



**HIRSCHMANN**

A **BELDEN** BRAND

Hirschmann Automation and Control GmbH

# **Eagle40-4F HiSecOS Rel. 07000**

**Referenz-Handbuch**

Grafische Benutzeroberfläche

**Anwender-Handbuch**

Konfiguration



**HIRSCHMANN**

A **BELDEN** BRAND

# Referenz-Handbuch

Grafische Benutzeroberfläche

Industrial Firewall

**EAGLE404F**

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.

© 2025 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](https://doc.hirschmann.com)

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

# Inhalt

	<b>Sicherheitshinweise</b> .....	7
	<b>Über dieses Handbuch</b> .....	9
	<b>Legende</b> .....	10
	<b>Hinweise zur grafischen Benutzeroberfläche</b> .....	11
	Banner .....	11
	Menübereich .....	13
	Dialogbereich .....	15
<b>1</b>	<b>Grundeinstellungen</b> .....	19
1.1	System .....	19
1.2	Netzwerk .....	23
1.2.1	Global .....	24
1.2.2	IPv4 .....	26
1.3	Software .....	27
1.4	Laden/Speichern .....	31
1.5	Externer Speicher .....	43
1.6	Port .....	46
1.7	Restart .....	52
<b>2</b>	<b>Zeit</b> .....	55
2.1	Grundeinstellungen .....	55
2.2	NTP .....	59
2.2.1	Global .....	60
2.2.2	Server .....	63
<b>3</b>	<b>Gerätesicherheit</b> .....	67
3.1	Benutzerverwaltung .....	67
3.2	Authentifizierungs-Liste .....	72
3.3	LDAP .....	74
3.3.1	LDAP Konfiguration .....	75
3.3.2	LDAP Rollen-Zuweisung .....	81
3.4	Management-Zugriff .....	83
3.4.1	Server .....	84
3.4.2	IP-Zugriffsbeschränkung .....	96
3.4.3	Web .....	100
3.4.4	Command Line Interface .....	101
3.4.5	SNMPv1/v2 Community .....	103
3.5	Pre-Login-Banner .....	104
<b>4</b>	<b>Netzsicherheit</b> .....	105
4.1	Netzsicherheit Übersicht .....	105
4.2	RADIUS .....	106
4.2.1	RADIUS Global .....	107
4.2.2	RADIUS Authentication-Server .....	108
4.2.3	RADIUS Authentication Statistiken .....	110

4.3	Asset	111
4.4	Protokoll	115
4.5	Paketfilter	118
4.5.1	Routed-Firewall-Modus	118
4.5.1.1	Global	120
4.5.1.2	Firewall-Lern-Modus	122
4.5.1.3	Paketfilter Regel	129
4.5.1.4	Paketfilter Zuweisung	135
4.5.1.5	Paketfilter Übersicht	138
4.5.2	Transparent-Firewall-Modus	139
4.5.2.1	Paketfilter Global	141
4.5.2.2	Paketfilter Regel	143
4.5.2.3	Paketfilter Zuweisung	151
4.5.2.4	Paketfilter Übersicht	154
4.6	Deep Packet Inspection	156
4.6.1	Deep Packet Inspection - Modbus Enforcer	157
4.6.2	Deep Packet Inspection - OPC Enforcer	163
4.6.3	Deep Packet Inspection - DNP3 Enforcer	166
4.6.3.1	DNP3-Profil	167
4.6.3.2	DNP3-Objekt	172
4.6.4	Deep Packet Inspection - IEC104 Enforcer	194
4.6.5	Deep Packet Inspection - AMP-Enforcer	201
4.6.5.1	AMP Global	203
4.6.5.2	AMP-Profil	206
4.6.6	Deep Packet Inspection - ENIP Enforcer	214
4.6.6.1	ENIP-Profil	215
4.6.6.2	ENIP-Objekt	220
4.7	DoS	249
4.7.1	DoS Global	250
<b>5</b>	<b>Virtual Private Network</b>	<b>255</b>
5.1	VPN Übersicht	255
5.2	VPN Zertifikate	264
5.3	VPN Verbindungen	268
<b>6</b>	<b>Switching</b>	<b>295</b>
6.1	Switching Global	295
6.2	Lastbegrenzer	297
6.3	Filter für MAC-Adressen	300
6.4	QoS/Priority	301
6.4.1	QoS/Priority Global	303
6.4.2	QoS/Priorität Port-Konfiguration	304
6.4.3	802.1D/p Zuweisung	305
6.5	VLAN	306
6.5.1	VLAN Global	307
6.5.2	VLAN Konfiguration	308
6.5.3	VLAN Port	310

<b>7</b>	<b>Routing</b> . . . . .	<b>313</b>
7.1	Routing Global . . . . .	313
7.2	Routing-Interfaces . . . . .	315
7.2.1	Routing-Interfaces Konfiguration . . . . .	316
7.2.2	Routing-Interfaces Sekundäre Interface-Adressen . . . . .	323
7.3	ARP . . . . .	324
7.3.1	ARP Global . . . . .	325
7.3.2	ARP Aktuell . . . . .	327
7.3.3	ARP Statisch . . . . .	329
7.4	Open Shortest Path First . . . . .	331
7.4.1	OSPF Global . . . . .	333
7.4.2	OSPF Areas . . . . .	342
7.4.3	OSPF Stub Areas . . . . .	344
7.4.4	OSPF Not So Stubby Areas . . . . .	346
7.4.5	OSPF Interfaces . . . . .	349
7.4.6	OSPF Virtual Links . . . . .	355
7.4.7	OSPF Ranges . . . . .	358
7.4.8	OSPF Diagnose . . . . .	360
7.5	Routing-Tabelle . . . . .	372
7.6	L3-Relay . . . . .	377
7.7	Loopback-Interface . . . . .	381
7.8	L3-Redundanz . . . . .	383
7.8.1	High Availability . . . . .	383
7.8.1.1	High Availability Konfiguration . . . . .	384
7.8.1.2	High Availability Status . . . . .	389
7.8.2	VRRP . . . . .	391
7.8.2.1	VRRP Konfiguration . . . . .	392
7.8.2.2	VRRP Statistiken . . . . .	403
7.8.2.3	VRRP Tracking . . . . .	405
7.9	NAT . . . . .	406
7.9.1	NAT Global . . . . .	408
7.9.2	1:1-NAT . . . . .	412
7.9.2.1	1:1-NAT Regel . . . . .	413
7.9.3	Destination-NAT . . . . .	416
7.9.3.1	Destination-NAT Regel . . . . .	418
7.9.3.2	Destination-NAT Zuweisung . . . . .	423
7.9.3.3	Destination-NAT Übersicht . . . . .	425
7.9.4	Masquerading-NAT . . . . .	427
7.9.4.1	Masquerading-NAT Regel . . . . .	429
7.9.4.2	Masquerading-NAT Zuweisung . . . . .	432
7.9.4.3	Masquerading-NAT Übersicht . . . . .	434
7.9.5	Double-NAT . . . . .	435
7.9.5.1	Double-NAT Regel . . . . .	437
7.9.5.2	Double-NAT Zuweisung . . . . .	440
7.9.5.3	Double-NAT Übersicht . . . . .	442

<b>8</b>	<b>Diagnose</b> .....	445
8.1	Statuskonfiguration .....	445
8.1.1	Gerätestatus .....	446
8.1.2	Sicherheitsstatus .....	450
8.1.3	Alarmer (Traps) .....	455
8.1.3.1	Trap Ziele .....	456
8.2	System .....	458
8.2.1	Systeminformationen .....	459
8.2.2	Konfigurations-Check .....	460
8.2.3	ARP .....	462
8.2.4	Selbsttest .....	463
8.3	Syslog .....	465
8.4	LLDP .....	467
8.4.1	LLDP Konfiguration .....	468
8.4.2	LLDP Topologie-Erkennung .....	472
8.5	Bericht .....	473
8.5.1	Bericht Global .....	474
8.5.2	Persistentes Ereignisprotokoll .....	479
8.5.3	System-Log .....	482
8.5.4	Audit-Trail .....	483
<b>9</b>	<b>Erweitert</b> .....	485
9.1	DNS .....	485
9.1.1	DNS-Client .....	485
9.1.1.1	DNS-Client Global .....	486
9.1.1.2	DNS-Client Aktuell .....	487
9.1.1.3	DNS-Client Statisch .....	488
9.1.2	DNS-Cache .....	489
9.1.2.1	DNS-Cache Global .....	490
9.2	Tracking .....	490
9.2.1	Tracking Konfiguration .....	492
9.2.2	Tracking Applikationen .....	498
9.3	Command Line Interface .....	499
<b>A</b>	<b>Stichwortverzeichnis</b> .....	501
<b>B</b>	<b>Technische Unterstützung</b> .....	505
<b>C</b>	<b>Leserkritik</b> .....	506

## 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:

•	Listenpunkt
–	Listenpunkt – zweite Ebene
	Wert eines Parameters
	Handlungsschritt
<a href="#">Verweis</a>	Querverweis mit Verknüpfung
<b>Anmerkung:</b>	Eine Anmerkung betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit.
<code>Courier</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

Zeigt das Hersteller-Logo.

Name des Dialogs

Zeigt den Namen des gegenwärtig im Dialogbereich angezeigten Dialogs.



Wenn Sie die Schaltfläche klicken, überträgt das aktive Gerät seine Konfigurationsprofile auf das Standby-Gerät. Die Schaltfläche funktioniert ausschließlich auf dem aktiven Firewall-Gerät.

Ein roter Punkt neben dem Symbol bedeutet, dass die Einstellungen zwischen dem aktiven und dem Standby-Gerät nicht synchronisiert sind.

Verwenden Sie diese Schaltfläche für die Funktion [High Availability](#). Siehe Dialog [Routing > L3-Redundanz > High Availability](#).



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



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



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



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

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


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



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

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

## Menübereich

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

Der Menübereich ist wie folgt unterteilt:

- [Symbolleiste](#)
- [Menübaum](#)

### Symbolleiste

Die Symbolleiste zeigt die folgenden Informationen:


#### Geräte-Software

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



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



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



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



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

## **Menübaum**

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



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



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

## Dialogbereich

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

Nachfolgend finden Sie nützliche Informationen zur Bedienung der Dialoge.

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

### Bedienelemente

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

Die Bedienelemente haben folgende visuelle Eigenschaften:

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

### Änderungsmarkierung

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

### Standard-Schaltflächen

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



Wendet die von Ihnen geänderten Einstellungen im Gerät an.

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



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

### Einstellungen speichern

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

Klicken Sie die Schaltfläche  .

---

#### Anmerkung:


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


---

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

Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.


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

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

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

### Anzeige aktualisieren

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

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

### Arbeiten mit Tabellen

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

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

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

### **Tabellenzeilen 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.

### **Tabellenzeilen 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.

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.

Sobald Sie mehrere Tabellenzeilen gewählt haben, können Sie eine Aktion auf jede dieser Tabellenzeilen gleichzeitig anwenden, zum Beispiel:

- die Werte in einer Tabellenspalte eingeben oder ändern
- mehrere Tabellenzeilen entfernen

# 1 Grundeinstellungen

Das Menü enthält die folgenden Dialoge:

- [System](#)
- [Netzwerk](#)
- [Software](#)
- [Laden/Speichern](#)
- [Externer Speicher](#)
- [Port](#)
- [Restart](#)

## 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 [Diagnose > Statuskonfiguration > Gerätestatus](#). Das Gerät löst einen Alarm aus, wenn ein überwachter Parameter vom gewünschten Zustand abweicht.

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

---

#### **Anmerkung:**

Das Gerät löst einen Alarm aus, wenn Sie an ein Gerät, das die Überwachung von 2 redundanten Netzteilen unterstützt, lediglich ein Netzteil anschließen. Um diesen Alarm zu vermeiden, deaktivieren Sie im Dialog [Diagnose > Statuskonfiguration > Gerätestatus](#) das Überwachen fehlender Netzteile.

---

## Sicherheits-Status



### Sicherheits-Status

Zeigt den Sicherheits-Status und die gegenwärtig vorliegenden 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 [Diagnose > Statuskonfiguration > Sicherheitsstatus](#). Das Gerät löst einen Alarm aus, wenn ein überwachter Parameter vom gewünschten Zustand abweicht.

Ein Tooltip zeigt die Ursache der gegenwärtig vorliegenden 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 [Status](#) im Dialog [Diagnose > 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:

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

- [Syslog](#)

#### 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:

[vorhanden](#)

[defekt](#)

[nicht vorhanden](#)

[unbekannt](#)

#### Betriebszeit

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

Mögliche Werte:

Zeit im Format [Tag\(e\)](#), [... h](#) [... m](#) [... s](#)

#### Temperatur [°C]

Zeigt die gegenwärtige Temperatur im Gerät in °C.

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

#### Obere Temp.-Grenze [°C]

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

Mögliche Werte:

-99 . 99 (ganze Zahl)

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

#### Untere Temp.-Grenze [°C]

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

Mögliche Werte:

-99 . 99 (ganze Zahl)

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

### LED-Status

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

#### Status



Gegenwärtig ist kein Alarm vorhanden. Der Gerätestatus ist OK.



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

#### Power



Mindestens eine der Versorgungsspannungen ist aktiv.

#### ACA



Kein externer Speicher ([ENM](#)) angeschlossen.

oder

Der externe Speicher ([ENM](#)) ist angeschlossen, jedoch nicht betriebsbereit.



Der externe Speicher ([ENM](#)) ist angeschlossen und betriebsbereit.

## Status Port

Dieser Rahmen zeigt eine vereinfachte Ansicht der Ports 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 Netzwerk

[Grundeinstellungen > Netzwerk]

Das Menü enthält die folgenden Dialoge:

- [Global](#)
- [IPv4](#)

## 1.21 Global

[Grundeinstellungen > Netzwerk > 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.

#### MAC-Adresse

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

### HiDiscovery Protokoll v1/v2

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

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

---

#### Anmerkung:

Mit der HiDiscovery-Software erreichen Sie das Gerät ausschließlich über Ports, die Mitglied desselben VLANs sind wie das Management des Geräts. Welchem Port welches VLAN zugewiesen ist, legen Sie fest im Dialog [Switching > VLAN > Konfiguration](#).

---

#### Funktion

Schaltet die Funktion HiDiscovery im Gerät ein/aus.

Mögliche Werte:

**An** (Voreinstellung)

Die Funktion HiDiscovery ist eingeschaltet.

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

**Aus**

Die Funktion HiDiscovery ist ausgeschaltet.

## Zugriff

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

Mögliche Werte:

`read-write` (Voreinstellung)

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

`read-only`

Die Funktion HiDiscovery hat lediglich Lesezugriff auf das Gerät. Das Gerät ermöglicht Ihnen, mit der Funktion HiDiscovery die IP-Parameter im Gerät anzusehen.

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

## 1.22 IPv4

[Grundeinstellungen > Netzwerk > IPv4]

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

### Management-Schnittstelle

VLAN-ID

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

Mögliche Werte:

1. . 4042 (Voreinstellung: 1)

Voraussetzung ist, dass im Dialog [Switching > VLAN > Konfiguration](#) das VLAN bereits eingerichtet ist.

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

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

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

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

### IP-Parameter

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

IP-Adresse

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

Mögliche Werte:

Gültige IPv4-Adresse

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 *Standard-Gateway* festgelegt ist. Die Einstellung im folgenden Dialog hat Vorrang:

- Dialog [Routing > Routing-Tabelle](#), Spalte [Next-Hop IP-Adresse](#), wenn der Wert in Spalte [Netz-Adresse](#) und in Spalte [Netzmaske](#) gleich 0. 0. 0. 0 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 [Li esmi ch](#)-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 bei der letzten Software-Aktualisierung oder nach Klicken der Schaltfläche [Wiederherstellen](#) in den Backup-Bereich kopiert.

#### Wiederherstellen

Das Gerät vertauscht die Images der Geräte-Software und dementsprechend die in den Feldern *Gespeicherte Version* und *Backup-Version* angezeigten Werte.

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

#### Bootcode

Zeigt Versionsnummer und Erstellungsdatum des Bootcodes.

### Software-Update


Das Gerät ermöglicht Ihnen, die Geräte-Software an dieser Stelle zu aktualisieren, wenn ein geeignetes Image der Geräte-Software außerhalb des Geräts verfügbar ist. Wenn ein geeignetes Image der Geräte-Software auf dem ausgewählten externen Speicher (EMM) gespeichert ist, verwenden Sie die Tabelle auf der Registerkarte *Dateisystem* weiter unten.

#### URL

Legt Pfad und Dateiname des Images der Geräte-Software fest, mit dem Sie die Geräte-Software aktualisieren.

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

- Software-Aktualisierung 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 SCP oder SFTP zum Gerät übertragen. Führen Sie die folgenden Schritte aus:

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

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

Übertragen Sie die Datei auf das Gerät in das Verzeichnis */upload/firmware*.

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 *ok* im Verzeichnis */upload/firmware* und löscht die übertragene Datei.

Das Gerät lädt die Geräte-Software beim nächsten Systemstart.

- Software-Aktualisierung 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:

- scp: // oder sftp: //<IP-Adresse>/<Pfad>/<Dateiname>

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

- scp: // oder sftp: //<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>

## Start

Aktualisiert die Geräte-Software.

- Um während des Software-Updates beim Management des Geräts angemeldet zu bleiben, bewegen Sie gelegentlich den Mauszeiger. Alternativ dazu können Sie, bevor Sie das Software-Update starten, einen ausreichend großen Wert im Dialog [Gerätesicherheit > Management-Zugriff > Web](#), Feld [Webinterface-Session Timeout \[min\]](#) festlegen.
- Das Gerät überträgt die bisher verwendete Geräte-Software in den Backup-Speicherbereich.
- Das Gerät überträgt die ausgewählte Datei in den Flash-Speicher und ersetzt die bisher verwendete Geräte-Software. Beim nächsten Systemstart startet das Gerät mit der Geräte-Software, die Sie übertragen haben.

## [Dateisystem]

### Tabelle

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

## Schaltflächen

### Update Firmware

Aktualisiert die Geräte-Software, wenn auf dem ausgewählten externen Speicher ([ENM](#)) ein geeignetes Image der Geräte-Software gespeichert ist. Voraussetzung ist, dass eine Tabellenzeile ausgewählt ist, für welche die Spalte [Datei Ort](#) den Wert [sd-card](#) oder [usb](#) zeigt.

- Vergewissern Sie sich, dass der betreffende externe Speicher in der Dropdown-Liste [Ausgewählter externer Speicher](#) ausgewählt ist. Siehe Dialog [Grundeinstellungen > Laden/Speichern](#), Rahmen [Externer Speicher](#).
- Um während des Software-Updates beim Management des Geräts angemeldet zu bleiben, bewegen Sie gelegentlich den Mauszeiger. Alternativ dazu können Sie, bevor Sie das Software-Update starten, einen ausreichend großen Wert im Dialog [Gerätesicherheit > Management-Zugriff > Web](#), Feld [Webinterface-Session Timeout \[min\]](#) festlegen.
- Das Gerät überträgt die bisher verwendete Geräte-Software in den Backup-Speicherbereich.
- Das Gerät überträgt die ausgewählte Datei in den Flash-Speicher und ersetzt die bisher verwendete Geräte-Software. Beim nächsten Systemstart startet das Gerät mit der Geräte-Software, die Sie übertragen haben.

## Datei Ort

Zeigt den Speicherort der Geräte-Software.

Mögliche Werte:

[ram](#)

Flüchtiger Speicher des Geräts

[flash](#)

Nichtflüchtiger Speicher ([NVM](#)) des Geräts

[sd-card](#)

Externer SD-Speicher (ACA31)

[usb](#)

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:

- [1](#)  
Beim nächsten Systemstart lädt das Gerät diese Geräte-Software.
- [2](#)  
Diese Geräte-Software hat das Gerät bei der letzten Software-Aktualisierung 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 *Konfigurations-Verschlüsselung* vergeben, speichert das Gerät sowohl das gegenwärtige als auch die zukünftigen Konfigurationsprofile in einem verschlüsselten Format.

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

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 nichtflüchtigen Speicher (NVM).

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



Zeigt ein Kontextmenü mit weiteren Funktionen für den betreffenden Dialog.

Speichern unter...

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

Geben Sie im Feld *Profilname* den Namen ein, unter dem Sie das Konfigurationsprofil speichern möchten (maximal 32 Zeichen).

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

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

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

---

**Anmerkung:**

Entscheiden Sie sich vor dem 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 (**RAM**).

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

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

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

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

#### Auswählen

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

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

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

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

#### Anmerkung:

Als „ausgewählt“ lassen sich ausschließlich Konfigurationsprofile kennzeichnen, die im nichtflüchtigen Speicher (NVM) gespeichert sind.

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

#### Importieren...

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

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

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

##### PC/URL

Das Gerät importiert das Konfigurationsprofil vom lokalen PC oder von einem Remote-Server.

##### Externer Speicher

Das Gerät importiert das Konfigurationsprofil vom ausgewählten externen Speicher (ENM). Siehe Rahmen *Externer Speicher*.

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

##### – Import vom PC

Befindet sich die Datei auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie diese in den



-Bereich. Alternativ dazu klicken Sie in den Bereich, um die Datei auszuwählen.

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

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

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

Übertragen Sie die Datei auf das Gerät in das Verzeichnis */nv/cfg*.

##### – Import 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:

scp: // oder sftp: //<IP-Adresse>/<Pfad>/<Dateiname>

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

scp: // oder sftp: //<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>

Wenn oben [Externer Speicher](#) ausgewählt ist, legen Sie im Rahmen [Import profile from external memory](#) die Datei des zu importierenden Konfigurationsprofils fest.

Wählen Sie in der Dropdown-Liste [Profilname](#) den Namen des zu importierenden Konfigurationsprofils.

Im Rahmen [Ziel](#) legen Sie fest, wo das Gerät das importierte Konfigurationsprofil speichert.

Im Feld [Profilname](#) legen Sie den Namen fest, unter dem das Gerät das Konfigurationsprofil speichert.

Im Feld [Speicherort](#) legen Sie den Speicherort für das Konfigurationsprofil fest. Voraussetzung ist, dass in der Dropdown-Liste [Select source](#) der Eintrag [PC/URL](#) ausgewählt ist.

#### RAM

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

#### NVM

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

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

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

Bezüglich Verschlüsselung des Konfigurationsprofils lesen Sie auch den Hilfetext zum Rahmen [Konfigurations-Verschlüsselung](#). Das Gerät importiert das Konfigurationsprofil unter den folgenden Bedingungen:

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

#### Exportieren...

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

Um die Datei auf Ihrem PC zu speichern, klicken Sie den Link in Spalte [Profilname](#), um den Speicherort zu wählen und den Dateinamen festzulegen.

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

- Export auf einen SCP- oder SFTP-Server  
Um die Datei auf einem SCP- oder SFTP-Server zu speichern, legen Sie den URL zur Datei in einer der folgenden Formen fest:
  - scp: // oder sftp: //<IP-Adresse>/<Pfad>/<Dateiname>  
Klicken Sie die Schaltfläche [Ok](#), um das Fenster [Anmeldeinformationen](#) zu öffnen. In diesem Fenster geben Sie [Benutzername](#) und [Passwort](#) ein, um sich am Server anzumelden.
  - scp: // oder sftp: //<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>

#### Running-Config als Skript speichern


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

#### Running-Config aus Skript laden

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

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

- Import vom PC

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

- Import 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:

`scp: //` oder `sftp: //<IP-Adresse>/<Pfad>/<Dateiname>`

#### Auf Lieferzustand zurücksetzen...

Setzt die Geräteeinstellungen auf die Voreinstellungen zurück.

- Das Gerät löscht die gespeicherten Konfigurationsprofile aus dem flüchtigen Speicher (RAM) und aus dem nichtflüchtigen Speicher (NVM).
- 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 (EMM) 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 (`running config`) aus dem flüchtigen Speicher (RAM).

#### Speicherort

Zeigt den Speicherort des Konfigurationsprofils.

Mögliche Werte:

RAM (flüchtiger Speicher des Geräts)

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

**NM** (nichtflüchtiger Speicher des Geräts)

Aus dem nichtflüchtigen Speicher lädt das Gerät das „ausgewählte“ Konfigurationsprofil beim Systemstart oder beim Anwenden der Funktion [Konfigurationsänderungen rückgängig machen](#).

Der nichtflüchtige Speicher bietet Platz für mehrere Konfigurationsprofile, abhängig von der Anzahl der im Konfigurationsprofil gespeicherten Einstellungen. Das Gerät verwaltet im nichtflüchtigen Speicher maximal 20 Konfigurationsprofile.

Sie können ein Konfigurationsprofil in den flüchtigen Speicher (**RAM**) laden. Führen Sie dazu die folgenden Schritte aus:

Wählen Sie die Tabellenzeile des Konfigurationsprofils.

Klicken Sie die Schaltfläche  und dann den Eintrag [Aktivieren](#).

**EMM** (externer Speicher)

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

Voraussetzung ist, dass im Dialog [Grundeinstellungen > Externer Speicher](#) das Kontrollkästchen [Sichere Konfiguration beim Speichern](#) markiert ist.

## Profilname

Zeigt die Bezeichnung des Konfigurationsprofils.

Mögliche Werte:

[running-config](#)


Bezeichnung des Konfigurationsprofils im flüchtigen Speicher (**RAM**).

[config](#)


Bezeichnung des werksseitig vorhandenen Konfigurationsprofils im nichtflüchtigen Speicher (**NM**).

benutzerdefinierter Name

Das Gerät ermöglicht Ihnen, ein Konfigurationsprofil mit benutzerdefiniertem Namen zu speichern. Wählen Sie dazu die Tabellenzeile eines vorhandenen Konfigurationsprofils, klicken die

Schaltfläche  und dann den Eintrag [Speichern unter...](#)

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

Um die Datei auf einem Remote-Server zu speichern, klicken Sie die Schaltfläche  und dann den Eintrag [Exportieren...](#)


## Letzte Änderung (UTC)

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

## Ausgewählt

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


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

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

Mögliche Werte:

**markiert**

Das Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet.

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

**unmarkiert**

Ein anderes Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet.

Verschlüsselung

Zeigt, ob das Konfigurationsprofil verschlüsselt ist.

Mögliche Werte:

**markiert**

Das Konfigurationsprofil ist verschlüsselt.

**unmarkiert**

Das Konfigurationsprofil ist unverschlüsselt.

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

Verifiziert

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

Mögliche Werte:

**markiert**

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

**unmarkiert**

Die Passwörter unterscheiden sich. Das Gerät ist außerstande, das Konfigurationsprofil zu entschlüsseln.

---

**Anmerkung:**

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

---

Software-Version

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

Fingerabdruck

Zeigt die im Konfigurationsprofil gespeicherte Prüfsumme.

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

## Verifiziert

Zeigt, ob die im Konfigurationsprofil gespeicherte Prüfsumme gültig ist.

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

Mögliche Werte:

**markiert**

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

**unmarkiert**

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

Mögliche Ursachen:

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

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

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

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

---

**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

Legt den externen Speicher fest, den das Gerät für Datei-Operationen verwendet.

Diese Einstellung wirkt sich wie folgt aus:

- Das Gerät speichert zum Beispiel eine Kopie der Dateien mit der Gerätekonfiguration auf dem ausgewählten externen Speicher (**ENM**).
- Das Gerät ermöglicht Ihnen, die Geräte-Software auf einfache Weise zu aktualisieren, wenn ein geeignetes Image der Geräte-Software auf dem ausgewählten externen Speicher gespeichert (**ENM**) ist. Siehe Dialog *Grundeinstellungen > Software*.

Mögliche Werte:

**sd**

Externer SD-Speicher (ACA31)

**usb**

Externer USB-Speicher (ACA21/ACA22)

## Status

Zeigt den Betriebszustand des ausgewählten externen Speichers (EMM).

Mögliche Werte:

**not Present**

Kein externer Speicher (EMM) angeschlossen.

**removed**

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

**ok**

Der externe Speicher (EMM) ist angeschlossen und betriebsbereit.

**out Of Memory**

Der Speicherplatz im externen Speicher (EMM) ist belegt.

**genericErr**

Das Gerät hat einen Fehler erkannt.

## Konfigurations-Verschlüsselung

### Aktiv

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

Mögliche Werte:

**markiert**

Die Konfigurations-Verschlüsselung ist aktiv.

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

**unmarkiert**

Die Konfigurations-Verschlüsselung ist inaktiv.

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

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

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

## Passwort setzen

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

Wenn Sie ein vorhandenes Passwort ändern, geben Sie in das Feld *Altes Passwort* das bisherige Passwort ein. Um anstelle von \*\*\*\*\* (Sternchen) das Passwort im Klartext anzuzeigen, markieren Sie das Kontrollkästchen *Passwort anzeigen*.

Geben Sie im Feld *Neues Passwort* das Passwort ein.

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

Markieren Sie das Kontrollkästchen *Konfiguration danach speichern*, um die Verschlüsselung auf das „ausgewählte“ Konfigurationsprofil im nichtflüchtigen Speicher (*NVM*) und im externen Speicher (*ENVM*) anzuwenden.

**Anmerkung:**

Wenden Sie diese Funktion ausschließlich dann an, wenn maximal ein Konfigurationsprofil im nichtflüchtigen Speicher (*NVM*) 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 *Grundeinstellungen > Laden/Speichern*.

Verschlüsseln Sie im neuen Gerät das Konfigurationsprofil. Siehe oben. Geben Sie dasselbe Passwort ein, das Sie im nicht mehr funktionierenden Gerät verwendet haben.

Installieren Sie im neuen Gerät den externen Speicher (*ENVM*) 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 (*ENVM*). Das Gerät kopiert die Einstellungen in den flüchtigen Speicher (*RAM*) und in den nichtflüchtigen Speicher (*NVM*).

**Anmerkung:**

Voraussetzung für das Laden eines Konfigurationsprofils vom externen Speicher (*ENVM*) ist, dass im Dialog *Grundeinstellungen > Externer Speicher* die Spalte *Konfigurations-Priorität* den Wert *erste* oder *zweite* zeigt. Dieser Wert ist voreingestellt.

## Löschen

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

Geben Sie im Feld *Altes Passwort* das bisherige Passwort ein.

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

Markieren Sie das Kontrollkästchen *Konfiguration danach speichern*, um die Verschlüsselung auch im „ausgewählten“ Konfigurationsprofil im nichtflüchtigen Speicher (NVM) und im externen Speicher (EMM) aufzuheben.

---

### Anmerkung:

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

---

## Konfigurationsänderungen rückgängig machen

### Funktion

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

Mögliche Werte:

#### An

Die Funktion ist eingeschaltet.

- Die Zeitspanne zwischen Verbindungsabbruch und Laden des Konfigurationsprofils legen Sie fest im Feld *Timeout [s] für Wiederherstellung nach Verbindungsabbruch*.
- Enthält der nichtflüchtige Speicher (NVM) mehrere Konfigurationsprofile, lädt das Gerät das als „ausgewählt“ gekennzeichnete Konfigurationsprofil.

#### Aus (Voreinstellung)

Die Funktion ist ausgeschaltet.

Schalten Sie die Funktion wieder aus, bevor Sie die grafische Benutzeroberfläche schließen. So vermeiden Sie, dass das Gerät das als „ausgewählt“ gekennzeichnete Konfigurationsprofil wiederherstellt.

---

### Anmerkung:

Bevor Sie die Funktion einschalten, speichern Sie die Einstellungen im Konfigurationsprofil. Die gegenwärtigen Einstellungen, die lediglich zwischengespeichert sind, bleiben somit erhalten.

---

### Timeout [s] für Wiederherstellung nach Verbindungsabbruch

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

Mögliche Werte:

30 . 600 (Voreinstellung: 600)

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

#### Watchdog IP-Adresse

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

Mögliche Werte:

IPv4-Adresse (Voreinstellung: 0.0.0.0)

### Information

#### NVM synchron mit running-config


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

Mögliche Werte:

**markiert**

Die Einstellungen stimmen überein.

**unmarkiert**

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

#### Externer Speicher und NVM synchron

Zeigt, ob die Einstellungen des „ausgewählten“ Konfigurationsprofils im externen Speicher (**ENM**) von den Einstellungen des „ausgewählten“ Konfigurationsprofils im nichtflüchtigen Speicher (**NM**) abweichen.

Mögliche Werte:

**markiert**

Die Einstellungen stimmen überein.

**unmarkiert**

Die Einstellungen weichen voneinander ab.

Mögliche Ursachen:

- An das Gerät ist kein externer Speicher (**ENM**) angeschlossen.
- Im Dialog *Grundeinstellungen > Externer Speicher* ist die Funktion *Sichere Konfiguration beim Speichern* 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 (EMM).

Mögliche Werte:

`sd`

Externer SD-Speicher (ACA31)

`usb`

Externer USB-Speicher (ACA21/ACA22)

#### Status

Zeigt den Betriebszustand des externen Speichers (EMM).

Mögliche Werte:

`notPresent`

Kein externer Speicher (EMM) angeschlossen.

`removed`

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

`ok`

Der externe Speicher (EMM) ist angeschlossen und betriebsbereit.

`outOfMemory`

Der Speicherplatz im externen Speicher (EMM) ist belegt.

`genericErr`

Das Gerät hat einen Fehler erkannt.

#### Schreibbar

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

Mögliche Werte:

`marked`

Das Gerät hat Schreibzugriff auf den externen Speicher (EMM).

`unmarked`

Das Gerät hat ausschließlich Lesezugriff auf den externen Speicher (EMM). Möglicherweise ist für den externen Speicher ein Schreibschutz aktiviert.

#### Automatisches Software-Update

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

Mögliche Werte:

**markiert** (Voreinstellung)

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

- die Datei des Geräte-Software-Images
- eine Textdatei `startupdate=<Dateiname_des_Software-Images>.bin`

**unmarkiert**

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:

**aktiv**

Das Gerät lädt das Konfigurationsprofil aus dem nichtflüchtigen Speicher (NM).

**erste, zweite**

Das Gerät lädt das Konfigurationsprofil von dem mit **erste** gekennzeichneten externen Speicher (ENM). Findet das Gerät dort kein Konfigurationsprofil, lädt es das Konfigurationsprofil von dem mit **zweite** gekennzeichneten externen Speicher (ENM) usw. .

Findet das Gerät auf dem externen Speicher (ENM) kein Konfigurationsprofil, lädt es das Konfigurationsprofil aus dem nichtflüchtigen Speicher (NM).

---

#### Anmerkung:

Beim Laden des Konfigurationsprofils aus dem externen Speicher (ENM) überschreibt das Gerät die Einstellungen des „ausgewählten“ Konfigurationsprofils im nichtflüchtigen Speicher (NM).

---

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


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

#### Sichere Konfiguration beim Speichern

Aktiviert/deaktiviert das Speichern einer Kopie im externen Speicher (ENM).

Mögliche Werte:

**markiert** (Voreinstellung)

Das Speichern einer Kopie ist aktiviert. Wenn Sie im Dialog *Grundeinstellungen > Laden/Speichern* die Schaltfläche  klicken, speichert das Gerät eine Kopie des Konfigurationsprofils auf dem aktiven externen Speicher (ENM).

**unmarkiert**

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:

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

Port an

Aktiviert/deaktiviert den Port.

Mögliche Werte:

`markiert` (Voreinstellung)

Der Port ist aktiv.

`unmarkiert`

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

#### Zustand

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

Mögliche Werte:

[markiert](#)

Der Port ist physisch eingeschaltet.

[unmarkiert](#)

Der Port ist physisch ausgeschaltet.

#### Autoneg.

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

Mögliche Werte:

[markiert](#) (Voreinstellung)

Die automatische Auswahl des Betriebsmodus ist aktiv.

Der Port handelt den Betriebsmodus mittels Auto-Negotiation selbständig aus und erkennt die Belegung der Anschlüsse des 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.

[unmarkiert](#)

Die automatische Auswahl des Betriebsmodus ist inaktiv.

Der Port arbeitet mit den Werten, die Sie in Spalte [Manuelle Konfiguration](#) und in Spalte [Manuelles Cable-Crossing](#) festlegen.

Ausgegraute Darstellung

Keine automatische Auswahl des Betriebsmodus.

#### Manuelle Konfiguration

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

Mögliche Werte:

[10M HDX](#)

Halbduplex-Verbindung

[10M FDX](#)

Vollduplex-Verbindung

[100M HDX](#)

Halbduplex-Verbindung

[100M FDX](#)

Vollduplex-Verbindung

[1G FDX](#)

Vollduplex-Verbindung

---

#### Anmerkung:

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

---

#### Link/ Aktuelle Betriebsart

Zeigt, welchen Betriebsmodus der Port gegenwärtig verwendet.

Mögliche Werte:

-

Kein Kabel angesteckt, keine Verbindung.

10M HDX  
Halbduplex-Verbindung  
10M FDX  
Voll duplex-Verbindung  
100M HDX  
Halbduplex-Verbindung  
100M FDX  
Voll duplex-Verbindung  
1G FDX  
Voll duplex-Verbindung

---

**Anmerkung:**

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

---

#### Manuelles Cable-Crossing

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

Voraussetzung ist, dass die Funktion *Autoneg.* ausgeschaltet ist.

Mögliche Werte:

*mdi*

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

*mdi x* (Voreinstellung auf Twisted-Pair-Ports)

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

*auto-mdi x*

Das Gerät erkennt das Sende- und Empfangsleitungspaar des angeschlossenen Geräts und stellt sich automatisch darauf ein.

Beispiel: Wenn Sie ein Endgerät über ein gekreuztes Kabel anschließen, stellt das Gerät den Port automatisch von *mdi x* auf *mdi* .

*unsupported* (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:

**markiert** (Voreinstellung)

Die Flusskontrolle auf dem Port ist aktiv.

Auf dem Port ist das Senden und Auswerten von Pause-Paketen (Vollduplex-Betrieb) oder Kollisionen (Halbduplex-Betrieb) aktiviert.

Um die Flusskontrolle im Gerät einzuschalten, aktivieren Sie zusätzlich die Funktion *Flusskontrolle* im Dialog *Switching > Global*.

Aktivieren Sie die Flusskontrolle außerdem auf dem Port des mit diesem Port verbundenen Geräts.

Auf einem Uplink-Port führt das Aktivieren der Flusskontrolle möglicherweise zu unerwünschten Sendeunterbrechungen im übergeordneten Netzsegment („Wandering Backpressure“).

**unmarkiert**

Die Flusskontrolle auf dem Port ist inaktiv.

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

## Trap senden

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

Mögliche Werte:

**markiert** (Voreinstellung)

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

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

**unmarkiert**

Das Senden von SNMP-Traps ist inaktiv.

## Power-State

Legt fest, ob der Port physisch eingeschaltet oder ausgeschaltet ist, nachdem Sie den Port in der Spalte *Port an* deaktiviert haben.

Mögliche Werte:

**markiert**

Das Gerät lässt den Port physisch eingeschaltet, wenn das Kontrollkästchen *Port an* nicht markiert ist. Ein Gerät, das an diesem Port angeschlossen ist, erkennt weiterhin den aktiven Link.

**unmarkiert** (Voreinstellung)

Der Port ist physisch ausgeschaltet. Der physische Zustand des Ports wird ausschließlich durch die Einstellung in Spalte *Port an* beeinflusst.

## Track-Name

Legt den Namen des Tracking-Objekts fest, mit dem das Gerät den physischen Port verknüpft.

Voraussetzung ist, dass im Dialog *Erweitert > Tracking > Konfiguration* das Feld *Track-Name* bereits eingerichtet ist.

Mögliche Werte:

[<Track name>](#) (Voreinstellung: -)

Das Gerät aktiviert oder deaktiviert automatisch den Verbindungs-Status eines physischen Ports, je nachdem, welches Tracking-Objekt aus der Dropdown-Liste gewählt ist.

Energie sparen

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

Mögliche Werte:

[no-power - save](#) (Voreinstellung)

Der Port bleibt aktiviert.

[auto-power - down](#)

Der Port schaltet in den Energiesparmodus.

[unsupported](#)

Der Port unterstützt diese Funktion nicht und bleibt aktiviert.

## [Statistiken]

Diese Registerkarte zeigt pro Port folgenden Überblick:

- Anzahl der vom Gerät empfangenen Datenpakete/Bytes
  - [Empfangene Pakete](#)
  - [Empfangene Oktets](#)
  - [Unicasts empfangen](#)
  - [Multicasts empfangen](#)
  - [Broadcasts empfangen](#)
- Anzahl der vom Gerät gesendeten oder vermittelten Datenpakete/Bytes
  - [Gesendete Pakete](#)
  - [Gesendete Oktets](#)
  - [Unicasts gesendet](#)
  - [Multicasts gesendet](#)
  - [Broadcasts gesendet](#)
- Anzahl der vom Gerät erkannten Fehler
  - [Empfangene Fragmente](#)
  - [Erkannte CRC-Fehler](#)
  - [Erkannte Kollisionen](#)
- Anzahl der vom Gerät empfangenen Datenpakete pro Größenkategorie
  - [Pakete 64 Byte](#)
  - [Pakete 65 bis 127 Byte](#)
  - [Pakete 128 bis 255 Byte](#)
  - [Pakete 256 bis 511 Byte](#)
  - [Pakete 512 bis 1023 Byte](#)
  - [Pakete 1024 bis 1518 Byte](#)
- Anzahl der vom Gerät verworfenen Datenpakete
  - [Empfangsseitig verworfene Pakete](#)
  - [Sendeseitig verworfene Pakete](#)

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

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

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

Klicken Sie im Dialog [Grundeinstellungen > Port](#) die Schaltfläche  .  
oder

Klicken Sie im Dialog [Grundeinstellungen > Restart](#) die Schaltfläche [Port-Statistiken leeren](#).

## 1.7 Restart

[Grundeinstellungen > Restart]

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

### Restart

Kaltstart...

Öffnet das Fenster [Restart](#), um einen Neustart des Geräts auszulösen.

Wenn sich das Konfigurationsprofil im flüchtigen Speicher ([RAM](#)) und das „ausgewählte“ Konfigurationsprofil im nichtflüchtigen Speicher ([NVM](#)) unterscheiden, zeigt das Gerät das Fenster [Warnung](#).

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

Um die geänderten Einstellungen zu verwerfen, klicken Sie im Fenster [Warnung](#) die Schaltfläche [Nein](#).

Das Gerät startet neu und durchläuft folgende Phasen:

- Das Gerät startet die Geräte-Software, die das Feld [Gespeicherte Version](#) im Dialog [Grundeinstellungen > Software](#) anzeigt.
- Das Gerät lädt die Einstellungen aus dem „ausgewählten“ Konfigurationsprofil. Siehe Dialog [Grundeinstellungen > Laden/Speichern](#).

---

#### Anmerkung:

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

---

### Schaltflächen

FDB leeren

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

ARP-Tabelle leeren

Entfernt aus der ARP-Tabelle die dynamisch eingerichteten Adressen.

Siehe Dialog [Diagnose > System > ARP](#).

Port-Statistiken leeren

Setzt die Zähler der Portstatistik auf 0.

Siehe Dialog [Grundeinstellungen > Port](#), Registerkarte [Statistiken](#).

#### Log-Datei leeren

Entfernt die protokollierten Einträge aus der Log-Datei.

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

#### Persistente Log-Datei leeren

Entfernt die Log-Dateien vom externen Speicher ([ENM](#)).

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

#### 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 2025, 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 [SNTP](#)-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 den Tag und die Ortszeit:  $Systemzeit = Systemzeit (UTC) + Lokaler Offset [min] + Sommerzeit$

Zeitquelle

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

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

Mögliche Werte:

[lokal](#)

Systemuhr des Geräts.

[ntp](#)

Der *NTP*-Client ist eingeschaltet und das Gerät ist durch einen *NTP*-Server synchronisiert. Siehe Dialog [Zeit > NTP](#).

Lokaler Offset [min]

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

Mögliche Werte:

-780 . 840 (Voreinstellung: 60)

## [Sommerzeit]

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

### Funktion

Sommerzeit

Schaltet den [Sommerzeit](#)-Modus ein/aus.

Mögliche Werte:

[An](#)

Die [Sommerzeit](#)-Modus ist eingeschaltet.

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

[Aus](#) (Voreinstellung)

Die [Sommerzeit](#)-Modus ist ausgeschaltet.

Die Sommerzeit-Einstellungen legen Sie in den Rahmen [Sommerzeit Beginn](#) und [Sommerzeit Ende](#) fest.

Profil...

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

Mögliche Werte:

[EU](#)

Sommerzeit-Einstellungen, die in der Europäischen Union gelten.

[USA](#)

Sommerzeit-Einstellungen, die in den Vereinigten Staaten gelten.

## Sommerzeit Beginn

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

Woche

Legt die Woche im gegenwärtigen Monat fest.

Mögliche Werte:

- (Voreinstellung)

erste

zweite

dritte

vierte

letzte

Tag

Legt den Wochentag fest.

Mögliche Werte:

- (Voreinstellung)

Sonntag

Montag

Dienstag

Mittwoch

Donnerstag

Freitag

Samstag

Monat

Legt den Monat fest.

Mögliche Werte:

- (Voreinstellung)

Januar

Februar

März

April

Mai

Juni

Juli

August

September

Oktober

November

Dezember

#### Systemzeit

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

Mögliche Werte:

<HH MM> (Voreinstellung: 00:00)

#### Sommerzeit Ende

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

#### Woche

Legt die Woche im gegenwärtigen Monat fest.

Mögliche Werte:

- (Voreinstellung)

erste

zweite

dritte

vierte

letzte

#### Tag

Legt den Wochentag fest.

Mögliche Werte:

- (Voreinstellung)

Sonntag

Montag

Dienstag

Mittwoch

Donnerstag

Freitag

Sonntag

#### Monat

Legt den Monat fest.

Mögliche Werte:

- (Voreinstellung)

Januar

Februar

März

April

Mai

Juni  
Juli  
August  
September  
Oktober  
November  
Dezember

#### Systemzeit

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

Mögliche Werte:

<HH MM> (Voreinstellung: 00:00)

## 22 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:

[An](#)

Der NTP-Client ist eingeschaltet.

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

[Aus](#) (Voreinstellung)

Der NTP-Client ist ausgeschaltet.

---

### Anmerkung:

Bevor Sie den Client einschalten, schalten Sie im Rahmen *Client und Server* die Funktion *Server* aus.

---

#### Modus

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

Mögliche Werte:

[uni cast](#) (Voreinstellung)

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

[broadcast](#)

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:

**An**

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.

**Aus** (Voreinstellung)

NTP-Client und NTP-Server sind ausgeschaltet.

---

### Anmerkung:

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

---

### Modus

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

Mögliche Werte:

**client-server** (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 *Zeit > NTP > Server* als aktiv gekennzeichnet sind.
- Der NTP-Server verteilt die Zeitinformation per Unicast an anfragende Clients.

**symmetric**

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 *Zeit > NTP > Server* 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:

**1..16** (Voreinstellung: 12)

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 [symmetri c](#).  
oder
- Das Gerät verwendet als Zeitquelle die lokale Systemuhr. Siehe Feld [Zeitquelle](#) im Dialog [Zeit > 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 **symmetri c** 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:

**marki ert**

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 **symmetri c** arbeitet, dann ist dieser Server an einem Cluster beteiligt.

**unmarki ert**

Die Verbindung zum NTP-Server ist deaktiviert.

#### IP-Adresse

Legt die IP-Adresse des NTP-Servers fest.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung: 0.0.0.0)

#### Initial burst

Aktiviert/deaktiviert den *Initial burst*-Modus.

Im Betrieb sendet der NTP-Client des Geräts ausschließlich einzelne Datenpakete, um die Zeit zu erfragen. Wenn der NTP-Server unerreichbar ist (Spalte *Status = not Responding*), dann sendet der NTP-Client des Geräts mehrere Datenpakete auf einmal (Burst), um sich schnellstmöglich zu synchronisieren.

Mögliche Werte:

*markiert*

Der *Initial burst*-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.

*unmarkiert* (Voreinstellung)

Der *Initial burst*-Modus ist inaktiv.

#### Burst

Aktiviert/deaktiviert den *Burst*-Modus.

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

Mögliche Werte:

*markiert*

Der *Burst*-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.

*unmarkiert* (Voreinstellung)

Der *Burst*-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 *Bevorzugt*.

Mögliche Werte:

`markiert`

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.

`unmarkiert` (Voreinstellung)

Keine bevorzugte Verwendung des NTP-Servers.

Status

Zeigt den Synchronisierungs-Status.

Mögliche Werte:

`ausgeschaltet`

Kein Server verfügbar.

`protocol Error`

`not Synchronized`

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

`not Responding`

Der Server ist verfügbar. Das Gerät erhält keine Zeitinformation.

`synchronizing`

Der Server ist verfügbar. Das Gerät erhält eine Zeitinformation.

`synchronized`

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

`genericError`

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 [Gerätesicherheit > Authentifizierungs-Liste](#).

#### 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 Command Line Interface über die serielle Verbindung ist die Anzahl erfolgloser Login-Versuche unbegrenzt.

---

Mögliche Werte:

0..5 (Voreinstellung: 0)

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 `administrator`, die Sperre aufzuheben.

Der Wert 0 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 [Richtlinien überprüfen](#).

Mögliche Werte:

1. . 64 (Voreinstellung: 6)

Zeitraum für Login-Versuche (min.)

Zeigt die Zeitspanne, nach der das Gerät den Zähler im Feld [Login-Versuche](#) zurücksetzt.

Mögliche Werte:

0. . 60 (Voreinstellung: 0)

### Passwort-Richtlinien

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

Die Einstellungen wirken auf Spalte [Passwort](#). Voraussetzung ist, dass das Kontrollkästchen in Spalte [Richtlinien überprüfen](#) markiert ist.

Großbuchstaben (min.)

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

Mögliche Werte:

0. . 16 (Voreinstellung: 1)

Der Wert 0 deaktiviert diese Richtlinie.

Kleinbuchstaben (min.)

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

Mögliche Werte:

0. . 16 (Voreinstellung: 1)

Der Wert 0 deaktiviert diese Richtlinie.

Ziffern (min.)

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

Mögliche Werte:

0. . 16 (Voreinstellung: 1)

Der Wert 0 deaktiviert diese Richtlinie.

#### Sonderzeichen (min.)

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

Mögliche Werte:

0..16 (Voreinstellung: 1)

Der Wert 0 deaktiviert diese Richtlinie.

### Tabelle

Jeder Benutzer benötigt ein aktives Benutzerkonto, um Zugriff auf das Management des Geräts zu erhalten. Die Tabelle ermöglicht Ihnen, Benutzerkonten einzurichten und zu verwalten. Um Einstellungen zu ändern, klicken Sie in der Tabelle den gewünschten Parameter und modifizieren den Wert.

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

#### Schaltflächen



Hinzufügen

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

- Im Feld *Benutzername* legen Sie die Bezeichnung des Benutzerkontos fest.  
Mögliche Werte:  
Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen




Löschen

Entfernt die ausgewählte Tabellenzeile.

#### Benutzername

Zeigt die Bezeichnung des Benutzerkontos.

Um ein Benutzerkonto hinzuzufügen, klicken Sie die Schaltfläche .

#### Aktiv

Aktiviert/deaktiviert das Benutzerkonto.

Mögliche Werte:

*markiert*

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

*unmarkiert* (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 *administrator* 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:

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

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

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

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

## Rolle

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

Mögliche Werte:

*unauthoriz ed*

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.

*guest* (Voreinstellung)

Der Benutzer ist berechtigt, das Gerät zu überwachen.

*audi tor*

Der Benutzer ist berechtigt, das Gerät zu überwachen und im Dialog *Diagnose > Bericht > Audit-Trail* die Protokoll-Datei zu speichern.

*oper ator*

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

*adm i nistrator*

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:

- *Adm i nistratori ve*-User: *adm i nistrator*
- *Logi n*-User: *oper ator*
- *NAS- Prompt*-User: *guest*

## Benutzer gesperrt

Entsperrt das Benutzerkonto.

Mögliche Werte:

`markiert`

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

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

`unmarkiert` (Voreinstellung)

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

## Richtlinien überprüfen

Aktiviert/deaktiviert das Prüfen des Passworts.

Mögliche Werte:

`markiert`

Das Prüfen des Passworts ist aktiviert.

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

`unmarkiert` (Voreinstellung)

Das Prüfen des Passworts ist deaktiviert.

## SNMP-Authentifizierung

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

Mögliche Werte:

`hmacmd5` (Voreinstellung)

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

`hmacsha`

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

## SNMP-Verschlüsselung

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

Mögliche Werte:

`kein`

Keine Verschlüsselung.

`des` (Voreinstellung)

DES-Verschlüsselung

`aesCfb128`

AES-128-Verschlüsselung

## 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:

- defaultLogi nAuthLi st
- defaultV24AuthLi st

### 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 mittels Command Line Interface über die serielle Verbindung möglich. In diesem Fall authentifiziert das Gerät den Benutzer mittels lokaler Benutzerverwaltung. Siehe Dialog [Gerätesicherheit > Benutzerverwaltung](#).

Schaltflächen



Hinzufügen

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

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



Löschen

Entfernt die ausgewählte Tabellenzeile.



Anwendungen zuordnen

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

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

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

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

Wenn Sie die Anwendung [Web Interface](#) abwählen, dann bricht die Verbindung zum Gerät ab, sobald Sie auf Schaltfläche [Ok](#) 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 [Zugeordnete Anwendungen](#) 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:

[lokal](#) (Voreinstellung)

Das Gerät authentifiziert die Benutzer mittels lokaler Benutzerverwaltung. Siehe Dialog [Gerätesicherheit > Benutzerverwaltung](#).

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

[radius](#)

Das Gerät authentifiziert die Benutzer mit einem RADIUS-Server im Netz. Den RADIUS-Server legen Sie im Dialog [Netzicherheit > RADIUS > Authentication-Server](#) fest.

[reject](#)

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

- Wenn die erste Richtlinie in der Authentifizierungsliste [lokal](#) 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 [lokal](#) ist und das Gerät die Anmelde-daten des Benutzers ablehnt, versucht das Gerät, den Benutzer mithilfe der anderen Richtlinien in der festgelegten Reihenfolge beim Management des Geräts anzumelden.


- Wenn die erste Richtlinie in der Authentifizierungsliste [radius](#) oder [ldap](#) ist und das Gerät die Anmeldung ablehnt, wird die Anmeldung sofort verweigert, ohne dass das Gerät versucht, den Benutzer über eine andere Richtlinie anzumelden. Bleibt die Antwort des RADIUS- oder LDAP-Servers aus, versucht das Gerät die Authentifizierung des Benutzers mit der nächsten Richtlinie.
- Wenn die erste Richtlinie in der Authentifizierungsliste [reject](#) ist, lehnen die Geräte die Benutzeranmeldung sofort ab, ohne eine andere Richtlinie anzuwenden.
- Vergewissern Sie sich, dass die Authentifizierungsliste [defaultV24AuthList](#) mindestens eine Richtlinie enthält, die vom Wert [reject](#) abweicht.

#### ldap

Das Gerät authentifiziert die Benutzer über Authentifizierungsdaten und die Zugriffsrolle, die an einem zentralen Ort gespeichert sind. Den vom Gerät verwendeten Active-Directory-Server legen Sie im Dialog [Gerätesicherheit > LDAP > Konfiguration](#) fest.

#### Zugeordnete Anwendungen

Zeigt die zugeordneten Anwendungen. Wenn Benutzer mit der betreffenden Anwendung auf das Gerät zugreifen, wendet das Gerät die festgelegten Richtlinien für die Authentifizierung an.

Um der Liste eine andere Anwendung zuzuordnen oder die Zuordnung aufzuheben, klicken Sie die Schaltfläche . Das Gerät ermöglicht Ihnen, jede Anwendung genau einer Liste zuzuordnen.

#### Aktiv

Aktiviert/deaktiviert die Liste.

Mögliche Werte:

[markiert](#) (Voreinstellung)

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

[unmarkiert](#)

Die Liste ist deaktiviert.

## 3.3 LDAP

[Gerätesicherheit > LDAP]

Das Lightweight Directory Access Protocol (LDAP) ermöglicht Ihnen, die Benutzer an einer zentralen Stelle im Netz zu authentifizieren und zu autorisieren. Ein weit verbreiteter, mit LDAP abfragbarer Verzeichnisdienst ist Active Directory®.

Das Gerät 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 *LDAP*-Client ein/aus.

Das Gerät verwendet den *LDAP*-Client, wenn Sie im Dialog *Gerätesicherheit > Authentifizierungs-Liste* den Wert *ldap* in einer der Spalten *Richtlinie 1* bis *Richtlinie 5* festlegen. Legen Sie zuvor im Dialog *Gerätesicherheit > LDAP > Rollen-Zuweisung* mindestens ein Mapping für die Zugriffsrolle *administrator* fest. Damit haben Sie nach Anmeldung über LDAP weiterhin als Administrator Zugriff auf das Management des Geräts.

Mögliche Werte:

*An*

Der *LDAP*-Client ist eingeschaltet.

*Aus* (Voreinstellung)

Der *LDAP*-Client ist ausgeschaltet.

### Konfiguration

Schaltflächen



Cache leeren

Löscht 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:

1..1440 (Voreinstellung: 10)

## Bind-Benutzer

Legt die Benutzerkennung in Form des „Distinguished Name“ (DN) fest, mit der das Gerät sich am LDAP-Server anmeldet.

Diese Angabe ist erforderlich, wenn der LDAP-Server bei der Anmeldung eine Benutzerkennung in Form des „Distinguished Name“ (DN) erfordert. In Active-Directory-Umgebungen ist diese Angabe nicht erforderlich.

Das Gerät 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 *Base DN* und *Benutzername-Attribut*.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

## Bind-Benutzer Passwort

Legt das Passwort fest, welches das Gerät bei der Anmeldung am LDAP-Server zusammen mit der in Feld *Bind-Benutzer* festgelegten Benutzerkennung verwendet.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

## Base DN

Legt den Startpunkt in Form des „Distinguished Name“ (DN) fest für die Suche im Verzeichnisbaum.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

## Benutzername-Attribut

Legt das LDAP-Attribut fest, das einen eindeutigen Benutzernamen enthält. Danach verwendet der Benutzer den in diesem Attribut enthaltenen Benutzernamen, um sich beim Management des Geräts anzumelden.

Häufig enthalten die LDAP-Attribute *userPrincipalName*, *mail*, *sAMAccountName* und *uid* einen eindeutigen Benutzernamen.

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

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

Mögliche Werte:

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

Default-Domain

Legt die Zeichenfolge fest, mit der das Gerät den Benutzernamen sich anmeldender Benutzer ergänzt, sofern der Benutzername kein @-Zeichen enthält.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

## CA certificate

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
- .PEMDateinamenserweiterung
- Base64-kodiert und umschlossen von den Zeilen  
-----BEGIN CERTIFICATE-----  
...  
-----END CERTIFICATE-----

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 SCP oder SFTP zum Gerät übertragen. Führen Sie die folgenden Schritte aus:

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

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

Übertragen Sie die Datei auf das Gerät in das Verzeichnis `/upload/dap-cert`.

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 `ok` im Verzeichnis `/upload/dap-cert` 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://` oder `sftp://`<IP-Adresse>/<Pfad>/<Dateiname>

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

– `scp://` oder `sftp://`<Benutzername>.<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>

Start

Überträgt die im Feld *URL* festgelegte Datei auf das Gerät.

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

**Tabelle**

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

Schaltflächen



Fügt eine Tabellenzeile hinzu.



Entfernt die ausgewählte Tabellenzeile.

Index

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

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 *Verbindungssicherheit* ein anderer Wert als *kein* festgelegt ist und das digitale Zertifikat ausschließlich DNS-Namen des Servers enthält.

#### Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung: 0.0.0.0)

DNS-Name im Format <domain>. <tl d> oder <host>. <domain>. <tl d>

Voraussetzung ist, dass Sie zusätzlich im Dialog *Erweitert > DNS > Client > Global* die Funktion *Client* einschalten.

Wenn Sie eine verschlüsselte Verbindung mithilfe eines digitalen Zertifikats herstellen, vergewissern Sie sich, dass die *Common Name*- oder *Subject Alternative Name*-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.

[\\_ldap.\\_tcp.<domain>.<tl d>](#)

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 *Adresse* der Wert [\\_ldap.\\_tcp.domain.tld](#) festgelegt ist, dann ignoriert das Gerät den hier festgelegten Wert.

#### Mögliche Werte:

0..65535 (2<sup>16</sup> - 1) (Voreinstellung: 389)

Ausnahme: Port 2222 ist für interne Funktionen reserviert.

#### Häufig verwendete TCP-Ports:

- LDAP: 389
- LDAP over SSL: 636
- Active Directory Global Catalogue: 3268
- Active Directory Global Catalogue SSL: 3269

#### Verbindungssicherheit

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

#### Mögliche Werte:

[kein](#)

Keine Verschlüsselung.

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

[ssl](#)

Verschlüsselung mit SSL.

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

[startTLS](#) (Voreinstellung)

Verschlüsselung mit startTLS-Erweiterung.

Das Gerät baut eine LDAP-Verbindung zum Server auf und verschlüsselt die Kommunikation.

Voraussetzung für die verschlüsselte Kommunikation ist, dass das Gerät die korrekte Uhrzeit verwendet. Wenn das digitale Zertifikat ausschließlich DNS-Namen enthält, dann legen Sie in Spalte *Adresse* den DNS-Namen des Servers fest. Schalten Sie die Funktion *Client* im Dialog *Erweitert > DNS > Client > Global* ein.

Wenn das 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:

`ok`

Der Server ist erreichbar.

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

`unreachable`

Server ist unerreichbar.

`other`

Das Gerät hat noch keine Verbindung zum Server aufgebaut.

### Aktiv

Aktiviert/deaktiviert die Verwendung des Servers.

Mögliche Werte:

`markiert`

Das Gerät verwendet den Server.

`unmarkiert` (Voreinstellung)

Das Gerät verwendet den Server nicht.

## 3.3.2 LDAP Rollen-Zuweisung

[ Gerätesicherheit > LDAP > Rollen-Zuweisung ]

Dieser Dialog ermöglicht Ihnen, bis zu 64 Mappings 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 *Übereinstimmende Regel*. Entweder erhält der Benutzer die Zugriffsrolle mit den weitreichenderen Berechtigungen oder die 1. in der Tabelle zutreffende Zugriffsrolle.

### Konfiguration

#### Übereinstimmende Regel

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

Mögliche Werte:

*highest* (Voreinstellung)

Das Gerät verwendet die Zugriffsrolle mit den weitreichenderen Berechtigungen.

*erste*

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

## Tabelle

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

### Schaltflächen



Hinzufügen

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

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

Mögliche Werte:

1 . 64



Löschen

Entfernt die ausgewählte Tabellenzeile.

### Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Sie legen die 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:

*unauthori zed* (Voreinstellung)

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

Weisen Sie diesen Wert zu, um das Benutzerkonto vorübergehend zu sperren. Wenn beim Zuweisen einer anderen Zugriffsrolle ein Fehler erkannt wird, dann weist das Gerät dem Benutzerkonto diese Zugriffsrolle zu.

*guest*

Der Benutzer ist berechtigt, das Gerät zu überwachen.

*audi tor*

Der Benutzer ist berechtigt, das Gerät zu überwachen und im Dialog *Diagnose > Bericht > Audit-Trail* die Protokoll-Datei zu speichern.

*oper at or*

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

*admi ni str ator*

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

### Typ

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

Mögliche Werte:

*attri bute* (Voreinstellung)

Die Spalte *Parameter* enthält ein Attribut mit einem Attributwert.

*group*

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

#### Parameter

Legt abhängig von der Einstellung in Spalte *Typ* eine Gruppe oder ein Attribut mit einem Attributwert fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Das Gerät unterscheidet zwischen Groß- und Kleinschreibung.

- Wenn in Spalte *Typ* der Wert *attribute* festgelegt ist, dann legen Sie das Attribut in der Form *AttributeName=Attributwert* fest.

Beispiel: *l=Germany*

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

Beispiel: *CN=admin-users, OU=Groups, DC=example, DC=com*

#### Aktiv

Aktiviert/deaktiviert das Mapping der Rolle.

Mögliche Werte:

*markiert*

Das Mapping der Rolle ist aktiv.

*unmarkiert* (Voreinstellung)

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 [SNMP](#).

Mögliche Werte:

[markiert](#)  
Server-Dienst ist aktiv.

[unmarkiert](#)  
Server-Dienst ist inaktiv.

#### SNMPv2

Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit SNMP Version 2 ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte [SNMP](#).

Mögliche Werte:

[markiert](#)  
Server-Dienst ist aktiv.

[unmarkiert](#)  
Server-Dienst ist inaktiv.

### SNMPv3

Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit SNMP Version 3 ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte [SNMP](#).

Mögliche Werte:

`marked`

Server-Dienst ist aktiv.

`unmarked`

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 [SSH](#).

Mögliche Werte:

`marked`

Server-Dienst ist aktiv.

`unmarked`

Server-Dienst ist inaktiv.

### HTTP server

Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit der grafischen Bedienoberfläche über HTTP ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte [HTTP](#).

Mögliche Werte:

`marked`

Server-Dienst ist aktiv.

`unmarked`

Server-Dienst ist inaktiv.

### HTTPS server

Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit der grafischen Bedienoberfläche über HTTPS ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte [HTTPS](#).

Mögliche Werte:

`marked`

Server-Dienst ist aktiv.

`unmarked`

Server-Dienst ist inaktiv.

## [SNMP]

Diese Registerkarte ermöglicht Ihnen, Einstellungen für den SNMP-Agenten des Geräts festzulegen und den Zugriff auf das Gerät mit unterschiedlichen SNMP-Versionen ein-/auszuschalten.

Der SNMP-Agent ermöglicht den Zugriff auf das Management des Geräts mit SNMP-basierten Anwendungen.

## Konfiguration

### SNMPv1

Aktiviert/deaktiviert den Zugriff auf das Gerät per SNMP Version 1.

Mögliche Werte:

**markiert**

Zugriff mittels SNMP-Version 1 ist aktiv.

- Die Community-Namen legen Sie fest im Dialog [Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community](#).

**unmarkiert** (Voreinstellung)

Zugriff mittels SNMP-Version 1 ist inaktiv.

### SNMPv2

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

Mögliche Werte:

**markiert**

Zugriff mittels SNMP-Version 2 ist aktiv.

- Die Community-Namen legen Sie fest im Dialog [Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community](#).

**unmarkiert** (Voreinstellung)

Zugriff mittels SNMP-Version 2 ist inaktiv.

### SNMPv3

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

Mögliche Werte:

**markiert** (Voreinstellung)

Zugriff ist aktiviert.

**unmarkiert**

Zugriff ist deaktiviert.

Netzmanagementsysteme wie Industrial HiVision verwenden dieses Protokoll, um mit dem Gerät zu kommunizieren.

### UDP-Port

Legt die Nummer des UDP-Ports fest, auf dem der SNMP-Agent Anfragen von Clients entgegennimmt.

Mögliche Werte:

1. . 65535 (2<sup>16</sup> - 1) (Voreinstellung: 161)

Ausnahme: Port 2222 ist für interne Funktionen reserviert.

Damit der SNMP-Agent nach einer Änderung den neuen Port verwendet, gehen Sie wie folgt vor:

Klicken Sie die Schaltfläche .

Wählen Sie im Dialog [Grundeinstellungen > Laden/Speichern](#) das aktive Konfigurationsprofil.

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

Starten Sie das Gerät neu.

## [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 SCP oder SFTP auf das Gerät und den angeschlossenen externen Speicher ([ENM](#)) zuzugreifen, benötigen Sie ebenfalls Zugriff auf den SSH-Server. Mit einem SCP- oder SFTP-Client, zum Beispiel WinSCP, haben Sie die Möglichkeit, Konfigurationsdateien oder eine aktualisierte Geräte-Software 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 Fingerabdruck dieses Schlüssels. Der Fingerabdruck 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 Fingerabdrücke zu vergleichen. Wenn die Zeichenfolgen übereinstimmen, dann ist der Client mit dem korrekten Server verbunden.

Das Gerät ermöglicht Ihnen, den *RSA-Host Key* direkt im Gerät zu generieren. Alternativ dazu können Sie Ihren eigenen privaten Schlüssel im PEM-Format auf das Gerät übertragen.

Darüber hinaus kann das Gerät beim Systemstart einen *RSA-Host Key* laden, der auf dem externen Speicher ([ENM](#)) abgelegt ist. Diese Funktion aktivieren Sie im Dialog [Grundeinstellungen > Externer Speicher](#), Spalte [SSH-Key automatisch uploaden](#).

