345139

ADMINISTRATOR-HANDBUCH

Administratorhandbuch für Stackable Managed Switches der Serie 500 von Cisco Small Business

Inhaltsverzeichnis

Kapitel 30: SNMP 599

2

Erste Schritte

In diesem Abschnitt erhalten Sie eine Einführung in das webbasierte Konfigurationsdienstprogramm. Die folgenden Themen werden behandelt:

- **Starten des webbasierten Konfigurationsdienstprogramms**
- **Kurzanleitung für die Gerätekonfiguration**
- **Benennungskonventionen für Schnittstellen**
- **Unterschiede zwischen 500-Geräten**
- **Fensternavigation**

Starten des webbasierten Konfigurationsdienstprogramms

In diesem Abschnitt wird beschrieben, wie Sie durch das webbasierte Switch-Konfigurationsdienstprogramm navigieren.

Wenn Sie einen Popup-Blocker verwenden, stellen Sie sicher, dass dieser deaktiviert ist.

Browser-Einschränkungen

Wenn die Verwaltungsstation über mehrere IPv6-Schnittstellen verfügt, verwenden Sie die globale IPv6-Adresse anstelle der IPv6-Link Local-Adresse, um über den Browser auf das Gerät zuzugreifen.

Starten des Konfigurationsdienstprogramms

So öffnen Sie das webbasierte Konfigurationsdienstprogramm:

SCHRITT 1 Öffnen Sie einen Webbrowser.

SCHRITT 2 Geben Sie die IP-Adresse des zu konfigurierenden Geräts in die Adresszeile des Browsers ein und drücken Sie die **Eingabetaste**.

HINWEIS Wenn das Gerät die werkseitig konfigurierte Standard-IP-Adresse 192.168.1.254 verwendet, blinkt die Betriebs-LED ununterbrochen. Wenn das Gerät eine vom DHCP-Server zugewiesene oder vom Administrator konfigurierte statische IP-Adresse verwendet, leuchtet die Betriebs-LED ständig.

Anmelden

Der Standardbenutzername lautet **cisco**, das Standardkennwort **cisco**. Wenn Sie sich das erste Mal mit dem Standardbenutzernamen und dem Standardkennwort anmelden, werden Sie aufgefordert, ein neues Kennwort einzugeben.

HINWEIS Wenn Sie noch keine Sprache für die grafische Benutzeroberfläche ausgewählt haben, wird die Sprache der Anmeldeseite durch die Sprachen bestimmt, die vom Browser angefordert werden bzw. die im Gerät konfiguriert sind. Wenn der Browser beispielsweise Chinesisch anfordert und Chinesisch im Gerät geladen ist, wird die Anmeldeseite automatisch auf Chinesisch angezeigt. Wenn Chinesisch im Gerät nicht geladen ist, wird die Anmeldeseite auf Englisch angezeigt.

Die im Gerät geladenen Sprachen haben einen Sprach- und Ländercode (en-US, en-GB usw.). Wenn die Anmeldeseite abhängig von der Browseranforderung automatisch in einer bestimmten Sprache angezeigt werden soll, müssen Sprach- und Ländercode der Browseranforderung mit der im Gerät geladenen Sprache übereinstimmen. Wenn die Browseranforderung nur den Sprachcode ohne Ländercode enthält (beispielsweise fr), wird die erste eingebettete Sprache mit übereinstimmendem Sprachcode verwendet (ohne Übereinstimmung mit dem Ländercode, beispielsweise fr_CA).

So melden Sie sich beim Gerätekonfigurations-Dienstprogramm an:

SCHRITT 1 Geben Sie den Benutzernamen/das Kennwort ein. Das Kennwort kann bis zu 64 ASCII-Zeichen lang sein. Die Regeln für die Kennwortkomplexität werden unter **Einrichten der Kennwortkomplexitätsregeln** beschrieben.

SCHRITT 2 Wenn Sie nicht Englisch als Sprache verwenden, wählen Sie im Dropdown-Menü *Sprache* die gewünschte Sprache aus. Im Abschnitt **Firmware/Sprache aktualisieren/sichern** erfahren Sie, wie Sie eine neue Sprache für das Gerät hinzufügen oder eine aktuelle Sprache aktualisieren.

SCHRITT 3 Wenn Sie sich zum ersten Mal mit der Standard-Benutzer-ID (**cisco**) und dem Standardkennwort (**cisco**) anmelden oder Ihr Kennwort abgelaufen ist, wird die Seite Kennwort ändern geöffnet. Weitere Informationen finden Sie unter **Kennwort-Ablaufzeit**.

SCHRITT 4 Wählen Sie aus, ob die **Erzwingung der Kennwortkomplexität** deaktiviert werden soll. Weitere Informationen zur Kennwortkomplexität finden Sie in Abschnitt **Einrichten der Kennwortkomplexitätsregeln**.

SCHRITT 5 Geben Sie das neue Kennwort ein und klicken Sie auf **Übernehmen**.

Nach erfolgreicher Anmeldung wird die Seite *Erste Schritte* geöffnet.

Wenn Sie einen falschen Benutzernamen oder ein falsches Kennwort eingegeben haben, wird eine Fehlermeldung angezeigt und im Fenster wird weiterhin die Anmeldeseite angezeigt. Wenn bei der Anmeldung Probleme auftreten, finden Sie weitere Informationen im Administratorhandbuch unter **Starten des Konfigurationsdienstprogramms**.

Aktivieren Sie das Kontrollkästchen **Diese Seite beim Starten nicht anzeigen**, um zu verhindern, dass die Seite Erste Schritte bei jeder Systemanmeldung angezeigt wird. Wenn Sie diese Option aktivieren, wird anstelle der Seite Erste Schritte die Seite Systemübersicht angezeigt.

HTTP/HTTPS

Sie können eine (nicht sichere) HTTP-Sitzung öffnen, indem Sie auf **Anmelden** klicken, oder Sie können eine (sichere) HTTPS-Sitzung öffnen, indem Sie auf **Sicheres Surfen (HTTPS)** klicken. Sie werden aufgefordert, die Anmeldung mit einem Standard-RSA-Schlüssel zu genehmigen. Anschließend wird eine HTTPS-Sitzung geöffnet.

HINWEIS Sie müssen den Benutzernamen/das Kennwort erst eingeben, wenn Sie auf die Schaltfläche **Sicheres Surfen (HTTPS)** geklickt haben**.**

Informationen zum Konfigurieren von HTTPS finden Sie unter **SSL-Server**.

Kennwort-Ablaufzeit

Die Seite „Neues Kennwort“ wird in folgenden Fällen angezeigt:

- Wenn Sie sich beim Gerät zum ersten Mal mit dem Standardbenutzernamen **cisco** und Standardkennwort **cisco** anmelden. Sie müssen auf dieser Seite das werkseitig festgelegte Standardkennwort ändern.
- Wenn das Kennwort abläuft, werden Sie auf dieser Seite gezwungen, ein neues Kennwort festzulegen.

Abmelden

Standardmäßig meldet sich die Anwendung nach zehn Minuten ohne Aktivität ab. Sie können den Standardwert ändern, wie im Abschnitt **Definieren des Timeouts für Sitzungsleerlauf** beschrieben.

VORSICHT Wenn die ausgeführte Konfiguration nicht in die Startkonfiguration kopiert wird, gehen beim Neustart des Geräts alle Änderungen seit dem letzten Speichern der Datei verloren. Speichern Sie vor dem Abmelden die aktuelle Konfiguration als Startkonfiguration, um alle während der aktuellen Sitzung vorgenommenen Änderungen zu speichern.

Auf der linken Seite des Anwendungslinks **Speichern** wird ein blinkendes rotes X angezeigt, um darauf hinzuweisen, dass Änderungen an der aktuellen Konfiguration noch nicht in der Startkonfigurationsdatei gespeichert wurden. Sie können das Blinken deaktivieren, indem Sie auf der Seite „Konfiguration kopieren/speichern“ auf die Schaltfläche **Blinkendes Speichersymbol deaktivieren** klicken.

Wenn das Gerät automatisch ein Gerät erkennt, beispielsweise ein IP-Telefon (siehe **Was ist ein Smartport?**), konfiguriert es den Port entsprechend für das Gerät. Diese Konfigurationsbefehle werden in die aktuelle Konfigurationsdatei geschrieben. Aus diesem Grund beginnt das Speichersymbol bei der Anmeldung zu blinken, auch wenn Sie keine Konfigurationsänderungen vorgenommen haben.

Wenn Sie auf **Speichern** klicken, wird die Seite „Konfiguration kopieren/speichern“ angezeigt. Speichern Sie die ausgeführte Konfiguration, indem Sie diese in die Startkonfigurationsdatei kopieren. Nach dem Speichervorgang werden das rote X und der Link zum Speichern nicht mehr angezeigt.

Um sich abzumelden, klicken Sie in der oberen rechten Ecke einer beliebigen Seite auf **Abmelden**. Das System meldet sich beim Gerät ab.

Wenn ein Timeout auftritt oder Sie sich absichtlich beim System abmelden, wird eine Nachricht angezeigt und die Seite „Anmeldung“ mit dem Hinweis geöffnet, dass Sie abgemeldet sind. Nach dem Anmelden öffnet die Anwendung wieder die Anfangsseite.

Welche Seite am Anfang angezeigt wird, hängt von der Option „Diese Seite beim Starten nicht anzeigen“ auf der Seite Erste Schritte ab. Wenn Sie diese Option nicht aktiviert haben, ist die Anfangsseite die Seite *Erste Schritte.* Wenn Sie diese Option aktiviert haben, ist die Seite Systemübersicht die Anfangsseite.

Kurzanleitung für die Gerätekonfiguration

Um die Gerätekonfiguration zu vereinfachen, enthält die Seite *Erste Schritte* Links zu den am häufigsten verwendeten Seiten.

Kategorie	Link-Name (auf der Seite)	Verlinkte Seite
Ersteinrichtung	Systemmodus und Stack-Verwaltung ändern	Seite Systemmodus und Stack-Verwaltung
	Verwaltungsanwendungen und -services ändern	Seite TCP/UDP-Services
	Geräte-IP-Adresse ändern	Seite IPv4-Schnittstelle
	VLAN erstellen	Seite VLAN erstellen
	Porteinstellungen konfigurieren	Seite Port-Einstellungen
Gerätestatus	Systemübersicht	Seite Systemübersicht
	Anschlussstatistik	Seite Schnittstelle
	RMON-Statistik	Seite Statistik
	Protokoll anzeigen	Seite RAM-Speicher
Schnellzugriff	Gerätekennwort ändern	Seite Benutzerkonten
	Gerätesoftware aktualisieren	Seite Firmware/Sprache aktualisieren/sichern
	Gerätekonfiguration sichern	Seite Konfiguration/Protokoll herunterladen/sichern
	MAC-basierte ACL erstellen	Seite MAC-basierte ACL
	IP-basierte ACL erstellen	Seite IPv4-basierte ACL
	QoS konfigurieren	Seite QoS-Eigenschaften
	Portspiegelung konfigurieren	Seite Port- und VLAN-Spiegelung

Die Seite „Erste Schritte“ enthält zwei Hotlinks, über die Sie zu Cisco-Webseiten gelangen, auf denen Sie weitere Informationen finden. Wenn Sie auf den Link **Support** klicken, gelangen Sie zur Supportseite für das Gerät, und wenn Sie auf den Link **Foren** klicken, gelangen Sie zur Seite der Small Business Support Community.

Benennungskonventionen für Schnittstellen

Auf der grafischen Benutzeroberfläche werden die Schnittstellen durch Verketten der folgenden Elemente angegeben:

- **Schnittstellentyp:** Die verschiedenen Gerätetypen verfügen über die folgenden Schnittstellentypen:
  - **Fast Ethernet (10/100 Bit)**: Für diese wird **FE** angezeigt.
  - **Gigabit Ethernet-Ports (10/100/1000 Bit)**: Für diese wird **GE** angezeigt.
  - **10 Gigabit Ethernet-Ports (10.000 Bits)**: Diese werden als **XG** angezeigt.
  - **LAG (Port-Channel)**: Für diese wird **LAG** angezeigt.
  - **VLAN**: Für diese wird **VLAN** angezeigt.
  - **Tunnel**: Für diese wird **Tunnel** angezeigt.
- **Einheitennummer**: Anzahl der Einheit im Stack. Bei eigenständigen Modi ist dies immer 1.
- **Slot-Nummer**: Die Slot-Nummer ist entweder 1 oder 2.
- **Schnittstellennummer: Port, LAG Tunnel oder VLAN-ID**

Unterschiede zwischen 500-Geräten

Dieses Handbuch ist für Geräte des Typs Sx500, SG500X, SG500XG und ESW2-550X relevant. Wenn eine Funktion nur auf eines der Geräte zutrifft, wird darauf hingewiesen.

Nachfolgend werden die Unterschiede zwischen den Geräten zusammengefasst:

- Die RIP- und VRRP-Funktionen werden nur auf den Geräten SG500X, SG500XG und ESW2-550X unterstützt, die im Standalone-Modus und im erweiterten Hybrid-Stack auf den Geräten SG500X und Sx500 ausgeführt werden. Weitere Details finden Sie unter **Administration: Stack-Verwaltung**.
- TCAM-Größe, siehe **TCAM-Auslastung**.
- Die Geräte verfügen über unterschiedliche Stack-Ports. Weitere Informationen hierzu finden Sie unter **Standardports für Stacks und Netzwerk**.
- Die je nach Kabeltyp verfügbaren Portgeschwindigkeiten unterscheiden sich bei diesen Geräten. Weitere Informationen hierzu finden Sie unter **Kabeltypen**.

- IPv4-Routing wird bei den Gerätetypen auf verschiedene Weise aktiviert:
  - **SG500XSG500XG/ESW2-550X**: IPv4-Routing muss auf der Seite „IPv4-Schnittstelle“ aktiviert werden.
  - **Sx500**: Wenn das Gerät vom Schicht-2-Systemmodus auf den Schicht-3-Systemmodus umgeschaltet wird, wird IPv4-Routing automatisch aktiviert.

Fensternavigation

In diesem Abschnitt werden die Funktionen des webbasiertes Switch-Konfigurationsdienstprogramms beschrieben.

Anwendungsheader

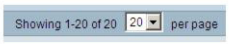
Der Anwendungsheader wird auf jeder Seite angezeigt. Er bietet die folgenden Anwendungslinks:

Anwendungslink-Name	Beschreibung
	Auf der linken Seite des Anwendungslinks **Speichern** wird ein blinkendes rotes X angezeigt, um darauf hinzuweisen, dass Änderungen durchgeführt wurden, die Sie noch nicht in der Startkonfiguration gespeichert haben. Sie können das Blinken des roten X auf der Seite *Konfiguration kopieren/speichern* deaktivieren. Klicken Sie auf **Speichern**, um die Seite Konfiguration kopieren/speichern anzuzeigen. Speichern Sie die aktuelle Konfigurationsdatei, indem Sie sie in die Startkonfigurationsdatei des Geräts kopieren. Nach dem Speichervorgang werden das rote X und der Link zum Speichern nicht mehr angezeigt. Beim Neustart des Geräts wird der Startkonfigurationsdateityp in die aktuelle Konfiguration kopiert und die Geräteparameter werden entsprechend den Daten in der aktuellen Konfiguration festgelegt.
Benutzername	Zeigt den Namen des beim Gerät angemeldeten Benutzers an. Der Standardbenutzername lautet **cisco**. (Das Standardkennwort lautet **cisco**).

Anwendungslink-Name	Beschreibung
Sprachmenü	Das Menü enthält die folgenden Optionen: ▪ **Sprache auswählen:** Wählen Sie eine der im Menü angezeigten Sprachen aus. Diese Sprache wird für das webbasierte Konfigurationsdienstprogramm verwendet. ▪ **Sprache herunterladen:** Fügt dem Gerät eine neue Sprache hinzu. ▪ **Sprache löschen:** Löscht die zweite Sprache aus dem Gerät. Die erste Sprache (Englisch) kann nicht gelöscht werden. ▪ **Debugging:** Wird zu Übersetzungszwecken verwendet. Wenn Sie diese Option auswählen, verschwinden alle Beschriftungen des webbasierten Konfigurationsdienstprogramms. An ihrer Stelle werden die IDs der Zeichenfolgen angezeigt, die den IDs in der Sprachdatei entsprechen. **HINWEIS** Verwenden Sie zum Aktualisieren einer Sprachdatei die Seite Firmware/Sprache aktualisieren/sichern.
Abmeldung	Klicken Sie auf diese Schaltfläche, um sich vom webbasiertes Switch-Konfigurationsdienstprogramm abzumelden.
Info	Zeigt den Namen und die Versionsnummer des Geräts an.
Hilfe	Zeigt die Online-Hilfe an.
	Das Symbol für den SYSLOG-Alarmstatus wird angezeigt, wenn eine SYSLOG-Meldung mit einem höheren Schweregrad als *Kritisch* protokolliert wird. Klicken Sie auf das Symbol, um die Seite RAM-Speicher zu öffnen. Nachdem Sie auf diese Seite zugegriffen haben, wird das Symbol für den Syslog-Alarmstatus nicht mehr angezeigt. Um die Seite anzuzeigen, ohne dass eine aktive Syslog-Nachricht vorliegt, klicken Sie auf **Status und Statistik** > **Protokoll anzeigen** > **RAM-Speicher**.

Verwaltungsschaltflächen

In der folgenden Tabelle werden die am häufigsten verwendeten Schaltflächen beschrieben, die auf den verschiedenen Seiten des Systems zur Verfügung stehen.

Schaltflächenname	Beschreibung
	Verwenden Sie das Pulldown-Menü, um die Anzahl der Einträge pro Seite zu konfigurieren.
	Zeigt ein obligatorisches Feld an.
Hinzufügen	Klicken Sie auf diese Schaltfläche, um die verbundene Seite Hinzufügen anzuzeigen und der Tabelle einen Eintrag hinzuzufügen. Geben Sie die Informationen ein, und klicken Sie auf **Übernehmen**, um sie in der ausgeführten Konfiguration zu speichern. Klicken Sie auf **Schließen**, um zur Hauptseite zurückzukehren. Klicken Sie auf **Speichern**, um die Seite Konfiguration kopieren/speichern anzuzeigen und die aktuelle Konfiguration im Startkonfigurationsdateityp des Geräts zu speichern.
Übernehmen	Klicken Sie auf diese Schaltfläche, um Änderungen in die aktuelle Konfiguration des Geräts zu übernehmen. Wird das Gerät neu gestartet, geht die aktuelle Konfiguration verloren, es sei denn, sie wird im Startkonfigurationsdateityp oder einem anderen Dateityp gespeichert. Klicken Sie auf **Speichern**, um die Seite Konfiguration kopieren/speichern anzuzeigen und die aktuelle Konfiguration im Startkonfigurationsdateityp des Geräts zu speichern.
Abbrechen	Klicken Sie auf diese Schaltfläche, um die auf der Seite durchgeführten Änderungen zu verwerfen.
Alle Schnittstellenzähler löschen	Klicken Sie auf diese Schaltfläche, um die Statistikzähler für alle Schnittstellen zu löschen.
Schnittstellenzähler löschen	Klicken Sie auf diese Schaltfläche, um die Statistikzähler für die ausgewählte Schnittstelle zu löschen.
Protokolle löschen	Löscht die Protokolldateien.
Tabelle löschen	Entfernt die Tabelleneinträge.

Schaltflächenname	Beschreibung
Schließen	Ruft die Hauptseite auf. Wenn Änderungen vorhanden sind, die nicht in die aktuelle Konfiguration übernommen wurden, wird eine Meldung angezeigt.
Einstellungen kopieren	Eine Tabelle enthält normalerweise einen oder mehrere Einträge mit Konfigurationseinstellungen. Anstatt jeden Eintrag einzeln zu ändern, können Sie einen Eintrag ändern und dann den ausgewählten Eintrag wie folgt in mehrere Einträge kopieren: 1. Wählen Sie den zu kopierenden Eintrag aus. Klicken Sie auf **Einstellungen kopieren**, um das Popup-Menü anzuzeigen. 2. Geben Sie in das Feld **nach** die Nummern der Zieleinträge ein. 3. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern. Klicken Sie auf **Schließen**, um zur Hauptseite zurückzukehren.
Entfernen	Wenn Sie einen Eintrag in der Tabelle ausgewählt haben, klicken Sie auf **Löschen**, um den Eintrag zu entfernen.
Details	Klicken Sie auf diese Schaltfläche, um Details zu dem ausgewählten Eintrag anzuzeigen.
Bearbeiten	Wählen Sie den Eintrag aus, und klicken Sie auf **Bearbeiten**. Die Seite Bearbeiten wird geöffnet, auf der Sie den Eintrag ändern können. 1. Klicken Sie auf **Übernehmen**, um die Änderungen in der aktuellen Konfiguration zu speichern. 2. Klicken Sie auf **Schließen**, um zur Hauptseite zurückzukehren.
Los	Geben Sie die Abfrage-Filterkriterien ein, und klicken Sie auf **Los**. Die Ergebnisse werden auf der Seite angezeigt.
Aktualisieren	Klicken Sie zum Aktualisieren der Zählerwerte auf **Aktualisieren**.
Testen	Klicken Sie auf **Testen**, um die entsprechenden Tests auszuführen.

3

Status und Statistik

In diesem Abschnitt wird beschrieben, wie Sie Gerätestatistiken anzeigen.

Die folgenden Themen werden behandelt:

- **Systemübersicht**
- **Ethernet-Schnittstellen**
- **Etherlike-Statistik**
- **GVRP-Statistik**
- **802.1X EAP-Statistik**
- **ACL-Statistik**
- **TCAM-Auslastung**
- **Integrität**
- **RMON**
- **Protokoll anzeigen**

Systemübersicht

Weitere Informationen hierzu finden Sie unter **Systemeinstellungen**.

Ethernet-Schnittstellen

Auf der Seite *Schnittstelle* werden Verkehrsstatistiken für jeden Port angezeigt. Sie können die Aktualisierungsrate für die Informationen auswählen.

Diese Seite ist nützlich, um den Umfang des gesendeten und empfangenen Verkehrs und die Übertragungsart (Unicast, Multicast und Broadcast) zu analysieren.

So zeigen Sie die Ethernet-Statistik an und/oder legen die Aktualisierungsrate fest:

SCHRITT 1 Wählen Sie **Status und Statistik** > **Schnittstelle**.

SCHRITT 2 Geben Sie die Parameter ein.

- **Schnittstelle**: Wählen Sie den Schnittstellentyp und die bestimmte Schnittstelle aus, für die Sie die Ethernet-Statistik anzeigen möchten.
- **Aktualisierungsrate**: Legen Sie den Zeitraum fest, der bis zum Aktualisieren der Ethernet-Statistik für die Schnittstelle verstreichen soll.

Im Bereich „Statistik empfangen“ werden Informationen zu empfangenen Paketen angezeigt.

- **Byte insgesamt (Oktette)**: Die empfangenen Oktette, einschließlich fehlerhafter Pakete und FCS-Oktette jedoch ausschließlich Frame-Bits.
- **Unicast-Pakete**: Fehlerfrei empfangene Unicast-Pakete.
- **Multicast-Pakete**: Fehlerfrei empfangene Multicast-Pakete.
- **Broadcast-Pakete**: Fehlerfrei empfangene Broadcast-Pakete.
- **Pakete mit Fehlern**: Empfangene Pakete mit Fehlern.

Im Bereich „Übertragungsstatistik“ werden Informationen zu gesendeten Paketen angezeigt.

- **Byte insgesamt (Oktette)**: Die übertragenen Oktette, einschließlich fehlerhafter Pakete und FCS-Oktette jedoch ausschließlich Frame-Bits.
- **Unicast-Pakete**: Fehlerfrei übertragene Unicast-Pakete.
- **Multicast-Pakete**: Fehlerfrei übertragene Multicast-Pakete.
- **Broadcast-Pakete**: Fehlerfrei übertragene Broadcast-Pakete.

So löschen Sie Statistikzähler oder zeigen sie an:

- Klicken Sie auf **Schnittstellenzähler löschen**, um die Zähler für die angezeigte Schnittstelle zu löschen.
- Klicken Sie auf **Alle Statistikschnittstellen anzeigen**, um alle Ports auf einer Seite anzuzeigen.

Etherlike-Statistik

Auf der Seite *Etherlike* werden Statistiken nach Port gemäß den Definitionen des Etherlike MIB-Standards angezeigt. Sie können die Aktualisierungsrate für die Informationen auswählen. Diese Seite bietet ausführlichere Informationen zu Fehlern in der physischen Schicht (Schicht 1), die zu einer Unterbrechung des Verkehrs führen können.

So zeigen Sie die Etherlike-Statistik an und/oder legen die Aktualisierungsrate fest:

SCHRITT 1 Wählen Sie **Status und Statistik** > **Etherlike**.

SCHRITT 2 Geben Sie die Parameter ein.

- **Schnittstelle**: Wählen Sie den Schnittstellentyp und die bestimmte Schnittstelle aus, für die Sie die Ethernet-Statistik anzeigen möchten.
- **Aktualisierungsrate**: Legen Sie den Zeitraum fest, der bis zum Aktualisieren der Etherlike-Statistik verstreichen soll.

Es werden die Felder für die ausgewählte Schnittstelle angezeigt.

- **Fehler bei Frame-Prüfsequenz**: Empfangene Frames, die die zyklischen Redundanzprüfungen nicht bestanden haben.
- **Einzelkollisions-Frames**: Frames, die in eine einzelne Kollision involviert waren, jedoch erfolgreich übertragen wurden.
- **Verspätete Kollisionen**: Kollisionen, die nach den ersten 512 Datenbits erkannt wurden.
- **Übermäßige Kollisionen**: Die Anzahl der Übertragungen, die aufgrund von übermäßigen Kollisionen abgelehnt wurden.
- **Zu große Pakete**: Empfangene Pakete, die größer als 2000 Oktette sind.
- **Interne MAC-Empfangsfehler**: Infolge von Empfängerfehlern zurückgewiesene Frames.
- **Empfangene Pausen-Frames**: Empfangene Flusssteuerungs-Pausen-Frames.
- **Gesendete Pausen-Frames**: Von der ausgewählten Schnittstelle übertragene Flusssteuerungs-Pausen-Frames.

So löschen Sie Statistikzähler:

- Klicken Sie auf **Schnittstellenzähler löschen**, um die ausgewählten Schnittstellenzähler zu löschen.
- Klicken Sie auf **Alle Statistikschnittstellen anzeigen**, um alle Ports auf einer Seite anzuzeigen.

GVRP-Statistik

Auf der Seite *GVRP* werden Informationen zu Frames des GARP VLAN-Registrierungsprotokolls (GVRP) angezeigt, die von einem Port gesendet oder empfangen wurden. GVRP ist ein standardbasiertes Schicht-2-Netzwerkprotokoll für die automatische Konfiguration von VLAN-Informationen für Switches. Es ist in der Ergänzung 802.1ak des 802.1Q-2005 definiert.

Die GVRP-Statistik für einen Port wird nur angezeigt, wenn GVRP global und für den Port aktiviert ist. Weitere Informationen finden Sie auf der Seite GVRP.

So zeigen Sie die GVRP-Statistik an und/oder legen die Aktualisierungsrate fest:

SCHRITT 1 Wählen Sie **Status und Statistik** > **GVRP**.

SCHRITT 2 Geben Sie die Parameter ein.

- **Schnittstelle**: Wählen Sie die bestimmte Schnittstelle aus, für die Sie die GVRP-Statistik anzeigen möchten.
- **Aktualisierungsrate**: Legen Sie den Zeitraum fest, der bis zum Aktualisieren der GVRP-Statistik verstreichen soll.

Im Bereich „Attributzähler“ werden die Zähler für die unterschiedlichen Pakettypen pro Schnittstelle angezeigt.

- **Join Empty**: Die Zahl der empfangenen/übertragenen GVRP Join Empty-Pakete.
- **Empty**: Die Zahl der empfangenen/übertragenen GVRP Empty-Pakete.
- **Leave Empty**: Die Zahl der empfangenen/übertragenen GVRP Leave Empty-Pakete.
- **Join In**: Die Zahl der empfangenen/übertragenen GVRP Join In-Pakete.
- **Leave In**: Die Zahl der empfangenen/übertragenen GVRP Leave In-Pakete.
- **Leave All**: Die Zahl der empfangenen/übertragenen GVRP Leave All-Pakete.

Im Bereich „GVRP-Fehlerstatistik“ werden die GVRP-Fehlerzähler angezeigt.

- **Ungültige Protokoll-ID**: Fehler durch ungültige Protokoll-ID.
- **Ungültiger Attributtyp**: Fehler durch ungültigen Attributtyp.
- **Ungültiger Attributwert**: Fehler durch ungültigen Attributwert.
- **Ungültige Attributlänge**: Fehler durch ungültige Attributlänge.
- **Ungültiges Ereignis**: Ungültige Ereignisse.

So löschen Sie Statistikzähler:

- Klicken Sie auf **Schnittstellenzähler löschen**, um die ausgewählten Zähler zu löschen.
- Klicken Sie auf **Alle Statistikschnittstellen anzeigen**, um alle Ports auf einer Seite anzuzeigen.

802.1X EAP-Statistik

Auf der Seite *802.1x EAP* werden ausführliche Informationen zu EAP-Frames (Extensible Authentication Protocol) angezeigt, die gesendet oder empfangen wurden. Informationen zum Konfigurieren der 802.1X-Funktion finden Sie auf der Seite 802.1X-Eigenschaften.

So zeigen Sie die EAP-Statistik an und/oder legen die Aktualisierungsrate fest:

SCHRITT 1 Klicken Sie auf **Status und Statistik** > **802.1x EAP**.

SCHRITT 2 Wählen Sie die **Schnittstelle** aus, die für die Statistik abgefragt wird.

SCHRITT 3 Legen Sie die **Aktualisierungsrate** fest, d. h. den Zeitraum, der bis zum Aktualisieren der EAP-Statistik verstreichen soll.

Es werden die Werte für die ausgewählte Schnittstelle angezeigt.

- **Empfangene EAPOL-Frames**: Am Port empfangene gültige EAPOL-Frames.
- **Gesendete EAPOL-Frames**: Vom Port gesendete gültige EAPOL-Frames.
- **Empfangene EAPOL-Start-Frames**: Am Port empfangene EAPOL-Start-Frames.
- **Empfangene EAPOL-Logoff-Frames**: Am Port empfangene EAPOL-Logoff-Frames.
- **Empfangene EAP-Antwort-/ID-Frames**: Am Port empfangene EAP-Antwort-/ID-Frames.
- **Empfangene EAP-Antwort-Frames**: Am Port empfangene EAP-Antwort-Frames (keine Antwort-/ID-Frames).
- **Gesendete EAP-Anforderungs-/ID-Frames**: Vom Port gesendete EAP-Anforderungs-/ID-Frames.
- **Gesendete EAP-Anforderungs-Frames**: Vom Port gesendete EAP-Anforderungs-Frames.
- **Empfangene ungültige EAPOL-Frames**: An diesem Port empfangene und nicht erkannte EAPOL-Frames.
- **Empfangene EAP-Längenfehler-Frames**: An diesem Port empfangene EAPOL-Frames mit einer ungültigen Paketkörperlänge.

- **Letzte EAPOL-Frame-Version**: Nummer der Protokollversion, die an den zuletzt empfangenen EAPOL-Frame angehängt war.
- **Letzte EAPOL-Frame-Quelle**: MAC-Adresse der Quelle, die an den zuletzt empfangenen EAPOL-Frame angehängt war.

So löschen Sie Statistikzähler:

- Klicken Sie auf **Schnittstellenzähler löschen**, um die ausgewählten Schnittstellenzähler zu löschen.
- Klicken Sie auf **Aktualisieren**, um die ausgewählten Schnittstellenzähler zurückzusetzen.
- Klicken Sie auf **Alle Schnittstellenstatistiken anzeigen**, um die Zähler aller Schnittstellen zu löschen.

ACL-Statistik

Wenn die ACL-Protokollierungsfunktion aktiviert ist, wird für Pakete, die den ACL-Regeln entsprechen, eine SYSLOG-Nachricht zur Information generiert.

So zeigen Sie die Schnittstellen an, auf denen Pakete auf der Basis von ACLs weitergeleitet oder abgelehnt wurden:

SCHRITT 1 Klicken Sie auf **Status und Statistik** > **ACL**.

SCHRITT 2 Legen Sie die **Aktualisierungsrate** (Zeitraum in Sekunden) fest, die bis zum Aktualisieren der Statistiken verstreichen soll. Für jeden Zeitraum wird eine neue Gruppe von Schnittstellen erstellt.

Die Schnittstellen, auf denen Pakete auf der Basis von ACL-Regeln weitergeleitet oder abgelehnt wurden, werden angezeigt.

So verwalten Sie Statistikzähler:

- Klicken Sie auf **Aktualisieren**, um die Zähler zurückzusetzen.
- Klicken Sie auf **Zähler löschen**, um die Zähler sämtlicher Schnittstellen zu löschen.

TCAM-Auslastung

Die Gerätearchitektur nutzt einen TCAM-Speicher (Ternary Content Addressable Memory), um Paketaktionen mit Leitungsgeschwindigkeit zu ermöglichen.

Im TCAM sind die von Anwendungen erzeugten Regeln gespeichert, beispielsweise ACLs (Access Control Lists, Zugriffssteuerungslisten), QoS (Quality of Service), IP-Routing und von Benutzern erstellte Regeln.

Einige Anwendungen weisen bei ihrer Initiierung Regeln zu. Darüber hinaus verwenden Prozesse, die beim Systemstart initialisiert werden, einige ihrer Regeln während des Startvorgangs.

Um die TCAM-Auslastung anzuzeigen, wählen Sie **Status und Statistik** > **TCAM-Auslastung**.

Die folgenden Felder werden für SG500X/SG500XG-Geräte, für Sx500-Geräte im Schicht-3-Systemmodus und für Geräte, die Teil eines Stacks sind (pro Einheit), angezeigt:

- **Einheit Nr.**: Einheit in dem Stack, für den die TCAM-Auslastung angezeigt wird. Für Geräte im Standalone-Modus nicht angezeigt.
- **Max. Anzahl von TCAM-Einträgen für Routing und Multicast-Routing**: Maximale Anzahl der für Routing und Multicast-Routing verfügbaren TCAM-Einträge.
- **IPv4-Routing**
  - **Verwendet**: Anzahl der für das IPv4-Routing verwendeten TCAM-Einträge.
  - **Maximum**: Anzahl der verfügbaren TCAM-Einträge, die für das IPv4-Routing verwendet werden können.
- **IPv4-Multicast-Routing**
  - **Verwendet**: Anzahl der für das IPv4-Multicast-Routing verwendeten TCAM-Einträge.
  - **Maximum**: Anzahl der verfügbaren TCAM-Einträge, die für das IPv4-Multicast-Routing verwendet werden können.
- **IPv6-Routing**
  - **Verwendet**: Anzahl der für das IPv6-Multicast-Routing verwendeten TCAM-Einträge.
  - **Maximum**: Anzahl der verfügbaren TCAM-Einträge, die für das IPv6-Multicast-Routing verwendet werden können.
- **IPv6-Multicast-Routing**: Anzahl der für das IPv6-Routing verwendeten TCAM-Einträge.
  - **Verwendet**: Anzahl der für das IPv6-Routing verwendeten TCAM-Einträge.
  - **Maximum**: Anzahl der verfügbaren TCAM-Einträge, die für das IPv6-Routing verwendet werden können.

- **Max. Anzahl von TCAM-Einträgen für Nicht-IP-Regeln**: Für Nicht-IP-Regeln maximal verfügbare TCAM-Einträge.
- **Nicht-IP-Regeln**
  - **Verwendet**: Anzahl der für Nicht-IP-Regeln verwendeten TCAM-Einträge.
  - **Maximum**: Anzahl der verfügbaren TCAM-Einträge, die für Nicht-IP-Regeln verwendet werden können.

Informationen zum Ändern der Zuordnung verschiedener Prozesse (für die Serie 500) finden Sie im Abschnitt **Router-Ressourcen**.

Integrität

Weitere Informationen hierzu finden Sie unter **Integrität**.

RMON

Mit RMON (Remote Networking Monitoring) können SNMP-Agenten im Gerät für einen bestimmten Zeitraum eine Datenverkehrsstatistik proaktiv überwachen und Traps an einen SNMP-Manager senden. Der lokale SNMP-Agent vergleicht die aktuellen Echtzeitzähler mit vordefinierten Schwellenwerten und generiert Alarmmeldungen, ohne hierzu eine zentrale SNMP-Verwaltungsplattform abfragen zu müssen. Auf diese Weise stehen effektive und proaktive Verwaltungsmechanismen zur Verfügung, sofern Sie in Bezug auf die Basislinie Ihres Netzwerks die richtigen Schwellenwerte konfiguriert haben.

RMON verringert den Datenverkehr zwischen Manager und Gerät, da der SNMP-Manager nicht so häufig Informationen vom Gerät abfragen muss, weil das Gerät dem SNMP-Manager Ereignisse in Form von Statusberichten umgehend meldet.

Mit dieser Funktion können Sie die folgenden Aktionen ausführen:

- Sie können die aktuelle Statistik (ab dem Zeitpunkt der Löschung der Zählerwerte) anzeigen. Des Weiteren können Sie die Werte dieser Zähler über einen Zeitraum sammeln und die erfassten Daten in einer Tabelle anzeigen, wobei jeder gesammelte Datensatz eine einzelne Zeile in der *Verlaufstabelle* einnimmt.
- Sie können interessante Änderungen der Zählerwerte definieren, wie das Erreichen einer bestimmten Anzahl verspäteter Kollisionen (definiert den Alarm), und angeben, welche Aktion beim Eintreten dieses Ereignisses (Protokollieren, Trap oder Protokollieren und Trap) erfolgen soll.

RMON-Statistik

Auf der Seite *Statistik* werden ausführliche Informationen zu den Paketgrößen sowie Informationen zu Fehlern in der physischen Schicht angezeigt. Die Informationen werden entsprechend dem RMON-Standard angezeigt. Ein zu großes Paket ist definiert als Ethernet-Frame mit den folgenden Kriterien:

- Die Paketlänge ist größer als die MRU-Größe in Byte.
- Es wurde kein Kollisionsereignis erkannt.
- Es wurde kein verspätetes Kollisionsereignis erkannt.
- Es wurde kein Rx-Fehlerereignis (Empfangen) erkannt.
- Das Paket hat einen gültigen CRC.

So zeigen Sie die RMON-Statistik an und/oder legen die Aktualisierungsrate fest:

SCHRITT 1 Klicken Sie auf **Status und Statistik > RMON > Statistik**.

SCHRITT 2 Wählen Sie die **Schnittstelle** aus, für die Sie die Ethernet-Statistik anzeigen möchten.

SCHRITT 3 Legen Sie die **Aktualisierungsrate** fest, d. h. den Zeitraum, der bis zum Aktualisieren der Schnittstellenstatistik verstreichen soll.

Für die ausgewählte Schnittstelle werden die folgenden statistischen Daten angezeigt:

- **Empfangene Bytes**: Die empfangenen Oktette, einschließlich fehlerhafter Pakete und FCS-Oktette jedoch ausschließlich Frame-Bits.
- **Drop-Ereignisse**: Gelöschte Pakete.
- **Empfangene Pakete**: Die Zahl der fehlerfrei empfangenen Pakete, einschließlich Multicast- und Broadcast-Paketen.
- **Empfangene Broadcast-Pakete**: Fehlerfrei empfangene Broadcast-Pakete. Multicast-Pakete sind hier nicht enthalten.
- **Empfangene Multicast-Pakete**: Fehlerfrei empfangene Multicast-Pakete.
- **CRC- & Ausrichtungsfehler**: Die Zahl der aufgetretenen CRC- und Ausrichtungsfehler.
- **Zu kleine Pakete**: Die empfangenen Pakete mit unzureichender Größe (weniger als 64 Oktette).
- **Zu große Pakete**: Die empfangenen Pakete mit unzulässiger Größe (mehr als 2000 Oktette).
- **Fragmente**: Empfangene Fragmente (Pakete mit weniger als 64 Oktetten, ausschließlich Frame-Bits aber einschließlich FCS-Oktette).

- **Jabber**: Die Gesamtzahl der empfangenen Pakete mit einer Länge von mehr als 1632 Oktetten. In diesem Wert sind Frame-Bits nicht enthalten. Enthalten sind jedoch FCS-Oktette mit einer fehlerhaften FCS (Frame Check Sequence) und einem ganzzahligen Wert von Oktetten (FCS-Fehler) oder einem fehlerhaften FCS und einem nicht ganzzahligen Wert von Oktetten (Alignment-Fehler). Ein Jabber-Paket ist definiert als Ethernet-Frame, der den folgenden Kriterien entspricht:
  - Die Paketdatenlänge ist größer als die MRU.
  - Das Paket hat einen ungültigen CRC.
  - Es wurde kein Rx-Fehlerereignis (Empfangen) erkannt.
- **Kollisionen**: Die empfangenen Kollisionen. Wenn Jumbo Frames aktiviert sind, wird der Schwellenwert für die Jabber Frames auf die maximale Jumbo Frame-Größe angehoben.
- **Frames mit 64 Byte**: Die Zahl der empfangenen Frames mit 64 Byte.
- **Frames mit 65 bis 127 Byte**: Die Zahl der empfangenen Frames mit 65 bis 127 Byte.
- **Frames mit 128 bis 255 Byte**: Die Zahl der empfangenen Frames mit 128 bis 255 Byte.
- **Frames mit 256 bis 511 Byte**: Die Zahl der empfangenen Frames mit 256 bis 551 Byte.
- **Frames mit 512 bis 1023 Byte**: Die Zahl der empfangenen Frames mit 512 bis 1023 Byte.
- **Frames mit mehr als 1024 Byte**: Die Zahl der empfangenen Frames mit 1024 bis 2000 Byte sowie Jumbo-Frames.

So löschen Sie Statistikzähler:

- Klicken Sie auf **Schnittstellenzähler löschen**, um die ausgewählten Schnittstellenzähler zu löschen.
- Klicken Sie auf **Alle Statistikschnittstellen anzeigen**, um alle Ports auf einer Seite anzuzeigen.

RMON-Verlauf

Mit der RMON-Funktion können Sie Statistiken pro Schnittstelle überwachen.

Auf der Seite „Verlaufssteuerungstabelle“ können Sie die Abfragehäufigkeit, die Anzahl der zu speichernden Abfragen und den Port für die Datenerfassung konfigurieren.

Sobald die Daten erfasst und gespeichert sind, können Sie sie auf der Seite Verlaufstabelle anzeigen, indem Sie auf **Verlaufstabelle** klicken.

So geben Sie RMON-Steuerungsinformationen ein:

SCHRITT 1 Wählen Sie **Status und Statistik** > **RMON** > **Verlauf**. Die auf dieser Seite angezeigten Felder definieren Sie unten auf der Seite *RMON-Verlauf hinzufügen.* Lediglich ein Feld auf dieser Seite können Sie nicht auf der Seite zum Hinzufügen definieren:

- **Aktuelle Anzahl von Stichproben**: RMON ist gemäß Standard berechtigt, nicht alle angeforderten Stichproben zu gewähren, sondern vielmehr die Zahl der Stichproben pro Anforderung zu beschränken. Aus diesem Grund repräsentiert dieses Feld die tatsächlich für die Anforderung gewährte Zahl von Stichproben, die gleich oder kleiner als der angeforderte Wert waren.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Neuer Verlaufseintrag**: Zeigt die Nummer des neuen Tabelleneintrags an.
- **Quellschnittstelle**: Wählen Sie den Typ der Schnittstelle aus, an der Verlaufsstichproben erfolgen sollen.
- **Max. Anzahl der zu behaltenden Stichproben**: Geben Sie die Zahl der zu speichernden Stichproben ein.
- **Stichprobenintervall**: Geben Sie das Intervall der an den Ports gesammelten Stichproben in Sekunden ein. Der Bereich beträgt 1 - 3600.
- **Eigentümer**: Geben Sie die RMON-Station oder den Benutzer ein, die bzw. der die RMON-Informationen angefordert hat.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Der Eintrag wird der Seite *Verlaufssteuerungstabelle* hinzugefügt und die aktuelle Konfigurationsdatei wird aktualisiert.

SCHRITT 5 Klicken Sie auf **Verlaufstabelle** (unten beschrieben), um die eigentliche Statistik anzuzeigen.

RMON-Verlaufstabelle

Auf der Seite Verlaufstabelle werden schnittstellenspezifische statistische Netzwerkstichproben angezeigt. Die Stichproben wurden in der oben beschriebenen Verlaufssteuerungstabelle konfiguriert.

So zeigen Sie die RMON-Verlaufsstatistik an:

SCHRITT 1 Wählen Sie **Status und Statistik** > **RMON** > **Verlauf**.

SCHRITT 2 Klicken Sie auf **Verlaufstabelle**.

SCHRITT 3 Wählen Sie in der Dropdownliste **Verlaufseintrags-Nr.** bei Bedarf die Eintragsnummer der anzuzeigenden Stichprobe aus.

Es werden die Felder für die ausgewählte Stichprobe angezeigt.

- **Eigentümer**: Eigentümer des Eintrags in der Verlaufstabelle.
- **Stichprobennr.**: Die Stichprobe, die für die Statistik verwendet wurde.
- **Drop-Ereignisse**: Pakete, die während des Stichprobenintervalls aufgrund fehlender Netzwerkressourcen ein Drop-Ereignis ausgelöst haben. Dies ist nicht unbedingt die genaue Zahl von Drop-Paketen, sondern die Häufigkeit, mit der Pakete mit Drop-Ereignis erkannt wurden.
- **Empfangene Bytes**: Die empfangenen Oktette, einschließlich fehlerhafter Pakete und FCS-Oktette jedoch ausschließlich Frame-Bits.
- **Empfangene Pakete**: Die Zahl der empfangenen Pakete, einschließlich fehlerhafter Pakete sowie Multicast- und Broadcast-Pakete.
- **Broadcast-Pakete**: Fehlerfrei empfangene Broadcast-Pakete ausschließlich Multicast-Paketen.
- **Multicast-Pakete**: Fehlerfrei empfangene Multicast-Pakete.
- **CRC- & Ausrichtungsfehler**: Die Zahl der aufgetretenen CRC- und Ausrichtungsfehler.
- **Zu kleine Pakete**: Die empfangenen Pakete mit unzureichender Größe (weniger als 64 Oktette).
- **Zu große Pakete**: Die empfangenen Pakete mit unzulässiger Größe (mehr als 2000 Oktette).
- **Fragmente**: Empfangene Fragmente (Pakete mit weniger als 64 Oktetten), ausschließlich Frame-Bits aber einschließlich FCS-Oktette.
- **Jabber**: Die Gesamtzahl der empfangenen Pakete, die mehr als 2000 Oktette lang sind. In diesem Wert sind Frame-Bits nicht enthalten. Enthalten sind jedoch FCS-Oktette mit einer fehlerhaften FCS (Frame Check Sequence) und einem ganzzahligen Wert von Oktetten (FCS-Fehler) oder einem fehlerhaften FCS und einem nicht ganzzahligen Wert von Oktetten (Alignment-Fehler).
- **Kollisionen**: Die empfangenen Kollisionen.
- **Auslastung**: Der Prozentwert des aktuellen Schnittstellenverkehrs im Vergleich mit dem maximalen Verkehr, den die Schnittstelle verarbeiten kann.

RMON-Ereignissteuerung

Sie können steuern, welche Vorkommnisse einen Alarm auslösen und welche Benachrichtigung erfolgt. Gehen Sie dazu wie folgt vor:

- **Seite „Ereignisse“**: Konfiguriert, was bei Auslösen eines Alarms geschieht. Dies kann eine beliebige Kombination aus Protokollen und Traps sein.
- **Seite „Alarme“**: Konfiguriert die Vorkommnisse, die einen Alarm auslösen.

So definieren Sie RMON-Ereignisse:

SCHRITT 1 Klicken Sie auf **Status und Statistik > RMON** > **Ereignisse**.

Auf dieser Seite werden vordefinierte Ereignisse angezeigt.

Die Felder auf dieser Seite werden mit Ausnahme des Felds „Uhrzeit“ über das Dialogfeld *RIMON-Ereignisse hinzufügen* definiert.

- **Uhrzeit**: Zeigt den Zeitpunkt des Ereignisses an. (Hierbei handelt es sich um eine schreibgeschützte Tabelle im übergeordneten Fenster, die nicht definiert werden kann).

  SCHRITT 2 Klicken Sie auf **Hinzufügen**.

  SCHRITT 3 Geben Sie die Parameter ein.

- **Ereigniseintrag**: Zeigt die Indexnummer des Ereigniseintrags für den neuen Eintrag an.
- **Community**: Geben Sie die SNMP-Community-Zeichenfolge ein, die mit den Traps gesendet werden soll (optional). Beachten Sie, dass die Community über die Seiten **Festlegen von Benachrichtigungsempfängern für SNMPv1 und -v2** oder **Definieren von Benachrichtigungsempfängern bei SNMPv3** definiert werden muss, damit der Trap die Netzwerkmanagementstation erreicht.
- **Beschreibung**: Geben Sie einen Namen für das Ereignis ein. Dieser Name wird auf der Seite RMON-Alarm hinzufügen verwendet, um einen Alarm mit einem Ereignis zu verbinden.
- **Benachrichtigungstyp**: Wählen Sie den Aktionstyp aus, den dieses Ereignis auslöst. Folgende Werte stehen zur Verfügung:
  - *Keine*: Es erfolgt keine Aktion, wenn der Alarm ausgelöst wird.
  - *Protokoll (Ereignisprotokolltabelle)*: Fügt der Ereignisprotokolltabelle einen Protokolleintrag hinzu, wenn der Alarm ausgelöst wird.
  - *Trap (SNMP-Manager und Syslog-Server)*: Sendet einen Trap an den Remote-Protokollserver, wenn der Alarm ausgelöst wird.
  - *Protokoll und Trap*: Fügt der Ereignisprotokolltabelle einen Protokolleintrag hinzu und sendet einen Trap an den Remote-Protokollserver, wenn der Alarm ausgelöst wird.
- **Eigentümer**: Geben Sie das Gerät oder den Benutzer ein, das bzw. der das Ereignis definiert hat.

