest im Feld .
- Enthält der permanente Speicher () mehrere Konfigurationsprofile, lädt das Gerät das als „ausgewählt“ gekennzeichnete Konfigurationsprofil.

(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 () lädt, wenn die Verbindung abbricht.

Mögliche Werte:

(Voreinstellung:)

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:)


Information

NVM synchron mit running-config

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

Mögliche Werte:

Die Einstellungen stimmen überein.

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 () abweichen.

Mögliche Werte:

Die Einstellungen stimmen überein.

Die Einstellungen weichen voneinander ab.

Mögliche Ursachen:

- An das Gerät ist kein externer Speicher angeschlossen.
- Im Dialog ist die Funktion ausgeschaltet.

1.5 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:

Externer USB-Speicher (ACA21/ACA22)

Status

Zeigt den Betriebszustand des externen Speichers.

Mögliche Werte:

Kein externer Speicher angeschlossen.

Jemand hat den externen Speicher während des Betriebs aus dem Gerät entfernt.

Der externe Speicher ist angeschlossen und betriebsbereit.

Der Speicherplatz im externen Speicher ist belegt.

Das Gerät hat einen Fehler erkannt.

Schreibbar

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

Mögliche Werte:

Das Gerät hat Schreibzugriff auf den externen Speicher.

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:

(Voreinstellung)

Das Gerät aktualisiert die Geräte-Software, wenn sich folgende Dateien im externen Speicher befinden:

- die Image-Datei der Geräte-Software
- eine Textdatei mit dem Inhalt `µ-5-h- .°k• h•m)k°ß• Å°-•© <©I`

Keine automatische Aktualisierung der Geräte-Software während des Systemstarts.

Konfigurations-Priorität

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

Mögliche Werte:

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

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 ().

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

Wenn die Spalte den Wert hat und das Konfigurationsprofil unver-schlüsselt ist, dann zeigt der Rahmen im Dialog einen Alarm.

Im Dialog , Registerkarte , Spalte legen Sie fest, ob das Gerät den Parameter überwacht.


Sichere Konfiguration beim Speichern

Aktiviert/deaktiviert das Speichern einer Kopie im externen Speicher.

Mögliche Werte:

(Voreinstellung)

Das Speichern einer Kopie ist aktiviert. Wenn Sie im Dialog

die Schaltfläche  klicken, speichert das Gerät eine Kopie des Konfigurationsprofils auf dem aktiven externen Speicher.

Das Speichern einer Kopie ist deaktiviert. Das Gerät speichert 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.

1.6 Port

[Grundeinstellungen > Port]

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

Der Dialog enthält die folgenden Registerkarten:

[\[Konfiguration\]](#)

[\[Statistiken\]](#)

[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:

–
–
–
–
–

Port an

Aktiviert/deaktiviert den Port.

Mögliche Werte:

(Voreinstellung)

Der Port ist aktiv.

Der Port ist inaktiv. Der Port sendet und empfängt keine Daten.

Zustand

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

Mögliche Werte:

Der Port ist physisch eingeschaltet.

Der Port ist physisch ausgeschaltet.

Autoneg.

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

Mögliche Werte:

(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 Twisted-Pair-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.

Die automatische Auswahl des Betriebsmodus ist inaktiv.

Der Port arbeitet mit den Werten, die Sie in Spalte und in Spalte festlegen.

Ausgegraute Darstellung

Keine automatische Auswahl des Betriebsmodus.

Manuelle Konfiguration

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

Mögliche Werte:

Halbduplex-Verbindung

Vollduplex-Verbindung

Halbduplex-Verbindung

Vollduplex-Verbindung

Vollduplex-Verbindung

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

Link/ Aktuelle Betriebsart

Zeigt, welchen Betriebsmodus der Port gegenwärtig verwendet.

Mögliche Werte:

Kein Kabel angesteckt, keine Verbindung.

Halbduplex-Verbindung

Vollduplex-Verbindung

Halbduplex-Verbindung

Vollduplex-Verbindung

Vollduplex-Verbindung

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

Manuelles Cable-Crossing

Legt die Belegung der Anschlüsse eines Twisted-Pair-Ports fest.

Voraussetzung ist, dass die Funktion ausgeschaltet ist.

Mögliche Werte:

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

(Voreinstellung auf Twisted-Pair-Ports)

Das Gerät hilft, das Vertauschen der Sende- und Empfangsleitungs-paare auf dem Port zu vermeiden.

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 auf .

(Voreinstellung auf optischen Ports oder Twisted-Pair-SFP-Ports)

Der Port unterstützt diese Funktion nicht.

Flusskontrolle

Aktiviert/deaktiviert die Flusskontrolle auf dem Port.

Mögliche Werte:

(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 -

im Dialog .

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 Sendeunterbrechungen im übergeordneten Netzsegment („Wandering Backpressure“).

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:

(Voreinstellung)

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

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

Das Senden von SNMP-Traps ist inaktiv.

Power-State

Legt fest, ob der Port physisch eingeschaltet oder ausgeschaltet ist, wenn Sie den Port mit der Funktion [deaktivieren](#).

Mögliche Werte:

Der Port bleibt physisch eingeschaltet. Ein angeschlossenes Gerät empfängt einen aktiven Link.

(Voreinstellung)

Der Port ist physisch ausgeschaltet.

Energie sparen

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

Mögliche Werte:

(Voreinstellung)

Der Port bleibt aktiviert.

Der Port schaltet in den Energiesparmodus.

Der Port unterstützt diese Funktion nicht und bleibt aktiviert.

[Statistiken]

Diese Registerkarte zeigt pro Port folgenden Überblick:

- Anzahl der vom Gerät empfangenen Datenpakete/Bytes
—
—
—
—
—
- Anzahl der vom Gerät gesendeten oder vermittelten Datenpakete/Bytes
—
—
—
—
—


- Anzahl der vom Gerät erkannten Fehler
—
—
—
- Anzahl der vom Gerät empfangenen Datenpakete pro Größenkategorie
—
—
—
—
—
—
- Anzahl der vom Gerät verworfenen Datenpakete
—
—

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 . Um absteigend zu sortieren, klicken Sie die Überschrift erneut.

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

Klicken Sie im Dialog
oder
Klicken Sie im Dialog

die Schaltfläche  .
die Schaltfläche .

1.7 Neustart

[Grundeinstellungen > Neustart]



Dieser Dialog ermöglicht Ihnen, das Gerät neu zu starten, Port-Zähler und die MAC-Adresstabelle (Forwarding Database) zurückzusetzen sowie Log-Dateien zu löschen.



Neustart

Kaltstart...

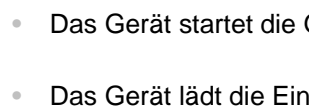
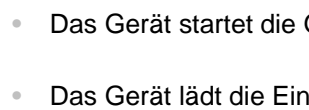
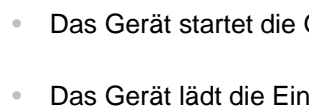
Öffnet das Fenster , um einen Neustart des Geräts auszulösen.

Wenn sich das Konfigurationsprofil im flüchtigen Speicher () und das „ausgewählte“ Konfigurationsprofil im permanenten Speicher () unterscheiden, zeigt das Gerät das Fenster .

Um die Einstellungen dauerhaft zu speichern, klicken Sie im Fenster  die Schaltfläche .

Um die geänderten Einstellungen zu verwerfen, klicken Sie im Fenster  die Schaltfläche .

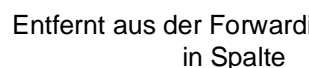
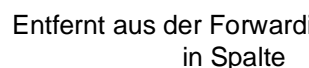
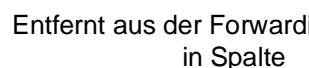
Das Gerät startet neu und durchläuft folgende Phasen:

- Das Gerät startet die Geräte-Software, die das Feld  im Dialog  anzeigt.
- Das Gerät lädt die Einstellungen aus dem „ausgewählten“ Konfigurationsprofil. Siehe Dialog .

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

Schaltflächen

FDB leeren

Entfernt aus der Forwarding-Tabelle (FDB) die MAC-Adressen, die im Dialog  in Spalte  den Wert  haben.

ARP-Tabelle leeren

Entfernt aus der ARP-Tabelle die dynamisch eingerichteten Adressen.

Siehe Dialog .

Port-Statistiken leeren

Setzt die Zähler der Portstatistik auf .

Siehe Dialog , Registerkarte .

Log-Datei leeren

Entfernt die protokollierten Einträge aus der Log-Datei.

Siehe Dialog

Persistente Log-Datei leeren

Entfernt die Log-Dateien vom externen Speicher.

Siehe Dialog

Firewall-Tabelle leeren

Entfernt die Information über offene Kommunikationsverbindungen aus der State-Tabelle der Firewall. Möglicherweise unterbricht das Gerät dabei offene Kommunikationsverbindungen.

2 Zeit

Das Menü enthält die folgenden Dialoge:

[Grundeinstellungen](#)
[NTP](#)

2.1 Grundeinstellungen

[Zeit > Grundeinstellungen]

Nach einem Neustart initialisiert das Gerät seine Uhr auf den 1. Januar 2024, 01.00 Uhr UTC+1. Stellen Sie die Uhrzeit neu ein, wenn Sie das Netzteil vom Gerät trennen oder das Gerät neu starten. Alternativ dazu legen Sie fest, dass das Gerät die korrekte Uhrzeit automatisch von einem -Server oder von einer PTP-Uhr bezieht.

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: = + +

Zeitquelle

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

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

Mögliche Werte:

Systemuhr des Geräts.

Der -Client ist eingeschaltet und das Gerät ist durch einen -Server synchronisiert. Siehe Dialog .

Lokaler Offset [min]

Legt die Differenz in Minuten zwischen koordinierter Weltzeit (UTC) und Ortszeit fest:

= -

Mögliche Werte:

(Voreinstellung:)

[Sommerzeit]

In dieser Registerkarte schalten Sie die Funktion 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 eine Stunde vor.

Funktion

Sommerzeit

Schaltet den -Modus ein/aus.

Mögliche Werte:

Die -Modus ist eingeschaltet.
Das Gerät stellt die Uhr automatisch auf Sommerzeit und wieder zurück.

(Voreinstellung)

Die -Modus ist ausgeschaltet.

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

Profil...

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

Mögliche Werte:

Sommerzeit-Einstellungen, die in der Europäischen Union gelten.

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)

Tag

Legt den Wochentag fest.

Mögliche Werte:
(Voreinstellung)

Monat

Legt den Monat fest.

Mögliche Werte:
(Voreinstellung)

Systemzeit

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

Mögliche Werte:

(Voreinstellung:)

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)

Tag

Legt den Wochentag fest.

Mögliche Werte:

(Voreinstellung)

Monat

Legt den Monat fest.

Mögliche Werte:

(Voreinstellung)

Systemzeit

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

Mögliche Werte:

(Voreinstellung:)

22 NTP

[Zeit > NTP]

Das Gerät ermöglicht Ihnen, die Systemzeit im Gerät und im Netz mit dem Network Time Protocol (NTP) zu synchronisieren.

Das Network Time Protocol (NTP) ist ein im RFC 5905 beschriebenes Verfahren für die Zeitsynchronisation im Netz.

Ausgehend von einer Referenzzeitquelle definiert NTP Hierarchie-Ebenen von Zeitservern und Clients. Die Hierarchie-Ebenen heißen Stratum. Geräte der 1. Ebene (Stratum 1) synchronisieren sich direkt auf die Referenzzeitquelle und stellen die Zeitinformation den Clients der 2. Ebene (Stratum 2) zur Verfügung. Als Referenzzeitquelle im Netz dient zum Beispiel ein GPS-Empfänger oder eine Funkuhr.

Der NTP-Client im Gerät wertet die Zeitinformation von mehreren Servern aus und justiert die eigene Uhr fortlaufend nach, um hohe Genauigkeit zu erreichen. Wenn Sie das Gerät auch als NTP-Server einrichten, dann verteilt es die Zeitinformation an die Clients im nachgeordneten Netzsegment.

Das Menü enthält die folgenden Dialoge:

Global
Server

2.2.1 Global

[Zeit > NTP > Global]

In diesem Dialog legen Sie fest, ob das Gerät als NTP-Client und -Server oder ausschließlich als NTP-Client arbeitet:

- Als NTP-Client bezieht das Gerät die koordinierte Weltzeit (UTC) von einem oder mehreren NTP-Servern im Netz.
- Als NTP-Server verteilt das Gerät die koordinierte Weltzeit (UTC) an NTP-Clients im nachgeordneten Netzsegment. Das Gerät bezieht die koordinierte Weltzeit (UTC) von einem oder mehreren NTP-Servern im Netz, sofern diese festgelegt sind.

Nur Client

Das Gerät überträgt die Zeitinformation ohne Authentifizierung im Management-VLAN sowie in Schicht 3 auf den eingerichteten IP-Interfaces.

Client

Schaltet den NTP-Client im Gerät ein/aus.

Mögliche Werte:

Der NTP-Client ist eingeschaltet.

Das Gerät bezieht die Zeitinformation von einem oder mehreren NTP-Servern im Netz.
(Voreinstellung)

Der NTP-Client ist ausgeschaltet.

Anmerkung: Bevor Sie den Client einschalten, schalten Sie im Rahmen die Funktion aus.

Modus

Legt fest, woher der NTP-Client die Zeitinformation bezieht.

Mögliche Werte:

(Voreinstellung)

Der NTP-Client bezieht die Zeitinformation aus Unicast-Antworten der Server, die im Dialog als aktiv gekennzeichnet sind.

Der NTP-Client des Geräts bezieht die Zeitinformation aus den Broadcast-Nachrichten.

Client und Server

Das Gerät überträgt die Zeitinformation ohne Authentifizierung im Management-VLAN sowie in Schicht 3 auf den eingerichteten IP-Interfaces.

Server

Schaltet den NTP-Client und den NTP-Server im Gerät ein/aus.

Mögliche Werte:

NTP-Client und NTP-Server sind eingeschaltet.

Der NTP-Client bezieht die Zeitinformation von einem oder mehreren NTP-Servern im Netz. Der NTP-Server verteilt die Zeitinformation an die NTP-Clients im nachgeordneten Netzsegment.

(Voreinstellung)

NTP-Client und NTP-Server sind ausgeschaltet.

Anmerkung: Wenn Sie NTP-Client und NTP-Server einschalten, schaltet das Gerät die Funktion im Rahmen , Feld aus.

Modus

Legt fest, in welchem Modus der NTP-Server arbeitet.

Mögliche Werte:

(Voreinstellung)

Mit dieser Einstellung bezieht das Gerät die Zeitinformation von NTP-Servern im Netz und verteilt sie an NTP-Clients im nachgeordneten Netzsegment.

- Der NTP-Client bezieht die Zeitinformation aus den Unicast-Antworten der Server, die im Dialog als aktiv gekennzeichnet sind.
- Der NTP-Server verteilt die Zeitinformation per Unicast an anfragende Clients.

Mit dieser Einstellung integrieren Sie das Gerät in ein Cluster von redundanten NTP-Servern. Das Gerät synchronisiert die Zeitinformation mit den anderen NTP-Servern im Cluster nach jeweils 64 Sekunden.

Kennzeichnen Sie im Dialog die am Cluster beteiligten NTP-Server als aktiv.

Legen Sie für die am Cluster beteiligten NTP-Server einen einheitlichen Wert für das Stratum fest.

Stratum

Legt den hierarchischen Abstand des Geräts von der Referenzzeitquelle fest.

Mögliche Werte:

(Voreinstellung:)

Beispiel: Geräte der ersten Ebene (Stratum 1) synchronisieren sich direkt auf die Referenzzeitquelle und stellen die Zeitinformation den Clients der zweiten Ebene (Stratum 2) zur Verfügung.

Unter den folgenden Voraussetzungen wertet das Gerät diesen Wert aus:

- Der NTP-Server im Gerät arbeitet im Modus .
oder
- Das Gerät verwendet als Zeitquelle die lokale Systemuhr. Siehe Feld im Dialog [Grundeinstellungen](#).

2.2.2 Server

[Zeit > NTP > Server]

In diesem Dialog legen Sie die NTP-Server fest.

- Der NTP-Client des Geräts bezieht die Zeitinformation aus den Unicast-Antworten der hier festgelegten Server.
- Wenn der NTP-Server des Geräts im Modus arbeitet, dann legen Sie hier die am Cluster beteiligten Server fest.
- Das Gerät ermöglicht Ihnen, bis zu 4 NTP-Server festzulegen.

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 hinzufügen, schließt das Gerät die erste Lücke.

Aktiv

Aktiviert/deaktiviert die Verbindung zum NTP-Server.

Mögliche Werte:

Die Verbindung zum NTP-Server ist aktiviert.

- Der NTP-Client des Geräts bezieht die Zeitinformation aus den Unicast-Antworten dieses Servers.
- Wenn der NTP-Server des Geräts im Modus arbeitet, dann ist dieser Server an einem Cluster beteiligt.

Die Verbindung zum NTP-Server ist deaktiviert.

IP-Adresse

Legt die IP-Adresse des NTP-Servers fest.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung:)

Initial burst

Aktiviert/deaktiviert den -Modus.

Im Betrieb sendet der NTP-Client des Geräts ausschließlich einzelne Datenpakete, um die Zeit zu erfragen. Wenn der NTP-Server unerreichbar ist (Spalte =), dann sendet der NTP-Client des Geräts mehrere Datenpakete auf einmal (Burst), um sich schnellstmöglich zu synchronisieren.

Mögliche Werte:

Der -Modus ist aktiv.

- Das Gerät sendet einmalig mehrere Datenpakete (Burst), wenn der NTP-Server unerreichbar ist.
- Verwenden Sie diese Einstellung ausschließlich dann, wenn Sie als Referenzzeitquelle einen eigenen, nicht-öffentlichen NTP-Server nutzen.
- Verwenden Sie diese Einstellung mit Sorgfalt, um die initiale Synchronisierung zu beschleunigen.

(Voreinstellung)

Der -Modus ist inaktiv.

Burst

Aktiviert/deaktiviert den -Modus.

Im Betrieb sendet der NTP-Client des Geräts ausschließlich einzelne Datenpakete, um die Zeit zu erfragen. Im -Modus sendet der NTP-Client des Geräts mehrere Datenpakete auf einmal (Burst), wenn der NTP-Server erreichbar und synchronisationsbereit ist.

Mögliche Werte:

Der -Modus ist aktiv.

- Das Gerät sendet je Polling-Intervall mehrere Datenpakete (Burst), wenn der Server erreichbar ist.
- Verwenden Sie diese Einstellung ausschließlich dann, wenn Sie als Referenzzeitquelle einen eigenen, nicht-öffentlichen NTP-Server nutzen.
- Verwenden Sie diese Einstellung mit Sorgfalt, um bei instabiler Verbindung zum NTP-Server die Präzision zu verbessern.

(Voreinstellung)

Der -Modus ist inaktiv.

Bevorzugt

Kennzeichnet den NTP-Server als bevorzugt zu verwendende Referenzzeitquelle, wenn mehrere NTP-Server festgelegt sind.

Ohne Kennzeichnung verwendet der NTP-Client des Geräts Standard-Algorithmen, um die Referenzzeitquelle auszuwählen.

Kennzeichnen Sie maximal 1 hinreichend genauen Server als .

Mögliche Werte:

Das Gerät verwendet den NTP-Server als bevorzugte Referenzzeitquelle. Verwenden Sie diese Einstellung, um zu vermeiden, dass der NTP-Client häufig zwischen gleichwertigen NTP-Servern wechselt.

(Voreinstellung)

Keine bevorzugte Verwendung des NTP-Servers.

Status

Zeigt den Synchronisierungs-Status.

Mögliche Werte:

Kein Server verfügbar.

Der Server ist verfügbar. Der Server selbst ist nicht synchronisiert.

Der Server ist verfügbar. Das Gerät erhält keine Zeitinformation.

Der Server ist verfügbar. Das Gerät erhält eine Zeitinformation.

Der Server ist verfügbar. Das Gerät hat seine Uhr auf den Server synchronisiert.

Geräteinterner Fehler.

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 sein Management, 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

Konfiguration

Dieser Rahmen ermöglicht Ihnen, Einstellungen für das Login festzulegen.

Login-Versuche

Legt die Anzahl der möglichen aufeinanderfolgenden erfolglosen 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 Verbindung ist die Anzahl der nacheinander erfolglosen Login-Versuche unbegrenzt.

Mögliche Werte:

(Voreinstellung:)

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

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

Der Wert deaktiviert die Sperre. Der Benutzer hat beliebig viele Versuche, sich beim Management des Geräts 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

Mögliche Werte:

(Voreinstellung:)

Zeitraum für Login-Versuche (min.)

Zeigt die Zeitspanne, nach der das Gerät den Zähler im Feld zurücksetzt.

Mögliche Werte:

(Voreinstellung:)

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 . Voraussetzung ist, dass das Kontrollkästchen in Spalte markiert ist.

Großbuchstaben (min.)

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

Mögliche Werte:

(Voreinstellung:)

Der Wert deaktiviert diese Richtlinie.

Kleinbuchstaben (min.)

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

Mögliche Werte:

(Voreinstellung:)

Der Wert deaktiviert diese Richtlinie.

Ziffern (min.)

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

Mögliche Werte:

(Voreinstellung:)

Der Wert deaktiviert diese Richtlinie.

Sonderzeichen (min.)

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

Mögliche Werte:

(Voreinstellung:)

Der Wert 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 , um eine Tabellenzeile hinzuzufügen.

- Im Feld 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 Benutzerkonto hinzuzufügen, klicken Sie die Schaltfläche .

Aktiv

Aktiviert/deaktiviert das Benutzerkonto.

Mögliche Werte:

Das Benutzerkonto ist aktiv. Das Gerät akzeptiert die Anmeldung eines Benutzers am Management des Geräts mit diesem Benutzernamen.

(Voreinstellung)

Das Benutzerkonto ist inaktiv. Das Gerät verweigert die Anmeldung eines Benutzers am Management des Geräts mit diesem Benutzernamen.

Wenn ausschließlich 1 Benutzerkonto mit der Zugriffsrolle existiert, ist dieses Benutzerkonto stets aktiv.

Passwort

Zeigt ***** (Sternchen) anstelle des Passworts, mit dem sich der Benutzer beim Management des Geräts 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:

-
-
-
-

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

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

Das Gerät prüft stets die Mindestlänge des Passworts, auch wenn das Kontrollkästchen in Spalte ist.

Rolle

Legt die Zugriffsrolle fest, die den Zugriff des Benutzers auf die einzelnen Funktionen des Geräts regelt.

Mögliche Werte:

Der Benutzer ist gesperrt, das Gerät verweigert die Anmeldung des Benutzers beim Management des Geräts.

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.

(Voreinstellung)

Der Benutzer ist berechtigt, das Gerät zu überwachen.

Der Benutzer ist berechtigt, das Gerät zu überwachen und im Dialog die Protokoll-Datei zu speichern.

Der Benutzer ist berechtigt, das Gerät zu überwachen und die Einstellungen zu ändern – mit Ausnahme der Sicherheitseinstellungen für den Zugriff auf das Gerät.

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:

- :
- :
- :

Benutzer gesperrt

Entsperrt das Benutzerkonto.

Mögliche Werte:

Das Benutzerkonto ist gesperrt. Der Benutzer hat keinen Zugriff auf das Management des Geräts.

Das Gerät sperrt einen Benutzer automatisch, wenn dieser zu oft nacheinander erfolglos versucht, sich anzumelden.

(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:

Das Prüfen des Passworts ist aktiviert.

Beim Einrichten oder Ändern des Passworts prüft das Gerät das Passwort gemäß der im Rahmen festgelegten Richtlinien.

(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:

(Voreinstellung)

Das Gerät verwendet für dieses Benutzerkonto das Protokoll HMAC-MD5.

Das Gerät verwendet für dieses Benutzerkonto das Protokoll HMAC-SHA.

SNMP-Verschlüsselung

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

Mögliche Werte:

Keine Verschlüsselung.

(Voreinstellung)

DES-Verschlüsselung

AES-128-Verschlüsselung

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

In der Voreinstellung sind die folgende Authentifizierungslisten verfügbar:

-
-

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 .

Schaltflächen



Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld 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 . 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 klicken.

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

Wenn Sie die Anwendung abwählen, dann bricht die Verbindung zum Gerät ab, sobald Sie auf Schaltfläche klicken.

Name

Zeigt die Bezeichnung der Liste.

Um eine Liste hinzuzufügen, 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 festgelegte Anwendung anwendet.

Das Gerät bietet Ihnen die Möglichkeit einer Fall-Back-Lösung. Legen Sie hierfür in den Richtlinienfeldern 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:

(Voreinstellung)

Das Gerät authentifiziert die Benutzer mittels der lokalen Benutzerverwaltung. Siehe Dialog .

Der Authentifizierungsliste können Sie diesen Wert nicht zuweisen.

Das Gerät authentifiziert die Benutzer mit einem RADIUS-Server im Netz. Den RADIUS-Server legen Sie im Dialog fest.


Abhängig von der Richtlinie, die Sie zuerst anwenden, akzeptiert das Gerät die Anmeldung des Benutzers beim Management des Geräts oder lehnt die Anmeldung ab. Mögliche Authentifizierungsszenarios sind:

- Wenn die erste Richtlinie in der Authentifizierungsliste ist und das Gerät die Anmelde-daten des Benutzers akzeptiert, meldet das Gerät den Benutzer beim Management des Geräts an, ohne die anderen Authentifizierungsrichtlinien anzuwenden.
- Wenn die erste Richtlinie in der Authentifizierungsliste ist und das Gerät die Anmelde-daten des Benutzers ablehnt, versucht das Gerät, den Benutzer mithilfe der anderen Richt-linien in der festgelegten Reihenfolge beim Management des Geräts anzumelden.
- Wenn die erste Richtlinie in der Authentifizierungsliste oder 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 Authentifi-zierung des Benutzers mit der nächsten Richtlinie.
- Wenn die erste Richtlinie in der Authentifizierungsliste ist, lehnen die Geräte die Benutzeranmeldung sofort ab, ohne eine andere Richtlinie anzuwenden.
- Vergewissern Sie sich, dass die Authentifizierungsliste mindestens eine Richtlinie enthält, die vom Wert abweicht.

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 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:

(Voreinstellung)

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

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 reicht die Zugangsdaten der Benutzer mittels Lightweight Directory Access Protocol (LDAP) 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 beim Management des Geräts 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 -Client ein/aus.

Das Gerät verwendet den -Client, wenn Sie im Dialog den Wert in einer der Spalten bis festlegen. Legen Sie zuvor im Dialog mindestens ein Mapping für die Zugriffsrolle fest. Damit haben Sie nach Anmeldung über LDAP weiterhin als Administrator Zugriff auf das Management des Geräts.

Mögliche Werte:

Der -Client ist eingeschaltet.

(Voreinstellung)

Der -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 beim Management des Geräts gültig bleibt. Wenn ein Benutzer sich innerhalb dieser Zeit erneut anmeldet, ist keine aufwendige LDAP-Suchoperation notwendig. Der Anmeldevorgang ist deutlich schneller.

Mögliche Werte:

(Voreinstellung:)

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 versucht, sich mit der Benutzerkennung am LDAP-Server zu authentifizieren, um den „Distinguished Name“ (DN) für die Benutzer zu finden, die sich beim Management des Geräts anmelden. Das Gerät sucht gemäß den Einstellungen in den Feldern und

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 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. Danach verwendet der Benutzer den in diesem Attribut enthaltenen Benutzernamen, um sich beim Management des Geräts anzumelden.

Häufig enthalten die LDAP-Attribute , , und einen eindeutigen Benutzernamen.

Unter der folgenden Voraussetzung fügt das Gerät die im Feld festgelegte Zeichenfolge an den Benutzernamen an:

- Der im Attribut enthaltene Benutzername enthält kein @-Zeichen.
- Im Feld ist ein Domänenname festgelegt.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen
(Voreinstellung:)

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

Um eine sichere Verbindung herzustellen, muss das Gerät ein gültiges digitales Zertifikat erhalten, damit es die Identität des Servers verifizieren kann. Voraussetzung ist, dass Sie das öffentliche Zertifikat des Servers auf das Gerät übertragen haben. Bitten Sie den Server-Administrator um ein digitales Zertifikat im X.509-Format. Hirschmann empfiehlt, aus Sicherheitsgründen ausschließlich digitale Zertifikate zu verwenden, die von einer Zertifizierungsstelle (Certification Authority, CA) signiert wurden.

URL


Legt Pfad und Dateiname des digitalen Zertifikats fest.

Das Gerät akzeptiert digitale Zertifikate mit den folgenden Eigenschaften:

- X.509-Format
- Dateinamenserweiterung
- Base64-kodiert und umschlossen von den Zeilen
"%C). À%24)B)ÀÀ4%"
%.À À%24)B)ÀÀ4%

Das Gerät bietet Ihnen folgende Möglichkeiten, die Datei auf das Gerät zu übertragen:

- Import vom PC

Befindet sich die Datei auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie diese in den -Bereich. Alternativ dazu klicken Sie in den Bereich, um die Datei auszuwählen. Außerdem können Sie die Datei von Ihrem PC mittels SFTP oder SCP zum Gerät übertragen. Führen Sie die folgenden Schritte aus:

Öffnen Sie auf Ihrem PC einen SFTP- oder SCP-Client, zum Beispiel WinSCP.

Öffnen Sie mit dem SFTP- oder SCP-Client eine Verbindung zum Gerät.

Übertragen Sie die Datei auf das Gerät in das Verzeichnis μ-j<°h jh°- >•m- .

Sobald die Datei vollständig übertragen ist, beginnt das Gerät, das digitale Zertifikat zu installieren. Wenn die Installation erfolgreich war, dann generiert das Gerät eine Datei <i> in im Verzeichnis μ-j<°h jh°- >•m- und löscht die übertragene Datei.

- Import von einem SCP- oder SFTP-Server

Befindet sich die Datei auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:

oder -->)0 Âhm• • 0-°h Â°-©l°k•

Klicken Sie die Schaltfläche , um das Fenster zu öffnen. In diesem Fenster geben Sie und ein, um sich am Server anzumelden.

oder --> "•lμ-#•ml°k• 0° n<m-)0 Âhm• • 0-°h Â°-©l°k•

Start

Überträgt die im Feld festgelegte Datei auf das Gerät.

Damit die Änderungen nach dem Übertragen eines digitalen Zertifikats in das Gerät wirksam werden, schalten Sie die Funktion aus und wieder ein. Siehe Rahmen .

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.

Legen Sie einen DNS-Namen fest, wenn in Spalte ein anderer Wert als festgelegt ist und das digitale Zertifikat ausschließlich DNS-Namen des Servers enthält.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung:)

DNS-Name im Format oder

Voraussetzung ist, dass Sie zusätzlich im Dialog die Funktion einschalten.

Wenn Sie eine verschlüsselte Verbindung mithilfe eines digitalen Zertifikats herstellen, vergewissern Sie sich, dass die - oder -Angabe im digitalen Zertifikat, das Sie auf das Gerät übertragen haben, mit dem hier festgelegten Wert übereinstimmt. Andernfalls kann das Gerät die Identität des Servers nicht verifizieren.

Mit diesem DNS-Namen erfragt das Gerät die LDAP-Server-Liste (SRV Resource Record) beim DNS-Server.

Ziel TCP-Port

Legt den TCP-Port fest, auf dem der Server die Anfragen erwartet.

Wenn in Spalte der Wert festgelegt ist, dann ignoriert das Gerät den hier festgelegten Wert.

Mögliche Werte:

(Voreinstellung:)

Ausnahme: Port ist für interne Funktionen reserviert.

Häufig verwendete TCP-Ports:

- :
- :
- :
- :

Verbindungssicherheit

Legt das Protokoll fest, das die Kommunikation zwischen Gerät und Authentication-Server verschlüsselt.

Mögliche Werte:

Keine Verschlüsselung.

Das Gerät baut eine LDAP-Verbindung zum Server auf und überträgt die Kommunikation inklusive Passwörter im Klartext.

Verschlüsselung mit SSL.

Das Gerät baut eine TLS-Verbindung zum Server auf und tunnelt darüber die LDAP-Kommunikation.

(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 digitale Zertifikat ausschließlich DNS-Namen enthält, dann legen Sie in Spalte den DNS-Namen des Servers fest. Schalten Sie die Funktion im Dialog ein.

Wenn das digitale Zertifikat im Feld Subject Alternative Name die IP-Adresse des Servers enthält, dann kann das Gerät die Identität des Servers auch ohne die DNS-Einstellungen verifizieren.

Status Server

Zeigt den Zustand der Verbindung und die Authentifizierung mit dem Authentication-Server.

Mögliche Werte:

Der Server ist erreichbar.

Wenn in Spalte ein anderer Wert als festgelegt ist, dann hat das Gerät das digitale Zertifikat des Servers verifiziert.

Server ist unerreichbar.

Das Gerät hat noch keine Verbindung zum Server aufgebaut.

Aktiv

Aktiviert/deaktiviert die Verwendung des Servers.

Mögliche Werte:

Das Gerät verwendet den Server.

(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 einzurichten, 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 beim Management des Geräts 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 . 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:

(Voreinstellung)

Das Gerät verwendet die Zugriffsrolle mit den weitreichenderen Berechtigungen.

Das Gerät wendet die Rolle mit dem kleineren Wert in Spalte 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 , um eine Tabellenzeile hinzuzufügen.

- Im Feld  legen Sie die Index-Nummer fest.
Mögliche Werte:



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.

Rolle

Legt die Zugriffsrolle fest, die den Zugriff des Benutzers auf die einzelnen Funktionen des Geräts regelt.

Mögliche Werte:

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.

(Voreinstellung)


Der Benutzer ist berechtigt, das Gerät zu überwachen.

Der Benutzer ist berechtigt, das Gerät zu überwachen und im Dialog die Protokoll-Datei zu speichern.

Der Benutzer ist berechtigt, das Gerät zu überwachen und die Einstellungen zu ändern – mit Ausnahme der Sicherheitseinstellungen für den Zugriff auf das Gerät.

Der Benutzer ist berechtigt, das Gerät zu überwachen und die Einstellungen zu ändern.

Typ

Legt fest, ob in Spalte  eine Gruppe oder ein Attribut mit einem Attributwert festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Die Spalte  enthält ein Attribut mit einem Attributwert.

Die Spalte  enthält den „Distinguished Name“ (DN) einer Gruppe.

Parameter

Legt abhängig von der Einstellung in Spalte 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 der Wert festgelegt ist, dann legen Sie das Attribut in der Form fest.

Beispiel:

- Wenn in Spalte der Wert festgelegt ist, dann legen Sie den „Distinguished Name“ (DN) einer Gruppe fest.

Beispiel:

Aktiv

Aktiviert/deaktiviert das Mapping der Rolle.

Mögliche Werte:

(Voreinstellung)

Das Mapping der Rolle ist aktiv.

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]
[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 [SNMPv1](#).

Mögliche Werte:

Server-Dienst ist aktiv.

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 [SNMPv2](#).

Mögliche Werte:

Server-Dienst ist aktiv.

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 .

Mögliche Werte:

Server-Dienst ist aktiv.

Server-Dienst ist inaktiv.

SSH-Server

Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit Secure Shell (SSH) ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte .

Mögliche Werte:

Server-Dienst ist aktiv.

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 .

Mögliche Werte:

Server-Dienst ist aktiv.

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 .

Mögliche Werte:

Server-Dienst ist aktiv.

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:

- Zugriff mittels SNMP-Version 1 ist aktiv.
 - Die Community-Namen legen Sie fest im Dialog [SNMPv1/v2 Community](#).
(Voreinstellung)
- Zugriff mittels SNMP-Version 1 ist inaktiv.

SNMPv2

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

Mögliche Werte:

- Zugriff mittels SNMP-Version 2 ist aktiv.
 - Die Community-Namen legen Sie fest im Dialog [SNMPv1/v2 Community](#).
(Voreinstellung)
- Zugriff mittels SNMP-Version 2 ist inaktiv.

SNMPv3

Aktiviert/deaktiviert den Zugriff auf das Gerät per SNMP Version 3.

Mögliche Werte:

- (Voreinstellung)
Zugriff ist aktiviert.
- 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:

- (Voreinstellung:)
Ausnahme: Port 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 das aktive Konfigurationsprofil.

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

Starten Sie das Gerät neu.

[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.

Um mit SFTP oder SCP auf das Gerät und den angeschlossenen externen Speicher zuzugreifen, benötigen Sie ebenfalls Zugriff auf den SSH-Server. Mit einem SFTP- oder SCP-Client, zum Beispiel WinSCP, haben Sie die Möglichkeit, Konfigurationsdateien oder ein Software-Update auf das Gerät zu laden.

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 generieren. Alternativ dazu übertragen Sie einen eigenen Host-Schlüssel im PEM-Format auf 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 , Spalte .

Funktion

SSH-Server

Schaltet den SSH-Server ein/aus.

Mögliche Werte:

(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.

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 Sie den -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:

(Voreinstellung:)
Ausnahme: Port 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.

Wenn Sie per Command Line Interface, SFTP oder SCP auf das Gerät zugreifen, stellt jede dieser Anwendungen eine eigenständige SSH-Verbindung zum Gerät her.

Mögliche Werte:

(Voreinstellung:)

Session Timeout [min]

Legt die Timeout-Zeit in Minuten fest. Bei Inaktivität des beim Management des Geräts angemeldeten Benutzers trennt das Gerät nach dieser Zeit die Verbindung.

Eine Änderung des Werts wird bei erneuter Anmeldung eines Benutzers beim Management des Geräts wirksam.

Mögliche Werte:

Deaktiviert die Funktion. Die Verbindung bleibt bei Inaktivität aufgebaut.
(Voreinstellung:)

Signatur

RSA vorhanden

Zeigt, ob ein RSA-Host-Key im Gerät vorhanden ist.

Mögliche Werte:

Schlüssel vorhanden.

Kein Schlüssel vorhanden.

Erstellen

Erzeugt einen Host-Key auf dem Gerät. Voraussetzung ist, dass der `ssh`-Server ausgeschaltet ist.

Länge des generierten Schlüssels:

- 2048 Bit (RSA)

Damit der SSH-Server den generierten Host-Key verwendet, starten Sie den SSH-Server neu.

Alternativ dazu übertragen Sie einen eigenen Host-Schlüssel im PEM-Format auf das Gerät. Siehe [Rahmen](#).

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:

Das Gerät erzeugt gegenwärtig einen RSA-Host-Key.

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 `ssh_fingerprint` anzeigt.

Mögliche Werte:



Das Feld `ssh_fingerprint_md5` zeigt den Fingerprint als hexadezimalen MD5-Hash.

(Voreinstellung)

Das Gerät unterstützt diese Einstellung nicht. Das Feld `ssh_fingerprint_md5` behält die bisherige Anzeige bei.

RSA-Fingerabdruck

Zeigt den Fingerprint des öffentlichen Host-Keys des SSH-Servers.

Wenn Sie die Einstellung im Feld `ssh_fingerprint_md5` 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, die Datei auf das Gerät zu übertragen:

- Import vom PC

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

Außerdem können Sie die Datei von Ihrem PC mittels SFTP oder SCP zum Gerät übertragen.

Führen Sie die folgenden Schritte aus:

Öffnen Sie auf Ihrem PC einen SFTP- oder SCP-Client, zum Beispiel WinSCP.

Öffnen Sie mit dem SFTP- oder SCP-Client eine Verbindung zum Gerät.

Übertragen Sie die Datei auf das Gerät in das Verzeichnis



Sobald die Datei vollständig übertragen ist, beginnt das Gerät, den Schlüssel zu installieren.


Wenn die Installation erfolgreich war, dann generiert das Gerät eine Datei im Verzeichnis und löscht die übertragene Datei.

- Import von einem SCP- oder SFTP-Server

Befindet sich die Datei auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:

oder `scp://hostname/path/to/keyfile`



Klicken Sie die Schaltfläche , um das Fenster  zu öffnen. In diesem

Fenster geben Sie  und  ein, um sich am Server anzumelden.

oder `scp://hostname/path/to/keyfile`

Start

Überträgt die im Feld  festgelegte Datei auf das Gerät.


Damit die Änderungen nach dem Übertragen eines digitalen Zertifikats auf das Gerät wirksam werden, schalten Sie die Funktion  aus und wieder ein. Siehe Rahmen .

[HTTP]

Diese Registerkarte ermöglicht Ihnen, das Hypertext Transfer Protocol (HTTP) für den Webserver 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 Hypertext Transfer Protocol (HTTP), verwenden Sie stattdessen das Hypertext Transfer Protocol Secure (HTTPS).

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 die Funktion ein/aus.

Mögliche Werte:

(Voreinstellung)

Die Funktion ist eingeschaltet.

Der Zugriff auf das Management des Geräts ist möglich über eine unverschlüsselte -
Verbindung.

Wenn die Funktion ebenfalls eingeschaltet ist, leitet das Gerät die Anfrage für eine -
Verbindung automatisch auf eine verschlüsselte -Verbindung um.

Die Funktion ist ausgeschaltet.

Wenn die Funktion eingeschaltet ist, ist der Zugriff auf das Management des Geräts über
eine verschlüsselte -Verbindung möglich.

Anmerkung: Wenn die Funktionen und ausgeschaltet sind, können Sie die Funktion
mit dem Kommando `enable` 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:

(Voreinstellung:)

Ausnahme: Port ist für interne Funktionen reserviert.


[HTTPS]

Diese Registerkarte ermöglicht Ihnen, das Hypertext Transfer Protocol Secure(HTTPS) für den
Webserver ein-/auszuschalten und die für HTTPS erforderlichen Einstellungen festzulegen.

Der Webserver liefert die grafische Benutzeroberfläche über eine verschlüsselte HTTP-Verbin-
dung aus.

Für die Verschlüsselung der HTTP-Verbindung ist ein digitales Zertifikat notwendig. Das Gerät
ermöglicht Ihnen, dieses digitale Zertifikat selbst zu generieren oder ein vorhandenes digitale Zerti-
fikat auf das Gerät zu übertragen.

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 die Funktion ein/aus.

Mögliche Werte:

(Voreinstellung)

Die Funktion ist eingeschaltet.

Der Zugriff auf das Management des Geräts ist möglich über eine verschlüsselte -Verbindung.

Wenn kein digitales Zertifikat vorhanden ist, erzeugt das Gerät ein digitales Zertifikat, bevor es die Funktion einschaltet.

Die Funktion ist ausgeschaltet.

Wenn die Funktion eingeschaltet ist, ist der Zugriff auf das Management des Geräts möglich über eine unverschlüsselte -Verbindung.

Anmerkung: Wenn die Funktionen und ausgeschaltet sind, können Sie die Funktion mit dem Kommando `enable` 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:

(Voreinstellung:)

Ausnahme: Port ist für interne Funktionen reserviert.

Zertifikat

Wenn das Gerät ein digitales Zertifikat verwendet, das nicht von einer dem Webbrowser bekannten Zertifizierungsstelle (Certification 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:

- Übertragen Sie auf das Gerät ein digitales Zertifikat, dessen Zertifizierungsstelle (Certification Authority, CA) Ihrem Webbrowser bekannt ist. Dies kann zusätzlich erfordern, dass Sie die Zertifizierungsstelle (Certification Authority, 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 ein digitales Zertifikat im Gerät vorhanden ist.

Mögliche Werte:

Ein digitales Zertifikat ist vorhanden.

Das digitale Zertifikat wurde entfernt.

Erstellen

Generiert ein digitales Zertifikat auf dem Gerät.

Bis zum Neustart verwendet der Webserver das vorherige Zertifikat.

Damit der Webserver das neu generierte digitale Zertifikat verwendet, starten Sie den Webserver neu. Der Neustart des Webserver ist ausschließlich über das Command Line Interface möglich.

Alternativ dazu übertragen Sie ein eigenes digitales Zertifikat auf das Gerät. Siehe Rahmen 
 

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:

Das Gerät generiert oder löscht gegenwärtig kein digitales Zertifikat.

Das Gerät löscht gegenwärtig ein digitales Zertifikat.

Das Gerät generiert gegenwärtig ein digitales 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 anzeigt.

Mögliche Werte:

Das Feld zeigt den SHA1-Fingerprint des digitalen Zertifikats.
(Voreinstellung)

Das Feld zeigt den SHA256-Fingerprint des digitalen Zertifikats.

Fingerabdruck

Hexadezimale Zeichenfolge des vom Server verwendeten digitalen Zertifikats.

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

Zertifikat-Import

URL

Legt Pfad und Dateiname des digitalen Zertifikats fest.

Das Gerät akzeptiert digitale Zertifikate mit den folgenden Eigenschaften:


- X.509-Format
- Dateinamenserweiterung
- Base64-kodiert und umschlossen von den Zeilen
—

oder

- RSA-Schlüssel mit 2048 bit Länge

Das Gerät bietet Ihnen folgende Möglichkeiten, die Datei auf das Gerät zu übertragen:

- Import vom PC



Befindet sich die Datei auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie diese in den -Bereich. Alternativ dazu klicken Sie in den Bereich, um die Datei auszuwählen. Außerdem können Sie die Datei von Ihrem PC mittels SFTP oder SCP zum Gerät übertragen. Führen Sie die folgenden Schritte aus:

- Öffnen Sie auf Ihrem PC einen SFTP- oder SCP-Client, zum Beispiel WinSCP.
- Öffnen Sie mit dem SFTP- oder SCP-Client eine Verbindung zum Gerät.
- Übertragen Sie die Datei auf das Gerät in das Verzeichnis `./`.
- Sobald die Datei vollständig übertragen ist, beginnt das Gerät, das Zertifikat zu installieren.
- Wenn die Installation erfolgreich war, dann generiert das Gerät eine Datei `cert` im Verzeichnis `./` und löscht die übertragene Datei.

- Import von einem SCP- oder SFTP-Server

Befindet sich die Datei auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:


– `scp://hostname/path/to/file` oder `sftp://hostname/path/to/file`

Klicken Sie die Schaltfläche , um das Fenster  zu öffnen. In diesem Fenster geben Sie `hostname` und `username` ein, um sich am Server anzumelden.

– `scp://hostname/path/to/file` oder `sftp://hostname/path/to/file`

Start

Überträgt die im Feld `File` festgelegte Datei auf das Gerät.

Damit die Änderungen nach dem Übertragen eines digitalen Zertifikats auf das Gerät wirksam werden, schalten Sie die Funktion `Apply` aus und wieder ein. Siehe Rahmen .

3.4.2 IP-Zugriffsbeschränkung

[Gerätesicherheit > Management-Zugriff > IP-Zugriffsbeschränkung]

Dieser Dialog ermöglicht Ihnen, den Zugriff auf das Management des Geräts für ausgewählte Anwendungen von einem festgelegten IP-Adressbereich aus oder über das festgelegte physische Interface zu beschränken.

- Wenn die Funktion ausgeschaltet ist, dann ist der Zugriff auf das Management des Geräts unbeschränkt. Jeder kann mit einer beliebigen Anwendung und von einer beliebigen IP-Adresse aus oder über ein beliebiges physisches Interface auf das Management des Geräts zugreifen.
- Bei eingeschalteter Funktion ist der Zugriff beschränkt. Jeder hat Zugriff auf das Management des Geräts ausschließlich unter den folgenden Bedingungen:
 - Mindestens eine Regel ist aktiv.
 - und
 - Sie greifen mit einer erlaubten Anwendung von einem zugelassenen IP-Adressbereich aus oder über ein zugelassenes physisches Interface auf das Gerät zu, wie in der Regel festgelegt.

Funktion

Funktion

Schaltet die Funktion ein/aus.

Mögliche Werte:

Die Funktion ist eingeschaltet.
Der Zugriff auf das Management des Geräts ist beschränkt.

Anmerkung: Bevor Sie die Funktion aktivieren, vergewissern Sie sich, dass die Tabelle mindestens eine aktive Regel enthält, welche Ihnen Zugriff auf das Management des Geräts gewährt. Andernfalls ist der Zugriff auf das Management des Geräts ausschließlich mithilfe des Command Line Interface über die serielle Verbindung möglich.

(Voreinstellung)
Die Funktion 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.

Die Priorität des Zugriffs auf das Management des Geräts basiert auf der Indexnummer.

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

Mögliche Werte:

Interface

Legt das physische Interface fest, über das Benutzer auf das Management des Geräts zugreifen können.

Voraussetzung ist, dass in Spalte und Spalte der Wert festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Benutzer haben über jedes Interface auf Grundlage der in Spalte angegebenen IP-Adresse eingeschränkten Zugriff auf das Management des Geräts.

Benutzer können auf das Management des Geräts ausschließlich über das festgelegte Interface eingeschränkt zugreifen.

Das Gerät unterstützt die Funktion ausschließlich auf physischen Interfaces, nicht auf logischen Interfaces.

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 .

Voraussetzung ist, dass in Spalte der Wert festgelegt ist.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung:)

Netzmaske

Legt den Bereich des in Spalte festgelegten Netzes fest.

Voraussetzung ist, dass in Spalte der Wert festgelegt ist.

Mögliche Werte:

Gültige Netzmaske (Voreinstellung:)

Ein Beispiel: Um den Zugriff von einer einzelnen IP-Adresse aus zu beschränken, legen Sie den Wert fest.

HTTP

Aktiviert/deaktiviert den HTTP-Zugriff.

Mögliche Werte:

(Voreinstellung)

HTTP-Zugriff ist aktiviert. Der Zugriff ist von dem nebenstehenden IP-Adressbereich aus oder über das nebenstehende physische Interface möglich.

HTTP-Zugriff ist inaktiv.

HTTPS

Aktiviert/deaktiviert den HTTPS-Zugriff.

Mögliche Werte:

(Voreinstellung)

HTTPS-Zugriff ist aktiv. Der Zugriff ist von dem nebenstehenden IP-Adressbereich aus oder über das nebenstehende physische Interface möglich.

HTTPS-Zugriff ist inaktiv.

SNMP

Aktiviert/deaktiviert den SNMP-Zugriff.

Mögliche Werte:

(Voreinstellung)

SNMP-Zugriff ist aktiv. Der Zugriff ist von dem nebenstehenden IP-Adressbereich aus oder über das nebenstehende physische Interface möglich.

SNMP-Zugriff ist inaktiv.

SSH

Aktiviert/deaktiviert den SSH-Zugriff.

Mögliche Werte:

(Voreinstellung)

SSH-Zugriff ist aktiv. Der Zugriff ist von dem nebenstehenden IP-Adressbereich aus oder über das nebenstehende physische Interface möglich.

SSH-Zugriff ist inaktiv.

Aktiv

Aktiviert/deaktiviert die Tabellenzeile.

Mögliche Werte:

Die Tabellenzeile ist aktiv. Das Gerät schränkt den Zugriff auf das Management des Geräts auf den festgelegten IP-Adressbereich oder über das festgelegte Interface für ausgewählte Anwendungen ein.

(Voreinstellung für neue Tabellenzeile)

Die Tabellenzeile ist inaktiv. Das Gerät schränkt den Zugriff auf das Management des Geräts von dem festgelegten IP-Adressbereich aus oder über das festgelegte Interface für ausgewählte Anwendungen nicht ein.

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 beim Management des Geräts angemeldeten Benutzers.

Mögliche Werte:

(Voreinstellung:)

Der Wert 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:

- V.24-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

() inklusive Leerzeichen

Wildcards

- Datum
- IP-Adresse
- MAC-Adresse
- Produktname
- Uhrzeit

Voreinstellung:

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 beim Management des Geräts angemeldet ist.

Mögliche Werte:

(Voreinstellung:)

Der Wert deaktiviert die Funktion, der Benutzer bleibt bei Inaktivität beim Management des Geräts angemeldet.

Eine Änderung des Werts wird bei erneuter Anmeldung eines Benutzers beim Management des Geräts wirksam.

Für den `server`-Server legen Sie das Timeout fest im Dialog `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 Einstellungen des Geräts. 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 `server`.

Funktion

Funktion

Schaltet die Funktion `server` ein/aus.

Mögliche Werte:

Die Funktion `server` ist eingeschaltet.
Das Gerät zeigt die im Feld `server` festgelegte Textinformation den Benutzern, die sich mit dem Command Line Interface beim Management des Geräts anmelden.

(Voreinstellung)

Die Funktion `server` ist ausgeschaltet.
Der Startbildschirm zeigt Informationen über das Gerät. Die Textinformation im Feld `server` 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
(`server`) inklusive Leerzeichen

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.

Anwendungen senden Anfragen mittels SNMPv1/v2 mit einem Community-Namen im SNMP-Datenpaket-Header. Abhängig vom Community-Namen (siehe Spalte) erhält die Anwendung die Berechtigung Lesen oder Lesen und Schreiben.

Den Zugriff auf das Gerät mittels SNMPv1/v2 aktivieren Sie im Dialog -
□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□

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:

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

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
- Das Gerät akzeptiert die folgenden Zeichen:
-
-
-
-
-
- (Voreinstellung für die Berechtigung Lesen und Schreiben)
- (Voreinstellung für die Berechtigung Lesen)

3.5 Pre-Login-Banner

[Gerätesicherheit > Pre-Login-Banner]

Dieser Dialog ermöglicht Ihnen, Benutzern einen Begrüßungs- oder Hinweistext anzuzeigen, bevor diese sich beim Management des Geräts anmelden.

Die Benutzer sehen den Text im Login-Dialog der grafischen Benutzeroberfläche und im Command Line Interface. Benutzer, die sich mit SSH beim Management des Geräts anmelden, sehen den Text – unabhängig vom verwendeten Client – vor oder während der Anmeldung.

Um den Text ausschließlich im Command Line Interface anzuzeigen, verwenden Sie die Einstellungen im Dialog

Funktion

Funktion

Schaltet die Funktion ein/aus.

Mit der Funktion zeigt das Gerät im Login-Dialog der grafischen Benutzeroberfläche und im Command Line Interface eine Begrüßung oder einen Hinweis.

Mögliche Werte:

Die Funktion ist eingeschaltet.
Das Gerät zeigt im Login-Dialog den im Feld festgelegten Text.
(Voreinstellung)

Die Funktion ist ausgeschaltet.
Das Gerät zeigt im Login-Dialog keinen Text. Haben Sie im Feld einen Text eingegeben, speichert das Gerät diesen Text.

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
() inklusive Leerzeichen

4 Netzsicherheit

Das Menü enthält die folgenden Dialoge:

Netzsicherheit Übersicht
RADIUS
Asset
Protokoll
Paketfilter
Deep Packet Inspection
DoS

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 eingerichteten -Regeln
Siehe Dialog
- die eingerichteten -Regeln
Siehe Dialog
- die eingerichteten -Regeln
Siehe Dialog
- die eingerichteten -Regeln
Siehe Dialog
- die eingerichteten -Regeln
Siehe Dialog
- die eingerichteten -Regeln
Siehe Dialog

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 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.

Das Gerät arbeitet in der Rolle des RADIUS-Clients, wenn Sie im Dialog einer Anwendung die Richtlinie 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:

- :
- :
- :

Das Menü enthält die folgenden Dialoge:

- [RADIUS Global](#)
- [RADIUS Authentication-Server](#)
- [RADIUS Authentication Statistiken](#)

4.21 RADIUS Global

[Netzicherheit > RADIUS > Global]

Dieser Dialog ermöglicht Ihnen, grundlegende Einstellungen für RADIUS festzulegen.

RADIUS-Konfiguration

Schaltflächen

 Zurücksetzen

Löscht die Statistik im Dialog

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:

(Voreinstellung:)

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:

(Voreinstellung:)

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:)

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.

4.2.2 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 , um eine Tabellenzeile hinzuzufügen.

- Im Feld  legen Sie die Index-Nummer fest.
- Im Feld  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 Index-Nummer 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: )

Sie können für mehrere Server den gleichen Namen festlegen. Wenn mehrere Server den gleichen Namen haben, gilt die Einstellung in Spalte .

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:

(Voreinstellung:)
Ausnahme: Port 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.

Primärer Server

Kennzeichnet den Authentication-Server als primär oder sekundär.

Mögliche Werte:

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 hat.

(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 den Wert in einer der Spalten bis festlegen.

Mögliche Werte:

(Voreinstellung)

Die Verbindung ist aktiv. Das Gerät sendet die Zugangsdaten zum Authentifizieren der Benutzer an diesen Server, wenn die obengenannten Voraussetzungen erfüllt sind.

Die Verbindung ist inaktiv. Das Gerät sendet keine Zugangsdaten an diesen Server.

4.2.3 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

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 den Zeitabstand 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.

4.3 Asset

[Netzicherheit > Asset]

Dieser Dialog ermöglicht Ihnen, die Einstellungen für die Verwaltung der Assets festzulegen. Ein Asset kann ein physisches Gerät repräsentieren, wie eine SPS (Speicherprogrammierbare Steuerung), einen Computer oder ein Gerät im Netz. Ein Asset kann auch ein virtuelles Objekt repräsentieren, wie einen Multicast-Adressbereich oder eine Multicast-Adresse. Assets bieten Flexibilität beim Einrichten und Pflegen von Firewall-Regeln. Das Gerät ermöglicht Ihnen, bis zu 100 Assets einzurichten.

Tabelle

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

Schaltflächen



Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld legen Sie einen eindeutigen Namen für das Asset fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen, mit Ausnahme des Zeichens

Nach Klicken der Schaltfläche fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile den im Feld festgelegten Namen zu.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die fortlaufende Nummer des Assets, auf das sich die Tabellenzeile bezieht. Das Gerät weist den Wert automatisch zu, wenn Sie eine Tabellenzeile hinzufügen.

Name

Legt einen eindeutigen Namen für das Asset fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen, mit Ausnahme des Zeichens

Beschreibung

Legt eine Beschreibung für das Asset fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen

Typ

Legt den Typ des Assets fest.

Mögliche Werte:

(Voreinstellung)

Hersteller

Legt den Hersteller des Assets fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen

Modell

Legt das Modell des Assets fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen

Ungefährer Standort

Legt einen allgemeinen Ort für das Asset fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen

Genauer Standort

Legt einen spezifischen Ort für das Asset fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen

Asset-Tag

Legt ein Tag zur Identifizierung des benutzerdefinierten Assets fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen

IP-Adresse

Legt die IP-Adresse des Assets fest.

Mögliche Werte:

(Voreinstellung)

Das Gerät akzeptiert jede IP-Adresse, die mit dem Asset verknüpft ist.

Gültige IPv4-Adresse

Das Gerät wendet die festgelegte IP-Adresse auf das Asset an.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Das Gerät wendet die festgelegte IP-Adresse in dem festgelegten Subnetz auf das Asset an.

Beispiel:

Ein der IP-Adresse vorangestelltes Ausrufezeichen () verkehrt den Ausdruck ins Gegenteil.

Das Gerät akzeptiert eine beliebige IP-Adresse oder das mit dem Asset verbundene Subnetz mit Ausnahme der festgelegten IP-Adresse oder des festgelegten Subnetzes.

Beispiel: oder

MAC-Adresse

Legt die MAC-Adresse des Assets fest.

Mögliche Werte:

(Voreinstellung)

Das Gerät akzeptiert jede MAC-Adresse, die mit dem Asset verknüpft ist.

Gültige MAC-Adresse

Das Gerät wendet die festgelegte MAC-Adresse auf das Asset an.

4.4 Protokoll

[Netzsicherheit > Protokoll]

In diesem Dialog legen Sie grundlegende Einstellungen für das benutzerdefinierte Protokoll fest. Das Gerät ermöglicht Ihnen, bis zu 50 benutzerdefinierte Protokolle einzurichten.



Tabelle

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

Schaltflächen





Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen. Im Feld  legen Sie einen eindeutigen Namen für das Protokoll fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen, mit Ausnahme der folgenden Zeichen:

—
—
—
—
—
—
—
—
—
—

Nach Klicken der Schaltfläche  fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile den im Feld  festgelegten Namen zu.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die fortlaufende Nummer des Protokolls, auf das sich die Tabellenzeile bezieht. Das Gerät weist den Wert automatisch zu, wenn Sie eine Tabellenzeile hinzufügen.

Protokollname

Legt einen eindeutigen Namen für das Protokoll fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen, mit Ausnahme der folgenden Zeichen:

-
-
-
-
-
-
-
-
-

Beschreibung

Legt eine Beschreibung für das Protokoll fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen

Protokolltyp

Legt den Protokolltyp für das benutzerdefinierte Protokoll fest, das das Gerät in der Paketfilter-Regel anwendet.

Mögliche Werte:

(Voreinstellung)

Ethertype

Legt das Ethertype-Schlüsselwort der Datenpakete fest, das der Schicht-2-Paketfilter anwendet.

Mögliche Werte:

(Voreinstellung)

Benutzerspezifischer Ethertype-Wert

Legt den Ethertype-Wert der Datenpakete in Dezimalschreibweise fest, den der Schicht-2-Paketfilter anwendet. Voraussetzung ist, dass in Spalte der Wert festgelegt ist.

Mögliche Werte:

(Voreinstellung:)

Protocol number

Legt die Protokollnummer für das benutzerdefinierte Protokoll fest, das der IPv4-Header benutzt. Voraussetzung ist, dass in Spalte ein anderer Wert als festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Port

Legt den Ziel-Port fest, den das Gerät in dem Datenpaket auswertet. Voraussetzung ist, dass in Spalte der Wert oder festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die Regel auf sämtliche Datenpakete an, ohne den Ziel-Port zu bewerten.

Das Gerät wendet die Regel ausschließlich auf Datenpakete an, die den festgelegten Ziel-Port enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Mit einem einzelnen Zahlenwert legen Sie einen Port fest, zum Beispiel .
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel .
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel .
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel .

Das Feld ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel eingeben, verwenden Sie 4 von 15 Zahlenwerten.

4.5 Paketfilter

[Netzsicherheit > Paketfilter]

In diesem Menü legen Sie die Einstellungen für die Funktionen fest.

Das Menü enthält die folgenden Dialoge:

- [Routed-Firewall-Modus](#)
- [Transparent-Firewall-Modus](#)

4.5.1 Routed-Firewall-Modus

[Netzsicherheit > Paketfilter > Routed-Firewall-Modus]

In diesem Menü legen Sie die Einstellungen für den -Paketfilter fest.

Der -Paketfilter enthält Regeln, die das Gerät nacheinander auf den Datenstrom auf seinen Router-Interfaces anwendet. Der -Paketfilter bewertet den Datenstrom statusorientiert und filtert unerwünschte Datenpakete selektiv. Das Gerät bewertet den Zustand der Verbindung und ermittelt auch, ob die Datenpakete zu einer bestimmten Verbindung gehören (Stateful Packet Inspection).

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.

Wenn keine Regel zutrifft, wendet das Gerät die Standard-Regel an. In der Voreinstellung hat die Standard-Regel den Wert . Das Gerät ermöglicht Ihnen, die Standard-Regel im Dialog zu ändern.

Das Gerät bietet Ihnen ein mehrstufiges Konzept für das Einrichten und Anwenden der -Regeln:

- Eine Regel hinzufügen.
- Die Regel einem Router-Interface zuweisen.
Bis zu diesem Schritt haben Änderungen keine Auswirkung auf das Verhalten des Geräts und auf den Datenstrom.
- Die Regel auf den Datenstrom anwenden.

Die Datenpakete durchlaufen die Filter-Funktionen des Geräts in folgender Reihenfolge:

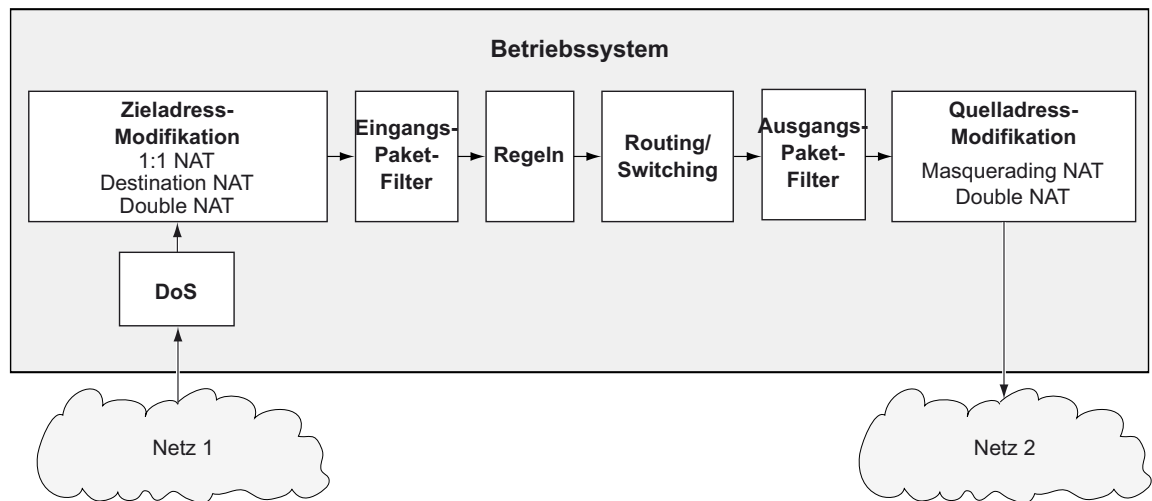


Abb. 1: Bearbeitungsreihenfolge der Datenpakete im Gerät

Das Menü enthält die folgenden Dialoge:

- [Global](#)
- [Firewall-Lern-Modus](#)
- [Paketfilter Regel](#)
- [Paketfilter Zuweisung](#)
- [Paketfilter Übersicht](#)

4.5.1.1 Global

[Netzicherheit > Paketfilter > Routed-Firewall-Modus > Global]

In diesem Dialog legen Sie die globalen Einstellungen für den -Paketfilter fest.

Konfiguration

Schaltflächen

 Änderungen anwenden

Wendet die im Gerät gespeicherten Regeln auf den Datenstrom an.

Das Gerät entfernt dabei auch die Zustandsinformationen des Paketfilters. Dies beinhaltet eventuell vorhandene DCE RPC-Informationen der Funktion . Das Gerät unterbricht hierbei offene Kommunikationsverbindungen.

Anmerkung: Während das Gerät die gespeicherten Regeln aktiviert, können Sie keine neuen Kommunikationsverbindungen herstellen.

L3-Firewall Erlaubte Regeln (max.)

Zeigt die maximale Anzahl erlaubter Firewall-Regeln für Datenpakete.

Default-Policy

Legt fest, wie die Firewall Datenpakete verarbeitet, wenn keine Regel zutrifft.

Mögliche Werte:

(Voreinstellung)

Das Gerät akzeptiert die Datenpakete.

Das Gerät verwirft die Datenpakete.

Das Gerät verwirft das Datenpaket und sendet eine ICMP Admin Prohibited-Nachricht an den Absender.

Prüfsumme validieren

Legt fest, wie die Firewall das Verbindungs-Tracking auf Grundlage der Datenpaket-Prüfsumme handhabt.

Mögliche Werte:

(Voreinstellung)

Das Gerät wertet die Prüfsumme im Datenpaket aus. Wenn der Wert ungültig ist, dann verwirft das Gerät das Datenpaket.

Das Gerät ignoriert die Prüfsumme. Das Gerät leitet das Datenpaket weiter, auch dann, wenn der Wert ungültig ist.


Information

Nicht angewendete Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten -Regeln von den im Gerät gespeicherten -Regeln unterscheiden.

Mögliche Werte:

Mindestens eine der im Gerät gespeicherten -Regeln enthält geänderte Einstellungen.

Wenn Sie die Schaltfläche  klicken, wendet das Gerät die -Regeln auf den Datenstrom an.

Das Gerät wendet die gespeicherten -Regeln auf den Datenstrom an.

4.5.1.2 Firewall-Lern-Modus

[Netzicherheit > Paketfilter > Routed-Firewall-Modus > FLM]

Dieser Dialog ermöglicht es Ihnen, die für den Zugriff auf das Netz zulässigen Verbindungen festzulegen.

Die maximale Anzahl von Regeln, die Sie mithilfe der Funktion `rule` festlegen können, ist abhängig von der Anzahl der im Dialog `rule` bereits erstellten Regeln. Das Gerät ermöglicht Ihnen, bis zu 2048 Regeln festzulegen.

Die Funktion `rule` gilt ausschließlich für Pakete, die das Gerät passieren und mit der Kette FORWARD übereinstimmen. Die Funktion `rule` wirkt sich nicht auf Pakete aus, die das Gerät an der Kette INPUT empfängt, und auf Pakete, die das Gerät an der Kette OUTPUT generiert. Während der Lernphase behält das Gerät den SSH-, SNMP- und GUI-Zugriff bei.

Für die Funktion `rule` ist erforderlich, dass Sie mindestens 2 Router-Interfaces im Gerät einrichten und auswählen.

Die Funktion `rule` kann maximal `2048` Verbindungen erlernen.

Anmerkung: Während der Lernphase ist das Netz vorübergehend gefährdet, da die Funktion `rule` Regeln einrichtet, die jedes Datenpaket auf den ausgewählten Ports akzeptieren.

Anmerkung: Wenn Sie auf einem Router-Interface die Funktion `rule` einschalten, dann ist auf diesem Router-Interface die Funktion `rule` unwirksam.

Der Dialog enthält die folgenden Registerkarten:

[\[Konfiguration\]](#)

[\[Regeln\]](#)

[Konfiguration]

Die Registerkarte ermöglicht Ihnen, die Funktion `rule` einzuschalten. Das Gerät überwacht bis zu 4 Interfaces, um herauszufinden, welche Art von Datenpaketen das Gerät über die Interfaces in das Netz vermittelt.

Funktion

Funktion

Schaltet die Funktion `rule` ein/aus.

Mögliche Werte:

Die Funktion `rule` ist eingeschaltet.

(Voreinstellung)

Die Funktion `rule` ist ausgeschaltet.

Information

Schaltflächen

 Start

Startet die Lernphase. Das Gerät filtert die Datenpakete an den aktiven Interfaces.

 Stop

Stoppt die Lernphase.

 Leeren

Leert den Speicher. Gelernte Daten können ausschließlich dann gelöscht werden, wenn die Funktion gestoppt wird.

Status

Zeigt den Zustand der aktiven -Anwendung.

Mögliche Werte:

Die Funktion ist inaktiv.

Das Gerät hat den Lernmodus angehalten. In der Registerkarte finden Sie Informationen zu den gelernten Daten.

Das Gerät erlernt Daten.

Das Gerät ist mit der Verarbeitung erlernter Daten beschäftigt.

Information

Zeigt den Status des -Anwendungsspeichers.

Für Lernen ausgewählte Interfaces

Zeigt die Interfaces, welche die Funktion aktiv überwacht. Das Gerät überwacht maximal 4 Interfaces.

Weitere Informationen

Zeigt eine Meldung zu einem speziellen Status.

Gelernte Einträge

Zeigt die Anzahl der Schicht-3-Einträge in der Verbindungstabelle.

Freier Speicher für Lerndaten [%]

Zeigt den prozentualen Anteil des freien Speicherplatzes, der für das Erlernen von Daten verfügbar ist.

[Regeln]

Diese Registerkarte zeigt den Typ der Daten, welche die ausgewählten Ports passieren. Sie können Regeln hinzufügen, um den Datenstrom zu verwalten, der das Gerät durchquert. Auf Grundlage der in der Tabelle angezeigten Daten können Sie nach Bedarf Daten akzeptieren oder ablehnen.

Die Registerkarte ist aktiv, nachdem das Gerät ein Datenpaket weitergeleitet hat und die Funktion wieder ausgeschaltet ist.

Tabelle Gelesene Einträge

Schaltflächen



Hinzufügen

Öffnet das Fenster , um eine Regel hinzuzufügen, sofern die Tabelle mindestens eine Tabellenzeile enthält. Die Tabelle zeigt die hinzugefügte Regel.

- Im Feld legen Sie einen Namen für die Regel fest.
- Im Feld legen Sie die Quelladresse der Datenpakete fest.
- Im Feld legen Sie die Zieladresse der Datenpakete fest.
- In der Dropdown-Liste wählen Sie den Protokolltyp der Datenpakete.
- Im Feld legen Sie den Ziel-Port der Datenpakete fest.
- Im Feld geben Sie an, ob das Gerät die Regel auf Datenpakete anwendet, die ein Router-Interface empfängt oder sendet.

Quelle Adresse

Zeigt die Quelladresse der Pakete.

Ziel Adresse

Zeigt die Zieladresse des Paketes.

Protokoll

Zeigt das IP-Protokoll auf der Basis von RFC 791 für die Protokollfilterung.

Ziel Port

Zeigt den Ziel-Port des Paketes.

Eingangs-Interface

Zeigt das Interface, welches das Paket empfangen hat.

Ausgangs-Interface

Zeigt das Interface, welches das Paket gesendet hat.

Erstes Vorkommen

Zeigt den Zeitpunkt, zu dem das Gerät das Paket zum ersten Mal ermittelt hat.

Connections by Rule Set

Zeigt die Anzahl der Verbindungen, die mit den in der unten stehenden Tabelle festgelegten Regeln übereinstimmen.

Connections by Selection

Zeigt die Anzahl der Verbindungen, die mit der Auswahl in der unten stehenden Tabelle übereinstimmen.

Tabelle Paketfilter-Regeln

Schaltflächen



Löschen

Entfernt die ausgewählte Tabellenzeile.