## Funktion

### SSH-Server

Schaltet den SSH-Server ein/aus.

Mögliche Werte:

[An](#) (Voreinstellung)

Der SSH-Server ist eingeschaltet.

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

Der Server lässt sich ausschließlich dann starten, wenn eine RSA-Signatur im Gerät vorhanden ist.

[Aus](#)

Der SSH-Server ist ausgeschaltet.

Wenn Sie den SSH-Server ausschalten, bleiben bestehende Verbindungen aufgebaut. Das Gerät sorgt dafür, den Aufbau neuer Verbindungen zu verhindern.

---

### Anmerkung:

Wenn Sie den [SSH-Server](#) ausschalten, dann ist der Zugriff auf das Management des Geräts ausschließlich mittels Command Line Interface über die serielle Verbindung möglich.

---

## Konfiguration

### TCP-Port

Legt die Nummer des TCP-Ports fest, auf dem das Gerät SSH-Anfragen von den Clients entgegennimmt.

Mögliche Werte:

1..65535 (2<sup>16</sup> - 1) (Voreinstellung: 22)

Ausnahme: Port 2222 ist für interne Funktionen reserviert.

Nach Ändern des Ports startet der Server automatisch neu. Bestehende Verbindungen bleiben aufgebaut.

### Sessions

Zeigt, wie viele SSH-Verbindungen gegenwärtig zum Gerät aufgebaut sind.

### Sitzungen (max.)

Legt fest, wie viele gleichzeitige SSH-Verbindungen zum Gerät maximal möglich sind.

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

Mögliche Werte:

1..5 (Voreinstellung: 5)

### 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:

0

Deaktiviert die Funktion. Die Verbindung bleibt bei Inaktivität aufgebaut.

1..160 (Voreinstellung: 5)

## Signatur

### RSA vorhanden

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

Mögliche Werte:

markiert

Der RSA-Host Key ist vorhanden.

unmarkiert

Der RSA-Host Key ist nicht vorhanden.

## Erstellen

Generiert einen *RSA-Host Key* im Gerät. Voraussetzung ist, dass der *SSH-Server* ausgeschaltet ist.

Länge des generierten Schlüssels:

- 2048 Bit (RSA)

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

Alternativ dazu können Sie Ihren eigenen privaten Schlüssel im PEM-Format auf das Gerät übertragen. Siehe Rahmen *Key-Import*.

## Löschen

Löscht den *RSA-Host Key* vom Gerät. Voraussetzung ist, dass der SSH-Server ausgeschaltet ist.

## Betriebszustand

Zeigt, ob das Gerät gegenwärtig einen *RSA-Host Key* generiert.

Möglicherweise hat ein anderer Benutzer diese Aktion ausgelöst.

Mögliche Werte:

*rsa*

Das Gerät generiert gegenwärtig einen *RSA-Host Key*.

*kein*

Das Gerät generiert keinen *RSA-Host Key*.

## Fingerabdruck

Der Fingerabdruck ist eine einfach zu prüfende Zeichenfolge, die den *RSA-Host Key* des SSH-Servers eindeutig identifiziert.

Nach Importieren eines neuen *RSA-Host Keys* zeigt das Gerät den bisherigen Fingerabdruck so lange, bis Sie den Server neu starten.

## Fingerabdruck Typ

Legt fest, welchen Fingerabdruck das Feld *RSA-Fingerabdruck* anzeigt.

Mögliche Werte:

*md5* (Voreinstellung)

Das Feld *RSA-Fingerabdruck* zeigt den Fingerabdruck als hexadezimalen MD5-Hash.

*sha256*

Das Gerät unterstützt diese Einstellung nicht. Das Feld *RSA-Fingerabdruck* behält die bisherige Anzeige bei.

## RSA-Fingerabdruck

Zeigt den Fingerabdruck des *RSA-Host Keys* des SSH-Servers.

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

**Key-Import**


## URL

Legt Pfad und Dateiname Ihres eigenen RSA-Keys fest.

Das Gerät akzeptiert den Schlüssel, wenn er 2048 Bit lang ist.

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 SCP oder SFTP zum Gerät übertragen. Führen Sie die folgenden Schritte aus:

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

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

Übertragen Sie die Datei auf das Gerät in das Verzeichnis */upl oad/ssh-key*.

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

Wenn die Installation erfolgreich war, dann generiert das Gerät eine Datei *ok* im Verzeichnis */upl oad/ssh-key* 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: // oder sftp: //<l P- Adresse>/<Pfad>/<Datei name>

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

– scp: // oder sftp: //<Benutzer name>:<Passwort>@<l P- Adresse>/<Pfad>/<Datei name>

## Start

Überträgt die im Feld *URL* festgelegte Datei auf das Gerät.

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

**[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 *HTTP* ein/aus.

Mögliche Werte:

*An* (Voreinstellung)

Die Funktion *HTTP* ist eingeschaltet.

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

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

*Aus*

Die Funktion *HTTP* ist ausgeschaltet.

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

---

**Anmerkung:**

Wenn die Funktionen *HTTP* und *HTTPS* ausgeschaltet sind, können Sie die Funktion *HTTP* mit dem Kommando `http server` im Command Line Interface einschalten, um die grafische Benutzeroberfläche zu erreichen.

---

**Konfiguration**

TCP-Port

Legt die Nummer des TCP-Ports fest, auf dem der Webserver HTTP-Anfragen von den Clients entgegennimmt.

Mögliche Werte:

1.. 65535 (2<sup>16</sup> - 1) (Voreinstellung: 80)

Ausnahme: Port 2222 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-Verbindung 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 Zertifikat 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 **HTTPS** ein/aus.

Mögliche Werte:

**An** (Voreinstellung)

Die Funktion **HTTPS** ist eingeschaltet.

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

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

**Aus**

Die Funktion **HTTPS** ist ausgeschaltet.

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

---

**Anmerkung:**

Wenn die Funktionen **HTTP** und **HTTPS** ausgeschaltet sind, können Sie die Funktion **HTTPS** mit dem Kommando `https server` im Command Line Interface einschalten, um die grafische Benutzeroberfläche zu erreichen.

---

**Konfiguration**

## TCP-Port

Legt die Nummer des TCP-Ports fest, auf dem der Webserver HTTPS-Anfragen von den Clients entgegennimmt.

Mögliche Werte:

1.. 65535 (2<sup>16</sup> - 1) (Voreinstellung: 443)

Ausnahme: Port 2222 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:

`markiert`

Ein digitales Zertifikat ist vorhanden.

`unmarkiert`

Das digitale Zertifikat wurde entfernt.

### Erstellen

Generiert ein digitales Zertifikat im 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.

Sie können ein digitales Zertifikat auf das Gerät übertragen. Siehe Rahmen [Zertifikat-Import](#).

### Löschen

Löscht das digitale Zertifikat.

Bis zum Neustart verwendet der Webserver das vorherige Zertifikat.

### Betriebszustand

Zeigt, ob das Gerät gegenwärtig ein digitales Zertifikat generiert oder löscht.

Möglicherweise hat ein anderer Benutzer die Aktion ausgelöst.

Mögliche Werte:

`kein`

Das Gerät generiert oder löscht gegenwärtig kein digitales Zertifikat.

`delete`

Das Gerät löscht gegenwärtig ein digitales Zertifikat.

`generate`

Das Gerät generiert gegenwärtig ein digitales Zertifikat.

## Fingerabdruck

Der Fingerabdruck 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 Fingerabdruck so lange, bis Sie den Server neu starten.

### Fingerabdruck Typ

Legt fest, welchen Fingerabdruck das Feld *Fingerabdruck* anzeigt.

Mögliche Werte:

*sha1*

Das Feld *Fingerabdruck* zeigt den SHA1-Fingerabdruck des digitalen Zertifikats.

*sha256* (Voreinstellung)

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

### Fingerabdruck

Hexadezimale Zeichenfolge des vom Server verwendeten digitalen Zertifikats.

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

## Zertifikat-Import

### URL


Legt Pfad und Dateiname des digitalen Zertifikats fest.

Das Gerät akzeptiert digitale Zertifikate mit den folgenden Eigenschaften:

- X.509-Format
- .PEMDateinamenserweiterung
- Base64-kodiert und umschlossen von den Zeilen
  - -----BEGIN PRIVATE KEY-----
  - ...
  - END PRIVATE KEY-----
  - oder
  - -----BEGIN CERTIFICATE-----
  - ...
  - END CERTIFICATE-----
- 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 SCP oder SFTP zum Gerät übertragen.

Führen Sie die folgenden Schritte aus:

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

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

Übertragen Sie die Datei auf das Gerät in das Verzeichnis `/upl oad/https-cert`.

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

Wenn die Installation erfolgreich war, dann generiert das Gerät eine Datei `ok` im Verzeichnis `/upl oad/https-cert` 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: // oder sftp: //<I P- Adresse>[: Port] /<Pfad>/<Datei name>

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

- scp: // oder sftp: //<Benutzer name>: <Passwort>@<I P- Adresse>[: Port] /<Pfad>/<Datei - name>

Start

Überträgt die im Feld *URL* festgelegte Datei auf das Gerät.

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

## 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 *IP-Zugriffsbeschränkung* ein/aus.

Mögliche Werte:

**An**

Die Funktion *IP-Zugriffsbeschränkung* 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 mittels Command Line Interface über die serielle Verbindung möglich.

---

**Aus** (Voreinstellung)

Die Funktion *IP-Zugriffsbeschränkung* ist ausgeschaltet.

### Tabelle

Sie haben die Möglichkeit, bis zu 16 Tabellenzeilen zu definieren und separat zu aktivieren.

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

## Schaltflächen



Hinzufügen

Fügt eine Tabellenzeile hinzu.



Löschen

Entfernt die ausgewählte Tabellenzeile.

## Index

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

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:

1..16

## Interface

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

Voraussetzung ist, dass in Spalte *Adresse* und Spalte *Netzmaske* der Wert 0.0.0.0 festgelegt ist.

Mögliche Werte:

*Alle* (Voreinstellung)

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

*<Port-Nummer>*

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

Das Gerät unterstützt die Funktion *IP-Zugriffsbeschränkung* 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 *Netzmaske*.

Voraussetzung ist, dass in Spalte *Interface* der Wert *Alle* festgelegt ist.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung: 0.0.0.0)

## Netzmaske

Legt den Bereich des in Spalte *Adresse* festgelegten Netzes fest.

Voraussetzung ist, dass in Spalte *Interface* der Wert *Alle* festgelegt ist.

Mögliche Werte:

Gültige Netzmaske (Voreinstellung: 0. 0. 0. 0)

Ein Beispiel: Um den Zugriff von einer einzelnen IP-Adresse aus zu beschränken, legen Sie den Wert 255. 255. 255. 255 fest.

HTTP

Aktiviert/deaktiviert den HTTP-Zugriff.

Mögliche Werte:

**markiert** (Voreinstellung)

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

**unmarkiert**

HTTP-Zugriff ist inaktiv.

HTTPS

Aktiviert/deaktiviert den HTTPS-Zugriff.

Mögliche Werte:

**markiert** (Voreinstellung)

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

**unmarkiert**

HTTPS-Zugriff ist inaktiv.

SNMP

Aktiviert/deaktiviert den SNMP-Zugriff.

Mögliche Werte:

**markiert** (Voreinstellung)

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

**unmarkiert**

SNMP-Zugriff ist inaktiv.

SSH

Aktiviert/deaktiviert den SSH-Zugriff.

Mögliche Werte:

**markiert** (Voreinstellung)

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

**unmarkiert**

SSH-Zugriff ist inaktiv.

## Aktiv

Aktiviert/deaktiviert die Tabellenzeile.

Mögliche Werte:

**markiert**

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.

**unmarkiert** (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:

0 . 160 (Voreinstellung: 5)

Der Wert 0 deaktiviert die Funktion, der Benutzer bleibt bei Inaktivität angemeldet.

## 3.4.4 Command Line Interface

[Gerätesicherheit > Management-Zugriff > CLI]

In diesem Dialog legen Sie Einstellungen für das Command Line Interface fest. Weitere Informationen zum Command Line Interface finden Sie im Referenzhandbuch „Command Line Interface“.

Der Dialog enthält die folgenden Registerkarten:

- [\[Global\]](#)
- [\[Login-Banner\]](#)

### [Global]

Diese Registerkarte ermöglicht Ihnen, den Prompt im Command Line Interface zu ändern und das automatische Schließen inaktiver Sitzungen des Command Line Interface über die serielle Verbindung zu aktivieren.

Sie können mittels Command Line Interface wie folgt auf das Management des Geräts zugreifen:

- durch eine serielle Verbindung über die V.24-Schnittstelle
- per SSH über Ethernet

### Konfiguration

#### Login-Prompt

Legt die Zeichenfolge fest, die das Gerät im Command Line Interface am Beginn jeder Kommandozeile anzeigt.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen  
(0x20..0x7E) inklusive Leerzeichen

Wildcards

- %d Datum
- %i IP-Adresse
- %m MAC-Adresse
- %p Produktname
- %s Produktname kurz
- %t Uhrzeit

Voreinstellung: (EAGLE)

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 mittels Command Line Interface über die serielle Verbindung beim Management des Geräts angemeldet ist.

Mögliche Werte:

0..160 (Voreinstellung: 5)

Der Wert 0 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 [SSH-Server](#) legen Sie das Timeout fest im Dialog [Gerätesicherheit > Management-Zugriff > Server](#).

## [Login-Banner]

In dieser Registerkarte ersetzen Sie den Startbildschirm im Command Line Interface durch einen individuellen Text.

In der Voreinstellung zeigt der Startbildschirm Informationen über das Gerät, zum Beispiel die Software-Version und 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 [Gerätesicherheit > Pre-Login-Banner](#).

## Funktion

### Funktion

Schaltet die Funktion [Login-Banner](#) ein/aus.

Mögliche Werte:

[An](#)

Die Funktion [Login-Banner](#) ist eingeschaltet.

Das Gerät zeigt die im Feld [Banner-Text](#) festgelegte Textinformation den Benutzern, die sich mit dem Command Line Interface beim Management des Geräts anmelden.

[Aus](#) (Voreinstellung)

Die Funktion [Login-Banner](#) ist ausgeschaltet.

Der Startbildschirm zeigt Informationen über das Gerät. Die Textinformation im Feld [Banner-Text](#) bleibt erhalten.

## Banner-Text

### Banner-Text

Legt die Textinformation fest, die das Gerät zu Beginn jeder Sitzung im Command Line Interface anzeigt.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..1024 Zeichen  
([0x20](#) . [0x7E](#)) inklusive Leerzeichen

[<Tabul ator >](#)

[<Ze i enunbr uch>](#)

## 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 *Community*) erhält die Anwendung die Berechtigung *Lesen* oder *Lesen und Schreiben*.

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

### Tabelle

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

#### Community

Zeigt die Berechtigung für SNMPv1/v2-Zugriff auf das Gerät.

Mögliche Werte:

*Write*

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

*Read*

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

#### Name

Legt den Community-Namen für die nebenstehende Berechtigung fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

Das Gerät akzeptiert die folgenden Zeichen:

– <space>

– 0..9

– a..z

– A..Z

– !"#\$%&'()\*+,-./:;<=>@[\\]^\_`{|}~

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

*public* (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 [Gerätesicherheit > Management-Zugriff > CLI](#).

### Funktion

Funktion

Schaltet die Funktion [Pre-Login-Banner](#) ein/aus.

Mit der Funktion [Pre-Login-Banner](#) zeigt das Gerät im Login-Dialog der grafischen Benutzeroberfläche und im Command Line Interface eine Begrüßung oder einen Hinweis.

Mögliche Werte:

[An](#)

Die Funktion [Pre-Login-Banner](#) ist eingeschaltet.

Das Gerät zeigt im Login-Dialog den im Feld [Banner-Text](#) festgelegten Text.

[Aus](#) (Voreinstellung)

Die Funktion [Pre-Login-Banner](#) ist ausgeschaltet.

Das Gerät zeigt im Login-Dialog keinen Text. Haben Sie im Feld [Banner-Text](#) einen Text eingegeben, 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  
(0x20 . 0x7E) inklusive Leerzeichen

<Tabul at or >

<Zeilenumbruch>

## 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 *Paketfilter L3*-Regeln  
Siehe Dialog [Netzsicherheit > Paketfilter > Routed-Firewall-Modus](#).
- die eingerichteten *Paketfilter L2*-Regeln  
Siehe Dialog [Netzsicherheit > Paketfilter > Transparent-Firewall-Modus](#).
- die eingerichteten *Destination-NAT*-Regeln  
Siehe Dialog [Routing > NAT > Destination-NAT](#).
- die eingerichteten *Double-NAT*-Regeln  
Siehe Dialog [Routing > NAT > Double-NAT](#).
- die eingerichteten *Masquerading-NAT*-Regeln  
Siehe Dialog [Routing > NAT > Masquerading-NAT](#).
- die eingerichteten *1:1-NAT*-Regeln  
Siehe Dialog [Routing > NAT > 1:1-NAT](#).

#### 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 [radi us](#) einer Anwendung die Richtlinie [Gerätesicherheit > Authentifizierungs-Liste](#) zuweisen. Das Gerät leitet die Zugangsdaten der Benutzer weiter an den primären Authentication-Server. Der Authentication-Server entscheidet, ob die Zugangsdaten gültig sind und übermittelt dem Gerät die Berechtigungen der Benutzer.

Den in der Antwort eines RADIUS-Servers übertragenen Service-Type weist das Gerät wie folgt einer im Gerät vorhandenen Zugriffsrolle zu:

- **Administrative-User:** `administrator`
- **Logi n-User:** `operator`
- **NAS-Prompt-User:** `guest`

Das Menü enthält die folgenden Dialoge:

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

## 4.21 RADIUS Global

[Netzsicherheit > RADIUS > Global]

Dieser Dialog ermöglicht Ihnen, grundlegende Einstellungen für RADIUS festzulegen.

### RADIUS-Konfiguration

Schaltflächen

 Zurücksetzen

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

Anfragen (max.)

Legt fest, wie viele Male das Gerät eine unbeantwortete Anfrage an den Authentication-Server wiederholt, bevor es die Anfrage an einen anderen Authentication-Server sendet.

Mögliche Werte:

1..15 (Voreinstellung: 4)

Timeout [s]

Legt fest, wie viele Sekunden das Gerät nach einer Anfrage an den Authentication-Server auf Antwort wartet, bevor es die Anfrage erneut sendet.

Mögliche Werte:

1..30 (Voreinstellung: 5)

NAS IP-Adresse (Attribut 4)

Legt die IP-Adresse fest, die das Gerät als Attribut 4 an den Authentication-Server überträgt. Legen Sie die IP-Adresse des Geräts oder eine andere, frei wählbare Adresse fest.

---

#### Anmerkung:

Das Gerät sendet das Attribut 4 ausschließlich dann mit, wenn das Paket durch die 802.1X-Authentifizierungsanfrage eines Endgeräts (Supplicant) ausgelöst wurde.

---

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung: 0.0.0.0)

In vielen Fällen befindet sich zwischen Gerät und Authentication-Server eine Firewall. Bei der Network Address Translation (NAT) in der Firewall ändert sich die ursprüngliche IP-Adresse, der Authentication-Server empfängt die übersetzte IP-Adresse des Geräts.

Die IP-Adresse in diesem Feld überträgt das Gerät unverändert über Network Address Translation (NAT) hinweg.

## 4.2.2 RADIUS Authentication-Server

[Netzicherheit > 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 [Erstellen](#), um eine Tabellenzeile hinzuzufügen.

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



Löschen

Entfernt die ausgewählte Tabellenzeile.

#### Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Sie legen die 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: [Default-RADIUS-Server](#))

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

#### Adresse

Legt die IP-Adresse des Servers fest.

Mögliche Werte:

Gültige IPv4-Adresse

#### Ziel UDP-Port

Legt die Nummer des UDP-Ports fest, auf dem der Server Anfragen entgegennimmt.

Mögliche Werte:

0..65535 (2<sup>16</sup> - 1) (Voreinstellung: 1812)

Ausnahme: Port 2222 ist für interne Funktionen reserviert.

#### Secret

Zeigt \*\*\*\*\* (Sternchen), wenn ein Passwort festgelegt ist, mit dem sich das Gerät beim Server anmeldet. Um das Passwort zu ändern, klicken Sie in das betreffende Feld.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..16 Zeichen

Das Passwort erfahren Sie vom Administrator des Authentication-Servers.

#### Primärer Server

Kennzeichnet den Authentication-Server als primär oder sekundär.

Mögliche Werte:

`markiert`

Der Server ist als primärer Authentication-Server gekennzeichnet. Das Gerät sendet die Zugangsdaten zum Authentifizieren der Benutzer an diesen Authentication-Server.

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

`unmarkiert` (Voreinstellung)

Der Server ist als sekundärer Authentication-Server gekennzeichnet. Das Gerät sendet die Zugangsdaten an den sekundären Authentication-Server, wenn es vom primären Authentication-Server keine Antwort erhält.

#### Aktiv

Aktiviert/deaktiviert die Verbindung zum Server.

Das Gerät verwendet den Server, wenn Sie im Dialog *Gerätesicherheit > Authentifizierungs-Liste* den Wert `radius` in einer der Spalten *Richtlinie 1* bis *Richtlinie 5* festlegen.

Mögliche Werte:

`markiert` (Voreinstellung)

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

`unmarkiert`

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

## 4.2.3 RADIUS Authentication Statistiken

[Netzsicherheit > RADIUS > Authentication-Statistiken]

Dieser Dialog zeigt Informationen über die Kommunikation zwischen dem Gerät und dem Authentication-Server. Die Tabelle zeigt die Informationen für jeden Server in einer separaten Tabellenzeile.

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



### Tabelle

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

Name

Zeigt den Namen des Servers.

IP-Adresse

Zeigt die IP-Adresse des Servers.

Zeit Round-Trip

Zeigt 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 *Erstellen*, um eine Tabellenzeile hinzuzufügen.

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

Mögliche Werte:

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

Nach Klicken der Schaltfläche *Ok* fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile den im Feld *Name* 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 *any*

### 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:

*computer* (Voreinstellung)

*control l er*

*devi ce*

*netw ork*

*netw ork-equi pment*

*broadcast*

*mul ti cast*

#### 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:

[any](#) (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: [192.168.112.0/25](#)

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: [! 1.1.1.1](#) oder [! 192.168.112.0/25](#)

#### MAC-Adresse

Legt die MAC-Adresse des Assets fest.

Mögliche Werte:

[any](#) (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 *Erstellen*, um eine Tabellenzeile hinzuzufügen. Im Feld *Protokollname* legen Sie einen eindeutigen Namen für das Protokoll fest.

Mögliche Werte:

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

- any
- i cmp
- i gmp
- i pi p
- tcp
- udp
- esp
- ah
- i cmpv6

Nach Klicken der Schaltfläche *Ok* fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile den im Feld *Protokollname* 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:

- any
- i cmp
- i gmp
- i pi p
- tcp

- udp
- esp
- ah
- i cmpv6

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:

- any (Voreinstellung)
- ethernet
- i cmp
- tcp
- udp

Ethertype

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

Mögliche Werte:

- custom (Voreinstellung)
- appletalk
- arp
- ibmna
- ipv4
- ipv6
- ipxold
- mplsncast
- mplsucast
- netbios
- novell
- pppoedisc
- rarp
- pppoess
- ipxnew
- profinet
- powerlink
- ethercat
- vlan8021q

#### Benutzerspezifischer Ethertype-Wert

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

Mögliche Werte:

1536 . 65535 ( $2^1 - 1$ ) (Voreinstellung: 0)

#### Protocol number

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

Mögliche Werte:

*any* (Voreinstellung)

0 . 255

#### Port

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

Mögliche Werte:

*any* (Voreinstellung)

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

1 . 65535 ( $2^1 - 1$ )

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 21.
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel 21, 80, 110.
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel 2000- 3000.
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel 21, 2000-3000, 65535.

Das Feld ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel 21, 2000- 3000, 65535 eingeben, verwenden Sie 4 von 15 Zahlenwerten.

## 4.5 Paketfilter

[Netzsicherheit > Paketfilter]

In diesem Menü legen Sie die Einstellungen für die Funktionen *Paketfilter* 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 *Routed-Firewall-Modus*-Paketfilter fest.

Der *Routed-Firewall-Modus*-Paketfilter enthält Regeln, die das Gerät nacheinander auf den Datenstrom auf seinen Router-Interfaces anwendet. Der *Routed-Firewall-Modus*-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 *accept*. Das Gerät ermöglicht Ihnen, die Standard-Regel im Dialog [Netzsicherheit > Paketfilter > Routed-Firewall-Modus > Global](#) zu ändern.

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

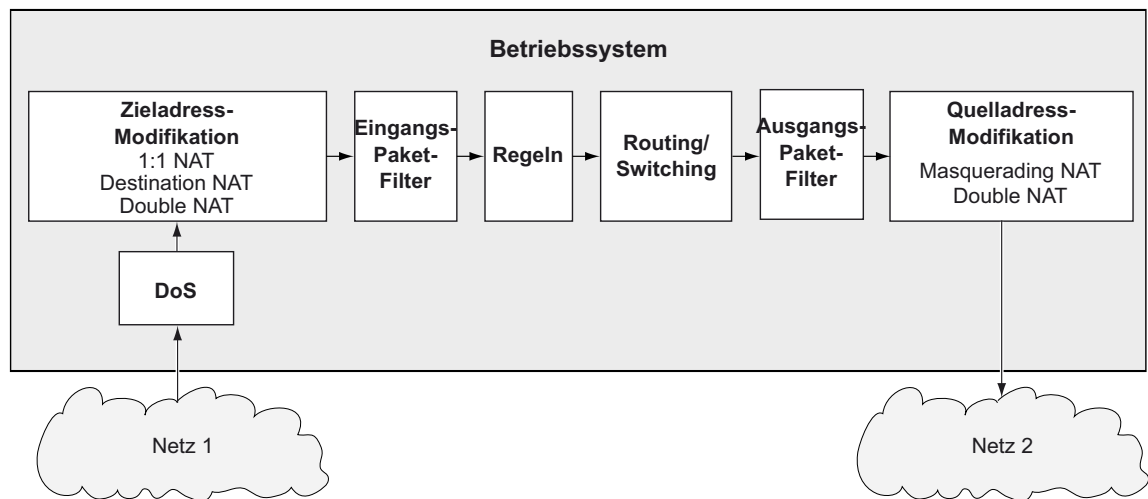


Abb. 1: Bearbeitungsreihenfolge der Datenpakete im Gerät

Das Menü enthält die folgenden Dialoge:

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

## 4.5.1.1 Global

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

In diesem Dialog legen Sie die globalen Einstellungen für den *Routed-Firewall-Modus*-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 *OPC Enforcer*. 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:

**accept** (Voreinstellung)  
Das Gerät akzeptiert die Datenpakete.

**drop**  
Das Gerät verwirft die Datenpakete.

**reject**  
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:

**markiert** (Voreinstellung)  
Das Gerät wertet die *Prüfsumme* im Datenpaket aus. Wenn der Wert ungültig ist, dann verwirft das Gerät das Datenpaket.

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

## Logging

### Log

Aktiviert/deaktiviert die Protokollierung in der System-Log-Datei für Fälle, in denen das Gerät die *Standardrichtlinie* auf ein Datenpaket anwendet. Dies ist dann der Fall, wenn keine *Paketfilter*-Regel existiert oder kein Datenpaket den eingerichteten Regeln entspricht.

Mögliche Werte:

[markiert](#)

Die Protokollierung ist aktiv.

Das Gerät erstellt einen Eintrag in der System-Log-Datei, wenn das Gerät die *Standardrichtlinie* auf die Datenpakete anwendet. Siehe Dialog [Diagnose > Bericht > System-Log](#).

[unmarkiert](#) (Voreinstellung)

Die Protokollierung ist inaktiv.

## Information


Nicht angewendete Änderungen vorhanden

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

Mögliche Werte:

[markiert](#)

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

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

[unmarkiert](#)

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

## 4.5.1.2 Firewall-Lern-Modus

[Netzsicherheit > 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 *FLM* festlegen können, ist abhängig von der Anzahl der im Dialog *Netzsicherheit > Paketfilter > Routed-Firewall-Modus > Regel* bereits erstellten Regeln. Das Gerät ermöglicht Ihnen, bis zu 2048 Regeln festzulegen.

Die Funktion *FLM* gilt ausschließlich für Pakete, die das Gerät passieren und mit der Kette *FORWARD* übereinstimmen. Die Funktion *FLM* 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 *FLM* ist erforderlich, dass Sie mindestens 2 Router-Interfaces im Gerät einrichten und auswählen.

Die Funktion *FLM* kann maximal 65535 Verbindungen erlernen.

---

### Anmerkung:

Während der Lernphase ist das Netz vorübergehend gefährdet, da die Funktion *FLM* Regeln einrichtet, die jedes Datenpaket auf den ausgewählten Ports akzeptieren.

---

### Anmerkung:

Wenn Sie auf einem Router-Interface die Funktion *VRRP* einschalten, dann ist auf diesem Router-Interface die Funktion *FLM* unwirksam.

---

Der Dialog enthält die folgenden Registerkarten:

- [\[Konfiguration\]](#)
- [\[Regeln\]](#)

### [Konfiguration]

Die Registerkarte ermöglicht Ihnen, die Funktion *FLM* 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 *FLM* ein/aus.

Mögliche Werte:

*An*

Die Funktion *FLM* ist eingeschaltet.

*Aus* (Voreinstellung)

Die Funktion *FLM* 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 *FLM* gestoppt wird.

### Status

Zeigt den Zustand der aktiven *FLM*-Anwendung.

Mögliche Werte:

*off*

Die Funktion ist inaktiv.

*stopped-data-not-present*

*stopped-data-present*

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

*learning*

Das Gerät erlernt Daten.

*pending*

Das Gerät ist mit der Verarbeitung erlernter Daten beschäftigt.

### Information

Zeigt den Status des *FLM*-Anwendungsspeichers.

### Für Lernen ausgewählte Interfaces

Zeigt die Interfaces, welche die Funktion *FLM* 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 *Gelernte Einträge* angezeigten Daten können Sie nach Bedarf Daten akzeptieren oder ablehnen.

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

**Tabelle Gelernte Einträge**

Schaltflächen



Hinzufügen

Öffnet das Fenster *Erstellen*, um eine Regel hinzuzufügen, sofern die Tabelle *Gelernte Einträge* mindestens eine Tabellenzeile enthält. Die Tabelle *Paketfilter-Regeln* zeigt die hinzugefügte Regel.

- Im Feld *Beschreibung* legen Sie einen Namen für die Regel fest.
- Im Feld *Quelle Adresse* legen Sie die Quelladresse der Datenpakete fest.
- Im Feld *Ziel Adresse* legen Sie die Zieladresse der Datenpakete fest.
- In der Dropdown-Liste *Protokoll* wählen Sie den Protokolltyp der Datenpakete.
- Im Feld *Ziel Port* legen Sie den Ziel-Port der Datenpakete fest.
- Im Feld *Eingangs-Interface* 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 [Bearbeiten](#), um die Parameter der ausgewählten Tabellenzeile zu bearbeiten.

#### Regel-Index

Zeigt die fortlaufende Nummer der [Paketfilter](#)-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:

[any](#) (Voreinstellung)

Das Gerät wendet die [Paketfilter](#)-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:

[any](#) (Voreinstellung)

Das Gerät wendet die [Paketfilter](#)-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:

[any](#) (Voreinstellung)

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

[i cnp](#)

Internet Control Message Protocol (RFC 792)

[i gmp](#)

Internet Group Management Protocol

[i pi p](#)

IP in IP tunneling (RFC 2003)

[t cp](#)

Transmission Control Protocol (RFC 793)

[udp](#)

User Datagram Protocol (RFC 768)

[esp](#)

IPsec Encapsulated Security Payload (RFC 2406)

[ah](#)

IPsec Authentication Header (RFC 2402)

[i cnpv6](#)

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 *Protokoll* der Wert *TCP* oder *UDP* festgelegt ist.

Mögliche Werte:

*any* (Voreinstellung)

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

1..65535 (2<sup>16</sup> - 1)

Das Gerät wendet die *Paketfilter*-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 21.
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel 21, 80, 110.
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel 2000-3000.
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel 21, 2000-3000, 65535.

Das Feld ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel 21, 2000-3000, 65535 eingeben, verwenden Sie 4 von 15 Zahlenwerten.

Aktion

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

Mögliche Werte:

*accept* (Voreinstellung)

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

*drop*

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

*reject*

Das Gerät verwirft das Datenpaket und informiert den Absender.

*enforce-ndbus*

Das Gerät wendet die in Spalte *Index DPI-Profil* festgelegte Regel auf die Datenpakete an.

*enforce-opc*

Das Gerät wendet die in Spalte *Index DPI-Profil* festgelegte Regel auf die Datenpakete an.

*enforce-dnp3*

Das Gerät wendet die in Spalte *Index DPI-Profil* festgelegte Regel auf die Datenpakete an.

*enforce-iec104*

Das Gerät wendet die in Spalte *Index DPI-Profil* festgelegte Regel auf die Datenpakete an.

*enforce-ethernetip*

Das Gerät wendet die in Spalte *Index DPI-Profil* festgelegte Regel auf die Datenpakete an.

### Eingangs-Interface

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

Mögliche Werte:

*kommand*

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

*gehend*

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

### Aktiv

Aktiviert/deaktiviert die Regel.

Mögliche Werte:

*markiert*

Die Regel ist aktiv.

*unmarkiert* (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 [Netzsicherheit > Paketfilter > Routed-Firewall-Modus > Zuweisung](#) 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 [Paketfilter](#)-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 [Netzsicherheit > Asset](#) fest.

Mögliche Werte:

[any](#) (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: [192.168.112.0/25](#)

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: ! 1. 1. 1. 1 oder ! 192. 168. 112. 0/25

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 *Netzsicherheit > Asset* fest.

Mögliche Werte:

[any](#) (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: [192. 168. 112. 0/25](#)

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: ! 1. 1. 1. 1 oder ! 192. 168. 112. 0/25

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:

[any](#) (Voreinstellung)

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

[i cnp](#)

Internet Control Message Protocol (RFC 792)

[i gmp](#)

Internet Group Management Protocol

[i pi p](#)

IP in IP tunneling (RFC 2003)

[t cp](#)

Transmission Control Protocol (RFC 793)

[udp](#)

User Datagram Protocol (RFC 768)

[esp](#)

IPsec Encapsulated Security Payload (RFC 2406)

[ah](#)

IPsec Authentication Header (RFC 2402)

i cnpv6

Internet Control Message Protocol for IPv6 (RFC 4443)

<user-defined protocols>

Das Gerät verarbeitet auch benutzerdefinierte Protokolle. Sie legen benutzerdefinierte Protokolle im Dialog [Netzsicherheit > Protokoll](#) fest.

Quelle Port

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

Mögliche Werte:

*any* (Voreinstellung)

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

1..65535 (2<sup>16</sup> - 1)

Das Gerät wendet die *Paketfilter*-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 [21](#).
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel [21, 80, 110](#).
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel [2000-3000](#).
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel [21, 2000-3000, 65535](#).

Das Feld ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel [21, 2000-3000, 65535](#) 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 *Protokoll* der Wert *tcp* oder *udp* festgelegt ist.

Mögliche Werte:

*any* (Voreinstellung)

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

1..65535 (2<sup>16</sup> - 1)

Das Gerät wendet die *Paketfilter*-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 [21](#).
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel [21, 80, 110](#).
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel [2000-3000](#).
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel [21, 2000-3000, 65535](#).

Das Feld ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel [21, 2000-3000, 65535](#) eingeben, verwenden Sie 4 von 15 Zahlenwerten.

Parameter

Legt zusätzliche Parameter für diese Regel fest.

Geben Sie Parameter in der folgenden Form an: `<param>=<val >`. 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 `mac` gilt unabhängig vom Protokoll. Außerdem haben Sie die Möglichkeit, eine Kombination aus gültigen Regeln und protokollspezifischen Regeln einzugeben.

Mögliche Werte:

`none` (Voreinstellung)

Sie haben keine zusätzlichen Parameter für diese Regel festgelegt.

`mac=de: ad: de: ad: be: ef`

Diese Regel gilt für Pakete mit der MAC-Quelladresse `de: ad: de: ad: be: ef`.

`type=<0 . 255>`

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).

`code=<0 . 255>`

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).

`frags=<true| false>`

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

`flags=<syn| ack| fin>`

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

`flags=syn`

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

`flags=syn|ack|fin`

Diese Regel gilt für Pakete, für die Sie das Flag `syn,ack` oder `or fin` gesetzt haben.

`mac=de: ad: de: ad: be: ef, state=new|rel, flags=syn`

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

Aktion

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

Mögliche Werte:

`accept` (Voreinstellung)

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

`drop`

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

`reject`

Das Gerät verwirft das Datenpaket und informiert den Absender.

`enforce-modbus`

Das Gerät wendet die in Spalte *Index DPI-Profil* festgelegte Regel auf die Datenpakete an.

Voraussetzung ist, dass in den Spalten *Quelle Adresse*, *Ziel Adresse* und *Ziel Port* ein anderer Wert als *any* festgelegt ist.

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

**enforce-opc**

Das Gerät wendet die in Spalte *Index DPI-Profil* festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten *Quelle Adresse*, *Ziel Adresse* und *Ziel Port* ein anderer Wert als *any* festgelegt ist.

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

**enforce-dnp3**

Das Gerät wendet die in Spalte *Index DPI-Profil* festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten *Quelle Adresse*, *Ziel Adresse* und *Ziel Port* ein anderer Wert als *any* festgelegt ist.

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

**enforce-iec104**

Das Gerät wendet die in Spalte *Index DPI-Profil* festgelegte Regel auf die Datenpakete an.

Voraussetzung ist, dass in den Spalten *Quelle Adresse*, *Ziel Adresse* und *Ziel Port* ein anderer Wert als *any* festgelegt ist.

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

**enforce-ethernetip**

Das Gerät wendet die in Spalte *Index DPI-Profil* festgelegte Regel auf die Datenpakete an.

Voraussetzung ist, dass in den Spalten *Quelle Adresse*, *Ziel Adresse* und *Ziel Port* ein anderer Wert als *any* 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 System-Log-Datei, wenn das Gerät die in dieser Tabellenzeile festgelegte *Paketfilter* Regel anwendet.

Mögliche Werte:

**markiert**

Die Protokollierung ist aktiv.

Das Gerät erstellt einen Eintrag in der System-Log-Datei, wenn das Gerät die in dieser Tabellenzeile festgelegte *Paketfilter*-Regel anwendet. Siehe Dialog *Diagnose > Bericht > System-Log*.

**unmarkiert** (Voreinstellung)

Die Protokollierung ist inaktiv.

## Trap

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

Mögliche Werte:

**markiert**

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

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

**unmarkiert** (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 *Aktion* einer der folgenden Werte festgelegt ist:

- [enforce-modbus](#)
- [enforce-opc](#)
- [enforce-dnp3](#)
- [enforce-iec104](#)
- [enforce-ethernetip](#)

Mögliche Werte:

0 (Voreinstellung)

Das Gerät wendet keine Regel auf die Datenpakete an.


1.. 32

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 [Netzsicherheit > Paketfilter > Routed-Firewall-Modus > Global](#) oder den Dialog [Netzsicherheit > Paketfilter > Routed-Firewall-Modus > Zuweisung](#).

Klicken Sie die Schaltfläche .

Mögliche Werte:

[markiert](#)

Die Regel ist aktiv.

[unmarkiert](#) (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 *Paketfilter*-Regeln zuzuweisen. Router-Interfaces richten Sie ein im Dialog *Routing > Interfaces > Konfiguration*.

### Information

#### Zuweisungen

Zeigt, wie viele Regeln für die Ports aktiv sind.


#### Nicht angewendete Änderungen vorhanden

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

Mögliche Werte:

*markiert*

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

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

*unmarkiert*

Das Gerät wendet die gespeicherten *Paketfilter*-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 *Erstellen*, um einem Router-Interface eine Regel zuzuweisen.

- In der Dropdown-Liste *Regel-Index* wählen Sie die Regel, die Sie dem Router-Interface zuweisen.
- In der Dropdown-Liste *Richtung* wählen Sie aus, ob das Gerät die Regel auf empfangene Datenpakete, auf zu sendende Datenpakete oder auf beide anwendet.
- In der Dropdown-Liste *Interface* 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 *OPC Enforcer*. 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 [Netzsicherheit > Paketfilter > Routed-Firewall-Modus > Regel](#).

Regel-Index

Zeigt die fortlaufende Nummer der *Paketfilter*-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 *Paketfilter*-Regel auf empfangene Datenpakete, auf zu sendende Datenpakete oder auf beide anwendet.

Mögliche Werte:

**kommend**

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

**gehend**

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

**bei de**

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

Priorität

Legt die Priorität der *Paketfilter*-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 **0** in aufsteigender Reihenfolge an.


Mögliche Werte:

0..4294967295 ( $2^{32} - 1$ ) (Voreinstellung: 1)

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 [Netzsicherheit > Paketfilter > Routed-Firewall-Modus > Global](#) oder den Dialog [Netzsicherheit > Paketfilter > Routed-Firewall-Modus > Zuweisung](#).

Klicken Sie die Schaltfläche .

Mögliche Werte:

[markiert](#)

Die Regel ist aktiv.

[unmarkiert](#) (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 *Paketfilter*-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 [Netzsicherheit > Paketfilter > Routed-Firewall-Modus > Regel](#).

#### Regel-Index

Zeigt die fortlaufende Nummer der *Paketfilter*-Regel.

#### Interface

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

#### Richtung

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

Mögliche Werte:

*kommend*

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

*gehend*

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

*bei de*

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

#### Priorität

Zeigt die Priorität der *Paketfilter*-Regel. Das Gerät wendet die Regeln beginnend mit Priorität 0 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 *Paketfilter*-Regel beschränkt ist. Das Gerät wendet die *Paketfilter*-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 *Netzsicherheit > Paketfilter > Routed-Firewall-Modus > Regel* fest.

Log

Zeigt, ob das Gerät einen Eintrag in der System-Log-Datei erstellt, wenn das Gerät die *Paketfilter*-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 *Transparent-Firewall-Modus*-Paketfilter fest. Der *Transparent-Firewall-Modus*-Paketfilter enthält Regeln, die das Gerät nacheinander auf den Datenstrom auf seinen nicht-routenden Ports oder VLAN-Interfaces anwendet. Der *Transparent-Firewall-Modus*-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 *accept*. Das Gerät ermöglicht Ihnen, die Standard-Regel im Dialog *Netzsicherheit > Paketfilter > Transparent-Firewall-Modus > Global* zu ändern.

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

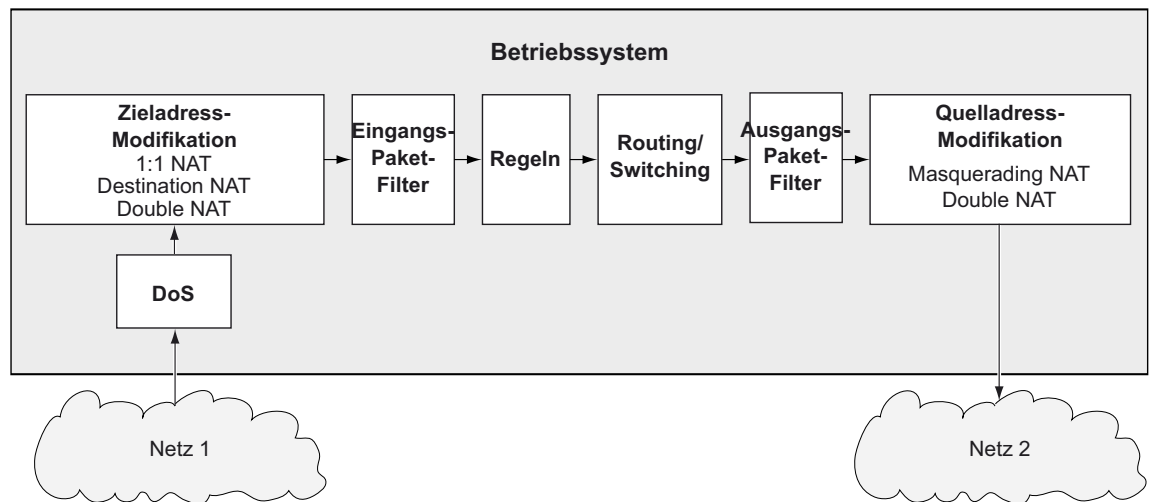


Abb. 2: Bearbeitungsreihenfolge der Datenpakete im Gerät

Das Menü enthält die folgenden Dialoge:

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

## 4.5.21 Paketfilter Global

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

In diesem Dialog legen Sie die globalen Einstellungen für den *Transparent-Firewall-Modus*-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:

**accept** (Voreinstellung)  
Das Gerät akzeptiert die Datenpakete.

**drop**  
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:

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

**unmarkiert**  
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 *Paketfilter*-Regeln von den im Gerät gespeicherten *Paketfilter*-Regeln unterscheiden.

Mögliche Werte:

*markiert*

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

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

*unmarkiert*

Das Gerät wendet die gespeicherten *Paketfilter*-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 [Netzsicherheit > Paketfilter > Transparent-Firewall-Modus > Zuweisung](#) 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 [Paketfilter](#)-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:

[accept](#) (Voreinstellung)

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

[drop](#)

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

[enforce-modbus](#)

Das Gerät wendet die in Spalte [Index DPI-Profil](#) festgelegte Regel auf die Datenpakete an.

Voraussetzung ist, dass in den Spalten [Quelle IP-Adresse](#), [Ziel IP-Adresse](#) und [Ziel Port](#) ein anderer Wert als [any](#) festgelegt ist.

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

[enforce-opc](#)

Das Gerät wendet die in Spalte *Index DPI-Profil* festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten *Quelle IP-Adresse*, *Ziel IP-Adresse* und *Ziel Port* ein anderer Wert als *any* festgelegt ist.

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

[enforce-ic104](#)

Das Gerät wendet die in Spalte *Index DPI-Profil* festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten *Quelle IP-Adresse*, *Ziel IP-Adresse* und *Ziel Port* ein anderer Wert als *any* festgelegt ist.

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

[enforce-dnp3](#)

Das Gerät wendet die in Spalte *Index DPI-Profil* festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten *Quelle IP-Adresse*, *Ziel IP-Adresse* und *Ziel Port* ein anderer Wert als *any* festgelegt ist.

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

[enforce-ethernetip](#)

Das Gerät wendet die in Spalte *Index DPI-Profil* festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten *Quelle IP-Adresse*, *Ziel IP-Adresse* und *Ziel Port* ein anderer Wert als *any* festgelegt ist.

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

[enforce-amp](#)

Das Gerät wendet die in Spalte *Index DPI-Profil* festgelegte Regel auf die Datenpakete an. Voraussetzung ist, dass in den Spalten *Quelle IP-Adresse*, *Ziel IP-Adresse* und *Ziel Port* ein anderer Wert als *any* 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 [Netzsicherheit > Asset](#) fest.

Mögliche Werte:

[any](#) (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: [00:11:22:33:44:55](#)

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 [Netzicherheit > Asset](#) fest.

Mögliche Werte:

[any](#) (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: [00: 11: 22: 33: 44: 55](#)

Name des Assets

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

### Ethertype

Legt das *Ethertype*-Schlüsselwort der MAC-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

[custom](#) (Voreinstellung)

Das Gerät wendet den in Spalte [Benutzerspezifischer Ether-type-Wert](#) festgelegten Wert an.

[apptalk](#)

[arp](#)

[ibnsna](#)

[ipv4](#)

[ipv6](#)

[ipxld](#)

[mplsnacast](#)

[mplsucast](#)

[netbios](#)

[novell](#)

[pppoedisc](#)

[rarp](#)

[pppoess](#)

[ipxnew](#)

[profinet](#)

[powerlink](#)

[ethercat](#)

[vlan8021q](#)

### 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 [Ether-type](#) der Wert [custom](#) festgelegt ist.

Mögliche Werte:

[0](#) (Voreinstellung)

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

1..5f

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.

600..ffff

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

VLAN-ID

Legt die VLAN-ID der Datenpakete fest, auf die das Gerät die Regel anwendet. Voraussetzung ist, dass in Spalte *Ether*type der Wert *vlan8021q* festgelegt ist.

Mögliche Werte:

*any* (Voreinstellung)

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

1..4042

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 *Netzsicherheit > Asset* fest.

Voraussetzungen:

- In Spalte *Ether*type ist der Wert *ipv4* festgelegt.
- In Spalte *Aktion* ist ein anderer Wert als *enforce-goose* festgelegt.

Mögliche Werte:

*any* (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: *192.168.112.0/25*

Ein der IP-Adresse vorangestelltes Ausrufezeichen (!) kehrt 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: *! 1.1.1.1* oder *! 192.168.112.0/25*

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 *Netzsicherheit > Asset* fest.

Voraussetzungen:

- In Spalte *Ether*type ist der Wert *ipv4* festgelegt.
- In Spalte *Aktion* ist ein anderer Wert als *enforce-goose* festgelegt.

Mögliche Werte:

[any](#) (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: [192.168.112.0/25](#)

Ein der IP-Adresse vorangestelltes Ausrufezeichen (!) kehrt 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: [!1.1.1.1](#) oder [!192.168.112.0/25](#)

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:

[any](#) (Voreinstellung)

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

[icmp](#)

Internet Control Message Protocol (RFC 792)

[igmp](#)

Internet Group Management Protocol

[ipip](#)

IP in IP tunneling (RFC 2003)

[tcp](#)

Transmission Control Protocol (RFC 793)

[udp](#)

User Datagram Protocol (RFC 768)

[esp](#)

IPsec Encapsulated Security Payload (RFC 2406)

[ah](#)

IPsec Authentication Header (RFC 2402)

[icmpv6](#)

Internet Control Message Protocol for IPv6

[<user-defined protocols>](#)

Das Gerät verarbeitet auch benutzerdefinierte Protokolle. Sie legen benutzerdefinierte Protokolle im Dialog [Netzicherheit > Protokoll](#) 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:

0 (Voreinstellung)

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

1.. 255

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 *Aktion* einer der folgenden Werte festgelegt ist:

- `enforce-modbus`
- `enforce-opc`
- `enforce-dnp3`
- `enforce-iec104`
- `enforce-amp`
- `enforce-ethernetip`

Mögliche Werte:

0 (Voreinstellung)

Das Gerät wendet keine Regel auf die Datenpakete an.

1.. 32

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

### Quelle Port

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

Voraussetzungen:

- In Spalte *Protokoll* ist der Wert `tcp` oder `udp` festgelegt.
- In Spalte *Aktion* ist ein anderer Wert als `enforce-goose` festgelegt.

Mögliche Werte:

`any` (Voreinstellung)

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

1.. 65535 (2<sup>16</sup> - 1)

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 `21`.
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel `21, 80, 110`.
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel `2000-3000`.
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel `21, 2000-3000, 65535`.

Die Spalte ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel `21, 2000-3000, 65535` eingeben, verwenden Sie 4 von 15 Zahlenwerten.

## Ziel Port

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

Voraussetzungen:

- In Spalte *Protokoll* ist der Wert `tcp` oder `udp` festgelegt.
- In Spalte *Aktion* ist ein anderer Wert als `enforce-goose` festgelegt.

Mögliche Werte:

`any` (Voreinstellung)

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

`1..65535 (216 - 1)`

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 `21`.
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel `21, 80, 110`.
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel `2000-3000`.
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel `21, 2000-3000, 65535`.

Die Spalte ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel `21, 2000-3000, 65535` 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:

`0` (Voreinstellung)

Keine Begrenzung der Datentransferrate.

`1..10000000 (107)`

Wenn die Datentransferrate auf dem Port den festgelegten Wert überschreitet, verwirft das Gerät überflüssige IP-Datenpakete. Voraussetzung ist, dass in Spalte *Burst-Size* ein Wert `>0` festgelegt ist. Die Maßeinheit des Limits legen Sie fest in Spalte *Einheit*.

## Burst-Size

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

Mögliche Werte:

`0` (Voreinstellung)

Keine Begrenzung des Datenvolumens.

`1..128`

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

Empfehlung:

- Wenn die Bandbreite bekannt ist:  
 $Burst-Size = \text{Bandbreite} \times \text{Zugelassene Dauer eines Bursts} / 8$
- Wenn die Bandbreite unbekannt ist:  
 $Burst-Size = 10 \times MTU$  (*Maximum Transmission Unit*) des Ports

Einheit

Legt die Maßeinheit fest für die in Spalte *Lastbegrenzung* festgelegte Datentransferrate.

Mögliche Werte:

- [pps](#) (Voreinstellung)  
Datenpakete pro Sekunde
- [kpbs](#)  
kByte pro Sekunde

Trap

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

Mögliche Werte:

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

Log

Aktiviert/deaktiviert die Protokollierung in der System-Log-Datei, wenn das Gerät die in dieser Tabellenzeile festgelegte *Paketfilter* Regel anwendet.



Mögliche Werte:

- [markiert](#)  
Die Protokollierung ist aktiv.  
Das Gerät erstellt einen Eintrag in der System-Log-Datei, wenn das Gerät die in dieser Tabellenzeile festgelegte *Paketfilter*-Regel anwendet. Siehe Dialog *Diagnose > Bericht > System-Log*.
- [unmarkiert](#) (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 *Netzsicherheit > Paketfilter > Transparent-Firewall-Modus > Global* oder den Dialog *Netzsicherheit > Paketfilter > Transparent-Firewall-Modus > Zuweisung*.
- Klicken Sie die Schaltfläche  .

Mögliche Werte:

- [markiert](#)  
Die Regel ist aktiv.
- [unmarkiert](#) (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 *Paketfilter*-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 *Paketfilter*-Regeln von den im Gerät gespeicherten *Paketfilter*-Regeln unterscheiden.

Mögliche Werte:

*markiert*

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

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

*unmarkiert*

Das Gerät wendet die gespeicherten *Paketfilter*-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 *Erstellen*, um einem nicht-routenden Port oder VLAN eine Regel zuzuweisen.

- In der Dropdown-Liste *Port/VLAN* wählen Sie den nicht-routenden Port oder das VLAN, auf den das Gerät die Regel anwendet. Wenn Sie in der Dropdown-Liste den Eintrag *VLAN: 1* wählen, wendet das Gerät die Regel auf alle Ports an, die mit VLAN 1 verknüpft sind.
- In der Dropdown-Liste *Richtung* wählen Sie aus, ob das Gerät die Regel auf empfangene Datenpakete oder auf zu sendende Datenpakete anwendet.
- In der Dropdown-Liste *Index* 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 [Netzicherheit > Paketfilter > Transparent-Firewall-Modus > Regel](#).

Index

Zeigt die fortlaufende Nummer der [Paketfilter](#)-Regel. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Typ

Zeigt, worauf das Gerät die Regel anwendet.

Mögliche Werte:


[Port](#)

Das Gerät wendet die [Paketfilter](#)-Regel bereits auf einen nicht-routenden Port an. Die zugehörige Port-Nummer finden Sie in Spalte [Port/VLAN](#).

[VLAN](#)

Das Gerät wendet die [Paketfilter](#)-Regel bereits auf ein nicht-routendes VLAN-Interface an. Die zugehörige VLAN-ID finden Sie in Spalte [Port/VLAN](#).

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:

[<Port - Nummer >](#)

Nummer des nicht-routenden Ports.

[VLAN: <VLAN I D>](#)

ID des VLANs.

Richtung

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

Mögliche Werte:

*kommend*

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

*gehend*

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

Priorität

Legt die Priorität der *Paketfilter*-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 0 in aufsteigender Reihenfolge an.


Mögliche Werte:

0 . 4294967295 ( $2^{32} - 1$ ) (Voreinstellung: 1)

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 *Netzsicherheit > Paketfilter > Transparent-Firewall-Modus > Global* oder den Dialog *Netzsicherheit > Paketfilter > Transparent-Firewall-Modus > Zuweisung*.

Klicken Sie die Schaltfläche  .

Mögliche Werte:

*markiert*

Die Regel ist aktiv.

*unmarkiert* (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 *Paketfilter*-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 *Netzsicherheit > Paketfilter > Transparent-Firewall-Modus > Regel*.

#### Index

Zeigt die fortlaufende Nummer der *Paketfilter*-Regel.

#### Richtung

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

Mögliche Werte:

##### kommend

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

##### gehend

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

#### Priorität

Zeigt die Priorität der *Paketfilter*-Regel. Das Gerät wendet die Regeln beginnend mit Priorität 0 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 *Ethertype*-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 *Ether-type* der Wert `cust om` 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 *Paketfilter*-Regel beschränkt ist. Das Gerät wendet die *Paketfilter*-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 *Netzicherheit > Paketfilter > Transparent-Firewall-Modus > Regel* 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 *Lastbegrenzung* festgelegte Datentransferrate.

Trap

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

Log

Zeigt, ob das Gerät einen Eintrag in der System-Log-Datei erstellt, wenn das Gerät die *Paketfilter*-Regel auf ein Datenpaket anwendet.

Aktiv

Zeigt, ob die Regel aktiv oder inaktiv ist.

## 4.6 Deep Packet Inspection

[Netzsicherheit > DPI]

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

Dieser Dialog ermöglicht Ihnen, die *DPI*-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 *Modbus Enforcer*-Einstellungen festzulegen und *Modbus TCP*-spezifische Profile zu definieren.

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 *Modbus Enforcer*-Profil (Kontrollkästchen in Spalte *Profil aktiv* ist markiert) wendet das Gerät die Profile auf den Datenstrom an.

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

### Information


Nicht angewendete Änderungen vorhanden

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

Mögliche Werte:

markiert

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

Um die noch ausstehenden Profile auf den Datenstrom anzuwenden, klicken Sie die Schaltfläche  .

---

### Anmerkung:

Wenn es im Gerät noch ausstehende Änderungen gibt, wendet das Gerät diese während des nächsten Systemstarts an.

unmarkiert

Die *Modbus Enforcer*-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 *Erstellen*, um eine Tabellenzeile hinzuzufügen.

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

Mögliche Werte:

1 . 32

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

 Löschen

Entfernt die ausgewählte Tabellenzeile.

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

 Kopieren

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

- Im Feld *Index* legen Sie eine neue Nummer fest, die das kopierte Profil identifiziert.

Mögliche Werte:

1 . 32

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

 Änderungen anwenden

Das Gerät wendet die festgelegten Profile auf den Datenstrom an.

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

### 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: `modbus`)

## Function Type

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

Mögliche Werte:

`read-only` (Voreinstellung)

Weist die *Funktionscodes* für die *read*-Funktion des *Modbus TCP* Protokolls zu.

1, 2, 3, 4, 7, 11, 12, 17, 20, 24

`read-write`

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

1, 2, 3, 4, 5, 6, 7, 11, 12, 15, 16, 17, 20, 21, 22, 23, 24

`programming`

Weist die *Funktionscodes* für die *programming*-Funktionen des *Modbus TCP* Protokolls zu.

1, 2, 3, 4, 5, 6, 7, 11, 12, 15, 16, 17, 20, 21, 22, 23, 24, 40, 42, 90, 125, 126

`alle`

Weist die *Funktionscodes* für jede Funktion des *Modbus TCP* Protokolls zu.

1, 2, . . . , 254, 255

`advanced`

Ermöglicht Ihnen, in Spalte *Function Code* benutzerdefinierte Werte festzulegen.

### Anmerkung:

Wenn Sie den Wert `advanced` festgelegt haben, lässt das Gerät zu Ihrer eigenen Sicherheit keine nachträglichen Änderungen dieses Wertes mehr zu. Das Gerät sorgt dafür, das Umstellen auf `read-only`, `read-write` oder `programming` zu verhindern. Dies vermeidet ein versehentliches Überschreiben der in Spalte *Function Code* manuell festgelegten Werte. Um eine Tabellenzeile mit dem Wert `read-only`, `read-write` oder `programming` festzulegen, fügen Sie eine Tabellenzeile hinzu.

## Function Code

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

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

- Wenn in Spalte *Function Type* der Wert `read-only`, `read-write` oder `programming` festgelegt ist, dann fügt das Gerät automatisch die zugehörigen *Funktionscodes* ein.
- Wenn in Spalte *Function Type* der Wert `advanced` 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 *Function Code*.
  - Der Dialog zeigt das Fenster *Function Code*. Siehe „[Function Code]“ auf Seite 161.
  - Wählen Sie in der Dropdown-Liste *Function Code* den gewünschten *Funktionscode*-Eintrag.
  - Klicken Sie die Schaltfläche *Hinzufügen*.
  - Um mehrere *Funktionscodes* hinzuzufügen, wiederholen Sie die zuvor beschriebenen Schritte.
  - Klicken Sie die Schaltfläche *Ok*.

Mögliche Werte:

<FC> | <AR>, <FC> | <AR>, ...

Das Gerät ermöglicht Ihnen, mehrere *Funktionscodes* und für manche *Funktionscodes* einen zusätzlichen Adressbereich festzulegen. Die Bedeutung der Nummern finden Sie im Abschnitt „Bedeutung der Function Code-Werte“ auf Seite 162.

– *Funktionscode* <FC> = 1..255

Sie trennen jeden *Funktionscode* jeweils durch ein Komma, zum Beispiel 1, 2, 3.

Für manche *Funktionscodes* ermöglicht Ihnen das Gerät, zusätzlich einen Adressbereich festzulegen. Sie trennen den Adressbereich vom *Funktionscode* mit einem senkrechten Strich (Pipe), zum Beispiel 1|128-255.

– *Adressbereich* <AR> = 0..65535 oder 0..65535|0..65535 (für *Funktionscodes*, die Lese- und Schreib-Adressbereiche erfordern)

Sie verbinden den Start- und Endwert des Bereichs mit einem Bindestrich, zum Beispiel 128-255.

Das Gerät bietet Ihnen auch die Möglichkeit, einen einzelnen Wert als Adressbereich angeben. Zum Beispiel ist das Festlegen des Adressbereichs 5-5 gleichbedeutend mit der einzelnen Adresse 5.

Kennung der Unit

Legt die *Modbus TCP*-Identifikationseinheit für das *Modbus Enforcer*-Profil fest.

Mögliche Werte:

`none` (Voreinstellung)

Das Gerät lässt Datenpakete ohne Identifikationseinheit zu.

0..255

Das Gerät lässt Datenpakete mit der festgelegten Identifikationseinheit zu.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Eine einzelne *Modbus TCP*-Identifikationseinheit mit einem einzelnen numerischen Wert, zum Beispiel 1.
- Mehrere *Modbus TCP*-Identifikationseinheiten mit numerischen Werten, die durch ein Komma getrennt sind, zum Beispiel 1, 2, 3.

Plausibilitätsprüfung

Aktiviert/deaktiviert die Plausibilitätsprüfung für Datenpakete.

Mögliche Werte:

`markiert` (Voreinstellung)

Die Plausibilitätsprüfung ist aktiv.

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

`unmarkiert`

Die Plausibilitätsprüfung ist inaktiv.

Ausnahme

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

Mögliche Werte:

`markiert`

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 *Modbus TCP*-Verbindung.

`unmarkiert` (Voreinstellung)

Das Senden einer *Exception*-Antwort ist inaktiv. Die *Modbus TCP*-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:

**markiert** (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.

**unmarkiert**

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

#### Profil aktiv

Aktiviert/deaktiviert das Profil.

Mögliche Werte:

**markiert**

Das Profil ist aktiv.

Das Gerät wendet die in dieser Tabellenzeile festgelegten *Modbus Enforcer*-Profile auf den Datenstrom an.

**unmarkiert** (Voreinstellung)

Das Profil ist inaktiv.

### [Function Code]

#### Function Code

Legt die *Funktionscodes* für das betreffende *Modbus Enforcer*-Profil fest.

Die Bedeutung der Nummern finden Sie im Abschnitt „Bedeutung der Function Code-Werte“ auf [Seite 162](#).

#### Adressbereich Lesen

Legt den Lese-Adressbereich für bestimmte *Funktionscodes* fest. Siehe Abschnitt „Bedeutung der Function Code-Werte“ auf [Seite 162](#).

Mögliche Werte:

0 . 65535 (2<sup>16</sup> - 1)

#### Adressbereich Schreiben

Legt den Schreib-Adressbereich für bestimmte *Funktionscodes* fest. Siehe Abschnitt „Bedeutung der Function Code-Werte“ auf [Seite 162](#).

Mögliche Werte:

0 . 65535 (2<sup>16</sup> - 1)

#### Hinzufügen

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



Löscht den Eintrag aus dem Feld *Function Code*.

### Bedeutung der Function Code-Werte

#	Bedeutung	Adressbereich (Lesen)	Adressbereich (Schreiben)
1	Read Coils	<0 . 65535>	-
2	Read Discrete Inputs	<0 . 65535>	-
3	Read Holding Registers	<0 . 65535>	-
4	Read Input Registers	<0 . 65535>	-
5	Write Single Coil	-	<0 . 65535>
6	Write Single Register	-	<0 . 65535>
7	Read Exception Status	-	-
8	Diagnostic	-	-
11	Get Comm Event Counter	-	-
12	Get Comm Event Log	-	-
13	Program (584/984)	-	-
14	Pol I (584/984)	-	-
15	Write Multiple Coils	-	<0 . 65535>
16	Write Multiple Registers	-	<0 . 65535>
17	Report Slave ID	-	-
20	Read File Record	-	-
21	Write File Record	-	-
22	Mask Write Register	-	<0 . 65535>
23	Read/Write Multiple Registers	<0 . 65535>	<0 . 65535>
24	Read FIFO Queue	<0 . 65535>	-
40	Program (Concept)	-	-
42	Concept Symbol Table	-	-
43	Encapsulated Interface Transport	-	-
48	Advantech Co. Ltd. - Management Functions	-	-
66	Scan Data Inc. - Expanded Read Holding Registers	-	-
67	Scan Data Inc. - Expanded Write Holding Registers	-	-
90	Unity Programming/OFS	-	-
100	Scattered Register Read	-	-
125	Schneider Electric - Firmware	-	-

## 4.6.2 Deep Packet Inspection - OPC Enforcer

[Netzsicherheit > DPI > OPC Enforcer]

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

*OPC* ist ein Integrationsprotokoll für industrielle Umgebungen. *OPC Enforcer* 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 *Routing* auf dem Router-Interface.

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

### Funktion

Nicht angewendete Änderungen vorhanden

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

Mögliche Werte:

markiert

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

Um die noch ausstehenden Profile auf den Datenstrom anzuwenden, klicken Sie die Schaltfläche  .

---

#### Anmerkung:

Wenn es im Gerät noch ausstehende Änderungen gibt, wendet das Gerät diese während des nächsten Systemstarts an.

unmarkiert

Die *OPC Enforcer*-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 *Erstellen*, um eine Tabellenzeile hinzuzufügen.

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

Mögliche Werte:

1 . 32

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



Löschen

Entfernt die ausgewählte Tabellenzeile.

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



Kopieren

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

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

Mögliche Werte:

1 . 32

Nach Klicken der Schaltfläche *Ok* fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld *Index* 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: *opc*)

#### Plausibilitätsprüfung

Aktiviert/deaktiviert die Plausibilitätsprüfung für Datenpakete.

Mögliche Werte:

`markiert` (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.

`unmarkiert`

Die Plausibilitätsprüfung ist inaktiv.

#### Fragmentprüfung

Aktiviert/deaktiviert die Fragment-Prüfung der Datenpakete.

Mögliche Werte:

`markiert` (Voreinstellung)

Die Fragment-Prüfung ist aktiv.

Das Gerät prüft die Datenpakete hinsichtlich der Fragment-Eigenschaften.

`unmarkiert`

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:

`1..300` (Voreinstellung: 5)

`0`

Der Wert `0` deaktiviert die Funktion. Die *OPC*-Datenverbindung bleibt ohne Zeitbegrenzung aufgebaut.

#### Profil aktiv

Aktiviert/deaktiviert das Profil.

Mögliche Werte:

`markiert`

Das Profil ist aktiv.

Das Gerät wendet die in dieser Tabellenzeile festgelegten *OPC Enforcer*-Profile auf den Datenstrom an.

`unmarkiert`

Das Profil ist inaktiv.

## 4.6.3 Deep Packet Inspection - DNP3 Enforcer

[Netzsicherheit > DPI > DNP3 Enforcer]

Dieser Dialog ermöglicht Ihnen, die *DNP3 Enforcer*- (*Distributed Network Protocol v3 Enforcer*)-Einstellungen festzulegen und *DNP3 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 *DNP3 Enforcer* 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 *DNP3 Enforcer*-Profil (Kontrollkästchen in Spalte *Profil aktiv* ist markiert) wendet das Gerät die Profile auf den Datenstrom an.