  SCHRITT 4 Klicken Sie auf **Übernehmen**. Das RMON-Ereignis wird in der aktuellen Konfigurationsdatei gespeichert.

  SCHRITT 5 Klicken Sie auf **Ereignisprotokolltabelle**, um das Protokoll der aufgetretenen und protokollierten Alarme anzuzeigen (siehe Beschreibung unten).

RMON-Ereignisprotokolle

Auf der Seite Ereignisprotokolltabelle wird das Protokoll der eingetretenen Ereignisse (Aktionen) angezeigt. Zwei Arten von Ereignissen können protokolliert werden: *Protokoll* oder *Protokoll und Trap*. Die mit dem Ereignis verbundene Aktion wird ausgeführt, wenn das Ereignis mit einem Alarm verbunden ist (siehe Seite Alarme) und die Bedingungen für den Alarm eingetreten sind.

SCHRITT 1 Klicken Sie auf **Status und Statistik > RMON** > **Ereignisse**.

SCHRITT 2 Klicken Sie auf **Ereignisprotokolltabelle**.

Auf dieser Seite werden folgende Felder angezeigt:

- **Ereigniseintrags-Nr.**: Die Protokolleintragsnummer des Ereignisses.
- **Protokoll-Nr.**: Protokollnummer (innerhalb des Ereignisses).
- **Protokollzeit**: Die Zeit, zu der der Protokolleintrag eingegeben wurde.
- **Beschreibung**: Die Beschreibung des Ereignisses, das den Alarm ausgelöst hat.

RMON-Alarme

RMON-Alarme bieten die Möglichkeit, Schwellenwerte und Stichprobenintervalle festzulegen, um Ausnahmeereignisse für Zähler oder jeden anderen vom Agent gepflegten SNMP-Objektzähler zu generieren. Für den Alarm müssen der steigende und der fallende Schwellenwert definiert werden. Wenn der steigende Schwellenwert überschritten wird, werden erst dann solche Ereignisse generiert, wenn der verbundene fallende Schwellenwert überschritten wird. Wenn ein fallender Alarm ausgegeben wurde, erfolgt die nächste Alarmauslösung, wenn ein steigender Schwellenwert überschritten wird.

Mit einem Ereignis können ein oder mehrere Alarme verbunden sein. Daraus ergibt sich, welche Aktion ausgeführt werden soll, wenn der Alarm auftritt.

Alarmzähler können in den Zählerwerten als absolute Werte oder als Differenz (Delta) erfasst werden.

So geben Sie RMON-Alarme ein:

SCHRITT 1 Klicken Sie auf **Status und Statistik > RMON** > **Alarme**. Alle bereits definierten Alarme werden angezeigt. Die Felder sind unten auf der Seite RMON-Alarm hinzufügen beschrieben. Darüber hinaus wird folgendes Feld angezeigt:

- **Zählerwert**: Zeigt den Wert der Statistik während des letzten Erfassungszeitraums an.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Alarmeintrags-Nr.**: Zeigt die Nummer des Alarmeintrags an.
- **Schnittstelle**: Wählen Sie den Typ der Schnittstelle aus, für die Sie die RMON-Statistik anzeigen möchten.
- **Zählername**: Wählen Sie die MIB-Variable für den Typ des überwachten Ereignisses aus.
- **Zählerwert**: Anzahl der Ereignisse.
- **Stichprobentyp**: Wählen Sie das Stichprobenverfahren für die Alarmgenerierung aus. Folgende Optionen sind möglich:
  - *Absolut*: Bei Überschreitung des Schwellenwerts wird ein Alarm generiert.
  - *Delta*: Subtrahiert den letzten Stichprobenwert vom aktuellen Wert. Die Differenz der Werte wird mit dem Schwellenwert verglichen. Wenn der Schwellenwert überschritten wurde, wird ein Alarm generiert.
- **Steigender Schwellenwert**: Geben Sie den Wert ein, der den Alarm für dieses Ereignis auslöst.
- **Steigendes Ereignis**: Wählen Sie ein Ereignis aus, das ausgeführt werden soll, wenn dieser Alarm ausgelöst wird. Ereignisse können Sie auf der Seite Ereignisse erstellen.
- **Fallender Schwellenwert**: Geben Sie den Wert ein, der den Alarm für dieses Ereignis auslöst.
- **Fallendes Ereignis**: Wählen Sie ein Ereignis aus, das ausgeführt werden soll, wenn dieser Alarm ausgelöst wird.
- **Auslöseralarm**: Wählen Sie das erste Ereignis aus, mit dem die Alarmgenerierung beginnen soll. Als Steigen gilt das Überschreiten des Schwellenwerts von einem unteren Schwellenwert zu einem höheren Schwellenwert.
  - *Steigender Alarm*: Ein steigender Wert löst den Alarm für Ansteigen aus.
  - *Fallender Alarm*: Ein fallender Wert löst den Alarm für Abfallen aus.
  - *Steigend und fallend*: Sowohl steigende als auch fallende Werte lösen den Alarm aus.
- **Intervall**: Geben Sie das Alarmintervall in Sekunden ein.
- **Eigentümer**: Geben Sie den Namen des Benutzers oder Netzwerkverwaltungssystems ein, der bzw. das den Alarm empfängt.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Der RMON-Alarm wird in der aktuellen Konfigurationsdatei gespeichert.

Protokoll anzeigen

Weitere Informationen hierzu finden Sie unter **Anzeigen von Speicherprotokollen**.

4

Administration: Systemprotokoll

In diesem Abschnitt wird die Systemprotokollierung beschrieben, über die das Gerät mehrere unabhängige Protokolle generieren kann. Die einzelnen Protokolle enthalten Meldungen, die Systemereignisse beschreiben.

Das Gerät generiert folgende lokale Protokolle:

- An die Konsolenschnittstelle gesendete Protokolle.
- Protokolle, die in eine zyklische Ereignisliste im Arbeitsspeicher geschrieben und beim Geräteneustart gelöscht werden.
- Protokolle, die in eine zyklische Protokolldatei geschrieben und im Flash-Speicher gespeichert werden. Diese bleiben bei einem Neustart erhalten.

Darüber hinaus können Sie SNMP-Traps und SYSLOG-Meldungen an SYSLOG-Remote-Server senden.

In diesem Abschnitt werden folgende Themen behandelt:

- **Festlegen der Systemprotokolleinstellungen**
- **Festlegen der Remote-Protokollierung**
- **Anzeigen von Speicherprotokollen**

Festlegen der Systemprotokolleinstellungen

Sie können die zu protokollierenden Ereignisse nach Schweregrad auswählen. Für jede Protokollmeldung ist ein Schweregrad angegeben. Die Angabe erfolgt dem ersten Buchstaben des Schweregrades zufolge, der mit einem Bindestrich (-) auf beiden Seiten angehängt ist (ausgenommen ist der Schweregrad *Notfall*, der durch den Buchstaben F gekennzeichnet ist). Beispielsweise besitzt die Protokollmeldung„ %INIT-I-InitCompleted: ... “den Schweregrad **I**, was anzeigt, dass die Meldung eine *Information* darstellt.

Es stehen die folgenden Schweregrade für Ereignisse zur Verfügung, aufgelistet von der höchsten bis zur niedrigsten Gewichtung:

- *Notfall*: Das System kann nicht verwendet werden.
- *Alarm*: Es ist eine Aktion erforderlich.

- *Kritisch*: Das System befindet sich in einem kritischen Zustand.
- *Fehler*: Das System befindet sich im Fehlerzustand.
- *Warnung*: Es ist eine Systemwarnung aufgetreten.
- *Hinweis*: Das System funktioniert ordnungsgemäß, jedoch ist ein Systemhinweis aufgetreten.
- *Informationen*: Geräteinformationen.
- *Debugging*: Detaillierte Informationen zu einem Ereignis.

Sie können für RAM- und Flash-Protokolle unterschiedliche Schweregrade auswählen. Diese Protokolle werden auf der Seite RAM-Speicher bzw. Flash-Speicher angezeigt.

Wenn Sie einen Schweregrad für das Speichern in einem Protokoll auswählen, werden alle höher gewichteten Schweregrade automatisch in diesem Protokoll gespeichert. Schweregrade mit einer geringeren Gewichtung werden nicht im Protokoll gespeichert.

Wenn Sie zum Beispiel **Warnung** auswählen, werden im Protokoll alle Schweregrade des Typs **Warnung** sowie alle höher gewichteten Schweregrade (Notfall, Alarm, Kritisch, Fehler und Warnung) gespeichert. Ereignisse mit einer geringeren Gewichtung als **Warnung** werden nicht gespeichert (Hinweis, Information und Debugging).

So legen Sie globale Protokollparameter fest:

SCHRITT 1 Klicken Sie auf **Administration** > **Systemprotokoll** > **Protokolleinstellungen**.

SCHRITT 2 Geben Sie die Parameter ein.

- **Protokollierung**: Dient zum Aktivieren der Meldungsprotokollierung.
- **Syslog-Aggregator**: Wählen Sie diese Option aus, um die Aggregierung von Syslog-Nachrichten und Traps zu aktivieren. Wenn diese Option aktiviert ist, werden identische und zusammenhängende SYSLOG-Nachrichten und Traps während der angegebenen maximalen Aggregationszeit aggregiert und in einer einzelnen Nachricht gesendet. Das Senden der aggregierten Meldungen erfolgt in der Reihenfolge des Empfangs. Jede Nachricht enthält Informationen dazu, wie häufig sie aggregiert wurde.
- **Max. Aggregationszeit**: Geben Sie das Zeitintervall für die Aggregation von SYSLOG-Meldungen ein.
- **Ersteller-Identifikator**: Mit dieser Option können Sie SYSLOG-Meldungen eine Ursprungs-ID hinzuzufügen. Folgende Optionen sind möglich:
  - *Keine*: Trägt keine Ursprungs-ID in SYSLOG-Meldungen ein.
  - *Hostname*: Trägt den Hostnamen des Systems in SYSLOG-Meldungen ein.
  - *IPv4-Adresse*: Trägt die IPv4-Adresse der sendenden Schnittstelle in SYSLOG-Meldungen ein.
  - *IPv6-Adresse*: Trägt die IPv6-Adresse der sendenden Schnittstelle in SYSLOG-Meldungen ein.
  - *Benutzerdefiniert*: Hier kann eine Beschreibung eingegeben werden, die in SYSLOG-Meldungen aufgenommen wird.

- **RAM-Speicherprotokollierung**: Wählen Sie die Schweregrade der im RAM zu protokollierenden Nachrichten aus.
- **Flash-Speicher-Protokollierung**: Wählen Sie die Schweregrade der im Flash-Speicher zu protokollierenden Nachrichten aus.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Festlegen der Remote-Protokollierung

Auf der Seite „Remote-Protokollserver“ können Sie SYSLOG-Remote-Server definieren, an die Protokollmeldungen gesendet werden. Für jeden Server können Sie den Schweregrad der empfangenen Meldungen konfigurieren.

So definieren Sie SYSLOG-Server:

SCHRITT 1 Wählen Sie **Administration** > **Systemprotokoll** > **Remote-Protokoll-Server**.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **IPv4-Quellschnittstelle**: Wählen Sie die Quellschnittstelle aus, deren IPv4-Adresse als Quell-IPv4-Adresse für SYSLOG-Nachrichten verwendet wird, die an SYSLOG-Server gesendet werden.
- **IPv6-Quellschnittstelle**: Wählen Sie die Quellschnittstelle aus, deren IPv6-Adresse als Quell-IPv6-Adresse für SYSLOG-Nachrichten verwendet wird, die an SYSLOG-Server gesendet werden.

HINWEIS Wenn Sie die Option „Auto“ auswählen, übernimmt das System die Quell-IP-Adresse aus der IP-Adresse, die auf der ausgehenden Schnittstelle definiert wurde.

Für jeden zuvor konfigurierten Protokollserver werden Informationen angezeigt. Die Felder werden nachstehend auf der Seite **Hinzufügen** beschrieben.

SCHRITT 3 Klicken Sie auf **Hinzufügen**.

SCHRITT 4 Geben Sie die Parameter ein.

- **Serverdefinition**: Wählen Sie aus, ob der Remote-Protokoll-Server anhand der IP-Adresse oder des Namens identifiziert wird.
- **IP-Version**: Wählen Sie das unterstützte IP-Format aus.

- **IPv6-Adresstyp**: Wählen Sie den IPv6-Adresstyp aus (falls IPv6 verwendet wird). Folgende Optionen sind möglich:
  - *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
  - *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.
- **Link Local-Schnittstelle**: Wählen Sie in der Liste die Link Local-Schnittstelle aus (falls der IPv6-Adresstyp „Link Local“ ausgewählt ist).
- **IP-Adresse/Name des Protokollservers**: Geben Sie die IP-Adresse oder den Domänennamen des Protokollservers ein.
- **UDP-Port**: Geben Sie den UDP-Port ein, an den die Protokollmeldungen gesendet werden.
- **Einrichtung**: Wählen Sie den Wert einer Einrichtung aus, von der Systemprotokolle an den Remote-Server gesendet werden. Einem Server kann nur ein Einrichtungswert zugewiesen werden. Wird ein zweiter Einrichtungscode zugewiesen, wird der erste Einrichtungswert überschrieben.
- **Beschreibung**: Geben Sie eine Server-Beschreibung ein.
- **Mindestschweregrad**: Wählen Sie den Mindestschweregrad von Systemprotokollmeldungen aus, die an den Server gesendet werden.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die Seite *Remote-Protokollserver hinzufügen* wird geschlossen, der SYSLOG-Server wird hinzugefügt und die aktuelle Konfigurationsdatei wird aktualisiert.

Anzeigen von Speicherprotokollen

Das Gerät kann in folgende Protokolle schreiben:

- Protokoll im RAM (wird beim Neustart gelöscht).
- Protokoll im Flash-Speicher (wird nur durch den Benutzer gelöscht).

Sie können für alle in die jeweiligen Protokolle geschriebenen Meldungen einen Schweregrad konfigurieren und eine Meldung an mehrere Protokolle senden, die sich auch auf externen SYSLOG-Servern befinden können.

RAM-Speicher

Auf der Seite *RAM-Speicher* werden alle im RAM (Cache) gespeicherten Meldungen in chronologischer Reihenfolge angezeigt. Die Einträge werden im RAM-Protokoll entsprechend der Konfiguration auf der Seite Protokolleinstellungen gespeichert.

Um Protokolleinträge anzuzeigen, wählen Sie **Status und Statistik** > **Protokoll anzeigen** > **RAM-Speicher**.

Oben auf der Seite wird eine Schaltfläche angezeigt, mit der Sie das blinkende Alarmsymbol deaktivieren können. **Klicken Sie auf.** Durch Klicken können Sie es deaktivieren und wieder aktivieren.

Die **Aktuelle Protokollierungsschwelle** gibt die Protokollierungsebenen an, die generiert werden. Sie können dies ändern, indem Sie neben dem Feldnamen auf **Bearbeiten** klicken.

Diese Seite enthält für alle Protokolldateien die folgenden Felder:

- **Protokollindex**: Nummer des Protokolleintrags.
- **Protokollzeit**: Die Uhrzeit der Meldungsgenerierung.
- **Schweregrad**: Schweregrad des Ereignisses.
- **Beschreibung**: Meldungstext, der das Ereignis beschreibt.

Klicken Sie auf **Protokolle löschen**, um die Protokollmeldungen zu entfernen. Die Meldungen werden gelöscht.

Flashspeicher

Auf der Seite *Flash-Speicher* werden alle im Flash-Speicher gespeicherten Meldungen in chronologischer Reihenfolge angezeigt. Ab welchem Schweregrad Ereignisse protokolliert werden, können Sie auf der Seite Protokolleinstellungen festlegen. Flash-Protokolle bleiben auch bei einem Geräteneustart erhalten. Sie können die Protokolle manuell löschen.

Um die Flash-Protokolle anzuzeigen, klicken Sie auf **Status und Statistik** > **Protokoll anzeigen** > **Flash-Speicher**.

Die **Aktuelle Protokollierungsschwelle** gibt die Protokollierungsebenen an, die generiert werden. Sie können dies ändern, indem Sie neben dem Feldnamen auf **Bearbeiten** klicken.

Diese Seite enthält für jede Protokolldatei folgende Felder:

- **Protokollindex**: Nummer des Protokolleintrags.
- **Protokollzeit**: Die Uhrzeit der Meldungsgenerierung.
- **Schweregrad**: Schweregrad des Ereignisses.
- **Beschreibung**: Meldungstext, der das Ereignis beschreibt.

Klicken Sie auf **Protokolle löschen**, um die Meldungen zu entfernen. Die Meldungen werden gelöscht.

5

Administration: Dateiverwaltung

In diesem Abschnitt wird die Verwaltung der Systemdateien beschrieben.

Folgende Themen werden behandelt:

- **Systemdateien**
- **Firmware/Sprache aktualisieren/sichern**
- **Aktives Image**
- **Konfiguration/Protokoll herunterladen/sichern**
- **Konfigurationsdateieigenschaften**
- **Konfiguration kopieren/speichern**
- **Automatische Konfiguration und Image-Aktualisierung über DHCP**

Systemdateien

Systemdateien sind Dateien, die Konfigurationsinformationen, Firmware-Images oder Bootcode enthalten.

Für diese Dateien können Sie verschiedene Aktionen ausführen, beispielsweise Auswählen der Firmwaredatei, von der das Gerät gestartet wird, internes Kopieren verschiedener Arten von Konfigurationsdateien im Gerät oder Kopieren von Dateien auf ein externes Gerät bzw. von einem externen Gerät (beispielsweise einem externen Server).

Für die Dateiübertragung sind folgende Methoden möglich:

- Internes Kopieren
- HTTP/HTTPS, das die vom Browser bereitgestellten Funktionen verwendet
- TFTF-/SCP-Client, erfordert einen TFTP-/SCP-Server.

Die Konfigurationsdateien auf dem Gerät werden durch ihren *Typ* definiert und enthalten die Einstellungen und Parameterwerte für das Gerät.

Wenn eine Konfiguration für das Gerät referenziert wird, dann anhand ihres *Konfigurationsdateityps (beispielsweise Startkonfiguration oder aktuelle Konfiguration)* und nicht anhand eines Dateinamens, den der Benutzer ändern kann.

Benutzer können Inhalte von einem Konfigurationsdateityp in einen anderen kopieren, sie können jedoch die Namen der Dateitypen nicht ändern.

Zu den anderen im Gerät gespeicherten Dateien gehören Firmware-, Boot-Code- und Protokolldateien, die als *Betriebsdateien* bezeichnet werden.

Bei den Konfigurationsdateien handelt es sich um Textdateien, die Sie auf ein externes Gerät wie beispielsweise einen PC kopieren und dann in einem Texteditor wie Notepad bearbeiten können.

Dateien und Dateitypen

Das Gerät verfügt über folgende Typen von Konfigurations- und Betriebsdateien:

- **Aktuelle Konfiguration**: Enthält die aktuell vom Gerät verwendeten Parameter. Dies ist der einzige Dateityp, der geändert wird, wenn Sie Parameterwerte im Gerät ändern.

  Wenn das Gerät neu gestartet wird, geht die aktuelle Konfiguration verloren. Die Startkonfiguration im Flash-Speicher überschreibt die im RAM gespeicherte aktuelle Konfiguration.

  Damit Änderungen am Gerät erhalten bleiben, müssen Sie die aktuelle Konfiguration in der Startkonfiguration oder einem anderen Dateityp speichern.

- **Startkonfiguration**: Die Parameterwerte, die durch Kopieren aus einer anderen Konfiguration (normalerweise der aktuellen Konfiguration) in der Startkonfiguration gespeichert wurden.

  Die Startkonfiguration befindet sich im Flash-Speicher und bleibt bei einem Geräteneustart erhalten. Dabei wird die Startkonfiguration in das RAM kopiert und als aktuelle Konfiguration identifiziert.

- **Spiegelkonfiguration**: Eine Kopie der Startkonfiguration, die das Gerät unter folgenden Umständen erstellt:

  - Das Gerät war 24 Stunden lang ununterbrochen in Betrieb.
  - Wenn innerhalb der letzten 24 Stunden keine Konfigurationsänderungen an der ausgeführten Konfiguration vorgenommen wurden.
  - Die Startkonfiguration ist mit der aktuellen Konfiguration identisch.

  Nur das System kann die Startkonfiguration in die Spiegelkonfiguration kopieren. Sie können jedoch Elemente aus der Spiegelkonfiguration in andere Dateitypen oder auf ein anderes Gerät kopieren.

  Die Option zum automatischen Kopieren der aktuellen Konfiguration in die Spiegelkonfiguration können Sie auf der Seite „Konfigurationsdateieigenschaften“ deaktivieren.

- **Backup-Konfiguration**: Eine manuell erstellte Kopie einer Konfigurationsdatei zum Schutz vor Systemausfällen oder zum Erhalten eines bestimmten Betriebszustands. Sie können die Spiegelkonfiguration, die Startkonfiguration oder die aktuelle Konfiguration in einer Backup-Konfigurationsdatei speichern. Die Backup-Konfiguration befindet sich im Flash-Speicher und bleibt bei einem Neustart des Geräts erhalten.
- **Firmware**: Das Programm, mit dem der Betrieb und die Funktionalität des Geräts gesteuert werden. Wird meist als *Image* bezeichnet.
- **Boot-Code**: Steuert den grundlegenden Systemstart und startet das Firmware-Image.
- **Sprachdatei**: Das Wörterbuch, das die Anzeige der Fenster des webbasierten Konfigurationsdienstprogramms in der ausgewählten Sprache ermöglicht.
- **Flash-Protokoll**: Im Flash-Speicher abgelegte SYSLOG-Meldungen.

Dateiaktionen

Sie können zum Verwalten von Firmware- und Konfigurationsdateien die folgenden Aktionen ausführen:

- Aktualisieren der Firmware oder des Bootcodes oder Ersetzen einer zweiten Sprache gemäß der Beschreibung im Abschnitt **Firmware/Sprache aktualisieren/sichern**.
- Anzeigen des aktuell verwendeten Firmware-Images oder Auswählen des beim nächsten Neustart verwendeten Images, wie im Abschnitt **Aktives Image** beschrieben.
- Speichern der Konfigurationsdateien auf dem Gerät an einem Speicherort auf einem anderen Gerät, wie im Abschnitt **Konfiguration/Protokoll herunterladen/sichern** beschrieben.
- Löschen der Dateitypen „Startkonfiguration“ oder „Sicherungskonfiguration“, wie im Abschnitt **Konfigurationsdateieigenschaften** beschrieben.
- Kopieren eines Konfigurationsdateityps in einen anderen Konfigurationsdateityp gemäß der Beschreibung im Abschnitt **Konfiguration kopieren/speichern**.
- Aktivieren des automatischen Uploads einer Konfigurationsdatei von einem DHCP-Server auf das Gerät gemäß der Beschreibung im Abschnitt **Automatische Konfiguration und Image-Aktualisierung über DHCP**.

In diesem Abschnitt werden die folgenden Themen behandelt:

- **Firmware/Sprache aktualisieren/sichern**
- **Aktives Image**
- **Konfiguration/Protokoll herunterladen/sichern**
- **Konfigurationsdateieigenschaften**
- **Konfiguration kopieren/speichern**
- **Automatische Konfiguration und Image-Aktualisierung über DHCP**

Firmware/Sprache aktualisieren/sichern

Der Prozess **Firmware/Sprache aktualisieren/sichern** kann für folgende Aufgaben verwendet werden:

- Aktualisieren oder Sichern des Firmware-Images
- Aktualisieren oder Sichern des Bootcodes
- Importieren oder Aktualisieren einer zweiten Sprachdatei

Es werden die folgenden Methoden für das Übertragen von Dateien unterstützt:

- HTTP/ HTTPS: Verwendet die vom Browser bereitgestellten Funktionen.
- TFTP: Erfordert einen TFTP-Server.
- Secure Copy Protocol (SCP): Erfordert einen SCP-Server.

Wenn eine neue Sprachdatei auf das Gerät geladen wird, kann die neue Sprache im Dropdown-Menü ausgewählt werden. (Das Gerät muss dazu nicht neu gestartet werden.) Diese Sprachdatei wird automatisch auf alle Geräte im Stack kopiert.

Alle Software-Images im Stack müssen identisch sein, damit der Stack ordnungsgemäß funktioniert. Wenn einem Stack ein Gerät hinzugefügt wird, dessen Software-Image nicht mit dem Software-Image des Masters identisch ist, lädt der Master automatisch das richtige Image in das neue Gerät.

Es gibt folgende Möglichkeiten, um Images im gesamten Stack zu aktualisieren:

- Das Image kann aktualisiert werden, bevor die Einheit mit dem Stack verbunden wird. Dies ist die empfohlene Methode.
- Gerät oder Stack aktualisieren. Wenn der Stack aktualisiert wird, werden die Slave-Einheiten automatisch aktualisiert. Gehen Sie dazu wie folgt vor:
  - Kopieren Sie das Image vom TFTP-/SCP-Server auf die Mastereinheit. Verwenden Sie dazu die Seite Firmware/Sprache aktualisieren/sichern.
  - Ändern Sie das aktive Image über die Seite Aktives Image.
  - Starten Sie über die Seite Neustart neu.

Im Gerät sind zwei Firmware-Images gespeichert. Eines der Images ist das *aktive Image*, das andere ist das *inaktive Image*.

Wenn Sie die Firmware aktualisieren, ersetzt das neue Image immer das inaktive Image.

Auch nach dem Hochladen neuer Firmware auf das Gerät wird dieses weiterhin mit dem aktiven Image (der alten Version) gestartet, bis Sie das neue Image anhand der im Abschnitt **Aktives Image** beschriebenen Vorgehensweise als aktives Image festlegen. Starten Sie anschließend das Gerät.

HINWEIS Wird das Gerät im Modus „Natives Stacking“ betrieben, wird die neue Firmware im Push-Verfahren an alle Stack-Einheiten übertragen. Wenn dem Stack ein neues Gerät mit einer anderen Firmwareversion hinzugefügt wird, synchronisiert die Mastereinheit automatisch die Firmwareversion mit dieser neu hinzugefügten Einheit. Dies geschieht transparent und ohne manuellen Eingriff.

Aktualisieren und Sichern der Firmware oder einer Sprachdatei

So aktualisieren oder sichern Sie ein Software-Image oder eine Sprachdatei:

SCHRITT 1 Wählen Sie **Administration** > **Dateiverwaltung** > **Firmware/Sprache aktualisieren/sichern**.

SCHRITT 2 Klicken Sie auf die Übertragungsmethode. Gehen Sie wie folgt vor:

- Wenn Sie **TFTP** ausgewählt haben, fahren Sie mit **Schritt 3** fort.
- Wenn Sie **über HTTP/HTTPS** ausgewählt haben, fahren Sie mit **Schritt 4** fort.
- Wenn Sie **über SCP** ausgewählt haben, fahren Sie mit **Schritt 5** fort.

SCHRITT 3 Wenn Sie **über TFTP** ausgewählt haben, geben Sie die Parameter gemäß der Beschreibung in diesem Schritt ein. Ansonsten fahren Sie mit **Schritt 4** fort.

Wählen Sie eine der folgenden **Speichermethoden** aus:

- **Upgrade**: Gibt an, dass der Dateityp auf dem Gerät durch eine neue Version dieses Dateityps ersetzt werden soll, die sich auf einem TFTP-Server befindet.
- **Backup**: Gibt an, dass eine Kopie des Dateityps in einer Datei auf einem anderen Gerät gespeichert werden soll.

Geben Sie Werte für die folgenden Felder ein:

- **Dateityp**: Wählen Sie den Typ der Zieldatei aus. Es werden nur gültige Dateitypen angezeigt. (Die Dateitypen werden im Abschnitt **Dateien und Dateitypen** beschrieben.)
- **TFTP-Serverdefinition**: Wählen Sie aus, ob der TFTP-Server **Nach IP-Adresse** oder **Nach Name** angegeben wird.
- **IP-Version**: Legen Sie fest, ob eine IPv4- oder eine IPv6-Adresse verwendet wird.

- **IPv6-Adresstyp**: Wählen Sie den IPv6-Adresstyp aus (falls IPv6 verwendet wird). Folgende Optionen sind möglich:
  - **Link Local**: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix FE80, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
  - **Global**: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.
- **Link Local-Schnittstelle**: Wählen Sie in der Liste die Link Local-Schnittstelle aus (wenn IPv6 verwendet wird).
- **IP-Adresse/Name des TFTP-Servers**: Geben Sie die IP-Adresse oder den Namen des TFTP-Servers ein.
- **(Bei einem Upgrade) Name der Quelldatei**: Geben Sie den Namen der Quelldatei ein.
- **(Bei einer Sicherung) Name der Zieldatei**: Geben Sie den Namen der Sicherungsdatei ein.

SCHRITT 4 Wenn Sie **über HTTP/HTTPS** ausgewählt haben, können Sie nur die **Speichermethode: Aktualisieren** verwenden. Geben Sie die Parameter gemäß der Beschreibung in diesem Schritt ein.

- **Dateityp**: Wählen Sie einen der folgenden Typen aus:
  - *Firmware-Image*: Wählen Sie diese Option aus, um das Firmware-Image zu aktualisieren.
  - *Sprachdatei*: Wählen Sie diese Option aus, um die Sprachdatei zu aktualisieren.
- **Dateiname**: Klicken Sie auf **Durchsuchen**, um eine Datei auszuwählen, oder geben Sie den Pfad und den Namen der Quelldatei für die Übertragung ein.

SCHRITT 5 Wenn Sie über **SCP (über SSH)** ausgewählt haben, finden Sie unter **SSH-Clientauthentifizierung** weitere Anweisungen. Geben Sie dann Werte für die folgenden Felder ein: (Es werden nur eindeutige Felder beschrieben, für nicht eindeutige Felder gelten die obigen Beschreibungen.)

- **SSH-Remoteserverauthentifizierung**: Um die SSH-Serverauthentifizierung (standardmäßig deaktiviert) zu aktivieren, klicken Sie auf **Bearbeiten**. Daraufhin gelangen Sie zur Seite **SSH-Serverauthentifizierung**, auf der Sie den SSH-Server konfigurieren können. Anschließend kehren Sie zu dieser Seite zurück. Verwenden Sie die Seite **SSH-Serverauthentifizierung**, um eine SSH-Benutzerauthentifizierungsmethode (Kennwort oder öffentlicher/privater Schlüssel) auszuwählen, einen Benutzernamen und ein Kennwort für das Gerät festzulegen (wenn die Kennwortmethode ausgewählt ist) und bei Bedarf einen RSA- oder DSA-Schlüssel zu generieren.

SSH-Clientauthentifizierung: Für die Clientauthentifizierung gibt es folgende Möglichkeiten:

- **Systemanmeldeinformationen für SSH-Client verwenden**: Legt permanente SSH-Benutzeranmeldeinformationen fest. Klicken Sie auf **Systemanmeldeinformationen**, um zur Seite SSH-Benutzerauthentifizierung zu wechseln, auf der Sie den Benutzer und das Kennwort zur zukünftigen Verwendung festlegen können.
- **Einmalige Anmeldeinformationen für SSH-Client verwenden**: Geben Sie Folgendes ein:
  - *Benutzername*: Geben Sie einen Benutzernamen für diese Kopieraktion ein.
  - *Kennwort*: Geben Sie ein Kennwort für diese Kopieraktion ein.

  HINWEIS Der Benutzername und das Kennwort für einmalige Anmeldeinformationen werden nicht in der Konfigurationsdatei gespeichert.

Wählen Sie eine der folgenden **Speichermethoden** aus:

- **Upgrade**: Gibt an, dass der Dateityp auf dem Gerät durch eine neue Version dieses Dateityps ersetzt werden soll, die sich auf einem TFTP-Server befindet.
- **Backup**: Gibt an, dass eine Kopie des Dateityps in einer Datei auf einem anderen Gerät gespeichert werden soll.

Geben Sie Werte für die folgenden Felder ein:

- **Dateityp**: Wählen Sie den Typ der Zieldatei aus. Es werden nur gültige Dateitypen angezeigt. (Die Dateitypen werden im Abschnitt **Dateien und Dateitypen** beschrieben).
- **SCP-Serverdefinition**: Wählen Sie aus, ob der SCP-Server anhand der IP-Adresse oder des Domänennamens angegeben wird.
- **IP-Version**: Legen Sie fest, ob eine IPv4- oder eine IPv6-Adresse verwendet wird.
- **IPv6-Adresstyp**: Wählen Sie den IPv6-Adresstyp aus (wenn dieser verwendet wird). Folgende Optionen sind möglich:
  - *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
  - *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.
- **Link-Local-Schnittstelle**: Wählen Sie in der Liste die Link-Local-Schnittstelle aus.
- **IP-Adresse/Name des SCP-Servers**: Geben Sie die IP-Adresse oder den Domänennamen des SCP-Servers ein.
- **(Bei einem Upgrade) Name der Quelldatei**: Geben Sie den Namen der Quelldatei ein.

- **(Bei einer Sicherung) Name der Zieldatei**: Geben Sie den Namen der Sicherungsdatei ein.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Wenn die Dateien, Kennwörter und Serveradressen richtig sind, ist Folgendes möglich:

- Wenn die SSH-Serverauthentifizierung aktiviert (auf der Seite SSH-Serverauthentifizierung) und der SCP-Server vertrauenswürdig ist, wird der Vorgang erfolgreich ausgeführt. Wenn der SCP-Server nicht vertrauenswürdig ist, wird der Vorgang nicht ausgeführt und es wird ein Fehler angezeigt.
- Wenn SSH-Serverauthentifizierung nicht aktiviert ist, wird der Vorgang für jeden SCP-Server erfolgreich ausgeführt.

Aktives Image

Im Gerät sind zwei Firmware-Images gespeichert. Eines der Images ist das *aktive Image*, das andere ist das *inaktive Image*. Das Gerät startet von dem Image, das Sie als *aktives Image* festlegen. Sie können das *inaktive Image* als *aktives Image* festlegen. (Sie können das Gerät wie in Abschnitt **Management-Schnittstelle** beschrieben neu starten.)

So wählen Sie das aktive Image aus:

SCHRITT 1 Wählen Sie **Administration** > **Dateiverwaltung** > **Aktives Image**.

Auf dieser Seite wird Folgendes angezeigt:

- **Aktives Image**: Zeigt die derzeit aktive Image-Datei auf dem Gerät an.
- **Versionsnummer des aktiven Image**: Zeigt die Firmware-Version des aktiven Image an.
- **Aktives Image nach Neustart**: Zeigt das nach dem Neustart aktive Image an.
- **Versionsnummer des aktiven Images nach Neustart**: Zeigt die Firmwareversion des aktiven Images nach dem Neustart an.

SCHRITT 2 Wählen Sie im Menü **Aktives Image nach Neustart** das Firmware-Image, das nach dem Neustart des Geräts als aktives Image verwendet werden soll. Im Feld **Versionsnummer des aktiven Image nach Neustart** wird die Firmware-Version des aktiven Image angezeigt, das nach dem Neustart des Geräts verwendet wird.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Einstellungen für das aktive Image werden aktualisiert.

Konfiguration/Protokoll herunterladen/sichern

Auf der Seite Konfiguration/Protokoll herunterladen/sichern können Sie folgende Aktionen ausführen:

- Sichern von Konfigurationsdateien oder Protokollen vom Gerät auf ein externes Gerät
- Wiederherstellen von Konfigurationsdateien von einem externen Gerät auf dem Gerät.

HINWEIS Wenn das Gerät im Stack-Modus betrieben wird, werden die Konfigurationsdateien der Mastereinheit verwendet.

Wenn Sie eine Konfigurationsdatei als aktuelle Konfiguration wiederherstellen, *fügt* die importierte Datei alle Konfigurationsbefehle hinzu, die in der alten Datei nicht vorhanden waren, und *überschreibt* alle Parameterwerte in den vorhandenen Konfigurationsbefehlen.

Wird eine Konfigurationsdatei in der Startkonfiguration oder eine Backup-Konfigurationsdatei wiederhergestellt, *ersetzt* die neue Datei die vorherige Datei.

Wenn Sie die Startkonfiguration wiederherstellen, müssen Sie das Gerät neu starten, damit die wiederhergestellte Startkonfiguration als aktuelle Konfiguration verwendet wird. Sie können das Gerät wie in Abschnitt **Management-Schnittstelle** beschrieben neu starten.

Abwärtskompatibilität der Konfigurationsdatei

Wenn Sie Konfigurationsdateien von einem externen Gerät auf dem Gerät wiederherstellen, können folgende Kompatibilitätsprobleme auftreten:

- **Warteschlangenmodus von 4 in 8 ändern**: Warteschlangenkonfigurationen müssen überprüft und angepasst werden, damit die QoS-Ziele mit dem neuen Warteschlangenmodus erreicht werden. Eine Liste der entsprechenden QoS-Befehle finden Sie im *CLI-Referenzhandbuch*.
- **Warteschlangenmodus von 8 in 4 ändern**: Konfigurationsbefehle für Warteschlangen, die mit dem neuen Warteschlangenmodus in Konflikt stehen, werden abgelehnt, d. h. das Herunterladen der Konfigurationsdatei schlägt fehl. Sie können den Warteschlangenmodus auf der Seite Systemmodus und Stack-Verwaltung ändern.
- **Systemmodus ändern**: Wenn der Systemmodus in einer Konfigurationsdatei enthalten ist, die auf das Gerät heruntergeladen wird, und wenn der Systemmodus in der Datei mit dem aktuellen Systemmodus übereinstimmt, dann wird diese Information ignoriert. Andernfalls wird der Systemmodus geändert. Folgende Fälle sind möglich:
  - Wird die Konfigurationsdatei auf das Gerät heruntergeladen (über die Seite „Konfiguration/ Protokoll herunterladen/sichern“), wird der Vorgang abgebrochen und eine Meldung angezeigt, die besagt, dass der Systemmodus auf der Seite „Systemmodus und Stack-Verwaltung“ geändert werden muss.

- Wird die Konfigurationsdatei im Rahmen einer automatischen Konfiguration heruntergeladen, wird die Startkonfigurationsdatei gelöscht und das Gerät startet automatisch mit dem neuen Systemmodus neu. Das Gerät wird mit einer leeren Konfigurationsdatei konfiguriert.

Informationen dazu, was geschieht, wenn die Stack-Modi geändert werden, finden Sie unter **Konfiguration nach Neustart**.

Herunterladen oder Sichern einer Konfigurations- oder Protokolldatei

So sichern Sie die Systemkonfigurationsdatei oder stellen diese wieder her:

SCHRITT 1 Klicken Sie auf **Administration** > **Dateiverwaltung** > **Konfiguration/Protokoll herunterladen/sichern**.

SCHRITT 2 Wählen Sie die **Übertragungsmethode** aus.

SCHRITT 3 Wenn Sie **über TFTP** ausgewählt haben, geben Sie die Parameter ein. Ansonsten fahren Sie mit **Schritt 4** fort.

Wählen Sie **Herunterladen** oder **Backup** als **Speichermethode** aus.

Herunterladen: Gibt an, dass der Dateityp im Gerät durch die Datei auf einem anderen Gerät ersetzt wird. Geben Sie Werte für die folgenden Felder ein:

a. **TFTP-Serverdefinition**: Wählen Sie aus, ob der TFTP-Server anhand der IP-Adresse oder des Domänennamens angegeben wird.

b. **IP-Version**: Legen Sie fest, ob eine IPv4- oder eine IPv6-Adresse verwendet wird.

HINWEIS Wenn Sie unter „Serverdefinition“ ausgewählt haben, dass der Server anhand des Namens ausgewählt wird, müssen Sie die Optionen für die IP-Version nicht auswählen.

c. **IPv6-Adresstyp**: Wählen Sie den IPv6-Adresstyp aus (wenn dieser verwendet wird). Folgende Optionen sind möglich:

- *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
- *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.

d. **Link-Local-Schnittstelle**: Wählen Sie in der Liste die Link-Local-Schnittstelle aus.

e. **IP-Adresse/Name des TFTP-Servers**: Geben Sie die IP-Adresse oder den Namen des TFTP-Servers ein.

f. **Name der Quelldatei**: Geben Sie den Namen der Quelldatei ein. Dateinamen dürfen keine Schrägstriche (\ oder /) enthalten, dürfen nicht mit einem Punkt (.) beginnen und müssen 1 bis 160 Zeichen enthalten. (Gültige Zeichen sind: A-Z, a-z, 0-9, „.“, „-“, „_“.)

g. **Typ der Zieldatei**: Geben Sie den Typ der Ziel-Konfigurationsdatei ein. Es werden nur gültige Dateitypen angezeigt. (Die Dateitypen werden im Abschnitt **Dateien und Dateitypen** beschrieben).

Sicherung: Gibt an, dass ein Dateityp in eine Datei auf einem anderen Gerät kopiert werden soll. Geben Sie Werte für die folgenden Felder ein:

a. **TFTP-Serverdefinition**: Wählen Sie aus, ob der TFTP-Server anhand der IP-Adresse oder des Domänennamens angegeben wird.

b. **IP-Version**: Legen Sie fest, ob eine IPv4- oder eine IPv6-Adresse verwendet wird.

c. **IPv6-Adresstyp**: Wählen Sie den IPv6-Adresstyp aus (wenn dieser verwendet wird). Folgende Optionen sind möglich:

   - *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
   - *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.

d. **Link-Local-Schnittstelle**: Wählen Sie in der Liste die Link-Local-Schnittstelle aus.

e. **IP-Adresse/Name des TFTP-Servers**: Geben Sie die IP-Adresse oder den Namen des TFTP-Servers ein.

f. **Typ der Quelldatei**: Geben Sie den Typ der Quell-Konfigurationsdatei ein. Es werden nur gültige Dateitypen angezeigt. (Die Dateitypen werden im Abschnitt **Dateien und Dateitypen** beschrieben).

g. **Sensible Daten**: Wählen Sie aus, wie sensible Daten in die Sicherungsdatei aufgenommen werden sollen. Folgende Optionen stehen zur Verfügung:

   - *Ausschließen*: Sensible Daten werden nicht in die Sicherungsdatei aufgenommen.
   - *Verschlüsselt*: Sensible Daten werden in verschlüsselter Form in die Sicherungsdatei aufgenommen.
   - *Unverschlüsselt*: Sensible Daten werden in unverschlüsselter Form in die Sicherungsdatei aufgenommen.

   HINWEIS Die verfügbaren Optionen für sensible Daten werden durch die SSD-Regeln des aktuellen Benutzers bestimmt. Details finden Sie auf der Seite Sicheres Verwalten sensibler Daten (SSD) > SSD-Regeln.

h. **Name der Zieldatei**: Geben Sie den Namen der Zieldatei ein. Dateinamen dürfen keine Schrägstriche (\ oder /) enthalten, der erste Buchstabe des Dateinamens darf kein Punkt (.) sein und der Dateiname muss aus 1 bis 160 Zeichen bestehen. (Gültige Zeichen sind: A-Z, a-z, 0-9, „.“, „-“, „_“.)

i. Klicken Sie auf **Übernehmen**. Die Datei wird aktualisiert oder gesichert.

SCHRITT 4 Wenn Sie **über HTTP/HTTPS** ausgewählt haben, geben Sie die Parameter gemäß der Beschreibung in diesem Schritt ein.

Wählen Sie die **Speichermethode**.

Wenn Sie als **Speichermethode** die Option *Herunterladen* auswählen (Ersetzen der Datei im Gerät durch eine neue Version von einem anderen Gerät), führen Sie die folgenden Schritte aus. Ansonsten fahren Sie mit der nächsten Prozedur in diesem Schritt fort.

a. **Name der Quelldatei**: Klicken Sie auf **Durchsuchen**, um eine Datei auszuwählen, oder geben Sie den Pfad und den Namen der Quelldatei für die Übertragung ein.

b. **Typ der Zieldatei**: Wählen Sie den Typ der Konfigurationsdatei aus. Es werden nur gültige Dateitypen angezeigt. (Die Dateitypen werden im Abschnitt **Dateien und Dateitypen** beschrieben).

c. Klicken Sie auf **Übernehmen**. Die Datei wird von dem anderen Gerät auf das Gerät übertragen.

Wenn Sie für **Speichermethode** die Option *Sicherung* (Kopieren einer Datei in ein anderes Gerät) auswählen, führen Sie die folgenden Schritte aus:

a. **Typ der Quelldatei**: Wählen Sie den Typ der Konfigurationsdatei aus. Es werden nur gültige Dateitypen angezeigt. (Die Dateitypen werden im Abschnitt **Dateien und Dateitypen** beschrieben).

b. **Sensible Daten**: Wählen Sie aus, wie sensible Daten in die Sicherungsdatei aufgenommen werden sollen. Folgende Optionen stehen zur Verfügung:

- *Ausschließen*: Sensible Daten werden nicht in die Sicherungsdatei aufgenommen.
- *Verschlüsselt*: Sensible Daten werden in verschlüsselter Form in die Sicherungsdatei aufgenommen.
- *Unverschlüsselt*: Sensible Daten werden in unverschlüsselter Form in die Sicherungsdatei aufgenommen.

HINWEIS Die verfügbaren Optionen für sensible Daten werden durch die SSD-Regeln des aktuellen Benutzers bestimmt. Details finden Sie auf der Seite Sicheres Verwalten sensibler Daten (SSD) > SSD-Regeln.

c. Klicken Sie auf **Übernehmen**. Die Datei wird aktualisiert oder gesichert.

SCHRITT 5 Wenn Sie **über SCP (über SSH)** ausgewählt haben, finden Sie unter **SSH-Clientkonfiguration über die grafische Oberfläche** weitere Anweisungen. Geben Sie dann Werte für die folgenden Felder ein:

- **SSH-Remoteserverauthentifizierung**: Zum Deaktivieren der SSH-Serverauthentifizierung (standardmäßig deaktiviert) klicken Sie auf **Bearbeiten**. Daraufhin gelangen Sie zur Seite **SSH-Serverauthentifizierung**, um dies zu konfigurieren. Anschließend kehren Sie zu dieser Seite zurück. Über die Seite **SSH-Serverauthentifizierung** können Sie eine SSH-Benutzerauthentifizierungsmethode (Kennwort oder öffentlicher/privater Schlüssel) auswählen, einen Benutzernamen und ein Kennwort für das Gerät festlegen (wenn die Kennwortmethode ausgewählt ist) und bei Bedarf einen RSA- oder DSA-Schlüssel generieren.

SSH-Clientauthentifizierung: Für die Clientauthentifizierung gibt es folgende Möglichkeiten:

- **Systemanmeldeinformationen für SSH-Client verwenden**: Legt permanente SSH-Benutzeranmeldeinformationen fest. Klicken Sie auf **Systemanmeldeinformationen**, um zur Seite SSH-Benutzerauthentifizierung zu wechseln, auf der Sie den Benutzer und das Kennwort zur zukünftigen Verwendung festlegen können.
- **Einmalige Anmeldeinformationen für SSH-Client verwenden**: Geben Sie Folgendes ein:
  - *Benutzername*: Geben Sie einen Benutzernamen für diese Kopieraktion ein.
  - *Kennwort*: Geben Sie ein Kennwort für diese Kopieraktion ein.
- **Speichermethode**: Wählen Sie aus, ob die Systemkonfigurationsdatei gesichert oder wiederhergestellt werden soll.
- **SCP-Serverdefinition**: Wählen Sie aus, ob der SCP-Server anhand der **IP-Adresse** oder des **Domänennamens** angegeben wird.
- **IP-Version**: Legen Sie fest, ob eine IPv4- oder eine IPv6-Adresse verwendet wird.
- **IPv6-Adresstyp**: Wählen Sie den IPv6-Adresstyp aus (wenn dieser verwendet wird). Folgende Optionen sind möglich:
  - *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
  - *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.
- **Link-Local-Schnittstelle**: Wählen Sie in der Liste die Link-Local-Schnittstelle aus.
- **IP-Adresse/Name des SCP-Servers**: Geben Sie die IP-Adresse oder den Domänennamen des SCP-Servers ein.

Wenn Sie als **Speichermethode** die Option *Herunterladen* auswählen (Ersetzen der Datei im Gerät durch eine neue Version von einem anderen Gerät), geben Sie Werte für folgende Felder ein.

- **Name der Quelldatei**: Geben Sie den Namen der Quelldatei ein.
- **Typ der Zieldatei**: Wählen Sie den Typ der Konfigurationsdatei aus. Es werden nur gültige Dateitypen angezeigt. (Die Dateitypen werden im Abschnitt **Dateien und Dateitypen** beschrieben).