Bearbeiten

Öffnet das Fenster , um die Parameter der ausgewählten Tabellenzeile zu bearbeiten.

Regel-Index

Zeigt die fortlaufende Nummer der -Regel.

Beschreibung

Legt einen Namen für die Regel fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen

Quelle Adresse

Legt die Quelladresse der Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die -Regel auf Datenpakete mit beliebiger Quelladresse an.

Gültige IPv4-Adresse

Das Gerät wendet die Regel auf Datenpakete mit der festgelegten Quelladresse an.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Das Gerät wendet die Regel auf Datenpakete mit der festgelegten Quelladresse im festgelegten Subnetz an.

Ziel Adresse

Legt die Zieladresse der Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die -Regel auf Datenpakete mit beliebiger Zieladresse an.

Gültige IPv4-Adresse

Das Gerät wendet die Regel auf Datenpakete mit der festgelegten Zieladresse an.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Das Gerät wendet die Regel auf Datenpakete mit der festgelegten Zieladresse im festgelegten Subnetz an.

Protokoll

Legt den Protokolltyp 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:

(Voreinstellung)

Das Gerät wendet die Regel auf jedes Datenpaket an, ohne das Protokoll zu bewerten.

Internet Control Message Protocol (RFC 792)

Internet Group Management Protocol

IP in IP tunneling (RFC 2003)

Transmission Control Protocol (RFC 793)

User Datagram Protocol (RFC 768)

IPsec Encapsulated Security Payload (RFC 2406)

IPsec Authentication Header (RFC 2402)

Internet Control Message Protocol for IPv6

Ziel Port

Legt den Ziel-Port der Datenpakete fest, auf die das Gerät die Regel anwendet. Voraussetzung ist, dass in Spalte der Wert oder festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die -Regel auf sämtliche Datenpakete an, ohne den Ziel-Port zu bewerten.

Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, die den festgelegten Ziel-Port enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Mit einem einzelnen Zahlenwert legen Sie einen Port fest, zum Beispiel .
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel .
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel .
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel .

Das Feld ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel eingeben, verwenden Sie 4 von 15 Zahlenwerten.

Aktion

Legt fest, wie das Gerät die Datenpakete behandelt, wenn es die Regel anwendet.

Mögliche Werte:

(Voreinstellung)

Das Gerät akzeptiert die Datenpakete gemäß den Ingress-Regeln. Anschließend wendet das Gerät die Egress-Regeln an, bevor der Port die Datenpakete sendet.

Das Gerät verwirft das Datenpaket, ohne den Absender zu informieren.

Das Gerät verwirft das Datenpaket und informiert den Absender.

Das Gerät wendet die in Spalte festgelegte Regel auf die Datenpakete an.

Das Gerät wendet die in Spalte festgelegte Regel auf die Datenpakete an.

Das Gerät wendet die in Spalte festgelegte Regel auf die Datenpakete an.

Das Gerät wendet die in Spalte festgelegte Regel auf die Datenpakete an.

Das Gerät wendet die in Spalte festgelegte Regel auf die Datenpakete an.

Eingangs-Interface

Zeigt, ob das Gerät die -Regel auf Datenpakete anwendet, die das Gerät über ein Router-Interface sendet oder empfängt.

Mögliche Werte:

Das Gerät wendet die -Regel auf Datenpakete an, die es auf dem Router-Interface empfängt.

Das Gerät wendet die -Regel auf Datenpakete an, die es auf dem Router-Interface sendet.

Aktiv

Aktiviert/deaktiviert die Regel.

Mögliche Werte:

Die Regel ist aktiv.
(Voreinstellung)

Die Regel ist inaktiv.

4.5.1.3 Paketfilter Regel

[Netzsicherheit > Paketfilter > Routed-Firewall-Modus > Regel]

Dieser Dialog ermöglicht Ihnen, Regeln für den Paketfilter einzurichten. Sie weisen die hier festgelegten Regeln im Dialog dem gewünschten Router-Interface zu.

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.

Regel-Index

Zeigt die fortlaufende Nummer der -Regel. Das Gerät weist den Wert automatisch zu, wenn Sie eine Tabellenzeile hinzufügen.

Beschreibung

Legt einen Namen für die Regel fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen

Quelle Adresse

Legt den Asset-Namen oder die Quelladresse der Datenpakete fest, auf die das Gerät die Regel anwendet. Wählen Sie in der Dropdown-Liste einen Eintrag oder legen Sie die Quelladresse fest. Sie legen den Asset-Namen im Dialog fest.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die Regel auf Datenpakete mit beliebigem Asset-Namen oder beliebiger Quelladresse an.

Gültige IPv4-Adresse

Das Gerät wendet die Regel auf Datenpakete mit der festgelegten Quelladresse an.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Das Gerät wendet die Regel auf Datenpakete mit der festgelegten Quelladresse im festgelegten Subnetz an.

Beispiel:

Ein der IP-Adresse vorangestelltes Ausrufezeichen () verkehrt den Ausdruck ins Gegenteil. Das Gerät wendet die Regel auf Datenpakete mit beliebiger Quelladresse oder Subnetz an, mit Ausnahme der festgelegten Quelladresse oder des festgelegten Subnetzes.

Beispiel: oder

Name des Assets

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

Ziel Adresse

Legt den Asset-Namen oder die Zieladresse der Datenpakete fest, auf die das Gerät die Regel anwendet. Wählen Sie in der Dropdown-Liste einen Eintrag oder legen Sie die Zieladresse fest. Sie legen den Asset-Namen im Dialog fest.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die Regel auf Datenpakete mit beliebigem Asset-Namen oder beliebiger Zieladresse an.

Gültige IPv4-Adresse

Das Gerät wendet die Regel auf Datenpakete mit der festgelegten Zieladresse an.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Das Gerät wendet die Regel auf Datenpakete mit der festgelegten Zieladresse im festgelegten Subnetz an.

Beispiel:

Ein der IP-Adresse vorangestelltes Ausrufezeichen () verkehrt den Ausdruck ins Gegenteil.

Das Gerät wendet die Regel auf Datenpakete mit beliebiger Zieladresse oder Subnetz an, mit Ausnahme der festgelegten Zieladresse oder des festgelegten Subnetzes.

Beispiel: oder

Name des Assets

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

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:

(Voreinstellung)

Das Gerät wendet die Regel auf jedes Datenpaket an, ohne das Protokoll zu bewerten.

Internet Control Message Protocol (RFC 792)

Internet Group Management Protocol

IP in IP tunneling (RFC 2003)

Transmission Control Protocol (RFC 793)

User Datagram Protocol (RFC 768)

IPsec Encapsulated Security Payload (RFC 2406)

IPsec Authentication Header (RFC 2402)

Internet Control Message Protocol for IPv6 (RFC 4443)

Das Gerät verarbeitet auch benutzerdefinierte Protokolle. Sie legen benutzerdefinierte Protokolle im Dialog fest.

Quelle Port

Legt den L4-Quell-Port der Datenpakete fest, auf die das Gerät die Regel anwendet. Voraussetzung ist, dass in Spalte der Wert oder festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die -Regel auf sämtliche Datenpakete an, ohne den L4-Quell-Port zu bewerten.

Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, die den festgelegten L4-Quell-Port enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Mit einem einzelnen Zahlenwert legen Sie einen Port fest, zum Beispiel .
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel .
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel .
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel .

Das Feld ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel eingeben, verwenden Sie 4 von 15 Zahlenwerten.

Ziel Port

Legt den L4-Ziel-Port der Datenpakete fest, auf die das Gerät die Regel anwendet. Voraussetzung ist, dass in Spalte der Wert oder festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die -Regel auf sämtliche Datenpakete an, ohne den L4-Ziel-Port zu bewerten.

Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, die den festgelegten L4-Ziel-Port enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Mit einem einzelnen Zahlenwert legen Sie einen Port fest, zum Beispiel .
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel .
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel .
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel .

Das Feld ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel eingeben, verwenden Sie 4 von 15 Zahlenwerten.

Parameter

Legt zusätzliche Parameter für diese Regel fest.

Geben Sie Parameter in der folgenden Form an: . Wenn Sie mehrere Parameter eingeben, trennen Sie diese durch ein Komma. Wenn Sie mehrere Werte eingeben, trennen Sie diese durch einen vertikalen Strich.

Einige Parameter sind gültig, wenn Sie ein bestimmtes Protokoll verwenden. Ausnahme: Der Wert gilt unabhängig vom Protokoll. Außerdem haben Sie die Möglichkeit, eine Kombination aus gültigen Regeln und protokollspezifischen Regeln einzugeben.

Mögliche Werte:

(Voreinstellung)

Sie haben keine zusätzlichen Parameter für diese Regel festgelegt.

Diese Regel gilt für Pakete mit der MAC-Quelladresse .

Diese Regel gilt für Pakete mit einem bestimmten ICMP-Typ. Geben Sie genau einen Wert ein (Informationen zur Bedeutung dieser Werte finden Sie in RFC 792).

Diese Regel gilt für Pakete mit einem bestimmten ICMP-Code. Geben Sie genau einen Wert ein (Informationen zur Bedeutung dieser Werte finden Sie in RFC 792).

Wenn dieser Wert ist, gilt diese Regel für fragmentierte Pakete, für die Sie bestimmte Regeln gesetzt haben.

Diese Regel gilt für Pakete, für die Sie bestimmte Flags gesetzt haben.

Diese Regel gilt für Pakete, für die Sie das Flag gesetzt haben.

Diese Regel gilt für Pakete, für die Sie das Flag , oder gesetzt haben.

Diese Regel gilt für Pakete, die von der MAC-Adresse stammen, sich in einer neuen oder zugehörigen Verbindung befinden und für die Sie das Flag gesetzt haben.

Aktion

Legt fest, wie das Gerät die Datenpakete verarbeitet, wenn es die Regel anwendet.

Mögliche Werte:

(Voreinstellung)

Das Gerät akzeptiert die Datenpakete gemäß den Ingress-Regeln. Anschließend wendet das Gerät die Egress-Regeln an, bevor der Port die Datenpakete sendet.

Das Gerät verwirft das Datenpaket, ohne den Absender zu informieren.

Das Gerät verwirft das Datenpaket und informiert den Absender.

Das Gerät wendet die in Spalte festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten , und ein anderer Wert als festgelegt ist.

Der Wert ist ausschließlich im Software-Level IN/SU/UN verfügbar. Siehe Merkmalswert Software level im Produktcode.

Das Gerät wendet die in Spalte festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten , und ein anderer Wert als festgelegt ist. Der Wert ist ausschließlich im Software-Level IN/UN verfügbar. Siehe Merkmalswert Software level im Produktcode.

Das Gerät wendet die in Spalte festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten , und ein anderer Wert als festgelegt ist. Der Wert ist ausschließlich im Software-Level SU/UN verfügbar. Siehe Merkmalswert Software level im Produktcode.

Das Gerät wendet die in Spalte festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten , und ein anderer Wert als festgelegt ist. Der Wert ist ausschließlich im Software-Level SU/UN verfügbar. Siehe Merkmalswert Software level im Produktcode.

Das Gerät wendet die in Spalte festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten , und ein anderer Wert als festgelegt ist. Der Wert ist ausschließlich im Software-Level IN/UN verfügbar. Siehe Merkmalswert Software level im Produktcode.

Log

Aktiviert/deaktiviert die Protokollierung in der Log-Datei.

Mögliche Werte:

Die Protokollierung ist aktiv. Wenn das Gerät die Regel auf ein Datenpaket anwendet, protokolliert das Gerät dies in der Log-Datei. Siehe Dialog (Voreinstellung)
Die Protokollierung ist inaktiv.

Trap

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine -Regel auf ein Datenpaket anwendet.

Mögliche Werte:

Das Senden von SNMP-Traps ist aktiv. Voraussetzung ist, dass im Dialog [Statuskonfiguration > Alarmer \(Traps\)](#) die Funktion eingeschaltet und mindestens ein Trap-Ziel festgelegt ist. Das Gerät sendet einen SNMP-Trap, wenn es die -Regel auf ein Datenpaket anwendet. (Voreinstellung)
Das Senden von SNMP-Traps ist inaktiv.

Index DPI-Profil

Zeigt an, welche Regel das Gerät auf die Datenpakete anwendet.

Voraussetzung ist, dass in Spalte einer der folgenden Werte festgelegt ist:

-
-
-
-
-

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet keine Regel auf die Datenpakete an.

Das Gerät wendet die Regel mit der festgelegten Index-Nummer auf die Datenpakete an.

Aktiv

Aktiviert/deaktiviert die Regel.

Um die Einstellungen auf den Datenstrom anzuwenden, führen Sie die folgenden Schritte aus:

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

Öffnen Sie den Dialog oder den Dialog .

Klicken Sie die Schaltfläche .

Mögliche Werte:

Die Regel ist aktiv.

(Voreinstellung)

Die Regel ist inaktiv.

4.5.1.4 Paketfilter Zuweisung

[Netzsicherheit > Paketfilter > Routed-Firewall-Modus > Zuweisung]

Dieser Dialog ermöglicht Ihnen, den Router-Interfaces des Geräts eine oder mehrere Regeln zuzuweisen. Router-Interfaces richten Sie ein im Dialog

Information

Zuweisungen


Zeigt, wie viele Regeln für die Ports aktiv sind.

Nicht angewendete Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten Regeln von den im Gerät gespeicherten Regeln unterscheiden.

Mögliche Werte:

Mindestens eine der im Gerät gespeicherten Regeln enthält geänderte Einstellungen.

Wenn Sie die Schaltfläche  klicken, wendet das Gerät die Regeln auf den Datenstrom an.

Das Gerät wendet die gespeicherten Regeln auf den Datenstrom an.

Tabelle

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

Schaltflächen



Hinzufügen

Öffnet das Fenster, um einem Router-Interface eine Regel zuzuweisen.

- In der Dropdown-Liste wählen Sie die Regel, die Sie dem Router-Interface zuweisen.
- In der Dropdown-Liste wählen Sie aus, ob das Gerät die Regel auf empfangene Datenpakete, auf zu sendende Datenpakete oder auf beide anwendet.
- In der Dropdown-Liste wählen Sie das Router-Interface, auf welches das Gerät die Regel anwendet.



Löschen

Entfernt die ausgewählte Tabellenzeile.



Änderungen anwenden

Wendet die im Gerät gespeicherten Regeln auf den Datenstrom an.

Das Gerät entfernt dabei auch die Zustandsinformationen des Paketfilters. Dies beinhaltet eventuell vorhandene DCE RPC-Informationen der Funktion `show ip firewall`. Das Gerät unterbricht hierbei offene Kommunikationsverbindungen.

Anmerkung: Während das Gerät die gespeicherten Regeln aktiviert, können Sie keine neuen Kommunikationsverbindungen herstellen.

Beschreibung

Zeigt den Namen der Regel. Die Beschreibung legen Sie fest im Dialog [Routed-Firewall-Modus > Regel](#).

Regel-Index

Zeigt die fortlaufende Nummer der `rule`-Regel. Sie legen den Regel-Index fest, wenn Sie eine Tabellenzeile hinzuzufügen.

Interface

Zeigt die Nummer des Router-Interfaces, auf welchem das Gerät die Regel anwendet. Sie legen die Nummer des Interfaces fest, wenn Sie eine Tabellenzeile hinzuzufügen.

Richtung

Zeigt, ob das Gerät die `rule`-Regel auf empfangene Datenpakete, auf zu sendende Datenpakete oder auf beide anwendet.

Mögliche Werte:

Das Gerät wendet die `rule`-Regel auf Datenpakete an, die es auf dem Router-Interface empfängt.

Das Gerät wendet die `rule`-Regel auf Datenpakete an, die es auf dem Router-Interface sendet.

Das Gerät wendet die `rule`-Regel auf Datenpakete an, die es auf dem Router-Interface sendet und empfängt.

Priorität

Legt die Priorität der `rule`-Regel fest.

Anhand der Priorität legen Sie die Reihenfolge fest, in welcher das Gerät die Regeln auf den Datenstrom anwendet. Das Gerät wendet die Regeln beginnend mit Priorität `1` in aufsteigender Reihenfolge an.


Mögliche Werte:


(Voreinstellung:)


Aktiv

Aktiviert/deaktiviert die Regel.

Um die Einstellungen auf den Datenstrom anzuwenden, führen Sie die folgenden Schritte aus:

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

Öffnen Sie den Dialog  oder den Dialog 

Klicken Sie die Schaltfläche  .

Mögliche Werte:

Die Regel ist aktiv.

(Voreinstellung)

Die Regel ist inaktiv.

4.5.1.5 Paketfilter Übersicht

[Netzsicherheit > Paketfilter > Routed-Firewall-Modus > Übersicht]

Dieser Dialog bietet Ihnen eine Übersicht über die definierten -Regeln.

Tabelle

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

Beschreibung

Zeigt den Namen der Regel. Die Beschreibung legen Sie fest im Dialog [Routed-Firewall-Modus > Regel](#).

Regel-Index

Zeigt die fortlaufende Nummer der -Regel.

Interface

Zeigt die Nummer des Router-Interfaces, auf welchem das Gerät die Regel anwendet.

Richtung

Zeigt, ob das Gerät die -Regel auf empfangene Datenpakete, auf zu sendende Datenpakete oder auf beide anwendet.

Mögliche Werte:

Das Gerät wendet die -Regel auf Datenpakete an, die es auf dem Router-Interface empfängt.

Das Gerät wendet die -Regel auf Datenpakete an, die es auf dem Router-Interface sendet.

Das Gerät wendet die -Regel auf Datenpakete an, die es auf dem Router-Interface sendet und empfängt.

Priorität

Zeigt die Priorität der -Regel. Das Gerät wendet die Regeln beginnend mit Priorität in aufsteigender Reihenfolge an.

Quelle Adresse

Zeigt den Asset-Namen oder die Quelladresse der Datenpakete, auf die das Gerät die Regel anwendet.

Quelle Port

Zeigt den Quell-TCP-Port oder Quell-UDP-Port der Datenpakete, auf die das Gerät die Regel anwendet.

Ziel Adresse

Zeigt den Asset-Namen oder die Zieladresse der Datenpakete, auf die das Gerät die Regel anwendet.

Ziel Port

Zeigt den Ziel-TCP-Port oder Ziel-UDP-Port der Datenpakete, auf die das Gerät die Regel anwendet.

Protokoll

Zeigt das IP-Protokoll, auf das die -Regel beschränkt ist. Das Gerät wendet die Regel ausschließlich auf Datenpakete mit dem festgelegten IP-Protokoll an.

Parameter

Zeigt zusätzliche Parameter für diese Regel.

Aktion

Zeigt, wie das Gerät die Datenpakete verarbeitet, wenn es die Regel anwendet.

Index DPI-Profil

Zeigt den Profil-Index der Funktion DPI-Enforcer. Den Profil-Index legen Sie im Dialog fest.

Log

Zeigt, ob das Gerät in der Log-Datei protokolliert, wenn es die Regel auf ein Datenpaket anwendet.

Trap

Zeigt, ob das Gerät einen SNMP-Trap sendet, wenn es die Regel auf ein Datenpaket anwendet.

4.5.2 Transparent-Firewall-Modus

[Netzsicherheit > Paketfilter > Transparent-Firewall-Modus]

In diesem Menü legen Sie die Einstellungen für den -Paketfilter fest. Der -Paketfilter enthält Regeln, die das Gerät nacheinander auf den Datenstrom auf seinen nicht-routenden Ports oder VLAN-Interfaces anwendet. Der -Paketfilter wertet jedes Datenpaket, das die Firewall durchläuft, anhand des Zustands der Verbindung wie unten beschrieben aus:

- Für IPv4 ist die Auswertung stateful.
- Für andere Protokolle auf Schicht 2 und Schicht 3 ist die Auswertung stateless

Das Gerät filtert gezielt die unerwünschten Datenpakete heraus, solange die Verbindung unbekannt ist.

- 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.
- Wenn keine Regel zutrifft, wendet das Gerät die Standard-Regel an. In der Voreinstellung hat die Standard-Regel den Wert `Deny`. Das Gerät ermöglicht Ihnen, die Standard-Regel im Dialog `Standard-Regel` zu ändern.

Das Gerät bietet Ihnen ein mehrstufiges Konzept für das Einrichten und Anwenden der Regeln:

- Eine Regel hinzufügen.
- Die Regel einem nicht-routenden Port oder VLAN zuweisen.
Bis zu diesem Schritt haben Änderungen keine Auswirkung auf das Verhalten des Geräts und auf den Datenstrom.
- Die Regel auf den Datenstrom anwenden.

Das Gerät verarbeitet Datenpakete in der folgenden Reihenfolge:

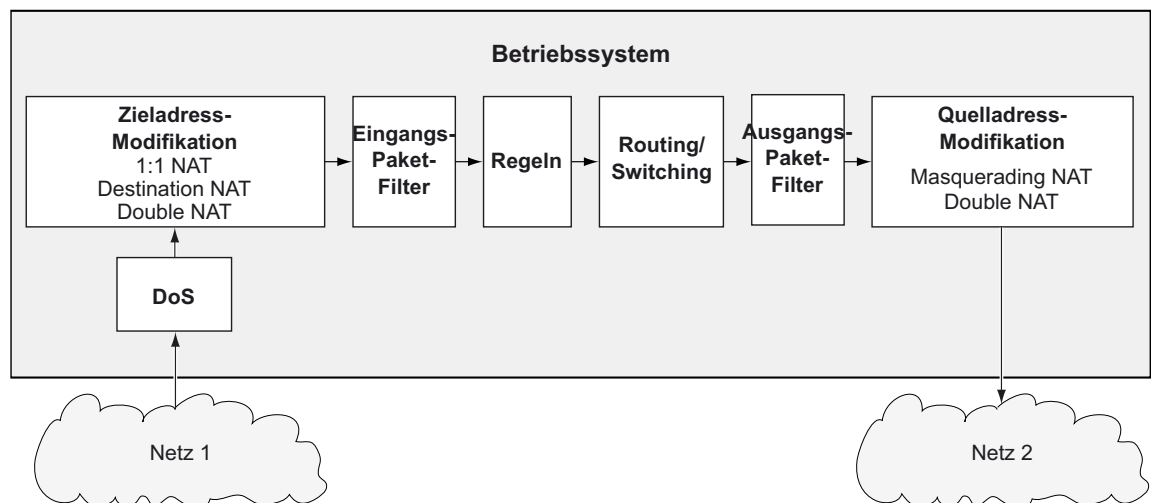


Abb. 2: Bearbeitungsreihenfolge der Datenpakete im Gerät

Das Menü enthält die folgenden Dialoge:

- [Paketfilter Global](#)
- [Paketfilter Regel](#)
- [Paketfilter Zuweisung](#)
- [Paketfilter Übersicht](#)

4.5.21 Paketfilter Global

[Netzicherheit > Paketfilter > Transparent-Firewall-Modus > Global]

In diesem Dialog legen Sie die globalen Einstellungen für den

-Paketfilter

fest.

Konfiguration

Schaltflächen

 Änderungen anwenden

Wendet die im Gerät gespeicherten Regeln auf den Datenstrom an.

Anmerkung: Während das Gerät die gespeicherten Regeln aktiviert, können Sie keine neuen Kommunikationsverbindungen herstellen.

L2-Firewall Erlaubte Regeln (max.)

Zeigt die maximale Anzahl erlaubter Firewall-Regeln für Datenpakete.

Default-Policy

Legt fest, wie die Firewall Datenpakete verarbeitet, wenn keine Regel zutrifft.

Mögliche Werte:

(Voreinstellung)

Das Gerät akzeptiert die Datenpakete.

Das Gerät verwirft die Datenpakete.

Beachten Sie, wenn Sie im weiteren Verlauf einem Port oder VLAN-Interface eine Regel zuweisen: Unabhängig vom Typ des Datenpakets akzeptiert das Gerät grundsätzlich ARP-Pakete.

FCS validieren

Legt fest, ob die Firewall die Frame Check Sequence der Datenpakete auswertet.

Mögliche Werte:

(Voreinstellung)

Das Gerät wertet die Frame Check Sequence im Datenpaket aus. Wenn der Wert ungültig ist, dann verwirft das Gerät das Datenpaket.

Das Gerät ignoriert die Frame Check Sequence. Das Gerät leitet das Datenpaket weiter, auch dann, wenn der Wert ungültig ist.


Information

Nicht angewendete Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten -Regeln von den im Gerät gespeicherten -Regeln unterscheiden.

Mögliche Werte:

Mindestens eine der im Gerät gespeicherten -Regeln enthält geänderte Einstellungen.

Wenn Sie die Schaltfläche  klicken, wendet das Gerät die -Regeln auf den Datenstrom an.

Das Gerät wendet die gespeicherten -Regeln auf den Datenstrom an.

4.5.2.2 Paketfilter Regel

[Netzsicherheit > Paketfilter > Transparent-Firewall-Modus > Regel]

Dieser Dialog ermöglicht Ihnen, Regeln für den Paketfilter einzurichten. Die hier festgelegten Regeln weisen Sie im Dialog den gewünschten nicht-routenden Ports oder VLANs zuweisen.

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 fortlaufende Nummer der -Regel. Das Gerät weist den Wert automatisch zu, wenn Sie eine Tabellenzeile hinzufügen.

Beschreibung

Legt einen Namen für die Regel fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen

Aktion

Legt fest, wie das Gerät die Datenpakete verarbeitet, wenn es die Regel anwendet.

Mögliche Werte:

(Voreinstellung)

Das Gerät akzeptiert die Datenpakete gemäß den Ingress-Regeln. Anschließend wendet das Gerät die Egress-Regeln an, bevor der Port die Datenpakete sendet.

Das Gerät verwirft das Datenpaket, ohne den Absender zu informieren.

Das Gerät wendet die in Spalte festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten , und ein anderer Wert als festgelegt ist.

Der Wert ist ausschließlich im Software-Level IN/SU/UN verfügbar. Siehe Merkmalswert Software level im Produktcode.

Das Gerät wendet die in Spalte festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten , und ein anderer Wert als festgelegt ist. Der Wert ist ausschließlich im Software-Level IN/UN verfügbar. Siehe Merkmalswert Software level im Produktcode.

Das Gerät wendet die in Spalte festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten , und ein anderer Wert als festgelegt ist. Der Wert ist ausschließlich im Software-Level SU/UN verfügbar. Siehe Merkmalswert Software level im Produktcode.

Das Gerät wendet die in Spalte festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten , und ein anderer Wert als festgelegt ist. Der Wert ist ausschließlich im Software-Level SU/UN verfügbar. Siehe Merkmalswert Software level im Produktcode.

Das Gerät wendet die in Spalte festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten , und ein anderer Wert als festgelegt ist. Der Wert ist ausschließlich im Software-Level IN/UN verfügbar. Siehe Merkmalswert Software level im Produktcode.

Das Gerät wendet die in Spalte festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten , und ein anderer Wert als festgelegt ist. Der Wert ist ausschließlich im Software-Level IN/UN verfügbar. Siehe Merkmalswert Software level im Produktcode.

Quelle MAC-Adresse

Legt den Asset-Namen oder die Quelladresse der MAC-Datenpakete fest, auf die das Gerät die Regel anwendet. Wählen Sie in der Dropdown-Liste einen Eintrag oder legen Sie die Quelladresse fest. Sie legen den Asset-Namen im Dialog fest.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die Regel auf MAC-Datenpakete mit beliebigem Asset-Namen oder beliebiger Quelladresse an.

Gültige MAC-Adresse

Das Gerät wendet die Regel auf MAC-Datenpakete mit der festgelegten Quelladresse an.

Beispiel:

Name des Assets

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

Ziel MAC-Adresse

Legt den Asset-Namen oder die Zieladresse der MAC-Datenpakete fest, auf die das Gerät die Regel anwendet. Wählen Sie in der Dropdown-Liste einen Eintrag oder legen Sie die Zieladresse fest. Sie legen den Asset-Namen im Dialog fest.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die Regel auf MAC-Datenpakete mit beliebigem Asset-Namen oder beliebiger Zieladresse an.

Gültige MAC-Adresse

Das Gerät wendet die Regel auf MAC-Datenpakete mit der festgelegten Zieladresse an.

Beispiel:

Name des Assets

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

Ethertype

Legt das Ether-type-Schlüsselwort der MAC-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet den in Spalte festgelegten Wert an.

Benutzerspezifischer Ether-type-Wert

Legt den Ether-type-Wert der MAC-Datenpakete fest, auf die das Gerät die Regel anwendet. Voraussetzung ist, dass in Spalte der Wert festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die Regel auf jedes MAC-Datenpaket an, ohne den Ether-type-Wert zu bewerten.

Das Gerät wendet die Regel auf Logical-Link-Control-Datenpakete (LLC) an, deren Längenfeld den festgelegten Wert enthält. Diese Werte sind ausschließlich für Port-basierte Regeln verfügbar.

Das Gerät wendet die Regel ausschließlich auf MAC-Datenpakete an, welche den hier festgelegten Ethertype-Wert enthalten.

VLAN-ID

Legt die VLAN-ID der Datenpakete fest, auf die das Gerät die Regel anwendet. Voraussetzung ist, dass in Spalte der Wert festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die Regel auf jedes Datenpaket an, ohne die VLAN-ID zu bewerten.

Das Gerät wendet die Regel ausschließlich auf Datenpakete an, welche die festgelegte VLAN-ID enthalten.

Quelle IP-Adresse

Legt den Asset-Namen oder die Quelladresse der IP-Datenpakete fest, auf die das Gerät die Regel anwendet. Wählen Sie in der Dropdown-Liste einen Eintrag oder legen Sie die Quelladresse fest. Sie legen den Asset-Namen im Dialog fest. Voraussetzung ist, dass in Spalte der Wert festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die Regel auf IP-Datenpakete mit beliebigem Asset-Namen oder beliebiger Quelladresse an.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Das Gerät wendet die Regel auf Datenpakete mit der festgelegten Quelladresse im festgelegten Subnetz an.

Beispiel:

Ein der IP-Adresse vorangestelltes Ausrufezeichen (!) verkehrt den Ausdruck ins Gegenteil.

Das Gerät wendet die Regel auf Datenpakete mit beliebiger Quelladresse oder Subnetz an, mit Ausnahme der festgelegten Quelladresse oder des festgelegten Subnetzes.

Beispiel: oder

Name des Assets

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

Ziel IP-Adresse

Legt den Asset-Namen oder die Zieladresse der IP-Datenpakete fest, auf die das Gerät die Regel anwendet. Wählen Sie in der Dropdown-Liste einen Eintrag oder legen Sie die Zieladresse fest. Sie legen den Asset-Namen im Dialog fest. Voraussetzung ist, dass in Spalte der Wert festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die Regel auf IP-Datenpakete mit beliebigem Asset-Namen oder beliebiger Zieladresse an.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Das Gerät wendet die Regel auf Datenpakete mit der festgelegten Zieladresse im festgelegten Subnetz an.

Beispiel:

Ein der IP-Adresse vorangestelltes Ausrufezeichen (`!`) verkehrt den Ausdruck ins Gegenteil. Das Gerät wendet die Regel auf Datenpakete mit beliebiger Zieladresse oder Subnetz an, mit Ausnahme der festgelegten Zieladresse oder des festgelegten Subnetzes.

Beispiel: `!` oder

Name des Assets

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

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:

(Voreinstellung)

Das Gerät wendet die Regel auf jedes Datenpaket an, ohne das Protokoll zu bewerten.

Internet Control Message Protocol (RFC 792)

Internet Group Management Protocol

IP in IP tunneling (RFC 2003)

Transmission Control Protocol (RFC 793)

User Datagram Protocol (RFC 768)

IPsec Encapsulated Security Payload (RFC 2406)

IPsec Authentication Header (RFC 2402)

Internet Control Message Protocol for IPv6

Das Gerät verarbeitet auch benutzerdefinierte Protokolle. Sie legen benutzerdefinierte Protokolle im Dialog `Protocol` fest.

TOS-Priorität

Legt den Wert für IP Precedence (ToS) im Header der IP-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die Regel auf jedes IP-Datenpaket an, ohne den ToS-Wert zu bewerten.

Das Gerät wendet die Regel ausschließlich auf IP-Datenpakete an, die den festgelegten ToS-Wert enthalten.

Index DPI-Profil

Zeigt an, welche Regel das Gerät auf die Datenpakete anwendet.

Voraussetzung ist, dass in Spalte einer der folgenden Werte festgelegt ist:

-
-
-
-
-
-

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet keine Regel auf die Datenpakete an.

Das Gerät wendet die Regel mit der festgelegten Index-Nummer auf die Datenpakete an.

Quelle Port

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

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die Regel auf sämtliche Datenpakete an, ohne den Quell-Port zu bewerten.

Das Gerät wendet die Regel ausschließlich auf Datenpakete an, die den festgelegten Quell-Port enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Mit einem einzelnen Zahlenwert legen Sie einen Port fest, zum Beispiel .
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel .
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel .
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel .

Die Spalte ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel eingeben, verwenden Sie 4 von 15 Zahlenwerten.

Ziel Port

Legt den Ziel-Port der Datenpakete fest, auf die das Gerät die Regel anwendet. Voraussetzung ist, dass in Spalte der Wert oder festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die Regel auf sämtliche Datenpakete an, ohne den Ziel-Port zu bewerten.

Das Gerät wendet die Regel ausschließlich auf Datenpakete an, die den festgelegten Ziel-Port enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Mit einem einzelnen Zahlenwert legen Sie einen Port fest, zum Beispiel .
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel .
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel .
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel .

Die Spalte ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel eingeben, verwenden Sie 4 von 15 Zahlenwerten.

Lastbegrenzung

Legt eine Begrenzung der Datenrate für den nicht-routenden Port oder das VLAN fest. Die Begrenzung gilt für gesendete und empfangene Datenpakete zusammen.

Mögliche Werte:

(Voreinstellung)

Keine Begrenzung der Datentransferrate.

Wenn die Datentransferrate auf dem Port den festgelegten Wert überschreitet, verwirft das Gerät überschüssige IP-Datenpakete. Voraussetzung ist, dass in Spalte ein Wert > festgelegt ist. Die Maßeinheit des Limits legen Sie fest in Spalte .

Burst-Size

Legt das Limit in KByte fest für das Datenvolumen während temporärer Bursts.

Mögliche Werte:

(Voreinstellung)

Keine Begrenzung des Datenvolumens.

Wenn das Datenvolumen während temporärer Bursts auf dem Port den festgelegten Wert überschreitet, verwirft das Gerät überschüssige MAC-Datenpakete.

Empfehlung:

- Wenn die Bandbreite bekannt ist:
= Bandbreite × Zugelassene Dauer eines Bursts / 8
- Wenn die Bandbreite unbekannt ist:
= 10 × MTU (Maximum Transmission Unit) des Ports

Einheit

Legt die Maßeinheit fest für die in Spalte festgelegte Datentransferrate.

Mögliche Werte:

(Voreinstellung)

Datenpakete pro Sekunde

kByte pro Sekunde

Trap

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine -Regel auf ein Datenpaket anwendet.

Mögliche Werte:

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

Das Gerät sendet einen SNMP-Trap, wenn es die -Regel auf ein Datenpaket anwendet.

(Voreinstellung)

Das Senden von SNMP-Traps ist inaktiv.

Log

Aktiviert/deaktiviert die Protokollierung in der Log-Datei.

Mögliche Werte:

Die Protokollierung ist aktiv.

Wenn das Gerät die Regel auf ein Datenpaket anwendet, protokolliert das Gerät dies in der Log-Datei. Siehe Dialog


(Voreinstellung)

Die Protokollierung ist inaktiv.

Aktiv

Aktiviert/deaktiviert die Regel.

Um die Einstellungen auf den Datenstrom anzuwenden, führen Sie die folgenden Schritte aus:

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

Öffnen Sie den Dialog oder den Dialog

Klicken Sie die Schaltfläche .

Mögliche Werte:

Die Regel ist aktiv.

(Voreinstellung)

Die Regel ist inaktiv.

4.5.23 Paketfilter Zuweisung

[Netzsicherheit > Paketfilter > Transparent-Firewall-Modus > Zuweisung]

Dieser Dialog ermöglicht Ihnen, den nicht-routenden Ports und VLANs des Geräts eine oder mehrere -Regeln zuzuweisen.

Information

Zuweisungen


Zeigt, wie viele Regeln für die nicht-routenden Ports und VLANs aktiv sind.

Nicht angewendete Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten -Regeln von den im Gerät gespeicherten -Regeln unterscheiden.

Mögliche Werte:

Mindestens eine der im Gerät gespeicherten -Regeln enthält geänderte Einstellungen.

Wenn Sie die Schaltfläche  klicken, wendet das Gerät die -Regeln auf den Datenstrom an.

Das Gerät wendet die gespeicherten -Regeln auf den Datenstrom an.

Tabelle

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

Schaltflächen



Hinzufügen

Öffnet das Fenster , um einem nicht-routenden Port oder VLAN eine Regel zuzuweisen.

- In der Dropdown-Liste wählen Sie den nicht-routenden Port oder das VLAN, auf den/ das das Gerät die Regel anwendet.
- In der Dropdown-Liste wählen Sie aus, ob das Gerät die Regel auf empfangene Datenpakete oder auf zu sendende Datenpakete anwendet.
- In der Dropdown-Liste wählen Sie die Regel aus, die Sie dem nicht-routenden Port oder VLAN zuweisen.



Löschen

Entfernt die ausgewählte Tabellenzeile.



Änderungen anwenden

Wendet die im Gerät gespeicherten Regeln auf den Datenstrom an.

Anmerkung: Während das Gerät die gespeicherten Regeln aktiviert, können Sie keine neuen Kommunikationsverbindungen herstellen.

Beschreibung

Zeigt den Namen der Regel. Die Beschreibung legen Sie fest im Dialog [Transparent-Firewall-Modus > Regel](#).

Index

Zeigt die fortlaufende Nummer der -Regel. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Typ

Zeigt, worauf das Gerät die Regel anwendet.

Mögliche Werte:

Das Gerät wendet die -Regel bereits auf einen nicht-routenden Port an.
Die zugehörige Port-Nummer finden Sie in Spalte .

Das Gerät wendet die -Regel bereits auf ein nicht-routendes VLAN-Interface an.
Die zugehörige VLAN-ID finden Sie in Spalte .

Port/VLAN

Zeigt die Nummer des nicht-routenden Ports oder das VLAN, auf den/das das Gerät die Regel anwendet. Um die Port-Nummer oder VLAN-ID festzulegen, klicken Sie die Schaltfläche .

Mögliche Werte:

Nummer des nicht-routenden Ports.

ID des VLANs.

Richtung

Zeigt, ob das Gerät die -Regel auf empfangene oder zu sendende Datenpakete anwendet.

Mögliche Werte:

Das Gerät wendet die -Regel auf Datenpakete an, die es auf dem nicht-routenden Ports oder VLAN-Interface empfängt.

Das Gerät wendet die -Regel auf Datenpakete an, die es auf dem nicht-routenden Ports oder VLAN-Interface sendet.

Priorität

Legt die Priorität der -Regel fest.

Anhand der Priorität legen Sie die Reihenfolge fest, in welcher das Gerät die Regeln auf den Datenstrom anwendet. Das Gerät wendet die Regeln beginnend mit Priorität in aufsteigender Reihenfolge an.

Mögliche Werte:

(Voreinstellung:)

Aktiv

Aktiviert/deaktiviert die Regel.

Um die Einstellungen auf den Datenstrom anzuwenden, führen Sie die folgenden Schritte aus:

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

Öffnen Sie den Dialog oder den Dialog .

Klicken Sie die Schaltfläche .

Mögliche Werte:

Die Regel ist aktiv.

(Voreinstellung)

Die Regel ist inaktiv.

4.5.24 Paketfilter Übersicht

[Netzsicherheit > Paketfilter > Transparent-Firewall-Modus > Übersicht]

Dieser Dialog bietet Ihnen eine Übersicht über die definierten -Regeln.

Tabelle

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

Beschreibung

Zeigt den Namen der Regel. Die Beschreibung legen Sie fest im Dialog [Transparent-Firewall-Modus > Regel](#).

Index

Zeigt die fortlaufende Nummer der -Regel.

Richtung

Zeigt, ob das Gerät die -Regel auf empfangene oder zu sendende Datenpakete anwendet.

Mögliche Werte:

Das Gerät wendet die -Regel auf Datenpakete an, die es auf dem nicht-routenden Ports oder VLAN-Interface empfängt.

Das Gerät wendet die -Regel auf Datenpakete an, die es auf dem nicht-routenden Ports oder VLAN-Interface sendet.

Priorität

Zeigt die Priorität der -Regel. Das Gerät wendet die Regeln beginnend mit Priorität in aufsteigender Reihenfolge an.

Typ

Zeigt, worauf das Gerät die Regel anwendet.

Port/VLAN

Zeigt die Nummer des nicht-routenden Ports oder das VLAN, auf den/das das Gerät die Regel anwendet.

Quelle MAC-Adresse

Zeigt den Asset-Namen oder die Quelladresse der MAC-Datenpakete, auf die das Gerät die Regel anwendet.

Ziel MAC-Adresse

Zeigt den Asset-Namen oder die Zieladresse der MAC-Datenpakete, auf die das Gerät die Regel anwendet.

Ethertype

Zeigt das Ether-type-Schlüsselwort der MAC-Datenpakete, auf die das Gerät die Regel anwendet.

Benutzerspezifischer Ether-type-Wert

Zeigt den Ether-type-Wert der MAC-Datenpakete, auf die das Gerät die Regel anwendet. Voraussetzung ist, dass in Spalte der Wert festgelegt ist.

Quelle IP-Adresse

Zeigt den Asset-Namen oder die Quelladresse der IP-Datenpakete, auf die das Gerät die Regel anwendet.

Ziel IP-Adresse

Zeigt den Asset-Namen oder die Zieladresse der IP-Datenpakete, auf die das Gerät die Regel anwendet.

Protokoll

Zeigt das IP-Protokoll, auf das die -Regel beschränkt ist. Das Gerät wendet die -Regel ausschließlich auf Datenpakete des festgelegten IP-Protokolls an.

TOS-Priorität

Zeigt den Wert für IP Precedence (ToS) im Header der IP-Datenpakete, auf die das Gerät die Regel anwendet.

Aktion

Zeigt, wie das Gerät die Datenpakete verarbeitet, wenn es die Regel anwendet.

Index DPI-Profil

Zeigt den Profil-Index der Funktion DPI-Enforcer. Den Profil-Index legen Sie im Dialog fest.

Quelle Port

Zeigt den Quell-TCP-Port oder Quell-UDP-Port der Datenpakete, auf die das Gerät die Regel anwendet.

Ziel Port

Zeigt den Ziel-TCP-Port oder Ziel-UDP-Port der Datenpakete, auf die das Gerät die Regel anwendet.

Lastbegrenzung

Zeigt die Begrenzung der Datenrate für den nicht-routenden Port oder das VLAN. Die Begrenzung gilt für gesendete und empfangene Datenpakete zusammen.

Burst-Size

Zeigt das Limit in KByte für das Datenvolumen während temporärer Bursts.

Einheit

Zeigt die Maßeinheit für die in Spalte festgelegte Datentransferrate.

Trap

Zeigt, ob das Gerät einen SNMP-Trap sendet, wenn es die Regel auf ein Datenpaket anwendet.

Log

Zeigt, ob das Gerät in der Log-Datei protokolliert, wenn es die Regel auf ein Datenpaket anwendet.

Aktiv

Zeigt, ob die Regel aktiv oder inaktiv ist.

4.6 Deep Packet Inspection

[Netzsicherheit > DPI]

Die Funktion ermöglicht Ihnen, Datenpakete zu überwachen und zu filtern. Die Funktion unterstützt Sie beim Schutz des Netzes vor unerwünschten Inhalten wie Spam oder Viren.

Die Funktion untersucht Datenpakete auf unerwünschte Merkmale und Protokollverletzungen. Das Protokoll untersucht den Header und den Nutzdateninhalt (Payload) der Datenpakete.

Dieser Dialog ermöglicht Ihnen, die -Einstellungen festzulegen. Das Gerät blockiert Datenpakete, die gegen die festgelegten Profile verstoßen. Im Falle eines erkannten Fehlers beendet das Gerät die Daten-Verbindung auf Anforderung des Benutzers.

- Das Menü enthält die folgenden Dialoge:
- [Deep Packet Inspection - Modbus Enforcer](#)
 - [Deep Packet Inspection - OPC Enforcer](#)
 - [Deep Packet Inspection - DNP3 Enforcer](#)
 - [Deep Packet Inspection - IEC104 Enforcer](#)
 - [Deep Packet Inspection - AMP-Enforcer](#)
 - [Deep Packet Inspection - ENIP Enforcer](#)

4.6.1 Deep Packet Inspection - Modbus Enforcer

[Netzsicherheit > DPI > Modbus Enforcer]

Dieser Dialog ermöglicht Ihnen, die spezifische Profile zu definieren.

-Einstellungen festzulegen und

-

Die Profile spezifizieren Funktionscodes sowie Register- oder Coil-Adressen. Der Funktionscode im Protokoll Modbus TCP legt den Zweck der Datenübertragung fest. Das Gerät blockiert Datenpakete, die gegen die festgelegten Profile verstoßen. Im Falle eines erkannten Fehlers beendet das Gerät die Daten-Verbindung auf Anforderung des Benutzers. Vordefinierte Funktionscode-Listen und der Funktionscode-Generator unterstützen Sie beim Festlegen der -Funktionscodes.

Bei aktiviertem -Profil (Kontrollkästchen in Spalte ist markiert) wendet das Gerät die Profile auf den Datenstrom an.

- Das Gerät lässt ausschließlich Datenpakete zu, welche die in Spalte festgelegten Funktionscodes enthalten.
- Das Gerät weist Datenpakete zurück, die abweichende Function-Codes enthalten, welche nicht in Spalte festgelegt sind.

Information

Nicht angewendete Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten gespeicherten Profilen unterscheiden.

-Profile von den im Gerät

Mögliche Werte:

Mindestens eines der aktiven geänderte Einstellungen.

-Profile, die im Gerät gespeichert sind, enthält

Wenn Sie die Schaltfläche  klicken, wendet das Gerät die festgelegten Profile an.

Die -Profile, die auf den Datenstrom angewendet werden, stimmen mit den Profilen überein, die im Gerät gespeichert sind.


Tabelle


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



Schaltflächen



Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld  legen Sie die Nummer des Profils fest.
Mögliche Werte:

Nach Klicken der Schaltfläche  fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld  festgelegte Nummer zu.



Löschen


Entfernt die ausgewählte Tabellenzeile.


Wenn für das Profil das Kontrollkästchen  markiert ist, hindert das Gerät Sie daran, das Profil zu entfernen.



Kopieren

Öffnet das Fenster , um eine bestehende Tabellenzeile zu kopieren. Voraussetzung ist, dass die Tabellenzeile für das zu kopierende Profil ausgewählt ist.




- Im Feld  legen Sie eine neue Nummer fest, die das kopierte Profil identifiziert.
Mögliche Werte:

Das Gerät fügt die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld  festgelegte Nummer zu.



Änderungen anwenden

Das Gerät wendet die festgelegten Profile auf den Datenstrom an.

Wenn Sie den Wert im Feld  geändert haben, wendet das Gerät die Änderung auf die -Liste an und aktualisiert die Anzeige in Spalte .

Index

Zeigt die fortlaufende Nummer des Profils, auf das sich die Tabellenzeile bezieht. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Beschreibung

Legt einen Namen für das Profil fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen
(Voreinstellung: )

Funktionstyp

Legt den Funktionstyp für das -Profil fest. Nach dem Klicken der Schaltfläche weist das Gerät die zugehörigen Typ-IDs zu.

Mögliche Werte:

(Voreinstellung)
Weist die Funktionscodes für die read-Funktion des Protokolls zu.

Weist die Funktionscodes für die read/write-Funktionen des Protokolls zu.

Weist die Funktionscodes für die programming-Funktionen des Protokolls zu.

Weist die Funktionscodes für jede Funktion des Protokolls zu.

Ermöglicht Ihnen, in Spalte benutzerdefinierte Werte festzulegen.

Anmerkung: Wenn Sie den Wert festgelegt haben, lässt das Gerät zu Ihrer eigenen Sicherheit keine nachträglichen Änderungen dieses Wertes mehr zu. Das Gerät sorgt dafür, das Umstellen auf , oder zu verhindern. Dies vermeidet ein versehentliches Überschreiben der in Spalte manuell festgelegten Werte. Um eine Tabellenzeile mit dem Wert , oder festzulegen, fügen Sie eine Tabellenzeile hinzu.

Funktionscode

Zeigt die Funktionscodes für das -Profil. Das Gerät lässt Datenpakete mit den festgelegten Eigenschaften zu.

Die Spalte zeigt unterschiedliche Werte, abhängig von dem in Spalte festgelegten Wert:

Wenn in Spalte der Wert , oder festgelegt ist, dann fügt das Gerät automatisch die zugehörigen Funktionscodes ein.

Wenn in Spalte der Wert festgelegt ist, dann ermöglicht Ihnen das Gerät, benutzerdefinierte Funktionscodes festzulegen. Führen Sie dazu die folgenden Schritte aus:

Klicken Sie für das betreffende Profil in die Spalte .

Der Dialog zeigt das Fenster . Siehe „[Funktionscode]“ auf Seite 157.

Wählen Sie in der Dropdown-Liste den gewünschten Funktionscode-Eintrag.

Klicken Sie die Schaltfläche .

Um mehrere Funktionscodes hinzuzufügen, wiederholen Sie die zuvor beschriebenen Schritte.

Klicken Sie die Schaltfläche .

Mögliche Werte:

- <
Das Gerät ermöglicht Ihnen, mehrere Funktionscodes und für manche Funktionscodes einen zusätzlichen Adressbereich festzulegen. Die Bedeutung der Nummern finden Sie im Abschnitt „Bedeutung der Funktionscode-Werte“ auf Seite 158.
- =
Sie trennen jeden Funktionscode jeweils durch ein Komma, zum Beispiel .
Für manche Funktionscodes ermöglicht Ihnen das Gerät, zusätzlich einen Adressbereich festzulegen. Sie trennen den Adressbereich vom Funktionscode mit einem senkrechten Strich (Pipe), zum Beispiel .
- = oder (für Funktionscodes, die Lese- und Schreib-Adressbereiche erfordern)
Sie verbinden den Start- und Endwert des Bereichs mit einem Bindestrich, zum Beispiel .
- .
Das Gerät bietet Ihnen auch die Möglichkeit, einen einzelnen Wert als Adressbereich angeben. Zum Beispiel ist das Festlegen des Adressbereichs gleichbedeutend mit der einzelnen Adresse .

Kennung der Unit

Legt die -Identifikationseinheit für das -Profil fest.

Mögliche Werte:

- (Voreinstellung)
Das Gerät lässt Datenpakete ohne Identifikationseinheit zu.
- Das Gerät lässt Datenpakete mit der festgelegten Identifikationseinheit zu.
Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:
 - Eine einzelne -Identifikationseinheit mit einem einzelnen numerischen Wert, zum Beispiel .
 - Mehrere -Identifikationseinheiten mit numerischen Werten, die durch ein Komma getrennt sind, zum Beispiel .

Plausibilitätsprüfung

Aktiviert/deaktiviert die Plausibilitätsprüfung für Datenpakete.

Mögliche Werte:

- (Voreinstellung)
Die Plausibilitätsprüfung ist aktiv.
Das Gerät prüft die Plausibilität der Datenpakete hinsichtlich Format und Spezifikation.
- Die Plausibilitätsprüfung ist inaktiv.

Ausnahme

Aktiviert/deaktiviert das Senden einer Exception-Antwort im Falle einer Protokollverletzung oder wenn die Plausibilitätsprüfung Fehler erkennt.

Mögliche Werte:

- Das Senden einer Exception-Antwort ist aktiv.
Wenn das Gerät eine Protokollverletzung oder Fehler bei der Plausibilitätsprüfung ermittelt, sendet es eine Exception-Antwort an die Endpunkte und beendet die -Verbindung.
- (Voreinstellung)
Das Senden einer Exception-Antwort ist inaktiv. Die -Verbindung bleibt aufgebaut.

TCP-Reset

Aktiviert/deaktiviert das Zurücksetzen der TCP-Verbindung im Falle einer Protokollverletzung oder wenn die Plausibilitätsprüfung einen Fehler erkennt.

Mögliche Werte:

(Voreinstellung)

Das Zurücksetzen der TCP-Verbindung ist aktiv.

Wenn das Gerät eine Protokollverletzung oder einen Fehler bei der Plausibilitätsprüfung erkennt, beendet es die TCP-Verbindung.

Das Zurücksetzen der TCP-Verbindung ist inaktiv. Die TCP-Verbindung bleibt aufgebaut.

Profil aktiv

Aktiviert/deaktiviert das Profil.

Mögliche Werte:

Das Profil ist aktiv.

Das Gerät wendet die in dieser Tabellenzeile festgelegten

-Profile auf die Daten-

pakete an.

(Voreinstellung)

Das Profil ist inaktiv.

[Funktionscode]

Funktionscode

Legt die Funktionscodes für das betreffende -Profil fest.

Die Bedeutung der Nummern finden Sie im Abschnitt „[Bedeutung der Funktionscode-Werte](#)“ auf [Seite 158](#).

Adressbereich Lesen

Legt den Lese-Adressbereich für bestimmte Funktionscodes fest. Siehe Abschnitt „[Bedeutung der Funktionscode-Werte](#)“ auf [Seite 158](#).

Mögliche Werte:

Adressbereich Schreiben

Legt den Schreib-Adressbereich für bestimmte Funktionscodes fest. Siehe Abschnitt „[Bedeutung der Funktionscode-Werte](#)“ auf [Seite 158](#).

Mögliche Werte:

Hinzufügen

Fügt die in der Dropdown-Liste ausgewählten Einträge in das Feld ein.



Entfernt den Eintrag aus dem Feld .

Bedeutung der Funktionscode-Werte

Bedeutung	Adressbereich (Lesen)	Adressbereich (Schreiben)

4.6.2 Deep Packet Inspection - OPC Enforcer

[Netzsicherheit > DPI > OPC Enforcer]

Dieser Dialog ermöglicht Ihnen, die - (OLE for Process Control Enforcer)-Einstellungen festzulegen und -spezifische Profile zu definieren.

OPC ist ein Integrationsprotokoll für industrielle Umgebungen. ist eine Funktion zur Unterstützung der Netzsicherheit. Das Gerät blockiert Datenpakete, die gegen die festgelegten Profile verstoßen. Auf Wunsch prüft das Gerät Datenpakete auf Plausibilität und Fragment-Eigenschaften. Das Gerät prüft und beobachtet OPC-Datenverbindungen und unterstützt beim Schutz gegen ungültige oder gefälschte Datenpakete. Die Funktion aktiviert TCP-Ports pro Datenverbindung dynamisch. Auf Anforderung eines OPC-Servers baut das Gerät die Datenverbindung ausschließlich zwischen dem OPC-Server und dem zugehörigen OPC-Client auf.

Voraussetzung ist, dass in Ihrem Endgerät der Authentication Level 5 oder niedriger eingerichtet ist, um die Deep Packet Inspection (DPI) durchzuführen. Das Endgerät kann ein Computer oder ein anderes Gerät sein, das in der Lage ist, OPC-Datenpakete zu senden. Authentication Level definiert die Art der Authentifizierung, die erforderlich ist, damit ein OPC-Client eine Verbindung zu einem OPC-Server herstellen kann.

Bei folgenden Ereignissen entfernt das Gerät die Zustandsinformationen aus dem Paketfilter:

- Beim Anwenden der im Gerät gespeicherten Profile auf den Datenstrom.
- Beim Aktivieren/Deaktivieren der Funktion auf dem Router-Interface.

Dies beinhaltet eventuell vorhandene DCE RPC-Informationen des s. Das Gerät unterbricht hierbei offene Kommunikationsverbindungen.

Funktion

Nicht angewendete Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten -Profile von den im Gerät gespeicherten Profilen unterscheiden. Wenn Sie die Schaltfläche klicken, wendet das Gerät die festgelegten Profile an.

Mögliche Werte:

Mindestens eines der aktiven -Profile, die im Gerät gespeichert sind, enthält geänderte Einstellungen.

Die -Profile, die auf den Datenstrom angewendet werden, stimmen mit den Profilen überein, die im Gerät gespeichert sind.


Tabelle


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



Schaltflächen



Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld  legen Sie die Nummer des Profils fest.
Mögliche Werte:

Nach Klicken der Schaltfläche  fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld  festgelegte Nummer zu.




Löschen


Entfernt die ausgewählte Tabellenzeile.


Wenn für das Profil das Kontrollkästchen  markiert ist, hindert das Gerät Sie daran, das Profil zu entfernen.



Kopieren

Öffnet das Fenster , um eine bestehende Tabellenzeile zu kopieren. Voraussetzung ist, dass die Tabellenzeile für das zu kopierende Profil ausgewählt ist.

- Im Feld  legen Sie die Nummer des Profils fest.
Mögliche Werte:

Das Gerät fügt die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld  festgelegte Nummer zu.



Änderungen anwenden

Das Gerät wendet die festgelegten Profile auf den Datenstrom an.


Index

Zeigt die fortlaufende Nummer des Profils, auf das sich die Tabellenzeile bezieht. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Beschreibung

Legt einen Namen für das Profil fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen
(Voreinstellung: )

Plausibilitätsprüfung

Aktiviert/deaktiviert die Plausibilitätsprüfung für Datenpakete.

Mögliche Werte:

(Voreinstellung)

Die Plausibilitätsprüfung ist aktiv.

Das Gerät prüft die Plausibilität der Datenpakete hinsichtlich Format und Spezifikation.

Das Gerät blockiert Datenpakete, die gegen die festgelegten Profile verstoßen.

Die Plausibilitätsprüfung ist inaktiv.

Fragmentprüfung

Aktiviert/deaktiviert die Fragment-Prüfung der Datenpakete.

Mögliche Werte:

(Voreinstellung)

Die Fragment-Prüfung ist aktiv.

Das Gerät prüft die Datenpakete hinsichtlich der Fragment-Eigenschaften.

Die Fragment-Prüfung ist inaktiv.

Timeout bei Verbindung

Legt die Zeit in Sekunden fest, nach der das Gerät die dynamischen TCP-Ports entfernt, wenn über die dynamischen TCP-Ports keine aktive OPC-Datenverbindung mehr besteht.

Mögliche Werte:

(Voreinstellung:)

Der Wert deaktiviert die Funktion. Die OPC-Datenverbindung bleibt ohne Zeitbegrenzung aufgebaut.

Profil aktiv

Aktiviert/deaktiviert das Profil.

Mögliche Werte:

Das Profil ist aktiv.

Das Gerät wendet die in dieser Tabellenzeile festgelegten

-Profile auf die Daten-

pakete an.

Das Profil ist inaktiv.

4.6.3 Deep Packet Inspection - DNP3 Enforcer

[Netzsicherheit > DPI > DNP3 Enforcer]

Dieser Dialog ermöglicht Ihnen, die Einstellungen festzulegen und

- (Distributed Network Protocol v3 Enforcer)-spezifische Profile zu definieren.

Das Protokoll DNP3 ist darauf ausgelegt, eine zuverlässige Kommunikation zwischen den Komponenten in Prozessautomatisierungssystemen zu ermöglichen. Das Protokoll umfasst Multiplexing, Fehlerprüfung, Verbindungssteuerung, Priorisierung und Schicht-2-Adressierungsdienste für die Benutzerdaten. Die Funktion [aktiviert](#) die Firewall-Funktionen der Deep Packet Inspection (DPI) für den DNP3-Datenstrom. Das Gerät blockiert Datenpakete, die gegen die festgelegten Profile verstoßen. Auf Wunsch prüft das Gerät Datenpakete auf Plausibilität und Fragment-Eigenschaften. Das Gerät prüft und überwacht DNP3-Datenverbindungen und unterstützt beim Schutz gegen ungültige oder gefälschte Datenpakete.

Bei aktiviertem [-Profil](#) (Kontrollkästchen in Spalte [ist markiert](#)) wendet das Gerät die Profile auf den Datenstrom an.

- Das Gerät lässt ausschließlich Datenpakete zu, welche die in Spalte [festgelegten Funktionscodes](#) enthalten.
- Das Gerät weist Datenpakete zurück, die abweichende Function-Codes enthalten, welche nicht in Spalte [festgelegt](#) sind.

Das Menü enthält die folgenden Dialoge:

[DNP3-Profil](#)

[DNP3-Objekt](#)

4.6.3.1 DNP3-Profil

[Netzsicherheit > DPI > DNP3 Enforcer > Profil]


Dieser Dialog ermöglicht Ihnen, Profile für die -Funktion anzulegen. Das Profil ermöglicht Ihnen, basierend auf den festgelegten Werten, Datenpakete weiterzuleiten oder zu verwerfen.

Information

Nicht angewendete Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten -Profile von den im Gerät gespeicherten Profilen unterscheiden.

Mögliche Werte:

Mindestens eines der aktiven -Profile, die im Gerät gespeichert sind, enthält geänderte Einstellungen.
Um die noch ausstehenden Profile auf den Datenstrom anzuwenden, klicken Sie die Schaltfläche .

Die -Profile, die auf den Datenstrom angewendet werden, stimmen mit den Profilen überein, die im Gerät gespeichert sind.

Tabelle

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

Schaltflächen

 Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld legen Sie die Nummer des Profils fest.

Mögliche Werte:

Nach Klicken der Schaltfläche fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld festgelegte Nummer zu.

 Löschen

Entfernt die ausgewählte Tabellenzeile.



Öffnet das Fenster , um eine bestehende Tabellenzeile zu kopieren. Voraussetzung ist, dass die Tabellenzeile für das zu kopierende Profil ausgewählt ist.

- Im Feld legen Sie eine neue Nummer fest, die das kopierte Profil identifiziert.
Mögliche Werte:

Das Gerät fügt die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld festgelegte Nummer zu.



Das Gerät wendet die festgelegten Profile auf den Datenstrom an.

Index

Zeigt die fortlaufende Nummer des Profils, auf das sich die Tabellenzeile bezieht. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Beschreibung

Legt einen Namen für das Profil fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen
(Voreinstellung:)

Funktionscode-Liste

Zeigt die Funktionscodes für das -Profil. Das Gerät lässt Datenpakete mit den festgelegten Eigenschaften zu.

Das Gerät ermöglicht Ihnen, mehrere Function-Codes festzulegen. Führen Sie dazu die folgenden Schritte aus:

- Klicken Sie für das betreffende Profil in die Spalte .
- Der Dialog zeigt das Fenster . Siehe „[\[Funktionscode-Liste\]](#)“ auf Seite 166.
- Wählen Sie in der Dropdown-Liste den gewünschten Funktionscode-Eintrag.
- Klicken Sie die Schaltfläche .
- Um mehrere Funktionscodes hinzuzufügen, wiederholen Sie die zuvor beschriebenen Schritte.
- Klicken Sie die Schaltfläche .

Mögliche Werte:

Die Bedeutung der Nummern finden Sie im Abschnitt „[Bedeutung der Funktionscode-Liste-Werte](#)“ auf Seite 166.

Index der Standard-Objektliste

Legt die in der Standard-Objektliste verwenden Index-Nummern fest.

Mögliche Werte:

(Voreinstellung)
Das Gerät wendet das -Profil auf jedes Datenpaket an, unabhängig von der Index-Nummer.

Das Gerät wendet das _____-Profil ausschließlich auf Datenpakete an, welche die festgelegte Index-Nummer enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Eine einzelne Index-Nummer mit einem einzelnen numerischen Wert, zum Beispiel _____.
- Mehrere Index-Nummern mit numerischen Werten, die durch ein Komma getrennt sind, zum Beispiel _____.
- Einen Bereich mit numerischen Werten, welche durch einen Bindestrich verbunden sind, zum Beispiel _____.
- Außerdem können Sie einzelne Zahlenwerte und Bereiche kombinieren, zum Beispiel _____.

Das Gerät wendet die Index-Nummer nicht auf das _____-Profil an.

CRC-Prüfung

Aktiviert/deaktiviert die CRC-Prüfung der Datenpakete, um die Prüfsumme zu validieren, die in den DNP3-Datenpaketen enthalten ist.

Mögliche Werte:

_____ (Voreinstellung)

Die CRC-Prüfung ist aktiv.

Das Gerät berechnet die Prüfsumme und vergleicht diese mit dem Prüfsummenfeld in den DNP3-Datenpaketen.

Die CRC-Prüfung ist inaktiv.

Plausibilitätsprüfung

Aktiviert/deaktiviert die Plausibilitätsprüfung für Datenpakete.

Mögliche Werte:

_____ (Voreinstellung)

Die Plausibilitätsprüfung ist aktiv.

Das Gerät prüft die Plausibilität der Datenpakete hinsichtlich Format und Spezifikation. Das Gerät blockiert Datenpakete, die gegen die festgelegten Profile verstoßen.

Die Plausibilitätsprüfung ist inaktiv.

Verkehr von und zur Outstation prüfen

Aktiviert/deaktiviert die Prüfung von Datenpaketen, die von einer Outstation stammen.

Mögliche Werte:

Die Prüfung der Datenpakete von der Outstation ist aktiv.

Die Prüfung der Datenpakete von der Outstation ist inaktiv.

TCP-Reset

Aktiviert/deaktiviert das Zurücksetzen der TCP-Verbindung im Falle einer Protokollverletzung oder wenn die Plausibilitätsprüfung einen Fehler erkennt.

Mögliche Werte:

(Voreinstellung)

Das Zurücksetzen der TCP-Verbindung ist aktiv.

Wenn das Gerät eine Protokollverletzung oder einen Fehler bei der Plausibilitätsprüfung erkennt, beendet es die TCP-Verbindung.

Das Zurücksetzen der TCP-Verbindung ist inaktiv. Die TCP-Verbindung bleibt aufgebaut.

Profil aktiv

Aktiviert/deaktiviert das Profil.

Mögliche Werte:

Das Profil ist aktiv.

Das Gerät wendet die in dieser Tabellenzeile festgelegten

-Profile auf die Daten-

pakete an.

Das Profil ist inaktiv.

[Funktionscode-Liste]

Funktionscode-Liste

Legt die Funktionscodes für das betreffende -Profil fest.

Die Bedeutung der Nummern finden Sie im Abschnitt „[Bedeutung der Funktionscode-Liste-Werte](#)“ auf Seite 166.

Hinzufügen

Fügt die in der Dropdown-Liste ausgewählten Einträge in das Feld ein.



Entfernt den Eintrag aus dem Feld

Bedeutung der Funktionscode-Liste-Werte

Bedeutung

Bedeutung

4.6.3.2 DNP3-Objekt

[Netzsicherheit > DPI > DNP3 Enforcer > Objekt]

Die Funktion DNP3 verwendet Objekte, um Werte und Informationen zwischen Geräten zu vermitteln. Die Funktion DNP3 verwendet Gruppennummern, um den Datentyp zu kategorisieren, und Variationsnummern, um festzulegen, wie die Daten innerhalb der Gruppe kodiert werden. Jede Instanz eines kodierten Informationselements, das eine eindeutige Gruppe und Variation in der Nachricht definiert, ist ein DNP3-Objekt.

Dieses Fenster ermöglicht Ihnen, benutzerdefinierte DNP3-Objekte hinzuzufügen sowie zuvor hinzugefügte benutzerdefinierte DNP3-Objekte anzusehen. Um zu kontrollieren, ob das hinzugefügte DNP3-Objekt in einer konkreten Request Message/Response Message gültig ist, prüfen Sie die folgenden Parameter:

-
-
-
-
-
-
-

Auf Grundlage der Norm IEEE 1815-2012 lässt die Funktion in der Voreinstellung den Datenstrom zu, der DNP3-Objekte enthält, die in der Standard-Objektliste vorhanden sind.

Tabelle

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

Schaltflächen



Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- In der Dropdown-Liste wählen Sie die Index-Nummer des Profils.
- Im Feld legen Sie die Index-Nummer des Objekts fest.

Mögliche Werte:

- In der Dropdown-Liste wählen Sie den Typ der Nachricht.
- Mögliche Werte:

- Im Feld legen Sie einen Mittelwert für den Klassifizierungstyp oder für die Klassifizierungstypen von Datenpaketen in einer Nachricht fest. Voraussetzung ist, dass im Feld ein gültiger Wert festgelegt ist.

Mögliche Werte:

- Im Feld legen Sie die Variation-Nummer fest. Voraussetzung ist, dass im Feld ein gültiger Wert festgelegt ist.

Mögliche Werte:

- Im `FunctionCode`-Feld legen Sie den Funktionscode fest. Der Funktionscode kennzeichnet den Zweck der Nachricht. Voraussetzung ist, dass im Feld `FunctionCode` ein gültiger Wert festgelegt ist.
Mögliche Werte:

`0` von den Mastern. Legen Sie einen einzelnen Zahlenwert fest, zum Beispiel `1`.

`1` von den Outstations. Legen Sie einen einzelnen Zahlenwert fest, zum Beispiel `1`.

- Im Feld `QualifierCode` legen Sie den Qualifier-Code jeweils ein Paar der Felder `QualifierCodePrefix` und `QualifierCodeArea` fest. Der Qualifier-Code ist ein 8-Bit-Wert, der den Präfix-Code und den Bereichs-Specifier-Code für das Objekt in einer DNP3-Nachricht definiert. Voraussetzung ist, dass im Feld `QualifierCode` ein gültiger Wert festgelegt ist.
Mögliche Werte:

Mit durch Komma getrennten hexadezimalen Werten legen Sie mehrere individuelle Qualifier-Codes für einen Satz der jeweiligen Felder `QualifierCodePrefix`, `QualifierCodeArea` und `QualifierCode` fest.

Nach Klicken der Schaltfläche `Add` fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist dieser Tabellenzeile die in den Feldern `Index`, `ObjectIndex`, `Type`, `GroupNo` und `QualifierCode` festgelegten Werte zu.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

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

Objekt-Index

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

Typ

Legt den Typ der Nachricht fest.

Mögliche Werte:

`0` Erstellt in der Objektliste ein Objekt Request-Nachricht.

`1` Erstellt in der Objektliste ein Objekt Response-Nachricht.

Gruppen-Nr.

Legt einen Mittelwert für den Klassifizierungstyp oder für die Klassifizierungstypen von Datenpaketen in einer Nachricht fest. Voraussetzung ist, dass im Feld `GroupNo` ein gültiger Wert festgelegt ist.

Mögliche Werte:

Jede Gruppennummer verwendet einen gemeinsamen Point Type und eine Methode zur Erstellung. Der Point Type definiert das Gerät in einer Outstation.

Variation

Legt die Variation-Nummer fest. Voraussetzung ist, dass im Feld ein gültiger Wert festgelegt ist. Das Gerät wendet das -Profil ausschließlich auf Datenpakete an, die den festgelegten Wert enthalten.

Die Funktion DNP3 ermöglicht die Auswahl von Kodierungsformaten für den als Variation-Nummer bekannten Typ von Datenpaketen. Jeder Wert im Feld verfügt über eine Folge von Variation-Nummern.

Mögliche Werte:

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Mit einem einzelnen Zahlenwert legen Sie eine einzelne Variation-Nummer fest, zum Beispiel .
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Bereich fest, zum Beispiel .

Funktion

Der Funktionscode kennzeichnet den Zweck der Nachricht. Voraussetzung ist, dass im Feld ein gültiger Wert festgelegt ist. Das Gerät wendet das -Profil ausschließlich auf Datenpakete an, die den festgelegten Wert enthalten.

Mögliche Werte:

von den Mastern. Legen Sie einen einzelnen Zahlenwert fest, zum Beispiel .

von den Outstations. Legen Sie einen einzelnen Zahlenwert fest, zum Beispiel .

Qualifier

Legt den Qualifier-Code für ein Paar der Felder , und fest. Der Qualifier-Code ist ein 8-Bit-Wert, der den Präfix-Code und den Bereichs-Specifier-Code für das Objekt in einer DNP3-Nachricht definiert. Voraussetzung ist, dass im Feld ein gültiger Wert festgelegt ist. Das Gerät wendet das -Profil ausschließlich auf Datenpakete an, die den festgelegten Wert enthalten.

Mögliche Werte:

Mit durch Komma getrennten hexadezimalen Werten legen Sie mehrere individuelle Qualifier-Codes für einen Satz der jeweiligen Felder , und fest.

Länge

Legt die Länge für das Objekt fest (optional). Voraussetzung ist, dass im Feld ein gültiger Wert festgelegt ist. Das Gerät wendet das -Profil ausschließlich auf Datenpakete an, die den festgelegten Wert enthalten.

Mögliche Werte:

Legen Sie einen einzelnen Zahlenwert fest, zum Beispiel .

Das zweite Byte der Objektdaten enthält die Länge des verbleibenden Teils der Daten.

Wenn die Anzahl der Bit-Werte kein Vielfaches von 8 beträgt, dann füllt das Gerät die gepackten Einzelbit-Werte bis zur nächsten Byte-Grenze auf.