- Das Gerät lässt ausschließlich Datenpakete zu, welche die in Spalte *Function Code-Liste* festgelegten *Funktionscodes* enthalten.
- Das Gerät weist Datenpakete zurück, die abweichende *Function-Codes* enthalten, welche nicht in Spalte *Function Code-Liste* 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 *DNP3 Enforcer*-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 *DNP3 Enforcer*-Profile von den im Gerät gespeicherten Profilen unterscheiden.

Mögliche Werte:

**markiert**

Mindestens eines der aktiven *DNP3 Enforcer*-Profile, die im Gerät gespeichert sind, enthält geänderte Einstellungen.

Um die noch ausstehenden Profile auf den Datenstrom anzuwenden, klicken Sie die Schaltfläche .

---

#### Anmerkung:

Wenn es im Gerät noch ausstehende Änderungen gibt, wendet das Gerät diese während des nächsten Systemstarts an.

**unmarkiert**

Die *DNP3 Enforcer*-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 *Erstellen*, um eine Tabellenzeile hinzuzufügen.

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

Mögliche Werte:

1 . 32

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

 Löschen

Entfernt die ausgewählte Tabellenzeile.



Kopieren

Öffnet das Fenster [Kopieren](#), um eine bestehende Tabellenzeile zu kopieren. Voraussetzung ist, dass die Tabellenzeile für das zu kopierende Profil ausgewählt ist.

- Im Feld [Index](#) legen Sie eine neue Nummer fest, die das kopierte Profil identifiziert.

Mögliche Werte:

1 . 32

Nach Klicken der Schaltfläche [Ok](#) fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld [Index](#) 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..32 Zeichen  
(Voreinstellung: [dnp3](#))

#### Function Code-Liste

Zeigt die *Funktionscodes* für das [DNP3 Enforcer](#)-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 [Function Code-Liste](#).

Der Dialog zeigt das Fenster [Function Code-Liste](#). Siehe „[\[Function Code-Liste\]](#)“ auf [Seite 170](#).

Wählen Sie in der Dropdown-Liste [Function Code-Liste](#) den gewünschten *Funktionscode*-Eintrag.

Klicken Sie die Schaltfläche [Hinzufügen](#).

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

Klicken Sie die Schaltfläche [Ok](#).

Mögliche Werte:

0 . 255

Die Bedeutung der Nummern finden Sie im Abschnitt „[Bedeutung der Function Code-Liste-Werte](#)“ auf [Seite 170](#).

## Index der Standard-Objektliste

Legt die in der *Standard-Objektliste* verwendeten *Index-Nummern* fest.

Mögliche Werte:

`all` (Voreinstellung)

Das Gerät wendet das *DNP3 Enforcer*-Profil auf jedes Datenpaket an, unabhängig von der *Index-Nummer*.

`1..317`

Das Gerät wendet das *DNP3 Enforcer*-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 `1`.
- Mehrere *Index-Nummern* mit numerischen Werten, die durch ein Komma getrennt sind, zum Beispiel `1, 2, 3`.
- Einen Bereich mit numerischen Werten, welche durch einen Bindestrich verbunden sind, zum Beispiel `7-25`.
- Außerdem können Sie einzelne Zahlenwerte und Bereiche kombinieren, zum Beispiel `2, 7-25, 56`.

`none`

Das Gerät wendet die *Index-Nummer* nicht auf das *DNP3 Enforcer*-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:

`markiert` (Voreinstellung)

Die CRC-Prüfung ist aktiv.

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

`unmarkiert`

Die CRC-Prüfung ist inaktiv.

## Plausibilitätsprüfung

Aktiviert/deaktiviert die Plausibilitätsprüfung für Datenpakete.

Mögliche Werte:

`markiert` (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.

`unmarkiert`

Die Plausibilitätsprüfung ist inaktiv.

## Verkehr von und zur Outstation prüfen

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

Mögliche Werte:

`markiert`

Die Prüfung der Datenpakete von der *Outstation* ist aktiv.

`unmarkiert`

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:

**markiert** (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.

**unmarkiert**

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

Profil aktiv

Aktiviert/deaktiviert das Profil.

Mögliche Werte:

**markiert**

Das Profil ist aktiv.

Das Gerät wendet die in dieser Tabellenzeile festgelegten *DNP3 Enforcer*-Profile auf den Datenstrom an.

**unmarkiert**

Das Profil ist inaktiv.

**[Function Code-Liste]**

Function Code-Liste

Legt die *Funktionscodes* für das betreffende *DNP3 Enforcer*-Profil fest.

Die Bedeutung der Nummern finden Sie im Abschnitt „Bedeutung der Function Code-Liste-Werte“ auf Seite 170.

Hinzufügen

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



Löscht den Eintrag aus dem Feld *Function Code-Liste*.

**Bedeutung der Function Code-Liste-Werte**

#	Bedeutung
0	Confirm
1	Read
2	Write
3	Select
4	Operate

#	Bedeutung
5	Direct Operate
6	Direct Operate-No Response Required
7	Freeze
8	Freeze-No Response Required
9	Freeze Clear
10	Freeze Clear-No Response Required
11	Freeze at Time
12	Freeze at Time-No Response Required
13	Cold Restart
14	Warm Restart
15	Initialize Data
16	Initialize Application
17	Start Application
18	Stop Application
19	Save Configuration
20	Enable Unsolicited Messages
21	Disable Unsolicited Messages
22	Assign Class
23	Delay Measurement
24	Record Current Time
25	Open File
26	Close File
27	Delete File
28	Get File Information
29	Authenticate File
30	Abort File Transfer
31	Active Configuration
32	Authentication Request
33	Authenticate Request-No Acknowledgment
129	Response
130	Unsolicited Response
131	Authentication Response

## 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:

- *Typ*
- *Gruppen-Nr.*
- *Variation*
- *Funktion*
- *Qualifier*
- *Länge*
- *Funktionsname*

Auf Grundlage der Norm IEEE 1815-2012 lässt die Funktion *DNP3 Enforcer* 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 *Erstellen*, um eine Tabellenzeile hinzuzufügen.

- In der Dropdown-Liste *Index* wählen Sie die *Index-Nummer* des Profils.
- Im Feld *Objekt-Index* legen Sie die *Index-Nummer* des Objekts fest.  
Mögliche Werte:  
1 . 256
- In der Dropdown-Liste *Typ* wählen Sie den Typ der Nachricht.  
Mögliche Werte:  
request  
response
- Im Feld *Gruppen-Nr.* legen Sie einen Mittelwert für den Klassifizierungstyp oder für die Klassifizierungstypen von Datenpaketen in einer Nachricht fest. Voraussetzung ist, dass im Feld *Typ* ein gültiger Wert festgelegt ist.  
Mögliche Werte:  
0 . 255
- Im Feld *Variation* legen Sie die *Variation-Nummer* fest. Voraussetzung ist, dass im Feld *Gruppen-Nr.* ein gültiger Wert festgelegt ist.  
Mögliche Werte:  
0 . 255

- Im *Funktion*-Feld legen Sie den *Funktionscode* fest. Der *Funktionscode* kennzeichnet den Zweck der Nachricht. Voraussetzung ist, dass im Feld *Variation* ein gültiger Wert festgelegt ist.  
Mögliche Werte:  
0 . 128  
*Request-Nachrichten* von den *Mastern*. Legen Sie einen einzelnen Zahlenwert fest, zum Beispiel 1.  
129 . 255  
*Response-Nachrichten* von den *Outstations*. Legen Sie einen einzelnen Zahlenwert fest, zum Beispiel 254.
- Im Feld *Qualifier* legen Sie den *Qualifier-Code* jeweils ein Paar der Felder *Gruppen-Nr.*, *Variation* und *Funktion* 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 *Funktion* ein gültiger Wert festgelegt ist.  
Mögliche Werte:  
0x00 . 0xf f  
Mit durch Komma getrennten hexadezimalen Werten legen Sie mehrere individuelle *Qualifier-Codes* für einen Satz der jeweiligen Felder *Gruppen-Nr.*, *Variation* und *Funktion* fest.

Nach Klicken der Schaltfläche *Ok* fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist dieser Tabellenzeile die in den Feldern *Index*, *Objekt-Index*, *Typ*, *Gruppen-Nr.*, *Variation*, *Funktion* und *Qualifier* 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:

*request*

Erstellt in der Objektliste ein Objekt *Request-Nachricht*.

*response*

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 *Typ* ein gültiger Wert festgelegt ist.

Mögliche Werte:

0 . 255

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

### Variation

Legt die *Variation-Nummer* fest. Voraussetzung ist, dass im Feld *Gruppen-Nr.* ein gültiger Wert festgelegt ist. Das Gerät wendet das *DNP3 Enforcer*-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 *Gruppen-Nr.* verfügt über eine Folge von *Variation-Nummern*.

Mögliche Werte:

0 . 255

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Mit einem einzelnen Zahlenwert legen Sie eine einzelne *Variation-Nummer* fest, zum Beispiel 1.
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Bereich fest, zum Beispiel 0-55.

### Funktion

Der *Funktionscode* kennzeichnet den Zweck der Nachricht. Voraussetzung ist, dass im Feld *Variation* ein gültiger Wert festgelegt ist. Das Gerät wendet das *DNP3 Enforcer*-Profil ausschließlich auf Datenpakete an, die den festgelegten Wert enthalten.

Mögliche Werte:

0 . 128

*Request-Nachrichten* von den *Mastern*. Legen Sie einen einzelnen Zahlenwert fest, zum Beispiel 1.

129 . 255

*Response-Nachrichten* von den *Outstations*. Legen Sie einen einzelnen Zahlenwert fest, zum Beispiel 254.

### Qualifier

Legt den *Qualifier-Code* für ein Paar der Felder *Gruppen-Nr.*, *Variation* und *Funktion* 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 *Funktion* ein gültiger Wert festgelegt ist. Das Gerät wendet das *DNP3 Enforcer*-Profil ausschließlich auf Datenpakete an, die den festgelegten Wert enthalten.

Mögliche Werte:

0x00 . 0xff

Mit durch Komma getrennten hexadezimalen Werten legen Sie mehrere individuelle *Qualifier-Codes* für einen Satz der jeweiligen Felder *Gruppen-Nr.*, *Variation* und *Funktion* fest.

### Länge

Legt die Länge für das Objekt fest (optional). Voraussetzung ist, dass im Feld *Funktion* ein gültiger Wert festgelegt ist. Das Gerät wendet das *DNP3 Enforcer*-Profil ausschließlich auf Datenpakete an, die den festgelegten Wert enthalten.

Mögliche Werte:

0 . 255

Legen Sie einen einzelnen Zahlenwert fest, zum Beispiel 1.

byte\_2

Das zweite Byte der Objektdaten enthält die Länge des verbleibenden Teils der Daten.

**single\_bit\_packed**

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.

**double\_bit\_packed**

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.

**variation**

Kennzeichnet die Länge des Objekts.

Funktionsname

Legt den Namen des *Funktionscodes* fest (optional). Voraussetzung ist, dass im Feld *Funktion* ein gültiger Wert festgelegt ist.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen
- Das Gerät lässt Datenpakete mit folgenden *Function-Namen* zu:
- READ
- WRITE
- SELECT

**[Index der Standard-Objektliste]**

Tab. 1: Request-Nachrichten

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
1	0	209- 239	1	READ	-	0x00
2	0	240	1	READ	-	0x00
3	0	240	2	WRITE	byte_2	0x00
4	0	241- 243	1	READ	-	0x00
5	0	245- 247	1	READ	-	0x00
6	0	245- 247	2	WRITE	byte_2	0x00
7	0	248- 250	1	READ	-	0x00
8	0	252	1	READ	-	0x00
9	0	254	1	READ	-	0x00 0x06
10	0	255	1	READ	-	0x00 0x06
11	1	0- 2	1	READ	-	0x00 0x01 0x06 0x17 0x28
12	1	0	22	ASSIGN CLASS	-	0x00 0x01 0x06 0x17 0x28

Tab. 1: Request-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
13	2	0-3	1	READ	-	0x06 0x07 0x08
14	3	0-2	1	READ	-	0x00 0x01 0x06 0x17 0x28
15	3	0	22	ASSIGN CLASS	-	0x00 0x01 0x06 0x17 0x28
16	4	0-3	1	READ	-	0x06 0x07 0x08
17	10	0	1	READ	-	0x00 0x01 0x06 0x17 0x28
18	10	0	22	ASSIGN CLASS	-	0x00 0x01 0x06 0x17 0x28
19	10	1	2	WRITE	single_bit_packed	0x00 0x01
20	10	2	1	READ	-	0x00 0x01 0x06 0x17 0x28
21	11	0-2	1	READ	-	0x06 0x07 0x08
22	12	0	22	ASSIGN_CLASS	-	0x00 0x01 0x06 0x17 0x28
23	12	1	3	SELECT	11	0x00 0x01 0x17 0x28
24	12	1	4	OPERATE	11	0x00 0x01 0x17 0x28

Tab. 1: Request-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
25	12	1	5	DI RECT_OPERATE	11	0x00 0x01 0x17 0x28
26	12	1	6	DI RECT_OPERATE_NR	11	0x00 0x01 0x17 0x28
27	12	2	3	SELECT	11	0x07 0x08
28	12	2	4	OPERATE	11	0x07 0x08
29	12	2	5	DI RECT_OPERATE	11	0x07 0x08
30	12	2	6	DI RECT_OPERATE_NR	11	0x07 0x08
31	12	3	3	SELECT	si ngl e_bi t_packed	0x00 0x01
32	12	3	4	OPERATE	si ngl e_bi t_packed	0x00 0x01
33	12	3	5	DI RECT_OPERATE	si ngl e_bi t_packed	0x00 0x01
34	12	3	6	DI RECT_OPERATE_NR	si ngl e_bi t_packed	0x00 0x01
35	13	0-2	1	READ	-	0x06 0x07 0x08
36	20	0-2	1	READ	-	0x00 0x01 0x06 0x17 0x28
37	20	5-6	1	READ	-	0x00 0x01 0x06 0x17 0x28
38	20	0	7	I MMEDI ATE_FREEZE	-	0x00 0x01 0x06 0x17 0x28
39	20	0	8	I MMEDI ATE_FREEZE_NR	-	0x00 0x01 0x06 0x17 0x28

Tab. 1: Request-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
40	20	0	9	FREEZE_CLEAR	-	0x00 0x01 0x06 0x17 0x28
41	20	0	10	FREEZE_CLEAR_NR	-	0x00 0x01 0x06 0x17 0x28
42	20	0	11	FREEZE_AT_TIME	-	0x00 0x01 0x06 0x17 0x28
43	20	0	12	FREEZE_AT_TIME_NR	-	0x00 0x01 0x06 0x17 0x28
44	20	0	22	ASSIGN_CLASS	-	0x00 0x01 0x06 0x17 0x28
45	21	0-2	1	READ	-	0x00 0x01 0x06 0x17 0x28
46	21	5-6	1	READ	-	0x00 0x01 0x06 0x17 0x28
47	21	9-10	1	READ	-	0x00 0x01 0x06 0x17 0x28
48	21	0	22	ASSIGN_CLASS	-	0x00 0x01 0x06 0x17 0x28
49	22	0-2	1	READ	-	0x06 0x07 0x08
50	22	5-6	1	READ	-	0x06 0x07 0x08

Tab. 1: Request-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
51	23	0-2	1	READ	-	0x06 0x07 0x08
52	23	5-6	1	READ	-	0x06 0x07 0x08
53	30	0-6	1	READ	-	0x00 0x01 0x06 0x17 0x28
54	30	0	7	IMMEDIATE_FREEZE	-	0x00 0x01 0x06 0x17 0x28
55	30	0	8	IMMEDIATE_FREEZE_NR	-	0x00 0x01 0x06 0x17 0x28
56	30	0	11	FREEZE_AT_TIME	-	0x00 0x01 0x06 0x17 0x28
57	30	0	12	FREEZE_AT_TIME_NR	-	0x00 0x01 0x06 0x17 0x28
58	30	0	22	ASSIGN_CLASS	-	0x00 0x01 0x06 0x17 0x28
59	31	0-8	1	READ	-	0x00 0x01 0x06 0x17 0x28
60	31	0	22	ASSIGN_CLASS	-	0x00 0x01 0x06 0x17 0x28
61	32	0-8	1	READ	-	0x06 0x07 0x08

Tab. 1: Request-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
62	33	0-8	1	READ	-	0x06 0x07 0x08
63	34	0-3	1	READ	-	0x00 0x01 0x06
64	34	1	2	VRI TE	2	0x00 0x01 0x17 0x28
65	34	2	2	VRI TE	4	0x00 0x01 0x17 0x28
66	34	3	2	VRI TE	4	0x00 0x01 0x17 0x28
67	40	0	1	READ	-	0x00 0x01 0x06
68	40	0	22	ASSIGN_CLASS	-	0x00 0x01 0x06 0x17 0x28
69	40	1-4	1	READ	-	0x00 0x01 0x06 0x17 0x28
70	41	0	22	ASSIGN_CLASS	-	0x00 0x01 0x06 0x17 0x28
71	41	1	3	SELECT	5	0x00 0x01 0x17 0x28
72	41	2	3	SELECT	3	0x00 0x01 0x17 0x28
73	41	3	3	SELECT	5	0x00 0x01 0x17 0x28

Tab. 1: Request-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
74	41	1	4	OPERATE	5	0x00 0x01 0x17 0x28
75	41	2	4	OPERATE	3	0x00 0x01 0x17 0x28
76	41	3	4	OPERATE	5	0x00 0x01 0x17 0x28
77	41	1	5	DI RECT_OPERATE	5	0x00 0x01 0x17 0x28
78	41	2	5	DI RECT_OPERATE	3	0x00 0x01 0x17 0x28
79	41	3	5	DI RECT_OPERATE	5	0x00 0x01 0x17 0x28
80	41	1	6	DI RECT_OPERATE_NR	5	0x00 0x01 0x17 0x28
81	41	2	6	DI RECT_OPERATE_NR	3	0x00 0x01 0x17 0x28
82	41	3	6	DI RECT_OPERATE_NR	5	0x00 0x01 0x17 0x28
83	42	0-8	1	READ	-	0x06 0x07 0x08
84	43	0-8	1	READ	-	0x06 0x07 0x08
85	50	1	1	READ	-	0x07
86	50	1	2	WRITE	6	0x07
87	50	2	11	FREEZE_AT_TIME	10	0x07
88	50	2	12	FREEZE_AT_TIME_NR	10	0x07
89	50	3	2	WRITE	10	0x07

Tab. 1: Request-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
90	50	4	1	READ	-	0x00 0x01 0x06 0x17 0x28
91	50	4	2	VRI TE	11	0x00 0x01 0x17 0x28
92	60	1	1	READ	-	0x06
93	60	2-4	1	READ	-	0x06 0x07 0x08
94	60	1-4	22	ASSI GN_CLASS	-	0x06
95	60	2-4	20	ENABLE_UNSQLI CI TED	-	0x06
96	60	2-4	21	DI SABLE_UNSQLI CI TED	-	0x06
97	70	2	29	FI LE_AUTHENTI CATE	QC_5B_count_1	0x5B
98	70	3	25	OPEN_FI LE	QC_5B_count_1	0x5B
99	70	3	27	DELETE_FI LE	QC_5B_count_1	0x5B
100	70	4	26	CLOSE_FI LE	QC_5B_count_1	0x5B
101	70	4	30	FI LE_ABORT	QC_5B_count_1	0x5B
102	70	5-6	1	READ	QC_5B_count_1	0x5B
103	70	5	2	VRI TE	QC_5B_count_1	0x5B
104	70	7	28	GET_FI LE_I NFORMATI ON	QC_5B_count_1	0x5B
105	70	8	31	ACTI VATE_CONFI GURATI ON	QC_5B_count_1	0x5B
106	80	1	1	READ	-	0x00 0x01
107	80	1	2	VRI TE	si ngl e_bi t_packed	0x00 0x01
108	81	1	1	READ	-	0x00 0x01
109	82	1	1	READ	-	0x00 0x01
110	83	1	1	READ	-	0x00 0x01
111	85	0	1	READ	-	0x06
112	85	1	1	READ	-	0x00 0x01 0x06 0x17 0x28
113	85	1	2	VRI TE	QC_5B	0x5B
114	86	0	22	ASSI GN_CLASS	-	0x00 0x01 0x06 0x17 0x28

Tab. 1: Request-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
115	86	1-3	1	READ	-	0x00 0x01 0x06 0x17 0x28
116	86	1	2	VRI TE	QC_5B	0x5B
117	86	3	2	VRI TE	QC_5B	0x5B
118	87	0	1	READ	-	0x06
119	87	1	1	READ	-	0x00 0x01 0x06 0x17 0x28
120	87	1	2	VRI TE	QC_5B	0x5B
121	87	1	3	SELECT	QC_5B	0x5B
122	87	1	4	OPERATE	QC_5B	0x5B
123	87	1	5	DI RECT_OPERATE	QC_5B	0x5B
124	87	1	6	DI RECT_OPERATE_NR	QC_5B	0x5B
125	88	0-1	1	READ	-	0x06 0x07 0x08
126	90	1	16	I NI TI ALI ZE_APPLI CATI ON	QC_5B	0x5B
127	90	1	17	START_APPLI CATI ON	QC_5B	0x5B
128	90	1	18	STOP_APPLI CATI ON	QC_5B	0x5B
129	101	1-3	1	READ	-	0x00 0x01 0x06 0x17 0x28
130	102	1	1	READ	-	0x00 0x01 0x03 0x04 0x05 0x06 0x17 0x28
131	102	1	2	VRI TE	1	0x00 0x01 0x03 0x04 0x05 0x17 0x28

Tab. 1: Request-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
132	110	128	1	READ	-	0x00 0x01 0x03 0x04 0x05 0x06 0x17 0x28
133	110	128	2	VRI TE	vari ati on	0x00 0x01 0x03 0x04 0x05 0x17 0x28
134	110	128	31	ACTI VATE_CONFI GURATI ON	vari ati on	0x5B
135	111	128	1	READ	-	0x06
136	112	128	2	VRI TE	vari ati on	0x00 0x01 0x17 0x28
137	113	0	1	READ	-	0x00 0x01 0x17 0x28
138	113	0	22	ASSI GN_CLASS	-	0x00 0x01 0x06 0x17 0x28

Tab. 2: Response-Nachrichten

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
139	0	209- 239	129	RESPONSE	byte_2	0x00 0x17
140	0	240	129	RESPONSE	byte_2	0x00 0x17
141	0	241- 243	129	RESPONSE	byte_2	0x00 0x17
142	0	245- 247	129	RESPONSE	byte_2	0x00 0x17
143	0	248- 250	129	RESPONSE	byte_2	0x00 0x17
144	0	252	129	RESPONSE	byte_2	0x00 0x17
145	0	255	129	RESPONSE	byte_2	0x00 0x17

Tab. 2: Response-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
146	1	1	129	RESPONSE	single_bit_packed	0x00 0x01 0x17 0x28
147	1	2	129	RESPONSE	1	0x00 0x01 0x17 0x28
148	2	1	129	RESPONSE	1	0x17 0x28
149	2	2	129	RESPONSE	7	0x17 0x28
150	2	3	129	RESPONSE	3	0x17 0x28
151	2	1	130	UNSOLICITED_RESPONSE	1	0x17 0x28
152	2	2	130	UNSOLICITED_RESPONSE	7	0x17 0x28
153	2	3	130	UNSOLICITED_RESPONSE	3	0x17 0x28
154	3	1	129	RESPONSE	double_bit_packed	0x00 0x01 0x17 0x28
155	3	2	129	RESPONSE	1	0x00 0x01 0x17 0x28
156	4	1	129	RESPONSE	1	0x17 0x28
157	4	2	129	RESPONSE	7	0x17 0x28
158	4	3	129	RESPONSE	3	0x17 0x28
159	4	1	130	UNSOLICITED_RESPONSE	1	0x17 0x28
160	4	2	130	UNSOLICITED_RESPONSE	7	0x17 0x28
161	4	3	130	UNSOLICITED_RESPONSE	3	0x17 0x28
162	10	2	129	RESPONSE	1	0x00 0x01 0x17 0x28
163	11	1	129	RESPONSE	1	0x17 0x28
164	11	2	129	RESPONSE	7	0x17 0x28

Tab. 2: Response-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
165	11	1	130	UNSOLICITATED_RESPONSE	1	0x17 0x28
166	11	2	130	UNSOLICITATED_RESPONSE	7	0x17 0x28
167	12	1	129	RESPONSE	11	0x00 0x01 0x17 0x28
168	12	2	129	RESPONSE	11	0x07 0x08
169	12	3	129	RESPONSE	single_bit_packed	0x00 0x01
170	13	1	129	RESPONSE	1	0x17 0x28
171	13	2	129	RESPONSE	7	0x17 0x28
172	13	1	130	UNSOLICITATED_RESPONSE	1	0x17 0x28
173	13	2	130	UNSOLICITATED_RESPONSE	7	0x17 0x28
174	20	1	129	RESPONSE	5	0x00 0x01 0x17 0x28
175	20	2	129	RESPONSE	3	0x00 0x01 0x17 0x28
176	20	5	129	RESPONSE	4	0x00 0x01 0x17 0x28
177	20	6	129	RESPONSE	2	0x00 0x01 0x17 0x28
178	21	1	129	RESPONSE	5	0x00 0x01 0x17 0x28
179	21	2	129	RESPONSE	3	0x00 0x01 0x17 0x28
180	21	5	129	RESPONSE	4	0x00 0x01 0x17 0x28

Tab. 2: Response-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
181	21	6	129	RESPONSE	2	0x00 0x01 0x17 0x28
182	21	9	129	RESPONSE	4	0x00 0x01 0x17 0x28
183	21	10	129	RESPONSE	2	0x00 0x01 0x17 0x28
184	22	1	129	RESPONSE	5	0x17 0x28
185	22	2	129	RESPONSE	3	0x17 0x28
186	22	1	130	UNSOLI CI TED_RESPONSE	5	0x17 0x28
187	22	2	130	UNSOLI CI TED_RESPONSE	3	0x17 0x28
188	22	5	129	RESPONSE	11	0x17 0x28
189	22	6	129	RESPONSE	9	0x17 0x28
190	22	5	130	UNSOLI CI TED_RESPONSE	11	0x17 0x28
191	22	6	130	UNSOLI CI TED_RESPONSE	9	0x17 0x28
192	23	1	129	RESPONSE	5	0x17 0x28
193	23	2	129	RESPONSE	3	0x17 0x28
194	23	1	130	UNSOLI CI TED_RESPONSE	5	0x17 0x28
195	23	2	130	UNSOLI CI TED_RESPONSE	3	0x17 0x28
196	23	5	129	RESPONSE	11	0x17 0x28
197	23	6	129	RESPONSE	9	0x17 0x28
198	23	5	130	UNSOLI CI TED_RESPONSE	11	0x17 0x28
199	23	6	130	UNSOLI CI TED_RESPONSE	9	0x17 0x28
200	30	1	129	RESPONSE	5	0x00 0x01 0x17 0x28

Tab. 2: Response-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
201	30	2	129	RESPONSE	3	0x00 0x01 0x17 0x28
202	30	3	129	RESPONSE	4	0x00 0x01 0x17 0x28
203	30	4	129	RESPONSE	2	0x00 0x01 0x17 0x28
204	30	5	129	RESPONSE	5	0x00 0x01 0x17 0x28
205	30	6	129	RESPONSE	9	0x00 0x01 0x17 0x28
206	31	1	129	RESPONSE	5	0x00 0x01 0x17 0x28
207	31	2	129	RESPONSE	3	0x00 0x01 0x17 0x28
208	31	3	129	RESPONSE	11	0x00 0x01 0x17 0x28
209	31	4	129	RESPONSE	9	0x00 0x01 0x17 0x28
210	31	5	129	RESPONSE	4	0x00 0x01 0x17 0x28
211	31	6	129	RESPONSE	2	0x00 0x01 0x17 0x28
212	31	7	129	RESPONSE	5	0x00 0x01 0x17 0x28

Tab. 2: Response-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
213	31	8	129	RESPONSE	9	0x00 0x01 0x17 0x28
214	32	1	129	RESPONSE	5	0x17 0x28
215	32	2	129	RESPONSE	3	0x17 0x28
216	32	3	129	RESPONSE	11	0x17 0x28
217	32	4	129	RESPONSE	9	0x17 0x28
218	32	5	129	RESPONSE	5	0x17 0x28
219	32	6	129	RESPONSE	9	0x17 0x28
220	32	7	129	RESPONSE	11	0x17 0x28
221	32	8	129	RESPONSE	15	0x17 0x28
222	32	1	130	UNSOLI CI TED_RESPONSE	5	0x17 0x28
223	32	2	130	UNSOLI CI TED_RESPONSE	3	0x17 0x28
224	32	3	130	UNSOLI CI TED_RESPONSE	11	0x17 0x28
225	32	4	130	UNSOLI CI TED_RESPONSE	9	0x17 0x28
226	32	5	130	UNSOLI CI TED_RESPONSE	5	0x17 0x28
227	32	6	130	UNSOLI CI TED_RESPONSE	9	0x17 0x28
228	32	7	130	UNSOLI CI TED_RESPONSE	11	0x17 0x28
229	32	8	130	UNSOLI CI TED_RESPONSE	15	0x17 0x28
230	33	1	129	RESPONSE	5	0x17 0x18
231	33	2	129	RESPONSE	3	0x17 0x28
232	33	3	129	RESPONSE	11	0x17 0x28
233	33	4	129	RESPONSE	9	0x17 0x28
234	33	5	129	RESPONSE	5	0x17 0x28

Tab. 2: Response-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
235	33	6	129	RESPONSE	9	0x17 0x28
236	33	7	129	RESPONSE	11	0x17 0x28
237	33	8	129	RESPONSE	15	0x17 0x28
238	33	1	130	UNSOLI CI TED_RESPONSE	5	0x17 0x28
239	33	2	130	UNSOLI CI TED_RESPONSE	3	0x17 0x28
240	33	3	130	UNSOLI CI TED_RESPONSE	11	0x17 0x28
241	33	4	130	UNSOLI CI TED_RESPONSE	9	0x17 0x28
242	33	5	130	UNSOLI CI TED_RESPONSE	5	0x17 0x28
243	33	6	130	UNSOLI CI TED_RESPONSE	9	0x17 0x28
244	33	7	130	UNSOLI CI TED_RESPONSE	11	0x17 0x28
245	33	8	130	UNSOLI CI TED_RESPONSE	15	0x17 0x28
246	34	1	129	RESPONSE	2	0x00 0x01
247	34	2-3	129	RESPONSE	4	0x00 0x01
248	40	1	129	RESPONSE	5	0x00 0x01 0x17 0x28
249	40	2	129	RESPONSE	3	0x00 0x01 0x17 0x28
250	40	3	129	RESPONSE	5	0x00 0x01 0x17 0x28
251	40	4	129	RESPONSE	9	0x00 0x01 0x17 0x28
252	41	1	129	RESPONSE	5	0x00 0x01 0x17 0x28

Tab. 2: Response-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
253	41	2	129	RESPONSE	3	0x00 0x01 0x17 0x28
254	41	3	129	RESPONSE	5	0x00 0x01 0x17 0x28
255	42	1	129	RESPONSE	5	0x17 0x28
256	42	2	129	RESPONSE	3	0x17 0x28
257	42	3	129	RESPONSE	11	0x17 0x28
258	42	4	129	RESPONSE	9	0x17 0x28
259	42	5	129	RESPONSE	5	0x17 0x28
260	42	6	129	RESPONSE	9	0x17 0x28
261	42	7	129	RESPONSE	11	0x17 0x28
262	42	8	129	RESPONSE	15	0x17 0x28
263	42	1	130	UNSOLI CI TED_RESPONSE	5	0x17 0x28
264	42	2	130	UNSOLI CI TED_RESPONSE	3	0x17 0x28
265	42	3	130	UNSOLI CI TED_RESPONSE	11	0x17 0x28
266	42	4	130	UNSOLI CI TED_RESPONSE	9	0x17 0x28
267	42	5	130	UNSOLI CI TED_RESPONSE	5	0x17 0x28
268	42	6	130	UNSOLI CI TED_RESPONSE	9	0x17 0x28
269	42	7	130	UNSOLI CI TED_RESPONSE	11	0x17 0x28
270	42	8	130	UNSOLI CI TED_RESPONSE	15	0x17 0x28
271	43	1	129	RESPONSE	5	0x17 0x28
272	43	2	129	RESPONSE	3	0x17 0x28
273	43	3	129	RESPONSE	11	0x17 0x28
274	43	4	129	RESPONSE	9	0x17 0x28

Tab. 2: Response-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifizier
275	43	5	129	RESPONSE	5	0x17 0x28
276	43	6	129	RESPONSE	9	0x17 0x28
277	43	7	129	RESPONSE	11	0x17 0x28
278	43	8	129	RESPONSE	15	0x17 0x28
279	43	1	130	UNSOLI CI TED_RESPONSE	5	0x17 0x28
280	43	2	130	UNSOLI CI TED_RESPONSE	3	0x17 0x28
281	43	3	130	UNSOLI CI TED_RESPONSE	11	0x17 0x28
282	43	4	130	UNSOLI CI TED_RESPONSE	9	0x17 0x28
283	43	5	130	UNSOLI CI TED_RESPONSE	5	0x17 0x28
284	43	6	130	UNSOLI CI TED_RESPONSE	9	0x17 0x28
285	43	7	130	UNSOLI CI TED_RESPONSE	11	0x17 0x28
286	43	8	130	UNSOLI CI TED_RESPONSE	15	0x17 0x28
287	50	1	129	RESPONSE	6	0x07
288	50	4	129	RESPONSE	11	0x00 0x01 0x17 0x28
289	51	1-2	129	RESPONSE	6	0x07
290	51	1-2	130	UNSOLI CI TED_RESPONSE	6	0x07
291	52	1-2	129	RESPONSE	2	0x07
292	70	2	129	RESPONSE	QC_5B_count_1	0x5B
293	70	4-7	129	RESPONSE	QC_5B_count_1	0x5B
294	70	4-7	130	UNSOLI CI TED_RESPONSE	QC_5B_count_1	0x5B
295	80	1	129	RESPONSE	2	0x00 0x01
296	81	1	129	RESPONSE	3	0x07
297	82	1	129	RESPONSE	QC_5B_count_1	0x5B
298	82	1	130	RESPONSE	QC_5B_count_1	0x5B
299	83	1-2	129	RESPONSE	QC_5B	0x5B
300	83	1	130	UNSOLI CI TED_RESPONSE	QC_5B	0x5B
301	85	1	129	RESPONSE	QC_5B	0x5B
302	86	1	129	RESPONSE	QC_5B	0x5B

Tab. 2: Response-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
303	86	2	129	RESPONSE	1	0x00 0x01 0x17 0x28
304	86	3	129	RESPONSE	QC_5B	0x5B
305	87	1	129	RESPONSE	QC_5B	0x5B
306	88	1	129	RESPONSE	QC_5B	0x5B
307	88	1	130	UNSOLI CI TED_RESPONSE	QC_5B	0x5B
308	91	1	129	RESPONSE	QC_5B	0x5B
309	101	1	129	RESPONSE	2	0x00 0x01 0x17 0x28
310	101	2	129	RESPONSE	4	0x00 0x01 0x17 0x28
311	101	3	129	RESPONSE	8	0x00 0x01 0x17 0x28
312	102	1	129	RESPONSE	1	0x00 0x01 0x03 0x04 0x05 0x17 0x28
313	110	128	129	RESPONSE	vari ati on	0x00 0x01 0x03 0x04 0x05 0x17 0x28
314	111	128	129	RESPONSE	vari ati on	0x00 0x01 0x03 0x04 0x05 0x17 0x28

Tab. 2: Response-Nachrichten (Forts.)

Index	Gruppe n-Nr.	Variation	Funktion	Funktionsname	Länge	Qualifier
315	111	128	130	UNSOLI CI TED_RESPONSE	vari ation	0x00 0x01 0x17 0x28
316	113	128	129	RESPONSE	vari ation	0x00 0x01 0x17 0x28
317	113	128	130	UNSOLI CI TED_RESPONSE	vari ation	0x00 0x01 0x17 0x28

### 4.6.4 Deep Packet Inspection - IEC104 Enforcer

[Netzsicherheit > DPI > IEC104 Enforcer]

Dieser Dialog ermöglicht Ihnen, die *IEC104 Enforcer*-Einstellungen festzulegen und *IEC104 Enforcer*-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 *IEC104 Enforcer* 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 *IEC104 Enforcer*-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:

- *Function Type*
- *Erweiterte Liste Type-ID*
- *Originator Adressliste*
- *Gemeinsame Adressliste*

## Funktion


Nicht angewendete Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten *IEC104 Enforcer*-Profile von den im Gerät gespeicherten Profilen unterscheiden.

Mögliche Werte:

**markiert**

Mindestens eines der aktiven *IEC104 Enforcer*-Profile, die im Gerät gespeichert sind, enthält geänderte Einstellungen.

Um die noch ausstehenden Profile auf den Datenstrom anzuwenden, klicken Sie die Schaltfläche .

---

### Anmerkung:

Wenn es im Gerät noch ausstehende Änderungen gibt, wendet das Gerät diese während des nächsten Systemstarts an.

**unmarkiert**

Die *IEC104 Enforcer*-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 *Erstellen*, um eine Tabellenzeile hinzuzufügen.

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

Mögliche Werte:

1..32

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

 Löschen

Entfernt die ausgewählte Tabellenzeile.

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



Kopieren

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

- Im Feld *Index* legen Sie die neue Nummer des kopierten Profils fest.

Mögliche Werte:

1 . 32

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



Änderungen anwenden

Das Gerät wendet die festgelegten Profile auf den Datenstrom an.

Wenn Sie die Werte im Feld *Function Type* 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: *iec104*)

#### Function Type

Legt den Funktionstyp für das *IEC104 Enforcer*-Profil fest. Nach dem Klicken der Schaltfläche  weist das Gerät die zugehörigen *Typ-IDs* zu.

Mögliche Werte:

*read-onl y*

Weist die *Type-IDs* für *read*-Funktion zu.

1, 3, 5, 7, 9, 11, 13, 15, 20, 21, 30- 40, 70, 100- 102

*read-wri te*

Weist die *Type-IDs* für *read/write*-Funktionen zu.

1, 3, 5, 7, 9, 11, 13, 15, 20, 21, 30- 40, 45- 51, 58- 64, 70, 100- 102

*common*

Weist die *Type-IDs* für *common*-Funktionen zu.

1, 3, 5, 7, 9, 11, 13, 15, 20, 21, 30- 40, 45- 51, 58- 64, 70, 100- 102, 110- 113, 120- 127

*any* (Voreinstellung)

Weist die *Type-IDs* für jede Funktion zu.

1, 2, . . . , 254, 255

Das Gerät akzeptiert keine nachträglichen Änderungen in Spalte *Erweiterte Liste Type-ID*.

*advanced*

Ermöglicht Ihnen, in Spalte *Erweiterte Liste Type-ID* benutzerdefinierte Werte festzulegen.

### Erweiterte Liste Type-ID

Zeigt die *Erweiterten Type-IDs* für das *IEC104 Enforcer*-Profil. Das Gerät lässt Datenpakete mit den festgelegten Eigenschaften zu. Voraussetzung ist, dass in Spalte *Function Type* ein anderer Wert als *any* 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 *Erweiterte Liste Type-ID*.

Der Dialog zeigt das Fenster *Erweiterte Liste Type-ID*.

Wählen Sie in der Dropdown-Liste *Erweiterte Liste Type-ID* den gewünschten *Type-ID*-Eintrag.

Klicken Sie die Schaltfläche *Hinzufügen*.

Um mehrere *Type-IDs* hinzuzufügen, wiederholen Sie die zuvor beschriebenen Schritte.

Klicken Sie die Schaltfläche *Ok*.

Mögliche Werte:

0 . 255

Die Bedeutung der Nummern finden Sie im Abschnitt „*Bedeutung der Erweiterte Liste Type-ID-Werte*“ auf Seite 200.

### Originator Adressliste

Legt die Adressen fest, die den Ursprung der Datenpakete repräsentieren. Voraussetzung ist, dass in Spalte *Übertragungsgröße Ursache* der Wert *2* festgelegt ist.

Mögliche Werte:

<Leer> (Voreinstellung)

Das Gerät lässt Datenpakete mit beliebiger *Originator*-Adresse zu.

0 . 255

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:

0 . 255

Das Gerät lässt Datenpakete mit der festgelegten *Common*-Adresse zu. Voraussetzung ist, dass in Spalte *Größe Common-Adresse* der Wert *1* festgelegt ist.

0 . 65535 (2<sup>16</sup> - 1)

Das Gerät lässt Datenpakete mit der festgelegten *Common*-Adresse zu. Voraussetzung ist, dass in Spalte *Größe Common-Adresse* der Wert *2* 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:

1

Die Datenpakete enthalten keine *Originator*-Adresse.

2 (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 *Gemeinsame Adressliste*.

Mögliche Werte:

- 1
- 2 (Voreinstellung)

Größe IO-Adresse

Legt die Größe der *Information Object Address* in Oktetts fest.

Mögliche Werte:

- 1
- 2
- 3 (Voreinstellung)

IEC\_60870\_5\_101 zulassen

Aktiviert/deaktiviert die in der *IEC101*-Spezifikation definierten *Type-IDs*.

Mögliche Werte:

*markiert*

Die in der *IEC101*-Spezifikation definierten *Type-IDs* sind aktiv.

Das Gerät lässt die *Type-ID*-Werte 2, 4, 6, 8, 10, 12, 14, 16, 17, 18, 19, 103, 104, 105, 106 zu – zusammen mit den *Type-IDs*, die auf den in Spalte *Function Type* oder *Erweiterte Liste Type-ID* festgelegten Werten basieren.

*unmarkiert* (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 *Function Type* oder *Erweiterte Liste Type-ID* festgelegten Werten basieren.

Plausibilitätsprüfung

Aktiviert/deaktiviert die Plausibilitätsprüfung für Datenpakete.

Mögliche Werte:

*markiert* (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.

*unmarkiert*

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:

`markiert` (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.

`unmarkiert`

Das Zurücksetzen der TCP-Verbindung ist inaktiv.

## Debug

Aktiviert/deaktiviert das Debugging für die Profile.

Mögliche Werte:

`markiert`

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 *TCP-Reset* das Kontrollkästchen markiert ist.

`unmarkiert` (Voreinstellung)

Das Debugging ist inaktiv.

## Profil aktiv

Aktiviert/deaktiviert das Profil.

Mögliche Werte:

`markiert`

Das Profil ist aktiv.

Das Gerät wendet die in dieser Tabellenzeile festgelegten *IEC104 Enforcer*-Profile auf den Datenstrom an.

`unmarkiert`

Das Profil ist inaktiv.

## [Erweiterte Liste Type-ID]

### Erweiterte Liste Type-ID

Legt die *Advanced Type-IDs* für das betreffende *IEC104 Enforcer*-Profil fest.

Die Bedeutung der Nummern finden Sie im Abschnitt „[Bedeutung der Erweiterte Liste Type-ID-Werte](#)“ auf Seite 200.

### Hinzufügen

Fügt die in der Dropdown-Liste ausgewählten Einträge in das Feld *Erweiterte Liste Type-ID* ein.



Löscht den Eintrag aus dem Feld *Erweiterte Liste Type-ID*.

**Bedeutung der Erweiterte Liste Type-ID-Werte**

#	Bedeutung
1	Single point information M <sub>SP</sub> _NA_1
2	Single point information with time tag M <sub>SP</sub> _TA_1
3	Double point information M <sub>DP</sub> _NA_1
4	Double point information with time tag M <sub>DP</sub> _TA_1
5	Step position information M <sub>ST</sub> _NA_1
6	Step position information with time tag M <sub>ST</sub> _TA_1
7	Bit string of 32 bit M <sub>BO</sub> _NA_1
8	Bit string of 32 bit with time tag M <sub>BO</sub> _TA_1
9	Measured value, normalized value M <sub>ME</sub> _NA_1
10	Measured value, normalized value with time tag M <sub>ME</sub> _TA_1
11	Measured value, scaled value M <sub>ME</sub> _NB_1
12	Measured value, scaled value with time tag M <sub>ME</sub> _TB_1
13	Measured value, short floating point value M <sub>ME</sub> _NC_1
14	Measured value, short floating point value with time tag M <sub>ME</sub> _TC_1
15	Integrated totals M <sub>IT</sub> _NA_1
16	Integrated totals with time tag M <sub>IT</sub> _TA_1
17	Event of protection equipment with time tag M <sub>EP</sub> _TA_1
18	Packed start events of protection equipment with time tag M <sub>EP</sub> _TB_1
19	Packed output circuit information of protection equipment with time tag M <sub>EP</sub> _TC_1
20	Packed single-point information with status change detection M <sub>PS</sub> _NA_1
21	Measured value, normalized value without quality descriptor M <sub>ME</sub> _ND_1
30	Single point information with time tag CP56Time2a M <sub>SP</sub> _TB_1
31	Double point information with time tag CP56Time2a M <sub>DP</sub> _TB_1
32	Step position information with time tag CP56Time2a M <sub>ST</sub> _TB_1
33	Bit string of 32 bit with time tag CP56Time2a M <sub>BO</sub> _TB_1
34	Measured value, normalized value with time tag CP56Time2a M <sub>ME</sub> _TD_1
35	Measured value, scaled value with time tag CP56Time2a M <sub>ME</sub> _TE_1
36	Measured value, short floating point value with time tag CP56Time2a M <sub>ME</sub> _TF_1
37	Integrated totals with time tag CP56Time2a M <sub>IT</sub> _TB_1
38	Event of protection equipment with time tag CP56Time2a M <sub>EP</sub> _TD_1
39	Packed start events of protection equipment with time tag CP56Time2a M <sub>EP</sub> _TE_1
40	Packed output circuit information of protection equipment with time tag CP56Time2a M <sub>EP</sub> _TF_1
45	Single command C <sub>SC</sub> _NA_1
46	Double command C <sub>DC</sub> _NA_1
47	Regulating step command C <sub>RC</sub> _NA_1
48	Setpoint command, normalized value C <sub>SE</sub> _NA_1
49	Setpoint command, scaled value C <sub>SE</sub> _NB_1
50	Setpoint command, short floating point value C <sub>SE</sub> _NC_1e
51	Bit string 32 bit C <sub>BO</sub> _NA_1

#	Bedeutung
58	Single command with time tag CP56Time2a C_SC_TA_1
59	Double command with time tag CP56Time2a C_DC_TA_1
60	Regulating step command with time tag CP56Time2a C_RC_TA_1
61	Setpoint command, normalized value with time tag CP56Time2a C_SE_TA_1
62	Setpoint command, scaled value with time tag CP56Time2a C_SE_TB_1
63	Setpoint command, short floating point value with time tag CP56Time2a C_SE_TC_1
64	Bit string 32 bit with time tag CP56Time2a C_BO_TA_1
70	End of initialization MEI_NA_1
100	(General -) Interrogation command C_IC_NA_1
101	Counter interrogation command C_CI_NA_1
102	Read command C_RD_NA_1
103	Clock synchronization command C_CS_NA_1
104	( IEC 101 ) Test command C_TS_NB_1
105	Reset process command C_RP_NC_1
106	( IEC 101 ) Delay acquisition command C_CD_NA_1
107	Test command with time tag CP56Time2a C_TS_TA_1
110	Parameter of measured value, normalized value P_ME_NA_1
111	Parameter of measured value, scaled value P_ME_NB_1
112	Parameter of measured value, short floating point value P_ME_NC_1
113	Parameter activation P_AC_NA_1
120	File ready F_FR_NA_1
121	Section ready F_SR_NA_1
122	Call directory, select file, call file, call section F_SC_NA_1
123	Last section, last segment F_LS_NA_1
124	Ack file, Ack section F_AF_NA_1
125	Segment F_SG_NA_1
126	F_DR_TA_1
127	QueryLog - Request archive file F_SC_NB_1

## 4.6.5 Deep Packet Inspection - AMP-Enforcer

[Netzsicherheit > DPI > AMP Enforcer]

Dieser Dialog ermöglicht Ihnen, die *AMP Enforcer*- (ASCII Message Protocol Enforcer)-Einstellungen festzulegen und *AMP Enforcer*-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 *AMP Enforcer*-Funktion unterstützt *Common ASCII Message Protocol (CAMP)* und *Non-Intelligent Terminal Protocol (NITP)* unter Verwendung von *TCP*. Das Gerät verwendet die *AMP Enforcer*-Funktion, um die *DPI*-Funktion auf den *CAMP*- und *NITP*-Datenstrom anzuwenden. Das Gerät führt die *DPI*-Funktion basierend auf der *Program and Mode Protect*-Funktion und dem festgelegten Profil aus.

Bei aktiviertem *AMP Enforcer*-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 *Program and Mode Protect*-Funktion.

- *Protokoll*
- *Message-Typ*
- *Adress-Klasse*
- *Geräteklasse*
- *Speicheradresse*
- *Datenwort*
- *Taskcode*
- *Taskcode-Daten*
- *Zeichen für Blockprüfung*
- *Zeichen für Fehlerprüfung*
- *Plausibilitätsprüfung*

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 *AMP Enforcer*-Profil fest.

### Protect-Modus

Program and Mode Protect

Aktiviert/deaktiviert die Prüfung der Datenpakete, welche die *Taskcodes* mit dem Wert *config* in Spalte *Modus* enthalten.

Mögliche Werte:

*marked* (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 *config* in Spalte *Modus* enthalten, für die *Taskcodes*, die in den Profilen festgelegt sind.

*unmarked*

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 *config* in Spalte *Modus* enthalten.

### Funktion


Nicht angewendete Änderungen vorhanden

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

Mögliche Werte:

*marked*

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

Um die noch ausstehenden Profile auf den Datenstrom anzuwenden, klicken Sie die Schaltfläche .

---

#### Anmerkung:

Wenn es im Gerät noch ausstehende Änderungen gibt, wendet das Gerät diese während des nächsten Systemstarts an.

---

*unmarked*

Die *AMP Enforcer*-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 *Erstellen*, um eine Tabellenzeile hinzuzufügen.

- Im Feld *Taskcode* legen Sie die Nummer des Profils fest.

Mögliche Werte:

00 . FF

Nach Klicken der Schaltfläche *Ok* fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld *Taskcode* 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 *AMP Enforcer*-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:

00 . FF

Sie finden die Bedeutung der voreingestellten *Taskcodes* im Abschnitt „Bedeutung der Taskcode-Werte“ auf Seite 213.

#### 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:

`conf i g`

Legt Kommandos fest, die mit der Modifikation der Steuerungseinstellungen, des Anwendungsprogramms oder des Betriebsmodus verknüpft sind.

`non-conf i g`

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 *AMP Enforcer*-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 *Erstellen*, um eine Tabellenzeile hinzuzufügen.

- Im Feld *Index* legen Sie die Nummer des Profils fest.  
Mögliche Werte:  
1 . 32

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

 Löschen

Entfernt die ausgewählte Tabellenzeile.

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

 Kopieren

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

- Im Feld *Index* legen Sie die neue Nummer des kopierten Profils fest.  
Mögliche Werte:  
1 . 32

Nach Klicken der Schaltfläche *Ok* fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist der Tabellenzeile die im Feld *Index* 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: `amp`)

## 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:

`camp`  
*Common ASCII Message Protocol*

`ni tp`  
*Non-Intelligent Terminal Protocol*

`any` (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 *Protokoll* der Wert `camp` festgelegt ist.

Mögliche Werte:

`any` (Voreinstellung)

Das Gerät wendet das Profil auf jedes Datenpaket an, ohne den Nachrichten-Typ zu bewerten.

`00 . 03` und `FF`

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: `02`

- Sie legen mehrere einzelne Nachrichten-Typen durch Hexadezimalwerte fest, die durch ein Komma getrennt sind.

Beispiel: `02, 03, FF`

`00 . 01, 04 . 09` und `FF`

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: `04`

- Sie legen mehrere einzelne Nachrichten-Typen durch Hexadezimalwerte fest, die durch ein Komma getrennt sind.

Beispiel: `04, 05, 06, FF`

Die Bedeutung der Hexadezimalwerte finden Sie im Abschnitt „*Bedeutung der Message-Typ-Werte*“ auf Seite 214.

### Adress-Klasse

Legt den jeweiligen Typ des Speichers fest, auf den auf dem Anlagenteil zugegriffen werden soll.

Voraussetzungen:

- In Spalte *Protokoll* ist der Wert *camp* festgelegt.
- In Spalte *Message-Typ* ist ein Hexadezimalwert im Bereich *00 . 01* oder *04 . 09* oder der Hexadezimalwert *FF* festgelegt.

Mögliche Werte:

*any* (Voreinstellung)

Das Gerät wendet das Profil auf jedes Datenpaket an, ohne die Adressklasse zu bewerten.

*0000 . FFFF*

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: *0000*
- Sie legen mehrere einzelne Adressklassen durch Hexadezimalwerte fest, die durch ein Komma getrennt sind.  
Beispiel: *0000, 0003, FFFF*
- Sie legen einen Bereich für eine Adressklasse durch Hexadezimalwerte fest, die mit einem Bindestrich verbunden sind.  
Beispiel: *0004-000A*
- Sie können auch Adressklassen und Bereiche für Adressklassen kombinieren.  
Beispiel: *0000, 0003, 0004-000A*

Das Feld ermöglicht Ihnen, bis zu 205 Hexadezimalwerte festzulegen. Wenn Sie zum Beispiel *0000, 0003, 0004-000A* eingeben, verwenden Sie 4 von 205 Hexadezimalwerten.

### Geräteklasse

Legt den Typ der Geräteklasse (des herstellerepezifischen Geräts) fest, auf den zugegriffen werden soll.

Voraussetzungen:

- In Spalte *Protokoll* ist der Wert *camp* festgelegt.
- In Spalte *Message-Typ* ist ein Hexadezimalwert im Bereich *00 . 03* oder der Hexadezimalwert *FF* festgelegt.

Mögliche Werte:

*any* (Voreinstellung)

Das Gerät wendet das Profil auf jedes Datenpaket an, ohne die Geräteklasse zu bewerten.

*0000 . FFFF*

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: *0000*
- Sie legen mehrere einzelne Geräteklassen durch Hexadezimalwerte fest, die durch ein Komma getrennt sind.  
Beispiel: *0000, 0003, FFFF*

- Sie legen einen Bereich für eine Geräteklasse durch Hexadezimalwerte fest, die mit einem Bindestrich verbunden sind.  
Beispiel: 0004-000A
- Sie können auch Geräteklassen und Bereiche für Geräteklassen kombinieren.  
Beispiel: 0000, 0003, 0004-000A  
Das Feld ermöglicht Ihnen, bis zu 205 Hexadezimalwerte festzulegen. Wenn Sie zum Beispiel 0000, 0003, 0004-000A eingeben, verwenden Sie 4 von 205 Hexadezimalwerten.

#### Speicheradresse

Legt die Startadresse des Speichers fest, der gelesen oder geschrieben werden soll.

Voraussetzungen:

- In Spalte *Protokoll* ist der Wert *camp* festgelegt.
- In Spalte *Message-Typ* ist ein Hexadezimalwert im Bereich 00 . 01 oder 04 . 09 oder der Hexadezimalwert FF festgelegt.

Mögliche Werte:

*any* (Voreinstellung)

Das Gerät wendet das Profil auf jedes Datenpaket an, ohne die Speicheradresse zu bewerten.

0000 . FFFF

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: 0000
- Sie legen mehrere einzelne Speicheradressen durch Hexadezimalwerte fest, die durch ein Komma getrennt sind.  
Beispiel: 0000, 0003, FFFF
- Sie legen einen Speicheradressbereich durch Hexadezimalwerte fest, die mit einem Bindestrich verbunden sind.  
Beispiel: 0004-000A
- Sie können auch Speicheradressen und Speicheradressbereiche kombinieren.  
Beispiel: 0000, 0003, 0004-000A  
Das Feld ermöglicht Ihnen, bis zu 205 Hexadezimalwerte festzulegen. Wenn Sie zum Beispiel 0000, 0003, 0004-000A 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 *Protokoll* ist der Wert *camp* festgelegt.
- In Spalte *Message-Typ* ist ein Hexadezimalwert im Bereich 00 . 01 oder 08 . 09 oder der Hexadezimalwert FF festgelegt.

Mögliche Werte:

*any* (Voreinstellung)

Das Gerät wendet das Profil auf jedes Datenpaket an, ohne das Datenwort zu bewerten.

0000 . FFFF

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: 0000

- Sie legen mehrere einzelne Datenwörter durch Hexadezimalwerte fest, die durch ein Komma getrennt sind.  
Beispiel: 0000, 0003, FFFF
- Sie legen einen Bereich für Datenwörter durch Hexadezimalwerte fest, die mit einem Bindestrich verbunden sind.  
Beispiel: 0004-000A
- Sie können auch Datenwörter und Bereiche von Datenwörtern kombinieren.  
Beispiel: 0000, 0003, 0004-000A  
Das Feld ermöglicht Ihnen, bis zu 205 Hexadezimalwerte festzulegen. Wenn Sie zum Beispiel 0000, 0003, 0004-000A eingeben, verwenden Sie 4 von 205 Hexadezimalwerten.

## Taskcode

Zeigt die *Taskcodes* für das *AMP Enforcer*-Profil. Sie können benutzerspezifische *Taskcodes* im *Netzsicherheit > DPI > AMP Enforcer > Global*-Dialog hinzufügen.

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

- *ni tp*
- *camp*  
Zusätzlich ist in Spalte *Message-Typ* ein Hexadezimalwert im Bereich 00 . 03 oder der Hexadezimalwert FF festgelegt.
- *any*  
Zusätzlich ist in Spalte *Message-Typ* der Wert *any* festgelegt.

Das Gerät ermöglicht Ihnen, mehrere *Taskcodes* festzulegen. Führen Sie dazu die folgenden Schritte aus:

Klicken Sie in die Spalte *Taskcode* des betreffenden Profils.  
Der Dialog zeigt das Fenster *Taskcode*.

Wählen Sie in der Dropdown-Liste *Taskcode* den gewünschten *Taskcode*.

Klicken Sie die Schaltfläche *Hinzufügen*.

Um mehrere *Taskcodes* hinzuzufügen, wiederholen Sie die zuvor beschriebenen Schritte.

Klicken Sie die Schaltfläche *Ok*.

Mögliche Werte:

*any* (Voreinstellung)

Das Gerät wendet jeden *Taskcode* an, der im Feld *Verfügbare Taskcodes* vorhanden ist.

00 . FF

Das Gerät lässt Datenpakete mit den festgelegten Codes zu.

Dieses Feld ermöglicht Ihnen, folgende Optionen festzulegen:

- Ein einzelner *Taskcode* mit einem einzelnen Hexadezimalwert.  
Beispiel: 00
- Mehrere *Taskcodes* mit Hexadezimalwerten, die durch ein Komma getrennt sind.  
Beispiel: 00, 01, 02

Die Bedeutung der Hexadezimalwerte finden Sie im Abschnitt „Bedeutung der *Taskcode*-Werte“ auf Seite 213.

## Taskcode-Daten

Legt die Taskcode-Daten für den *Taskcode* fest.

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

- *camp*  
Zusätzlich sind in Spalte *Message-Typ* ein Hexadezimalwert im Bereich *00* . *03* oder der Hexadezimalwert *FF* sowie in Spalte *Taskcode* ein einzelner Hexadezimalwert festgelegt.
- *ni tp*  
Zusätzlich ist in Spalte *Taskcode* ein einzelner Hexadezimalwert festgelegt.

Mögliche Werte:

*0* . *F*

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 *Protokoll* ist der Wert *camp* und in Spalte *Message-Typ* ist ein Hexadezimalwert im Bereich *00* . *03* oder der Hexadezimalwert *FF* festgelegt.  
oder
- In Spalte *Protokoll* ist der Wert *ni tp* festgelegt.

Mögliche Werte:

*marked* (Voreinstellung)

Die Prüfung ist aktiv.

*unmarked*

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 *Protokoll* ist der Wert *camp* festgelegt.
- In Spalte *Message-Typ* ist ein Hexadezimalwert im Bereich *00* . *09* oder der Hexadezimalwert *FF* festgelegt.

Mögliche Werte:

*marked* (Voreinstellung)

Die Prüfung ist aktiv.

*unmarked*

Die Prüfung ist inaktiv.

## Debug

Aktiviert/deaktiviert das Debugging für die Profile.

Mögliche Werte:

`marked`

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 `TCP-Reset` das Kontrollkästchen markiert ist.

`unmarked` (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:

`marked` (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.

`unmarked`

Das Zurücksetzen der TCP-Verbindung ist inaktiv.

## Plausibilitätsprüfung

Aktiviert/deaktiviert die Plausibilitätsprüfung für Datenpakete.

Mögliche Werte:

`marked` (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.

`unmarked`

Die Plausibilitätsprüfung ist inaktiv.

## Profil aktiv

Aktiviert/deaktiviert das Profil.

Mögliche Werte:

`marked`

Das Profil ist aktiv.

Das Gerät wendet die in dieser Tabellenzeile festgelegten `AMP Enforcer`-Profile auf den Datenstrom an.

`unmarked`

Das Profil ist inaktiv.

**[Taskcode]**

Taskcode

Legt die *Taskcodes* für das betreffende *AMP Enforcer*-Profil fest.

Die Bedeutung der Hexadezimalwerte finden Sie im Abschnitt „[Bedeutung der Taskcode-Werte](#)“ auf Seite 213.

Hinzufügen

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



Löscht den Eintrag aus dem Feld *AMP Enforcer*.

**Bedeutung der Taskcode-Werte**

#	Bedeutung
01	Read Word Memory Random
02	Write Word Memory Area Random
30	Read Operational Status
32	Program to Run Mode
33	Go to Program Mode
34	Execute Power-up
35	Execute Complete (Warm) Start
36	Execute Partial (Hot) Start
50	Read User Word Area Block
51	Write User Word Area Starting at Address
58	Set Controller Time of Day Clock
59	Write Discrete I/O Status or Force via Data Element Type
5A	Write Block
6B	Read Discrete I/O Status or Force via Data Element Type
71	Read Controller Time of Day Clock
7D	Read SF/Loop Processor Mode
7E	Read Random
7F	Read Block
88	Select Number of SF Module Task Codes Per Scan
89	Read Number of SF Module Task Codes Per Scan
99	Write VME Memory Area Block/Random
9A	Read VME Memory Area Block/Random

### Bedeutung der Message-Typ-Werte

#	Bedeutung
00	Module General Query Command
01	Module General Response Command
02	Packet T/C Command
03	Packed T/C Response
04	Read data Command
05	Read data Response
06	Write data Command
07	Write data Response
08	Mem Exch Command
09	Mem Exch Response
FF	Protocol Error

## 4.6.6 Deep Packet Inspection - ENIP Enforcer

[Netzsicherheit > DPI > ENIP Enforcer]

Dieser Dialog ermöglicht Ihnen, die *ENIP Enforcer*- (*Ethernet Industrial Protocol Enforcer*)-Einstellungen festzulegen und *ENIP Enforcer*-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 *ENIP Enforcer*-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 *ENIP Enforcer*, 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 *ENIP Enforcer* 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 *ENIP Enforcer*-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:

- *Function Type*
- *Plausibilitätsprüfung*
- *Standard-Objektliste*
- *Wildcard Service-Liste*
- *Embedded PCCC zulassen* (*Programmable Controller Communication Commands*)

Das Menü enthält die folgenden Dialoge:

- *ENIP-Profil*
- *ENIP-Objekt*

## 4.6.6.1 ENIP-Profil

[Netzicherheit > DPI > ENIP Enforcer > Profil]

In diesem Dialog legen Sie die globalen Einstellungen für das *ENIP Enforcer*-Profil fest.

### Funktion


Nicht angewendete Änderungen vorhanden

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

Mögliche Werte:

**marked**

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

Um die noch ausstehenden Profile auf den Datenstrom anzuwenden, klicken Sie die Schaltfläche  .

---

#### Anmerkung:

Wenn es im Gerät noch ausstehende Änderungen gibt, wendet das Gerät diese während des nächsten Systemstarts an.

**unmarked**

Die *ENIP Enforcer*-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 *Erstellen*, um eine Tabellenzeile hinzuzufügen.

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

Mögliche Werte:

1 . 32

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



Löschen

Entfernt die ausgewählte Tabellenzeile.

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



Kopieren

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

- Im Feld *Index* legen Sie die neue Nummer des kopierten Profils fest.  
Mögliche Werte:  
1 . 32

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



Änderungen anwenden

Das Gerät wendet die festgelegten Profile auf den Datenstrom an.

Wenn Sie die Werte im Feld *Function Type* 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: *eni p*)

#### Function Type

Legt den Funktionstyp für das *ENIP Enforcer*-Profil fest. Nach Klicken der Schaltfläche  weist das Gerät die zugehörigen *Class-IDs* und *Service-Codes* zu.

Mögliche Werte:

*read-onl y*

Weist die *Class-IDs* für die *read*-Funktion zu.

Die Liste der Nur-Lesen- (readonly-) *Class-IDs* finden Sie in [Tabelle 4 auf Seite 230](#).

*read-wri te*

Weist die *Class-IDs* für die *read/write*-Funktionen zu.

Die Liste der Schreib-Lese-*Class-IDs* finden Sie in [Tabelle 5 auf Seite 235](#).

**any** (Voreinstellung)

Weist die *Class-IDs* für jede Funktion zu. Wenn der Funktionstyp *any* ist, können Sie keine benutzerdefinierten *Class-IDs* durch den *Objekt*-Wert festlegen.

**advanced**

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:

**marked**

DPI für *PCCC-Nachrichten* ist aktiv. Das Gerät weist die *Befehlscodes* und *Funktionscodes* zu, die dem in Spalte *Function Type* festgelegten Wert entsprechen.

Sie finden die Listen der *Befehlscodes* und *Funktionscodes* in den folgenden Tabellen:

- Siehe Tabelle 6 auf Seite 245.
- Siehe Tabelle 7 auf Seite 245.
- Siehe Tabelle 8 auf Seite 247.

**unmarked** (Voreinstellung)

DPI für *PCCC-Nachrichten* ist inaktiv.

#### Plausibilitätsprüfung

Aktiviert/deaktiviert die Plausibilitätsprüfung für Datenpakete.

Mögliche Werte:

**marked** (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.

**unmarked**

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:

**marked** (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.

**unmarked**

Das Zurücksetzen der TCP-Verbindung ist inaktiv.

## Debug

Aktiviert/deaktiviert das Debugging für die Profile.

Mögliche Werte:

`marked`

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 `TCP-Reset` das Kontrollkästchen markiert ist.

`unmarked` (Voreinstellung)

Das Debugging ist inaktiv.

## Standard-Objektliste

Legt die in der *Standard-Objektliste* verwendeten *Index-Nummern* fest.

Mögliche Werte:

`all`

Das Gerät wendet das *ENIP Enforcer*-Profil auf jedes Datenpaket an, unabhängig von der *Index-Nummer*.

`1..347`

Das Gerät wendet das *ENIP Enforcer*-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: `1`

- Mehrere *Index-Nummern* legen Sie mit durch Komma getrennte Zahlenwerten fest.

Beispiel: `1, 2, 3`

- Einen *Index-Nummern*-Bereich legen Sie mit durch einen Bindestrich verbundene Zahlenwerte fest.

Beispiel: `7-25`

- Sie können auch *Index-Nummern* und *Index-Nummern*-Bereiche kombinieren.

Beispiel: `2, 7-25, 56`

Das Feld ermöglicht Ihnen, bis zu 347 Zahlenwerte festzulegen. Wenn Sie zum Beispiel `2, 7-25, 56` eingeben, verwenden Sie 4 von 347 Zahlenwerten.

Die Liste der *Class-IDs* und der dazugehörigen *Service-Codes* finden Sie in [Tabelle 3 auf Seite 221](#).

`none` (Voreinstellung)

Das Gerät wendet die *Index-Nummer* nicht auf das *ENIP Enforcer*-Profil an.

## Wildcard Service-Liste

Legt die *Service-Codes* fest, die das Gerät für alle gültigen *Class-IDs* erlaubt.