Wenn Sie für **Speichermethode** die Option *Sicherung* (Kopieren einer Datei in ein anderes Gerät) auswählen, geben Sie Werte für die folgenden Felder ein (zusätzlich zu den oben aufgeführten Feldern):

- **Typ der Quelldatei**: Wählen Sie den Typ der Konfigurationsdatei aus. Es werden nur gültige Dateitypen angezeigt. (Die Dateitypen werden im Abschnitt **Dateien und Dateitypen** beschrieben).
- **Sensible Daten**: Wählen Sie aus, wie sensible Daten in die Sicherungsdatei aufgenommen werden sollen. Folgende Optionen stehen zur Verfügung:
  - *Ausschließen*: Sensible Daten werden nicht in die Sicherungsdatei aufgenommen.
  - *Verschlüsselt*: Sensible Daten werden in verschlüsselter Form in die Sicherungsdatei aufgenommen.
  - *Unverschlüsselt*: Sensible Daten werden in unverschlüsselter Form in die Sicherungsdatei aufgenommen.

  HINWEIS Die verfügbaren Optionen für sensible Daten werden durch die SSD-Regeln des aktuellen Benutzers bestimmt. Details finden Sie auf der Seite Sicheres Verwalten sensibler Daten (SSD) > SSD-Regeln.
- **Name der Zieldatei**: Name der Datei, in die die Daten kopiert werden.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die Datei wird aktualisiert oder gesichert.

Konfigurationsdateieigenschaften

Die Seite „Konfigurationsdateieigenschaften“ zeigt an, wann verschiedene Systemkonfigurationsdateien erstellt wurden. Außerdem können Sie die Startkonfigurationsdatei und die Backup-Konfigurationsdatei löschen. Die anderen Konfigurationsdateitypen können Sie nicht löschen.

HINWEIS Wenn das Gerät im Stack-Modus betrieben wird, werden die Konfigurationsdateien der Mastereinheit verwendet.

So legen Sie fest, ob Spiegelkonfigurationsdateien erstellt werden, löschen Konfigurationsdateien und zeigen an, wann Konfigurationsdateien erstellt wurden:

SCHRITT 1 Klicken Sie auf **Administration** > **Dateiverwaltung** > **Konfigurationsdateieigenschaften**.

Auf dieser Seite werden folgende Felder angezeigt:

- **Name der Konfigurationsdatei**: Der Typ der Systemdatei.
- **Erstellungszeit**: Datum und Uhrzeit der letzten Dateibearbeitung.

SCHRITT 2 Deaktivieren Sie bei Bedarf die Option **Automatische Spiegelkonfiguration**. Damit wird die automatische Erstellung von Spiegelkonfigurationsdateien deaktiviert. Wenn Sie diese Funktion deaktivieren, wird die vorhandene Spiegelkonfigurationsdatei gegebenenfalls gelöscht. Eine Beschreibung der Spiegeldateien und Gründe für das Deaktivieren der automatischen Erstellung von Spiegelkonfigurationsdateien finden Sie unter **Systemdateien**.

SCHRITT 3 Wählen Sie bei Bedarf die Startkonfiguration und/oder die Backup-Konfiguration aus und klicken Sie auf **Dateien löschen**, um diese Dateien zu löschen.

Konfiguration kopieren/speichern

Wenn Sie in einem Fenster auf **Übernehmen** klicken, werden Ihre Änderungen an den Konfigurationseinstellungen des Geräts *nur* in der aktuellen Konfiguration gespeichert. Um die Parameter in der aktuellen Konfiguration zu erhalten, müssen Sie die aktuelle Konfiguration in einen anderen Konfigurationstyp kopieren oder auf einem anderen Gerät speichern.

VORSICHT Wenn Sie die aktuelle Konfiguration nicht in die Startkonfiguration oder in eine andere Konfigurationsdatei kopieren, gehen alle Änderungen seit dem letzten Speichern der Datei verloren, wenn das Gerät neu gestartet wird.

Folgende Kopierkombinationen sind für interne Dateien zulässig:

- Kopieren aus der ausgeführten Konfiguration in die Startkonfiguration oder Backup-Konfiguration.
- Kopieren aus der Startkonfiguration in die aktuelle Konfiguration, Startkonfiguration oder Backup-Konfiguration.

- Kopieren aus der Backup-Konfiguration in die aktuelle Konfiguration, Startkonfiguration oder Backup-Konfiguration.
- Kopieren aus der Spiegelkonfiguration in die aktuelle Konfiguration, Startkonfiguration oder Backup-Konfiguration.

So kopieren Sie einen Konfigurationsdateityp in einen anderen Konfigurationsdateityp:

SCHRITT 1 Wählen Sie **Administration** > **Dateiverwaltung** > **Konfiguration kopieren/speichern**.

SCHRITT 2 Wählen Sie unter **Name der Quelldatei** die zu kopierende Datei aus. Es werden nur gültige Dateitypen angezeigt (siehe Beschreibung im Abschnitt **Dateien und Dateitypen**).

SCHRITT 3 Wählen Sie den **Namen der Zieldatei** aus, die Sie mit der Quelldatei überschreiben möchten.

SCHRITT 4 Wählen Sie die Option **Sensible Daten**, wenn Sie eine Konfigurationsdatei sichern, und wählen Sie eines der folgenden Formate für die Sicherungsdatei aus.

- **Ausschließen**: Sensible Daten werden nicht in die Sicherungsdatei aufgenommen.
- **Verschlüsselt**: Sensible Daten werden in verschlüsselter Form in die Sicherungsdatei aufgenommen.
- **Unverschlüsselt**: Sensible Daten werden in unverschlüsselter Form in die Sicherungsdatei aufgenommen.

HINWEIS Die verfügbaren Optionen für sensible Daten werden durch die SSD-Regeln des aktuellen Benutzers bestimmt. Details finden Sie auf der Seite Sicheres Verwalten sensibler Daten (SSD) > SSD-Regeln.

SCHRITT 5 Das Feld **Blinkendes Speichersymbol** gibt an, ob ein Symbol blinkt, wenn nicht gespeicherte Daten vorhanden sind. Zum Deaktivieren bzw. Aktivieren dieser Funktion klicken Sie auf **Blinkendes Speichersymbol aktivieren/deaktivieren**.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die Datei wird kopiert.

Automatische Konfiguration und Image-Aktualisierung über DHCP

Mit der Funktion „Automatische Konfiguration und Image-Aktualisierung“ können Sie Switches der Serien Cisco Small Business 200, 300 und 500 in einem Netzwerk auf einfache Weise automatisch konfigurieren und deren Firmware aktualisieren. Mit diesem Prozess kann der Administrator remote sicherstellen, dass die Konfiguration und Firmware dieser Geräte im Netzwerk auf dem aktuellen Stand sind.

Diese Funktion umfasst folgende Bestandteile:

- **Automatische Image-Aktualisierung**: Automatischer Download eines Firmware-Images von einem remoten TFTP/SCP-Server. Im Anschluss an den automatischem Konfigurations- und Image-Aktualisierungsprozess startet das Gerät selbständig neu und lädt das Firmware-Image.
- **Automatische Konfiguration**: Automatischer Download einer Konfigurationsdatei von einem remoten TFTP-Server. Im Anschluss an den automatischem Konfigurations- und Image-Aktualisierungsprozess startet das Gerät selbständig neu und lädt die Konfigurationsdatei.

HINWEIS Werden sowohl „Automatische Image-Aktualisierung“ als auch „Automatische Konfiguration“ angefordert, wird zunächst die automatische Image-Aktualisierung durchgeführt. Nach dem Neustart erfolgt dann die automatische Konfiguration und schließlich ein letzter Neustart.

Wenn Sie diese Funktion verwenden möchten, müssen Sie einen DHCP-Server im Netzwerk mit den Speicherorten und Namen der Konfigurationsdatei und des Firmware-Images der Geräte konfigurieren. Die Geräte im Netzwerk werden standardmäßig als DHCP-Clients konfiguriert. Bei der Zuordnung der IP-Adressen durch den DHCP-Server erhalten die Geräte zusätzlich Informationen zur Konfigurationsdatei und zum Firmware-Image. Wenn sich die Konfigurationsdatei und/oder das Firmware-Image von den zurzeit auf dem Gerät verwendeten Dateien unterscheiden, führt das Gerät nach dem Download der Datei und/oder des Images einen Neustart durch. In diesem Abschnitt werden diese Prozesse beschrieben.

Die Funktion zur automatischen Aktualisierung und Konfiguration stellt sicher, das die Konfigurationsdateien und Firmware-Images der Geräte im Netzwerk stets auf dem neuesten Stand sind. Darüber hinaus ermöglicht sie eine schnelle Installation neuer Geräte im Netzwerk, da ein Gerät im Auslieferungszustand so konfiguriert ist, dass es seine Konfigurationsdatei und sein Software-Image ohne jeglichen manuellen Eingriff vom Systemadministrator abruft. Wenn das Gerät erstmals eine IT-Adresse vom DHCP-Server anfordert, lädt es die vom DHCP-Server angegebene Konfigurationsdatei und/oder das angegebene Image herunter und startet selbständig neu.

Der Prozess „Automatische Konfiguration“ unterstützt das Herunterladen einer Konfigurationsdatei, die sensible Daten, wie RADIUS-Serverschlüssel und SSH-/SSL-Schlüssel, enthält. Verwenden Sie hierzu die Funktionen Secured Copy Protocol (SCP) und Secure Sensitive Data (SSD). (Siehe auch **SSH-Clientauthentifizierung** und **Sicherheit: Sicheres Verwalten sensibler Daten (SSD)**).

Downloadprotokolle (TFTP oder SCP)

Konfigurationsdateien und Firmware-Images können entweder von einem TFTP-Server oder von einem SCP-Server heruntergeladen werden.

Der Benutzer konfiguriert das zu verwendende Protokoll wie folgt:

- **Automatisch nach Dateierweiterung**: (Standard) Wenn diese Option aktiviert ist, verweist eine benutzerdefinierte Dateierweiterung darauf, dass Dateien mit dieser Erweiterung via SCP (über SSH) heruntergeladen werden, während alle anderen Dateien über TFTP heruntergeladen werden. Wenn beispielsweise die Dateierweiterung *.xyz* angegeben ist, werden Dateien mit der Erweiterung *.xyz* mit SCP heruntergeladen und Dateien mit anderen Erweiterungen werden mit TFTP heruntergeladen. Die Standarderweiterung ist .scp.
- **Nur TFTP**: Der Download erfolgt unabhängig von der Dateinamenserweiterung der Konfigurationsdatei über TFTP.
- **Nur SCP**: Der Download erfolgt unabhängig von der Dateinamenserweiterung der Konfigurationsdatei über SCP (über SSH).

SSH-Clientauthentifizierung

SCP ist SSH-basiert. Die SSH-Remoteserverauthentifizierung ist standardmäßig deaktiviert, sodass das Gerät im Auslieferungszustand jeden SSH-Remoteserver akzeptiert. Sie können die SSH-Remoteserverauthentifizierung aktivieren, so dass nur Server verwendet werden können, die in der Liste der vertrauenswürdigen Server enthalten sind.

SSH-Clientauthentifizierungsparameter sind erforderlich, damit der Client (d. h. das Gerät) auf den SSH-Server zugreifen kann. Die Standardparameter für die SSH-Clientauthentifizierung lauten:

- SSH-Authentifizierungsmethode: Anhand von Benutzername und Kennwort
- SSH-Benutzername: „anonymous“
- SSH-Kennwort: „anonymous“

HINWEIS Die SSH-Clientauthentifizierungsparameter können auch verwendet werden, wenn Sie eine Datei manuell herunterladen (d. h. nicht über die Funktion für die Automatische DHCP-Konfiguration und Image-Aktualisierung).

Prozess zur automatischen Konfiguration und Image-Aktualisierung

Die automatische DHCP-Konfiguration verwendet gegebenenfalls den Namen und die Adresse des Konfigurationsservers und der Konfigurationsdatei in den empfangenen DHCP-Nachrichten. Zusätzlich verwendet die DHCP-Image-Aktualisierung gegebenenfalls den Namen der indirekten Firmwaredatei in den Nachrichten. Diese Informationen sind als DHCP-Optionen in den **Angebotsnachrichten** von den DHCPv4-Servern und in den **Informationsantworten** von den DHCPv6-Servern angegeben.

Sollten diese Informationen nicht in den DHCP-Servernachrichten enthalten sein, werden Sicherungsdaten abgerufen, die auf der Seite „Automatische DHCP-Konfiguration und Image-Aktualisierung“ konfiguriert wurden.

Bei der Auslösung des Prozesses zur automatischen Konfiguration und Image-Aktualisierung (siehe **Auslöser für die automatische Konfiguration und Image-Aktualisierung**), finden die nachstehend beschriebenen Ereignisse statt.

Die automatische Image-Aktualisierung wird gestartet:

- Der Switch verwendet gegebenenfalls den Namen der indirekten Datei aus der Option 125 (DHCPv4) und der Option 60 (DHCPv6) aus den empfangenen DHCP-Nachrichten.
- Hat der DHCP-Server den indirekten Dateinamen der Firmware-Image-Datei nicht gesendet, wird der Name der indirekten Backup-Image-Datei (von der Seite „Automatische DHCP-Konfiguration und Image-Aktualisierung“) verwendet.
- Der Switch lädt die indirekte Image-Datei herunter und extrahiert den Namen der Image-Datei des TFTP/SCP-Servers aus ihr.
- Der Switch vergleicht die Version des Images vom TFTP-Server mit der Version des aktiven Images des Switches.
- Sollten sich diese Versionen unterscheiden, wird die neue Version auf das inaktive Image geladen und ein Neustart durchgeführt und das inaktive Image wird zum aktiven Image.
- Bei Verwendung des SCP-Protokolls wird eine SYSLOG-Nachricht generiert, die auf den anstehenden Neustart hinweist.
- Bei Verwendung des SCP-Protokolls wird eine SYSLOG-Nachricht generiert, die den Abschluss des Prozesses zur automatischen Aktualisierung bestätigt.
- Bei Verwendung des TFTP-Protokolls generiert der Kopiervorgang SYSLOG-Nachrichten.

Die automatische Konfiguration wird gestartet:

- Das Gerät verwendet gegebenenfalls den Namen und die Adresse des TFTP/SCP-Servers und den Namen und die Adresse der Konfigurationsdatei (DHCPv4-Optionen: 66,150 und 67; DHCPv6-Optionen: 59 und 60) aus der empfangenen DHCP-Nachricht.
- Sollte der DHCP-Server die Informationen nicht senden, werden die IP-Adresse bzw. der Name des Backupservers und der Name der Backupkonfigurationsdatei (von der Seite „Automatische DHCP-Konfiguration und Image-Aktualisierung“ verwendet.
- Die neue Konfigurationsdatei wird verwendet, wenn sich ihr Name vom Namen der zuvor auf dem Gerät verwendeten Konfigurationsdatei unterscheidet oder das Gerät noch nie konfiguriert wurde.
- Das Gerät wird nach Abschluss des Prozesses zur automatischen Konfiguration und Image-Aktualisierung mit der neuen Konfiguration neu gestartet.
- Der Kopiervorgang generiert SYSLOG-Nachrichten.

Fehlende Optionen

- Wenn der DHCP-Server bei einer DHCP-Option keine TFTP/SCP-Serveradresse gesendet hat und der Parameter für die Adresse des Backup-TFTP-Servers nicht konfiguriert wurde, geschieht Folgendes:
  - ***SCP***: Die automatische Konfiguration wird angehalten.
  - ***TFTP***: Das Gerät sendet TFTP-Anforderungsnachrichten an eine eingeschränkte Broadcast-Adresse (IPv4) oder an alle Knotenadressen (IPv6) seiner IP-Schnittstellen und fährt beim ersten antwortenden TFTP-Server mit der automatischen Konfiguration und der automatischen Image-Aktualisierung fort.

Auswahl des Downloadprotokolls

- Das Kopierprotokoll (SCP/TFTP) wird wie unter **Downloadprotokolle (TFTP oder SCP)** beschrieben ausgewählt.

SCP

- Beim Herunterladen über SCP akzeptiert das Gerät jeden angegebenen SCP-/SSH-Server (ohne Authentifizierung), wenn eine der folgenden Aussagen zutrifft:
  - Der SSH-Serverauthentifizierungsprozess ist deaktiviert. Die SSH-Serverauthentifizierung ist standardmäßig deaktiviert, damit Konfigurationsdateien für Geräte mit werkseitiger Standardkonfiguration (z. B. Geräte im Auslieferungszustand) heruntergeladen werden können.
  - Der SSH-Server ist in der Liste der vertrauenswürdigen SSH-Server konfiguriert.

  Wenn der SSH-Serverauthentifizierungsprozess aktiviert ist und der SSH-Server nicht in der Liste der vertrauenswürdigen SSH-Server gefunden wird, wird der automatische Konfigurationsprozess angehalten.
- Wenn die Informationen verfügbar sind, wird zum Download der Konfigurationsdatei oder des Images auf den SCP-Server zugegriffen.

Auslöser für die automatische Konfiguration und Image-Aktualisierung

Die automatische Konfiguration und Image-Aktualisierung über DHCPv6 wird ausgelöst, wenn die folgenden Bedingungen erfüllt sind:

- Die IP-Adresse des Geräts wird beim Neustart dynamisch zugewiesen bzw. erneuert, durch eine administrative Maßnahme explizit erneuert oder aufgrund einer abgelaufenen Lease automatisch erneuert. Die explizite Erneuerung kann auf der Seite „IPv4-Schnittstelle“ aktiviert werden.
- Wenn die automatische Image-Aktualisierung aktiviert wurde, wird der Prozess zur automatischen Image-Aktualisierung ausgelöst, sobald der Name einer indirekten Image-Datei von einem DHCP-Server oder ein Name für eine indirekten Backup-Image-Datei konfiguriert wurde. „Indirekt“ bedeutet, dass es sich nicht um die Image-Datei handelt, sondern vielmehr um eine Datei, die den Namen des Pfads zum Image enthält.

- Bei aktivierter automatischer Konfiguration wird der automatische Konfigurationsprozess ausgelöst, sobald der Konfigurationsdateiname von einem DHCP-Server empfangen wird bzw. sobald ein Name für die Backupkonfigurationsdatei konfiguriert wurde.

Die automatische Konfiguration und Image-Aktualisierung über DHCPv6 wird ausgelöst, wenn folgende Bedingungen erfüllt sind:

- Ein DHCPv6-Server sendet Daten an das Gerät. Das geschieht in folgenden Fällen:
  - Wenn eine IPv6-fähige Schnittstelle als statusloser DHCPv6-Konfigurationsclient definiert ist.
  - Wenn der Server DHCPv6-Meldungen empfängt (z. B. wenn Sie auf der Seite IPv6-Schnittstellen auf **Neustart** klicken).
  - Wenn die DHCPv6-Daten vom Gerät aktualisiert werden.
  - Wenn der statuslose DHCPv6-Client aktiviert ist, nach dem Neustart des Geräts.
- Wenn die DHCPv6-Serverpakete die Option für den Konfigurationsdateinamen enthalten.
- Der Prozess zur automatischen Image-Aktualisierung wird ausgelöst, sobald der Name einer indirekten Image-Datei vom DHCP-Server oder ein Name der indirekten Backup-Image-Datei konfiguriert ist. „Indirekt“ bedeutet, dass es sich nicht um die Image-Datei handelt, sondern vielmehr um eine Datei, die den Namen des Pfads zum Image enthält.

Automatische Konfiguration und Image-Aktualisierung bei einem Stack

Der aktuelle Master eines Stacks ist für die automatische Konfiguration und Image-Aktualisierung des gesamten Stacks verantwortlich. Zur automatischen Konfiguration wird die neue Konfigurationsdatei auf die Mastereinheit heruntergeladen. Zur automatischen Image-Aktualisierung wird das inaktive Image der Mastereinheit mit dem neuen Image überschrieben. Nach dem Neustart wird das neue Image auf alle Einheiten des Stacks kopiert.

Sicherstellen einer einwandfreien Funktion

Damit sichergestellt ist, dass die Funktion zur automatischen Konfiguration und Image-Aktualisierung einwandfrei funktioniert, beachten Sie Folgendes:

- Eine Konfigurationsdatei, die auf dem TFTP-/SCP-Server abgelegt wird, muss die Datei- und Formatanforderungen einer unterstützten Konfigurationsdatei erfüllen. Der Typ und das Format der Datei werden geprüft, jedoch erfolgt vor dem Laden der Datei in die Startkonfiguration keine Validitätsprüfung der *Konfigurationsparameter*.
- Um bei IPv4 sicherzustellen, dass das Gerät die Konfigurations- und Image-Datei beim Prozess zur automatischen Konfiguration und Image-Aktualisierung ordnungsgemäß herunterlädt, sollte dem Gerät stets dieselbe IP-Adresse zugewiesen werden. Dadurch wird sichergestellt, dass das Gerät immer dieselbe IP-Adresse aufweist und dieselben Informationen für die automatische Konfiguration und Image-Aktualisierung erhält.

Automatische DHCP-Konfiguration und Image-Aktualisierung

Die folgenden Seiten der GUI dienen zur Konfiguration des Geräts:

- Administration > Dateiverwaltung > Automatische DHCP-Konfiguration und Image-Aktualisierung: Dient zum Konfigurieren des Geräts als DHCP-Client.
- Administration > Verwaltungsschnittstelle > IPv4-Schnittstelle (in L2) oder IP-Konfiguration > IPv4-Management und -Schnittstellen > IPv4-Schnittstellen (in L3): Dient zum Erneuern der IP-Adresse über DHCP, wenn sich das Gerät im Schicht-2-Systemmodus befindet.

Standardeinstellungen und Konfiguration

Dies sind die Standardwerte auf dem System:

- Automatische Konfiguration ist aktiviert.
- Automatische Image-Aktualisierung ist aktiviert.
- Das Gerät ist als DHCP-Client aktiviert.
- Die SSH-Remoteserverauthentifizierung ist deaktiviert.

Vorbereitung des Prozesses zur automatischen Konfiguration und Image-Aktualisierung

Damit Sie diese Funktion verwenden können, muss das Gerät entweder als DHCPv4- oder als DHCPv6-Client konfiguriert sein. Der auf dem Gerät definierte DHCP-Clienttyp korreliert mit dem Schnittstellentyp, der auf dem Gerät definiert ist.

Serverseitige Vorbereitung für die automatische Konfiguration

Bereiten Sie DHCP- und TFTP/SCP-Server wie folgt vor:

TFTP/SCP-Server

- Stellen Sie eine Konfigurationsdatei ins Arbeitsverzeichnis. Diese Datei können Sie erstellen, indem Sie eine Konfigurationsdatei von einem Gerät kopieren. Beim Starten des Geräts wird diese Datei zur ausgeführten Konfigurationsdatei.

DHCP-Server

Konfigurieren Sie den DHCP-Server mit folgenden Optionen:

- DHCPv4:
  - 66 (einzelne Serveradresse) oder 150 (Liste von Serveradressen)
  - 67 (Name der Konfigurationsdatei)

- DHCPv6
  - Option 59 (Serveradresse)
  - Optionen 60 (Name der Konfigurationsdatei plus Name einer indirekten Image-Datei, getrennt durch ein Komma)

Vorbereitungen für die automatische Image-Aktualisierung

Bereiten Sie die DHCP- und TFTP/SCP-Server wie folgt vor:

TFTP/SCP-Server

1. Erstellen Sie ein Unterverzeichnis im Hauptverzeichnis. Legen Sie dort eine Software-Image-Datei ab.
2. Erstellen Sie eine indirekte Datei mit einem Pfad und dem Namen der Firmwareversion (z. B. indirect-cisco.txt mit dem Inhalt cisco\cisco-version.ros).
3. Kopieren Sie diese indirekte Datei in das Hauptverzeichnis des TFTP/SCP-Servers.

DHCP-Server

Konfigurieren Sie den DHCP-Server mit den folgenden Optionen:

- DHCPv4: Option 125 (indirekter Dateiname)
- DHCPv6: Optionen 60 (Name der Konfigurationsdatei plus Name einer indirekten Image-Datei, getrennt durch ein Komma)

DHCP-Client-Workflow

SCHRITT 1 Konfigurieren Sie auf der Seite „Administration > Dateiverwaltung > Automatische DHCP-Konfiguration“ die Parameter für die automatische Konfiguration und/oder automatische Image-Aktualisierung.

SCHRITT 2 Legen Sie auf der Seite **Definieren einer IPv4-Schnittstelle im Schicht-2-Systemmodus** oder **Definieren einer IPv4-Schnittstelle im Schicht-3-Systemmodus** den IP-Adresstyp auf „Dynamisch“ fest und/oder definieren Sie das Gerät auf der Seite **IPv6-Schnittstelle** als statusfreien DHCPv6-Client.

Webkonfiguration

So konfigurieren Sie die automatische Konfiguration und/oder die automatische Aktualisierung:

SCHRITT 1 Klicken Sie auf **Administration** > **Dateiverwaltung** > **Automatische DHCP-Konfiguration und Image-Aktualisierung**.

SCHRITT 2 Geben Sie die Werte ein.

- **Automatische Konfiguration über DHCP**: Wählen Sie dieses Feld aus, um die automatische DHCP-Konfiguration zu aktivieren. Diese Funktion ist standardmäßig aktiviert, kann aber hier deaktiviert werden.
- **Downloadprotokoll**: Wählen Sie eine der folgenden Optionen aus:
  - *Automatisch nach Dateierweiterung*: Wählen Sie diese Option aus, um anzugeben, dass die automatische Konfiguration abhängig von der Erweiterung der Konfigurationsdatei das TFTP- oder SCP-Protokoll verwendet. Wenn diese Option ausgewählt ist, muss die Erweiterung der Konfigurationsdatei nicht zwangsläufig angegeben werden. Wenn sie nicht angegeben ist, wird die Standarderweiterung (siehe unten) verwendet.
  - *Dateierweiterung für SCP*: Wenn **Automatisch nach Dateierweiterung** ausgewählt ist, können Sie hier eine Dateierweiterung angeben. Alle Dateien mit dieser Erweiterung werden über SCP heruntergeladen. Wenn keine Erweiterung eingegeben ist, wird die Standarddateierweiterung **.scp** verwendet.
  - *Nur TFTP*: Wählen Sie diese Option aus, um anzugeben, dass für die automatische Konfiguration nur das TFTP-Protokoll verwendet werden soll.
  - *Nur SCP*: Wählen Sie diese Option aus, um anzugeben, dass für die automatische Konfiguration nur das SCP-Protokoll verwendet werden soll.
- **Automatische Image-Aktualisierung über DHCP**: Wählen Sie dieses Feld aus, um die Aktualisierung des Firmware-Images vom DHCP-Server zu ermöglichen. Diese Funktion ist standardmäßig aktiviert, kann aber hier deaktiviert werden.
- **Downloadprotokoll**: Wählen Sie eine der folgenden Optionen aus:
  - *Automatisch nach Dateierweiterung*: Wählen Sie diese Option aus, um anzugeben, dass die automatische Aktualisierung abhängig von der Erweiterung der Image-Datei das TFTP- oder SCP-Protokoll verwendet. Wenn diese Option ausgewählt ist, muss die Erweiterung der Image-Datei nicht zwangsläufig angegeben werden. Wenn sie nicht angegeben ist, wird die Standarderweiterung (siehe unten) verwendet.
  - *Dateierweiterung für SCP*: Wenn **Automatisch nach Dateierweiterung** ausgewählt ist, können Sie hier eine Dateierweiterung angeben. Alle Dateien mit dieser Erweiterung werden über SCP heruntergeladen. Wenn keine Erweiterung eingegeben ist, wird die Standarddateierweiterung **.scp** verwendet.

  - *Nur TFTP*: Wählen Sie diese Option aus, um anzugeben, dass für die automatische Aktualisierung nur das TFTP-Protokoll verwendet werden soll.
  - *Nur SCP*: Wählen Sie diese Option aus, um anzugeben, dass für die automatische Aktualisierung nur das SCP-Protokoll verwendet werden soll.

- **SSH-Einstellungen für SCP**: Wenn Sie SCP zum Herunterladen der Konfigurationsdateien verwenden, wählen Sie eine der folgenden Optionen aus:
- **SSH-Remoteserverauthentifizierung**: Klicken Sie auf den Link **Aktivieren/Deaktivieren**, um zur Seite SSH-Serverauthentifizierung zu navigieren. Dort können Sie die Authentifizierung des SSH-Servers aktivieren, der für den Download verwendet werden soll, und bei Bedarf den vertrauenswürdigen SSH-Server eingeben.
- **SSH-Clientauthentifizierung**: Klicken Sie auf den Link Systemanmeldeinformationen, um auf der Seite SSH-Benutzerauthentifizierung Benutzeranmeldeinformationen einzugeben.
- **Backupserverdefinition**: Wählen Sie aus, ob der Backupserver **Nach IP-Adresse** oder **Nach Name** konfiguriert wird.
- **IP-Version**: Legen Sie fest, ob eine IPv4- oder eine IPv6-Adresse verwendet wird.
- **IPv6-Adresstyp**: Wählen Sie den IPv6-Adresstyp aus (falls IPv6 verwendet wird). Folgende Optionen sind möglich:
  - **Link Local**: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix FE80, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
  - **Global**: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.
- **Link Local-Schnittstelle**: Wählen Sie in der Liste die Link Local-Schnittstelle aus (wenn IPv6 verwendet wird).

SCHRITT 3 Geben Sie die folgenden optionalen Informationen ein, die verwendet werden, wenn der DHCP-Server die erforderlichen Informationen nicht bereitstellt.

- **Backupserver-IP-Adresse/Name**: Geben Sie die IP-Adresse oder den Namen des Backupservers ein.
- **Name der Backupkonfigurationsdatei**: Geben Sie den Namen der Backupkonfigurationsdatei ein.
- **Name der indirekten Backup-Image-Datei**: Geben Sie den Namen einer indirekten Image-Datei an, die verwendet werden soll. Dies ist eine Datei, die den Pfad zum Image enthält. Ein Beispiel für einen Namen einer indirekten Image-Datei: indirect-cisco.scp. Diese Datei enthält den Pfad und den Namen des Firmware-Images.

Die folgenden Felder werden angezeigt:

- **Letzte IP-Adresse von Server für automatische Konfiguration**: Die Adresse des letzten Backupservers.
- **Name der letzten Datei für automatische Konfiguration**: Der Name der letzten Konfigurationsdatei.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Parameter werden in die aktuelle Konfigurationsdatei kopiert.

6

Administration: Stack-Verwaltung

In diesem Abschnitt wird die Verwaltung von Stacks beschrieben. Die folgenden Themen werden behandelt:

- **Übersicht**
- **Einheitentypen im Stack**
- **Stack-Topologie**
- **Zuordnung von Einheiten-IDs**
- **Masterauswahlprozess**
- **Stack-Änderungen**
- **Fehler bei einer Einheit im Stack**
- **Automatische Softwaresynchronisierung im Stack**
- **Stack-Einheitenmodus**
- **Stack-Ports**
- **Standardkonfiguration**
- **Interaktionen mit anderen Funktionen**
- **Systemmodi**

Übersicht

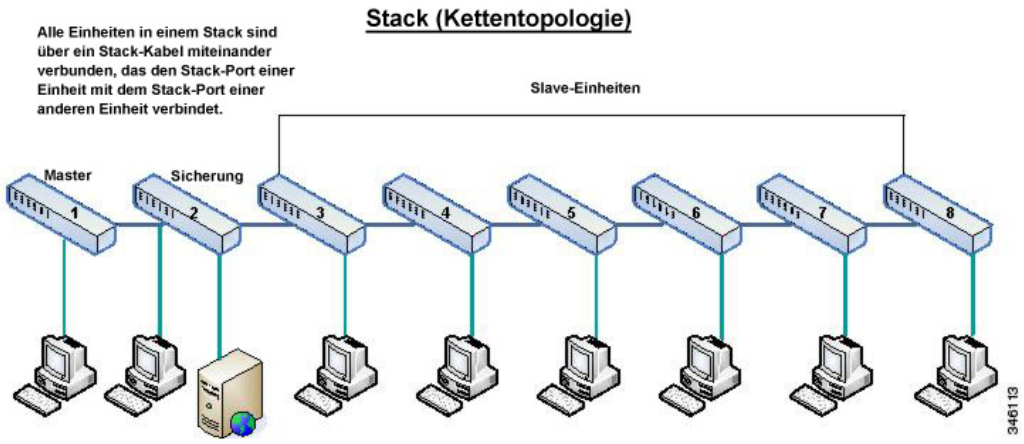
Geräte können entweder eigenständig eingesetzt werden (Standalone-Modus) oder im Rahmen verschiedener Stacking-Modi zu Stacks aus bis zu acht Geräten verbunden werden (siehe **Stack-Einheitenmodus**).

Die Geräte (Einheiten) in einem Stack werden über Stack-Ports verbunden. Diese Geräte werden dann gemeinsam als ein einziges logisches Gerät verwaltet. In manchen Fällen können Stack-Ports Mitglieder in einer LAG (Link Aggregation Group, Link-Aggregationsgruppe) werden, wodurch sich die Bandbreite des Stack-Ports erhöht. Weitere Informationen hierzu finden Sie unter **Stack-Port-Link-Aggregation**.

Der Stack basiert auf einem Modell mit einem einzigen Master/Backup und mehreren Slaves.

Die folgende Abbildung zeigt acht zu einem Stack verbundene Geräte:

Stack-Architektur (Kettentopologie)



Ein Stack bietet die folgenden Vorteile:

- Die Netzwerkkapazität kann dynamisch erweitert oder verringert werden. Der Administrator kann durch Hinzufügen einer Einheit die Anzahl der Ports im Stack dynamisch erhöhen und diesen weiterhin zentral verwalten. Entsprechend können Einheiten entfernt werden, um die Netzwerkkapazität zu verringern.
- Das Stack-System unterstützt Redundanz auf folgende Weise:
  - Die Backup-Einheit wird zum Master des Stacks, wenn beim ursprünglichen Master Fehler auftreten.
  - Das Stack-System unterstützt zwei Arten von Topologien: Kette (siehe **„Stack-Architektur (Kettentopologie)“**) und Ring (siehe **„Stack in Ringtopologie“**). Wenn in einer Ringtopologie an einem der Stack-Ports Fehler auftreten, funktioniert der Stack in der Kettentopologie weiter (siehe **Stack-Topologie**).
  - An den Ports in einem Ring-Stack wird ein Prozess unterstützt, der als Fast Stack-Link-Failover bezeichnet wird und die Dauer der Datenpaketverluste bei Fehlern an einem der Stack-Ports reduzieren soll. Bis zur Umstellung des Stacks auf die neue Kettentopologie führt der zurzeit inaktive Stack-Port für die Pakete, die über ihn gesendet werden sollten, mithilfe der verbleibenden Stacking-Links einen Loopback aus, damit die Pakete ihr Ziel erreichen. Beim Fast Stack-Link-Failover bleiben die Master-/Backup-Einheiten aktiv und funktionsfähig.

    HINWEIS Die Funktion „Fast Stack-Link-Failover“ ist nur für ein oder zwei Stacks aktiv. Weitere Informationen hierzu finden Sie unter **Stack-Port-Link-Aggregation**.

Einheitentypen im Stack

Ein Stack besteht aus maximal acht Einheiten. Eine Einheit in einem Stack weist einen der folgenden Typen auf:

- **Master**: Die ID der Mastereinheit muss 1 oder 2 entsprechen. Der Stack wird über die Mastereinheit verwaltet, die sich selbst, die Backup-Einheit und die Slave-Einheiten verwaltet.
- **Backup**: Wenn die Mastereinheit ausfällt, übernimmt die Backup-Einheit deren Funktion (Switchover). Die ID der Backup-Einheit muss 1 oder 2 entsprechen.
- **Slave**: Diese Einheiten werden von der Mastereinheit verwaltet.

Damit eine Gruppe von Einheiten als Stack fungiert, muss eine als Master aktivierte Einheit vorhanden sein. Wenn bei der als Master aktivierten Einheit Fehler auftreten, bleibt der Stack funktionsfähig, solange eine Backup-Einheit vorhanden ist (die aktive Einheit, die die Masterrolle übernimmt).

Wenn zusätzlich zur Mastereinheit auch die Backup-Einheit ausfällt und nur noch die Slave-Einheiten funktionsfähig sind, stellen diese nach einer Minute ebenfalls ihre Funktion ein. Wenn Sie also beispielsweise ein Kabel an eine Slave-Einheit anschließen, die über einer Minute ohne Master gelaufen ist, dann wird die Verbindung nicht wieder hergestellt.

Abwärtskompatibilität bei der Anzahl der Einheiten im Stack

Ältere Versionen des Geräts unterstützten im Gegensatz zur aktuellen Version statt acht nur vier Einheiten. Ältere Softwareversionen können aktualisiert werden, ohne dass die Konfigurationsdateien geändert werden müssen.

Wird eine Firmwareversion, die keine Hybrid-Stack-Modi unterstützt, in den Stack geladen und der Stack neu gestartet, wird der Stack in den Modus Natives Stack zurückgesetzt. Wenn ein Gerät im Hybrid-Stack-Modus mit einer Firmwareversion geladen wird, die Hybrid-Stack-Modi nicht unterstützt, wird sein Modus auf den Standardsystemmodus (SG500X/EWS2-550X: L3 und L2, Sx500: L2) zurückgesetzt.

Bei manueller Konfiguration der Einheiten-IDs eines Stacks, werden Einheiten, deren ID größer als 4 ist, auf automatische Nummerierung umgestellt.

Einheiten-LEDs

Das Gerät verfügt über vier als 1, 2, 3 und 4 gekennzeichnete Kontrollleuchten (LEDs), die die IDs der einzelnen Einheiten anzeigen (Beispiel: für die Einheiten-ID=1 leuchtet nur LED1, alle anderen LEDs sind aus). Zur Unterstützung von Einheiten-IDs größer 4, wird die Anzeige entsprechend der Definition unten geändert:

- Einheiten 1 bis 4: die jeweilige LED (1-4) leuchtet.
- Einheit 5: LED 1 und 4 leuchten.

- Einheit 6: LED 2 und 4 leuchten.
- Einheit 7: LED 3 und 4 leuchten.
- Einheit 8: LED 1, 3 und 4 leuchten.

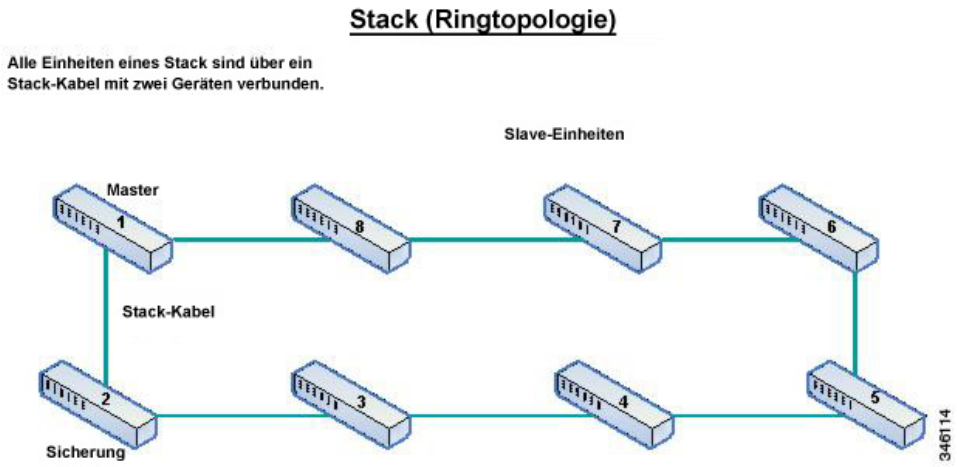
Stack-Topologie

Stack-Topologietypen

Die Einheiten in einem Stack können in einem der folgenden Topologietypen verbunden sein:

- **Kettentopologie**: Jede Einheit ist mit der benachbarten Einheit verbunden, aber zwischen der ersten und der letzten Einheit gibt es keine Kabelverbindung. Eine Kettentopologie ist in der Abbildung unter **„Stack-Architektur (Kettentopologie)“** gezeigt.
- **Ringtopologie**: Jede Einheit ist mit der benachbarten Einheit verbunden. Die letzte Einheit ist mit der ersten Einheit verbunden. In der folgenden Abbildung sehen Sie ein Stack aus acht Einheiten in Ringtopologie:

Stack in Ringtopologie



Eine Ringtopologie ist zuverlässiger als eine Kettentopologie. Der Ausfall einer Verbindung in einem Ring beeinträchtigt die Funktionsfähigkeit des Stacks nicht, wohingegen der Ausfall einer Verbindung in einer Kette dazu führt, dass der Stack unterbrochen wird.

Topologieerkennung

Ein Stack wird durch einen Prozess eingerichtet, der als Topologieerkennung bezeichnet wird. Der Prozess wird durch eine Änderung des Status (aktiv bzw. nicht aktiv) eines Ports ausgelöst.

Nachfolgend einige Beispiele für Ereignisse, die diesen Prozess auslösen:

- Ändern der Stack-Topologie von Ring in Kette.
- Zusammenführen von zwei Stacks in einem einzigen Stack.
- Aufteilen des Stacks.
- Einsetzen weiterer Slave-Einheiten in den Stack, beispielsweise weil die Einheiten vorher aufgrund eines Fehlers vom Stack getrennt wurden. Dies kann in einer Kettentopologie geschehen, wenn bei einer Einheit in der Mitte des Stacks ein Fehler auftritt.

Bei der Topologieerkennung tauschen die einzelnen Einheiten in einem Stack Pakete aus, die Topologieinformationen enthalten.

Nach Abschluss der Topologieerkennung enthält jede Einheit die Tabelle mit den Stack-Zuordnungsinformationen aller Einheiten im Stack.

Zuordnung von Einheiten-IDs

Nach Abschluss der Topologieerkennung wird jeder Einheit im Stack eine eindeutige Einheiten-ID zugeordnet.

Die Einheiten-ID können Sie auf der Seite „Systemmodus und Stack-Verwaltung“ folgendermaßen festlegen:

- **Automatisch (Autom.)**: Die Einheiten-ID wird durch den Topologieerkennungsprozess zugeordnet. Dies ist die Standardeinstellung.
- **Manuell**: Die Einheiten-ID wird manuell auf eine Ganzzahl von 1 bis 8 festgelegt.

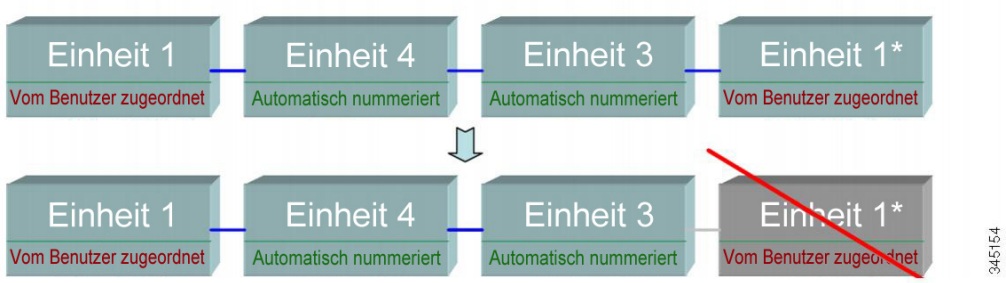
Doppelte Einheiten-IDs

Wenn Sie zwei separaten Einheiten die gleiche Einheiten-ID zuweisen, können Sie nur eine der Einheiten mit dieser Einheiten-ID dem Stack hinzufügen.

Wenn Sie die automatische Nummerierung ausgewählt haben, wird der doppelten Einheit eine neue Einheitennummer zugeordnet. Wenn Sie die automatische Nummerierung nicht ausgewählt haben, wird die doppelte Einheit heruntergefahren.

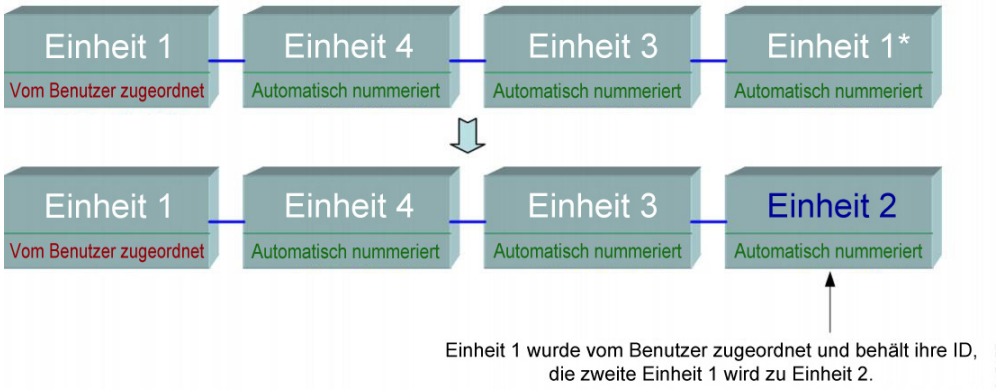
In der folgenden Abbildung sehen Sie zwei Einheiten, denen manuell die gleiche Einheiten-ID zugeordnet wurde. Einheit 1 wird nicht in den Stack integriert und wird heruntergefahren. Die Einheit war beim Masterauswahlprozess zwischen den als Master aktivierten Einheiten (1 und 2) nicht erfolgreich.

Herunterfahren der doppelten Einheit



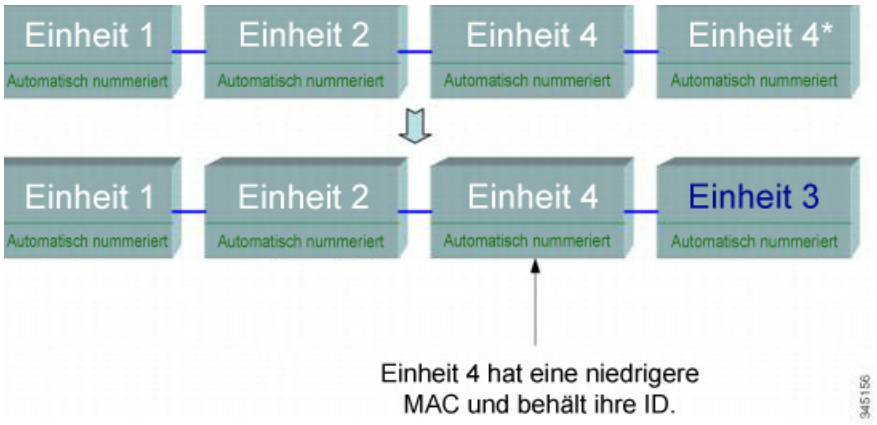
Die folgende Abbildung zeigt einen Fall, in dem eine der (automatisch nummerierten) doppelten Einheiten neu nummeriert wird.

Neu nummerierte doppelte Einheit



Die folgende Abbildung zeigt einen Fall, in dem eine der doppelten Einheiten neu nummeriert wird. Die Einheit mit der niedrigeren MAC behält ihre Einheiten-ID (eine Beschreibung dieses Prozesses finden Sie unter **Masterauswahlprozess**).

Doppelte Einheiten-IDs bei zwei Einheiten mit automatisch nummerierter Einheiten-ID



HINWEIS Wenn ein neuer Stack die maximale Anzahl an Einheiten (8) übersteigt, werden alle überzähligen Einheiten heruntergefahren.

Masterauswahlprozess

Die Mastereinheit wird aus den als Master aktivierten Einheiten (1 und 2) ausgewählt. Bei der Auswahl der Mastereinheit werden diese Faktoren mit der folgenden Priorität berücksichtigt:

- **Als Master erzwingen**: Wenn diese Option für eine Einheit aktiviert ist, wird die Einheit ausgewählt.
- **Systembetriebszeit**: Die als Master aktivierten Einheiten tauschen ihre Betriebszeit aus. Diese wird in Abschnitten von je zehn Minuten gemessen. Die Einheit, die mehr Abschnitte vorweisen kann, wird ausgewählt. Wenn beide Einheiten dieselbe Abschnittsanzahl aufweisen, aber die Einheiten-ID einer Einheit manuell festgelegt wurde, während die andere automatisch zugewiesen wurde, wird die Einheit mit der manuell definierten Einheiten-ID ausgewählt. Andernfalls wird die Einheit mit der niedrigsten Einheiten-ID ausgewählt. Wenn beide Einheiten-IDs identisch sind, wird die Einheit mit der niedrigeren MAC-Adresse ausgewählt. **Hinweis:** Die Betriebszeit der Backup-Einheit wird beibehalten, wenn diese im Rahmen des Switchover als Master ausgewählt wird.
- **Einheiten-ID**: Wenn beide Einheiten gleich viele Zeitabschnitte aufweisen, wird die Einheit mit der niedrigeren Einheiten-ID ausgewählt.
- **MAC-Adresse**: Wenn beide Einheiten-IDs identisch sind, wird die Einheit mit der niedrigeren MAC-Adresse ausgewählt.

HINWEIS Ein Stack ist nur funktionsfähig, wenn eine Mastereinheit vorhanden ist. Eine Mastereinheit ist definiert als die aktive Einheit, die die Masterrolle übernimmt. Der Stack muss nach dem Masterauswahlprozess eine Einheit 1 und/oder eine Einheit 2 enthalten. Anderenfalls wird der Stack einschließlich seiner Einheiten teilweise heruntergefahren. Dabei wird der Stack nicht vollständig ausgeschaltet, sondern die Funktionen zur Weiterleitung des Datenverkehrs werden angehalten.

Stack-Änderungen

In diesem Abschnitt werden verschiedene Ereignisse beschrieben, die eine Änderung am Stack verursachen können. Eine Stack-Topologie ändert sich in einem der folgenden Fälle:

- Mindestens eine Einheit wird mit dem Stack verbunden und/oder vom Stack getrennt.
- Der Link an einem der Stack-Ports ist aktiv oder nicht aktiv.
- Der Stack wechselt zwischen Ring- und Kettenformation.