Wenn die Anzahl der Doppelbit-Werte kein Vielfaches von 4 beträgt, dann füllt das Gerät die gepackten Doppelbit-Werte bis zur nächsten Byte-Grenze auf.

Kennzeichnet die Länge des Objekts.

Funktionsname

Legt den Namen des Funktionscodes fest (optional). Voraussetzung ist, dass im Feld ein gültiger Wert festgelegt ist.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen
- Das Gerät lässt Datenpakete mit folgenden Function-Namen zu:
-
-
-

[Index der Standard-Objektliste]

Index	Gruppe	Variation	Funktion	Funktionsname	Länge	Qualifier
	n-Nr.					

Index	Gruppe	Variation	Funktion	Funktionsname	Länge	Qualifier

Index	Gruppe	Variation	Funktion	Funktionsname	Länge	Qualifizier
	n-Nr.					

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier

Index	Gruppe	Variation	Funktion	Funktionsname	Länge	Qualifizier
	n-Nr.					

Index	Gruppe	Variation	Funktion	Funktionsname	Länge	Qualifier

Index	Gruppe	Variation	Funktion	Funktionsname	Länge	Qualifizier

Index	Gruppe	Variation	Funktion	Funktionsname	Länge	Qualifier
n-Nr.						

Index	Gruppe	Variation	Funktion	Funktionsname	Länge	Qualifier

Index	Gruppe	Variation	Funktion	Funktionsname	Länge	Qualifier

Index	Gruppe	Variation	Funktion	Funktionsname	Länge	Qualifizier
	n-Nr.					

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier

Index	Gruppe	Variation	Funktion	Funktionsname	Länge	Qualifier
		n-Nr.				
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						
<hr/>						

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier

Index	Gruppe	Variation	Funktion	Funktionsname	Länge	Qualifier

Index	Gruppe	Variation	Funktion	Funktionsname	Länge	Qualifizier

Index	Gruppe	Variation	Funktion	Funktionsname	Länge	Qualifier

Index	Gruppe	Variation	Funktion	Funktionsname	Länge	Qualifizier
	n-Nr.					

Index	Gruppe	Variation	Funktion	Funktionsname	Länge	Qualifier

4.6.4 Deep Packet Inspection - IEC104 Enforcer

[Netzsicherheit > DPI > IEC104 Enforcer]

Dieser Dialog ermöglicht Ihnen, die -Einstellungen festzulegen und -spezifische Profile zu definieren.

Das IEC104-Protokoll ist ein Kommunikationsprotokoll, das im Bereich der Automatisierung verwendet wird. Das IEC104-Protokoll dient der Übertragung der IEC104-Datenpakete zwischen einer Leitstelle (Client) und einer Substation (Server) über ein TCP/IP-Netz. Die Funktion aktiviert die Firewall-Funktionen der Deep Packet Inspection (DPI) für den IEC104-Datenstrom. Der Type-IDs im IEC104-Protokoll legt den Zweck der Datenübertragung fest. Das Gerät blockiert Datenpakete, die gegen die festgelegten Profile verstoßen.

Wenn das -Profil aktiv ist, wendet das Gerät das Profil auf den Datenstrom an.

Das Gerät lässt ausschließlich Datenpakete zu, welche die in den folgenden Spalten festgelegten Werte enthalten:

-
-
-
-

Funktion

Nicht angewendete Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten -Profile von den im Gerät gespeicherten Profilen unterscheiden.

Wenn Sie die Schaltfläche klicken, wendet das Gerät die festgelegten Profile an.

Mögliche Werte:

Mindestens eines der aktiven -Profile, die im Gerät gespeichert sind, enthält geänderte Einstellungen.

Die -Profile, die auf den Datenstrom angewendet werden, stimmen mit den Profilen überein, die im Gerät gespeichert sind.

Tabelle

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

Schaltflächen

 Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld legen Sie die Nummer des Profils fest.
Mögliche Werte:

Nach Klicken der Schaltfläche fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld festgelegte Nummer zu.

 Löschen

Entfernt die ausgewählte Tabellenzeile.

Wenn für das Profil das Kontrollkästchen markiert ist, hindert das Gerät Sie daran, das Profil zu entfernen.

 Kopieren

Öffnet das Fenster , um eine bestehende Tabellenzeile zu kopieren. Voraussetzung ist, dass die Tabellenzeile für das zu kopierende Profil ausgewählt ist.

- Im Feld legen Sie die neue Nummer des kopierten Profils fest.
Mögliche Werte:

Das Gerät fügt die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld festgelegte Nummer zu.

 Änderungen anwenden

Das Gerät wendet die festgelegten Profile auf den Datenstrom an.

Wenn Sie die Werte im Feld geändert haben, dann weist das Gerät dem zugehörigen Profil die betreffenden Werte zu.

Index

Zeigt die fortlaufende Nummer des Profils, auf das sich die Tabellenzeile bezieht. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Beschreibung

Legt einen Namen für das Profil fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen
(Voreinstellung:)

Funktionstyp

Legt den Funktionstyp für das -Profil fest. Nach dem Klicken der Schaltfläche ✓
weist das Gerät die zugehörigen Typ-IDs zu.

Mögliche Werte:

Weist die Type-IDs für read-Funktion zu.

Weist die Type-IDs für read/write-Funktionen zu.

Weist die Type-IDs für common-Funktionen zu.

(Voreinstellung)

Weist die Type-IDs für jede Funktion zu.

Das Gerät akzeptiert keine nachträglichen Änderungen in Spalte .

Ermöglicht Ihnen, in Spalte benutzerdefinierte Werte festzulegen.

Erweiterte Liste Type-ID

Zeigt die Erweiterten Type-IDs für das -Profil. Das Gerät lässt Datenpakete mit den festgelegten Eigenschaften zu. Voraussetzung ist, dass in Spalte ein anderer Wert als festgelegt ist.

Das Gerät ermöglicht Ihnen, mehrere Advanced Type-IDs festzulegen. Führen Sie dazu die folgenden Schritte aus:

Klicken Sie für das betreffende Profil in die Spalte .

Der Dialog zeigt das Fenster .

Wählen Sie in der Dropdown-Liste den gewünschten Type-ID-Eintrag.

Klicken Sie die Schaltfläche .

Um mehrere Type-IDs hinzuzufügen, wiederholen Sie die zuvor beschriebenen Schritte.

Klicken Sie die Schaltfläche .

Mögliche Werte:

Die Bedeutung der Nummern finden Sie im Abschnitt „[Bedeutung der Erweiterte Liste Type-ID-Werte](#)“ auf Seite 195.

Originator Adressliste

Legt die Adressen fest, die den Ursprung der Datenpakete repräsentieren. Voraussetzung ist, dass in Spalte der Wert festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Das Gerät lässt Datenpakete mit beliebiger Originator-Adresse zu.

Das Gerät lässt Datenpakete mit der festgelegten Originator-Adresse zu.

Gemeinsame Adressliste

Legt die Adressen fest, an die das Gerät die IEC104-Datenpakete weiterleitet.

Mögliche Werte:

Das Gerät lässt Datenpakete mit der festgelegten Common-Adresse zu. Voraussetzung ist, dass in Spalte der Wert festgelegt ist.

Das Gerät lässt Datenpakete mit der festgelegten Common-Adresse zu. Voraussetzung ist, dass in Spalte der Wert festgelegt ist.

Übertragungsgröße Ursache

Legt die Größe in Oktetts fest, um welche die jeweiligen Felder in den Datenpaketen variieren dürfen. Das Gerät führt die Funktion DPI basierend auf diesen Einstellungen aus.

Mögliche Werte:

Die Datenpakete enthalten keine Originator-Adresse.

(Voreinstellung)

Die Datenpakete enthalten eine Originator-Adresse.

Größe Common-Adresse

Legt die Größe der Common-Adressen in Oktetts fest, an welche das Gerät die IEC104-Datenpakete weiterleitet. Diese Einstellung hat Auswirkungen auf die Einstellung in Spalte .

Mögliche Werte:

(Voreinstellung)

Größe IO-Adresse

Legt die Größe der Information Object Address in Oktetts fest.

Mögliche Werte:

(Voreinstellung)

IEC_60870_5_101 zulassen

Aktiviert/deaktiviert die in der IEC101-Spezifikation definierten Type-IDs.

Mögliche Werte:

Die in der IEC101-Spezifikation definierten Type-IDs sind aktiv.
Das Gerät lässt die Type-ID-Werte zusammen mit den Type-IDs, die auf den in Spalte oder festgelegten Werten basieren.

(Voreinstellung)

Die in der IEC101-Spezifikation definierten Type-IDs sind inaktiv.
Das Gerät lässt ausschließlich die Type-ID-Werte zu, die auf den in Spalte oder festgelegten Werten basieren.

Plausibilitätsprüfung

Aktiviert/deaktiviert die Plausibilitätsprüfung für Datenpakete.

Mögliche Werte:

(Voreinstellung)

Die Plausibilitätsprüfung ist aktiv.
Das Gerät prüft die Plausibilität der Datenpakete hinsichtlich Format und Spezifikation. Das Gerät blockiert Datenpakete, die gegen die festgelegten Profile verstoßen.

Die Plausibilitätsprüfung ist inaktiv.

TCP-Reset

Aktiviert/deaktiviert das Zurücksetzen der TCP-Verbindung im Falle einer Protokollverletzung oder wenn die Plausibilitätsprüfung einen Fehler erkennt.

Mögliche Werte:

(Voreinstellung)

Das Zurücksetzen der TCP-Verbindung ist aktiv.
Wenn das Gerät eine Protokollverletzung oder einen Fehler bei der Plausibilitätsprüfung erkennt, beendet es die TCP-Verbindung. Das Gerät baut die TCP-Verbindung bei erneuter Anfrage wieder auf.

Das Zurücksetzen der TCP-Verbindung ist inaktiv.

Debug

Aktiviert/deaktiviert das Debugging für die Profile.

Mögliche Werte:

Das Debugging ist aktiv.
Das Gerät sendet das Reset-Paket zusammen mit den Informationen über die Beendigung der TCP-Verbindung. Voraussetzung ist, dass in Spalte das Kontrollkästchen markiert ist.

(Voreinstellung)

Das Debugging ist inaktiv.

Profil aktiv

Aktiviert/deaktiviert das Profil.

Mögliche Werte:

- Das Profil ist aktiv.
Das Gerät wendet die in dieser Tabellenzeile festgelegten -Profile auf die Datenpakete an.
- Das Profil ist inaktiv.

[Erweiterte Liste Type-ID]

Erweiterte Liste Type-ID

Legt die Advanced Type-IDs für das betreffende -Profil fest.

Die Bedeutung der Nummern finden Sie im Abschnitt [„Bedeutung der Erweiterte Liste Type-ID-Werte“](#) auf Seite 195.

Hinzufügen

Fügt die in der Dropdown-Liste ausgewählten Einträge in das Feld ein.



Entfernt den Eintrag aus dem Feld .

Bedeutung der Erweiterte Liste Type-ID-Werte

Bedeutung

Bedeutung

4.6.5 Deep Packet Inspection - AMP-Enforcer

[Netzsicherheit > DPI > AMP Enforcer]

Dieser Dialog ermöglicht Ihnen, die - (ASCII Message Protocol Enforcer)-Einstellungen festzulegen und -spezifische Profile zu definieren.

Das ASCII Message Protocol (AMP) ist ein Kommunikationsprotokoll, das in der Automatisierungsindustrie in weitem Umfang für Supervisory Control and Data Acquisition (SCADA) und Systemintegration verwendet wird. Das ASCII Message Protocol (AMP) ist darauf ausgelegt, eine zuverlässige Kommunikation zwischen Teilen von Industrieanlagen zu ermöglichen. Das ASCII Message Protocol (AMP) wird für die Überwachung und Steuerung von Anlagen im Bereich der Automatisierungstechnik verwendet, zum Beispiel für Speicherprogrammierbare Steuerungen (SPS), Sensoren und Messgeräte.

Das Gerät verwendet die Funktion Deep Packet Inspection (DPI), um Datenpakete zu verwerfen, die gegen eines der festgelegten Profile verstoßen. Die -Funktion unterstützt Common ASCII Message Protocol (CAMP) und Non-Intelligent Terminal Protocol (NITP) unter Verwendung von TCP. Das Gerät verwendet die -Funktion, um die DPI-Funktion auf den CAMP- und NITP-Datenstrom anzuwenden. Das Gerät führt die DPI-Funktion basierend auf der -Funktion und dem festgelegten Profil aus.

Bei aktiviertem -Profil wendet das Gerät das Profil auf den Datenstrom an. Das Gerät lässt ausschließlich Datenpakete zu, welche die in den folgenden Spalten festgelegten Werte enthalten, abhängig von der -Funktion.

-
-
-
-
-
-
-
-
-
-
-

Das Menü enthält die folgenden Dialoge:

- [AMP Global](#)
- [AMP-Profil](#)

4.6.5.1 AMP Global

[Netzsicherheit > DPI > AMP Enforcer > Global]

In diesem Dialog legen Sie die globalen Einstellungen für das -Profil fest.

Protect-Modus

Program and Mode Protect

Aktiviert/deaktiviert die Prüfung der Datenpakete, welche die Taskcodes mit dem Wert in Spalte enthalten.

Mögliche Werte:

(Voreinstellung)

Die Überprüfung ist aktiv. Das Gerät leitet nur die Datenpakete weiter, die den in den Profilen festgelegten Parametern entsprechen. Das Gerät verwirft Datenpakete, die den Wert in Spalte enthalten, für die Taskcodes, die in den Profilen festgelegt sind.

Die Überprüfung ist inaktiv. Das Gerät leitet die Datenpakete weiter, die mit den in den Profilen festgelegten Parametern übereinstimmen, einschließlich jener Datenpakete, die Taskcodes mit dem Wert in Spalte enthalten.

Funktion

Nicht angewendete Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten -Profile von den im Gerät gespeicherten Profilen unterscheiden.

Mögliche Werte:

Mindestens eines der aktiven -Profile, die im Gerät gespeichert sind, enthält geänderte Einstellungen.

Wenn Sie die Schaltfläche  klicken, wendet das Gerät die festgelegten Profile an.


Die -Profile, die auf den Datenstrom angewendet werden, stimmen mit den Profilen überein, die im Gerät gespeichert sind.


Tabelle



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

Schaltflächen

 Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld  legen Sie die Nummer des Profils fest.
Mögliche Werte:

Nach Klicken der Schaltfläche  fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld  festgelegten Taskcode zu.

 Löschen


Entfernt die ausgewählte Tabellenzeile.

 Änderungen anwenden

Das Gerät wendet die festgelegten Profile auf den Datenstrom an.

Wenn Sie die Werte in dem Feld geändert haben, dann weist das Gerät dem zugehörigen Profil die betreffenden Werte zu.

Taskcode

Legt den benutzerdefinierten Taskcode für das -Profil fest, repräsentiert durch 2 ASCII-Zeichen. Die Taskcodes sind die Kommando- oder Antwort-Nachrichten, die verknüpft sind mit:

einer Modifikation der Einstellungen, des Anwendungsprogramms oder des Betriebsmodus des Anlagenteils.

Lesen oder Schreiben der Daten für Anlagenteile.

Mögliche Werte:

Sie finden die Bedeutung der voreingestellten Taskcodes im Abschnitt „[Bedeutung der Taskcode-Werte](#)“ auf Seite 208.

Beschreibung

Legt einen Namen für den Taskcode fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

Modus

Legt den zutreffenden Modus für den Taskcode fest.

Mögliche Werte:

Legt Kommandos fest, die mit der Modifikation der Steuerungseinstellungen, des Anwendungsprogramms oder des Betriebsmodus verknüpft sind.

Legt Lese-/Schreib-Kommandos fest, mit Ausnahme der Kommandos, die mit der Modifikation der Steuerungseinstellungen, des Anwendungsprogramms oder des Betriebsmodus verknüpft sind.

4.6.5.2 ANP-Profil

[Netzsicherheit > DPI > AMP Enforcer > Profil]

Dieser Dialog ermöglicht Ihnen, Profile für die -Funktion anzulegen. Das Profil ermöglicht Ihnen, basierend auf den festgelegten Werten, Datenpakete weiterzuleiten oder zu verwerfen.

Tabelle

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

Schaltflächen

 Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld legen Sie die Nummer des Profils fest.
Mögliche Werte:

Nach Klicken der Schaltfläche fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld festgelegte Nummer zu.

 Löschen

Entfernt die ausgewählte Tabellenzeile.

Wenn für das Profil das Kontrollkästchen markiert ist, hindert das Gerät Sie daran, das Profil zu entfernen.

 Kopieren

Öffnet das Fenster , um eine bestehende Tabellenzeile zu kopieren. Voraussetzung ist, dass die Tabellenzeile für das zu kopierende Profil ausgewählt ist.

- Im Feld legen Sie die neue Nummer des kopierten Profils fest.
Mögliche Werte:

Das Gerät fügt die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld festgelegte Nummer zu.

Index

Zeigt die fortlaufende Nummer des Profils, auf das sich die Tabellenzeile bezieht. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Beschreibung

Legt einen Namen für das Profil fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen
(Voreinstellung:)

Protokoll

Legt den TCP-Nutzlast-Protokolltyp der Datenpakete fest, auf die das Gerät das Profil anwendet. Das Gerät wendet das Profil ausschließlich auf Datenpakete an, die den festgelegten Wert im Feld Protocol enthalten.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet das Profil auf jedes Datenpaket an, ohne das Protokoll zu bewerten.

Message-Typ

Legt fest, ob die Nachricht vom Typ Kommando oder Antwort ist. Voraussetzung ist, dass in Spalte der Wert festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet das Profil auf jedes Datenpaket an, ohne den Nachrichten-Typ zu bewerten.
und

Das Gerät wendet das Profil ausschließlich auf Datenpakete an, die den festgelegten Nachrichten-Typ enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Sie legen den Nachrichten-Typ mit einem einzelnen Hexadezimalwert fest.
Beispiel:
- Sie legen mehrere einzelne Nachrichten-Typen durch Hexadezimalwerte fest, die durch ein Komma getrennt sind.
Beispiel:

und

Das Gerät wendet das Profil ausschließlich auf Datenpakete an, die den festgelegten Nachrichten-Typ enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Sie legen den Nachrichten-Typ mit einem einzelnen Hexadezimalwert fest.
Beispiel:
- Sie legen mehrere einzelne Nachrichten-Typen durch Hexadezimalwerte fest, die durch ein Komma getrennt sind.
Beispiel:

Die Bedeutung der Hexadezimalwerte finden Sie im Abschnitt „[Bedeutung der Message-Typ-Werte](#)“ auf Seite 209.

Adress-Klasse

Legt den jeweiligen Typ des Speichers fest, auf den auf dem Anlagenteil zugegriffen werden soll.

Voraussetzungen:

- In Spalte ist der Wert festgelegt.
- In Spalte ist ein Hexadezimalwert im Bereich oder oder der Hexadezimalwert festgelegt.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet das Profil auf jedes Datenpaket an, ohne die Adressklasse zu bewerten.

Das Gerät wendet das Profil ausschließlich auf Datenpakete an, welche die festgelegten Adressklasse enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Sie legen die Adressklasse mit einem einzelnen Hexadezimalwert fest.
Beispiel:
- Sie legen mehrere einzelne Adressklassen durch Hexadezimalwerte fest, die durch ein Komma getrennt sind.
Beispiel:
- Sie legen einen Bereich für eine Adressklasse durch Hexadezimalwerte fest, die mit einem Bindestrich verbunden sind.
Beispiel: -
- Sie können auch Adressklassen und Bereiche für Adressklassen kombinieren.
Beispiel:
Das Feld ermöglicht Ihnen, bis zu 205 Hexadezimalwerte festzulegen. Wenn Sie zum Beispiel eingeben, verwenden Sie 4 von 205 Hexadezimalwerten.

Geräteklasse

Legt den Typ der Geräteklasse (des herstellerspezifischen Geräts) fest, auf den zugegriffen werden soll.

Voraussetzungen:

- In Spalte ist der Wert festgelegt.
- In Spalte ist ein Hexadezimalwert im Bereich oder der Hexadezimalwert festgelegt.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet das Profil auf jedes Datenpaket an, ohne die Geräteklasse zu bewerten.

Das Gerät wendet das Profil ausschließlich auf Datenpakete an, welche die festgelegte Geräteklasse enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Sie legen eine Geräteklasse mit einem einzelnen Hexadezimalwert fest.
Beispiel:
 - Sie legen mehrere einzelne Geräteklassen durch Hexadezimalwerte fest, die durch ein Komma getrennt sind.
Beispiel:
 - Sie legen einen Bereich für eine Geräteklasse durch Hexadezimalwerte fest, die mit einem Bindestrich verbunden sind.
Beispiel: -????????
 - Sie können auch Geräteklassen und Bereiche für Geräteklassen kombinieren.
Beispiel: -????????
- Das Feld ermöglicht Ihnen, bis zu 205 Hexadezimalwerte festzulegen. Wenn Sie zum Beispiel eingeben, verwenden Sie 4 von 205 Hexadezimalwerten.

Speicheradresse

Legt die Startadresse des Speichers fest, der gelesen oder geschrieben werden soll.

Voraussetzungen:

- In Spalte ist der Wert festgelegt.
- In Spalte ist ein Hexadezimalwert im Bereich oder oder der Hexadezimalwert festgelegt.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet das Profil auf jedes Datenpaket an, ohne die Speicheradresse zu bewerten.

Das Gerät wendet das Profil ausschließlich auf Datenpakete an, welche die festgelegte Speicheradresse enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Sie legen eine Speicheradresse mit einem einzelnen Hexadezimalwert fest.
Beispiel:
 - Sie legen mehrere einzelne Speicheradressen durch Hexadezimalwerte fest, die durch ein Komma getrennt sind.
Beispiel:
 - Sie legen einen Speicheradressbereich durch Hexadezimalwerte fest, die mit einem Bindestrich verbunden sind.
Beispiel: -????????
 - Sie können auch Speicheradressen und Speicheradressbereiche kombinieren.
Beispiel: -????????
- Das Feld ermöglicht Ihnen, bis zu 205 Hexadezimalwerte festzulegen. Wenn Sie zum Beispiel eingeben, verwenden Sie 4 von 205 Hexadezimalwerten.

Datenwort

Legt die Startadresse fest, welche die Anlage verwendet, um Daten aus dem Paket zu lesen.

Voraussetzungen:

- In Spalte ist der Wert festgelegt.
- In Spalte ist ein Hexadezimalwert im Bereich oder oder der Hexadezimalwert festgelegt.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet das Profil auf jedes Datenpaket an, ohne das Datenwort zu bewerten.

Das Gerät wendet das Profil ausschließlich auf Datenpakete an, die das festgelegte Datenwort enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Sie legen ein Datenwort mit einem einzelnen Hexadezimalwert fest.
Beispiel:
- Sie legen mehrere einzelne Datenwörter durch Hexadezimalwerte fest, die durch ein Komma getrennt sind.
Beispiel:
- Sie legen einen Bereich für Datenwörter durch Hexadezimalwerte fest, die mit einem Bindestrich verbunden sind.
Beispiel:
- Sie können auch Datenwörter und Bereiche von Datenwörtern kombinieren.
Beispiel:

Das Feld ermöglicht Ihnen, bis zu 205 Hexadezimalwerte festzulegen. Wenn Sie zum Beispiel eingeben, verwenden Sie 4 von 205 Hexadezimalwerten.

Taskcode

Zeigt die Taskcodes für das -Profil. Sie können benutzerspezifische Taskcodes im -Dialog hinzufügen.

Voraussetzung ist, dass in Spalte einer der folgenden Werte festgelegt ist:

-
-
- Zusätzlich ist in Spalte ein Hexadezimalwert im Bereich oder der Hexadezimalwert festgelegt.
- Zusätzlich ist in Spalte der Wert festgelegt.

Das Gerät ermöglicht Ihnen, mehrere Taskcodes festzulegen. Führen Sie dazu die folgenden Schritte aus:

Klicken Sie in die Spalte des betreffenden Profils.

Der Dialog zeigt das Fenster .

Wählen Sie in der Dropdown-Liste den gewünschten Taskcode.

Klicken Sie die Schaltfläche .

Um mehrere Taskcodes hinzuzufügen, wiederholen Sie die zuvor beschriebenen Schritte.

Klicken Sie die Schaltfläche .

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet jeden Taskcode an, der im Feld vorhanden ist.

Das Gerät lässt Datenpakete mit den festgelegten Codes zu.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Ein einzelner Taskcode mit einem einzelnen Hexadezimalwert.

Beispiel:

- Mehrere Taskcodes mit Hexadezimalwerten, die durch ein Komma getrennt sind.

Beispiel:

Die Bedeutung der Hexadezimalwerte finden Sie im Abschnitt „Bedeutung der Taskcode-Werte“ auf Seite 208.

Taskcode-Daten

Legt die Taskcode-Daten für den Taskcode fest.

Voraussetzung ist, dass in Spalte einer der folgenden Werte festgelegt ist:

- Zusätzlich sind in Spalte ein Hexadezimalwert im Bereich oder der Hexadezimalwert sowie in Spalte ein einzelner Hexadezimalwert festgelegt.
- Zusätzlich ist in Spalte ein einzelner Hexadezimalwert festgelegt.

Mögliche Werte:

Das Gerät wendet das Profil ausschließlich auf Datenpakete an, die den festgelegten Taskcode enthalten. Die maximale Länge ist 72 Byte.

Zeichen für Fehlerprüfung

Aktiviert/deaktiviert die Fehlerprüfung der Zeichen in den CAMP- und NITP-Datenpaketen.

Voraussetzung:

- In Spalte ist der Wert und in Spalte ist ein Hexadezimalwert im Bereich oder der Hexadezimalwert festgelegt.
- In Spalte ist der Wert festgelegt.

Mögliche Werte:

(Voreinstellung)

Die Prüfung ist aktiv.

Die Prüfung ist inaktiv.

Zeichen für Blockprüfung

Aktiviert/deaktiviert die Überprüfung der Block check characters, um die Prüfsumme in den CAMP-Datenpaketen zu validieren.

Voraussetzungen:

- In Spalte ist der Wert festgelegt.
- In Spalte ist ein Hexadezimalwert im Bereich oder der Hexadezimalwert festgelegt.

Mögliche Werte:

(Voreinstellung)

Die Prüfung ist aktiv.

Die Prüfung ist inaktiv.

Debug

Aktiviert/deaktiviert das Debugging für die Profile.

Mögliche Werte:

Das Debugging ist aktiv.

Das Gerät sendet das Reset-Paket zusammen mit den Informationen über die Beendigung der TCP-Verbindung. Voraussetzung ist, dass in Spalte das Kontrollkästchen markiert ist.

(Voreinstellung)

Das Debugging ist inaktiv.

TCP-Reset

Aktiviert/deaktiviert das Zurücksetzen der TCP-Verbindung im Falle einer Protokollverletzung oder wenn die Plausibilitätsprüfung einen Fehler erkennt.

Mögliche Werte:

(Voreinstellung)

Das Zurücksetzen der TCP-Verbindung ist aktiv.

Wenn das Gerät eine Protokollverletzung oder einen Fehler bei der Plausibilitätsprüfung erkennt, beendet es die TCP-Verbindung. Das Gerät baut die TCP-Verbindung bei einer neuen Verbindungsanfrage wieder auf.

Das Zurücksetzen der TCP-Verbindung ist inaktiv.

Plausibilitätsprüfung

Aktiviert/deaktiviert die Plausibilitätsprüfung für Datenpakete.

Mögliche Werte:

(Voreinstellung)

Die Plausibilitätsprüfung ist aktiv.

Das Gerät prüft die Plausibilität der Datenpakete hinsichtlich Format und Spezifikation. Das Gerät blockiert Datenpakete, die gegen die festgelegten Profile verstoßen.

Die Plausibilitätsprüfung ist inaktiv.

Profil aktiv

Aktiviert/deaktiviert das Profil.

Mögliche Werte:

- Das Profil ist aktiv.
Das Gerät wendet die in dieser Tabellenzeile festgelegten -Profile auf die Datenpakete an.
- Das Profil ist inaktiv.

[Taskcode]

Taskcode

Legt die Taskcodes für das betreffende -Profil fest.

Die Bedeutung der Hexadezimalwerte finden Sie im Abschnitt „[Bedeutung der Taskcode-Werte](#)“ auf Seite 208.

Hinzufügen

Fügt die in der Dropdown-Liste ausgewählten Einträge in das Feld ein.



Entfernt den Eintrag aus dem Feld .

Bedeutung der Taskcode-Werte

Bedeutung

Bedeutung

Bedeutung der Message-Typ-Werte

Bedeutung

4.6.6 Deep Packet Inspection - ENIP Enforcer

[Netzsicherheit > DPI > ENIP Enforcer]

Dieser Dialog ermöglicht Ihnen, die - (Ethernet Industrial Protocol Enforcer)-Einstellungen festzulegen und -spezifische Profile zu definieren.

Das Ethernet Industrial Protocol (ENIP) ist Teil des Common Industrial Protocol (CIP). Das Protokoll Common Industrial Protocol (CIP) definiert die Objektstruktur und legt den Austausch der Nachrichten fest. Die -Funktion wendet die Funktion Deep Packet Inspection (DPI) auf den ENIP- und CIP-Datenstrom an. Das Ethernet Industrial Protocol (ENIP) wird verwendet, um industrielle Automatisierungsausrüstung wie SPS (Speicherprogrammierbare Steuerungen), Sensoren oder Zähler zu überwachen und zu steuern.

Das Gerät verwendet die Funktion , um die DPI-Funktion auf dem Datenstrom auszuführen. Das Gerät führt die DPI-Funktion basierend auf den Werten aus, die in den festgelegten Profilen definiert sind. Das Gerät blockiert Datenpakete, die gegen die festgelegten Profile verstoßen.

Anmerkung: Die Funktion führt die DPI-Funktion lediglich für Pakete aus, die eine explizite Anfrage enthalten, und verwirft Pakete, die eine implizite Anfrage enthalten. Eine explizite Anfrage enthält CIP-Messages over TCP. Eine implizite Anfrage enthält CIP-Messages over UDP.

Wenn das -Profil aktiv ist, wendet das Gerät das Profil auf den Datenstrom an. Das Gerät lässt ausschließlich Datenpakete zu, welche die in den folgenden Spalten festgelegten Werte enthalten:

-
-
-
-
-

(Programmable Controller Communication Commands)

Das Menü enthält die folgenden Dialoge:

- [ENIP-Profil](#)
- [ENIP-Objekt](#)

4.6.6.1 ENIP-Profil

[Netzsicherheit > DPI > ENIP Enforcer > Profil]

In diesem Dialog legen Sie die globalen Einstellungen für das -Profil fest.

Funktion

Nicht angewendete Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten -Profile von den im Gerät gespeicherten Profilen unterscheiden.

Mögliche Werte:

Mindestens eines der aktiven -Profile, die im Gerät gespeichert sind, enthält geänderte Einstellungen.

Wenn Sie die Schaltfläche  klicken, wendet das Gerät die festgelegten Profile an.

Die -Profile, die auf den Datenstrom angewendet werden, stimmen mit den Profilen überein, die im Gerät gespeichert sind.

Tabelle

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

Schaltflächen

 Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld legen Sie die Nummer des Profils fest.

Mögliche Werte:

Nach Klicken der Schaltfläche fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld festgelegte Nummer zu.

 Löschen

Entfernt die ausgewählte Tabellenzeile.

Wenn für das Profil das Kontrollkästchen markiert ist, hindert das Gerät Sie daran, das Profil zu entfernen.



Öffnet das Fenster , um eine bestehende Tabellenzeile zu kopieren. Voraussetzung ist, dass die Tabellenzeile für das zu kopierende Profil ausgewählt ist.

- Im Feld legen Sie die neue Nummer des kopierten Profils fest.
Mögliche Werte:

Das Gerät fügt die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld festgelegte Nummer zu.



Das Gerät wendet die festgelegten Profile auf den Datenstrom an.

Wenn Sie die Werte im Feld geändert haben, dann weist das Gerät dem zugehörigen Profil die betreffenden Werte zu.

Index

Zeigt die fortlaufende Nummer des Profils, auf das sich die Tabellenzeile bezieht. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Beschreibung

Legt einen Namen für das Profil fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen
(Voreinstellung:)

Funktionstyp

Legt den Funktionstyp für das -Profil fest. Nach Klicken der Schaltfläche weist das Gerät die zugehörigen Class-IDs und Service-Codes zu.

Mögliche Werte:

Weist die Class-IDs für die read-Funktion zu.
Die Liste der Nur-Lesen- (readonly-) Class-IDs finden Sie in [Tabelle 4 auf Seite 225](#).

Weist die Class-IDs für die read/write-Funktionen zu.
Die Liste der Schreib-Lese-Class-IDs finden Sie in [Tabelle 5 auf Seite 230](#).

(Voreinstellung)

Weist die Class-IDs für jede Funktion zu. Wenn der Funktionstyp any ist, können Sie keine benutzerdefinierten Class-IDs durch den -Wert festlegen.

Ermöglicht Ihnen, benutzerdefinierte Class-IDs festzulegen.

Embedded PCCC zulassen

Aktiviert/deaktiviert DPI für PCCC-Nachrichten, die in Datenpaketen verpackt sind. PCCC-Nachrichten sind in das Ethernet Industrial Protocol (ENIP) eingebettet. Das Aktivieren dieser Einstellung ist sinnvoll beim Absichern von Netzverkehr von und zu PLC-5- und MicroLogix- Controllern.

Mögliche Werte:

DPI für PCCC-Nachrichten ist aktiv. Das Gerät weist die Befehlscodes und Funktionscodes zu, die dem in Spalte festgelegten Wert entsprechen.

Sie finden die Listen der Befehlscodes und Funktionscodes in den folgenden Tabellen:

- [Siehe Tabelle 6 auf Seite 240.](#)
- [Siehe Tabelle 7 auf Seite 240.](#)
- [Siehe Tabelle 8 auf Seite 242.](#)

(Voreinstellung)

DPI für PCCC-Nachrichten ist inaktiv.

Plausibilitätsprüfung

Aktiviert/deaktiviert die Plausibilitätsprüfung für Datenpakete.

Mögliche Werte:

(Voreinstellung)

Die Plausibilitätsprüfung ist aktiv.

Das Gerät prüft die Plausibilität der Datenpakete hinsichtlich Format und Spezifikation. Das Gerät blockiert Datenpakete, die gegen die festgelegten Profile verstoßen.

Die Plausibilitätsprüfung ist inaktiv.

TCP-Reset

Aktiviert/deaktiviert das Zurücksetzen der TCP-Verbindung im Falle einer Protokollverletzung oder wenn die Plausibilitätsprüfung einen Fehler erkennt.

Mögliche Werte:

(Voreinstellung)

Das Zurücksetzen der TCP-Verbindung ist aktiv.

Wenn das Gerät eine Protokollverletzung oder einen Fehler bei der Plausibilitätsprüfung erkennt, beendet es die TCP-Verbindung. Das Gerät baut die TCP-Verbindung bei einer neuen Verbindungsanfrage wieder auf.

Das Zurücksetzen der TCP-Verbindung ist inaktiv.

Debug

Aktiviert/deaktiviert das Debugging für die Profile.

Mögliche Werte:

Das Debugging ist aktiv.

Das Gerät sendet das Reset-Paket zusammen mit den Informationen über die Beendigung der TCP-Verbindung. Voraussetzung ist, dass in Spalte das Kontrollkästchen markiert ist.

(Voreinstellung)

Das Debugging ist inaktiv.

Standard-Objektliste

Legt die in der Standard-Objektliste verwendeten Index-Nummern fest.

Mögliche Werte:

Das Gerät wendet das -Profil auf jedes Datenpaket an, unabhängig von der Index-Nummer.

Das Gerät wendet das -Profil ausschließlich auf Datenpakete an, welche die festgelegten Class-IDs und Service-Codes in der festgelegten Index-Nummer enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Mit einem einzelnen Zahlenwert legen Sie eine einzelne Index-Nummer fest.
Beispiel:
- Mehrere Index-Nummern legen Sie mit durch Komma getrennte Zahlenwerten fest.
Beispiel:
- Einen Index-Nummern-Bereich legen Sie mit durch einen Bindestrich verbundene Zahlenwerte fest.
Beispiel:
- Sie können auch Index-Nummern und Index-Nummern-Bereiche kombinieren.
Beispiel:

Das Feld ermöglicht Ihnen, bis zu 347 Zahlenwerte festzulegen. Wenn Sie zum Beispiel eingeben, verwenden Sie 4 von 347 Zahlenwerten.

Die Liste der Class-IDs und der dazugehörigen Service-Codes finden Sie in [Tabelle 3 auf Seite 216](#).

(Voreinstellung)

Das Gerät wendet die Index-Nummer nicht auf das -Profil an.

Wildcard Service-Liste

Legt die Service-Codes fest, die das Gerät für alle gültigen Class-IDs erlaubt.

Mögliche Werte:

Das Gerät wendet das Profil ausschließlich auf Datenpakete an, welche die festgelegten Service-Codes enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Sie legen eine Service-Liste mit einem einzelnen Hexadezimalwert fest.
Beispiel:
- Sie legen mehrere einzelne Service-Codes durch Hexadezimalwerte fest, die durch ein Komma getrennt sind.
Beispiel:

Das Feld ermöglicht Ihnen, bis zu 128 Hexadezimalwerte festzulegen. Wenn Sie zum Beispiel eingeben, verwenden Sie 4 von 128 Hexadezimalwerten.

Profil aktiv

Aktiviert/deaktiviert das Profil.

Mögliche Werte:

Das Profil ist aktiv.

Das Gerät wendet die in dieser Tabellenzeile festgelegten -Profile auf die Datenpakete an.

(Voreinstellung)

Das Profil ist inaktiv.

4.6.6.2 ENIP-Objekt

[Netzsicherheit > DPI > ENIP Enforcer > Objekt]

Die ENIP-Funktion verwendet Objekte, um Werte und Informationen zwischen Geräten zu vermitteln. Die ENIP-Funktion verwendet Class-IDs und Service-Codes, um festzulegen, wie die Daten innerhalb des Objekts codiert sind. Jede Instanz eines codierten Informationselements, die eine eindeutige Class-ID und einen eindeutigen Service-Code in einer Nachricht definiert, ist ein ENIP-Objekt.

Dieses Fenster ermöglicht Ihnen, benutzerdefinierte ENIP-Objekte hinzuzufügen sowie zuvor hinzugefügte benutzerdefinierte ENIP-Objekte anzusehen. Um zu kontrollieren, ob ein hinzugefügtes ENIP-Objekt gültig ist, prüfen Sie die folgenden Parameter:

-
-


Tabelle



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


Schaltflächen







Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- In der Dropdown-Liste  wählen Sie die Index-Nummer des Profils.
- Im Feld  legen Sie die benutzerdefinierten Class-IDs fest.
Mögliche Werte:

- Im Feld  legen Sie die Service-Codes fest.
Mögliche Werte:

Nach Klicken der Schaltfläche  fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist dieser Tabellenzeile die in den Feldern ,  und  festgelegten Werte zu.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

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

Class-ID

Legt die benutzerdefinierten Class-IDs für das -Profil fest.
 Mögliche Werte:

Service-Codes

Legt die Service-Codes fest.
 Mögliche Werte:

- Das Gerät wendet das Profil ausschließlich auf Datenpakete an, welche die festgelegten Service-Codes enthalten.
 Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:
- Sie legen eine Service-Liste mit einem einzelnen Hexadezimalwert fest.
 Beispiel:
 - Sie legen mehrere einzelne Service-Codes durch Hexadezimalwerte fest, die durch ein Komma getrennt sind.
 Beispiel:
 Das Feld ermöglicht Ihnen, bis zu 128 Hexadezimalwerte festzulegen. Wenn Sie zum eingeben, verwenden Sie 4 von 128 Hexadezimalwerten.

Beschreibung

Zeigt den Namen des Objekts.

[Standard-Objektliste]

Index	Class-ID	Service-Codes

Index	Class-ID	Service-Codes
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____	1	_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____
_____		_____

Index	Class-ID	Service-Codes

Class-ID	Service-Codes

1. Ein Paket mit [] = [] enthält eingebettete CIP-Messages. In diesem Fall führt das Gerät eine zusätzliche Stufe von DPI für die Datenpakete durch, welche die Service Code-Werte [], [] und [] enthalten. Das Gerät blockiert ein Datenpaket, wenn es andere als die vorstehenden Service Code-Werte für diese [] enthält.

Tab. 5: Class-IDs für Funktionstyp

Class-ID	Service-Codes

Class-ID	Service-Codes

[Liste der PCCC-Befehlscodes für unterschiedliche Funktionstypen]

Befehlscodes	Funktionscodes

Befehlscodes	Funktionscodes

Befehlscodes	Funktionscodes

Befehlscodes	Funktionscodes

Befehlscodes	Funktionscodes

4.7 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](#)

4.7.1 DoS Global

[Netzicherheit > 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:

Der Filter ist aktiv.

(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:

Der Filter ist aktiv.

(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:

Der Filter ist aktiv.
(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:

Der Schutz ist aktiv.
(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:

Der Schutz ist aktiv.
(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:

Der Schutz ist aktiv.
(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:

- Der Filter ist aktiv.
(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:

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

IP-Source-Route verwerfen

Aktiviert/deaktiviert die Filterung der empfangenen IP-Datenpakete mit Strict Source Routing oder Loose Source Routing. Das Strict Source Routing oder Loose Source Routing ist eine Option im IP-Header, bei welcher der Absender den Routing-Pfad festlegt. Die Datenpakete folgen diesem Routing-Pfad, um das Ziel zu erreichen.

Mögliche Werte:

- (Voreinstellung)
- Der Filter ist aktiv. Das Gerät verwirft IP-Datenpakete mit einem festgelegten Routing-Pfad im IP-Header.
- 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:

- Der Filter ist aktiv.
(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 festgelegte Größe überschreitet und verwirft diese.

Mögliche Werte:

- Der Filter ist aktiv.
(Voreinstellung)
- Der Filter ist inaktiv.

Erlaubte Payload-Größe [Byte]

Legt die maximal erlaubte Payload-Größe von ICMP-Paketen in Byte fest.

Mögliche Werte:

(Voreinstellung:)

4.8 Intrusion Detection System

[Netzsicherheit > IDS]

Dieser Dialog ermöglicht Ihnen, den Zustand der Funktion zu überwachen.

Die Funktion überwacht den Verkehr im Netz und alarmiert, wenn die Funktion eine ungewöhnliche Aktivität feststellt.

Voraussetzungen, um die Funktion im Gerät zu verwenden:

- CylusOne-Probe
- CylusOne-Plattform
- Ein lokales Benutzerkonto mit der Zugriffsrolle

Die CylusOne-Probe ist im Gerät eingebaut. Das Gerät verwendet die CylusOne-Probe, um an den Ports Datenpakete abzufangen. Die Ports wählen Sie im Dashboard der CylusOne-Plattform aus. Die CylusOne-Probe untersucht die Datenpakete und sendet die Daten an die CylusOne-Plattform.

Die CylusOne-Plattform wertet die von der CylusOne-Probe empfangenen Daten aus. Wenn die CylusOne-Plattform eine ungewöhnliche oder potenziell unsichere Aktivität im Datenstrom erkennt, dann zeigt das Dashboard der CylusOne-Plattform Alarmmeldungen basierend auf dem Verhaltensmuster der Datenpakete. Dies hilft dabei, Bedrohungen kontinuierlich und zeitnah zu erkennen.

Die folgende Tabelle zeigt die Bezeichnung der Ports im Gerät sowie deren Entsprechung im Dashboard der CylusOne-Plattform. Die tatsächliche Anzahl der Ports ist abhängig von der Hardware-Ausstattung des Geräts:

Bezeichnung des Ports im Gerät	Bezeichnung des Ports im Dashboard der CylusOne-Plattform

Status

Status IDS

Zeigt den Betriebszustand der CylusOne-Probe im Gerät.

Mögliche Werte:

Die CylusOne-Probe ist im Gerät aktiv.

Die CylusOne-Probe ist im Gerät inaktiv.

5 Virtual Private Network

Das Menü enthält die folgenden Dialoge:

- [VPN Übersicht](#)
- [VPN Zertifikate](#)
- [VPN Verbindungen](#)

5.1 VPN Übersicht

[Virtual Private Network > Übersicht]

Virtuelle private Netzwerke (VPN) gewährleisten eine sichere Kommunikation für entfernte Benutzer oder Zweigniederlassungen und bieten ihnen die Möglichkeit, eine Verbindung mit Servern in anderen Zweigniederlassungen oder sogar anderen Unternehmen, die öffentliche Netze nutzen, herzustellen. Obwohl der VPN-Tunnel ein öffentliches Netz verwendet, weist er dasselbe Verhalten wie ein privates Netz auf.

VPN-Tunnel bieten eine sichere Kommunikation, um den gegenwärtigen Trend zu verstärkter Telearbeit und zum globalen Geschäftsbetrieb zu unterstützen. In solchen Fällen können entfernte Benutzer oder Zweigniederlassungen eine Verbindung zueinander sowie zu zentralen Ressourcen herstellen.

Um eine sichere Kommunikation zu gewährleisten, nutzen virtuelle private Netzwerke IP-Sicherheit (IPsec). Um Sicherheit zu gewährleisten, verfügt IPsec über 2 Funktionen, nämlich: Datenverschlüsselung und Datenintegrität. Um mittels der Verschlüsselung die Authentifizierung und Integrität der Quelle zu sichern, verwendet das Gerät IPsec Encapsulating Security Payload (ESP). So kennen nur der Absender und der Empfänger den Sicherheitsschlüssel.

Das Gerät verwendet ferner die Methode der ausgehandelten „Security Associations“ (SA). Das erste empfangene Paket initiiert eine Verhandlung zwischen dem Absender und dem Empfänger darüber, welche Security-Association-Parameter die Geräte nutzen werden. Die Geräte verwenden für den Verhandlungsprozess Internet Key Exchange (IKE). Bei der Verhandlung der Parameter einigen sich die sendenden und empfangenden Geräte auf die Authentifizierungs- und Datensicherheitsmethoden. Die Geräte nehmen darüber hinaus eine gegenseitige Authentifizierung vor und generieren einen gemeinsam verwendeten Schlüssel („Shared Key“). Die Geräte nutzen den „Shared Key“ zur Verschlüsselung der in den einzelnen Paketen enthaltenen Daten.

Der Dialog enthält Registerkarten, welche die gegenwärtigen VPN-Tunnel und die zugehörigen Status zeigen.

Die Registerkarte [\[Fehler\]](#) zeigt erkannte Fehler, die bei der Fehlersuche für einen VPN-Tunnel nützlich sein können.

Der Dialog enthält die folgenden Registerkarten:

- [\[Übersicht\]](#)
- [\[Diagnose\]](#)
- [\[Verbindungsfehler\]](#)

Verbindung

Verbindungen (max.)

Zeigt die maximale Anzahl der unterstützten VPN-Tunnel. Das Gerät schränkt die maximale Anzahl von aktiven VPN-Tunneln auf die unter festgelegte Menge ein.

Max. Aktive Verbindungen

Zeigt die maximale Anzahl der aktiven VPN-Tunnel, die unterstützt werden.

[Übersicht]

Tabelle

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

VPN index

Zeigt den Index der Tabellenzeile zur eindeutigen Identifizierung eines VPN-Tunnels.

VPN Beschreibung

Zeigt den benutzerdefinierten Namen für den VPN-Tunnel.

VPN active

Zeigt, ob der VPN-Tunnel aktiv/inaktiv ist.

Das Gerät beschränkt die maximale Anzahl von eingerichteten VPN-Tunneln auf den im Feld gezeigten Wert. Das Gerät beschränkt außerdem die maximale Anzahl von aktiven VPN-Tunneln auf den im Feld festgelegten Wert.

Mögliche Werte:

Der VPN-Tunnel ist aktiv.

Der VPN-Tunnel ist inaktiv.

Used IKE version

Zeigt die Version des IKE-Protokolls, das der VPN-Tunnel verwendet.

Mögliche Werte:

Das Gerät verwendet das IKE-Protokoll Version (ISAKMP).

Das Gerät verwendet das IKE-Protokoll Version .

Startup

Zeigt die Ausgangsrolle zur Aushandlung des Schlüsselaustauschs für den VPN-Tunnel.

Mögliche Werte:

Wenn Sie das Gerät als Initiator für den VPN-Tunnel festlegen, dann initiiert das Gerät aktiv den Internet Key Exchange (IKE) und die Parameterverhandlung.

Wenn Sie das Gerät als Responder für den VPN-Tunnel festlegen, dann wartet das Gerät darauf, dass der Initiator einen Schlüsselaustausch (IKE) und die Aushandlung der Verbindungsparameter beginnt.

Betriebsstatus

Zeigt den gegenwärtigen Status des VPN-Tunnels.

Mögliche Werte:

VPN-Tunnel ist aufgebaut.

VPN-Tunnel ist nicht aufgebaut.

Wenn Sie den VPN-Tunnel für dieses Gerät als Initiator festlegen, dann gibt der Wert an, dass der Schlüsselaustausch und der Verhandlungsalgorithmus laufen. Wenn der VPN-Tunnel für dieses Gerät der Responder ist, dann gibt der Wert an, dass der VPN-Tunnel auf den Beginn des Prozesses wartet.

Die IKE-SA ist aktiv. Das Gerät hat für diese Instanz jedoch mindestens eine nicht hergestellte IPsec-SA erkannt.

Das Gerät wartet auf den Abschluss der Konfiguration, bevor das Gerät die Einrichtung des VPN-Tunnel startet. Beispielsweise weist das Gerät eine nicht erfolgreiche Hostnamen-Auflösung auf.

Der Schlüsselaustausch wird ausgeführt. Das Gerät zeigt den Wert nach Ablauf des IKE- oder IPsec-Lebensdauer-Timers.

Verbindung hergestellt [s]

Zeigt den Zeitraum in Sekunden, nach dem das Gerät den VPN-Tunnel für dieses Gerät aufgebaut hat. Das Gerät aktualisiert den Wert nach jeder erneuten IKE-Authentifizierung.

Lokaler Host

Zeigt den Namen und/oder die IP-Adresse des lokalen Hosts, den das Gerät mittels IKE erkannt hat.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..128 Zeichen

Ferner Host

Zeigt den Namen und/oder die IP-Adresse des entfernten Hosts, die das Gerät mittels IKE erkannt hat.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..128 Zeichen

IKE proposal

Zeigt die Algorithmen, die IKE für den Schlüsselaustausch verwendet.

Das Gerät zeigt eine Kombination der Parameter , und .

Wenn Sie in dem Dialog einen IKE-Algorithmus für das Gerät einrichten und für den entfernten Endpunkt ein Algorithmus mit höherer Sicherheit eingerichtet ist, dann ist es möglich, dass sowohl die lokalen als auch die entfernten Geräte den entfernten Algorithmus verwenden.

Das Gerät zeigt die gegenwärtig für diese Verbindung verwendete Verschlüsselungssammlung.

IPsec proposal

Zeigt den Algorithmus, den IPsec für die Datenkommunikation verwendet.

Das Gerät zeigt eine Kombination der Parameter , und .

Wenn Sie einen IPsec-Algorithmus für die Instanz im Dialog auswählen und für den entfernten Endpunkt ein besserer Algorithmus mit höherer Sicherheit eingerichtet ist, dann ist es möglich, dass sowohl die lokalen als auch die entfernten Geräte den besseren Algorithmus verwenden.

Das Gerät zeigt die gegenwärtig für diese Verbindung verwendete Verschlüsselungssammlung.

Tunnels

Zeigt die Anzahl der IPsec-Tunnel innerhalb des VPN-Netzwerks.

[Diagnose]

Tabelle

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

VPN index

Zeigt den Index der Tabellenzeile zur eindeutigen Identifizierung eines VPN-Tunnels.

VPN Beschreibung

Zeigt den benutzerdefinierten Namen für den VPN-Tunnel.

VPN active

Zeigt, ob der VPN-Tunnel aktiv/inaktiv ist.

Das Gerät beschränkt die maximale Anzahl von eingerichteten VPN-Tunneln auf den im Feld gezeigten Wert. Das Gerät beschränkt außerdem die maximale Anzahl von aktiven VPN-Tunneln auf den im Feld festgelegten Wert.

Mögliche Werte:

Der VPN-Tunnel ist aktiv.

Der VPN-Tunnel ist inaktiv.

Tunnel index

Zeigt den Indexwert, der zusammen mit dem Wert in Spalte den Eintrag in der Verbindungstunnel-Infotabelle identifiziert.

Traffic selector index

Zeigt den Indexwert, der zusammen mit dem Wert in Spalte den Eintrag in der Traffic-Selector-Tabelle identifiziert, der auf den IPsec-Tunnel abgebildet ist.

Mögliche Werte:

Der Index des Traffic-Selectors ist unbekannt.

Betriebsstatus

Zeigt den gegenwärtigen Status des VPN-Tunnels.

Mögliche Werte:

Die „Internet Key Exchange Security Association“ (IKE-SA) und jede „Internet Protocol Security-Security Association“ (IPsec-SA) ist aktiv.

Die IKE-SA und IPsec-SAs sind inaktiv.

Wenn Sie den VPN-Tunnel für diese Instanz als Initiator festlegen, gibt der Wert an, dass der Schlüsselaustausch und der Verhandlungsalgorithmus laufen. Wenn der VPN-Tunnel für diese Instanz der Responder ist, dann gibt der Wert an, dass der VPN-Tunnel auf den Beginn des Prozesses wartet.

Die IKE-SA ist aktiv. Das Gerät hat für diese Instanz jedoch mindestens eine nicht hergestellte IPsec-SA erkannt.

Das Gerät wartet auf den Abschluss der Konfiguration, bevor das Gerät die Einrichtung des VPN-Tunnel startet. Beispielsweise weist das Gerät eine nicht erfolgreiche Hostnamen-Auflösung auf.

Der Schlüsselaustausch wird ausgeführt. Das Gerät zeigt den Wert nach Ablauf des IKE- oder IPsec-Lebensdauer-Timers.

IKE Neu-Authentifizierung [s]

Zeigt die verbleibende Zeit bis zur nächsten IKE-Neuauthentifizierung in Sekunden. Der Wert 0 gibt an, dass die Neuauthentifizierung nicht eingerichtet ist.

Nächstes IKE Re-Keying [s]

Zeigt die verbleibende Zeit bis zur nächsten IKE-Schlüssel-Erzeugung in Sekunden. Der Wert 0 gibt an, dass der Schlüsselwechsel nicht eingerichtet ist.

IKE initiator SPI

Zeigt den „Security Parameter Index“ (SPI) des Initiators abhängig vom Gerät, das Sie als Initiator festlegen. Wenn Sie beispielsweise dieses Gerät als Initiator festlegen, ist dieser Wert der SPI des lokalen Geräts.

IKE responder SPI

Zeigt den SPI des Responders abhängig vom Gerät, das Sie als Initiator festlegen. Wenn Sie beispielsweise dieses Gerät als Initiator festlegen, ist dieser Wert der SPI des entfernten Geräts.

Local traffic selector

Zeigt den lokalen Traffic-Selector für diesen IPsec-Tunnel. Als Ergebnis des Aushandlungsprozesses zwischen den Teilnehmern können sich der lokale Traffic-Selector und der eingerichtete Traffic-Selector unterscheiden.

Remote traffic selector

Zeigt den Remote-Traffic-Selector für diesen IPsec-Tunnel. Als Ergebnis des Aushandlungsprozesses zwischen den Teilnehmern können sich der Traffic-Selector und der eingerichtete Traffic-Selector unterscheiden.

Tunnel status

Zeigt den gegenwärtigen Betriebsstatus des IPsec-Tunnels.

Mögliche Werte:

Der IPsec-Vorschlag wird ausgeführt. Für diese IPsec-SA wurden keine Traffic-Selectors oder Sicherheitsparameter ausgehandelt.

Schlüsselaustausch und Algorithmus für die Aushandlung ist für diese IPsec-SA abgeschlossen, der Tunnel ist jedoch inaktiv.

Die Richtlinien für die Verschlüsselung des Datenstroms sind eingerichtet, der Aushandlungsprozess hat jedoch noch nicht begonnen.

Die Authentifizierung der Peers ist eingerichtet, aber der IPsec-Vorschlag für diesen Tunnel wird noch ausgeführt.

Die IPsec-SA ist installiert.

Das Gerät aktualisiert die Sicherheitszuordnung.

Der Schlüsselaustausch für diesen IPsec-SA wird ausgeführt. Das Gerät zeigt den Wert nach Ablauf des IPsec Lifetime-Timers.

Der Schlüsselaustausch für diesen IPsec-SA ist abgeschlossen und das Gerät richtet einen neuen Tunnel ein. Nach Ablauf des vorherigen IPsec-Vorschlags ist der Tunnel aktiv.

Der Schlüsselaustausch für diesen IPsec-SA ist fehlgeschlagen. Das Gerät versucht automatisch, einen neuen Schlüsselaustausch zu initiieren.

Das Gerät ersetzt den IPsec-Tunnel während der erneuten Schlüsselerzeugung. Das Gerät lässt den Tunnel für verzögerte Pakete geöffnet. Der alte und der neue Tunnel sind in der Voreinstellung 5 Sekunden lang gleichzeitig geöffnet. Nach Ablauf des Timers für die IPsec-Lifetime löscht das Gerät den Tunnel.

Der Timer für die IPsec-Lifetime ist abgelaufen. Das Gerät löscht den Tunnel.

IPsec input SPI

Zeigt den IPsec-Security-Parameter-Index (SPI), den das Gerät auf die Daten anwendet, die das Gerät aus dem VPN-Tunnel empfängt. Der SPI ermöglicht dem Gerät die Auswahl der SA, mit der das Gerät ein empfangenes Paket verarbeitet.

IPsec output SPI

Zeigt den IPsec-Security-Parameter-Index (SPI), den das Gerät auf die Daten anwendet, die das Gerät an den VPN-Tunnel sendet.

Nächstes IPsec Re-Keying [s]

Zeigt die verbleibende Zeit in Sekunden, bis die nächste Schlüsselerzeugung für diesen IPsec-Tunnel beginnt.

IPsec Tunnel-Input [Byte]

Zeigt die Anzahl der in diesem VPN-Tunnel empfangenen Bytes.

IPsec Tunnel-Input [Pakete]

Zeigt die Anzahl der in diesem VPN-Tunnel empfangenen Pakete.

IPsec-Daten zuletzt empfangen [s]

Zeigt die Zeit in Sekunden, die seit dem letzten Empfang von Daten im VPN-Tunnel vergangen ist.

IPsec Tunnel-Output [Byte]

Zeigt die Anzahl der in diesen VPN-Tunnel gesendeten Bytes.

IPsec Tunnel-Output [Pakete]

Zeigt die Anzahl der in diesen VPN-Tunnel gesendeten Pakete.

IPsec-Daten zuletzt gesendet [s]

Zeigt die Zeit seit dem letzten Senden von Daten durch den VPN-Tunnel in Sekunden.

[Verbindungsfehler]

Tabelle

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

VPN index

Zeigt den Index der Tabellenzeile zur eindeutigen Identifizierung eines VPN-Tunnels.

VPN Beschreibung

Zeigt den benutzerdefinierten Namen für den VPN-Tunnel.

VPN active

Zeigt, ob der VPN-Tunnel aktiv/inaktiv ist.

Das Gerät beschränkt die maximale Anzahl von eingerichteten VPN-Tunneln auf den im Feld gezeigten Wert. Das Gerät beschränkt außerdem die maximale Anzahl von aktiven VPN-Tunneln auf den im Feld festgelegten Wert.

Mögliche Werte:

Der VPN-Tunnel ist aktiv.

Der VPN-Tunnel ist inaktiv.

Letzter Verbindungsfehler

Zeigt die letzte für diesen VPN-Tunnel aufgetretene Fehlerbenachrichtigung.

Wenn die Verbindung inaktiv bleibt, hilft Ihnen dieser Wert dabei, erkannte Fehler zu isolieren. Dieser Wert hilft Ihnen, zu bestimmen, ob ein erkannter Fehler im Vorschlagsaustausch oder während des Tunnelaufbaus aufgetreten ist.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..512 Zeichen

5.2 VPN Zertifikate

[Virtual Private Network > Zertifikate]

Eine Zertifizierungsstelle (Certification Authority, CA) stellt digitale Zertifikate zur Authentifizierung der Identität von Geräten aus, die einen VPN-Tunnel anfordern. Sie richten die Geräte, die einen VPN-Tunnel bilden, so ein, dass sie der Zertifizierungsstelle (Certification Authority, CA) vertrauen, welche das digitale Zertifikat signiert hat. Das Gerät betrachtet ein von einer Zertifizierungsstelle (Certification Authority, CA) signiertes digitales Zertifikat als gültig. Die Verwendung einer Zertifizierungsstelle (Certification Authority, CA) ermöglicht Ihnen, die auf das Gerät übertragenen digitalen Zertifikate zu erneuern und zu ändern, ohne den VPN-Tunnel zu beeinträchtigen. Voraussetzung ist, dass die tatsächlichen Identitätsinformationen korrekt sind.

Die Verwendung von digitalen Zertifikaten ermöglicht Ihnen außerdem die Reduzierung erforderlicher Wartungsarbeiten. Dies liegt darin begründet, dass Sie digitale Zertifikate seltener als vorinstallierte Schlüssel (Pre-Shared Keys oder auch PSK) ändern. Die Zertifizierungsstelle (Certification Authority, CA) generiert digitale Zertifikate mit Gültigkeitsbeginn und Ablaufdatum. Das digitale Zertifikat ist ausschließlich während dieses Zeitraums gültig. Nach Ablauf eines digitalen Zertifikats benötigt das Gerät ein neues digitales Zertifikat.

Sie generieren mithilfe der Anwendung „strongSwan“ in Verbindung mit dem Linux-Betriebssystem ein selbst signiertes Zertifikat.

Anmerkung: Algorithmen für die RC2 Zertifikatsverschlüsselung werden nicht unterstützt, zum Beispiel PKCS12-Container mit RC2-Verschlüsselung oder Passphrasenschutz.

Tabelle

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

Schaltflächen

 Löschen

Entfernt die ausgewählte Tabellenzeile.


 Hochladen

Öffnet das Fenster , um der Tabelle ein digitale Zertifikat hinzuzufügen.

- Im Feld geben Sie die in diesem digitalen Zertifikat verwendete Passphrase ein.
Mögliche Werte:
 - Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen
- Im Feld legen Sie den Pfad und den Dateinamen des digitalen Zertifikats fest.

Das Gerät bietet Ihnen folgende Möglichkeiten, die Datei auf das Gerät zu übertragen:

- Import vom PC

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

Außerdem können Sie die Datei von Ihrem PC mittels SFTP oder SCP zum Gerät übertragen.

Führen Sie die folgenden Schritte aus:

Öffnen Sie auf Ihrem PC einen SFTP- oder SCP-Client, zum Beispiel WinSCP.

Öffnen Sie mit dem SFTP- oder SCP-Client eine Verbindung zum Gerät.

Übertragen Sie die Datei auf das Gerät in das Verzeichnis `µ-j<°h x-| ›*m-`.

Sobald die Datei vollständig übertragen ist, beginnt das Gerät, das digitale Zertifikat zu installieren. Wenn die Installation erfolgreich war, dann generiert das Gerät eine Datei `<ì` im Verzeichnis `µ-j<°h x-| ›*m-` und löscht die übertragene Datei.

Index

Zeigt den Index der Tabellenzeile des digitalen Zertifikats.

Mögliche Werte:

Dateiname

Zeigt den Namen der auf das Gerät hochgeladenen Datei.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..64 Zeichen

Betreff

Zeigt das Betreff-Feld des digitalen Zertifikats.

Das Betreff-Feld des digitalen Zertifikats enthält eine Kombination der folgenden Angaben: Land (C), Bundesland (ST), Organisation (O), Organisationseinheit (OU), allgemeiner Name (CN) und E-Mail-Adresse des Empfängers (emailAddress).

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

Aussteller

Zeigt den Aussteller des digitalen Zertifikats.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

Gültig ab

Zeigt, seit wann das digitale Zertifikat gültig ist.

Mögliche Werte:

Datums- und Zeitstempel

Gültig bis

Zeigt, wann das digitale Zertifikat ungültig wird.

Mögliche Werte:

Datums- und Zeitstempel

Typ

Zeigt den Typ der verwendeten Container-Datei.

Mögliche Werte:

Die übertragene Datei ist ein digitales Zertifikat, das von einer Zertifizierungsstelle (CA) signiert wurde.

Die übertragene Datei ist ein Peer-Zertifikat.

Die übertragene Datei ist ein p12-Bundle.

Die übertragene Datei ist eine Schlüsseldatei mit Passwortverschlüsselung.

Die übertragene Datei ist ein p12-Bundle mit Passwortverschlüsselung.

Hochgeladen am

Zeigt, wann das digitale Zertifikat zuletzt auf das Gerät übertragen wurde.

Mögliche Werte:

Datums- und Zeitstempel

Private key status

Zeigt den Status des privaten Schlüssels im Peer-Zertifikat. Verwenden Sie ein Peer-Zertifikat mit einem privaten Schlüssel.

Mögliche Werte:

Das Peer-Zertifikat enthält keinen privaten Schlüssel.

Das Gerät hat den privaten Schlüssel gefunden und aus dem Peer-Zertifikat extrahiert.

Das Gerät hat einen privaten Schlüssel ausfindig gemacht. Die Passphrase des Schlüssels fehlt jedoch, und das Gerät hat die Übertragung unterbrochen.

Private Key Datei

Zeigt den Namen der privaten Schlüsseldatei.

Das Gerät ermöglicht Ihnen, alphanumerische Zeichen mit Bindestrichen, Unterstrichen und Punkten einzugeben.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

Aktive Verbindungen

Zeigt die Anzahl der aktiven Verbindungen, welche dieses digitale Zertifikat verwenden.

Das Gerät ermöglicht Ihnen nur dann, das digitale Zertifikat zu löschen, wenn der Wert `0` ist.

Mögliche Werte:

5.3 VPN Verbindungen

[Virtual Private Network > Verbindungen]

Dieser Dialog ermöglicht Ihnen, VPN-Tunnel einzurichten.


Anmerkung: Das Gerät verwendet Software für die Verschlüsselung vom Typ DES- und AES-Galois/Counter-Mode (GCM).


Tabelle

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

Schaltflächen

 Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- In der Dropdown-Liste  wählen Sie eine vorhandene Beschreibung oder legen eine neue Beschreibung fest. Um eine neue Beschreibung einzugeben, klicken Sie das Symbol

.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen

- Im Feld  legen Sie den Index des Traffic-Selektors für den VPN-Tunnel fest.

Mögliche Werte:

–

 Löschen

Entfernt die ausgewählte Tabellenzeile.

 Wizard

Öffnet das Fenster , das Sie dabei unterstützt, die Ports mit der Adresse eines oder mehrerer erwünschter Absender zu verknüpfen. Siehe „[\[Wizard: VPN-Konfiguration\]](#)“ auf Seite 277.

VPN Beschreibung

Legt den benutzerdefinierten Namen für den VPN-Tunnel fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..128 Zeichen

Traffic selector index

Zeigt den Indexwert, der zusammen mit dem Wert in Spalte den Eintrag in der Traffic-Selektor-Tabelle identifiziert.

Mögliche Werte:

Das Gerät ermöglicht Ihnen, einen verfügbaren Wert innerhalb des angegebenen Bereichs festzulegen.

Status

Zeigt, ob der VPN-Tunnel aktiv/inaktiv ist.

Das Gerät beschränkt die maximale Anzahl von eingerichteten VPN-Tunneln auf den im Feld gezeigten Wert. Das Gerät beschränkt außerdem die maximale Anzahl von aktiven VPN-Tunneln auf den im Feld gezeigten Wert.

Mögliche Werte:

Der VPN-Tunnel ist aktiv.
(Voreinstellung)
Der VPN-Tunnel ist inaktiv.

Beschreibung Traffic-Selector

Legt den Namen des Traffic-Selektors fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..128 Zeichen

Quelle Adresse (CIDR)

Legt IP-Adresse und Netzmaske des Quell-Hosts fest. Wenn das Gerät über einen VPN-Tunnel Pakete weiterleitet, welche diese IP-Quelleadresse enthalten, wendet das Gerät die in dieser Tabellenzeile festgelegten Einstellungen an. Außerdem wendet das Gerät die zugehörigen IPsec- und IKE-SA-Einstellungen auf jedes weitergeleitete IP-Paket an, das diese Adresse enthält.

Mögliche Werte:

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation
(Voreinstellung)

Das Gerät wendet die Einstellungen in dieser Tabellenzeile auf jedes durch das Gerät weitergeleitete Datenpaket an.

Quelle Einschränkungen

Legt die optionalen Einschränkungen hinsichtlich der Quellen auf der Grundlage von Namen oder Zahlen fest, die für festgelegt sind. Das Gerät sendet ausschließlich den festgelegten Datentyp durch den VPN-Tunnel.

Beispiele:

- entspricht
- entspricht
- entspricht

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

(Voreinstellung)

Das Gerät verwendet als Einschränkung.

Ziel Adresse (CIDR)

Legt IP-Adresse und Netzmaske des Ziels fest. Wenn das Gerät über einen VPN-Tunnel Pakete weiterleitet, welche diese IP-Zieladresse enthalten, wendet das Gerät die in dieser Tabellenzeile festgelegten Einstellungen an. Außerdem wendet das Gerät für jedes weitergeleitete IP-Paket mit dieser Adresse die zugehörigen IPsec- und IKE-SA-Einstellungen an.

Mögliche Werte:

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

(Voreinstellung)

Das Gerät wendet die Einstellungen in dieser Tabellenzeile auf jedes durch das Gerät weitergeleitete Datenpaket an.

Ziel Einschränkungen

Legt die optionalen Einschränkungen hinsichtlich des Ziels auf der Grundlage von Namen oder Zahlen fest, die für festgelegt sind. Das Gerät erwartet vom VPN-Tunnel ausschließlich den festgelegten Datentyp.

Beispiele:

- entspricht
- entspricht
- entspricht

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

(Voreinstellung)

Das Gerät verwendet als Einschränkung.

Version

Legt die Version des IKE-Protokolls für die VPN-Verbindung fest.

Mögliche Werte:

(Voreinstellung)

Das VPN startet mit dem Protokoll IKEv2 als Initiator und akzeptiert IKEv1/v2 als Responder.

Das VPN startet mit dem Protokoll IKEv1.

Das VPN startet mit dem Protokoll IKEv2.

Startup

Legt fest, ob das Gerät mit dieser Instanz als Responder oder Initiator startet.

Wenn Sie den lokalen Peer als Responder festlegen und der entfernte Peer Datenpakete an einen bestimmten Selektor sendet, versucht das Gerät, als Responder die Verbindung herzustellen. Der Verbindungsaufbau als Responder ist abhängig von weiteren Einstellungen für diese Verbindung. Wenn Sie zum Beispiel im Feld den Wert festlegen, kann das Gerät die Verbindung nicht initiieren.

Mögliche Werte:

Wenn Sie festlegen, dass das Gerät als Initiator startet, dann beginnt das Gerät das Austauschen der Schlüssel mit dem Responder.

(Voreinstellung)

Wenn Sie festlegen, dass das Gerät als Responder startet, dann wartet das Gerät darauf, dass der Initiator mit dem Austauschen der Schlüssel und dem Aushandeln der Parameter beginnt.

DPD Timeout [s]

Legt die Zeitüberschreitung in Sekunden fest, nach welcher der lokale Peer den entfernten Peer als inaktiv erklärt, wenn der inaktive Peer nicht antwortet.

Mögliche Werte:

(Voreinstellung:)

Der Wert 0 deaktiviert diese Funktion. Die Voreinstellung ist 2 Minuten. Maximal können 24 Stunden eingestellt werden.

IKE-Lifetime [s]

Legt die Lebensdauer der IKE Security Association zwischen 2 Netzwerkgeräten in Sekunden zur Sicherung der Kommunikation fest. Die Geräte stellen nach dem Austausch eines Satzes vordefinierter Schlüssel eine Security Association her.

Mögliche Werte:

(Voreinstellung:)

Die Voreinstellung ist 8 Stunden. Maximal können 24 Stunden eingestellt werden.

IKE Exchange Modus

Legt die Verwendung des Exchange Mode Phase 1 für IKEv1 fest.

Die IKE-Phase 1 dient dem Aufbau eines sicheren authentifizierten Kommunikationskanals. Um einen geheimen gemeinsamen Schlüssel (Shared Key) zu generieren, verwendet das Gerät den Diffie-Hellman-Algorithmus für den Schlüsselaustausch. Das Gerät verwendet den geheimen gemeinsamen Schlüssel zur weiteren Verschlüsselung der IKE-Kommunikation.

Mögliche Werte:

(Voreinstellung)

Der Hauptmodus für Phase 1 bietet Identitätsschutz.

Zur Reduzierung von Roundtrips verwenden Sie den Aggressive Mode.

Authentifizierung

Legt den Authentifizierungstyp fest, den das Gerät verwendet.

Mögliche Werte:

(Voreinstellung)

Wählen Sie diesen Wert aus, damit das Gerät einen zuvor generierten und auf den entfernten und lokalen Geräten gespeicherten Schlüssel verwendet.