Mögliche Werte:

`0x00..0x7F`

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: `0x00`

- Sie legen mehrere einzelne *Service-Codes* durch Hexadezimalwerte fest, die durch ein Komma getrennt sind.

Beispiel: `0x02, 0x03, 0x04, 0x05`

Das Feld ermöglicht Ihnen, bis zu 128 Hexadezimalwerte festzulegen. Wenn Sie zum Beispiel `0x02, 0x03, 0x04, 0x05` eingeben, verwenden Sie 4 von 128 Hexadezimalwerten.

#### Profil aktiv

Aktiviert/deaktiviert das Profil.

Mögliche Werte:

`marked`

Das Profil ist aktiv.

Das Gerät wendet die in dieser Tabellenzeile festgelegten *ENIP Enforcer*-Profile auf den Datenstrom an.

`unmarked` (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:

- [Class-ID](#)
- [Service-Codes](#)

### Tabelle

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

#### Schaltflächen



Hinzufügen

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

- In der Dropdown-Liste [Index](#) wählen Sie die *Index-Nummer* des Profils.
- Im Feld [Class-ID](#) legen Sie die benutzerdefinierten *Class-IDs* fest.

Mögliche Werte:

[0x00](#) . [0xFFFFFFFF](#)

- Im Feld [Service-Codes](#) legen Sie die *Service-Codes* fest.

Mögliche Werte:

[0x00](#) . [0x7F](#)

Nach Klicken der Schaltfläche [Ok](#) fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist dieser Tabellenzeile die in den Feldern [Index](#), [Class-ID](#) und [Service-Codes](#) 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 *ENIP Enforcer*-Profil fest.

Mögliche Werte:

0x00 . 0xFFFFFFFF

Service-Codes

Legt die *Service-Codes* fest.

Mögliche Werte:

0x00 . 0x7F

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: 0x00
  - Sie legen mehrere einzelne *Service-Codes* durch Hexadezimalwerte fest, die durch ein Komma getrennt sind.  
 Beispiel: 0x02, 0x03, 0x04, 0x05
- Das Feld ermöglicht Ihnen, bis zu 128 Hexadezimalwerte festzulegen. Wenn Sie zum Beispiel 0x02, 0x03, 0x04, 0x05 eingeben, verwenden Sie 4 von 128 Hexadezimalwerten.

Beschreibung

Zeigt den Namen des Objekts.

**[Standard-Objektliste]**

Tab. 3: *Standard-Objektliste*

Index	Class-ID	Service-Codes
1	0x01 = Identity	0x01=Get Attributes All
2		0x05= Reset
3		0x0E= Get Attribute Signal
4		0x10= Set Attribute Signal
5		0x11= Find Next Object Instance
6		0x18= Get Member
7	0x02 = Message Router	0x01= Get Attributes All
8		0x0E = Get Attribute Single
9		0x4B = Write Data Table (Rockwell)
10	0x04 = Assembly	0x08 = Create
11		0x09 = Delete
12		0x0E = Get Attribute Single
13		0x10 = Set Attribute Single
14		0x18 = Get Member
15		0x19 = Set Member
16		0x1A = Insert Member
17		0x1B = Remove Member

Tab. 3: Standard-Objektliste (Forts.)

Index	Class-ID	Service-Codes
18	Ox05 = Connecti on	Ox05 = Reset
19		Ox08 = Create
20		Ox09 = Delete
21		Ox0D = Appl y Attri butes
22		Ox0E = Get Attri bute Si ngl e
23		Ox10 = Set Attri bute Si ngl e
24		Ox11 = Fi nd Next Obj ect Instance
25		Ox4B = Connecti on Bi nd
26		Ox4C = Producti on Appli cati on Lookup
27		Ox4E = Safety Cl ose
28		Ox54 = Safety Open
29		Ox06 = Off-Li nk Connecti on Manager <sup>1</sup>
30	Ox02 = Set Attri butes Al l	
31	Ox0E = Get Attri bute Si ngl e	
32	Ox10 = Set Attri bute Si ngl e	
33	Ox4E = Forward Cl ose	
34	Ox52 = Unconnected Send	
35	Ox54 = Forward Open	
36	Ox56 = Get Connecti on Data	
37	Ox57 = Search Connecti on Data	
38	Ox5A = Get Connecti on Owner	
39	Ox5B = Large Forward Open	
40	Ox07 = Regi ster	
41		Ox10 = Set Attri bute Si ngl e
42	Ox08 = Di screte I nput Poi nt	Ox01 = Get Attri butes Al l
43		Ox02 = Set Attri butes Al l
44		Ox0E = Get Attri bute Si ngl e
45		Ox10 = Set Attri bute Si ngl e
46	Ox09 = Di screte Output Poi nt	Ox01 = Get Attri butes Al l
47		Ox02 = Set Attri butes Al l
48		Ox0E = Get Attri bute Si ngl e
49		Ox10 = Set Attri bute Si ngl e
50	Ox0A = Anal og I nput Poi nt	Ox01 = Get Attri butes Al l
51		Ox02 = Set Attri butes Al l
52		Ox0E = Get Attri bute Si ngl e
53		Ox10 = Set Attri bute Si ngl e
54	Ox0B = Anal og Output Poi nt	Ox01 = Get Attri butes Al l
55		Ox02 = Set Attri butes Al l
56		Ox0E = Get Attri bute Si ngl e
57		Ox10 = Set Attri bute Si ngl e
58	Ox0E = Presence Sensi ng	Ox0E = Get Attri bute Si ngl e
59		Ox10 = Set Attri bute Si ngl e

Tab. 3: Standard-Objektliste (Forts.)

Index	Class-ID	Service-Codes
60	0x0F = Parameter	0x01 = Get Attributes All
61		0x05 = Reset
62		0x0D = Apply Attributes
63		0x0E = Get Attribute Single
64		0x10 = Set Attribute Single
65		0x15 = Restore
66		0x16 = Save
67		0x18 = Get Member
68		0x4B = Get EnumString
69	0x10 = Parameter Group	0x01 = Get Attributes All
70		0x0E = Get Attribute Single
71		0x10 = Set Attribute Single
72	0x12 = Group	0x01 = Get Attributes All
73		0x0E = Get Attribute Single
74	0x1D = Discrete Input Group	0x01 = Get Attributes All
75		0x02 = Set Attributes All
76		0x0E = Get Attribute Single
77		0x10 = Set Attribute Single
78	0x1E = Discrete Output Group	0x01 = Get Attributes All
79		0x02 = Set Attributes All
80		0x0E = Get Attribute Single
81		0x10 = Set Attribute Single
82	0x1F = Discrete Group	0x01 = Get Attributes All
83		0x0E = Get Attribute Single
84	0x20 = Analog Input Group	0x01 = Get Attributes All
85		0x02 = Set Attributes All
86		0x0E = Get Attribute Single
87		0x10 = Set Attribute Single
88	0x21 = Analog Output Group	0x01 = Get Attributes All
89		0x02 = Set Attributes All
90		0x0E = Get Attribute Single
91		0x10 = Set Attribute Single
92	0x22 = Analog Group	0x01 = Get Attributes All
93		0x0E = Get Attribute Single
94		0x10 = Set Attribute Single

Tab. 3: Standard-Objektliste (Forts.)

Index	Class-ID	Service-Codes
95	Ox23 = Position Sensor Object	Ox05 = Reset
96		Ox0D = Apply Attributes
97		Ox0E = Get Attribute Single
98		Ox10 = Set Attribute Single
99		Ox15 = Restore
100		Ox16 = Save
101		Ox18 = Get Member
102		Ox19 = Set Member
103	Ox24 = Position Controller Supervisor Object	Ox0E = Get Attribute Single
104		Ox10 = Set Attribute Single
105	Ox25 = Position Controller Object	Ox0E = Get Attribute Single
106		Ox10 = Set Attribute Single
107	Ox26 = Block Sequencer Object	Ox0E = Get Attribute Single
108		Ox10 = Set Attribute Single
109	Ox27 = Command Block Object	Ox0E = Get Attribute Single
110		Ox10 = Set Attribute Single
111	Ox28 = Motor Data Object	Ox0E = Get Attribute Single
112		Ox10 = Set Attribute Single
113		Ox15 = Restore
114		Ox16 = Save
115	Ox29 = Control Supervisor Object	Ox0E = Get Attribute Single
116		Ox10 = Set Attribute Single
117		Ox05 = Reset
118	Ox2A = AC/DC Drive Object	Ox0E = Get Attribute Single
119		Ox10 = Set Attribute Single
120		Ox15 = Restore
121		Ox16 = Save
122	Ox2B = Acknowledge Handler Object	Ox08 = Create
123		Ox09 = Delete
124		Ox0E = Get Attribute Single
125		Ox10 = Set Attribute Single
126		Ox4B = Add AckData Path
127	Ox4C = Remove AckData Path	
128	Ox2C = Overload Object	Ox0E = Get Attribute Single
129		Ox10 = Set Attribute Single
130		Ox15 = Restore
131		Ox16 = Save
132	Ox2D = Softstart Object	Ox0E = Get Attribute Single
133		Ox10 = Set Attribute Single
134		Ox15 = Restore
135		Ox16 = Save

Tab. 3: Standard-Objektliste (Forts.)

Index	Class-ID	Service-Codes
136	Ox2E = Selection Object	Ox05 = Reset
137		Ox06 = Start
138		Ox07 = Stop
139		Ox08 = Create
140		Ox09 = Delete
141		Ox0E = Get Attribute Single
142		Ox10 = Set Attribute Single
143		Ox18 = Get Member
144		Ox19 = Set Member
145		Ox1A = Insert Member
146	Ox1B = Remove Member	
147	Ox30 = S-Device Supervisor Object	Ox05 = Reset
148		Ox06 = Start
149		Ox07 = Stop
150		Ox0E = Get Attribute Single
151		Ox10 = Set Attribute Single
152		Ox4B = Abort
153		Ox4C = Recover
154		Ox4E = Perform Diagnostics
155	Ox31 = S-Analog Sensor Object	Ox01 = Get Attributes All
156		Ox0E = Get Attribute Single
157		Ox4B = Zero Adjust
158		Ox4C = Gain Adjust
159	Ox32 = S-Analog Actuator Object	Ox0E = Get Attribute Single
160		Ox10 = Set Attribute Single
161	Ox33 = S-Single Stage Controller Object	Ox0E = Get Attribute Single
162		Ox10 = Set Attribute Single
163		Ox63 = Calibrate
164	Ox34 = S-Gas Calibration Object	Ox0E = Get Attribute Single
165		Ox10 = Set Attribute Single
166		Ox4B = Get All Instances
167	Ox35 = Trip Point Object	Ox0E = Get Attribute Single
168		Ox10 = Set Attribute Single

Tab. 3: Standard-Objektliste (Forts.)

Index	Class-ID	Service-Codes
169	Ox37 = File Object	Ox06 = Start
170		Ox07 = Stop
171		Ox08 = Create
172		Ox09 = Delete
173		Ox0E = Get Attribute Single
174		Ox10 = Set Attribute Single
175		Ox15 = Restore
176		Ox16 = Save
177		Ox18 = Get Member
178		Ox4B = Initiate Upload
179		Ox4C = Initiate Download
180		Ox4D = Initiate Partial Read
181		Ox4E = Initiate Partial Write
182		Ox4F = Upload Transfer
183	Ox50 = Download Transfer	
184	Ox51 = Clear File	
185	Ox38 = S-Partial Pressure Object	Ox01 = Get Attributes All
186		Ox08 = Create
187		Ox09 = Delete
188		Ox0E = Get Attribute Single
189		Ox10 = Set Attribute Single
190		Ox4B = Create Range
191		Ox4C = Get Instance List
192		Ox4D = Get Pressures
193		Ox4E = Get All Pressures
194		Ox4F = Group Enable
195	Ox40 = S-Sensor Calibration Object	Ox0E = Get Attribute Single
196		Ox10 = Set Attribute Single
197		Ox4B = Get all Instances
198	Ox41 = Event Log Object	Ox05 = Reset
199		Ox06 = Start
200		Ox07 = Stop
201		Ox0E = Get Attribute Single
202		Ox10 = Set Attribute Single
203		Ox18 = Get Member
204		Ox19 = Set Member
205		Ox1A = Insert Member
206		Ox1B = Remove Member

Tab. 3: Standard-Objektliste (Forts.)

Index	Class-ID	Service-Codes	
207	0x42 = Motion Device Axis Object	0x03 = Get Attribute List	
208		0x04 = Set Attribute List	
209		0x0E = Get Attribute Single	
210		0x10 = Set Attribute Single	
211		0x1C = GroupSync	
212		0x4B = Get Axis Attributes List	
213		0x4C = Set Axis Attributes List	
214		0x4D = Set Cyclic Write List	
215		0x4E = Set Cyclic Read List	
216		0x4F = Run Motor Test	
217		0x50 = Get Motor Test Data	
218		0x51 = Run Inertia Test	
219		0x52 = Get Inertia Test Data	
220		0x53 = Run Hookup Test	
221	0x54 = Get Hookup Test Data		
222	0x43 = Time Sync Object	0x01 = Get Attributes All	
223		0x03 = Get Attribute List	
224		0x04 = Set Attribute List	
225		0x0E = Get Attribute Single	
226		0x10 = Set Attribute Single	
227		0x44 = Modbus Object	0x0E = Get Attribute Single
228	0x4B = Read Discrete Inputs		
229	0x4C = Read Coils		
230	0x4D = Read Input Registers		
231	0x4E = Read Holding Registers		
232	0x4F = Write Coils		
233	0x50 = Write Holding Registers		
234	0x51 = Modbus Passthrough		
235	0x45 = Originator Connection List Object		0x08 = Create
236			0x09 = Delete
237		0x4C = Connection Read	
238	0x46 = Modbus Serial Link Object	0x01 = Get Attributes All	
239		0x05 = Reset	
240		0x0E = Get Attribute Single	
241		0x10 = Set Attribute Single	
242		0x4B = Get And Clear	

Tab. 3: Standard-Objektliste (Forts.)

Index	Class-ID	Service-Codes	
243	Ox47 = Device Level Ring (DLR) Object	Ox01 = Get Attributes All	
244		Ox0E = Get Attribute Single	
245		Ox10 = Set Attribute Single	
246		Ox18 = Get Member	
247		Ox4B = Verify Fault Location	
248		Ox4C = Clear Rapid Faults	
249		Ox4D = Restart Signal	
250		Ox4E = Clear Gateway Partial Fault	
251		Ox48 = QoS Object	Ox01 = Get Attributes All
252			Ox0E = Get Attribute Single
253	Ox10 = Set Attribute Single		
254	Ox4D = Target Connection List Object	Ox01 = Get Attributes All	
255		Ox0E = Get Attribute Single	
256		Ox4C = Connection Read	
257	Ox4E = Base Energy Object	Ox01 = Get Attributes All	
258		Ox03 = Get Attribute List	
259		Ox04 = Set Attribute List	
260		Ox05 = Reset	
261		Ox08 = Create	
262		Ox09 = Delete	
263		Ox0E = Get Attribute Single	
264		Ox10 = Set Attribute Single	
265		Ox18 = Get Member	
266		Ox19 = Set Member	
267		Ox1A = Insert Member	
268		Ox1B = Remove Member	
269		Ox4B = Start Metering	
270		Ox4C = Stop Metering	
271		Ox4F = Electrical Energy Object	Ox01 = Get Attributes All
272	Ox03 = Get Attribute List		
273	Ox0E = Get Attribute Single		
274	Ox50 = Non-Electrical Energy Object	Ox01 = Get Attributes All	
275		Ox03 = Get Attribute List	
276		Ox0E = Get Attribute Single	
277	Ox51 = Base Switch Object	Ox01 = Get Attributes All	
278		Ox0E = Get Attribute Single	
279		Ox10 = Set Attribute Single	
280	Ox52 = SNMP Object	Ox01 = Get Attributes All	
281		Ox0E = Get Attribute Single	
282		Ox10 = Set Attribute Single	

Tab. 3: Standard-Objektliste (Forts.)

Index	Class-ID	Service-Codes
283	Ox53 = Power Management Object	Ox01 = Get Attributes All
284		Ox03 = Get Attribute List
285		Ox04 = Set Attribute List
286		Ox0E = Get Attribute Single
287		Ox10 = Set Attribute Single
288		Ox18 = Get Member
289		Ox19 = Set Member
290		Ox4D = Power Management
291		Ox4E = Set Pass Code
292		Ox4F = Clear Pass Code
293	Ox54 = RSTP Bridge Object	Ox01 = Get Attributes All
294		Ox0E = Get Attribute Single
295		Ox10 = Set Attribute Single
296	Ox55 = RSTP Port Object	Ox01 = Get Attributes All
297		Ox0E = Get Attribute Single
298		Ox10 = Set Attribute Single
299	OxF3 = Connection Configuration Object	Ox01 = Get Attributes All
300		Ox02 = Set Attributes All
301		Ox08 = Create
302		Ox09 = Delete
303		Ox0E = Get Attribute Single
304		Ox10 = Set Attribute Single
305		Ox15 = Restore
306		Ox4B = Kick Timer
307		Ox4C = Open Connection
308		Ox4D = Close Connection
309		Ox4E = Stop Connection
310		Ox4F = Change Start
311		Ox50 = Get Status
312		Ox51 = Change Complete
313	Ox52 = Audit Changes	
314	OxF4 = Port Object	Ox01 = Get Attributes All
315		Ox05 = Reset
316		Ox0E = Get Attribute Single
317		Ox10 = Set Attribute Single
318	OxF5 = TCP/IP Interface Object	Ox01 = Get Attributes All
319		Ox02 = Set Attributes All
320		Ox0E = Get Attribute Single
321		Ox10 = Set Attribute Single

Tab. 3: Standard-Objektliste (Forts.)

Index	Class-ID	Service-Codes
322	0xF6 = EtherNet Link Object	0x01 = Get Attributes All
323		0x0E = Get Attribute Single
324		0x10 = Set Attribute Single
325		0x4C = Get And Clear
326	0x300 = Module Diagnostics	0x01 = Get Attributes All
327		0x0E = Get Attribute Single
328	0x301 = Input/OCnx	0x01 = Get Attributes All
329		0x0E = Get Attribute Single
330	0x302 = Local Slaves	0x01 = Get Attributes All
331		0x0E = Get Attribute Single
332	0x400 = Service Port Control Object	0x01 = Get Attributes All
333		0x0E = Get Attribute Single
334	0x401 = Dynamic I/O Control Object	0x01 = Get Attributes All
335		0x0E = Get Attribute Single
336	0x402 = Router Diagnostics Object	0x01 = Get Attributes All
337		0x0E = Get Attribute Single
338	0x403 = Router Routing Table Object	0x01 = Get Attributes All
339		0x0E = Get Attribute Single
340	0x404 = SMTP	0x01 = Get Attributes All
341		0x0E = Get Attribute Single
342		0x32 = Clear All
343	0x405 = SNMP	0x01 = Get Attributes All
344		0x0E = Get Attribute Single
345		0x32 = Clear All
346	0x406 = HSBY	0x01 = Get Attributes All
347		0x0E = Get Attribute Single

- Ein Paket mit *Class-ID=0x06* enthält eingebettete CIP-Messages. In diesem Fall führt das Gerät eine zusätzliche Stufe von DPI für die Datenpakete durch, welche die *Service Code*-Werte *0x4E*, *0x52*, *0x54* und *0x5B* enthalten. Das Gerät blockiert ein Datenpaket, wenn es andere als die vorstehenden *Service Code*-Werte für diese *Class-ID* enthält.

**[Liste der Class-IDs für unterschiedliche Funktionstypen]**

Tab. 4: Class-IDs für Funktionstyp read-only

Class-ID	Service-Codes
0x01 = Identity	0x01=Get Attributes All
	0x0E= Get Attribute Signal
	0x11= Find Next Object Instance
	0x18= Get Member

Tab. 4: Class-IDs für Funktionstyp read-only (Forts.)

Class-ID	Service-Codes
0x02 = Message Router	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x4B = Write Data Table (Rockwell)
	0x54
0x04 = Assembly	0x0E = Get Attribute Single
	0x18 = Get Member
0x05 = Connection	0x08 = Create
	0x0E = Get Attribute Single
	0x11 = Find Next Object Instance
	0x4C = Production Application Lookup
0x06 = Off-Link Connection Manager <sup>1</sup>	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x4C
	0x4E = Forward Close
	0x52 = Unconnected Send
	0x54 = Forward Open
	0x56 = Get Connection Data
	0x57 = Search Connection Data
	0x59
	0x5A = Get Connection Owner
	0x5B = Large Forward Open
0x07 = Register	0x0E = Get Attribute Single
0x08 = Discrete Input Point	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x09 = Discrete Output Point	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x0A = Analog Input Point	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x0B = Analog Output Point	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x0E = Presence Sensing	0x0E = Get Attribute Single
0x0F = Parameter	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x18 = Get Member
	0x4B = Get Enum String
0x10 = Parameter Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x12 = Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x1D = Discrete Input Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single

Tab. 4: Class-IDs für Funktionstyp read-only (Forts.)

Class-ID	Service-Codes
0x1E = Discrete Output Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x1F = Discrete Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x20 = Analog Input Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x21 = Analog Output Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x22 = Analog Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x23 = Position Sensor Object	0x0E = Get Attribute Single
	0x18 = Get Member
0x24 = Position Controller Supervisor Object	0x0E = Get Attribute Single
0x25 = Position Controller Object	0x0E = Get Attribute Single
0x26 = Block Sequencer Object	0x0E = Get Attribute Single
0x27 = Command Block Object	0x0E = Get Attribute Single
0x28 = Motor Data Object	0x0E = Get Attribute Single
0x29 = Control Supervisor Object	0x0E = Get Attribute Single
0x2A = AC/DC Drive Object	0x0E = Get Attribute Single
0x2B = Acknowledge Handler Object	0x0E = Get Attribute Single
0x2C = Overload Object	0x0E = Get Attribute Single
0x2D = Softstart Object	0x0E = Get Attribute Single
0x2E = Selection Object	0x0E = Get Attribute Single
	0x18 = Get Member
0x30 = S-Device Supervisor Object	0x0E = Get Attribute Single
0x31 = S-Analog Sensor Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x32 = S-Analog Actuator Object	0x0E = Get Attribute Single
0x33 = S-Single Stage Controller Object	0x0E = Get Attribute Single
0x34 = S-Gas Calibration Object	0x0E = Get Attribute Single
	0x4B = Get All Instances
0x35 = Trip Point Object	0x0E = Get Attribute Single
0x37 = File Object	0x0E = Get Attribute Single
	0x18 = Get Member
	0x4B = Initiate Upload
	0x4D = Initiate Partial Read
	0x4F = Upload Transfer

Tab. 4: Class-IDs für Funktionstyp read-only (Forts.)

Class-ID	Service-Codes
0x38 = S-Partial Pressure Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x4C = Get Instance List
	0x4D = Get Pressures
	0x4E = Get All Pressures
0x40 = S-Sensor Calibration Object	0x0E = Get Attribute Single
	0x4B = Get all Instances
0x41 = Event Log Object	0x0E = Get Attribute Single
	0x18 = Get Member
0x42 = Motion Device Axis Object	0x03 = Get Attribute List
	0x0E = Get Attribute Single
	0x4B = Get Axis Attributes List
	0x50 = Get Motor Test Data
	0x52 = Get Inertia Test Data
0x43 = Time Sync Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x0E = Get Attribute Single
0x44 = Modbus Object	0x0E = Get Attribute Single
	0x4B = Read Discrete Inputs
	0x4C = Read Coils
	0x4D = Read Input Registers
0x45 = Modbus Object	0x4E = Read Holding Registers
	0x4C = Connection Read
0x45 = Originator Connection List Object	0x4C = Connection Read
	0x4C = Connection Read
0x46 = Modbus Serial Link Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x47 = Device Level Ring (DLR) Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x18 = Get Member
0x48 = CoS Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x4D = Target Connection List Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x4E = Base Energy Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x0E = Get Attribute Single
	0x18 = Get Member
0x4F = Electrical Energy Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x0E = Get Attribute Single

Tab. 4: Class-IDs für Funktionstyp read-only (Forts.)

Class-ID	Service-Codes
0x50 = Non-Electrical Energy Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x0E = Get Attribute Single
0x51 = Base Switch Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x52 = SNMP Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x53 = Power Management Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x0E = Get Attribute Single
	0x18 = Get Member
0x54 = RSTP Bridge Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x55 = RSTP Port Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x91 = ANSI Extended Symbol Segment	0x03
	0x55
0x6B	0x55
0x6C	0x01
0xAC	0x01
	0x4C
0xB2	0x08
	0x4E
	0x4F
0xF3 = Connection Configuration Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x4C = Open Connection
	0x4D = Close Connection
	0x4E = Stop Connection
0x50 = Get Status	
0xF4 = Port Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0xF5 = TCP/IP Interface Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0xF6 = EtherNet Link Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x300 = Module Diagnostics	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x301 = Input/OCnx	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x302 = Local Slaves	0x01 = Get Attributes All
	0x0E = Get Attribute Single

Tab. 4: Class-IDs für Funktionstyp read-only (Forts.)

Class-ID	Service-Codes
0x400 = Service Port Control Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x401 = Dynamic IO Control Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x402 = Router Diagnostics Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x403 = Router Routing Table Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x404 = SMTP	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x405 = SNTP	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x406 = HSBY	0x01 = Get Attributes All
	0x0E = Get Attribute Single

- Ein Paket mit *Class-ID=0x06* enthält eingebettete CIP-Messages. In diesem Fall führt das Gerät eine zusätzliche Stufe von DPI für die Datenpakete durch, welche die *Service Code*-Werte 0x4E, 0x52, 0x54 und 0x5B enthalten. Das Gerät blockiert ein Datenpaket, wenn es andere als die vorstehenden *Service Code*-Werte für diese *Class-ID* enthält.

Tab. 5: Class-IDs für Funktionstyp read-write

Class-ID	Service-Codes
0x01 = Identity	0x01=Get Attributes All
	0x0E= Get Attribute Signal
	0x10= Set Attribute Signal
	0x11= Find Next Object Instance
	0x18= Get Member
0x02 = Message Router	0x01= Get Attributes All
	0x0E = Get Attribute Single
	0x4B = Write Data Table (Rockwell)
	0x54
0x04 = Assembly	0x08 = Create
	0x09 = Delete
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x18 = Get Member
	0x19 = Set Member
	0x1A = Insert Member
	0x1B = Remove Member
	0x4B
	0x4C

Tab. 5: Class-IDs für Funktionstyp read-write (Forts.)

Class-ID	Service-Codes
0x05 = Connecti on	0x05 = Reset
	0x08 = Create
	0x09 = Delete
	0x0D = Apply Attri butes
	0x0E = Get Attri bute Singl e
	0x10 = Set Attri bute Singl e
	0x11 = Fi nd Next Obj ect Instance
	0x4B = Connecti on Bi nd
	0x4C = Producti on Appli cati on Lookup
	0x4E = Safety Cl ose
	0x54 = Safety Open
0x06 = Off-Li nk Connecti on Manager <sup>1</sup>	0x01 = Get Attri butes Al l
	0x02 = Set Attri butes Al l
	0x0E = Get Attri bute Singl e
	0x10 = Set Attri bute Singl e
	0x4C
	0x4E = Forward Cl ose
	0x52 = Unconnected Send
	0x54 = Forward Open
	0x56 = Get Connecti on Data
	0x57 = Search Connecti on Data
	0x59
	0x5A = Get Connecti on Owner
	0x5B = Large Forward Open
0x07 = Regi ster	0x0E = Get Attri bute Singl e
	0x10 = Set Attri bute Singl e
0x08 = Di screte Input Poi nt	0x01 = Get Attri butes Al l
	0x02 = Set Attri butes Al l
	0x0E = Get Attri bute Singl e
	0x10 = Set Attri bute Singl e
0x09 = Di screte Output Poi nt	0x01 = Get Attri butes Al l
	0x02 = Set Attri butes Al l
	0x0E = Get Attri bute Singl e
	0x10 = Set Attri bute Singl e
0x0A = Anal og Input Poi nt	0x01 = Get Attri butes Al l
	0x02 = Set Attri butes Al l
	0x0E = Get Attri bute Singl e
	0x10 = Set Attri bute Singl e
0x0B = Anal og Output Poi nt	0x01 = Get Attri butes Al l
	0x02 = Set Attri butes Al l
	0x0E = Get Attri bute Singl e
	0x10 = Set Attri bute Singl e

Tab. 5: Class-IDs für Funktionstyp read-write (Forts.)

Class-ID	Service-Codes
0x0E = Presence Sensing	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x0F = Parameter	0x01 = Get Attributes All
	0x05 = Reset
	0x0D = Apply Attributes
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x15 = Restore
	0x16 = Save
	0x18 = Get Member
0x10 = Parameter Group	0x4B = Get Enum String
	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x12 = Group	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x1D = Discrete Input Group	0x01 = Get Attributes All
	0x02 = Set Attributes All
	0x0E = Get Attribute Single
0x1E = Discrete Output Group	0x10 = Set Attribute Single
	0x01 = Get Attributes All
	0x02 = Set Attributes All
0x1F = Discrete Group	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x01 = Get Attributes All
0x20 = Analog Input Group	0x0E = Get Attribute Single
	0x02 = Set Attributes All
	0x10 = Set Attribute Single
	0x01 = Get Attributes All
0x21 = Analog Output Group	0x02 = Set Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x01 = Get Attributes All
0x22 = Analog Group	0x02 = Set Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single

Tab. 5: Class-IDs für Funktionstyp read-write (Forts.)

Class-ID	Service-Codes
0x23 = Position Sensor Object	0x05 = Reset
	0x0D = Apply Attributes
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x15 = Restore
	0x16 = Save
	0x18 = Get Member
0x24 = Position Controller Supervisor Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x25 = Position Controller Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x26 = Block Sequencer Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x27 = Command Block Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x28 = Motor Data Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x15 = Restore
0x29 = Control Supervisor Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x2A = AC/DC Drive Object	0x05 = Reset
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x15 = Restore
0x2B = Acknowledge Handler Object	0x16 = Save
	0x08 = Create
	0x09 = Delete
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x2C = Overload Object	0x4B = Add AckData Path
	0x4C = Remove AckData Path
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x2D = Softstart Object	0x15 = Restore
	0x16 = Save
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x2E = Softstart Object	0x15 = Restore
	0x16 = Save
	0x0E = Get Attribute Single

Tab. 5: Class-IDs für Funktionstyp read-write (Forts.)

Class-ID	Service-Codes
0x2E = Selection Object	0x05 = Reset
	0x06 = Start
	0x07 = Stop
	0x08 = Create
	0x09 = Delete
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x18 = Get Member
	0x19 = Set Member
	0x1A = Insert Member
	0x1B = Remove Member
0x30 = S-Device Supervisor Object	0x05 = Reset
	0x06 = Start
	0x07 = Stop
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x4B = Abort
	0x4C = Recover
0x4E = Perform Diagnostics	
0x31 = S-Analog Sensor Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x4B = Zero Adjust
	0x4C = Gain Adjust
0x32 = S-Analog Actuator Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x33 = S-Single Stage Controller Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x63 = Calibrate
0x34 = S-Gas Calibration Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x4B = Get All Instances
0x35 = Trip Point Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single

Tab. 5: Class-IDs für Funktionstyp read-write (Forts.)

Class-ID	Service-Codes
0x37 = File Object	0x06 = Start
	0x07 = Stop
	0x08 = Create
	0x09 = Delete
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x15 = Restore
	0x16 = Save
	0x18 = Get Member
	0x4B = Initiate Upload
	0x4C = Initiate Download
	0x4D = Initiate Partial Read
	0x4E = Initiate Partial Write
	0x4F = Upload Transfer
	0x50 = Download Transfer
	0x51 = Clear File
0x38 = S-Partial Pressure Object	0x01 = Get Attributes All
	0x08 = Create
	0x09 = Delete
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x4B = Create Range
	0x4C = Get Instance List
	0x4D = Get Pressures
0x40 = S-Sensor Calibration Object	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x4B = Get all Instances
	0x4E = Get All Pressures
0x41 = Event Log Object	0x05 = Reset
	0x06 = Start
	0x07 = Stop
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x18 = Get Member
	0x19 = Set Member
	0x1A = Insert Member
	0x1B = Remove Member

Tab. 5: Class-IDs für Funktionstyp read-write (Forts.)

Class-ID	Service-Codes
0x42 = Motion Device Axis Object	0x03 = Get Attribute List
	0x04 = Set Attribute List
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x1C = GroupSync
	0x4B = Get Axis Attributes List
	0x4C = Set Axis Attributes List
	0x4D = Set Cyclic Write List
	0x4E = Set Cyclic Read List
	0x4F = Run Motor Test
	0x50 = Get Motor Test Data
	0x51 = Run Inertia Test
	0x52 = Get Inertia Test Data
	0x53 = Run Hookup Test
	0x54 = Get Hookup Test Data
	0x43 = Time Sync Object
0x03 = Get Attribute List	
0x04 = Set Attribute List	
0x0E = Get Attribute Single	
0x10 = Set Attribute Single	
0x44 = Modbus Object	0x0E = Get Attribute Single
	0x4B = Read Discrete Inputs
	0x4C = Read Coils
	0x4D = Read Input Registers
	0x4E = Read Holding Registers
	0x4F = Write Coils
	0x50 = Write Holding Registers
0x51 = Modbus Passthrough	
0x45 = Originator Connection List Object	0x08 = Create
	0x09 = Delete
	0x4C = Connection Read
0x46 = Modbus Serial Link Object	0x01 = Get Attributes All
	0x05 = Reset
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x4B = Get And Clear

Tab. 5: Class-IDs für Funktionstyp read-write (Forts.)

Class-ID	Service-Codes
0x47 = Device Level Ring (DLR) Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x18 = Get Member
	0x4B = Verify Fault Location
	0x4C = Clear Rapid Faults
	0x4D = Restart Sign On
	0x4E = Clear Gateway Partial Fault
0x48 = CoS Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x4D = Target Connection List Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x4C = Connection Read
0x4E = Base Energy Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x04 = Set Attribute List
	0x05 = Reset
	0x08 = Create
	0x09 = Delete
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x18 = Get Member
	0x19 = Set Member
	0x1A = Insert Member
	0x1B = Remove Member
	0x4B = Start Metering
	0x4C = Stop Metering
0x4F = Electrical Energy Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x0E = Get Attribute Single
0x50 = Non-Electrical Energy Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x0E = Get Attribute Single
0x51 = Base Switch Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x52 = SNMP Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single

Tab. 5: Class-IDs für Funktionstyp read-write (Forts.)

Class-ID	Service-Codes
0x53 = Power Management Object	0x01 = Get Attributes All
	0x03 = Get Attribute List
	0x04 = Set Attribute List
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x18 = Get Member
	0x19 = Set Member
	0x4D = Power Management
	0x4E = Set Pass Code
	0x4F = Clear Pass Code
0x54 = RSTP Bridge Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x55 = RSTP Port Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0x91 = ANSI Extended Symbol Segment	0x03
	0x55
0x6B	0x55
0x6C	0x01
0xAC	0x01
	0x4C
0xB2	0x08
	0x4E
	0x4F
0xF3 = Connection Configuration Object	0x01 = Get Attributes All
	0x02 = Set Attributes All
	0x08 = Create
	0x09 = Delete
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x15 = Restore
	0x4B = Kick Timer
	0x4C = Open Connection
	0x4D = Close Connection
	0x4E = Stop Connection
	0x4F = Change Start
	0x50 = Get Status
	0x51 = Change Complete
	0x52 = Audit Changes

Tab. 5: Class-IDs für Funktionstyp read-write (Forts.)

Class-ID	Service-Codes
0xF4 = Port Object	0x01 = Get Attributes All
	0x05 = Reset
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0xF5 = TCP/IP Interface Object	0x01 = Get Attributes All
	0x02 = Set Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
0xF6 = EtherNet Link Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x10 = Set Attribute Single
	0x4C = Get And Clear
0x300 = Module Diagnostics	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x301 = Input/Output	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x302 = Local Slaves	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x400 = Service Port Control Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x401 = Dynamic I/O Control Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x402 = Router Diagnostics Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x403 = Router Routing Table Object	0x01 = Get Attributes All
	0x0E = Get Attribute Single
0x404 = SMP	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x32 = Clear All
0x405 = SNMP	0x01 = Get Attributes All
	0x0E = Get Attribute Single
	0x32 = Clear All
0x406 = HSBY	0x01 = Get Attributes All
	0x0E = Get Attribute Single

- Ein Paket mit *Class-ID=0x06* enthält eingebettete CIP-Messages. In diesem Fall führt das Gerät eine zusätzliche Stufe von DPI für die Datenpakete durch, welche die *Service Code*-Werte *0x4E*, *0x52*, *0x54* und *0x5B* enthalten. Das Gerät blockiert ein Datenpaket, wenn es andere als die vorstehenden *Service Code*-Werte für diese *Class-ID* enthält.

**[Liste der PCCC-Befehlscodes für unterschiedliche Funktionstypen]**

Tab. 6: PCCC-Befehlscodes für Funktionstyp *read-only*

Befehlscodes	Funktionscodes
0x0F	0x04
	0x09
	0xA7
	0xA2
	0x17
	0x29
	0x68
	0x01
0x01	None
0x04	None
0x06	0x00
	0x01
	0x03
	0x09

Tab. 7: PCCC-Befehlscodes für Funktionstyp *read-write*

Befehlscodes	Funktionscodes
0x00	None

Tab. 7: PCCC-Befehlscodes für Funktionstyp *read-write* (Forts.)

Befehlscodes	Funktionscodes
0x0F	0x02
	0x04
	0x03
	0x5E
	0x09
	0x08
	0xA7
	0xAF
	0xA2
	0xAA
	0x17
	0x26
	0x79
	0x29
	0x0A
	0x12
	0x68
	0x67
	0x53
	0x55
	0x06
	0x01
	0x00
	0x18
0x01	None
0x02	None
0x03	None
0x04	None
0x05	None
0x06	0x03
	0x00
	0x01
	0x09
	0x07
	0x08
	0x06
	0x0A
	0x05
	0x04
0x02	

Tab. 7: PCCC-Befehlscodes für Funktionstyp *read-write* (Forts.)

Befehlscodes	Funktionscodes
0x07	0x00
	0x01
	0x03
0x08	None

Tab. 8: PCCC-Befehlscodes für Funktionstypen *any* und *advanced*

Befehlscodes	Funktionscodes
0x00	None

Tab. 8: PCCC-Befehlscodes für Funktionstypen *any* und *advanced* (Forts.)

Befehlscodes	Funktionscodes
0x0F	0x8F
	0x02
	0x3A
	0x82
	0x41
	0x50
	0x52
	0x05
	0x04
	0x03
	0x11
	0x57
	0x5E
	0x81
	0x09
	0x08
	0xA7
	0xAF
	0xA2
	0xAA
	0x17
	0x26
	0x79
	0x29
	0x0A
	0x12
	0x3A
	0x80
	0x07
	0x68
	0x67
	0x53
	0x55
	0x06
0x01	
0x00	
0x18	
0x01	None
0x02	None
0x03	None
0x04	None
0x05	None

Tab. 8: PCCC-Befehlscodes für Funktionstypen *any* und *advanced* (Forts.)

Befehlscodes	Funktionscodes	
0x06	0x03	
	0x00	
	0x01	
	0x09	
	0x07	
	0x08	
	0x06	
	0x0A	
	0x05	
	0x04	
	0x02	
	0x07	0x00
		0x01
0x03		
0x04		
0x05		
0x06		
0x08	None	

## 4.7 DoS

[Netzicherheit > 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.

#### Null-Scan Filter

Aktiviert/deaktiviert den Null-Scan-Filter.

Das Gerät erkennt und verwirft eingehende TCP-Datenpakete mit den folgenden Eigenschaften:

- Keine TCP-Flags sind gesetzt.
- Die TCP-Sequenznummer ist 0.

Mögliche Werte:

**markiert**

Der Filter ist aktiv.

**unmarkiert** (Voreinstellung)

Der Filter ist inaktiv.

#### Xmas Filter

Aktiviert/deaktiviert den Xmas-Filter.

Das Gerät erkennt und verwirft eingehende TCP-Datenpakete mit den folgenden Eigenschaften:

- Die TCP-Flags *FIN*, *URG* und *PSH* sind gleichzeitig gesetzt.
- Die TCP-Sequenznummer ist 0.

Mögliche Werte:

**markiert**

Der Filter ist aktiv.

**unmarkiert** (Voreinstellung)

Der Filter ist inaktiv.

#### SYN/FIN Filter

Aktiviert/deaktiviert den SYN/FIN-Filter.

Das Gerät erkennt eingehende Datenpakete mit gleichzeitig gesetzten TCP-Flags *SYN* und *FIN* und verwirft diese.

Mögliche Werte:

`markiert`

Der Filter ist aktiv.

`unmarkiert` (Voreinstellung)

Der Filter ist inaktiv.

#### TCP-Offset Schutz

Aktiviert/deaktiviert den TCP-Offset-Schutz.

Der TCP-Offset-Schutz erkennt eingehende TCP-Datenpakete, deren Fragment-Offset-Feld des IP-Headers gleich 1 ist und verwirft diese.

Der TCP-Offset-Schutz akzeptiert UDP- und ICMP-Pakete mit Fragment-Offset-Feld des IP-Headers gleich 1.

Mögliche Werte:

`markiert`

Der Schutz ist aktiv.

`unmarkiert` (Voreinstellung)

Der Schutz ist inaktiv.

#### TCP-SYN Schutz

Aktiviert/deaktiviert den TCP-SYN-Schutz.

Der TCP-SYN-Schutz erkennt eingehende Datenpakete mit gesetztem TCP-Flag SYN und L4-Quell-Port <1024 und verwirft diese.

Mögliche Werte:

`markiert`

Der Schutz ist aktiv.

`unmarkiert` (Voreinstellung)

Der Schutz ist inaktiv.

#### L4-Port Schutz

Aktiviert/deaktiviert den L4-Port-Schutz.

Der L4-Port-Schutz erkennt eingehende TCP- und UDP-Datenpakete, bei denen Quell-Port-Nummer und Ziel-Port-Nummer identisch sind, und verwirft diese.

Mögliche Werte:

`markiert`

Der Schutz ist aktiv.

`unmarkiert` (Voreinstellung)

Der Schutz ist inaktiv.

#### Min.-Header-Size Filter

Aktiviert/deaktiviert den Minimal-Header-Filter.

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

Mögliche Werte:

`markiert`

Der Filter ist aktiv.

`unmarkiert` (Voreinstellung)

Der Filter ist inaktiv.

Min. Größe TCP-Header

Zeigt die minimale Größe eines gültigen TCP-Headers.

## IP

Land-Attack Filter

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

Mögliche Werte:

`markiert`

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

`unmarkiert` (Voreinstellung)

Der Filter ist inaktiv.

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:

`markiert` (Voreinstellung)

Der Filter ist aktiv. Das Gerät verwirft IP-Datenpakete mit einem festgelegten Routing-Pfad im IP-Header.

`unmarkiert`

Der Filter ist inaktiv.

## ICMP

Dieser Dialog bietet Ihnen Filtermöglichkeiten für folgende ICMP-Parameter:

- Fragmentierte Datenpakete
- ICMP-Pakete ab einer bestimmten Größe

Fragmentierte Pakete filtern

Aktiviert/deaktiviert den Filter für fragmentierte ICMP-Pakete.

Der Filter erkennt fragmentierte ICMP-Pakete und verwirft diese.

Mögliche Werte:

`markiert`

Der Filter ist aktiv.

`unmarkiert` (Voreinstellung)

Der Filter ist inaktiv.

Anhand Paket-Größe verwerfen

Aktiviert/deaktiviert den Filter für eingehende ICMP-Pakete.

Der Filter erkennt ICMP-Pakete, deren Payload-Größe die im Feld *Erlaubte Payload-Größe [Byte]* festgelegte Größe überschreitet und verwirft diese.

Mögliche Werte:

`markiert`

Der Filter ist aktiv.

`unmarkiert` (Voreinstellung)

Der Filter ist inaktiv.

Erlaubte Payload-Größe [Byte]

Legt die maximal erlaubte Payload-Größe von ICMP-Paketen in Byte fest.

Mögliche Werte:

`0..1472` (Voreinstellung: `512`)



## 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 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 Parameter der Security Association (SA) 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 [Verbindungsfehler](#) 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 [Max. Aktive Verbindungen](#) 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 [Verbindungen \(max.\)](#) gezeigten Wert. Das Gerät beschränkt außerdem die maximale Anzahl von aktiven VPN-Tunneln auf den im Feld [Max. Aktive Verbindungen](#) festgelegten Wert.

Mögliche Werte:

[markiert](#)

Der VPN-Tunnel ist aktiv.

[unmarkiert](#)

Der VPN-Tunnel ist inaktiv.

### Used IKE version

Zeigt die Version des IKE-Protokolls, das der VPN-Tunnel verwendet.

Mögliche Werte:

[ikev1](#)

Das Gerät verwendet das IKE-Protokoll Version 1 (ISAKMP).

[ikev2](#)

Das Gerät verwendet das IKE-Protokoll Version 2.

## Startup

Zeigt die Ausgangsrolle zur Aushandlung des Schlüsselaustauschs für den VPN-Tunnel.

Mögliche Werte:

### `initiator`

Wenn Sie das Gerät als *Initiator* für den VPN-Tunnel festlegen, dann initiiert das Gerät aktiv den Internet Key Exchange (IKE) und die Parameterverhandlung.

### `responder`

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:

### `up`

VPN-Tunnel ist aufgebaut.

### `down`

VPN-Tunnel ist nicht aufgebaut.

### `negotiation`

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.

### `constructing`

Die IKE-SA ist aktiv. Das Gerät hat für diese Instanz jedoch mindestens eine nicht hergestellte IPsec-SA erkannt.

### `dormant`

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.

### `re-keying`

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 *IKE key agreement*, *IKE integrity (MAC)* und *IKE encryption*.

Wenn Sie in dem Dialog [Virtual Private Network > Verbindungen](#) 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 *IPsec key agreement*, *IPsec integrity (MAC)* und *IPsec encryption*.

Wenn Sie einen IPsec-Algorithmus für die Instanz im Dialog [Virtual Private Network > Verbindungen](#) 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 *Verbindungen (max.)* gezeigten Wert. Das Gerät beschränkt außerdem die maximale Anzahl von aktiven VPN-Tunneln auf den im Feld *Max. Aktive Verbindungen* festgelegten Wert.

Mögliche Werte:

`markiert`

Der VPN-Tunnel ist aktiv.

`unmarkiert`

Der VPN-Tunnel ist inaktiv.

#### Tunnel index

Zeigt den Indexwert, der zusammen mit dem Wert in Spalte *VPN index* den Eintrag in der Verbindungstunnel-Infotabelle identifiziert.

#### Traffic selector index

Zeigt den Indexwert, der zusammen mit dem Wert in Spalte *VPN index* den Eintrag in der Traffic-Selector-Tabelle identifiziert, der auf den IPsec-Tunnel abgebildet ist.

Mögliche Werte:

`0`

Der Index des Traffic-Selectors ist unbekannt.

`1..16`

#### Betriebsstatus

Zeigt den gegenwärtigen Status des VPN-Tunnels.

Mögliche Werte:

`up`

Die Internet Key Exchange Security Association (IKE-SA) und jede Internet Protocol Security-Security Association (IPsec-SA) ist aktiv.

`down`

Die IKE-SA und IPsec-SAs sind inaktiv.

#### negotiation

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.

#### constructing

Die IKE-SA ist aktiv. Das Gerät hat für diese Instanz jedoch mindestens eine nicht hergestellte IPsec-SA erkannt.

#### dormant

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.

#### re-keying

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:

### unbekannt

Der IPsec-Vorschlag wird ausgeführt. Für diese IPsec-SA wurden keine Traffic-Selectors oder Sicherheitsparameter ausgehandelt.

### created

Schlüsselaustausch und Algorithmus für die Aushandlung ist für diese IPsec-SA abgeschlossen, der Tunnel ist jedoch inaktiv.

### routed

Die Richtlinien für die Verschlüsselung des Datenstroms sind eingerichtet, der Aushandlungsprozess hat jedoch noch nicht begonnen.

### installing

Die Authentifizierung der Peers ist eingerichtet, aber der IPsec-Vorschlag für diesen Tunnel wird noch ausgeführt.

### installed

Die IPsec-SA ist installiert.

### updating

Das Gerät aktualisiert die Sicherheitszuordnung.

### re-keying

Der Schlüsselaustausch für diesen IPsec-SA wird ausgeführt. Das Gerät zeigt den Wert nach Ablauf des IPsec Lifetime-Timers.

### re-keyed

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.

### re-trying

Der Schlüsselaustausch für diesen IPsec-SA ist fehlgeschlagen. Das Gerät versucht automatisch, einen neuen Schlüsselaustausch zu initiieren.

### deleting

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.

### destroying

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 Security Association (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 [Verbindungen \(max.\)](#) gezeigten Wert. Das Gerät beschränkt außerdem die maximale Anzahl von aktiven VPN-Tunneln auf den im Feld [Max. Aktive Verbindungen](#) festgelegten Wert.

Mögliche Werte:

[markiert](#)

Der VPN-Tunnel ist aktiv.

[unmarkiert](#)

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 *Zertifikat hochladen*, um der Tabelle ein digitale Zertifikat hinzuzufügen.

- Im Feld *Passphrase (privater Schlüssel)* geben Sie die in diesem digitalen Zertifikat verwendete Passphrase ein.  
Mögliche Werte:
  - Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen
- Im Feld *URL* 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 SCP oder SFTP zum Gerät übertragen.

Führen Sie die folgenden Schritte aus:

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

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

Übertragen Sie die Datei auf das Gerät in das Verzeichnis /upl oad/vpn-cert .

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 ok im Verzeichnis /upl oad/vpn-cert und löscht die übertragene Datei.

#### Index

Zeigt den Index der Tabellenzeile des digitalen Zertifikats.

Mögliche Werte:

1..100

#### 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 den Zeitpunkt (Datum und Uhrzeit), seit dem 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:

[ca](#)

Die übertragene Datei ist ein digitales Zertifikat, das von einer Zertifizierungsstelle (CA) signiert wurde.

[peer](#)

Die übertragene Datei ist ein Peer-Zertifikat.

[pkcs12](#)

Die übertragene Datei ist ein p12-Bundle.

[encr ypt edkey](#)

Die übertragene Datei ist eine Schlüsseldatei mit Passwortverschlüsselung.

[encr ypt edpkcs12](#)

Die übertragene Datei ist ein p12-Bundle mit Passwortverschlüsselung.

#### Hochgeladen am

Zeigt den Zeitpunkt (Datum und Uhrzeit), zu dem 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:

[kein](#)

Das Peer-Zertifikat enthält keinen privaten Schlüssel.

[vorhanden](#)

Das Gerät hat den privaten Schlüssel gefunden und aus dem Peer-Zertifikat extrahiert.

[not Found](#)

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:

[0 . 256](#)

## 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 *Erstellen*, um eine Tabellenzeile hinzuzufügen.

- In der Dropdown-Liste *VPN Beschreibung* wählen Sie eine vorhandene Beschreibung oder legen eine neue Beschreibung fest. Um eine neue Beschreibung einzugeben, klicken Sie die Schaltfläche **+**.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen

- Im Feld *Traffic selector index* legen Sie den Index des Traffic-Selektors für den VPN-Tunnel fest.

Mögliche Werte:

1..16



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 „[\[Wizard: VPN-Konfiguration\]](#)“ auf Seite 281.

#### 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 *VPN index* den Eintrag in der Traffic-Selektor-Tabelle identifiziert.

Mögliche Werte:

1..16

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 *Verbindungen (max.)* gezeigten Wert. Das Gerät beschränkt außerdem die maximale Anzahl von aktiven VPN-Tunneln auf den im Feld *Max. Aktive Verbindungen* gezeigten Wert.

Mögliche Werte:

*markiert*

Der VPN-Tunnel ist aktiv.

*unmarkiert* (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

*any* (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 `<Protokol l /Port t>` festgelegt sind. Das Gerät sendet ausschließlich den festgelegten Datentyp durch den VPN-Tunnel.

Beispiele:

- `tcp/http` entspricht `6/80`
- `udp` entspricht `udp/any`
- `/53` entspricht `any/53`

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

`<leer>` (Voreinstellung)

Das Gerät verwendet `any/any` 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

`any` (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 `<Protokol l /Port t>` festgelegt sind. Das Gerät erwartet vom VPN-Tunnel ausschließlich den festgelegten Datentyp.

Beispiele:

- `tcp/http` entspricht `6/80`
- `udp` entspricht `udp/any`
- `/53` entspricht `any/53`

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

`<leer>` (Voreinstellung)

Das Gerät verwendet `any/any` als Einschränkung.

#### Version

Legt die Version des IKE-Protokolls für die VPN-Verbindung fest.

Mögliche Werte:

`auto` (Voreinstellung)

Das VPN startet mit dem Protokoll IKEv2 als *Initiator* und akzeptiert IKEv1/v2 als *Responder*.

**i kev1**

Das VPN startet mit dem Protokoll IKEv1.

**i kev2**

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 *Ferner Endpunkt* den Wert *any* festlegen, kann das Gerät die Verbindung nicht initiieren.

Mögliche Werte:

**i n i t i a t o r**

Wenn Sie festlegen, dass das Gerät als *Initiator* startet, dann beginnt das Gerät das Austauschen der Schlüssel mit dem *Responder*.

**r e s p o n d e r** (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.

## IKEv1 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.

Das Gerät unterstützt die Funktion *IKEv1 DPD Timeout [s]* mittels IKEv1.

Mögliche Werte:

**0**

Deaktiviert die Funktion.

**1. . 86400 (24 h)** (Voreinstellung: 120)

## 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:

**300. . 86400** (Voreinstellung: 28800)

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:

[mai n](#) (Voreinstellung)

Der Hauptmodus für Phase 1 bietet Identitätsschutz.

[aggressi ve](#)

Zur Reduzierung von Roundtrips verwenden Sie den Aggressive Mode.

Authentifizierung

Legt den Authentifizierungstyp fest, den das Gerät verwendet.

Mögliche Werte:

[psk](#) (Voreinstellung)

Wählen Sie diesen Wert aus, damit das Gerät einen zuvor generierten und auf den entfernten und lokalen Geräten gespeicherten Schlüssel verwendet.

[i ndi vi dual x509](#)

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.

[pkcs12](#)

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 [Authentifizierung](#) der Wert [psk](#) 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 *Authentifizierung* der Wert *i ndi vi dual x509* 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 *Authentifizierung* festlegen:

– *i ndi vi dual x509*

Das digitale Zertifikat bindet die Identität des lokalen Peers an den festgelegten öffentlichen Schlüssel, den die in Spalte *IKE auth. cert. CA* festgelegte Zertifizierungsstelle (Certification Authority, CA) signiert hat.

– *pkcs12*

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 *IKE auth. cert. CA* 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 *Authentifizierung* der Wert *i ndi vi dual x509* 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 *Authentifizierung* ist der Wert *i ndi vi dual x509* festgelegt.
- Der im Gerät gespeicherte Schlüssel wird mit einer Passphrase verschlüsselt.

Der Schlüssel erfordert, dass Sie in Spalte *Verschlüsselter Key/PKCS12-Passphrase* 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 *Encrypted private key* oder im *pkcs12*-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 *IKE local ID* verwendet.

Mögliche Werte:

*default* (Voreinstellung)

Das Verhalten ist abhängig von dem Wert, den Sie in Spalte *Authentifizierung* festlegen:

– *psk*

Das Gerät verwendet die in Spalte *Lokaler Endpunkt* festgelegte IP-Adresse als lokale Kennung.

– *individual x509* oder *pkcs12*

Das Gerät verwendet den im lokalen *IKE auth. cert. local*-Zertifikat enthaltenen Distinguished Name (DN).

*address*

In Spalte *IKE local ID* verwendet das Gerät die IP-Adresse oder den Hostnamen aus Spalte *Lokaler Endpunkt*.

*id*

Das Gerät identifiziert den in Spalte *IKE local ID* 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 *foo.bar.com*
- eine E-Mail-Adresse
- Den in Spalte *IKE auth. cert. remote* 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 in Spalte *IKE Local-Identifizier Typ* festgelegt ist.

Mögliche Werte:

<leer> (Voreinstellung)

Wenn Sie in Spalte *IKE Local-Identifizier Typ* den Wert *i d* 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 `foo.bar.com`
- eine E-Mail-Adresse
- Ein X.500 Distinguished Name

Benutzen Sie zum Hinzufügen eines Eintrags die folgende Syntax als Beispiel:

`CN = XY-D, C = DE, L = NT, ST = BW O = COMPANY, OU = DEV, E = testuser@company.com`

#### Ferner Identifizier Typ

Legt den Typ der entfernten Peer-Kennung fest, die das Gerät für den Parameter *Remote-ID* verwendet.

Mögliche Werte:

*any* (Voreinstellung)

Das Gerät akzeptiert jede empfangene Kennung ohne weitergehende Überprüfung.

*address*

In Spalte *Remote-ID* verwendet das Gerät die IP-Adresse oder den Hostnamen aus Spalte *Ferner Endpunkt*.

*i d*

Das Gerät identifiziert den in Spalte *Remote-ID* festgelegten Wert als einen der folgenden Typen:

- eine IPv4-Adresse oder ein DNS-Hostname
- Schlüsselbezeichner, der festlegt, welche Daten das Gerät zur Weitergabe von herstellerspezifischen 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 `foo.bar.com`
- eine E-Mail-Adresse
- Den in Spalte *IKE auth. cert. remote* enthaltenen *ASN.1 X.500 Distinguished Name (DN)*. Die lokalen und entfernten Geräte tauschen ihre digitalen Zertifikate aus, um die Security Association (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, 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 in Spalte *Ferner Identifizier Typ* festgelegt ist.

Mögliche Werte:

<leer> (Voreinstellung)

Wenn Sie in Spalte *Ferner Identifizier Typ* den Wert *i d* 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 `foo.bar.com`

- eine E-Mail-Adresse
  - Ein X.500 Distinguished Name
- Benutzen Sie zum Hinzufügen eines Eintrags die folgende Syntax als Beispiel:  
CN = XY-D, C = DE, L = NT, ST = BW, O = COMPANY, OU = DEV, E = testuser@company.com

## IKE key agreement

Legt fest, welchen Diffie-Hellman- (DH-) Algorithmus zur Schlüsselvereinbarung das Gerät zur Ermittlung des IKE-SA-Sitzungsschlüssels verwendet.

Mögliche Werte:

[any](#)

Das Gerät akzeptiert jeden Algorithmus, wenn das Gerät als *Responder* festgelegt wurde.

[modp1024](#) (Voreinstellung)

Der Wert stellt einen RSA-Algorithmus mit 1024-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 2 gehört.

[modp1536](#)

Der Wert stellt einen RSA-Algorithmus mit 1536-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 5 gehört.

[modp2048](#)

Der Wert stellt einen RSA-Algorithmus mit 2048-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 14 gehört.

[modp3072](#)

Der Wert stellt einen RSA-Algorithmus mit 3072-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 15 gehört.

[modp4096](#)

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:

[any](#)

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.

[hmacmd5](#)

Das Gerät verwendet den Message-Digest-Algorithmus 5 (MD5) zur Berechnung der Hash-Funktion.

[hmacsha1](#) (Voreinstellung)

Das Gerät verwendet den Secure-Hash-Algorithmus Version 1 (SHA-1) zur Berechnung der Hash-Funktion.

[hmacsha256](#)

Das Gerät verwendet SHA-256 (Teil der Version-2-Familie) zur Berechnung der Hash-Funktion, die das Gerät mit 32-Bit-Wörtern berechnet.

#### [hmacsha384](#)

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.

#### [hmacsha512](#)

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 [hmacsha256](#) oder höher zu verwenden.

---

## IKE encryption

Legt den IKE-Verschlüsselungsalgorithmus fest, den das Gerät verwendet.

Mögliche Werte:

#### [any](#)

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.

#### [des](#)

Das Gerät verwendet die Data-Encryption-Standard- (DES)-Blockchiffre für die Verschlüsselung von Nachrichtendaten mit einem 56-Bit-Schlüssel.

#### [des3](#)

Das Gerät verwendet die Triple-DES-Blockchiffre für die Verschlüsselung von Nachrichtendaten, die den 56-Bit-Schlüssel des DES 3 Mal pro Block anwendet.

#### [aes128](#) (Voreinstellung)

Das Gerät verwendet Advanced Encryption Standard (AES) mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 128 Key-Bits.

#### [aes192](#)

Das Gerät verwendet AES mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 192 Key-Bits.

#### [aes256](#)

Das Gerät verwendet AES mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 256 Key-Bits.

---

**Anmerkung:**

Wir empfehlen, die Einstellung [aes128](#) oder höher zu verwenden.

---

## Lokaler Endpunkt

Legt den Hostnamen oder die IP-Adresse des lokalen IPsec-VPN-Tunnel-Endpunktes fest.

Mögliche Werte:

#### [any](#) (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:

[any](#) (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 *Version* den Wert *ikev1* festlegen, dann nimmt das Gerät stets die erneute Authentifizierung des VPN-Tunnels vor, selbst wenn Sie die Markierung des Kontrollkästchens aufheben.

Mögliche Werte:

[markiert](#)

Das Gerät generiert eine neue IKE-SA und versucht, die IPsec SAs erneut zu generieren.

[unmarkiert](#) (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:

[any](#)

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.

[modp1024](#) (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.

[modp1536](#)

Der Wert stellt einen RSA-Algorithmus mit 1536-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 5 gehört.

[modp2048](#)

Der Wert stellt einen RSA-Algorithmus mit 2048-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 14 gehört.

[modp3072](#)

Der Wert stellt einen RSA-Algorithmus mit 3072-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 15 gehört.

#### [modp4096](#)

Der Wert stellt einen RSA-Algorithmus mit 4096-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 16 gehört.

#### [kein](#)

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:

#### [any](#)

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.

#### [hmacmd5](#)

Das Gerät verwendet den Message-Digest-Algorithmus 5 (MD5) zur Berechnung der Hash-Funktion.

#### [hmacsha1](#) (Voreinstellung)

Das Gerät verwendet den Secure-Hash-Algorithmus Version 1 (SHA-1) zur Berechnung der Hash-Funktion.

#### [hmacsha256](#)

Das Gerät verwendet SHA-256 (Teil der Version-2-Familie) zur Berechnung der Hash-Funktion, die das Gerät mit 32-Bit-Wörtern berechnet.

#### [hmacsha384](#)

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.

#### [hmacsha512](#)

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 [hmacsha256](#) oder höher zu verwenden.

---

### IPsec encryption

Legt den IPsec-Verschlüsselungsalgorithmus fest, den das Gerät verwendet.

Mögliche Werte:

#### [any](#)

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.

#### [des](#)

Das Gerät verwendet die Data-Encryption-Standard- (DES)-Blockchiffre für die Verschlüsselung von Nachrichtendaten mit einem 56-Bit-Schlüssel.

#### [des3](#)

Das Gerät verwendet die Triple-DES-Blockchiffre für die Verschlüsselung von Nachrichtendaten, die den 56-Bit-Schlüssel des DES 3 Mal pro Block anwendet.

**aes128** (Voreinstellung)

Das Gerät verwendet Advanced Encryption Standard (AES) mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 128 Key-Bits.

**aes192**

Das Gerät verwendet AES mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 192 Key-Bits.

**aes256**

Das Gerät verwendet AES mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 256 Key-Bits.

**aes128ctr**

AES-CTR mit 128 Key-Bits.

**aes192ctr**

AES-CTR mit 192 Key-Bits.

**aes256ctr**

AES-CTR mit 256 Key-Bits.

**aes128gcm64**

Das Gerät verwendet AES-Galois/Counter Mode (GCM) mit einem 64-Bit-ICV (Integrity Check Value) und 128 Key-Bits.

**aes128gcm96**

AES-GCM mit einem 96-Bit-ICV und 128 Key-Bits.

**aes128gcm128**

AES-GCM mit einem 128-Bit-ICV und 128 Key-Bits.

**aes192gcm64**

AES-GCM mit einem 64-Bit-ICV und 192 Key-Bits.

**aes192gcm96**

AES-GCM mit einem 96-Bit-ICV und 192 Key-Bits.

**aes192gcm128**

AES-GCM mit einem 128-Bit-ICV und 192 Key-Bits.

**aes256gcm64**

AES-GCM mit einem 64-Bit-ICV und 256 Key-Bits.

**aes256gcm96**

AES-GCM mit einem 96-Bit-ICV und 256 Key-Bits.

**aes256gcm128**

AES-GCM mit einem 128-Bit-ICV und 256 Key-Bits.

---

**Anmerkung:**

Wir empfehlen, die Einstellung [aes128](#) 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:

[300](#) . [28800](#) (Voreinstellung: [3600](#))

Die Voreinstellung ist eine Stunde. Maximal können 8 Stunden eingestellt werden.

#### Margin-Time [s]

Legt die Zeitspanne in Sekunden vor Ablauf der *IKE-Lifetime [s]* und der *IPsec lifetime [s]* fest, nach der das Gerät mit dem Aushandeln eines neuen Schlüssels beginnt.

Mögliche Werte:

1. . 1800 (Voreinstellung: 150)

Die Voreinstellung entspricht 2,5 Minuten. Der Maximalwert beträgt eine halbe Stunde.

#### Log informational entries

Aktiviert/deaktiviert Protokolleinträge ausschließlich für die Fehlersuche.

Mögliche Werte:

*markiert*

Das Gerät empfängt und verarbeitet die Informationsnachrichten für diesen VPN-Tunnel und trägt die Nachricht in das Ereignisprotokoll ein.

*unmarkiert* (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:

*markiert*

Das Gerät trägt die für diese Verbindung empfangenen Nachrichten, die nicht von strongSwan stammen, in das Ereignisprotokoll ein.

*unmarkiert* (Voreinstellung)

Das Gerät ignoriert sonstige für diese Verbindung empfangene Nachrichten, die nicht von strongSwan stammen.

## [Wizard: VPN-Konfiguration]

Im Fenster *Wizard* ermöglicht Ihnen, einen VPN-Tunnel einzurichten. Das Gerät ermöglicht Ihnen außerdem, direkt über den Dialog einen VPN-Tunnel hinzuzufügen oder zu ändern.

Das Fenster *Wizard* 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 *VPN index* und *VPN Beschreibung* einen VPN-Tunnel fest.

#### VPN index

Legt die Index-Nummer für den VPN-Tunnel fest.

Mögliche Werte:

1..256

#### 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 *IKE auth. cert. CA* 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 *Verschlüsselter Key/PKCS12-Passphrase* 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 *Encrypted private key* 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 *Encrypted private key* 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:

*any* (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:

*any* (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-Quelladresse 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-Quelladresse in dem Bereich enthält, der durch die IP-Quelladresse und die Netzmaske festgelegt ist.

#### Mögliche Werte:

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

[any](#) (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 `<Protokol /Port>` festgelegt sind. Das Gerät sendet ausschließlich den festgelegten Datentyp durch den VPN-Tunnel.

#### Beispiele:

- `tcp/http` entspricht `6/80`
- `udp` entspricht `udp/any`
- `/53` entspricht `any/53`

#### Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

`<Leer>` (Voreinstellung)

Das Gerät verwendet `any/any` 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

[any](#) (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 `<Protokol /Port>` festgelegt sind. Das Gerät erwartet vom VPN-Tunnel ausschließlich den festgelegten Datentyp.

#### Beispiele:

- `tcp/http` entspricht `6/80`
- `udp` entspricht `udp/any`
- `/53` entspricht `any/53`

#### Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

`<Leer>` (Voreinstellung)

Das Gerät verwendet `any/any` als Einschränkung.



Löscht die betreffende Tabellenzeile.

#### Hinzufügen

Fügt in der Tabelle *Add traffic selector* 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:

`1..1800` (Voreinstellung: `150`)

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:

**auto** (Voreinstellung)

Das VPN startet mit dem Protokoll IKEv2 als *Initiator* und akzeptiert IKEv1/v2 als *Responder*.

**i ke v1**

Das VPN startet mit dem Protokoll IKEv1 (ISAKMP).

**i ke v2**

Das VPN startet mit dem Protokoll IKEv2.

### Startup

Legt fest, ob das Gerät mit dieser Instanz als *Responder* oder *Initiator* startet.

Mögliche Werte:

**i n i t i a t o r**

Das Gerät beginnt das Austauschen der Schlüssel mit dem *Responder*.

**r e s p o n d e r** (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 *Ferner Endpunkt* den Wert **any** festlegen, dann unterbindet das Gerät das entfernte Gerät daran, die Verbindung zu initiieren.