Das Hinzufügen oder Entfernen von Einheiten in einem Stack löst Topologieänderungen, den Masterwahlprozess und/oder die Zuordnung von Einheiten-IDs aus.

Verbinden einer neuen Einheit

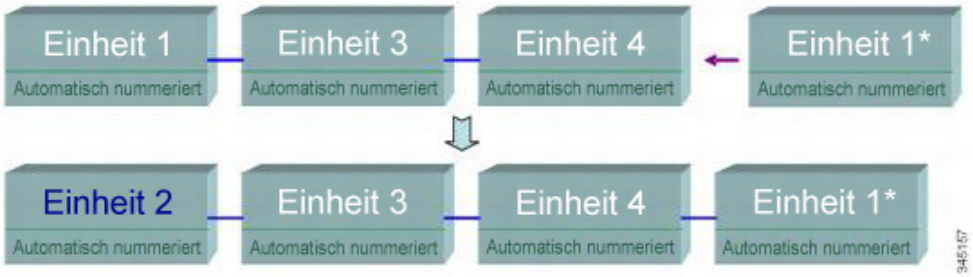
Beim Einsetzen einer Einheit in den Stack wird eine Änderung der Stack-Topologie ausgelöst. Die Einheiten-ID wird zugeordnet (bei automatischer Nummerierung) und die Konfiguration wird vom Master heruntergeladen.

Einer der folgenden Fälle kann eintreten, wenn Sie eine neue Einheit mit einem vorhandenen Stack verbinden:

- Es sind keine doppelten Einheiten-IDs vorhanden.
  - Einheiten mit benutzerdefinierten IDs behalten ihre Einheiten-ID.
  - Einheiten mit automatisch zugeordneten IDs behalten ihre Einheiten-ID.
  - Einheiten mit Werkseinstellungen erhalten automatisch Einheiten-IDs, beginnend bei der niedrigsten verfügbaren ID.
- Es ist mindestens eine doppelte Einheiten-ID vorhanden. Die automatische Nummerierung löst die Konflikte und ordnet Einheiten-IDs zu. Bei manueller Nummerierung behält nur eine Einheit ihre Einheiten-ID und die anderen werden heruntergefahren.
- Die Anzahl der Einheiten im Stack überschreitet die zulässige Anzahl. Die neuen Einheiten im Stack werden heruntergefahren und eine SYSLOG-Meldung wird generiert und auf der Mastereinheit angezeigt.

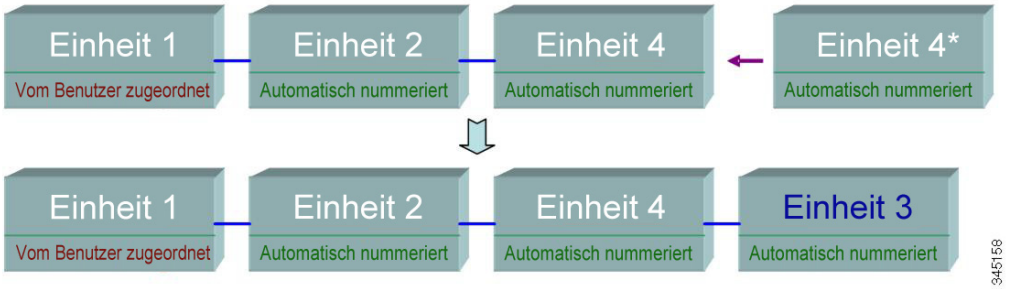
Die folgende Abbildung zeigt ein Beispiel für die automatische Nummerierung beim Hinzufügen einer als Master aktivierten Einheit zum Stack. Es gibt zwei Einheiten mit der Einheiten-ID 1. Mithilfe des Masterauswahlprozesses wird die am besten geeignete Einheit als Mastereinheit ausgewählt. Die beste Einheit ist diejenige, die die meisten Betriebszeitabschnitte von 10 Minuten vorweisen kann. Die andere Einheit wird als Backup festgelegt.

Automatisch nummerierte als Master aktivierte Einheit



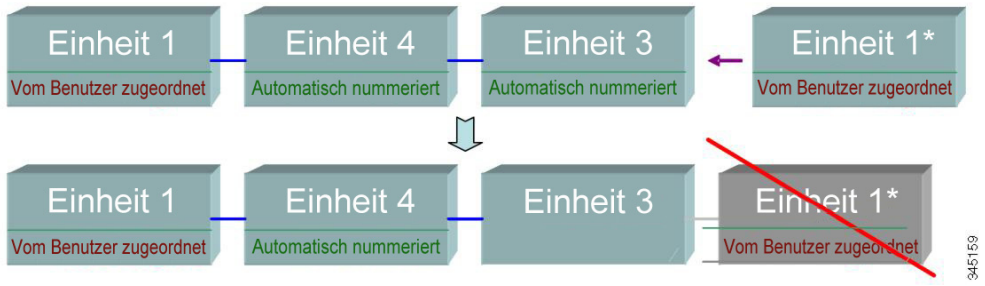
Die folgende Abbildung zeigt ein Beispiel für die automatische Nummerierung beim Hinzufügen einer neuen Einheit zum Stack. Die vorhandene Einheit behält ihre ID. Die neue Einheit erhält die niedrigste verfügbare ID.

Automatisch nummerierte Einheit



Die folgende Abbildung zeigt, was geschieht, wenn eine als Master aktivierte Einheit mit der vom Benutzer zugeordneten Einheiten-ID 1 einem Stack hinzugefügt wird, der bereits eine Mastereinheit mit der vom Benutzer zugeordneten Einheiten-ID 1 hat. Die neuere Einheit 1 wird nicht dem Stack hinzugefügt und wird heruntergefahren.

Als Master aktivierte Einheit mit vom Benutzer zugeordneter ID



Fehler bei einer Einheit im Stack

Fehler bei einer Mastereinheit

Wenn beim Master ein Fehler auftritt, übernimmt die Backup-Einheit die Masterrolle und sorgt dafür, dass der Stack weiterhin normal funktioniert.

Damit die Backup-Einheit an die Stelle des Masters treten kann, bleiben beide Einheiten durchgehend im Modus „Warm Standby“. Im Modus „Warm Standby“ werden der Master und die Backup-Einheiten mit der (in der Startkonfigurationsdatei sowie in der aktuellen Konfigurationsdatei enthaltenen) statischen Konfiguration synchronisiert. Backup-Konfigurationsdateien werden nicht synchronisiert. Die Backup-Konfigurationsdatei bleibt auf dem bisherigen Master.

Dynamische Prozessstatusinformationen, beispielsweise die STP-Statustabelle, dynamisch gelernte MAC-Adressen, dynamisch gelernte Smartport-Typen, MAC-Multicast-Tabellen, LACP und GVRP werden nicht synchronisiert.

Beim Konfigurieren eines Masters wird die Backup-Einheit sofort synchronisiert. Die Synchronisierung erfolgt, sobald der Befehl ausgeführt wird. Dies geschieht transparent.

Wird eine Einheit in einen aktiven Stack eingesetzt und als Backup-Einheit ausgewählt, wird sie vom Master mit der aktuellen Konfiguration synchronisiert. Anschließend wird die SYSLOG-Meldung über den Abschluss der Synchronisierung generiert. Diese SYSLOG-Meldung ist einmalig und wird nur angezeigt, wenn die Backup-Einheit mit der Mastereinheit konvergiert und sieht folgendermaßen aus: %DSYNCH-I-SYNCH_SUCCEEDED: Synchronisierung mit Einheit 2 wurde erfolgreich abgeschlossen.

Switchover zwischen Master und Backup

Wenn bei einem Master ein Fehler auftritt oder Sie die Option „Als Master erzwingen“ für die Backup-Einheit konfigurieren, kommt es zu einem Switchover.

Die Backup-Einheit wird zum Master und alle ihre Prozesse und Protokoll-Stacks werden entsprechend initialisiert, um die Verantwortung für den gesamten Stack zu übernehmen. Daher wird vorübergehend über diese Einheit kein Datenverkehr weitergeleitet. Die Slave-Einheiten bleiben jedoch aktiv.

HINWEIS Wenn STP verwendet wird und die Portverbindungen aktiv sind, wechselt der Status des STP-Ports vorübergehend in Blockieren, sodass er weder Datenverkehr weiterleiten noch MAC-Adressen erkennen kann. Dadurch sollen Spanning Tree-Schleifen zwischen aktiven Einheiten verhindert werden.

Behandlung von Slave-Einheiten

Während die Backup-Einheit zum Master wird, bleiben die aktiven Slave-Einheiten aktiv und leiten weiterhin Pakete basierend auf der Konfiguration des ursprünglichen Masters weiter. Dadurch werden Unterbrechungen des Datenverkehrs in den Einheiten minimiert.

Wenn die Backup-Einheit vollständig in den Masterstatus übergegangen ist, initialisiert sie die Slave-Einheiten einzeln, indem sie folgende Vorgänge ausführt:

- Sie löscht die Konfiguration der Slave-Einheit und setzt sie auf die Standardeinstellungen zurück (um eine falsche Konfiguration über die neue Mastereinheit zu verhindern). Daher wird kein Verkehr an die Slave-Einheit weitergeleitet.
- Sie übernimmt die zugehörigen Benutzerkonfigurationen in die Slave-Einheit.
- Sie tauscht dynamisch Informationen wie beispielsweise den STP-Status von Ports, dynamische MAC-Adressen und den Status (aktiv bzw. nicht aktiv) von Links zwischen dem Master und der Slave-Einheit aus. Die Paketweiterleitung in der Slave-Einheit wird fortgesetzt, wenn der Status ihrer Ports vom Master gemäß STP auf Weiterleiten festgelegt wurde.

  HINWEIS Das Paket-Flooding an unbekannte Unicast-MAC-Adressen findet statt, bis die MAC-Adressen gelernt bzw. erneut gelernt wurden.

Erneutes Verbinden der ursprünglichen Mastereinheit nach einem Failover

Wenn der ursprüngliche Master nach einem Failover wieder verbunden wird, wird der Masterauswahlprozess ausgeführt. Wenn der ursprüngliche Master (Einheit 1) erneut als Master ausgewählt wird, wird der aktuelle Master (Einheit 2, das heißt die ursprüngliche Backup-Einheit) neu gestartet und wird wieder zum Backup.

HINWEIS Beim Failover zwischen Master und Backup wird die Uhrzeit der Backup-Einheit beibehalten.

Automatische Softwaresynchronisierung im Stack

In allen Einheiten im Stack muss die gleiche Softwareversion (Firmware und Bootcode) ausgeführt werden. Die einzelnen Einheiten in einem Stack laden automatisch Firmware und Bootcode von der Mastereinheit herunter, wenn in der Einheit und im Master eine andere Firmware und/oder ein anderer Bootcode ausgeführt wird. Die Einheit wird automatisch mit der neuen Version gestartet.

Stack-Einheitenmodus

Der Stack-Einheitenmodus eines Geräts zeigt an, ob es als Teil eines Stacks konfiguriert ist oder eigenständig betrieben wird.

Die Geräte können in einem der folgenden Stack-Einheitenmodi betrieben werden:

- **Standalone**: Ein Gerät im Stack-Einheitenmodus „Standalone“ ist mit keinem anderen Gerät verbunden und besitzt keinen designierten Stack-Port.
- **Natives Stacking**: Ein Gerät im Modus Natives Stacking kann über seine Stack-Ports mit weiteren Geräten *desselben Typs* zu einem Stack verbunden werden. Alle Einheiten eines nativen Stacks müssen denselben Typ aufweisen (entweder alle Sx500s, alle SG500Xs/ESW2-550Xs oder alle SG500XGs).
- **Basis-Hybrid**: Ein Gerät im Basis-Hybrid-Modus kann zur Bildung eines Stacks mit Sx500- und SG500X-/ESW2-550X-Geräten verbunden werden. Einzige Einschränkung: VRRP oder RIP werden nicht unterstützt. Aus diesem Grund wird der Modus Basis-Hybrid genannt (im Gegensatz zu Erweitertes Hybrid). In diesem Modus zeigt die grafische Oberfläche die Seiten für Sx500 an, auch wenn es sich beim Stack-Master um ein SG500X/ESW2-550X-Gerät handelt, da die Funktionen denen des Sx500 entsprechen.

  In diesem Modus kann jedes Gerät die Master- bzw. Backup-Rolle übernehmen. Nur die 5G-Stacking-Ports können als Stack-Ports verwendet werden.
- **Erweitertes Hybrid**: Ein Gerät im erweiterten Hybrid-Modus kann zur Bildung eines Stacks mit Sx500- und SG500X-/ESW2-550X-Geräten verbunden werden. In diesem Modus werden VRRP und/oder RIP unterstützt, der Modus bietet jedoch keine Unterstützung für die automatische Nummerierung der Einheiten, da nur die Geräte des Typs SG500X oder ESW2-550X als Master oder Backup fungieren können.

  Sx500-Geräte können lediglich als Slaves eingesetzt werden; es sind also bis zu sechs Sx500-Einheiten mit zwei SG500X-/ESW2-550Xs-Geräten zu einem Stack kombinierbar.
- **Erweitertes Hybrid XG**: Ein Gerät im erweiterten Hybrid-XG-Modus kann zur Bildung eines Stacks mit SG500X-/ESW2-550X- und SG500XG-Geräten verbunden werden.

  Alle Einheiten können als Master- oder Slave-Einheiten fungieren.

Optionen für die Stack-Konfiguration

Nachfolgend werden einige typische Stack-Konfigurationen beschrieben:

Mögliche Stack-Konfiguration	Mögliche RIP-/ VRRP-Unterstützung	Geschwindigkeit von Stack-Ports
Der Stack besteht komplett aus SG500Xs-Einheiten im Modus „Natives Stacking“.	Aktiviert/Deaktiviert	1 GBit/10 GBit oder 1 GBit/5 GBit
Der Stack besteht komplett aus ESW2-550Xs-Einheiten im Modus „Natives Stacking“.	Aktiviert/Deaktiviert	1 GBit/10 GBit oder 1 GBit/5 GBit
Der Stack besteht komplett aus SG500s-Einheiten im Modus „Natives Stacking“.	Nicht unterstützt.	1 GBit/5 GBit (Standard) oder 1 GBit Kupfer/SFP (Kombination)
Der Stack besteht aus Geräten verschiedener Typen im Modus „Basis-Hybrid“. ▪ **Master:** Entweder SG500X, ESW2-550X oder Sx500s ▪ **Backup:** Jeder Gerätetyp ▪ **Slaves:** Jeder Gerätetyp	Nicht unterstützt.	1 GBit/5 GBit
Der Stack besteht aus Geräten verschiedener Typen im Modus „Erweitertes Hybrid“. ▪ **Master:** SG500X ▪ **Backup:** SG500X ▪ **Slaves:** Jeder Gerätetyp	Aktiviert/Deaktiviert	1 GBit/5 GBit
Der Stack besteht aus Geräten verschiedener Typen im Modus „Erweitertes Hybrid XG“. ▪ **Master:** SG500X/ESW2-550X oder SG500XG ▪ **Backup:** SG500X/ESW2-550X oder SG500XG ▪ **Slaves:** Jeder Gerätetyp	Aktiviert/Deaktiviert	1G oder 10G

Konsistenz der Stack-Einheitenmodi im Stack

Innerhalb eines Stacks müssen alle Einheiten denselben Stack-Einheitenmodus haben.

Bei der Initialisierung des Stacks wird ein Topologie-Erkennungsalgorithmus ausgeführt, der die Daten der Stack-Einheiten erfasst.

Sobald eine Einheit als Master ausgewählt ist, kann sie die Aufnahmeanfrage ihres Nachbarn zum Stack ablehnen, wenn dieser einen anderen Stack-Einheitenmodus aufweist. Wird eine Einheit aufgrund ihres Stack-Einheitenmodus abgelehnt, wird sie faktisch heruntergefahren (ihre Ports können keinen Datenverkehr empfangen/senden), und alle ihre LEDs (Kontrollleuchten für System, Lüfter, Einheiten-ID, Netzwerkports und Stack-Ports) leuchten auf. Die Informationen zum Stack-Einheitenmodus werden auf der Mastereinheit als SYSLOG-Fehler angezeigt.

Hinweis: Dieser Fehler kann nur behoben werden, indem die Einheit vom Stromnetz genommen und dann erneut angeschlossen wird.

Ändern des Stack-Einheitenmodus

Sie können den Stack-Einheitenmodus eines Geräts ändern, um es aus einem Stack zu entfernen (Stack-Einheitenmodus in Standalone ändern) oder um es als Teil eines Stacks zu konfigurieren (Stack-Einheitenmodus in Natives Stacking, Basis-Hybrid oder Erweitertes Hybrid ändern).

In den folgenden Abschnitten werden der Systemmodus und die Konfiguration der Geräte nach dem Neustart im Anschluss an eine Änderung des Stack-Einheitenmodus behandelt.

Systemmodus nach Neustart (500-Geräte)

Wenn der Stack-Einheitenmodus eines Geräts geändert wird, wird nach dem Neustart möglicherweise der Systemmodus geändert:

- **Sx500-Geräte**: Der Systemmodus (Schicht-2- oder Schicht-3-Systemmodus) der Sx500-Backup- und -Slave-Einheiten wird von der als Master aktivierten Einheit übernommen. Wenn der Systemmodus vor dem Neustart nicht explizit eingestellt wurde, wird nach dem Neustart der Schicht-2-Systemmodus verwendet (Standardwert). Wenn Sie möchten, dass das Gerät nach dem Neustart Schicht 3 hat, muss dies vor dem Neustart explizit eingestellt werden.
- **SG500X/ESW2-550X-Geräte**: Wenn sich das Gerät im Modus „Standalone“ oder „Natives Stacking“ befindet, ist der Systemmodus immer Schicht 2 oder Schicht 3. Befindet es sich im Modus „Basis-Hybrid“ oder „Erweitertes Hybrid“, verhält es sich wie oben für Sx500-Geräte beschrieben. Befindet sich das Gerät im Modus Basis-Hybrid oder Erweitertes Hybrid, verhält es sich wie oben für Sx500-Geräte beschrieben.
- **SG500XG-Geräte**: Immer Schicht 2 und Schicht 3.

Konfiguration nach Neustart

Wenn Sie den Stack-Modus eines Geräts ändern und das Gerät neu starten, wird die Startkonfigurationsdatei in der Regel **entfernt**, da sie möglicherweise Konfigurationsinformationen enthält, die sich für den neuen Modus nicht eignen.

Sie wird in den folgenden Fällen nach dem Start beibehalten:

- **SG500X/ESW2-550X-Geräte:**
  - **Standalone in Natives Stacking:** Wird nur beibehalten, wenn die Einheit zwangsweise zum Master mit der Einheiten-ID = 1 wird.
  - **Basis-Hybrid in erweitertes Hybrid:** Wird nur beibehalten, wenn die Einheit zwangsweise zum Master mit der Einheiten-ID = 1 wird.
  - **Basis-Hybrid in erweitertes Hybrid XG:** Wird nur beibehalten, wenn die Einheit zwangsweise zum Master mit der Einheiten-ID = 1 wird.
- **SG500XG:**
  - **Standalone in Natives Stacking:** Wird nur beibehalten, wenn die Einheit zwangsweise zum Master mit der Einheiten-ID = 1 wird.
  - **Natives Stacking in erweitertes Hybrid XG:** Wird nur beibehalten, wenn die Einheit zwangsweise zum Master mit der Einheiten-ID = 1 wird.
- **Sx500-Geräte:**
  - **Standalone in Natives Stacking:** Wird nur beibehalten, wenn die Einheit zwangsweise zum Master mit der Einheiten-ID = 1 wird.
  - **Standalone in Basis-Hybrid:** Wird nur beibehalten, wenn die Einheit zwangsweise zum Master mit der Einheiten-ID = 1 wird.
  - **Natives Stacking in Basis-Hybrid:** Wird nur beibehalten, wenn die Einheit zwangsweise zum Master mit der Einheiten-ID = 1 wird.

Stack-Ports

Die Ports in einem Stack müssen einen der folgenden Porttypen aufweisen:

- **Netzwerkport**: Auch als Uplink-Ports bekannt. Diese Ports sind mit dem Netzwerk verbunden.
- **Stack-Ports**: Ports, die zwei Einheiten eines Stack miteinander verbinden. Über Stack-Ports werden Daten und Protokollpakete zwischen den Einheiten übertragen.

Sie müssen dem System (auf der Seite Systemmodus und Stack-Verwaltung) signalisieren, welche Ports Sie als Stack-Ports verwenden möchten. Alle nicht als Stack-Ports angegebenen (reservierten) Stack-Ports werden als Netzwerkports betrachtet.

Stack-Port-Link-Aggregation

Beim Herstellen einer Verbindung zwischen zwei benachbarten Einheiten, werden die Ports, über die sie verbunden werden, automatisch einer Stack-LAG zugewiesen. Mit dieser Funktion kann die Stack-Bandbreite des Stack-Ports über die eines einzelnen Ports hinaus erweitert werden.

Bis zu zwei Stack-LAGs pro Einheit sind möglich.

Der Stack-LAG kann je nach Einheitentyp zwischen zwei und acht Stack-Ports aufweisen.

Stack-Portstatus

Stack-Ports können einen der folgenden Status aufweisen:

- **Inaktiv**: Der Betriebsstatus des Ports ist „Inaktiv“ oder der Betriebsstatus des Stack-Ports ist zwar „Aktiv“, aber es kann kein Datenverkehr über den Port fließen.
- **Aktiv**: Der Stack-Port wurde zu einer Stack-LAG mit dem Betriebsstatus „Aktiv“ hinzugefügt. Datenverkehr *kann* durch den Port fließen und er ist ein Mitglied einer Stack-LAG.
- **Standby**: Der Betriebsstatus des Ports ist „Aktiv“ und bidirektionaler Verkehr kann durch den Port fließen. Der Port kann aber nicht zu einer Stack-LAG hinzugefügt werden und er leitet auch keinen Verkehr weiter. Mögliche Ursachen für den „Standby“-Status eines Ports:
  - Für die Verbindung eines einzelnen Nachbars werden Stack-Ports mit unterschiedlichen Geschwindigkeiten verwendet.
  - Eine Einheit ist mit mehr als zwei Nachbareinheiten verbunden.

Abwärtskompatibilität

Die Betriebseigenschaften eines Stacks mit Geräten, die Unterstützung für Stack-Port-LAGs bieten und Geräten, die diese Funktion nicht unterstützen, werden unter **Abwärtskompatibilität** erläutert.

Physische Einschränkungen für Stack-LAGs

Folgende Faktoren schränken den Einsatz von Stack-LAGs ein:

- Die Stack-Ports einer Stack-LAG müssen der Beschreibung in **Tabelle 1** bis **Tabelle 4** entsprechen.
- Die Ports einer Stack-LAG müssen dieselbe Geschwindigkeit aufweisen.

- Wenn Sie versuchen, eine Einheit mit einem Stack zu verbinden, der keine Ring- oder Kettentopologie aufweist (z. B. wenn Sie versuchen, eine Einheit mit mehr als zwei Nachbarn in einer Sterntopologie zu verbinden), können nur zwei Stack-LAGs aktiv sein, die übrigen Stack-Ports werden in den Standby-Modus versetzt (inaktiv).

Empfohlene Stack-Verbindungen

In den folgenden Tabellen wird beschrieben, wie Sie Einheiten je nach Typ der im Stack verwendeten Einheiten auf optimale Weise zu einem Stack verbinden.

Sollte bei einem Port in einer Stack-LAG ein Fehler auftreten, wird der Datenverkehr auf dem Stack unter den verbleibenden Stack-Ports in der Stack-LAG neu verteilt. Dies kann dazu führen, dass sich die Stack-Verbindungen von einer empfohlenen Konfiguration in eine nicht empfohlene Konfiguration ändern.

Tabelle 1 Sx500-Stack mit Sx500 oder SG500X/ESW2-550X

Anzahl der aktiven Stack-Ports	Empfohlene Verbindungen für Stack-Ports beim Sx500
1	S1 oder S2 oder S3 oder S4
2	Folgende Fälle sind möglich: Fall 1: S1 mit einem Nachbarn und S2 mit einem anderen Nachbarn Fall 2: S3 mit einem Nachbarn und S4 mit einem anderen Nachbarn Fall 3: S1 und S2 mit demselben Nachbarn Fall 4: S3 und S4 mit demselben Nachbarn

Tabelle 2 SG500X- und ESW2550X-Stacks mit Sx500, SG500X/ESW2-550X oder SG500XG

Anzahl der aktiven Stack-Ports	Empfohlene Verbindungen für Stack-Ports beim SG500X
1	S1 oder S2 oder XG1 oder XG2
2	Fall 1: S1 mit einem Nachbarn und S2 mit einem anderen Nachbarn Fall 2: XG1 mit einem Nachbarn und XG2 mit einem anderen Nachbarn Fall 3: S1 und S2 mit demselben Nachbarn Fall 4: XG1 und XG2 mit demselben Nachbarn
4	S1 und S2 mit demselben Nachbarn und XG1 und XG2 mit einem anderen Nachbarn

Tabelle 3 SG500XG-Stack mit SG500X/ESW2-550X

Anzahl der aktiven Stack-Ports	Empfohlene Verbindungen für Stack-Ports beim SG500XG
1	Beliebiger Port
2	Ein Port mit einem Nachbarn und ein anderer mit einem anderen Nachbarn 2 Ports mit demselben Nachbarn
4	2 Ports mit einem Nachbarn und 2 andere Ports mit einem anderen Nachbarn

Tabelle 4 Sx500XG-Stack mit Sx500XG

Anzahl der aktiven Stack-Ports	Empfohlene Verbindungen für Stack-Ports beim Sx500XG
1	Beliebiger Port
2	1 Port mit einem Nachbarn und der andere Port mit einem anderen Nachbarn 2 Ports mit demselben Nachbarn
4	2 Ports mit einem Nachbarn und die anderen beiden Ports mit einem anderen Nachbarn 4 Ports mit demselben Nachbarn
8	4 Ports mit einem Nachbarn und die anderen 4 Ports mit einem anderen Nachbarn.

Standardports für Stacks und Netzwerk

Nachfolgend finden Sie die Standardports für Stacks und Netzwerk:

- **Sx500-Geräte**: Wenn ein Sx500-Gerät im Modus „Natives Stacking“ betrieben wird, fungieren S1, S2 und 1G als normale Netzwerkports und S3, S4 und 5G standardmäßig als Stack-Ports.
- **SG500X/ESW2-550X-Geräte**: S1, S2 und 10G sind standardmäßig Stack-Ports. Sie können S1/S2/10G manuell und S1/S2/5G als Netzwerkports oder Stack-Ports umkonfigurieren.
- **SG500XG-Geräte**: Alle Ports können als Stack oder Netzwerk fungieren. Standardmäßig wird das Gerät im Modus „Standalone“ betrieben.

Wenn Sie ein Gerät von einem Stacking-Modus in den Standalone-Modus umstellen, werden die Stack-Ports automatisch zu normalen Netzwerkports.

Port-Geschwindigkeiten

Die Geschwindigkeit der Stack-Ports kann manuell festgelegt oder auf automatische Auswahl eingestellt werden. Nachfolgend werden die verfügbaren Typen von Stack-Ports und deren Geschwindigkeiten in den verschiedenen Gerätetypen beschrieben:

Gerätetyp	Portpaar	Im Stack mögliche Geschwindigkeiten	Automatische Auswahl der Geschwindigkeit verfügbar
Sx500	S1, S2	1G	Nein
Sx500	S3, S4	5G/1G	Ja
SG500X/ **ESW2-550X**	S1, S2 - XG	10G/1G	Ja
SG500X/ **ESW2-550X**	S1, S2 - 5G	5G/1G	Ja
SG500XG	**Ein beliebiges Portpaar von XG1 - XG16**	1 Gbit/s oder 10 Gbit/s	Ja

Automatische Auswahl der Port-Geschwindigkeit

Wenn das Kabel an den Port angeschlossen ist, können Sie festlegen, dass der Stacking-Kabeltyp automatisch erkannt wird (die autom. Erkennung ist die Standardeinstellung). Das System ermittelt den Stack-Kabeltyp automatisch und wählt die höchste von Kabel und Port unterstützte Geschwindigkeit.

Wird der Kabeltyp nicht erkannt, wird der Benutzer über eine eingeblendete SYSLOG-Meldung (Information) dazu aufgefordert, die Port-Geschwindigkeit manuell zu konfigurieren.

Verbinden von Einheiten

Zwei Einheiten können nur zu einem Stack zusammengeschlossen werden, wenn die Ports auf beiden Seiten der Verbindung dieselbe Geschwindigkeit haben. Sie haben zwei Möglichkeiten, die Geschwindigkeit der Stack-Ports zu konfigurieren:

- automatisch
- durch Einstellung der gleichen Geschwindigkeit auf beiden Seiten der Verbindung

Kabeltypen

Jeder Typ von Stack-Port kann mit bestimmten Kabeltypen verwendet werden.

Wenn als Stack-Modus „Natives Stacking“ eingestellt ist, können Sie als Stacking-Kabel entweder Glasfaser- oder Kupferkabel verwenden. Wenn beide Kabel (Glasfaser und Kupfer) angeschlossen sind, wird Glasfaser bevorzugt. Duale Verbindungen können für die Redundanz verwendet werden. Wenn sich das Übertragungsmedium ändert, beispielsweise wenn das Glasfaserkabel entfernt und das Kupferkabel aktiv wird, initiiert das System ein Topologieänderungsereignis.

Nachfolgend werden die möglichen Kombinationen von Kabeltypen und Ports beschrieben.

	Stack-Ports			Netzwerkports		
Anschlusstyp	**S1, S2 oder 5G für SG500X/ ESW2-550X und S3, S4 für Sx500**	**S1, S2 beim Sx500**	**S1, S2 - XG beim SG500X/ ESW2-550X**	**S1, S2 - 5G für SG500X und S3, S4 für Sx500**	**S1, S2 beim Sx500**	**S1, S2 - XG beim SG500X**
Cisco SFP-H10GB-CU1M – Passives Kupferkabel	5G	1G	10G	1G	1G	10G
Cisco SFP-H10GB-CU3M – Passives Kupferkabel	5G	1G	10G	1G	1G	10G
Cisco SFP-H10GB-CU5M – Passives Kupferkabel	5G	1G	10G	1G	1G	10G
Cisco SFP-10G-SR	Nicht unterstützt	Nicht unterstützt	10G	Nicht unterstützt	Nicht unterstützt	10G
Cisco SFP-10G-LRM	Nicht unterstützt	Nicht unterstützt	10G	Nicht unterstützt	Nicht unterstützt	10G
Cisco SFP-10G-LR	Nicht unterstützt	Nicht unterstützt	10G	Nicht unterstützt	Nicht unterstützt	10G
1G-SFP-Modul MGBSX1	1G	1G	1G	1G	1G	1G
1G-SFP-Modul MGBT1	1G	1G	1G	1G	1G	1G

Stack-Ports				Netzwerkports		
Anschlusstyp	**S1, S2 oder 5G für SG500X/ ESW2-550X und S3, S4 für Sx500**	**S1, S2 beim Sx500**	**S1, S2 - XG beim SG500X/ ESW2-550X**	**S1, S2 - 5G für SG500X und S3, S4 für Sx500**	**S1, S2 beim Sx500**	**S1, S2 - XG beim SG500X**
1G-SFP-Modul MGBLX1	1G	1G	1G	1G	1G	1G
1G-SFP-Modul MGBBX1	1G	1G	1G	1G	1G	1G
100-MBit/s-SFP-Modul MFELX1	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	100 MBit/s	Nicht unterstützt
100-MBit/s-SFP-Modul MFEFX1	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	100 MBit/s	Nicht unterstützt
100-MBit/s-SFP-Modul MFEBX1	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	100 MBit/s	Nicht unterstützt
Sonstige SFPs	1G	Gemäß: Vom Benutzer erzwungene Geschwindigkeit EEPROM-Geschwindigkeit Geschwindigkeit 1G	Gemäß: Vom Benutzer erzwungene Geschwindigkeit EEPROM-Geschwindigkeit Geschwindigkeit 1G	1G	Gemäß: Vom Benutzer erzwungene Geschwindigkeit EEPROM-Geschwindigkeit Geschwindigkeit 1G	Gemäß: Vom Benutzer erzwungene Geschwindigkeit EEPROM-Geschwindigkeit Geschwindigkeit 10G

Stack-Ports oder Netzwerk-Ports	
Anschlusstyp	**Alle Ports**
Cisco SFP-H10GB-CU1M – Passives Kupferkabel	1 Gbit/s - 10 Gbit/s
Cisco SFP-H10GB-CU3M – Passives Kupferkabel	1 Gbit/s - 10 Gbit/s
Cisco SFP-H10GB-CU5M – Passives Kupferkabel	1 Gbit/s - 10 Gbit/s
Cisco SFP-10G-SR	Nicht unterstützt

Stack-Ports oder Netzwerk-Ports	
Anschlusstyp	**Alle Ports**
Cisco SFP-10G-LRM	Nicht unterstützt
Cisco SFP-10G-LR	Nicht unterstützt
1G-SFP-Modul MGBSX1	1G
1G-SFP-Modul MGBT1	1G
1G-SFP-Modul MGBLX1	1G
1G-SFP-Modul MGBBX1	1G
100-MBit/s-SFP-Modul MFELX1	Nicht unterstützt
100-MBit/s-SFP-Modul MFEFX1	Nicht unterstützt
100-MBit/s-SFP-Modul MFEBX1	Nicht unterstützt
Sonstige SFPs	1G

Standardkonfiguration

Im Folgenden werden die Gerätestandardeinstellungen in den diversen Stacking-Modi dargestellt:

Gerätetyp	Stack-Modus	Standard-Stack-Ports	Standard-Systemmodus
Sx500	Nativer Stack	S3-S4 5Gbit/s-Stack	Schicht 2
	Basis-Hybrid	S3-S4 5Gbit/s-Stack	Schicht 2
	Erweitertes Hybrid	S3-S4 5Gbit/s-Stack	Schicht 2
SG500X/ ESW2-550X	Nativer Stack	S1-S2 10Gbit/s-Stack	Schicht 2 + Schicht 3
	Basis-Hybrid	S1-S2 5Gbit/s-Stack	Schicht 2
	Erweitertes Hybrid	S1-S2 5Gbit/s-Stack	Schicht 2
	Erweitertes Hybrid XG	S1-S2 5Gbit/s-Stack	Schicht 2
SG500XG	Nativer Stack	Der Benutzer kann ein beliebiges Paar auswählen.	Schicht 2 + Schicht 3
	Erweitertes Hybrid XG	Der Benutzer kann ein beliebiges Paar auswählen.	Schicht 2 + Schicht 3

Interaktionen mit anderen Funktionen

RIP und VRRP werden im Stack-Modus „Basis-Hybrid“ nicht unterstützt.

Systemmodi

Auf der Seite Systemmodus und Stack-Verwaltung können Sie Folgendes tun:

- den Stack-Modus eines Geräts in „Standalone“ ändern
- den Stack-Modus eines Geräts in einen der Stacking-Modi ändern sowie die Einheiten-ID, die Stack-Ports und die Geschwindigkeit des Stack-Ports für alle Geräte eines Stacks ändern
- Ändern des Systemmodus (Schicht 2/3) eines eigenständigen Geräts oder des Stacks.
- den Warteschlangenmodus von vier in acht unterstützte Warteschlangen und umgekehrt ändern

Informationen zu diesen Modi sind in der Konfigurationsdatei wie folgt gespeichert:

- **Header der Konfigurationsdatei**: enthält den Systemmodus und den Warteschlangenmodus (auch wenn die Standardwerte verwendet werden).
- **Text der Konfigurationsdatei**: enthält die Konfigurationsbefehle.

Abwärtskompatibilität

Folgende Modi wurden in der aktuellen Softwareversion des Geräts erweitert. Gehen Sie vorsichtig vor, wenn Sie diese Funktionen in älteren Softwareversionen verwenden:

- **Stack-Port-LAG**: Wenn eine Einheit, deren Software Stack-Ports in LAGs unterstützt, mit einer Einheit verbunden wird, deren Software keine Stack-Ports in LAGs unterstützt, dann wird der Stack-Port, der die Einheiten verbindet, nicht zum Mitglied der Stack-LAG gemacht. Die Einheiten werden über die Stack-Ports verbunden und der Stack-Master kopiert die Software auf die andere Einheit. Welche Software kopiert wird, hängt davon ab, welche Einheit zum Master wird.
- **Warteschlangenmodus**: Kann zwischen vier QoS-Warteschlangen und acht QoS-Warteschlangen umgeschaltet werden. Das Aktualisieren von älteren Softwareversionen, die acht Warteschlangen nicht unterstützten, funktioniert problemlos, da auch in der aktuellen Software vier Warteschlangen als Standardwarteschlangenmodus eingestellt sind. Wenn Sie den Warteschlangenmodus jedoch in acht Warteschlangen ändern, müssen Sie die Konfiguration überprüfen und dahingehend anpassen, damit die gewünschten QoS-Ziele mit dem neuen Warteschlangenmodus übereinstimmen. Änderungen am Warteschlangemodus werden nach dem Neustart des Systems wirksam. Warteschlangenkonfigurationen, die zu Konflikten mit dem neuen Warteschlangenmodus führen, werden abgelehnt.

- **Stacking-Modus**: Der Stacking-Modus wurde um Hybrid-Stacking-Modi erweitert. Upgrades von älteren Softwareversionen stellen kein Problem dar, da das Gerät mit einem vorhandenen Stacking-Modus (Natives Stacking) gestartet wird. Wenn die Software eines Geräts, das im Hybrid-Stacking-Modus konfiguriert wurde, auf einem Gerät verwendet werden soll, das Hybrid-Stacking nicht unterstützt, müssen Sie die Gerätekonfiguration zunächst in den Modus Natives Stacking ändern.

Systemmodus und Stack-Verwaltung

So konfigurieren Sie den Stack:

SCHRITT 1 Klicken Sie auf **Administration** > **Systemmodus und Stack-Verwaltung**.

Der Betriebsstatus eines eigenständigen Geräts oder eines Stacks wird im Block **Betriebsstatus** angezeigt:

- **Stack-Modus**: Zeigt für das Gerät einen der folgenden Werte an:
  - *Standalone*: Das Gerät ist nicht Teil eines Stacks.
  - *Natives Stacking*: Das Gerät ist Teil eines Stacks, in dem alle Einheiten dem gleichen Typ angehören.
  - *Basis-Hybrid-Stacking*: Das Gerät ist Teil eines Stacks, das aus Geräten der Typen SG500X und Sx500 bestehen kann, wobei die Funktion Sx500 eingestellt ist.
  - *Erweitertes Hybrid-Stacking*: Das Gerät ist Teil eines Stacks, das aus Geräten der Typen SG500X und Sx500 bestehen kann, wobei die Funktion SG500X eingestellt ist.
  - *Erweitertes Hybrid-Stacking XG*: Das Gerät ist Teil eines Stacks, das aus Geräten der Typen SG500X/ESW2-550X und SG500XG bestehen kann, wobei die Funktion SG500X eingestellt ist.
- **Stack-Topologie**: Zeigt an, ob es sich bei der Topologie des Stacks um eine Kette oder einen Ring handelt.
- **Systemmodus**: Zeigt an, ob der Stack bzw. die eigenständigen Geräte im Schicht-2, Schicht-3- oder im Schicht-2- und Schicht-3-Systemmodus betrieben werden.
- **Stack-Master**: Zeigt die Einheiten-ID der Mastereinheit des Stacks an.
- **Masterwahlstatus**: Zeigt an, wie die Stack-Mastereinheit ausgewählt wurde. Weitere Informationen hierzu finden Sie unter **Masterauswahlprozess**.

SCHRITT 2 Nehmen Sie Eingaben für die folgenden Felder unter **Administrativer Status** vor.

- **Stack-Master**: Wählen Sie die Mastereinheit des Stacks aus. Folgende Optionen stehen zur Verfügung:
  - *Autom. auswählen*: Das System wählt den Master aus. Weitere Informationen hierzu finden Sie unter **Masterauswahlprozess**.

- *Einheit 1*: Einheit 1 als Mastereinheit nach dem Neustart auswählen.
- *Einheit 2*: Einheit 2 als Mastereinheit nach dem Neustart auswählen.

- **Systemmodus**: Wählen Sie den Schicht 2- oder den Schicht 3-Modus aus.

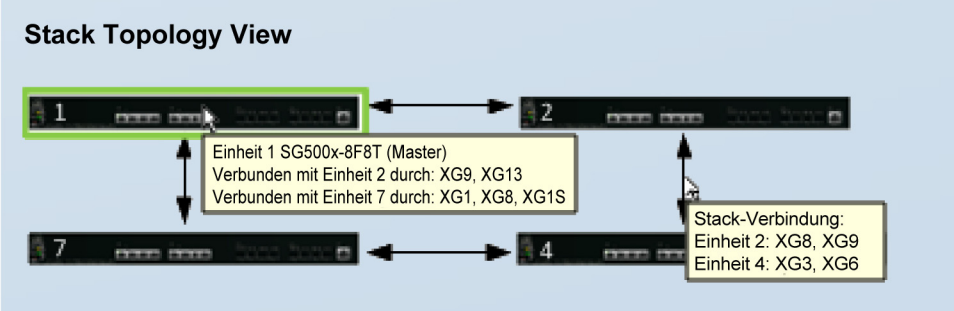
  HINWEIS Nur auf Geräten verfügbar, auf denen die Option „Systemmodus“ vorhanden ist.

- **Warteschlangenmodus**: Wählen Sie aus, ob auf dem Gerät vier oder acht QoS-Warteschlangen konfiguriert werden sollen. Weitere Informationen hierzu finden Sie unter **Konfigurieren von QoS-Warteschlangen**.

  HINWEIS Wenn es sich um ein Sx500-Gerät handelt und der Stack-Einheitenmodus von „Natives Stacking“ in „Standalone“ geändert wird, befindet sich das Gerät nach dem Neustart im Schicht-2-Systemmodus, es sei denn, Sie ändern das Feld **Systemmodus** jetzt in „Schicht 3“.

Stack-Topologie-Ansicht

Diese Ansicht zeigt, wie die Geräte im Stack miteinander verbunden sind. Wenn Sie auf die Verbindungspfeile zwischen den Geräten klicken, wird eine QuickInfo mit der Einheitennummer, den Typen von Stack-Ports, die mit den Einheiten verbunden sind, und die Anzahl der verbundenen Einheiten angezeigt. Nachstehend ist ein entsprechendes Beispiel abgebildet:

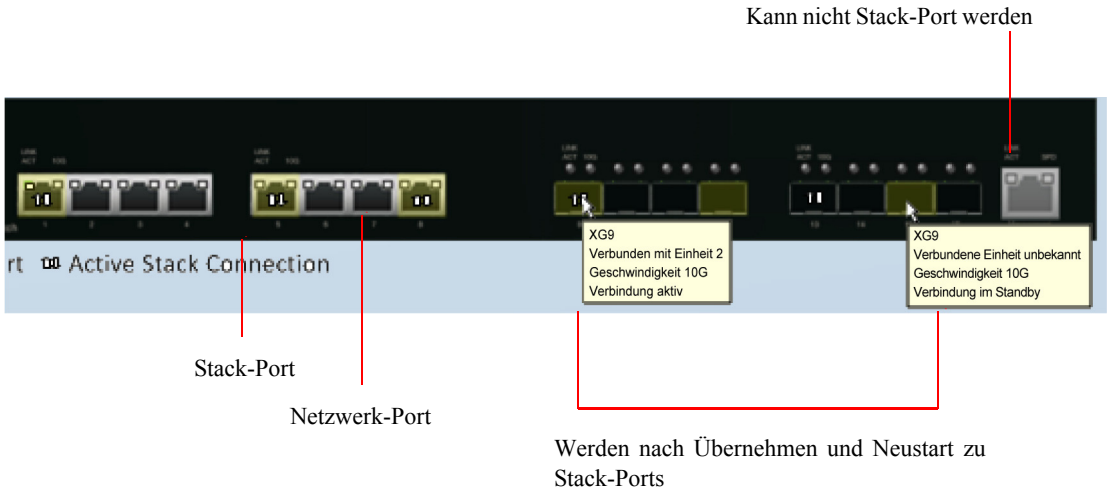


Einheitenansicht und Stack-Port-Konfiguration

So wählen Sie Stack-Ports für ein Gerät aus:

a. Klicken Sie in der Stack-Topologie-Ansicht auf ein Gerät. Die Ports auf diesem Gerät werden in dieser Ansicht angezeigt.

b. Wenn Sie auf einen Port klicken, wird eine QuickInfo angezeigt, die Aufschluss über die Port-Nummer, die mit ihm verbundene Einheit, die Port-Geschwindigkeit und den Verbindungsstatus gibt. Nachstehend ist ein entsprechendes Beispiel gezeigt.:



c. Klicken Sie auf die (schwarzen) Netzwerkports, die Sie als Stacking-Ports (graue Ports) auswählen möchten. Diese Ports sind derzeit Netzwerkports. Wenn Sie auf **Übernehmen und Neustart** klicken, werden sie nach dem Neustart zu Stack-Ports.

d. Um Stack-Parameter für Geräte im Stack zu konfigurieren, klicken Sie in der Stack-Topologie auf das Gerät und geben Sie Werte für die folgenden Felder für das Gerät und die Stacking-Ports ein.

- **Einheiten-ID nach dem Zurücksetzen**: Wählen Sie eine Einheiten-ID aus oder wählen Sie „Autom.“ aus, um die Zuweisung der Einheiten-ID dem System zu überlassen.
- **Einheit 1 – Stack-Modus**: Wählen Sie einen Stack-Modus aus.
- **Einheit 1 – Stack-Verbindungsgeschwindigkeit**: Wählen Sie die Geschwindigkeit für die Stack-Ports aus. Wählen Sie „Autom.“, um dem System die Auswahl der Geschwindigkeit zu überlassen.

SCHRITT 3 Klicken Sie auf **Übernehmen und Neustart**. Die Parameter werden in die ausgeführte Konfigurationsdatei kopiert und der Stack wird neu gestartet.

7

Administration

In diesem Abschnitt wird beschrieben, wie Sie Systeminformationen anzeigen und die verschiedenen Optionen für das Gerät konfigurieren.

Die folgenden Themen werden behandelt:

- **Gerätemodelle**
- **Systemeinstellungen**
- **Konsoleneinstellungen (Unterstützung für automatische Baudrate)**
- **Management-Schnittstelle**
- **Systemmodus und Stack-Verwaltung**
- **Benutzerkonten**
- **Definieren des Timeouts für Sitzungsleerlauf**
- **Zeiteinstellungen**
- **Systemprotokoll**
- **Dateiverwaltung**
- **Neustarten des Geräts**
- **Routing-Ressourcen**
- **Integrität**
- **Diagnose**
- **Erkennung – Bonjour**
- **Erkennung – LLDP**
- **Erkennung – CDP**
- **Ping**
- **Traceroute**

Gerätemodelle

Sie können mit dem webbasierten Switch-Konfigurationsdienstprogramm alle Modelle verwalten.

Wenn das Gerät im Schicht-3-Systemmodus betrieben wird, sind die VLAN-Ratenbegrenzung und die QoS-Überwachungsvorrichtungen deaktiviert. Die anderen Funktionen des erweiterten QoS-Modus werden weiterhin verwendet.

Nur die SG500X-/SG500XG-/ESW2-550X-Modelle unterstützen VRRP (Virtual Router Redundancy Protocol) und RIP (Routing Information Protocol).

HINWEIS Informationen zu Benennungskonventionen für Ports finden Sie unter **Benennungskonventionen für Schnittstellen**.

In der folgenden Tabelle werden die verschiedenen Modelle, die Anzahl und Art ihrer Ports sowie deren Informationen zu Power over Ethernet (PoE) beschrieben.