Wählen Sie diesen Wert, damit das Gerät ein digitales Zertifikat im X.509-Format verwendet. Verwenden Sie ein separates Zertifikat für Zertifizierungsstelle (Certification Authority, CA) und die lokale Identifikation.

Damit das Gerät einen PKCS12-Container mit den erforderlichen digitalen Zertifikaten verwendet, der auch die Zertifizierungsstelle (Certification Authority, CA) einschließt, wählen Sie diesen Wert aus.

Pre-shared Key

Legt den vorinstallierten Schlüssel („Pre-shared Key“) fest. Voraussetzung ist, dass in Spalte der Wert festgelegt ist.

Mögliche Werte:

Alphanumerische ASCII-Zeichenkette mit 0..128 Zeichen, ohne doppelte Anführungszeichen und Zeilenumbruch-Zeichen.

Das Gerät ermöglicht Ihnen außerdem, vorinstallierte geheime Schlüssel als Hexadezimal- oder Base64-kodierte Binärwerte zu generieren. Das Gerät interpretiert eine Zeichenfolge, die mit `0x` beginnt, als eine Abfolge von Hexadezimalziffern. Analog hierzu interpretiert das Gerät eine mit mehreren Nullen beginnende Zeichenfolge als Base64-kodierte Binärdaten.

IKE auth. cert. CA

Legt den Namen der Zertifizierungsstelle (Certification Authority, CA) fest, die das digitale Zertifikat ausstellt hat. Das Gerät verwendet dieses digitale Zertifikat zur Zertifizierung der Signatur der lokalen und entfernten Zertifikate. Voraussetzung ist, dass in Spalte der Wert festgelegt ist.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..128 Zeichen

IKE auth. cert. local

Legt den Dateinamen des digitalen Zertifikats fest, welches das lokale Gerät verwendet. Das Gerät verwendet dieses digitale Zertifikat zur Authentifizierung des lokalen Peers auf der entfernten Seite.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..128 Zeichen

Das Verhalten ist abhängig von dem Wert, den Sie in Spalte festlegen:

—

Das digitale Zertifikat bindet die Identität des lokalen Peers an den festgelegten öffentlichen Schlüssel, den die in Spalte festgelegte Zertifizierungsstelle (Certification Authority, CA) signiert hat.

—

Das digitale Zertifikat im PKCS-Bündel bindet die Identität der lokalen Gegenstelle an den festgelegten öffentlichen Schlüssel. Das Gerät führt diese Prüfung unabhängig von dem digitalen Zertifikat durch, das die Spalte anzeigt.

IKE auth. cert. remote

Legt den Dateinamen des digitalen Zertifikats fest, welches das entfernte Gerät verwendet. Das Gerät verwendet dieses digitale Zertifikat für die Authentifizierung des entfernten Peers auf der lokalen Seite. Dieses digitale Zertifikat verknüpft die Identität des entfernten Peers mit dem festgelegten öffentlichen Schlüssel. Voraussetzung ist, dass in Spalte der Wert festgelegt ist.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen

Der Wert ist optional, da in der Regel der entfernte Peer das digitale Zertifikat sendet und das Gerät ausschließlich die Gültigkeit des digitalen Zertifikats prüft.

Encrypted private key

Legt den Dateinamen für den privaten Schlüssel fest.

Voraussetzungen:

- In Spalte ist der Wert festgelegt.
- Der im Gerät gespeicherte Schlüssel wird mit einer Passphrase verschlüsselt.

Der Schlüssel erfordert, dass Sie in Spalte die Passphrase festlegen. Das Gerät betrachtet den Schlüssel und das digitale Zertifikat als nicht übereinstimmend, bis der Schlüssel entschlüsselt wird.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen

Verschlüsselter Key/PKCS12-Passphrase

Legt die Passphrase fest, die das Gerät für die Entschlüsselung des privaten Schlüssels verwendet, der in Spalte oder im -Zertifikat-Container festgelegt ist.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen

IKE Local-Identifizier Typ

Legt den Typ der lokalen Peer-Kennung fest, die das Gerät für den Parameter verwendet.

Mögliche Werte:

(Voreinstellung)

Das Verhalten ist abhängig von dem Wert, den Sie in Spalte festlegen:

- Das Gerät verwendet die in Spalte festgelegte IP-Adresse als lokale Kennung.
- oder
- Das Gerät verwendet den im lokalen -Zertifikat enthaltenen Distinguished Name (DN).

In Spalte verwendet das Gerät die IP-Adresse oder den Hostnamen aus Spalte

Das Gerät identifiziert den in Spalte festgelegten Wert als einen der folgenden Typen:

- eine IPv4-Adresse oder ein DNS-Hostname
- Schlüsselbezeichner, der festlegt, welche Daten das Gerät zur Weitergabe von hersteller-spezifischen Informationen verwendet. Das Gerät verwendet die Informationen, um zu identifizieren, welchen vorinstallierten Schlüssel (Pre-shared key) das Gerät für die Aggressive-Mode-Authentifizierung bei Verhandlungen verwendet.
- eine Web-Adresse mit FQDN, zum Beispiel
- eine E-Mail-Adresse
- Den in Spalte enthaltenen ASN.1 X.500 Distinguished Name (DN). Die lokalen und entfernten Geräte tauschen ihre digitalen Zertifikate aus, um die security asso-
□□□□□□ aufzubauen. □□□□□□□□□□

IKE local ID

Legt die lokale Peer-Kennung fest, die das Gerät während der Phase-1-Verhandlungen in der ID-Nutzlast an das entfernte Gerät sendet. Das Gerät verwendet die ID-Nutzlast, um den Initiator der Security Association (SA) zu identifizieren. Der Responder verwendet die Identität zur Ermittlung der korrekten Anforderung im Zusammenhang mit den Host-Systemrichtlinien für die SA.

Die Formate für diesen Parameter sind abhängig vom Wert, der in Spalte festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Wenn Sie in Spalte den Wert festlegen, dann legen Sie den Wert unter Verwendung einer der folgenden Möglichkeiten fest:

- eine IPv4-Adresse oder ein DNS-Hostname
- Ein zuvor definierter Schlüsselbezeichner, der Daten festlegt, die das Gerät zur Weitergabe von herstellereigenen Informationen verwendet.
- eine Web-Adresse mit FQDN, zum Beispiel
- eine E-Mail-Adresse
- Ein X.500 Distinguished Name

Benutzen Sie zum Hinzufügen eines Eintrags die folgende Syntax als Beispiel:

Ferner Identifier Typ

Legt den Typ der entfernten Peer-Kennung fest, die das Gerät für den Parameter verwendet. ver-

Mögliche Werte:

(Voreinstellung)

Das Gerät akzeptiert jede empfangene Kennung ohne weitergehende Überprüfung.

In Spalte verwendet das Gerät die IP-Adresse oder den Hostnamen aus Spalte

Das Gerät identifiziert den in Spalte festgelegten Wert als einen der folgenden Typen:

- eine IPv4-Adresse oder ein DNS-Hostname
- Schlüsselbezeichner, der festlegt, welche Daten das Gerät zur Weitergabe von herstellereigenen Informationen verwendet. Das Gerät verwendet die Informationen, um festzustellen, welchen vorinstallierten Schlüssel (Pre-shared Key) das Gerät für die Authentifizierung im Aggressive-Mode während Phase-1-Aushandlungen verwendet.
- eine Web-Adresse mit FQDN, zum Beispiel
- eine E-Mail-Adresse
- Den in Spalte enthaltenen ASN.1 X.500 Distinguished Name (DN). Die lokalen und entfernten Geräte tauschen ihre digitalen Zertifikate aus, um die SA aufzubauen.

Remote-ID

Legt die Kennung für den entfernten Peer fest, die das Gerät während Phase-1-Verhandlungen mit dem Wert für die ID-Nutzlast vergleicht. Das Gerät verwendet die ID-Nutzlast zur Identifizierung des Initiators der SA. Der Responder verwendet die Identität zur Ermittlung der korrekten Anforderung im Zusammenhang mit den Host-Systemrichtlinien für die SA.

Die Formate für diesen Parameter sind abhängig vom Wert, der in Spalte festgelegt ist. fest-

Mögliche Werte:

(Voreinstellung)

Wenn Sie in Spalte den Wert festlegen, dann legen Sie den Wert unter Verwendung einer der folgenden Möglichkeiten fest:

- eine IPv4-Adresse oder ein DNS-Hostname
- Ein zuvor definierter Schlüsselbezeichner, der Daten festlegt, die das Gerät zur Weitergabe von herstellerspezifischen Informationen verwendet.
- eine Web-Adresse mit FQDN, zum Beispiel
- eine E-Mail-Adresse
- Ein X.500 Distinguished Name

Benutzen Sie zum Hinzufügen eines Eintrags die folgende Syntax als Beispiel:

IKE key agreement

Legt fest, welchen Diffie-Hellman- (DH-) Algorithmus zur Schlüsselvereinbarung das Gerät zur Ermittlung des IKE-SA-Sitzungsschlüssels verwendet.

Mögliche Werte:

Das Gerät akzeptiert jeden Algorithmus, wenn das Gerät als Responder festgelegt wurde.

(Voreinstellung)

Der Wert stellt einen RSA-Algorithmus mit 1024-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 2 gehört.

Der Wert stellt einen RSA-Algorithmus mit 1536-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 5 gehört.

Der Wert stellt einen RSA-Algorithmus mit 2048-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 14 gehört.

Der Wert stellt einen RSA-Algorithmus mit 3072-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 15 gehört.

Der Wert stellt einen RSA-Algorithmus mit 4096-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 16 gehört.

IKE integrity (MAC)

Legt fest, welchen Message Authentication Code- (MAC-) Algorithmus das Gerät für die IKE-Integrität verwendet. Um die Dateien im VPN zu sichern, mischt (hasht) der Hash-based Message Authentication Code- (HMAC-) Prozess im sendenden Gerät die Nachrichtendaten mit einem gemeinsamen geheimen Schlüssel. Das empfangende Gerät mischt die Ergebnisse (Hash-Wert) erneut mit dem geheimen Schlüssel und wendet anschließend die Hash-Funktion ein 2. Mal an.

Mögliche Werte:

Wenn Sie das Gerät als Responder festlegen, akzeptiert das Gerät jeden Algorithmus. Wenn Sie das Gerät als Initiator festlegen, verwendet das Gerät verschiedene vordefinierte Algorithmen.

Das Gerät verwendet den Message-Digest-Algorithmus 5 (MD5) zur Berechnung der Hash-Funktion.

(Voreinstellung)

Das Gerät verwendet den Secure-Hash-Algorithmus Version 1 (SHA-1) zur Berechnung der Hash-Funktion.

Das Gerät verwendet SHA-256 (Teil der Version-2-Familie) zur Berechnung der Hash-Funktion, die das Gerät mit 32-Bit-Wörtern berechnet.

Das Gerät verwendet SHA-384 (Teil der Version-2-Familie) zur Berechnung der Hash-Funktion, die das Gerät auf der Grundlage einer kürzeren Version von SHA-512 berechnet.

Das Gerät verwendet SHA-512 (Teil der Version-2-Familie) zur Berechnung der Hash-Funktion, die das Gerät mit 64-Bit-Wörtern berechnet.

Anmerkung: Wir empfehlen, die Einstellung oder höher zu verwenden.

IKE encryption

Legt den IKE-Verschlüsselungsalgorithmus fest, den das Gerät verwendet.

Mögliche Werte:

Wenn Sie das Gerät als Responder festlegen, akzeptiert das Gerät jeden Algorithmus. Wenn Sie das Gerät als Initiator festlegen, verwendet das Gerät verschiedene vordefinierte Algorithmen.

Das Gerät verwendet die Data-Encryption-Standard- (DES)-Blockchiffre für die Verschlüsselung von Nachrichtendaten mit einem 56-Bit-Schlüssel.

Das Gerät verwendet die Triple-DES-Blockchiffre für die Verschlüsselung von Nachrichtendaten, die den 56-Bit-Schlüssel des DES 3 Mal pro Block anwendet.

(Voreinstellung)

Das Gerät verwendet Advanced Encryption Standard (AES) mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 128 Key-Bits.

Das Gerät verwendet AES mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 192 Key-Bits.

Das Gerät verwendet AES mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 256 Key-Bits.

Anmerkung: Wir empfehlen, die Einstellung oder höher zu verwenden.

Lokaler Endpunkt

Legt den Hostnamen oder die IP-Adresse des lokalen IPsec-VPN-Tunnel-Endpunktes fest.

Mögliche Werte:

(Voreinstellung)

Das Gerät verwendet die IP-Adresse des Interfaces, welches das Gerät zur Weiterleitung von Daten zum entfernten Endpunkt verwendet.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Hostname

Alphanumerische ASCII-Zeichenfolge mit 1..128 Zeichen

Ferner Endpunkt

Legt den Hostnamen oder die IP-Adresse des entfernten IPsec-VPN-Tunnel-Endpunktes fest.

Mögliche Werte:

(Voreinstellung)

Das Gerät akzeptiert jede IP-Adresse während der Einrichtung einer IKE-SA als VPN-Responder.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Wenn Sie festlegen, dass das Gerät für diesen VPN-Tunnel der Responder ist, akzeptiert das Gerät während der IKE-SA-Einrichtung ein Netz in CIDR-Notation.

Hostname

Alphanumerische ASCII-Zeichenfolge mit 1..128 Zeichen

Re-authentication

Aktiviert/deaktiviert die Peer-Neuauthentifizierung nach einer IKE-SA-Schlüssel-Erzeugung. Wenn Sie in Spalte den Wert festlegen, dann nimmt das Gerät stets die erneute Authentifizierung des VPN-Tunnels vor, selbst wenn Sie die Markierung des Kontrollkästchens aufheben.

Mögliche Werte:

Das Gerät generiert eine neue IKE-SA und versucht, die IPsec SAs erneut zu generieren.

(Voreinstellung)

Wenn Sie das Protokoll IKEv2 verwenden, führt das Gerät für den VPN-Tunnel eine Schlüssel-Generierung aus und behält die IPsec SAs bei.

IPsec key agreement

Legt fest, welchen Diffie-Hellman-Algorithmus zur Schlüsselvereinbarung das Gerät zur Ermittlung des IPsec-SA-Sitzungsschlüssels verwendet. Bei aktivierter Perfect Forward Secrecy (PFS)-Funktion bleibt die Integrität von später generierten Schlüsseln erhalten, wenn die Kompromittierung eines Einzelschlüssels vorliegt.

Mögliche Werte:

Wenn Sie das Gerät als Responder festlegen, akzeptiert das Gerät jeden Algorithmus. Wenn Sie das Gerät als Initiator festlegen, verwendet das Gerät verschiedene vordefinierte Algorithmen.

(Voreinstellung)

Der Wert stellt einen Rivest, Shamir und Adleman (RSA)-Algorithmus mit 1024-Bit-Modulus dar. Dieser Wert gehört zur Diffie-Hellman- (DH)-Gruppe 2.

Der Wert stellt einen RSA-Algorithmus mit 1536-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 5 gehört.

Der Wert stellt einen RSA-Algorithmus mit 2048-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 14 gehört.

Der Wert stellt einen RSA-Algorithmus mit 3072-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 15 gehört.

Der Wert stellt einen RSA-Algorithmus mit 4096-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 16 gehört.

Das Gerät schaltet die Funktion PFS aus. Das Ausschalten der Funktion PFS wird als Verletzung der Vertraulichkeit und daher als ein Sicherheitsrisiko betrachtet.

IPsec integrity (MAC)

Legt den Algorithmus für die IPsec-Integrität (MAC) fest, den das Gerät für die Instanz verwendet. Um die Dateien im VPN zu sichern, mischt (hasht) der Hash-based Message Authentication Code (HMAC-) Prozess im sendenden Gerät die Nachrichtendaten mit einem gemeinsamen geheimen Schlüssel. Das empfangende Gerät mischt die Ergebnisse (Hash-Wert) erneut mit dem geheimen Schlüssel und wendet anschließend die Hash-Funktion ein 2. Mal an.

Mögliche Werte:

Wenn Sie das Gerät als Responder festlegen, akzeptiert das Gerät jeden Algorithmus. Wenn Sie das Gerät als Initiator festlegen, verwendet das Gerät verschiedene vordefinierte Algorithmen.

Das Gerät verwendet den Message-Digest-Algorithmus 5 (MD5) zur Berechnung der Hash-Funktion.

(Voreinstellung)

Das Gerät verwendet den Secure-Hash-Algorithmus Version 1 (SHA-1) zur Berechnung der Hash-Funktion.

Das Gerät verwendet SHA-256 (Teil der Version-2-Familie) zur Berechnung der Hash-Funktion, die das Gerät mit 32-Bit-Wörtern berechnet.

Das Gerät verwendet SHA-384 (Teil der Version-2-Familie) zur Berechnung der Hash-Funktion, die das Gerät auf der Grundlage einer kürzeren Version von SHA-512 berechnet.

Das Gerät verwendet SHA-512 (Teil der Version-2-Familie) zur Berechnung der Hash-Funktion, die das Gerät mit 64-Bit-Wörtern berechnet.

Anmerkung: Wir empfehlen, die Einstellung oder höher zu verwenden.

IPsec encryption

Legt den IPsec-Verschlüsselungsalgorithmus fest, den das Gerät verwendet.

Mögliche Werte:

Wenn Sie das Gerät als Responder festlegen, akzeptiert das Gerät jeden Algorithmus. Wenn Sie das Gerät als Initiator festlegen, verwendet das Gerät verschiedene vordefinierte Algorithmen.

Das Gerät verwendet die Data-Encryption-Standard- (DES)-Blockchiffre für die Verschlüsselung von Nachrichtendaten mit einem 56-Bit-Schlüssel.

Das Gerät verwendet die Triple-DES-Blockchiffre für die Verschlüsselung von Nachrichtendaten, die den 56-Bit-Schlüssel des DES 3 Mal pro Block anwendet.

(Voreinstellung)

Das Gerät verwendet Advanced Encryption Standard (AES) mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 128 Key-Bits.

Das Gerät verwendet AES mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 192 Key-Bits.

Das Gerät verwendet AES mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 256 Key-Bits.

AES-CTR mit 128 Key-Bits.

AES-CTR mit 192 Key-Bits.

AES-CTR mit 256 Key-Bits.

Das Gerät verwendet AES-Galois/Counter Mode (GCM) mit einem 64-Bit-ICV (Integrity Check Value) und 128 Key-Bits.

AES-GCM mit einem 96-Bit-ICV und 128 Key-Bits.

AES-GCM mit einem 128-Bit-ICV und 128 Key-Bits.

AES-GCM mit einem 64-Bit-ICV und 192 Key-Bits.

AES-GCM mit einem 96-Bit-ICV und 192 Key-Bits.

AES-GCM mit einem 128-Bit-ICV und 192 Key-Bits.

AES-GCM mit einem 64-Bit-ICV und 256 Key-Bits.

AES-GCM mit einem 96-Bit-ICV und 256 Key-Bits.

AES-GCM mit einem 128-Bit-ICV und 256 Key-Bits.

Anmerkung: Wir empfehlen, die Einstellung oder höher zu verwenden.

IPsec lifetime [s]

Legt die Lebensdauer der IPsec Security Association zwischen 2 Netzwerkgeräten in Sekunden zur Sicherung der Kommunikation fest. Die Geräte stellen nach dem Austausch eines Satzes vordefinierter Schlüssel eine Security Association her.

Mögliche Werte:

(Voreinstellung:)

Die Voreinstellung ist eine Stunde. Maximal können 8 Stunden eingestellt werden.

Margin-Time [s]

Legt die Zeitspanne in Sekunden vor Ablauf der und der fest, nach der das Gerät mit dem Aushandeln eines neuen Schlüssels beginnt.

Mögliche Werte:

(Voreinstellung:)

Die Voreinstellung entspricht 2,5 Minuten. Der Maximalwert beträgt eine halbe Stunde.

Log informational entries

Aktiviert/deaktiviert Protokolleinträge ausschließlich für die Fehlersuche.

Mögliche Werte:

Das Gerät empfängt und verarbeitet die Informationsnachrichten für diesen VPN-Tunnel und trägt die Nachricht in das Ereignisprotokoll ein.

(Voreinstellung)

Das Gerät empfängt und verarbeitet die Informationsnachrichten für diese Verbindung ohne einen Eintrag in das Ereignisprotokoll.

Log unhandled messages

Aktiviert/deaktiviert die Nachrichtenverarbeitung für Nachrichten, die strongSwan nicht bekannt sind, ausschließlich im Rahmen der Fehlersuche.

Mögliche Werte:

Das Gerät trägt die für diese Verbindung empfangenen Nachrichten, die nicht von strongSwan stammen, in das Ereignisprotokoll ein.

(Voreinstellung)

Das Gerät ignoriert sonstige für diese Verbindung empfangene Nachrichten, die nicht von strongSwan stammen.

[Wizard: VPN-Konfiguration]

Im Fenster ermöglicht Ihnen, einen VPN-Tunnel einzurichten. Das Gerät ermöglicht Ihnen außerdem, direkt über den Dialog einen VPN-Tunnel hinzuzufügen oder zu ändern.

Das Fenster führt Sie durch die folgenden Schritte:

- [Eintrag erstellen oder auswählen](#)
- [Authentifizierung](#)
- [Endpoint and traffic selectors](#)
- [Advanced configuration](#)

Eintrag erstellen oder auswählen

VPN

Zeigt die vorhandenen VPN-Tunnel, die im Gerät eingerichtet sind. Wählen Sie einen Eintrag, um fortzufahren. Alternativ dazu legen Sie in den Feldern und einen VPN-Tunnel fest.

VPN index

Legt die Index-Nummer für den VPN-Tunnel fest.

Mögliche Werte:

VPN Beschreibung

Legt die benutzerdefinierte Beschreibung für den VPN-Tunnel fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..128 Zeichen


Authentifizierung

In den folgenden Registerkarten können Sie für jeden VPN-Tunnel die Authentifizierungsmethoden festlegen:

- [Authentifizierung - Pre-shared Key](#)

Authentifizierung - Pre-shared Key

Pre-shared Key

Legt den vorinstallierten Schlüssel („Pre-shared Key“) fest. Sie können die festgelegten Werte anzeigen, indem Sie das Symbol  klicken.

Mögliche Werte:

Alphanumerische ASCII-Zeichenkette mit 0..128 Zeichen, ohne doppelte Anführungszeichen und Zeilenumbruch-Zeichen.

Das Gerät ermöglicht Ihnen außerdem, vorinstallierte geheime Schlüssel als Hexadezimal- oder Base64-kodierte Binärwerte zu generieren. Das Gerät interpretiert eine Zeichenfolge, die mit `0x` beginnt, als Folge aus Hexadezimalziffern. Analog hierzu interpretiert das Gerät eine mit mehreren Nullen beginnende Zeichenfolge als Base64-kodierte Binärdaten.

Authentifizierung - X.509

IKE auth. cert. local

Legt den Namen des im digitalen Zertifikat eingetragenen lokalen Peers fest. Das Gerät verwendet dieses digitale Zertifikat zur Authentifizierung des lokalen Peers auf der entfernten Seite. Das digitale Zertifikat bindet die Identität des lokalen Peers an den festgelegten öffentlichen Schlüssel, den die im Feld festgelegte Zertifizierungsstelle (CA) signiert hat.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..128 Zeichen

IKE auth. cert. CA

Legt den Namen der Zertifizierungsstelle (Certification Authority, CA) fest, die das digitale Zertifikat signiert hat. Das Gerät verwendet dieses digitale Zertifikat zur Zertifizierung der Signatur der lokalen und entfernten Zertifikate.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..128 Zeichen


Encrypted private key

Legt den Dateinamen für den privaten Schlüssel fest. Voraussetzung ist, dass der im Gerät gespeicherte Schlüssel mit einer Passphrase verschlüsselt ist. Der Schlüssel erfordert, dass Sie im Feld die Passphrase festlegen. Das Gerät betrachtet den Schlüssel und das digitale Zertifikat als nicht übereinstimmend, bis der Schlüssel entschlüsselt wird.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen

Verschlüsselter Key/PKCS12-Passphrase

Legt die Passphrase fest, die das Gerät für die Entschlüsselung des privaten Schlüssels verwendet, der im Feld festgelegt ist. Sie können die Passphrase anzeigen, indem Sie das Symbol  klicken.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen

Authentifizierung - PKCS 12


IKE auth. cert. local

Legt den Namen des im digitalen Zertifikat eingetragenen lokalen Peers fest. Das Gerät verwendet dieses digitale Zertifikat zur Authentifizierung des lokalen Peers auf der entfernten Seite.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..128 Zeichen

Verschlüsselter Key/PKCS12-Passphrase

Legt die Passphrase fest, die das Gerät für die Entschlüsselung des privaten Schlüssels verwendet, der im Feld festgelegt ist. Sie können die Passphrase anzeigen, indem Sie das Symbol  klicken.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen

Endpoint and traffic selectors

Lokaler Endpunkt

Legt den Hostnamen oder die IP-Adresse des lokalen IPsec-VPN-Tunnel-Endpunktes fest.

Mögliche Werte:

(Voreinstellung)

Das Gerät verwendet die IP-Adresse des Interfaces, welches das Gerät zur Weiterleitung von Daten zum entfernten Endpunkt verwendet.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Hostname

Alphanumerische ASCII-Zeichenfolge mit 1..128 Zeichen

Ferner Endpunkt

Legt den Hostnamen oder die IP-Adresse des entfernten IPsec-VPN-Tunnel-Endpunktes fest.

Mögliche Werte:

(Voreinstellung)

Das Gerät akzeptiert jede IP-Adresse während der Einrichtung einer IKE-SA als VPN-Responder.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Wenn Sie festlegen, dass das Gerät für diesen VPN-Tunnel der Responder ist, akzeptiert das Gerät während der IKE-SA-Einrichtung ein Netz in CIDR-Notation.

Hostname

Alphanumerische ASCII-Zeichenfolge mit 1..128 Zeichen

Add traffic selector

Beschreibung Traffic-Selector

Legt die benutzerdefinierte Beschreibung für den Traffic-Selektor fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..128 Zeichen

Quelle Adresse (CIDR)

Legt IP-Adresse und Netzmaske des Quell-Hosts fest. Wenn das Gerät über einen VPN-Tunnel Pakete weiterleitet, welche diese IP-Quelleadresse enthalten, wendet das Gerät die in diesem Feld festgelegten Einstellungen an. Außerdem wendet das Gerät die zugehörigen IPsec- und IKE-SA-Einstellungen auf jedes weitergeleitete IP-Paket an, das die -IP-Quelleadresse in dem Bereich enthält, der durch die IP-Quelleadresse und die Netzmaske festgelegt ist.

Mögliche Werte:

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation
(Voreinstellung)

Das Gerät wendet die Einstellungen auf jedes durch das Gerät weitergeleitete Datenpaket an.

Quelle Einschränkungen

Legt die optionalen Einschränkungen hinsichtlich der Quellen auf der Grundlage von Namen oder Zahlen fest, die für festgelegt sind. Das Gerät sendet ausschließlich den festgelegten Datentyp durch den VPN-Tunnel.

Beispiele:

- entspricht
- entspricht
- entspricht

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen
(Voreinstellung)

Das Gerät verwendet als Einschränkung.

Ziel Adresse (CIDR)

Legt IP-Adresse und Netzmaske des Ziels fest. Wenn das Gerät über einen VPN-Tunnel Pakete weiterleitet, welche diese IP-Zieladresse enthalten, wendet das Gerät die in diesem Feld festgelegten Einstellungen an. Außerdem wendet das Gerät die zugehörigen IPsec- und IKE-SA-Einstellungen auf jedes weitergeleitete IP-Paket an, das die IP-Zieladresse in dem Bereich enthält, der durch die IP-Zieladresse und die Netzmaske festgelegt ist.

Mögliche Werte:

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation
(Voreinstellung)

Das Gerät wendet die Einstellungen auf jedes durch das Gerät weitergeleitete Datenpaket an.

Ziel Einschränkungen

Legt die optionalen Einschränkungen hinsichtlich des Ziels auf der Grundlage von Namen oder Zahlen fest, die für festgelegt sind. Das Gerät erwartet vom VPN-Tunnel ausschließlich den festgelegten Datentyp.

Beispiele:

- entspricht
- entspricht
- entspricht

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen
(Voreinstellung:)
Das Gerät verwendet als Einschränkung.



Entfernt die betreffende Tabellenzeile.

Hinzufügen

Fügt in der Tabelle eine Tabellenzeile hinzu.

Advanced configuration

In den folgenden Registerkarten können Sie für jeden VPN-Tunnel die Parameter festlegen:

- [Advanced configuration - Allgemein](#)

Advanced configuration - Allgemein

Margin-Time [s]

Legt die Zeit in Sekunden vor dem Ablauf der Verbindung oder des Kanals zur Schlüsselgenerierung fest. Anschließend versucht das Gerät, einen Austausch zu verhandeln.

Mögliche Werte:

(Voreinstellung:)
Die Voreinstellung entspricht 2,5 Minuten. Der Maximalwert beträgt eine halbe Stunde.

Advanced configuration - IKE/Key-exchange

Version

Legt die Version des IKE-Protokolls für die VPN-Verbindung fest.

Mögliche Werte:

(Voreinstellung)

Das VPN startet mit dem Protokoll IKEv2 als Initiator und akzeptiert IKEv1/v2 als Responder.

Das VPN startet mit dem Protokoll IKEv1 (ISAKMP).

Das VPN startet mit dem Protokoll IKEv2.

Startup

Legt fest, ob das Gerät mit dieser Instanz als Responder oder Initiator startet.

Mögliche Werte:

Das Gerät beginnt das Austauschen der Schlüssel mit dem Responder.

(Voreinstellung)

Das Gerät wartet auf den Initiator, um mit dem Austauschen der Schlüssel und dem Aushandeln der Parameter zu beginnen.

Wenn der entfernte Peer Datenpakete an einen bestimmten Selektor sendet, versucht das Gerät, als Responder die Verbindung herzustellen. Der Verbindungsaufbau als Responder ist abhängig von weiteren Einstellungen für diese Verbindung. Wenn Sie zum Beispiel im Feld den Wert festlegen, dann unterbindet das Gerät das entfernte Gerät daran, die Verbindung zu initiieren.

DPD Timeout [s]

Legt die Zeitüberschreitung in Sekunden fest, nach welcher der lokale Peer den entfernten Peer als inaktiv erklärt, wenn der inaktive Peer nicht antwortet.

Mögliche Werte:

Deaktiviert das Timeout.

(Voreinstellung:)

Die Voreinstellung ist 2 Minuten. Maximal können 24 Stunden eingestellt werden.

IKE-Lifetime [s]

Legt die Lebensdauer der IKE Security Association zwischen 2 Netzwerkgeräten in Sekunden zur Sicherung der Kommunikation fest. Die Geräte stellen nach dem Austausch eines Satzes vordefinierter Schlüssel eine Security Association her.

Mögliche Werte:

(Voreinstellung:)

Die Voreinstellung ist 8 Stunden. Maximal können 24 Stunden eingestellt werden.

IKE Local-Identifizier Typ

Legt den Typ der lokalen Peer-Kennung fest, die das Gerät für den Parameter verwendet. verwendet.

Mögliche Werte:

(Voreinstellung)

Das Verhalten ist abhängig von dem Wert, den Sie für die folgenden Authentifizierungsmethoden festlegen:

- Das Gerät verwendet die im Feld festgelegte IP-Adresse als lokale Kennung. Sie finden das Feld im Abschnitt „Endpoint and traffic selectors“ auf Seite 280.
- oder
- Das Gerät verwendet den im lokalen -Zertifikat enthaltenen Distinguished Name (DN).

Im Feld verwendet das Gerät die IP-Adresse oder den Hostnamen aus Feld . Sie finden das Feld im Abschnitt „Endpoint and traffic selectors“ auf Seite 280.

Das Gerät identifiziert den im Feld festgelegten Wert als einen der folgenden Typen:

- eine IPv4-Adresse oder ein DNS-Hostname
- Schlüsselbezeichner, der festlegt, welche Daten das Gerät zur Weitergabe von herstellereigenen Informationen verwendet. Das Gerät verwendet die Informationen, um zu identifizieren, welchen vorinstallierten Schlüssel (Pre-shared key) das Gerät für die Aggressive-Mode-Authentifizierung bei Verhandlungen verwendet.
- eine Web-Adresse mit FQDN, zum Beispiel
- eine E-Mail-Adresse
- Den im Feld enthaltenen ASN.1 X.500 Distinguished Name (DN). Die lokalen und entfernten Geräte tauschen ihre digitalen Zertifikate aus, um die Security-Association (SA) aufzubauen.

IKE local ID

Legt die lokale Peer-Kennung fest, die das Gerät während der Phase-1-Verhandlungen in der ID-Nutzlast an das entfernte Gerät sendet. Das Gerät verwendet die ID-Nutzlast, um den Initiator der Security Association (SA) zu identifizieren. Der Responder verwendet die Identität zur Ermittlung der korrekten Anforderung im Zusammenhang mit den Host-Systemrichtlinien für die Security Association (SA).

Die Formate für diesen Parameter sind abhängig vom Wert, der im Feld festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Wenn Sie im Feld den Wert festlegen, dann legen Sie den Wert unter Verwendung einer der folgenden Möglichkeiten fest:

- eine IPv4-Adresse oder ein DNS-Hostname
 - Ein zuvor definierter Schlüsselbezeichner, der Daten festlegt, die das Gerät zur Weitergabe von herstellereigenen Informationen verwendet.
 - eine Web-Adresse mit FQDN, zum Beispiel
 - eine E-Mail-Adresse
 - Ein X.500 Distinguished Name
- Benutzen Sie zum Hinzufügen eines Eintrags die folgende Syntax als Beispiel:

Ferner Identifier Typ

Legt den Typ der entfernten Peer-Kennung fest, die das Gerät für den Parameter verwendet. verwendet.

Mögliche Werte:

(Voreinstellung)

Das Gerät akzeptiert jede empfangene Kennung ohne weitergehende Überprüfung.

Im Feld verwendet das Gerät die IP-Adresse oder den Hostnamen aus Feld . Sie finden das Feld im Abschnitt „Endpoint and traffic selectors“ auf Seite 280.

Das Gerät identifiziert den im Feld festgelegten Wert als einen der folgenden Typen:

- eine IPv4-Adresse oder ein DNS-Hostname
- Schlüsselbezeichner, der festlegt, welche Daten das Gerät zur Weitergabe von herstellere-spezifischen Informationen verwendet. Das Gerät verwendet die Informationen, um zu identifizieren, welchen vorinstallierten Schlüssel (Pre-shared key) das Gerät für die Aggressive-Mode-Authentifizierung bei Verhandlungen verwendet.
- eine Web-Adresse mit FQDN, zum Beispiel
- eine E-Mail-Adresse
- Den im Feld enthaltenen ASN.1 X.500 Distinguished Name (DN). Die lokalen und entfernten Geräte tauschen ihre digitalen Zertifikate aus, um die SA aufzubauen.

Remote-ID

Legt die Kennung für den entfernten Peer fest, die das Gerät während Phase-1-Verhandlungen mit dem Wert für die ID-Nutzlast vergleicht. Das Gerät verwendet die ID-Nutzlast zur Identifizierung des Initiators der SA. Der Responder verwendet die Identität zur Ermittlung der korrekten Anforderung im Zusammenhang mit den Host-Systemrichtlinien für die SA.

Die Formate für diesen Parameter sind abhängig vom Wert, der im Feld festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Wenn Sie im Feld den Wert festlegen, dann legen Sie den Wert unter Verwendung einer der folgenden Möglichkeiten fest:

- eine IPv4-Adresse oder ein DNS-Hostname
- Ein zuvor definierter Schlüsselbezeichner, der Daten festlegt, die das Gerät zur Weitergabe von herstellere-spezifischen Informationen verwendet.
- eine Web-Adresse mit FQDN, zum Beispiel
- eine E-Mail-Adresse
- Ein X.500 Distinguished Name

Benutzen Sie zum Hinzufügen eines Eintrags die folgende Syntax als Beispiel:

IKE Exchange Modus

Legt die Verwendung des Exchange Mode Phase 1 für IKEv1 fest.

Die IKE-Phase 1 dient dem Aufbau eines sicheren authentifizierten Kommunikationskanals. Um einen geheimen gemeinsamen Schlüssel (Shared Key) zu generieren, verwendet das Gerät den Diffie-Hellman- (DH-) Algorithmus für den Schlüsselaustausch. Das Gerät verwendet den geheimen gemeinsamen Schlüssel zur weiteren Verschlüsselung der IKE-Kommunikation.

Mögliche Werte:

(Voreinstellung)

Der Hauptmodus für Phase 1 bietet Identitätsschutz.

Zur Reduzierung von Roundtrips verwenden Sie den Aggressive Mode.

IKE key agreement

Legt fest, welchen Diffie-Hellman- (DH-) Algorithmus zur Schlüsselvereinbarung das Gerät zur Ermittlung des IKE-SA-Sitzungsschlüssels verwendet.

Mögliche Werte:

Das Gerät akzeptiert jeden Algorithmus, wenn das Gerät als Responder festgelegt wurde.

(Voreinstellung)

Der Wert stellt einen RSA-Algorithmus mit 1024-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 2 gehört.

Der Wert stellt einen RSA-Algorithmus mit 1536-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 5 gehört.

Der Wert stellt einen RSA-Algorithmus mit 2048-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 14 gehört.

Der Wert stellt einen RSA-Algorithmus mit 3072-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 15 gehört.

Der Wert stellt einen RSA-Algorithmus mit 4096-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 16 gehört.

IKE integrity (MAC)

Legt fest, welchen Message Authentication Code- (MAC-) Algorithmus das Gerät für die IKE-Integrität verwendet. Um die Dateien im VPN zu sichern, mischt (hasht) der Hash-based Message Authentication Code- (HMAC-) Prozess im sendenden Gerät die Nachrichtendaten mit einem gemeinsamen geheimen Schlüssel. Das empfangende Gerät mischt die Ergebnisse (Hash-Wert) erneut mit dem geheimen Schlüssel und wendet anschließend die Hash-Funktion ein 2. Mal an.

Mögliche Werte:

Wenn Sie das Gerät als Responder festlegen, akzeptiert das Gerät jeden Algorithmus. Wenn Sie das Gerät als Initiator festlegen, verwendet das Gerät verschiedene vordefinierte Algorithmen.

Das Gerät verwendet den Message-Digest-Algorithmus 5 (MD5) zur Berechnung der Hash-Funktion.

(Voreinstellung)

Das Gerät verwendet den Secure-Hash-Algorithmus Version 1 (SHA-1) zur Berechnung der Hash-Funktion.

Das Gerät verwendet SHA-256 (Teil der Version-2-Familie) zur Berechnung der Hash-Funktion, die das Gerät mit 32-Bit-Wörtern berechnet.

Das Gerät verwendet SHA-384 (Teil der Version-2-Familie) zur Berechnung der Hash-Funktion, die das Gerät auf der Grundlage einer kürzeren Version von SHA-512 berechnet.

Das Gerät verwendet SHA-512 (Teil der Version-2-Familie) zur Berechnung der Hash-Funktion, die das Gerät mit 64-Bit-Wörtern berechnet.

Anmerkung: Wir empfehlen, die Einstellung oder höher zu verwenden.

IKE encryption

Legt den IKE-Verschlüsselungsalgorithmus fest, den das Gerät verwendet.

Mögliche Werte:

Wenn Sie das Gerät als Responder festlegen, akzeptiert das Gerät jeden Algorithmus. Wenn Sie das Gerät als Initiator festlegen, verwendet das Gerät verschiedene vordefinierte Algorithmen.

Das Gerät verwendet die Data-Encryption-Standard- (DES)-Blockchiffre für die Verschlüsselung von Nachrichtendaten mit einem 56-Bit-Schlüssel.

Das Gerät verwendet die Triple-DES-Blockchiffre für die Verschlüsselung von Nachrichtendaten, die den 56-Bit-Schlüssel des DES 3 Mal pro Block anwendet.

(Voreinstellung)

Das Gerät verwendet Advanced Encryption Standard (AES) mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 128 Key-Bits.

Das Gerät verwendet AES mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 192 Key-Bits.

Das Gerät verwendet AES mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 256 Key-Bits.

Anmerkung: Wir empfehlen, die Einstellung oder höher zu verwenden.

Advanced configuration - IPsec/Data-exchange

IPsec lifetime [s]

Legt die Lebensdauer der IPsec Security Association zwischen 2 Netzwerkgeräten in Sekunden zur Sicherung der Kommunikation fest. Die Geräte stellen nach dem Austausch eines Satzes vordefinierter Schlüssel eine Security Association her.

Mögliche Werte:

(Voreinstellung:)

Die Voreinstellung ist eine Stunde. Maximal können 8 Stunden eingestellt werden.

IPsec integrity (MAC)

Legt den Algorithmus für die IPsec-Integrität (MAC) fest, den das Gerät für die Instanz verwendet. Um die Dateien im VPN zu sichern, mischt (hasht) der Hash-based Message Authentication Code- (HMAC-) Prozess im sendenden Gerät die Nachrichtendaten mit einem gemeinsamen geheimen Schlüssel. Das empfangende Gerät mischt die Ergebnisse (Hash-Wert) erneut mit dem geheimen Schlüssel und wendet anschließend die Hash-Funktion ein 2. Mal an.

Mögliche Werte:

Wenn Sie das Gerät als Responder festlegen, akzeptiert das Gerät jeden Algorithmus. Wenn Sie das Gerät als Initiator festlegen, verwendet das Gerät verschiedene vordefinierte Algorithmen.

Das Gerät verwendet den Message-Digest-Algorithmus 5 (MD5) zur Berechnung der Hash-Funktion.

(Voreinstellung)

Das Gerät verwendet den Secure-Hash-Algorithmus Version 1 (SHA-1) zur Berechnung der Hash-Funktion.

Das Gerät verwendet SHA-256 (Teil der Version-2-Familie) zur Berechnung der Hash-Funktion, die das Gerät mit 32-Bit-Wörtern berechnet.

Das Gerät verwendet SHA-384 (Teil der Version-2-Familie) zur Berechnung der Hash-Funktion, die das Gerät auf der Grundlage einer kürzeren Version von SHA-512 berechnet.

Das Gerät verwendet SHA-512 (Teil der Version-2-Familie) zur Berechnung der Hash-Funktion, die das Gerät mit 64-Bit-Wörtern berechnet.

Anmerkung: Wir empfehlen, die Einstellung oder höher zu verwenden.

IPsec encryption

Legt den IPsec-Verschlüsselungsalgorithmus fest, den das Gerät verwendet.

Mögliche Werte:

Wenn Sie das Gerät als Responder festlegen, akzeptiert das Gerät jeden Algorithmus. Wenn Sie das Gerät als Initiator festlegen, verwendet das Gerät verschiedene vordefinierte Algorithmen.

Das Gerät verwendet die Data-Encryption-Standard- (DES)-Blockchiffre für die Verschlüsselung von Nachrichtendaten mit einem 56-Bit-Schlüssel.

Das Gerät verwendet die Triple-DES-Blockchiffre für die Verschlüsselung von Nachrichtendaten, die den 56-Bit-Schlüssel des DES 3 Mal pro Block anwendet.

(Voreinstellung)

Das Gerät verwendet Advanced Encryption Standard (AES) mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 128 Key-Bits.

Das Gerät verwendet AES mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 192 Key-Bits.

Das Gerät verwendet AES mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 256 Key-Bits.

AES-CTR mit 128 Key-Bits.

AES-CTR mit 192 Key-Bits.

AES-CTR mit 256 Key-Bits.

AES-GCM mit einem 64-Bit-ICV und 128 Key-Bits.

AES-GCM mit einem 96-Bit-ICV und 128 Key-Bits.

AES-GCM mit einem 128-Bit-ICV und 128 Key-Bits.

AES-GCM mit einem 64-Bit-ICV und 192 Key-Bits.

AES-GCM mit einem 96-Bit-ICV und 192 Key-Bits.

AES-GCM mit einem 128-Bit-ICV und 192 Key-Bits.

AES-GCM mit einem 64-Bit-ICV und 256 Key-Bits.

AES-GCM mit einem 96-Bit-ICV und 256 Key-Bits.

AES-GCM mit einem 128-Bit-ICV und 256 Key-Bits.

Anmerkung: Wir empfehlen, die Einstellung oder höher zu verwenden.

IPsec key agreement

Legt fest, welchen Diffie-Hellman-Algorithmus zur Schlüsselvereinbarung das Gerät zur Ermittlung des IPsec-SA-Sitzungsschlüssels verwendet. Bei aktivierter Perfect Forward Secrecy (PFS)-Funktion bleibt die Integrität von später generierten Schlüsseln erhalten, wenn die Kompromittierung eines Einzelschlüssels vorliegt.

Mögliche Werte:

Wenn Sie das Gerät als Responder festlegen, akzeptiert das Gerät jeden Algorithmus. Wenn Sie das Gerät als Initiator festlegen, verwendet das Gerät verschiedene vordefinierte Algorithmen.

(Voreinstellung)

Der Wert stellt einen Rivest-Shamir-Adleman- (RSA)-Algorithmus mit 1024-Bit-Modulus dar. Dieser Wert gehört zur Diffie-Hellman- (DH)- Gruppe 2.

Der Wert stellt einen RSA-Algorithmus mit 1536-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 5 gehört.

Der Wert stellt einen RSA-Algorithmus mit 2048-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 14 gehört.

Der Wert stellt einen RSA-Algorithmus mit 3072-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 15 gehört.

Der Wert stellt einen RSA-Algorithmus mit 4096-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 16 gehört.

Das Gerät schaltet die Funktion PFS aus. Das Ausschalten der Funktion PFS wird als Verletzung der Vertraulichkeit und daher als ein Sicherheitsrisiko betrachtet.

6 Switching

Das Menü enthält die folgenden Dialoge:

- Switching Global
- Lastbegrenzer
- Filter für MAC-Adressen
- QoS/Priority
- VLAN

6.1 Switching Global

[Switching > Global]

Dieser Dialog ermöglicht Ihnen, folgende Einstellungen festzulegen:

- Aging-Time für die Einträge in der MAC-Adresstabelle (Forwarding Database) ändern
- Flusskontrolle im Gerät einschalten

Wenn in der Warteschlange eines Ports sehr viele Datenpakete gleichzeitig eintreffen, dann führt dies möglicherweise zum Überlaufen des Port-Speichers. Beispielsweise passiert dies dann, wenn das Gerät Daten auf einem Gigabit-Port empfängt und diese an einen Port mit niedrigerer Bandbreite weiterleitet. Das Gerät verwirft überschüssige Datenpakete.

Der in 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 einem Uplink-Port führt dies möglicherweise zu unerwünschten Sendeunterbrechungen im übergeordneten Netzsegment („Wandering Backpressure“). Der Flusskontrollmechanismus verringert das Netz somit auf die Bandbreite, die das langsamste Gerät im Netz verarbeiten kann.

Konfiguration

MAC-Adresse

Zeigt die MAC-Adresse des Geräts.

Aging-Time [s]

Legt die Aging-Zeit in Sekunden fest.

Mögliche Werte:

(Voreinstellung:)

Das Gerät überwacht das Alter der gelernten Unicast-MAC-Adressen. Adresseinträge, die ein bestimmtes Alter (Aging-Zeit) überschreiten, löscht das Gerät aus seiner MAC-Adresstabelle (Forwarding Database).

Die MAC-Adresstabelle (Forwarding Database) finden Sie im Dialog

Im Zusammenhang mit der Router-Redundanz wählen Sie eine Zeit 30 s.

Flusskontrolle

Aktiviert/deaktiviert die Flusskontrolle im Gerät.

Mögliche Werte:

Die Flusskontrolle ist im Gerät aktiviert.

Aktivieren Sie die Flusskontrolle zusätzlich auf den erforderlichen Ports. Siehe Dialog
, Registerkarte , Kontrollkästchen in Spalte .

(Voreinstellung)

Die Flusskontrolle ist im Gerät deaktiviert.

6.2 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:

[\[Eingang\]](#)

[Eingang]

In dieser Registerkarte schalten Sie die Funktion ein. Der Schwellenwert 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.

Einheit

Legt die Einheit für den Schwellenwert fest:

Mögliche Werte:

(Voreinstellung)

Der Schwellenwert ist festgelegt in Prozent der Datenrate des Ports.

Der Schwellenwert ist festgelegt in Datenpaketen pro Sekunde.

Broadcast Modus

Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene Broadcast-Datenpakete.

Mögliche Werte:

(Voreinstellung)

Bei Überschreiten des Schwellenwerts verwirft das Gerät auf diesem Port die Überlast an Broadcast-Datenpaketen.

Broadcast Schwellenwert

Legt den Schwellenwert für empfangene Broadcasts auf diesem Port fest.

Mögliche Werte:

(Voreinstellung:)

Der Wert deaktiviert die Lastbegrenzerfunktion auf diesem Port.

Wenn Sie in Spalte den Wert auswählen, dann geben Sie einen Prozentwert zwischen und ein.

Wenn Sie in Spalte den Wert auswählen, dann geben Sie einen Absolutwert für die Datenrate ein.

Multicast Modus

Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene Multicast-Datenpakete.

Mögliche Werte:

(Voreinstellung)

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

Multicast Schwellenwert

Legt den Schwellenwert für empfangene Multicasts auf diesem Port fest.

Mögliche Werte:

(Voreinstellung:)

Der Wert deaktiviert die Lastbegrenzerfunktion auf diesem Port.

Wenn Sie in Spalte den Wert auswählen, dann geben Sie einen Prozentwert zwischen und ein.

Wenn Sie in Spalte den Wert auswählen, dann geben Sie einen Absolutwert für die Datenrate ein.

Unknown unicast mode

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

Mögliche Werte:

(Voreinstellung)

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

Unicast Schwellenwert

Legt den Schwellenwert für empfangene Unicasts mit unbekannter Zieladresse auf diesem Port fest.

Mögliche Werte:

(Voreinstellung:)

Der Wert deaktiviert die Lastbegrenzerfunktion auf diesem Port.

Wenn Sie in Spalte den Wert auswählen, dann geben Sie einen Prozentwert zwischen und ein.

Wenn Sie in Spalte den Wert auswählen, dann geben Sie einen Absolutwert für die Datenrate ein.

6.3 Filter für MAC-Adressen

[Switching > Filter für MAC-Adressen]



Dieser Dialog ermöglicht Ihnen, Adressfilter für die MAC-Adresstabelle (Forwarding Database) 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 keine Tabellenzeile für die Zieladresse, vermittelt das Gerät das Datenpaket vom Empfangsport an jeden anderen Port.

Tabelle


Um die gelernten MAC-Adressen aus der MAC-Adresstabelle (Forwarding Database) zu entfernen, klicken Sie im Dialog  die Schaltfläche .



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

Schaltflächen



Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld  legen Sie die Ziel-MAC-Adresse fest.
- Im Feld  legen Sie die VLAN-ID fest.
- Im Listenfeld wählen Sie die Ports aus.
Wenn die Ziel-MAC-Adresse eine Unicast-Adresse ist, wählen Sie genau einen Port aus.
Wenn die Ziel-MAC-Adresse eine Multicast- oder Broadcast-Adresse ist, wählen Sie einen oder mehrere Ports aus.
Wählen Sie keinen Port aus, um einen Discard-Filter hinzuzufügen. Das Gerät verwirft Datenpakete mit der in der Tabellenzeile festgelegten Ziel-MAC-Adresse.





Löschen

Entfernt die ausgewählte Tabellenzeile.



FDB leeren

Entfernt aus der Forwarding-Tabelle (FDB) die MAC-Adressen, die in Spalte  den Wert  haben.

Adresse

Zeigt die Ziel-MAC-Adresse, auf die sich die Tabellenzeile bezieht.

VLAN-ID

Zeigt die ID des VLANs, auf das sich die Tabellenzeile bezieht.

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:

Adressfilter automatisch durch das Gerät eingerichtet anhand empfangener Datenpakete.

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

Adressfilter manuell eingerichtet. Der Adressfilter bleibt dauerhaft eingerichtet.

<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.

Der Port vermittelt Datenpakete an die Zieladresse. Das Gerät hat den Filter anhand empfangener Datenpakete automatisch eingerichtet.

Der Port vermittelt Datenpakete an die Zieladresse. Ein Benutzer hat den Filter eingerichtet.

Der Port vermittelt Datenpakete an die Zieladresse. Ein Benutzer hat den Filter eingerichtet.

6.4 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, Port-Priorität).

Anmerkung: Wenn Sie die Funktionen in diesem Menü nutzen, dann schalten Sie die Flusskontrolle aus. Die Flusskontrolle ist ausgeschaltet, wenn im Dialog  , Rahmen  -  das Kontrollkästchen  unmarkiert ist.

Das Menü enthält die folgenden Dialoge:

[QoS/Priority Global](#)

[QoS/Priorität Port-Konfiguration](#)

[802.1D/p Zuweisung](#)

6.4.1 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:

(Voreinstellung:)

Im Dialog 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:

(Voreinstellung:)

Einige Werte in der Liste haben zusätzlich ein DSCP-Schlüsselwort, zum Beispiel , und . Diese Werte sind kompatibel zum IP Precedence-Modell.

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).

6.4.2 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 .

Mögliche Werte:

(Voreinstellung:)

6.4.3 802.1D/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 sehen Sie, welche VLAN-Priorität welcher Verkehrsklasse zugewiesen ist. 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:

- ist der Warteschlange mit der niedrigsten Priorität zugewiesen.
- ist der Warteschlange mit der höchsten Priorität zugewiesen.

Anmerkung: Unter anderem Redundanzmechanismen nutzen die höchste Verkehrsklasse. Wählen Sie deshalb für Anwendungsdaten eine andere Verkehrsklasse.

Werksseitige Zuweisung der VLAN-Priorität zu Verkehrsklassen

VLAN-Priorität	Verkehrsklasse	Inhaltskennzeichnung gemäß IEEE 802.1D
2		Normale Daten ohne Priorisierung
0		Zeitunkritische Daten und Hintergrunddienste
1		Normale Daten
3		Wichtige Daten
4		Zeitkritische Daten mit hoher Priorität
5		Bildübertragung mit Verzögerungen und Jitter <100 ms
6		Sprachübertragung mit Verzögerungen und Jitter <10 ms
7		Daten für Netzmanagement und Redundanzmechanismen

6.5 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.
- Verbessertes 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 Menü enthält die folgenden Dialoge:

- [VLAN Global](#)
- [VLAN Konfiguration](#)
- [VLAN Port](#)

6.5.1 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 das VLAN für das Management des Geräts geändert haben.

Größte VLAN-ID

Größtmögliche ID, die Sie einem VLAN zuweisen können.

Siehe Dialog

VLANs (max.)

Zeigt die maximale Anzahl der im Gerät einrichtbaren VLANs.

Siehe Dialog

VLANs

Anzahl der VLANs, die im Gerät gegenwärtig eingerichtet sind.

Siehe Dialog

Das VLAN 1 ist dauerhaft im Gerät eingerichtet.

6.5.2 VLAN Konfiguration

[Switching > VLAN > Konfiguration]

In diesem Dialog verwalten Sie die VLANs. Um ein VLAN einzurichten, fügen Sie eine weitere Tabellenzeile hinzu. 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 richtet das Gerät dynamische VLANs ein:

- : Das Gerät richtet ein VLAN für jedes Router-Interface ein.


Tabelle


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

Schaltflächen



Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

Im Feld  legen Sie die VLAN-ID fest.



Löschen

Entfernt die ausgewählte Tabellenzeile.

VLAN-ID

ID des VLANs.

Das Gerät unterstützt bis zu 64 gleichzeitig eingerichtete VLANs.

Mögliche Werte:

Status

Zeigt, auf welche Weise das VLAN eingerichtet ist.

Mögliche Werte:

VLAN

VLAN eingerichtet durch den Benutzer.

Wenn Sie die Einstellungen im permanenten Speicher speichern, dann bleiben die VLANs mit dieser Einstellung nach einem Neustart eingerichtet.

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.

= Tagged

Der Port ist Mitglied des VLANs und vermittelt die Datenpakete mit VLAN-Tag. Verwenden Sie diese Einstellung zum Beispiel auf Uplink-Ports.

= Tagged Learned

Der Port ist Mitglied des VLANs und vermittelt die Datenpakete mit VLAN-Tag.

Das Gerät hat den Eintrag mit der Funktion `no` oder `yes` automatisch eingerichtet.

= Forbidden

Der Port ist kein Mitglied des VLANs und vermittelt keine Datenpakete dieses VLANs.

= 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.

= Untagged Learned

Der Port ist Mitglied des VLANs und vermittelt die Datenpakete ohne VLAN-Tag.

Das Gerät hat den Eintrag mit der Funktion `no` oder `yes` 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.

6.5.3 VLAN Port

[Switching > VLAN > Port]

In diesem Dialog legen Sie fest, wie das Gerät empfangene Datenpakete behandelt, die kein VLAN-Tag haben oder deren VLAN-Tag von der VLAN-ID des Ports abweicht.

Dieser Dialog ermöglicht Ihnen, den Ports ein VLAN zuzuweisen und damit die Port-VLAN-ID festzulegen.

Außerdem legen Sie für jeden Port fest, wie das Gerät Datenpakete vermittelt, wenn eine der folgenden Situationen eintritt:

- Der Port empfängt Datenpakete ohne VLAN-Tag.
- Der Port empfängt Datenpakete mit VLAN-Prioritätsinformation (VLAN-ID , priority tagged).
- Die VLAN-ID im VLAN-Tag des Datenpakets unterscheidet sich von der VLAN-ID des Ports.

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 VLAN-ID fest, welche das Gerät den empfangenen Datenpaketen zuweist, die kein VLAN-Tag enthalten.

Voraussetzungen:

- In Spalte ist der Wert festgelegt.

Mögliche Werte:

(Voreinstellung:)

Ein bereits eingerichtetes VLAN

Akzeptierte Datenpakete

Legt fest, ob der Port empfangene Datenpakete ohne VLAN-Tag überträgt oder verwirft.

Mögliche Werte:

(Voreinstellung)

Der Port akzeptiert Datenpakete sowohl mit als auch ohne VLAN-Tag.

Der Port akzeptiert ausschließlich Datenpakete, die mit einer VLANID markiert sind.

Ingress-Filtering

Aktiviert/deaktiviert die Eingangsfilterung.

Mögliche Werte:

(Voreinstellung)

Die Eingangsfilterung ist aktiv.

Das Gerät vergleicht die im Datenpaket enthaltene VLAN-ID mit den VLANs, in denen der Port Mitglied ist. Siehe Dialog [VLAN-Filterung](#). Stimmt die VLAN-ID im Datenpaket mit einem dieser VLANs überein, vermittelt das Gerät das Datenpaket. Andernfalls verwirft das Gerät das Datenpaket.

Die Eingangsfilterung 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.

7 Routing

Das Menü enthält die folgenden Dialoge:

- [Routing Global](#)
- [Routing-Interfaces](#)
- [ARP](#)
- [Open Shortest Path First](#)
- [Routing-Tabelle](#)
- [L3-Relay](#)
- [Loopback-Interface](#)
- [Multicast Routing](#)
- [L3-Redundanz](#)
- [NAT](#)

7.1 Routing Global

[Routing > Global]

Das Menü ermöglicht Ihnen, die Einstellungen der Routing-Funktionen zur Vermittlung von Daten auf Schicht 3 des ISO/OSI-Schichtenmodells festzulegen.

Aus Sicherheitsgründen sind folgende Funktionen im Gerät dauerhaft deaktiviert:

- Beim Source Routing enthält das Datenpaket die Routing-Information und überschreibt damit die Einstellungen im Router.
- ICMP-Redirect-Datenpakete sind imstande, die Routing-Tabelle zu verändern. Das Gerät ignoriert generell empfangene ICMP-Redirect-Datenpakete. Die Einstellung im Dialog [Interfaces > Konfiguration](#), Spalte [ICMP-Redirect](#) hat ausschließlich Einfluss auf den Versand der ICMP-Redirect-Datenpakete.

Gemäß RFC 2644 vermittelt das Gerät keine Broadcast-Datenpakete aus externen Netzen in ein lokales Netz. Dieses Verhalten unterstützt Sie dabei, die Geräte im lokalen Netz vor Überlast zu schützen, hervorgerufen zum Beispiel durch Smurf-Attacken.

Dieser Dialog ermöglicht Ihnen, die Routing-Funktion im Gerät einzuschalten sowie weitere Einstellungen festzulegen.

Funktion

Funktion

Schaltet die Funktion [Routing](#) im Gerät ein/aus.

Mögliche Werte:

Die Funktion [Routing](#) ist eingeschaltet.
Aktivieren Sie die Routing-Funktion zusätzlich auf den Router-Interfaces. Siehe Dialog [Interfaces > Konfiguration](#).
(Voreinstellung)
Die Funktion [Routing](#) ist ausgeschaltet.

ICMP-Filter

Im Rahmen [ICMP-Filter konfigurieren](#) haben Sie die Möglichkeit, die Übertragung von ICMP-Nachrichten auf den eingerichteten Router-Interfaces zu begrenzen. Eine Begrenzung ist aus mehreren Gründen sinnvoll:

- Eine große Anzahl von ICMP Error-Nachrichten beeinflusst die Leistung des Routers und reduziert die verfügbare Bandbreite im Netz.
- Böswillige Absender verwenden ICMP Redirect-Nachrichten, um Man-in-the-Middle-Angriffe durchzuführen oder um Datenpakete mittels „Black hole“ zwecks Überwachung oder Denial-of-Service (DoS) umzuleiten.
- Ein ICMP Echo Reply-Paket ist die Antwort auf ein ICMP Echo Request-Paket, das sich missbrauchen lässt, um verwundbare Geräte und Router im Netz ausfindig zu machen.

Echo-Reply senden

Aktiviert/deaktiviert auf den Router-Interfaces das Antworten auf Pings.

Mögliche Werte:

(Voreinstellung)

Das Antworten auf Pings ist aktiv.

Das Gerät antwortet auf ein empfangenes >ICMP Echo Request-Paket mit einem ICMP Echo Reply-Paket.

Das Antworten auf Pings ist inaktiv.

Redirects senden

Aktiviert/deaktiviert auf den Router-Interfaces das Senden von ICMP Redirect-Nachrichten.

Mögliche Werte:

(Voreinstellung)

Das Senden von ICMP Redirect-Nachrichten ist aktiv.

Im Dialog [ICMP-Filter konfigurieren](#) haben Sie die Möglichkeit, das Senden auf jedem Router-Interface einzeln zu aktivieren. Siehe Funktion [ICMP-Filter konfigurieren](#).

Das Senden von ICMP Redirect-Nachrichten ist inaktiv.

Diese Einstellung vermeidet die Vervielfältigung von Datenpaketen, wenn sowohl Hardware- als auch Software-Funktionen des Geräts eine Kopie desselben Datenpakets weiterleiten.

Rate limit interval [ms]

Legt den durchschnittlichen Mindestzeitraum in Millisekunden zwischen jedem vom Gerät gesendeten ICMP Echo Request-Paket fest. Das Gerät begrenzt seine ICMP Echo Reply-Pakete auf eine durch einen Token-Bucket-Algorithmus bestimmte Anzahl.

Mögliche Werte:

(Voreinstellung:)

Rate limit ist ausgeschaltet.

(Voreinstellung:)

- In Phasen, in denen das Gerät kein ICMP-Paket sendet, sammelt es Token, um bei Bedarf Bursts zu senden.
- Im Falle eines Bursts ist das Intervall kürzer als hier festgelegt.
- Der maximal zulässige Wert für die Rate limit-Übertragung beträgt 100 Datenpakete je 1000 ms.

Rate limit burst size

Zeigt die maximale Anzahl von ICMP-Datenpaketen, die das Gerät während eines Bursts an jeden Empfänger sendet.

Mögliche Werte:

Information

Default-TTL

Zeigt den fest eingestellten TTL-Wert , den das Gerät in IP-Pakete einfügt, die das Management des Geräts sendet.

TTL (Time To Live, auch „Hop-Count“ genannt) kennzeichnet die maximale Anzahl von Routing-Schritten, die das gesendete ICMP Echo Request-Paket auf seinem Weg vom Absender zum Empfänger durchlaufen darf. Jeder Router auf dem Übertragungsweg reduziert den Wert im IP-Paket um . Empfängt ein Router ein IP-Paket mit dem TTL-Wert , verwirft er das IP-Paket. Dieser Router meldet an den Absender, dass er das IP-Paket verworfen hat.

7.2 Routing-Interfaces

[Routing > Interfaces]

Dieses Menü ermöglicht Ihnen, die Einstellungen für die Router-Interfaces festzulegen.

Das Menü enthält die folgenden Dialoge:


[Routing-Interfaces Konfiguration](#)

[Routing-Interfaces Sekundäre Interface-Adressen](#)

7.21 Routing-Interfaces Konfiguration

[Routing > Interfaces > Konfiguration]

Dieser Dialog ermöglicht Ihnen, die Einstellungen für die Router-Interfaces festzulegen.



Um ein Port-basiertes Router-Interface einzurichten, bearbeiten Sie die Tabellenzeilen. Um ein VLAN-basiertes Router-Interface einzurichten, verwenden Sie das Fenster .

Tabelle

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

Schaltflächen




Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen. Im Feld  legen Sie die VLAN-ID fest.



Entfernt die ausgewählte Tabellenzeile.



Öffnet das Fenster , das Sie dabei unterstützt, die Ports mit der Adresse eines oder mehrerer erwünschter Absender zu verknüpfen. Siehe „[\[Wizard: VLAN-Router-Interface einrichten\]](#)“ auf Seite 315.

Port

Zeigt die Nummer des zum Router-Interface gehörenden Ports oder VLANs.

Name

Bezeichnung des Ports.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

Das Gerät akzeptiert die folgenden Zeichen:

—
—
—
—
—

Port an

Aktiviert/deaktiviert den Port.

Mögliche Werte:

(Voreinstellung)

Der Port ist aktiv.

Der Port ist inaktiv. Der Port sendet und empfängt keine Daten.

Status Port

Zeigt den Betriebszustand des Ports.

Mögliche Werte:

Der Port ist eingeschaltet.

Der Port ist ausgeschaltet.

IP-Adresse

Legt die IP-Adresse für das Router-Interface fest.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung:)

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

- Management-Port
- Router-Interface
- Loopback-Interface

Netzmaske

Legt die Netzmaske für das Router-Interface fest.

Mögliche Werte:

Gültige IPv4-Netzmaske (Voreinstellung:)

Routing

Aktiviert/deaktiviert die Funktion auf dem Router-Interface.

Dabei entfernt das Gerät die Zustandsinformationen des Paketfilters. Dies beinhaltet eventuell vorhandene DCE RPC-Informationen des OPC-Enforcers. Das Gerät unterbricht hierbei offene Kommunikationsverbindungen.

Mögliche Werte:

Die Funktion ist aktiv.

- Beim Port-basierten Routing wandelt das Gerät den Port in ein Router-Interface um. Das Aktivieren der Funktion entfernt den Port aus den VLANs, in denen er bisher Mitglied war. Das Deaktivieren der Funktion stellt die Zuweisung NICHT wieder her, der Port ist in keinem VLAN Mitglied.
- Beim VLAN-basierten Routing leitet das Gerät die Datenpakete im zugehörigen VLAN weiter.

(Voreinstellung)

Die Funktion ist inaktiv.

Beim VLAN-basierten Routing ist das Gerät über das Router-Interface weiterhin erreichbar, wenn für das Router-Interface die IP-Adresse und die Netzmaske eingerichtet sind.

Proxy-ARP

Aktiviert/deaktiviert die Funktion auf dem Router-Interface. Diese Funktion ermöglicht Ihnen, Endgeräte aus anderen Netzen anzubinden, als wären diese Endgeräte im selben Netz erreichbar.

Mögliche Werte:

Die Funktion ist aktiv.

Das Gerät antwortet auf ARP-Anfragen von Endgeräten, die sich in anderen Netzen befinden.

(Voreinstellung)

Die Funktion ist inaktiv.

MTU-Wert

Legt die maximal zulässige Größe der IP-Pakete auf dem Router-Interface in Byte fest.

Mögliche Werte:

Stellt den voreingestellten Wert () wieder her.

(Voreinstellung:)

ICMP unreachable

Zeigt, ob auf dem Router-Interface das Senden von ICMP Destination Unreachable-Nachrichten aktiv ist.

Mögliche Werte:

Das Router-Interface sendet ICMP Destination Unreachable-Nachrichten.

ICMP redirects

Zeigt, ob auf dem Router-Interface das Senden von ICMP Redirect-Nachrichten aktiv ist.

Mögliche Werte:

Das Router-Interface sendet ICMP Redirect-Nachrichten.

(Voreinstellung)

Das Router-Interface sendet keine ICMP Redirect-Nachrichten.

[Wizard: VLAN-Router-Interface einrichten]

Das Fenster ermöglicht Ihnen, VLAN-basierte Router-Interfaces einzurichten.

Das Fenster führt Sie durch die folgenden Schritte:

- [VLAN erstellen oder auswählen](#)
- [VLAN einrichten](#)

VLAN erstellen oder auswählen

VLAN-ID

Zeigt die im Gerät eingerichteten VLANs. Um fortzufahren, wählen Sie einen Eintrag aus der Liste. Alternativ dazu legen Sie im Feld unten einen Wert fest.

VLAN-ID

Legt die ID eines VLANs fest. Alternativ wählen Sie einen Eintrag in der -Übersicht oben. Sie können ein VLAN auch im Dialog einrichten.

Mögliche Werte:

VLAN einrichten

VLAN-ID

Zeigt die ID des VLANs, das Sie im vorhergehenden -Schritt festgelegt haben.

Name

Legt die Bezeichnung des VLANs fest. Diese Einstellung überschreibt die für den Port im Dialog festgelegte Einstellung.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen
(hexadezimaler ASCII-Code) einschließlich Leerzeichen

<Port-Nummer>

Zeigt die Nummer des Ports.

Member

Aktiviert/deaktiviert die Mitgliedschaft des Ports im VLAN. Als Mitglied des VLANs gehört der Port zum einzurichtenden Router-Interface. Diese Einstellung überschreibt die im Dialog [VLAN > Konfiguration](#) für den Port festgelegte Einstellung.

Mögliche Werte:

Der Port ist Mitglied des VLANs.

Der Port ist kein Mitglied des VLANs.

Untagged

Aktiviert/deaktiviert auf dem Port das Senden der Datenpakete mit VLAN-Tag. Diese Einstellung überschreibt die im Dialog für den Port festgelegte Einstellung.

Mögliche Werte:

Der Port sendet die Datenpakete ohne VLAN-Tag.
Verwenden Sie diese Einstellung, wenn das angeschlossene Gerät keine VLAN-Tags auswertet, zum Beispiel an Ports, an die direkt ein Endgerät angeschlossen ist.

Der Port sendet die Datenpakete mit VLAN-Tag.

Port VLAN-ID

Legt die VLAN-ID fest, welche das Gerät den empfangenen Datenpaketen zuweist, die kein VLAN-Tag enthalten. Diese Einstellung überschreibt die für den Port im Dialog , Spalte festgelegte Einstellung.

Mögliche Werte:

Ein bereits eingerichtetes VLAN (Voreinstellung:)

Virtuellen Router-Port einrichten

Das Gerät ermöglicht Ihnen, für ein Router-Interface bis zu 2 IP-Adressen (1 primäre, 1 weitere) und insgesamt bis zu 64 IP-Adressen einzurichten.

Wenn Sie dem Router-Interface einen Port zuweisen, der bereits Datenpakete in ein anderes VLAN sendet, zeigt das Gerät beim Schließen des Fensters eine Meldung:

- Wenn Sie die Schaltfläche klicken, senden die betreffenden Ports die Datenpakete künftig ausschließlich im Router-VLAN.

Im Dialog haben die betreffenden Ports in der Tabellenzeile des Router-VLANs den Wert oder , in den Zeilen anderer VLANs den Wert .

- Wenn Sie die Schaltfläche klicken, senden die betreffenden Ports die Datenpakete im Router-VLAN und in anderen VLANs. Diese Einstellung führt möglicherweise zu unerwünschtem Verhalten und kann auch ein Sicherheitsrisiko darstellen.

Primäre Adresse

Adresse

Legt die primäre IP-Adresse für das Router-Interface fest.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung:)

Netzmaske

Legt die primäre Netzmaske für das Router-Interface fest.

Mögliche Werte:

Gültige IPv4-Netzmaske (Voreinstellung:)

Sekundäre Adressen

Adresse

Legt eine weitere IP-Adresse für das Router-Interface fest (Multinetting).

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung:)

Anmerkung: Legen Sie eine IP-Adresse fest, die sich von der primären IP-Adresse des Router-Interfaces unterscheidet.

Netzmaske

Legt die Netzmaske für die sekundäre IP-Adresse fest.

Mögliche Werte:

Gültige IPv4-Netzmaske (Voreinstellung:)

Hinzufügen

Fügt ein VLAN-basiertes Router-Interface hinzu.