### IKEv1 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.

Das Gerät unterstützt die Funktion *IKEv1 DPD Timeout [s]* mittels IKEv1.

Mögliche Werte:

**0**

Deaktiviert die Funktion.

**1.. 86400 (24 h)** (Voreinstellung: 120)

### 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:

**300.. 86400** (Voreinstellung: 28800)

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 *IKE local ID* verwendet.

Mögliche Werte:

*default* (Voreinstellung)

Das Verhalten ist abhängig von dem Wert, den Sie für die folgenden Authentifizierungsmethoden festlegen:

- *Pre-shared Key*  
Das Gerät verwendet die im Feld *Lokaler Endpunkt* festgelegte IP-Adresse als lokale Kennung. Sie finden das Feld *Lokaler Endpunkt* im Abschnitt „Endpoint and traffic selectors“ auf Seite 284.
- *X.509* oder *PKCS 12*  
Das Gerät verwendet den im lokalen *IKE auth. cert. local*-Zertifikat enthaltenen Distinguished Name (DN).

*address*

Im Feld *IKE local ID* verwendet das Gerät die IP-Adresse oder den Hostnamen aus Feld *Lokaler Endpunkt*. Sie finden das Feld *Lokaler Endpunkt* im Abschnitt „Endpoint and traffic selectors“ auf Seite 284.

*id*

Das Gerät identifiziert den im Feld *IKE local ID* 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 *foo.bar.com*
- eine E-Mail-Adresse
- Den im Feld *IKE auth. cert. remote* 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 *IKE Local-Identifizier Typ* festgelegt ist.

Mögliche Werte:

*<local ID>* (Voreinstellung)

Wenn Sie im Feld *IKE Local-Identifizier Typ* den Wert *id* 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 *foo.bar.com*
- eine E-Mail-Adresse
- Ein X.500 Distinguished Name

Benutzen Sie zum Hinzufügen eines Eintrags die folgende Syntax als Beispiel:

*CN = XY-D, C = DE, L = NT, ST = BW O = COMPANY, OU = DEV, E = testuser@exampl e.com*

## Ferner Identifier Typ

Legt den Typ der entfernten Peer-Kennung fest, die das Gerät für den Parameter *Remote-ID* verwendet.

Mögliche Werte:

*any* (Voreinstellung)

Das Gerät akzeptiert jede empfangene Kennung ohne weitergehende Überprüfung.

*address*

Im Feld *Remote-ID* verwendet das Gerät die IP-Adresse oder den Hostnamen aus Feld *Ferner Endpunkt*. Sie finden das Feld *Ferner Endpunkt* im Abschnitt „Endpoint and traffic selectors“ auf Seite 284.

*id*

Das Gerät identifiziert den im Feld *Remote-ID* 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 `foo.bar.com`
- eine E-Mail-Adresse
- Den im Feld *IKE auth. cert. remote* enthaltenen *ASN.1 X.500 Distinguished Name (DN)*. Die lokalen und entfernten Geräte tauschen ihre digitalen Zertifikate aus, um die Security Association (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, 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 *Ferner Identifier Typ* festgelegt ist.

Mögliche Werte:

*<Id>* (Voreinstellung)

Wenn Sie im Feld *Ferner Identifier Typ* den Wert *id* 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 `foo.bar.com`
- eine E-Mail-Adresse
- Ein X.500 Distinguished Name

Benutzen Sie zum Hinzufügen eines Eintrags die folgende Syntax als Beispiel:

`CN = XY-D, C = DE, L = NT, ST = BW O = COMPANY, OU = DEV, E = testuser@example.com`

## 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:

[main](#) (Voreinstellung)

Der Hauptmodus für Phase 1 bietet Identitätsschutz.

[aggressive](#)

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:

[any](#)

Das Gerät akzeptiert jeden Algorithmus, wenn das Gerät als *Responder* festgelegt wurde.

[modp1024](#) (Voreinstellung)

Der Wert stellt einen RSA-Algorithmus mit 1024-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 2 gehört.

[modp1536](#)

Der Wert stellt einen RSA-Algorithmus mit 1536-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 5 gehört.

[modp2048](#)

Der Wert stellt einen RSA-Algorithmus mit 2048-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 14 gehört.

[modp3072](#)

Der Wert stellt einen RSA-Algorithmus mit 3072-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 15 gehört.

[modp4096](#)

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:

[any](#)

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.

[hmacmd5](#)

Das Gerät verwendet den Message-Digest-Algorithmus 5 (MD5) zur Berechnung der Hash-Funktion.

[hmacsha1](#) (Voreinstellung)

Das Gerät verwendet den Secure-Hash-Algorithmus Version 1 (SHA-1) zur Berechnung der Hash-Funktion.

[hmacsha256](#)

Das Gerät verwendet SHA-256 (Teil der Version-2-Familie) zur Berechnung der Hash-Funktion, die das Gerät mit 32-Bit-Wörtern berechnet.

#### [hmacsha384](#)

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.

#### [hmacsha512](#)

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 [hmacsha256](#) oder höher zu verwenden.

---

## IKE encryption

Legt den IKE-Verschlüsselungsalgorithmus fest, den das Gerät verwendet.

Mögliche Werte:

#### [any](#)

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.

#### [des](#)

Das Gerät verwendet die Data-Encryption-Standard- (DES)-Blockchiffre für die Verschlüsselung von Nachrichtendaten mit einem 56-Bit-Schlüssel.

#### [des3](#)

Das Gerät verwendet die Triple-DES-Blockchiffre für die Verschlüsselung von Nachrichtendaten, die den 56-Bit-Schlüssel des DES 3 Mal pro Block anwendet.

#### [aes128](#) (Voreinstellung)

Das Gerät verwendet Advanced Encryption Standard (AES) mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 128 Key-Bits.

#### [aes192](#)

Das Gerät verwendet AES mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 192 Key-Bits.

#### [aes256](#)

Das Gerät verwendet AES mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 256 Key-Bits.

---

**Anmerkung:**

Wir empfehlen, die Einstellung [aes128](#) 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:

[300](#) . [28800](#) (Voreinstellung: [3600](#))

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:

[any](#)

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.

[hmacmd5](#)

Das Gerät verwendet den Message-Digest-Algorithmus 5 (MD5) zur Berechnung der Hash-Funktion.

[hmacsha1](#) (Voreinstellung)

Das Gerät verwendet den Secure-Hash-Algorithmus Version 1 (SHA-1) zur Berechnung der Hash-Funktion.

[hmacsha256](#)

Das Gerät verwendet SHA-256 (Teil der Version-2-Familie) zur Berechnung der Hash-Funktion, die das Gerät mit 32-Bit-Wörtern berechnet.

[hmacsha384](#)

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.

[hmacsha512](#)

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 [hmacsha256](#) oder höher zu verwenden.

---

## IPsec encryption

Legt den IPsec-Verschlüsselungsalgorithmus fest, den das Gerät verwendet.

Mögliche Werte:

[any](#)

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.

[des](#)

Das Gerät verwendet die Data-Encryption-Standard- (DES)-Blockchiffre für die Verschlüsselung von Nachrichtendaten mit einem 56-Bit-Schlüssel.

[des3](#)

Das Gerät verwendet die Triple-DES-Blockchiffre für die Verschlüsselung von Nachrichtendaten, die den 56-Bit-Schlüssel des DES 3 Mal pro Block anwendet.

[aes128](#) (Voreinstellung)

Das Gerät verwendet Advanced Encryption Standard (AES) mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 128 Key-Bits.

[aes192](#)

Das Gerät verwendet AES mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 192 Key-Bits.

[aes256](#)

Das Gerät verwendet AES mit einer Blockgröße von 128 Bits und einer Schlüssellänge von 256 Key-Bits.

[aes128ctr](#)

AES-CTR mit 128 Key-Bits.

[aes192ctr](#)

AES-CTR mit 192 Key-Bits.

[aes256ctr](#)

AES-CTR mit 256 Key-Bits.

[aes128gcm64](#)

AES-GCM mit einem 64-Bit-ICV und 128 Key-Bits.

[aes128gcm96](#)

AES-GCM mit einem 96-Bit-ICV und 128 Key-Bits.

[aes128gcm128](#)

AES-GCM mit einem 128-Bit-ICV und 128 Key-Bits.

[aes192gcm64](#)

AES-GCM mit einem 64-Bit-ICV und 192 Key-Bits.

[aes192gcm96](#)

AES-GCM mit einem 96-Bit-ICV und 192 Key-Bits.

[aes192gcm128](#)

AES-GCM mit einem 128-Bit-ICV und 192 Key-Bits.

[aes256gcm64](#)

AES-GCM mit einem 64-Bit-ICV und 256 Key-Bits.

[aes256gcm96](#)

AES-GCM mit einem 96-Bit-ICV und 256 Key-Bits.

[aes256gcm128](#)

AES-GCM mit einem 128-Bit-ICV und 256 Key-Bits.

---

**Anmerkung:**

Wir empfehlen, die Einstellung [aes128](#) 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:

[any](#)

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.

[modp1024](#) (Voreinstellung)

Der Wert stellt einen Rivest-Shamir-Adleman- (RSA)-Algorithmus mit 1024-Bit-Modulus dar. Dieser Wert gehört zur Diffie-Hellman- (DH)- Gruppe 2.

[modp1536](#)

Der Wert stellt einen RSA-Algorithmus mit 1536-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 5 gehört.

[modp2048](#)

Der Wert stellt einen RSA-Algorithmus mit 2048-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 14 gehört.

[modp3072](#)

Der Wert stellt einen RSA-Algorithmus mit 3072-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 15 gehört.

[modp4096](#)

Der Wert stellt einen RSA-Algorithmus mit 4096-Bit-Modulus dar, der zur DH-Gruppe DH-Gruppe 16 gehört.

[kein](#)

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 überflüssige 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:

10 . 500000 (Voreinstellung: 30)

Das Gerät überwacht das Alter der gelernten Unicast-MAC-Adressen. Adresseinträge, die ein bestimmtes Alter (Aging-Zeit) überschreiten, löscht das Gerät aus seiner MAC-Adresstabelle (Forwarding Database).

Die MAC-Adresstabelle (Forwarding Database) finden Sie im Dialog [Switching > Filter für MAC-Adressen](#).

Im Zusammenhang mit der Router-Redundanz wählen Sie eine Zeit 30 s.

#### Flusskontrolle

Aktiviert/deaktiviert die Flusskontrolle im Gerät.

Mögliche Werte:

**markiert**

Die Flusskontrolle ist im Gerät aktiviert.

Aktivieren Sie die Flusskontrolle zusätzlich auf den erforderlichen Ports. Siehe Dialog [Grundeinstellungen > Port](#), Registerkarte [Konfiguration](#), Kontrollkästchen in Spalte [Flusskontrolle](#).

**unmarkiert** (Voreinstellung)

Die Flusskontrolle ist im Gerät deaktiviert.

## 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 *Lastbegrenzer* 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:

[Prozent](#) (Voreinstellung)

Der Schwellenwert ist festgelegt in Prozent der Datenrate des Ports.

[pps](#)

Der Schwellenwert ist festgelegt in Datenpaketen pro Sekunde.

#### Broadcast Modus

Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene Broadcast-Datenpakete.

Mögliche Werte:

- `markiert`
- `unmarkiert` (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:

`0 . 14880000` (Voreinstellung: `0`)

Der Wert `0` deaktiviert die Lastbegrenzerfunktion auf diesem Port.

Wenn Sie in Spalte *Einheit* den Wert *Prozent* auswählen, dann geben Sie einen Prozentwert zwischen `1` und `100` ein.

Wenn Sie in Spalte *Einheit* den Wert *pps* auswählen, dann geben Sie einen Absolutwert für die Datenrate ein.

#### Multicast Modus

Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene Multicast-Datenpakete.

Mögliche Werte:

- `markiert`
- `unmarkiert` (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:

`0 . 14880000` (Voreinstellung: `0`)

Der Wert `0` deaktiviert die Lastbegrenzerfunktion auf diesem Port.

Wenn Sie in Spalte *Einheit* den Wert *Prozent* auswählen, dann geben Sie einen Prozentwert zwischen `0` und `100` ein.

Wenn Sie in Spalte *Einheit* den Wert *pps* 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:

`markiert`  
`unmarkiert` (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:

`0` . `14880000` (Voreinstellung: `0`)

Der Wert `0` deaktiviert die Lastbegrenzerfunktion auf diesem Port.

Wenn Sie in Spalte *Einheit* den Wert *Prozent* auswählen, dann geben Sie einen Prozentwert zwischen `0` und `100` ein.

Wenn Sie in Spalte *Einheit* den Wert *pps* 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 empfangenden Port an den in der Tabellenzeile festgelegten Port.
- Existiert keine Tabellenzeile für die Zieladresse, vermittelt das Gerät das Datenpaket vom empfangenden Port an jeden anderen Port.

### Tabelle

Um die gelernten MAC-Adressen aus der MAC-Adresstabelle (Forwarding Database) zu entfernen, klicken Sie im Dialog *Grundeinstellungen > Restart* die Schaltfläche *FDB leeren*.

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

#### Schaltflächen



Hinzufügen

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

- Im Feld *MAC-Adresse* legen Sie die Ziel-MAC-Adresse fest.
- Im Feld *VLAN-ID* 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

Löscht die MAC-Adressen, die in Spalte *Status* den Wert *Learned* haben, aus der Forwarding-Tabelle (FDB).

#### 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:

**Lear ned**

Adressfilter automatisch durch das Gerät eingerichtet anhand empfangener Datenpakete.

**Mgmt**

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

**Per manent**

Adressfilter manuell eingerichtet. Der Adressfilter bleibt dauerhaft eingerichtet.

## &lt;Port-Nummer&gt;

Zeigt, wie der betreffende Port Datenpakete vermittelt, die an nebenstehende Zieladresse adressiert sind.

Mögliche Werte:

-

Der Port vermittelt keine Datenpakete an die Zieladresse.

**Lear ned**

Der Port vermittelt Datenpakete an die Zieladresse. Das Gerät hat den Filter anhand empfangener Datenpakete automatisch eingerichtet.

**Uni cast stati c**

Der Port vermittelt Datenpakete an die Zieladresse. Ein Benutzer hat den Filter eingerichtet.

**Ml ti cast stati sch**

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 [Switching > Global](#), Rahmen [Konfiguration](#), das Kontrollkästchen [Flusskontrolle](#) unmarkiert ist.

---

Das Menü enthält die folgenden Dialoge:

- [QoS/Priority Global](#)
- [QoS/Priorität Port-Konfiguration](#)
- [802.1D/p Zuweisung](#)

## 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:

0 . 7 (Voreinstellung: 0)

Im Dialog *Switching > QoS/Priority > 802.1D/p Zuweisung* weisen Sie jeder VLAN-Priorität eine *Verkehrsklasse* zu.

#### IP-DSCP Wert für Management-Pakete

Legt den IP-DSCP-Wert für zu sendende Management-Datenpakete fest. Abhängig vom IP-DSCP-Wert weist das Gerät das Datenpaket einer bestimmten *Verkehrsklasse* zu und dementsprechend einer bestimmten Warteschlange des Ports.

Mögliche Werte:

0 (be/cs0) . . 63 (Voreinstellung: 0 (be/cs0))

Einige Werte in der Liste haben zusätzlich ein DSCP-Schlüsselwort, zum Beispiel 0 (be/cs0) , 10 (af 11) und 46 (ef) . 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 *Trust-Mode*.

Mögliche Werte:

0 . 7 (Voreinstellung: 0)

## 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:

0..7

0 ist der Warteschlange mit der niedrigsten Priorität zugewiesen.

7 ist der Warteschlange mit der höchsten Priorität zugewiesen.

### Anmerkung:

Unter anderem Redundanzmechanismen nutzen die höchste *Verkehrsklasse*. Wählen Sie deshalb für Anwendungsdaten eine andere *Verkehrsklasse*.

### Werkseitige Zuweisung der VLAN-Priorität zu Verkehrsklassen

VLAN-Priorität	Verkehrsklasse	Inhaltskennzeichnung gemäß IEEE 802.1D
0	2	Best Effort Normale Daten ohne Priorisierung
1	0	Background Zeitunkritische Daten und Hintergrunddienste
2	1	Standard Normale Daten
3	3	Excellent Effort Wichtige Daten
4	4	Controlled Load Zeitkritische Daten mit hoher Priorität

VLAN-Priorität	Verkehrsklasse	Inhaltskennzeichnung gemäß IEEE 802.1D
5	5	<b>Vi deo</b> Bildübertragung mit Verzögerungen und Jitter <100 ms
6	6	<b>Voi ce</b> Sprachübertragung mit Verzögerungen und Jitter <10 ms
7	7	<b>Netw ork Contr ol</b> 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.
- Verbesserter Durchsatz
  - Datenpakete lassen sich in VLANs priorisiert übertragen. Bei höherer Priorisierung überträgt das Gerät die Daten eines VLANs bevorzugt, zum Beispiel mit zeitkritischen Anwendungen wie VoIP-Telefonaten.
  - Die Netzlast reduziert sich erheblich, wenn sich Datenpakete und Broadcasts in kleinen Netzsegmenten anstatt im gesamten Netz ausbreiten.
- Höhere Sicherheit
  - Das Verteilen der Datenpakete auf einzelne logische Netze erschwert ungewolltes Abhören und härtet das System gegen Angriffe, wie MAC-Flooding oder MAC-Spoofing.

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

Das Gerät vermittelt die markierten Datenpakete eines VLANs ausschließlich an Ports, die demselben VLAN zugewiesen sind. Dies reduziert die Netzlast.

Das Gerät lernt die MAC-Adressen für jedes VLAN separat (Independent VLAN Learning).

Das 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 [Grundeinstellungen > Netzwerk > Global](#) das VLAN für das Management des Geräts geändert haben.

Größte VLAN-ID

Größtmögliche ID, die Sie einem VLAN zuweisen können.

Siehe Dialog [Switching > VLAN > Konfiguration](#).

VLANs (max.)

Zeigt die maximale Anzahl der im Gerät einrichtbaren VLANs.

Siehe Dialog [Switching > VLAN > Konfiguration](#).

VLANs

Anzahl der VLANs, die im Gerät gegenwärtig eingerichtet sind.

Siehe Dialog [Switching > VLAN > Konfiguration](#).

Das VLAN 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:

- *Routing*: 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 *Erstellen*, um eine Tabellenzeile hinzuzufügen.

Im Feld *VLAN-ID* 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:

1 . . 4042

#### Status

Zeigt, auf welche Weise das VLAN eingerichtet ist.

Mögliche Werte:

*other*

VLAN 1

*permanent*

VLAN eingerichtet durch den Benutzer.

Wenn Sie die Einstellungen im nichtflüchtigen 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 0..32 Zeichen

<Port-Nummer>

Legt fest, ob der betreffende Port Datenpakete des VLANs vermittelt und ob die Datenpakete ein VLAN-Tag enthalten.

Mögliche Werte:

- (Voreinstellung)

Der Port ist kein Mitglied des VLANs und vermittelt keine Datenpakete des VLANs.

**T** = Tagged

Der Port ist Mitglied des VLANs und vermittelt die Datenpakete mit VLAN-Tag. Verwenden Sie diese Einstellung zum Beispiel auf Uplink-Ports.

**LT** = Tagged Learned

Der Port ist Mitglied des VLANs und vermittelt die Datenpakete mit VLAN-Tag.

Das Gerät hat den Eintrag mit der Funktion *GVRP* oder *MVRP* automatisch eingerichtet.

**F** = Forbidden

Der Port ist kein Mitglied des VLANs und vermittelt keine Datenpakete dieses VLANs.

**U** = Untagged (Voreinstellung für VLAN 1)

Der Port ist Mitglied des VLANs und vermittelt die Datenpakete ohne VLAN-Tag. Verwenden Sie diese Einstellung, wenn das angeschlossene Gerät kein VLAN-Tag auswertet, zum Beispiel auf EndPorts.

**LU** = Untagged Learned

Der Port ist Mitglied des VLANs und vermittelt die Datenpakete ohne VLAN-Tag.

Das Gerät hat den Eintrag mit der Funktion *GVRP* oder *MVRP* automatisch eingerichtet.

---

**Anmerkung:**

Vergewissern Sie sich, dass der Port, an dem die Netzmanagement-Station angeschlossen ist, Mitglied des VLANs ist, in welchem das Gerät die Management-Daten vermittelt. In der Voreinstellung vermittelt das Gerät die Management-Daten im VLAN 1. Andernfalls brechen die Verbindungen zum Management des Geräts ab, sobald Sie die Änderungen anwenden. Der Zugriff auf das Management des Geräts ist dann ausschließlich mittels Command Line Interface über die serielle Verbindung 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 0, 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 *Akzeptierte Datenpakete* ist der Wert `admi tAl l` festgelegt.

Mögliche Werte:

- `1..4042` (Voreinstellung: 1)
- Ein bereits eingerichtetes VLAN

Akzeptierte Datenpakete

Legt fest, ob der Port empfangene Datenpakete ohne VLAN-Tag überträgt oder verwirft.

Mögliche Werte:

- `admi tAl l` (Voreinstellung)  
Der Port akzeptiert Datenpakete sowohl mit als auch ohne VLAN-Tag.
- `admi tOnl yVl anTagged`  
Der Port akzeptiert ausschließlich Datenpakete, die mit einer VLANID `1` markiert sind.

## Ingress-Filtering

Aktiviert/deaktiviert die Eingangsfilerung.

Mögliche Werte:

**markiert** (Voreinstellung)

Die Eingangsfilerung ist aktiv.

Das Gerät vergleicht die im Datenpaket enthaltene VLAN-ID mit den VLANs, in denen der Port Mitglied ist. Siehe Dialog [Switching > VLAN > Konfiguration](#). Stimmt die VLAN-ID im Datenpaket mit einem dieser VLANs überein, vermittelt das Gerät das Datenpaket. Andernfalls verwirft das Gerät das Datenpaket.

**unmarkiert**

Die Eingangsfilerung ist inaktiv.

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



## 7 Routing

Das Menü enthält die folgenden Dialoge:

- [Routing Global](#)
- [Routing-Interfaces](#)
- [ARP](#)
- [Open Shortest Path First](#)
- [Routing-Tabelle](#)
- [L3-Relay](#)
- [Loopback-Interface](#)
- [L3-Redundanz](#)
- [NAT](#)

### 7.1 Routing Global

[Routing > Global]

Das Menü [Routing](#) 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:

- [Source Routing](#)  
Beim Source Routing enthält das Datenpaket die Routing-Information und überschreibt damit die Einstellungen im Router.
- [ICMP-Redirects](#)  
ICMP-Redirect-Datenpakete sind imstande, die Routing-Tabelle zu verändern. Das Gerät ignoriert generell empfangene ICMP-Redirect-Datenpakete. Die Einstellung im Dialog [Routing > Interfaces > Konfiguration](#), Spalte [ICMP redirects](#) 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:

[An](#)

Die Funktion [Routing](#) ist eingeschaltet.

Aktivieren Sie die Routing-Funktion zusätzlich auf den Router-Interfaces. Siehe Dialog [Routing > Interfaces > Konfiguration](#).

[Aus](#) (Voreinstellung)

Die Funktion [Routing](#) ist ausgeschaltet.

## ICMP-Filter

Im Rahmen *ICMP-Filter* 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:

`markiert` (Voreinstellung)

Das Antworten auf Pings ist aktiv.

Das Gerät antwortet auf ein empfangenes *>ICMP Echo Request*-Paket mit einem *ICMP Echo Reply*-Paket.

`unmarkiert`

Das Antworten auf Pings ist inaktiv.

### Redirects senden

Aktiviert/deaktiviert auf den Router-Interfaces das Senden von *ICMP Redirect*-Nachrichten.

Mögliche Werte:

`markiert` (Voreinstellung)

Das Senden von *ICMP Redirect*-Nachrichten ist aktiv.

Im Dialog *Routing > Interfaces > Konfiguration* haben Sie die Möglichkeit, das Senden auf jedem Router-Interface einzeln zu aktivieren. Siehe Funktion *ICMP redirects*.

`unmarkiert`

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:

`0` . `2147483647` ( $2^{31} - 1$ ) (Voreinstellung: `1000`)

*Rate limit* ist ausgeschaltet.

`10` . `2147483647` ( $2^{31} - 1$ ) (Voreinstellung: `1000`)

– 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:

6

#### Information

#### Default-TTL

Zeigt den fest eingestellten TTL-Wert [64](#), 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 1. Empfängt ein Router ein IP-Paket mit dem TTL-Wert [1](#), 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 [Wizard](#).

### Anmerkung:

Um den Verlust von Datenpaketen zu vermeiden, empfehlen wir, das Gerät über einen einzigen Port mit einem Gerät zu verbinden, das Shared VLAN Learning (SVL) unterstützt, anstatt über jeweils einen Port für jedes VLAN-Interface.

### Tabelle

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

Schaltflächen



Hinzufügen

Öffnet das Fenster [Erstellen](#), um eine Tabellenzeile hinzuzufügen. Im Feld [VLAN-ID](#) legen Sie die VLAN-ID 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 „[\[Wizard: VLAN-Router-Interface einrichten\]](#)“ auf [Seite 319](#).

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:

- [<space>](#)
- [0 . 9](#)
- [a . z](#)

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

#### Port an

Aktiviert/deaktiviert den Port.

Mögliche Werte:

`markiert` (Voreinstellung)

Der Port ist aktiv.

`unmarkiert`

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

#### Status Port

Zeigt den Betriebszustand des Ports.

Mögliche Werte:

`up`

Der Port ist eingeschaltet.

`down`

Der Port ist ausgeschaltet.

#### IP-Adresse

Legt die IP-Adresse für das Router-Interface fest.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung: `0.0.0.0`)

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: `0.0.0.0`)

#### Routing

Aktiviert/deaktiviert die Funktion *Routing* 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:

`markiert`

Die Funktion *Routing* ist aktiv.

- Beim Port-basierten Routing wandelt das Gerät den Port in ein Router-Interface um. Das Aktivieren der Funktion *Routing* entfernt den Port aus den VLANs, in denen er bisher Mitglied war. Das Deaktivieren der Funktion *Routing* 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.

`unmarkiert` (Voreinstellung)

Die Funktion *Routing* 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 *Proxy-ARP* auf dem Router-Interface. Diese Funktion ermöglicht Ihnen, Endgeräte aus anderen Netzen anzubinden, als wären diese Endgeräte im selben Netz erreichbar.

Mögliche Werte:

`markiert`

Die Funktion *Proxy-ARP* ist aktiv.

Das Gerät antwortet auf ARP-Anfragen von Endgeräten, die sich in anderen Netzen befinden.

`unmarkiert` (Voreinstellung)

Die Funktion *Proxy-ARP* ist inaktiv.

#### MTU-Wert

Legt die maximal zulässige Größe der IP-Pakete auf dem Router-Interface in Byte fest.

Mögliche Werte:

`0`

Stellt den voreingestellten Wert (1500) wieder her.

`68 . 1500` (Voreinstellung: 1500)

#### Track-Name

Legt den Namen des Tracking-Objekts fest, mit dem das Gerät das Routing-Interface verknüpft.

Voraussetzung ist, dass im Dialog *Erweitert > Tracking > Konfiguration* das Feld *Track-Name* bereits eingerichtet ist.

Mögliche Werte:

`<Track name>` (Voreinstellung: -)

Das Gerät aktiviert oder deaktiviert automatisch den Verbindungs-Status eines Routing-Interfaces, je nachdem, welches Tracking-Objekt aus der Dropdown-Liste gewählt ist.

#### ICMP unreachable

Zeigt, ob auf dem Router-Interface das Senden von *ICMP Destination Unreachable*-Nachrichten aktiv ist.

Mögliche Werte:

`markiert`

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:

[markiert](#)

Das Router-Interface sendet *ICMP Redirect*-Nachrichten.

[unmarkiert](#) (Voreinstellung)

Das Router-Interface sendet keine *ICMP Redirect*-Nachrichten.

## [Wizard: VLAN-Router-Interface einrichten]

Das Fenster *Wizard* ermöglicht Ihnen, VLAN-basierte Router-Interfaces einzurichten.

Das Fenster *Wizard* 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 *VLAN-ID* unten einen Wert fest.

#### VLAN-ID

Legt die ID eines VLANs fest. Alternativ wählen Sie einen Eintrag in der *VLAN-ID*-Übersicht oben. Sie können ein VLAN auch im Dialog *Switching > VLAN > Konfiguration* einrichten.

Mögliche Werte:

[1..4042](#)

### VLAN einrichten

#### VLAN-ID

Zeigt die ID des VLANs, das Sie im vorhergehenden *Wizard*-Schritt festgelegt haben.

#### Name

Legt die Bezeichnung des VLANs fest. Diese Einstellung überschreibt die für den Port im Dialog *Switching > VLAN > Konfiguration* festgelegte Einstellung.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen  
(hexadezimaler ASCII-Code [0x20](#)..[0x7E](#)) 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 [Switching > VLAN > Konfiguration](#) für den Port festgelegte Einstellung.

Mögliche Werte:

**markiert**

Der Port ist Mitglied des VLANs.

**unmarkiert**

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 [Switching > VLAN > Konfiguration](#) für den Port festgelegte Einstellung.

#### Mögliche Werte:

##### [markiert](#)

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.

##### [unmarkiert](#)

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 [Switching > VLAN > Port](#), Spalte [Port VLAN-ID](#) festgelegte Einstellung.

#### Mögliche Werte:

Ein bereits eingerichtetes VLAN (Voreinstellung: 1)

## Virtuellen Router-Port einrichten

Das Gerät ermöglicht Ihnen, für ein Router-Interface bis zu 32 IP-Adressen (1 primäre, 31 sekundäre) und insgesamt bis zu 1024 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 [Wizard](#) eine Meldung:

- Wenn Sie die Schaltfläche [Ja](#) klicken, senden die betreffenden Ports die Datenpakete künftig ausschließlich im Router-VLAN.  
Im Dialog [Switching > VLAN > Konfiguration](#) haben die betreffenden Ports in der Tabellenzeile des Router-VLANs den Wert **U** oder **T**, in den Zeilen anderer VLANs den Wert **-**.
- Wenn Sie die Schaltfläche [Nein](#) klicken, senden die betreffenden Ports die Datenpakete im Router-VLAN und in anderen VLANs. Diese Einstellung kann zu unerwünschtem Verhalten führen und kann auch ein Sicherheitsrisiko darstellen.  
Verwenden Sie diese Einstellung nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.

### Primäre Adresse

#### Adresse

Legt die primäre IP-Adresse für das Router-Interface fest.

Mögliche Werte:

Gültige IPv4-Adresse

#### Netzmaske

Legt die primäre Netzmaske für das Router-Interface fest.

Mögliche Werte:

Gültige IPv4-Netzmaske

### Sekundäre Adressen

#### Adresse

Legt eine weitere IP-Adresse für das Router-Interface fest (Multinetting).

Mögliche Werte:

Gültige IPv4-Adresse

---

#### **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

#### 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 32 IP-Adressen (1 primäre, 31 sekundäre) und insgesamt bis zu 1024 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 *Erstellen*, um dem in der Tabelle ausgewählten Router-Interface eine weitere IP-Adresse hinzuzufügen.

- In der Dropdown-Liste *Port* wählen Sie den Port oder das VLAN, der/das dem Router-Interface zugewiesen wird.
- Im Feld *Weitere IP-Adresse* legen Sie die IP-Adresse fest.  
Mögliche Werte:  
Gültige IPv4-Adresse
- Im Feld *Weitere Netzmaske* 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 *Routing > Interfaces > Konfiguration*.

#### Netzmaske

Zeigt die primäre Netzmaske des Router-Interfaces. Siehe Dialog [Routing > Interfaces > Konfiguration](#).

#### 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:

15 . 21600 (Voreinstellung: 1200)

#### 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:

1 . 10 (Voreinstellung: 1)

#### Wiederholungen

Legt fest, wie viele Male das Gerät eine gescheiterte Anfrage wiederholt, bevor es die Anfrage an diese Adresse verwirft.

Mögliche Werte:

0 . 10 (Voreinstellung: 4)

### 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 [Routing > ARP > Aktuell](#).
- Adressen der Geräte, die an das Management des Geräts angeschlossen sind. Siehe Dialog [Diagnose > System > ARP](#).

### 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 0 zurückzusetzen, klicken Sie im Dialog [Routing > ARP > Aktuell](#) die Schaltfläche  .

### Aktuelle statische Einträge

Zeigt, wie viele statisch eingerichtete Einträge die ARP-Tabelle gegenwärtig enthält. Siehe Dialog [Routing > ARP > Statisch](#).

### 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

Löscht die dynamisch eingerichteten Adressen aus der ARP-Tabelle.

#### 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**


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 [Routing > ARP > Global](#), Feld [Aging-Time \[s\]](#).

statisch

Statisch eingerichteter Eintrag.

Der Eintrag bleibt erhalten, wenn Sie mit der Schaltfläche  die dynamisch eingerichteten Adressen aus der ARP-Tabelle entfernen.

lokal

Kennzeichnet die IP/MAC-Adresszuweisung des Router-Interfaces.

invalid

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 *Wizard*, das Sie dabei unterstützt, die Ports mit der Adresse eines oder mehrerer erwünschter Absender zu verknüpfen. Siehe „[\[Wizard: ARP\]](#)“ auf Seite 330.

#### 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:

[<Router - I nterface>](#)

Das Gerät wendet die IP/MAC-Adresszuweisung auf diesem Router-Interface an.

[no port](#)

Die IP/MAC-Adresszuweisung ist gegenwärtig keinem Router-Interface zugewiesen.

#### Aktiv

Zeigt, ob die IP/MAC-Adresszuweisung aktiv oder inaktiv ist.

Mögliche Werte:

[marki ert](#)

Die IP/MAC-Adresszuweisung ist aktiv. Die ARP-Tabelle des Geräts enthält die IP/MAC-Adresszuweisung als statischen Eintrag.

[unmarki ert](#) (Voreinstellung)

Die IP/MAC-Adresszuweisung ist inaktiv.

## [Wizard: ARP]

Das Fenster *Wizard* 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 *Statische Einträge* ein. Klicken Sie dazu die Schaltfläche *Hinzufügen*.

Schließen Sie das Fenster *Wizard*. Klicken Sie dazu die Schaltfläche *Fertig*.

Legen Sie das Router-Interface in Spalte *Port* fest.

Aktivieren Sie die IP/MAC-Adresszuweisung. Markieren Sie dazu das Kontrollkästchen in Spalte *Aktiv*.

### 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*-Paketten 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:

**An**

Die Funktion *OSPF* ist eingeschaltet.

**Aus** (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:

<IP-Adresse eines Interfaces> (Voreinstellung: 0.0.0.0)

### 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:

-1 (Voreinstellung)

Der Router speichert weitere Einträge, bis der Speicher voll ist.

0..2147483647 ( $2^{31} - 1$ )

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:

1..4294967 (Voreinstellung: 100)

### Pfade (max.)

Legt die maximale Anzahl von ECMP-Routen fest, die *OSPF* der Routing-Tabelle hinzufügt, wenn in einem Subnetz mehrere Pfade mit denselben Pfadkosten und unterschiedlichen Next-Hops existieren.

Mögliche Werte:

1..4 (Voreinstellung: 4)

5..16

Verfügbar, wenn gegenwärtig das Routing-Profil *pv4DataCenter* verwendet wird. Siehe Rahmen *Routing-Profil* im Dialog *Routing > Global*.

#### Standard-Metrik

Legt den voreingestellten Metrik-Wert für die Funktion *OSPF* fest.

Mögliche Werte:

0 (Voreinstellung)

Die Funktion *OSPF* weist aus externen Routen gelernten Quellen (statisch oder direkt verbunden) automatisch Kosten von 20 zu.

1.. 16777214 ( $2^2 - 2$ )

#### Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung an einem OSPF-Parameter erkennt.

Mögliche Werte:

markiert

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

Das Gerät sendet einen SNMP-Trap, wenn es Änderungen an den OSPF-Parametern erkennt.

unmarkiert (Voreinstellung)

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:

0

Der Router beginnt unmittelbar nach dem Empfang des *Topology Change*-Pakets mit der SPF-Berechnung.

1.. 65535 ( $2^1 - 1$ ) (Voreinstellung: 5)

#### Hold-Time [s]

Legt die Mindestzeit in Sekunden zwischen aufeinander folgenden SPF-Berechnungen fest.

Mögliche Werte:

0.. 65535 ( $2^1 - 1$ ) (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:

0..2147483647 ( $2^{31} - 1$ ) (Voreinstellung: 0)

Der Wert 0 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:

markiert

Der Router ist ein ASBR.

unmarkiert

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:

markiert

Der Router ist ein ABR.

unmarkiert

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 *OSPF* die *Standard-Routen* leitet
- den Routen-Typ, den die Funktion *OSPF* für die Pfad-Kostenberechnung verwendet

### RFC 1583 Kompatibilität

Die Network Working Group entwickelt und verbessert die Funktion *OSPF* 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:

*An* (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.

*Aus*

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 *OSPF* 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:

1.. 255 (Voreinstellung: 110)

## Präferenz (inter)

Legt die „Administrative Distanz“ zwischen Routern in unterschiedlichen Areas (Inter-Area-OSPF-Routen) fest.

Mögliche Werte:

1.. 255 (Voreinstellung: 110)

## Präferenz (extern)

Legt die „Administrative Distanz“ zwischen Routern außerhalb der Areas (externe OSPF-Routen) fest.

Mögliche Werte:

1.. 255 (Voreinstellung: 110)

**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:

**markiert**

Der Router meldet *Standard-Routen*.

**unmarkiert** (Voreinstellung)

Der Router unterdrückt Meldungen über *Standard-Routen*.

## Advertise always

Zeigt, ob der Router stets 0.0.0.0/0 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 0.0.0.0 und der Maske 0.0.0.0 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:

`markiert`

Der Router meldet stets `0.0.0.0/0` als *Standard-Route*.

`unmarkiert` (Voreinstellung)

Das Gerät verwendet die im Parameter *Advertise* festgelegten Einstellungen.

#### Metrik

Legt die Metrik der *Standard-Route* fest, welche die Funktion *OSPF* meldet, wenn diese von anderen Protokollen gelernt wurde.

Mögliche Werte:

`0`

Das Gerät verwendet den im Feld *Standard-Metrik* festgelegten Wert.

`1..16777214 (224 - 2)`

#### Metrik Typ

Zeigt den Metrik-Typ der *Standard-Route*, die Funktion *OSPF* meldet, wenn sie von einem anderen Protokoll gelernt wurde.

Mögliche Werte:

`external Type1`

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.

`external Type2` (Voreinstellung)

Umfasst ausschließlich die externen Pfadkosten.

### [Redistribution]

Ein Router, bei dem auf einem gerouteten Interface die Funktion *OSPF* ausgeschaltet ist, propagiert nicht das Netz dieses Interfaces auf seinen anderen Interfaces. Das Netz ist somit unerreichbar. Um solche Netze zu propagieren, schalten Sie *Redistribution* 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 *OSPF* umzuwandeln, zum Beispiel Kosten und Entfernung.

Die Anzahl der Routen, die das Gerät über die Funktion *OSPF* 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 *OSPF* 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:

*connected*

Der Router ist direkt mit der Route verbunden.

*statisch*

Ein Netzadministrator hat die Route im Router festgelegt.

### Aktiv

Aktiviert/deaktiviert die Routen-Neuverteilung vom Quellprotokoll in OSPF.

Mögliche Werte:

*markiert*

Die Neuverteilung von Routen, die vom Quellprotokoll gelernt wurden, ist aktiv.

*unmarkiert* (Voreinstellung)

Die OSPF-Routen-Neuverteilung ist inaktiv.

### Metrik

Legt den Metrikwert fest für Routen, die durch dieses Protokoll neu verteilt werden.

Mögliche Werte:

0 (Voreinstellung)

Das Gerät verwendet den im Feld *Standard-Metrik* festgelegten Wert.

1..16777214 ( $2^28 - 2$ )

### Metrik Typ

Legt den Routen-Metriktyp fest, den die Funktion *OSPF* von anderen Quellprotokollen neu verteilt.

Mögliche Werte:

*external Type1*

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.

*external Type2* (Voreinstellung)

Dieser Metriktyp gilt ausschließlich für die externen Pfadkosten.

## Tag

Legt einen Tag für Routen fest, die in die Funktion *OSPF* neu verteilt werden.

Wenn Sie einen Routen-Tag setzen, weist die Funktion *OSPF* 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:

0.. 4294967295 ( $2^{32} - 1$ ) (Voreinstellung: 0)

## Subnetze

Aktiviert/deaktiviert die Routen-Neuverteilung für Subnetze in die Funktion *OSPF*.

Die Funktion *OSPF* verteilt ausschließlich Netzklassen in die OSPF-Domäne um. Um die Subnetz-Routen in OSPF neu zu verteilen, aktivieren Sie den Subnetz-Parameter.

Mögliche Werte:

*markiert* (Voreinstellung)

Der Router verteilt Netzklassen und Subnetz-Routen in OSPF um.

*unmarkiert*

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 [Erstellen](#), um eine Tabellenzeile hinzuzufügen.

- Im Feld [Area-ID](#) 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:

[area](#) (Voreinstellung)

Der Router importiert *Type 5 AS external*-LSAs in die Area.

[stub area](#)

Der Router ignoriert *Type 5 AS external*-LSAs.

[nssa](#)

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 *OSPF* 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 *OSPF* 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 [Routing > OSPF > Areas](#) den Wert in Spalte *Area Typ* auf *stub area*.
- Erstellen Sie eine Stub-Area. Führen Sie dazu die folgenden Schritte aus:  
Fügen Sie im Dialog [Routing > OSPF > Areas](#) eine Tabellenzeile hinzu.  
Ändern Sie den Wert in Spalte *Area Typ* auf *stub area*.

### 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:

0 . 16777215 ( $2^24 - 1$ ) (Voreinstellung: 1)

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:

OSPF *metric* (Voreinstellung)

Der ABR meldet die Metrik als OSPF-intern, das den Kosten einer Intra-Area-Route zum ABR entspricht.

#### External type 1

Der ABR meldet die Metrik als **External type 1**, der den Kosten der internen OSPF-Metrik plus der externen Metrik des ASBR entspricht.

#### External type 2

Der ABR meldet die Metrik als **External type 2**, 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:

#### markiert

Der Router importiert keine Area-Summaries. Die Stub-Area basiert vollständig auf der *Standard-Route*. Dadurch wird die *Standard-Route* zu einer Totally-Stubby-Area.

#### unmarkiert (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 [Routing > OSPF > Areas](#) den Wert in Spalte [Area Typ](#) auf [nssa](#).
- Erstellen Sie eine NSSA. Führen Sie dazu die folgenden Schritte aus:  
Fügen Sie im Dialog [Routing > OSPF > Areas](#) eine Tabellenzeile hinzu.  
Ändern Sie den Wert in Spalte [Area Typ](#) auf [nssa](#).

### 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:

[markiert](#) (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.

[unmarkiert](#)

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:

[markiert](#)

Der Router generiert *Type 7 default*-LSAs und sendet sie in die NSSA.

[unmarkiert](#) (Voreinstellung)

Der Router unterdrückt *Type 7 default*-LSAs.

### Standard-Metrik

Legt die im *Type 7 default*-LSA gemeldete Metrik fest.

Mögliche Werte:

1.. 16777214 ( $2^24 - 2$ ) (Voreinstellung: 10)

### Standard-Metrik Typ

Legt den im *Type 7 default*-LSA gemeldeten Metrik-Typ fest.

Mögliche Werte:

`ospfMetric`

Der Router meldet die Metrik als OSPF-intern, das den Kosten einer Intra-Area-Route zum ABR entspricht.

`comparable`

Der Router meldet die Metrik als *external Type 1*, der den Kosten der internen OSPF-Metrik plus der externen Metrik des ASBR entspricht.

`noncomparable`

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:

`always`

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.

`candidate` (Voreinstellung)

Der Router übersetzt *Type 7*-LSAs in *Type 5*-LSAs.

Um Routing-Loops zu vermeiden, nimmt die Funktion *OSPF* eine Übersetzerauswahl vor. Sind mehrere Kandidaten vorhanden, wählt die Funktion *OSPF* 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:

`enabled`

Die *Translator role* des Routers ist auf `always` gesetzt.

`selected`

Als Kandidat übersetzt der NSSA Border Router *Type 7*-LSAs in *Type 5*-LSAs.

`disabled`

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:

0..65535 (2<sup>16</sup> - 1) (Voreinstellung: 40)

## 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 *OSPF* 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:

`markiert`

Der Router unterdrückt den Import von Summary-Routen, wodurch die Area zu einer Totally-NSSA wird.

`unmarkiert` (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* unterstützt mehrere Authentifizierungstypen. Richten Sie die Authentifizierungstypen für jedes Interface ein. Die Option *md5* 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:

*markiert*

Der Router meldet die auf dem Interface auf dem Interface festgelegten Werte und das Interface als interne OSPF-Route.

*unmarkiert* (Voreinstellung)

Das Interface ist in Bezug auf die Funktion *OSPF* extern.

Area-ID

Legt die Area-ID der Domäne fest, zu der das Interface eine Verbindung herstellt.

Mögliche Werte:

<Area-ID>

Die Area-IDs legen Sie im Dialog *Routing > OSPF > Areas* 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:

0

Der Router ist außerstande, der *Designated Router (DR)* in diesem Netz zu werden.

1.. 255 (Voreinstellung: 1)

## 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:

0.. 3600 (Voreinstellung: 1)

## 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:

0.. 3600 (Voreinstellung: 5)

## 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:

1.. 65535 ( $2^16 - 1$ ) (Voreinstellung: 10)

## 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 *Hello-Intervall [s]* fest. Legen Sie den gleichen Wert für die Router-Interfaces innerhalb desselben Bereiches fest.

Mögliche Werte:

1.. 65535 (2<sup>16</sup> - 1) (Voreinstellung: 40)

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:

**down** (Voreinstellung)

Das Interface ist im initialen Zustand und blockiert die Datenpakete.

**loopback**

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.

**waiting**

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 **waiting**-Zustand verlässt und einen DR wählt. Die Dauer dieses Timers entspricht dem Wert im Feld *Dead-Intervall [s]*.

**pointToPoint**

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 *Hello-Intervall [s]* Sekunden ein *Hello*-Paket, um eine Adjacency mit dem Nachbarn herzustellen.

**designatedRouter**

Der Router ist der DR für das Multi-Access-Netz und stellt Adjacencies mit anderen Routern her.

**backupDesignatedRouter**

Der Router ist der BDR für das Multi-Access-Netz und stellt Adjacencies mit anderen Routern her.

**otherDesignatedRouter**

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: 0.0.0.0)

## Backup designated router

Zeigt die IP-Adresse des Backup Designated Routers.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung: 0.0.0.0)

## 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:

[broadcast](#)

Verwenden Sie diesen Wert für Broadcast-Netze wie Ethernet und IEEE 802.5. Die Funktion *OSPF* führt eine Auswahl von DR und BDR durch, mit denen die nicht-designierten Router eine Adjacency herstellen.

[nbnr](#)

Verwenden Sie diesen Wert für Non-Broadcast-Multi-Access-Netze, zum Beispiel X.25 und ähnliche Technologien. Die Funktion *OSPF* führt eine DR- und BDR-Auswahl durch, um die Anzahl der hergestellten Adjacencies einzuschränken.

[point-to-point](#)

Verwenden Sie diesen Wert für Netze, die lediglich 2 Interfaces verbinden.

[point-to-multipoint](#)

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 [simple](#) 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:

[kein](#) (Voreinstellung)

Die Netz-Authentifizierung ist deaktiviert.

### simple

Der Router verwendet Klartext-Authentifizierung. In diesem Fall sendet der Router die Passwörter als Klartext.

### MD5

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 *Auth Typ* der Eintrag *simple* ausgewählt ist
- mit 16 Zeichen, wenn in der Dropdown-Liste *Auth Typ* 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 *MD5* fest.

Die Option *MD5* 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 Typ* der Wert *MD5* festgelegt ist.

Mögliche Werte:

0..255 (Voreinstellung: 0)

## Kosten

Legt die interne Metrik fest.

Die Funktion *OSPF* verwendet als Metrik die Kosten der Datenverbindung. Die Funktion *OSPF* verwendet diesen Wert auch zur Berechnung der SPF-Routen. Die Funktion *OSPF* 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 *Autocost reference bandwidth* festgelegt und beträgt in der Voreinstellung 100 Mbit/s. Siehe Dialog *Routing > OSPF > Global*, Registerkarte *Allgemein*.

Beispiel:

Die Bandbreite auf dem Interface beträgt 10 Mbit/s.

Die Metrik ist 100 Mbit/s geteilt durch 10 Mbit/s gleich 10.

Mögliche Werte:

*auto* (Voreinstellung)

Das Gerät berechnet die Metrik und passt den Wert bei einer Änderung der Bandbreite auf dem Interface automatisch an.

1..65535 (2<sup>16</sup> - 1)

Die Funktion *OSPF* verwendet als Metrik den hier festgelegten Wert.

### Calculated cost

Zeigt den Metrik-Wert, den die Funktion *OSPF* gegenwärtig für dieses Interface verwendet.

### MTU ignorieren

Aktiviert/deaktiviert die IP-MTU-Mismatch-Erkennung (*MTU: Maximum Transmission Unit*) an diesem OSPF-Interface.

#### Mögliche Werte:

**markiert**

Deaktiviert die IP-MTU-Prüfung und ermöglicht Adjacencys, wenn der MTU-Wert auf den Interfaces unterschiedlich ist.

**unmarkiert** (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 *OSPF* 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 *Erstellen*, um eine Tabellenzeile hinzuzufügen.

- In der Dropdown-Liste *Area-ID* wählen Sie die Area-ID für die neue Tabellenzeile.
- Im Feld *Nachbar-ID* 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:

0 . 3600 (Voreinstellung: 1)

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:

0 . 3600 (Voreinstellung: 5)

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 *Hello-Intervall [s]* fest. Legen Sie den gleichen Wert für die Router-Interfaces innerhalb desselben Bereiches fest.

Mögliche Werte:

1 . 65535 ( $2^1 - 1$ ) (Voreinstellung: 40)

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:

1 . 65535 ( $2^1 - 1$ ) (Voreinstellung: 10)

Status

Zeigt den Zustand des virtuellen OSPF-Interfaces.

Mögliche Werte:

**down** (Voreinstellung)

Das Interface ist im initialen Zustand und blockiert die Datenpakete.

**pointToPoint**

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 *Hello-Intervall [s]* 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 `simple` 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:

`kein` (Voreinstellung)

Die Netz-Authentifizierung ist deaktiviert.

`simple`

Der Router verwendet Klartext-Authentifizierung. In diesem Fall sendet der Router die Passwörter als Klartext.

`MD5`

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 `Auth Typ` der Eintrag `simple` ausgewählt ist

– mit 16 Zeichen, wenn in der Dropdown-Liste `Auth Typ` 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 `MD5` fest.

Die Option `md5` 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 `Auth Typ` der Wert `MD5` festgelegt ist.

Mögliche Werte:

`0..255` (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 [OSPF](#), 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 [Erstellen](#), um eine Tabellenzeile hinzuzufügen.

- In der Dropdown-Liste [Area-ID](#) wählen Sie die Area-ID des Adressbereichs aus.
- In der Dropdown-Liste [LSDB Typ](#) wählen Sie die Route-Informationen, die durch den Adressbereich zusammengefasst sind.

Mögliche Werte:

[summaryLink](#)

Der Area-Bereich fasst *Type 5*-Routen-Informationen zusammen.

[nssaExternalLink](#)

Der Area-Bereich fasst *Type 7*-Routen-Informationen zusammen.

- Im Feld [Netzwerk](#) 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:

[summaryLink](#)

Der Area-Bereich fasst *Type 5*-Routen-Informationen zusammen.

[nssaExternalLink](#)

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:

[advertiseMatching](#) (Voreinstellung)

Der Router meldet den Bereich in anderen Areas.

[doNotAdvertiseMatching](#)

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 *OSPF* 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.
- *Type 1*-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.

- *Type 2-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.
- *Type 3-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* generiert hat.
- *Type 4-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* generiert hat.
- *Type 5-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 *OSPF* 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 5 s 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 5 s 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:

#### [routerLi nk](#)

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.

#### [networ kLi nk](#)

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.

#### summaryLink

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.

#### asSummaryLink

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.

#### asExternalLink

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.

#### nssaExternalLink

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:

<Router ID>

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 *Sende-Verzögerung [s]* 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 Erfassung 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:

**down** (Voreinstellung)

Initialer Zustand einer Nachbarkonversation oder eines Routers, der die Konversation aufgrund des Ablaufs des *Dead-Intervall [s]* Timers beendet hat.

**attempt**

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 *Hello-Intervall [s]* festgelegt ist, *Hello*-Pakete an den Nachbarn sendet.

**init**

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.

**twoWay**

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.

**exchangeStart**

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 *Sequenz-*Nummer zu bestimmen.

**exchange**

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.

**loading**

Der Router sendet LS-Request-Pakete an den Nachbarn, die Informationen zu den ausstehenden Datenbank-Updates anfordern, welche im Datenaustausch-Status gesendet wurden.

**full**

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* erfordert eine kontinuierliche Verbindung der Autonomous-System-Backbone-Area. Außerdem erfordert die Funktion *OSPF*, 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* 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:

2, 6, 10, 14, 34, 38, 42, 46

Zeigt, dass der virtuelle Nachbar die Metrik Type of Service (TOS) 0 in AS-External-LSAs unterstützt.

0, 4, 8, 12, 32, 36, 40, 44

Zeigt, dass der virtuelle Nachbar TOS-Metriken unterstützt, bei denen es sich nicht um TOS 0 handelt.

4, 6, 12, 14, 36, 38, 44, 46

Zeigt, dass der virtuelle Nachbar Multicast-Routing unterstützt.

8, 10, 12, 14, 40, 42, 44, 46

Zeigt, dass der virtuelle Nachbar *Type 7*-LSAs unterstützt.

32, 34, 36, 38, 40, 42, 44, 46

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:

**down** (Voreinstellung)

Initialer Zustand einer Nachbarkonversation oder eines Routers, der die Konversation aufgrund des Ablaufs des *Dead-Intervall [s]* Timers beendet hat.

**attempt**

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 *Hello-Intervall [s]* festgelegt ist, *Hello*-Pakete an den Nachbarn sendet.

#### init

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.

#### twoWay

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.

#### exchangeStart

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 *Sequenz*-Nummer zu bestimmen.

#### exchange

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.

#### loading

Der Router sendet LS-Request-Pakete an den Nachbarn, die Informationen zu den ausstehenden Datenbank-Updates anfordern, welche im Datenaustausch-Status gesendet wurden.

#### full

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 [Routing > OSPF > Interfaces](#) in Spalte [Retrans-Intervall \[s\]](#) 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:

`markiert`

Der Router unterdrückt *Hello*-Pakete.

`unmarkiert`

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:

`asExternal Link`

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 *Sende-Verzögerung [s]* 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:

[i n t r a](#)

Eintrag für Routen aus dem OSPF innerhalb einer Area.

[i n t e r](#)

Eintrag für Routen aus dem OSPF zwischen Areas.

[e x t - t y p e 1](#)

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).

#### [ext-type2](#)

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).

#### [nssa-type1](#)

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).

#### [nssa-type2](#)

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:

1. . 255 (Voreinstellung: 1)

Routen mit dem Wert 255 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 *Erstellen*, um eine statische Route hinzuzufügen.

- Im Feld *Netz-Adresse* legen Sie die Adresse des Zielnetzes fest.  
Mögliche Werte:  
Gültige IPv4-Adresse  
Wenn Sie eine *Standard-Route (0.0.0.0)* festlegen, dann legen Sie im Feld *Next-Hop IP-Adresse* ein *Standard-Gateway* fest. Diese Einstellung hat Vorrang vor der Einstellung im folgenden Dialog:  
– Dialog *Grundeinstellungen > Netzwerk > IPv4*, Feld *Gateway-Adresse*
- Im Feld *Netzmaske* legen Sie die Netzmaske fest, die den Netzpräfix in der Adresse des Zielnetzes kennzeichnet.  
Mögliche Werte:  
Gültige IPv4-Netzmaske
- Im Feld *Next-Hop IP-Adresse* legen Sie IP-Adresse des nächsten Routers auf dem Pfad ins Zielnetz fest.  
Mögliche Werte:  
Gültige IPv4-Adresse  
Um eine *reject*-Route zu erstellen, legen Sie in diesem Feld den Wert *0.0.0.0* fest. Mit dieser Route verwirft das Gerät IP-Pakete, die an das Zielnetz adressiert sind, und informiert den Absender.
- Im Feld *Präferenz* legen Sie die Preference-Kennzahl fest, anhand der das Gerät entscheidet, welche von mehreren vorhandenen Routen zum Zielnetz es verwendet.  
Mögliche Werte:  
*1..255*  
Bei der Routing-Entscheidung bevorzugt das Gerät die Route mit dem numerisch niedrigsten Wert. Voreingestellt ist der im Rahmen *Konfiguration*, Feld *Präferenz* festgelegte Wert.
- In der Dropdown-Liste *Track-Name* 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 *Typ* und *Track-ID*.



Löschen

Entfernt die ausgewählte Tabellenzeile.

## Port

Zeigt das Router-Interface, über welches das Gerät an das Zielnetz adressierte IP-Pakete gegenwärtig sendet.

Mögliche Werte:

[<Router-Interface>](#)

Das Gerät vermittelt an das Zielnetz adressierte IP-Pakete über dieses Router-Interface.

[no port](#)

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:

[l o k a l](#)

Das Router-Interface ist mit dem Zielnetz direkt verbunden.

[E x t e r n](#)

Das Router-Interface ist mit dem Zielnetz über einen Router ([Next-Hop IP-Adresse](#)) verbunden.

[r e j e c t](#)

Das Gerät verwirft an das Zielnetz adressierte IP-Pakete und informiert den Absender.

[o t h e r](#)

Die Route ist inaktiv. Siehe Kontrollkästchen [Aktiv](#).

## Protokoll


Zeigt, wer diese Route erzeugt hat.

Mögliche Werte:

[l o k a l](#)

Das Gerät hat diese Route beim Einrichten des Router-Interfaces hinzugefügt. Siehe Dialog [Routing > Interfaces > Konfiguration](#).

### net mngt

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 [Routing > Global](#) ausgewählt ist, kann ECMP bis zu 4 Routen verwenden. Wenn Sie das Routing-Profil [pv4DataCenter](#) wählen, kann ECMP bis zu 16 Routen verwenden.

### ospf

Die Funktion *OSPF* hat diese Route hinzugefügt. Siehe Dialog [Routing > OSPF](#).

### 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:

0


Reserviert für Routen, die das Gerät beim Einrichten der Router-Interfaces hinzugefügt hat. Diese Routen haben in Spalte *Protokoll* den Wert *lokal*.

1.. 254

Bei der Routing-Entscheidung bevorzugt das Gerät die Route mit dem numerisch niedrigsten Wert.

255

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 [Erweitert > Tracking > Konfiguration](#).

Mögliche Werte:

Name des Tracking-Objekts, zusammensetzt aus *Typ* und *Track-ID*.

-

Kein Tracking-Objekt ausgewählt.

Diese Funktion ist ausschließlich für statische Routen nutzbar. (Spalte *Protokoll* = *netmngt*)

Aktiv

Zeigt, ob die Route aktiv oder inaktiv ist.

Mögliche Werte:

*markiert*

Die Route ist aktiv, das Gerät verwendet die Route.

*unmarkiert*

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 *L3-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 *L3-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 *L3-Relay* ein/aus.

Mögliche Werte:

*An*

Die Funktion *L3-Relay* ist global eingeschaltet.

*Aus* (Voreinstellung)

Die Funktion *L3-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:

`markiert`

Das Gerät fügt die Circuit-ID des DHCP-L3-Relay-Agenten zu den Suboptionen für Client-Anfragen hinzu.

`unmarkiert` (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:

`0..100` (Voreinstellung: `0`)

Wenn ein lokaler BOOTP/DHCP-Server im Netz fehlt, dann setzen Sie den Wert auf `0`.

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 `1`.

Übersteigt die Anzahl der Hops eines empfangenen BOOTP/DHCP-Paketes 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:

`1..16` (Voreinstellung: `4`)

### Information

Die folgenden Feldern zeigen die Werte seit dem letzten Neustart des Geräts. Nach einem Neustart setzt das Gerät die Werte auf `0` 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 *Erstellen*, um eine Tabellenzeile hinzuzufügen.

- Im Feld *Port* legen Sie das Port-basierte Router-Interface fest.

---

#### Anmerkung:

Auf VLAN-basierten Router-Interfaces unterstützt das Gerät die Funktion *L3-Relay* nicht.

---

#### Mögliche Werte:

*All* (Voreinstellung)

Das Gerät verarbeitet die Datenpakete, die es auf all seinen Interfaces empfangen hat.

Relay-Einträge mit diesem Wert legen eine globale Konfiguration fest.

*<verfügbare Interfaces>*

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 **UDP-Port** 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 **IP-Adresse** festgelegte IP-Adresse weiter.  
Mögliche Werte:
  - dhcp**  
Entspricht dem UDP-Port **67**.  
Das Gerät leitet Dynamic Host Configuration Protocol (DHCP)-Anfragen für IP-Adress-Zuweisung und Netzparameter weiter.
- Im Feld **IP-Adresse** 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 **0.0.0.0** 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 **0.0.0.0** einzugeben, stellen Sie sicher, dass im Feld **Port** ein von **All** verschiedener Wert festgelegt ist.
  - Um eine von **0.0.0.0** verschiedene IP-Adresse einzugeben, stellen Sie sicher, dass im Feld **Port** der Wert **All** 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 **L3-Relay** 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.

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 [Erstellen](#), um ein Loopback-Interface hinzuzufügen.

- Im Feld *Index* legen Sie die Nummer fest, die das Loopback-Interface eindeutig identifiziert.  
Mögliche Werte:  
1 . 8



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: 0.0.0.0)

### Subnet-Maske

Legt die Netzmaske für das Loopback-Interface fest.

Mögliche Werte:

Gültige IPv4-Netzmaske (Voreinstellung: 0.0.0.0)

Beispiel: 255.255.255.255

### Aktiv

Zeigt, ob das Loopback-Interface aktiv oder inaktiv ist.

Mögliche Werte:

`markiert` (Voreinstellung)

Das Loopback-Interface ist aktiv.

Beim Senden von SNMP-Traps verwendet das Gerät als Absender die IP-Adresse des 1. Loopback-Interfaces.

`unmarkiert`

Das Loopback-Interface ist inaktiv.

## 7.8 L3-Redundanz

[ Routing > L3-Redundanz ]

Das Menü enthält die folgenden Dialoge:

- [High Availability](#)
- [VRRP](#)

### 7.8.1 High Availability

[ Routing > L3-Redundanz > High Availability ]

Mit der Funktion *High Availability* trägt ein Firewall-Gerätepaar dazu bei, die Konnektivität des Netzes kontinuierlich zu gewährleisten, indem es auf erkannte Ausfälle oder Unterbrechungen reagiert. Das Hochverfügbarkeits (High Availability, HA)-Setup besteht aus zwei Firewall-Geräten. Ein Gerät hat die primäre Rolle. Das andere Gerät hat die sekundäre Rolle, die als Backup dient.

Im Normalbetrieb ist das Gerät in der primären Rolle im aktiven Zustand und kontrolliert den Datenfluss. Das Gerät in der sekundären Rolle ist im Standby-Zustand. Der Umschaltprozess basiert auf dem Virtual Router Redundancy Protocol (VRRP). Das primäre Firewall-Gerät sendet regelmäßig *Advertisement*-Nachrichten über seinen Betriebszustand an das sekundäre Firewall-Gerät. Wenn das sekundäre Firewall-Gerät innerhalb einer bestimmten Zeitspanne keine *Advertisement*-Nachrichten empfängt, stellt es fest, dass das primäre Firewall-Gerät möglicherweise nicht funktionsfähig ist. Das sekundäre Firewall-Gerät wird dann aktiv und greift ein, um die Konnektivität des Netzes mit minimaler Unterbrechung aufrechtzuerhalten. Sobald das primäre Firewall-Gerät wieder betriebsbereit ist, wird es zum Standby-Gerät.

Das Menü enthält die folgenden Dialoge:

- [High Availability Konfiguration](#)
- [High Availability Status](#)

## 7.8.1.1 High Availability Konfiguration

[Routing > L3-Redundanz > High Availability > Konfiguration]

Dieser Dialog ermöglicht Ihnen, die Einstellungen für die Funktion *High Availability* festzulegen.

### Funktion

Funktion

Schaltet die Funktion *High Availability* im Gerät ein/aus.

Voraussetzungen für das Einschalten der Funktion *High Availability*:

- Im Dialog *Routing > L3-Redundanz > VRRP > Konfiguration* ist die Funktion *VRRP* eingerichtet und die Funktion *Preempt-Modus* ist eingeschaltet.
- Im Dialog *Routing > L3-Redundanz > VRRP > Tracking* ist die VRRP-ID mit einem Tracking-Objekt verknüpft.
- In den Feldern der Rahmen *HA Rolle*, *VRRP-Interface*, *VRRP-ID*, *Primär* und *Sekundär* sind Werte festgelegt.

Mögliche Werte:

**An**

Die Funktion *High Availability* ist eingeschaltet.

Das Gerätepaar arbeitet zusammen, um eine kontinuierliche Firewall-Konnektivität des Netzes mit minimalen Unterbrechungen zu gewährleisten.

**Aus** (Voreinstellung)

Die Funktion *High Availability* ist ausgeschaltet.

### HA Rolle

HA Rolle

Legt die Rolle des High-Availability- (HA-) Geräts fest.

Mögliche Werte:

**kein** (Voreinstellung)

Dem Gerät ist keine High-Availability- (HA-) Rolle zugewiesen. Um die High-Availability- (HA-) Funktion zu nutzen, wählen Sie entweder die Rolle **primär** oder **sekundär**.

**primär**

Das Gerät arbeitet als primäres Firewall-Gerät.

**sekundär**

Das Gerät arbeitet als sekundäres Firewall-Gerät.

## VRRP-Interface

### Internes VRRP-Interface

Legt die Interface-Nummer für die Kommunikation mit dem internen Netz fest.

Voraussetzung ist, dass im Feld *Internes VRRP* der Wert - festgelegt ist.

Mögliche Werte:

<Interface-Nummer> (Voreinstellung: -)

### Externes VRRP-Interface

Legt die Interface-Nummer für die Kommunikation mit dem externen Netz fest.

Voraussetzung ist, dass im Feld *Externes VRRP* der Wert - festgelegt ist.

Mögliche Werte:

<Interface-Nummer> (Voreinstellung: -)

## VRRP-ID

### Internes VRRP

Legt die VRRP-ID für das interne Netz fest.

Voraussetzungen für das Einrichten von *Internal VRRP*:

- Im Dialog *Routing > L3-Redundanz > VRRP > Konfiguration* ist die VRRP-ID festgelegt und der *VRRP*-Betrieb ist eingeschaltet.
- Im Feld *Internes VRRP-Interface* ist ein Interface ausgewählt.

Mögliche Werte:

<VRRP ID> (Voreinstellung: -)

### Externes VRRP

Legt die VRRP-ID für das externe Netz fest.

Voraussetzungen für das Einrichten von *External VRRP*:

- Im Dialog *Routing > L3-Redundanz > VRRP > Konfiguration* ist die VRRP-ID festgelegt und der *VRRP*-Betrieb ist eingeschaltet.
- Im Feld *Externes VRRP-Interface* ist ein Interface ausgewählt.

Mögliche Werte:

<VRRP I D> (Voreinstellung: -)

## Sicherheit

### Sicherheitsschlüssel

Legt das Passwort fest, welches das Gerät zum Verschlüsseln und Entschlüsseln der Konfigurationsprofile verwendet.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 8..32 Zeichen

Das Gerät akzeptiert die folgenden Zeichen:

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

Verwenden Sie für das primäre und das sekundäre Firewall-Gerät denselben Wert.

### Sicherer Modus

Aktiviert/deaktiviert die Verschlüsselung der Konfigurationsprofile, wenn eines zwischen den High-Availability- (HA-) Geräten übertragen wird.

Mögliche Werte:

**marked**

Der Modus ist aktiv. Das Gerät verschlüsselt die Konfigurationsprofile.

Voraussetzung ist, dass im *Sicherheitsschlüssel*-Feld ein gültiger Wert festgelegt ist.