Modellname	Produkt-ID (PID)	Beschreibung der Ports am Gerät	Leistung für PoE	Zahl der Ports mit PoE-Unterstützung
SF500-24	SF500-24-K9	10/100 Stackable Managed Switch mit 24 Ports	n/v	n/v
SF500-24MP	SF500-24MP-K9	10/100 Max PoE Stackable Managed Switch mit 24 Ports	375 W	24
SF500-24P	SF500-24P-K9	10/100 PoE Stackable Managed Switch mit 24 Ports	180 W	24
SF500-48	SF500-48-K9	10/100 Stackable Managed Switch mit 48 Ports	n/v	n/v
SF500-48MP	SF500-48MP-K9	10/100 Max PoE Stackable Managed Switch mit 48 Ports	740 W	48
SF500-48P	SF500-48P-K9	10/100 PoE Stackable Managed Switch mit 48 Ports	375 W	48
SG500-28	SG5000-28-K9	Stackable Managed Switch mit 28 Gigabit-Ports	n/v	n/v
SG500-28MPP	SG500-28MPP-K9	Gigabit-PoE-Managed Switch mit 28 Ports	740 W	24
SG500-28P	SG500-28P-K9	PoE Stackable Managed Switch mit 28 Gigabit-Ports	180 W	24

Modellname	Produkt-ID (PID)	Beschreibung der Ports am Gerät	Leistung für PoE	Zahl der Ports mit PoE-Unterstützung
SG500-52	SG500-52-K9	Stackable Managed Switch mit 52 Gigabit-Ports	n/v	n/v
SG500-52MP	SG500-52MP-K9	Gigabit-Max-PoE-Managed Switch mit 52 Ports	740 W	48
SG500-52P	SG500-52P-K9	PoE Stackable Managed Switch mit 52 Gigabit-Ports	375 W	48
SG500X-24	SG500X-24-K9	Stackable Managed Switch mit 24 Gigabit-Ports und 4 10-Gigabit-Ports	n/v	n/v
SG500X-24P	SG500X-24P-K9	PoE Stackable Managed Switch mit 24 Gigabit-Ports und 4 10-Gigabit-Ports	375 W	24
SG500X-24MPP	SG500X-24MPP-K9	Gigabit-PoE-Managed Switch mit 24 Ports	740 W	24
SG500X-48	SG500X-48-K9	Stackable Managed Switch mit 48 Gigabit-Ports und 4 10-Gigabit-Ports	n/v	n/v
SG500X-48MP	SG500X-48MP-K9	Gigabit-Max-PoE-Managed Switch mit 48 Ports	740 W	48
SG500X-48P	SG500X-48P-K9	PoE Stackable Managed Switch mit 48 Gigabit-Ports und 4 10-Gigabit-Ports	375 W	48
ESW2-550X-48	ESW2-550X-48-K9	Stackable Managed Switch mit 48 Gigabit-Ports und 4 10-Gigabit-Ports	n/v	n/v
ESW2-550X-48DC	ESW2-550X-48DC-K9	Stackable Managed Switch mit 48 Gigabit-Ports und 4 10-Gigabit-Ports	n/v	n/v
SG500XG-8F8T	SG500XG-8F8T-K9	Stackable Managed Switch mit 10 Gigabit und 16 Ports	n/v	n/v

Systemeinstellungen

Die Seite Systemübersicht bietet eine grafische Übersicht über das Gerät und zeigt den Gerätestatus, Hardwareinformationen, Informationen zur Firmwareversion, den allgemeinen PoE-Status und weitere Informationen an.

Anzeigen der Systemübersicht

So zeigen Sie die Systembeschreibung an:

SCHRITT 1 Klicken Sie auf **Status und Statistik** > **Systemübersicht**.

Systembeschreibung:

- **System-Stack-Mode**: Zeigt an, ob das Gerät Teil eines Stacks ist. Weitere Informationen zu Stack-Modi finden Sie im Abschnitt **Stack-Einheitenmodus**.

  HINWEIS Wenn sich das System im Modus „Natives Stacking“ befindet, basiert die angezeigte Firmware-Versionsnummer auf der Version des Masters.

- **Systembetriebsmodus**: Gibt an, ob das System im Schicht-2- oder Schicht-3-Systemmodus für 500-Geräte betrieben wird.
- **Systembeschreibung**: Eine Beschreibung des Systems.
- **Systemstandort**: Physischer Standort des Geräts. Klicken Sie auf **Bearbeiten**, um die Seite Systemeinstellungen aufzurufen und diesen Wert einzugeben.
- **Systemkontakt**: Name einer Kontaktperson. Klicken Sie auf **Bearbeiten**, um die Seite Systemeinstellungen aufzurufen und diesen Wert einzugeben.
- **Hostname**: Name des Geräts. Klicken Sie auf **Bearbeiten**, um die Seite Systemeinstellungen aufzurufen und diesen Wert einzugeben. Standardmäßig setzt sich der Hostname des Geräts aus dem Wort *switch* und den drei am wenigsten signifikanten Bytes der MAC-Adresse des Geräts (die sechs Hexadezimalstellen ganz rechts) zusammen.
- **Systemobjekt-ID**: Eindeutige Anbieter-ID des Netzwerk-Management-Untersystems der Entität (wird bei SNMP verwendet).
- **Systembetriebszeit**: Die seit dem letzten Neustart verstrichene Zeit.
- **Aktuelle Zeit**: Die aktuelle Systemzeit.
- **MAC-Basisadresse**: MAC-Adresse des Geräts. Wenn sich das System im Stack-Modus befindet, wird die MAC-Basisadresse der Mastereinheit angezeigt.

- **Jumbo Frames**: Status der Jumbo Frame-Unterstützung. Die Unterstützung können Sie auf der Seite Porteinstellungen im Menü Portverwaltung aktivieren oder deaktivieren.

  HINWEIS Die Unterstützung für Jumbo-Frames wird erst wirksam, wenn sie aktiviert wurde und das Gerät neu gestartet wurde.

Softwareinformationen:

- **Firmware-Version (aktives Image)**: Firmware-Versionsnummer des aktiven Image.

  HINWEIS Wenn sich das System im Stack-Modus befindet, basiert die angezeigte Firmware-Versionsnummer auf der Version des Masters. Weitere Informationen zu Stack-Modi finden Sie im Abschnitt **Stack-Einheitenmodus**.

- **Firmware-MD5-Prüfsumme (aktives Image)**: MD5-Prüfsumme des aktiven Image.
- **Firmware-Version (inaktives Image)**: Firmware-Versionsnummer des aktiven Image. Wenn sich das System im Stack-Modus befindet, wird die Version der Mastereinheit angezeigt.
- **Firmware-MD5 Prüfsumme (inaktives Image)**: MD5-Prüfsumme des inaktiven Images.
- **Boot-Version**: Nummer der Boot-Version.
- **Boot-MD5-Prüfsumme**: MD5-Prüfsumme der Boot-Version.
- **Gebietsschema**: Gebietsschema der ersten Sprache. (Immer Englisch.)
- **Sprachversion**: Sprachpaketversion der ersten Sprache (Englisch).
- **Sprach-MD5-Prüfsumme**: MD5-Prüfsumme der Sprachdatei.

Status der TCP/UDP-Services:

- **HTTP-Service**: Ob HTTP aktiviert oder deaktiviert ist.
- **HTTPS-Service**: Ob HTTPS aktiviert oder deaktiviert ist.
- **SNMP-Service**: Ob SNMP aktiviert oder deaktiviert ist.
- **Telnet-Service**: Ob Telnet aktiviert oder deaktiviert ist.
- **SSH-Service**: Ob SSH aktiviert oder deaktiviert ist.

PoE-Leistungsinformationen zur Mastereinheit: (bei Geräten, die PoE unterstützen)

- **Maximal verfügbare PoE-Leistung (W)**: Die maximale Leistung, die vom PoE bereitgestellt werden kann.
- **Insgesamte PoE-Leistungsaufnahme (W)**: Die insgesamt für angeschlossene PoE-Geräte bereitgestellte PoE-Leistung.
- **PoE-Leistungsmodus**: Portbegrenzung oder Klassenbegrenzung.

Wenn Sie den Link *Detail* neben **PoE-Leistungsinformationen zur Mastereinheit** auswählen, gelangen Sie direkt zur Seite Portverwaltung > PoE > Eigenschaften. Auf dieser Seite werden die PoE-Leistungsinformationen zu den einzelnen Einheiten angezeigt.

Die Einheiten im Stack werden grafisch dargestellt, zusammen mit den folgenden Informationen zu jeder Einheit:

- **Einheiten-ID der Mastereinheit**
- **Modellbeschreibung**: Beschreibung des Gerätemodells.
- **Seriennummer**: Seriennummer.
- **PID VID**: Teilenummer und Versions-ID.

Systemeinstellungen

So geben Sie Systemeinstellungen ein:

SCHRITT 1 Wählen Sie **Administration** > **Systemeinstellungen**.

SCHRITT 2 Zeigen Sie die Systemeinstellungen an oder ändern Sie sie.

- **Systembeschreibung**: Zeigt eine Beschreibung des Geräts an.
- **Systemstandort**: Geben Sie den physischen Standort des Geräts ein.
- **Systemkontakt**: Geben Sie den Namen einer Kontaktperson ein.
- **Hostname**: Wählen Sie den Hostnamen dieses Geräts aus. Dieser Wert wird in der Eingabeaufforderung von CLI-Befehlen verwendet:
  - *Standard verwenden*: Der Hostname (Systemname) dieser Switches lautet standardmäßig: *switch123456*, wobei 123456 für die letzten drei Bytes der Geräte-MAC-Adresse im hexadezimalen Format steht.
  - *Benutzerdefiniert*: Geben Sie den Hostnamen ein. Es sind nur Buchstaben, Ziffern und Bindestriche zulässig. Der Hostname darf nicht mit einem Bindestrich beginnen oder enden. Sonderzeichen, Satzzeichen oder Leerzeichen sind nicht zulässig (gemäß RFC1033, 1034, 1035).
- **Einstellungen für benutzerdef. Banner**: Die folgenden Banner können definiert werden:
  - **Anmeldebanner**: Geben Sie den Text ein, der vor der Anmeldung auf der Seite „Anmeldung“ angezeigt werden soll. Klicken Sie auf **Vorschau**, um die Ergebnisse anzuzeigen.
  - **Begrüßungsbanner**: Geben Sie den Text ein, der nach der Anmeldung auf der Seite „Anmeldung“ angezeigt werden soll. Klicken Sie auf **Vorschau**, um die Ergebnisse anzuzeigen.

HINWEIS Wenn Sie über das webbasierte Konfigurationsdienstprogramm ein Anmeldebanner definieren, wird das Banner damit auch für die CLI-Schnittstellen (Konsole, Telnet und SSH) aktiviert.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um die Werte in der aktuellen Konfigurationsdatei zu speichern.

Konsoleneinstellungen (Unterstützung für automatische Baudrate)

Für die Geschwindigkeit des Konsolen-Ports kann einer der folgenden Werte festgelegt werden: „4800“, „9600“, „19200“, „38400“, „57600“ und „115200“ oder „Automatische Erkennung“.

Wenn die automatische Erkennung aktiviert ist, erkennt das Gerät automatisch die Geschwindigkeit der Konsole.

Wenn die automatische Erkennung nicht aktiviert ist, wird die Geschwindigkeit des Konsolen-Ports automatisch auf die letzte manuell festgelegte Geschwindigkeit festgelegt (standardmäßig 115.200).

Wenn die automatische Erkennung aktiviert ist, aber die Baudrate der Konsole noch nicht erkannt wurde, verwendet das System zum Anzeigen von Text (beispielsweise für die Startinformationen) die Geschwindigkeit 115.200.

Sobald die automatische Erkennung auf der Seite „Konsoleneinstellungen“ aktiviert ist, können Sie sie aktivieren, indem Sie die Konsole mit dem Gerät verbinden und zweimal die EINGABETASTE drücken. Das Gerät erkennt die Baudrate automatisch.

So aktivieren Sie die automatische Erkennung oder legen die Baudrate der Konsole manuell fest:

SCHRITT 1 Klicken Sie auf **Administration** > **Konsoleneinstellungen**.

SCHRITT 2 Wählen Sie eine der folgenden Optionen aus:

- **Automatische Erkennung**: Die Baudrate der Konsole wird automatisch erkannt.
- **Statisch**: Wählen Sie eine der verfügbaren Geschwindigkeiten aus.

Management-Schnittstelle

Weitere Informationen hierzu finden Sie unter **IPv4-Management und -Schnittstellen**.

Systemmodus und Stack-Verwaltung

Weitere Informationen hierzu finden Sie unter **Administration: Stack-Verwaltung**.

Benutzerkonten

Weitere Informationen hierzu finden Sie unter **Definieren von Benutzern**.

Definieren des Timeouts für Sitzungsleerlauf

Mit dem *Timeout für Sitzungsleerlauf* legen Sie fest, wie lange Verwaltungssitzungen im Leerlauf bleiben können, bis eine Zeitüberschreitung erfolgt und Sie sich erneut anmelden müssen, um eine der folgenden Sitzungen wiederherzustellen:

- **HTTP-Sitzungstimeout**
- **HTTPS-Sitzungstimeout**
- **Konsolensitzungstimeout**
- **Telnet-Sitzungstimeout**
- **SSH-Sitzungstimeout**

So legen Sie das Timeout für Sitzungsleerlauf für verschiedene Sitzungstypen fest:

SCHRITT 1 Klicken Sie auf **Administration** > **Timeout für Sitzungsleerlauf**.

SCHRITT 2 Wählen Sie in der entsprechenden Liste das Timeout für jede Sitzung aus. Der Standardwert für das Timeout beträgt 10 Minuten.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um die Konfigurationseinstellungen des Geräts festzulegen.

Zeiteinstellungen

Weitere Informationen hierzu finden Sie unter **Administration: Zeiteinstellungen**.

Systemprotokoll

Weitere Informationen hierzu finden Sie unter **Administration: Systemprotokoll**.

Dateiverwaltung

Weitere Informationen hierzu finden Sie unter **Administration: Dateiverwaltung**.

Neustarten des Geräts

Manche Änderungen der Konfiguration, beispielsweise das Aktivieren der Jumbo-Frame-Unterstützung, werden erst nach einem Neustart des Systems wirksam. Durch den Geräteneustart wird jedoch die aktuelle Konfiguration gelöscht. Deshalb müssen Sie die aktuelle Konfiguration als Startkonfiguration speichern, bevor Sie das Gerät neu starten. Durch Klicken auf **Übernehmen** wird die Konfiguration nicht als Startkonfiguration gespeichert. Weitere Informationen zu Dateien und Dateitypen finden Sie im Abschnitt **Systemdateien**.

Sie können die Gerätekonfiguration sichern, indem Sie *Administration > Dateiverwaltung > Konfiguration kopieren/speichern* auswählen oder oben im Fenster auf **Speichern** klicken. Sie können die Konfiguration auch von einem Remote-Gerät hochladen. Weitere Informationen hierzu finden Sie im Abschnitt **Konfiguration/Protokoll herunterladen/sichern**.

Vielleicht möchten Sie den Neustart auf einen günstigen Zeitpunkt in der Zukunft festlegen. In folgenden Fällen könnte dies sinnvoll sein:

- Sie führen Aktionen an einem Remote-Gerät aus, die unter Umständen dazu führen, dass die Verbindung zum Remote-Gerät unterbrochen wird. Wenn Sie einen Neustart im Voraus planen, wird die aktuelle Konfiguration wiederhergestellt und auch die Verbindung zum Remote-Gerät kann wiederhergestellt werden. Wenn diese Aktionen erfolgreich verlaufen, kann der verzögerte Neustart abgebrochen werden.

- Das erneute Laden des Geräts führt zu einem Verlust der Netzwerkverbindung. Mit dem verzögerten Neustart können Sie den Neustart für einen Zeitpunkt planen, der für die Benutzer besser geeignet ist, beispielsweise in der Nacht.

So starten Sie das Gerät neu:

SCHRITT 1 Wählen Sie **Administration** > **Neustart**.

SCHRITT 2 Klicken Sie auf die Schaltfläche **Neustart**, um das Gerät neu zu starten.

- **Neustart**: Startet das Gerät neu. Beim Neustart des Geräts gehen alle nicht gespeicherten Informationen der aktuellen Konfiguration verloren. Damit die aktuelle Konfiguration beim Neustart erhalten bleibt, müssen Sie in der rechten oberen Ecke des jeweiligen Fensters auf **Speichern** klicken. Wenn die Option „Speichern“ nicht angezeigt wird, entspricht die aktuelle Konfiguration der Startkonfiguration und es ist keine Aktion erforderlich.
- **Neustart abbrechen**: Bricht einen Neustart ab, sofern ein Neustart für die Zukunft geplant wurde.

  Folgende Optionen stehen zur Verfügung:

  - *Sofort*: Sofortiger Neustart.
  - *Datum*: Geben Sie das Datum (Monat/Tag) und die Uhrzeit (Stunden und Minuten) für den geplanten Neustart ein. Damit planen Sie, die Software zum festgelegten Termin (24-Stunden-Format verwenden) neu zu laden. Wenn Sie den Monat und den Tag angeben, wird die Software zu der Uhrzeit und dem Datum neu geladen, die/das Sie festgelegt haben. Wenn Sie Monat und Tag nicht angeben, wird die Software zur festgelegten Uhrzeit des aktuellen Tages (sofern sie noch nicht verstrichen ist) oder am nächsten Tag (wenn die festgelegte Uhrzeit bereits verstrichen ist) erneut geladen. Wenn Sie 00:00 angeben, wird das erneute Laden für Mitternacht geplant. Das erneute Laden muss innerhalb von 24 Tagen erfolgen.

    HINWEIS Diese Option kann nur verwendet werden, wenn die Systemzeit entweder manuell oder per SNTP eingestellt wurde.

  - *In*: Neustart innerhalb der angegebenen Anzahl von Stunden und Minuten. Es können maximal 24 Tage festgelegt werden.
- **Standardwerkseinstellungen wiederherstellen**: Startet das Gerät mit der werkseitigen Standardkonfiguration neu. Dabei werden die Startkonfigurationsdatei und die Backup-Konfigurationsdatei gelöscht.

  Für die ID der Stack-Einheit ist „Autom.“ festgelegt, und beim Sx500 ist als Systemmodus „Schicht 2“ eingestellt.

  Die Spiegelkonfigurationsdatei wird beim Wiederherstellen der Werkseinstellungen nicht gelöscht.
- **Startkonfigurationsdatei löschen**: Aktivieren Sie diese Option, um die Startkonfiguration im Gerät beim nächsten Start zu löschen.

HINWEIS Wenn sich das Gerät im Modus „Natives Stacking“ befindet, werden mit dieser Schaltfläche die Werkseinstellungen im gesamten Stack wiederhergestellt.

HINWEIS Das Löschen der Startkonfigurationsdatei und Neustarten ist nicht mit dem Neustarten mit Werkseinstellungen identisch. Das Neustarten mit Werkseinstellungen hat tiefer greifende Auswirkungen.

Routing-Ressourcen

Die TCAM-Zuweisung wird von Sx500- und SG500X-/ESW2-550X-Geräten unterschiedlich behandelt: Das Sx500 verfügt über einen einzelnen TCAM, der für alle Routing- und ACL-Regeln verwendet wird. Die SG500X-/SG500XG-/ESW2-550X-Geräte verfügen über zwei TCAMs, einen für die Routing- und einen für ACL-Regeln.

Wenn sich SG500X-/ESW2-550X-Geräte im Stacking-Modus Hybrid befinden, verfügen sie über nur einen TCAM (wie Sx500-Geräte). Weitere Informationen hierzu finden Sie unter **Stack-Einheitenmodus**.

TCAM-Einträge werden in die folgenden Gruppen unterteilt:

- **IP-Einträge**: TCAM-Einträge, die für statische IP-Routen, IP-Schnittstellen und IP-Hosts reserviert sind.
- **Nicht-IP-Einträge**: TCAM-Einträge, die für andere Anwendungen wie beispielsweise ACL-Regeln, CoS-Überwachungsvorrichtungen und VLAN-Ratenbegrenzungen reserviert sind.

Wenn auf dem Gerät IPv4-Routing aktiviert ist, beschreibt die folgende Tabelle die Anzahl der TCAM-Einträge, die von den verschiedenen Funktionen verwendet werden:

Logische Entität	IPv4
IP-Nachbar	1 Eintrag
IP-Adresse auf einer Schnittstelle	2 Einträge
IP-Remote-Route	1 Eintrag

Wenn auf dem Gerät IPv6-Routing aktiviert ist, finden Sie die Anzahl der TCAM-Einträge, die von den verschiedenen Funktionen verwendet werden, in der nachfolgenden Tabelle:

Logische Entität	IPv4	IPv6 (PCL TCAM)	IPv6 (Router TCAM)
IP-Nachbar	1 Eintrag	1 Eintrag	4 Einträge
IP-Adresse auf einer Schnittstelle	2 Einträge	2 Einträge	8 Einträge
IP-Remote-Route	1 Eintrag	1 Eintrag	4 Einträge
On-Link-Präfix		1 Eintrag	4 Einträge

Auf der Seite „Routing-Ressourcen“ können Sie die TCAM-Zuweisung anpassen.

Wenn Sie die TCAM-Zuweisung auf falsche Weise ändern, wird eine Fehlermeldung angezeigt. Wenn Ihre TCAM-Zuweisung gültig ist, wird eine Meldung angezeigt, aus der hervorgeht, dass ein Neustart mit den neuen Einstellungen ausgeführt wird. Es gibt zwei Möglichkeiten, die Routing-Ressourcen unsachgemäß zu ändern:

- Die Anzahl der zugewiesenen TCAM-Einträge ist niedriger als die der zurzeit verwendeten.
- Die Anzahl der zugewiesenen TCAM-Einträge ist höher als die für die jeweilige Kategorie maximal verfügbare Anzahl (die Maximalwerte werden auf der Seite angezeigt).

So zeigen Sie Routing-Ressourcen an und ändern sie:

SCHRITT 1 Klicken Sie auf **Administration** > **Routing-Ressourcen**.

Für IPv4-Routing-Ressourcen werden folgende Felder angezeigt:

- **Nachbarn (1 TCAM-Eintrag pro Nachbar)**: **Anzahl** entspricht der Anzahl der auf dem Gerät aufgezeichneten Nachbarn und **TCAM-Einträge** entspricht der Anzahl der TCAM-Einträge, die für Nachbarn verwendet werden.
- **Schnittstellen (2 TCAM-Einträge pro Schnittstelle)**: **Anzahl** entspricht der Anzahl der IP-Adressen der Schnittstellen auf dem Gerät und **TCAM-Einträge** entspricht der Anzahl der TCAM-Einträge, die für IP-Adressen verwendet werden.
- **Routen (1 TCAM-Eintrag pro Route)**: **Anzahl** entspricht der Anzahl der auf dem Gerät aufgezeichneten Routen und **TCAM-Einträge** entspricht der Anzahl der TCAM-Einträge, die für die Routen verwendet werden.
- **Gesamt**: Zeigt die Anzahl der aktuell verwendeten TCAM-Einträge an.

- **Max. Einträge**: Wählen Sie eine der folgenden Optionen:
  - *Standard verwenden*: Für das Sx500 entspricht die Anzahl der TCAM-Einträge 25 % der TCAM-Größe. Für das SG500X/SG500XG entspricht die Anzahl der Router-TCAM-Einträge 50 % der Router-TCAM-Größe.
  - *Benutzerdefiniert*: Geben Sie einen Wert ein.

IPv4-Multicast-Routing-Ressourcen (nur für SG500XG- und SG500X-Geräte)

- **IPv4-Multicast-Routen (2 TCAM-Einträge pro Route)**: **Anzahl** gibt die Anzahl der auf dem Gerät aufgezeichneten Multicast-Routen an und **TCAM-Einträge** gibt die Anzahl der TCAM-Einträge an, die für Multicast-Routen verwendet werden.
- **Max. Einträge**: Wählen Sie eine der folgenden Optionen:
  - *Standard verwenden*: Für das Sx500 entspricht die Anzahl der TCAM-Einträge 25 % der TCAM-Größe. Für das SG500X/SG500XG entspricht die Anzahl der Router-TCAM-Einträge 50 % der Router-TCAM-Größe.
  - *Benutzerdefiniert*: Geben Sie einen Wert ein.

IPv6-Routing-Ressourcen (nur für SG500XG- und SG500X-Geräte)

- **Nachbarn (4 TCAM-Einträge pro Route)**: **Anzahl** entspricht der Anzahl der auf dem Gerät aufgezeichneten Nachbarn und **TCAM-Einträge** entspricht der Anzahl der TCAM-Einträge, die für Nachbarn verwendet werden.
- **Schnittstellen (8 TCAM-Einträge pro Route)**: **Anzahl** entspricht der Anzahl der Schnittstellen auf dem Gerät und **TCAM-Einträge** entspricht der Anzahl der TCAM-Einträge, die für Schnittstellen verwendet werden.
- **On Link-Präfixe (4 TCAM-Einträge pro Präfix)**: **Anzahl** entspricht der Anzahl der Link-Präfixe, die auf dem Gerät aufgezeichnet sind und **TCAM-Einträge** gibt die Anzahl der für sie verwendeten TCAM-Einträge an.
- **Gesamt**: Die Gesamtanzahl der verwendeten TCAM-Einträge.
- **Max. Einträge**: Wählen Sie eine der folgenden Optionen:
  - *Standard verwenden*: Für das Sx500 entspricht die Anzahl der TCAM-Einträge 25 % der TCAM-Größe. Für das SG500X/SG500XG entspricht die Anzahl der Router-TCAM-Einträge 50 % der Router-TCAM-Größe.
  - *Benutzerdefiniert*: Geben Sie einen Wert ein.

IPv6-Multicast-Routing-Ressourcen (nur für SG500XG- und SG500X-Geräte)

- **IPv6-Multicast-Routen (8 TCAM-Einträge pro Route)**: **Anzahl** gibt die Anzahl der auf dem Gerät aufgezeichneten Multicast-Routen an und **TCAM-Einträge** gibt die Anzahl der TCAM-Einträge an, die für Multicast-Routen verwendet werden.

- **Max. Einträge**: Wählen Sie eine der folgenden Optionen:
  - *Standard verwenden*: Für das Sx500 entspricht die Anzahl der TCAM-Einträge 25 % der TCAM-Größe. Für das SG500X/SG500XG entspricht die Anzahl der Router-TCAM-Einträge 50 % der Router-TCAM-Größe.
  - *Benutzerdefiniert*: Geben Sie einen Wert ein.

TCAM-Ressourcen-Tabelle

Folgende Felder werden für jede Einheit angezeigt:

- **Max. Anzahl von TCAM-Einträgen für Routing und Multicast-Routing**: Anzahl der für das Routing und Multicast-Routing verfügbaren TCAM Einträge.
- **IPv4-Routing**
  - **In Verwendung:** Anzahl der für das IPv4-Routing verwendeten TCAM-Einträge.
  - **Maximum:** Maximale Anzahl der für das IPv4-Routing verfügbaren TCAM-Einträge.
- **IPv4-Multicast-Routing**
  - **In Verwendung:** Anzahl der für das IPv4-Multicast-Routing verwendeten TCAM-Einträge.
  - **Maximum:** Maximale Anzahl der für das IPv4-Multicast-Routing verfügbaren TCAM-Einträge.
- **IPv6-Routing**
  - **In Verwendung:** Anzahl der für das IPv6-Routing verwendeten TCAM-Einträge.
  - **Maximum:** Maximale Anzahl der für das IPv6-Routing verfügbaren TCAM-Einträge.
- **IPv6-Multicast-Routing**
  - **In Verwendung:** Anzahl der für das IPv6-Multicast-Routing verwendeten TCAM-Einträge.
  - **Maximum:** Maximale Anzahl der für das IPv6-Multicast-Routing verfügbaren TCAM-Einträge.
- **Maximum TCAM-Einträge für Nicht-IP-Regeln**: Anzahl der für Nicht-IP-Regeln verfügbaren TCAM-Einträge.
- **Nicht-IP-Regeln**
  - **In Verwendung:** Anzahl der für Nicht-IP-Regeln verwendeten TCAM-Einträge.
  - **Maximum:** Maximale Anzahl der für Nicht-IP-Regeln verfügbaren TCAM-Einträge.

SCHRITT 2 Speichern Sie die neuen Einstellungen, indem Sie auf **Übernehmen** klicken. Daraufhin wird die Gültigkeit der Einstellungen für Routing-Ressourcen überprüft. Wenn sie ungültig ist, wird eine Fehlermeldung angezeigt. Wenn sie gültig sind, werden die Einstellungen in die aktuelle Konfigurationsdatei kopiert.

HINWEIS Eine Übersicht der tatsächlich verwendeten und verfügbaren TCAM-Einträge wird unten auf dieser Seite angezeigt. Eine Erläuterung der einzelnen Felder finden Sie unter **TCAM-Auslastung**.

SCHRITT 3 Speichern Sie die neuen Einstellungen, indem Sie auf **Übernehmen** klicken. Daraufhin wird die Gültigkeit der TCAM-Zuweisung überprüft. Wenn sie ungültig ist, wird eine Fehlermeldung angezeigt. Wenn die Zuweisung richtig ist, wird sie in die aktuelle Konfigurationsdatei kopiert und ein Neustart wird durchgeführt.

Integrität

Auf der Zustandsseite wird der Lüfterstatus aller Geräte mit Lüftern angezeigt. Je nach Modell kann ein Gerät über einen oder mehrere Lüfter verfügen. Einige Modelle haben keine Lüfter.

Manche Geräte besitzen einen Temperatursensor zum Schutz der Hardware vor Überhitzung. Bei einer Überhitzung und in der darauf folgenden Abkühlphase werden vom Gerät folgende Aktionen durchgeführt:

Ereignis	Aktion
Mindestens ein Temperatursensor überschreitet den Warnschwellenwert	Das System generiert: ▪ SYSLOG-Meldung ▪ SNMP-Trap
Mindestens ein Temperatursensor überschreitet den kritischen Schwellenwert	Das System generiert: ▪ SYSLOG-Meldung ▪ SNMP-Trap Folgende Aktionen werden durchgeführt: ▪ System-LED leuchtet dauerhaft Gelb (sofern die Hardware das unterstützt). ▪ Ports deaktivieren: Wenn die kritische Temperatur für zwei Minuten überschritten wird, werden alle Ports heruntergefahren. ▪ (Geräte, die PoE unterstützen) PoE-Stromkreis unterbrechen, sodass weniger Strom verbraucht und weniger Wärme abgegeben wird.

Ereignis	Aktion
Abkühlphase im Anschluss an den kritischen Schwellenwert wurde überschritten (alle Sensoren liegen unter dem Warnschwellenwert - 2 °C).	Nachdem alle Sensoren auf den Warnschwellenwert - 2 °C herabgekühlt sind, wird die PHY wieder aktiviert und alle Ports wieder hochgefahren. Wenn der Lüfterstatus OK ist, werden die Ports aktiviert. (Geräte, die PoE unterstützen) Der PoE-Stromkreis wird wieder aktiviert.

Um die Parameter für den Gerätezustand anzuzeigen, wählen Sie **Status und Statistik** > **Zustand**.

Auf der Seite „Zustand“ werden die folgenden Felder angezeigt:

- **Lüfterstatus**: Der Status des Lüfters. Folgende Werte sind möglich:
  - *OK*: Der Lüfter befindet sich im Normalbetrieb.
  - *Fehler*: Der Lüfter befindet sich nicht im Normalbetrieb.
  - *n/v*: Eine Lüfter-ID ist für das jeweilige Modell nicht verfügbar.
- **Lüfterrichtung**: (relevante Geräte) Die Laufrichtung der Lüfter (z. B. von vorne nach hinten).
- **Temperatur**: Folgende Optionen sind möglich:
  - *OK*: Die Temperatur liegt unter dem Schwellenwert für „Warnung“.
  - *Warnung*: Die Temperatur liegt zwischen dem Schwellenwert für „Warnung“ und dem Schwellenwert „Kritisch“.
  - *Kritisch*: Die Temperatur liegt über dem Schwellenwert „Kritisch“.

Im Standalone-Modus werden für das Gerät die folgenden Felder angezeigt:

- **Lüfterstatus**: Der Status des Lüfters. Folgende Werte sind möglich:
  - *OK*: Der Lüfter bzw. die Lüfter befinden sich im Normalbetrieb.
  - *Fehler*: Der Lüfter bzw. die Lüfter arbeiten nicht ordnungsgemäß.
  - *n/v*: Ein Lüfter ist für dieses Modell nicht verfügbar.
- **Lüfterrichtung**: Die Laufrichtung der Lüfter.
- **Temperatur**: Folgende Optionen sind möglich:
  - *OK*: Die Temperatur liegt unter dem Schwellenwert für „Warnung“.

- *Warnung*: Die Temperatur liegt zwischen dem Schwellenwert für „Warnung“ und dem Schwellenwert „Kritisch“.
- *Kritisch*: Die Temperatur liegt über dem Schwellenwert „Kritisch“.

Befindet sich das Gerät im Modus „Nativer Stack“, werden auf der Zustandsseite für die einzelnen Einheiten die obigen Felder angezeigt:

Diagnose

Weitere Informationen hierzu finden Sie unter **Administration: Diagnose**.

Erkennung – Bonjour

Weitere Informationen hierzu finden Sie unter **Bonjour**.

Erkennung – LLDP

Weitere Informationen hierzu finden Sie unter **Konfigurieren von LLDP**.

Erkennung – CDP

Weitere Informationen hierzu finden Sie unter **Konfigurieren von CDP**.

Ping

Mit dem Dienstprogramm Ping können Sie die Erreichbarkeit eines Remote-Hosts testen und die Umlaufzeit von Paketen messen, die vom Gerät an ein Zielgerät gesendet werden.

Ping sendet ICMP-Echo-Anforderungspakete (Internet Control Message Protocol) an den Zielhost und wartet auf eine ICMP-Antwort, die manchmal als „Pong“ bezeichnet wird. Dabei misst das Dienstprogramm die Umlaufzeit und zeichnet Paketverluste auf.

So verwenden Sie Ping für einen Host:

SCHRITT 1 Klicken Sie auf **Administration > Ping**.

SCHRITT 2 Konfigurieren Sie Ping, indem Sie Werte in die folgenden Felder eingeben:

- **Hostdefinition**: Wählen Sie aus, ob die Quellschnittstelle anhand ihrer IP-Adresse oder ihres Namens angegeben wird. Dieses Feld wirkt sich auf die Schnittstellen aus, die im Feld „Quell-IP“ angezeigt werden. Siehe unten.
- **IP-Version**: Wenn die Quellschnittstelle anhand der IP-Adresse identifiziert wird, wählen Sie „IPv4“ oder „IPv6“ aus, um anzugeben, dass die IP-Adresse im ausgewählten Format eingegeben wird.
- **Quell-IP**: Wählen Sie die Quellschnittstelle aus, deren IPv4-Adresse als Quell-IPv4-Adresse für die Kommunikation mit dem Ziel verwendet wird. Wenn das Feld „Hostdefinition“ „Nach Name“ lautete, werden alle IPv4- und IPv6-Adressen in diesem Dropdownfeld angezeigt. Wenn das Feld „Hostdefinition“ „Nach IP-Adresse“ lautete, werden nur die bestehenden IP-Adressen des Typs angezeigt, der im Feld „IP-Version“ definiert wurde.

  HINWEIS Wenn Sie die Option „Autom.“ ausgewählt haben, verarbeitet das System die Quelladresse auf der Basis der Zieladresse.
- **Typ der Ziel-IPv6-Adresse**: Wählen Sie „Link-Local“ oder „Global“ als IPv6-Adresstyp aus, der als Ziel-IP-Adresse eingegeben wird.
  - *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
  - *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.
- **Link Local-Schnittstelle**: Wenn der IPv6-Adresstyp „Link Local“ entspricht, wählen Sie aus, von wo der Empfang erfolgt.
- **Ziel-IP-Adresse/Name**: Die Adresse oder der Hostname des Geräts, an das der Ping gesendet werden soll. Ob es sich dabei um eine IP-Adresse oder um einen Hostnamen handelt, hängt von der Hostdefinition ab.
- **Ping-Intervall**: Gibt an, wie lange das System zwischen den Ping-Paketen wartet. Ping wird so oft wiederholt, wie im Feld **Anzahl der Pings** konfiguriert. Dabei spielt es keine Rolle, ob der Ping erfolgreich war. Wählen Sie aus, ob Sie das Standardintervall verwenden möchten, oder geben Sie einen eigenen Wert an.
- **Anzahl der Pings**: Gibt an, wie oft der Ping-Vorgang ausgeführt wird. Wählen Sie aus, ob Sie die Standardeinstellung verwenden möchten, oder geben Sie einen eigenen Wert an.

- **Status**: Zeigt an, ob der Ping erfolgreich war oder fehlgeschlagen ist.

SCHRITT 3 Klicken Sie auf **Ping aktivieren**, um den Ping an den Host zu senden. Der Ping-Status wird angezeigt und zur Liste der Nachrichten wird eine Nachricht hinzugefügt, aus der das Ergebnis des Ping-Vorgangs hervorgeht.

SCHRITT 4 Sie können die Ping-Ergebnisse im Abschnitt **Ping-Zähler und -Status** der Seite anzeigen.

Traceroute

Traceroute erkennt die IP-Routen, über die Pakete weitergeleitet werden. Hierzu wird ein IP-Paket an den Zielhost und zurück an das Gerät gesendet. Auf der Seite Traceroute werden die einzelnen Hops zwischen dem Gerät und einem Zielhost sowie die Umlaufzeit zu jedem dieser Hops angezeigt.

SCHRITT 1 Klicken Sie auf **Administration > Traceroute**.

SCHRITT 2 Konfigurieren Sie Traceroute, indem Sie Informationen in die folgenden Felder eingeben:

- **Hostdefinition**: Wählen Sie aus, ob Hosts anhand der IP-Adresse oder anhand des Namens identifiziert werden.
- **IP-Version**: Wenn der Host anhand der IP-Adresse identifiziert wird, wählen Sie IPv4 oder IPv6 aus, um anzugeben, dass die IP-Adresse im ausgewählten Format eingegeben wird.
- **Quell-IP**: Wählen Sie die Quellschnittstelle aus, deren IPv4-Adresse als Quell-IPv4-Adresse für Nachrichten im Rahmen der Kommunikation verwendet wird. Wenn das Feld „Hostdefinition“ „Nach Name“ lautete, werden alle IPv4- und IPv6-Adressen in diesem Dropdownfeld angezeigt. Wenn das Feld „Hostdefinition“ „Nach IP-Adresse“ lautete, werden nur die bestehenden IP-Adressen des Typs angezeigt, der im Feld „IP-Version“ definiert wurde.
- **Host-IP-Adresse/Name**: Geben Sie die Hostadresse oder den Hostnamen ein.
- **TTL**: Geben Sie die maximale Anzahl der Hops ein, die Traceroute zulässt. Dadurch soll verhindert werden, dass der gesendete Frame eine Endlosschleife durchläuft. Der Traceroute-Befehl wird beendet, wenn das Ziel oder dieser Wert erreicht ist. Wenn Sie den Standardwert (30) verwenden möchten, wählen Sie **Standard verwenden** aus.
- **Timeout**: Geben Sie an, wie lange das System auf die Rückkehr eines Frames wartet, bis dieser für verloren erklärt wird, oder wählen Sie **Standard verwenden** aus.

SCHRITT 3 Klicken Sie auf **Traceroute aktivieren**. Der Vorgang wird ausgeführt.

Eine Seite wird geöffnet, auf der in den folgenden Feldern die Umlaufzeit (Round Trip Time, RTT) und der Status für jeden Weg angezeigt werden:

- **Index**: Zeigt die Nummer des Hops an.
- **Host**: Zeigt einen Stopp auf der Route zum Ziel an.
- **Umlaufzeit** *(1-3)*: Zeigt die Umlaufzeit in Millisekunden für den ersten bis dritten Frame und den Status des ersten bis dritten Vorgangs an.

8

Administration: Zeiteinstellungen

Synchronisierte Systemuhren bilden einen gemeinsamen Referenzrahmen für alle Geräte im Netzwerk. Die Synchronisierung der Netzwerkzeit ist sehr wichtig, da alle Vorgänge zur Verwaltung, Sicherung, Planung und Fehlerbehebung in einem Netzwerk auf den zeitlichen Ablauf von Ereignissen ausgerichtet sind. Ohne synchronisierte Uhren ist keine korrekte Koordination der Protokolldateien zwischen Geräten (beispielsweise beim Nachverfolgen von Sicherheitsverletzungen oder der Netzwerkverwendung) möglich.

Durch die zeitliche Abstimmung werden auch die Konflikte in gemeinsam genutzten Dateisystemen verringert, denn die Änderungszeiten müssen konsistent sein, unabhängig davon, auf welchem Computer sich das Dateisystem befindet.

Aus diesen Gründen ist es entscheidend, dass die Uhrzeit aller Geräte im Netzwerk richtig konfiguriert wird.

HINWEIS Das Gerät unterstützt SNTP (Simple Network Time Protocol, einfaches Netzwerkzeitprotokoll). Wenn es aktiviert ist, synchronisiert das Gerät seine Uhrzeit dynamisch mit der eines SNTP-Servers. Das Gerät wird nur als SNTP-Client betrieben und kann keine Zeitdienste für andere Geräte leisten.

In diesem Abschnitt werden die Optionen für das Konfigurieren der Systemzeit, Zeitzone und Sommerzeit beschrieben. Die folgenden Themen werden behandelt:

- **Optionen für die Systemzeit**
- **SNTP-Modi**
- **Konfigurieren der Systemzeit**

Optionen für die Systemzeit

Die Systemzeit kann manuell durch den Benutzer oder dynamisch über einen SNTP-Server festgelegt werden oder über den PC synchronisiert werden, auf dem die grafische Benutzeroberfläche ausgeführt wird. Falls ein SNTP-Server verwendet wird, werden die manuellen Zeiteinstellungen überschrieben, wenn die Kommunikation mit dem Server hergestellt wird.

Während des Startvorgangs konfiguriert das Gerät immer die Uhrzeit, Zeitzone und Sommerzeit. Diese Parameter werden von dem PC, auf dem die grafische Benutzeroberfläche ausgeführt wird, über SNTP, über manuell festgelegte Werte oder, falls all dies erfolglos ist, aus den Werkseinstellungen bezogen.

Uhrzeit

Die Systemzeit des Geräts kann mit den folgenden Methoden festgelegt werden:

- **Manuell**: Der Benutzer muss die Uhrzeit manuell festlegen.
- **Über den PC**: Die Uhrzeit kann anhand von Browserinformationen vom PC bezogen werden.

  Die Konfiguration der Uhrzeit über den Computer wird in der aktuellen Konfigurationsdatei gespeichert. Sie müssen die aktuelle Konfiguration in die Startkonfiguration kopieren, damit das Gerät nach dem Neustart die Uhrzeit des Computers verwendet. Nach dem Neustart wird die Uhrzeit bei der ersten Webanmeldung beim Gerät festgelegt.

  Wenn Sie diese Funktion zum ersten Mal konfigurieren und die Uhrzeit noch nicht festgelegt war, wird das Gerät auf die vom PC empfangene Uhrzeit festgelegt.

  Diese Methode für das Beziehen der Uhrzeit funktioniert bei HTTP- und HTTPS-Verbindungen.
- **SNTP**: Die Uhrzeit kann von SNTP-Zeitservern bezogen werden. SNTP gewährleistet eine auf die Millisekunde genaue Synchronisierung der Netzwerkzeit des Geräts. Als Uhrzeitquelle wird dabei ein SNTP-Server verwendet. Wenn Sie beim Angeben eines SNTP-Servers die Identifizierung anhand des Hostnamens auswählen, werden auf der grafischen Benutzeroberfläche drei Vorschläge angezeigt:
  - time-a.timefreq.bldrdoc.gov
  - time-b.timefreq.bldrdoc.gov
  - time-c.timefreq.bldrdoc.gov

Wenn die Uhrzeit mit einer der drei oben genannten Quellen festgelegt wurde, wird sie nicht erneut vom Browser festgelegt.

HINWEIS SNTP ist die empfohlene Methode für die Uhrzeiteinstellung.

Zeitzone und Sommerzeit

Die Zeitzone und die Sommerzeit können wie folgt auf dem Gerät eingestellt werden:

- Dynamische Konfiguration des Geräts über einen DHCP-Server, wobei gilt:
  - Wenn die dynamische Sommerzeit aktiviert und verfügbar ist, hat sie immer Vorrang vor der manuellen Konfiguration der Sommerzeit.
  - Falls der Server, der die Quellparameter bereitstellt, ausfällt oder die dynamische Konfiguration vom Benutzer deaktiviert wurde, werden die manuellen Einstellungen verwendet.
  - Die dynamische Konfiguration der Zeitzone und der Sommerzeit wird fortgeführt, nachdem die Lease-Zeit der IP-Adresse abgelaufen ist.

- Die manuelle Konfiguration der Zeitzone und der Sommerzeit wird nur dann verwendet, wenn die dynamische Konfiguration deaktiviert oder nicht erfolgreich ist.

  HINWEIS Der DHCP-Server muss die DHCP-Option 100 bereitstellen, damit die dynamische Zeitzonenkonfiguration erfolgen kann.

SNTP-Modi

Das Gerät kann die Systemzeit mit einer der folgenden Methoden von einem SNTP-Server empfangen:

- **Client-Broadcast-Empfang (passiver Modus)**: SNTP-Server übertragen die Uhrzeit und das Gerät hört diese Broadcasts mit. Wenn das Gerät in diesem Modus arbeitet, muss kein Unicast-SNTP-Server festgelegt werden.
- **Client-Broadcast-Übertragung (aktiver Modus)**: Das Gerät fordert als SNTP-Client in regelmäßigen Abständen SNTP-Zeitaktualisierungen an. In diesem Modus wird eine der folgenden Methoden verwendet:
  - **SNTP-Anycast-Client-Modus**: Das Gerät überträgt Zeitanforderungspakete an alle SNTP-Server im Subnetz und wartet auf eine Antwort.
  - **Unicast-SNTP-Server-Modus**: Das Gerät sendet Unicast-Anfragen an die Liste der manuell konfigurierten SNTP-Server und wartet auf eine Antwort.

Das Gerät unterstützt die gleichzeitige Aktivierung aller oben genannten Modi und wählt entsprechend der kürzesten Entfernung von der Referenzuhr die beste von einem SNTP-Server empfangene Systemzeit aus.

Konfigurieren der Systemzeit

Auswählen einer Quelle für die Systemzeit

Auf der Seite „Systemzeit“ können Sie die Quelle für die Systemzeit auswählen. Wenn Sie die Quelle „Manuell“ ausgewählt haben, können Sie hier die Uhrzeit eingeben.

VORSICHT Wenn die Systemzeit manuell festgelegt wird und das Gerät neu gestartet wird, muss die manuelle Zeiteinstellung neu eingegeben werden.

So legen Sie die Systemzeit fest:

SCHRITT 1 Klicken Sie auf **Administration** > **Zeiteinstellungen** > **Systemzeit**.

Die folgenden Felder werden angezeigt:

- **Tatsächliche Zeit (Statisch)**: Die Systemzeit des Geräts. Hier wird die DHCP-Zeitzone oder das Akronym für die benutzerdefinierte Zeitzone angezeigt, sofern definiert.
- **Letzter synchronisierter Server**: Adresse, Stratum und Typ des SNTP-Servers, von dem die Systemzeit zuletzt bezogen wurde.

SCHRITT 2 Geben Sie die folgenden Parameter ein:

Einstellungen für Quelle der Uhr: Wählen Sie die Quelle für das Einstellen der Systemuhr aus.

- **Hauptuhrzeitquelle (SNTP-Server)**: Wenn diese Option aktiviert ist, wird die Systemzeit von einem SNTP-Server bezogen. Um diese Funktion zu verwenden, müssen Sie außerdem auf der Seite „SNTP-Schnittstelleneinstellungen“ eine Verbindung mit einem SNTP-Server konfigurieren. Erzwingen Sie optional auf der Seite „SNTP-Authentifizierung“ die Authentifizierung der SNTP-Sitzungen.
- **Alternative Quelle für Uhr (PC über aktive HTTP/HTTPS-Sitzungen)**: Wählen Sie diese Option aus, um Datum und Uhrzeit mithilfe des HTTP-Protokolls über den konfigurierenden Computer festzulegen.

  HINWEIS Die Einstellungen für die Uhrzeitquelle müssen Sie auf eine der oben genannten Optionen festlegen, damit die RIP-MD5-Authentifizierung möglich ist. Dies unterstützt auch Funktionen, die die Uhrzeit verwenden. Beispiel: Uhrzeitbasierte ACL, Port und 802.1-Portauthentifizierung, die von manchen Geräten unterstützt werden.

Manuelle Einstellungen: Legen Sie Datum und Uhrzeit manuell fest. Die lokale Uhrzeit wird verwendet, wenn keine alternative Zeitquelle (beispielsweise ein SNTP-Server) verfügbar ist:

- **Datum**: Geben Sie das Systemdatum ein.
- **Lokale Zeit**: Geben Sie die Systemzeit ein.

Zeitzoneneinstellungen: Es wird die lokale Uhrzeit über den DHCP-Server oder die Zeitzonendifferenz verwendet.

- **Zeitzone von DHCP abrufen**: Wählen Sie diese Option, um die dynamische Konfiguration der Zeitzone und der Sommerzeit vom DHCP-Server zu aktivieren. Ob einer oder beide dieser Parameter konfiguriert werden können, hängt von den im DHCP-Paket enthaltenen Informationen ab. Wenn diese Option aktiviert ist, *muss der DHCP-Client auf dem Gerät aktiviert sein*.

  HINWEIS Der DHCP-Client unterstützt Option 100 für die Bereitstellung der dynamischen Zeitzoneneinstellung.
- **Zeitzone über DHCP**: Zeigt das Akronym der über den DHCP-Server konfigurierten Zeitzone an. Dieses Akronym wird im Feld **Aktuelle Zeit** angezeigt.

- **Zeitzonendifferenz**: Wählen Sie die Differenz zwischen *GMT* (Greenwich Mean Time) und der lokalen Uhrzeit in Stunden aus. Die Zeitzonendifferenz für Paris beträgt beispielsweise GMT +1 und die für New York GMT –5.
- **Zeitzonenakronym**: Geben Sie einen Namen ein, der diese Zeitzone darstellt. Dieses Akronym wird im Feld **Aktuelle Zeit** angezeigt.

Einstellungen für Sommer-/Winterzeit: Wählen Sie aus, wie die Sommerzeit definiert ist:

- **Sommerzeit**: Wählen Sie diese Option aus, um die Sommerzeit zu aktivieren.
- **Zeitdifferenz**: Geben Sie die Differenz zur Greenwich Mean Time (GMT) in Minuten (von 1 - 1440) ein. Der Standardwert lautet „60“.
- **Sommerzeit-Typ**: Klicken Sie auf eine der folgenden Optionen:
  - *USA*: Die Sommerzeit wird gemäß den in den USA geltenden Daten festgelegt.
  - *Europäisch*: Die Sommerzeit wird gemäß den Daten festgelegt, die in der EU und anderen Ländern, in denen dieser Standard gilt, verwendet werden.
  - *Nach Datum*: Die Sommerzeit wird manuell festgelegt, normalerweise für Länder außerhalb der USA oder Europas. Geben Sie die nachstehend beschriebenen Parameter ein.
  - *Wiederkehrend*: Die Sommerzeit tritt jedes Jahr zur gleichen Zeit auf.