7.2.2 Routing-Interfaces Sekundäre Interface-Adressen

[Routing > Interfaces > Sekundäre Interface-Adressen]

Dieser Dialog ermöglicht Ihnen, den Router-Interfaces weitere IP-Adressen zuzuweisen. Verwenden Sie diese Funktion, um ein Router-Interface an mehrere Subnetze anzubinden.

Das Gerät ermöglicht Ihnen, für ein Router-Interface bis zu 2 IP-Adressen (1 primäre, 1 weitere) und insgesamt bis zu 64 IP-Adressen einzurichten.


Tabelle




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

Schaltflächen



Hinzufügen

Öffnet das Fenster , um dem in der Tabelle ausgewählten Router-Interface eine weitere IP-Adresse hinzuzufügen.

- In der Dropdown-Liste  wählen Sie den Port oder das VLAN, der/das dem Router-Interface zugewiesen wird.
- Im Feld  legen Sie die IP-Adresse fest.
Mögliche Werte:
Gültige IPv4-Adresse
- Im Feld  legen Sie die Netzmaske fest.
Mögliche Werte:
Gültige IPv4-Netzmaske

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

- Management-Port
- Router-Interface
- Loopback-Interface




Löschen

Entfernt die ausgewählte Tabellenzeile.

Port

Zeigt die Nummer des zum Router-Interface gehörenden Ports oder VLANs.

IP-Adresse

Zeigt die primäre IP-Adresse des Router-Interfaces. Siehe Dialog  -

Netzmaske

Zeigt die primäre Netzmaske des Router-Interfaces. Siehe Dialog
□□.□□□□□□

Weitere IP-Adresse

Zeigt weitere IP-Adressen, die dem Router-Interface zugewiesen sind.

Weitere Netzmaske

Zeigt weitere Netzmasken, die dem Router-Interface zugewiesen sind.

7.3 ARP

[Routing > ARP]

Das Gerät lernt die MAC-Adresse, die zu einer IP-Adresse gehört, mittels Address Resolution Protocol (ARP).

Das Menü enthält die folgenden Dialoge:

- [ARP Global](#)
- [ARP Aktuell](#)
- [ARP Statisch](#)

7.3.1 ARP Global

[Routing > ARP > Global]

Dieser Dialog ermöglicht Ihnen, die ARP-Parameter einzustellen und statistische Größen zu betrachten.

Konfiguration

Aging-Time [s]

Legt die durchschnittliche Zeit in Sekunden fest, nach der das Gerät einen Eintrag aus der ARP-Tabelle entfernt. Tatsächlich entfernt das Gerät einen Eintrag nach einer zufällig bestimmten Zeit, die im Bereich $(0,5..1,5) \times$ des hier festgelegten Werts liegt.

Findet innerhalb dieser Zeit ein Datenaustausch mit dem zugehörigen Gerät statt, dann beginnt die Zeitmessung von vorne.

Mögliche Werte:

(Voreinstellung:)

Response Timeout [s]

Legt die Zeit in Sekunden fest, nach der das Gerät auf eine Antwort wartet, bevor es die Anfrage als gescheitert betrachtet.

Mögliche Werte:

(Voreinstellung:)

Wiederholungen

Legt fest, wie viele Male das Gerät eine gescheiterte Anfrage wiederholt, bevor es die Anfrage an diese Adresse verwirft.

Mögliche Werte:

(Voreinstellung:)

Information

Aktuelle Einträge

Zeigt, wie viele Einträge die ARP-Tabelle gegenwärtig enthält.

Dies umfasst:


- Adressen der Geräte, die an den Router-Interfaces angeschlossen sind. Siehe Dialog [ARP > Aktuell](#).
- Adressen der Geräte, die an das Management des Geräts angeschlossen sind. Siehe Dialog

Einträge (max.)

Zeigt, wie viele Einträge die ARP-Tabelle maximal enthalten kann.

Spitzenwert

Zeigt, wie viele Einträge die ARP-Tabelle bereits maximal enthalten hat.

Um den Zähler auf den Wert zurückzusetzen, klicken Sie im Dialog die Schaltfläche .

Aktuelle statische Einträge

Zeigt, wie viele statisch eingerichtete Einträge die ARP-Tabelle gegenwärtig enthält. Siehe Dialog

Statische Einträge (max.)

Zeigt, wie viele statisch eingerichtete Einträge die ARP-Tabelle maximal enthalten kann.

7.3.2 ARP Aktuell

[Routing > ARP > Aktuell]

Dieser Dialog ermöglicht Ihnen, die ARP-Tabelle einzusehen und die dynamisch eingerichteten Einträge zu löschen.

Tabelle

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

Schaltflächen

 Löschen

Entfernt die ausgewählte Tabellenzeile.

 ARP-Tabelle leeren

Entfernt aus der ARP-Tabelle die dynamisch eingerichteten Adressen.

Port

Zeigt das Router-Interface, an dem das Gerät die IP/MAC-Adresszuweisung gelernt hat.

IP-Adresse

Zeigt die IP-Adresse des Geräts, das auf eine ARP-Anfrage auf diesem Router-Interface geantwortet hat.

MAC-Adresse

Zeigt die MAC-Adresse des Geräts, das auf eine ARP-Anfrage auf diesem Router-Interface geantwortet hat.

Letztes Update

Zeigt die Zeit in Sekunden, seit der die gegenwärtigen Einstellungen des Eintrags in der ARP-Tabelle eingetragen sind.

Typ

Zeigt, auf welche Art der ARP-Eintrag eingerichtet ist.


Mögliche Werte:

Dynamisch eingerichteter Eintrag.

Wenn bis zum Ablauf der Aging-Time kein Datenpaket an das zugehörige Gerät gesendet oder von diesem empfangen wurde, entfernt das Gerät diesen Eintrag aus der ARP-Tabelle.

Die Aging-Time legen Sie fest im Dialog , Feld .

Statisch eingerichteter Eintrag.

Der Eintrag bleibt erhalten, wenn Sie mit der Schaltfläche  die dynamisch eingerichteten Adressen aus der ARP-Tabelle entfernen.

Kennzeichnet die IP/MAC-Adresszuweisung des Router-Interfaces.

Ungültiger Eintrag.

7.3.3 ARP Statisch

[Routing > ARP > Statisch]

Dieser Dialog ermöglicht Ihnen, selbst festgelegte IP/MAC-Adresszuweisungen in die ARP-Tabelle einzufügen.

Tabelle

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

Schaltflächen



Löschen

Entfernt die ausgewählte Tabellenzeile.



Wizard

Öffnet das Fenster , das Sie dabei unterstützt, die Ports mit der Adresse eines oder mehrerer erwünschter Absender zu verknüpfen. Siehe „[\[Wizard: ARP\]](#)“ auf Seite 325.

IP-Adresse

Zeigt die IP-Adresse des statischen ARP-Eintrags.

MAC-Adresse

Zeigt die MAC-Adresse, die das Gerät der IP-Adresse beim Beantworten einer ARP-Anfrage zuweist.

Port

Zeigt das Router-Interface, auf dem das Gerät die IP/MAC-Adresszuweisung anwendet.

Mögliche Werte:

Das Gerät wendet die IP/MAC-Adresszuweisung auf diesem Router-Interface an.

Die IP/MAC-Adresszuweisung ist gegenwärtig keinem Router-Interface zugewiesen.

Aktiv

Zeigt, ob die IP/MAC-Adresszuweisung aktiv oder inaktiv ist.

Mögliche Werte:

Die IP/MAC-Adresszuweisung ist aktiv. Die ARP-Tabelle des Geräts enthält die IP/MAC-Adresszuweisung als statischen Eintrag.

(Voreinstellung)

Die IP/MAC-Adresszuweisung ist inaktiv.

[Wizard: ARP]


Das Fenster  ermöglicht Ihnen, die IP/MAC-Adresszuweisungen in die ARP-Tabelle einzufügen. Voraussetzung ist, dass mindestens 1 Router-Interface eingerichtet ist.

ARP-Tabelle bearbeiten


Führen Sie die folgenden Schritte aus:


Legen Sie die IP-Adresse und die zugeordnete MAC-Adresse fest.

Anmerkung: Überprüfen Sie die MAC-Adresse sorgfältig. Dies kann helfen, das Netz vor unautorisierten Geräten zu schützen, die einen Man-in-the-Middle (MITM)-Angriff ausführen könnten.


Tragen Sie die IP-/MAC-Adresszuweisung im Feld  ein. Klicken Sie dazu die Schaltfläche .

Schließen Sie das Fenster . Klicken Sie dazu die Schaltfläche .

Legen Sie das Router-Interface in Spalte  fest.

Aktivieren Sie die IP/MAC-Adresszuweisung. Markieren Sie dazu das Kontrollkästchen in Spalte .

Statische Einträge

Zeigt die eingerichteten statischen Einträge. Sie können einen statischen Eintrag entfernen, indem Sie das Icon  klicken.

IP-Adresse

Legt die IP-Adresse des statischen ARP-Eintrags fest.

Mögliche Werte:

Gültige IPv4-Adresse

MAC-Adresse

Legt die MAC-Adresse fest, die das Gerät beim Antworten auf eine ARP-Anfrage der IP-Adresse zuweist.

Mögliche Werte:

Gültige MAC-Adresse

7.4 Open Shortest Path First

[Routing > OSPF]

Open Shortest Path First (OSPF) (OSPF) Version 2 ist ein im RFC 2328 beschriebenes Routing-Protokoll für Netze mit einer großen Anzahl von Routern.

Im Unterschied zu Distanzvektor-Routing-Protokollen wie RIP, die auf dem Hop-Count basieren, bietet OSPF einen Link-Status-Algorithmus. Der Link-State-Algorithmus von OSPF basiert auf den Pfadkosten, das heißt, Kriterium für die Routing-Entscheidungen sind die Pfadkosten anstatt des Hop-Counts. Die Pfadkosten ergeben sich aus der folgenden Berechnung: $(100 \text{ Mbit/s}) / (\text{Bandbreite in Mbit/s})$. OSPF unterstützt auch Netze mit Variable Length Subnet Masking (VLSM) und Classless Inter-Domain Routing (CIDR).

Die OSPF-Konvergenz des gesamten Netzes ist langsam. Nach der Initialisierung reagiert das Protokoll jedoch rasch auf Änderungen der Topologie. Die Konvergenzzeit von OSPF beträgt je nach Größe des Netzes 5 bis 15 Sekunden.

OSPF unterstützt die Aufteilung von Netzen in Bereiche (Areas) und reduziert so den Aufwand zur Verwaltung des gesamten Netzes (OSPF-Domäne). Die am Netz teilnehmenden Router kennen und verwalten ausschließlich ihre eigene Area, indem sie Link State Advertisements (LSAs) in die Area fluten. Mithilfe der LSAs erzeugt jeder Router eine eigene Topologie-Datenbank.

- Die Area Border Router (ABR) fluten LSAs in eine „Area“, um die lokalen Netze über die Ziele in anderen Areas innerhalb der OSPF-Domäne zu informieren. Die Designated Router (DR) senden LSAs, um über Ziele in anderen Areas zu informieren.
- Mit Hello-Paketen identifizieren sich benachbarte Router periodisch und signalisieren ihre Erreichbarkeit. Wenn ein Router die Hello-Pakete eines anderen Routers nicht erhält, sieht der Router diesen Router nach Ablauf eines Dead Interval Timers als nicht erreichbar an.

Das Gerät ermöglicht Ihnen, den Algorithmus md5 für die Datenübertragung zu verwenden. Legen Sie bei Verwendung des md5-Modus für Geräte in derselben Area dieselben Werte fest. Legen Sie relevanter Werte für die Area fest, die mit den ABR und ASBR verbunden ist.

OSPF teilt die Router in die folgenden Rollen ein:

- Designated Router (DR)
- Backup Designated Router (BDR)
- Area Border Router (ABR)
- Autonomous System Boundary Router (ASBR)

Das Menü enthält die folgenden Dialoge:

- OSPF Global
- OSPF Areas
- OSPF Stub Areas
- OSPF Not So Stubby Areas
- OSPF Interfaces
- OSPF Virtual Links
- OSPF Ranges
- OSPF Diagnose

7.4.1 OSPF Global

[Routing > OSPF > Global]

Dieser Dialog ermöglicht Ihnen, die Grundeinstellungen für **OSPF** festzulegen.

Das Menü enthält die folgenden Dialoge:

- [Allgemein]
- [Konfiguration]
- [Redistribution]

[Allgemein]

Diese Registerkarte ermöglicht Ihnen, **OSPF** im Gerät einzuschalten und die Netzparameter festzulegen.

Funktion

Funktion

Schaltet die Funktion **OSPF** im Gerät ein/aus.

Mögliche Werte:

- Die Funktion **OSPF** ist eingeschaltet.
(Voreinstellung)
- Die Funktion **OSPF** ist ausgeschaltet.

Konfiguration

Router-ID

Legt die eindeutige Kennung für den Router im autonomen System (AS) fest. Es beeinflusst die Wahl der Designated Router (DR) und der Backup Designated Router (BDR). Verwenden Sie idealerweise die IP -Adresse eines Router-Interfaces im Gerät.

Mögliche Werte:

(Voreinstellung:)

External LSDB limit

Legt die maximale Anzahl von nicht-voreingestellten Autonomous-System-External-LSA-Einträgen fest, die das Gerät in der Link-Status-Datenbank speichert. Sobald diese Grenze erreicht ist, wechselt der Router in den Overflow-Zustand.

Mögliche Werte:

(Voreinstellung)

Der Router speichert weitere Einträge, bis der Speicher voll ist.

Das Gerät speichert bis zur festgelegten Anzahl von Einträgen.

Legen Sie denselben Wert in den Routern des OSPF-Backbones und jeder anderen regulären OSPF-Area fest.

Externe LSAs

Zeigt die gegenwärtige Anzahl von nicht-voreingestellten Autonomous-System-External-LSA-Einträgen, die das Gerät in der Link-Status-Datenbank vorhält.

Autocost reference bandwidth

Legt eine Referenz zur Berechnung der Bandbreite von Router-Interfaces in Mbit/s fest. Verwenden Sie den Wert für Metrik-Berechnungen.

Mögliche Werte:

(Voreinstellung:)

Pfade (max.)

Legt die maximale Anzahl von ECMP-Routen fest, die der Routing-Tabelle hinzufügt, wenn in einem Subnetz mehrere Pfade mit denselben Pfadkosten und unterschiedlichen Next-Hops existieren.

Mögliche Werte:

(Voreinstellung:)

Verfügbar, wenn gegenwärtig das Routing-Profil
 Rahmen im Dialog

verwendet wird. Siehe

Standard-Metrik

Legt den voreingestellten Metrik-Wert für die Funktion `ospf cost` fest.

Mögliche Werte:

(Voreinstellung) `1`

Die Funktion `ospf cost` weist aus externen Routen gelernten Quellen (statisch oder direkt verbunden) automatisch Kosten von 20 zu.

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung an einem OSPF-Parameter erkennt.

Mögliche Werte:

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

Das Gerät sendet einen SNMP-Trap, wenn es Änderungen an den OSPF-Parametern erkennt.

(Voreinstellung) `enable`

Das Senden von SNMP-Traps ist inaktiv.

Shortest path first

Verzögerungszeit [s]

Legt die Wartezeit in Sekunden fest, die das Gerät nach einer Topologieänderung einhält, bis das Gerät eine SPF-Berechnung startet.

Mögliche Werte:

Der Router beginnt unmittelbar nach dem Empfang des Topology Change-Pakets mit der SPF-Berechnung.

(Voreinstellung: `0`)

Hold-Time [s]

Legt die Mindestzeit in Sekunden zwischen aufeinander folgenden SPF-Berechnungen fest.

Mögliche Werte:

(Voreinstellung: `10`)

Der Wert `0` bedeutet, dass der Router sofort nach Abschluss einer SPF-Berechnung die nächste SPF-Berechnung startet.

Exit-Overflow Intervall [s]

Legt die Zeit in Sekunden fest, die ein Router nach Beginn des Overflow-Zustands wartet, bevor er versucht, den Overflow-Zustand zu verlassen. Wenn der Router den Overflow-Zustand verlässt, sendet er neue, nicht voreingestellte AS-External-LSAs.

Mögliche Werte:

(Voreinstellung:)

Der Wert bedeutet, dass der Router bis zu einem Neustart im Overflow-Zustand verbleibt.

Information

ASBR status

Zeigt, ob das Gerät als Autonomous System Boundary Router (ASBR) arbeitet.

Mögliche Werte:

Der Router ist ein ASBR.

Der Router funktioniert in einer anderen Rolle als in der Rolle eines ASBR.

ABR status

Zeigt, ob das Gerät als Area Border Router (ABR) arbeitet.

Mögliche Werte:

Der Router ist ein ABR.

Der Router funktioniert in einer anderen Rolle als in der Rolle eines ABR.

Externe LSA-Checksumme

Zeigt die Link-Status-Prüfsummen der in der Link-Status-Datenbank gespeicherten externen LSAs. Dieser Wert ermöglicht Ihnen zu erkennen, ob Änderungen in der Link-Status-Datenbank des Routers auftreten, und die Link-Status-Datenbank mit der von anderen Routern zu vergleichen.

Neues LSA entstanden

Zeigt die Anzahl von neuen Link-Status-Advertisements dieses Routers. Der Router zählt diese Zahl jedes Mal hoch, wenn er ein neues Link-Status-Advertisement (LSA) erzeugt.

Empfangene LSA

Zeigt die Anzahl der empfangenen LSAs, die der Router als neue Instanzen vorsieht. Diese Anzahl schließt neuere Instanzen oder selbst erzeugte LSAs aus.

[Konfiguration]

Dieser Dialog ermöglicht Ihnen, folgende Einstellungen festzulegen:

- die Art, in der das Gerät die Pfadkosten berechnet
- wie die Funktion die Standard-Routen leitet
- den Routen-Typ, den die Funktion für die Pfad-Kostenberechnung verwendet

RFC 1583 Kompatibilität

Die Network Working Group entwickelt und verbessert die Funktion stetig weiter und fügt Parameter hinzu. Dieser Router stellt Parameter gemäß RFC 2328 bereit. Über die Parameter in diesem Dialog stellen Sie die Kompatibilität des Routers mit gemäß RFC 1583 entwickelten Routern her. Das Aktivieren der Kompatibilitätsfunktion ermöglicht Ihnen, das Gerät in einem Netz mit gemäß RFC 1583 entwickelten Routern zu installieren.

RFC 1583 Kompatibilität

Aktiviert/deaktiviert die Kompatibilität des Geräts mit Routern, die gemäß RFC 1583 entwickelt wurden.

Um Routing-Loops zu verhindern, stellen Sie diese Funktion für die OSPF-fähigen Router in einer OSPF-Domäne auf denselben Wert.

Mögliche Werte:

(Voreinstellung)

Aktivieren Sie die Funktion, wenn sich in der Domäne Router befinden, welche die in RFC 2328 beschriebene externe Pfad-Präferenz-Funktionalität nicht in ihrer Software enthalten.

Deaktivieren Sie die Funktion, wenn jeder Router in der Domäne die in RFC 2328 beschriebene externe Pfad-Präferenz-Funktionalität in seiner Software enthält.

Präferenzen

Die Einstellungen in diesem Dialog sind Metrik-Werte, die das Gerät zum Auflösen eines Tie-Breaker zwischen identischen Routen mit unterschiedlichen Distanztypen verwendet. Dies ist beispielsweise der Fall, wenn eine Route sich innerhalb der lokalen Area (Intra-Area) und die andere sich außerhalb der lokalen Area (Inter-Area oder externe Area) befindet. Verfügen die Intra-Area, die Inter-Area und die externe Area über dieselben Metrik-Werte, lautet die Präferenz-Reihenfolge Intra-Area, Inter-Area und externe Area.

Die Funktion betrachtet Routen mit Präferenzwert 255 als unerreichbar.

Präferenz (intra)

Legt die „Administrative Distanz“ zwischen Routern innerhalb derselben Area (Intra-Area-OSPF-Routen) fest.

Mögliche Werte:

(Voreinstellung:)

Präferenz (inter)

Legt die „Administrative Distanz“ zwischen Routern in unterschiedlichen Areas (Inter-Area-OSPF-Routen) fest.

Mögliche Werte:

(Voreinstellung:)

Präferenz (extern)

Legt die „Administrative Distanz“ zwischen Routern außerhalb der Areas (externe OSPF-Routen) fest.

Mögliche Werte:

(Voreinstellung:)

Default route

Advertise

Aktiviert/deaktiviert OSPF-Meldungen auf Standard-Routen, die von anderen Protokollen gelernt wurden.

So melden Area Border Router von Stub-Areas eine Standard-Route an die Stub-Area über Summary Link Advertisements. Bei der Einrichtung des Routers als einen AS-Boundary-Router meldet dieser die Standard-Route über AS-External-Link-Advertisements.

Mögliche Werte:

Der Router meldet Standard-Routen.

(Voreinstellung)

Der Router unterdrückt Meldungen über Standard-Routen.

Advertise always

Zeigt, ob der Router stets als Standard-Route meldet.

Beim Weiterleiten eines IP -Pakets leitet der Router das Paket stets zu der Zieladresse mit der größten Übereinstimmung weiter. Eine Standard-Route mit der Zieladresse und der Maske gilt als Übereinstimmung für jede IP-Zieladresse. Das Abgleichen jeder IP-Zieladresse ermöglicht einem AS Boundary Router, als Gateway für Ziele außerhalb des AS zu arbeiten.

Mögliche Werte:

Der Router meldet stets _____ als Standard-Route.
(Voreinstellung)
Das Gerät verwendet die im Parameter _____ festgelegten Einstellungen.

Metrik

Legt die Metrik der Standard-Route fest, welche die Funktion _____ meldet, wenn diese von anderen Protokollen gelernt wurde.

Mögliche Werte:

Das Gerät verwendet den im Feld _____ festgelegten Wert.

Metrik Typ

Zeigt den Metrik-Typ der Standard-Route, die Funktion _____ meldet, wenn sie von einem anderen Protokoll gelernt wurde.

Mögliche Werte:

Umfasst sowohl die externen Pfadkosten vom ABR zum ASBR, der die Route erzeugt hat, als auch die internen Pfadkosten zum ABR, der die Route in der lokalen Area gemeldet hat.
(Voreinstellung)
Umfasst ausschließlich die externen Pfadkosten.

[Redistribution]

Ein Router, bei dem auf einem gerouteten Interface die Funktion _____ ausgeschaltet ist, propagiert nicht das Netz dieses Interfaces auf seinen anderen Interfaces. Das Netz ist somit unerreichbar. Um solche Netze zu propagieren, schalten Sie _____ ein für "verbundene" Netze.

Bei der Verwaltung verschiedener Abteilungen durch mehrere Netzadministratoren oder in herstellerunabhängigen Netzen mit mehreren Protokollen ist die Neuverteilung nützlich. Die OSPF-Neuverteilung ermöglicht Ihnen, die Routen-Informationen in ein Ziel von anderen Protokollen in _____ umzuwandeln, zum Beispiel Kosten und Entfernung.

Die Anzahl der Routen, die das Gerät über die Funktion _____ lernt, ist auf die Größe der Routing-Tabelle begrenzt.

Tabelle

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

Quelle

Zeigt das Quellprotokoll, aus dem die Funktion die Routen neu verteilt. Dieses Objekt dient außerdem als Bezeichner für die Tabellenzeile.

Das Aktivieren einer Tabellenzeile ermöglicht dem Gerät, Routen aus dem betreffenden Quellprotokoll in OSPF weiterzuverteilen.

Mögliche Werte:

Der Router ist direkt mit der Route verbunden.

Ein Netzadministrator hat die Route im Router festgelegt.

Aktiv

Aktiviert/deaktiviert die Routen-Neuverteilung vom Quellprotokoll in OSPF.

Mögliche Werte:

Die Neuverteilung von Routen, die vom Quellprotokoll gelernt wurden, ist aktiv.

(Voreinstellung)

Die OSPF-Routen-Neuverteilung ist inaktiv.

Metrik

Legt den Metrikwert fest für Routen, die durch dieses Protokoll neu verteilt werden.

Mögliche Werte:

(Voreinstellung)

Das Gerät verwendet den im Feld festgelegten Wert.

Metrik Typ

Legt den Routen-Metriktyp fest, den die Funktion von anderen Quellprotokollen neu verteilt.

Mögliche Werte:

Dieser Metriktyp umfasst sowohl die externen Pfadkosten vom ABR zum ASBR, der die Route erzeugt hat, als auch die internen Pfadkosten zum ABR, der die Route in der lokalen Area gemeldet hat.

(Voreinstellung)

Dieser Metriktyp gilt ausschließlich für die externen Pfadkosten.

Tag

Legt einen Tag für Routen fest, die in die Funktion `ospf redistribute` neu verteilt werden.

Wenn Sie einen Routen-Tag setzen, weist die Funktion `ospf redistribute` den Wert zu jeder neu verteilten Route dieses Quellprotokolls zu. Diese Funktion ist nützlich, wenn 2 oder mehr Border Router ein Autonomous System mit einem externen Netz verbinden. Um eine doppelte Neuverteilung zu vermeiden, legen Sie in jedem Border-Router denselben Wert fest, wenn Sie dasselbe Protokoll umverteilen.

Mögliche Werte:

(Voreinstellung: `0`)

Subnetze

Aktiviert/deaktiviert die Routen-Neuverteilung für Subnetze in die Funktion `ospf redistribute`.

Die Funktion `ospf redistribute` verteilt ausschließlich Netzklassen in die OSPF-Domäne um. Um die Subnetz-Routen in OSPF neu zu verteilen, aktivieren Sie den Subnetz-Parameter.

Mögliche Werte:

(Voreinstellung)

Der Router verteilt Netzklassen und Subnetz-Routen in OSPF um.

Der Router verteilt ausschließlich Netzklassen in OSPF um.

7.4.2 OSPF Areas

[Routing > OSPF > Areas]

OSPF unterstützt die Aufteilung von Netzen in Bereiche (Areas) und reduziert so den Aufwand zur Verwaltung des Netzes. Die am Netz teilnehmenden Router kennen und verwalten ausschließlich ihre eigene Area, indem sie Link State Advertisements (LSAs) in die Area fluten. Mithilfe der LSAs erzeugt jeder Router eine eigene Topologie-Datenbank.

Das Gerät ermöglicht Ihnen, bis zu 64 OSPF-Areas festzulegen.


Tabelle


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

Schaltflächen



Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld  legen Sie die Area-ID für die neue Tabellenzeile fest.
Mögliche Werte:
Oktett-Wert, angezeigt wie eine IPv4-Adresse



Löschen

Entfernt die ausgewählte Tabellenzeile.

Area-ID

Zeigt die Area-ID.

Area Typ

Legt die Importrichtlinie für AS-External-LSAs für die Area fest, die den Area-Typ bestimmt.


OSPF-Importrichtlinien gelten ausschließlich für externe Routen. Eine externe Route ist eine Route außerhalb des autonomen OSPF-Systems.

Mögliche Werte:

 (Voreinstellung)

Der Router importiert Type 5 AS external-LSAs in die Area.

 Der Router ignoriert Type 5 AS external-LSAs.

 Der Router übersetzt Type 7 AS external-LSAs in Type 5 NSSA summary-LSAs und importiert sie in die Area.

SPF runs

Zeigt, wie oft der Router die Intra-Area-Routing-Tabelle berechnet hat, welche die Link-Status-Datenbank dieser Area verwendet. Der Router verwendet den Dijkstra-Algorithmus für die Routen-Berechnung.

Area-Border Router

Zeigt die Gesamtzahl der ABR, die innerhalb dieser Area erreichbar sind. Die Anzahl der erreichbaren Router ist zunächst 0. Die Funktion `show ospf border-routers` berechnet die Anzahl bei jedem SPF-Durchlauf.

AS-Boundary Router

Zeigt die Gesamtzahl der ASBR, die innerhalb dieser Area erreichbar sind. Die Anzahl der erreichbaren ASBR ist zunächst 0. Die Funktion `show ospf asbr` berechnet die Anzahl bei jedem SPF-Durchlauf.

Area-LSAs

Zeigt die Gesamtzahl der Link State Advertisements in der Link-Status-Datenbank dieser Area, jedoch keine AS-External-LSAs.

Area-LSA Checksumme

Zeigt die Gesamtzahl der LS-Prüfsummen, die in der LS-Datenbank dieser Area enthalten sind. Diese Summe schließt Type 5 external-LSAs aus. Sie verwenden die Summe, um zu bestimmen, ob eine Änderung in einer LS-Datenbank eines Routers stattgefunden hat, und um die LS-Datenbank mit anderen Routern abzugleichen.

7.4.3 OSPF Stub Areas

[Routing > OSPF > Stub Areas]

OSPF ermöglicht Ihnen, bestimmte Areas als Stub-Areas festzulegen. Der Area Border Router (ABR) einer Stub-Area trägt die von externen AS-LSAs gelernten Informationen in seine Datenbank ein, ohne die AS-External-LSAs über die Stub-Area hinweg zu fluten. Der ABR sendet stattdessen eine Summary-LSA in die Stub-Area und meldet damit eine Standard-Route. Die in der Summary-LSA gemeldete Standard-Route gehört nur zu einer bestimmten Stub-Area. Bei der Weiterleitung von Daten an AS-External-Ziele verwenden die Router in einer Stub-Area ausschließlich den Standard-ABR. Durch Senden einer Summary-LSA, die anstelle der AS-External-LSAs die Standard-Route enthält, werden die Größe der Link-Status-Datenbank und somit der Speicherplatzbedarf für einen internen Router einer Stub-Area verringert.

Das Gerät bietet Ihnen folgende Möglichkeiten, eine Stub-Area hinzuzufügen:

- Wandeln Sie eine Area in eine Stub-Area um. Führen Sie dazu den folgenden Schritt aus:
Ändern Sie im Dialog den Wert in Spalte auf .
- Erstellen Sie eine Stub-Area. Führen Sie dazu die folgenden Schritte aus:
Fügen Sie im Dialog eine Tabellenzeile hinzu.
Ändern Sie den Wert in Spalte auf .

Tabelle

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

Area-ID

Zeigt die Area-ID für die Stub-Area.

Default cost

Legt den Wert der externen Metrik für den Metriktyp fest.

Mögliche Werte:

Der Router setzt den voreingestellten Wert so, dass dieser innerhalb des Bereichs den geringeren Kosten für den Metrik-Typ entspricht.

Metrik Typ

Legt den Metrik-Typ fest, der für die in der Area gemeldete Standard-Route verwendet wird.

Der Border Router einer Stub-Area meldet eine Standard-Route als Netz-Summary-LSA.

Mögliche Werte:

(Voreinstellung)

Der ABR meldet die Metrik als OSPF-intern, das den Kosten einer Intra-Area-Route zum ABR entspricht.

Der ABR meldet die Metrik als , der den Kosten der internen OSPF-Metrik plus der externen Metrik des ASBR entspricht.

Der ABR meldet die Metrik als , der den Kosten der externen Metrik des ASBR entspricht. Verwenden Sie diesen Wert für NSSAs.

Totally stub

Aktiviert/deaktiviert den Import von Summary-LSAs in die Stub-Areas.

Mögliche Werte:

Der Router importiert keine Area-Summarys. Die Stub-Area basiert vollständig auf der Standard-Route zu einer Totally-Stubby-Area.

(Voreinstellung)

Der Router fasst Summary-LSAs zusammen und gibt sie an die Summary-LSAs in der Stub-Area weiter.

7.4.4 OSPF Not So Stubby Areas

[Routing > OSPF > NSSA]

NSSAs ähneln der OSPF-Stub-Area. NSSAs verfügen jedoch über eine zusätzliche Funktion zum Importieren von begrenzten AS-External-Routen. Der ABR sendet externe Routen aus der NSSA aus, indem der ABR Type 7 AS external-LSAs in Type 5 AS external-LSAs umwandelt. Der ASBR in einer NSSA erzeugt Type 7-LSAs. Der einzige Unterschied zwischen Type 5-LSAs und Type 7-LSAs besteht darin, dass der Router das N-Bit für NSSAs setzt. Für beide NSSA-Nachbarn ist das „N“-Bit eingestellt. Dadurch wird eine OSPF Nachbarschafts-Adjacency hergestellt.

Außer dem internen Datenstrom arbeiten NSSAs wie Transit-Areas, da sie aus externen Quellen stammende Daten an andere Areas innerhalb der OSPF-Domäne transportieren.

Das Gerät bietet Ihnen folgende Möglichkeiten, eine NSSA hinzuzufügen:

- Wandeln Sie eine Area in eine NSSA um. Führen Sie dazu den folgenden Schritt aus:
Ändern Sie im Dialog den Wert in Spalte auf .
- Erstellen Sie eine NSSA. Führen Sie dazu die folgenden Schritte aus:
Fügen Sie im Dialog eine Tabellenzeile hinzu.
Ändern Sie den Wert in Spalte auf .

Tabelle

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

Area-ID

Zeigt die Area -ID, für welche die Tabelleneinträge gelten.

Neu verteilen

Aktiviert/deaktiviert die Umverteilung externer Routen in die NSSA.

Mögliche Werte:

(Voreinstellung)

Die NSSA-ASBRs unterdrücken die Umverteilung von externen Routen in die NSSA. Außerdem beendet der ASBR das Generieren von Type 7 external-LSAs für externe Routen.

Die NSSA-ASBRs verteilen externe Routen in die NSSA um.

Originate default info

Aktiviert/deaktiviert das Generieren von Type 7 default-LSAs.

Voraussetzung ist, dass der Router ein NSSA-ABR oder ASBR ist.

Mögliche Werte:

Der Router generiert Type 7 default-LSAs und sendet sie in die NSSA.

(Voreinstellung)

Der Router unterdrückt Type 7 default-LSAs.

Standard-Metrik

Legt die im Type 7 default-LSA gemeldete Metrik fest.

Mögliche Werte:

(Voreinstellung:)

Standard-Metrik Typ

Legt den im Type 7 default-LSA gemeldeten Metrik-Typ fest.

Mögliche Werte:

Der Router meldet die Metrik als OSPF-intern, das den Kosten einer Intra-Area-Route zum ABR entspricht.

Der Router meldet die Metrik als external Type 1, der den Kosten der internen OSPF-Metrik plus der externen Metrik des ASBR entspricht.

Der Router meldet die Metrik als external Type 2, der den Kosten der externen Metrik des ASBR entspricht.

Translator role

Legt die Fähigkeit eines NSSA Border Routers zur Übersetzung von Type 7-LSAs in Type 5-LSAs fest.

NSSA Area Border Router empfangen Type 5-LSAs, die Informationen zu externen Routen enthalten. Die NSSA Border Router blockieren Type 5-LSAs, die in die NSSA eintreten könnten. Bei Verwendung von Type 7-LSAs informieren die Border Router einander von externe Routen. Die ABR übersetzen die Type 7-LSAs anschließend in Type 5 external-LSAs und fluten die Informationen in das übrige OSPF-Netz.

Mögliche Werte:

Der Router übersetzt Type 7-LSAs in Type 5-LSAs.
Wenn der Router Type 5-LSAs von einem anderen Router mit einer Router -ID empfängt, die höher ist als seine eigene Router -ID, entfernt der Router seine Type 5-LSAs.

(Voreinstellung)

Der Router übersetzt Type 7-LSAs in Type 5-LSAs.
Um Routing-Loops zu vermeiden, nimmt die Funktion eine Übersetzerauswahl vor. Sind mehrere Kandidaten vorhanden, wählt die Funktion den Router aus, der eine höhere Router -ID als der Übersetzer besitzt.

Translator status

Zeigt, ob und wie der Router Type 7-LSAs in Type 5-LSAs übersetzt.

Mögliche Werte:

Die des Routers ist auf gesetzt.

Als Kandidat übersetzt der NSSA Border Router Type 7-LSAs in Type 5-LSAs.

Ein anderer NSSA Border Router übersetzt Type 7-LSAs in Type 5-LSAs.

Translator-Stability Intervall [s]

Legt die Zeit in Sekunden fest, in welcher der Router die Übersetzung von Type 7-LSAs in Type 5-LSAs fortsetzt, nachdem der Router eine Übersetzungsauswahl verloren hat.

Mögliche Werte:

(Voreinstellung:)

Translator events

Zeigt die Anzahl von Übersetzer-Statusänderungen seit dem letzten Systemstart.

Unregelmäßigkeiten in Bezug auf den Wert dieses Zählers treten auf, wenn die Funktion ausgeschaltet ist, und können außerdem während der Neuinitialisierung des Management-Systems auftreten.

Totally NSSA

Aktiviert/deaktiviert den Import von Summary-Routen in die NSSA als Type 3 summary-LSAs.

Mögliche Werte:

Der Router unterdrückt den Import von Summary-Routen, wodurch die Area zu einer Totally-NSSA wird.

(Voreinstellung)

Der Router importiert Summary-Routen in die NSSA als Type 3 summary-LSAs.

7.4.5 OSPF Interfaces

[Routing > OSPF > Interfaces]

Dieser Dialog ermöglicht Ihnen, die OSPF-Parameter im Router-Interface festzulegen, zu aktivieren und anzuzeigen.

Das Gerät ermöglicht Ihnen, bis zu 64 OSPF-Router-Interfaces zu aktivieren.

Um Informationen zur Erreichbarkeit zwischen den Routern auszutauschen, verwendet das Gerät das OSPF-Routing-Protokoll. Das Gerät verwendet von Netzteilnehmern gelernte Routing-Informationen, um den Next-Hop zum Ziel zu bestimmen. Um die Datenpakete korrekt weiterzuleiten, authentifiziert der Router OSPF-Protokollverkehr und vermeidet so, dass bösartige oder fehlerhafte Routing-Informationen in die Routing-Tabelle gelangen.

Die Funktion `ospf authentication` unterstützt mehrere Authentifizierungstypen. Richten Sie die Authentifizierungstypen für jedes Interface ein. Die Option `ospf authentication message-digest` zur verschlüsselten Authentifizierung unterstützt Sie dabei, das Netz gegen passive Angriffe zu schützen, und bietet einen wesentlichen Schutz gegen aktive Angriffe. Bei Anwendung der Option für die verschlüsselte Authentifizierung fügt jeder Router den übermittelten OSPF-Paketen ein „message digest“ hinzu. Empfänger verwenden den „Shared Secret Key“ und den empfangenen Digest, um sich zu vergewissern, ob jedes empfangene OSPF-Paket authentisch ist.

Tabelle

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

Port

Zeigt das Interface, auf das sich die Tabellenzeile bezieht.

IP-Adresse

Zeigt die IP-Adresse dieses OSPF-Interfaces.

Aktiv

Aktiviert/deaktiviert den administrativen OSPF-Status des Interfaces.

Mögliche Werte:

Der Router meldet die auf dem Interface auf dem Interface festgelegten Werte und das Interface als interne OSPF-Route.

(Voreinstellung)

Das Interface ist in Bezug auf die Funktion `ospf authentication` extern.

Area-ID

Legt die Area-ID der Domäne fest, zu der das Interface eine Verbindung herstellt.

Mögliche Werte:

Die Area-IDs legen Sie im Dialog `ospf area` fest.

Priorität

Legt die Priorität dieses Interfaces fest.

In Multi-Access-Netzen verwendet der Router den Wert im Algorithmus für die Auswahl der Designated Router (DR). Wenn der gleiche Wert auf mehreren Routern festgelegt ist, entscheidet die Router-ID. Die höchste Router-ID gewinnt.

Mögliche Werte:

Der Router ist außerstande, der Designated Router (DR) in diesem Netz zu werden.
 (Voreinstellung:)

Sende-Verzögerung [s]

Legt die geschätzte Anzahl von Sekunden für die Übertragung eines Link State update-Pakets über dieses Interface fest.

Diese Einstellung ist für langsame Datenverbindungen nützlich. Der Timer erhöht das Alter der LS-Updates, um geschätzte Verzögerungen auf dem Interface auszugleichen. Wird das Paketalter zu sehr erhöht, ist die Antwort jünger als das ursprüngliche Paket.

Mögliche Werte:

(Voreinstellung:)

Retrans-Intervall [s]

Legt für Adjacencies, die zu diesem Interface gehören, die Zeit in Sekunden bis zur erneuten Übertragung von Link State Advertisement fest.

Sie verwenden diesen Wert ebenfalls, wenn Sie die Datenbank-Beschreibung und die Link-Status-Request-Pakete erneut übertragen.

Mögliche Werte:

(Voreinstellung:)

Hello-Intervall [s]

Legt die Zeit in Sekunden zwischen den Übertragungen von Hello-Paketen auf dem Interface fest.

Stellen Sie für Router, die einem gemeinsamen Netz angehören, denselben Wert ein. Vergewissern Sie sich, dass jeder Router in einem Bereich den gleichen Wert hat.

Mögliche Werte:

(Voreinstellung:)

Dead-Intervall [s]

Legt die Zeit in Sekunden fest, die das Gerät auf Hello-Pakete wartet, bevor es den benachbarten Router als nicht erreichbar deklariert.

Legen Sie den Wert als Vielfaches von fest. Legen Sie den gleichen Wert für die Router-Interfaces innerhalb desselben Bereiches fest.

Mögliche Werte:

(Voreinstellung:)

Legen Sie einen niedrigeren Wert fest, um einen nicht erreichbaren Nachbarn schneller zu erkennen.

Anmerkung: Kleinere Werte sind anfällig für Interoperabilitätsprobleme.

Status

Zeigt den Zustand des OSPF-Interfaces.

Mögliche Werte:

(Voreinstellung)

Das Interface ist im initialen Zustand und blockiert die Datenpakete.

Das Interface ist ein Loopback-Interface des Geräts. Obwohl Pakete nicht über das Loopback-Interface versendet werden, melden die Router-LSAs weiterhin die Interface-Adresse weiter.

Gilt ausschließlich für Interfaces, die mit Broadcast- oder Non-Broadcast-Multi-Access-Netzen (NBMA) verbunden sind. In diesem Zustand versucht der Router, den Zustand des DR- und BDR-Netzes durch Senden und Empfangen von Hello Paketen zu identifizieren. Der Wartezeit-Timer bewirkt, dass das Interface den -Zustand verlässt und einen DR wählt. Die Dauer dieses Timers entspricht dem Wert im Feld .

Gilt ausschließlich für Interfaces, die mit Punkt-zu-Punkt- oder Punkt-zu-Mehrpunkt-Verbindungen angebunden sind, sowie für Virtual-Link-Netze. Das Interface sendet in diesem Zustand im Abstand von Sekunden ein Hello-Paket, um eine Adjacency mit dem Nachbarn herzustellen.

Der Router ist der DR für das Multi-Access-Netz und stellt Adjacencies mit anderen Routern her.

Der Router ist der BDR für das Multi-Access-Netz und stellt Adjacencies mit anderen Routern her.

Der Router ist ausschließlich ein Netzteilnehmer. Der Router stellt ausschließlich mit dem DR und dem BDR Adjacencies her und überwacht seine Netz-Nachbarn.

Designated router

Zeigt die IP-Adresse des Designated Routers.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung:)

Backup designated router

Zeigt die IP-Adresse des Backup Designated Routers.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung:)

Ereignisse

Zeigt, wie oft dieses OSPF-Interface seinen Zustand ändert oder wie oft der Router einen Fehler erkannt hat.

Netzwerktyp

Legt den OSPF-Netztyp des autonomen Systems fest.

Mögliche Werte:

Verwenden Sie diesen Wert für Broadcast-Netze wie Ethernet und IEEE 802.5. Die Funktion `ospf dr bdr` führt eine Auswahl von DR und BDR durch, mit denen die nicht-designierten Router eine Adjacency herstellen.

Verwenden Sie diesen Wert für Non-Broadcast-Multi-Access-Netze, zum Beispiel X.25 und ähnliche Technologien. Die Funktion `ospf dr bdr` führt eine DR- und BDR-Auswahl durch, um die Anzahl der hergestellten Adjacencys einzuschränken.

Verwenden Sie diesen Wert für Netze, die lediglich 2 Interfaces verbinden.

Verwenden Sie diesen Wert, wenn Sie mehrere Punkt-zu-Punkt-Verbindungen in einem Non-Broadcast-Netz erfassen. Jeder Router im Netz sendet Hello-Pakete an andere Router im Netz, jedoch ohne eine DR- und BDR-Auswahl.

Auth Typ

Legt den Authentifizierungstyp für ein Interface fest.

Wenn Sie `ospf authentication-mode` oder `ospf authentication-key` festlegen, ist es für diesen Router erforderlich, dass andere Router einen Authentifizierungsprozess durchlaufen, bevor dieser Router die betreffenden Router als Nachbarn akzeptiert.

Wenn Sie die Authentifizierung zum Schutz des Netzes verwenden, verwenden Sie für jeden Router in Ihrem autonomen System denselben Typ und Schlüssel.

Mögliche Werte:

`none` (Voreinstellung)

Die Netz-Authentifizierung ist deaktiviert.

Der Router verwendet Klartext-Authentifizierung. In diesem Fall sendet der Router die Passwörter als Klartext.

Der Router verwendet die MD5-Authentifizierung über den Message-Digest-Algorithmus. Dieser Authentifizierungstyp unterstützt Sie dabei, das Netz sicherer zu machen.

Auth key

Legt den Authentifizierungsschlüssel fest.

Nach Eingabe zeigt das Feld `*****` (Sternchen) anstelle des Authentifizierungsschlüssels.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 16 Zeichen

– mit 8 Zeichen, wenn in der Dropdown-Liste `ospf authentication-mode` der Eintrag `simple` ausgewählt ist

– mit 16 Zeichen, wenn in der Dropdown-Liste `ospf authentication-mode` der Eintrag `md5` ausgewählt ist

Wenn Sie einen kürzeren Authentifizierungsschlüssel festlegen, füllt das Gerät die verbleibenden Stellen mit `0`.

Auth key ID

Legt für die Authentifizierungsschlüssel-ID den Wert `auth-key-id` fest.

Die Option `ospf authentication` zur verschlüsselten Authentifizierung unterstützt Sie dabei, das Netz gegen passive Angriffe zu schützen, und bietet einen wesentlichen Schutz gegen aktive Angriffe.

Voraussetzung für das Ändern dieses Wertes ist, dass in Spalte `auth-key-id` der Wert `auth-key-id` festgelegt ist.

Mögliche Werte:

(Voreinstellung: `0`)

Kosten

Legt die interne Metrik fest.

Die Funktion `ospf cost` verwendet als Metrik die Kosten der Datenverbindung. Die Funktion `ospf cost` verwendet diesen Wert auch zur Berechnung der SPF-Routen. Die Funktion `ospf cost` bevorzugt die Route mit dem niedrigeren Wert.

Zur Berechnung der Kosten teilen Sie die Referenzbandbreite durch die Bandbreite auf dem Interface. Die Referenzbandbreite ist im Feld `ospf cost-reference-bandwidth` festgelegt und beträgt in der Voreinstellung 100 Mbit/s. Siehe Dialog `ospf cost-reference-bandwidth`, Registerkarte `ospf`.

Beispiel:

Die Bandbreite auf dem Interface beträgt 10 Mbit/s.

Die Metrik ist $100 \text{ Mbit/s} / 10 \text{ Mbit/s} = 10$.

Mögliche Werte:

(Voreinstellung)

Das Gerät berechnet die Metrik und passt den Wert bei einer Änderung der Bandbreite auf dem Interface automatisch an.

Die Funktion `ospf cost` verwendet als Metrik den hier festgelegten Wert.

Calculated cost

Zeigt den Metrik-Wert, den die Funktion `ospf cost` gegenwärtig für dieses Interface verwendet.

MTU ignorieren

Aktiviert/deaktiviert die IP-MTU-Mismatch-Erkennung (MTU: Maximum Transmission Unit) an diesem OSPF-Interface.

Mögliche Werte:

Deaktiviert die IP-MTU-Prüfung und ermöglicht Adjacencys, wenn der MTU-Wert auf den Interfaces unterschiedlich ist.

(Voreinstellung)

Der Router prüft, ob Nachbarn denselben MTU-Wert an den Interfaces verwenden.

7.4.6 OSPF Virtual Links

[Routing > OSPF > Virtual Links]

Die Funktion `ospfv3 virtual-link` erfordert, dass Sie jede Area mit der Backbone-Area verbinden. Der physische Standort lässt häufig keine direkte Verbindung zum Backbone zu. Virtuelle Datenverbindungen bieten Ihnen die Möglichkeit, physisch getrennte Areas über eine Transit-Area mit der Backbone-Area zu verbinden. Sie legen beide Router an den Endpunkten einer virtuellen Daten-Link als ABR an einer Punkt-zu-Punkt-Verbindung fest.

Tabelle

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

Schaltflächen



Hinzufügen

Öffnet das Fenster `ospfv3 virtual-link`, um eine Tabellenzeile hinzuzufügen.

- In der Dropdown-Liste `Area` wählen Sie die Area-ID für die neue Tabellenzeile.
- Im Feld `Neighbor` legen Sie die Router-ID des virtuellen Nachbarn fest.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Area-ID

Zeigt die Area-ID der Transit-Area, mit welcher der virtuelle Link die einzelnen Areas miteinander verbindet.

Nachbar-ID

Zeigt die Router-ID des virtuellen Nachbarn.

Der Router lernt den Wert aus den vom virtuellen Nachbarn empfangenen Hello-Paketen. Der Wert ist ein statistischer Wert für virtuelle Adjacencys.

Sende-Verzögerung [s]

Legt die geschätzte Anzahl von Sekunden für die Übertragung eines LS-Update-Pakets über dieses Interface fest.

Diese Einstellung ist für langsame Datenverbindungen nützlich. Der Timer erhöht das Alter der LS-Updates, um geschätzte Verzögerungen auf dem Interface auszugleichen. Wird das Paketalter zu sehr erhöht, ist die Antwort jünger als das ursprüngliche Paket.

Mögliche Werte:

(Voreinstellung:)

Retrans-Intervall [s]

Legt für Adjacencies, die zu diesem Interface gehören, die Zeit in Sekunden bis zur erneuten Übertragung von Link State Advertisement fest.

Sie verwenden diesen Wert ebenfalls, wenn Sie die Datenbank-Beschreibung (DD) und die Link-Status-Request-Pakete erneut übertragen.

Mögliche Werte:

(Voreinstellung:)

Dead-Intervall [s]

Legt die Zeit in Sekunden fest, die das Gerät auf Hello-Pakete wartet, bevor es den benachbarten Router als nicht erreichbar deklariert.

Legen Sie den Wert als Vielfaches von fest. Legen Sie den gleichen Wert für die Router-Interfaces innerhalb desselben Bereiches fest.

Mögliche Werte:

(Voreinstellung:)

Legen Sie einen niedrigeren Wert fest, um einen nicht erreichbaren Nachbarn schneller zu erkennen.

Anmerkung: Kleinere Werte sind anfällig für Interoperabilitätsprobleme.

Hello-Intervall [s]

Legt die Zeit in Sekunden zwischen den Übertragungen von Hello-Paketen auf dem Interface fest.

Stellen Sie für Router, die einem gemeinsamen Netz angehören, denselben Wert ein.

Mögliche Werte:

(Voreinstellung:)

Status

Zeigt den Zustand des virtuellen OSPF-Interfaces.

Mögliche Werte:

(Voreinstellung)

Das Interface ist im initialen Zustand und blockiert die Datenpakete.

Gilt ausschließlich für Interfaces, die mit Punkt-zu-Punkt- oder Punkt-zu-Mehrpunkt-Verbindungen angebunden sind, sowie für Virtual-Link-Netze. Das Interface sendet in diesem Zustand im Abstand von Sekunden ein Hello-Paket, um eine Adjacency mit dem Nachbarn herzustellen.

Ereignisse

Zeigt, wie oft dieses Interface aufgrund eines empfangenen Ereignisses seinen Status geändert hat.

Auth Typ

Legt den Authentifizierungstyp für eine virtuelle Datenverbindung fest.

Wenn Sie `clear-text` oder `md5` festlegen, ist es für diesen Router erforderlich, dass andere Router einen Authentifizierungsprozess durchlaufen, bevor dieser Router die betreffenden Router als Nachbarn akzeptiert.

Wenn Sie die Authentifizierung zum Schutz des Netzes verwenden, verwenden Sie für jeden Router in Ihrem autonomen System denselben Typ und Schlüssel.

Mögliche Werte:

(Voreinstellung)

Die Netz-Authentifizierung ist deaktiviert.

Der Router verwendet Klartext-Authentifizierung. In diesem Fall sendet der Router die Passwörter als Klartext.

Der Router verwendet die MD5-Authentifizierung über den Message-Digest-Algorithmus. Dieser Authentifizierungstyp unterstützt Sie dabei, das Netz sicherer zu machen.

Auth key

Legt den Authentifizierungsschlüssel fest.

Nach Eingabe zeigt das Feld `*****` (Sternchen) anstelle des Authentifizierungsschlüssels.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 16 Zeichen

– mit 8 Zeichen, wenn in der Dropdown-Liste `short` der Eintrag ausgewählt ist

– mit 16 Zeichen, wenn in der Dropdown-Liste `full` der Eintrag ausgewählt ist

Wenn Sie einen kürzeren Authentifizierungsschlüssel festlegen, füllt das Gerät die verbleibenden Stellen mit `0`.

Auth key ID

Legt für die Authentifizierungsschlüssel-ID den Wert `0` fest.

Die Option `no-authentication-key` zur verschlüsselten Authentifizierung unterstützt Sie dabei, das Netz gegen passive Angriffe zu schützen, und bietet einen wesentlichen Schutz gegen aktive Angriffe.

Voraussetzung für das Festlegen dieses Wertes ist, dass Spalte `Authentication Key ID` der Wert `0` festgelegt ist.

Mögliche Werte:

(Voreinstellung: `0`)

7.4.7 OSPF Ranges

[Routing > OSPF > Ranges]

In großen Areas reduzieren OSPF-Nachrichten, die ins Netzwerk geflutet werden, die verfügbare Bandbreite und vergrößern die Routing-Tabelle. Eine große Routing-Tabelle erhöht den Grad der CPU-Verarbeitung, die der Router zum Eintragen der Informationen in die Routing-Tabelle benötigt. Eine große Routing-Tabelle reduziert außerdem die Größe des verfügbaren Speichers. Um die Anzahl von OSPF-Nachrichten zu verringern, die das Netz fluten, ermöglicht Ihnen die Funktion [eine große Area in kleinere Subnetze aufzuteilen](#).

Zum Zusammenfassen der Routing-Information, die in ein und aus einem Subnetz fließen, legt der Area Border Router (ABR) das Subnetz als einen einzelnen Adressbereich fest. Der ABR meldet jeden Adressbereich als eine einzelne Route an die externe Area. Die vom ABR für das Subnetz gemeldete IP-Adresse ist ein Paar aus Adresse und Maske. Nicht gemeldete Areas ermöglichen Ihnen, das Vorhandensein von Subnetzen vor anderen Areas zu verbergen.

Der Router legt die Kosten der gemeldeten Route als die höheren Kosten in den eingestellten Komponenten-Subnetzen fest.

Tabelle

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

Schaltflächen



Hinzufügen

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

- In der Dropdown-Liste [Area](#) wählen Sie die Area-ID des Adressbereichs aus.
- In der Dropdown-Liste [Route](#) wählen Sie die Route-Informationen, die durch den Adressbereich zusammengefasst sind.

Mögliche Werte:

[Area](#) Der Area-Bereich fasst Type 5-Routen-Informationen zusammen.

[Area](#) Der Area-Bereich fasst Type 7-Routen-Informationen zusammen.

- Im Feld [IP-Adresse](#) legen Sie die IP-Adresse für das Subnetz der Area fest.
- Im Feld [Netzmaske](#) legen Sie die Netzmaske für das Subnetz der Area fest.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Area-ID

Zeigt die Area -ID des Adressbereichs.

LSDB Typ

Zeigt, welche Route-Informationen durch den Adressbereich zusammengefasst sind.

Mögliche Werte:

Der Area-Bereich fasst Type 5-Routen-Informationen zusammen.

Der Area-Bereich fasst Type 7-Routen-Informationen zusammen.

Netzwerk

Zeigt die IP-Adresse für das Subnetz der Area.

Netzmaske

Zeigt die Netzmaske für das Subnetz der Area.

Effekt

Legt die externe Verbindungsstatusmeldung der Subnetz-Bereiche fest.

Mögliche Werte:

(Voreinstellung)

Der Router meldet den Bereich in anderen Areas.

Der Router hält Bereichs-Verbindungsstatusmeldungen an andere externe Areas zurück.

7.4.8 OSPF Diagnose

[Routing > OSPF > Diagnose]

Um ordnungsgemäß zu funktionieren, basiert die Funktion auf 2 grundlegenden Prozessen.

- Herstellen von Adjacencys
- Nach dem Herstellen von Adjacencys tauschen die benachbarten Router Informationen aus und aktualisieren ihre Routing-Tabellen.

Die in den Registerkarten angezeigten Statistiken helfen Ihnen beim Analysieren der OSPF-Prozesse.

Der Dialog enthält die folgenden Registerkarten:

[Statistiken]
[Link-State Datenbank]
[Nachbarn]
[Virtuelle Nachbarn]
[Link-State Externe Datenbank]
[Route]

[Statistiken]

Um die 2 Grundprozesse durchzuführen, senden und empfangen OSPF-Router verschiedene Nachrichten mit Informationen zum Herstellen von Adjacencys und aktualisieren Routing-Tabellen. Die Zähler in der Registerkarte zeigen, wie viele Nachrichten-Datenpakete die OSPF-Interfaces übertragen haben.

- Link State Acknowledgments (LSAcks) liefern im Rahmen des Link-Status-Datenverkehrs eine Antwort zu einem Link State update (LS update)-Request.
- Die Hello-Pakete ermöglichen einem Router, weitere OSPF-Router in der Area zu erkennen und Adjacencys zwischen den benachbarten Geräten herzustellen. Nach dem Aufbau der Adjacencys, übermitteln die Router ihre Anmeldeinformationen, um eine Rolle als Designated Router (DR), als Backup Designated Router (BDR) oder ausschließlich als ein Teilnehmer im OSPF-Netz herzustellen. Die Router verwenden dann die Hello-Pakete, um Informationen zu den OSPF-Einstellungen im autonomen System (Autonomous System, AS) auszutauschen.
- DD-Nachrichten (Database Description: Datenbankbeschreibung) enthalten Beschreibungen zur AS- oder Area-Topologie. Die Nachrichten übertragen die Inhalte der Link-Status-Datenbank für das AS oder der Area von einem Router an weitere Router in der betreffenden Area.
- Link-Status-Requests (LS-Requests) bieten eine Methode zum Anfordern von aktualisierten Informationen zu einem Teil der Link-Status-Datenbank (LSDB). Die Nachricht legt die Datenverbindung oder Datenverbindungen fest, für die der anfragende Router gegenwärtige Informationen benötigt.
- LS-Update-Nachrichten enthalten aktualisierte Information zum Status bestimmter Datenverbindungen der LSDB. Der Router sendet die Updates als Antwort auf eine LS-Request-Nachricht. Der Router überträgt auch regelmäßig Broadcast- oder Multicast-Nachrichten. Der Router verwendet den Nachrichteninhalte zur Aktualisierung der Informationen in den LSDB der Router, welche diese Nachrichten empfangen.
- LSAs enthalten die lokalen Routing-Informationen für die OSPF-Area. Der Router sendet die LSAs an andere Router in einer OSPF-Area und ausschließlich an Interfaces, die den Router mit der betreffenden OSPF-Area verbinden.
- -LSAs sind Router-LSAs. Jeder Router in einer Area erzeugt ein Router-LSA. Ein einzelnes Router-LSA beschreibt den Status sowie die Kosten jeder Datenverbindung in der betreffenden Area. Der Router flutet Type 1-LSAs ausschließlich in der eigenen Area.

- -LSAs sind Network-LSAs. Der DR generiert eine Network-LSA auf der Grundlage von Informationen, die über die Type 1-LSAs empfangen wurden. Der DR erzeugt in seiner eigenen Area eine Network-LSA für jedes Broadcast- und NBMA-Netz, mit dem der DR verbunden ist. Die LSA beschreibt jeden Router, der an das Netz angeschlossen ist – einschließlich des DR selbst. Der Router flutet Type 2-LSAs ausschließlich in der eigenen Area.
- -LSAs sind Network Summary-LSAs. Ein Area Border Router (ABR) generiert eine einzelne ASBR-Summary-LSA anhand der Informationen, die in den von den DR empfangenen Type 1- und Type 2-LSAs enthalten sind. Der ABR sendet Netz-Summary-LSAs, die Inter-Area-Ziele beschreiben. Der Router flutet Type 3-LSAs in jede Area, die mit dem Router verbunden ist, mit Ausnahme der Area, für die der Router die Type 3-LSA erzeugt hat.
- -LSAs sind Autonomous System Boundary Router (ASBR) summary-LSAs. Ein ABR generiert eine einzelne ASBR-Summary-LSA anhand der Informationen, die in den von den DR empfangenen Type 1- und Type 2-LSAs enthalten sind. Der ABR sendet Type 4-LSAs an andere Areas als die Area, in der er sich befindet, um die ASBRs zu beschreiben, von denen der ABR Type 5-LSAs empfangen hat. Der Router flutet Type 4-LSAs in jede Area, die mit dem Router verbunden ist, mit Ausnahme der Area, für die der Router die Type 4-LSA erzeugt hat.
- -LSAs sind AS external-LSAs. Die AS-Boundary-Router generieren die AS external-LSAs, die Ziele außerhalb des AS beschreiben. Die Type 5-LSAs enthalten Informationen, die von anderen Routing-Prozessen in die Funktion umverteilt werden. Der Router flutet Type 5-LSAs in jeder Area, mit Ausnahme von Stub- und NSSA-Areas.

Funktion

LSA wiederholt gesendet

Zeigt die Gesamtzahl der LSAs, die seit dem Zurücksetzen der Zähler erneut übertragen wurden. Wenn der Router dasselbe LSA an mehrere Nachbarn sendet, erhöht der Router die Anzahl schrittweise für jeden Nachbarn.

Hello empfangen

Zeigt die Gesamtzahl der OSPFv2-Hello-Pakete, die seit dem Zurücksetzen der Zähler empfangen wurden.

Hello gesendet

Zeigt die Gesamtzahl der OSPFv2-Hello-Pakete, die seit dem Zurücksetzen der Zähler übertragen wurden.

Empfangene DB Descriptions

Zeigt die Gesamtzahl der OSPFv2-DD-Pakete, die seit dem Zurücksetzen der Zähler empfangen wurden.

Gesendete DB Descriptions

Zeigt die Gesamtzahl der OSPFv2-DD-Pakete, die seit dem Zurücksetzen der Zähler übertragen wurden.

LS Requests empfangen

Zeigt die Gesamtzahl der OSPFv2-Link-Status-Request-Pakete, die seit dem Zurücksetzen der Zähler empfangen wurden.

LS Requests gesendet

Zeigt die Gesamtzahl der OSPFv2-Link-Status-Request-Pakete, die seit dem Zurücksetzen der Zähler übertragen wurden.

LS Updates empfangen

Zeigt die Gesamtzahl der OSPFv2-LS-Update-Pakete, die seit dem Zurücksetzen der Zähler empfangen wurden.

LS Updates gesendet

Zeigt die Gesamtzahl der OSPFv2-LS-Update-Pakete, die seit dem Zurücksetzen der Zähler übertragen wurden.

LS ACK Updates empfangen

Zeigt die Gesamtzahl der OSPFv2-LS-Acknowledgement-Pakete, die seit dem Zurücksetzen der Zähler empfangen wurden.

LS ACK Updates gesendet

Zeigt die Gesamtzahl der OSPFv2-LS-Acknowledgement-Pakete, die seit dem Zurücksetzen der Zähler übertragen wurden.

Max. Rate innerhalb 5s empfangener LSU

Zeigt die maximale Rate der OSPFv2-Update-Pakete, die seit dem Zurücksetzen der Zähler in einem 5-Sekunden-Intervall empfangen wurden. Zeigt die Rate in Paketen pro Sekunde. Das bedeutet, dass die Anzahl der innerhalb des 5-Sekunden-Intervalls empfangenen Pakete durch 5 geteilt wird.

Max. Rate innerhalb 5s gesendeter LSU

Zeigt die maximale Rate der OSPFv2-Update-Pakete, die seit dem Zurücksetzen der Zähler in einem 5-Sekunden-Intervall übertragen wurden. Zeigt die Rate in Paketen pro Sekunde. Das bedeutet, dass die Anzahl der innerhalb des 5-Sekunden-Intervalls übertragenen Pakete durch 5 geteilt wird.

Typ-1 (router) LSAs empfangen

Zeigt die Anzahl der Type 1 router-LSAs, die seit dem Zurücksetzen der Zähler empfangen wurden.

Typ-2 (network) LSAs empfangen

Zeigt die Anzahl der Type 2 network-LSAs, die seit dem Zurücksetzen der Zähler empfangen wurden.

Typ-3 (summary) LSAs empfangen

Zeigt die Anzahl der Type 3 network summary-LSAs, die seit dem Zurücksetzen der Zähler empfangen wurden.

Typ-4 (ASBR) LSAs empfangen

Zeigt die Anzahl der Type 4 ASBR summary-LSAs, die seit dem Zurücksetzen der Zähler empfangen wurden.

Typ-5 (external) LSAs empfangen

Zeigt die Anzahl der Type 5 external-LSAs, die seit dem Zurücksetzen der Zähler empfangen wurden.

[Link-State Datenbank]

Ein Router führt eine separate Link-Status-Datenbank für jede Area, zu der er gehört.

Der Router fügt der Datenbank in den folgenden Fällen LSAs hinzu:

- Wenn der Router ein LSA empfängt, zum Beispiel beim Fluten.
- Wenn der Router das LSA erzeugt.

Wenn ein Router ein LSA aus der Datenbank löscht, entfernt er das LSA auch aus den Link-Status-Retransmission-Listen der anderen Router im Netz. Ein Router löscht in den folgenden Fällen ein LSA aus der zugehörigen Datenbank:

- Eine neuere Instanz überschreibt das LSA während des Flutungsvorganges.
- Der Router erzeugt eine neuere Instanz einer selbst erzeugten LSA.
- Das LSA veraltet und der Router entfernt das LSA aus der Routing-Domäne.

Tabelle

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

Area-ID

Zeigt die Area-ID, von welcher der Router das LSA empfangen hat.

Typ

Zeigt den Typ der empfangenen LSAs.

Jeder LSA-Typ verfügt über ein separates Format für die Verbindungsstatusmeldung.

Mögliche Werte:

Der Router hat die Informationen von einem anderen Router aus derselben Area empfangen. Router melden ihre Existenz und listen die Datenverbindungen zu anderen Routern innerhalb derselben Area auf, in einem Type 1-LSA. Die Link-Status -ID ist die Ausgangs-Router -ID.

Der Router hat die Informationen von einem DR an einem Broadcast-Segment empfangen, das Type 2-LSA verwendet. Der DR stellt die Informationen, die in Type 1-LSAs empfangen wurden, zusammen und listet die durch das Segment miteinander verbundenen Router auf. Die Link-Status -ID ist die IP -Interface-Adresse des DR.

Der Router hat die Informationen von einem ABR empfangen, der Type 3-LSA zur Beschreibung von Routen zu Netzen verwendet. Bevor ABR die Routing-Informationen an andere Areas senden, stellen ABR von Type 1-LSAs und Type 2-LSAs gelernte Informationen zusammen, die von den angeschlossenen Areas empfangen wurden. Die Link-Status -ID ist die Zielnetz-Nummer, die aus dem Summarization-Prozess resultiert.

Der Router hat die Informationen von einem ABR empfangen, der Type 4-LSA zur Beschreibung von Routen zu ASBR verwendet. Bevor ABR die Routing-Informationen an andere Areas senden, stellen ABR von Type 1-LSAs und Type 2-LSAs gelernte Informationen zusammen, die von den angeschlossenen Areas empfangen wurden. Die Link-Status -ID ist die Zielnetz-Nummer.

Der Router hat die Informationen von einem ASBR empfangen, der Type 5-LSA zur Beschreibung von Routen zu einem anderen AS verwendet. Die Link-Status -ID ist die Router -ID des ASBR.

Der Router hat die Informationen von einem Router in einer NSSA empfangen, der Type 7-LSA verwendet.

LSID

Zeigt den Link-Status-ID(LSID)-Wert, der im LSA empfangen wurde.

Die LSID ist ein Feld im LSA-Header. Das Feld enthält abhängig vom LSA-Typ entweder eine Router-ID oder eine IP-Adresse.

Mögliche Werte:

Gültige IPv4-Adresse

Router-ID

Zeigt die Router-ID, die den Ausgangs-Router eindeutig identifiziert.

Sequenz

Zeigt den Wert des Sequenzfeldes in einer LSA.

Der Router untersucht den Inhalt des LS-Prüfsummen-Feldes immer dann, wenn das Feld für die LS-Sequenznummer angibt, dass 2 Instanzen eines LSA miteinander übereinstimmen. Weichen die Werte voneinander ab, betrachtet der Router die Instanz mit der höheren LS-Prüfsumme als die aktuelle Instanz.

Alter

Zeigt das Alter des LSA in Sekunden.

Wenn der Router das LSA generiert, setzt der Router das LSA-Alter auf den Wert `0`. Bei der Übertragung des LSA durch die Router im Netz erhöhen die Router den Wert schrittweise um den in Spalte `Alter` festgelegten Wert.

Wenn ein Router 2 LSAs für dasselbe Segment empfängt, die identische LS-Sequenznummern und LS-Prüfsummen aufweisen, prüft der Router das Alter der LSAs.

- LSAs mit dem maximalen Alter akzeptiert der Router sofort.
- Andernfalls akzeptiert der Router das LSA mit dem geringeren Alter.

Checksumme

Zeigt den Inhalt der Prüfsumme.

Das Feld ist eine Prüfsumme für den gesamten Inhalt der LSA, mit Ausnahme des Feldes „Alter“. Der Wert im Age-Feld des Advertisements erhöht sich mit jedem Router, der die Nachricht überträgt. Der Router kann die Nachricht senden, ohne das Prüfsummenfeld zu aktualisieren, wenn er das Age-Feld nicht berücksichtigt.

[Nachbarn]

Das Hello-Paket ist zuständig für die Nachbarerkennung und -pflege sowie für die bidirektionale Kommunikation zwischen Nachbarn.

Während der Erkennung vergleichen die Router an einem Segment ihre Einstellungen auf Kompatibilität. Sind die Router kompatibel, stellen die Router Adjacencies her. Die Router erkennen ihren Master- oder Slave-Status anhand der in den Hello-Paketen enthaltenen Informationen.

Um ihre Routing-Datenbanken zu synchronisieren, tauschen sie nach der Erkennung ihrer Rollen Routing-Informationen aus. Nach Abschluss der Aktualisierung der Router-Datenbanken ist eine vollständige Adjacency der Nachbarn hergestellt und das LSA führt seine Adjacency in der Liste auf.

Tabelle

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

Nachbar-ID

Zeigt die Router -ID des benachbarten Routers.

Der Router lernt den Wert aus den vom Nachbarn empfangenen Hello-Paketen. Der Wert ist ein statistischer Wert für virtuelle Adjacencies.

IP-Adresse

Zeigt die IP-Adresse des benachbarten Router-Interface, das an den Port angeschlossen ist.

Der Router verwendet den Wert beim Senden von Unicast-Protokollpaketen zu dieser Adjacency als IP-Zieladresse. Wenn der benachbarte Router der DR ist, wird der Router auch in Router-LSAs als Link-ID für das angeschlossene Netz verwendet. Der Router lernt die IP-Adresse des Nachbarn, wenn der Router Hello-Pakete vom Nachbarn empfängt. Für virtuelle Datenverbindungen lernt der Router die IP-Adresse des Nachbarn beim Aufbau der Routing-Tabelle.

Interface

Zeigt das Interface, auf das sich die Tabellenzeile bezieht.

Status

Zeigt den Status der Beziehung zu dem in dieser Instanz aufgeführten Nachbarn.

Ein Ereignis bewirkt eine Statusänderung, wie der Empfang eines Hello-Pakets. Dieses Ereignis hat abhängig vom gegenwärtigen Status des Nachbarn verschiedene Auswirkungen. Außerdem lösen die Router abhängig vom Status der Änderung des Nachbarn eine DR-Auswahl aus.

Mögliche Werte:

(Voreinstellung)

Initialer Zustand einer Nachbarkonversation oder eines Routers, der die Konversation aufgrund des Ablaufs des Timers beendet hat.

Dieser Status gilt nur für Nachbarn, die mit den NBMA-Netzen verbunden sind. Die Informationen dieses Nachbarn werden nicht aufgelöst. Der Router versucht aktiv, den Nachbarn zu kontaktieren, indem er in einem Intervall, das in Spalte festgelegt ist, Hello-Pakete an den Nachbarn sendet.

Der Router hat kürzlich von seinem Nachbarn ein Hello-Paket empfangen. Der Router hat ausschließlich eine unidirektionale Kommunikation mit dem Nachbarn aufgebaut. So fehlt beispielsweise die Router-ID dieses Routers im Hello-Paket des Nachbarn. Das zugehörige Interface listet beim Senden von Hello-Paketen Nachbarn mit diesem Status oder einem höheren Status auf.