**unmarked** (Voreinstellung)

Der Modus ist inaktiv. Das Gerät verschlüsselt die Konfigurationsprofile nicht.

## Primär

### IP-Adresse

Legt die IP-Adresse für das primäre Firewall-Gerät fest.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung: 0.0.0.0)

### Netzmaske

Legt die Netzmaske für das primäre Firewall-Gerät fest.

Mögliche Werte:

Gültige IPv4-Netzmaske (Voreinstellung: 0.0.0.0)

### HA-Interface

Legt die für die Kommunikation zwischen dem primären und dem sekundären Firewall-Gerät verwendete Interface-Nummer fest.

Mögliche Werte:

<Interface-Nummer> (Voreinstellung: -)

Verwenden Sie für das primäre und das sekundäre Firewall-Gerät dieselbe Interface-Nummer.

## Sekundär

### IP-Adresse

Legt die IP-Adresse für das sekundäre Firewall-Gerät fest.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung: 0.0.0.0)

### Netzmaske

Legt die Netzmaske für das sekundäre Firewall-Gerät fest.

Mögliche Werte:

Gültige IPv4-Netzmaske (Voreinstellung: 0.0.0.0)

### HA-Interface

Legt die für die Kommunikation zwischen dem primären und dem sekundären Firewall-Gerät verwendete Interface-Nummer fest.

Mögliche Werte:

<Interface-Nummer> (Voreinstellung: -)

Verwenden Sie für das primäre und das sekundäre Firewall-Gerät dieselbe Interface-Nummer.

## Heartbeat

### Intervall [s]

Gibt das Sendeintervall in Sekunden zwischen aufeinanderfolgenden High-Availability- (HA-) Zustandsnachrichten an.

Mögliche Werte:

1..5 (Voreinstellung: 1)

Verwenden Sie für das primäre und das sekundäre Firewall-Gerät denselben Wert.

### Wiederholungen

Legt die maximale Anzahl aufeinanderfolgender Verbindungsversuche zwischen dem primären und dem sekundären Firewall-Gerät fest, bevor die *Heartbeat*-Nachrichten als verloren gelten.

Mögliche Werte:

1..10 (Voreinstellung: 3)

Verwenden Sie für das primäre und das sekundäre Firewall-Gerät denselben Wert.

## Standby-Konfiguration

### Standby Wartungsmodus

Aktiviert/deaktiviert die Änderung von Konfigurationsprofilen auf dem Standby-Gerät.

Mögliche Werte:

`marked`

Der Modus ist aktiv. Sie können auf dem Standby-Gerät Konfigurationsprofile ändern und Wartungsarbeiten (wie Firmware-Aktualisierung, Neustart) durchführen.

`unmarked` (Voreinstellung)

Der Modus ist inaktiv. Sie können auf dem Standby-Gerät die Konfigurationsprofile nicht ändern.

## Manuell umschalten

### Switchover

Schaltet das Firewall-Gerät manuell vom `aktiv`-Status in den `standby`-Status. Die Schaltfläche funktioniert ausschließlich auf dem aktiven Firewall-Gerät. Voraussetzung ist, dass die Konfigurationsprofile des aktiven Geräts auf das Standby-Gerät übertragen sind.

## 7.8.1.2 High Availability Status

[ Routing > L3-Redundanz > High Availability > Status ]

Dieser Dialog gibt Ihnen einen Überblick über den Status der Funktion *High Availability*.

### Status

#### HA Link

Zeigt den Betriebsstatus der Verbindung zwischen dem primären und dem sekundären Firewall-Gerät.

Mögliche Werte:

*up*

Die Verbindung zwischen den Geräten ist aktiv und funktionsfähig.

*down*

Die Verbindung zwischen den Geräten ist inaktiv.

#### Heartbeat

Zeigt den Status der Verbindung zwischen dem primären und dem sekundären Firewall-Gerät.

Mögliche Werte:

*i nakti v*

Die Funktion *High Availability* ist ausgeschaltet.

*unreachabl e*

Eines der Geräte ist für das andere nicht erreichbar.

*err ei chbar*

Die Geräte können sich gegenseitig erreichen.

### Primär

#### Zustand

Zeigt den Status des primären Firewall-Geräts.

Mögliche Werte:

*i nakti v*

Die Funktion *High Availability* ist ausgeschaltet.

*i ni t*

Das Gerät ist im *Init*-Zustand. Das Gerät wartet auf mögliche Ereignisse, um den nächsten Zustand einzunehmen.

*akti v*

Das Gerät ist im *aktiven* Zustand.

*standby*

Das Gerät ist im *Standby*-Zustand.

**standaloneActive**

Das Gerät befand sich im Zustand *aktiv* und die *Heartbeat*-Wiederholungsversuche sind abgelaufen. Die Verbindung zwischen dem primären und dem sekundären Firewall-Gerät ist unterbrochen.

**standaloneStandby**

Das Gerät befand sich im Zustand *standby* und die *Heartbeat*-Wiederholungsversuche sind abgelaufen. Die Verbindung zwischen dem primären und dem sekundären Firewall-Gerät ist unterbrochen.

**inSync**

Das Standby-Firewall-Gerät synchronisiert gerade seine Einstellungen.

**outOfSync**

Die Einstellungen des primären Firewall-Geräts sind nicht mit denen des sekundären Firewall-Geräts synchronisiert.

## Sekundär

### Zustand

Zeigt den Status des sekundären Firewall-Geräts.

Mögliche Werte:

**inactive**

Die Funktion *High Availability* ist ausgeschaltet.

**init**

Das Gerät ist im *Init*-Zustand. Das Gerät wartet auf mögliche Ereignisse, um den nächsten Zustand einzunehmen.

**active**

Das Gerät ist im *aktiven* Zustand.

**standby**

Das Gerät ist im *Standby*-Zustand.

**standaloneActive**

Das Gerät befand sich im Zustand *aktiv* und die *Heartbeat*-Wiederholungsversuche sind abgelaufen. Die Verbindung zwischen dem primären und dem sekundären Firewall-Gerät ist unterbrochen.

**standaloneStandby**

Das Gerät befand sich im Zustand *standby* und die *Heartbeat*-Wiederholungsversuche sind abgelaufen. Die Verbindung zwischen dem primären und dem sekundären Firewall-Gerät ist unterbrochen.

**inSync**

Das Standby-Firewall-Gerät synchronisiert gerade seine Einstellungen.

**outOfSync**

Die Einstellungen des primären Firewall-Geräts sind nicht mit denen des sekundären Firewall-Geräts synchronisiert.

## 7.8.2 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 *VRRP* finden Sie im Anwender-Handbuch „Konfiguration“.

---

Das Menü enthält die folgenden Dialoge:

- [VRRP Konfiguration](#)
- [VRRP Statistiken](#)
- [VRRP Tracking](#)

## 7.8.21 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 [VRRP](#)-Redundanz im Gerät ein/aus.

Mögliche Werte:

[An](#)

Die Funktion [VRRP](#) ist eingeschaltet.

[Aus](#) (Voreinstellung)

Die Funktion [VRRP](#) ist ausgeschaltet.

### Konfiguration

Trap senden (VRRP-Master)

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät der VRRP-Master ist.

Mögliche Werte:

[markiert](#)

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

Das Gerät sendet einen SNMP-Trap, wenn es der VRRP-Master ist.

[unmarkiert](#) (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:

**markiert**

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

Das Gerät sendet einen SNMP-Trap, wenn es ein VRRP-Paket mit Authentifizierungsinformation empfängt.

**unmarkiert** (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 [Erstellen](#), 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 397](#).

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:

`markiert`

Die VRRP-Instanz ist aktiv.

`unmarkiert` (Voreinstellung)

Die VRRP-Instanz ist inaktiv.

## Betriebszustand

Zeigt den Status der Tabellenzeile. Der Betriebsmodus des entsprechenden virtuellen Routers bestimmt den Status einer gegenwärtig aktiven Tabellenzeile.

Mögliche Werte:

`aktiv`

Die Instanz ist erreichbar.

`notInService`

Die Instanz existiert im Gerät, ihr fehlen allerdings notwendige Information und sie ist unerreichbar.

`notReady`

Die Instanz existiert im Gerät, ihr fehlen allerdings notwendige Information und sie ist unerreichbar.

## Zustand

Zeigt den VRRP-Zustand.

Mögliche Werte:

`initialize`

VRRP initialisiert sich gerade, die Funktion ist inaktiv, oder der Master-Router ist noch unbenannt.

`backup`

Der Router beobachtet die Möglichkeit, Master-Router zu werden.

`master`

Der Router ist der Master-Router.

## Basis Priorität

Legt die Priorität des virtuellen Routers fest. Wenn sich der Wert vom Wert im Feld *Priorität* unterscheidet, dann ist das überwachte Objekt nicht erreichbar oder der virtuelle Router ist Inhaber der IP-Adresse.

Mögliche Werte:

`1..254` (Voreinstellung: `100`)

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 `50` dem primären Router und den Wert `100` dem nächsten Router zu. Wiederholen Sie den Vorgang für den Wert `150` usw. Diese Aufteilung vereinfacht das spätere Hinzufügen eines weiteren Routers mit einer Priorität zwischen den bestehenden Werten, zum Beispiel mit dem Wert `75`.

## Priorität

Zeigt den Wert für die *VRRP*-Priorität. Die Priorität legen Sie fest im Dialog *Routing > OSPF > Interfaces*. 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 *VRRP*, dem Inhaber der IP-Adresse den Prioritätswert **255** zuzuweisen und den Router als Master-Router zu deklarieren.

Mögliche Werte:

**0**

Je größer die Zahl, desto höher die Priorität. Das Deaktivieren oder Entfernen eines *VRRP*-Routers, der die Master-Rolle inne hat, zwingt die Instanz zum Senden einer Nachricht mit Prioritätswert **0**. So wird den anderen Backup-Routern mitgeteilt, dass der Master-Router nicht teilnimmt. Das Senden des Prioritätswerts **0** erzwingt einen neuen Auswahlprozess.

**1.. 255**

Der Wert **255** 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 **0.0.0.0**.

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:

**markiert** (Voreinstellung)

Der *Preempt-Modus* ist aktiv. Der Router übernimmt die Master-Router-Rolle von einem Router mit niedrigerer *VRRP*-Priorität, ohne dass ein Auswahlprozess stattfindet.

**unmarkiert**

Der *Preempt-Modus* 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 *1:1-NAT*-Regeln verwendet. Voraussetzung ist, dass im Dialog [Routing > Interfaces > Konfiguration](#) für das betreffende Interface, welches von der VRRP-Instanz verwendet wird, das Kontrollkästchen *Proxy-ARP* unmarkiert ist.

Mögliche Werte:

**markiert**

Die Funktion *Proxy ARP* ist aktiv.

Das Gerät antwortet auf empfangene ARP-Anfragen von Endgeräten, die sich in anderen Netzen befinden.

**unmarkiert** (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: **0.0.0.0**)

Die Voreinstellung **0.0.0.0** zeigt, dass der Router die niedrigere IP-Adresse als *Master IP-Adresse* verwendet.

Sie können die IP-Adresse eines Router-Interfaces auswählen, das im Dialog [Routing > Interfaces > Konfiguration](#) eingerichtet ist.

## Master IP-Adresse

Zeigt die gegenwärtige IP-Adresse des Master-Router-Interfaces.

Mögliche Werte:

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

**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 [Routing > L3-Redundanz > VRRP > Konfiguration](#) das Fenster *Wizard*.

Öffnen Sie im Fenster *Wizard* die Seite *Eintrag erstellen oder auswählen*.

- Wählen Sie in der Dropdown-Liste *Port* ein Router-Interface.
- Legen Sie in Spalte *VRID* den Virtual Router Identifier fest.

Öffnen Sie im Fenster *Wizard* die Seite *Eintrag bearbeiten*.

– Legen Sie in Registerkarte *VRRP*, Rahmen *Konfiguration* die Werte für folgende Parameter fest:

*Priorität*


*Preempt-Modus*

*Advertisement-Intervall [s]*

*Ping-Antwort*

Wählen Sie in der Dropdown-Liste die IP-Adresse für den *VRRP Master-Kandidat*.

Klicken Sie die Schaltfläche *Fertig*, um die Einstellungen in die VRRP-Router-Interface-Tabelle zu übernehmen.

Wählen Sie im Dialog *Routing > L3-Redundanz > VRRP > Konfiguration*, Rahmen *Funktion* das Optionfeld *An*. Klicken Sie anschließend die Schaltfläche .

### **Vorhandene VRRP-Router-Instanz bearbeiten**

Führen Sie einen der folgenden Schritte aus:

Wählen Sie im Dialog *Routing > L3-Redundanz > VRRP > Konfiguration* 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 *Routing > L3-Redundanz > VRRP > Konfiguration* eine Tabellenzeile und

klicken Sie die Schaltfläche .

## **[Wizard: VRRP-Konfiguration]**

Das Fenster *Wizard* 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 *Wizard* 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 *VRID* unten einen Wert fest.

### Port

Legt das Port-basierte oder VLAN-basierte Router-Interface fest. Im Dialog *Routing > Interfaces > Konfiguration* prüfen Sie, ob auf dem Port ein Router-Interface eingerichtet ist.

Mögliche Werte:

[<Port number>](#)

Port-basiertes Router-Interface

[VLAN/ <VLAN ID>](#)

VLAN-basiertes Router-Interface

### VRID

Legt den Virtual Router Identifier fest.

Mögliche Werte:

[1.. 255](#)

Ein virtueller Router verwendet *00-00-5E-00-01-XX* als seine MAC-Adresse. Der hier festgelegte Wert ersetzt das letzte Oktett (*XX*) in der MAC-Adresse. Weisen Sie jedem physischen Router innerhalb einer virtuellen Router-Instanz einen eindeutigen Wert zu. Das Gerät ändert den wirk-samen Prioritätswert in [255](#) 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 *VRRP*-Redundanz für die gegenwärtige Instanz ein/aus.

Mögliche Werte:

[An](#)

Die Funktion *VRRP* ist für die gegenwärtige Instanz eingeschaltet.

[Aus](#) (Voreinstellung)

Die Funktion *VRRP* ist für die gegenwärtige Instanz ausgeschaltet.

## Konfiguration

### Basis Priorität

Legt die Priorität des virtuellen Routers fest. Wenn sich der Wert vom Wert im Feld *Priorität* unterscheidet, dann ist das überwachte Objekt nicht erreichbar oder der virtuelle Router ist Inhaber der IP-Adresse.

#### Mögliche Werte:

1. . 254 (Voreinstellung: 100)

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 50 dem primären Router und den Wert 100 dem nächsten Router zu. Wiederholen Sie den Vorgang für den Wert 150 usw. Diese Aufteilung vereinfacht das spätere Hinzufügen eines weiteren Routers mit einer Priorität zwischen den bestehenden Werten, zum Beispiel mit dem Wert 75.

### Priorität

Zeigt den Wert für die *VRRP*-Priorität. Die Priorität legen Sie fest im Dialog *Routing > OSPF > Interfaces*. 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 *VRRP*, dem Inhaber der IP-Adresse den Prioritätswert 255 zuzuweisen und den Router als Master-Router zu deklarieren.

#### Mögliche Werte:

0

Je größer die Zahl, desto höher die Priorität. Das Deaktivieren oder Entfernen eines *VRRP*-Routers, der die Master-Rolle inne hat, zwingt die Instanz zum Senden einer Nachricht mit Prioritätswert 0. So wird den anderen Backup-Routern mitgeteilt, dass der Master-Router nicht teilnimmt. Das Senden des Prioritätswerts 0 erzwingt einen neuen Auswahlprozess.

1. . 255

Der Wert 255 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:

markiert (Voreinstellung)

Der *Preempt-Modus* ist aktiv. Der Router übernimmt die Master-Router-Rolle von einem Router mit niedrigerer VRRP-Priorität, ohne dass ein Auswahlprozess stattfindet.

unmarkiert

Der *Preempt-Modus* 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:

1..255 (Voreinstellung: 1)

**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 *1:1-NAT*-Regeln verwendet. Voraussetzung ist, dass im Dialog [Routing > Interfaces > Konfiguration](#) für das betreffende Interface, welches von der VRRP-Instanz verwendet wird, das Kontrollkästchen *Proxy-ARP* unmarkiert ist.

Mögliche Werte:

markiert

Die Funktion *Proxy ARP* ist aktiv.

Das Gerät antwortet auf empfangene ARP-Anfragen von Endgeräten, die sich in anderen Netzen befinden.

unmarkiert (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: 0.0.0.0)

Sie können die IP-Adresse eines Router-Interfaces auswählen, das im Dialog [Routing > Interfaces > Konfiguration](#) eingerichtet ist.

## Tracking

### Aktuelle Track-Einträge

Zeigt die im Gerät verfügbaren Tracking-Objekte. Tracking-Objekte richten Sie ein im Dialog [Erweitert > Tracking > Konfiguration](#). Wählen Sie einen Eintrag, um fortzufahren. Alternativ dazu wählen Sie im Feld [Track-Name](#) 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:

- *Interface*  
Das Gerät überwacht den Link-Status seiner physischen Ports, Link-Aggregation-, LRE- oder VLAN-Router-Interfaces.
- *Ping*  
Das Gerät überwacht die Route zu einem entfernten Router oder Endgerät durch periodisches Senden von *ICMP Echo Request*-Paketten.
- *Logical*  
Das Gerät überwacht logisch miteinander verknüpfte Tracking-Objekte und ermöglicht somit komplexe Überwachungsaufgaben.

### Zugewiesene Track-Einträge

Zeigt die Tracking-Objekte mit zugewiesenem [Dekrement](#)-Wert. Sie können einen Eintrag entfernen, indem Sie das Symbol **✕** 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 [Erweitert > Tracking > Konfiguration](#).

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 *Typ* und *Track-ID*.

Dekrement

Legt den Wert fest, um den die VRRP-Instanz die Priorität des virtuellen Routers reduziert, wenn das Überwachungsergebnis negativ ist.

Mögliche Werte:

1.. 253

---

**Anmerkung:**

Wenn im Dialog *Routing > L3-Redundanz > VRRP > Konfiguration* der Wert in Spalte *Priorität* gleich 255 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 *Zugewiesene Track-Einträge* einen Eintrag basierend auf den in den Feldern *Track-Name* und *Dekrement* festgelegten Werten hinzu.

## Virtuelle IP-Adressen

IP-Adresse

Zeigt die primäre IP-Adresse des Router-Interfaces.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung: 0. 0. 0. 0)

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 *Routing > Interfaces > Konfiguration*.

Virtuelle IP-Adressen

Zeigt die virtuelle IP-Adresse, die Sie im Feld *IP-Adresse* festgelegt haben. Sie können einen Eintrag entfernen, indem Sie das Symbol **X** 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 *Virtuelle IP-Adressen* einen Eintrag basierend auf den im Feld *IP-Adresse* festgelegten Werten hinzu.

## 7.8.2.2 VRRP Statistiken

[Routing > L3-Redundanz > VRRP > Statistiken]

Der Dialog zeigt die Anzahl der Zähler, die für die Funktion **VRRP** 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 255.

### Null-Prioritätspakete empfangen

Zeigt die Anzahl der empfangenen VRRP-Nachrichten mit Priorität gleich 0.

### Null-Prioritätspakete gesendet

Zeigt die Anzahl der VRRP-Nachrichten, die das Gerät mit der Priorität 0 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.

## 7.8.23 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 Ready**.

### Tabelle

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

Schaltflächen



Hinzufügen

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

- In der Dropdown-Liste *Port VRID* wählen Sie Interface und Router-ID eines eingerichteten virtuellen Routers aus.
- In der Dropdown-Liste *Track-Name* 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 *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 *Typ* und *Track-ID*.

Logische Tracker, die mehrere Tracker kombinieren

-

Kein Tracking-Objekt ausgewählt.

Tracking-Objekte richten Sie ein im Dialog *Erweitert > Tracking > Konfiguration*.

#### 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.. 253

---

**Anmerkung:**

Wenn im Dialog [Routing > L3-Redundanz > VRRP > Konfiguration](#) der Wert in Spalte *Priorität* gleich 255 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:

*not Ready*

Das Tracking-Objekt ist nicht aktiv.

*up*

Das Überwachungsergebnis ist positiv:

- Der Link-Status ist aktiv.
- oder
- Der entfernte Router oder das Endgerät ist erreichbar.

*down*

Das Überwachungsergebnis ist negativ:

- Der Link-Status ist inaktiv.
- oder
- Der entfernte Router oder das Endgerät ist unerreichbar.

Eine Kombination der Tracker *up* und *down*.

#### Aktiv

Zeigt, ob die Überwachung des Tracking-Objekts aktiv oder inaktiv ist.

Mögliche Werte:

*markiert*

Überwachung des Tracking-Objekts ist aktiv.

*unmarkiert*

Die Überwachung des Tracking-Objekts ist inaktiv. Sie aktivieren die Überwachung im Dialog [Erweitert > Tracking > Konfiguration](#), Spalte *Aktiv*.

## 7.9 NAT

[Routing > NAT]

Das Menü enthält die folgenden Dialoge:

- [NAT Global](#)
- [1:1-NAT](#)
- [Destination-NAT](#)

- Masquerading-NAT
- Double-NAT


## 7.9.1 NAT Global

[Routing > NAT > NAT Global]

Network Address Translation (*NAT*) umfasst mehrere Verfahren, die automatisiert die IP-Adressinformation im Datenpaket verändern. Wenn im Gerät eingerichtet, ermöglicht die Funktion *NAT* Kommunikationsverbindungen zwischen Geräten in unterschiedlichen Netzen.

Dieser Dialog zeigt, wie viele *NAT*-Regeln für die einzelnen *NAT*-Verfahren einrichtbar sind und signalisiert Änderungen an aktiven *NAT*-Regeln.

Das Gerät bietet Ihnen ein mehrstufiges Konzept für das Einrichten und Anwenden der *NAT*-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 *1:1-NAT*-Regeln auf den Datenstrom an.

Das Gerät entfernt dabei auch die Zustandsinformationen des Paketfilters. Dies beinhaltet eventuell vorhandene *DCE RPC*-Informationen der Funktion *OPC Enforcer*. 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 *1:1-NAT*-Regeln an, die Sie im Gerät einrichten können.

1:1-NAT Eingerichtete Regeln


Zeigt die Anzahl der im Gerät eingerichteten *1:1-NAT*-Regeln.

### 1:1-NAT Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten *1:1-NAT*-Regeln von den gespeicherten *1:1-NAT*-Regeln unterscheiden.

Mögliche Werte:

*markiert*

Mindestens eine gespeicherte *1:1-NAT*-Regel enthält geänderte Einstellungen. Um die noch ausstehenden Regeln auf den Datenstrom anzuwenden, klicken Sie die Schaltfläche .

*unmarkiert*

Das Gerät wendet die gespeicherten *1:1-NAT*-Regeln auf den Datenstrom an.

## Destination-NAT

### Schaltflächen

 Commit

Wendet die im Gerät gespeicherten *Destination-NAT*-Regeln auf den Datenstrom an.

Das Gerät entfernt dabei auch die Zustandsinformationen des Paketfilters. Dies beinhaltet eventuell vorhandene *DCE RPC*-Informationen der Funktion *OPC Enforcer*. 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 *Destination-NAT*-Regeln an, die Sie im Gerät einrichten können.

### Destination-NAT Eingerichtete Regeln

Zeigt die Anzahl der im Gerät eingerichteten *Destination-NAT*-Regeln.

### Destination-NAT Eingerichtete Interfaces


Zeigt die Anzahl der im Gerät eingerichteten *Destination-NAT*-Router-Interfaces.

### Destination-NAT Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten *Destination-NAT*-Regeln von den gespeicherten *Destination-NAT*-Regeln unterscheiden.

Mögliche Werte:

*markiert*

Mindestens eine gespeicherte *Destination-NAT*-Regel enthält geänderte Einstellungen. Um die noch ausstehenden Regeln auf den Datenstrom anzuwenden, klicken Sie die Schaltfläche .

*unmarkiert*

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

## Masquerading-NAT

Schaltflächen

 Commit

Wendet die im Gerät gespeicherten *Masquerading-NAT*-Regeln auf den Datenstrom an.

Das Gerät entfernt dabei auch die Zustandsinformationen des Paketfilters. Dies beinhaltet eventuell vorhandene *DCE RPC*-Informationen der Funktion *OPC Enforcer*. 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 *Masquerading-NAT*-Regeln an, die Sie im Gerät einrichten können.

Masquerading-NAT Eingerichtete Regeln

Zeigt die Anzahl der im Gerät eingerichteten *Masquerading-NAT*-Regeln.

Masquerading-NAT Eingerichtete Interfaces

Zeigt die Anzahl der im Gerät eingerichteten *Masquerading-NAT*-Router-Interfaces.

Masquerading-NAT Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten *Masquerading-NAT*-Regeln von den gespeicherten *Masquerading-NAT*-Regeln unterscheiden.

Mögliche Werte:

*markiert*

Mindestens eine gespeicherte *Masquerading-NAT*-Regel enthält geänderte Einstellungen. Um die noch ausstehenden Regeln auf den Datenstrom anzuwenden, klicken Sie die Schaltfläche

 .

*unmarkiert*

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

## Double-NAT

### Schaltflächen

 Commit

Wendet die im Gerät gespeicherten *Double-NAT*-Regeln auf den Datenstrom an.

Das Gerät entfernt dabei auch die Zustandsinformationen des Paketfilters. Dies beinhaltet eventuell vorhandene *DCE RPC*-Informationen der Funktion *OPC Enforcer*. 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 *Double-NAT*-Regeln an, die Sie im Gerät einrichten können.

### Double-NAT Eingerichtete Regeln

Zeigt die Anzahl der im Gerät eingerichteten *Double-NAT*-Regeln.

### Double-NAT Eingerichtete Interfaces


Zeigt die Anzahl der im Gerät eingerichteten *Double-NAT*-Router-Interfaces.

### Double-NAT Änderungen vorhanden

Zeigt, ob sich die auf den Datenstrom angewendeten *Double-NAT*-Regeln von den gespeicherten *Double-NAT*-Regeln unterscheiden.

Mögliche Werte:

*markiert*

Mindestens eine gespeicherte *Double-NAT*-Regel enthält geänderte Einstellungen. Um die noch ausstehenden Regeln auf den Datenstrom anzuwenden, klicken Sie die Schaltfläche .

*unmarkiert*

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

## 7.9.2 1:1-NAT

[Routing > NAT > 1:1-NAT]

Die Funktion **1:1-NAT** ermöglicht Ihnen, innerhalb eines lokalen Netzes Kommunikationsverbindungen zu Endgeräten aufzubauen, die sich in anderen Netzen befinden. Der **NAT-Router** „verschiebt“ die Endgeräte virtuell in das öffentliche Netz. Dazu ersetzt der **NAT-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 **1:1-NAT**-Verfahren ist, dass der **NAT-Router** selbst auf ARP-Anfragen antwortet. Aktivieren Sie hierzu für das betreffende Interface die Funktion **Proxy-ARP** im Dialog **Routing > Interfaces > Konfiguration** oder im Dialog **Routing > L3-Redundanz > VRRP > Konfiguration**.

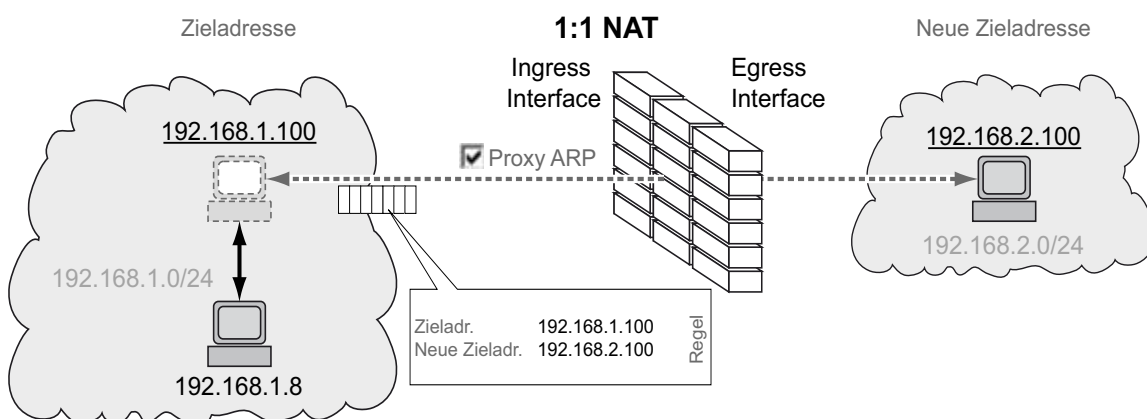


Abb. 3: Funktionsprinzip der Funktion 1:1-NAT

Um die Funktion **NAT** 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:

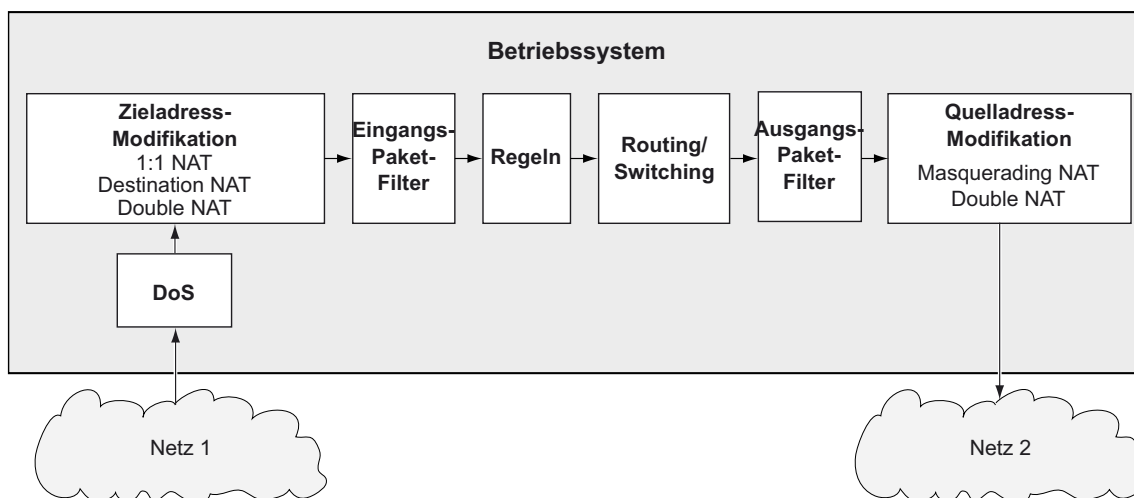


Abb. 4: Bearbeitungsreihenfolge der Datenpakete im Gerät

Das Menü enthält die folgenden Dialoge:

- [1:1-NAT Regel](#)

## 7.9.21 1:1-NAT Regel

[Routing > NAT > 1:1-NAT > Regel]

In diesem Dialog richten Sie die *1:1-NAT*-Regeln ein und weisen Router-Interfaces zu, auf die das Gerät die *1:1-NAT*-Regeln anwendet. Das Gerät ermöglicht, bis zu 255 *1:1-NAT*-Regeln einzurichten.

### Tabelle

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

Schaltflächen



Hinzufügen

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

- Im Feld *Ziel Adresse* 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 *Neue Adresse Ziel* festgelegte Zieladresse.

Mögliche Werte:

Gültige IPv4-Adresse

Das Gerät wendet die *1:1-NAT*-Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Zieladresse enthalten.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Das Gerät wendet die *1:1-NAT*-Regel ausschließlich auf Datenpakete an, die eine Zieladresse im hier festgelegten Subnetz enthalten.

- Im Feld *Neue Adresse Ziel* 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 *Ok* fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist dieser Tabellenzeile die in den Feldern *Ziel Adresse* und *Neue Adresse Ziel* 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 **1:1-NAT**-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 **1:1-NAT**-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 **0** in aufsteigender Reihenfolge an.

Mögliche Werte:

**0** . **6500** (Voreinstellung: **0**)

## Eingangs-Interface

Weist der **1:1-NAT**-Regel das Router-Interface zu, auf dem das Gerät die Datenpakete empfängt. Die **1:1-NAT**-Regel macht im hier angeschlossenen Netz das Ziel-Endgerät virtuell erreichbar.

Mögliche Werte:

**<Interface-Nummer>**

Das Gerät wendet die **1:1-NAT**-Regel ausschließlich auf diesem Router-Interface an, und zwar ausschließlich auf Datenpakete, die an die in Spalte **Ziel Adresse** festgelegte IP-Adresse adressiert sind.

**no Port**

Der **1:1-NAT**-Regel ist kein Router-Interface zugewiesen. Jemand hat das Router-Interface nach dem letzten Bearbeiten der **1:1-NAT**-Regel entfernt.

Die ARP-Proxy-Funktion auf diesem Router-Interface schalten Sie im Dialog **Routing > Interfaces > Konfiguration** ein.

## Ziel Adresse

Legt die Zieladresse der Datenpakete fest, auf die das Gerät die **1:1-NAT**-Regel anwendet. Das Gerät vermittelt Datenpakete mit dieser Zieladresse an die in Spalte **Neue Adresse Ziel** festgelegte Zieladresse.

Mögliche Werte:

Gültige IPv4-Adresse

Das Gerät wendet die **1:1-NAT**-Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Zieladresse enthalten.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Das Gerät wendet die **1:1-NAT**-Regel ausschließlich auf Datenpakete an, die eine Zieladresse im hier festgelegten Subnetz enthalten.

#### Ausgangs-Interface

Weist der *1:1-NAT*-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:

`<Interface-Nummer>`

Das Gerät vermittelt die modifizierten Datenpakete auf diesem Router-Interface.

`no Port`

Der *1:1-NAT*-Regel ist kein Router-Interface zugewiesen. Jemand hat das Router-Interface nach dem letzten Bearbeiten der *1:1-NAT*-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 *1:1-NAT*-Regel auf ein Datenpaket anwendet.

Mögliche Werte:

`markiert`

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

Das Gerät sendet einen SNMP-Trap, wenn es die *1:1-NAT*-Regel auf ein Datenpaket anwendet.

`unmarkiert` (Voreinstellung)

Das Senden von SNMP-Traps ist inaktiv.

#### Log

Aktiviert/deaktiviert die Protokollierung in der System-Log-Datei, wenn das Gerät die in dieser Tabellenzeile festgelegte *1:1-NAT* Regel anwendet.

Mögliche Werte:

`markiert`

Die Protokollierung ist aktiv.

Das Gerät erstellt einen Eintrag in der System-Log-Datei, wenn das Gerät die in dieser Tabellenzeile festgelegte *1:1-NAT*-Regel anwendet. Siehe Dialog *Diagnose > Bericht > System-Log*.

`unmarkiert` (Voreinstellung)

Die Protokollierung ist inaktiv.

Aktiv

Aktiviert/deaktiviert die **1:1-NAT**-Regel.

Mögliche Werte:

**markiert**

Die Regel ist aktiv.

**unmarkiert** (Voreinstellung)

Die Regel ist inaktiv.

### 7.9.3 Destination-NAT

[Routing > NAT > Destination-NAT]

Die Funktion **Destination-NAT** ermöglicht Ihnen, in einem lokalen Netz den Datenstrom ausgehender Kommunikationsverbindungen auf einen oder über einen Server umzuleiten.

Eine spezielle Form der Funktion **Destination-NAT** 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 **NAT-Router** auf, die Funktion **Destination-NAT** kümmert sich um die Weiterleitung in die Produktionszelle.

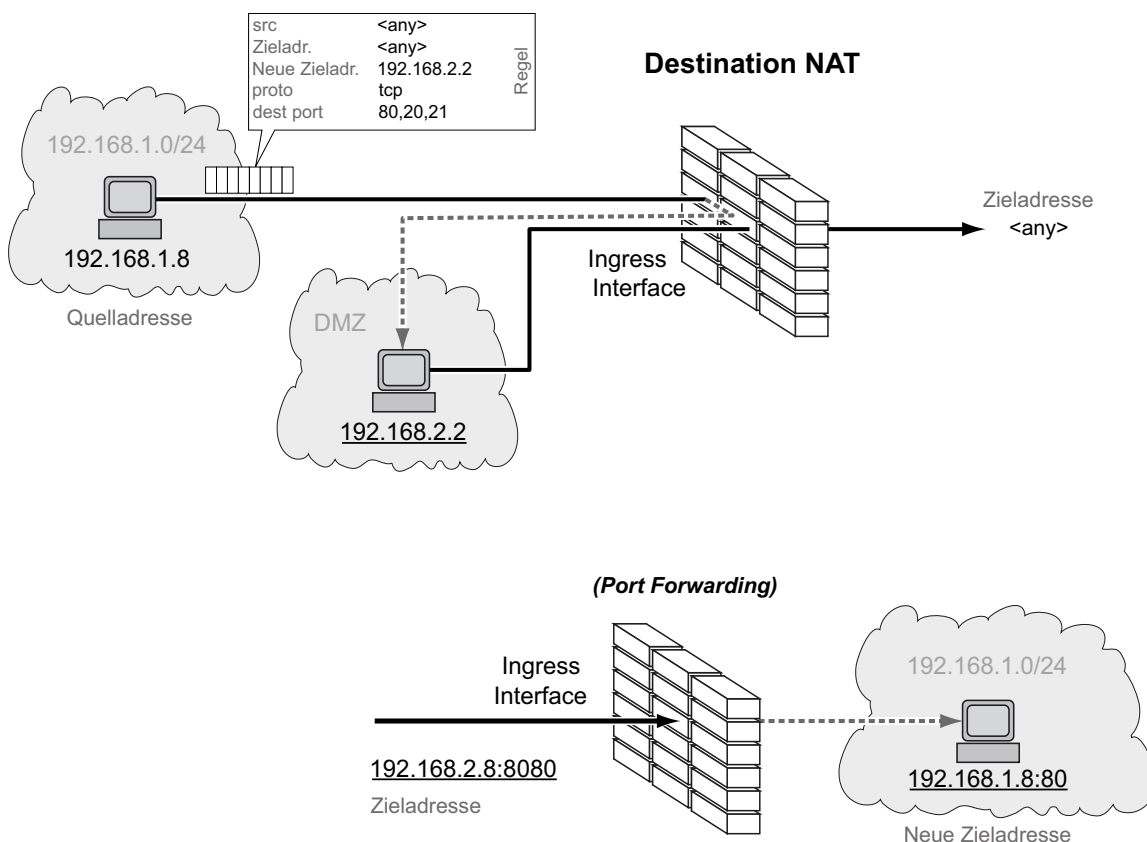


Abb. 5: Funktionsprinzip der Funktion **Destination-NAT**

Um die Funktion **NAT** 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:

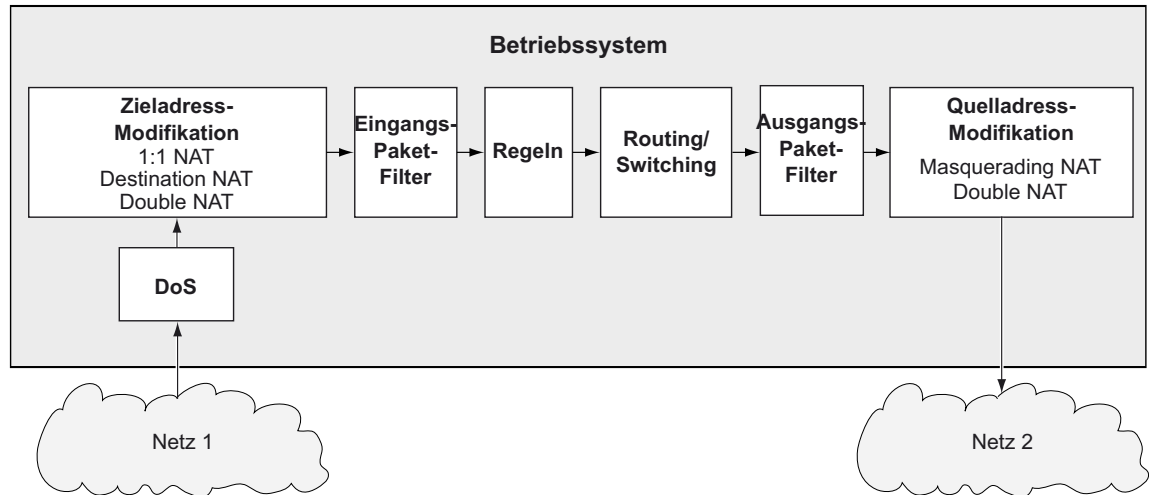


Abb. 6: Bearbeitungsreihenfolge der Datenpakete im Gerät

Das Menü enthält die folgenden Dialoge:

- [Destination-NAT Regel](#)
- [Destination-NAT Zuweisung](#)
- [Destination-NAT Übersicht](#)

### 7.9.3.1 Destination-NAT Regel

[Routing > NAT > Destination-NAT > Regel]

In diesem Dialog richten Sie die *Destination-NAT*-Regeln ein.

Ein Router-Interface weisen Sie der betreffenden *Destination-NAT*-Regel im Dialog *Routing > NAT > Destination-NAT > Zuweisung* zu.

Eine Übersicht, welche *Destination-NAT*-Regel welchem Router-Interface zugewiesen ist, finden Sie im Dialog *Routing > NAT > Destination-NAT > Übersicht*.

Das Gerät ermöglicht, bis zu 255 *Destination-NAT*-Regeln einzurichten.

#### Tabelle

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

#### Schaltflächen



Hinzufügen

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

- Im Feld *Neue Adresse Ziel* 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 *Ok* fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist dieser Tabellenzeile den im Feld *Neue Adresse Ziel* 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 *Destination-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 *Destination-NAT*-Regel anwendet.

Mögliche Werte:

*any* (Voreinstellung)

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

Gültige IPv4-Adresse

Das Gerät wendet die *Destination-NAT*-Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.

Gültige IPv4-Adresse und Netzmaske in CIDR-Notation

Das Gerät wendet die *Destination-NAT*-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 *Destination-NAT*-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 *Destination-NAT*-Regel anwendet. Voraussetzung ist, dass im Feld *Protokoll* der Wert *TCP* oder *UDP* festgelegt ist.

Mögliche Werte:

*any* (Voreinstellung)

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

1..65535 (2<sup>16</sup> - 1)

Das Gerät wendet die *Destination-NAT*-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 *21*.
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel *21, 80, 110*.
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel *2000-3000*.
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel *21, 2000-3000, 65535*.

Die Spalte ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel *21, 2000-3000, 65535* eingeben, verwenden Sie 4 von 15 Zahlenwerten.

#### Ziel Adresse

Legt die Zieladresse der Datenpakete fest, auf die das Gerät die *Destination-NAT*-Regel anwendet. Das Gerät vermittelt Datenpakete mit dieser Zieladresse an die in Spalte *Neue Adresse Ziel* festgelegte Zieladresse.

Mögliche Werte:

*any*

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

**Gültige IPv4-Adresse**

Das Gerät wendet die *Destination-NAT*-Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Zieladresse enthalten.

**Gültige IPv4-Adresse und Netzmaske in CIDR-Notation**

Das Gerät wendet die *Destination-NAT*-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 *Destination-NAT*-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 *Destination-NAT*-Regel anwendet.

**Mögliche Werte:**

*any* (Voreinstellung)

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

1.. 65535 (2<sup>16</sup> - 1)

Das Gerät wendet die *Destination-NAT*-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 21.
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel 21, 80, 110.
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel 2000- 3000.
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel 21, 2000-3000, 65535.

Die Spalte ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel 21, 2000- 3000, 65535 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:**

*any*

Das Gerät behält im Datenpaket den ursprünglichen Ziel-Port bei.

1.. 65535 (2<sup>16</sup> - 1)

Das Gerät ersetzt den Ziel-Port im Datenpaket durch diesen neuen Ziel-Port.

## Protokoll

Beschränkt die *Destination-NAT*-Regel auf ein IP-Protokoll. Das Gerät wendet die *Destination-NAT*-Regel ausschließlich auf Datenpakete des festgelegten IP-Protokolls an.

Mögliche Werte:

`i cnp`

Internet Control Message Protocol (RFC 792)

`i grp`

Internet Group Management Protocol

`i pi p`

IP in IP tunneling (RFC 1853)

`t cp`

Transmission Control Protocol (RFC 793)

`udp`

User Datagram Protocol (RFC 768)

`esp`

IPsec Encapsulated Security Payload (RFC 2406)

`ah`

IPsec Authentication Header (RFC 2402)

`i cnpv6`

Internet Control Message Protocol for IPv6

`any` (Voreinstellung)

Das Gerät wendet die *Destination-NAT*-Regel auf sämtliche Datenpakete an, ohne das IP-Protokoll zu bewerten.

## Log

Aktiviert/deaktiviert die Protokollierung in der System-Log-Datei, wenn das Gerät die in dieser Tabellenzeile festgelegte *Destination-NAT* Regel anwendet.

Mögliche Werte:

`markiert`

Die Protokollierung ist aktiv.

Das Gerät erstellt einen Eintrag in der System-Log-Datei, wenn das Gerät die in dieser Tabellenzeile festgelegte *Destination-NAT*-Regel anwendet. Siehe Dialog *Diagnose > Bericht > System-Log*.

`unmarkiert` (Voreinstellung)

Die Protokollierung ist inaktiv.

## Trap

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

Mögliche Werte:

`markiert`

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

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

`unmarkiert` (Voreinstellung)

Das Senden von SNMP-Traps ist inaktiv.

Aktiv

Aktiviert/deaktiviert die *Destination-NAT*-Regel.

Mögliche Werte:

**markiert**


Die Regel ist aktiv.

**unmarkiert** (Voreinstellung)

Die Regel ist inaktiv.

## 7.9.3.2 Destination-NAT Zuweisung

[ Routing > NAT > Destination-NAT > Zuweisung ]

In diesem Dialog weisen Sie die *Destination-NAT*-Regeln einem Router-Interface zu. Klicken Sie dazu die Schaltfläche .

Die *Destination-NAT*-Regeln fügen Sie im Dialog *Routing > NAT > Destination-NAT > Regel* hinzu und bearbeiten diese.

Eine Übersicht, welche *Destination-NAT*-Regel welchem Router-Interface zugewiesen ist, finden Sie im Dialog *Routing > NAT > Destination-NAT > Übersicht*.

### 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 *Zuweisen*. In diesem Fenster weisen Sie einer bestehenden *Destination-NAT*-Regel ein eingerichtetes Router-Interface zu.

#### Port

Zeigt die Nummer des Router-Interfaces, auf welches das Gerät die *Destination-NAT*-Regel anwendet.

#### Regel-Index

Zeigt die fortlaufende Nummer der *Destination-NAT*-Regel. Siehe Spalte *Index* im Dialog *Routing > NAT > Destination-NAT > Regel*. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

#### Regelname

Zeigt den Namen der *Destination-NAT*-Regel. Siehe Spalte *Regelname* im Dialog *Routing > NAT > Destination-NAT > Regel*.

### Richtung

Zeigt, ob das Gerät die *Destination-NAT*-Regel auf Datenpakete anwendet, die das Gerät sendet oder empfängt.

Mögliche Werte:

**kommand**

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

### Priorität

Legt die Priorität der *Destination-NAT*-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 **1** in aufsteigender Reihenfolge an.

Mögliche Werte:

**1..6500** (Voreinstellung: 1)

### Aktiv

Aktiviert/deaktiviert die *Destination-NAT*-Regel.

Mögliche Werte:

**markiert**

Die Regel ist aktiv.

**unmarkiert** (Voreinstellung)

Die Regel ist inaktiv.

### 7.9.3.3 Destination-NAT Übersicht

[ Routing > NAT > Destination-NAT > Übersicht ]

In diesem Dialog finden Sie eine Übersicht, welche *Destination-NAT*-Regel welchem Router-Interface zugewiesen ist.

Die *Destination-NAT*-Regeln fügen Sie im Dialog *Routing > NAT > Destination-NAT > Regel* hinzu und bearbeiten diese.

Ein Router-Interface weisen Sie der betreffenden *Destination-NAT*-Regel im Dialog *Routing > NAT > Destination-NAT > Zuweisung* zu.

#### 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 *Destination-NAT*-Regel anwendet.

Regel-Index

Zeigt die fortlaufende Nummer der *Destination-NAT*-Regel. Siehe Spalte *Index* im Dialog *Routing > NAT > Destination-NAT > Regel*.

Regelname

Zeigt den Namen der *Destination-NAT*-Regel. Siehe Spalte *Regelname* im Dialog *Routing > NAT > Destination-NAT > Regel*.

Ziel Adresse

Zeigt die Zieladresse der Datenpakete, auf die das Gerät die *Destination-NAT*-Regel anwendet. Das Gerät vermittelt Datenpakete mit dieser Zieladresse an die in Spalte *Neue Adresse Ziel* festgelegte Zieladresse.

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 *Destination-NAT*-Regel auf ein Datenpaket anwendet.

Mögliche Werte:

*markiert*

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

*unmarkiert*

Das Gerät sendet keinen SNMP-Trap.

## Log

Zeigt, ob das Gerät einen Eintrag in der System-Log-Datei erstellt, wenn das Gerät die *Destination-NAT*-Regel auf ein Datenpaket anwendet.

## Richtung

Zeigt, ob das Gerät die *Destination-NAT*-Regel auf Datenpakete anwendet, die das Gerät sendet oder empfängt.

Mögliche Werte:

*kommend*

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

## Priorität

Zeigt die Priorität der *Destination-NAT*-Regel.

Das Gerät wendet die Regeln beginnend mit Priorität 1 in aufsteigender Reihenfolge auf den Datenstrom an.

## 7.9.4 Masquerading-NAT

[Routing > NAT > Masquerading-NAT]

Die Funktion *Masquerading-NAT* versteckt beliebig viele Endgeräte hinter der IP-Adresse des *NAT*-Routers und verbirgt somit die Struktur eines Netzes vor anderen Netzen. Dazu ersetzt der *NAT*-Router im Datenpaket die Absenderadresse durch seine eigene IP-Adresse. Zusätzlich ersetzt der *NAT*-Router im Datenpaket den Quell-Port durch einen eigenen Wert, um die Antwort-Datenpakete später wieder an den ursprünglichen Absender zu vermitteln.

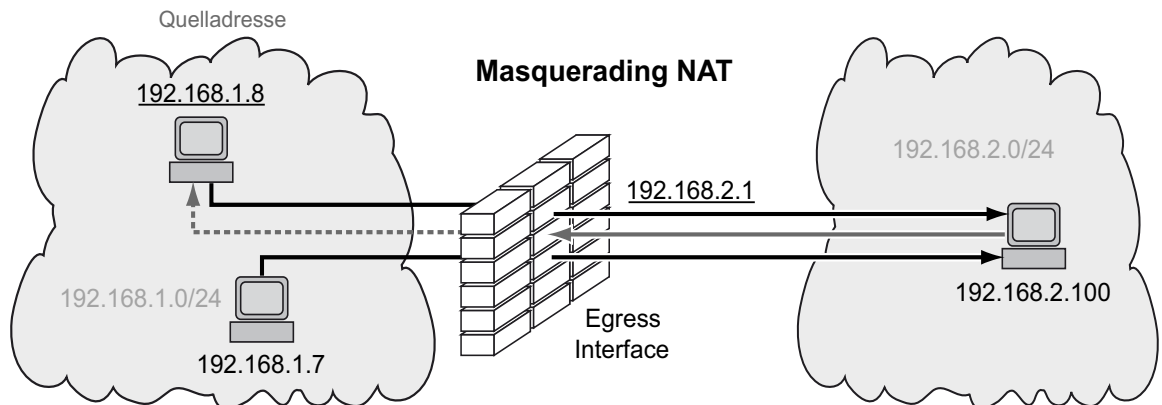


Abb. 7: Funktionsprinzip der Funktion *Masquerading-NAT*

Um die Funktion *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 *VRRP* einschalten, dann ist auf diesem Router-Interface die Funktion *Masquerading-NAT* unwirksam.

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

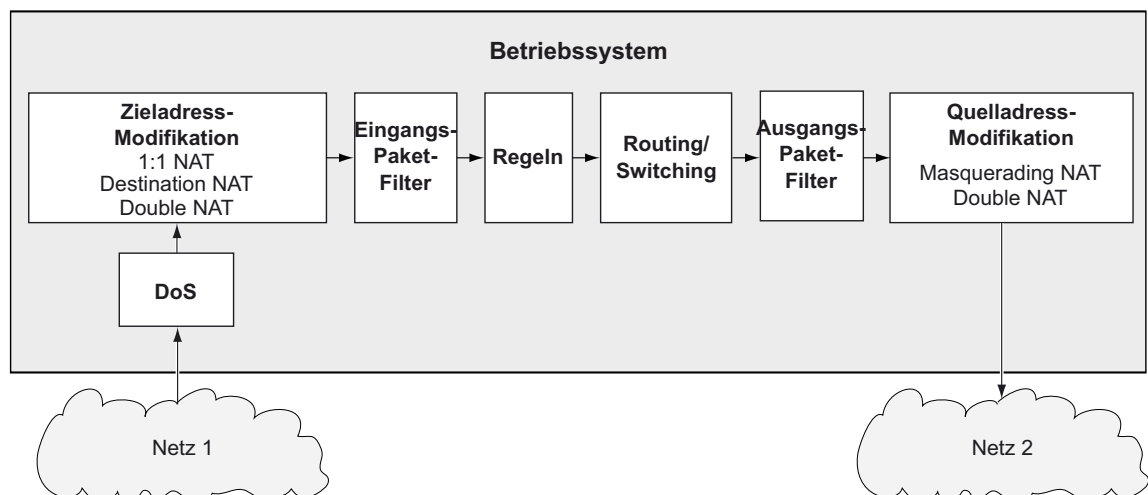


Abb. 8: Bearbeitungsreihenfolge der Datenpakete im Gerät

Das Menü enthält die folgenden Dialoge:

- [Masquerading-NAT Regel](#)
- [Masquerading-NAT Zuweisung](#)
- [Masquerading-NAT Übersicht](#)

## 7.9.4.1 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 *Routing > NAT > Masquerading-NAT > Zuweisung* zu.

Eine Übersicht, welche *Masquerading-NAT*-Regel welchem Router-Interface zugewiesen ist, finden Sie im Dialog *Routing > NAT > 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:

[any](#)

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

**Gültige IPv4-Adresse**

Das Gerät wendet die *Masquerading-NAT*-Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.

**Gültige IPv4-Adresse und Netzmaske in CIDR-Notation**

Das Gerät wendet die *Masquerading-NAT*-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 *Masquerading-NAT*-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 *Masquerading-NAT*-Regel anwendet.

**Mögliche Werte:**

**any** (Voreinstellung)

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

**1..65535** (2<sup>16</sup> - 1)

Das Gerät wendet die *Masquerading-NAT*-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 **21**.
- Mit durch Komma getrennten Zahlenwerten legen Sie mehrere einzelne Ports fest, zum Beispiel **21, 80, 110**.
- Mit durch Bindestrich verbundenen Zahlenwerten legen Sie einen Port-Bereich fest, zum Beispiel **2000-3000**.
- Außerdem können Sie Ports und Port-Bereiche kombinieren, zum Beispiel **21, 2000-3000, 65535**.

Die Spalte ermöglicht Ihnen, bis zu 15 Zahlenwerte festzulegen. Wenn Sie zum Beispiel **21, 2000-3000, 65535** eingeben, verwenden Sie 4 von 15 Zahlenwerten.

## Protokoll

Beschränkt die *Masquerading-NAT*-Regel auf ein IP-Protokoll. Das Gerät wendet die *Masquerading-NAT*-Regel ausschließlich auf Datenpakete des festgelegten IP-Protokolls an.

**Mögliche Werte:**

**tcp**

Transmission Control Protocol (RFC 793)

**udp**

User Datagram Protocol (RFC 768)

**any** (Voreinstellung)

Das Gerät wendet die *Masquerading-NAT*-Regel auf sämtliche Datenpakete an, ohne das IP-Protokoll zu bewerten.

## Log

Aktiviert/deaktiviert die Protokollierung in der System-Log-Datei, wenn das Gerät die in dieser Tabellenzeile festgelegte *Masquerading-NAT* Regel anwendet.

Mögliche Werte:

`markiert`

Die Protokollierung ist aktiv.

Das Gerät erstellt einen Eintrag in der System-Log-Datei, wenn das Gerät die in dieser Tabellenzeile festgelegte *Masquerading-NAT*-Regel anwendet. Siehe Dialog [Diagnose > Bericht > System-Log](#).

`unmarkiert` (Voreinstellung)

Die Protokollierung ist inaktiv.

## Trap

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

Mögliche Werte:

`markiert`

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

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

`unmarkiert` (Voreinstellung)

Das Senden von SNMP-Traps ist inaktiv.

## IPsec exempt

Aktiviert/deaktiviert das Anwenden der *Masquerading-NAT*-Regel auf IPsec-Datenpakete.

Mögliche Werte:

`markiert`

Das Gerät wendet die *Masquerading-NAT*-Regel auf IPsec-Datenpakete nicht an. Das Gerät sendet IPsec-Datenpakete unmodifiziert durch den VPN-Tunnel.

`unmarkiert` (Voreinstellung)

Das Gerät wendet die *Masquerading-NAT*-Regel auf IPsec-Datenpakete an. Abhängig von den Einstellungen des Traffic-Selectors in den Spalten *Quelle Adresse (CIDR)* und *Quelle Einschränkungen* sendet das Gerät IPsec-Datenpakete durch den VPN-Tunnel. Siehe Dialog [Virtual Private Network > Verbindungen](#).

## Aktiv

Aktiviert/deaktiviert die *Masquerading-NAT*-Regel.

Mögliche Werte:

`markiert`


Die Regel ist aktiv.

`unmarkiert` (Voreinstellung)

Die Regel ist inaktiv.

## 7.9.4.2 Masquerading-NAT Zuweisung

[Routing > NAT > Masquerading-NAT > Zuweisung]

In diesem Dialog weisen Sie die *Masquerading-NAT*-Regeln einem Router-Interface zu. Klicken Sie dazu die Schaltfläche .

Die *Masquerading-NAT*-Regeln fügen Sie im Dialog *Routing > NAT > Masquerading-NAT > Regel* hinzu und bearbeiten diese.

Eine Übersicht, welche *Masquerading-NAT*-Regel welchem Router-Interface zugewiesen ist, finden Sie im Dialog *Routing > NAT > Masquerading-NAT > Übersicht*.

### 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 *Zuweisen*. In diesem Fenster weisen Sie einer bestehenden *Masquerading-NAT*-Regel ein eingerichtetes Router-Interface zu.

#### Port

Zeigt die Nummer des Router-Interfaces, auf welches das Gerät die *Masquerading-NAT*-Regel anwendet.

#### Regel-Index

Zeigt die fortlaufende Nummer der *Masquerading-NAT*-Regel. Siehe Spalte *Index* im Dialog *Routing > NAT > Masquerading-NAT > Regel*. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

#### Regelname

Zeigt den Namen der *Masquerading-NAT*-Regel. Siehe Spalte *Regelname* im Dialog *Routing > NAT > Masquerading-NAT > Regel*.

#### Richtung

Zeigt, ob das Gerät die *Masquerading-NAT*-Regel auf Datenpakete anwendet, die das Gerät sendet oder empfängt.

Mögliche Werte:

*gehend*

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

#### Priorität

Legt die Priorität der *Masquerading-NAT*-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 **1** in aufsteigender Reihenfolge an.

Mögliche Werte:

*1.. 6500* (Voreinstellung: **1**)

#### Aktiv

Aktiviert/deaktiviert die *Masquerading-NAT*-Regel.

Mögliche Werte:

*markiert*

Die Regel ist aktiv.

*unmarkiert* (Voreinstellung)

Die Regel ist inaktiv.

### 7.9.4.3 Masquerading-NAT Übersicht

[Routing > NAT > Masquerading-NAT > Übersicht]

In diesem Dialog finden Sie eine Übersicht, welche *Masquerading-NAT*-Regel welchem Router-Interface zugewiesen ist.

Die *Masquerading-NAT*-Regeln fügen Sie im Dialog *Routing > NAT > Masquerading-NAT > Regel* hinzu und bearbeiten diese.

Ein Router-Interface weisen Sie der betreffenden *Masquerading-NAT*-Regel im Dialog *Routing > NAT > Masquerading-NAT > Zuweisung* zu.

#### 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 *Masquerading-NAT*-Regel anwendet.

Regel-Index

Zeigt die fortlaufende Nummer der *Masquerading-NAT*-Regel. Siehe Spalte *Index* im Dialog *Routing > NAT > Masquerading-NAT > Regel*.

Regelname

Zeigt den Namen der *Masquerading-NAT*-Regel. Siehe Spalte *Regelname* im Dialog *Routing > NAT > Masquerading-NAT > Regel*.

Trap

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

Mögliche Werte:

`narkiert`

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

`unnarkiert`

Das Gerät sendet keinen SNMP-Trap.

Log

Zeigt, ob das Gerät einen Eintrag in der System-Log-Datei erstellt, wenn das Gerät die *Masquerading-NAT*-Regel auf ein Datenpaket anwendet.

Richtung

Zeigt, ob das Gerät die *Masquerading-NAT*-Regel auf Datenpakete anwendet, die das Gerät sendet oder empfängt.

Mögliche Werte:

*gehend*

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

Priorität

Zeigt die Priorität der *Masquerading-NAT*-Regel.

Das Gerät wendet die Regeln beginnend mit Priorität 1 in aufsteigender Reihenfolge auf den Datenstrom an.

## 7.9.5 Double-NAT

[Routing > NAT > Double-NAT]

Die Funktion *Double-NAT* ermöglicht Ihnen, Kommunikationsverbindungen zwischen Endgeräten in unterschiedlichen IP-Netzen aufzubauen, die keine Möglichkeit bieten, ein *Standard-Gateway* oder eine *Standard-Route* festzulegen. Der *NAT*-Router „verschiebt“ die Endgeräte virtuell in das jeweils andere Netz. Dazu ersetzt der *NAT*-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 *Double-NAT* ist, dass der *NAT*-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.

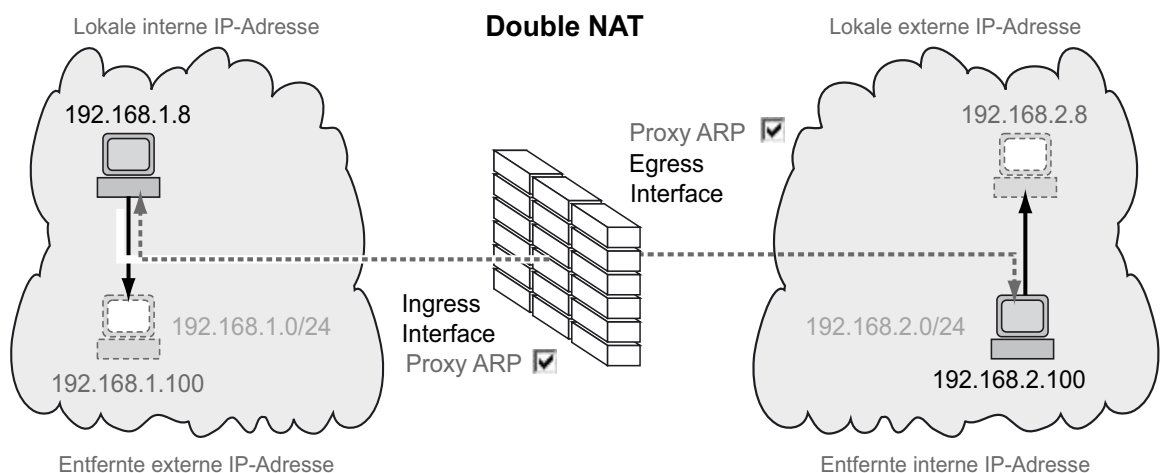


Abb. 9: Funktionsprinzip der Funktion *Double-NAT*

Um die Funktion *NAT* 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:

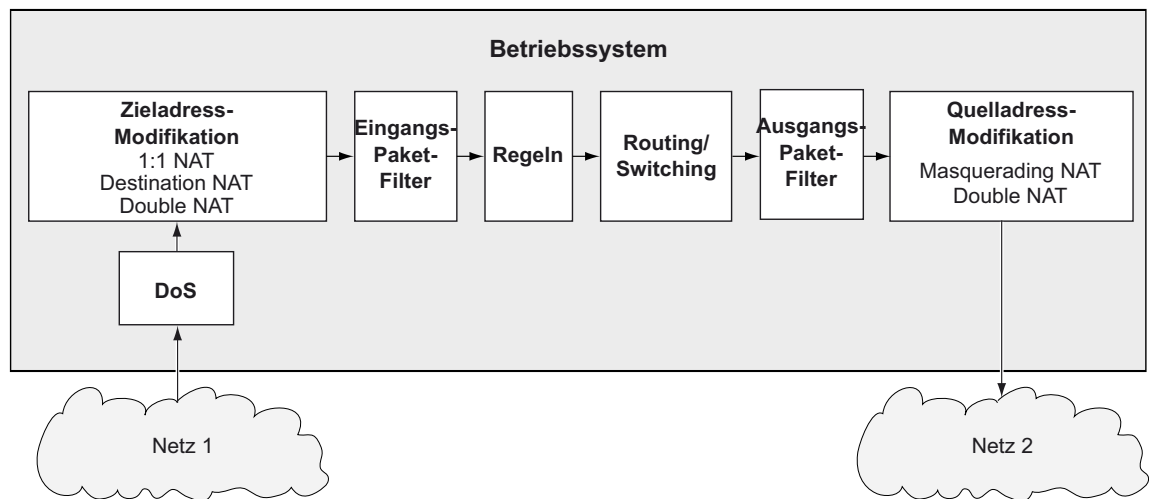


Abb. 10: Bearbeitungsreihenfolge der Datenpakete im Gerät

Das Menü enthält die folgenden Dialoge:

- [Double-NAT Regel](#)
- [Double-NAT Zuweisung](#)
- [Double-NAT Übersicht](#)

## 7.9.5.1 Double-NAT Regel

[Routing > NAT > Double-NAT > Regel]

In diesem Dialog richten Sie die *Double-NAT*-Regeln ein.

Die Router-Interface weisen Sie der betreffenden *Double-NAT*-Regel im Dialog *Routing > NAT > Double-NAT > Zuweisung* zu.

Eine Übersicht, welche *Double-NAT*-Regel welchen Router-Interfaces zugewiesen ist, finden Sie im Dialog *Routing > NAT > Double-NAT > Übersicht*.

Das Gerät ermöglicht, bis zu 255 *Double-NAT*-Regeln einzurichten.

### Tabelle

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

Schaltflächen



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

- Im Feld *Lokale interne IP-Adresse* legen Sie für das im ersten Netz platzierte Endgerät die tatsächliche IP-Adresse fest.  
Mögliche Werte:  
Gültige IPv4-Adresse  
Das Gerät wendet die *Double-NAT*-Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.
- Im Feld *Lokale externe IP-Adresse* 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 *Double-NAT*-Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.

- Im Feld *Ferne interne IP-Adresse* legen Sie für das im zweiten Netz platzierte Endgerät die tatsächliche IP-Adresse fest.  
Mögliche Werte:  
Gültige IPv4-Adresse  
Das Gerät wendet die *Double-NAT*-Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.
- Im Feld *Ferne externe IP-Adresse* 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 *Double-NAT*-Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.  
Nach Klicken der Schaltfläche *Ok* fügt das Gerät die Tabellenzeile hinzu. Das Gerät weist dieser Tabellenzeile die in den Feldern *Lokale interne IP-Adresse*, *Lokale externe IP-Adresse*, *Ferne interne IP-Adresse* und *Ferne externe IP-Adresse* 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 *Double-NAT*-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 *Double-NAT*-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 *Double-NAT*-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 *Double-NAT*-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 *Double-NAT*-Regel ausschließlich auf Datenpakete an, welche die hier festgelegte Quelladresse enthalten.

#### Log

Aktiviert/deaktiviert die Protokollierung in der System-Log-Datei, wenn das Gerät die in dieser Tabellenzeile festgelegte *Double-NAT* Regel anwendet.

##### Mögliche Werte:

*markiert*

Die Protokollierung ist aktiv.

Das Gerät erstellt einen Eintrag in der System-Log-Datei, wenn das Gerät die in dieser Tabellenzeile festgelegte *Double-NAT*-Regel anwendet. Siehe Dialog *Diagnose > Bericht > System-Log*.

*unmarkiert* (Voreinstellung)

Die Protokollierung ist inaktiv.

#### Trap

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

##### Mögliche Werte:

*markiert*

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

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

*unmarkiert* (Voreinstellung)

Das Senden von SNMP-Traps ist inaktiv.