  Wenn Sie *Nach Datum* auswählen, können Sie Anfang und Ende der Sommerzeit anpassen.
  - **Von**: Tag und Uhrzeit des Beginns der Sommerzeit.
  - **Bis**: Tag und Uhrzeit des Endes der Sommerzeit.

  Wenn Sie *Wiederkehrend* auswählen, können Sie Anfang und Ende der Sommerzeit anderweitig anpassen.
- **Von**: Datum, an dem die Sommerzeit jedes Jahr beginnt.
  - *Tag*: Wochentag, an dem die Sommerzeit jedes Jahr beginnt.
  - *Woche*: Woche innerhalb des Monats, in der die Sommerzeit jedes Jahr beginnt.
  - *Monat*: Monat des Jahres, in dem die Sommerzeit jedes Jahr beginnt.
  - *Uhrzeit*: Uhrzeit, zu der die Sommerzeit jedes Jahr beginnt.
- **Bis**: Datum, an dem die Sommerzeit jedes Jahr endet. Wenn die Sommerzeit lokal beispielsweise immer am vierten Freitag im Oktober um 5:00 Uhr endet, lauten die Parameter wie folgt:
  - *Tag*: Wochentag, an dem die Sommerzeit jedes Jahr endet.
  - *Woche*: Woche innerhalb des Monats, in der die Sommerzeit jedes Jahr endet.

- *Monat*: Monat des Jahres, in dem die Sommerzeit jedes Jahr endet.
- *Uhrzeit*: Uhrzeit, zu der die Sommerzeit jedes Jahr endet.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Systemzeitwerte werden in die aktuelle Konfigurationsdatei geschrieben.

Hinzufügen eines Unicast-SNTP-Servers

Sie können bis zu 16 Unicast-SNTP-Server konfigurieren.

HINWEIS Um einen Unicast-SNTP-Server anhand des Namens anzugeben, müssen Sie zuerst DNS-Server für das Gerät konfigurieren (siehe **DNS-Einstellungen**).

So fügen Sie einen Unicast-SNTP-Server hinzu:

SCHRITT 1 Klicken Sie auf **Administration** > **Zeiteinstellungen** > **SNTP-Unicast**.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **SNTP-Unicast-Client**: Wählen Sie diese Option aus, um das Gerät zu aktivieren und damit SNTP-vordefinierte Unicast-Clients mit Unicast-SNTP-Servern zu verwenden.
- **IPv4-Quellschnittstelle**: Wählen Sie die IPv4-Schnittstelle aus, deren IPv4-Adresse als Quell-IPv4-Adresse in Nachrichten für die Kommunikation mit dem SNTP-Server verwendet wird.
- **IPv6-Quellschnittstelle**: Wählen Sie die IPv6-Schnittstelle aus, deren IPv6-Adresse als Quell-IPv6-Adresse in Nachrichten für die Kommunikation mit dem SNTP-Server verwendet wird.

  HINWEIS Wenn Sie die Option „Auto“ auswählen, übernimmt das System die Quell-IP-Adresse aus der IP-Adresse, die auf der ausgehenden Schnittstelle definiert wurde.

Auf dieser Seite werden folgende Informationen für die einzelnen Unicast-SNTP-Server angezeigt:

- **SNTP-Server**: IP-Adresse des SNTP-Servers. Der Server oder Hostname mit der geringsten Entfernung wird ausgewählt.
- **Abrufintervall**: Zeigt an, ob Abrufe aktiviert oder deaktiviert sind.
- **Authentifizierungsschlüssel-ID**: Schlüssel-ID, die für die Kommunikation zwischen dem SNTP-Server und dem Gerät verwendet wird.
- **Stratum-Ebene**: Die als numerischer Wert ausgedrückte Entfernung von der Referenzuhr. Ein SNTP-Server kann nur als primärer Server (Stratum-Ebene 1) festgelegt werden, wenn das Abrufintervall aktiviert ist.

- **Status**: Status des SNTP-Servers. Folgende Werte sind gültig:
  - *Oben*: Der SNTP-Server arbeitet derzeit ordnungsgemäß.
  - *Unten*: Der SNTP-Server ist derzeit nicht verfügbar.
  - *Unbekannt*: Der SNTP-Server wird derzeit vom Gerät gesucht.
  - *In Bearbeitung*: Wird angezeigt, wenn der SNTP-Server dem eigenen Zeitserver nicht vollständig vertraut (beispielsweise beim ersten Starten des SNTP-Servers).
- **Letzte Antwort**: Datum und Uhrzeit, zu der zum letzten Mal eine Antwort von diesem SNTP-Server empfangen wurde.
- **Versatz**: Der geschätzte Zeitunterschied zwischen der Server-Uhr und der lokalen Uhr in Millisekunden. Der Host ermittelt diesen Versatzwert mit dem in RFC 2030 beschriebenen Algorithmus.
- **Verzögerung**: Die geschätzte Umlaufverzögerung, die aufgrund des Netzwerkpfads zwischen der Server-Uhr und der lokalen Uhr auftritt (in Millisekunden). Der Host ermittelt diesen Verzögerungswert mit dem in RFC 2030 beschriebenen Algorithmus.
- **Quelle**: Methode zur Definition des SNTP-Servers. Beispiel: manuell oder über DHCPv6-Server.
- **Schnittstelle**: Die Schnittstelle, an der Pakete empfangen werden.

SCHRITT 3 Zum Hinzufügen eines Unicast-SNTP-Servers aktivieren Sie die Option **SNTP-Unicast-Client**.

SCHRITT 4 Klicken Sie auf **Hinzufügen**.

SCHRITT 5 Geben Sie die folgenden Parameter ein:

- **Serverdefinition**: Wählen Sie aus, ob der SNTP-Server über seine IP-Adresse identifiziert werden soll oder ob Sie den Namen eines bekannten SNTP-Servers aus der Liste auswählen möchten.

HINWEIS Wenn Sie einen bekannten SNTP-Server angeben möchten, muss das Gerät mit dem Internet verbunden und mit einem DNS-Server konfiguriert sein oder so konfiguriert sein, dass ein DNS-Server durch die Verwendung von DHCP identifiziert wird (siehe **DNS-Einstellungen**).

- **IP-Version**: Wählen Sie die Version der IP-Adresse aus: **Version 6** oder **Version 4**.
- **IPv6-Adresstyp**: Wählen Sie den IPv6-Adresstyp aus (falls IPv6 verwendet wird). Folgende Optionen sind möglich:
  - *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.

  - *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.

- **Link Local-Schnittstelle**: Wählen Sie in der Liste die Link Local-Schnittstelle aus (falls der IPv6-Adresstyp „Link Local“ ausgewählt ist).
- **SNTP-Server-IP-Adresse**: Geben Sie die IP-Adresse des SNTP-Servers ein. Das Format hängt vom ausgewählten Adresstyp ab.
- **SNTP-Server**: Wählen Sie den Namen des SNTP-Servers aus einer Liste bekannter NTP-Server aus. Falls Sie **Sonstiges** auswählen, geben Sie den Namen des SNTP-Servers in das nebenstehende Feld ein.
- **Abrufintervall**: Wählen Sie diese Option, um die Befragung des SNTP-Servers nach Systemzeitinformationen zu aktivieren. Alle NTP-Server, die für das Polling registriert sind, werden befragt. Die Uhrzeit des erreichbaren Servers mit dem niedrigsten Stratum-Wert (Entfernung von der Referenzuhr) wird ausgewählt. Der Server mit dem niedrigsten Stratum-Wert wird als primärer Server betrachtet. Der Server mit dem nächstniedrigeren Stratum-Wert gilt als sekundärer Server und so weiter. Wenn der primäre Server nicht verfügbar ist, befragt das Gerät alle Server, für die das Polling aktiviert ist, und wählt einen neuen Primärserver mit niedrigstem Stratum-Wert aus.
- **Authentifizierung**: Aktivieren Sie das Kontrollkästchen, um die Authentifizierung zu aktivieren.
- **Authentifizierungsschlüssel-ID**: Falls die Authentifizierung aktiviert ist, wählen Sie den Wert der Schlüssel-ID aus. (Authentifizierungsschlüssel werden auf der Seite „SNTP-Authentifizierung“ erstellt.)

SCHRITT 6 Klicken Sie auf **Übernehmen**. Der STNP-Server wird hinzugefügt, und Sie werden zur Hauptseite zurückgeleitet.

Konfigurieren des SNTP-Modus

Das Gerät kann sich im aktiven und/oder passiven Modus befinden (weitere Informationen finden Sie unter **SNTP-Modi**).

So aktivieren Sie den Empfang von SNTP-Paketen von allen Servern im Subnetz und/oder die Übertragung von Zeitanforderungen an SNTP-Server:

SCHRITT 1 Klicken Sie auf **Administration** > **Zeiteinstellungen** > **SNTP-Multicast/-Anycast**.

SCHRITT 2 Wählen Sie unter den folgenden Optionen aus:

- **SNTP IPv4 Multicast Client Mode (Client Broadcast Reception)**: Wählen Sie diese Option, um IPv4-Multicast-Übertragungen für die Systemzeit von einem beliebigen SNTP-Server im Subnetz zu empfangen.

- **SNTP IPv6 Multicast Client Mode (Client Broadcast Reception)**: Wählen Sie diese Option, um IPv6-Multicast-Übertragungen für die Systemzeit von einem beliebigen SNTP-Server im Subnetz zu empfangen.
- **SNTP IPv4 Anycast Client Mode (Client Broadcast Transmission)**: Wählen Sie diese Option, um SNTP-IPv4-Synchronisierungspakete zum Anfordern von Systemzeitinformationen zu übertragen. Die Pakete werden an alle SNTP-Server im Subnetz übertragen.
- **SNTP IPv6 Anycast Client Mode (Client Broadcast Transmission)**: Wählen Sie diese Option, um SNTP-IPv6-Synchronisierungspakete zum Anfordern von Systemzeitinformationen zu übertragen. Die Pakete werden an alle SNTP-Server im Subnetz übertragen.

SCHRITT 3 Wenn sich das System im Schicht-3-Systemmodus befindet, klicken Sie auf **Hinzufügen**, um die Schnittstelle für den SNTP-Empfang bzw. die SNTP-Übertragung anzugeben.

Wählen Sie eine Schnittstelle aus und wählen Sie die Empfangs- bzw. Übertragungsoptionen aus.

SCHRITT 4 Klicken Sie auf **Übernehmen**, um die Einstellungen in der aktuellen Konfigurationsdatei zu speichern.

Festlegen von SNTP-Authentifizierung

SNTP-Clients können Antworten mithilfe von HMAC-MD5 authentifizieren. Ein SNTP-Server wird einem Schlüssel zugeordnet, der zusammen mit der Antwort selbst als Eingabe für die MD5-Funktion verwendet wird. Das MD5-Ergebnis ist ebenfalls im Antwortpaket enthalten.

Auf der Seite „SNTP-Authentifizierung“ können Sie die Authentifizierungsschlüssel konfigurieren, die bei der Kommunikation mit einem SNTP-Server verwendet werden, für den eine Authentifizierung erforderlich ist.

Der Authentifizierungsschlüssel wird auf dem SNTP-Server in einem separaten Vorgang erstellt, der vom Typ des verwendeten SNTP-Servers abhängt. Weitere Informationen hierzu erhalten Sie vom Systemadministrator des SNTP-Servers.

Workflow

SCHRITT 1 Aktivieren Sie die Authentifizierung auf der Seite „SNTP-Authentifizierung“.

SCHRITT 2 Erstellen Sie auf der Seite „SNTP-Authentifizierung“ einen Schlüssel.

SCHRITT 3 Ordnen Sie diesen Schlüssel auf der Seite „SNTP-Unicast“ einem SNTP-Server zu.

So aktivieren Sie SNTP-Authentifizierung und definieren Schlüssel:

SCHRITT 1 Klicken Sie auf **Administration** > **Zeiteinstellungen** > **SNTP-Authentifizierung**.

SCHRITT 2 Wählen Sie **SNTP-Authentifizierung**, um die Authentifizierung einer SNTP-Sitzung zwischen dem Gerät und einem SNTP-Server zu unterstützen.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um das Gerät zu aktualisieren.

SCHRITT 4 Klicken Sie auf **Hinzufügen**.

SCHRITT 5 Geben Sie die folgenden Parameter ein:

- **Authentifizierungsschlüssel-ID**: Geben Sie die Nummer ein, mit der dieser SNTP-Authentifizierungsschlüssel intern identifiziert wird.
- **Authentifizierungsschlüssel**: Geben Sie den Schlüssel ein, der für die Authentifizierung verwendet wird (bis zu acht Zeichen). Der SNTP-Server muss diesen Schlüssel zur Synchronisierung an das Gerät senden.
- **Vertrauensw. Schlüssel**: Wählen Sie diese Option, wenn das Gerät Synchronisierungsinformationen von einem SNTP-Server nur unter Verwendung dieses Authentifizierungsschlüssels empfangen soll.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die SNTP-Authentifizierungsparameter werden in die aktuelle Konfigurationsdatei geschrieben.

Zeitbereich

Zeitbereiche können definiert und den folgenden Befehlstypen zugeordnet werden, damit sie nur im jeweiligen Zeitbereich angewendet werden:

- ACLs
- 802.1X-Portauthentifizierung
- Portstatus
- Zeitbasiertes PoE

Es gibt zwei Arten von Zeitbereichen:

- **Absolut**: Diese Art von Zeitbereich beginnt an einem bestimmten Datum oder sofort und endet an einem bestimmten Datum oder gilt unbegrenzt. Der Zeitbereich wird auf den Seiten unter „Zeitbereich“ erstellt. Sie können ein wiederkehrendes Element hinzufügen.
- **Wiederkehrend**: Diese Art von Zeitbereich enthält ein Zeitbereichselement, das einem absoluten Bereich hinzugefügt wird und wiederkehrend beginnt und endet. Dieser Zeitbereich wird auf den Seiten unter „Wiederkehrender Bereich“ definiert.

Wenn ein Zeitbereich sowohl absolute als auch wiederkehrende Bereiche umfasst, wird der zugeordnete Prozess nur dann aktiviert, wenn sowohl die absolute Startzeit als auch der wiederkehrende Zeitbereich erreicht ist. Der Prozess wird deaktiviert, wenn einer der beiden Zeitbereiche erreicht ist.

Das Gerät unterstützt maximal 10 absolute Zeitbereiche.

Alle Zeitangaben werden als Angaben der Zeit in der lokalen Zeitzone interpretiert (Sommerzeit hat hierauf keinen Einfluss). Um sicherzustellen, dass die Einträge für den Zeitbereich zu den gewünschten Zeiten wirksam werden, müssen Sie die Systemzeit festlegen.

Die Zeitbereichsfunktion kann für folgende Zwecke verwendet werden:

- Beschränkung des Netzwerkzugriffs von Computern beispielsweise auf die Geschäftszeiten. Außerhalb dieses Zeitraums werden die Netzwerkports sowie der Zugriff auf das restliche Netzwerk gesperrt (siehe **Konfigurieren von Ports** und **Konfigurieren von LAG-Einstellungen**).
- Beschränkung des PoE-Betriebs auf einen bestimmten Zeitraum.

Absoluter Zeitbereich

So definieren Sie einen absoluten Zeitbereich:

SCHRITT 1 Klicken Sie auf **Administration** > **Zeiteinstellungen** > **Zeitbereich**.

Die vorhandenen Zeitbereiche werden angezeigt.

SCHRITT 2 Zum Hinzufügen eines neuen Zeitbereichs klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **Zeitbereichsname**: Geben Sie einen Namen für den neuen Zeitbereich ein.
- **Absolute Startzeit**: Definieren Sie die absolute Startzeit, indem Sie Folgendes eingeben:
  - *Sofort*: Wählen Sie diese Option aus, damit der Zeitbereich sofort beginnt.
  - *Datum, Uhrzeit*: Geben Sie Datum und Uhrzeit für den Beginn des Zeitbereichs ein.
- **Absolute Endzeit**: Definieren Sie die absolute Endzeit, indem Sie Folgendes eingeben:
  - *Unbegrenzt*: Wählen Sie diese Option aus, damit der Zeitbereich nie endet.
  - *Datum, Uhrzeit*: Geben Sie Datum und Uhrzeit für das Ende des Zeitbereichs ein.

SCHRITT 4 Zum Hinzufügen eines wiederkehrenden Zeitbereichs klicken Sie auf **Wiederkehrender Bereich**.

Wiederkehrender Zeitbereich

Sie können einem absoluten Zeitbereich ein wiederkehrendes Element hinzufügen. Dadurch begrenzen Sie den Vorgang auf bestimmte Zeiträume innerhalb des absoluten Bereichs.

So fügen Sie einem absoluten Zeitbereich ein wiederkehrendes Zeitbereichselement hinzu:

SCHRITT 1 Klicken Sie auf **Administration** > **Zeiteinstellungen** > **Wiederkehrender Bereich**.

Die vorhandenen wiederkehrenden Zeitbereiche werden angezeigt (nach einem bestimmten absoluten Zeitbereich gefiltert).

SCHRITT 2 Wählen Sie den absoluten Zeitbereich aus, dem Sie den wiederkehrenden Bereich hinzufügen möchten.

SCHRITT 3 Zum Hinzufügen eines neuen wiederkehrenden Zeitbereichs klicken Sie auf **Hinzufügen**.

SCHRITT 4 Geben Sie Werte für die folgenden Felder ein:

- **Wiederkehrende Startzeit**: Geben Sie das Datum und die Uhrzeit für den wiederkehrenden Beginn des Zeitbereichs ein.
- **Wiederkehrende Endzeit**: Geben Sie das Datum und die Uhrzeit für das wiederkehrende Ende des Zeitbereichs ein.

SCHRITT 5 Klicken Sie auf **Übernehmen**.

SCHRITT 6 Klicken Sie auf **Zeitbereich**, um auf Absoluter Zeitbereich zuzugreifen.

9

Administration: Diagnose

In diesem Abschnitt wird beschrieben, wie Sie die Port-Spiegelung konfigurieren, Kabeltests durchführen und die Informationen für den Gerätebetrieb anzeigen.

Die folgenden Themen werden behandelt:

- **Tests für Kupferports**
- **Anzeigen des Status des optischen Moduls**
- **Konfigurieren der Port- und VLAN-Spiegelung**
- **Anzeigen der CPU-Auslastung und Secure Core Technology**

Tests für Kupferports

Auf der Seite *Kupfertest* werden die Ergebnisse der integrierten Kabeltests angezeigt, die von Virtual Cable Tester (VCT) an den Kupferkabeln ausgeführt wurden.

VCT führt zwei Arten von Tests aus:

- Die TDR-Technologie (Time Domain Reflectometry) prüft die Qualität und Eigenschaften eines Kupferkabels, das an einen Port angeschlossen ist. Es können Kabel bis zu einer Länge von 140 Metern getestet werden. Die Ergebnisse werden im Abschnitt Testergebnisse auf der Seite Kupfertest angezeigt.
- DSP-basierte Tests werden an aktiven GE-Verbindungen ausgeführt, um die Kabellänge zu messen. Die Ergebnisse werden im Abschnitt Erweiterte Informationen auf der Seite Kupfertest angezeigt.

Voraussetzungen für die Ausführung des Kupfer-Port-Tests

Führen Sie vor dem Test die folgenden Schritte aus:

- (Obligatorisch) Deaktivieren Sie den Modus für kurze Reichweite (siehe Seite Portverwaltung > Green Ethernet > Eigenschaften).
- (Optional) Deaktivieren Sie EEE (siehe Seite Portverwaltung > Green Ethernet > Eigenschaften).

Verwenden Sie für Kabeltests mit VCT ein Datenkabel der Kategorie 5.

Die Testergebnisse sind bis auf eine Abweichung von +/- 10 für den erweiterten Test und +/- 2 für den Basistest genau.

VORSICHT Wird ein Port getestet, wird er in den inaktiven Status versetzt und die Kommunikation unterbrochen. Nach dem Test wird der Port wieder aktiviert. Es wird davon abgeraten, den Kupfer-Port-Test an einem Port durchzuführen, den Sie verwenden, um das webbasierte Switch-Konfigurationsdienstprogramm auszuführen, da dies die Kommunikation mit diesem Gerät unterbrechen würde.

So testen Sie an Ports angeschlossene Kupferkabel:

SCHRITT 1 Klicken Sie auf **Administration** > **Diagnose** > **Kupfertest**.

SCHRITT 2 Wählen Sie den Port für den Test aus.

SCHRITT 3 Klicken Sie auf **Kupfertest**.

SCHRITT 4 Wenn die Meldung angezeigt wird, klicken Sie auf **OK**, um zu bestätigen, dass die Verbindung getrennt werden kann, oder auf **Abbrechen**, um den Test abzubrechen.

Im Block „Testergebnisse“ werden die folgenden Felder angezeigt:

- **Letzte Aktualisierung**: Zeitpunkt des zuletzt am Port durchgeführten Tests.
- **Testergebnisse**: Die Ergebnisse des Kabeltests. Folgende Werte sind möglich:
  - *OK*: Das Kabel hat den Test bestanden.
  - *Kein Kabel*: Es ist kein Kabel an den Port angeschlossen.
  - *Kabel nur einseitig verbunden*: Das Kabel ist nur an einer Seite angeschlossen.
  - *Kabel mit Kurzschluss*: Im Kabel ist ein Kurzschluss aufgetreten.
  - *Unbekanntes Testergebnis*: Es ist ein Fehler aufgetreten.
- **Abstand zu Fehler**: Es wurde der Abstand vom Port zu der Stelle des Kabels ermittelt, an der der Fehler festgestellt wurde.
- **Operativer Portstatus**: Zeigt an, ob der Port aktiv ist.

Wenn es sich beim getesteten Port um einen Giga-Port handelt, werden im Abschnitt **Erweiterte Informationen** folgende Informationen angezeigt, die bei jedem Aufruf der Seite aktualisiert werden:

- **Kabellänge:** Gibt die geschätzte Länge an.
- **Paar**: Das getestete Kabelpaar.
- **Status**: Status des Kabelpaars. Rot zeigt einen Fehler an, Grün zeigt an, dass der Status OK ist.
- **Kanal**: Der Kabelkanal gibt an, ob es sich um gekreuzte oder ungekreuzte Kabel handelt.
- **Polarität**: Gibt an, ob die automatische Polaritätserkennung und -korrektur für das Kabelpaar aktiviert wurde.
- **Paarversatz**: Verzögerungsdifferenz zwischen beiden Kabelpaaren.

HINWEIS Bei einer Portgeschwindigkeit von 10 MBit/s können die TDR-Tests nicht ausgeführt werden.

Anzeigen des Status des optischen Moduls

Auf der Seite Status des optischen Moduls werden die Betriebsbedingungen angezeigt, die vom SFP-Transceiver (Small FormFactor Pluggable) gemeldet werden. Einige Informationen sind möglicherweise für SFPs nicht verfügbar, die den digitalen Diagnose-Überwachungsstandard SFF-8472 nicht unterstützen.

MSA-kompatible SFPs

Die folgenden FE SFP-Transceiver (100 MBit/s) werden unterstützt:

- MFEBX1: 100BASE-BX-20U SFP-Transceiver für Einzelmodus-Leiter, 1310 nm Wellenlänge, Unterstützung bis 20 km.
- MFEFX1: 100BASE-FX SFP-Transceiver für Multimodus-Leiter, 1310 nm Wellenlänge, Unterstützung bis 2 km.
- MFELX1: 100BASE-LX SFP-Transceiver für Einzelmodus-Leiter, 1310 nm Wellenlänge, Unterstützung bis 10 km.

Die folgenden GE SFP-Transceiver (1000 Mbps) werden unterstützt:

- MGBBX1: 1000BASE-BX-20U SFP-Transceiver für Einzelmodus-Leiter, 1310 nm Wellenlänge, Unterstützung bis 40 km.
- MGBLH1: 1000BASE-LH SFP-Transceiver für Einzelmodus-Leiter, 1310 nm Wellenlänge, Unterstützung bis 40 km.

- MGBLX1: 1000BASE-LX SFP-Transceiver für Einzelmodus-Leiter, 1310 nm Wellenlänge, Unterstützung bis 10 km.
- MGBSX1: 1000BASE-SX SFP-Transceiver für Multimodus-Leiter, 850 nm Wellenlänge, Unterstützung bis 550 m.
- MGBT1: 1000BASE-T SFP-Transceiver für Kupferkabel der Kategorie 5, Unterstützung bis 100 m.

Zum Anzeigen der Ergebnisse optischer Tests klicken Sie auf **Administration** > **Diagnose** > **Status des optischen Moduls**.

Auf dieser Seite werden folgende Felder angezeigt:

- **Port**: Nummer des Ports, an den der SFP angeschlossen ist.
- **Beschreibung**: Die Beschreibung für den optischen Transceiver.
- **Seriennummer**: Die Seriennummer des optischen Transceiver.
- **PID**: Die VLAN-ID.
- **VID**: Die ID des optischen Transceiver.
- **Temperatur**: Betriebstemperatur (Celsius) des SFP.
- **Spannung**: Die Betriebsspannung des SFP.
- **Aktuell**: Der aktuelle Stromverbrauch des SFP.
- **Ausgangsleistung**: Die übertragene optische Leistung.
- **Eingangsleistung**: Die empfangene optische Leistung.
- **Transmitter-Fehler**: Der Remote-SFP meldet einen Signalverlust. Mögliche Werte sind Wahr, Falsch und Kein Signal.
- **Signalverlust**: Der lokale SFP meldet einen Signalverlust. Mögliche Werte sind Wahr und Falsch.
- **Daten bereit**: Der SFP ist betriebsbereit. Mögliche Werte sind Wahr und Falsch.

Konfigurieren der Port- und VLAN-Spiegelung

Die Port-Spiegelung wird bei Netzwerkgeräten verwendet, um eine Kopie der Netzwerkpakete an einem einzelnen Geräteport, an mehreren Geräteports oder in einem gesamten VLAN an eine Netzwerk-Überwachungsverbindung oder einen anderen Port am Gerät zu senden. Diese Funktion wird normalerweise für Netzwerkgeräte verwendet, bei denen eine Überwachung des Netzwerkverkehrs erforderlich ist, beispielsweise für ein Intrusion Detection System. Ein an den Überwachungsport angeschlossenes Netzwerk-Analysegerät verarbeitet die Datenpakete für die Diagnose, Fehlerbehebung und Leistungsüberwachung.

Es können bis zu acht Quellen gespiegelt werden. Es kann jede beliebige Kombination von acht einzelnen Ports und/oder VLANs verwendet werden.

Wird an einem Netzwerk-Port ein Paket empfangen, das einem VLAN mit aktivierter Spiegelung zugewiesen ist, wird das Paket auch dann an den Analyse-Port gespiegelt, wenn das Paket empfangen oder verworfen wurde. Vom Gerät gesendete Pakete werden gespiegelt, wenn die Funktion Transmit (Tx) Mirroring aktiviert ist.

Das Spiegeln garantiert nicht, dass der gesamte Verkehr von den Quell-Ports am Analyse-Port (Ziel-Port) empfangen wird. Werden mehr Daten an den Analyse-Port gesendet, als dieser unterstützt, können Daten verloren gehen.

Die VLAN-Spiegelung ist nur in manuell erstellten VLANs aktiv. Wenn beispielsweise VLAN 23 von GVRP erstellt wurde und Sie VLAN 34 manuell erstellt haben und eine Port-Spiegelung erstellen, die VLAN 23 und/oder VLAN 34 einschließt, und dann später VLAN 34 löschen, wird der Status in der Port-Spiegelung auf **Nicht bereit** festgelegt, da VLAN 34 nicht mehr in der Datenbank vorhanden ist und VLAN 23 nicht manuell erstellt wurde.

Systemweit wird nur eine Instanz der Spiegelung unterstützt. Der Analyse-Port (oder Ziel-Port für die VLAN- oder Port-Spiegelung) ist für alle gespiegelten VLANs und Ports gleich.

So aktivieren Sie die Spiegelung:

SCHRITT 1 Wählen Sie **Administration** > **Diagnose** > **Port- und VLAN-Spiegelung**.

Die folgenden Felder werden angezeigt:

- **Ziel-Port**: Port, an den der Verkehr kopiert wird. Dies ist der Analyse-Port.
- **Quellschnittstelle**: Schnittstelle, Port oder VLAN, von der bzw. dem Verkehr an den Analyse-Port gesendet wird.
- **Typ**: Überwachungstyp: Empfangener Verkehr (Rx), gesendeter Verkehr (Tx) oder beides.

- **Status**: Zeigt einen der folgenden Werte an:
  - *Aktiv*: Quell- und Zielschnittstelle sind aktiv und leiten Verkehr weiter.
  - *Nicht bereit*: Quelle und/oder Ziel ist inaktiv oder leitet aus irgendeinem Grund keinen Verkehr weiter.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, um einen zu spiegelnden Port oder ein zu spiegelndes VLAN hinzuzufügen.

SCHRITT 3 Geben Sie die Parameter ein:

- **Ziel-Port**: Wählen Sie den Analyse-Port, an den Pakete kopiert werden. An diesen Port ist ein Netzwerk-Analysegerät angeschlossen, beispielsweise ein PC, auf dem Wireshark ausgeführt wird. Ein als Analyse-Ziel-Port identifizierter Port wird als solcher verwendet, bis alle Einträge entfernt werden.
- **Quellschnittstelle**: Wählen Sie den Quell-Port oder das Quell-VLAN für die Spiegelung des Verkehrs aus.
- **Typ**: Legen Sie fest, ob der ankommende, der ausgehende Verkehr oder beide Verkehrstypen an den Analyse-Port gespiegelt werden soll bzw. sollen. Wird **Port** gewählt, stehen folgende Optionen zur Verfügung:
  - *Nur Rx*: Port-Spiegelung für empfangene Pakete.
  - *Nur Tx*: Port-Spiegelung für gesendete Pakete.
  - *Tx und Rx*: Port-Spiegelung für empfangene und gesendete Pakete.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Port-Spiegelung wird der aktuellen Konfiguration hinzugefügt.

Anzeigen der CPU-Auslastung und Secure Core Technology

Das Gerät verarbeitet neben dem Datenverkehr für Endbenutzer folgende Arten von Datenverkehr:

- Verwaltungsverkehr
- Protokollverkehr
- Snooping-Verkehr

Zu starker Datenverkehr belastet die Prozessorleistung und kann den normalen Gerätebetrieb beeinträchtigen. Das Gerät stellt mithilfe der SCT-Funktion (Secure Core Technology) sicher, dass Verwaltungs- und Protokollverkehr unabhängig vom insgesamt eingehenden Datenverkehr empfangen und verarbeitet wird. SCT ist im Gerät standardmäßig aktiviert und kann nicht deaktiviert werden.

Es gibt keine Interaktionen mit anderen Funktionen.

So zeigen Sie die CPU-Auslastung an:

SCHRITT 1 Klicken Sie auf **Administration > Diagnose > CPU-Auslastung**.

Die Seite CPU-Auslastung wird geöffnet.

Im Feld CPU-Eingangsgeschwindigkeit wird die Anzahl der pro Sekunde bei der CPU eingehenden Frames angezeigt.

Im Fenster wird ein Diagramm der CPU-Auslastung angezeigt. Die Y-Achse bildet den Prozentsatz der Auslastung ab, die X-Achse ist die Zahl der Stichproben.

SCHRITT 2 Vergewissern Sie sich, dass das Kontrollkästchen **CPU-Auslastung** aktiviert ist.

SCHRITT 3 Legen Sie die **Aktualisierungsrate** (Zeitraum in Sekunden) fest, die bis zum Aktualisieren der Statistiken verstreichen soll. Für jeden Zeitraum wird ein neues Abbild erstellt.

SCHRITT 4 Klicken Sie auf **Übernehmen**.

10

Administration: Erkennung

Dieser Abschnitt enthält Informationen zum Konfigurieren von Discovery.

Die folgenden Themen werden behandelt:

- **Bonjour**
- **LLDP und CDP**
- **Konfigurieren von LLDP**
- **Konfigurieren von CDP**

Bonjour

Als Bonjour-Client führt das Gerät regelmäßig einen Broadcast von Bonjour Discovery-Protokollpaketen an direkt verbundene IP-Subnetze durch und weist damit auf sein Vorhandensein und die von ihm angebotenen Services (beispielsweise HTTP, HTTPS und Telnet) hin. (Auf der Seite „Sicherheit > TCP/UDP-Services“ können Sie die Services aktivieren oder deaktivieren.) Das Gerät kann von einem Netzwerkverwaltungssystem oder von anderen Anwendungen von Drittanbietern erkannt werden. Bonjour ist für das Verwaltungs-VLAN standardmäßig aktiviert. Geräte werden von der Bonjour-Konsole automatisch erkannt und angezeigt.

Bonjour im Schicht-2-Systemmodus

Wenn sich das Gerät im Schicht-2-Systemmodus befindet, ist Bonjour Discovery global aktiviert. Die Funktion kann nicht für einzelne Ports oder VLANs deaktiviert werden. Das Gerät kündigt alle Services an, die vom Administrator basierend auf der Konfiguration auf der Seite „Services“ aktiviert wurden.

Wenn Bonjour Discovery und IGMP gleichzeitig aktiviert sind, wird die IP-Multicast-Adresse von Bonjour auf der Seite „Hinzufügen von IP-Multicast-Gruppenadressen“ angezeigt.

Wenn Bonjour Discovery aktiviert ist, stoppt das Gerät sämtliche Servicetyp-Ankündigungen und antwortet auf keinerlei Serviceanforderungen von Netzwerkverwaltungsanwendungen.

So aktivieren Sie Bonjour global, wenn sich das System im Schicht-2-Systemmodus befindet:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – Bonjour**.

SCHRITT 2 Wählen Sie **Aktivieren** aus, um Bonjour **Discovery** auf dem Gerät global zu aktivieren.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Bonjour wird für das Gerät entsprechend der Auswahl aktiviert oder deaktiviert.

Bonjour im Schicht-3-Systemmodus

Im Schicht-3-Systemmodus können Sie jeder Schnittstelle (VLAN, Port oder LAG) eine IP-Adresse zuweisen. Wenn Bonjour aktiviert ist, kann das Gerät Bonjour Discovery-Pakete an alle Schnittstellen mit IP-Adresse versenden. Sie können Bonjour einzelnen Ports und/oder VLANs zuweisen. Wenn Bonjour aktiviert ist, kann das Gerät Bonjour Discovery-Pakete an Schnittstellen senden, deren IP-Adressen Bonjour in der Tabelle für Bonjour-Discovery-Schnittstellensteuerung zugeordnet sind. Wenn das Gerät im Schicht-3-Systemmodus betrieben wird, gehen Sie zu **IP-Konfiguration** > **Verwaltungs- und IP-Schnittstelle** > **IPv4-Schnittstelle**, um eine IP-Adresse für eine Schnittstelle zu konfigurieren.

Wenn eine Schnittstelle gelöscht wird (z. B. ein VLAN), werden Goodbye-Pakete gesendet, um die Registrierung der vom Gerät angekündigten Services in der benachbarten Cache-Tabelle im lokalen Netzwerk rückgängig zu machen. Die Tabelle für Bonjour-Discovery-Schnittstellensteuerung enthält Schnittstellen mit IP-Adressen, die der Bonjour-Funktion zugeordnet sind. Bonjour-Ankündigungen können nur an die in dieser Tabelle aufgeführten Schnittstellen gesendet werden. Informationen hierzu finden Sie in der Tabelle für Bonjour Discovery-Schnittstellensteuerung auf der Seite „Administration > Discovery – Bonjour“. Wenn die verfügbaren Services geändert werden, werden diese Änderungen angekündigt. Dabei wird die Registrierung von Services, die ausgeschaltet werden, aufgehoben, und Services, die eingeschaltet werden, werden registriert. Wird eine IP-Adresse geändert, wird diese Änderung angekündigt.

Wenn Bonjour deaktiviert ist, sendet das Gerät keine Bonjour Discovery-Ankündigungen und hört andere Geräte auch nicht auf gesendete Bonjour Discovery-Ankündigungen ab.

So konfigurieren Sie Bonjour, wenn sich das Gerät im Schicht-3-Systemmodus befindet:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – Bonjour**.

SCHRITT 2 Wählen Sie die Option **Aktivieren** aus, um Bonjour **Discovery** global zu aktivieren.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um die aktuelle Konfigurationsdatei zu aktualisieren.

Die Tabelle für die Bonjour-Discovery-Schnittstellensteuerung zeigt den **Schnittstellennamen** der Schnittstellen an, für die Bonjour aktiviert ist, sowie deren **IP-Adresse**.

SCHRITT 4 Zum Aktivieren von Bonjour für eine Schnittstelle klicken Sie auf **Hinzufügen.**

SCHRITT 5 Wählen Sie die Schnittstelle aus und klicken Sie auf **Übernehmen**.

HINWEIS Klicken Sie auf **Löschen**, um Bonjour für eine Schnittstelle zu deaktivieren (dabei wird der Löschvorgang ohne zusätzlichen Befehl wie beispielsweise „Übernehmen“ ausgeführt).

LLDP und CDP

LLDP (Link Layer Discovery Protocol) und CDP (Cisco Discovery Protocol) sind Verbindungsschichtprotokolle, mit denen direkt verbundene LLDP- und CDP-fähige Nachbarn sich selbst und ihre Funktionen ankündigen. Das Gerät sendet standardmäßig regelmäßig eine LLDP/CDP-Ankündigung an alle Schnittstellen und verarbeitet eingehende LLDP- und CDP-Pakete gemäß den Anforderungen der Protokolle. In LLDP und CDP werden Ankündigungen als TLV (Type, Length, Value, Typ, Länge, Wert) im Paket codiert.

Anmerkungen zur CDP/LLDP-Konfiguration:

- CDP/LLDP kann global oder pro Port aktiviert oder deaktiviert werden. Die CDP/LLDP-Funktion eines Ports ist nur relevant, wenn CDP/LLDP global aktiviert ist.
- Wenn CDP/LLDP global aktiviert ist, filtert das Gerät eingehende CDP/LLDP-Pakete von Ports, für die CDP/LLDP deaktiviert ist.
- Wenn CDP/LLDP global deaktiviert ist, kann das Gerät so konfiguriert werden, dass alle eingehenden CDP/LLDP-Pakete mit VLAN-fähigem Überlauf oder nicht VLAN-fähigem Überlauf verworfen werden. Beim VLAN-fähigen Überlauf wird ein eingehendes CDP/LLDP-Paket an das VLAN geflutet, in dem das Paket empfangen wird (mit Ausnahme des Eingangsports). Beim nicht VLAN-fähigen Überlauf wird ein eingehendes CDP/LLDP-Paket an alle Ports mit Ausnahme des Eingangsports geflutet. Standardmäßig werden CDP/LLDP-Pakete verworfen, wenn CDP/LLDP global deaktiviert ist. Sie können das Verwerfen bzw. Fluten von eingehenden CDP- und LLDP-Paketen auf der Seite „CDP-Eigenschaften“ bzw. „LLDP-Eigenschaften“ konfigurieren.
- Für Auto-Smartport muss CDP und/oder LLDP aktiviert sein. Mit Auto-Smartport wird eine Schnittstelle automatisch basierend auf der von der Schnittstelle empfangenen CDP/LLDP-Ankündigung konfiguriert.
- CDP- und LLDP-Endgeräte (beispielsweise IP-Telefone) lernen die Voice-VLAN-Konfiguration anhand von CDP- und LLDP-Ankündigungen. Standardmäßig ist das Senden von CDP- und LLDP-Ankündigungen, die auf dem im Gerät konfigurierten Voice-VLAN basieren, im Gerät aktiviert. Weitere Informationen finden Sie unter **Voice-VLAN**.

HINWEIS Bei CDP/LLDP wird nicht unterschieden, ob der Port zu einer LAG gehört oder nicht. Wenn sich mehrere Ports in einer LAG befinden, sendet CDP/LLDP Pakete an die einzelnen Ports, ohne die Tatsache zu berücksichtigen, dass die Ports zu einer LAG gehören.

Die Verwendung von CDP/LLDP ist unabhängig vom STP-Status einer Schnittstelle.

Wenn die 802.1X-Portzugriffssteuerung an einer Schnittstelle aktiviert ist, sendet und empfängt das Gerät nur dann CDP/LLDP-Pakete über die Schnittstelle, wenn diese authentifiziert und autorisiert ist.

Wenn ein Port Ziel einer Spiegelung ist, sieht CDP/LLDP ihn als deaktiviert an.

HINWEIS CDP und LLDP sind Verbindungsschichtprotokolle, mit denen direkt verbundene CDP/LLDP-fähige Geräte sich selbst und ihre Funktionen ankündigen. In Bereitstellungen, in denen die CDP/LLDP-fähigen Geräte nicht direkt verbunden sind und durch nicht CDP/LLDP-fähige Geräte voneinander getrennt sind, können die CDP/LLDP-fähigen Geräte möglicherweise die Ankündigung von anderen Geräten nur dann empfangen, wenn die nicht CDP/LLDP-fähigen Geräte die empfangenen CDP/LLDP-Pakete fluten. Wenn die nicht CDP/LLDP-fähigen Geräte einen VLAN-fähigen Überlauf ausführen, können die CDP/LLDP-fähigen Geräte einander nur dann hören, wenn sie sich im gleichen VLAN befinden. Ein CDP/LLDP-fähiges Gerät kann Ankündigungen von mehreren Geräten empfangen, wenn die nicht CDP/LLDP-fähigen Geräte die CDP/LLDP-Pakete fluten.

Konfigurieren von LLDP

In diesem Abschnitt wird beschrieben, wie Sie LLDP konfigurieren. Die folgenden Themen werden behandelt:

- **LLDP-Übersicht**
- **LLDP-Eigenschaften**
- **LLDP-Port-Einstellungen**
- **LLDP MED-Netzwerkrichtlinien**
- **LLDP MED-Porteinstellungen**
- **LLDP-Portstatus**
- **LLDP-Local-Informationen**
- **LLDP-Nachbarinformationen**
- **LLDP-Statistik**
- **LLDP-Überlastung**

LLDP-Übersicht

Das LLDP-Protokoll ermöglicht Netzwerkmanagern die Fehlerbehebung und die Verbesserung der Netzwerkverwaltung in Umgebungen, in denen mehrere Anbieter vertreten sind. LLDP standardisiert Methoden für die Ankündigung von Netzwerkgeräten gegenüber anderen Systemen und zum Speichern der erkannten Informationen.

Durch LLDP wird es einem Gerät ermöglicht, seine Identifikation, Konfiguration und Funktionen Nachbargeräten gegenüber anzukündigen. Diese speichern die Daten daraufhin in einer Management Information Base (MIB). Das Netzwerkverwaltungssystem modelliert die Topologie des Netzwerks durch Abfragen dieser MIB-Datenbanken.

LLDP ist ein Verbindungsschichtprotokoll. Standardmäßig beendet und verarbeitet das Gerät alle eingehenden LLDP-Pakete gemäß den Anforderungen des Protokolls.

Es gibt für das LLDP-Protokoll eine Erweiterung, LLDP MED (LLDP Media Endpoint Discovery), die Informationen von Medien-Endpunktgeräten wie beispielsweise VoIP-Telefonen und Videotelefonen bereitstellt und akzeptiert. Weitere Informationen zu LLDP-MED finden Sie unter **LLDP MED-Netzwerkrichtlinien**.

LLDP-Konfigurations-Workflow

Im Folgenden finden Sie Beispiele und eine vorgeschlagene Reihenfolge für Aktionen, die Sie mit der LLDP-Funktion ausführen können. Weitere Anleitungen für die LLDP-Konfiguration finden Sie im Abschnitt „LLDP/CDP“. Die LLDP-Konfigurationsseiten können Sie über das Menü **Administration > Discovery – LLDP** aufrufen.

1. Geben Sie auf der Seite „LLDP-Eigenschaften“ globale LLDP-Parameter wie beispielsweise das Zeitintervall für das Senden von LLDP-Updates ein.
2. Konfigurieren Sie LLDP pro Port auf der Seite „Porteinstellungen“. Auf dieser Seite können Sie Schnittstellen für das Senden bzw. Empfangen von LLDP-PDUs, das Senden von SNMP-Benachrichtigungen, die anzukündigenden TLVs und das Ankündigen der Verwaltungsadresse des Geräts konfigurieren.
3. Erstellen Sie auf der Seite „LLDP-MED-Netzwerkrichtlinien“ LLDP-MED-Netzwerkrichtlinien.
4. Ordnen Sie auf der Seite „LLDP-MED-Porteinstellungen“ LLDP-MED-Netzwerkrichtlinien und die optionalen LLDP-MED-TLVs den gewünschten Schnittstellen zu.
5. Wenn die Funktionen von LLDP-Geräten mit Auto-Smartport erkannt werden sollen, aktivieren Sie LLDP auf der Seite „Smartport-Eigenschaften“.
6. Zeigen Sie auf der Seite „LLDP-Überlastung“ Informationen zur Überlastung an.

LLDP-Eigenschaften

Auf der Seite „Eigenschaften“ können Sie allgemeine LLDP-Parameter eingeben. Beispielsweise können Sie die Funktion global aktivieren oder deaktivieren und Timer festlegen.

So geben Sie LLDP-Eigenschaften ein:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – LLDP** > **Eigenschaften**.

SCHRITT 2 Geben Sie die Parameter ein.

- **LLDP-Status**: Wählen Sie diese Option aus, um LLDP für das Gerät zu aktivieren (standardmäßig aktiviert).
- **Bearbeitung von LLDP-Frames**: Wenn LLDP nicht aktiviert ist, wählen Sie die Aktion aus, die bei Empfang eines Pakets ausgeführt werden soll, das den ausgewählten Kriterien entspricht:
  - *Filterung*: Das Paket wird gelöscht.
  - *Überlauf*: Das Paket wird an alle VLAN-Mitglieder weitergeleitet.
- **TLV-Bekanntgabeintervall**: Geben Sie das Zeitintervall in Sekunden ein, nach dem jeweils Updates von LLDP-Ankündigungen gesendet werden sollen, oder verwenden Sie die Standardeinstellung.
- **Intervall für SNMP-Benachrichtigungen über Topologieänderungen**: Geben Sie den Mindestzeitraum zwischen zwei SNMP-Benachrichtigungen ein.
- **Multiplikator für Halten**: Geben Sie die Zeitspanne, die LLDP-Pakete vor dem Verwerfen beibehalten werden, in Vielfachen des TLV-Ankündigungsintervalls ein. Wenn beispielsweise das TLV-Ankündigungsintervall 30 Sekunden beträgt und der Multiplikator für das Halten gleich 4 ist, werden LLDP-Pakete nach 120 Sekunden verworfen.
- **Neuinitialisierungsverzögerung**: Geben Sie die Zeitspanne in Sekunden ein, die zwischen Deaktivierung und Neuinitialisierung von LLDP nach einem LLDP-Deaktivierungs-/Neuinitialisierungszyklus verstreichen soll.
- **Übertragungsverzögerung**: Geben Sie die Zeitspanne in Sekunden ein, die zwischen aufeinanderfolgenden Übertragungen von LLDP-Frames aufgrund von Änderungen in der lokalen System-MIB verstreichen soll.
- **Geräte-ID-Ankündigung**: Wählen Sie eine der folgenden Optionen für die Ankündigung in den LLDP-Nachrichten aus:
  - *MAC-Adresse*: Kündigen Sie die MAC-Adresse des Geräts an.
  - *Hostname*: Kündigen Sie den Hostnamen dieses Geräts an.

SCHRITT 3 Geben Sie im Feld **Schnellstart-Wiederholungsanzahl** ein, wie oft LLDP-Pakete gesendet werden sollen, wenn der LLDP-MED-Schnellstartmechanismus initialisiert wird. Dies kommt dann vor, wenn sich ein neues Endpunktgerät mit dem Gerät verbindet. Eine Beschreibung von LLDP-MED finden Sie im Abschnitt „LLDP-MED-Netzwerkrichtlinien“.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die LLDP-Eigenschaften werden der aktuellen Konfigurationsdatei hinzugefügt.

LLDP-Port-Einstellungen

Auf der Seite „Porteinstellungen“ können Sie LLDP- und SNMP-Benachrichtigungen für einzelne Ports aktivieren und die in LLDP-PDUs gesendeten TLVs eingeben.

Die LLDP-MED-TLVs, die angekündigt werden sollen, können Sie auf der Seite „LLDP-MED-Porteinstellungen“ auswählen. Ebenso können Sie den TLV für die Verwaltungsadresse des Geräts konfigurieren.

So definieren Sie die LLDP-Porteinstellungen:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – LLDP** > **Porteinstellungen**.

Diese Seite enthält die LLDP-Informationen für den Port.

SCHRITT 2 Wählen Sie einen Port aus, und klicken Sie auf **Bearbeiten**.