Die Kommunikation zwischen 2 Routern ist bidirektional. Der Router verifiziert den Vorgang, indem er den Inhalt des Hello-Pakets untersucht. Die Router wählen im oder nach dem bidirektionalen Zustand einen DR und BDR aus dem Satz von Nachbarn.

Erster Schritt beim Einrichten einer Adjacency zwischen 2 benachbarten Routern. Ziel dieses Schritts ist es, zu entscheiden, welcher Router der Master ist, und um die initiale Nummer zu bestimmen.

Der Router macht seine gesamte Link-Status-Datenbank bekannt, indem er DD-Pakete (Database Description) an den Nachbarn sendet. Der Router bestätigt explizit jedes DD-Paket. Jedes Paket verfügt über eine Sequenznummer. Die Adjacencys lassen nur zu, dass zu einem bestimmten Zeitpunkt jeweils ein DD-Paket aussteht. In diesem Zustand sendet der Router LS-Request-Pakete, die aktuelle Datenbankinformationen anfordern. Die Adjacencys sind vollständig in der Lage, OSPF-Routing-Protokoll-Pakete zu übertragen.

Der Router sendet LS-Request-Pakete an den Nachbarn, die Informationen zu den ausstehenden Datenbank-Updates anfordern, welche im Datenaustausch-Status gesendet wurden.

Die benachbarten Router weisen eine vollständige Adjacency auf. Die Adjacencys erscheinen nun in Router-LSAs und Netz-LSAs.

Dead time

Zeigt den Zeitraum, der verbleibt, bevor der Router den Nachbarn als nicht erreichbar deklariert. Der Timer initiiert das Herunterzählen, nachdem der Router ein Hello-Paket empfängt.

[Virtuelle Nachbarn]

Die Funktion `ospf virtual-link` erfordert eine kontinuierliche Verbindung der Autonomous-System-Backbone-Area. Außerdem erfordert die Funktion `ospf virtual-link`, dass jede Area über eine Verbindung zur Backbone-Area verfügt. Der physische Standort von Routern lässt häufig nicht zu, dass eine Area direkt an die Backbone-Area angeschlossen wird. Virtuelle Datenverbindungen bieten Ihnen die Möglichkeit, physisch getrennte Areas mit der Backbone-Area zu verbinden.

Die ABR der Backbone-Area und die physisch getrennte Area bilden über eine Transit-Area eine Punkt-zu-Punkt-Verbindung. Wenn die ABR eine Adjacency herstellen, schließen die Backbone-Router-LSAs die Datenverbindung und den OSPF-Paketfluss über die virtuelle Datenverbindung ein. Außerdem schließt die Routing-Datenbank jedes Endpunkt-Routers die Link-Status-Informationen des anderen Endpunkt-Routers ein.

Anmerkung: Die Funktion `ospf virtual-link` ermöglicht Ihnen, mit Ausnahme von Stub-Areas durch jeden Area-Typ virtuelle Datenverbindungen festzulegen.

Tabelle

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

Area-ID

Zeigt die Transit-Area-ID der virtuellen Datenverbindung.

Router-ID

Zeigt die Router-ID des anderen virtuellen Endpunkt-ABR.

Nach der Bildung von virtuellen Adjacencys überträgt die virtuelle Datenverbindung OSPF-Pakete wie Hello-Pakete und LS-Update-Pakete, die Datenbankinformationen enthalten. Voraussetzung ist, dass die LSAs des Nachbar-Routers die Router-ID des lokalen Routers enthalten.

IP-Adresse

Zeigt die IP-Adresse des virtuellen Nachbarn.

Der Router verwendet die IP-Adresse, um OSPF-Pakete über das Transit-Netz an den virtuellen Nachbarn zu senden.

Optionen

Zeigt die Informationen, die im Feld Options des LSA enthalten sind. Dieser Wert zeigt die Funktionsmerkmale des virtuellen Nachbarn.

Das Options-Feld, das in den Hello-Paketen verwendet wird, ermöglicht einem Router, seine optionalen Funktionsmerkmale zu identifizieren und anderen Routern mitzuteilen. Dieser Mechanismus ermöglicht Ihnen, verschiedene Router mit unterschiedlichen Funktionsmerkmalen innerhalb einer Routing-Domäne zu verwenden.

Der Router unterstützt 4 Optionen, indem er, abhängig von den Funktionsmerkmalen des Routers, folgende Bits im Feld Options entweder auf einen hohen oder einen niedrigen Wert setzt. Das Feld zeigt den Wert, indem die folgenden Options-Bits addiert werden. Sie lesen die Felder vom niedrigwertigen zum höchstwertigen Bit.

- Die Router geben ihre Fähigkeit bekannt, TOS 0 in AS-External-Routen zu verarbeiten, wenn das E-Bit auf einen hohen Wert gesetzt ist. Das E-Bit ist das zweite Bit im Feld Options und repräsentiert den Wert 2^1 oder 2.
- Die Router geben ihre Fähigkeit zur Verarbeitung von Multicast-Routen bekannt, wenn das MC-Bit auf einen hohen Wert gesetzt ist. Das MC-Bit ist das dritte Bit im Feld Options und repräsentiert den Wert 2^2 oder 4.
- Die Router geben ihre Fähigkeit zur Verarbeitung von AS-External-Routen in einer NSSA-Summary mit Type 7-LSAs bekannt, wenn das N/P-Bit auf einen hohen Wert gesetzt ist. Das N/P-Bit ist das vierte Bit im Feld Options und repräsentiert den Wert 2^3 oder 8.
- Die Router geben ihre Fähigkeit zur Verarbeitung von Request-Circuits bekannt, wenn das DC-Bit auf einen hohen Wert gesetzt ist. Das DC-Bit ist das sechste Bit im Feld Options und repräsentiert den Wert 2^5 oder 32.

In besonderen Fällen setzt der Router das E-Bit auf einen niedrigen Wert.

- Die Router geben ihre Fähigkeit zur Verarbeitung von TOS-Metriken bekannt, bei denen es sich nicht um TOS 0 handelt, wenn das E-Bit auf einen niedrigen Wert gesetzt ist. Das E-Bit ist das zweite Bit im Feld Options und repräsentiert den Wert 0, wenn es auf einen niedrigen Wert gesetzt ist.

Mögliche Werte:

Zeigt, dass der virtuelle Nachbar die Metrik Type of Service (TOS) 0 in AS-External-LSAs unterstützt.

Zeigt, dass der virtuelle Nachbar TOS-Metriken unterstützt, bei denen es sich nicht um TOS 0 handelt.

Zeigt, dass der virtuelle Nachbar Multicast-Routing unterstützt.

Zeigt, dass der virtuelle Nachbar Type 7-LSAs unterstützt.

Zeigt, dass der virtuelle Nachbar Demand-Circuits unterstützt.

Status

Zeigt den Status der Beziehung zu dem in dieser Instanz aufgeführten Nachbarn.

Ein Ereignis bewirkt eine Statusänderung, wie der Empfang eines Hello-Pakets. Dieses Ereignis hat abhängig vom gegenwärtigen Status des Nachbarn verschiedene Auswirkungen. Außerdem lösen die Router abhängig vom Status der Änderung des Nachbarn eine DR-Auswahl aus.

Mögliche Werte:

(Voreinstellung)

Initialer Zustand einer Nachbarkonversation oder eines Routers, der die Konversation aufgrund des Ablaufs des Timers beendet hat.

Dieser Status gilt nur für Nachbarn, die mit den NBMA-Netzen verbunden sind. Die Informationen des Nachbarn werden nicht aufgelöst. Der Router versucht aktiv, den Nachbarn zu kontaktieren, indem er in einem Intervall, das in Spalte festgelegt ist, Hello-Pakete an den Nachbarn sendet.

Der Router hat kürzlich von seinem Nachbarn ein Hello-Paket empfangen. Der Router hat ausschließlich eine unidirektionale Kommunikation mit dem Nachbarn aufgebaut. So fehlt beispielsweise die Router-ID dieses Routers im Hello-Paket des Nachbarn. Das zugehörige Interface listet beim Senden von Hello-Paketen Nachbarn mit diesem Status oder einem höheren Status auf.

Die Kommunikation zwischen 2 Routern ist bidirektional. Der Router verifiziert den Vorgang, indem er den Inhalt des Hello-Pakets untersucht. Die Router wählen im oder nach dem bidirektionalen Zustand einen DR und BDR aus dem Satz von Nachbarn.

Erster Schritt beim Einrichten einer Adjacency zwischen 2 benachbarten Routern. Ziel dieses Schritts ist es, zu entscheiden, welcher Router der Master ist, und um die initiale Nummer zu bestimmen.

Der Router macht seine gesamte Link-Status-Datenbank bekannt, indem er DD-Pakete (Database Description) an den Nachbarn sendet. Der Router bestätigt explizit jedes DD-Paket. Jedes Paket verfügt über eine Sequenznummer. Die Adjacencys lassen nur zu, dass zu einem bestimmten Zeitpunkt jeweils ein DD-Paket aussteht. In diesem Zustand sendet der Router LS-Request-Pakete, die aktuelle Datenbankinformationen anfordern. Die Adjacencys sind vollständig in der Lage, OSPF-Routing-Protokoll-Pakete zu übertragen.

Der Router sendet LS-Request-Pakete an den Nachbarn, die Informationen zu den ausstehenden Datenbank-Updates anfordern, welche im Datenaustausch-Status gesendet wurden.

Die benachbarten Router weisen eine vollständige Adjacency auf. Die Adjacencys erscheinen nun in Router-LSAs und Netz-LSAs.

Ereignisse

Zeigt, wie oft dieses Interface aufgrund eines empfangenen Ereignisses seinen Status geändert hat. Zum Beispiel, wenn das Gerät ein Hello-Paket empfangen oder das Gerät eine bidirektionale Kommunikation aufgebaut hat.

Länge der Retransmission-Queue

Zeigt die Länge der Übertragungswiederholungsliste.

Um die LSAs aus einem Interface zum Nachbarn zu fluten, setzt der Router die LSAs auf die Link-Status-Übertragungswiederholungsliste der Adjacency. Um die LSA-Flutung zu validieren, überträgt der Router die LSAs erneut, bis der Nachbar den Empfang der LSAs bestätigt. Die Länge des Zeitraums zwischen den Übertragungswiederholungen richten Sie im Dialog

in Spalte ein.

Unterdrückte Hellos

Zeigt, ob der Router Hello-Pakete an den Nachbarn unterdrückt.

Das Unterdrücken der Übertragung von Hello-Paketen an den Nachbarn ermöglicht, Demand-Circuits an Punkt-zu-Punkt-Verbindungen in Zeiträumen der Inaktivität zu schließen. In NBMA-Netzen bleibt der Circuit durch die regelmäßige Übertragung von LSAs aktiv.

Mögliche Werte:

Der Router unterdrückt Hello-Pakete.

Der Router überträgt Hello-Pakete.

[Link-State Externe Datenbank]

Die Tabelle zeigt den Inhalt der externen Link-Status-Datenbank, wobei für jede eindeutige Link-Status-ID ein Eintrag existiert. Externe Datenverbindungen ermöglichen der Area, eine Verbindung zu Zielen außerhalb des autonomen Systems herstellen. Router geben Informationen zu den externen Datenverbindungen im gesamten Netz in Form von Link State updates weiter.

Tabelle

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

Typ

Zeigt den Typ der Link State Advertisement. Wenn der Router eine externe Link State Advertisement erkennt, trägt der Router die Informationen in die Tabelle ein.

Mögliche Werte:

LSID

Zeigt, dass die Link-Status-ID ein LS-Typ-spezifisches Feld ist, das entweder eine Router-ID oder eine IP-Adresse enthält. Der Wert identifiziert die in der Nachricht beschriebene Routing-Domäne.

Router-ID

Zeigt die Router-ID, die den Ausgangs-Router eindeutig identifiziert.

Sequenz

Zeigt den Wert des Sequenzfeldes in einer LSA.

Der Router untersucht den Inhalt des LS-Prüfsummen-Feldes immer dann, wenn das Feld für die LS-Sequenznummer angibt, dass 2 Instanzen eines LSA miteinander übereinstimmen. Weichen die Werte voneinander ab, betrachtet der Router die Instanz mit der höheren LS-Prüfsumme als die aktuelle Instanz.

Alter

Zeigt das Alter des LSA in Sekunden.

Wenn der Router das LSA generiert, setzt der Router das LSA-Alter auf den Wert `0`. Bei der Übertragung des LSA durch die Router im Netz erhöhen die Router den Wert schrittweise um den in Spalte `Alter` festgelegten Wert.

Wenn ein Router 2 LSAs für dasselbe Segment empfängt, die identische LS-Sequenznummern und LS-Prüfsummen aufweisen, prüft der Router das Alter der LSAs.

- LSAs mit dem maximalen Alter verwirft der Router sofort.
- Andernfalls verwirft der Router LSAs dem geringeren Alter.

Checksumme

Zeigt den Inhalt der Prüfsumme.

Das Feld ist eine Prüfsumme für den gesamten Inhalt der LSA, mit Ausnahme des Feldes „Alter“. Der Wert im Feld „Alter“ der Verbindungsstatusmeldung steigt während der Übertragung der Nachricht im Netz durch die Router. Der Router kann die Nachricht senden, ohne das Prüfsummenfeld zu aktualisieren, wenn er das Age-Feld nicht berücksichtigt.

[Route]

Der Dialog zeigt die anhand der Verbindungsstatusmeldungen (LSA: Link State Advertisements) gelernten OSPF-Routen-Informationen.

Tabelle

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

IP-Adresse

Zeigt die IP-Adresse des Netzes oder Subnetzes für die Route.

Netzmaske

Zeigt die Netzmaske für das Netz oder Subnetz.

Metrik

Zeigt die Routenkosten zum Erreichen des Netzes, die im SPF-Algorithmus berechnet wurden.

Typ

Zeigt den Typ der von OSPF gelernten Route.

Mögliche Werte:

Eintrag für Routen aus dem OSPF innerhalb einer Area.

Eintrag für Routen aus dem OSPF zwischen Areas.

Diese Routen wurden von einem Autonomous System Boundary Router (ASBR) in die OSPF-Area importiert. Diese Routen verwenden die Kosten in Bezug auf die Verbindung zwischen dem ASBR und der Route (einschließlich dieses Geräts).

Diese Routen wurden von einem Autonomous System Boundary Router (ASBR) in die OSPF-Area importiert. Diese Routen verwenden nicht die Kosten in Bezug auf die Verbindung zwischen dem ASBR und der Route (einschließlich dieses Geräts).

Diese Routen wurden von einem Autonomous System Boundary Router (ASBR) in die Not-So-Stub-Area importiert. Diese Routen verwenden die Kosten in Bezug auf die Verbindung zwischen dem ASBR und der Route (einschließlich dieses Geräts).

Diese Routen wurden von einem Autonomous System Boundary Router (ASBR) in die Not-So-Stub-Area importiert. Diese Routen verwenden nicht die Kosten in Bezug auf die Verbindung zwischen dem ASBR und der Route (einschließlich dieses Geräts).

7.5 Routing-Tabelle

[Routing > Routing-Tabelle]

Dieser Dialog zeigt die Routing-Tabelle mit den im Gerät eingerichteten Routen. Anhand der Routing-Tabelle lernt das Gerät, über welches Router-Interface es IP-Pakete vermittelt, die an Empfänger in einem anderen Netz adressiert sind.

Konfiguration

Präferenz

Legt die Preference-Kennzahl fest, die das Gerät per Voreinstellung den neu eingerichteten, statischen Routen zuweist.

Mögliche Werte:

(Voreinstellung:)

Routen mit dem Wert ignoriert das Gerät bei der Routing-Entscheidung.

Tabelle

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

Schaltflächen



Hinzufügen

Öffnet das Fenster , um eine statische Route hinzuzufügen.

- Im Feld legen Sie die Adresse des Zielnetzes fest.
 Mögliche Werte:
 Gültige IPv4-Adresse
 Wenn Sie eine Standard-Route () festlegen, dann legen Sie im Feld ein Standard-Gateway fest. Diese Einstellung hat Vorrang vor der Einstellung im folgenden Dialog:
 – Dialog , Feld
- Im Feld legen Sie die Netzmaske fest, die den Netzpräfix in der Adresse des Zielnetzes kennzeichnet.
 Mögliche Werte:
 Gültige IPv4-Netzmaske
- Im Feld legen Sie IP-Adresse des nächsten Routers auf dem Pfad ins Zielnetz fest.
 Mögliche Werte:
 Gültige IPv4-Adresse
 Um eine -Route zu erstellen, legen Sie in diesem Feld den Wert fest. Mit dieser Route verwirft das Gerät IP-Pakete, die an das Zielnetz adressiert sind, und informiert den Absender.
- Im Feld legen Sie die Preference-Kennzahl fest, anhand der das Gerät entscheidet, welche von mehreren vorhandenen Routen zum Zielnetz es verwendet.
 Mögliche Werte:

 Bei der Routing-Entscheidung bevorzugt das Gerät die Route mit dem numerisch niedrigsten Wert. Voreingestellt ist der im Rahmen , Feld festgelegte Wert.
- In der Dropdown-Liste wählen Sie das Tracking-Objekt aus, mit dem das Gerät die Route verknüpft.
 Mögliche Werte:

 Kein Tracking-Objekt ausgewählt.
 Name des Tracking-Objekts, zusammengesetzt aus und .



Löschen

Entfernt die ausgewählte Tabellenzeile.

Port

Zeigt das Router-Interface, über welches das Gerät an das Zielnetz adressierte IP-Pakete gegenwärtig sendet.

Mögliche Werte:

Das Gerät vermittelt an das Zielnetz adressierte IP-Pakete über dieses Router-Interface.

Die statische Route ist gegenwärtig keinem Router-Interface zugewiesen.

Netz-Adresse

Zeigt die Adresse des Zielnetzes.

Netzmaske

Zeigt die Netzmaske.

Next-Hop IP-Adresse

Zeigt die IP-Adresse des nächsten Routers auf dem Pfad ins Zielnetz.

Typ

Zeigt den Typ der Route.

Mögliche Werte:

Das Router-Interface ist mit dem Zielnetz direkt verbunden.

Das Router-Interface ist mit dem Zielnetz über einen Router () verbunden.

Das Gerät verwirft an das Zielnetz adressierte IP-Pakete und informiert den Absender.


Die Route ist inaktiv. Siehe Kontrollkästchen .

Protokoll

Zeigt, wer diese Route erzeugt hat.

Mögliche Werte:

Das Gerät hat diese Route beim Einrichten des Router-Interfaces hinzugefügt. Siehe Dialog .

Ein Benutzer hat diese statische Route mit der Schaltfläche  hinzugefügt.

Anmerkung: Sie können statische Routen mit gleichem Ziel und Präferenz, aber mit unterschiedlichen nächsten Hops erstellen. Das Gerät verwendet den ECMP-Forwarding-Mechanismus (Equal Cost Multi Path), um für Lastverteilung und Redundanz über das Netz zu sorgen. Abhängig vom Routing-Profil, das im Dialog ausgewählt ist, kann ECMP bis zu 4 Routen verwenden. Wenn Sie das Routing-Profil wählen, kann ECMP bis zu 16 Routen verwenden.

Die Funktion hat diese Route hinzugefügt. Siehe Dialog .

Präferenz

Legt die „Administrative Distanz“ der Route fest.


Das Gerät verwendet diesen Wert anstatt der Metrik, wenn die Metrik der Routen nicht vergleichbar ist.

Mögliche Werte:

Reserviert für Routen, die das Gerät beim Einrichten der Router-Interfaces hinzugefügt hat. Diese Routen haben in Spalte den Wert .

Bei der Routing-Entscheidung bevorzugt das Gerät die Route mit dem numerisch niedrigsten Wert.

Das Gerät ignoriert die Route bei der Routing-Entscheidung.

Die Administrative Distanz ist einstellbar für statische, mit der Schaltfläche  hinzugefügte Routen.

Metrik

Zeigt die Metrik der Route.

Das Gerät sendet die Datenpakete über die Route mit dem numerisch niedrigsten Wert.

Letztes Update [s]

Zeigt die Zeit in Sekunden, seit der die gegenwärtigen Einstellungen der Route in der Routing-Tabelle eingetragen sind.

Track-Name

Legt das Tracking-Objekt fest, mit dem das Gerät die Route verknüpft.

Das Gerät aktiviert oder deaktiviert automatisch statische Routen – abhängig vom Link-Status eines Interfaces oder von der Erreichbarkeit eines entfernten Routers oder Endgeräts.

Tracking-Objekte richten Sie ein im Dialog .

Mögliche Werte:

Name des Tracking-Objekts, zusammensetzt aus und .

Kein Tracking-Objekt ausgewählt.

Diese Funktion ist ausschließlich für statische Routen nutzbar. (Spalte =)

Aktiv

Zeigt, ob die Route aktiv oder inaktiv ist.

Mögliche Werte:

Die Route ist aktiv, das Gerät verwendet die Route.

Die Route ist inaktiv.

7.6 L3-Relay

[Routing > L3-Relay]

Clients in einem Schicht-3-Subnetz senden Bootstrap Protocol (BOOTP)-/Dynamic Host Configuration Protocol (DHCP)-Broadcast-Nachrichten an den DHCP-Server, um Informationen zu Netzwerkeinstellungen, wie IP-Adressen, anzufordern. Router helfen dabei, eine Grenze für Broadcast-Nachrichten zu schaffen, so dass BOOTP/DHCP-Anfragen auf das lokale Subnetz beschränkt bleiben. Die Funktion `ip dhcp relay` fungiert als ein Proxy für Clients, die Information von einem BOOTP-/DHCP-Server in einem anderen Layer 3-Netzsegment anfordern.

Wenn Sie das Client-Gerät so konfigurieren, dass es seine Netzwerkeinstellungen von einem Dynamic Host Configuration Protocol (DHCP)-Server abrufen, der sich in einem anderen Subnetz befindet, kann das Netzwerkgerät mit der Funktion `ip dhcp relay` Anfragen an einen BOOTP/DHCP-Server weiterleiten, der sich in einem anderen Netzwerk befindet.

Mithilfe von IP-Helper-Adressen und UDP-Helper-Ports leitet die L3-Relay-Funktion Dynamic Host Configuration Protocol (DHCP)-Pakete zwischen den Clients und den Servern weiter. Die IP-Helper-Adresse ist die IP-Adresse des DHCP-Servers.

Clients verwenden den UDP-Helper-Port, um Broadcast-Anfragen an DHCP-Server auf UDP-Port `67` zu senden.

Funktion

Funktion

Schaltet die Funktion `ip dhcp relay` ein/aus.

Mögliche Werte:

Die Funktion `ip dhcp relay` ist global eingeschaltet.
(Voreinstellung)

Die Funktion `ip dhcp relay` ist global ausgeschaltet.

Konfiguration

Circuit-ID

Aktiviert/deaktiviert den Circuit-ID-Option-Modus für BOOTP/DHCP.

Das Netzwerkgerät sendet die Circuit-ID-Suboption-Information, die den lokalen Agenten identifiziert, an den DHCP-Server. Wenn der DHCP-Server antwortet, dann erkennt das Netzwerkgerät seine Rolle als den L3-Relay-Agenten. Die Suboption-Information hilft dem Netzwerkgerät dabei, die Antworten an den richtigen Agenten zurückzusenden.

Mögliche Werte:

Das Gerät fügt die Circuit-ID des DHCP-L3-Relay-Agenten zu den Suboptionen für Client-Anfragen hinzu.

(Voreinstellung)

Das Gerät fügt die Circuit-ID seines DHCP-L3-Relay-Agenten nicht zu den Suboptionen für Client-Anfragen hinzu.

BOOTP/DHCP Wartezeit (min.)

Legt die Mindestzeit in Sekunden fest, die das Gerät wartet, bevor es die BOOTP/DHCP-Anfrage weiterleitet.

Die Endgeräte senden Broadcast-Anfragen in das lokale Netz. Die Einstellung ermöglicht einem lokalen BOOTP/DHCP-Server, auf die Client-Anfrage zu antworten, bevor der Router die Client-Anfrage weiterleitet.

Mögliche Werte:

(Voreinstellung:)

Wenn ein lokaler BOOTP/DHCP-Server im Netz fehlt, dann setzen Sie den Wert auf .

BOOTP/DHCP-Hops (max.)

Legt die Höchstzahl an kaskadierten Relay-Agent-Geräten fest, welche die BOOTP/DHCP-Anfrage weiterleiten dürfen. Jedes Relay-Agent-Gerät, das eine Nachricht weiterleitet, erhöht den Hop-Count-Wert um .

Übersteigt die Anzahl der Hops eines empfangenen BOOTP/DHCP-Pakets die hier angegebene maximale Anzahl von Hops, dann verwirft das Gerät die BOOTP-Anfrage. Dies verhindert, dass sich die Nachricht innerhalb des Netzes unendlich oft wiederholt.

Mögliche Werte:

(Voreinstellung:)

Information

Die folgenden Feldern zeigen die Werte seit dem letzten Neustart des Geräts. Nach einem Neustart setzt das Gerät die Werte auf zurück.

DHCP-Client empfangene Messages

Zeigt die Anzahl der vom Gerät empfangenen DHCP-Requests der Clients.

DHCP-Client weitergeleitete Messages

Zeigt die Anzahl der DHCP-Requests, die das Gerät an die in der Tabelle festgelegten Server weitergeleitet hat.

DHCP-Server empfangene Messages

Zeigt die Anzahl der DHCP-Offers, die das Gerät von den in der Tabelle festgelegten Servern empfangen hat.

DHCP-Server weitergeleitete Messages

Zeigt die Anzahl der DHCP-Offers, die das Gerät von den in der Tabelle festgelegten Servern empfangen und an die Clients weitergeleitet hat.

Empfangene UDP-Nachrichten

Zeigt die Anzahl der vom Gerät empfangenen UDP-Requests der Clients.

Weitergeleitete UDP-Nachrichten

Zeigt die Anzahl der UDP-Requests, die das Gerät an die in der Tabelle festgelegten Server weitergeleitet hat.

Pakete mit abgelaufener TTL

Zeigt die Anzahl der vom Gerät empfangenen UDP-Pakete mit abgelaufenem TTL-Wert.

Verworfen Pakete

Zeigt die Anzahl der UDP-Pakete, die das Gerät verworfen hat.


Tabelle

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

Schaltflächen



Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld  legen Sie das Port-basierte Router-Interface fest.

Anmerkung: Auf VLAN-basierten Router-Interfaces unterstützt das Gerät die Funktion nicht.

Mögliche Werte:

(Voreinstellung)

Das Gerät verarbeitet die Datenpakete, die es auf all seinen Interfaces empfangen hat. Relay-Einträge mit diesem Wert legen eine globale Konfiguration fest.

Das Gerät verarbeitet die Datenpakete, die es auf den festgelegten Interfaces empfangen hat.

Konfigurationen von Interfaces haben Vorrang vor globalen Konfigurationen. Wenn der Ziel-UDP-Port für ein Paket mit einem Eintrag in einem Eingangs-Interface übereinstimmt, dann verarbeitet das Gerät das Paket entsprechend der Interface-Konfiguration. Wenn keiner der Interface-Einträge auf das Paket zutrifft, dann verarbeitet das Gerät das Datenpaket entsprechend der globalen Konfiguration.

- Im Feld legen Sie die Werte der UDP-Helper-Ports für Datenpakete fest, die das Gerät an diesem Interface empfängt. Bei aktiver Funktion leitet das Gerät erhaltene Datenpakete mit diesem Ziel-UDP-Port-Wert an die in im Feld festgelegte IP-Adresse weiter.
Mögliche Werte:

Entspricht dem UDP-Port .
Das Gerät leitet Dynamic Host Configuration Protocol (DHCP)-Anfragen für IP-Adress-Zuweisung und Netzparameter weiter.

- Im Feld legen Sie die Werte der IP-Helper-Adresse für Datenpakete fest, die das Gerät an diesem Interface empfängt.
Mögliche Werte:
Gültige IP-Adresse
Die IP-Adresse mit legt den Eintrag als Discard-Eintrag fest. Das Gerät verwirft Datenpakete, die mit einem Discard-Eintrag übereinstimmen. Discard-Einträge legen Sie ausschließlich auf den Interfaces fest.
Voraussetzungen:
 - Um die IP-Adresse einzugeben, stellen Sie sicher, dass im Feld ein von verschiedenen Wert festgelegt ist.
 - Um eine von verschiedene IP-Adresse einzugeben, stellen Sie sicher, dass im Feld der Wert festgelegt ist.



Löschen

Entfernt die ausgewählte Tabellenzeile.



Statistiken zurücksetzen

Setzt die Tabellenstatistik zurück.

Port

Zeigt das Port-basierte Router-Interface, auf das sich die Tabellenzeile bezieht.

Anmerkung: Auf VLAN-basierten Router-Interfaces unterstützt das Gerät die Funktion nicht.

UDP-Port

Zeigt die Ziel-UDP-Port für erhaltene Client-Nachrichten, die an dem an dem Interface empfangen werden. Das Gerät leitet DHCP-Anfragen, die den UDP-Port-Kriterien entsprechen, an die festgelegte IP-Helper-Adresse weiter.

IP-Adresse

Zeigt die IP-Helper-Adresse für Datenpakete, die an dem Interface empfangen werden.

Treffer

Zeigt die aktuelle Anzahl der Datenpakete an, die das Interface für den angegebenen UDP-Port seit dem letzten Neustart des Geräts gesendet hat.

Status

Zeigt, ob die IP-Helper-Adresse und die UDP-Port-Einträge, die dem jeweiligen Port hinzugefügt wurden, aktiv sind.

7.7 Loopback-Interface

[Routing > Loopback-Interface]

Ein Loopback-Interface ist eine virtuelle Netzchnittstelle ohne Bezug zu einem physischen Port. Loopback-Interfaces sind ständig verfügbar, solange das Gerät in Betrieb ist.

Das Gerät ermöglicht Ihnen, Router-Interfaces auf Grundlage von Loopback-Interfaces einzurichten. Über ein solches Router-Interface ist das Gerät stets erreichbar, auch bei Inaktivität einzelner Router-Interfaces.

Im Gerät lassen sich bis zu 8 Loopback-Interfaces einrichten.


Tabelle


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

Schaltflächen



Hinzufügen

Öffnet das Fenster  , um ein Loopback-Interface hinzuzufügen.

- Im Feld  legen Sie die Nummer fest, die das Loopback-Interface eindeutig identifiziert. Mögliche Werte:



Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Nummer, die das Loopback-Interface eindeutig identifiziert. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Port

Zeigt die Bezeichnung des Loopback-Interfaces.

IP-Adresse

Legt die IP-Adresse für das Loopback-Interface fest.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung:)

Subnet-Maske

Legt die Netzmaske für das Loopback-Interface fest.

Mögliche Werte:

Gültige IPv4-Netzmaske (Voreinstellung:)

Beispiel:

Aktiv

Zeigt, ob das Loopback-Interface aktiv oder inaktiv ist.

Mögliche Werte:

(Voreinstellung)

Das Loopback-Interface ist aktiv.

Beim Senden von SNMP-Traps verwendet das Gerät als Absender die IP-Adresse des 1. Loopback-Interfaces.

Das Loopback-Interface ist inaktiv.

7.8 Multicast Routing

[Routing > Multicast Routing]

Das Menü enthält die folgenden Dialoge:

- [Multicast-Routing Global](#)
- [Statisches Multicast-Routing](#)
- [Multicast-Routing IGMP Querier](#)

7.8.1 Multicast-Routing Global

[Routing > Multicast Routing > Global]

IP-Multicast-Routing ist die Verteilung von IP-Datenpaketen unter einer IP-Adresse gleichzeitig an mehrere Teilnehmer.

Mit diesem Menü können Sie globale Einstellungen der Funktion [IP-Multicast-Routing](#) festlegen und zeigen.

Der Dialog enthält die folgenden Registerkarten:
[\[Konfiguration\]](#)

[Konfiguration]

Diese Registerkarte ermöglicht Ihnen, IP-Multicast-Routing zu aktivieren.

Funktion

Funktion

Schaltet die Funktion [IP-Multicast-Routing](#) ein/aus.

Mögliche Werte:

- Die Funktion [IP-Multicast-Routing](#) ist eingeschaltet.
(Voreinstellung)
- Die Funktion [IP-Multicast-Routing](#) ist ausgeschaltet.

7.8.2 Statisches Multicast-Routing

[Routing > Multicast Routing > Statisches Multicast-Routing]

Die Funktion [Statisches Multicast-Routing](#) ermöglicht dem Gerät, Datenpakete von einer einzigen Quelle an mehrere Ziele im Netz effizient zu verteilen.

Durch die Verwendung statischer Multicast-Routen können Netzadministratoren die Pfade von Multicast-Datenpaketen innerhalb des Netzes vordefinieren. Dies hilft, das Fluten von Multicast-Datenpaketen in Netzpfaden zu verhindern, in denen kein bekannter Empfänger angeschlossen ist. Dies kann dazu beitragen, unnötige Bandbreitennutzung in diesen Pfaden zu vermeiden.

Das Menü enthält die folgenden Dialoge:
[Statisches Multicast-Routing Global](#)
[Statische Multicast-Routing-Tabelle](#)

7.8.21 Statisches Multicast-Routing Global

[Routing > Multicast Routing > Statisches Multicast-Routing > Global]

In diesem Dialog legen Sie die globalen Einstellungen für die Funktion fest.

Funktion

Funktion

Schaltet die Funktion im Gerät ein/aus.

Voraussetzungen:

- Die Funktion ist eingeschaltet. Siehe Dialog .
- Das Kontrollkästchen ist für das betreffende Interface markiert. Siehe Dialog [Interfaces > Konfiguration](#).
- Die Funktion ist eingeschaltet. Siehe Dialog .
- Die Funktion ist eingeschaltet. Siehe Dialog .

Mögliche Werte:

Die Funktion ist eingeschaltet.
Denken Sie daran, die Funktion auf den Router-Interfaces zu aktivieren.
(Voreinstellung)
Die Funktion ist ausgeschaltet.

Tabelle

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

Port

Zeigt die Nummer des zum Router-Interface gehörenden Ports oder VLANs.

Aktiv

Aktiviert/deaktiviert die Funktion auf dem Router-Interface.

Mögliche Werte:

Die Funktion ist auf diesem Router-Interface aktiv.
Denken Sie daran, die Funktion im Rahmen zu aktivieren.
(Voreinstellung)
Die Funktion ist auf dem Router-Interface inaktiv.

7.8.2.2 Statische Multicast-Routing-Tabelle

[Routing > Multicast Routing > Statisches Multicast-Routing > Routing-Tabelle]

In diesem Dialog legen Sie die Einstellungen für die Multicast-Gruppe fest und definieren den Routing-Pfad für Multicast-Datenpakete innerhalb des Netzes.

Der Dialog enthält die folgenden Registerkarten:

[\[Multicast-Gruppe\]](#)

[\[Multicast-Route\]](#)

[Multicast-Gruppe]

In dieser Registerkarte legen Sie die Einstellungen für die Multicast-Gruppe fest. Eine Multicast-Gruppe ist eine Gruppe von Hosts, die daran interessiert sind, identische Multicast-Datenpakete zu empfangen. Diese Multicast-Gruppe wird durch eine Multicast-IP-Adresse identifiziert, die man als Gruppenadresse bezeichnet.


Tabelle


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

Schaltflächen



Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld  legen Sie die Nummer der Multicast-Gruppe fest.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Gruppe Index

Zeigt die fortlaufende Nummer der Multicast-Gruppe an, auf die sich die Tabellenzeile bezieht. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Inbound Interface

Legt das Router-Interface fest, über welches das Gerät die Multicast-Datenpakete empfängt. Wählen Sie in der Dropdown-Liste einen Eintrag, um fortzufahren.

Mögliche Werte:

Das Gerät empfängt die Multicast-Datenpakete auf diesem Router-Interface.

Quelle Adresse

Legt die IP-Quelladresse in den Multicast-Datenpaketen fest, die das Gerät routen soll.

Mögliche Werte:

Gültige IPv4-Adresse

Quelle Netzmaske

Legt die Netzmaske für die IP-Quelladressen in den Multicast-Datenpaketen fest, die das Gerät routen soll.

Mögliche Werte:

Gültige IPv4-Netzmaske (Voreinstellung:)

Gruppe Adresse

Legt die Multicast-IP-Adresse fest. Diese Adresse identifiziert eine Multicast-Gruppe, der Hosts beitreten können, um identische Multicast-Datenpakete zu empfangen.

Mögliche Werte:

Gültige IPv4-Adresse

Gruppe Netzmaske

Legt die Netzmaske für die Gruppenadresse fest.

Mögliche Werte:

Gültige IPv4-Netzmaske (Voreinstellung:)

Aktiv

Aktiviert/deaktiviert die Multicast-Gruppe.

Voraussetzungen:

- In Spalte ist ein Router-Interface gewählt.
- In Spalte ist eine gültige Multicast-IP-Adresse festgelegt.

Mögliche Werte:

Die Multicast-Gruppe ist aktiv.

Hosts können dieser Multicast-Gruppe beitreten, um Multicast-Datenpakete zu empfangen.

Die Multicast-Gruppe ist inaktiv.

Hosts können dieser Multicast-Gruppe nicht beitreten.

[Multicast-Route]


In dieser Registerkarte legen Sie die Multicast-Routen fest, über die das Gerät empfangene Multicast-Datenpakete weiterleitet.


Tabelle

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

Schaltflächen



Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld  legen Sie die Nummer der Multicast-Route fest.



Entfernt die ausgewählte Tabellenzeile.

Route Index

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

Inbound Interface

Legt das Router-Interface fest, über welches das Gerät die Multicast-Datenpakete empfängt. Wählen Sie in der Dropdown-Liste einen Eintrag, um fortzufahren.

Mögliche Werte:

Das Gerät empfängt die Multicast-Datenpakete auf diesem Router-Interface.

Quelle Adresse

Legt die IP-Quelladresse in den Multicast-Datenpaketen fest, die das Gerät routen soll.

Mögliche Werte:

Gültige IPv4-Adresse

Quelle Netzmaske

Legt die Netzmaske für die IP-Quelladressen in den Multicast-Datenpaketen fest, die das Gerät routen soll.

Mögliche Werte:

Gültige IPv4-Netzmaske (Voreinstellung:)

Gruppe Adresse

Legt die Multicast-IP-Adresse fest. Diese Adresse identifiziert eine Multicast-Gruppe, der Hosts beitreten können, um identische Multicast-Datenpakete zu empfangen.

Mögliche Werte:

Gültige IPv4-Adresse

Gruppe Netzmaske

Legt die Netzmaske für die Gruppenadresse fest.

Mögliche Werte:

Gültige IPv4-Netzmaske (Voreinstellung:)

Outbound Interface

Legt die Router-Interfaces fest, über welche das Gerät die Multicast-Datenpakete weiterleitet.

Das Gerät ermöglicht Ihnen, mehrere Router-Interfaces festzulegen. Führen Sie dazu die folgenden Schritte aus:

Klicken Sie in die Spalte der betreffenden Tabellenzeile.

Der Dialog zeigt das Fenster .

Wählen Sie in der Liste die gewünschten Interfaces.

Klicken Sie die Schaltfläche .

Mögliche Werte:

Das Gerät routet die Multicast-Datenpakete über diese Router-Interfaces.

Aktiv

Aktiviert/deaktiviert die Multicast-Route.

Voraussetzungen:

- In Spalte ist ein Router-Interface gewählt.
- In Spalte ist eine gültige Multicast-IP-Adresse festgelegt.
- In Spalte ist mindestens ein Router-Interface gewählt.

Mögliche Werte:

Die Multicast-Route ist aktiv.

Das Gerät leitet empfangene Multicast-Datenpakete über diese Multicast-Route weiter.

Die Multicast-Route ist inaktiv.

Das Gerät leitet empfangene Multicast-Datenpakete nicht über diese Multicast-Route weiter.

7.9 Multicast-Routing IGMP Querier

[Routing > Multicast Routing > IGMP Querier]

Das Internet Group Management Protocol (IGMP) ist ein Kommunikationsprotokoll, das zur Verwaltung von Multicast-Gruppenmitgliedschaften innerhalb eines Netzes eingesetzt wird. Mit der Funktion `igmp querier` sendet das Gerät in festgelegten Intervallen aktiv IGMP-Anfragen aus, um IGMP-fähige Hosts zu identifizieren, die am Empfang von Multicast-Datenpaketen interessiert sind.

Bei Empfang einer Abfrage antworten die Hosts mit einer IGMP-Report-Nachricht, die die Details zu den Multicast-Gruppen enthält, denen sie beitreten möchten. Jeder Host antwortet üblicherweise mit einer IGMP-Report-Nachricht pro Anfrage, unabhängig davon, wie vielen Multicast-Gruppen der Host beitreten möchte.

Daher verfolgt das Gerät die von den Hosts empfangenen Antworten und überträgt Multicast-Datenpakete ausschließlich an diejenigen Hosts, die ihr Interesse erklärt haben. Dadurch bleibt mehr Bandbreite in den Netzpfaden verfügbar, in denen kein bekannter Empfänger vorhanden ist.

Funktion

Funktion

Schaltet die Funktion `igmp querier` im Gerät ein/aus.

Mögliche Werte:

Die Funktion `igmp querier` ist eingeschaltet.

Denken Sie daran, die Funktion `igmp querier` auf den Router-Interfaces zu aktivieren.

(Voreinstellung)

Die Funktion `igmp querier` ist ausgeschaltet.

Konfiguration

Query Intervall

Legt das Intervall in Sekunden fest, in dem das Gerät Abfragen an die IGMP-fähigen Hosts vom ausgehenden Router-Interface sendet. Die IGMP-fähigen Hosts im Netzwerk antworten auf die Abfrage mit einer IGMP-Benachrichtigung.

Mögliche Werte:

(Voreinstellung:)

Query-Response Intervall

Legt die maximale Zeit in Sekunden fest, in dem jeder Host in einem Netz auf die Abfrage antworten soll, die das Gerät mit der Funktion sendet. Nur die Hosts, die innerhalb dieser Zeit auf die Anfrage antworten, bleiben Mitglieder der Multicast-Gruppe.

Mögliche Werte:

(Voreinstellung:)

Query-Last-Member Intervall

Legt die Zeit in Sekunden zwischen gruppenspezifischen Abfragen fest, während der das Gerät eine Abfrage sendet, um zu prüfen, ob noch Gruppenmitglieder am Empfang von Multicast-Datenpaketen interessiert sind. Wenn ein Host eine Multicast-Gruppe verlässt, sendet er eine Leave Group Message an das Gerät.

Mögliche Werte:

(Voreinstellung:)

Robustheit

Legt fest, wie viele Abfrage-Antwort-Intervalle das Gerät wartet, bevor es einen Host nicht mehr als Mitglied einer bestimmten Multicast-Gruppe betrachtet. Wenn zum Beispiel der Wert im Feld und der Wert im Feld ist, dann würde das Gerät 20 Sekunden warten, bevor es einen Host als inaktiv betrachtet.

Ein höherer Wert im Feld bedeutet, dass das Gerät länger wartet und den Hosts mehr Zeit zum Antworten gibt, bevor das Gerät die Hosts als inaktiv betrachtet und sie aus einer Multicast-Gruppe entfernt. Dies kann dazu beitragen, die Zuverlässigkeit der Multicast-Verteilung in Situationen zu erhöhen, in denen Datenpaketverluste oder intermittierende Konnektivitätsprobleme häufig sind.

Mögliche Werte:

(Voreinstellung:)

Verwenden Sie höhere Werte für die Robustheit, wenn Sie häufige Paketverluste in einem Subnetz erwarten.

Tabelle

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

Port

Zeigt die Nummer des zum Router-Interface gehörenden Ports oder VLANs.

Version

Legt die für das Router-Interface verwendete IGMP-Version fest.

Mögliche Werte:

IGMPv2
 (Voreinstellung)
 IGMPv3

Aktiv

Aktiviert/deaktiviert die Funktion auf dem Router-Interface.

Mögliche Werte:

Die Funktion ist auf diesem Router-Interface aktiv.
 Denken Sie daran, die Funktion im Rahmen zu aktivieren.
 (Voreinstellung)
 Die Funktion ist auf dem Router-Interface inaktiv.

7.10 L3-Redundanz

[Routing > L3-Redundanz]

Das Menü enthält die folgenden Dialoge:

[VRRP](#)

7.10.1 VRRP

[Routing > L3-Redundanz > VRRP]

Das Virtual Router Redundancy Protocol (VRRP) ist ein Verfahren, das es dem Gerät ermöglicht, auf den Ausfall eines Routers zu reagieren.

VRRP findet seine Anwendung in Netzen mit Endgeräten, die ausschließlich einen Eintrag für das Standard-Gateway unterstützen. Wenn das Standard-Gateway ausfällt, sorgt VRRP dafür, dass die Endgeräte ein redundantes Gateway finden.

Anmerkung: Weitere Informationen zur Funktion finden Sie im Anwender-Handbuch „Konfiguration“.

Das Menü enthält die folgenden Dialoge:

[VRRP Konfiguration](#)

[VRRP Statistiken](#)

[VRRP Tracking](#)

7.1Q.1.1 VRRP Konfiguration

[Routing > L3-Redundanz > VRRP > Konfiguration]

Dieser Dialog ermöglicht Ihnen, folgende Einstellungen festzulegen:

- bis zu 8 virtuelle Router pro Router-Interface
- bis zu 2 Adressen pro virtuellem Router

Funktion

Funktion

Schaltet die -Redundanz im Gerät ein/aus.

Mögliche Werte:

Die Funktion ist eingeschaltet.

(Voreinstellung)

Die Funktion ist ausgeschaltet.

Konfiguration

Trap senden (VRRP-Master)

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät der VRRP-Master ist.

Mögliche Werte:

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

Das Gerät sendet einen SNMP-Trap, wenn es der VRRP-Master ist.

(Voreinstellung)

Das Senden von SNMP-Traps ist inaktiv.

Trap senden (Fehler VRRP-Authentifizierung)

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät ein VRRP-Paket mit Authentifizierungsinformation empfängt.

Anmerkung: Das Gerät unterstützt ausschließlich VRRP-Pakete ohne Authentifizierungsinformationen. Um das Gerät in Verbindung mit anderen Geräten zu betreiben, die VRRP-Authentifizierung unterstützen, vergewissern Sie sich, dass auf diesen Geräten die VRRP-Authentifizierung nicht angewendet wird.

Mögliche Werte:

Das Senden von SNMP-Traps ist aktiv. Voraussetzung ist, dass im Dialog [Statuskonfiguration > Alarme \(Traps\)](#) die Funktion [eingeschaltet](#) und mindestens ein Trap-Ziel festgelegt ist.
Das Gerät sendet einen SNMP-Trap, wenn es ein VRRP-Paket mit Authentifizierungsinformation empfängt.
(Voreinstellung)
Das Senden von SNMP-Traps ist inaktiv.

Information

Version

Legt die VRRP-Version fest.

Tabelle

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

Schaltflächen

 Hinzufügen

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

- In der Dropdown-Liste [Port](#) wählen Sie die Nummer des Ports.
- Im Feld [VRID](#) legen Sie den Virtual Router Identifier (VRID) fest.

 Löschen

Entfernt die ausgewählte Tabellenzeile.

 Wizard

Öffnet das Fenster [Wizard](#), das Sie dabei unterstützt, die Ports mit der Adresse eines oder mehrerer erwünschter Absender zu verknüpfen. Siehe [„\[Wizard: VRRP-Konfiguration\]“](#) auf [Seite 393](#).

Port

Zeigt die Port-Nummer, auf die sich die Tabellenzeile bezieht.

VRID

Zeigt den Virtual Router Identifier.

Aktiv

Aktiviert/deaktiviert die in dieser Tabellenzeile festgelegte VRRP-Instanz.

Mögliche Werte:

- Die -Instanz ist aktiv.
(Voreinstellung)
- Die -Instanz ist inaktiv.

Betriebszustand

Zeigt den Status der Tabellenzeile. Der Betriebsmodus des entsprechenden virtuellen Routers bestimmt den Status einer gegenwärtig aktiven Tabellenzeile.

Mögliche Werte:

- Die Instanz ist erreichbar.
- Die Instanz existiert im Gerät, ihr fehlen allerdings notwendige Information und sie ist unerreichbar.
- Die Instanz existiert im Gerät, ihr fehlen allerdings notwendige Information und sie ist unerreichbar.

Zustand

Zeigt den VRRP-Zustand.

Mögliche Werte:

- VRRP initialisiert sich gerade, die Funktion ist inaktiv, oder der Master-Router ist noch unbenannt.
- Der Router beobachtet die Möglichkeit, Master-Router zu werden.
- Der Router ist der Master-Router.

Basis Priorität

Legt die Priorität des virtuellen Routers fest. Wenn sich der Wert vom Wert im Feld unterscheidet, dann ist das überwachte Objekt nicht erreichbar oder der virtuelle Router ist Inhaber der IP-Adresse.

Mögliche Werte:

(Voreinstellung:)

Je größer die Zahl, desto höher die Priorität. Verteilen Sie die Prioritätswerte gleichmäßig auf die Router, wenn Sie mehrere VRRP-Router in einer einzelnen Instanz einrichten. Weisen Sie beispielsweise den Prioritätswert dem primären Router und den Wert dem nächsten Router zu. Wiederholen Sie den Vorgang für den Wert usw. Diese Aufteilung vereinfacht das spätere Hinzufügen eines weiteren Routers mit einer Priorität zwischen den bestehenden Werten, zum Beispiel mit dem Wert .

Priorität

Zeigt den Wert für die `priority`-Priorität. Die Priorität legen Sie fest im Dialog `Priority`. Der Router mit dem höchsten Wert für die Priorität übernimmt die Master-Router-Rolle. Wenn die IP-Adresse des virtuellen Routers mit der IP-Adresse eines Router-Interfaces übereinstimmt, dann ist der Router der Inhaber der IP-Adresse. Wenn ein Inhaber der IP-Adresse existiert, dann ermöglicht die Funktion `priority`, dem Inhaber der IP-Adresse den Prioritätswert `priority` zuzuweisen und den Router als Master-Router zu deklarieren.

Mögliche Werte:

Je größer die Zahl, desto höher die Priorität. Das Deaktivieren oder Entfernen eines `priority`-Routers, der die Master-Rolle inne hat, zwingt die Instanz zum Senden einer Nachricht mit Prioritätswert `priority`. So wird den anderen Backup-Routern mitgeteilt, dass der Master-Router nicht teilnimmt. Das Senden des Prioritätswerts `priority` erzwingt einen neuen Auswahlprozess.

Der Wert `priority` bedeutet, dass der virtuelle Router der Inhaber der IP-Adresse ist.

Virtuelle IP-Adresse

Zeigt die virtuelle IP-Adresse im Subnetz der primären IP-Adresse auf dem Interface. Wenn keine Übereinstimmung gefunden wird, gibt das Gerät eine unbestimmte virtuelle Adresse aus. Wenn keine virtuelle Adresse eingerichtet ist, meldet das Gerät `None`.

Mögliche Werte:

Gültige IPv4-Adresse

Preempt-Modus

Aktiviert/deaktiviert den Preempt-Modus. Diese Einstellung legt fest, ob dieser Router als Backup-Router einem Master-Router mit niedrigerer VRRP-Priorität die Rolle als Master-Router entzieht.

Mögliche Werte:

`enable` (Voreinstellung)

Der `enable` ist aktiv. Der Router übernimmt die Master-Router-Rolle von einem Router mit niedrigerer VRRP-Priorität, ohne dass ein Auswahlprozess stattfindet.

Der `disable` ist inaktiv. Der Router übernimmt die Rolle eines Backup-Routers und wartet auf Nachrichten (Advertisements) des Master-Routers. Nachdem das Master-Down-Intervall abgelaufen ist und keine Advertisements vom Master-Router empfangen wurden, nimmt der Router am Auswahlprozess für den Master-Router teil.

Proxy-ARP

Aktiviert/deaktiviert die Funktion Proxy ARP auf dem virtuellen Router-Interface. Diese Funktion ermöglicht Ihnen, Geräte in anderen Netzen so zu erreichen, als wären diese Geräte im lokalen Netz. Die Proxy-ARP-Funktion ist erforderlich, wenn das Gerät die VRRP-Instanz mit - Regeln verwendet. Voraussetzung ist, dass im Dialog für das betreffende Interface, welches von der VRRP-Instanz verwendet wird, das Kontrollkästchen unmarkiert ist.

Mögliche Werte:

Die Funktion Proxy ARP ist aktiv.

Das Gerät antwortet auf empfangene ARP-Anfragen von Endgeräten, die sich in anderen Netzen befinden.

(Voreinstellung)

Die Funktion Proxy ARP ist inaktiv.

VRRP Master-Kandidat

Legt die IP-Adresse des primären virtuellen Routers fest. Physische Router innerhalb einer virtuellen Router-Instanz verwenden die VRRP-IP-Adresse, um zu kommunizieren. Wenn die IP-Adresse des virtuellen Routers mit der IP-Adresse eines Router-Interfaces übereinstimmt, dann ist der Router der Inhaber der IP-Adresse und Master-Router.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung:)

Die Voreinstellung zeigt, dass der Router die niedrigere IP-Adresse als verwendet.

Sie können die IP-Adresse eines Router-Interfaces auswählen, das im Dialog [Interfaces > Konfiguration](#) eingerichtet ist.

Master IP-Adresse

Zeigt die gegenwärtige IP-Adresse des Master-Router-Interfaces.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung:)

VRRP-Router-Instanz einrichten

Das Gerät ermöglicht Ihnen, bis zu 8 virtuelle Router pro Router-Interface einzurichten.

Bevor Sie eine VRRP-Router-Instanz einrichten, vergewissern Sie sich, dass das Netz.Routing ordnungsgemäß funktioniert, und geben Sie die IP-Adressen auf den für die VRRP-Instanzen verwendeten Router-Interfaces ein.

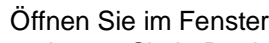
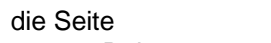


Führen Sie die folgenden Schritte aus:

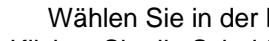
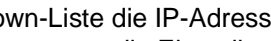
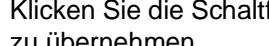
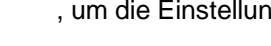
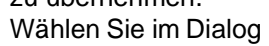

Öffnen Sie im Dialog das Fenster .

Öffnen Sie im Fenster die Seite .

– Wählen Sie in der Dropdown-Liste ein Router-Interface.

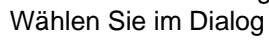
– Legen Sie in Spalte den Virtual Router Identifier fest.

Öffnen Sie im Fenster  die Seite .
– Legen Sie in Registerkarte , Rahmen  die Werte für folgende Parameter fest:

Wählen Sie in der Dropdown-Liste die IP-Adresse für den .
Klicken Sie die Schaltfläche , um die Einstellungen in die VRRP-Router-Interface-Tabelle zu übernehmen.
Wählen Sie im Dialog , Rahmen  das Optionsfeld . Klicken Sie anschließend die Schaltfläche  ✓.

Vorhandene VRRP-Router-Instanz bearbeiten

Führen Sie einen der folgenden Schritte aus:

Wählen Sie im Dialog , Rahmen  eine Tabellenzeile und

klicken Sie zum Bearbeiten die Schaltfläche .

oder

Doppelklicken Sie ein Feld in der Tabelle und bearbeiten den Wert direkt.

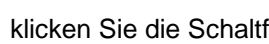
oder

Rechtsklicken Sie in ein Feld und wählen Sie einen Wert.

VRRP-Router-Instanz löschen

Führen Sie den folgenden Schritt aus:

Wählen Sie im Dialog , Rahmen  eine Tabellenzeile und


klicken Sie die Schaltfläche .

[Wizard: VRRP-Konfiguration]

Das Fenster  hilft Ihnen beim Einrichten einer VRRP-Router-Instanz.

Voraussetzungen:

- Routing funktioniert ordnungsgemäß.
- Auf den in der VRRP-Instanz verwendeten Router-Interfaces sind die IP-Adressen festgelegt.

Das Fenster  führt Sie durch die folgenden Schritte:

- [Eintrag erstellen oder auswählen](#)
- [Eintrag bearbeiten](#)
- [Tracking](#)
- [Virtuelle IP-Adressen](#)

Eintrag erstellen oder auswählen

VRRP-Instanzen

Zeigt die im Gerät verfügbaren Instanzen. Wählen Sie einen Eintrag, um fortzufahren. Alternativ dazu wählen Sie einen Port und legen im Feld unten einen Wert fest.

Port

Legt das Port-basierte oder VLAN-basierte Router-Interface fest. Im Dialog [Konfiguration](#) prüfen Sie, ob auf dem Port ein Router-Interface eingerichtet ist.

Mögliche Werte:

Port-basiertes Router-Interface

VLAN-basiertes Router-Interface

VRID

Legt den Virtual Router Identifier fest.

Mögliche Werte:

Ein virtueller Router verwendet als seine MAC-Adresse. Der hier festgelegte Wert ersetzt das letzte Oktett () in der MAC-Adresse. Weisen Sie jedem physischen Router innerhalb einer virtuellen Router-Instanz einen eindeutigen Wert zu. Das Gerät ändert den wirksamen Prioritätswert in für einen physischen Router, der dieselbe IP-Adresse aufweist wie der virtuelle Router.

Eintrag bearbeiten

Mit den folgenden Registerkarten können Sie die Parameter für jede Instanz festlegen:

- [Eintrag bearbeiten - VRRP](#)

Eintrag bearbeiten - VRRP

Funktion

Schaltet die -Redundanz für die gegenwärtige Instanz ein/aus.

Mögliche Werte:

Die Funktion ist für die gegenwärtige Instanz eingeschaltet.
(Voreinstellung)

Die Funktion ist für die gegenwärtige Instanz ausgeschaltet.

Konfiguration

Basis Priorität

Legt die Priorität des virtuellen Routers fest. Wenn sich der Wert vom Wert im Feld unterscheidet, dann ist das überwachte Objekt nicht erreichbar oder der virtuelle Router ist Inhaber der IP-Adresse.

Mögliche Werte:

(Voreinstellung:)

Je größer die Zahl, desto höher die Priorität. Verteilen Sie die Prioritätswerte gleichmäßig auf die Router, wenn Sie mehrere VRRP-Router in einer einzelnen Instanz einrichten. Weisen Sie beispielsweise den Prioritätswert dem primären Router und den Wert dem nächsten Router zu. Wiederholen Sie den Vorgang für den Wert usw. Diese Aufteilung vereinfacht das spätere Hinzufügen eines weiteren Routers mit einer Priorität zwischen den bestehenden Werten, zum Beispiel mit dem Wert .

Priorität

Zeigt den Wert für die -Priorität. Die Priorität legen Sie fest im Dialog . Der Router mit dem höchsten Wert für die Priorität übernimmt die Master-Router-Rolle. Wenn die IP-Adresse des virtuellen Routers mit der IP-Adresse eines Router-Interfaces übereinstimmt, dann ist der Router der Inhaber der IP-Adresse. Wenn ein Inhaber der IP-Adresse existiert, dann ermöglicht die Funktion , dem Inhaber der IP-Adresse den Prioritätswert zuzuweisen und den Router als Master-Router zu deklarieren.

Mögliche Werte:

Je größer die Zahl, desto höher die Priorität. Das Deaktivieren oder Entfernen eines -Routers, der die Master-Rolle inne hat, zwingt die Instanz zum Senden einer Nachricht mit Prioritätswert . So wird den anderen Backup-Routern mitgeteilt, dass der Master-Router nicht teilnimmt. Das Senden des Prioritätswerts erzwingt einen neuen Auswahlprozess.

Der Wert bedeutet, dass der virtuelle Router der Inhaber der IP-Adresse ist.

Preempt-Modus

Aktiviert/deaktiviert den Preempt-Modus. Diese Einstellung legt fest, ob dieser Router als Backup-Router einem Master-Router mit niedrigerer VRRP-Priorität die Rolle als Master-Router entzieht.

Mögliche Werte:

(Voreinstellung)

Der ist aktiv. Der Router übernimmt die Master-Router-Rolle von einem Router mit niedrigerer VRRP-Priorität, ohne dass ein Auswahlprozess stattfindet.

Der ist inaktiv. Der Router übernimmt die Rolle eines Backup-Routers und wartet auf Nachrichten (Advertisements) des Master-Routers. Nachdem das Master-Down-Intervall abgelaufen ist und keine Advertisements vom Master-Router empfangen wurden, nimmt der Router am Auswahlprozess für den Master-Router teil.

Advertisement-Intervall [s]

Legt den zeitlichen Abstand zwischen Nachrichten des Master-Routers in Sekunden fest.

Mögliche Werte:

(Voreinstellung:)

Anmerkung: Je länger das Nachrichtenintervall ist, desto größer wird der Zeitraum, über den Backup-Router auf eine Nachricht des Master-Routers warten, bevor die Backup-Router einen neuen Auswahlprozess starten (Master-Down-Intervall). Legen Sie außerdem denselben Wert für jeden Teilnehmer in einer bestimmten Instanz des virtuellen Routers fest.

Proxy-ARP

Aktiviert/deaktiviert die Funktion Proxy ARP auf dem virtuellen Router-Interface. Diese Funktion ermöglicht Ihnen, Geräte in anderen Netzen so zu erreichen, als wären diese Geräte im lokalen Netz. Die Proxy-ARP-Funktion ist erforderlich, wenn das Gerät die VRRP-Instanz mit - Regeln verwendet. Voraussetzung ist, dass im Dialog für das betreffende Interface, welches von der VRRP-Instanz verwendet wird, das Kontrollkästchen unmarkiert ist.

Mögliche Werte:

Die Funktion Proxy ARP ist aktiv.

Das Gerät antwortet auf empfangene ARP-Anfragen von Endgeräten, die sich in anderen Netzen befinden.

(Voreinstellung)

Die Funktion Proxy ARP ist inaktiv.

VRRP Master-Kandidat

Legt die IP-Adresse des primären virtuellen Routers fest. Physische Router innerhalb einer virtuellen Router-Instanz verwenden die VRRP-IP-Adresse, um zu kommunizieren. Wenn die IP-Adresse des virtuellen Routers mit der IP-Adresse eines Router-Interfaces übereinstimmt, dann ist der Router der Inhaber der IP-Adresse und Master-Router.

Mögliche Werte:

Gültige IP-Adresse (Voreinstellung:)

Sie können die IP-Adresse eines Router-Interfaces auswählen, das im Dialog [Interfaces > Konfiguration](#) eingerichtet ist.

Tracking

Aktuelle Track-Einträge

Zeigt die im Gerät verfügbaren Tracking-Objekte. Tracking-Objekte richten Sie ein im Dialog [Tracking-Objekt konfigurieren](#). Wählen Sie einen Eintrag, um fortzufahren. Alternativ dazu wählen Sie im Feld [Tracking-Objekt auswählen](#) unten ein Tracking-Objekt.

Jedes Tracking-Objekt enthält folgende Parameter, die mit Bindestrich voneinander getrennt sind:

- Typ des Tracking-Objekts
- Identifikationsnummer des Tracking-Objekts
- Name des Tracking-Objekts

Es gibt die folgenden Arten von Tracking-Objekten:

- Das Gerät überwacht den Link-Status seiner physischen Ports, Link-Aggregation-, LRE- oder VLAN-Router-Interfaces.
- Das Gerät überwacht die Route zu einem entfernten Router oder Endgerät durch periodisches Senden von ICMP Echo Request-Paketen.
- Das Gerät überwacht logisch miteinander verknüpfte Tracking-Objekte und ermöglicht somit komplexe Überwachungsaufgaben.

Zugewiesene Track-Einträge

Zeigt die Tracking-Objekte mit zugewiesenem [VRRP-Instanz](#)-Wert. Sie können einen Eintrag entfernen, indem Sie das Symbol **X** klicken.

Track-Name

Legt den Namen des Tracking-Objekts fest, mit dem der virtuelle Router verknüpft ist. Wählen Sie in der Dropdown-Liste einen Eintrag, um fortzufahren. Tracking-Objekte richten Sie ein im Dialog [Tracking-Objekt konfigurieren](#).

Wenn das Ergebnis für ein Tracking-Objekt negativ ist, reduziert die [VRRP-Instanz](#) die Priorität des virtuellen Routers. Das Tracking-Objekt ist beispielsweise dann negativ, wenn das überwachte Interface inaktiv ist oder der überwachte Router nicht erreichbar ist.

Mögliche Werte:

Name des Tracking-Objekts, zusammensetzt aus [Name](#) und [ID](#).

Dekrement

Legt den Wert fest, um den die VRRP-Instanz die Priorität des virtuellen Routers reduziert, wenn das Überwachungsergebnis negativ ist.

Mögliche Werte:

(Voreinstellung: [1](#))

Anmerkung: Wenn im Dialog [VRRP-Instanz konfigurieren](#) der Wert in Spalte [VRRP-Instanz](#) [1](#) ist, dann ist der virtuelle Router der Inhaber der IP-Adresse. In diesem Fall bleibt die Priorität des virtuellen Routers unverändert.

Hinzufügen

Fügt im Feld einen Eintrag basierend auf den in den Feldern und festgelegten Werten hinzu.

Virtuelle IP-Adressen

IP-Adresse

Zeigt die primäre IP-Adresse des Router-Interfaces.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung:)

Multinetting

Zeigt die sekundäre IP-Adresse für das Router-Interface und die Subnetzmaske der sekundären IP-Adressen. Sekundäre IP-Adresse und Subnetzmaske legen Sie fest im Dialog [Interfaces > Konfiguration](#).

Virtuelle IP-Adressen

Zeigt die virtuelle IP-Adresse, die Sie im Feld festgelegt haben. Sie können einen Eintrag entfernen, indem Sie das Symbol klicken.

IP-Adresse

Legt die zugewiesene IP-Adresse für den Master-Router innerhalb des virtuellen Routers fest.

Mögliche Werte:

Gültige IPv4-Adresse

Hinzufügen

Fügt im Feld einen Eintrag basierend auf den im Feld festgelegten Werten hinzu.

7.1Q 1.2 VRRP Statistiken

[Routing > L3-Redundanz > VRRP > Statistiken]

Der Dialog zeigt die Anzahl der Zähler, die für die Funktion relevante Ereignisse erfassen.

Information

Prüfsummenfehler

Zeigt die Anzahl der empfangenen VRRP-Nachrichten mit falscher Prüfsumme.

Versionsfehler

Zeigt die Anzahl der empfangenen VRRP-Nachrichten mit unbekannter oder nicht unterstützter Versionsnummer.

VRID Fehler

Zeigt die Anzahl der empfangenen VRRP-Nachrichten mit einem ungültigen Virtual Router Identifier für diesen virtuellen Router.

Tabelle

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

Port

Zeigt die Router-Interface-Nummer, auf die sich die Tabellenzeile bezieht.

VRID

Zeigt den Virtual Router Identifier.

Master geworden

Zeigt, wie oft das Gerät die Master-Rolle übernommen hat. Eine hohe Zahl kann ein Hinweis auf ein instabiles Netz sein.

Advertise empfangen

Zeigt die Anzahl der empfangenen VRRP-Nachrichten.

Intervall-Fehler

Zeigt die Anzahl der vom Router außerhalb des Nachrichtenintervalls empfangenen VRRP-Nachrichten. Dieser Wert ermöglicht Ihnen, zu bestimmen, ob in der Instanz des virtuellen Routers für die Router dasselbe Nachrichtenintervall festgelegt wird.

Authentifizierungs-Fehler

Zeigt die Anzahl der empfangenen VRRP-Nachrichten mit Authentifizierungsfehler.

IP-TTL Fehler

Zeigt die Anzahl der empfangenen VRRP-Nachrichten mit einer IP-TTL ungleich .

Null-Prioritätspakete empfangen

Zeigt die Anzahl der empfangenen VRRP-Nachrichten mit Priorität gleich .

Null-Prioritätspakete gesendet

Zeigt die Anzahl der VRRP-Nachrichten, die das Gerät mit der Priorität gesendet hat.

Empfangene ungültige Pakete

Zeigt die Anzahl der empfangenen VRRP-Nachrichten mit ungültigem Typ.

Adressfehler

Zeigt die Anzahl der empfangenen VRRP-Nachrichten, für welche die Adressliste nicht mit der lokal für den virtuellen Router eingerichteten Adressliste übereinstimmt.

Ungültiger Typ Authentifizierung

Zeigt die Anzahl der empfangenen VRRP-Nachrichten mit ungültigem Authentifizierungstyp.

Authentication type mismatch

Zeigt die Anzahl der empfangenen VRRP-Nachrichten mit fehlerhaftem Authentifizierungstyp.

Paketlängenfehler

Zeigt die Anzahl der empfangenen VRRP-Nachrichten mit fehlerhafter Paketlänge.

7.1Q 1.3 VRRP Tracking

[Routing > L3-Redundanz > VRRP > Tracking]

VRRP-Tracking ermöglicht Ihnen, Aktionen eines bestimmten Objektes zu überwachen und auf eine Änderung des Objektstatus zu reagieren. Die Funktion wird periodisch über das überwachte Objekt informiert und zeigt Änderungen in der Tabelle. Die Tabelle zeigt den Objektstatus entweder als `Up`, als `Down` oder als `Not Tracked`.

Tabelle

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

Schaltflächen



Hinzufügen

Öffnet das Fenster `Table`, um eine Tabellenzeile hinzuzufügen.

- In der Dropdown-Liste `Router` wählen Sie Interface und Router-ID eines eingerichteten virtuellen Routers aus.
- In der Dropdown-Liste `Tracking Object` wählen Sie das Tracking-Objekt aus, mit dem das Gerät den virtuellen Router verknüpft.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Port

Zeigt die Router-Interface-Nummer des virtuellen Routers.

VRID

Zeigt die VRID (virtuelle Router Identifikation) für diesen virtuellen Router.

Track-Name

Zeigt den Namen des Tracking-Objekts, mit dem der virtuelle Router verknüpft ist.

Wenn das Ergebnis für ein Tracking-Objekt negativ ist, reduziert die `Priority`-Instanz die Priorität des virtuellen Routers. Das Tracking-Objekt ist beispielsweise dann negativ, wenn das überwachte Interface inaktiv ist oder der überwachte Router nicht erreichbar ist.

Mögliche Werte:

Name des Tracking-Objekts, zusammensetzt aus `Interface` und `Router ID`.
Logische Tracker, die mehrere Tracker kombinieren

Kein Tracking-Objekt ausgewählt.

Tracking-Objekte richten Sie ein im Dialog `Tracking Object`.

Dekrement

Legt den Wert fest, um den die VRRP-Instanz die Priorität des virtuellen Routers reduziert, wenn das Überwachungsergebnis negativ ist.

Mögliche Werte:

(Voreinstellung:)

Anmerkung: Wenn im Dialog der Wert in Spalte -
gleich ist, dann ist der virtuelle Router der Inhaber der IP-Adresse. In diesem Fall bleibt die
Priorität des virtuellen Routers unverändert.

Status

Zeigt das Überwachungsergebnis des Tracking-Objekts.

Mögliche Werte:

Das Tracking-Objekt ist nicht aktiv.

Das Überwachungsergebnis ist positiv:

- Der Link-Status ist aktiv.
oder
- Der entfernte Router oder das Endgerät ist erreichbar.

Das Überwachungsergebnis ist negativ:

- Der Link-Status ist inaktiv.
oder
- Der entfernte Router oder das Endgerät ist unerreichbar.

Eine Kombination der Tracker und .

Aktiv

Zeigt, ob die Überwachung des Tracking-Objekts aktiv oder inaktiv ist.

Mögliche Werte:

Überwachung des Tracking-Objekts ist aktiv.

Die Überwachung des Tracking-Objekts ist inaktiv. Sie aktivieren die Überwachung im Dialog
, Spalte .

7.11 NAT

[Routing > NAT]

Das Menü enthält die folgenden Dialoge:

[NAT Global](#)
[1:1-NAT](#)
[Destination-NAT](#)
[Masquerading-NAT](#)
[Double-NAT](#)


7.11.1 NAT Global

[Routing > NAT > NAT Global]

Network Address Translation () umfasst mehrere Verfahren, die automatisiert die IP-Adressinformation im Datenpaket verändern. Wenn im Gerät eingerichtet, ermöglicht die Funktion Kommunikationsverbindungen zwischen Geräten in unterschiedlichen Netzen.

Dieser Dialog zeigt, wie viele -Regeln für die einzelnen -Verfahren einrichtbar sind und signalisiert Änderungen an aktiven -Regeln.

Das Gerät bietet Ihnen ein mehrstufiges Konzept für das Einrichten und Anwenden der -Regeln:

- Eine Regel hinzufügen.
- Die Regel einem Router-Interface zuweisen.
Bis zu diesem Schritt haben Änderungen keine Auswirkung auf das Verhalten des Geräts und auf den Datenstrom.
- Die Regel auf den Datenstrom anwenden. Klicken Sie dazu die Schaltfläche  im betreffenden Rahmen.

1:1-NAT

Schaltflächen

 Commit

Wendet die im Gerät gespeicherten -Regeln auf den Datenstrom an.