#### Aktiv

Aktiviert/deaktiviert die *Double-NAT*-Regel.

##### Mögliche Werte:

*markiert*


Die Regel ist aktiv.

*unmarkiert* (Voreinstellung)

Die Regel ist inaktiv.

## 7.9.5.2 Double-NAT Zuweisung

[Routing > NAT > Double-NAT > Zuweisung]

In diesem Dialog weisen Sie die *Double-NAT*-Regeln einem Router-Interface zu. Klicken Sie dazu die Schaltfläche .

Die *Double-NAT*-Regeln fügen Sie im Dialog *Routing > NAT > Double-NAT > Regel* hinzu und bearbeiten diese.

Eine Übersicht, welche *Double-NAT*-Regel welchen Router-Interfaces zugewiesen ist, finden Sie im Dialog *Routing > NAT > Double-NAT > Übersicht*.

### 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 *Zuweisen*. In diesem Fenster weisen Sie einer bestehenden *Double-NAT*-Regel ein eingerichtetes Router-Interface zu.

#### Port

Zeigt die Nummer des Router-Interfaces, auf welches das Gerät die *Double-NAT*-Regel anwendet.

#### Regel-Index

Zeigt die fortlaufende Nummer der *Double-NAT*-Regel. Siehe Spalte *Index* im Dialog *Routing > NAT > Double-NAT > Regel*. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

#### Regelname

Zeigt den Namen der *Double-NAT*-Regel. Siehe Spalte *Regelname* im Dialog *Routing > NAT > Double-NAT > Regel*.

#### Richtung

Zeigt, ob das Gerät die *Double-NAT*-Regel auf Datenpakete anwendet, die das Gerät sendet oder empfängt.

Mögliche Werte:

*kommand*


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

gehend

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

bei de

Das Gerät wendet die *Double-NAT*-Regel auf Datenpakete an, die es auf dem Router-Interface empfängt oder sendet.

Sie können den Wert ändern, wenn Sie die Schaltfläche  klicken.

Priorität

Legt die Priorität der *Double-NAT*-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 1 in aufsteigender Reihenfolge an.

Mögliche Werte:

1.. 6500 (Voreinstellung: 1)

Aktiv

Aktiviert/deaktiviert die *Double-NAT*-Regel.

Mögliche Werte:

markiert

Die Regel ist aktiv.

unmarkiert (Voreinstellung)

Die Regel ist inaktiv.

### 7.9.5.3 Double-NAT Übersicht

[Routing > NAT > Double-NAT > Übersicht]

In diesem Dialog finden Sie eine Übersicht, welche *Double-NAT*-Regel welchem Router-Interface zugewiesen ist.

Die *Double-NAT*-Regeln fügen Sie im Dialog *Routing > NAT > Double-NAT > Regel* hinzu und bearbeiten diese.

Die Router-Interface weisen Sie der betreffenden *Double-NAT*-Regel im Dialog *Routing > NAT > Double-NAT > Zuweisung* zu.

#### 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 *Double-NAT*-Regel anwendet.

Regel-Index

Zeigt die fortlaufende Nummer der *Double-NAT*-Regel. Siehe Spalte *Index* im Dialog *Routing > NAT > Double-NAT > Regel*.

Regelname

Zeigt den Namen der *Double-NAT*-Regel. Siehe Spalte *Regelname* im Dialog *Routing > NAT > Double-NAT > Regel*.

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 *Double-NAT*-Regel auf ein Datenpaket anwendet.

Mögliche Werte:

*markiert*

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

*unmarkiert*

Das Gerät sendet keinen SNMP-Trap.

## Log

Zeigt, ob das Gerät einen Eintrag in der System-Log-Datei erstellt, wenn das Gerät die *Double-NAT*-Regel auf ein Datenpaket anwendet.

## Richtung

Zeigt, ob das Gerät die *Double-NAT*-Regel auf Datenpakete anwendet, die das Gerät sendet oder empfängt.

Mögliche Werte:

*kommend*

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

*gehend*

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

*beide*

Das Gerät wendet die *Double-NAT*-Regel auf Datenpakete an, die es auf dem Router-Interface empfängt oder sendet.

## Priorität

Zeigt die Priorität der *Double-NAT*-Regel.

Das Gerät wendet die Regeln beginnend mit Priorität **1** in aufsteigender Reihenfolge auf den Datenstrom an.



## 8 Diagnose

Das Menü enthält die folgenden Dialoge:

- [Statuskonfiguration](#)
- [System](#)
- [Syslog](#)
- [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 `error` oder `ok` im Rahmen *Geräte-Status*. Das Gerät bestimmt diesen Status anhand der einzelnen Überwachungsergebnisse.

Das Gerät zeigt ermittelte Fehler in der Registerkarte *Status* und zusätzlich im Dialog *Grundeinstellungen > System*, Rahmen *Geräte-Status*.

Der Dialog enthält die folgenden Registerkarten:

- [\[Global\]](#)
- [\[Port\]](#)
- [\[Status\]](#)

### [Global]

#### Geräte-Status

##### Geräte-Status

Zeigt den gegenwärtigen Status des Geräts. Das Gerät bestimmt den Status aus den einzelnen überwachten Parametern.

Mögliche Werte:

`ok`

`error`

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

## Traps

### Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung an einer überwachten Funktion erkennt.

Mögliche Werte:

**markiert** (Voreinstellung)

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

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

**unmarkiert**

Das Senden von SNMP-Traps ist inaktiv.

## Tabelle

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

### Verbindungsfehler

Aktiviert/deaktiviert die Überwachung des Linkstatus auf dem Port/Interface.

Mögliche Werte:

**markiert**

Die Überwachung ist aktiv.

Der Wert im Rahmen [Geräte-Status](#) wechselt auf **error**, wenn der Link auf einem überwachten Port/Interface abbricht.

In der Registerkarte [Port](#) haben Sie die Möglichkeit, die zu überwachenden Ports/Interfaces einzeln auszuwählen.

**unmarkiert** (Voreinstellung)

Die Überwachung ist inaktiv.

### Temperatur

Aktiviert/deaktiviert die Überwachung der Temperatur im Gerät.

Mögliche Werte:

**markiert** (Voreinstellung)

Die Überwachung ist aktiv.

Wenn die Temperatur den festgelegten oberen Schwellenwert überschreitet oder den festgelegten unteren Schwellenwert unterschreitet, wechselt der Wert im Rahmen [Geräte-Status](#) auf **error**.

**unmarkiert**

Die Überwachung ist inaktiv.

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

Externer Speicher wurde entfernt

Aktiviert/deaktiviert die Überwachung des aktiven externen Speichers (ENM).

Mögliche Werte:

**markiert**

Die Überwachung ist aktiv.

Der Wert im Rahmen *Geräte-Status* wechselt auf *error*, wenn Sie den aktiven externen Speicher (ENM) aus dem Gerät entfernen.

**unmarkiert** (Voreinstellung)

Die Überwachung ist inaktiv.

Den aktiven externen Speicher legen Sie fest im Dialog *Grundeinstellungen > Laden/Speichern*, Rahmen *Externer Speicher*.

Externer Speicher und NVM nicht synchron

Aktiviert/deaktiviert die Überwachung der Konfigurationsprofile im Gerät und im externen Speicher (ENM).

Mögliche Werte:

**markiert**

Die Überwachung ist aktiv.

In folgenden Situationen wechselt der Wert im Rahmen *Geräte-Status* auf *error*:

- Das Konfigurationsprofil existiert ausschließlich im Gerät.
- Das Konfigurationsprofil im Gerät unterscheidet sich vom Konfigurationsprofil im externen Speicher (ENM).

**unmarkiert** (Voreinstellung)

Die Überwachung ist inaktiv.

Netzteil 1

Netzteil 2

Aktiviert/deaktiviert die Überwachung des Netzteils.

Mögliche Werte:

**markiert** (Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen *Geräte-Status* wechselt auf *error*, wenn das Gerät einen Fehler am Netzteil feststellt.

**unmarkiert**

Die Überwachung ist inaktiv.

## [Port]

### Tabelle

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

Port

Zeigt die Nummer des Ports.

Verbindungsfehler melden

Aktiviert/deaktiviert die Überwachung des Links auf dem Port/Interface.

Mögliche Werte:

**markiert**

Die Überwachung ist aktiv.

Der Wert im Rahmen *Geräte-Status* wechselt auf **error**, wenn der Link auf dem ausgewählten Port/Interface abbricht.

**unmarkiert** (Voreinstellung)

Die Überwachung ist inaktiv.

Die Einstellung ist wirksam, wenn Sie in der Registerkarte *Global* das Kontrollkästchen *Verbindungsfehler* markieren.

## [Status]

### Tabelle

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

Zeitstempel

Zeigt Datum und Uhrzeit des Ereignisses.

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 `error` oder `ok` im Rahmen *Sicherheits-Status*. Das Gerät bestimmt diesen Status anhand der einzelnen Überwachungsergebnisse.

Das Gerät zeigt ermittelte Fehler in der Registerkarte *Status* und zusätzlich im Dialog *Grundeinstellungen > System*, Rahmen *Sicherheits-Status*.

Der Dialog enthält die folgenden Registerkarten:

- [Global]
- [Port]
- [Status]

### [Global]

#### Sicherheits-Status

Sicherheits-Status

Zeigt den gegenwärtigen Status der sicherheitsrelevanten Einstellungen im Gerät. Das Gerät bestimmt den Status aus den einzelnen überwachten Parametern.

Mögliche Werte:

`ok`

`error`

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

#### Traps

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung an einer überwachten Funktion erkennt.

Mögliche Werte:

`markiert`

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

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

`unmarkiert` (Voreinstellung)

Das Senden von SNMP-Traps ist inaktiv.

## Tabelle

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

### Passwort-Voreinstellung unverändert

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

Mögliche Werte:

**markiert** (Voreinstellung)

Die Überwachung ist aktiv.

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

**unmarkiert**

Die Überwachung ist inaktiv.

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

### Min. Passwort-Länge kürzer als 8

Aktiviert/deaktiviert die Überwachung der Richtlinie *Min. Passwort-Länge*.

Mögliche Werte:

**markiert** (Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen *Sicherheits-Status* wechselt auf **error**, wenn für die Richtlinie *Min. Passwort-Länge* ein Wert kleiner als 8 festgelegt ist.

**unmarkiert**

Die Überwachung ist inaktiv.

Die Richtlinie für die *Min. Passwort-Länge* legen Sie fest im Dialog *Gerätesicherheit > Benutzerverwaltung*, Rahmen *Konfiguration*.

### Passwort-Richtlinien deaktiviert

Aktiviert/deaktiviert die Überwachung der Passwort-Richtlinien-Einstellungen.

Mögliche Werte:

**markiert** (Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen *Sicherheits-Status* wechselt auf **error**, wenn für mindestens eine der folgenden Richtlinien ein Wert kleiner als 1 festgelegt ist.

– *Großbuchstaben (min.)*

– *Kleinbuchstaben (min.)*

– *Ziffern (min.)*

– *Sonderzeichen (min.)*

**unmarkiert**

Die Überwachung ist inaktiv.

Die Einstellungen für die Richtlinie legen Sie fest im Dialog *Gerätesicherheit > Benutzerverwaltung*, Rahmen *Passwort-Richtlinien*.

## Prüfen der Passwort-Richtlinien im Benutzerkonto deaktiviert

Aktiviert/deaktiviert die Überwachung der Funktion *Richtlinien überprüfen*.

Mögliche Werte:

*markiert*

Die Überwachung ist aktiv.

Der Wert im Rahmen *Sicherheits-Status* wechselt auf *error*, wenn die Funktion *Richtlinien überprüfen* bei mindestens ein Benutzerkonto inaktiv ist.

*unmarkiert* (Voreinstellung)

Die Überwachung ist inaktiv.

Die Funktion *Richtlinien überprüfen* aktivieren Sie im Dialog *Gerätesicherheit > Benutzerverwaltung*.

## HTTP-Server aktiv

Aktiviert/deaktiviert die Überwachung des HTTP-Servers.

Mögliche Werte:

*markiert* (Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen *Sicherheits-Status* wechselt auf *error*, wenn Sie den HTTP-Server einschalten.

*unmarkiert*

Die Überwachung ist inaktiv.

Den HTTP-Server schalten Sie ein/aus im Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *HTTP*.

## SNMP unverschlüsselt

Aktiviert/deaktiviert die Überwachung des SNMP-Servers.

Mögliche Werte:

*markiert* (Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen *Sicherheits-Status* wechselt auf *error*, wenn mindestens eine der folgenden Bedingungen zutrifft:

- Die Funktion *SNMPv1* ist eingeschaltet.
- Die Funktion *SNMPv2* ist eingeschaltet.
- Die Verschlüsselung für *SNMPv3* ist ausgeschaltet.

Die Verschlüsselung schalten Sie ein im Dialog *Gerätesicherheit > Benutzerverwaltung*, Spalte *SNMP-Verschlüsselung*.

*unmarkiert*

Die Überwachung ist inaktiv.

Die Einstellungen für den SNMP-Agenten legen Sie fest im Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SNMP*.

## Zugriff auf System Monitor 1 über die serielle Schnittstelle möglich

Aktiviert/deaktiviert die Überwachung der Option zum Starten des System Monitors 1.

Wenn aktiv, können Sie den System Monitor 1 über die serielle Verbindung beim Systemstart starten.

Mögliche Werte:

[markiert](#)

Die Überwachung ist aktiv.

Der Wert im Rahmen *Sicherheits-Status* wechselt auf [error](#), wenn Sie die Option zum Starten des System Monitors 1 aktivieren.

[unmarkiert](#) (Voreinstellung)

Die Überwachung ist inaktiv.

Der Wert im Rahmen *Sicherheits-Status* bleibt unverändert, wenn Sie die Option zum Starten des System Monitors 1 aktivieren.

Sie aktivieren/deaktivieren die Option zum Starten des System Monitors 1 im Dialog [Diagnose > System > Selbsttest](#).

Speichern des Konfigurationsprofils auf dem externen Speicher möglich

Aktiviert/deaktiviert die Überwachung des Konfigurationsprofils im externen Speicher ([ENMM](#)).

Mögliche Werte:

[markiert](#)

Die Überwachung ist aktiv.

Der Wert im Rahmen *Sicherheits-Status* wechselt auf [error](#), wenn das Speichern des Konfigurationsprofils auf dem externen Speicher ([ENMM](#)) aktiv ist.

[unmarkiert](#) (Voreinstellung)

Die Überwachung ist inaktiv.

Das Speichern des Konfigurationsprofils im externen Speicher ([Grundeinstellungen > Externer Speicher](#)) aktivieren/deaktivieren Sie im Dialog [ENMM](#)

Verbindungsabbruch auf eingeschalteten Ports

Aktiviert/deaktiviert die Überwachung des Links auf den aktiven Ports.

Mögliche Werte:

[markiert](#)

Die Überwachung ist aktiv.

Der Wert im Rahmen *Sicherheits-Status* wechselt auf [error](#), wenn der Link auf einem aktiven Port abbricht. In der Registerkarte *Port* haben Sie die Möglichkeit, die zu überwachenden Ports einzeln auszuwählen.

[unmarkiert](#) (Voreinstellung)

Die Überwachung ist inaktiv.

Zugriff mit HiDiscovery möglich

Aktiviert/deaktiviert die Überwachung der Funktion HiDiscovery.

Mögliche Werte:

[markiert](#) (Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen *Sicherheits-Status* wechselt auf [error](#), wenn Sie die Funktion HiDiscovery einschalten.

[unmarkiert](#)

Die Überwachung ist inaktiv.

Die Funktion HiDiscovery schalten Sie im Dialog [Grundeinstellungen > Netzwerk > Global](#) ein/aus.

#### Unverschlüsselte Konfiguration vom externen Speicher laden

Aktiviert/deaktiviert die Überwachung des Ladens unverschlüsselter Konfigurationsprofile vom externen Speicher (EMM).

Mögliche Werte:

**markiert** (Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen *Sicherheits-Status* wechselt auf **error**, wenn die Einstellungen dem Gerät ermöglichen, ein unverschlüsseltes Konfigurationsprofil vom externen Speicher (EMM) zu laden. Der Rahmen *Sicherheits-Status* im Dialog *Grundeinstellungen > System* zeigt einen Alarm, wenn folgende Voraussetzungen erfüllt sind:

- Das im externen Speicher (EMM) gespeicherte Konfigurationsprofil ist unverschlüsselt. und
- Die Spalte *Konfigurations-Priorität* im Dialog *Grundeinstellungen > Externer Speicher* hat den Wert **erste** oder **zweite**.

**unmarkiert**

Die Überwachung ist inaktiv.

#### Self-signed HTTPS-Zertifikat vorhanden

Aktiviert/deaktiviert die Überwachung des digitalen Zertifikats des HTTP-Servers.

Mögliche Werte:

**markiert** (Voreinstellung)

Die Überwachung ist aktiv.

Der Wert im Rahmen *Sicherheits-Status* wechselt auf **error**, wenn der HTTPS-Server ein selbst generiertes digitales Zertifikat verwendet.

**unmarkiert**

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:

**markiert**

Die Überwachung ist aktiv.

Der Wert im Rahmen *Sicherheits-Status* wechselt auf **error**, wenn der Port eingeschaltet ist (Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*, Kontrollkästchen *Port an* ist **markiert**) und wenn der Link auf dem Port abbricht.

**unmarkiert** (Voreinstellung)

Die Überwachung ist inaktiv.

Diese Einstellung ist wirksam, wenn Sie im Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus*, Registerkarte *Global*, das Kontrollkästchen *Verbindungsabbruch auf eingeschalteten Ports* markieren.

### [Status]

#### Tabelle

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

#### Zeitstempel

Zeigt Datum und Uhrzeit des Ereignisses.

#### 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:

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

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:

**An** (Voreinstellung)

Das Senden von SNMP-Traps ist eingeschaltet.

**Aus**

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

**trap** (Voreinstellung)

## Tabelle

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

### Schaltflächen



Hinzufügen

Öffnet das Fenster *Erstellen*, um eine Tabellenzeile hinzuzufügen. Damit richten Sie ein Trap-Ziel im Gerät ein.

- Im Feld *Name* legen Sie einen Namen für das Trap-Ziel fest.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

- Im Feld *Adresse* legen Sie IP-Adresse und Port des Trap-Ziels fest.

Mögliche Werte:

<I Pv4- Adresse>: <Port >

Wenn Sie keinen Port festlegen, fügt das Gerät automatisch den Port 162 dem Trap-Ziel hinzu.



Löschen

Entfernt die ausgewählte Tabellenzeile.

### Name

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

### Adresse

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

Mögliche Werte:

<I Pv4- Adresse>: <Port >

Wenn Sie keinen Port festlegen, fügt das Gerät automatisch den Port 162 dem Trap-Ziel hinzu.

### Aktiv

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

Mögliche Werte:

**markiert** (Voreinstellung)

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

**unmarkiert**

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

## 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

Speichert die HTML-Seite auf Ihrem PC mittels Webbrowser-Dialog.

## 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 **ERROR** das Gerät beim Konfigurations-Check erkannt hat.



Warnung

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

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




Information

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

## Tabelle

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



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

ID

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

Level

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

Das Gerät unterscheidet die folgenden Zustände:

- **Information**  
Die Leistungsfähigkeit der Kommunikation zwischen den beiden Geräten ist nicht beeinträchtigt.
- **Warnung**  
Die Leistungsfähigkeit der Kommunikation zwischen den beiden Geräten kann beeinträchtigt sein.
- **Fehler**  
Die Kommunikation zwischen den beiden Geräten ist beeinträchtigt.

Nachricht

Zeigt eine Zusammenfassung der erkannten Abweichungen.

## 8.23 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

Löscht die dynamisch eingerichteten Adressen aus der ARP-Tabelle.

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:

**statisch**

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

**dynamisch**

Dynamischer Eintrag. Das Gerät löscht den dynamischen Eintrag nach Überschreiten der *Aging-Time [s]*, falls das Gerät während dieser Zeit keine Daten von diesem Gerät empfängt.

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:

- Aktiviert/deaktiviert die Option zum Starten des System Monitors 1 während des Systemstarts.
- Festlegen, wie sich das Gerät im verhält, wenn es einen Fehler erkennt.

### Konfiguration

Die folgenden Einstellungen sperrern Ihnen dauerhaft den Zugang zum Gerät, wenn das Gerät beim Neustart kein lesbares Konfigurationsprofil findet.

- Kontrollkästchen *SysMon1 ist verfügbar* ist *unmarkiert*.
- Kontrollkästchen *Bei Fehler Default-Konfiguration laden* ist *unmarkiert*.

Dies ist zum Beispiel dann der Fall, wenn sich das Passwort des zu ladenden Konfigurationsprofils von dem im Gerät festgelegten Passwort unterscheidet. Um das Gerät wieder entsperren zu lassen, wenden Sie sich an Ihren Vertriebspartner.

#### SysMon1 ist verfügbar

Aktiviert/deaktiviert die Option zum Starten des System Monitors 1 während des Systemstarts.

Mögliche Werte:

*markiert* (Voreinstellung)

Während des Systemstarts zeigt das Startmenü den Eintrag System Monitor 1.

Um den System Monitor 1 tatsächlich zu starten, wählen Sie diesen Eintrag während des Systemstarts.

*unmarkiert*

Während des Systemstarts zeigt das Startmenü keinen Eintrag System Monitor 1.

Niemand kann den System Monitor 1 starten.

Der System Monitor 1 bietet Funktionen zur Wiederherstellung der Einstellungen des Geräts.

#### Bei Fehler Default-Konfiguration laden

Aktiviert/deaktiviert das Laden der Werkseinstellungen, falls das Gerät beim Neustart kein lesbares Konfigurationsprofil findet.

Mögliche Werte:

*markiert* (Voreinstellung)

Das Gerät lädt die Werkseinstellungen.

*unmarkiert*

Das Gerät bricht den Neustart ab und hält an. Der Zugriff auf das Management des Geräts ist ausschließlich mittels Command Line Interface über die serielle Verbindung möglich.

Um das Gerät wieder über das Netz erreichbar zu machen, starten Sie den System Monitor 1 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:

#### task

Das Gerät erkennt Fehler in ausgeführten Anwendungen, zum Beispiel wenn eine Task abbricht oder nicht verfügbar ist.

#### resource

Das Gerät erkennt Fehler in den verfügbaren Ressourcen, zum Beispiel bei knapp werdendem Speicher.

#### software

Das Gerät erkennt Software-Fehler, zum Beispiel Fehler beim Konsistenz-Check.

#### hardware

Das Gerät erkennt Hardware-Fehler, zum Beispiel im Chipsatz.

### Aktion

Legt das Verhalten des Geräts fest, wenn das nebenstehende Ereignis eintritt.

Mögliche Werte:

#### logOnly

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

#### sendTrap

Das Gerät sendet einen SNMP-Trap.

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

#### reboot (Voreinstellung)

Das Gerät löst einen Neustart aus.

## 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:

**An**

Das Senden von Ereignissen ist eingeschaltet.

Das Gerät sendet die in der Tabelle festgelegten Ereignisse zum jeweils festgelegten Syslog-Server.

**Aus** (Voreinstellung)

Das Senden von Ereignissen ist ausgeschaltet.

### 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:

1..8

IP-Adresse

Legt die IP-Adresse des Syslog-Servers fest.

Mögliche Werte:

Gültige IPv4-Adresse (Voreinstellung: 0.0.0.0)

DNS-Name im Format <domain>. <tl d> oder <host>. <domain>. <tl d>

Voraussetzung ist, dass Sie zusätzlich im Dialog *Erweitert > DNS > Client > Global* die Funktion *Client* einschalten.

Wenn Sie eine verschlüsselte Verbindung mithilfe eines digitalen Zertifikats herstellen, vergewissern Sie sich, dass die *Common Name*- oder *Subject Alternative Name*-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:

1..65535 (2<sup>16</sup> - 1) (Voreinstellung: 514)

Min. Schweregrad

Legt den Mindest-Schweregrad der Ereignisse fest. Das Gerät sendet einen Log-Eintrag für Ereignisse mit diesem Schweregrad und mit dringlicheren Schweregraden an den Syslog-Server.

Mögliche Werte:

emergency

alert

critical

error

warning (Voreinstellung)

notice

informational

debug

Typ

Legt den Typ des Log-Eintrags fest, den das Gerät übermittelt.

Mögliche Werte:

syslog (Voreinstellung)

audittrail

Aktiv

Aktiviert bzw. deaktiviert die Übermittlung der Ereignisse zum Syslog-Server.

Mögliche Werte:

[markiert](#)

Das Gerät sendet Ereignisse zum Syslog-Server.

[unmarkiert](#) (Voreinstellung)

Die Übermittlung der Ereignisse zum Syslog-Server ist deaktiviert.

## 8.4 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](#)

## 8.4.1 LLDP Konfiguration

[ Diagnose > LLDP > Konfiguration ]

Dieser Dialog ermöglicht Ihnen, die Topologie-Erkennung für jeden Port einzurichten.

### Funktion

Funktion

Schaltet die Funktion *LLDP* ein/aus.

Mögliche Werte:

*An* (Voreinstellung)

Die Funktion *LLDP* ist eingeschaltet.

Die Topologie-Erkennung mit LLDP ist im Gerät aktiv.

*Aus*

Die Funktion *LLDP* ist ausgeschaltet.

### Konfiguration

Sende-Intervall [s]

Legt das Intervall in Sekunden fest, in dem das Gerät LLDP-Datenpakete sendet.

Mögliche Werte:

5 . 32768 (2<sup>1</sup>) (Voreinstellung: 30)

Sende-Intervall Multiplikator

Legt den Faktor zur Bestimmung des Time-to-live-Werts für die LLDP-Datenpakete fest.

Mögliche Werte:

2 . 10 (Voreinstellung: 4)

Der im LLDP-Header kodierte Time-to-live-Wert ergibt sich aus der Multiplikation dieses Wertes mit dem Wert im Feld *Sende-Intervall [s]*.

Reinitialisierungs-Verzögerung [s]

Zeigt die Verzögerung in Sekunden für die Re-Initialisierung eines Ports.

Wenn in Spalte *Funktion* der Wert *Aus* festgelegt ist, dann versucht das Gerät nach Ablauf der hier festgelegten Zeit den Port erneut zu initialisieren.

Sende-Verzögerung [s]

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:

5..3600 (Voreinstellung: 5)

Nach Senden eines Benachrichtigungs-Traps wartet das Gerät mindestens die hier festgelegte Zeit, bis es den nächsten Benachrichtigungs-Trap sendet.

#### **Tabelle**

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

#### Port

Zeigt die Nummer des Ports.

#### Funktion

Legt fest, ob der Port LLDP-Datenpakete überträgt.

Mögliche Werte:

[transmit](#)

Der Port sendet LLDP-Datenpakete, speichert jedoch keine Informationen über benachbarte Geräte.

[receive](#)

Der Port empfängt LLDP-Datenpakete, sendet jedoch keine Informationen an benachbarte Geräte.

[receive and transmit](#) (Voreinstellung)

Der Port sendet LLDP-Datenpakete und speichert Informationen über benachbarte Geräte.

[ausgeschaltet](#)

Der Port sendet keine LLDP-Datenpakete und speichert keine Informationen über benachbarte Geräte.

#### Benachrichtigung

Aktiviert/deaktiviert LLDP-Benachrichtigungen auf dem Port.

Mögliche Werte:

[markiert](#)

LLDP-Benachrichtigungen auf dem Port sind aktiv.

[unmarkiert](#) (Voreinstellung)

LLDP-Benachrichtigungen auf dem Port sind inaktiv.

#### Port-Beschreibung senden

Aktiviert/deaktiviert das Senden des TLV (Type-Length-Value) mit der Port-Beschreibung.

Mögliche Werte:

`markiert` (Voreinstellung)

Das Senden des TLV ist aktiv.

Das Gerät sendet den TLV mit der Port-Beschreibung.

`unmarkiert`

Das Senden des TLV ist inaktiv.

Das Gerät sendet keinen TLV mit der Port-Beschreibung.

#### Systemname senden

Aktiviert/deaktiviert das Senden des TLV (Type-Length-Value) mit dem Gerätenamen.

Mögliche Werte:

`markiert` (Voreinstellung)

Das Senden des TLV ist aktiv.

Das Gerät sendet den TLV mit dem Gerätenamen.

`unmarkiert`

Das Senden des TLV ist inaktiv.

Das Gerät sendet keinen TLV mit dem Gerätenamen.

#### Systembeschreibung senden

Aktiviert/deaktiviert das Senden des TLV (Type-Length-Value) mit der Systembeschreibung.

Mögliche Werte:

`markiert` (Voreinstellung)

Das Senden des TLV ist aktiv.

Das Gerät sendet den TLV mit der Systembeschreibung.

`unmarkiert`

Das Senden des TLV ist inaktiv.

Das Gerät sendet keinen TLV mit der Systembeschreibung.

#### System-Ressourcen senden

Aktiviert/deaktiviert das Senden des TLV (Type-Length-Value) mit den System-Ressourcen (Leistungsfähigkeitsdaten).

Mögliche Werte:

`markiert` (Voreinstellung)

Das Senden des TLV ist aktiv.

Das Gerät sendet den TLV mit den System-Ressourcen.

`unmarkiert`

Das Senden des TLV ist inaktiv.

Das Gerät sendet keinen TLV mit den System-Ressourcen.

#### Nachbarn (max.)

Begrenzt für diesen Port die Anzahl der zu erfassenden benachbarten Geräte.

Mögliche Werte:

1..50 (Voreinstellung: 10)

#### Modus FDB

Legt fest, welche Funktion das Gerät verwendet, um benachbarte Geräte auf diesem Port zu erfassen.

Mögliche Werte:

[l l dpOnl y](#)

Das Gerät verwendet ausschließlich LLDP-Datenpakete, um benachbarte Geräte auf diesem Port zu erfassen.

[macOnl y](#)

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.

[bei de](#)

Das Gerät verwendet LLDP-Datenpakete und gelernte MAC-Adressen, um benachbarte Geräte auf diesem Port zu erfassen.

[autoDetect](#) (Voreinstellung)

Wenn das Gerät auf diesem Port LLDP-Datenpakete empfängt, dann arbeitet das Gerät wie mit der Einstellung [l l dpOnl y](#). Andernfalls arbeitet das Gerät wie mit der Einstellung [macOnl y](#).

## 8.4.2 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. 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:

`markiert`

Das angeschlossene Gerät unterstützt kein LLDP.

Das Gerät verwendet Informationen aus seiner MAC-Adresstabelle (Forwarding Database).

`unmarkiert`

Das angeschlossene Gerät unterstützt aktiv LLDP.

#### Nachbar-Adresse

Zeigt die IPv4-Adresse oder den Hostnamen, mit der/dem der Zugriff auf das Management des Nachbargeräts möglich ist.

#### Nachbar IPv6-Adresse

Zeigt die IPv6-Adresse, mit welcher der Zugriff auf das Management des Nachbargeräts möglich ist.

#### Nachbar-Port Beschreibung

Zeigt eine Beschreibung für den Port des Nachbargeräts.

#### Nachbar-Systemname

Zeigt den Gerätenamen des Nachbargeräts.

#### Nachbar-Systembeschreibung

Zeigt eine Beschreibung für das Nachbargerät.

#### Port-ID

Zeigt die ID des Ports, über den das Nachbargerät mit dem Gerät verbunden ist.

#### Autonegotiation-Unterstützung

Zeigt, ob der Port des Nachbargeräts Auto-Negotiation unterstützt.

#### Autonegotiation

Zeigt, ob Auto-Negotiation auf dem Port des Nachbargeräts aktiv ist.

#### Unterstützt PoE

Zeigt, ob der Port des Nachbargeräts Power over Ethernet (PoE) unterstützt.

#### PoE eingeschaltet

Zeigt, ob Power over Ethernet (PoE) auf dem Port des Nachbargeräts aktiv ist.

## 8.5 Bericht

[Diagnose > Bericht]

Das Menü enthält die folgenden Dialoge:

- [Bericht Global](#)
- [Persistentes Ereignisprotokoll](#)
- [System-Log](#)
- [Audit-Trail](#)

## 8.5.1 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



Generiert 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 477](#).

#### Funktion

Schaltet die Funktion *Console-Logging* ein/aus.

Mögliche Werte:

*An*

Die Funktion *Console-Logging* ist eingeschaltet.  
Das Gerät protokolliert die Ereignisse auf der Konsole.

*Aus* (Voreinstellung)

Die Funktion *Console-Logging* ist ausgeschaltet.

#### Schweregrad

Legt den Mindest-Schweregrad für die Ereignisse fest. Das Gerät protokolliert Ereignisse mit diesem Schweregrad und mit dringlicheren Schweregraden. Weitere Informationen finden Sie unter „[Bedeutung der Ereignis-Schweregrade](#)“ auf [Seite 477](#).

Das Gerät gibt die Meldungen auf der seriellen Schnittstelle aus.

Mögliche Werte:

*emergency*

*al er t*

*cri ti cal*

*error*

*var ni ng* (Voreinstellung)

[noti ce](#)  
[i nformati onal](#)  
[debug](#)

## SNMP-Logging

Wenn Sie die Protokollierung von SNMP-Anfragen einschalten, sendet das Gerät diese als Ereignisse mit dem voreingestellten Schweregrad [noti ce](#) an die Liste der Syslog-Server. Der voreingestellte Mindest-Schweregrad für einen Syslog-Server-Eintrag ist [cri ti cal](#).

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 [var ni ng](#) oder [err or](#). 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 [cri ti cal](#) oder höher. Das Gerät sendet dann SNMP-Anfragen als Ereignisse mit dem Schweregrad [cri ti cal](#) oder schwerer an die Syslog-Server. Setzen Sie ausschließlich den Mindest-Schweregrad bei einem oder mehreren Syslog-Server-Einträgen auf [noti ce](#) 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:

[An](#)

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 [Schweregrad Get-Request](#) aus.

[Aus](#) (Voreinstellung)

Die Protokollierung ist ausgeschaltet.

### Logge SNMP Set-Requests

Schaltet die Protokollierung für den Empfang von *SNMP Set Requests* ein/aus.

Mögliche Werte:

[An](#)

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 [Schweregrad Set-Request](#) aus.

[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 477.

Mögliche Werte:

- emergency
- alert
- critical
- error
- warning
- notice (Voreinstellung)
- informational
- debug

## 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 477.

Mögliche Werte:

- emergency
- alert
- critical
- error
- warning
- notice (Voreinstellung)
- informational
- debug

**Buffered-Logging**

Das Gerät puffert protokollierte Ereignisse in 2 getrennten Speicherbereichen, damit die Log-Einträge für dringliche Ereignisse erhalten bleiben.

Dieser Rahmen ermöglicht Ihnen, den Mindest-Schweregrad für Ereignisse festzulegen, die das Gerät im höher priorisierten Speicherbereich puffert.

## Schweregrad

Legt den Mindest-Schweregrad für die Ereignisse fest. Das Gerät puffert Log-Einträge für Ereignisse mit diesem Schweregrad und mit dringlicheren Schweregraden im höher priorisierten Speicherbereich. Weitere Informationen finden Sie unter „[Bedeutung der Ereignis-Schweregrade](#)“ auf Seite 477.

Mögliche Werte:

- emergency
- alert
- critical

error  
warning (Voreinstellung)  
notice  
informational  
debug

## CLI-Logging

### Funktion

Schaltet die Funktion *CLI-Logging* ein/aus.

Mögliche Werte:

**An**

Die Funktion *CLI-Logging* ist eingeschaltet.

Das Gerät protokolliert jeden Befehl, den es über das Command Line Interface empfängt.

**Aus** (Voreinstellung)

Die Funktion *CLI-Logging* ist ausgeschaltet.

## Support-Informationen: Dateien im ZIP-Archiv

Dateiname	Format	Bemerkungen
audittrail.htm	HTML	Enthält die im <i>Audit Trail</i> -Protokoll chronologisch aufgezeichneten Systemereignisse und gespeicherten Änderungen durch die Benutzer.
config.xml	XML	Enthält die im „ausgewählten“ Konfigurationsprofil gespeicherten Einstellungen des Geräts. Der Dateiname entspricht dem Namen des gegenwärtig „ausgewählten“ Konfigurationsprofils.
defaultconfig.xml	XML	Enthält die Voreinstellungen des Geräts.
runningconfig.xml	XML	Enthält die gegenwärtigen Betriebseinstellungen des Geräts.
script	TEXT	Enthält die Ausgaben des Kommandos <code>show running-config script</code> .
supportinfo.htm	HTML	Enthält geräteinterne Service-Information.
systeminfo.htm	HTML	Enthält Information über die gegenwärtigen Einstellungen und Betriebsparameter.
systemlog.htm	HTML	Enthält die in der Log-Datei protokollierten Ereignisse. Siehe Dialog <i>Diagnose &gt; Bericht &gt; System-Log</i> .

## Bedeutung der Ereignis-Schweregrade

Schweregrad	Bedeutung
emergency	Gerät nicht betriebsbereit
alert	Sofortiger Bedienereingriff erforderlich
critical	Kritischer Zustand

Schweregrad	Bedeutung
error	Fehlerhafter Zustand
warning	Warnung
notice	Signifikanter, normaler Zustand
informational	Informierende Nachricht
debug	Debug-Nachricht

## 8.5.2 Persistentes Ereignisprotokoll

[Diagnose > Bericht > Persistentes Ereignisprotokoll]

Das Gerät ermöglicht Ihnen, die Log-Einträge in einer Datei im externen Speicher (ENM) 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 (ENM) 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 (ENM) ausreichend Speicherplatz verfügbar.

### Anmerkung:

Vergewissern Sie sich, dass ein externer Speicher (ENM) angeschlossen ist. Um festzustellen, ob ein externer Speicher (ENM) angeschlossen ist, siehe Spalte *Status* im Dialog *Grundeinstellungen > Externer Speicher*. Wir empfehlen, die Verbindung des externen Speichers mit der Funktion *Gerätetestatus* zu überwachen, siehe Parameter *Externer Speicher wurde entfernt* im Dialog *Diagnose > Statuskonfiguration > Gerätestatus*.

### Funktion

Funktion

Schaltet die Funktion *Persistentes Ereignisprotokoll* ein/aus.

Aktivieren Sie die Funktion ausschließlich dann, wenn der externe Speicher (ENM) im Gerät verfügbar ist.

Mögliche Werte:

**An** (Voreinstellung)

Die Funktion *Persistentes Ereignisprotokoll* ist eingeschaltet.

Das Gerät speichert die Log-Einträge in einer Datei im externen Speicher (ENM).

**Aus**

Die Funktion *Persistentes Ereignisprotokoll* ist ausgeschaltet.

### Konfiguration

Max. Datei-Größe [kByte]

Legt die maximale Größe der Log-Datei in KBytes fest. Wenn die Log-Datei die festgelegte Größe erreicht, archiviert das Gerät diese Datei und speichert die folgenden Log-Einträge in einer neu generierten Datei.

Mögliche Werte:

0 . 4096 (Voreinstellung: 1024)

Der Wert 0 deaktiviert das Speichern der Log-Einträge in der Log-Datei.

Dateien (max.)

Legt die Anzahl an Log-Dateien fest, die das Gerät im externen Speicher (ENM) vorhält.

Sobald die festgelegte maximale Anzahl an Dateien erreicht ist, löscht das Gerät die älteste Datei und benennt die verbleibenden Dateien um.

Mögliche Werte:

0 . 25 (Voreinstellung: 4)

Der Wert 0 deaktiviert das Speichern der Log-Einträge in der Log-Datei.

Schweregrad

Legt den Mindest-Schweregrad der Ereignisse fest. Das Gerät speichert den Log-Eintrag für Ereignisse mit diesem Schweregrad und mit dringlicheren Schweregraden in der Log-Datei im externen Speicher (ENM).

Mögliche Werte:

- emergency
- al er t
- cri ti cal
- err or
- var ni ng (Voreinstellung)
- noti ce
- i nfor mati onal
- debug

Ziel der Log-Datei

Legt den Typ des externen Speichers für die Protokollierung fest.

Mögliche Werte:

- sd (Voreinstellung)  
Externer SD-Speicher (ACA31)
- usb  
Externer USB-Speicher (ACA21/ACA22)

**Tabelle**

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

Schaltflächen

 Persistente Log-Datei leeren

Löscht die Log-Dateien aus dem externen Speicher (ENM).

## Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht.

Mögliche Werte:

1..25

Das Gerät legt diese Nummer automatisch fest.

## Dateiname

Zeigt den Dateinamen der Log-Datei im externen Speicher ([EMM](#)).

Mögliche Werte:

messages

messages.X

## Datei-Größe [Byte]

Zeigt die Größe der Log-Datei im externen Speicher ([EMM](#)) in Bytes.

## 8.5.3 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:

[CSV](#)

Das Gerät stellt die Datei im CSV-Format bereit.

[HTML](#)

Das Gerät stellt die Datei im HTML-Format bereit.



Log-Datei leeren

Leert die System-Log-Datei im Gerät.

## 8.5.4 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 das Gerät. Dies ermöglicht Ihnen, nachzuvollziehen, WER WANN WAS im Gerät ändert. Voraussetzung ist, dass Ihrem Benutzerkonto die Zugriffsrolle [audi tor](#) oder [adm in strator](#) 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 Aktualisierungen der Geräte-Software
- Konfigurationsänderungen mittels HiDiscovery
- Aktualisierung der Geräte-Software und automatisches Konfigurieren des Geräts über den externen Speicher ([ENMM](#))
- 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 1 während des Systemstarts möglich. Ein Angreifer, der sich physisch Zugriff auf das Gerät verschafft, kann mittels des System Monitors 1 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 Zugriff auf den System Monitor 1. Siehe Dialog [Diagnose > System > Selbsttest](#), Kontrollkästchen [SysMon1 ist verfügbar](#).

Schaltflächen

 Audit-Trail Datei speichern

Speichert die HTML-Seite auf Ihrem PC mittels Webbrowser-Dialog.



## 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 [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 *Client* ein.

#### Funktion

Funktion

Schaltet die Funktion *Client* ein/aus.

Mögliche Werte:

*An*

Die Funktion *Client* ist eingeschaltet.

Das Gerät sendet Anfragen zur Auflösung von Hostnamen in IP-Adressen an einen DNS-Server.

*Aus* (Voreinstellung)

Die Funktion *Client* ist ausgeschaltet.

## 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.

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 &gt; DNS &gt; Client &gt; 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:

[user](#)

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 [Erstellen](#), um eine Tabellenzeile hinzuzufügen.

- Im Feld [Index](#) legen Sie die Index-Nummer fest.

Mögliche Werte:

[1](#) . [4](#)

Das Gerät ermöglicht Ihnen, bis zu 4 externe DNS-Server festzulegen.

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

Mögliche Werte:

- Gültige IPv4-Adresse



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 *Erweitert > DNS > Client > Global* ist die Funktion *DNS client* eingeschaltet.
- Im Rahmen *Konfiguration* ist in der Dropdown-Liste *Quelle* der Eintrag *user* ausgewählt.

Mögliche Werte:

**markiert** (Voreinstellung)

Die Tabellenzeile ist aktiv.

Das Gerät sendet Anfragen an den in der ersten aktiven Tabellenzeile festgelegten DNS-Server. Erhält das Gerät von diesem Server keine Antwort, sendet es Anfragen an den in der nächsten aktiven Tabellenzeile festgelegten DNS-Server. Das entsprechende Timeout legen Sie im Rahmen *Konfiguration*, Feld *Request Timeout [s]* fest.

**unmarkiert**

Die Tabellenzeile ist inaktiv.

Das Gerät sendet keine Anfragen an diesen DNS-Server.

## 9.1.2 DNS-Cache

[Erweitert > DNS > Cache]

Die *Cache*-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 *Cache* ein. Ist die Funktion *Cache* 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 *Cache* ein/aus.

Mögliche Werte:

*An* (Voreinstellung)

Die Funktion *Cache* ist eingeschaltet.

*Aus*

Die Funktion *Cache* 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.
- Wenn sich der Status des Tracking-Objekts ändert, aktiviert/deaktiviert das Gerät das mit dem Tracking-Objekt verknüpfte Interface. Das Gerät zeigt die zugehörige Anwendung im Dialog *Erweitert > Tracking > Applikationen*.

Sobald Sie die Tracking-Objekte im Dialog [Erweitert > Tracking > Konfiguration](#) eingerichtet haben, können Sie Applikationen mit den Tracking-Objekten verknüpfen:

- Statische Routen verknüpfen Sie mit einem Tracking-Objekt im Dialog [Routing > Routing-Tabelle](#), Spalte [Track-Name](#).
- Virtuelle Router verknüpfen Sie mit einem Tracking-Objekt im Dialog [Routing > L3-Redundanz > VRRP > Tracking](#). Klicken Sie die Schaltfläche , um das Fenster [Erstellen](#) zu öffnen und in der Dropdown-Liste [Track-Name](#) das Tracking-Objekt auszuwählen.
- Sie verknüpfen den Interface-Status mit einem Tracking-Objekt im Dialog [Grundeinstellungen > Port](#), Spalte [Track-Name](#).

Das Menü enthält die folgenden Dialoge:

- [Tracking Konfiguration](#)
- [Tracking Applikationen](#)

## 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 *Erstellen*, um eine Tabellenzeile hinzuzufügen.

- In der Dropdown-Liste *Typ* wählen Sie den Typ des Tracking-Objekts.

Mögliche Werte:

*interface*

Das Gerät überwacht den Link-Status seiner physischen Ports, Link-Aggregation-, LRE- oder VLAN-Router-Interfaces.

*ping*

Das Gerät überwacht die Route zu einem entfernten Router oder Endgerät durch periodisches Senden von *ICMP Echo Request*-Paketen.

*logical*

Das Gerät überwacht logisch miteinander verknüpfte Tracking-Objekte und ermöglicht somit komplexe Überwachungsaufgaben.

- Im Feld *Track-ID* legen Sie die Identifikationsnummer des Tracking-Objektes fest.

Mögliche Werte:

*1..256*



Löschen

Entfernt die ausgewählte Tabellenzeile.

#### Typ

Legt den Typ des Tracking-Objekts fest.

Mögliche Werte:

*interface*

Das Gerät überwacht den Link-Status seiner physischen Ports, Link-Aggregation-, LRE- oder VLAN-Router-Interfaces.

*ping*

Das Gerät überwacht die Route zu einem entfernten Router oder Endgerät durch periodisches Senden von *ICMP Echo Request*-Paketen.

*logical*

Das Gerät überwacht logisch miteinander verknüpfte Tracking-Objekte und ermöglicht somit komplexe Überwachungsaufgaben.

#### Track-ID

Legt die Identifikationsnummer des Tracking-Objektes fest.

Mögliche Werte:

1..256

Dieser Bereich steht jedem Typ (*interface*, *ping* und *logical*) zur Verfügung.

#### Track-Name

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

#### Aktiv

Aktiviert/deaktiviert die Überwachung des Tracking-Objekts.

Mögliche Werte:

*markiert*

Die Überwachung ist aktiv. Das Gerät überwacht das Tracking-Objekt.

*unmarkiert* (Voreinstellung)

Die Überwachung ist inaktiv.

#### Beschreibung

Legt die Beschreibung fest.

Beschreiben Sie hier, wofür das Gerät das Tracking-Objekt verwendet.

Mögliche Werte:

Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

#### Status

Zeigt das Überwachungsergebnis des Tracking-Objekts.

Mögliche Werte:

*up*

Das Überwachungsergebnis ist positiv:

- Der Link-Status ist aktiv.
- oder
- Der entfernte Router oder das Endgerät ist erreichbar.
- oder
- Das Ergebnis der logischen Verknüpfung ist *WAHR*.

*down*

Das Überwachungsergebnis ist negativ:

- Der Link-Status ist inaktiv.
- oder
- Der entfernte Router oder das Endgerät ist unerreichbar.
- oder
- Das Ergebnis der logischen Verknüpfung ist *FALSCH*.

*not Ready*

Die Überwachung des Tracking-Objekts ist inaktiv. Sie aktivieren die Überwachung in Spalte *Aktiv*.

## Änderungen

Zeigt die Anzahl der Zustandsänderungen, seitdem das Tracking-Objekt aktiv ist.

## Letzte Änderung

Zeigt den Zeitpunkt der letzten Zustandsänderung.

## Trap senden

Aktiviert/deaktiviert das Senden eines SNMP-Traps, wenn jemand das Tracking-Objekt aktiviert oder deaktiviert.

Mögliche Werte:

`markiert`

Das Gerät sendet einen SNMP-Trap, wenn jemand das Tracking-Objekt in Spalte `Aktiv` aktiviert oder deaktiviert.

`unmarkiert` (Voreinstellung)

Das Gerät sendet keinen SNMP-Trap.

## Port

Legt für Tracking-Objekte des Typs `interface` das zu überwachende Interface fest.

Mögliche Werte:

`<Interface-Nummer>`

Nummer des physischen Ports, des Link-Aggregation-, LRE- oder VLAN-Router-Interfaces.

`no Port`

Kein Tracking-Objekt des Typs `interface`.

## Link-Up Verzögerung [s]

Legt die Zeit in Sekunden fest, nach der das Gerät das Überwachungsergebnis als positiv erkennt. Wenn der Link auf dem Interface länger als die hier festgelegte Zeit aktiv ist, zeigt Spalte `Status` den Wert `up`.

Mögliche Werte:

`0..255`

`-`

Kein Tracking-Objekt des Typs `logical`.

## Link-Down Verzögerung [s]

Legt die Zeit in Sekunden fest, nach der das Gerät das Überwachungsergebnis als negativ erkennt. Wenn der Link auf dem Interface länger als die hier festgelegte Zeit inaktiv ist, zeigt Spalte `Status` den Wert `down`.

Mögliche Werte:

`0..255`

`-`

Kein Tracking-Objekt des Typs `interface`.

Link-Aggregation-, LRE- und VLAN-Router-Interfaces haben ein negatives Überwachungsergebnis, wenn die Verbindung jedes aggregierten Ports unterbrochen ist.

Ein VLAN-Router-Interface hat ein negatives Überwachungsergebnis, wenn die Verbindung zu jedem physischen Port und Link-Aggregation-Interface, das Mitglied im VLAN ist, unterbrochen ist.

#### Ping-Port

Legt für Tracking-Objekte des Typs [ping](#) das Router-Interface fest, über welches das Gerät die *ICMP Echo Request*-Pakete sendet.

Mögliche Werte:

- [<Interface-Nummer>](#)  
Nummer des Router-Interfaces.
- [noName](#)  
Kein Router-Interface zugewiesen.
- Kein Tracking-Objekt des Typs [ping](#).

#### IP-Adresse

Legt die IP-Adresse des zu überwachenden entfernten Routers oder Endgeräts fest.

Mögliche Werte:

- Gültige IPv4-Adresse
- Kein Tracking-Objekt des Typs [ping](#).

#### Ping-Intervall [ms]

Legt das Intervall in Millisekunden fest, in welchem das Gerät periodisch *ICMP Echo Request*-Pakete sendet.

Mögliche Werte:

- [100 . 20000](#) (Voreinstellung: [1000](#))  
Wenn Sie einen Wert [<1000](#) festlegen, können Sie maximal 16 Tracking-Objekte des Typs [ping](#) einrichten.
- Kein Tracking-Objekt des Typs [ping](#).

#### 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 [Status](#) den Wert [down](#).

Mögliche Werte:

- [1 . 10](#) (Voreinstellung: [3](#))
- Kein Tracking-Objekt des Typs [ping](#).

## Ankommende Ping-Antworten

Legt fest, nach wie vielen empfangenen Antworten das Gerät das Überwachungsergebnis als positiv erkennt. Wenn das Gerät nacheinander sooft wie hier festgelegt eine Antwort auf gesendete *ICMP Echo Request*-Pakete empfängt, dann zeigt Spalte *Status* den Wert *up*.

Mögliche Werte:

1..10 (Voreinstellung: 2)

-

Kein Tracking-Objekt des Typs *ping*.

## Ping Timeout [ms]

Legt die Zeit in Millisekunden fest, in der das Gerät auf eine Antwort wartet. Empfängt das Gerät während dieser Zeit keine Antwort, wertet es dies als ausbleibende Antwort. Siehe Spalte *Ausbleibende Ping-Antworten*.

Mögliche Werte:

10..10000 (Voreinstellung: 100)

Wenn eine große Anzahl an Ping-Tracking-Objekten im Gerät eingerichtet ist, legen Sie den Wert ausreichend groß fest. Bei mehr als 100 Instanzen sollten Sie mindestens 200 ms festlegen.

-

Kein Tracking-Objekt des Typs *ping*.

## Ping TTL

Legt den TTL-Wert im IP-Header fest, mit dem das Gerät die *ICMP Echo Request*-Pakete 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.

Mögliche Werte:

-

Kein Tracking-Objekt des Typs *ping*.

1..255 (Voreinstellung: 128)

## Best route

Zeigt die Nummer des Router-Interfaces, über das die beste Route zum zu überwachenden Router oder Endgerät führt.

Mögliche Werte:

<Port-Nummer>

Nummer des Router-Interfaces.

no Port

Keine Route vorhanden.

-

Kein Tracking-Objekt des Typs *ping*.

#### Logischer Operand A

Legt für Tracking-Objekte des Typs `logical` den ersten Operanden der logischen Verknüpfung fest.

Mögliche Werte:

Eingerichtete Tracking-Objekte

-

Kein Tracking-Objekt des Typs `logical`.

#### Logischer Operand B

Legt für Tracking-Objekte des Typs `logical` den zweiten Operanden der logischen Verknüpfung fest.

Mögliche Werte:

Eingerichtete Tracking-Objekte

-

Kein Tracking-Objekt des Typs `logical`.

#### Operator

Verknüpft die in den Feldern *Logischer Operand A* und *Logischer Operand B* festgelegten Tracking-Objekte.

Mögliche Werte:

`and`

Logische UND-Verknüpfung

`or`

Logische ODER-Verknüpfung

-


Kein Tracking-Objekt des Typs `logical`.

## 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 [Routing > Routing-Tabelle](#), Spalte [Track-Name](#).
- Virtuelle Router verknüpfen Sie mit einem Tracking-Objekt im Dialog [Routing > L3-Redundanz > VRRP > Tracking](#). Klicken Sie die Schaltfläche , um das Fenster [Erstellen](#) zu öffnen und in der Dropdown-Liste [Track-Name](#) das Tracking-Objekt auszuwählen.
- Sie verknüpfen den Interface-Status mit einem Tracking-Objekt im Dialog [Grundeinstellungen > Port](#), Spalte [Track-Name](#).

### Tabelle

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

Typ

Zeigt den Typ des Tracking-Objekts.

Track-ID

Zeigt die Identifikationsnummer des Tracking-Objektes.

Applikation

Zeigt den Namen der Applikation, die mit dem Tracking-Objekte verknüpft ist.

Mögliche Werte:

- Tracking-Objekte des Typs [Logical](#)
- Statische Routen
- Virtuelle Router einer VRRP-Instanz
- Interface-Status

Track-Name

Zeigt den Namen des Tracking-Objekts, der sich aus den in Spalte [Typ](#) und Spalte [Track-ID](#) angezeigten Werten zusammensetzt.

## 9.3 Command Line Interface

[Erweitert > CLI]

Dieser Dialog ermöglicht Ihnen, mit dem Command Line Interface auf das Gerät zuzugreifen.

Voraussetzungen:

- Im Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH* ist der SSH-Server eingeschaltet.
- Installieren Sie auf Ihrer Workstation eine SSH-fähige Client-Anwendung, die in Ihrem Betriebssystem einen Handler für URLs registriert, die mit `ssh: //` beginnen.

### Schaltflächen

SSH-Verbindung starten

Öffnet die SSH-fähige Client-Anwendung.

Wenn Sie die Schaltfläche klicken, übergibt die Web-Anwendung den URL des Geräts beginnend mit `ssh: //` und den Benutzernamen des gegenwärtig angemeldeten Benutzers.

Wenn der Webbrowser eine SSH-fähige Client-Anwendung findet, dann stellt der SSH-fähige Client eine Verbindung mit dem SSH-Protokoll zum Management des Geräts her.



## A Stichwortverzeichnis

<b>0-9</b>	
1to1-NAT .....	412
802.1D/p-Mapping .....	305
<b>A</b>	
Aging-Time .....	295
Alarm .....	455
ARP .....	318, 324
ARP-Tabelle .....	52, 324, 462
Audit-Trail .....	483
Ausgangs-Lastbegrenzer .....	297
Authentifizierungs-Liste .....	72
<b>B</b>	
Benutzerverwaltung .....	67
Betriebszeit .....	21
<b>C</b>	
CLI .....	101
Command Line Interface .....	101
Community-Namen .....	103
<b>D</b>	
Deep Packet Inspection (DPI) .....	156
Default Gateway .....	373, 391, 435
Default Route .....	337, 338, 344, 435
Destination-NAT .....	416
DHCP L3 Relay .....	377
Digitales Zertifikat .....	20, 35, 77, 94, 264, 454
DNP3 Enforcer .....	166
DNS .....	485
DNS-Cache .....	489
DNS-Client .....	486
Domain Name System .....	485
DoS .....	249
Double-NAT .....	435
DPI .....	156
DPI DNP3 Enforcer .....	166
DPI Modbus Enforcer .....	157
DPI OPC Enforcer .....	163
<b>E</b>	
Eingangs-Lastbegrenzer .....	297
Einstellungen .....	31
Einstellungen zurücksetzen .....	35
ENVM .....	29, 36, 43, 480
Ereignis-Schweregrad .....	477
Externer Speicher .....	22, 29, 36, 43, 448, 453, 480
<b>F</b>	
FDB (MAC-Adresstabelle) .....	52, 300
Fingerprint .....	89, 94
Firewall-Lernmodus .....	122
Firewall-Tabelle .....	53
Flash-Speicher .....	29
Flusskontrolle .....	295

<b>G</b>	
Geräte-Software	27
Geräte-Software Backup	27
Gerätestatus	19, 446
<b>H</b>	
HiDiscovery	24, 453, 483
Host Key	90
HTML	459, 482
HTTP	90
HTTPS	91
HTTP-Server	452
<b>I</b>	
ICMP-Redirect	313, 319
Industrial HiVision	9, 86
Ingress Filtering	311
IP-Zugriffsbeschränkung	96
<b>K</b>	
Konfigurations-Check	460
Konfigurationsprofil	16, 31
<b>L</b>	
L3 Relay (DHCP)	377
Laden/Speichern	31
Lastbegrenzer	297
LDAP	72
Link-Status	447
LLDP	467
Logdatei	52, 53, 482
Login-Banner	102, 104
Loopback-Interface	381
<b>M</b>	
MAC-Adress-Filter	300
MAC-Adresstabelle (Forwarding Database)	52, 300
Management-VLAN	24
Management-Zugriff	24, 96
Modbus Enforcer	157
<b>N</b>	
NAT	412, 435
NAT (Network Address Translation)	408
Network Address Translation (NAT)	408
Network Time Protocol	59
Netzteil	21, 448
Neustart	52
NTP	59
NVM	16, 29, 36
<b>O</b>	
OPC Enforcer	163
OSPF	331

<b>P</b>	
Passwort	68, 451
Passwort-Länge	68, 451
Persistente Log-Datei	53
Persistentes Ereignisprotokoll	479
Port-Konfiguration	304
Port-Priorität	304
Port-Statistiken	52
Port-VLAN	310
Port-Weiterleitung	416
Pre-Login-Banner	104
Proxy-ARP	318
<b>Q</b>	
Queues	303
<b>R</b>	
RADIUS	72, 106
RAM	35
RAM-Selbsttest	463
Relay (DHCP)	377
Router-Interface	308, 316
Routing-Tabelle	372
<b>S</b>	
Schulungsangebote	505
Schwellenwerte Netzlast	297
Schweregrad	477
Secure Shell (SSH)	87
Selbsttest	463
Serielle Schnittstelle	452
Sicherheitsstatus	20, 450
SNMP-Server	85, 452
SNMP-Traps	49, 335, 392, 447, 450, 455, 494
SNMPv1/v2	103
Software-Aktualisierung	27
Software-Backup	27
Sommerzeit	56
Source Routing	313
SSH-Server	87
Standard-Gateway	373, 391, 435
Standard-Route	337, 338, 344, 435
Stratum	59, 61
Support-Informationen	474
Support-Informationen (ZIP-Archiv)	477
Syslog	465
System Monitor 1	463
Systeminformationen	459
System-Log	482
Systemzeit	55

<b>T</b>	
Technische Fragen	505
Technische Unterlagen	505
Technische Unterstützung	505
Temperatur	21, 447
Time To Live (TTL)	315
Topologie-Erkennung	472
Tracking	405, 490
Traps	49, 335, 392, 447, 450, 455, 494
Trap-Ziel	456
Trust Modus	304
TTL (Time To Live)	315
<b>V</b>	
Verschlüsselung	31
Virtual Local Area Network	306
Virtual Router Redundancy Protocol	391
VLAN	26, 306
VLAN Konfiguration	308
VLAN-Ports	310
VRRP	391
VRRP-Statistik	403
VRRP-Tracking	405
<b>W</b>	
Warteschlange (Queue)	303
Watchdog	31, 41
Webserver	90, 91
Werkseinstellungen	35
<b>Z</b>	
Zähler-Reset	52
Zertifikat	20, 35, 77, 93, 94, 264, 454
ZIP-Archiv mit Support-Informationen	477
Zugriffsbeschränkung	96
Zurücksetzen auf Werkseinstellungen	35

## 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](http://www.belden.com).

Technische Unterstützung erhalten Sie unter [my.belden.com](http://my.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](http://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](http://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



**HIRSCHMANN**

---

A **BELDEN** BRAND













-



-  
-



-

-





-

-

---

---

---

---

---

---

---

---

---

---

---

---

---







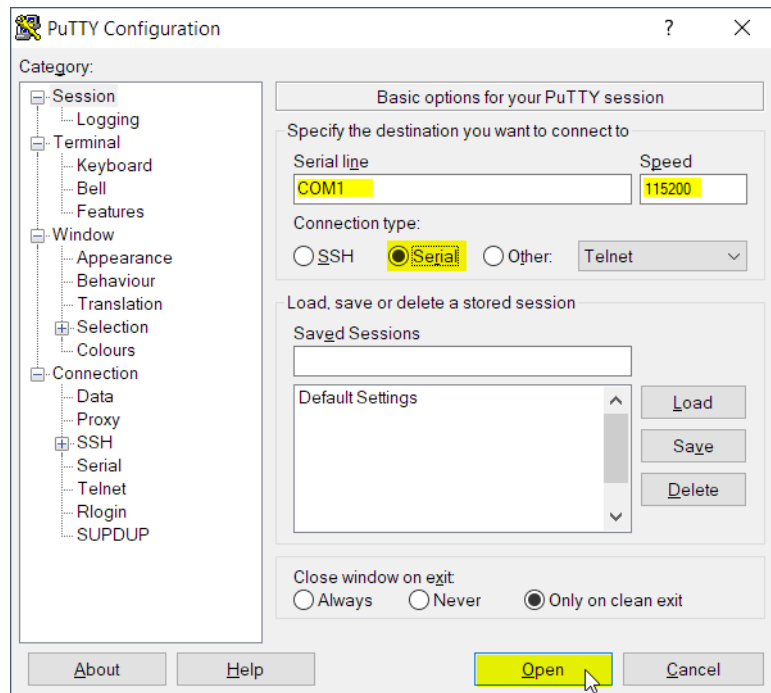




-



-

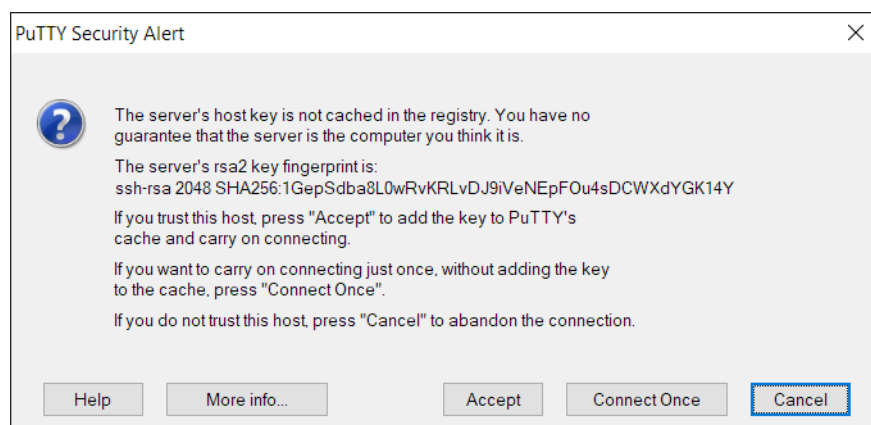
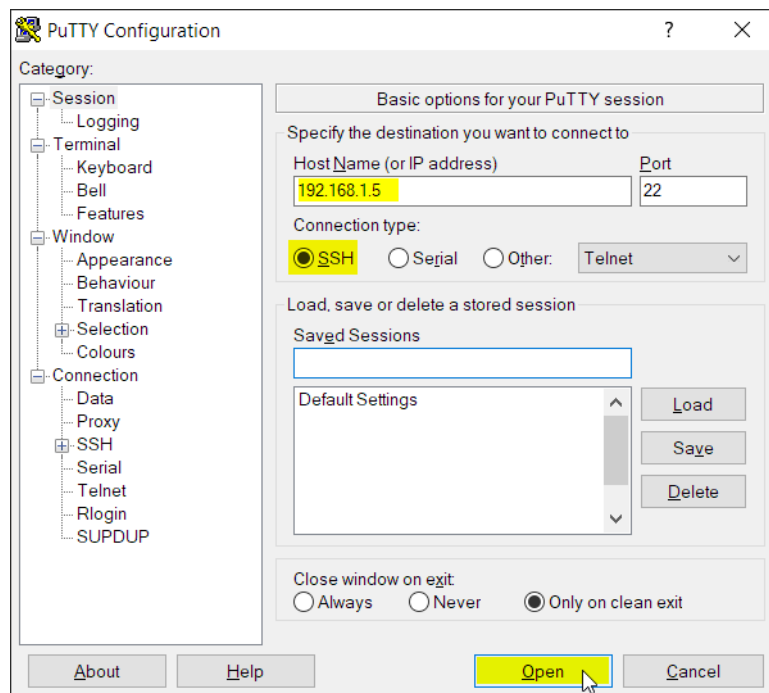