Auf dieser Seite sind die folgenden Felder verfügbar:

- **Schnittstelle**: Wählen Sie den zu bearbeitenden Port aus.
- **Administrationsstatus**: Wählen Sie die LLDP-Veröffentlichungsoption für den Port aus. Folgende Werte sind möglich:
  - *Nur Tx*: Nur Veröffentlichung, keine Erkennung.
  - *Nur Rx*: Nur Erkennung, keine Veröffentlichung.
  - *Tx und Rx*: Erkennung und Veröffentlichung.
  - *Deaktiviert*: LLDP ist für den Port deaktiviert.
- **SNMP-Benachrichtigung**: Wählen Sie **Aktivieren** aus, um Benachrichtigungen über eine Topologieänderung an SNMP-Benachrichtigungsempfänger wie beispielsweise ein SNMP-Verwaltungssystem zu senden.

Geben Sie das Zeitintervall zwischen Benachrichtigungen in das Feld „Intervall für SNMP-Benachrichtigung über Topologieänderung“ auf der Seite „LLDP-Eigenschaften“ ein. Definieren Sie SNMP-Benachrichtigungsempfänger auf der Seite SNMP > Benachrichtigungsempfänger V1.2 und/oder SNMP > Benachrichtigungsempfänger V3.

- **Ausgewählte optionale TLVs**: Wählen Sie die Informationen, die vom Gerät veröffentlicht werden sollen, indem Sie das TLV in die Liste **Verfügbare optionale TLVs** verschieben. Die verfügbaren TLVs enthalten die folgenden Informationen:
  - *Portbeschreibung*: Informationen zum Port, einschließlich Hersteller, Produktname und Hardware- bzw. Software-Version.
  - *Systemname*: Name, der dem System zugewiesen ist (in alphanumerischem Format). Der Wert ist gleich dem sysName-Objekt.
  - *Systembeschreibung*: Beschreibung der Netzwerk-Entität (in alphanumerischem Format). Dies schließt den Systemnamen und die Versionen der Hardware, des Betriebssystems und der vom Gerät unterstützten Software ein. Der Wert ist gleich dem sysDescr-Objekt.
  - *Systemfunktionen*: Primäre Funktionen des Geräts und Informationen dazu, ob diese Funktionen aktiviert sind. Die Funktionen werden durch zwei Oktette angegeben. Die Bits 0 bis 7 kennzeichnen Sonstige, Repeater, Bridge, WLAN-AP, Router, Telefon, DOCSIS-Kabelgerät bzw. Station. Die Bits 8 bis 15 sind reserviert.
  - *802.3 MAC-PHY*: Duplex- und Bit-Ratenkapazität sowie die aktuellen Duplex- und Bit-Rateneinstellungen des sendenden Geräts. Außerdem wird angegeben, ob die aktuellen Einstellungen auf automatische Aushandlung oder manuelle Konfigurierung zurückgehen.
  - *802.3-Link-Aggregation*: Gibt an, ob der Link (der mit dem Port, über den die LLDP-PDU übertragen wird, verknüpft ist) aggregiert werden kann. Gibt außerdem an, ob der Link aktuell aggregiert ist, und, falls ja, die Kennung des aggregierten Ports.
  - *Maximale 802.3-Frame-Größe*: Maximale Frame-Größenkapazität der MAC-/PHY-Implementierung.

Optionaler TLV für Verwaltungsadresse

- **Ankündigungsmodus**: Wählen Sie eine der folgenden Arten, um die IP-Verwaltungsadresse des Geräts anzukündigen:
  - *Automatische Ankündigung*: Gibt an, dass die Software automatisch eine Verwaltungsadresse auswählt, die von allen IP-Adressen des Geräts angekündigt wird. Wenn mehrere IP-Adressen vorhanden sind, wählt die Software die niedrigste der dynamischen IP-Adressen aus. Wenn keine dynamischen Adressen vorhanden sind, wählt die Software die niedrigste statische IP-Adresse aus.
  - *Ohne*: Die IP-Verwaltungsadresse wird nicht angekündigt.

  - *Manuelle Ankündigung*: Wählen Sie diese Option und die anzukündigende IP-Verwaltungsadresse. Es wird empfohlen, diese Option auszuwählen, wenn sich das Gerät im Schicht-3-Systemmodus befindet und mit mehreren IP-Adressen konfiguriert ist (dies ist bei SG500X/ESW2-550X-Geräten immer der Fall).

- **IP-Adresse**: Wenn die manuelle Ankündigung ausgewählt wurde, wählen Sie die IP-Verwaltungsadresse unter den verfügbaren Adressen aus.

Die folgenden Felder beziehen sich auf das **802.1-VLAN und Protokoll**:

- **PVID**: Wählen Sie diese Option aus, um die PVID über TLV anzukündigen.
- **Port- und Protokoll-VLAN-ID**: Wählen Sie diese Option aus, um die Port- und Protokoll-VLAN-ID anzukündigen. Diese sind auf der Seite **Protokollbasierte VLANs** definiert.
- **VLAN-ID**: Wählen Sie die VLANs aus, die angekündigt werden.
- **Protokoll-IDs**: Wählen Sie die Protokolle aus, die angekündigt werden.
- Ausgewählte Protokoll-IDs: Zeigt ausgewählte Protokolle an.

SCHRITT 3 Geben Sie die relevanten Informationen ein, und klicken Sie auf **Übernehmen**. Die Porteinstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

LLDP MED-Netzwerkrichtlinien

LLDP Media Endpoint Discovery (LLDP MED) ist eine Erweiterung von LLDP, die zusätzliche Funktionen zur Unterstützung von Medien-Endpunktgeräten bietet.

- Ermöglicht die Ankündigung und Erkennung von Netzwerkrichtlinien für Echtzeitanwendungen wie beispielsweise Sprache und/oder Video.
- Bietet die Erkennung des Standorts von Geräten und erlaubt so die Erstellung von Standortdatenbanken, und, im Fall von Voice over Internet Protocol (VoIP), einen Notrufservice unter Verwendung von IP-Telefonstandortinformationen.
- Informationen für die Fehlerbehebung. LLDP MED sendet in folgenden Fällen Alarme an Netzwerkmanager:
  - Port-Geschwindigkeit und Duplexmoduskonflikte
  - Fehlkonfiguration von QoS-Richtlinien

Einrichten der LLDP MED-Netzwerkrichtlinie

Eine LLDP MED-Netzwerkrichtlinie ist ein Satz verwandter Konfigurationseinstellungen für eine bestimmte Echtzeitanwendung wie beispielsweise Sprache oder Video. Wenn eine Netzwerkrichtlinie konfiguriert ist, kann diese in die ausgehenden LLDP-Pakete an das angeschlossene LLDP-Medienendpunktgerät eingeschlossen werden. Das Medienendpunktgerät muss seinen Verkehr gemäß den Vorgaben in der empfangenen Richtlinie senden. Beispielsweise kann eine Richtlinie für VoIP-Verkehr erstellt werden, die folgende Anweisungen für VoIP-Telefone enthält:

- Sprachdaten über VLAN 10 als Paket mit Tag und mit 802.1p-Priorität 5 senden.
- Sprachverkehr mit DSCP 46 senden.

Netzwerkrichtlinien werden auf der Seite „LLDP-MED-Porteinstellungen“ Ports zugeordnet. Ein Administrator kann manuell eine oder mehrere Netzwerkrichtlinien konfigurieren sowie die Schnittstellen, an die die Richtlinien gesendet werden sollen. Es ist Aufgabe des Administrators, die VLANs und ihre Portmitgliedschaften gemäß den Netzwerkrichtlinien und den zugeordneten Schnittstellen manuell zu erstellen.

Außerdem kann ein Administrator das Gerät anweisen, automatisch eine Netzwerkrichtlinie für Sprachanwendungen zu generieren und anzukündigen, die auf dem vom Gerät verwalteten Voice-VLAN basiert. Im Abschnitt „Auto-Voice-VLAN“ finden Sie Details zur Verwaltung des Voice-VLANs auf dem Gerät.

So definieren Sie eine LLDP-MED-Netzwerkrichtlinie:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – LLDP** > **LLDP-MED-Netzwerkrichtlinien**.

Diese Seite enthält die zuvor erstellten Netzwerkrichtlinien.

SCHRITT 2 Wählen Sie für LLDP-MED-Netzwerkrichtlinien für Sprachanwendungen die Option **Autom.** aus, wenn das Gerät automatisch eine Netzwerkrichtlinie für Sprachanwendungen basierend auf dem von ihm verwalteten Voice-VLAN generieren und ankündigen soll.

HINWEIS Wenn dieses Kontrollkästchen aktiviert ist, können Sie nicht manuell Richtlinien für Sprachnetzwerke konfigurieren.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um diese Einstellung der aktuellen Konfigurationsdatei hinzuzufügen.

SCHRITT 4 Klicken Sie zum Definieren einer neuen Richtlinie auf **Hinzufügen**.

SCHRITT 5 Geben Sie die Werte ein:

- **Netzwerkrichtliniennummer**: Wählen Sie die Nummer der zu erstellenden Richtlinie aus.
- **Anwendung**: Wählen Sie in der Liste den Anwendungstyp (Verkehrstyp) aus, für den die Netzwerkrichtlinie definiert werden soll.

- **VLAN-ID**: Geben Sie die ID des VLANs ein, an das der Datenverkehr gesendet werden soll.
- **VLAN-Typ**: Wählen Sie aus, ob der Datenverkehr mit oder ohne Tag erfolgen soll.
- **Benutzerpriorität**: Wählen Sie die Priorität, die von dieser Netzwerkrichtlinie auf den Datenverkehr angewendet werden soll. Dies ist der CoS-Wert.
- **DSCP-Wert**: Wählen Sie den DSCP-Wert, der mit den von Nachbarn gesendeten Anwendungsdaten verknüpft werden soll. Dieser Wert gibt an, wie der an das Gerät gesendete Anwendungsverkehr zu markieren ist.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die Netzwerkrichtlinie wird definiert.

HINWEIS Sie müssen über die LLDP MED-Porteinstellungen die Schnittstellen manuell so konfigurieren, dass diese die gewünschten manuell definierten Netzwerkrichtlinien für die ausgehenden LLDP-Pakete enthalten.

LLDP MED-Porteinstellungen

Auf der Seite *LLDP-MED-Porteinstellungen* können Sie die LLDP-MED-TLVs und/oder die Netzwerkrichtlinien auswählen, die in der ausgehenden LLDP-Ankündigung für die gewünschten Schnittstellen enthalten sein sollen. Netzwerkrichtlinien werden auf der Seite „LLDP MED-Netzwerkrichtlinien“ konfiguriert.

HINWEIS Wenn die LLDP-MED-Netzwerkrichtlinien für Sprachanwendungen (auf der Seite „LLDP-MED-Netzwerkrichtlinien“) auf „Autom.“ festgelegt sind und Auto-Voice-VLAN verwendet wird, generiert das Gerät automatisch eine LLDP MED-Netzwerkrichtlinie für Sprachanwendungen für alle LLDP-MED-fähigen Ports, die Mitglied des Voice-VLANs sind.

So konfigurieren Sie LLDP-MED auf den einzelnen Ports:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – LLDP** > **LLDP-MED-Porteinstellungen**.

Die Seite enthält die folgenden LLDP-MED-Einstellungen für sämtliche Ports (wobei die Liste nur die Felder umfasst, die auf der Seite **Bearbeiten** nicht beschrieben sind):

- **Ort**: Ob der Standort-TLV übertragen wird.
- **PoE**: Ob der POE-PSE-TLV übertragen wird.
- **Bestand**: Ob der Bestands-TLV übertragen wird.

SCHRITT 2 Aus der Meldung oben auf der Seite geht hervor, ob die LLDP MED-Netzwerkrichtlinie für die Sprachanwendung automatisch generiert wird (siehe **LLDP (Übersicht)**). Klicken Sie auf den Link, um den Modus zu ändern.

SCHRITT 3 Um einem Port zusätzliche LLDP-MED-TLVs und/oder eine oder mehrere benutzerdefinierte LLDP-MED-Netzwerkrichtlinien zuzuordnen, wählen Sie den Port aus und klicken Sie auf **Bearbeiten**.

SCHRITT 4 Geben Sie die Parameter ein:

- **Schnittstelle**: Wählen Sie die zu konfigurierende Schnittstelle aus.
- **LLDP-MED-Status**: Zum Aktivieren/Deaktivieren von LLDP-MED für diesen Port.
- **SNMP-Benachrichtigung**: Wählen Sie aus, ob bei Erkennen einer Endstation mit MED-Unterstützung, beispielsweise eines SNMP-Verwaltungssystems, bei einer Topologieänderung SNMP-Benachrichtigungen an einzelne Ports gesendet werden.
- **Ausgewählte optionale TLVs**: Wählen Sie die TLVs aus, die vom Gerät veröffentlicht werden können, indem Sie sie aus der Liste **Verfügbare optionale TLVs** in die Liste **Ausgewählte optionale TLVs** verschieben.
- **Verfügbare Netzwerkrichtlinien**: Wählen Sie die LLDP MED-Netzwerkrichtlinien aus, die von LLDP veröffentlicht werden sollen, indem Sie sie aus der Liste **Verfügbare Netzwerkrichtlinien** in die Liste **Ausgewählte Netzwerkrichtlinien** verschieben. Diese wurden auf der Seite „LLDP-MED-Netzwerkrichtlinien“ *erstellt.* Um eine oder mehrere benutzerdefinierte Netzwerkrichtlinien in die Ankündigung einzuschließen, müssen Sie außerdem unter **Verfügbare optionale TLVs** die Option **Netzwerkrichtlinie** auswählen.

  HINWEIS In den folgenden Feldern müssen Sie Eingaben in Hexadezimalzeichen in genau dem Datenformat vornehmen, das im LLDP MED-Standard (ANSI-TIA-1057_final_for_publication.pdf) definiert ist.

  - **Standortkoordinaten**: Geben Sie die Koordinaten des Standorts ein, die von LLDP veröffentlicht werden sollen.
  - **Standort-Hausadresse**: Geben Sie die Hausadresse ein, die von LLDP veröffentlicht werden soll.
  - **Standort (ECS) ELIN**: Geben Sie den Standort des Emergency Call Service (ECS) ELIN ein, der von LLDP veröffentlicht werden soll.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die LLDP MED-Porteinstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

LLDP-Portstatus

Die Seite „Tabelle für LLDP-Portstatus“ enthält die globalen LLDP-Informationen für jeden Port.

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – LLDP** > **LLDP-Portstatus**, um den LLDP-Portstatus anzuzeigen.

SCHRITT 2 Klicken Sie auf **LLDP: Details zu lokalen Informationen**, um die Details der LLDP- und LLDP MED-TLVs einzusehen, die an den Nachbarn gesendet wurden.

SCHRITT 3 Klicken Sie auf **LLDP: Details zu Nachbarinformationen**, um Einzelheiten zu den LLDP- und LLDP MED-TLVs einzusehen, die vom Nachbarn empfangen wurden.

Globale Information zum LLDP-Portstatus

- **Geräte-ID-Subtyp**: Typ der Geräte-ID (z. B. MAC-Adresse).
- **Geräte-ID**: Kennung des Geräts. Wenn es sich beim Geräte-ID-Subtyp um eine MAC-Adresse handelt, wird die MAC-Adresse des Geräts angezeigt.
- **Systemname**: Der Name des Geräts.
- **Systembeschreibung**: Beschreibung des Geräts (in alphanumerischem Format).
- **Unterstützte Systemfunktionen**: Die primären Funktionen des Geräts, wie z. B. Bridge, WLAN-AP oder Router.
- **Aktivierte Systemfunktionen**: Die aktivierte(n) primäre(n) Funktion(en) des Geräts.
- **Port-ID-Subtyp**: Art der Port-Kennung, die angezeigt wird.

Tabelle für LLDP-Portstatus

- **Schnittstelle**: Kennung des Ports.
- **LLDP-Status**: Die LLDP-Veröffentlichungsoption.
- **LLDP-MED-Status**: Aktiviert oder deaktiviert.
- **PoE, lokal**: Angekündigte PoE-Informationen, lokal.
- **Remote-PoE**: Die vom Nachbarn angekündigten PoE-Informationen.
- **Anzahl Nachbarn**: Anzahl der erkannten Nachbarn.
- **Nachbarfunktionen des 1. Geräts**: Zeigt die aktivierten primären Gerätefunktionen des Nachbarn an, z. B. Bridge oder Router.

LLDP-Local-Informationen

So können Sie den angekündigten LLDP-Status des lokalen Ports anzeigen:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – LLDP** > **LLDP – Lokale Informationen**.

SCHRITT 2 Wählen Sie die Schnittstelle aus, für die Sie die LLDP-Local-Informationen anzeigen möchten.

Auf dieser Seite werden die folgenden Felder für die ausgewählte Schnittstelle angezeigt:

Global

- **Geräte-ID-Subtyp**: Typ der Geräte-ID (z. B. die MAC-Adresse).
- **Geräte-ID**: Kennung des Geräts. Wenn es sich beim Geräte-ID-Subtyp um eine MAC-Adresse handelt, wird die MAC-Adresse des Geräts angezeigt.
- **Systemname**: Der Name des Geräts.
- **Systembeschreibung**: Beschreibung des Geräts (in alphanumerischem Format).
- **Unterstützte Systemfunktionen**: Die primären Funktionen des Geräts, wie z. B. Bridge, WLAN-AP oder Router.
- **Aktivierte Systemfunktionen**: Die aktivierte(n) primäre(n) Funktion(en) des Geräts.
- **Port-ID-Subtyp**: Art der Port-Kennung, die angezeigt wird.
- **Port-ID**: Kennung des Ports.
- **Portbeschreibung**: Informationen zum Port, einschließlich Hersteller, Produktname und Hardware- bzw. Software-Version.

Verwaltungsadresse

Anzeige der Adresstabelle des lokalen LLDP-Agenten. Andere standortferne Manager können diese Adresse verwenden, um Informationen über das lokale Gerät abzufragen. Die Adresse besteht aus den folgenden Elementen:

- **Adress-Subtyp**: Typ der Verwaltungs-IP-Adresse, die im Feld „Verwaltungsadresse“ angegeben ist, z. B. IPv4.
- **Adresse**: Zurückgegebene Adresse, die am besten zur Verwendung für Verwaltungszwecke geeignet ist, normalerweise eine Schicht-3-Adresse.
- **Schnittstellen-Subtyp**: Zur Definition der Schnittstellennummer verwendete Nummerierungsmethode.
- **Schnittstellennummer**: Die jeweilige, mit dieser Verwaltungsadresse assoziierte Schnittstelle.

MAC/PHY-Details

- **Autom. Aushandlung unterstützt**: Der Status ist „Automatische Aushandlung der Port-Geschwindigkeit wird unterstützt“.
- **Autom. Aushandlung aktiviert**: Der Status ist „Automatische Aushandlung der Port-Geschwindigkeit ist aktiviert“.
- **Bekannt gegebene Funktionen der autom. Aushandlung**: Funktionen der autom. Aushandlung der Portgeschwindigkeit, z. B. 1000BASE-T-Halbduplexmodus, 100BASE-TX-Vollduplexmodus.
- **Betriebs-MAU-Typ**: Art der Medium Attachment Unit (MAU). Die MAU führt physische Schichtfunktionen aus, einschließlich der Datenkonvertierung von der Ethernet-Schnittstellenkollisionserkennung und der Bit-Injektion in das Netzwerk, z. B. 100BASE-TX-Vollduplexmodus.

802.3-Details

- **Maximale 802.3-Frame-Größe**: Die maximal unterstützte IEEE-802.3-Frame-Größe.

802.3-Link-Aggregation

- **Aggregationsfähigkeit**: Angabe, ob die Schnittstelle aggregiert werden kann.
- **Aggregationsstatus**: Angabe, ob die Schnittstelle aggregiert ist.
- **Aggregations-Port-ID**: Angekündigte ID der aggregierten Schnittstelle.

802.3 Energy Efficient Ethernet (EEE) (wenn das Gerät EEE unterstützt)

- **Lokales Tx**: Gibt an, wie lange (in Mikrosekunden) der sendende Link-Partner nach dem Verlassen des Energiesparmodus im Leerlauf (Low Power Idle, LPI) wartet, bevor er mit dem Senden von Daten beginnt.
- **Lokales Rx**: Gibt an, wie lange (in Mikrosekunden) der empfangende Link-Partner im Anschluss an den Energiesparmodus im Leerlauf (Low Power Idle, LPI) den Link-Partner zu warten auffordert, bevor Daten übertragen werden.
- **Remote-Tx-Echo**: Gibt den vom lokalen Link-Partner wiedergegebenen Tx-Wert des Remote-Link-Partners an.
- **Remote-Rx-Echo**: Gibt den vom lokalen Link-Partner wiedergegebenen Rx-Wert des Remote-Link-Partners an.

MED-Details

- **Unterstützte Funktionen**: Vom Port unterstützte MED-Funktionen.
- **Aktuelle Funktionen**: Vom Port unterstützte, aktivierte MED-Funktionen.
- **Geräteklasse**: LLDP-MED-Endpunktgeräteklasse. Die möglichen Geräteklassen sind:
  - *Endpunktklasse 1*: Eine allgemeine Endpunktklasse, die grundlegende LLDP-Services bietet.
  - *Endpunktklasse 2*: Eine Medien-Endpunktklasse, die sowohl Medien-Streaming- als auch Klasse-1-Funktionen bietet.
  - *Endpunktklasse 3*: Eine Klasse von Kommunikationsgeräten, die Klasse-1- und -2-Funktionen bietet plus Standort, Notruf, Unterstützung für Schicht-2-Geräte und Verwaltungsfunktionen für Geräteinformationen.
- **PoE-Gerätetyp**: PoE-Typ des Ports, zum Beispiel „powered“.
- **PoE-Stromquelle**: Stromquelle des Ports.
- **PoE-Strompriorität**: Strompriorität des Ports.
- **PoE-Stromwert**: Stromwert des Ports.
- **Hardware-Version**: Versionsnummer der Hardware.
- **Firmware-Version**: Versionsnummer der Firmware.
- **Software-Version**: Versionsnummer der Software.
- **Seriennummer**: Seriennummer des Geräts.
- **Herstellername**: Name des Herstellers des Geräts.
- **Modellname**: Modellname des Geräts.
- **Bestands-ID**: Die Bestands-ID.

Standortinformationen

- **Hausadresse**: Anschrift.
- **Koordinaten**: Koordinaten auf der Karte: Breite, Länge und Höhe.
- **ECS-ELIN**: Device’s Emergency Call Service (ECS) Emergency Location Identification Number (ELIN): Standortnummer des Geräts bei Notfällen.

Tabelle für Netzwerkrichtlinien

- **Anwendungstyp**: Anwendungstyp der Netzwerkrichtlinie, zum Beispiel Sprache.
- **VLAN-ID**: ID des VLAN, für das die Netzwerkrichtlinie definiert wurde.
- **VLAN-Typ**: Typ des VLAN, für das die Netzwerkrichtlinie definiert wurde. Folgende Feldwerte sind möglich:
  - *Mit Tag*: Dies bedeutet, dass die Netzwerkrichtlinie für VLANs mit Tag definiert ist.
  - *Ohne Tag*: Dies bedeutet, dass die Netzwerkrichtlinie für VLANs ohne Tag definiert ist.
- **Benutzerpriorität**: Die Benutzerpriorität der Netzwerkrichtlinie.
- **DSCP**: DSCP der Netzwerkrichtlinie.

SCHRITT 3 Klicken Sie unten auf der Seite auf **Tabelle für LLDP-Portstatus**, um die Details zur **Tabelle für LLDP-Port-Status** anzuzeigen.

LLDP-Nachbarinformationen

Die Seite „LLDP-Nachbarinformationen“ enthält Informationen, die von Nachbargeräten empfangen wurden.

Nach einem Timeout (auf der Grundlage des Werts, der vom Nachbar-Time-to-Live-TLV empfangen wurde, während dessen keine LLDP-PDU von einem Nachbarn empfangen wurde), werden die Informationen gelöscht.

So können Sie die LLDP-Nachbarinformationen anzeigen:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery: LLDP** > **LLDP-Nachbarinformationen**.

SCHRITT 2 Wählen Sie die Schnittstelle aus, für die Sie die LLDP-Nachbarinformationen anzeigen möchten.

Auf dieser Seite werden die folgenden Felder für die ausgewählte Schnittstelle angezeigt:

- **Lokaler Port**: Nummer des lokalen Ports, an den der Nachbar angeschlossen ist.
- **Geräte-ID-Subtyp**: Typ der Geräte-ID (z. B. MAC-Adresse).
- **Geräte-ID**: Kennung des 802-LAN-Nachbargeräts.
- **Port-ID-Subtyp**: Art der Port-Kennung, die angezeigt wird.
- **Port-ID**: Kennung des Ports.

- **Systemname**: Veröffentlichter Name des Geräts.
- **Time-to-Live**: Zeitraum in Sekunden, nach dem die Informationen über diesen Nachbarn gelöscht werden.

SCHRITT 3 Wählen Sie einen lokalen Port aus, und klicken Sie auf **Details**.

Die Seite „LLDP-Nachbarinformationen“ enthält die folgenden Felder:

Portdetails

- **Lokaler Port**: Port-Nummer.
- **MSAP-Eintrag**: Eintragsnummer des Device Media Service Access Point (MSAP).

Basisdetails

- **Geräte-ID-Subtyp**: Typ der Geräte-ID (z. B. MAC-Adresse).
- **Geräte-ID**: Kennung des 802-LAN-Nachbargeräts.
- **Port-ID-Subtyp**: Art der Port-Kennung, die angezeigt wird.
- **Port-ID**: Kennung des Ports.
- **Portbeschreibung**: Informationen zum Port, einschließlich Hersteller, Produktname und Hardware- bzw. Software-Version.
- **Systemname**: Veröffentlichter Name des Systems.
- **Systembeschreibung**: Beschreibung der Netzwerk-Entität (in alphanumerischem Format). Dies schließt den Systemnamen und die Versionen der Hardware, des Betriebssystems und der vom Switch unterstützten Netzwerk-Software ein. Der Wert ist gleich dem sysDescr-Objekt.
- **Unterstützte Systemfunktionen**: Die primären Funktionen des Geräts. Die Funktionen werden durch zwei Oktette angegeben. Die Bits 0 bis 7 kennzeichnen Sonstige, Repeater, Bridge, WLAN-AP, Router, Telefon, DOCSIS-Kabelgerät bzw. Station. Die Bits 8 bis 15 sind reserviert.
- **Aktivierte Systemfunktionen**: Die aktivierte(n) primäre(n) Funktion(en) des Geräts.

Verwaltungsadresstabelle

- **Adresssubtyp**: Der Subtyp der verwalteten Adresse, z. B. MAC oder IPv4.
- **Adresse**: Verwaltungsadresse.
- **Schnittstellen-Subtyp**: Portsubtyp.
- **Schnittstellennummer**: Portnummer.

MAC/PHY-Details

- **Autom. Aushandlung unterstützt**: Der Status ist „Automatische Aushandlung der Port-Geschwindigkeit wird unterstützt“. Die möglichen Werte sind „Wahr“ und „Falsch“.
- **Autom. Aushandlung aktiviert**: Der Status ist „Automatische Aushandlung der Port-Geschwindigkeit ist aktiviert“. Die möglichen Werte sind „Wahr“ und „Falsch“.
- **Angekündigte Funktionen der autom. Aushandlung**: Funktionen der autom. Aushandlung der Port-Geschwindigkeit, z. B. 1000BASE-T-Halbduplexmodus, 100BASE-TX-Vollduplexmodus.
- **Betriebs-MAU-Typ**: Art der Medium Attachment Unit (MAU). Die MAU führt physische Schichtfunktionen aus, einschließlich der Konvertierung digitaler Daten von der Ethernet-Schnittstellenkollisionserkennung und der Bit-Injektion in das Netzwerk, z. B. 100BASE-TX-Vollduplexmodus.

802.3 Power via MDI

- **Port-Klasse für MDI Power-Unterstützung**: Angekündigte Port-Klasse für Power-Unterstützung.
- **PSE MDI Power-Unterstützung**: Angabe, ob MDI-Power vom Port unterstützt wird.
- **PSE MDI Power-Status**: Angabe, ob MDI-Power für den Port aktiviert ist.
- **PSE Power Pair-Steuerungsfunktion**: Angabe, ob die Power Pair-Steuerung vom Port unterstützt wird.
- **PSE Power Pair**: Der vom Port unterstützte Typ der Power Pair-Steuerung.
- **PSE Power-Klasse**: Angekündigte Power-Klasse des Ports.

802.3-Details

- **Maximale 802.3-Frame-Größe**: Angekündigte maximale Frame-Größe, die vom Port unterstützt wird.

802.3-Link-Aggregation

- **Aggregationsfähigkeit**: Angabe, ob der Port aggregiert werden kann.
- **Aggregationsstatus**: Angabe, ob der Port aggregiert ist.
- **Aggregations-Port-ID**: Angekündigte ID des aggregierten Ports.

802.3 Energy Efficient Ethernet (EEE)

- **Remote Tx**: Gibt an, wie lange (in Mikrosekunden) der sendende Link-Partner nach dem Verlassen des Energiesparmodus im Leerlauf (Low Power Idle, LPI) wartet, bevor er mit dem Senden von Daten beginnt.

- **Remote Rx**: Gibt an, wie lange (in Mikrosekunden) der empfangende Link-Partner im Anschluss an den Energiesparmodus im Leerlauf (Low Power Idle, LPI) den Link-Partner zu warten auffordert, bevor Daten übertragen werden.
- **Lokal-Tx-Echo**: Gibt den vom lokalen Link-Partner wiedergegebenen Tx-Wert des Remote-Link-Partners an.
- **Lokal-Rx-Echo**: Gibt den vom lokalen Link-Partner wiedergegebenen Rx-Wert des Remote-Link-Partners an.

MED-Details

- **Unterstützte Funktionen**: Für den Port aktivierte MED-Funktionen.
- **Aktuelle Funktionen**: Vom Port angekündigte, aktivierte MED-TLVs.
- **Geräteklasse**: LLDP-MED-Endpunktgeräteklasse. Die möglichen Geräteklassen sind:
  - *Endpunktklasse 1*: Eine allgemeine Endpunktklasse, die grundlegende LLDP-Services bietet.
  - *Endpunktklasse 2*: Eine Medien-Endpunktklasse, die sowohl Medien-Streaming- als auch Klasse-1-Funktionen bietet.
  - *Endpunktklasse 3*: Eine Klasse von Kommunikationsgeräten, die Klasse-1- und Klasse-2-Funktionen bietet plus Standort, Notruf, Unterstützung für Schicht-2-Switches und Verwaltungsfunktionen für Geräteinformationen.
- **PoE-Gerätetyp**: PoE-Typ des Ports, zum Beispiel „powered“.
- **PoE-Stromquelle**: Stromquelle des Ports.
- **PoE-Strompriorität**: Strompriorität des Ports.
- **PoE-Stromwert**: Stromwert des Ports.
- **Hardware-Version**: Versionsnummer der Hardware.
- **Firmware-Version**: Versionsnummer der Firmware.
- **Software-Version**: Versionsnummer der Software.
- **Seriennummer**: Seriennummer des Geräts.
- **Herstellername**: Name des Herstellers des Geräts.
- **Modellname**: Modellname des Geräts.
- **Bestands-ID**: Die Bestands-ID.

802.1-VLAN und Protokoll

- **PVID**: Angekündigte Port-VLAN-ID.

PPVIDs

PPVID-Tabelle

- **VID**: Protokoll-VLAN-ID.
- **Unterstützt**: Unterstützte Port- und Protokoll-VLAN-IDs.
- **Aktiviert**: Aktivierte Port- und Protokoll-VLAN-IDs.

VLAN-IDs

VLAN-ID-Tabelle

- **VID**: Port- und Protokoll-VLAN-ID.
- **VLAN-Name**: Angekündigte VLAN-Namen.

Protokoll-IDs

- **Protokoll-ID**: Die angekündigte Protokoll-ID.

Standortinformationen

Geben Sie die folgenden Datenstrukturen in Hexadezimalzeichen ein, wie in Abschnitt 10.2.4 des ANSI-TIA-1057-Standards beschrieben:

- **Hausadresse**: (Haus-)Anschrift.
- **Koordinaten**: Standortkoordinaten auf der Karte, Breite, Länge und Höhe.
- **ECS-ELIN**: Device's Emergency Call Service (ECS) Emergency Location Identification Number (ELIN): Standortnummer des Geräts bei Notfällen.
- **Unbekannt**: Standortinformationen nicht bekannt.

Netzwerkrichtlinie

Tabelle für Netzwerkrichtlinien

- **Anwendungstyp**: Anwendungstyp der Netzwerkrichtlinie, zum Beispiel Voice.
- **VLAN-ID**: ID des VLAN, für das die Netzwerkrichtlinie definiert wurde.
- **VLAN-Typ**: Typ des VLAN, mit oder ohne Tag, für den die Netzwerkrichtlinie definiert wurde.

- **Benutzerpriorität**: Die Benutzerpriorität der Netzwerkrichtlinie.
- **DSCP**: DSCP der Netzwerkrichtlinie.

SCHRITT 4 Wählen Sie einen Port aus und klicken Sie auf **Tabelle für LLDP-Portstatus**, um die Details der Tabelle für den LLDP-Portstatus anzuzeigen.

LLDP-Statistik

Auf der Seite „LLDP-Statistik“ werden LLDP-Statistikinformationen für die einzelnen Ports angezeigt.

So können Sie die LLDP-Statistik anzeigen:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – LLDP** > **LLDP-Statistik**.

Für die einzelnen Ports werden folgende Felder angezeigt:

- **Schnittstelle**: Kennung der Schnittstelle.
- **Gesamte Tx-Frames**: Anzahl der übertragenen Frames.
- **Rx-Frames**
  - *Gesamt*: Anzahl der empfangenen Frames.
  - *Verworfen*: Gesamtzahl der empfangenen Frames, die verworfen wurden.
  - *Fehler*: Anzahl der empfangenen Frames mit Fehlern.
- **Rx-TLVs**
  - *Verworfen*: Gesamtzahl der empfangenen TLVs, die verworfen wurden.
  - *Nicht erkannt*: Gesamtzahl der empfangenen TLVs, die nicht erkannt wurden.
- **Anzahl Löschungen Nachbarinformationen**: Anzahl der Altersüberschreitungen bei Nachbarn der Schnittstelle.

SCHRITT 2 Klicken Sie auf **Aktualisieren**, um die aktuellste Statistik anzuzeigen.

LLDP-Überlastung

LLDP fügt den LLDP-Paketen Informationen in Form von LLDP- und LLDP MED-TLVs hinzu. Eine LLDP-Überlastung tritt auf, wenn die Gesamtmenge der Informationen, die in ein LLDP-Paket eingeschlossen werden sollen, die von einer Schnittstelle unterstützte maximale PDU-Größe überschreitet.

Auf der Seite „LLDP-Überlastung“ wird die Anzahl der Bytes mit LLDP/LLDP-MED-Informationen, die Anzahl der verfügbaren Bytes für zusätzliche LLDP-Informationen sowie der Überlastungsstatus der einzelnen Schnittstellen angezeigt.

So können Sie die LLDP-Überlastungsinformationen anzeigen:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – LLDP** > **LLDP-Überlastung**.

Diese Seite enthält für die einzelnen Ports die folgenden Felder:

- **Schnittstelle**: Kennung des Ports.
- **Insgesamt verwendete Bytes**: Gesamtanzahl der Bytes mit LLDP-Informationen in jedem Paket.
- **Noch verfügbare Bytes**: Gesamtanzahl der noch verfügbaren Bytes für zusätzliche LLDP-Informationen in jedem Paket.
- **Status**: Angabe, ob TLVs übertragen werden oder ob sie überlastet sind.

SCHRITT 2 Wenn Sie Einzelheiten zur Überlastung eines Ports anzeigen möchten, wählen Sie den Port aus und klicken Sie auf **Details**.

Diese Seite enthält für die einzelnen vom Port gesendeten TLVs die folgenden Informationen:

- **Obligatorische LLDP-TLVs**
  - *Größe (Byte)*: Gesamtgröße der obligatorischen TLVs in Byte.
  - *Status*: Angabe, ob die Gruppe obligatorischer TLVs übertragen wird oder ob sie überlastet war.
- **LLDP MED-Funktionen**
  - *Größe (Byte)*: Gesamtgröße der LLDP-MED-Funktionspakete in Byte.
  - *Status*: Angabe, ob die LLDP-MED-Funktionspakete übertragen wurden oder ob sie überlastet waren.
- **LLDP MED-Standort**
  - *Größe (Byte)*: Gesamtgröße der LLDP-MED-Standortpakete in Byte.
  - *Status*: Angabe, ob die LLDP-MED-Standortpakete übertragen wurden oder ob sie überlastet waren.

- **LLDP MED-Netzwerkrichtlinien**
  - *Größe (Byte)*: Gesamtgröße der LLDP-MED-Netzwerkrichtlinienpakete in Byte.
  - *Status*: Angabe, ob die LLDP-MED-Netzwerkrichtlinienpakete übertragen wurden oder ob sie überlastet waren.
- **Erweiterte LLDP MED Power via MDI**
  - *Größe (Byte)*: Gesamtgröße der Pakete für „Erweiterte LLDP MED Power via MDI“ in Byte.
  - *Status*: Angabe, ob die Pakete für „Erweiterte LLDP MED Power via MDI“ übertragen wurden oder ob sie überlastet waren.
- **802.3-TLVs**
  - *Größe (Byte)*: Gesamtgröße der LLDP-MED-802.3-TLV-Pakete in Byte.
  - *Status*: Angabe, ob die LLDP-MED-802.3-TLV-Pakete übertragen wurden oder ob sie überlastet waren.
- **Optionale LLDP-TLVs**
  - *Größe (Byte)*: Gesamtgröße der optionalen LLDP-MED-TLV-Pakete in Byte.
  - *Status*: Angabe, ob die optionalen LLDP-MED-TLV-Pakete übertragen wurden oder ob sie überlastet waren.
- **LLDP MED-Bestand**
  - *Größe (Byte)*: Gesamtgröße der LLDP-MED-Bestands-TLV-Pakete in Byte.
  - *Status*: Angabe, ob die LLDP-MED-Bestands-TLV-Pakete übertragen wurden oder ob sie überlastet waren.
- **Gesamt**
  - *Gesamt (Byte)*: Gesamtanzahl der Bytes mit LLDP-Informationen in jedem Paket.
  - *Noch verfügbare Bytes*: Gesamtanzahl der noch verfügbaren, zu sendenden Bytes für zusätzliche LLDP-Informationen in jedem Paket.

Konfigurieren von CDP

In diesem Abschnitt wird beschrieben, wie Sie CDP konfigurieren.

Die folgenden Themen werden behandelt:

- **CDP-Eigenschaften**
- **CDP-Schnittstelleneinstellungen**
- **CDP-Local-Informationen**
- **CDP-Nachbarinformationen**
- **CDP-Statistik**

CDP-Eigenschaften

Das CDP-Protokoll (Cisco Discovery Protocol) ist ähnlich wie LLDP ein Verbindungsschichtprotokoll, mit dem direkt verbundene Nachbarn sich selbst und ihre Funktionen untereinander ankündigen. Im Gegensatz zu LLDP ist CDP ein proprietäres Protokoll von Cisco.

CDP-Konfigurations-Workflow

Der folgende Workflow ist ein Beispiel für das Konfigurieren von CDP auf dem Gerät. Weitere Anleitungen für die CDP-Konfiguration finden Sie im Abschnitt zu LLDP bzw. CDP.

SCHRITT 1 Geben Sie auf der Seite „CDP-Eigenschaften“ die globalen CDP-Parameter ein.

SCHRITT 2 Konfigurieren Sie auf der Seite „Schnittstelleneinstellungen“ CDP für die einzelnen Schnittstellen.

SCHRITT 3 Wenn die Funktionen von CDP-Geräten mit Auto-Smartport erkannt werden sollen, aktivieren Sie CDP auf der Seite „Smartport-Eigenschaften“.

Unter **Identifizieren des Smartport-Typs** wird beschrieben, wie CDP zum Identifizieren von Geräten für die Smartport-Funktion verwendet wird.

So geben Sie allgemeine CDP-Eigenschaften ein:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – CDP** > **Eigenschaften**.

SCHRITT 2 Geben Sie die Parameter ein.

- **CDP-Status**: Wählen Sie diese Option, um CDP für das Gerät zu aktivieren.

- **Bearbeitung von CDP-Frames**: Wenn CDP nicht aktiviert ist, wählen Sie die Aktion aus, die bei Empfang eines Pakets ausgeführt werden soll, das den ausgewählten Kriterien entspricht:
  - *Bridging*: Das Paket wird basierend auf dem VLAN weitergeleitet.
  - *Filterung*: Das Paket wird gelöscht.
  - *Überlauf*: Nicht VLAN-fähiger Überlauf, bei dem eingehende CDP-Pakete an alle Ports mit Ausnahme des Eingangsports weitergeleitet werden.
- **CDP-Voice-VLAN-Ankündigung**: Wählen Sie diese Option, damit das Gerät das Voice-VLAN in CDP an allen CDP-fähigen Ports ankündigt, die Mitglied des Voice-VLANs sind. Die Voice-VLAN-ID konfigurieren Sie auf der Seite „Voice-VLAN-Eigenschaften“.
- **Obligatorische CDP TLVs-Validierung**: Wenn diese Option ausgewählt ist, werden eingehende CDP-Pakete, die nicht die obligatorischen CDP-TLVs enthalten, verworfen und der Fehlerzähler für ungültige Daten wird erhöht.
- **CDP-Version**: Wählen Sie die Version von CDP aus, die verwendet werden soll.
- **CDP-Haltezeit**: Die Zeitspanne (in Vielfachen des TLV-Ankündigungsintervalls), während der CDP-Pakete vor dem Verwerfen beibehalten werden. Wenn beispielsweise das TLV-Ankündigungsintervall 30 Sekunden beträgt und der Multiplikator für das Halten gleich 4 ist, werden LLDP-Pakete nach 120 Sekunden verworfen. Folgende Optionen sind möglich:
  - *Standard verwenden*: Die Standarddauer (180 Sekunden) wird verwendet.
  - *Benutzerdefiniert*: Geben Sie die Dauer in Sekunden ein.
- **CDP-Übertragungsgeschwindigkeit**: Die Rate (in Sekunden), mit der CDP-Ankündigungsupdates gesendet werden. Folgende Optionen sind möglich:
  - *Standard verwenden*: Die Standardrate (60 Sekunden) wird verwendet.
  - *Benutzerdefiniert*: Geben Sie die Rate in Sekunden ein.
- **Format der Geräte-ID**: Wählen Sie das Format der Geräte-ID aus (MAC-Adresse oder Seriennummer). Folgende Optionen sind möglich:
  - *MAC-Adresse*: Verwenden Sie die MAC-Adresse des Geräts als Geräte-ID.
  - *Seriennummer*: Verwenden Sie die Seriennummer des Geräts als Geräte-ID.
  - *Hostname*: Verwenden Sie den Hostnamen des Geräts als Geräte-ID.
- **Quellschnittstelle**: Die IP-Adresse, die im TLV der Frames verwendet werden soll. Folgende Optionen sind möglich:
  - *Standard verwenden*: Die IP-Adresse der ausgehenden Schnittstelle wird verwendet.
  - *Benutzerdefiniert*: Die IP-Adresse der Schnittstelle (im Feld **Schnittstelle**) wird im Adress-TLV verwendet.

- **Schnittstelle**: Wenn Sie *Benutzerdefiniert* unter **Quellschnittstelle** ausgewählt haben, wählen Sie die Schnittstelle aus.
- **Syslog-Voice-VLAN stimmt nicht überein**: Aktivieren Sie diese Option, damit eine SYSLOG-Nachricht gesendet wird, wenn eine Nichtübereinstimmung beim Voice-VLAN erkannt wird. Dies bedeutet, dass die Informationen zum Voice-VLAN im eingehenden Frame nicht mit der Ankündigung des lokalen Geräts übereinstimmen.
- **Syslog-Natives-VLAN stimmt nicht überein**: Aktivieren Sie diese Option, damit eine SYSLOG-Nachricht gesendet wird, wenn eine Nichtübereinstimmung beim nativen VLAN erkannt wird. Dies bedeutet, dass die Informationen zum nativen VLAN im eingehenden Frame nicht mit der Ankündigung des lokalen Geräts übereinstimmen.
- **Syslog Duplex stimmt nicht überein**: Aktivieren Sie diese Option, damit eine SYSLOG-Nachricht gesendet wird, wenn Duplexinformationen nicht übereinstimmen. Dies bedeutet, dass die Duplexinformationen im eingehenden Frame nicht mit der Ankündigung des lokalen Geräts übereinstimmen.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die LLDP-Eigenschaften werden definiert.

CDP-Schnittstelleneinstellungen

Auf der Seite „Schnittstelleneinstellungen“ können Sie CDP für einzelne Ports aktivieren bzw. deaktivieren. Außerdem können Benachrichtigungen ausgelöst werden, wenn Konflikte mit CDP-Nachbarn vorliegen. Der Konflikt kann sich auf Voice-VLAN-Daten, natives VLAN oder Duplex beziehen.

Durch Festlegen dieser Eigenschaften können Sie die Informationsarten auswählen, die Geräten mit Unterstützung für das LLDP-Protokoll zur Verfügung gestellt werden sollen.

Auf der Seite „LLDP-MED-Schnittstelleneinstellungen“ können Sie die LLDP-MED-TLVs auswählen, die angekündigt werden sollen.

So definieren Sie die CDP-Schnittstelleneinstellungen:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – CDP** > **Schnittstelleneinstellungen**.

Auf dieser Seite werden die folgenden CDP-Informationen für die einzelnen Schnittstellen angezeigt.

- **CDP-Status**: Die CDP-Veröffentlichungsoption für den Port.
- **Konflikte mit CDP-Nachbarn werden gemeldet**: Der Status der Berichterstellungsoptionen, die Sie auf der Seite **Bearbeiten** aktivieren bzw. deaktivieren können (Voice-VLAN/Natives VLAN/Duplex).
- **Anzahl der Nachbarn**: Die Anzahl der erkannten Nachbarn.

Unten auf der Seite befinden sich vier Schaltflächen:

- **Einstellungen kopieren**: Wählen Sie diese Option aus, um eine Konfiguration von einem Port an einen anderen zu kopieren.
- **Bearbeiten**: Diese Felder werden unten in Schritt 2 erläutert.
- **Details zu lokalen CDP-Informationen**: Über diese Schaltfläche gelangen Sie zur Seite „Administration > Discovery – CDP > Lokale CDP-Informationen“.
- **Details zu CDP-Nachbarinformationen**: Über diese Schaltfläche gelangen Sie zur Seite „Administration > Discovery – CDP > CDP-Nachbarinformationen“.

SCHRITT 2 Wählen Sie einen Port aus, und klicken Sie auf **Bearbeiten**.

Auf dieser Seite sind die folgenden Felder verfügbar:

- **Schnittstelle**: Wählen Sie die Schnittstelle aus, die definiert werden soll.
- **CDP-Status**: Wählen Sie diese Option aus, um die CDP-Veröffentlichungsoption für den Port zu aktivieren oder zu deaktivieren.

  HINWEIS Die nächsten drei Felder sind aktiv, wenn das Gerät so eingerichtet wurde, dass Traps an die Verwaltungsstation gesendet werden.
- **Syslog-Voice-VLAN stimmt nicht überein**: Wählen Sie diese Option aus, damit eine SYSLOG-Nachricht gesendet wird, wenn eine Nichtübereinstimmung beim Voice-VLAN erkannt wird. Dies bedeutet, dass die Informationen zum Voice-VLAN im eingehenden Frame nicht mit der Ankündigung des lokalen Geräts übereinstimmen.
- **Syslog-Native-VLAN stimmt nicht überein**: Wählen Sie diese Option aus, damit eine SYSLOG-Nachricht gesendet wird, wenn eine Nichtübereinstimmung beim Native-VLAN erkannt wird. Dies bedeutet, dass die Informationen zum nativen VLAN im eingehenden Frame nicht mit der Ankündigung des lokalen Geräts übereinstimmen.
- **Syslog-Duplex stimmt nicht überein**: Wählen Sie diese Option aus, um das Senden einer SYSLOG-Nachricht bei Erkennung einer Nichtübereinstimmung bei den Duplexinformationen zu aktivieren. Dies bedeutet, dass die Duplexinformationen im eingehenden Frame nicht mit der Ankündigung des lokalen Geräts übereinstimmen.

SCHRITT 3 Geben Sie die relevanten Informationen ein, und klicken Sie auf **Übernehmen**. Die Porteinstellungen werden in die aktuelle Konfiguration geschrieben.

CDP-Local-Informationen

So zeigen Sie über das CDP-Protokoll angekündigte Informationen zum lokalen Gerät an:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – CDP** > **Lokale CDP-Informationen**.

SCHRITT 2 Wählen Sie einen lokalen Port aus. Daraufhin werden die folgenden Felder angezeigt:

- **Schnittstelle**: Die Nummer des lokalen Ports.
- **CDP-Status**: Zeigt an, ob CDP aktiviert ist.
- **Geräte-ID-TLV**
  - **Geräte-ID-Typ**: Der Typ der Geräte-ID, die im Geräte-ID-TLV angekündigt wird.
  - **Geräte-ID**: Die Geräte-ID, die im Geräte-ID-TLV angekündigt wird.
- **Systemnamens-TLV**
  - **Systemname**: Der Systemname des Geräts.
- **Adress-TLV**
  - **Adresse 1 - 3**: IP-Adressen (im Geräte-Adress-TLV angekündigt).
- **Port-TLV**
  - **Port-ID**: Die Kennung des im Port-TLV angekündigten Ports.
- **Funktions-TLV**
  - **Funktionen**: Die im Port-TLV angekündigten Funktionen.
- **Versions-TLV**
  - **Version**: Informationen zur im Gerät ausgeführten Softwareversion.
- **Plattform-TLV**
  - **Plattform**: Die Kennung der im Plattform-TLV angekündigten Plattform.
- **TLV für natives VLAN**
  - **Natives VLAN**: Die Kennung des nativen VLANs, die im nativen VLAN-TLV angekündigt wird.
- **Voll-/Halbduplex-TLV**
  - **Duplex**: Gibt an, ob es sich um einen Halb- oder Vollduplexport handelt, der im Voll- oder Halbduplex-TLV angekündigt wird.