Das Gerät entfernt dabei auch die Zustandsinformationen des Paketfilters. Dies beinhaltet eventuell vorhandene DCE RPC-Informationen der Funktion . Das Gerät unterbricht daraufhin offene Kommunikationsverbindungen.

Anmerkung: Während das Gerät die gespeicherten Regeln aktiviert, können Sie keine neuen Kommunikationsverbindungen herstellen.

1:1-NAT Regeln (max.)

Zeigt die maximale Anzahl an -Regeln an, die Sie im Gerät einrichten können.


1:1-NAT Eingerichtete Regeln

Zeigt die Anzahl der im Gerät eingerichteten -Regeln.

1:1-NAT Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten -Regeln von den gespeicherten -Regeln unterscheiden.

Mögliche Werte:

Mindestens eine gespeicherte -Regel enthält geänderte Einstellungen. Um die noch ausstehenden Regeln auf den Datenstrom anzuwenden, klicken Sie die Schaltfläche .

Das Gerät wendet die gespeicherten -Regeln auf den Datenstrom an.

Destination-NAT

Schaltflächen

 Commit

Wendet die im Gerät gespeicherten -Regeln auf den Datenstrom an.

Das Gerät entfernt dabei auch die Zustandsinformationen des Paketfilters. Dies beinhaltet eventuell vorhandene DCE RPC-Informationen der Funktion . Das Gerät unterbricht daraufhin offene Kommunikationsverbindungen.

Anmerkung: Während das Gerät die gespeicherten Regeln aktiviert, können Sie keine neuen Kommunikationsverbindungen herstellen.

Destination-NAT Regeln (max.)

Zeigt die maximale Anzahl an -Regeln an, die Sie im Gerät einrichten können.

Destination-NAT Eingerichtete Regeln

Zeigt die Anzahl der im Gerät eingerichteten -Regeln.


Destination-NAT Eingerichtete Interfaces

Zeigt die Anzahl der im Gerät eingerichteten -Router-Interfaces.

Destination-NAT Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten -Regeln von den gespeicherten -Regeln unterscheiden.

Mögliche Werte:

Mindestens eine gespeicherte -Regel enthält geänderte Einstellungen. Um die noch ausstehenden Regeln auf den Datenstrom anzuwenden, klicken Sie die Schaltfläche .

Das Gerät wendet die gespeicherten -Regeln auf den Datenstrom an.

Masquerading-NAT

Schaltflächen

 Commit

Wendet die im Gerät gespeicherten -Regeln auf den Datenstrom an.

Das Gerät entfernt dabei auch die Zustandsinformationen des Paketfilters. Dies beinhaltet eventuell vorhandene DCE RPC-Informationen der Funktion . Das Gerät unterbricht daraufhin offene Kommunikationsverbindungen.

Anmerkung: Während das Gerät die gespeicherten Regeln aktiviert, können Sie keine neuen Kommunikationsverbindungen herstellen.

Masquerading-NAT Regeln (max.)

Zeigt die maximale Anzahl an -Regeln an, die Sie im Gerät einrichten können.

Masquerading-NAT Eingerichtete Regeln

Zeigt die Anzahl der im Gerät eingerichteten -Regeln.

Masquerading-NAT Eingerichtete Interfaces

Zeigt die Anzahl der im Gerät eingerichteten -Router-Interfaces.

Masquerading-NAT Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten -Regeln von den gespeicherten -Regeln unterscheiden.

Mögliche Werte:

Mindestens eine gespeicherte -Regel enthält geänderte Einstellungen. Um die noch ausstehenden Regeln auf den Datenstrom anzuwenden, klicken Sie die Schaltfläche

 .

Das Gerät wendet die gespeicherten -Regeln auf den Datenstrom an.

Double-NAT

Schaltflächen

 Commit

Wendet die im Gerät gespeicherten -Regeln auf den Datenstrom an.

Das Gerät entfernt dabei auch die Zustandsinformationen des Paketfilters. Dies beinhaltet eventuell vorhandene DCE RPC-Informationen der Funktion . Das Gerät unterbricht daraufhin offene Kommunikationsverbindungen.

Anmerkung: Während das Gerät die gespeicherten Regeln aktiviert, können Sie keine neuen Kommunikationsverbindungen herstellen.

Double-NAT Regeln (max.)

Zeigt die maximale Anzahl an -Regeln an, die Sie im Gerät einrichten können.

Double-NAT Eingerichtete Regeln

Zeigt die Anzahl der im Gerät eingerichteten -Regeln.


Double-NAT Eingerichtete Interfaces

Zeigt die Anzahl der im Gerät eingerichteten -Router-Interfaces.

Double-NAT Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten -Regeln von den gespeicherten -Regeln unterscheiden.

Mögliche Werte:

Mindestens eine gespeicherte -Regel enthält geänderte Einstellungen. Um die noch ausstehenden Regeln auf den Datenstrom anzuwenden, klicken Sie die Schaltfläche .

Das Gerät wendet die gespeicherten -Regeln auf den Datenstrom an.

7.11.2 1:1-NAT

[Routing > NAT > 1:1-NAT]

Die Funktion ermöglicht Ihnen, innerhalb eines lokalen Netzes Kommunikationsverbindungen zu Endgeräten aufzubauen, die sich in anderen Netzen befinden. Der -Router „verschiebt“ die Endgeräte virtuell in das öffentliche Netz. Dazu ersetzt der -Router beim Vermitteln im Datenpaket die virtuelle durch die tatsächliche IP-Adresse. Eine typische Anwendung ist das Anbinden mehrerer identisch aufgebauter Produktionszellen mit gleichen IP-Adressen an eine Server-Farm.

Voraussetzung für das -Verfahren ist, dass der -Router selbst auf ARP-Anfragen antwortet. Aktivieren Sie hierzu für das betreffende Interface die Funktion im Dialog oder im Dialog .

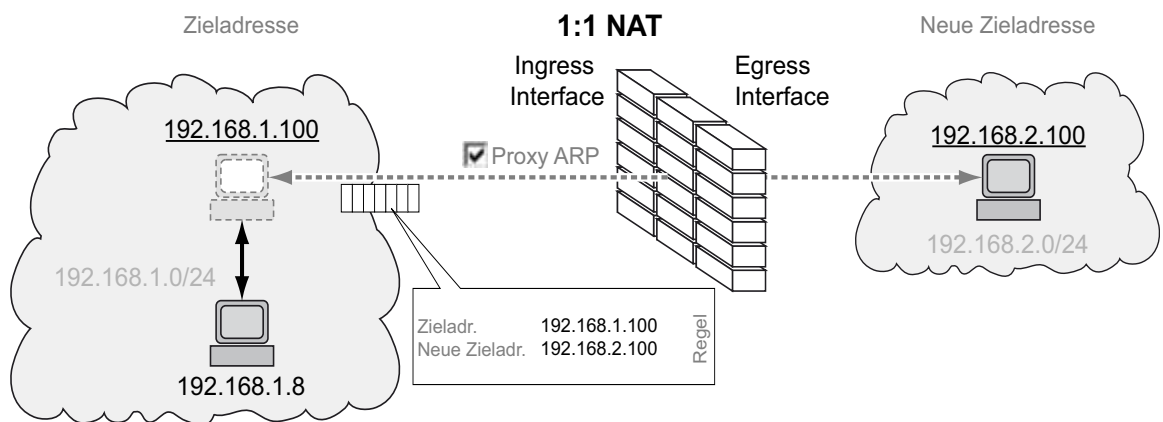


Abb. 3: Funktionsprinzip der Funktion

Um die Funktion zu nutzen, richten Sie für jedes Netz ein Router-Interface ein und schalten Sie die Routing-Funktion im Gerät ein.

Die Datenpakete durchlaufen die Filter-Funktionen des Geräts in folgender Reihenfolge:

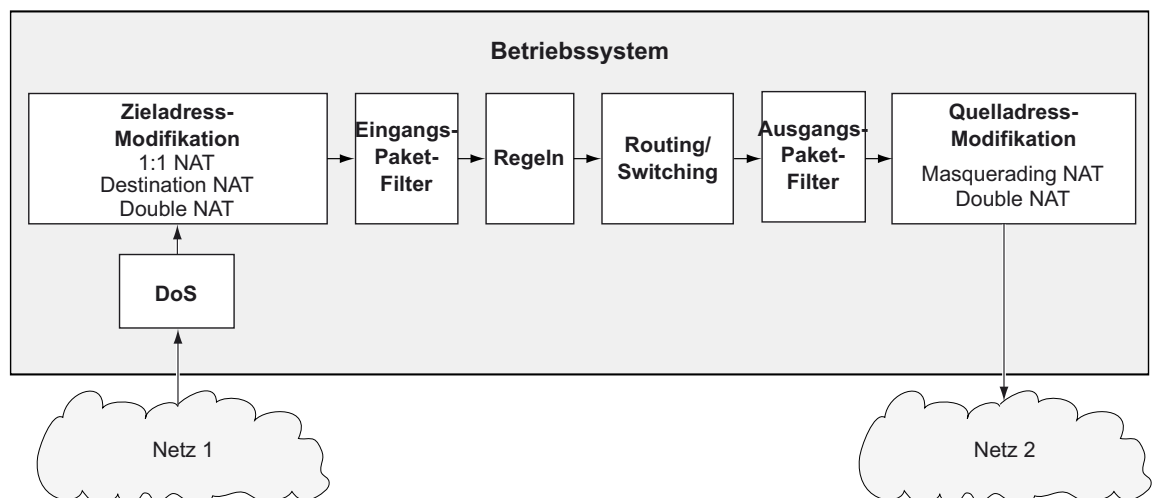


Abb. 4: Bearbeitungsreihenfolge der Datenpakete im Gerät

Das Menü enthält die folgenden Dialoge:

[1:1-NAT Regel](#)

7.11.21 1:1-NAT Regel

[Routing > NAT > 1:1-NAT > Regel]

In diesem Dialog richten Sie die -Regeln ein und weisen Router-Interfaces zu, auf die das Gerät die -Regeln anwendet. Das Gerät ermöglicht, bis zu 255 -Regeln einzurichten.

Tabelle

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

Schaltflächen



Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld legen Sie die Ziel-Adresse der Datenpakete fest, auf welche das Gerät die Regel anwendet. Das Gerät vermittelt Datenpakete mit dieser Zieladresse an die in Spalte festgelegte Zieladresse.

Mögliche Werte:

Gültige IPv4-Adresse

Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Zieladresse enthalten.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, die eine Zieladresse im hier festgelegten Subnetz enthalten.

- Im Feld legen Sie die IP-Adresse des Ziel-Endgeräts fest. Das Gerät vermittelt die Datenpakete an die hier festgelegte Zieladresse.

Mögliche Werte:

Gültige IPv4-Adresse

Das Gerät ersetzt die Zieladresse im Datenpaket durch diese neue Zieladresse.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Das Gerät ersetzt die Zieladresse im Datenpaket durch eine Zieladresse im hier festgelegten Subnetz.

Nach Klicken der Schaltfläche fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist dieser Tabellenzeile die in den Feldern und festgelegten Werte zu.



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.

Regelname

Zeigt den Namen der -Regel. Um den Namen zu ändern, klicken Sie in das betreffende Feld.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen

Priorität

Legt die Priorität der -Regel fest.

Anhand der Priorität legen Sie die Reihenfolge fest, in welcher das Gerät mehrere Regeln auf den Datenstrom anwendet. Das Gerät wendet die Regeln beginnend mit Priorität in aufsteigender Reihenfolge an.

Mögliche Werte:

(Voreinstellung:)

Eingangs-Interface

Weist der -Regel das Router-Interface zu, auf dem das Gerät die Datenpakete empfängt. Die -Regel macht im hier angeschlossenen Netz das Ziel-Endgerät virtuell erreichbar.

Mögliche Werte:

Das Gerät wendet die -Regel ausschließlich auf diesem Router-Interface an, und zwar ausschließlich auf Datenpakete, die an die in Spalte festgelegte IP-Adresse adressiert sind.

Der -Regel ist kein Router-Interface zugewiesen. Jemand hat das Router-Interface nach dem letzten Bearbeiten der -Regel entfernt.

Die ARP-Proxy-Funktion auf diesem Router-Interface schalten Sie im Dialog [Konfiguration](#) ein.

Ziel Adresse

Legt die Zieladresse der Datenpakete fest, auf die das Gerät die -Regel anwendet. Das Gerät vermittelt Datenpakete mit dieser Zieladresse an die in Spalte festgelegte Zieladresse.

Mögliche Werte:

Gültige IPv4-Adresse

Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Zieladresse enthalten.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, die eine Zieladresse im hier festgelegten Subnetz enthalten.

Ausgangs-Interface

Weist der -Regel das Router-Interface zu, auf dem das Gerät die modifizierten Datenpakete vermittelt. Im hier angeschlossenen Netz ist das Ziel-Endgerät tatsächlich erreichbar.

Mögliche Werte:

Das Gerät vermittelt die modifizierten Datenpakete auf diesem Router-Interface.

Der -Regel ist kein Router-Interface zugewiesen. Jemand hat das Router-Interface nach dem letzten Bearbeiten der -Regel entfernt.

Neue Adresse Ziel

Legt die tatsächliche IP-Adresse des Ziel-Endgeräts fest. Das Gerät vermittelt die Datenpakete an die hier festgelegte Zieladresse.

Mögliche Werte:

Gültige IPv4-Adresse

Das Gerät ersetzt die Zieladresse im Datenpaket durch diese neue Zieladresse.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Das Gerät ersetzt die Zieladresse im Datenpaket durch eine Zieladresse im hier festgelegten Subnetz.

Trap

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine -Regel auf ein Datenpaket anwendet.

Mögliche Werte:

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

Das Gerät sendet einen SNMP-Trap, wenn es die -Regel auf ein Datenpaket anwendet.
(Voreinstellung)

Das Senden von SNMP-Traps ist inaktiv.

Log

Aktiviert/deaktiviert die Protokollierung in der Log-Datei. Siehe Dialog .

Mögliche Werte:

Die Protokollierung ist aktiviert.

Wenn das Gerät die Regel auf ein Datenpaket anwendet, protokolliert das Gerät dies in der Log-Datei.

(Voreinstellung)

Die Protokollierung ist deaktiviert.

Aktiv

Aktiviert/deaktiviert die -Regel.

Mögliche Werte:

- Die Regel ist aktiv.
- (Voreinstellung)
- Die Regel ist inaktiv.

7.11.3 Destination-NAT

[Routing > NAT > Destination-NAT]

Die Funktion ermöglicht Ihnen, in einem lokalen Netz den Datenstrom ausgehender Kommunikationsverbindungen auf einen oder über einen Server umzuleiten.

Eine spezielle Form der Funktion ist die Port-Weiterleitung. Die Port-Weiterleitung verwenden Sie, um die Struktur eines Netzes nach außen hin zu verbergen und dennoch Kommunikationsverbindungen von außen in das Netz hinein zuzulassen. Eine typische Anwendung ist die Fernwartung eines PCs in einer Produktionszelle. Die Wartungsstation baut die Kommunikationsverbindung zum -Router auf, die Funktion kümmert sich um die Weiterleitung in die Produktionszelle.

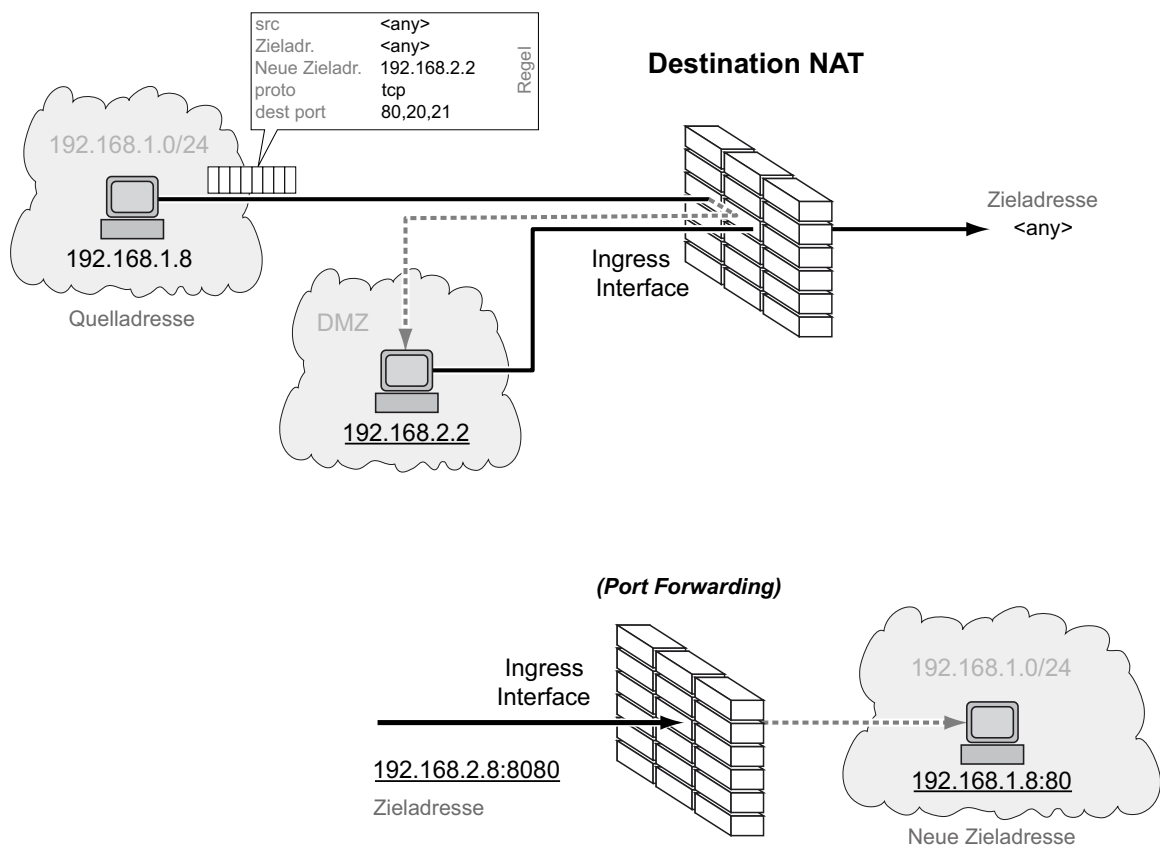


Abb. 5: Funktionsprinzip der Funktion

Um die Funktion zu nutzen, richten Sie für jedes Netz ein Router-Interface ein und schalten Sie die Routing-Funktion im Gerät ein.

Die Datenpakete durchlaufen die Filter-Funktionen des Geräts in folgender Reihenfolge:

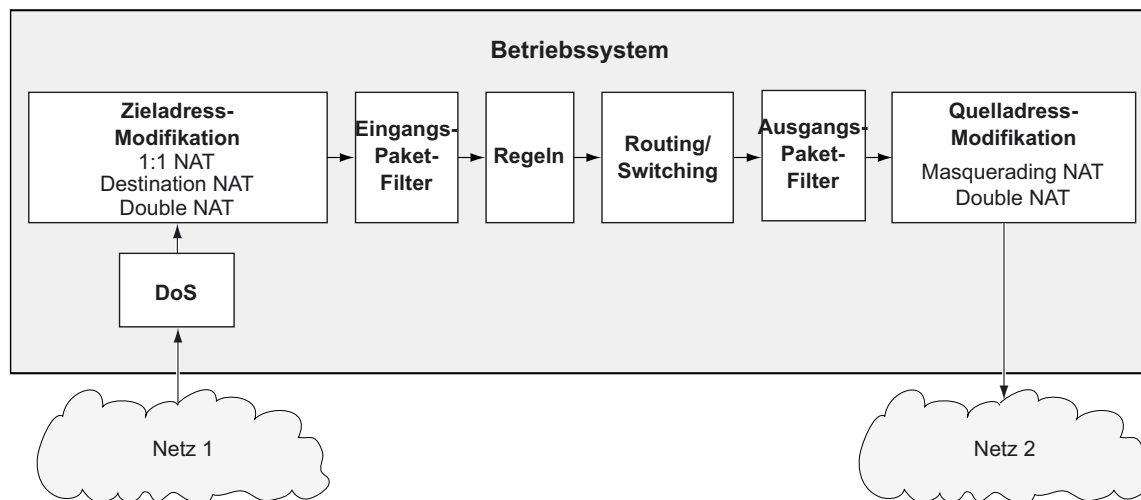


Abb. 6: Bearbeitungsreihenfolge der Datenpakete im Gerät

Das Menü enthält die folgenden Dialoge:

- [Destination-NAT Regel](#)
- [Destination-NAT Zuweisung](#)
- [Destination-NAT Übersicht](#)

7.11.3.1 Destination-NAT Regel

[Routing > NAT > Destination-NAT > Regel]

In diesem Dialog richten Sie die -Regeln ein.

Ein Router-Interface weisen Sie der betreffenden -Regel im Dialog [Destination-NAT > Zuweisung](#) zu.

Eine Übersicht, welche -Regel welchem Router-Interface zugewiesen ist, finden Sie im Dialog .

Das Gerät ermöglicht, bis zu 255 -Regeln einzurichten.

Tabelle

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

Schaltflächen

 Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld legen Sie die IP-Adresse des Ziel-Endgeräts fest. Das Gerät vermittelt die Datenpakete an die hier festgelegte Zieladresse.

Mögliche Werte:

Gültige IPv4-Adresse

Das Gerät ersetzt die Zieladresse im Datenpaket durch diese neue Zieladresse.

Nach Klicken der Schaltfläche fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist dieser Tabellenzeile den im Feld festgelegten Wert zu.

 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.

Regelname

Zeigt den Namen der -Regel. Um den Namen zu ändern, klicken Sie in das betreffende Feld.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen

Quelle Adresse

Legt die Quelladresse der Datenpakete fest, auf die das Gerät die -Regel anwendet.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die -Regel auf Datenpakete mit beliebiger Quelladresse an.

Gültige IPv4-Adresse

Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, die eine Quelladresse im hier festgelegten Subnetz enthalten.

Ein der IP-Adresse vorangestelltes Ausrufezeichen (!) verkehrt den Ausdruck ins Gegenteil.

Das Gerät wendet die -Regel auf Datenpakete an, welche die hier festgelegte Quelladresse NICHT enthalten.

Quelle Port

Legt den Quell-Port der Datenpakete fest, auf die das Gerät die -Regel anwendet. Voraussetzung ist, dass im Feld der Wert oder festgelegt ist.

Mögliche Werte:

(Voreinstellung)

Das Gerät wendet die -Regel auf sämtliche Datenpakete an, ohne den Quell-Port zu bewerten.

Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, die den festgelegten Quell-Port enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Mit einem einzelnen Zahlenwert legen Sie einen Port fest, zum Beispiel .
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel .
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel .
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel .

Die Spalte ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel eingeben, verwenden Sie 4 von 15 Zahlenwerten.

Ziel Adresse

Legt die Zieladresse der Datenpakete fest, auf die das Gerät die -Regel anwendet. Das Gerät vermittelt Datenpakete mit dieser Zieladresse an die in Spalte festgelegte Zieladresse.

Mögliche Werte:

Das Gerät wendet die -Regel auf Datenpakete mit beliebiger Zieladresse an.

Gültige IPv4-Adresse
Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Zieladresse enthalten.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation
Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, die eine Zieladresse im hier festgelegten Subnetz enthalten.

Ein der IP-Adresse vorangestelltes Ausrufezeichen () verkehrt den Ausdruck ins Gegenteil.
Das Gerät wendet die -Regel auf Datenpakete an, welche die hier festgelegte Zieladresse NICHT enthalten.

Ziel Port

Legt den Ziel-Port der Datenpakete fest, auf die das Gerät die -Regel anwendet.

Mögliche Werte:

(Voreinstellung)
Das Gerät wendet die -Regel auf sämtliche Datenpakete an, ohne den Ziel-Port zu bewerten.

Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, die den festgelegten Ziel-Port enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Mit einem einzelnen Zahlenwert legen Sie einen Port fest, zum Beispiel .
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel .
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel .
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel .

Die Spalte ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel eingeben, verwenden Sie 4 von 15 Zahlenwerten.

Neue Adresse Ziel

Legt die tatsächliche IP-Adresse des Ziel-Endgeräts fest. Das Gerät vermittelt die Datenpakete an die hier festgelegte Zieladresse.

Mögliche Werte:

Gültige IPv4-Adresse
Das Gerät ersetzt die Zieladresse im Datenpaket durch diese neue Zieladresse.

Ziel neuer Port

Legt den Port des Ziel-Endgeräts fest. Das Gerät vermittelt die Datenpakete an den hier festgelegten Ziel-Port.

Mögliche Werte:

Das Gerät behält im Datenpaket den ursprünglichen Ziel-Port bei.

Das Gerät ersetzt den Ziel-Port im Datenpaket durch diesen neuen Ziel-Port.

Protokoll

Beschränkt die -Regel auf ein IP-Protokoll. Das Gerät wendet die Regel ausschließlich auf Datenpakete des festgelegten IP-Protokolls an. -

Mögliche Werte:

Internet Control Message Protocol (RFC 792)

Internet Group Management Protocol

IP in IP tunneling (RFC 1853)

Transmission Control Protocol (RFC 793)

User Datagram Protocol (RFC 768)

IPsec Encapsulated Security Payload (RFC 2406)

IPsec Authentication Header (RFC 2402)

Internet Control Message Protocol for IPv6
(Voreinstellung)

Das Gerät wendet die -Regel auf sämtliche Datenpakete an, ohne das IP-Protokoll zu bewerten.

Log

Aktiviert/deaktiviert die Protokollierung in der Log-Datei. Siehe Dialog

Mögliche Werte:

Die Protokollierung ist aktiviert.

Wenn das Gerät die Regel auf ein Datenpaket anwendet, protokolliert das Gerät dies in der Log-Datei.

(Voreinstellung)

Die Protokollierung ist deaktiviert.

Trap

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine -Regel auf ein Datenpaket anwendet.

Mögliche Werte:

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

Das Gerät sendet einen SNMP-Trap, wenn es die -Regel auf ein Datenpaket anwendet.

(Voreinstellung)

Das Senden von SNMP-Traps ist inaktiv.

Aktiv

Aktiviert/deaktiviert die -Regel.

Mögliche Werte:


Die Regel ist aktiv.

(Voreinstellung)

Die Regel ist inaktiv.

7.11.3.2 Destination-NAT Zuweisung

[Routing > NAT > Destination-NAT > Zuweisung]

In diesem Dialog weisen Sie die -Regeln einem Router-Interface zu. Klicken Sie dazu die Schaltfläche .

Die -Regeln fügen Sie im Dialog hinzu und bearbeiten diese.

Eine Übersicht, welche -Regel welchem Router-Interface zugewiesen ist, finden Sie im Dialog .

Tabelle

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

Schaltflächen

 Löschen

Entfernt die ausgewählte Tabellenzeile.

 Zuweisen

Öffnet das Fenster . In diesem Fenster weisen Sie einer bestehenden -Regel ein eingerichtetes Router-Interface zu.

Port

Zeigt die Nummer des Router-Interfaces, auf welches das Gerät die -Regel anwendet.

Regel-Index

Zeigt die fortlaufende Nummer der -Regel. Siehe Spalte im Dialog [NAT > Destination-NAT > Regel](#). Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Regelname

Zeigt den Namen der -Regel. Siehe Spalte im Dialog [Destination-NAT > Regel](#).

Richtung

Zeigt, ob das Gerät die
oder empfängt.

-Regel auf Datenpakete anwendet, die das Gerät sendet

Mögliche Werte:

Das Gerät wendet die
face empfängt.

-Regel auf Datenpakete an, die es auf dem Router-Inter-
face empfängt.

Priorität

Legt die Priorität der

-Regel fest.

Anhand der Priorität legen Sie die Reihenfolge fest, in welcher das Gerät mehrere Regeln auf den Datenstrom anwendet. Das Gerät wendet die Regeln beginnend mit Priorität in aufsteigender Reihenfolge an.

Mögliche Werte:

(Voreinstellung:)

Aktiv

Aktiviert/deaktiviert die

-Regel.

Mögliche Werte:

Die Regel ist aktiv.

(Voreinstellung)

Die Regel ist inaktiv.

7.11.3.3 Destination-NAT Übersicht

[Routing > NAT > Destination-NAT > Übersicht]

In diesem Dialog finden Sie eine Übersicht, welche Router-Interface zugewiesen ist.

-Regel welchem Router-Inter-

Die -Regeln fügen Sie im Dialog hinzu und bearbeiten diese.

hinzunehmen

Ein Router-Interface weisen Sie der betreffenden [Destination-NAT > Zuweisung](#) zu.

-Regel im Dialog

Tabelle

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

Port

Zeigt die Nummer des Router-Interfaces, auf welches das Gerät die Regel anwendet.

-Regel

Regel-Index

Zeigt die fortlaufende Nummer der [NAT > Destination-NAT > Regel](#).

-Regel. Siehe Spalte

im Dialog

Regelname

Zeigt den Namen der [Destination-NAT > Regel](#).

-Regel. Siehe Spalte

im Dialog

Ziel Adresse

Zeigt die Zieladresse der Datenpakete, auf die das Gerät die Regel anwendet. Das Gerät vermittelt Datenpakete mit dieser Zieladresse an die in Spalte festgelegte Zieladresse.

-Regel anwendet. Das festgelegte

Neue Adresse Ziel

Zeigt die tatsächliche IP-Adresse des Ziel-Endgeräts. Das Gerät vermittelt die Datenpakete an die hier festgelegte Zieladresse.

Trap

Zeigt, ob das Gerät einen SNMP-Trap sendet, wenn es die -Regel auf ein Datenpaket anwendet.

Mögliche Werte:

Das Gerät sendet einen SNMP-Trap. Voraussetzung ist, dass im Dialog [Statuskonfiguration > Alarmer \(Traps\)](#) die Funktion eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.

Das Gerät sendet keinen SNMP-Trap.

Log

Zeigt, ob das Gerät in der Log-Datei protokolliert, wenn es die -Regel auf ein Datenpaket anwendet.

Mögliche Werte:

Wenn das Gerät die Regel auf ein Datenpaket anwendet, protokolliert das Gerät dies in der Log-Datei. Siehe Dialog [Log-Einstellungen](#).

Protokollierung ist ausgeschaltet.

Richtung

Zeigt, ob das Gerät die -Regel auf Datenpakete anwendet, die das Gerät sendet oder empfängt.

Mögliche Werte:

Das Gerät wendet die -Regel auf Datenpakete an, die es auf dem Router-Interface empfängt.

Priorität

Zeigt die Priorität der -Regel.

Das Gerät wendet die Regeln beginnend mit Priorität in aufsteigender Reihenfolge auf den Datenstrom an.

7.11.4 Masquerading-NAT

[Routing > NAT > Masquerading-NAT]

Die Funktion `masquerading-nat` versteckt beliebig viele Endgeräte hinter der IP-Adresse des `masquerading-nat`-Routers und verbirgt somit die Struktur eines Netzes vor anderen Netzen. Dazu ersetzt der `masquerading-nat`-Router im Datenpaket die Absenderadresse durch seine eigene IP-Adresse. Zusätzlich ersetzt der `masquerading-nat`-Router im Datenpaket den Quell-Port durch einen eigenen Wert, um die Antwort-Datenpakete später wieder an den ursprünglichen Absender zu vermitteln.

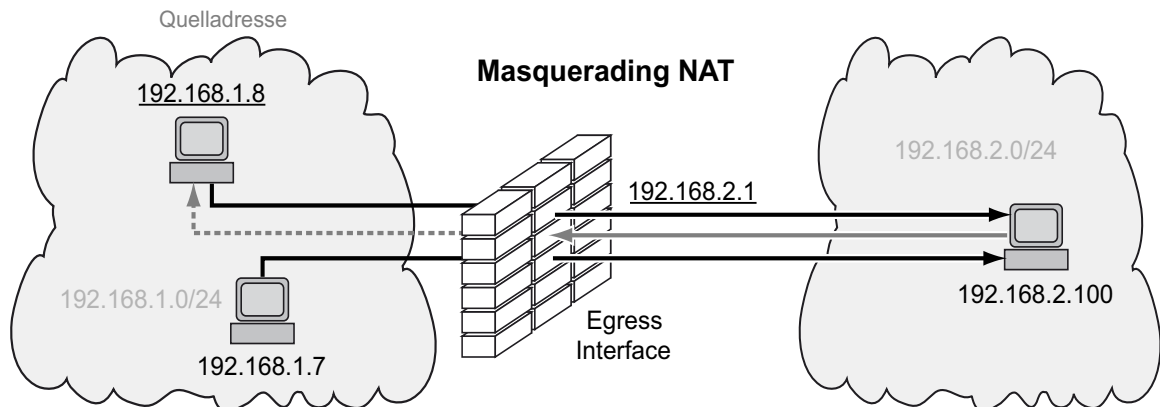


Abb. 7: Funktionsprinzip der Funktion

Um die Funktion `masquerading-nat` zu nutzen, richten Sie für jedes Netz ein Router-Interface ein und schalten Sie die Routing-Funktion im Gerät ein.

Anmerkung: Wenn Sie auf einem Router-Interface die Funktion `masquerading-nat` einschalten, dann ist auf diesem Router-Interface die Funktion `destination-nat` unwirksam.

Die Datenpakete durchlaufen die Filter-Funktionen des Geräts in folgender Reihenfolge:

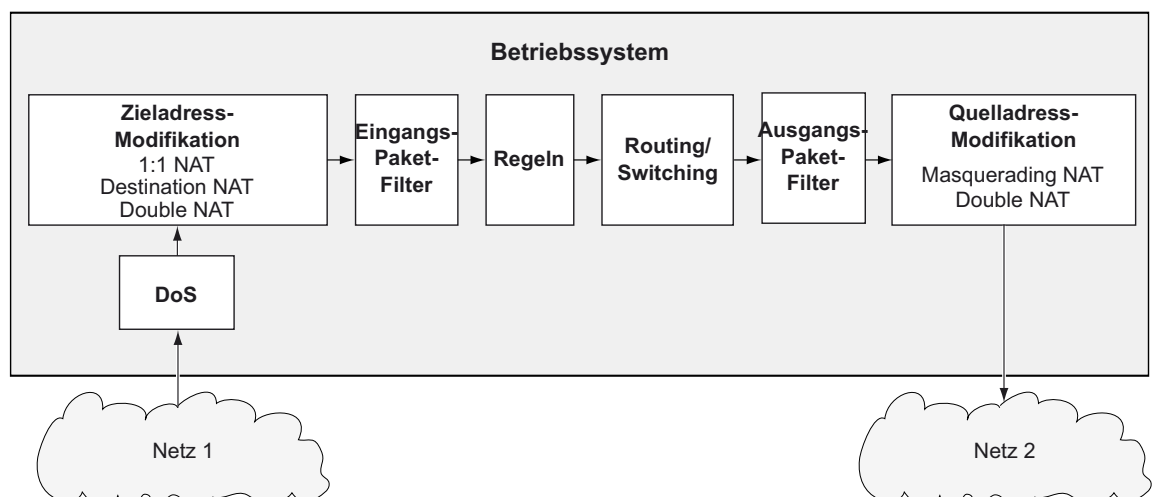


Abb. 8: Bearbeitungsreihenfolge der Datenpakete im Gerät

Das Menü enthält die folgenden Dialoge:

- [Masquerading-NAT Regel](#)
- [Masquerading-NAT Zuweisung](#)
- [Masquerading-NAT Übersicht](#)

7.11.4.1 Masquerading-NAT Regel

[Routing > NAT > Masquerading-NAT > Regel]

In diesem Dialog richten Sie die **Masquerading-NAT**-Regeln ein.

Ein Router-Interface weisen Sie der betreffenden **Masquerading-NAT**-Regel im Dialog **NAT > Masquerading-NAT > Zuweisung** zu.

Eine Übersicht, welche **Masquerading-NAT**-Regel welchem Router-Interface zugewiesen ist, finden Sie im Dialog **Masquerading-NAT > Übersicht**.

Das Gerät ermöglicht, bis zu 128 **Masquerading-NAT**-Regeln einzurichten.

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.

Regelname

Zeigt den Namen der **Masquerading-NAT**-Regel. Um den Namen zu ändern, klicken Sie in das betreffende Feld.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen

Quelle Adresse

Legt die Quelladresse der Datenpakete fest, auf die das Gerät die **Masquerading-NAT**-Regel anwendet.

Mögliche Werte:

Das Gerät wendet die **Masquerading-NAT**-Regel auf Datenpakete mit beliebiger Quelladresse an.

Gültige IPv4-Adresse
 Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation
 Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, die eine Quelladresse im hier festgelegten Subnetz enthalten.

Ein der IP-Adresse vorangestelltes Ausrufezeichen () verkehrt den Ausdruck ins Gegenteil.
 Das Gerät wendet die -Regel auf Datenpakete an, welche die hier festgelegte Quelladresse NICHT enthalten.

Quelle Port

Legt den Quell-Port der Datenpakete fest, auf die das Gerät die -Regel anwendet.

Mögliche Werte:

(Voreinstellung)
 Das Gerät wendet die -Regel auf sämtliche Datenpakete an, ohne den Quell-Port zu bewerten.

Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, die den festgelegten Quell-Port enthalten.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Mit einem einzelnen Zahlenwert legen Sie einen Port fest, zum Beispiel .
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel .
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel .
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel .

Die Spalte ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel eingeben, verwenden Sie 4 von 15 Zahlenwerten.

Protokoll

Beschränkt die -Regel auf ein IP-Protokoll. Das Gerät wendet die -Regel ausschließlich auf Datenpakete des festgelegten IP-Protokolls an.

Mögliche Werte:

Transmission Control Protocol (RFC 793)

User Datagram Protocol (RFC 768)

(Voreinstellung)
 Das Gerät wendet die -Regel auf sämtliche Datenpakete an, ohne das IP-Protokoll zu bewerten.

Log

Aktiviert/deaktiviert die Protokollierung in der Log-Datei. Siehe Dialog

Mögliche Werte:

Die Protokollierung ist aktiviert.
Wenn das Gerät die
Gerät dies in der Log-Datei.

(Voreinstellung)

Die Protokollierung ist deaktiviert.

Regel auf ein Datenpaket anwendet, protokolliert das

Trap

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine
auf ein Datenpaket anwendet.

-Regel

Mögliche Werte:

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

Das Gerät sendet einen SNMP-Trap, wenn es die
anwendet.

(Voreinstellung)

Das Senden von SNMP-Traps ist inaktiv.

-Regel auf ein Datenpaket

IPsec exempt

Aktiviert/deaktiviert das Anwenden der

-Regel auf IPsec-Datenpakete.

Mögliche Werte:

Das Gerät wendet die -Regel auf IPsec-Datenpakete nicht an. Das Gerät
sendet IPsec-Datenpakete unmodifiziert durch den VPN-Tunnel.

(Voreinstellung)

Das Gerät wendet die -Regel auf IPsec-Datenpakete an. Abhängig von den
Einstellungen des Traffic-Selectors in den Spalten und -

sendet das Gerät IPsec-Datenpakete durch den VPN-Tunnel. Siehe Dialog

Aktiv

Aktiviert/deaktiviert die

-Regel.

Mögliche Werte:


Die Regel ist aktiv.

(Voreinstellung)

Die Regel ist inaktiv.

7.11.4.2 Masquerading-NAT Zuweisung

[Routing > NAT > Masquerading-NAT > Zuweisung]

In diesem Dialog weisen Sie die -Regeln einem Router-Interface zu. Klicken Sie dazu die Schaltfläche .

Die -Regeln fügen Sie im Dialog hinzu und bearbeiten diese.

Eine Übersicht, welche -Regel welchem Router-Interface zugewiesen ist, finden Sie im Dialog .

Tabelle

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

Schaltflächen

 Löschen

Entfernt die ausgewählte Tabellenzeile.

 Zuweisen

Öffnet das Fenster . In diesem Fenster weisen Sie einer bestehenden -Regel ein eingerichtetes Router-Interface zu.

Port

Zeigt die Nummer des Router-Interfaces, auf welches das Gerät die -Regel anwendet.

Regel-Index

Zeigt die fortlaufende Nummer der -Regel. Siehe Spalte im Dialog [NAT > Masquerading-NAT > Regel](#). Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Regelname

Zeigt den Namen der -Regel. Siehe Spalte im Dialog [Masquerading-NAT > Regel](#).

Richtung

Zeigt, ob das Gerät die
oder empfängt.

-Regel auf Datenpakete anwendet, die das Gerät sendet

Mögliche Werte:

Das Gerät wendet die
Interface sendet.

-Regel auf Datenpakete an, die es auf dem Router-

Priorität

Legt die Priorität der

-Regel fest.

Anhand der Priorität legen Sie die Reihenfolge fest, in welcher das Gerät mehrere Regeln auf den Datenstrom anwendet. Das Gerät wendet die Regeln beginnend mit Priorität in aufsteigender Reihenfolge an.

Mögliche Werte:

(Voreinstellung:)

Aktiv

Aktiviert/deaktiviert die

-Regel.

Mögliche Werte:

Die Regel ist aktiv.

(Voreinstellung)

Die Regel ist inaktiv.

7.11.4.3 Masquerading-NAT Übersicht

[Routing > NAT > Masquerading-NAT > Übersicht]

In diesem Dialog finden Sie eine Übersicht, welche Router-Interface zugewiesen ist.

-Regel welchem Router-Inter-

Die -Regeln fügen Sie im Dialog hinzu und bearbeiten diese.

hinzu

Ein Router-Interface weisen Sie der betreffenden NAT > Masquerading-NAT > Zuweisung zu.

-Regel im Dialog

Tabelle

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

Port

Zeigt die Nummer des Router-Interfaces, auf welches das Gerät die Regel anwendet.

-Regel

Regel-Index

Zeigt die fortlaufende Nummer der NAT > Masquerading-NAT > Regel.

-Regel. Siehe Spalte im Dialog

Regelname

Zeigt den Namen der Masquerading-NAT > Regel.

-Regel. Siehe Spalte im Dialog

Trap

Zeigt, ob das Gerät einen SNMP-Trap sendet, wenn es die Regel auf ein Datenpaket anwendet.

-Regel auf ein Daten-

Mögliche Werte:

Das Gerät sendet einen SNMP-Trap. Voraussetzung ist, dass im Dialog Statuskonfiguration > Alarme (Traps) die Funktion eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.

Das Gerät sendet keinen SNMP-Trap.

Log

Zeigt, ob das Gerät in der Log-Datei protokolliert, wenn es die **Log**-Regel auf ein Datenpaket anwendet.

Mögliche Werte:

Wenn das Gerät die **Log**-Regel auf ein Datenpaket anwendet, protokolliert das Gerät dies in der Log-Datei. Siehe Dialog **Log**.

Protokollierung ist ausgeschaltet.

Richtung

Zeigt, ob das Gerät die **Outgoing**-Regel auf Datenpakete anwendet, die das Gerät sendet oder empfängt.

Mögliche Werte:

Das Gerät wendet die **Outgoing**-Regel auf Datenpakete an, die es auf dem Router-Interface sendet.

Priorität

Zeigt die Priorität der **Outgoing**-Regel.

Das Gerät wendet die Regeln beginnend mit Priorität **1** in aufsteigender Reihenfolge auf den Datenstrom an.

7.11.5 Double-NAT

[Routing > NAT > Double-NAT]

Die Funktion ermöglicht Ihnen, Kommunikationsverbindungen zwischen Endgeräten in unterschiedlichen IP-Netzen aufzubauen, die keine Möglichkeit bieten, ein Standard-Gateway oder eine Standard-Route festzulegen. Der -Router „verschiebt“ die Endgeräte virtuell in das jeweils andere Netz. Dazu ersetzt der -Router beim Vermitteln die Quelladresse und die Zieladresse im Datenpaket. Eine typische Anwendung ist das Verbinden von Steuerungen, die sich in unterschiedlichen Netzen befinden.

Voraussetzung für die Funktion ist, dass der -Router selbst auf ARP-Anfragen aus dem jeweiligen Netz antwortet. Schalten Sie dazu auf dem Ingress-Interface und auf dem Egress-Interface die ARP-Proxy-Funktion ein.

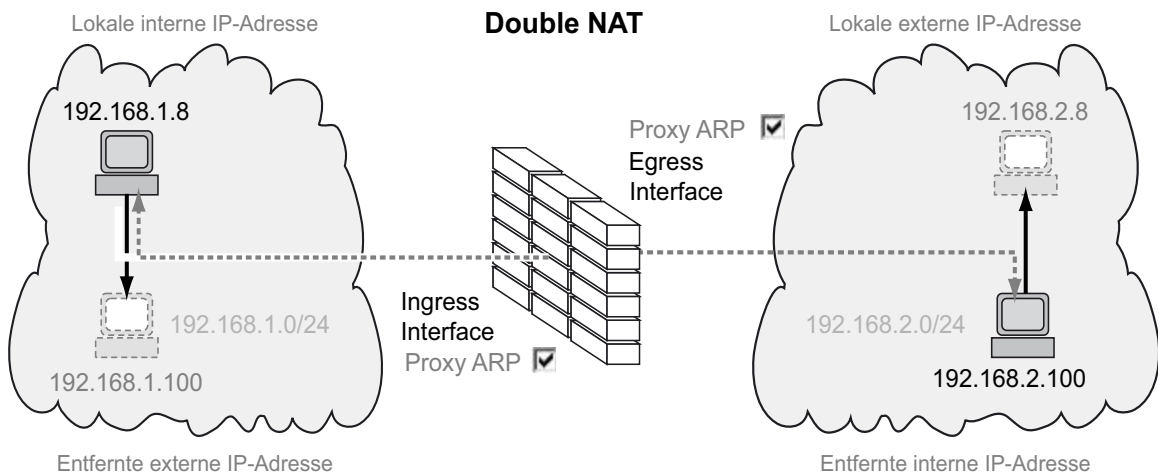


Abb. 9: Funktionsprinzip der Funktion

Um die Funktion zu nutzen, richten Sie für jedes Netz ein Router-Interface ein und schalten Sie die Routing-Funktion im Gerät ein.

Die Datenpakete durchlaufen die Filter-Funktionen des Geräts in folgender Reihenfolge:

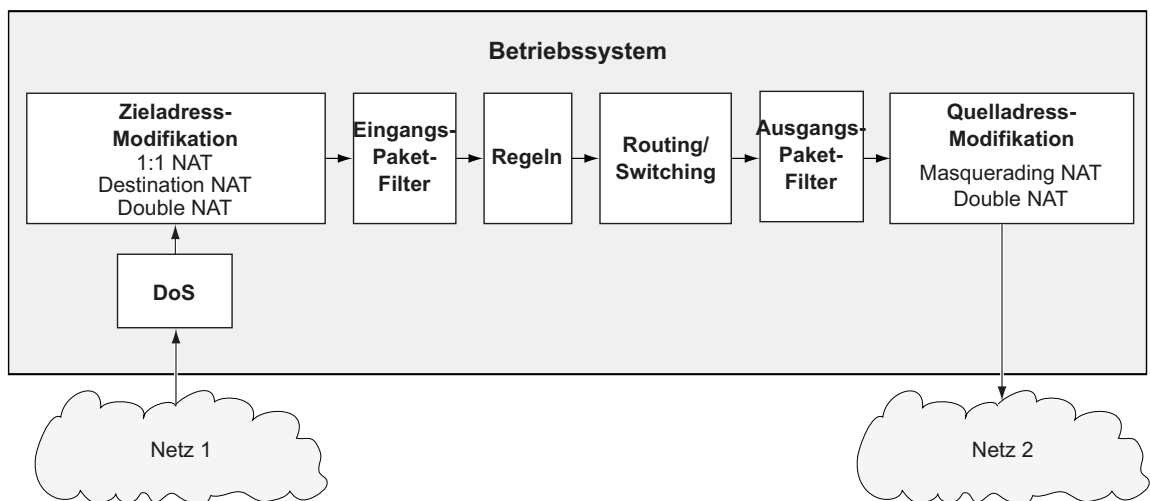


Abb. 10: Bearbeitungsreihenfolge der Datenpakete im Gerät

Das Menü enthält die folgenden Dialoge:

- Double-NAT Regel
- Double-NAT Zuweisung
- Double-NAT Übersicht

7.11.5.1 Double-NAT Regel

[Routing > NAT > Double-NAT > Regel]

In diesem Dialog richten Sie die -Regeln ein.

Die Router-Interface weisen Sie der betreffenden -Regel im Dialog [Double-NAT > Zuweisung](#) zu.

Eine Übersicht, welche -Regel welchen Router-Interfaces zugewiesen ist, finden Sie im Dialog .

Das Gerät ermöglicht, bis zu 255 -Regeln einzurichten.

Tabelle

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

Schaltflächen



Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

- Im Feld legen Sie für das im ersten Netz platzierte Endgerät die tatsächliche IP-Adresse fest.
Mögliche Werte:
Gültige IPv4-Adresse
Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.
- Im Feld legen Sie für das im ersten Netz platzierte Endgerät die virtuelle IP-Adresse im zweiten Netz fest.
Mögliche Werte:
Gültige IPv4-Adresse
Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.

- Im Feld legen Sie für das im zweiten Netz platzierte Endgerät die tatsächliche IP-Adresse fest.
Mögliche Werte:
Gültige IPv4-Adresse
Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.
- Im Feld legen Sie für das im zweiten Netz platzierte Endgerät die virtuelle IP-Adresse im ersten Netz fest.
Mögliche Werte:
Gültige IPv4-Adresse
Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.
Nach Klicken der Schaltfläche fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist dieser Tabellenzeile die in den Feldern , , und festgelegten Werte zu.



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.

Regelname

Zeigt den Namen der -Regel. Um den Namen zu ändern, klicken Sie in das betreffende Feld.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen

Lokale interne IP-Adresse

Legt für das im ersten Netz platzierte Endgerät die tatsächliche IP-Adresse fest.

Mögliche Werte:

Gültige IPv4-Adresse

Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.

Lokale externe IP-Adresse

Legt für das im ersten Netz platzierte Endgerät die virtuelle IP-Adresse im zweiten Netz fest.

Mögliche Werte:

Gültige IPv4-Adresse

Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.

Ferne interne IP-Adresse

Legt für das im zweiten Netz platzierte Endgerät die tatsächliche IP-Adresse fest.

Mögliche Werte:

Gültige IPv4-Adresse

Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.

Ferne externe IP-Adresse

Legt für das im zweiten Netz platzierte Endgerät die virtuelle IP-Adresse im ersten Netz fest.

Mögliche Werte:

Gültige IPv4-Adresse

Das Gerät wendet die -Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.

Log

Aktiviert/deaktiviert die Protokollierung in der Log-Datei. Siehe Dialog

.

Mögliche Werte:

Die Protokollierung ist aktiviert.

Das Gerät protokolliert das Anwenden der -Regel auf ein Datenpaket in der Log-Datei.

(Voreinstellung)

Die Protokollierung ist deaktiviert.

Trap

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine -Regel auf ein Datenpaket anwendet.

Mögliche Werte:

Das Senden von SNMP-Traps ist aktiv. Voraussetzung ist, dass im Dialog

[Statuskonfiguration > Alarme \(Traps\)](#) die Funktion eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.

Das Gerät sendet einen SNMP-Trap, wenn es die -Regel auf ein Datenpaket anwendet.

(Voreinstellung)

Das Senden von SNMP-Traps ist inaktiv.

Aktiv

Aktiviert/deaktiviert die -Regel.

Mögliche Werte:


Die Regel ist aktiv.

(Voreinstellung)

Die Regel ist inaktiv.

7.11.5.2 Double-NAT Zuweisung

[Routing > NAT > Double-NAT > Zuweisung]

In diesem Dialog weisen Sie die -Regeln einem Router-Interface zu. Klicken Sie dazu die Schaltfläche .

Die -Regeln fügen Sie im Dialog hinzu und bearbeiten diese.

Eine Übersicht, welche -Regel welchen Router-Interfaces zugewiesen ist, finden Sie im Dialog .

Tabelle

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

Schaltflächen

 Löschen

Entfernt die ausgewählte Tabellenzeile.

 Zuweisen

Öffnet das Fenster . In diesem Fenster weisen Sie einer bestehenden -Regel ein eingerichtetes Router-Interface zu.

Port

Zeigt die Nummer des Router-Interfaces, auf welches das Gerät die -Regel anwendet.

Regel-Index

Zeigt die fortlaufende Nummer der -Regel. Siehe Spalte im Dialog [Double-NAT > Regel](#). Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Regelname

Zeigt den Namen der -Regel. Siehe Spalte im Dialog .

Richtung

Zeigt, ob das Gerät die -Regel auf Datenpakete anwendet, die das Gerät sendet oder empfängt.

Mögliche Werte:


Das Gerät wendet die -Regel auf Datenpakete an, die es auf dem Router-Interface empfängt.

Das Gerät wendet die
sendet.

-Regel auf Datenpakete an, die es auf dem Router-Interface

Das Gerät wendet die
empfängt oder sendet.

-Regel auf Datenpakete an, die es auf dem Router-Interface

Sie können den Wert ändern, wenn Sie die Schaltfläche  klicken.

Priorität

Legt die Priorität der -Regel fest.

Anhand der Priorität legen Sie die Reihenfolge fest, in welcher das Gerät mehrere Regeln auf den Datenstrom anwendet. Das Gerät wendet die Regeln beginnend mit Priorität in aufsteigender Reihenfolge an.

Mögliche Werte:

(Voreinstellung:)

Aktiv

Aktiviert/deaktiviert die -Regel.

Mögliche Werte:

Die Regel ist aktiv.

(Voreinstellung)

Die Regel ist inaktiv.

7.11.5.3 Double-NAT Übersicht

[Routing > NAT > Double-NAT > Übersicht]

In diesem Dialog finden Sie eine Übersicht, welche

-Regel welchem Router-Interface

Die -Regeln fügen Sie im Dialog hinzu und bearbeiten diese.

Die Router-Interface weisen Sie der betreffenden [Double-NAT > Zuweisung](#) zu.

-Regel im Dialog

Tabelle

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

Port

Zeigt die Nummer des Router-Interfaces, auf welches das Gerät die

-Regel anwendet.

Regel-Index

Zeigt die fortlaufende Nummer der [Double-NAT > Regel](#).

-Regel. Siehe Spalte

im Dialog

Regelname

Zeigt den Namen der

-Regel. Siehe Spalte

im Dialog

Lokale interne IP-Adresse

Zeigt für das im ersten Netz platzierte Endgerät die tatsächliche IP-Adresse.

Lokale externe IP-Adresse

Zeigt für das im ersten Netz platzierte Endgerät die virtuelle IP-Adresse im zweiten Netz.

Ferne interne IP-Adresse

Zeigt für das im zweiten Netz platzierte Endgerät die tatsächliche IP-Adresse.

Ferne externe IP-Adresse

Zeigt für das im zweiten Netz platzierte Endgerät die virtuelle IP-Adresse im ersten Netz.

Trap

Zeigt, ob das Gerät einen SNMP-Trap sendet, wenn es die -Regel auf ein Datenpaket
 anwendet.

Mögliche Werte:

Das Gerät sendet einen SNMP-Trap. Voraussetzung ist, dass im Dialog eingeschaltet und mindestens
[Statuskonfiguration > Alarmer \(Traps\)](#) die Funktion ein Trap-Ziel festgelegt ist.

Das Gerät sendet keinen SNMP-Trap.

Log

Zeigt, ob das Gerät in der Log-Datei protokolliert, wenn es die -Regel auf ein Daten-
 paket anwendet.

Mögliche Werte:

Wenn das Gerät die Regel auf ein Datenpaket anwendet, protokolliert das Gerät
 dies in der Log-Datei. Siehe Dialog .

Protokollierung ist ausgeschaltet.

Richtung

Zeigt, ob das Gerät die -Regel auf Datenpakete anwendet, die das Gerät sendet oder
 empfängt.

Mögliche Werte:

Das Gerät wendet die -Regel auf Datenpakete an, die es auf dem Router-Interface
 empfängt.

Das Gerät wendet die -Regel auf Datenpakete an, die es auf dem Router-Interface
 sendet.

Das Gerät wendet die -Regel auf Datenpakete an, die es auf dem Router-Interface
 empfängt oder sendet.

Priorität

Zeigt die Priorität der -Regel.

Das Gerät wendet die Regeln beginnend mit Priorität in aufsteigender Reihenfolge auf den
 Datenstrom an.

8 Diagnose

Das Menü enthält die folgenden Dialoge:

- Statuskonfiguration
- System
- Syslog
- Ports
- LLDP
- Bericht

8.1 Statuskonfiguration

[Diagnose > Statuskonfiguration]

Das Menü enthält die folgenden Dialoge:

- Gerätestatus
- Sicherheitsstatus
- Alarme (Traps)

8.1.1 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 `OK` oder `Warn` im Rahmen `Geräte-Status`. Das Gerät bestimmt diesen Status anhand der einzelnen Überwachungsergebnisse.

Das Gerät zeigt ermittelte Fehler in der Registerkarte `Fehler` und zusätzlich im Dialog `Geräte-Status`, 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:

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:

(Voreinstellung)

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

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

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:

Die Überwachung ist aktiv.

Der Wert im Rahmen wechselt auf , wenn der Link auf einem überwachten Port/Interface abbricht.

In der Registerkarte haben Sie die Möglichkeit, die zu überwachenden Ports/Interfaces einzeln auszuwählen.

(Voreinstellung)

Die Überwachung ist inaktiv.

Temperatur

Aktiviert/deaktiviert die Überwachung der Temperatur im Gerät.

Mögliche Werte:

(Voreinstellung)

Die Überwachung ist aktiv.

Wenn die Temperatur den festgelegten oberen Schwellenwert überschreitet oder den festgelegten unteren Schwellenwert unterschreitet, wechselt der Wert im Rahmen auf

Die Überwachung ist inaktiv.

Die Schwellenwerte für die Temperatur legen Sie fest im Dialog , Feld und Feld .

Externen Speicher entfernen

Aktiviert/deaktiviert die Überwachung des aktiven externen Speichers.

Mögliche Werte:

Die Überwachung ist aktiv.

Der Wert im Rahmen wechselt auf , wenn Sie den aktiven externen Speicher aus dem Gerät entfernen.

(Voreinstellung)

Die Überwachung ist inaktiv.

Externer Speicher nicht synchron

Aktiviert/deaktiviert die Überwachung der Konfigurationsprofile im Gerät und im externen Speicher.

Mögliche Werte:

Die Überwachung ist aktiv.

In folgenden Situationen wechselt der Wert im Rahmen auf :

- Das Konfigurationsprofil existiert ausschließlich im Gerät.
- Das Konfigurationsprofil im Gerät unterscheidet sich vom Konfigurationsprofil im externen Speicher.

(Voreinstellung)

Die Überwachung ist inaktiv.

Netzteil

Aktiviert/deaktiviert die Überwachung des Netzteils.

Mögliche Werte:

(Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen wechselt auf , wenn das Gerät einen Fehler am Netzteil feststellt.

Die Überwachung ist inaktiv.

[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:

Die Überwachung ist aktiv.

Der Wert im Rahmen wechselt auf , wenn der Link auf dem ausgewählten Port/Interface abbricht.

(Voreinstellung)

Die Überwachung ist inaktiv.

Die Einstellung ist wirksam, wenn Sie in der Registerkarte das Kontrollkästchen -
 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 .

Ursache

Zeigt das Ereignis, das den SNMP-Trap ausgelöst hat.

8.1.2 Sicherheitsstatus

[Diagnose > Statuskonfiguration > Sicherheitsstatus]

Dieser Dialog gibt einen Überblick über den Zustand der sicherheitsrelevanten Einstellungen im Gerät.

Das Gerät zeigt seinen gegenwärtigen Status als oder im Rahmen . Das Gerät bestimmt diesen Status anhand der einzelnen Überwachungsergebnisse.

Das Gerät zeigt ermittelte Fehler in der Registerkarte und zusätzlich im Dialog , Rahmen .

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:

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:

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

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

(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

Mögliche Werte:

(Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen wechselt auf , wenn Sie für das Benutzerkonto das voreingestellte Passwort unverändert verwenden.

Die Überwachung ist inaktiv.

Das Passwort legen Sie fest im Dialog

Min. Passwort-Länge kürzer als 8

Aktiviert/deaktiviert die Überwachung der Richtlinie

Mögliche Werte:

(Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen wechselt auf , wenn für die Richtlinie ein Wert kleiner als festgelegt ist.

Die Überwachung ist inaktiv.

Die Richtlinie für die legen Sie fest im Dialog

□□□Rahmen

Passwort-Richtlinien deaktiviert

Aktiviert/deaktiviert die Überwachung der Passwort-Richtlinien-Einstellungen.

Mögliche Werte:

(Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen wechselt auf , wenn für mindestens eine der folgenden Richtlinien ein Wert kleiner als festgelegt ist.

–

–

–

–

Die Überwachung ist inaktiv.

Die Einstellungen für die Richtlinie legen Sie fest im Dialog
Rahmen

Prüfen der Passwort-Richtlinien im Benutzerkonto deaktiviert

Aktiviert/deaktiviert die Überwachung der Funktion .

Mögliche Werte:

Die Überwachung ist aktiv.

Der Wert im Rahmen wechselt auf , wenn die Funktion -

□□□□ bei mindestens ein Benutzerkonto inaktiv ist.

(Voreinstellung)

Die Überwachung ist inaktiv.

Die Funktion aktivieren Sie im Dialog .

HTTP-Server aktiv

Aktiviert/deaktiviert die Überwachung des HTTP-Servers.

Mögliche Werte:

(Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen wechselt auf , wenn Sie den HTTP-Server einschalten.

Die Überwachung ist inaktiv.

Den HTTP-Server schalten Sie ein/aus im Dialog , Registerkarte .

SNMP unverschlüsselt

Aktiviert/deaktiviert die Überwachung des SNMP-Servers.

Mögliche Werte:

(Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen wechselt auf , wenn mindestens eine der folgenden Bedingungen zutrifft:

- Die Funktion ist eingeschaltet.
- Die Funktion ist eingeschaltet.
- Die Verschlüsselung für SNMPv3 ist ausgeschaltet.

Die Verschlüsselung schalten Sie ein im Dialog , Spalte .

Die Überwachung ist inaktiv.

Die Einstellungen für den SNMP-Agenten legen Sie fest im Dialog , Registerkarte .

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:

Die Überwachung ist aktiv.
Der Wert im Rahmen wechselt auf , wenn Sie den System-Monitor aktivieren.

(Voreinstellung)

Die Überwachung ist inaktiv.

Den System-Monitor aktivieren/deaktivieren Sie im Dialog .

Speichern des Konfigurationsprofils auf dem externen Speicher möglich

Aktiviert/deaktiviert die Überwachung des Konfigurationsprofils im externen Speicher.

Mögliche Werte:

Die Überwachung ist aktiv.
Der Wert im Rahmen wechselt auf , wenn das Speichern des Konfigurationsprofils auf dem externen Speicher aktiv ist.

(Voreinstellung)

Die Überwachung ist inaktiv.

Das Speichern des Konfigurationsprofils im externen Speicher aktivieren/deaktivieren Sie im Dialog .

Verbindungsabbruch auf eingeschalteten Ports

Aktiviert/deaktiviert die Überwachung des Links auf den aktiven Ports.

Mögliche Werte:

Die Überwachung ist aktiv.
Der Wert im Rahmen wechselt auf , wenn der Link auf einem aktiven Port abbricht. In der Registerkarte haben Sie die Möglichkeit, die zu überwachenden Ports einzeln auszuwählen.

(Voreinstellung)

Die Überwachung ist inaktiv.

Zugriff mit HiDiscovery möglich

Aktiviert/deaktiviert die Überwachung der Funktion HiDiscovery.

Mögliche Werte:

(Voreinstellung)

Die Überwachung ist aktiv.
Der Wert im Rahmen wechselt auf , wenn Sie die Funktion HiDiscovery einschalten.

Die Überwachung ist inaktiv.

Die Funktion HiDiscovery schalten Sie im Dialog ein/aus.

Unverschlüsselte Konfiguration vom externen Speicher laden

Aktiviert/deaktiviert die Überwachung des Ladens unverschlüsselter Konfigurationsprofile vom externen Speicher.

Mögliche Werte:

(Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen wechselt auf , wenn die Einstellungen dem Gerät ermöglichen, ein unverschlüsseltes Konfigurationsprofil vom externen Speicher zu laden.

Der Rahmen im Dialog zeigt einen Alarm, wenn folgende Voraussetzungen erfüllt sind:

- Das im externen Speicher gespeicherte Konfigurationsprofil ist unverschlüsselt.
und
- Die Spalte im Dialog hat den Wert .

Die Überwachung ist inaktiv.

Self-signed HTTPS-Zertifikat vorhanden

Aktiviert/deaktiviert die Überwachung des digitalen Zertifikats des HTTP-Servers.

Mögliche Werte:

(Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen wechselt auf , wenn der HTTPS-Server ein selbst generiertes digitales Zertifikat verwendet.

Die Überwachung ist inaktiv.

[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:

Die Überwachung ist aktiv.

Der Wert im Rahmen wechselt auf , wenn der Port eingeschaltet ist (Dialog , Registerkarte , Kontrollkästchen ist) und wenn der Link auf dem Port abbricht.

(Voreinstellung)

Die Überwachung ist inaktiv.

Diese Einstellung ist wirksam, wenn Sie im Dialog , Registerkarte , das Kontrollkästchen 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 .

Ursache

Zeigt das Ereignis, das den SNMP-Trap ausgelöst hat.

8.1.3 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:

-
-

Beim Einrichten von Loopback-Interfaces verwendet das Gerät die IP-Adresse des ersten Loopback-Interfaces als Absender der SNMP-Traps. Andernfalls verwendet das Gerät die Adresse des Management des Geräts.

Das Menü enthält die folgenden Dialoge:

[Trap Ziele](#)

8.1.3.1 Trap Ziele

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

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

Funktion

Funktion

Schaltet das Senden von SNMP-Traps ein/aus.

Mögliche Werte:

(Voreinstellung)

Das Senden von SNMP-Traps ist eingeschaltet.

Das Senden von SNMP-Traps ist ausgeschaltet.

SNMPv1/v2-Trap-Community

Name

Legt die Community-Zeichenfolge fest, die das Gerät in jedem SNMPv1/v2-Trap zur Authentifizierung an das Trap-Ziel sendet.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

(Voreinstellung)

Tabelle

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

Schaltflächen



Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen. Damit richten Sie ein Trap-Ziel auf dem Gerät ein.

- Im Feld legen Sie einen Namen für das Trap-Ziel fest.
Mögliche Werte:
Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen
- Im Feld legen Sie IP-Adresse und Port des Trap-Ziels fest.
Mögliche Werte:

Wenn Sie keinen Port festlegen, fügt das Gerät automatisch den Port dem Trap-Ziel hinzu.



Entfernt die ausgewählte Tabellenzeile.

Name

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

Adresse

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

Mögliche Werte:

Wenn Sie keinen Port festlegen, fügt das Gerät automatisch den Port dem Trap-Ziel hinzu.

Aktiv

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

Mögliche Werte:

(Voreinstellung)

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

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

8.2 System

[Diagnose > System]

Das Menü enthält die folgenden Dialoge:

- Systeminformationen
- Konfigurations-Check
- ARP
- Selbsttest

8.21 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.

8.2.2 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: Der Dialog zeigt die am Nachbargerät angeschlossenen erkannten Geräte so, als wären sie direkt am Gerät angeschlossen.

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 das Gerät beim Konfigurations-Check erkannt hat.



Warnung

Zeigt, wie viele Abweichungen des Levels 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 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:

- Die Leistungsfähigkeit der Kommunikation zwischen den beiden Geräten ist nicht beeinträchtigt.
- Die Leistungsfähigkeit der Kommunikation zwischen den beiden Geräten kann beeinträchtigt sein.
- Die Kommunikation zwischen den beiden Geräten ist beeinträchtigt.

Nachricht

Zeigt eine Zusammenfassung der erkannten Abweichungen.

8.2.3 ARP

[Diagnose > System > ARP]

Dieser Dialog zeigt die MAC- und IP-Adressen der Nachbargeräte, die mit dem Management des Geräts verbunden sind.

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 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:

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

Dynamischer Eintrag. Das Gerät löscht den dynamischen Eintrag nach Überschreiten der , falls das Gerät während dieser Zeit keine Daten von diesem Gerät empfängt.

Aktiv

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

8.24 Selbsttest

[Diagnose > System > Selbsttest]

Dieser Dialog ermöglicht Ihnen, Folgendes zu tun:

- 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 sperrn Ihnen dauerhaft den Zugang zum Gerät, wenn das Gerät beim Neustart kein lesbares Konfigurationsprofil findet.

- Kontrollkästchen ist .
- Kontrollkästchen ist .

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.

SysMon1 ist verfügbar

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

Mögliche Werte:

(Voreinstellung)

Das Gerät ermöglicht Ihnen, während des Systemstarts in den System-Monitor zu wechseln.

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:

(Voreinstellung)

Das Gerät lädt die Werkseinstellungen.

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. Nach dem Systemstart verwendet das Gerät die Werkseinstellungen.

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:

Das Gerät erkennt Fehler in ausgeführten Anwendungen, zum Beispiel wenn eine Task abbricht oder nicht verfügbar ist.

Das Gerät erkennt Fehler in den verfügbaren Ressourcen, zum Beispiel bei knapp werdendem Speicher.

Das Gerät erkennt Software-Fehler, zum Beispiel Fehler beim Konsistenz-Check.

Das Gerät erkennt Hardware-Fehler, zum Beispiel im Chipsatz.

Aktion

Legt das Verhalten des Geräts fest, wenn das nebenstehende Ereignis eintritt.

Mögliche Werte:

Das Gerät protokolliert den Fehler in der Log-Datei. Siehe Dialog

.

Das Gerät sendet einen SNMP-Trap.

Voraussetzung ist, dass im Dialog

eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.

die Funktion

(Voreinstellung)

Das Gerät löst einen Neustart aus.

8.3 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:

Das Senden von Ereignissen ist eingeschaltet.
Das Gerät sendet die in der Tabelle festgelegten Ereignisse zum jeweils festgelegten Syslog-Server.

(Voreinstellung)

Das Senden von Ereignissen ist ausgeschaltet.

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 hinzufügen, schließt das Gerät die erste Lücke.

Mögliche Werte:

IP-Adresse

Legt die IP-Adresse des Syslog-Servers fest.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung:)

DNS-Name im Format oder

Voraussetzung ist, dass Sie zusätzlich im Dialog die Funktion einschalten.

Wenn Sie eine verschlüsselte Verbindung mithilfe eines digitalen Zertifikats herstellen, vergewissern Sie sich, dass die - oder -Angabe im digitalen Zertifikat, das Sie auf das Gerät übertragen haben, mit dem hier festgelegten Wert übereinstimmt. Andernfalls kann das Gerät die Identität des Servers nicht verifizieren.

Ziel UDP-Port

Legt den UDP-Port fest, auf dem der Syslog-Server die Log-Einträge erwartet.

Mögliche Werte:

(Voreinstellung:)

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:

(Voreinstellung)

Typ

Legt den Typ des Log-Eintrags fest, den das Gerät übermittelt.

Mögliche Werte:

(Voreinstellung)

Aktiv

Aktiviert bzw. deaktiviert die Übermittlung der Ereignisse zum Syslog-Server.

Mögliche Werte:

Das Gerät sendet Ereignisse zum Syslog-Server.

(Voreinstellung)

Die Übermittlung der Ereignisse zum Syslog-Server ist deaktiviert.

8.4 Ports

[Diagnose > Ports]

Das Menü enthält die folgenden Dialoge:

8.5 LLDP

[Diagnose > LLDP]

Das Gerät ermöglicht Ihnen, Informationen über benachbarte Geräte zu sammeln. Dazu nutzt das Gerät das Link Layer Discovery Protocol (LLDP). Diese Informationen ermöglichen einer Netzmanagement-Station, die Struktur des Netzes darzustellen.

Dieses Menü ermöglicht Ihnen, die Topologie-Erkennung einzurichten und die empfangenen Informationen in Tabellenform anzuzeigen.

Das Menü enthält die folgenden Dialoge:

[LLDP Konfiguration](#)

[LLDP Topologie-Erkennung](#)

8.5.1 LLDP Konfiguration

[Diagnose > LLDP > Konfiguration]

Dieser Dialog ermöglicht Ihnen, die Topologie-Erkennung für jeden Port einzurichten.

Funktion

Funktion

Schaltet die Funktion ein/aus.

Mögliche Werte:

(Voreinstellung)

Die Funktion ist eingeschaltet.

Die Topologie-Erkennung mit LLDP ist auf dem Gerät aktiv.

Die Funktion ist ausgeschaltet.

Konfiguration

Sende-Intervall [s]

Legt das Intervall in Sekunden fest, in dem das Gerät LLDP-Datenpakete sendet.

Mögliche Werte:

(Voreinstellung:)

Sende-Intervall Multiplikator

Legt den Faktor zur Bestimmung des Time-to-live-Werts für die LLDP-Datenpakete fest.

Mögliche Werte:

(Voreinstellung:)

Der im LLDP-Header kodierte Time-to-live-Wert ergibt sich aus der Multiplikation dieses Wertes mit dem Wert im Feld .