---

---

---

-



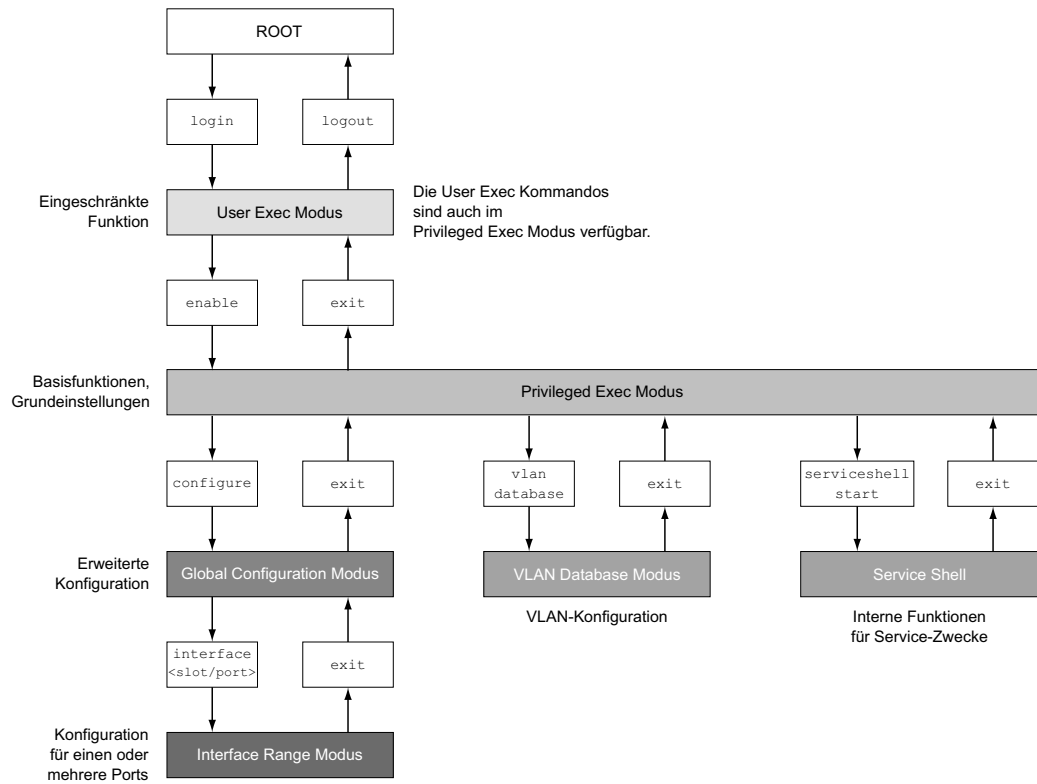
---

---

---

-

-





-

-

---

---

-

---

-

-

---

-

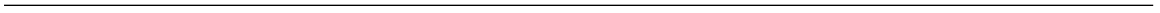
---

---

---







-





---

-

---

---

---



---

---

---





---

-

---

---

-

---

---

---

-

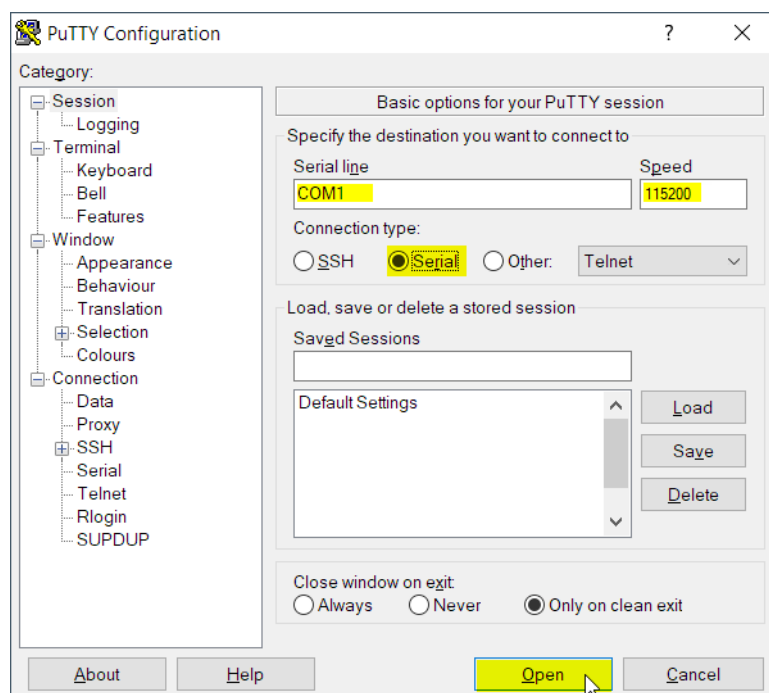
-

---

---

---







-



-





-



-

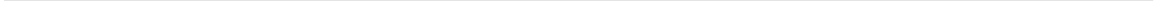
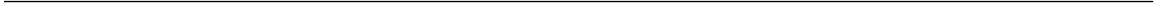
-

- -

-

-

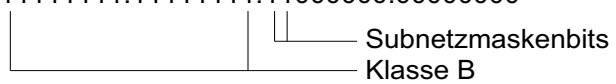
-



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



Dezimale Darstellung

129.218.65.17

└─── 128 < 129 191 > Klasse B

Binäre Darstellung

10000001.11011010.01000001.00010001

└─── Subnetz 1  
└─── Netzadresse

Dezimale Darstellung

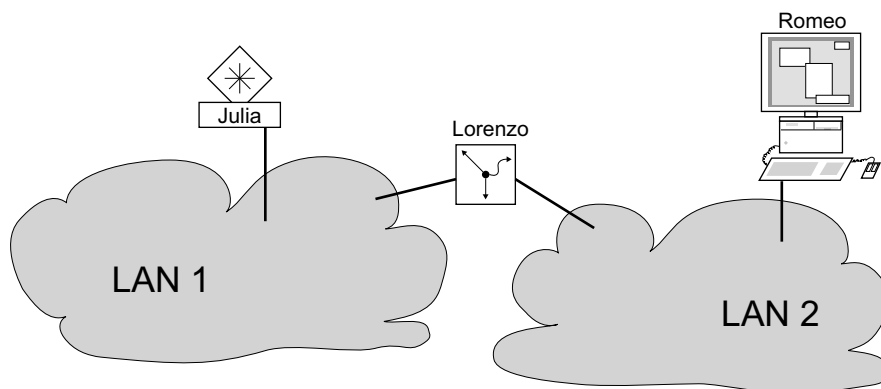
129.218.129.17

└─── 128 < 129 191 > Klasse B

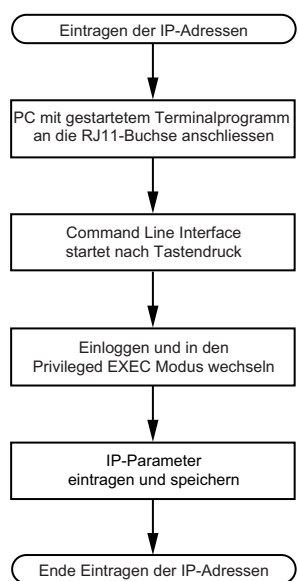
Binäre Darstellung

10000001.11011010.10000001.00010001

└─── Subnetz 2



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	



---

```
NOTE: Enter '?' for Command Help. Command help displays all opt
that are valid for the particular mode.
For the syntax of a particular command form, please
consult the documentation.
```

```
! ( ) >
```



-  
-

-

-

-

-

File Edit Options ?							
Id #	MAC Address	Writable	IP Address	Net Mask	Default Gateway	Product	Name
1	00:80:63:A4:CC:00	<input checked="" type="checkbox"/>	10.115.0.76	255.255.224.0	10.115.0.3		
2	00:80:63:C0:50:00	<input type="checkbox"/>	10.115.0.33	255.255.224.0	10.115.0.3		
3	00:80:63:A3:40:00	<input type="checkbox"/>	10.115.0.70	255.255.224.0	10.115.0.3		
4	00:80:63:98:14:00	<input type="checkbox"/>	10.115.0.17	255.255.224.0	10.115.0.3		
5	00:80:63:96:E4:00	<input type="checkbox"/>	0.0.0.0	0.0.0.0	0.0.0.0		
6	00:80:63:46:00:06	<input checked="" type="checkbox"/>	192.168.2.181	255.255.255.0	192.168.2.1		
7	00:80:63:A3:40:40	<input type="checkbox"/>	10.115.0.59	255.255.224.0	10.115.0.3		
8	00:80:63:A4:CC:40	<input type="checkbox"/>	10.115.0.81	255.255.224.0	10.115.0.3		
9	00:80:63:6E:38:4E	<input checked="" type="checkbox"/>	192.168.2.174	255.255.255.0	192.168.2.1		
10	00:80:63:18:2A:61	<input checked="" type="checkbox"/>	192.168.2.170	255.255.255.0	192.168.2.1		
11	00:80:63:A3:40:80	<input type="checkbox"/>	10.115.0.66	255.255.224.0	10.115.0.3		
12	00:80:63:A4:CC:80	<input type="checkbox"/>	10.115.0.80	255.255.224.0	10.115.0.3		
13	00:80:63:61:AC:81	<input checked="" type="checkbox"/>	192.168.2.176	255.255.255.0	192.168.2.1		
14	00:80:63:98:10:95	<input type="checkbox"/>	10.115.0.22	255.255.224.0	10.115.0.3		
15	00:80:63:61:AC:AB	<input checked="" type="checkbox"/>	192.168.2.40	255.255.255.0	192.168.2.1		
16	00:80:63:3B:5C:BD	<input checked="" type="checkbox"/>	192.168.2.178	255.255.255.0	192.168.2.1		
17	00:80:63:A3:40:C0	<input type="checkbox"/>	10.115.0.72	255.255.224.0	10.115.0.3		
18	00:80:63:8F:2C:BE	<input type="checkbox"/>	10.115.0.40	255.255.224.0	10.115.0.3		
19	00:80:63:88:38:EC	<input checked="" type="checkbox"/>	192.168.110.92	255.255.255.0	0.0.0.0		
20	00:80:63:9B:11:00	<input type="checkbox"/>	10.115.0.35	255.255.224.0	10.115.0.3		
21	00:80:63:A4:CD:00	<input type="checkbox"/>	10.115.0.77	255.255.224.0	10.115.0.3		
22	00:80:63:99:41:08	<input type="checkbox"/>	10.115.0.13	255.255.224.0	10.115.0.3		
23	00:80:63:17:35:08	<input checked="" type="checkbox"/>	192.168.2.164	255.255.255.0	192.168.2.1		
24	00:80:63:44:19:2E	<input checked="" type="checkbox"/>	10.115.5.130	255.255.224.0	10.115.0.3		

Properties

MAC Address: 00:80:63:A3:40:00

Name: Power Unit 1 Switch 2

IP Configuration

IP Address: 10 . 115 . 0 . 70 Set Default ()

Net Mask: 255 . 255 . 224 . 0 Set Default ()

Default Gateway: 10 . 115 . 0 . 3 Set Default ()

Save As Default

Ok Cancel

---

-



-

---

✓

---

✓



---

-

-

---

---



-

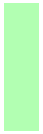
-

-

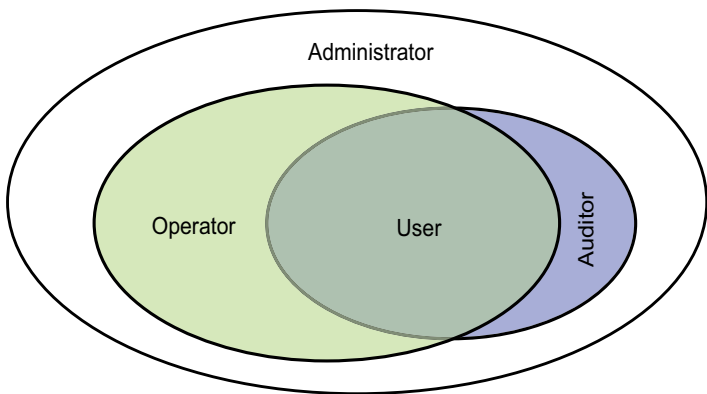




⌘ +







-  
-  
-  
-  
-

---



-

---

-

---



-



-








---

---

---



+

✓



---

---







---

---

---

---

---



- -  
- -  
- -



-  
-  
-



-

-

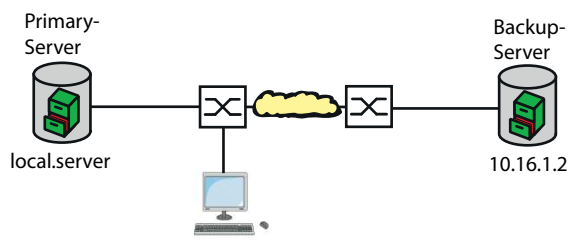
-

-

-

-

-



A series of horizontal lines for writing, consisting of a top line, a bottom line, and several intermediate lines.



-

-



+

+

-

-

-

-

-



-  
-



-

-

-

-

-

-

-

-

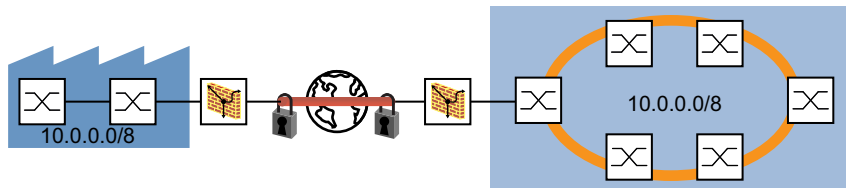
-



-

-

-







-

-

-

-

---

-  
-  
-

---

---

---

-

---

---

---

---

---

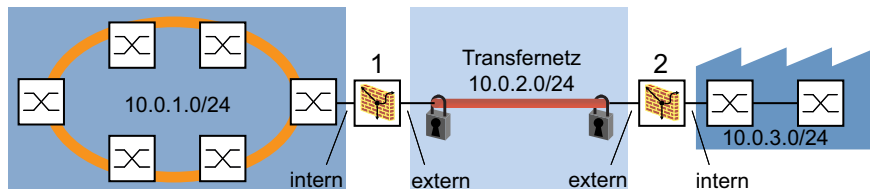
---

---

---

---

---















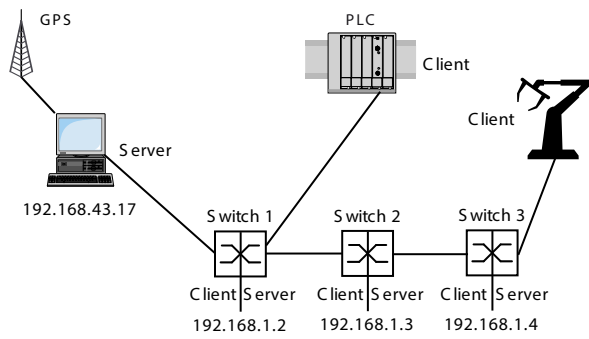
-



-

-





---




⌘+





.



⊕



.











≡

- -  
- -  
- -  
- -  
- -



-

-

-

-

-

-

-



-



≡



-



-

-

-

-



-

-

-

-

-





-  
-  
-  
-  
-  
-  
-



≡

-



---

---

---



---

---





-

-

-

-

-



-

-



-

-

-

-

-



-

-



-

-

-

-





-



---

---

---



-  
✓

-

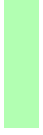


-

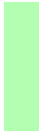


-





-



-



-

-



---

+

✓

---




+

+





-

-

-

-

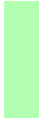
-



-



-





Q

✓

✓

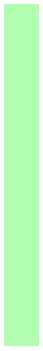
.



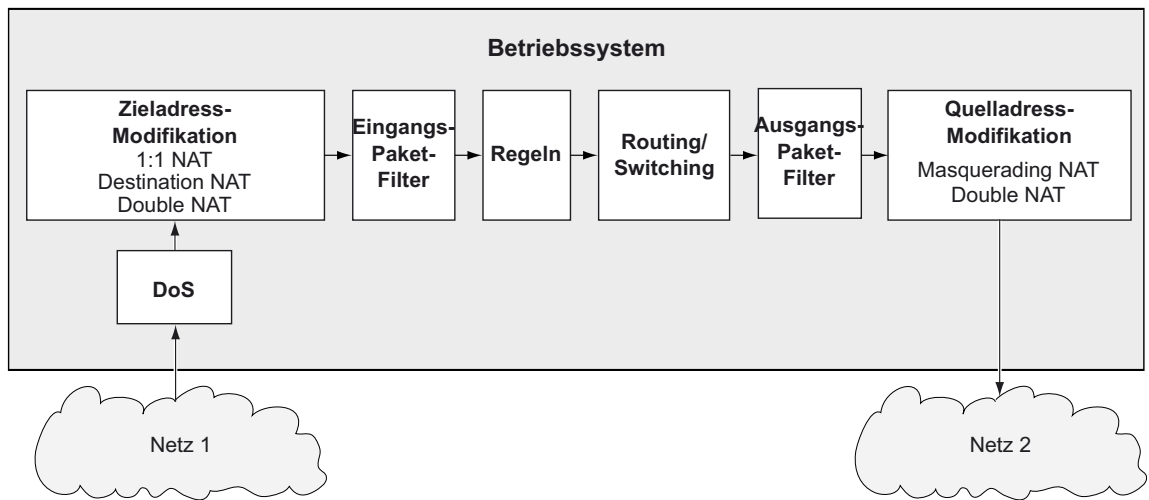
-













-



B+





-

-



-

-



B+





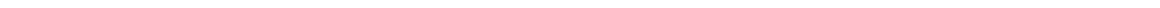
-

-

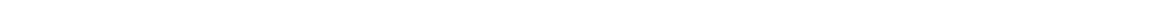
-

-

-



-





---

---

---

---



---

---

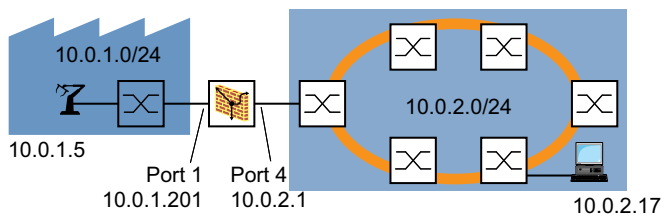
---

---

---

---







田+







-

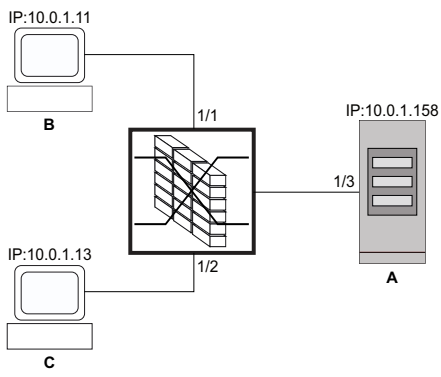
-

-



-

-





+





田+



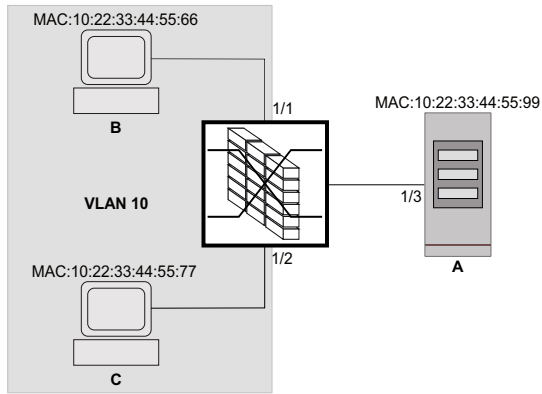
-

-



-

-





+





田+



-  
-



-

-

---

-

-

---

-

---

-

-





---

---









-

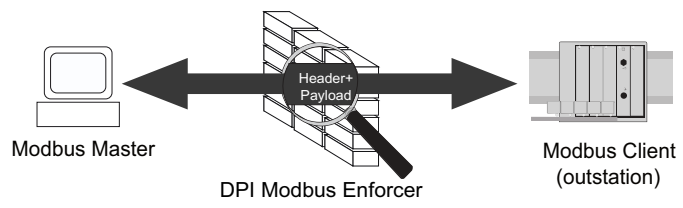


-



-



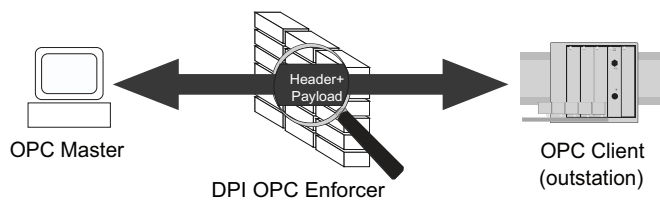




B+









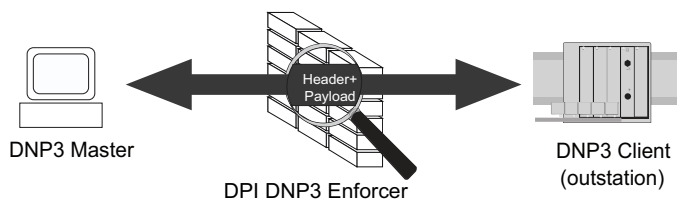
B+



-









B+



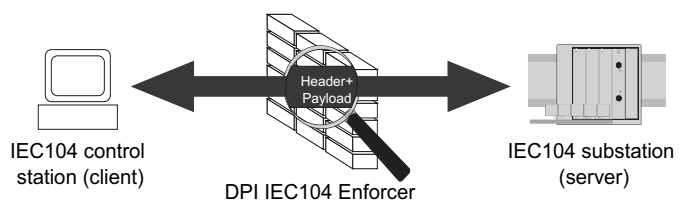


田+

✓

-







⌘+



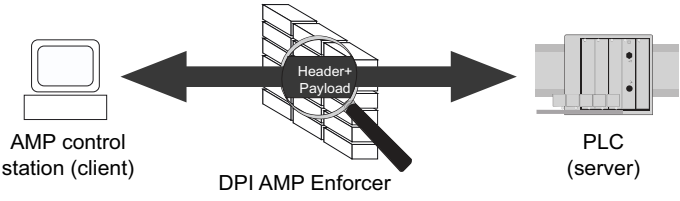




-

-

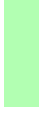
-





B+

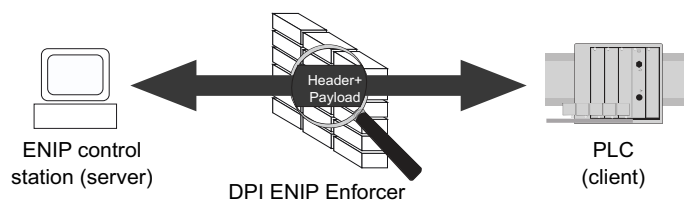




⌘+









B+

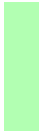
B+





-







-

-

-

-

-

-

-

-

-

-



+





-  
-  
-



-



0  
x







-

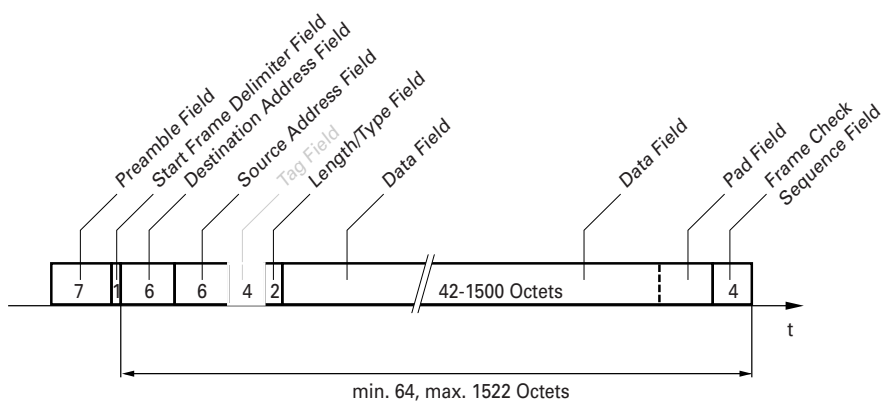
-

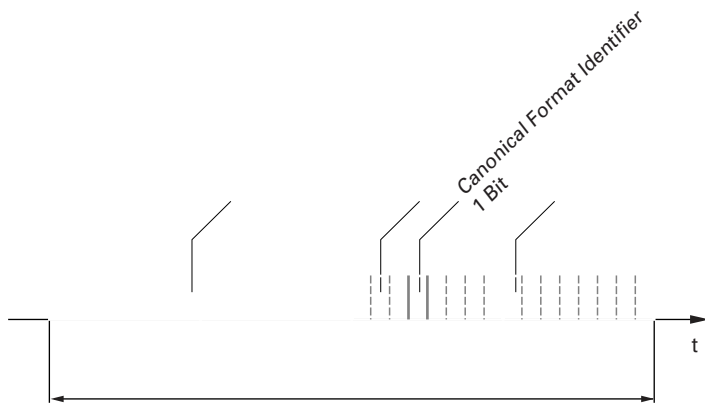
-

-

-





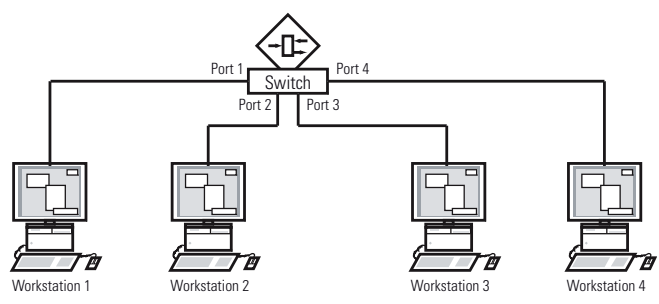




-

-

-





---

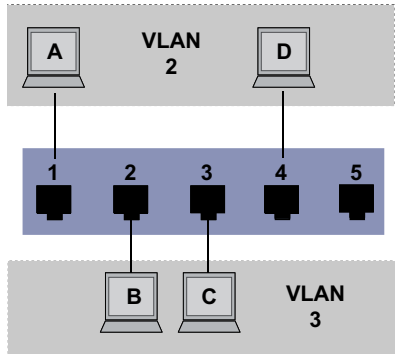
-

-

---

-

---



\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_



⌘  
+



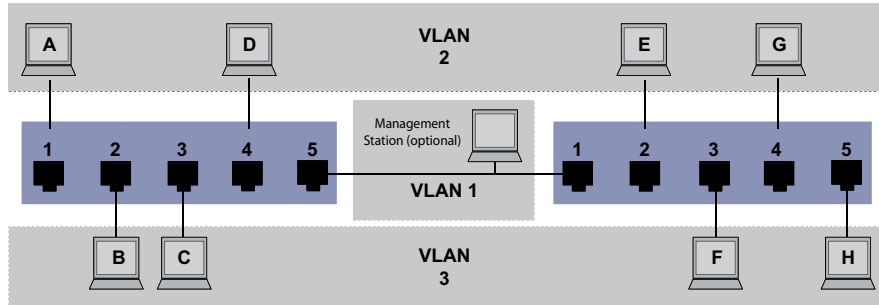


-

-

-

-



---

---

---

---

---

---

---

---

---

[Blue header bar]

[Lined text area 1]

[Blue header bar]

[Lined text area 2]

[Blue header bar]

[Lined text area 3]







-

-

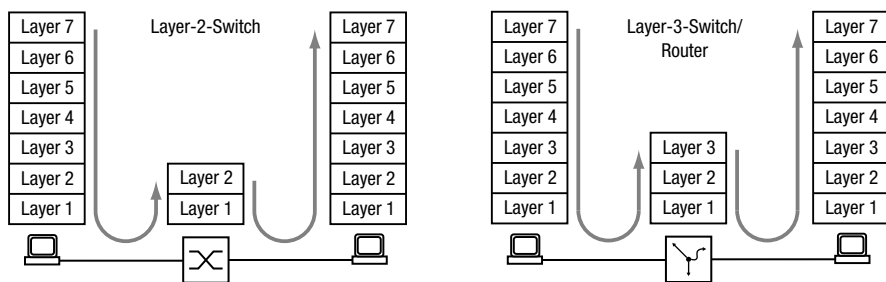
-

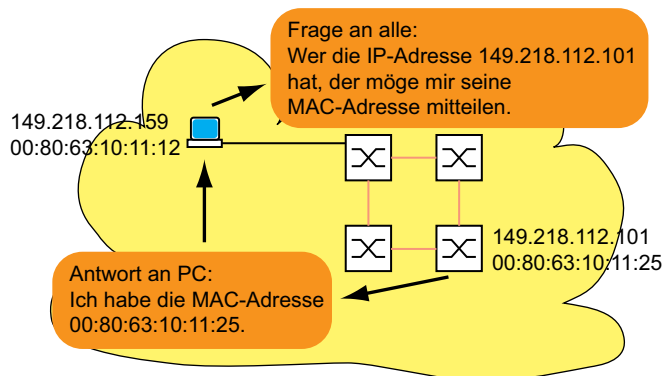
-

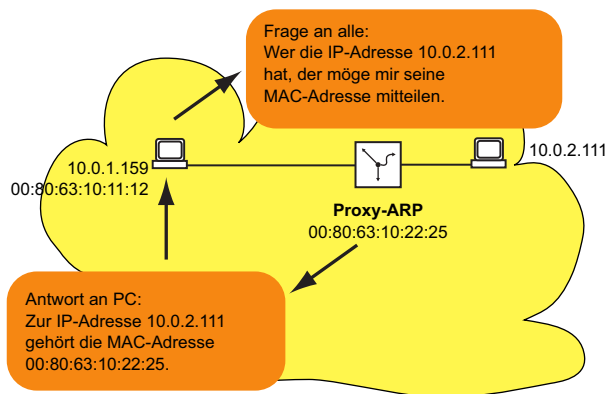
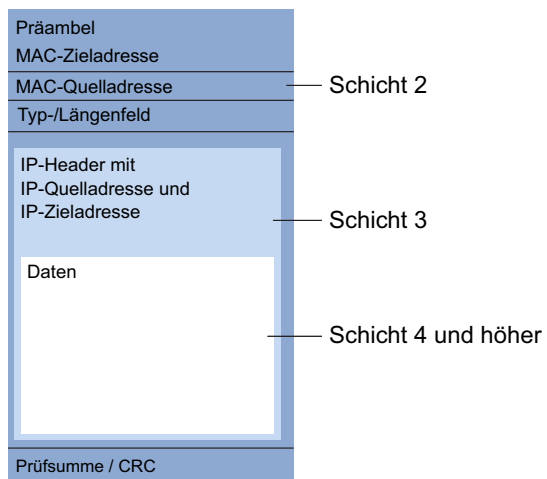


-

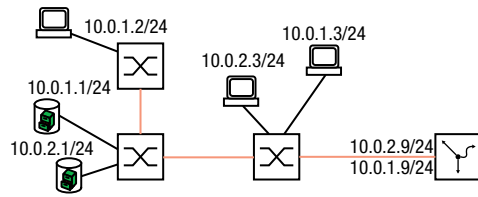


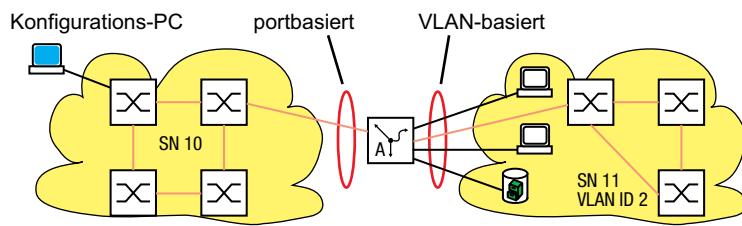


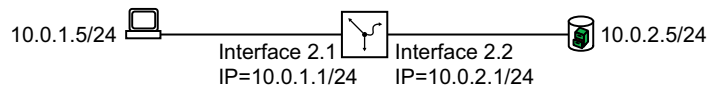




IP-Adresse dezimal	Netzmaske dezimal	IP-Adresse binär
149.218.112.1	255.255.255.128	10010101 11011010 01110000 00000001
149.218.112.127		10010101 11011010 01110000 01111111
		———— 25 Maskenbits ———
CIDR-Schreibweise: 149.218.112.0/25		
		└—— Maskenbits







-

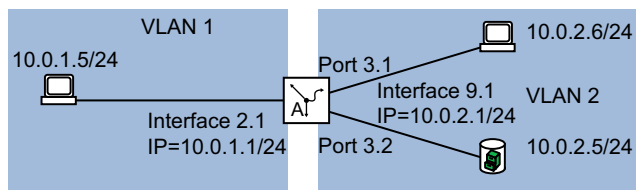
-

-

-

---

---



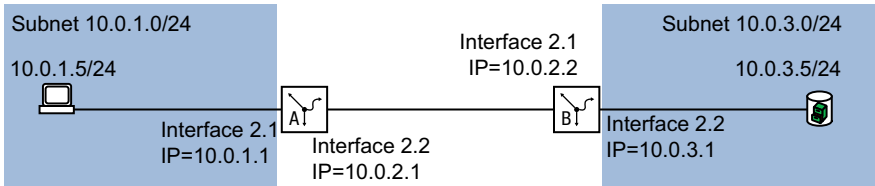
-

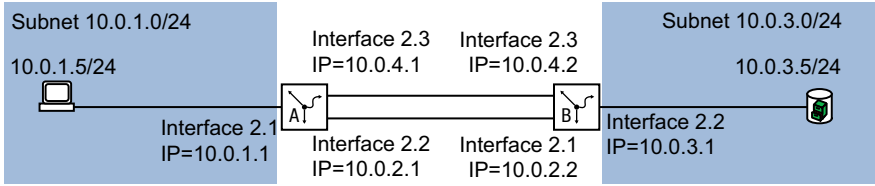


-

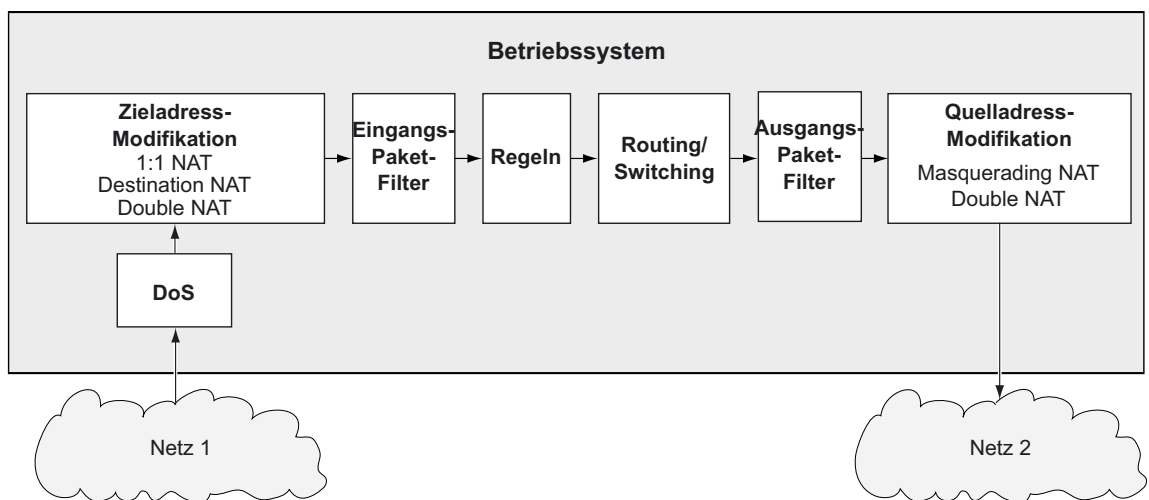
-

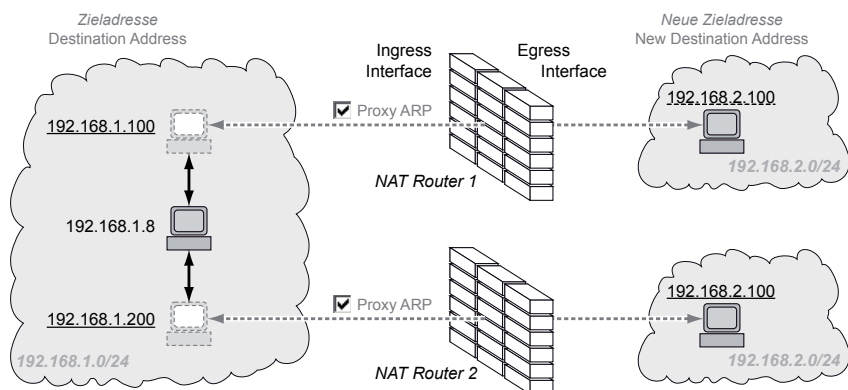
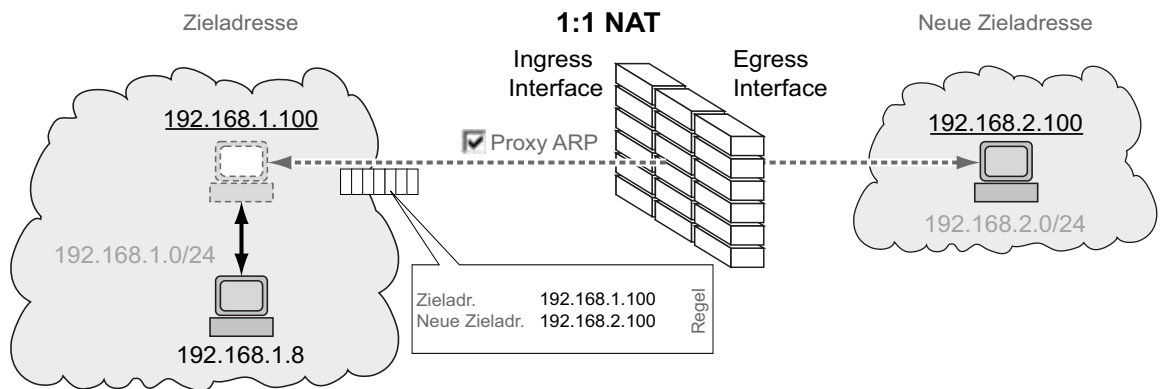








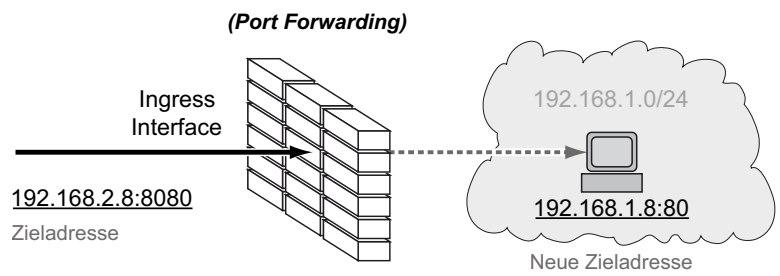
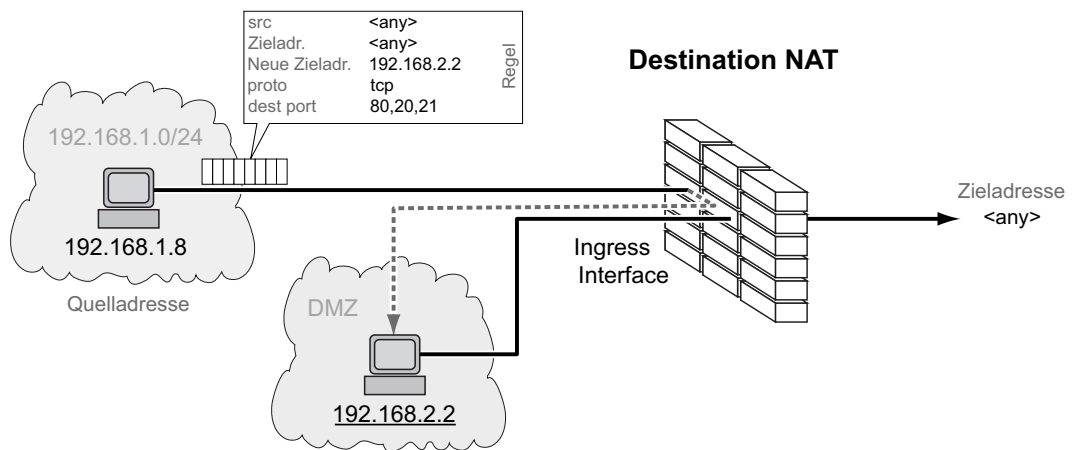






-






---



---



---



---



---



Blue vertical bar

Blue vertical bar

Blue vertical bar

Blue vertical bar

⌘+

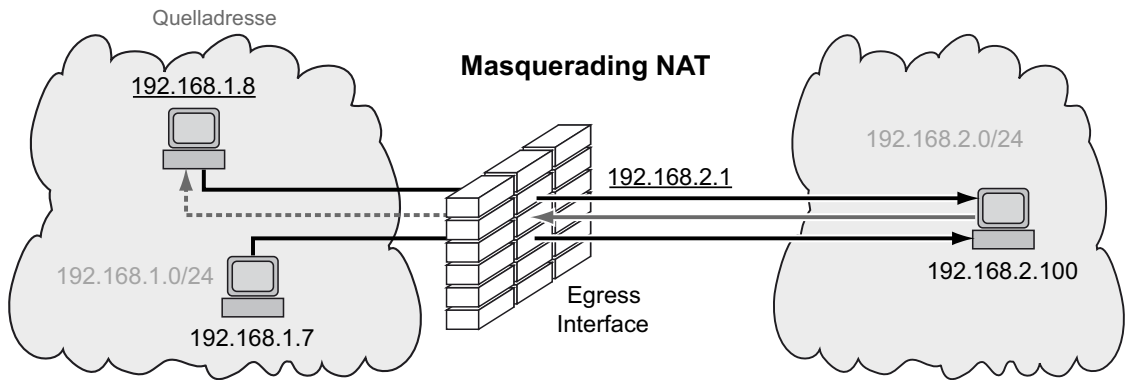
.

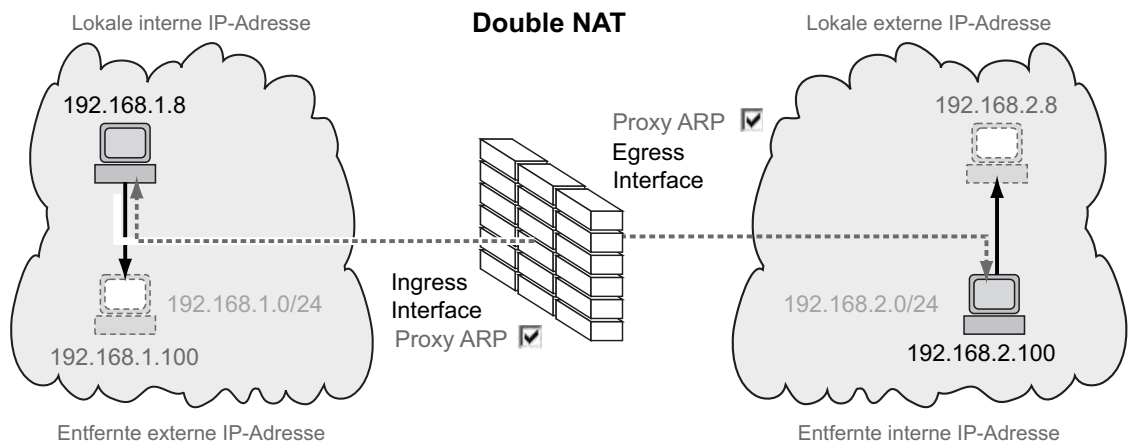
.

✓

✓

✓







Blue bar

✓

-

Blue bar

⊞  
+

-

Blue bar

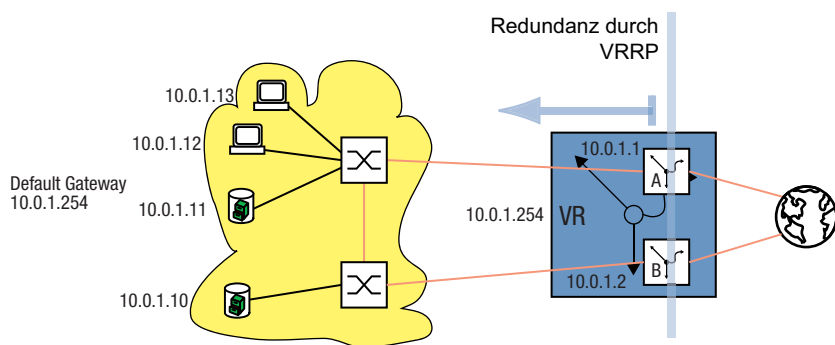
✓

Blue bar

✓

-





---

00:00:5e:00:01:xx

Variable Bestandteil = VRID  
Fester Bestandteil

---

---

---

---

-

-

-

-

-

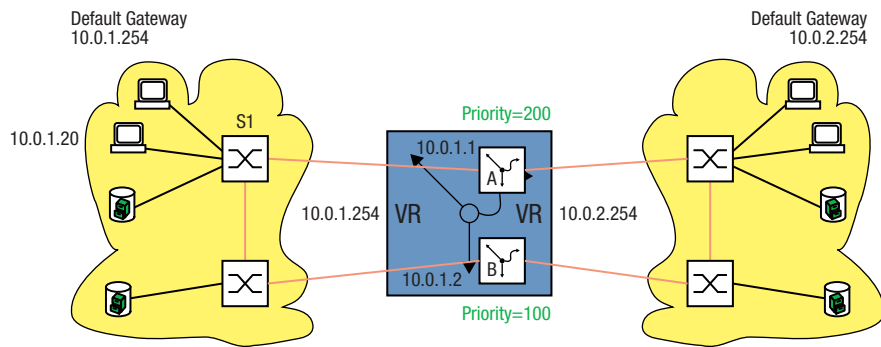
-

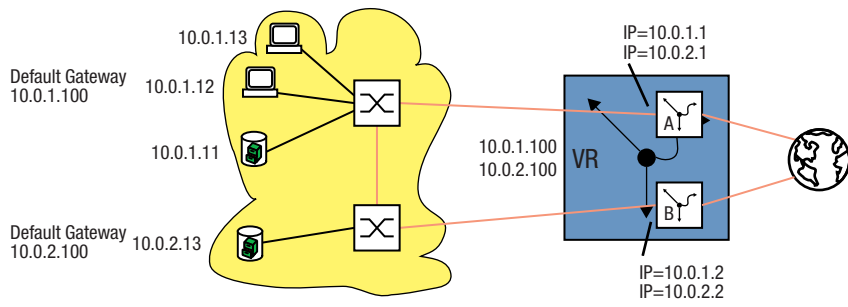
-

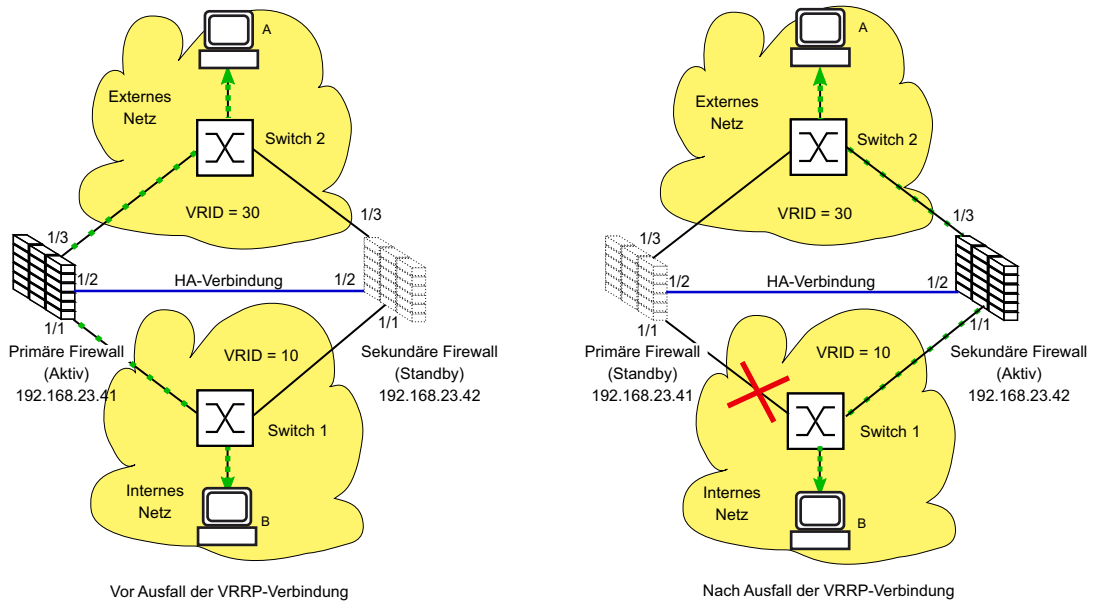


-

-







◀ ■ ■ ■ ▶ Datenpaketfluss zwischen den Netzwerken





-

-

-

-

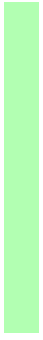


-  
✓  
✓



-  
-







-

-

-

-

-

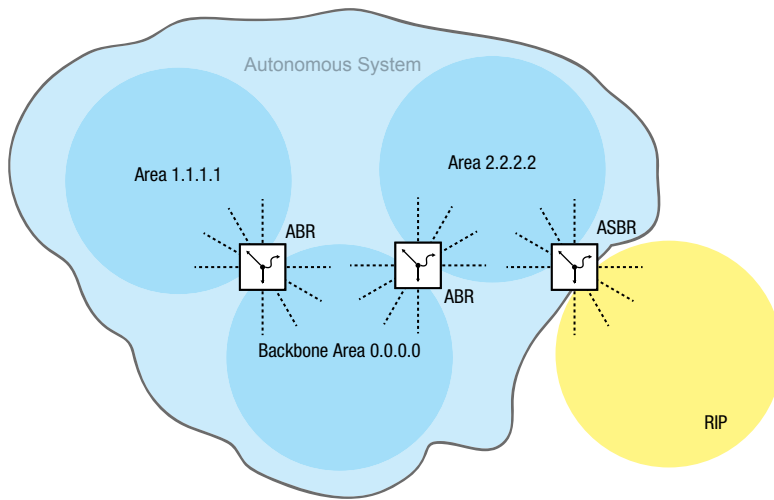


-



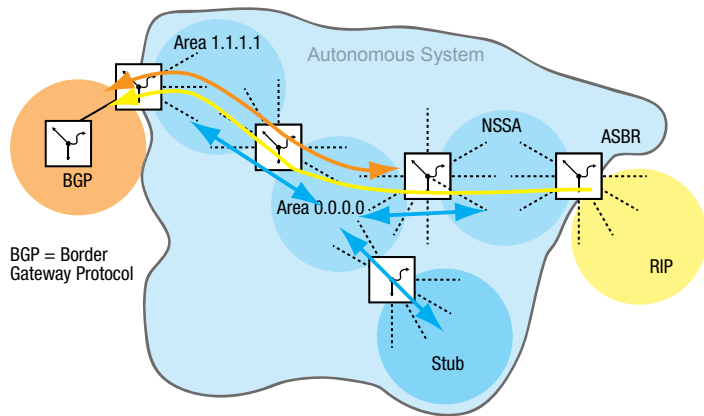
-

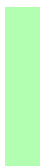
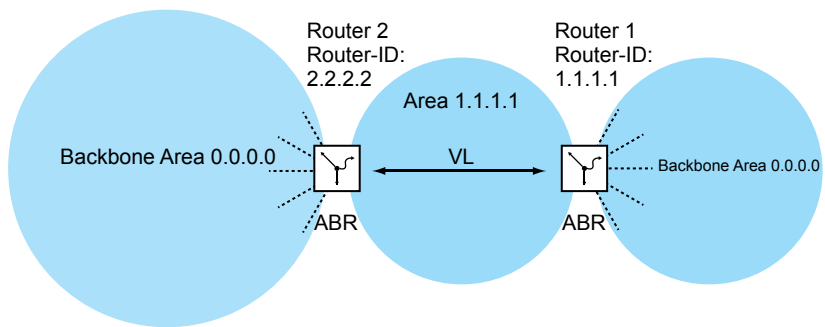
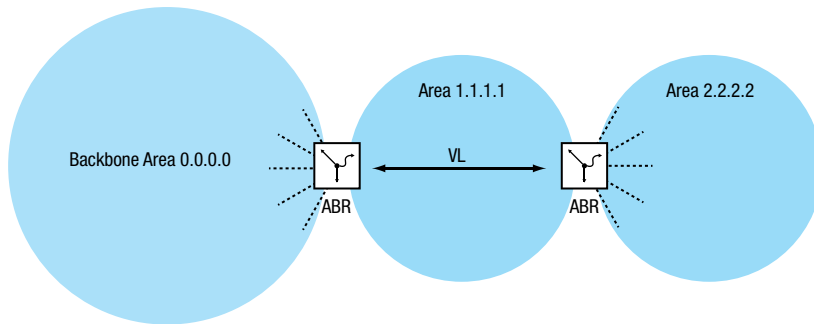






-







-

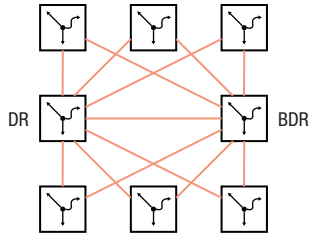
-

---

-

-

-





---

---

---

---

---

---

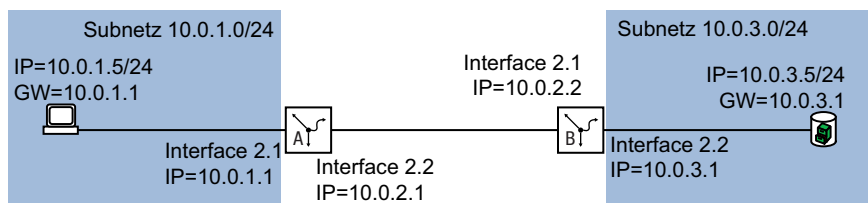
---

---

---

-  
-  
-  
-  
-





---

-



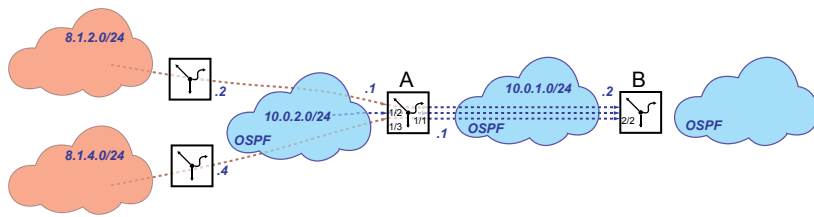
-

-

-

-





1

2

3

4

5

-

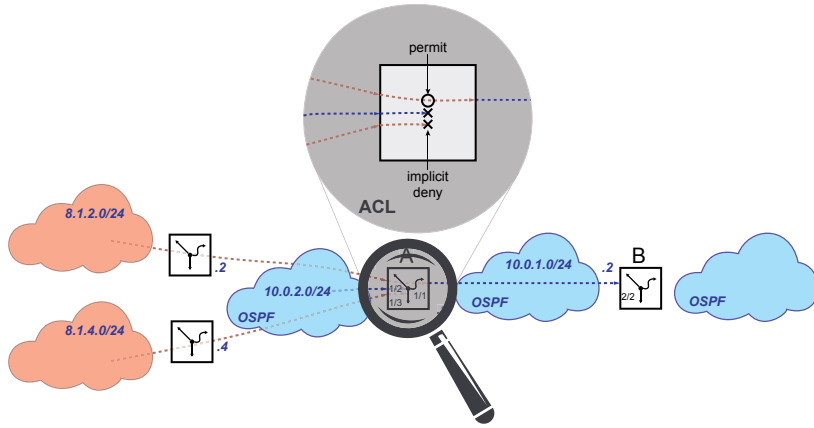
-

-

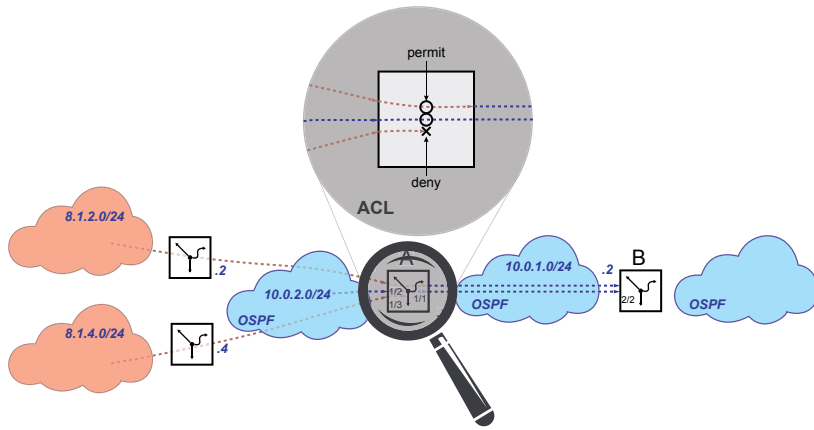
-

-







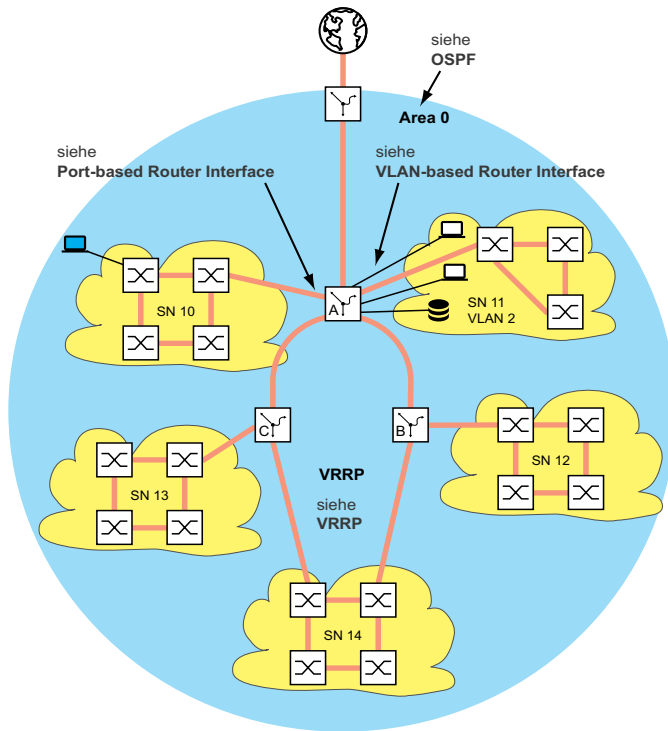


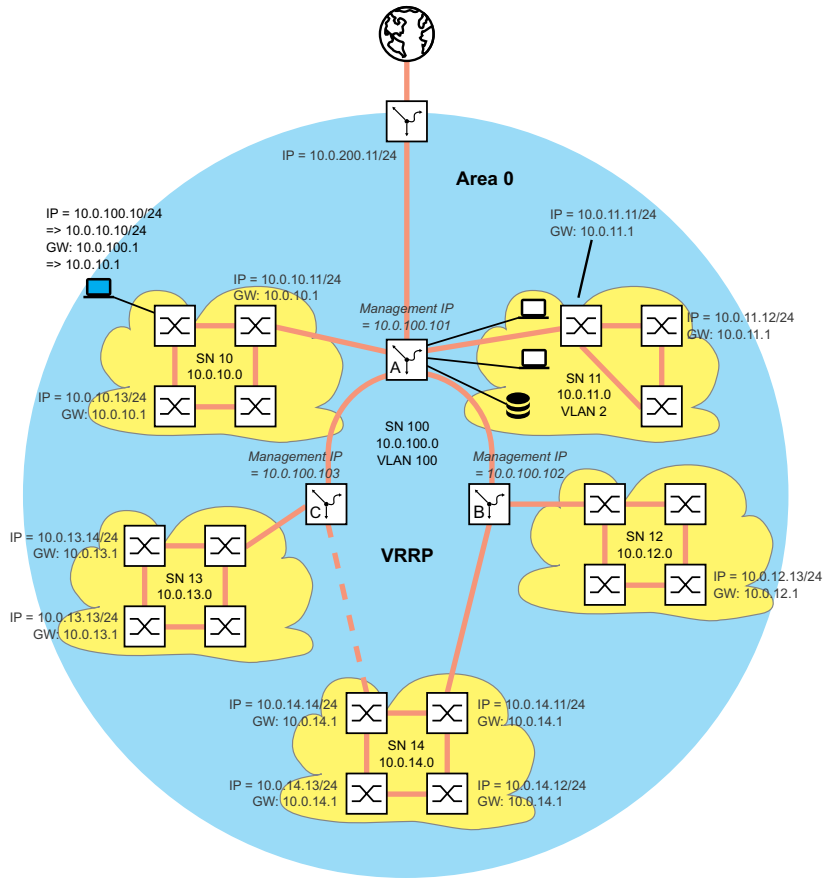


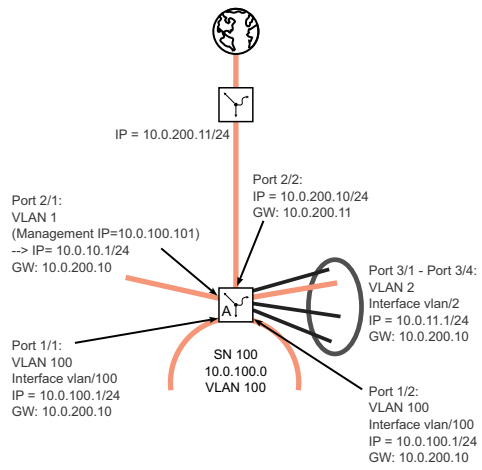




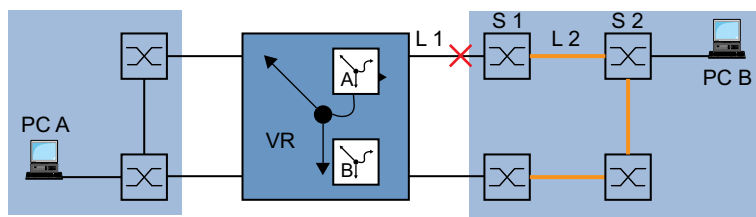






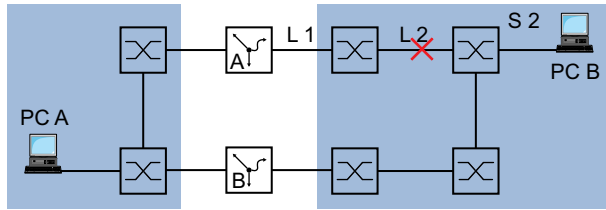








-





-

---

-

---

---



⌘  
+



✓

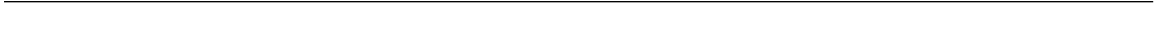
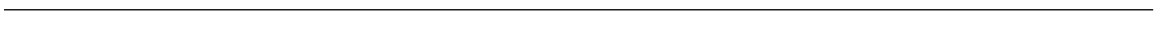
-

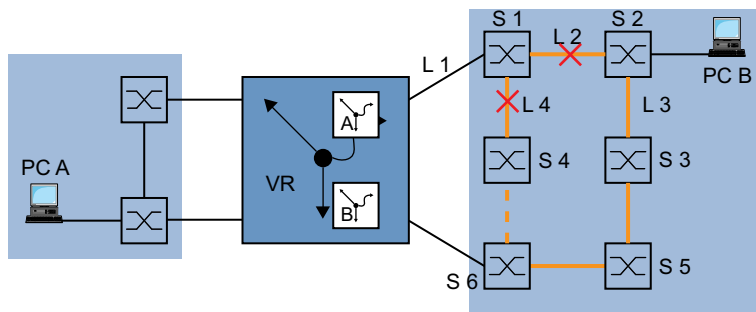


B+



.

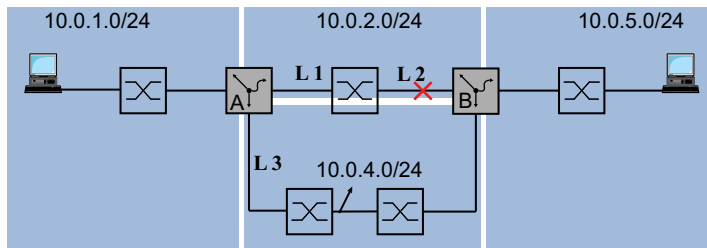




⊞  
+







\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

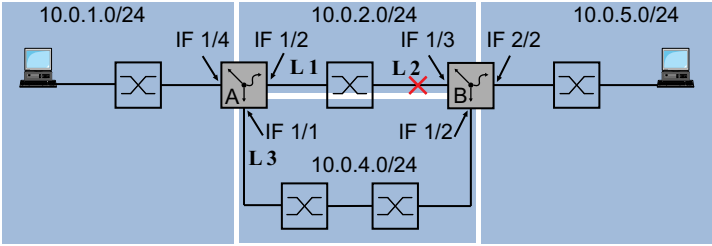
\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_



⊞  
+

⊞  
+





B+

B+



-











-

-

-



⌘ +



-

---

-  
-

-

-  
-

-

---

-

-

---





-



-



-







-



-



-

-



-

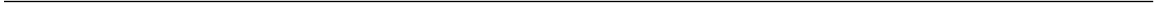


-



-







-

-

-



-







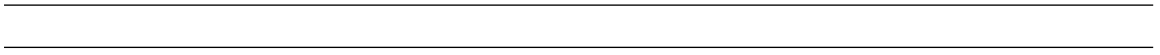
-

-

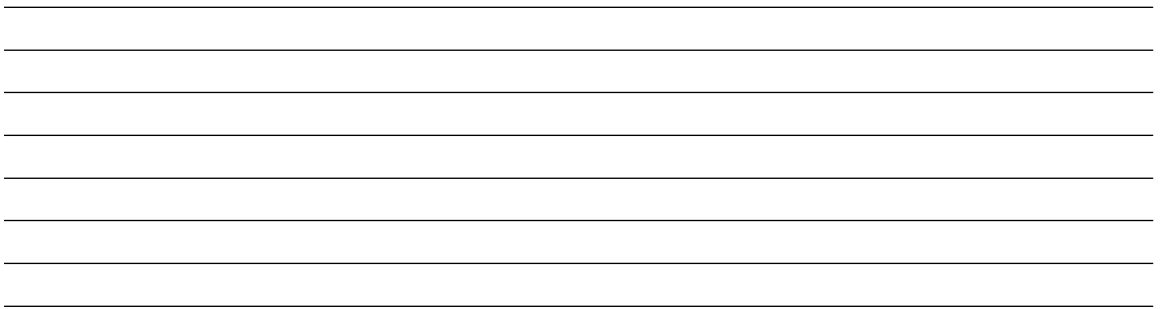
-



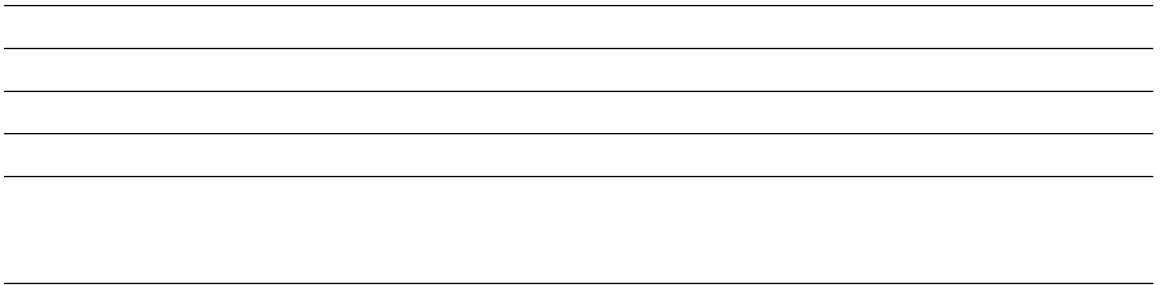
-



-



-





-

-

-

-







-

-

-



---

---

---



B+



.



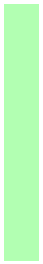
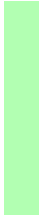


-  
-



-  
-









田+





-

-



-

-

-




---

---

---

---

---

---

---

---

---

---

-  
-  
-


-




-







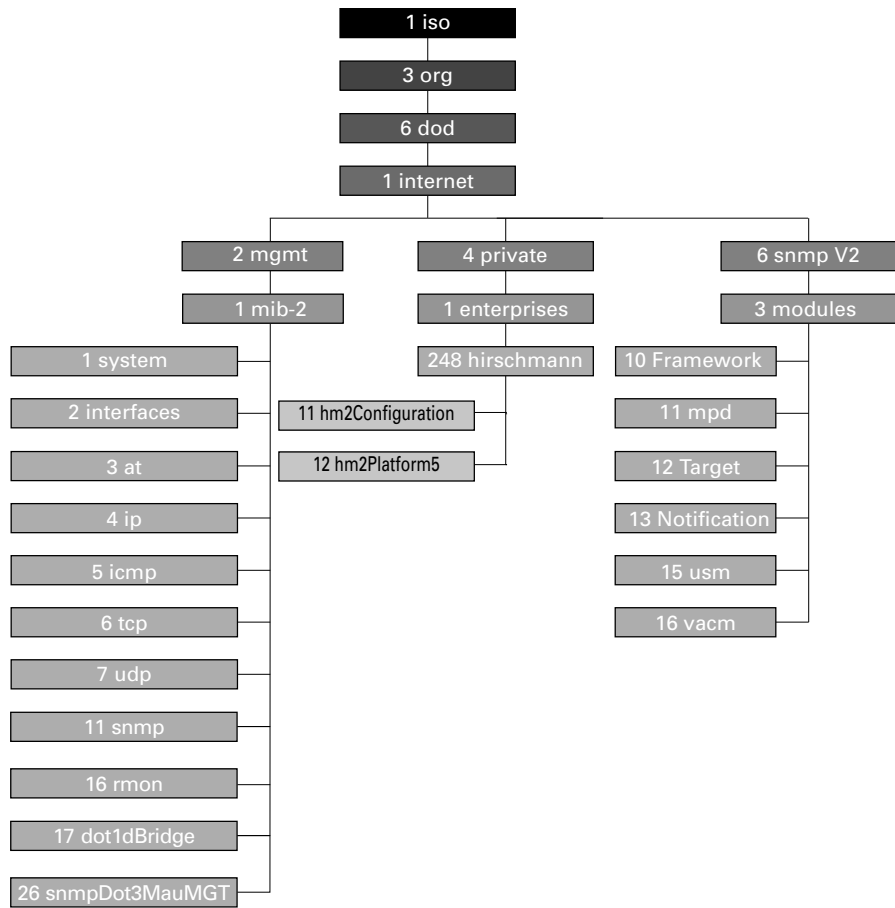
















-

-

---

---

---

---

---

---

---

---

-

-



\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

---

---

---

---

---

---

---

---

---

---











-

-





-



-

-



\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_





**HIRSCHMANN**

---

A **BELDEN** BRAND