Reinitialisierungs-Verzögerung [s]

Zeigt die Verzögerung in Sekunden für die Re-Initialisierung eines Ports.

Wenn in Spalte der Wert festgelegt ist, dann versucht das Gerät nach Ablauf der hier festgelegten Zeit den Port erneut zu initialisieren.

Sende-Verzögerung [s]

Zeigt die Verzögerung in Sekunden für das Senden von aufeinanderfolgenden LLDP-Datenpaketen, nachdem sich die Einstellungen des Geräts geändert haben.

Benachrichtigungs-Intervall [s]

Legt das Intervall in Sekunden für das Senden von LLDP-Benachrichtigungen fest.

Mögliche Werte:

(Voreinstellung:)

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:

Der Port sendet LLDP-Datenpakete, speichert jedoch keine Informationen über benachbarte Geräte.

Der Port empfängt LLDP-Datenpakete, sendet jedoch keine Informationen an benachbarte Geräte.

(Voreinstellung)

Der Port sendet LLDP-Datenpakete und speichert Informationen über benachbarte Geräte.

Der Port sendet keine LLDP-Datenpakete und speichert keine Informationen über benachbarte Geräte.

Benachrichtigung

Aktiviert/deaktiviert LLDP-Benachrichtigungen auf dem Port.

Mögliche Werte:

LLDP-Benachrichtigungen auf dem Port sind aktiv.

(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:

(Voreinstellung)

Das Senden des TLV ist aktiv.

Das Gerät sendet den TLV mit der Port-Beschreibung.

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:

(Voreinstellung)

Das Senden des TLV ist aktiv.

Das Gerät sendet den TLV mit dem Gerätenamen.

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:

(Voreinstellung)

Das Senden des TLV ist aktiv.

Das Gerät sendet den TLV mit der Systembeschreibung.

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:

(Voreinstellung)

Das Senden des TLV ist aktiv.

Das Gerät sendet den TLV mit den System-Ressourcen.

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:

(Voreinstellung:)

Modus FDB

Legt fest, welche Funktion das Gerät verwendet, um benachbarte Geräte auf diesem Port zu erfassen.

Mögliche Werte:

Das Gerät verwendet ausschließlich LLDP-Datenpakete, um benachbarte Geräte auf diesem Port zu erfassen.

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 MAC-Adresstabelle (Forwarding Database) für diesen Port vorhanden ist.

Das Gerät verwendet LLDP-Datenpakete und gelernte MAC-Adressen, um benachbarte Geräte auf diesem Port zu erfassen.

(Voreinstellung)

Wenn das Gerät auf diesem Port LLDP-Datenpakete empfängt, dann arbeitet das Gerät wie mit der Einstellung . Andernfalls arbeitet das Gerät wie mit der Einstellung .

8.5.2 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.

Dieser Dialog 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 MAC-Adresstabelle (Forwarding Database) 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:

Das angeschlossene Gerät unterstützt kein LLDP.

Das Gerät verwendet Informationen aus seiner MAC-Adresstabelle (Forwarding Database).

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.

8.6 Bericht

[Diagnose > Bericht]

Das Menü enthält die folgenden Dialoge:

- [Bericht Global](#)
- [Persistentes Ereignisprotokoll](#)
- [System-Log](#)
- [Audit-Trail](#)

8.6.1 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

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 472](#).

Funktion

Schaltet die Funktion ein/aus.

Mögliche Werte:

Die Funktion ist eingeschaltet.
Das Gerät protokolliert die Ereignisse auf der Konsole.
(Voreinstellung)
Die Funktion 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 472](#).

Das Gerät gibt die Meldungen auf der seriellen Schnittstelle aus.

Mögliche Werte:

(Voreinstellung)

SNMP-Logging

Wenn Sie die Protokollierung von SNMP-Anfragen einschalten, sendet das Gerät diese als Ereignisse mit dem voreingestellten Schweregrad an die Liste der Syslog-Server. Der voreingestellte Mindest-Schweregrad für einen Syslog-Server-Eintrag ist .

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 generiert, auf oder . 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 separaten Syslog-Server-Eintrag hinzuzufügen. Setzen Sie ausschließlich den Schweregrad der SNMP-Anfragen auf oder höher. Das Gerät sendet dann SNMP-Anfragen als Ereignisse mit dem Schweregrad oder schwerer an die Syslog-Server.

Setzen Sie ausschließlich den Mindest-Schweregrad bei einem oder mehreren Syslog-Server-Einträgen auf oder niedriger. Das Gerät sendet dann u. U. sehr viele Ereignisse an die Syslog-Server.

Logge SNMP Get-Requests

Schaltet die Protokollierung für den Empfang von SNMP Get Requests ein/aus.

Mögliche Werte:

Die Protokollierung ist eingeschaltet.
Das Gerät protokolliert jeden empfangenen SNMP Get Request als Ereignis im Syslog. Den Schweregrad für dieses Ereignis wählen Sie in der Dropdown-Liste aus.
(Voreinstellung)
Die Protokollierung ist ausgeschaltet.

Logge SNMP Set-Requests

Schaltet die Protokollierung für den Empfang von SNMP Set Requests ein/aus.

Mögliche Werte:

Die Protokollierung ist eingeschaltet.
Das Gerät protokolliert jeden empfangenen SNMP Set Request als Ereignis im Syslog. Den Schweregrad für dieses Ereignis wählen Sie in der Dropdown-Liste aus.
(Voreinstellung)
Die Protokollierung ist ausgeschaltet.

Schweregrad Get-Request

Legt den Schweregrad des Ereignisses fest, welches das Gerät bei empfangenen SNMP Get Requests protokolliert. Weitere Informationen finden Sie unter „[Bedeutung der Ereignis-Schweregrade](#)“ auf Seite 472.

Mögliche Werte:

(Voreinstellung)

Schweregrad Set-Request

Legt den Schweregrad des Ereignisses fest, welches das Gerät bei empfangenen SNMP Set Requests protokolliert. Weitere Informationen finden Sie unter „[Bedeutung der Ereignis-Schweregrade](#)“ auf Seite 472.

Mögliche Werte:

(Voreinstellung)

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 472.

Mögliche Werte:

(Voreinstellung)

CLI-Logging

Funktion

Schaltet die Funktion ein/aus.

Mögliche Werte:

- Die Funktion ist eingeschaltet.
 Das Gerät protokolliert jeden Befehl, den es über das Command Line Interface empfängt.
 (Voreinstellung)
- Die Funktion ist ausgeschaltet.

Support-Informationen: Dateien im ZIP-Archiv

Dateiname	Format	Bemerkungen
š±Ÿ¥° °@š¥" ¨°@"	HTML	Enthält die im Audit Trail-Protokoll chronologisch aufgezeichneten Systemereignisse und gespeicherten Änderungen durch die Benutzer.
›<l -©ß 9kj	XML	Enthält die im „ausgewählten“ Konfigurationsprofil gespeicherten Einstellungen des Geräts.
h•-°µj-›<l -©ß 9kj	XML	Enthält die Voreinstellungen des Geräts.
›m©-	TEXT	Enthält die Ausgaben des Kommandos @<n µµll©lß##### #####
µµll©lß›<l -©ß 9kj	XML	Enthält die gegenwärtigen Betriebseinstellungen des Geräts.
µ-›<m-©l -< @-kj	HTML	Enthält geräteinterne Service-Information.
ñ -•k©l -< @-kj	HTML	Enthält Information über die gegenwärtigen Einstellungen und Betriebsparameter.
ñ -•kj<ß @-kj	HTML	Enthält die in der Log-Datei protokollierten Ereignisse. Siehe Dialog

Bedeutung der Ereignis-Schweregrade

Schweregrad	Bedeutung
	Gerät nicht betriebsbereit
	Sofortiger Bedienereingriff erforderlich
	Kritischer Zustand
	Fehlerhafter Zustand
	Warnung

Schweregrad	Bedeutung
	Signifikanter, normaler Zustand
	Informelle Nachricht
	Debug-Nachricht

8.6.2 Persistentes Ereignisprotokoll

[Diagnose > Bericht > Persistentes Ereignisprotokoll]

Das Gerät ermöglicht Ihnen, die Log-Einträge in einer Datei im externen Speicher dauerhaft 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 generierten 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 im Dialog . Wir empfehlen, die Verbindung des externen Speichers mit der Funktion zu überwachen, siehe Parameter im Dialog .

Funktion

Funktion

Schaltet die Funktion ein/aus.

Aktivieren Sie die Funktion ausschließlich dann, wenn der externe Speicher im Gerät verfügbar ist.

Mögliche Werte:

(Voreinstellung)

Die Funktion ist eingeschaltet.

Das Gerät speichert die Log-Einträge in einer Datei im externen Speicher.

Die Funktion 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 generierten Datei.

Mögliche Werte:

(Voreinstellung:)

Der Wert 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:

(Voreinstellung:)

Der Wert 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:

(Voreinstellung)

Ziel der Log-Datei

Legt den Typ des externen Speichers für die Protokollierung fest.

Mögliche Werte:

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:

Das Gerät legt diese Nummer automatisch fest.

Dateiname

Zeigt den Dateinamen der Log-Datei im externen Speicher.

Mögliche Werte:

Datei-Größe [Byte]

Zeigt die Größe der Log-Datei im externen Speicher in Bytes.

8.6.3 System-Log


[Diagnose > Bericht > System-Log]

Dieser Dialog zeigt die System-Log-Datei. Das Gerät protokolliert geräteinterne Ereignisse in der System-Log-Datei. Das Gerät behält die protokollierten Ereignisse auch nach einem Neustart bei.

Um die Datei System-Log zu durchsuchen, verwenden Sie die Suchfunktion Ihres Webbrowsers.

Der Dialog ermöglicht Ihnen, eine Kopie der System-Log-Datei auf Ihren Computer herunterzuladen. Das Gerät stellt die herunterzuladende Datei im HTML- oder CSV-Format bereit.

Schaltflächen

 Log-Datei speichern

Lädt eine Kopie der System-Log-Datei gemäß den Einstellungen des Webbrowsers auf Ihren Computer herunter.

Mögliche Werte:

Das Gerät stellt die Datei im CSV-Format bereit.

Das Gerät stellt die Datei im HTML-Format bereit.

 Log-Datei leeren

Leert die System-Log-Datei im Gerät.

8.6.4 Audit-Trail

[Diagnose > Bericht > Audit-Trail]

Dieser Dialog zeigt den 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 `audit` oder `audit-read` zugewiesen ist.

Unter anderem protokolliert das Gerät die folgenden Benutzeraktionen:

- Anmeldung eines Benutzers beim Management des Geräts 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 zu vieler aufeinanderfolgender erfolgloser Anmeldeversuche.
- Sperrung des Zugriffs auf des Management des Geräts aufgrund erfolgloser Anmeldeversuche
- Im Command Line Interface ausgeführte Befehle, außer `show`-Befehle
- Änderungen an Konfigurationsvariablen
- Änderungen der Systemzeit
- Datei-Transfer-Operationen einschließlich Firmware-Updates
- Konfigurationsänderungen 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 `System-Monitor`, Kontrollkästchen `System-Monitor`.

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.

9 Erweitert

Das Menü enthält die folgenden Dialoge:

- [DNS](#)
- [Tracking](#)
- [Command Line Interface](#)

9.1 DNS

[Erweitert > DNS]

Das Menü enthält die folgenden Dialoge:

- [DNS-Client](#)
- [DNS-Cache](#)

9.1.1 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 [DNS-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](#)

9.1.1.1 DNS-Client Global

[Erweitert > DNS > Client > Global]

In diesem Dialog schalten Sie die Funktion ein.

Funktion

Funktion

Schaltet die Funktion ein/aus.

Mögliche Werte:

Die Funktion ist eingeschaltet.

Das Gerät sendet Anfragen zur Auflösung von Hostnamen in IP-Adressen an einen DNS-Server.

(Voreinstellung)

Die Funktion ist ausgeschaltet.

9.1.1.2 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.

9.1.1.3 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, bis zu 4 IP-Adressen festzulegen.

Konfiguration

Quelle

Legt die Quelle fest, aus der das Gerät die IP-Adresse anzufragender DNS-Server bezieht.

Mögliche Werte:

Das Gerät verwendet die in der Tabelle festgelegten IP-Adressen.


Tabelle


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

Schaltflächen



Hinzufügen

Öffnet das Fenster , um eine Tabellenzeile hinzuzufügen.

Im Feld  legen Sie die Index-Nummer fest.

Mögliche Werte:

–

Das Gerät ermöglicht Ihnen, bis zu 4 externe DNS-Server festzulegen.

Im Feld  legen Sie die IP-Adresse des DNS-Servers fest.

Mögliche Werte:

– Gültige IPv4-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

Aktiv

Aktiviert/deaktiviert die Tabellenzeile.

Voraussetzungen:

- Im Dialog ist die Funktion DNS client eingeschaltet.
- Im Rahmen ist in der Dropdown-Liste der Eintrag ausgewählt.

Mögliche Werte:

(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 , Feld fest.

Die Tabellenzeile ist inaktiv.

Das Gerät sendet keine Anfragen an diesen DNS-Server.

9.1.2 DNS-Cache

[Erweitert > DNS > Cache]

Die -Funktion ermöglicht dem Gerät, auf Anfragen zur Auflösung von Hostnamen in IP-Adressen zu antworten.

Das Menü enthält die folgenden Dialoge:

[DNS-Cache Global](#)

9.1.21 DNS-Cache Global

[Erweitert > DNS > Cache > Global]

In diesem Dialog schalten Sie die Funktion ein. Ist die Funktion eingeschaltet, arbeitet das Gerät als Caching-DNS-Server.

Fragt ein nachgeordnetes Gerät die IP-Adresse eines unbekanntes Hostnames an, liefert der Caching-DNS-Server die IP-Adresse zurück, wenn er einen passenden Eintrag in seinem Cache findet.

Der Cache bietet Speicherplatz für bis zu 128 Hostnamen mit zugehöriger IP-Adresse.

Funktion

Schaltflächen



Cache leeren

Löscht jeden Eintrag aus dem DNS-Cache.

Funktion

Schaltet die Funktion ein/aus.

Mögliche Werte:

(Voreinstellung)

Die Funktion ist eingeschaltet.

Die Funktion ist ausgeschaltet.

9.2 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.

Sobald Sie die Tracking-Objekte im Dialog eingerichtet haben,
können Sie Applikationen mit den Tracking-Objekten verknüpfen:

- Statische Routen verknüpfen Sie mit einem Tracking-Objekt im Dialog ,
Spalte
- Virtuelle Router verknüpfen Sie mit einem Tracking-Objekt im Dialog

[VRRP > Tracking](#). Klicken Sie die Schaltfläche , um das Fenster zu öffnen und in
der Dropdown-Liste das Tracking-Objekt auszuwählen.

Das Menü enthält die folgenden Dialoge:

- [Tracking Konfiguration](#)
- [Tracking Applikationen](#)

9.21 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 , um eine Tabellenzeile hinzuzufügen.

- In der Dropdown-Liste  wählen Sie den Typ des Tracking-Objekts.
Mögliche Werte:

Das Gerät überwacht den Link-Status seiner physischen Ports, Link-Aggregation-, LRE- oder VLAN-Router-Interfaces.

Das Gerät überwacht die Route zu einem entfernten Router oder Endgerät durch periodisches Senden von ICMP Echo Request-Paketen.

Das Gerät überwacht logisch miteinander verknüpfte Tracking-Objekte und ermöglicht somit komplexe Überwachungsaufgaben.

- Im Feld  legen Sie die Identifikationsnummer des Tracking-Objektes fest.
Mögliche Werte:



Löschen

Entfernt die ausgewählte Tabellenzeile.

Typ

Legt den Typ des Tracking-Objekts fest.

Mögliche Werte:

Das Gerät überwacht den Link-Status seiner physischen Ports, Link-Aggregation-, LRE- oder VLAN-Router-Interfaces.

Das Gerät überwacht die Route zu einem entfernten Router oder Endgerät durch periodisches Senden von ICMP Echo Request-Paketen.

Das Gerät überwacht logisch miteinander verknüpfte Tracking-Objekte und ermöglicht somit komplexe Überwachungsaufgaben.

Track-ID

Legt die Identifikationsnummer des Tracking-Objektes fest.

Mögliche Werte:

Dieser Bereich steht jedem Typ (, und) zur Verfügung.

Track-Name

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

Aktiv

Aktiviert/deaktiviert die Überwachung des Tracking-Objekts.

Mögliche Werte:

Die Überwachung ist aktiv. Das Gerät überwacht das Tracking-Objekt.
(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:

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.

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.

Die Überwachung des Tracking-Objekts ist inaktiv. Sie aktivieren die Überwachung in Spalte

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:

Das Gerät sendet einen SNMP-Trap, wenn jemand das Tracking-Objekt in Spalte aktiviert oder deaktiviert.

(Voreinstellung)

Das Gerät sendet keinen SNMP-Trap.

Port

Legt für Tracking-Objekte des Typs das zu überwachende Interface fest.

Mögliche Werte:

Nummer des physischen Ports, des Link-Aggregation-, LRE- oder VLAN-Router-Interfaces.

Kein Tracking-Objekt des Typs .

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 den Wert .

Mögliche Werte:

Kein Tracking-Objekt des Typs .

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 den Wert .

Mögliche Werte:

Kein Tracking-Objekt des Typs .

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.

Ping-Port

Legt für Tracking-Objekte des Typs `ICMP Echo Request` das Router-Interface fest, über welches das Gerät die ICMP Echo Request-Pakete sendet.

Mögliche Werte:

Nummer des Router-Interfaces.

Kein Router-Interface zugewiesen.

Kein Tracking-Objekt des Typs `ICMP Echo Request`.

IP-Adresse

Legt die IP-Adresse des zu überwachenden entfernten Routers oder Endgeräts fest.

Mögliche Werte:

Gültige IPv4-Adresse

Kein Tracking-Objekt des Typs `ICMP Echo Request`.

Ping-Intervall [ms]

Legt das Intervall in Millisekunden fest, in welchem das Gerät periodisch ICMP Echo Request-Pakete sendet.

Mögliche Werte:

(Voreinstellung: `1000`)

Wenn Sie einen Wert `< 1000` festlegen, können Sie maximal 16 Tracking-Objekte des Typs `ICMP Echo Request` einrichten.

Kein Tracking-Objekt des Typs `ICMP Echo Request`.

Ausbleibende Ping-Antworten

Legt fest, nach wie vielen ausbleibenden Antworten das Gerät das Überwachungsergebnis als negativ erkennt. Wenn das Gerät nacheinander sooft wie hier festgelegt keine Antwort auf gesendete ICMP Echo Request-Pakete empfängt, dann zeigt Spalte `Ergebnis` den Wert `Negative`.

Mögliche Werte:

(Voreinstellung: `3`)

Kein Tracking-Objekt des Typs `ICMP Echo Request`.

Logischer Operand A

Legt für Tracking-Objekte des Typs fest.

den ersten Operanden der logischen Verknüpfung

Mögliche Werte:

Eingerichtete Tracking-Objekte

Kein Tracking-Objekt des Typs

.

Logischer Operand B

Legt für Tracking-Objekte des Typs fest.

den zweiten Operanden der logischen Verknüpfung

Mögliche Werte:

Eingerichtete Tracking-Objekte

Kein Tracking-Objekt des Typs

.

Operator

Verknüpft die in den Feldern Objekte.

und

festgelegten Tracking-

Mögliche Werte:

Logische UND-Verknüpfung

Logische ODER-Verknüpfung

Kein Tracking-Objekt des Typs




.




9.2.2 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  , Spalte .
- Virtuelle Router verknüpfen Sie mit einem Tracking-Objekt im Dialog .

[VRRP > Tracking](#). Klicken Sie die Schaltfläche , um das Fenster  zu öffnen und in der Dropdown-Liste  das Tracking-Objekt auszuwählen.

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 
- Statische Routen 
- Virtuelle Router einer VRRP-Instanz 

Track-Name

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

9.3 Command Line Interface

[Erweitert > CLI]

Dieser Dialog ermöglicht Ihnen, mit dem Command Line Interface auf das Gerät zuzugreifen.

Voraussetzungen:

- Im Dialog [SSH-Server konfigurieren](#), Registerkarte [SSH-Server](#) 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 Management des Geräts her.

A Stichwortverzeichnis

0-9	
1to1-NAT	407
802.1D/p-Mapping	301
A	
Aging-Time	291
Alarm	449
ARP	314, 319
ARP-Tabelle	49, 319, 456
Audit-Trail	478
Ausgangs-Lastbegrenzer	293
Authentifizierungs-Liste	66
B	
Benutzerverwaltung	61
Betriebszeit	21
C	
CLI	96
Command Line Interface	96
Community-Namen	98
D	
Deep Packet Inspection (DPI)	152
Default Gateway	367, 387, 430
Default Route	332, 333, 339, 430
Destination-NAT	411
DHCP L3 Relay	371
Digitales Zertifikat	20, 34, 72, 89, 260, 448
DNP3 Enforcer	162
DNS	479
DNS-Cache	483
DNS-Client	480
Domain Name System	479
DoS	244
Double-NAT	430
DPI	152
DPI DNP3 Enforcer	162
DPI Modbus Enforcer	153
DPI OPC Enforcer	159
E	
Eingangs-Lastbegrenzer	293
Einstellungen	30
ENVM	29, 34, 37, 41, 442, 447, 475
Ereignis-Schweregrad	472
Externer Speicher	22, 29, 34, 37, 41, 475
F	
FDB (MAC-Adresstabelle)	49, 296
Fingerprint	84, 88
Firewall-Lernmodus	118
Firewall-Tabelle	50
Flash-Speicher	29
Flusskontrolle	291

G	
Geräte-Software	27
Geräte-Software Backup	27
Gerätestatus	19, 440
H	
Häufig gestellte Fragen	499
HiDiscovery	24, 447, 478
Host-Key	85
HTML	453, 477
HTTP	85
HTTPS	86
HTTP-Server	446
I	
ICMP-Redirect	309, 314
Industrial HiVision	9, 81
Ingress Filtering	307
IP-Zugriffsbeschränkung	91
K	
Konfigurations-Check	454
Konfigurationsprofil	16, 30
L	
L3 Relay (DHCP)	371
Laden/Speichern	30
Lastbegrenzer	293
LDAP	66
LLDP	462
Logdatei	49, 50, 477
Login-Banner	97, 99
Loopback-Interface	375
M	
MAC-Adress-Filter	296
MAC-Adresstabelle (Forwarding Database)	49, 296
Management-VLAN	24
Management-Zugriff	24, 91
Modbus Enforcer	153
Multicast-Routing	378
N	
NAT	407, 430
NAT (Network Address Translation)	403
Network Address Translation (NAT)	403
Network Time Protocol	55
Netzteil	21, 442
Neustart	49
NTP	55
NVM	16, 29, 34
O	
OPC Enforcer	159
OSPF	326

P	
Passwort	62, 445
Passwort-Länge	62, 445
Persistente Log-Datei	50
Persistentes Ereignisprotokoll	474
Port-Konfiguration	300
Port-Priorität	300
Port-Statistiken	49
Port-VLAN	306
Port-Weiterleitung	411
Pre-Login-Banner	99
Proxy-ARP	314
Q	
Queues	299
R	
RADIUS	66, 102
RAM	34
RAM-Test	457
Relay (DHCP)	371
Router-Interface	304, 312
Routing-Tabelle	366
S	
Schulungsangebote	499
Schwellenwerte Netzlast	293
Schweregrad	472
Secure Shell (SSH)	82
Selbsttest	457
Serielle Schnittstelle	446
Sicherheitsstatus	20, 444
SNMP-Server	80, 446
SNMP-Traps	47, 330, 388, 441, 444, 449, 488
SNMPv1/v2	98
Software-Backup	27
Software-Update	27
Sommerzeit	52
Source Routing	309
SSH-Server	82
Standard-Gateway	367, 387, 430
Standard-Route	332, 333, 339, 430
Stratum	55, 57
Support-Informationen	469
Support-Informationen (ZIP-Archiv)	472
Syslog	459
Systeminformationen	453
System-Log	477
System-Monitor	457
Systemzeit	51

T	
Technische Fragen	499
Temperatur	21, 441
Time To Live (TTL)	311
Topologie-Erkennung	467
Tracking	401, 484
Traps	47, 330, 388, 441, 444, 449, 488
Trap-Ziel	450
Trust Modus	300
TTL (Time To Live)	311
V	
Verschlüsselung	30
Virtual Local Area Network	302
Virtual Router Redundancy Protocol	387
VLAN	24, 302
VLAN Konfiguration	304
VLAN-Ports	306
VRRP	387
VRRP-Statistik	399
VRRP-Tracking	401
W	
Warteschlange (Queue)	299
Watchdog	30, 39
Webserver	85, 86
Z	
Zähler-Reset	49
Zertifikat	20, 34, 72, 88, 89, 260, 448
ZIP-Archiv mit Support-Informationen	472
Zugriffsbeschränkung	91

B Technische 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.belden.com.

Technische Unterstützung erhalten 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 IRD-NT
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Deutschland



HIRSCHMANN

A **BELDEN** BRAND







- [Barcode]

[Barcode]
[Barcode]
[Barcode]
[Barcode]

[Barcode]
[Barcode]
[Barcode]
[Barcode]



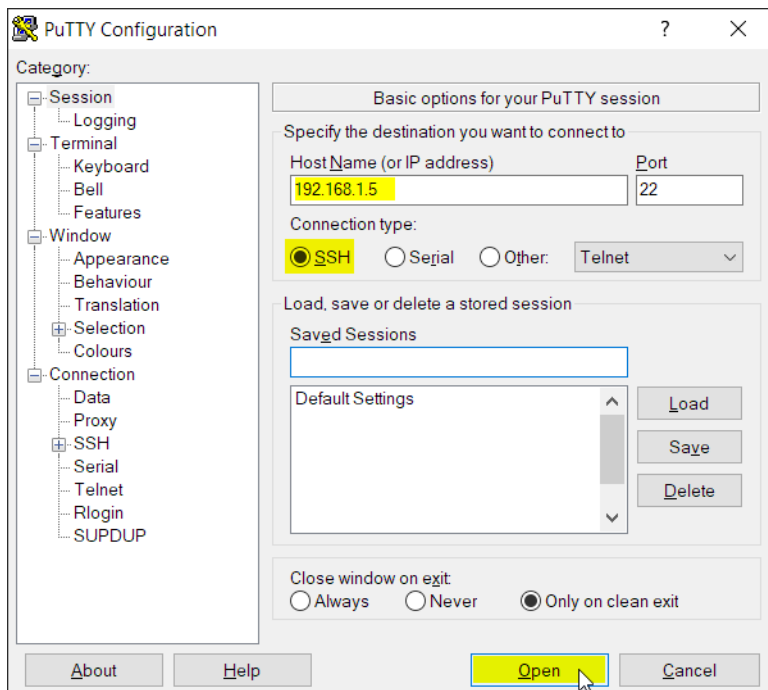
<p>-----</p> <p>.....</p> <p>.....</p> <p>.....</p>




□□□□□□□□□□□□□□□□□□□□□□□□







PuTTY Security Alert

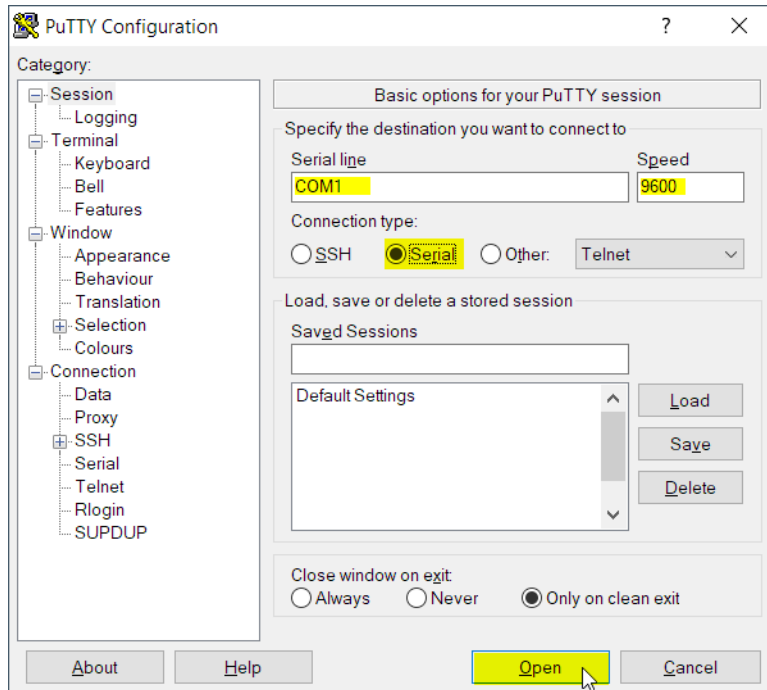
 The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.

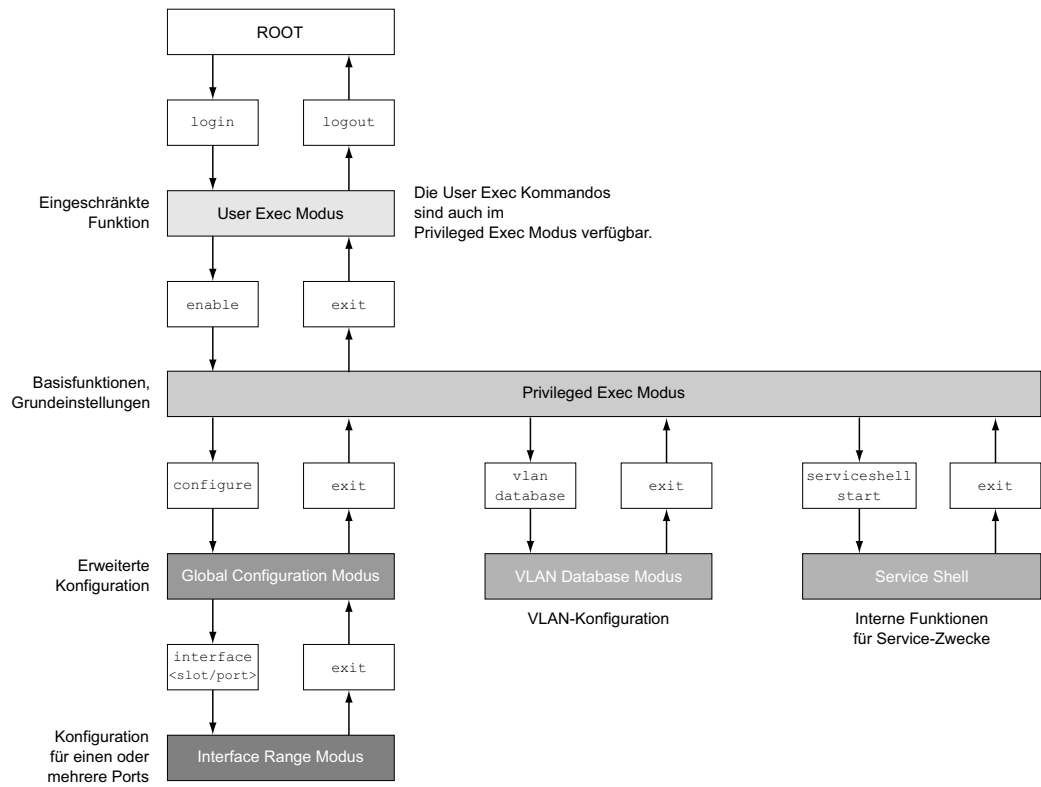
The server's rsa2 key fingerprint is:
ssh-rsa 2048 SHA256:1GepSdba8L0wRvKRLvDJ9iVeNEpFOu4sDCWXdyGK14Y

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.



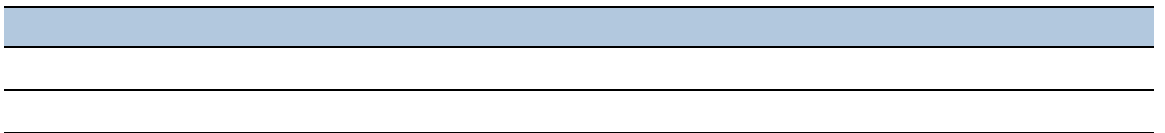






□□□□□□□□□□

-



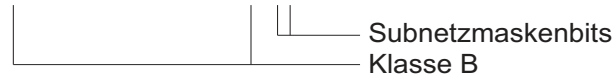




0	Net ID - 7 bits	Host ID - 24 bits	Klasse A
1 0	Net ID - 14 bits	Host ID - 16 bits	Klasse B
1 1 0	Net ID - 21 bits	Host ID - 8 bits	Klasse C
1 1 1 0	Multicast Group ID - 28 bits		Klasse D
1 1 1 1	reserved for future use - 28 bits		Klasse E

Dezimale Darstellung
255.255.192.0

Binäre Darstellung
11111111.11111111.11000000.00000000



000

000
0-00000000000000000000

000

000
000
000

000
000
000

00000000 000
00
00000000000000000000

000
000
000
000

00000000000000000000

IP-Adresse, dezimal	Netzmaske, dezimal	IP-Adresse, binär
192.168.112.1	255.255.255.128	11000000 10101000 01110000 00000001
192.168.112.127		11000000 10101000 01110000 01111111

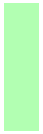
|----- 25 Maskenbits -----|

CIDR-Schreibweise: 192.168.112.0/25
 |
 |----- Maskenbits

000
000



⌘ +





XXXXXXXXXXXXXXXX





□□□□□□□□□□□□□□□□□□□□

-

□□□□□□□□□□

-

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

-

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

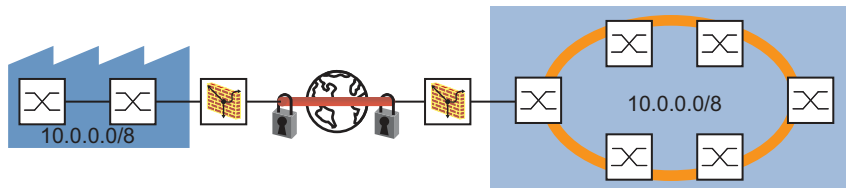
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□

-

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

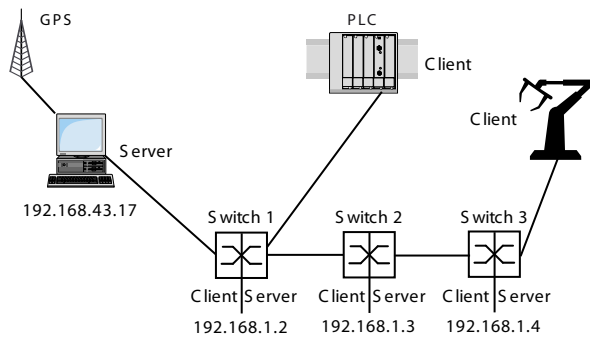
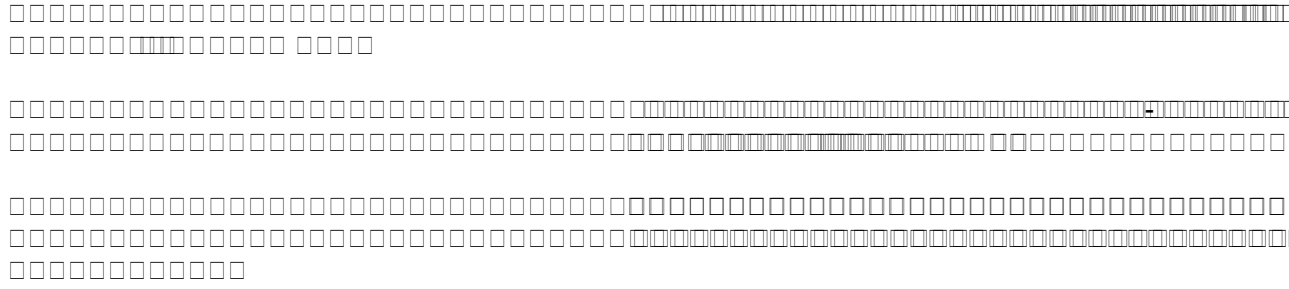














☑
B+



-□□□□□□□□□□□□□□□□



⊞+



-□□□□□□□□□□□□□□□□



□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□







[Grid pattern]

[Grid pattern]

[Grid pattern]

[Grid pattern]

.....
.....

.....
.....



=



.....
.....
.....

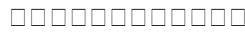
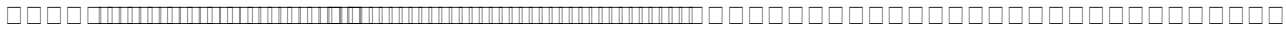
.....
.....





-





-



□□□□□□□□□□

□□□□□□□□□□



-

-



□□□□□□□□

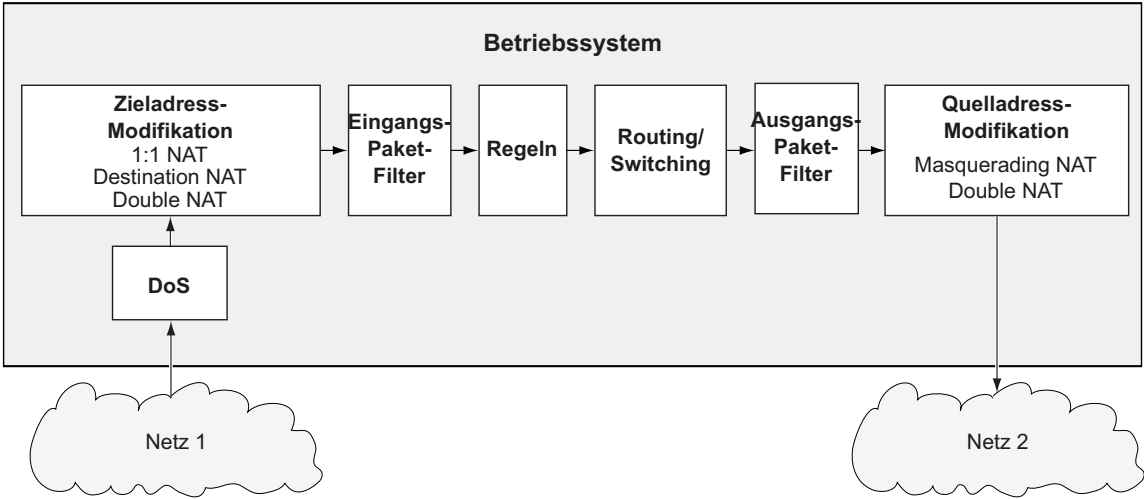
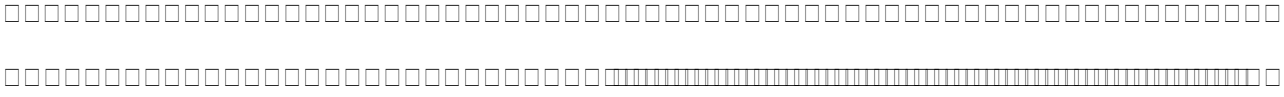
-

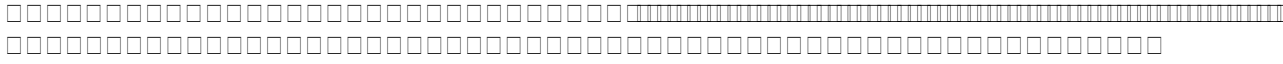


□□□□□□□□

-

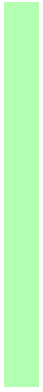






B+







Four horizontal lines for text entry

Grid of small squares with a dash on the right side

Grid of small squares with a dash on the right side



Grid of small squares with a dash on the right side



Grid of small squares

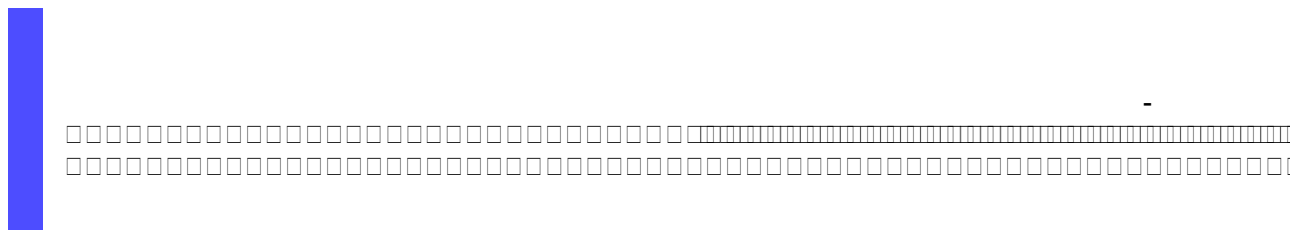
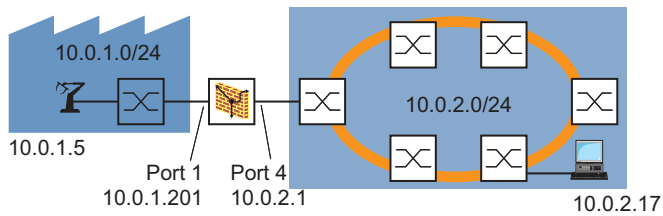
Grid of small squares

Grid of small squares

Grid of small squares with a checkmark and a dash on the right side

Grid of small squares with an upward arrow icon

Grid of small squares with a dash on the right side





⌘+





⌘





□□□□□□□□□□

-

□□□□□□□□□□

-



田+

✓



□□□□□□□□□□

-

□□□□□□□□□□

-



+





□□□□□□□□□□

-

□□□□□□□□□□

-



田+

✓



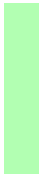
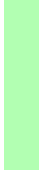
□□□□□□□□□□

-

□□□□□□□□□□

-



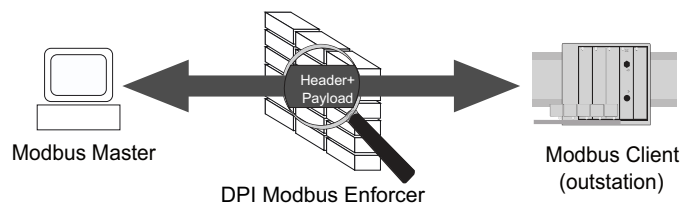




□□□□□□□□□□□□□□□□

-





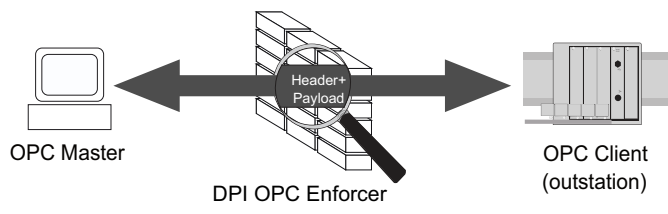
-



⌘
+









⌘ +



□□□□□□□□□□

-







B+





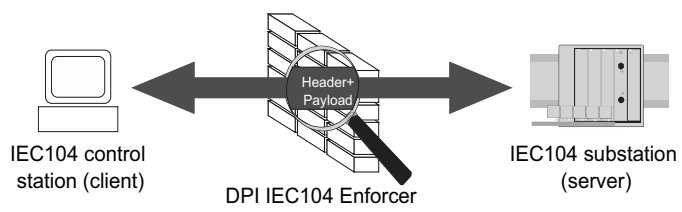
田+

✓

□□□□□□□□□□

-

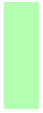


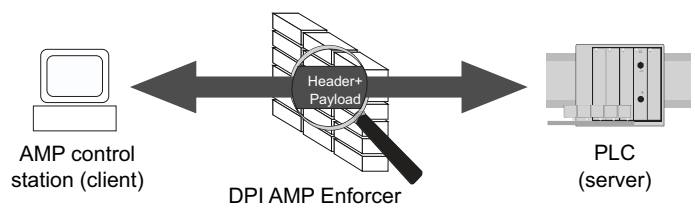
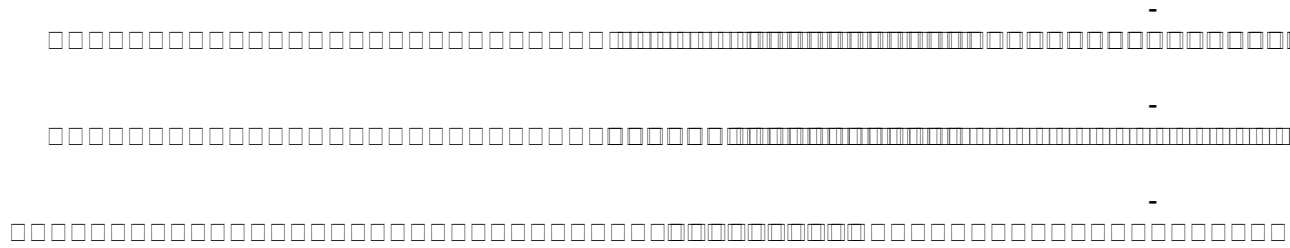




⌘
+



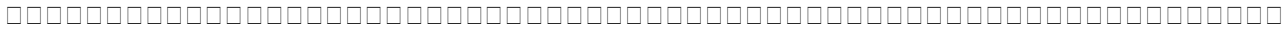




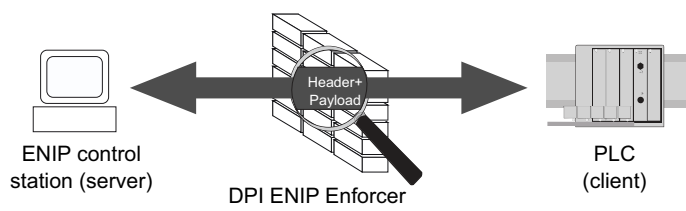
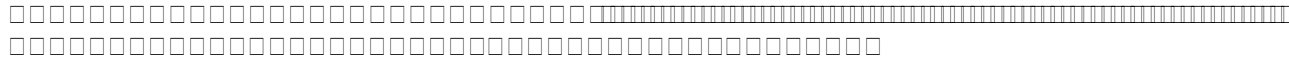


⌘+











⌘+

⌘+

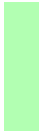




□□□□□□□□□□

-







-□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□

-□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□

-□□□□□□□□□□□□□□□□□□□□□□□□□□□□



□□□□□□□□□□□□



-

-
[Placeholder text consisting of two lines of empty boxes]

[Placeholder text consisting of three lines of empty boxes]

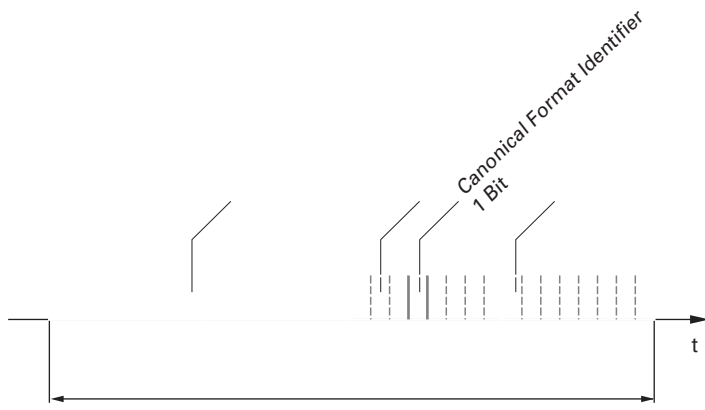
[Placeholder text consisting of a single line of empty boxes]

[Placeholder text consisting of a single line of empty boxes]

[Placeholder text consisting of two lines of empty boxes]

[Placeholder text consisting of two lines of empty boxes]





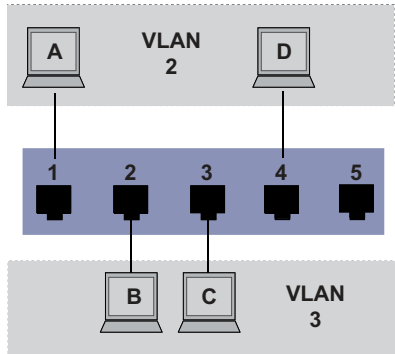


- [REDACTED]

- [REDACTED]

- [REDACTED]







⌘
+





-□□□□□

-□□□□□

-□□□□□

-□□□□□

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]







-□□□□□□

-□□□□□□

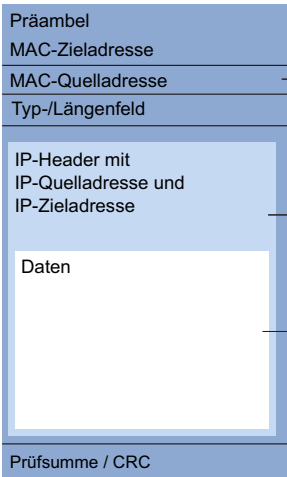
-□□□□□□

-□□□□□□

-□□□□□□



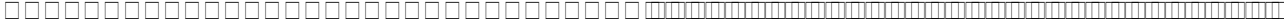
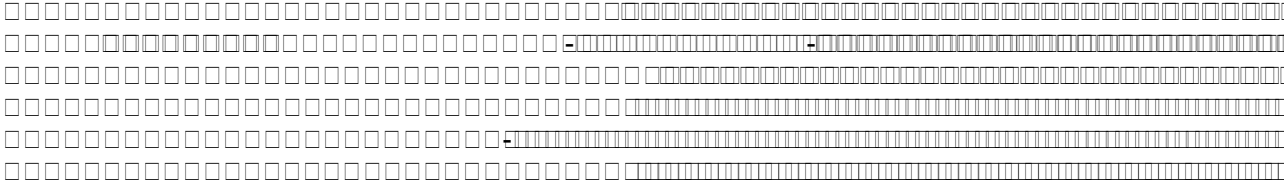
-[]



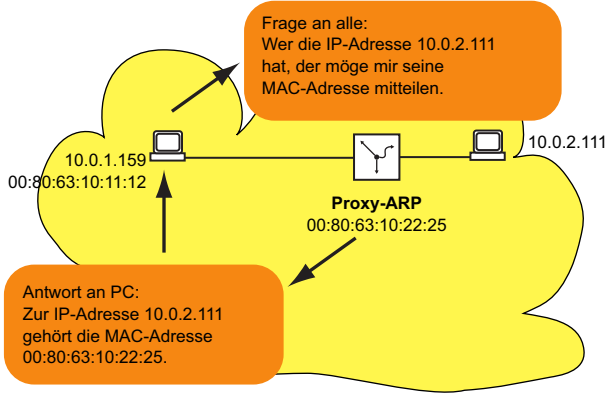
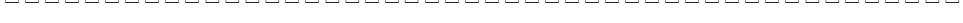
Schicht 2

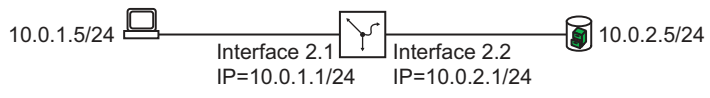
Schicht 3

Schicht 4 und höher



-[]





```

-□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□
-
□□□□□□□□□□□□□□□□□□
-□□□□□□□□□□□□□□□□□□
-
□□□□□□□□□□□□□□□□□□
```




□□□□□□□□□□□□□□

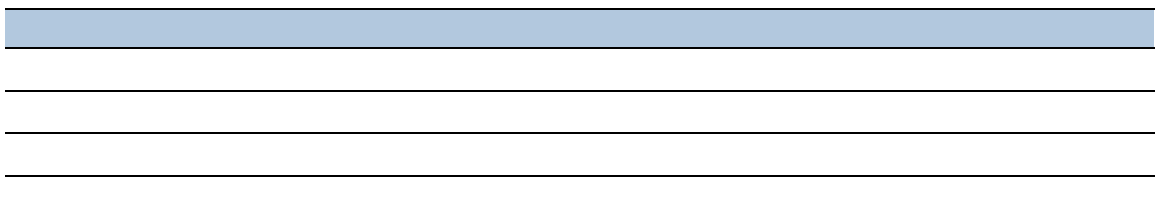
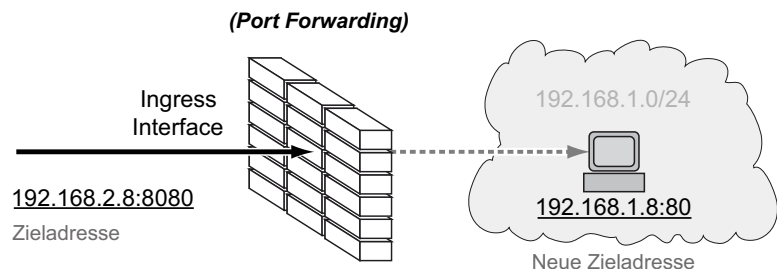
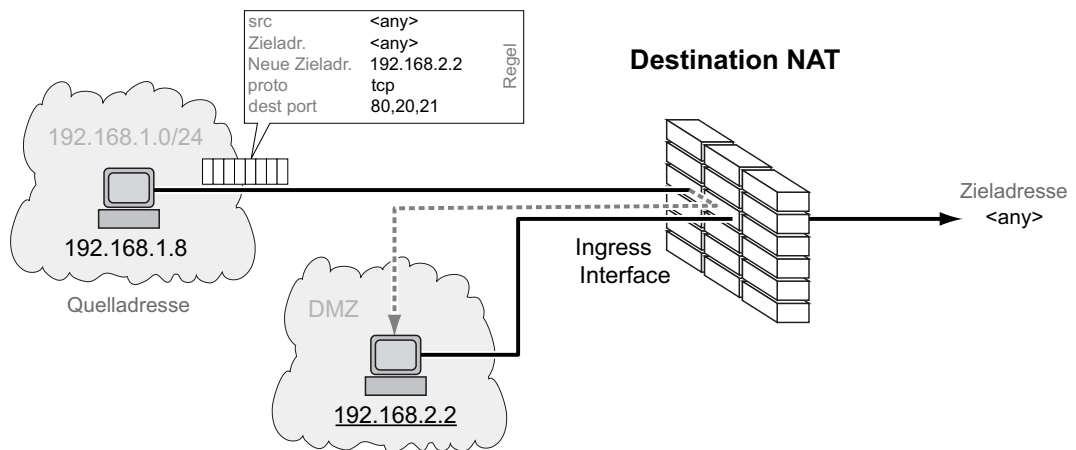
-



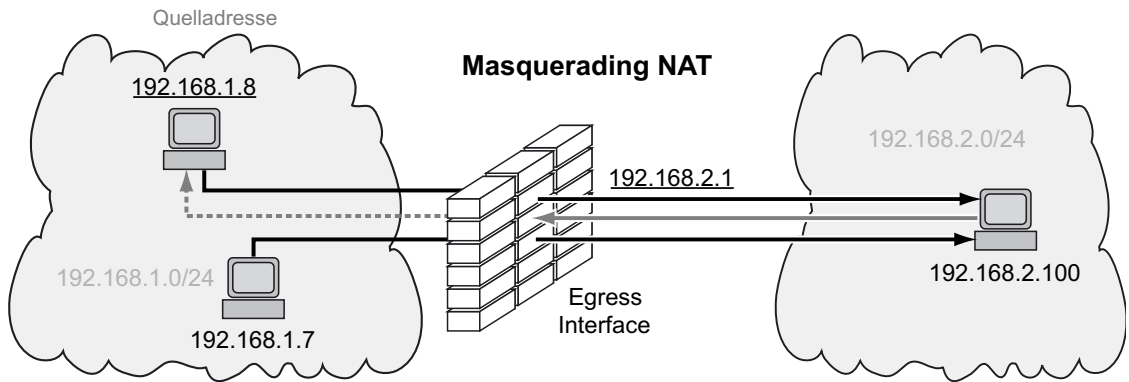
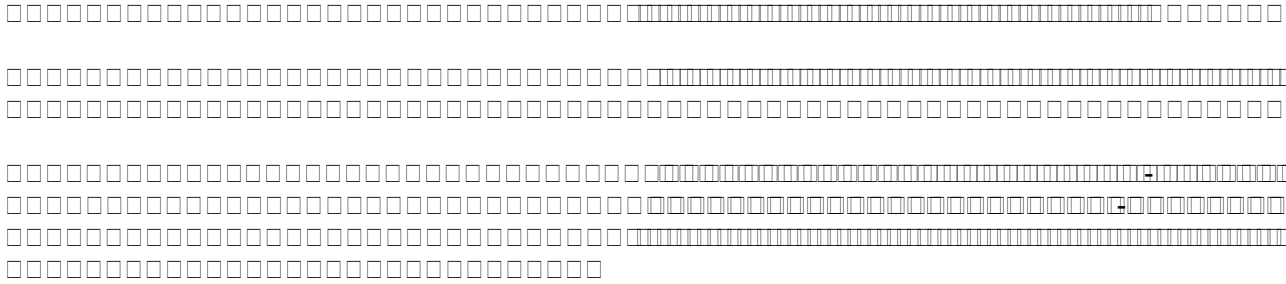
□□□□□□□□□□□□□□□□□□□□□□□□□□

-



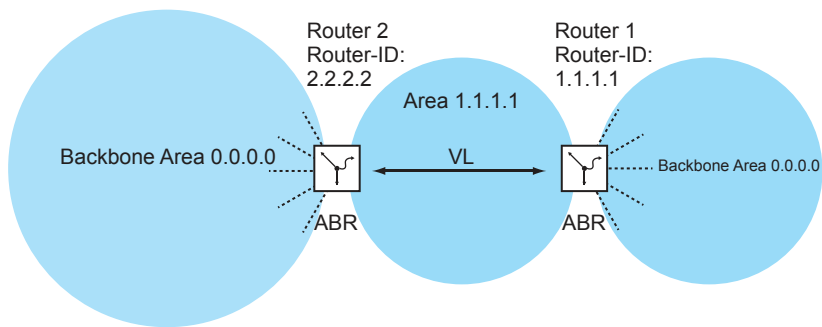
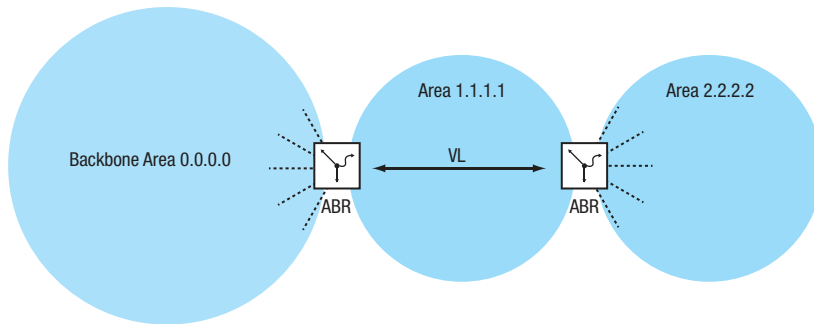


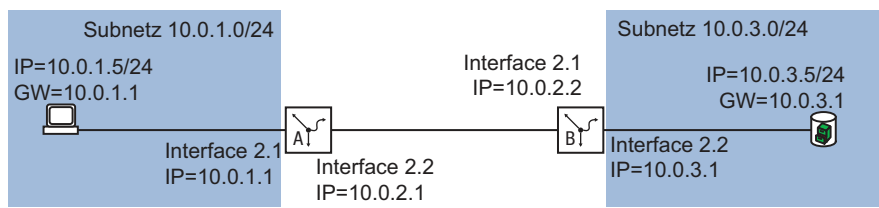
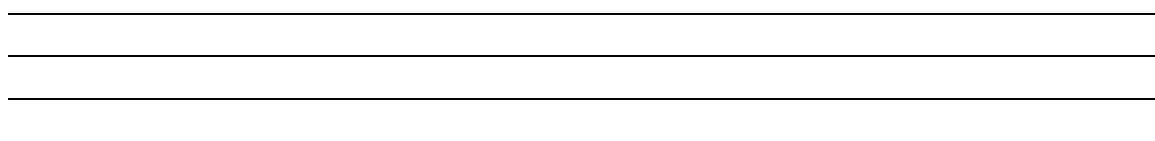
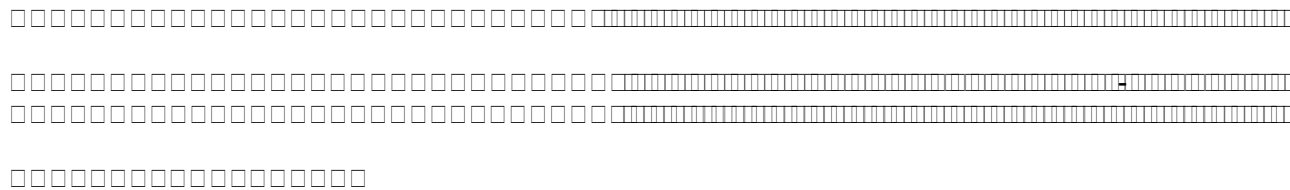


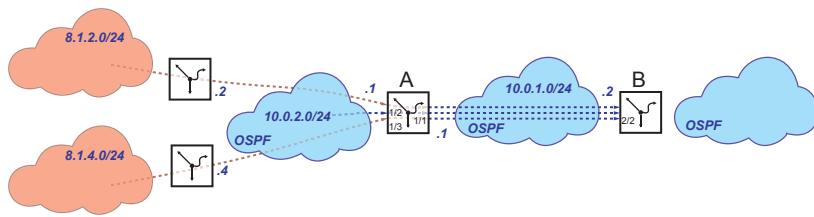


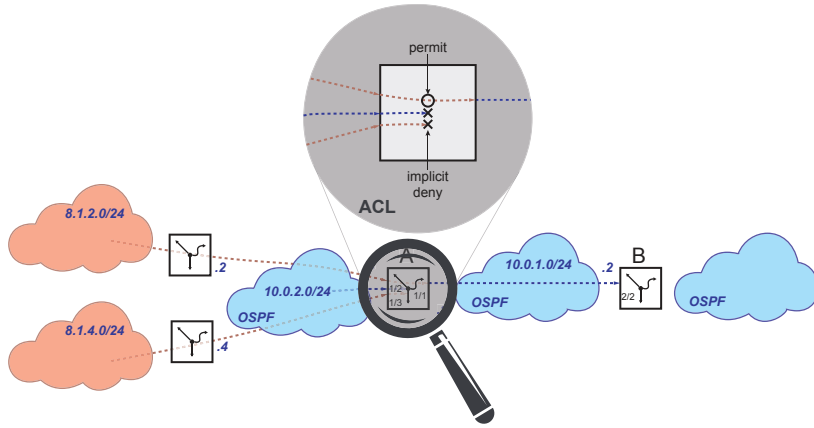


□□□□□□□□□□□□□□□□





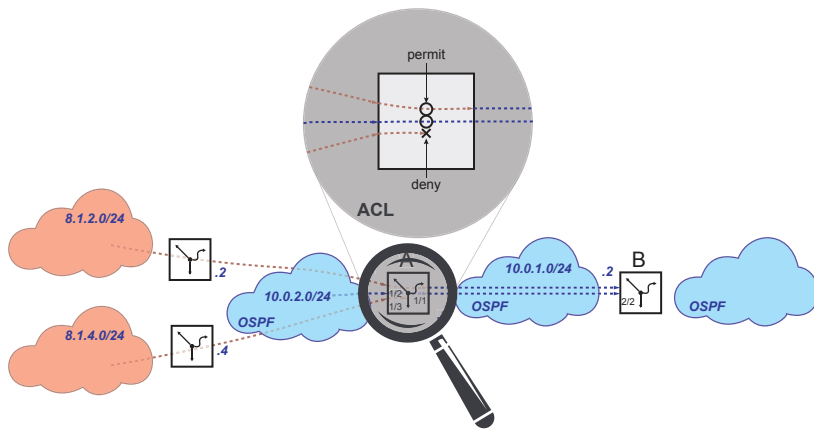


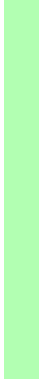




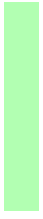
-
□□□
□□□
□□□
□□□













⌘ +





☰
+

✓

✓



□□□□□□□□



□□□□□□□□□□□□□□



-

-





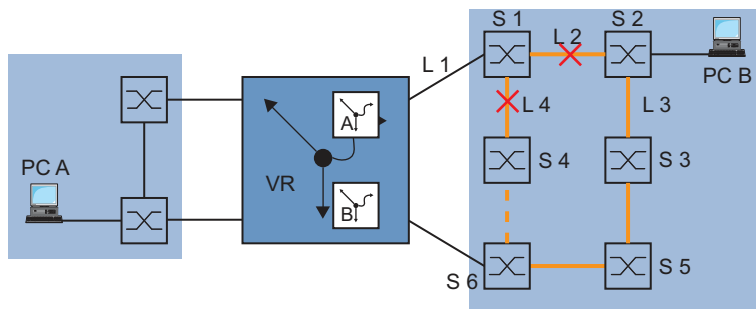


B+



□□□□□□□□□□

-



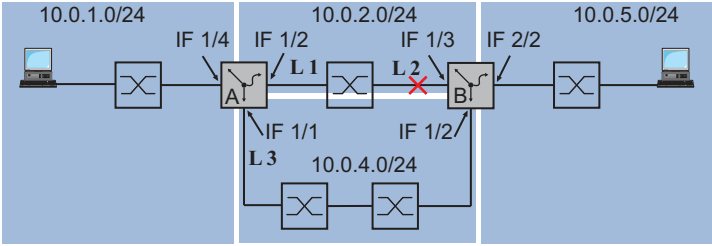
⊞
+



□□□□□□□□□□

-





⊞
+

⊞
+

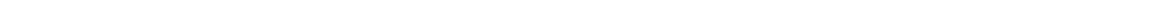




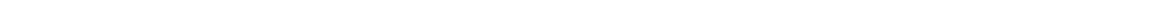
□□□□□□□□□□□□□□□□□□□□□□□□□□



□□□□□□□□



□□□



□□



XX
XXXXXXXXXXXXXXXXXXXX



BB
+







□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□



□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□



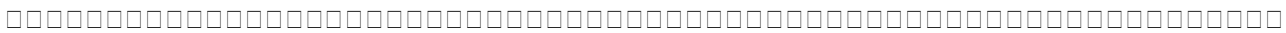
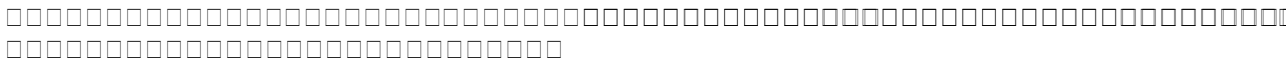
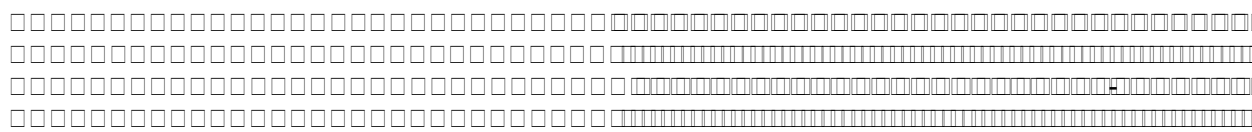
□□

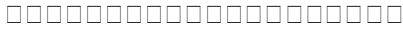
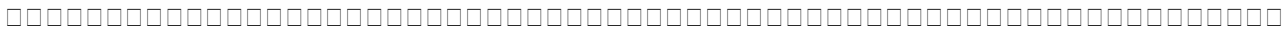














□□□□ □□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□□

-
-

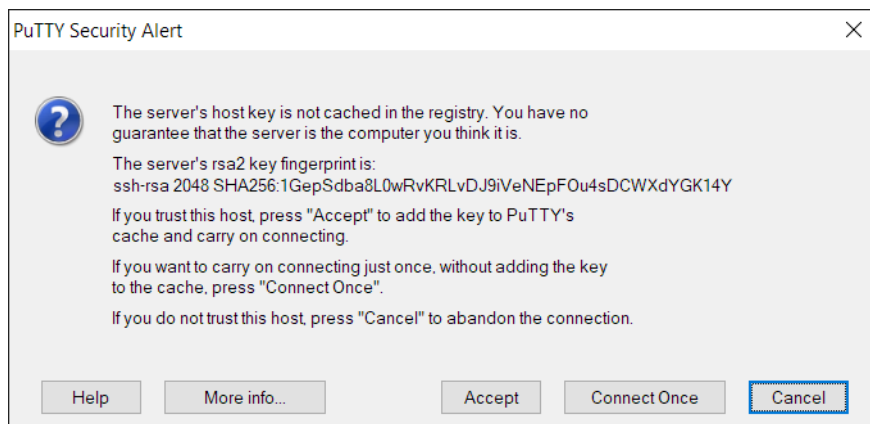
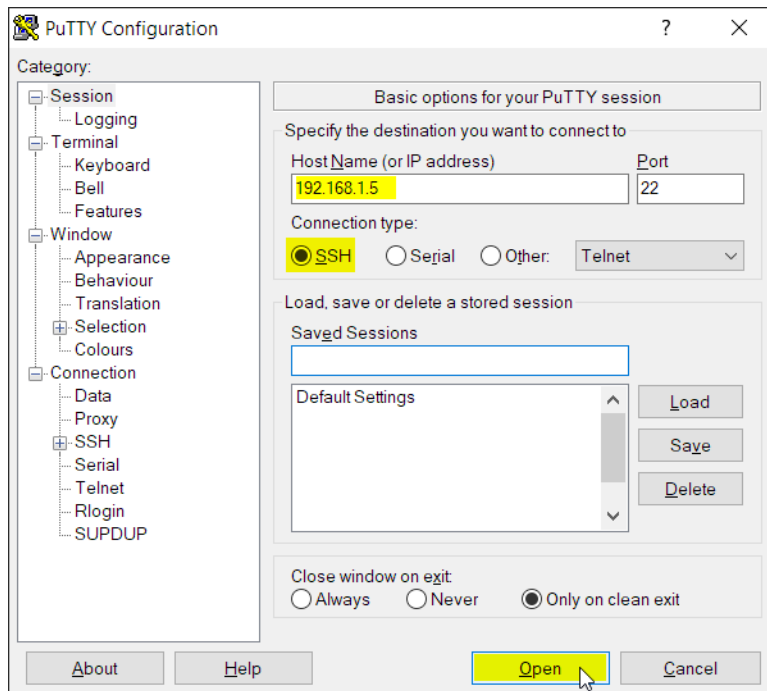
□□□□ □□□□□□□□□□□□ □□□□□□□□□□□□ □□□□□□□□□□□□
□□□□□□□□□□□□

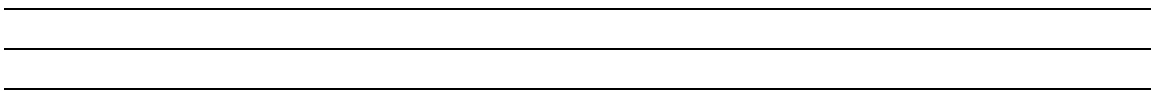


□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

-□□□□□□□□□□□□□□□□

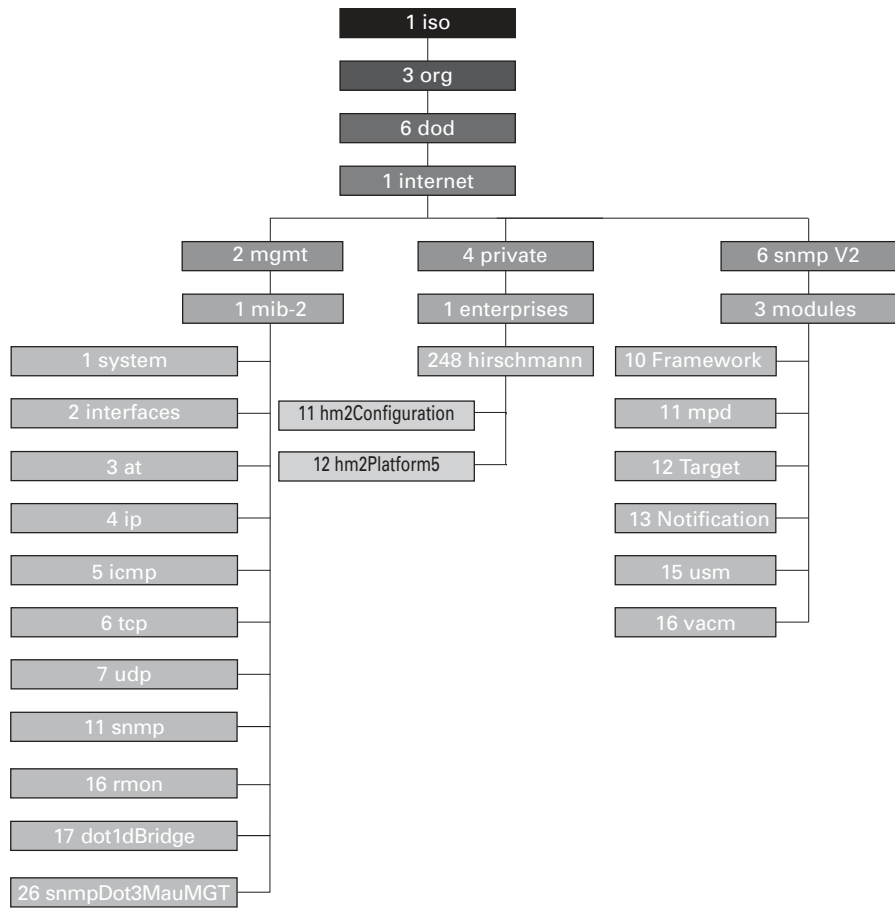








□□□□□□□□□□□□□□□□



- □□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□





Handwriting practice sheet with 25 horizontal lines.









A series of 20 horizontal black lines, evenly spaced, providing a template for text entry.



HIRSCHMANN

A **BELDEN** BRAND