- **Appliance-TLV**
  - **Appliance ID**: Der Typ des an den Port angeschlossenen Geräts, der im Appliance-TLV angekündigt wird.
  - **Appliance VLAN-ID**: Das VLAN im von der Appliance verwendeten Gerät. Wenn es sich bei der Appliance beispielsweise um ein IP-Telefon handelt, ist dies das Voice-VLAN.
- **TLV für erweiterte Vertrauensstell.**
  - **Erweitertes Trust**: Wenn diese Option aktiviert ist, ist der Port vertrauenswürdig, das heißt, dem Host bzw. Server, von dem das Paket empfangen wird, wird vertraut, die Pakete selbst zu kennzeichnen. In diesem Fall werden die an einem solchen Port empfangenen Pakete nicht erneut gekennzeichnet. Wenn die Option deaktiviert ist, ist der Port nicht vertrauenswürdig. In diesem Fall ist das folgende Feld relevant.
- **TLV für CoS für nicht vertrauenswürdige Ports**
  - **CoS für nicht vertrauenswürdige Ports**: Wenn „Erweitertes Trust“ für den Port deaktiviert ist, wird in diesen Feldern der Schicht-2-CoS-Wert (das heißt ein 802.1D/802.1p-Prioritätswert) angezeigt. Dies ist der CoS Wert, mit dem alle empfangenen Pakete an einem nicht vertrauenswürdigen Port vom Gerät kommentiert werden.
- **Leistungs-TLV**
  - **Anforderungs-ID**: Die letzte empfangene Leistungsanforderungs-ID entspricht dem letzten in einem Leistungsanforderungs-TLV empfangenen Feld „Anforderungs-ID“. Die ID entspricht 0, wenn seit der letzten Aktivierung der Schnittstelle kein Leistungsanforderungs-TLV empfangen wurde.
  - **Leistungsmanagement-ID**: Dieser Wert wird bei jedem Eintreten eines der folgenden Ereignisse um 1 (oder 2, um den Wert 0 zu vermeiden) erhöht:

    Der Wert im Feld „Verfügbare Leistung“ oder „Management-Leistungsstufe“ wird geändert.

    Es wird ein Leistungsanforderungs-TLV mit einem Anforderungs-ID-Feld empfangen, das sich vom letzten empfangenen Satz (oder vom ersten empfangenen Wert) unterscheidet.

    Die Schnittstelle wird deaktiviert.
  - **Verfügbare Leistung**: Die vom Port verbrauchte Leistung.
  - **Management-Leistungsstufe**: Zeigt die Anforderung des Lieferanten an das betriebene Gerät für dessen Leistungsaufnahme-TLV an. In diesem Feld wird für das Gerät immer „Keine Präferenz“ angezeigt.

CDP-Nachbarinformationen

Auf der Seite „CDP-Nachbarinformationen“ werden CDP-Informationen angezeigt, die von Nachbargeräten empfangen wurden.

Nach einem Timeout (auf der Grundlage des Werts, der vom Nachbar-Time-to-Live-TLV empfangen wurde, während dessen keine CDP-PDU von einem Nachbarn empfangen wurde), werden die Informationen gelöscht.

So zeigen Sie die CDP-Nachbarinformationen an:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – CDP** > **CDP-Nachbarinformationen**.

SCHRITT 2 Um einen Filter auszuwählen, aktivieren Sie das Kontrollkästchen **Filter,** wählen Sie eine lokale Schnittstelle aus und klicken Sie dann auf **Los**.

Der Filter wird ausgelöst und **Filter löschen** wird aktiviert.

SCHRITT 3 Klicken Sie auf **Filter löschen**, um den Filter zu beenden.

Die Seite „CDP-Nachbarinformationen“ enthält die folgenden Felder für den Link-Partner (den Nachbarn):

- **Geräte-ID**: Die Geräte-ID des Nachbarn.
- **Systemname**: Der Systemname des Nachbarn.
- **Lokale Schnittstelle**: Die Nummer des lokalen Ports, an den der Nachbar angeschlossen ist.
- **Version der Ankündigung**: Die CDP-Protokollversion.
- **Time-to-Live (Sek.)**: Der Zeitraum (in Sekunden), nach dem die Informationen über diesen Nachbarn gelöscht werden.
- **Funktionen**: Die vom Nachbarn angekündigten Funktionen.
- **Plattform**: Informationen aus dem Plattform-TLV des Nachbarn.
- **Nachbarschnittstelle**: Die Ausgangsschnittstelle des Nachbarn.

SCHRITT 4 Wählen Sie ein Gerät aus und klicken Sie auf **Details**.

Diese Seite enthält folgende Felder für den Nachbarn:

- **Geräte-ID**: Die Kennung des Nachbargeräts.
- **Systemname**: Der Name der benachbarten Geräte-ID.
- **Lokale Schnittstelle**: Die Schnittstellennummer des Ports, über den der Frame eingegangen ist.
- **Version der Ankündigung**: Die Version von CDP.

- **Time-to-Live**: Zeitraum in Sekunden, nach dem die Informationen über diesen Nachbarn gelöscht werden.
- **Funktionen**: Die primären Funktionen des Geräts. Die Funktionen werden durch zwei Oktette angegeben. Die Bits 0 bis 7 kennzeichnen Sonstige, Repeater, Bridge, WLAN-AP, Router, Telefon, DOCSIS-Kabelgerät bzw. Station. Die Bits 8 bis 15 sind reserviert.
- **Plattform**: Die Kennung der Plattform des Nachbarn.
- **Nachbarschnittstelle**: Die Schnittstellennummer des Nachbarn, über den der Frame eingegangen ist.
- **Natives VLAN**: Das native VLAN des Nachbarn.
- **Anwendung**: Der Name der Anwendung, die auf dem Nachbarn ausgeführt wird.
- **Duplex**: Gibt an, ob die Nachbarschnittstelle im Halb- oder Vollduplex-Modus betrieben wird.
- **Adressen**: Die Adressen des Nachbarn.
- **Gezogener Strom**: Die Menge der vom Nachbarn an der Schnittstelle verbrauchten Leistung.
- **Version**: Die Softwareversion des Nachbarn.

HINWEIS Wenn Sie auf die Schaltfläche **Tabelle löschen** klicken, werden alle verbundenen Geräte von CDP getrennt. Wenn Auto-Smartport aktiviert ist, werden alle Porttypen in die Standardeinstellung geändert.

CDP-Statistik

Auf der Seite „CDP-Statistik“ werden Informationen zu CDP-Frames angezeigt, die über einen Port gesendet oder empfangen wurden. CDP-Pakete werden von Geräten empfangen, die an die Schnittstellen des Switch angeschlossen sind, und für die Smartport-Funktion verwendet. Weitere Informationen hierzu finden Sie unter **Konfigurieren von CDP**.

Die CDP-Statistik für einen Port wird nur angezeigt, wenn CDP global und für den Port aktiviert ist. Verwenden Sie hierzu die Seiten „CDP-Eigenschaften“ und „CDP-Schnittstelleneinstellungen“.

So zeigen Sie die CDP-Statistik an:

SCHRITT 1 Klicken Sie auf **Administration > Discovery – CDP > CDP-Statistik**.

Für jede Schnittstelle werden die folgenden Felder angezeigt:

Empfangene/gesendete Pakete:

- **Version 1**: Die Anzahl der empfangenen bzw. gesendeten Pakete mit CDP-Version 1.
- **Version 2**: Die Anzahl der empfangenen bzw. gesendeten Pakete mit CDP-Version 2.
- **Gesamt**: Die Gesamtanzahl der empfangenen bzw. gesendeten CDP-Pakete.

Im Abschnitt „CDP-Fehlerstatistik“ werden die CDP-Fehlerzähler angezeigt.

- **Unzulässige Prüfsumme**: Die Anzahl der empfangenen Pakete mit unzulässigem Prüfsummenwert.
- **Andere Fehler**: Die Anzahl der empfangenen Pakete mit anderen Fehlern als unzulässigen Prüfsummen.
- **Nachbarn über Maximum**: Die Anzahl der Fälle, in denen Paketinformationen nicht im Cache gespeichert werden konnten, da der Speicherplatz nicht ausreichte.

Zum Löschen aller Zähler für alle Schnittstellen klicken Sie auf **Alle Schnittstellenzähler löschen**. Zum Löschen aller Zähler für eine Schnittstelle klicken Sie auf **Schnittstellenzähler löschen**.

11

Portverwaltung

In diesem Abschnitt werden die Portkonfiguration, die Link-Aggregation und die Green Ethernet-Funktion beschrieben.

Die folgenden Themen werden behandelt:

- **Konfigurieren von Ports**
- **Loopback-Erkennung**
- **Link-Aggregation**
- **UDLD**
- **Konfigurieren von Green Ethernet**

Konfigurieren von Ports

Workflow

Führen Sie zum Konfigurieren von Ports folgende Aktionen durch:

1. Konfigurieren Sie den Port auf der Seite „Porteinstellungen“.
2. Aktivieren bzw. deaktivieren Sie das LAG-Protokoll (Link Aggregation Control, Link-Aggregationssteuerung) und konfigurieren Sie die potenziellen Mitgliedsports auf der Seite „LAG-Verwaltung“ mit den gewünschten LAGs. Standardmäßig sind alle LAGs leer.
3. Konfigurieren Sie auf der Seite „LAG-Einstellungen“ die Ethernet-Parameter wie beispielsweise die Geschwindigkeit und die automatische Aushandlung für die LAGs.
4. Konfigurieren Sie auf der Seite „LACP“ die LACP-Parameter für die Ports, die Mitglieder oder Kandidaten einer dynamischen Link-Aggregationsgruppe sind.
5. Konfigurieren Sie auf der Seite „Eigenschaften“ Green Ethernet und 802.3 Energy Efficient Ethernet.
6. Konfigurieren Sie auf der Seite „Porteinstellungen“ den Green Ethernet-Energiemodus und 802.3 Energy Efficient Ethernet pro Port.
7. Falls PoE vom Gerät unterstützt wird und für dieses aktiviert ist, konfigurieren Sie das Gerät wie unter **Portverwaltung: PoE** beschrieben.

Anschlusskonfiguration

Ports können auf den folgenden Seiten konfiguriert werden:

Porteinstellungen

Auf der Seite „Porteinstellungen“ werden die globalen und die spezifischen Einstellungen für alle Ports angezeigt. Auf dieser Seite können Sie die gewünschten Ports auswählen, um sie auf der Seite „Porteinstellungen bearbeiten“ zu bearbeiten.

So konfigurieren Sie Porteinstellungen:

SCHRITT 1 Klicken Sie auf **Portverwaltung** > **Porteinstellungen**.

SCHRITT 2 Wählen Sie **Jumbo-Frames** aus, damit Pakete mit einer Größe von bis zu 10 KB unterstützt werden. Wenn die Option **Jumbo Frames** nicht aktiviert ist (Standardeinstellung), unterstützt das System eine Paketgröße von bis zu 2.000 Byte. Damit die Jumbo-Frames wirksam werden, muss das Gerät nach der Aktivierung der Funktion neu gestartet werden.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um die globale Einstellung zu aktualisieren.

Änderungen an der Jumbo Frame-Konfiguration werden erst wirksam, *nachdem* Sie die aktuelle Konfiguration explizit auf der Seite „Konfiguration kopieren/speichern“ in der Startkonfigurationsdatei gespeichert haben und das Gerät neu gestartet wurde.

SCHRITT 4 Wählen Sie zum Aktualisieren der Porteinstellungen den gewünschten Port aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 5 Ändern Sie die folgenden Parameter:

- **Schnittstelle**: Wählen Sie die Portnummer aus.
- **Port-Beschreibung**: Geben Sie den benutzerdefinierten Namen oder einen Kommentar für den Port ein.
- **Porttyp**: Zeigt den Porttyp und die Geschwindigkeit an. Folgende Optionen sind möglich:
  - *Kupferports*: Reguläre Ports, keine Kombinationsports; unterstützen die folgenden Werte: 10M, 100M und 1000M (Typ: Kupfer).
  - *Kupfer-Kombinationsports*: Kombinationsport, an den ein CAT5-Kupferkabel angeschlossen ist; unterstützt die folgenden Werte: 10M, 100M und 1000M (Typ: ComboC).
  - *Glasfaser-Kombinationsports*: *GBIC-Port (Gigabit Interface Converter) für SFP-Glasfaser*; unterstützt die folgenden Werte: 100M und 1000M (Typ: ComboF).
  - 10G-Glasfaser: Ports mit der Geschwindigkeit 1G oder 10G.

HINWEIS Falls beide Ports verwendet werden, hat bei Kombinationsports SFP-Glasfaser Vorrang.

- **Administrativer Status**: Wählen Sie aus, ob der Port aktiv oder nicht aktiv sein muss, wenn das Gerät neu gestartet wird.
- **Betriebsstatus**: Zeigt an, ob der Port zurzeit aktiv ist. Wenn der Port aufgrund eines Fehlers nicht aktiv ist, wird die Fehlerbeschreibung angezeigt.
- **Leitungsstatus SNMP-Traps**: Wählen Sie diese Option aus, um die Generierung von SNMP-Traps zu aktivieren, die Benachrichtigungen bei Änderungen am Link-Status des Ports versenden.
- **Zeitbereich**: Wählen Sie diese Option, um den Zeitbereich zu aktivieren, in dem der Port den Status „Aktiv“ hat. Wenn der Zeitbereich nicht aktiv ist, ist der Port heruntergefahren. Ein konfigurierter Zeitbereich ist nur wirksam, wenn der Port administrativ aktiv ist. Wenn noch kein Zeitbereich definiert ist, klicken Sie auf **Bearbeiten**, um zur Seite „Zeitbereich“ zu wechseln.
- **Zeitbereichsname**: Wählen Sie das Profil, durch das der Zeitbereich spezifiziert wird.
- **Status des Betriebszeitbereichs**: Zeigt an, ob der Zeitbereich zurzeit aktiv oder inaktiv ist.
- **Automatisch aushandeln**: Mit dieser Option aktivieren Sie die automatische Aushandlung für den Port. Durch die automatische Aushandlung wird ermöglicht, dass ein Port dem Port-Link-Partner seine Übertragungsgeschwindigkeit, den Duplex-Modus und seine Funktionen für die Datenflusssteuerung ankündigt.
- **Autom. Aushandlung für Betrieb**: Zeigt den aktuellen Status der automatischen Aushandlung für den Port an.
- **Geschwindigkeit von Administrationsport**: Wählen Sie die Geschwindigkeit des Ports aus. Die verfügbaren Geschwindigkeiten hängen vom Porttyp ab. Die Option *Administrationsgeschwindigkeit* können Sie nur dann festlegen, wenn die automatische Aushandlung für den Port deaktiviert ist.
- **Geschwindigkeit von Betriebs-Port**: Zeigt die aktuelle Port-Geschwindigkeit an, die das Ergebnis der Aushandlung ist.
- **Administrativer Duplex-Modus**: Wählen Sie den Duplex-Modus für den Port aus. Dieses Feld ist nur dann konfigurierbar, wenn die automatische Aushandlung deaktiviert ist und für die Port-Geschwindigkeit 10M oder 100M festgelegt wurde. Bei einer Portgeschwindigkeit von 1G wird immer der Vollduplex-Modus verwendet. Folgende Optionen sind möglich:
  - *Halb*: Die Schnittstelle unterstützt die Übertragung zwischen dem Gerät und dem Client immer nur in eine Richtung (nicht in beide Richtungen gleichzeitig).
  - *Voll*: Die Schnittstelle unterstützt die Übertragung zwischen dem Gerät und dem Client in beide Richtungen gleichzeitig.
- **Betriebs-Duplex-Modus**: Zeigt den aktuellen Duplex-Modus des Ports an.

- **Automatische Ankündigung**: Wählen Sie die Funktionen aus, die bei der automatischen Aushandlung angekündigt werden, wenn diese aktiviert ist. Folgende Optionen sind möglich:
  - *Max. Fähigkeit*: Alle Port-Geschwindigkeiten und Duplex-Modus-Einstellungen können akzeptiert werden.
  - *10 halb*: Geschwindigkeit von 10 MBit/s und halber Duplex-Modus.
  - *10 voll*: Geschwindigkeit von 10 MBit/s und voller Duplex-Modus.
  - *100 halb*: Geschwindigkeit von 100 MBit/s und halber Duplex-Modus.
  - *100 voll*: Geschwindigkeit von 100 MBit/s und voller Duplex-Modus.
  - *1000 voll*: Geschwindigkeit von 1000 MBit/s und voller Duplex-Modus.
- **Betriebsankündigung**: Zeigt die Funktionen an, die dem Nachbargerät des Ports zurzeit angekündigt wurden. Die möglichen Optionen sind im Feld *Administrationsankündigung* angegeben.
- **Präferenzmodus**: Wählen Sie den Master-Slave-Modus der Schnittstelle für den Betrieb mit automatischer Aushandlung aus. Wählen Sie eine der folgenden Optionen aus:
  - *Slave*: Aushandlungsbeginn mit der Präferenz, dass der Geräteport im Prozess der automatischen Aushandlung als Slave fungiert.
  - *Master*: Aushandlungsbeginn mit der Präferenz, dass der Geräteport im Prozess der automatischen Aushandlung als Slave fungiert.
- **Nachbarankündigung**: Zeigt die Funktionen an, die vom Nachbargerät (Link-Partner) angekündigt werden.
- **Rückstau**: Wählen Sie den Rückstau-Modus für den Port aus (wird zusammen mit dem Halbduplex-Modus verwendet), um die Paketempfangsgeschwindigkeit zu verringern, wenn sich Daten beim Gerät anstauen. Damit wird der Remote-Port durch Blockieren des Signals deaktiviert, sodass von diesem keine Pakete mehr gesendet werden können.
- **Flusssteuerung**: Aktivieren oder deaktivieren Sie die Flusssteuerung für 802.3x, oder aktivieren Sie die automatische Aushandlung der Flusssteuerung für den Port (nur bei vollem Duplex-Modus).
- **MDI/MDIX**: Status des MDI *(Media Dependent Interface)* oder des MDIX *(Media Dependent Interface with Crossover)* des Ports.

  Folgende Optionen sind möglich:
  - *MDIX*: Wählen Sie diese Option aus, um die Übertragungs- und Empfangspaare des Ports zu vertauschen.
  - *MDI*: Wählen Sie diese Option, um dieses Gerät über ein ungekreuztes Kabel mit einer Station zu verbinden.
  - *Automatisch*: Mit dieser Option können Sie das Gerät so konfigurieren, dass von ihm automatisch die korrekten Pinbelegungen für die Verbindung mit einem anderen Gerät erkannt werden.

- **Betriebs-MDI/MDIX**: Zeigt die aktuelle MDI/MDIX-Einstellung an.
- **Mitglied in LAG**: Zeigt an, ob der Port Mitglied einer LAG ist.
- **Geschützter Port**: Wählen Sie diese Option, wenn der Port geschützt werden soll. (Ein geschützter Port wird auch als PVE (Private VLAN Edge) bezeichnet.) Geschützte Ports verfügen über folgende Funktionen:
  - Geschützte Ports bieten Schicht-2-Isolierung zwischen Schnittstellen (Ethernet-Ports und LAGs (Link Aggregation Groups)), die das gleiche VLAN nutzen.
  - Von geschützten Ports empfangene Pakete können nur an ungeschützte Ausgangs-Ports weitergeleitet werden. Die Filterregeln von geschützten Ports werden auch auf Pakete angewendet, die durch Software weitergeleitet werden, beispielsweise durch Snooping-Anwendungen.
  - Der Schutz von Ports besteht unabhängig von einer VLAN-Mitgliedschaft. Mit geschützten Ports verbundene Geräte können nicht miteinander kommunizieren, selbst dann nicht, wenn sie alle Mitglieder desselben VLANs sind.
  - Sowohl Ports als auch LAGs können als geschützt festgelegt werden. Geschützte LAGs werden im Abschnitt **Konfigurieren von LAG-Einstellungen** beschrieben.
- **Mitglied in LAG**: Zeigt die Nummer der LAG an, falls der Port Mitglied einer LAG ist. Anderenfalls bleibt das Feld leer.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die Porteinstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Wiederherstellungseinstellungen nach Fehlern

Auf dieser Seite wird die automatische Reaktivierung eines Ports aktiviert, der aufgrund eines Fehlers heruntergefahren wurde, nachdem das Intervall für automatische Wiederherstellung verstrichen war.

So konfigurieren Sie die Wiederherstellungseinstellungen nach Fehlern:

SCHRITT 1 Klicken Sie auf **Portverwaltung** > **Wiederherstellungseinstellungen nach Fehlern**.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **Intervall für automatische Wiederherstellung**: Geben Sie die Verzögerungszeit für die automatische Wiederherstellung nach Fehlern (sofern aktiviert) im Anschluss an das Herunterfahren eines Ports an.

Automatische ErrDisable-Wiederherstellung

- **Portsicherheit**: Wählen Sie diese Option aus, um die automatische Wiederherstellung nach Fehlern zu aktivieren, wenn ein Port aufgrund von Portsicherheitsverletzungen heruntergefahren wurde.

- **Verstoß gegen einzelnen 802.1x-Host**: Wählen Sie diese Option aus, um die automatische Wiederherstellung nach Fehlern zu aktivieren, wenn der Port von 802.1x heruntergefahren wurde.
- **ACL-Verweigerung**: Wählen Sie diese Option aus, damit der Mechanismus für die automatische Wiederherstellung nach Fehlern durch eine ACL-Aktion aktiviert wird.
- **STP BPDU Guard**: Wählen Sie diese Option aus, um den Mechanismus für die automatische Wiederherstellung nach Fehlern zu aktivieren, wenn der Port durch einen STP BPDU Guard heruntergefahren wurde.
- **STP-Loopback-Guard**: Wählen Sie diese Option aus, um die automatische Wiederherstellung nach Fehlern zu aktivieren, wenn der Port durch einen STP-Loopback-Guard heruntergefahren wurde.
- **UDLD**: Wählen Sie diese Option aus, um die automatische Wiederherstellung nach Fehlern für den UDLD-Status zum Herunterfahren zu aktivieren.
- **Loopback-Erkennung**: Wählen Sie diese Option aus, um die automatische Wiederherstellung nach Fehlern für Ports zu aktivieren, die durch Loopback-Erkennung heruntergefahren wurden.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um die globale Einstellung zu aktualisieren.

So reaktivieren Sie einen Port manuell:

SCHRITT 1 Klicken Sie auf **Portverwaltung** > **Wiederherstellungseinstellungen nach Fehlern**.

Daraufhin wird eine Liste mit den nicht aktivierten Schnittstellen und deren **Deaktivierungsgrund** angezeigt.

SCHRITT 2 Wählen Sie Schnittstelle aus, die reaktiviert werden soll.

SCHRITT 3 Klicken Sie auf **Reaktivieren**.

Loopback-Erkennung

Die Loopback-Erkennung (LBD) bietet Schutz vor Schleifen (Loops), indem Schleifenprotokollpakete aus Ports übertragen werden, auf denen der Schleifenschutz aktiviert wurde. Wenn der Switch ein Schleifenprotokollpaket aussendet und dann dasselbe Paket zurückerhält, fährt er den Port herunter, der das Paket empfangen hat.

Der Loopback-Schutz arbeitet unabhängig von STP. Nach der Erkennung einer Schleife wird der Port, der die Schleifen empfangen hat, in den heruntergefahrenen Zustand versetzt. Es wird ein Trap gesendet und das Ereignis wird protokolliert. Netzwerkmanager können ein Erkennungsintervall definieren, das die Zeitspanne zwischen LBD-Paketen festlegt.

Folgende Fälle von Schleifen können vom Loopback-Erkennungsprotokoll erkannt werden:

- **Kurzschluss**: Ein Port, der sämtlichen empfangenen Verkehr zurückschleift.
- **Direkte Mehrportschleife zwischen mehreren Ports**: Der Switch ist mit einem anderen Switch verbunden, wobei mehr als ein Port und STP deaktiviert sind.
- **LAN-Segmentschleife**: Der Switch ist über einen oder mehrere Ports mit einem LAN-Segment verbunden, das Schleifen aufweist.

Funktionsweise von LBD

Der LBD-Protokoll sendet in regelmäßigen Abständen per Broadcast ein Loopback-Erkennungspaket. Ein Switch erkennt eine Schleife, wenn er seine eigenen LBD-Pakete empfängt.

Folgende Bedingungen müssen erfüllt sein, damit ein Port LBD-aktiv ist:

- LBD ist global aktiviert.
- LBD ist für den Port aktiviert.
- Der Port ist funktionsfähig (der Betriebsstatus ist „Aktiv“).
- Der Port weist den STP-Status „Weiterleitung/Deaktivieren“ (MSTP-Instanzweiterleitungsstatus, Instanz 0) auf.

LBD-Frames werden auf LBD-aktiven Ports über die Warteschlange mit der höchsten Priorität übertragen (bei LAGs wird LBD auf jedem aktiven Portmitglied in der LAG übertragen).

Wird eine Schleife erkannt, führt der Switch folgende Aktionen durch:

- Die empfangenden Ports oder LAGs werden in den Status „Fehler – Deaktivieren“ versetzt.
- Der Switch setzt ein entsprechendes SNMP-Trap ab.
- Er erzeugt eine entsprechende SYSLOG-Nachricht.

Konfigurieren der Loopback-Erkennung

Standardeinstellungen und Konfiguration

Die Loopback-Erkennung ist standardmäßig nicht aktiviert.

Interaktionen mit anderen Funktionen

Wenn STP auf einem Port aktiviert ist, auf dem die Loopback-Erkennung aktiviert ist, muss der Port im STP-Weiterleitungsstatus arbeiten.

Konfigurieren des LBD-Workflows

So aktivieren und konfigurieren Sie LBD:

SCHRITT 1 Aktivieren Sie die Loopback-Erkennung auf der Seite „Loopback-Erkennungseinstellungen“ systemweit.

SCHRITT 2 Aktivieren Sie die Loopback-Erkennung auf der Seite „Loopback-Erkennungseinstellungen“ für die Zugriffsports.

SCHRITT 3 Aktivieren Sie die automatische Wiederherstellung für die Loopback-Erkennung auf der Seite „Wiederherstellungseinstellungen nach Fehlern.“

So konfigurieren Sie die Loopback-Erkennung:

SCHRITT 1 Klicken Sie auf **Portverwaltung** > **Loopback-Erkennungseinstellungen**.

SCHRITT 2 Wählen Sie im globalen Feld der **Loopback-Erkennung** die Option **Aktivieren** aus, um die Funktion zu aktivieren.

SCHRITT 3 Geben Sie das **Erkennungsintervall** an. Dies ist das Intervall zwischen der Übertragung von LBD-Paketen.

SCHRITT 4 Klicken Sie auf **Übernehmen**, um die Konfiguration in der aktuellen Konfigurationsdatei zu speichern.

Die folgenden Felder zum **Loopback-Erkennungsstatus** werden für jede Schnittstelle angezeigt:

- **Administrativ**: Die Loopback-Erkennung ist aktiviert.
- **Operativ**: Die Loopback-Erkennung ist aktiviert, aber auf der Schnittstelle nicht aktiv.

SCHRITT 5 Legen Sie im Feld **Schnittstellentyp ist gleich** fest, ob LBD auf Ports oder LAGs aktiviert werden soll.

SCHRITT 6 Wählen Sie die Ports oder LAGs aus, für die LBD aktiviert werden soll und klicken Sie auf **Bearbeiten**.

SCHRITT 7 Wählen Sie im Feld „Loopback-Erkennungsstatus“ für den ausgewählten Port bzw. die ausgewählte LAG **Aktivieren** aus.

SCHRITT 8 Klicken Sie auf **Übernehmen**, um die Konfiguration in der aktuellen Konfigurationsdatei zu speichern.

Link-Aggregation

In diesem Abschnitt wird beschrieben, wie Sie LAGs konfigurieren. Die folgenden Themen werden behandelt:

- **Link-Aggregation – Übersicht**
- **Standardeinstellungen und Konfiguration**
- **Workflow von statischen und dynamischen LAGs**
- **Definieren der LAG-Verwaltung**
- **Konfigurieren von LAG-Einstellungen**
- **Konfigurieren von LACP**

Link-Aggregation – Übersicht

LACP (Link Aggregation Control Protocol, Link-Aggregationsteuerungsprotokoll) ist Bestandteil der IEEE-Spezifikation 802.3az, gemäß der mehrere physische Ports gebündelt werden können, sodass ein einziger logischer Kanal (LAG) entsteht. LAGs bewirken eine Vervielfachung der Bandbreite, erhöhte Flexibilität der Ports und Verknüpfungsredundanz zwischen zwei Geräten.

Es werden zwei Typen von LAGs unterstützt:

- **Statisch**: Eine LAG ist statisch, wenn bei ihr LACP deaktiviert wurde. Bei der Gruppe der Ports, die einer statischen LAG zugewiesen sind, handelt es sich immer um aktive Mitglieder. Nach der manuellen Erstellung einer LAG kann die LACP-Option nur dann hinzugefügt oder entfernt werden, wenn die LAG bearbeitet und ein Mitglied entfernt wird (das Mitglied kann vor der Anwendung wieder hinzugefügt werden). Die LACP-Schaltfläche ist dann zur Bearbeitung verfügbar.
- **Dynamisch**: Eine LAG ist dynamisch, wenn LACP für sie aktiviert ist. Bei der Gruppe der Ports, die einer dynamischen LAG zugewiesen sind, handelt es sich um Kandidatenports. LACP bestimmt, welche Kandidatenports aktive Mitgliedsports sind. Die nicht aktiven Mitgliedsports dienen als *Standby*-Ports, die bei Bedarf jederzeit einen ausfallenden aktiven Mitgliedsport ersetzen können.

Lastausgleich

Die Last des an eine LAG geleiteten Datenverkehrs wird auf die aktiven Mitgliedsports aufgeteilt, sodass eine effektive Bandbreite erzielt wird, die nahe an der aggregierten Bandbreite aller aktiven Mitgliedsports der LAG liegt.

Der Ausgleich der Datenlast zwischen den aktiven Mitgliedsports einer LAG wird über eine Hash-basierte Verteilungsfunktion verwaltet. Diese verteilt Unicast- und Multicast-Datenverkehr basierend auf den Paket-Header-Informationen für Schicht 2 oder Schicht 3.

Das Gerät unterstützt beim Lastenausgleich zwei Modi:

- **Nach MAC-Adressen**: Basierend auf der Quell-MAC-Adresse und der Ziel-MAC-Adresse der einzelnen Pakete.
- **Nach IP- und MAC-Adresse**: Basiert bei IP-Paketen auf der Quell-IP-Adresse und der Ziel-IP-Adresse und bei Nicht-IP-Paketen auf der Quell-MAC-Adresse und der Ziel-MAC-Adresse.

LAG-Verwaltung

Eine LAG wird vom System wie ein einzelner logischer Port behandelt. Dabei verfügt die LAG ähnlich wie ein normaler Port über Port-Attribute, wie Zustand und Geschwindigkeit.

Das Gerät unterstützt 32 LAGs mit bis zu acht Ports in einer LAG-Gruppe.

Jede LAG weist folgende Merkmale auf:

- Alle Ports in einer LAG müssen denselben Medientyp aufweisen.
- Damit ein Port zu einer LAG hinzugefügt werden kann, darf dieser zu keinem VLAN gehören außer zum Standard-VLAN.
- Ein Port darf immer nur einer LAG zugewiesen sein (nicht mehreren gleichzeitig).
- Einer statischen LAG dürfen höchstens acht Ports zugewiesen werden, und dynamische LAGs dürfen höchstens 16 potentielle Ports umfassen.
- Bei allen Ports in einer LAG muss die automatische Aushandlung deaktiviert sein. Für die LAG selbst kann die automatische Aushandlung aber aktiviert sein.
- Wenn ein Port einer LAG hinzugefügt wird, wird die Konfiguration der LAG auf den Port angewendet. Wenn der Port aus der LAG entfernt wird, wird wieder seine ursprüngliche Konfiguration angewendet.
- Von Protokollen wie Spanning Tree werden alle Ports in der LAG als ein einziger Port betrachtet.

Standardeinstellungen und Konfiguration

Ports sind standardmäßig weder Mitglieder einer LAG noch Kandidaten für Mitglieder einer LAG.

Workflow von statischen und dynamischen LAGs

Nach der manuellen Erstellung einer LAG kann LACP nur dann hinzugefügt oder entfernt werden, wenn die LAG bearbeitet wird und ein Mitglied entfernt wird. Erst dann ist die LACP-Schaltfläche zur Bearbeitung verfügbar.

Führen Sie zum Konfigurieren einer **statischen** LAG folgende Aktionen durch:

1. Deaktivieren Sie LACP für die LAG, um diese zu einer statischen LAG zu machen. Weisen Sie der statischen LAG bis zu acht aktive Mitgliedsports zu, indem Sie die Ports in der **Portliste** auswählen und in die Liste **LAG-Mitglieder** ziehen. Wählen Sie den Lastenausgleichsalgorithmus für die LAG aus. Führen Sie diese Aktionen auf der Seite „LAG-Verwaltung“ aus.
2. Konfigurieren Sie auf der Seite „LAG-Einstellungen“ verschiedene Aspekte der LAG, beispielsweise die Geschwindigkeit und die Flusssteuerung.

Führen Sie zum Konfigurieren einer **dynamischen** LAG folgende Aktionen durch:

1. Aktivieren Sie LACP für die LAG. Weisen Sie der dynamischen LAG bis zu 16 Kandidatenports zu, indem Sie auf der Seite „LAG-Verwaltung“ die Ports in der **Portliste** auswählen und in die Liste **LAG-Mitglieder** verschieben.
2. Konfigurieren Sie auf der Seite „LAG-Einstellungen“ verschiedene Aspekte der LAG, beispielsweise die Geschwindigkeit und die Flusssteuerung.
3. Legen Sie auf der Seite „LACP“ die LACP-Priorität und das Timeout für die Ports in der LAG fest.

Definieren der LAG-Verwaltung

Auf der Seite „LAG-Verwaltung“ werden die globalen und die LAG-spezifischen Einstellungen angezeigt. Außerdem können Sie auf dieser Seite die globalen Einstellungen konfigurieren sowie die gewünschte LAG auswählen und auf der Seite „LAG-Mitgliedschaft bearbeiten“ bearbeiten.

So wählen Sie den Lastenausgleichsalgorithmus für die LAG aus:

SCHRITT 1 Klicken Sie auf **Portverwaltung** > **Link-Aggregation** > **LAG-Verwaltung**.

SCHRITT 2 Wählen Sie unter **Lastausgleichsalgorithmus** einen der folgenden Algorithmen aus:

- *MAC-Adresse*: Der Lastenausgleich wird basierend auf der Quell-MAC-Adresse und der Ziel-MAC-Adresse der einzelnen Pakete durchgeführt.
- *IP/MAC-Adresse*: Der Lastenausgleich wird bei IP-Paketen basierend auf der IP-Quelladresse und der IP-Zieladresse und bei Nicht-IP-Paketen basierend auf der MAC-Quelladresse und der MAC-Zieladresse durchgeführt.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Der Lastenausgleichsalgorithmus wird in der aktuellen Konfigurationsdatei gespeichert.

So definieren Sie die Mitgliedsports oder Kandidatenports in einer LAG:

SCHRITT 1 Wählen Sie die zu konfigurierende LAG aus, und klicken Sie auf **Bearbeiten**.

Für jede LAG werden folgende Felder angezeigt (wobei nur Felder auf der Seite „Bearbeiten“ beschrieben werden)

- **Link State**: Ob der Port aktiv oder inaktiv ist.
- **Aktives Mitglied**: Aktive Ports in der LAG.
- **Standby-Mitglied**: Kandidatenports für diese LAG.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **LAG**: Wählen Sie die LAG-Nummer aus.
- **LAG-Name**: Geben Sie den LAG-Namen oder einen Kommentar ein.
- **LACP**: Wählen Sie diese Option aus, um LACP für die ausgewählte LAG zu aktivieren. Dadurch wird die LAG zu einer dynamischen LAG. Dieses Feld kann erst aktiviert werden, wenn Sie im nächsten Feld einen Port in die LAG verschoben haben.
- **Einheit/Slot**: Zeigt das Stacking-Mitglied an, für das LAG-Informationen definiert sind.
- **Port-Liste**: Ziehen Sie die Ports, die der LAG zugewiesen werden sollen, aus der **Port-Liste** in die Liste **LAG-Mitglieder**. Jeder statischen LAG können bis zu acht Ports zugewiesen werden und jeder dynamischen LAG 16 Ports. Dies sind Kandidatenports.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die LAG-Mitgliedschaft wird in der aktuellen Konfigurationsdatei gespeichert.

Konfigurieren von LAG-Einstellungen

Auf der Seite „LAG-Einstellungen“ wird eine Tabelle mit den aktuellen Einstellungen für alle LAGs angezeigt. Sie können die Einstellungen ausgewählter LAGs konfigurieren und außer Kraft gesetzte LAGs über die Seite „LAG-Einstellungen bearbeiten“ wieder aktivieren.

So konfigurieren Sie die LAG-Einstellungen oder reaktivieren eine außer Kraft gesetzte LAG:

SCHRITT 1 Klicken Sie auf **Portverwaltung** > **Link-Aggregation** > **LAG-Einstellungen**.

SCHRITT 2 Wählen Sie eine LAG aus und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **LAG**: Wählen Sie die LAG-ID-Nummer aus.
- **LAG-Typ**: Zeigt den Port-Typ der LAG an.
- **Beschreibung**: Geben Sie den LAG-Namen oder einen Kommentar ein.
- **Administrativer Status**: Legen Sie fest, ob die ausgewählte LAG aktiv oder nicht aktiv sein soll.
- **Betriebsstatus**: Zeigt an, ob die LAG momentan in Betrieb ist.
- **Leitungsstatus SNMP-Traps**: Wählen Sie diese Option aus, um die Generierung von SNMP-Traps zu aktivieren, die Benachrichtigungen bei Änderungen am Link-Status des Ports im LAG versenden.
- **Zeitbereich**: Wählen Sie diese Option, um den Zeitbereich zu aktivieren, in dem der Port den Status „Aktiv“ hat. Wenn der Zeitbereich nicht aktiv ist, ist der Port heruntergefahren. Ein konfigurierter Zeitbereich ist nur wirksam, wenn der Port administrativ aktiv ist. Wenn noch kein Zeitbereich definiert ist, klicken Sie auf **Bearbeiten**, um zur Seite „Zeitbereich“ zu wechseln.
- **Zeitbereichsname**: Wählen Sie das Profil, durch das der Zeitbereich spezifiziert wird.
- **Status des Betriebszeitbereichs**: Zeigt an, ob der Zeitbereich zurzeit aktiv oder inaktiv ist.
- **Vorübergehend deakt. LAG reaktivieren**: Mit dieser Option können Sie einen Port wieder aktivieren, falls die LAG durch die Sicherheitsoption zum Sperren von Ports oder durch die ACL-Konfigurationen deaktiviert wurde.
- **Autom. Aushandlung für Administration**: Mit dieser Option aktivieren oder deaktivieren Sie die automatische Aushandlung für die LAG. Die automatische Aushandlung ist ein Protokoll zwischen zwei Link-Partnern, mit dessen Hilfe eine LAG ihrem Partner ihre Übertragungsgeschwindigkeit und Flusssteuerungseinstellung ankündigen kann. (Die Standardeinstellung für die Flusssteuerung ist *deaktiviert*.) Es wird empfohlen, die automatische Aushandlung auf beiden Seiten eines aggregierten Links beizubehalten oder auf beiden Seiten zu deaktivieren. Dabei muss sichergestellt sein, dass die Link-Geschwindigkeiten identisch sind.
- **Autom. Aushandlung für Betrieb**: Zeigt die Einstellung für die automatische Aushandlung an.

- **Administrationsgeschwindigkeit**: Wählen Sie die Geschwindigkeit der LAG aus.
- **Betriebs-LAG-Geschwindigkeit**: Zeigt die aktuelle Geschwindigkeit an, mit der die LAG betrieben wird.
- **Administrationsankündigung**: Wählen Sie die Funktionen aus, die von der LAG angekündigt werden sollen. Folgende Optionen sind möglich:
  - *Max. Fähigkeit*: Alle LAG-Geschwindigkeiten und beide Duplex-Modi sind verfügbar.
  - *10 voll*: Die LAG kündigt eine Geschwindigkeit von 10 MBit/s an, und voller Duplexmodus wird verwendet.
  - *100 voll*: Die LAG kündigt eine Geschwindigkeit von 100 MBit/s an, und voller Duplexmodus wird verwendet.
  - *1000 voll*: Die LAG kündigt eine Geschwindigkeit von 1000 MBit/s an, und voller Duplexmodus wird verwendet.
  - *10000 voll*: Die LAG kündigt eine Geschwindigkeit von 10000 MBit/s an, und voller Duplexmodus wird verwendet.
- **Betriebsankündigung**: Zeigt den Staus der Administrationsankündigung an. Die LAG kündigt der benachbarten LAG ihre Funktionen an, um mit dem Aushandlungsprozess zu beginnen. Die möglichen Werte sind im Feld *Administrationsankündigung* angegeben.
- **Administrationsflusssteuerung**: Legen Sie die Flusssteuerung auf **Aktivieren** oder **Deaktivieren** fest oder aktivieren Sie **Autom. Aushandlung** für die Flusssteuerung der LAG.
- **Flusssteuerung in Betrieb**: Zeigt die aktuelle Einstellung für die Flusssteuerung an.
- **Geschützte LAG**: Wählen Sie diese Option, um die LAG als geschützten Port mit Schicht-2-Isolierung festzulegen. Details zu geschützten Ports und LAGs finden Sie in der Beschreibung der Portkonfiguration im Abschnitt **Festlegen der grundlegenden Portkonfiguration**.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Konfigurieren von LACP

Bei dynamischen Ports ist LACP aktiviert. LACP wird für jeden in der LAG definierten Kandidatenport ausgeführt.

Prioritäten und Regeln für LACP

Anhand der LACP-Systempriorität und der LACP-Portpriorität wird festgelegt, welche der Kandidatenports in einer dynamischen LAG, für die mehr als acht Kandidatenports konfiguriert wurden, als aktive Mitgliedsports dienen.

Die ausgewählten potentiellen Ports der LAG sind alle mit demselben Remote-Gerät verbunden. Sowohl die lokalen Switches als auch die Remote-Switches haben eine LACP-Systempriorität.

Mit dem folgenden Algorithmus wird bestimmt, ob LACP-Portprioritäten des lokalen Geräts oder des Remote-Geräts angewendet werden: Die LACP-Systempriorität des lokalen Geräts wird mit der LACP-Systempriorität des Remote-Geräts verglichen. Das Gerät mit der niedrigsten Priorität steuert die Auswahl des Kandidatenports für die LAG. Wenn beide Prioritäten gleich sind, werden die MAC-Adressen des lokalen Geräts und des Remote-Geräts miteinander verglichen. Die Priorität des Geräts mit der niedrigsten MAC-Adresse steuert die Auswahl des Kandidatenports für die LAG.

Eine dynamische LAG kann bis zu 16 Ethernet-Ports des gleichen Typs umfassen. Bis zu acht Ports können aktiv sein, und bis zu acht Ports können im Standby-Modus sein. Wenn eine dynamische LAG mehr als acht Ports umfasst, legt das Gerät auf der Steuerungsseite des Links mithilfe von Portprioritäten fest, welche Ports in der LAG gebündelt werden und welche Ports in den Hot-Standby-Modus versetzt werden. Die Portprioritäten auf dem anderen Gerät (dem nicht steuernden Ende des Links) werden ignoriert.

Zusätzlich gelten folgende Regeln bei der Auswahl der aktiven Ports oder Standby-Ports für dynamisches LACP:

- Alle Links, die mit einer unterschiedlichen Geschwindigkeit betrieben werden als mit der höchsten Geschwindigkeit eines aktiven Mitglieds oder die im Halbduplex-Modus arbeiten, dienen als Standby. Alle aktiven Ports in einer dynamischen LAG werden mit derselben Baud-Rate betrieben.
- Wenn die Port-LACP-Priorität des Links niedriger als die der momentan aktiven Link-Mitglieder ist und die Höchstanzahl für aktive Mitglieder bereits erreicht ist, wird der Link inaktiviert und in den Standby-Modus versetzt.

LACP ohne Link-Partner

Damit LACP eine LAG erstellen kann, müssen die Ports an beiden Enden des Links für LACP konfiguriert werden, sodass sie LACP-PDUs senden und empfangene PDUs verarbeiten.

In bestimmten Fällen kann jedoch ein Link-Partner vorübergehend nicht für LACP konfiguriert sein. Ein Beispiel für einen solchen Fall ist ein Link-Partner auf einem Gerät, das seine Konfiguration über das Autokonfigurationsprotokoll empfängt. Die Ports dieses Geräts sind noch nicht für LACP konfiguriert. Wenn der LAG-Link nicht hochgefahren werden kann, kann das Gerät nicht konfiguriert werden. Ein ähnlicher Fall liegt bei Computern mit zwei NICs vor, die über das Netzwerk gestartet werden (z. B. PXE) und ihre LAG-Konfiguration erst nach dem Hochfahren empfangen.

Wenn mehrere für LACP konfigurierte Ports konfiguriert sind und der Link an einem oder mehreren Ports hochgefahren wird, für diese Ports aber keine LACP-Antworten vom Link-Partner empfangen werden, wird der erste Port mit hochgefahrenem Link der LACP-LAG hinzugefügt und aktiviert (die anderen Ports werden zu Nichtkandidaten). Auf diese Weise kann das Nachbargerät beispielsweise seine IP-Adresse über DHCP und seine Konfiguration über die Autokonfiguration beziehen.

Festlegen der LACP-Parametereinstellungen

Auf der Seite „LACP“ können Sie die Kandidatenports für die LAG und die LACP-Parameters pro Port konfigurieren.

Wenn alle anderen Faktoren gleich sind und für eine LAG mehr potenzielle Ports konfiguriert wurden als die zulässige Höchstzahl aktiver Ports (8), wählt das Gerät aus der dynamischen LAG auf dem Gerät die Ports mit der höchsten Priorität als aktiv aus.

HINWEIS Für Ports, die nicht Mitglieder einer dynamischen LAG sind, ist die LACP-Einstellung nicht relevant.

So legen Sie die LACP-Einstellungen fest:

SCHRITT 1 Klicken Sie auf **Portverwaltung** > **Link-Aggregation** > **LACP**.

SCHRITT 2 Geben Sie die LACP-Systempriorität ein. Weitere Informationen hierzu finden Sie unter **Prioritäten und Regeln für LACP**.

SCHRITT 3 Wählen Sie einen Port aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 4 Geben Sie Werte für die folgenden Felder ein:

- **Port**: Wählen Sie die Nummer des Ports aus, dem Timeout- und Prioritätswerte zugewiesen werden.
- **LACP-Port-Priorität**: Geben Sie den LACP-Prioritätswert für den Port ein. Weitere Informationen hierzu finden Sie unter **Festlegen der LACP-Parametereinstellungen**.
- **LACP-Timeout**: Zeitintervall zwischen dem Senden und Empfangen aufeinanderfolgender LACP-PDUs. Wählen Sie aus, ob die periodischen Übertragungen von LACP-PDUs abhängig von der festgelegten LACP-Timeout-Voreinstellung mit einer **niedrigen** oder **hohen** Übertragungsrate ausgeführt werden sollen.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

UDLD

Weitere Informationen hierzu finden Sie unter **Portverwaltung: Unidirectional Link Detection**.

PoE

Weitere Informationen hierzu finden Sie unter **Portverwaltung: PoE**.

Konfigurieren von Green Ethernet

In diesem Kapitel wird die Green Ethernet-Funktion beschrieben, mit der auf dem Gerät Strom gespart werden kann.

Das Kapitel enthält die folgenden Abschnitte:

Green Ethernet (Übersicht)

Green Ethernet ist eine allgemeine Bezeichnung für eine Kombination von Funktionen für den Umweltschutz und zur Verringerung des Stromverbrauchs von Geräten. Im Unterschied zu EEE (Energy Efficient Ethernet) ist bei Green Ethernet die Energieerkennung für alle Geräte aktiviert, bei EEE hingegen nur für Gigabyte-Ports.

Mit der Green Ethernet-Funktion kann der Gesamtstromverbrauch auf verschiedene Arten reduziert werden:

- **Energieerkennungsmodus**: (nicht verfügbar auf SG500XG)Der Port wechselt bei inaktiven Links in den inaktiven Modus und spart dadurch Strom, während er weiterhin den administrativen Status „Oben“ (in Betrieb) beibehält. Das Umschalten von diesem Modus in den vollen Betriebsmodus geschieht schnell, ist transparent, und es gehen dabei keine Frames verloren. Dieser Modus wird sowohl von GE-Ports als auch von FE-Ports unterstützt.
- **Modus für kurze Reichweite**: Diese Funktion ermöglicht Stromeinsparungen bei kurzen Kabeln. Nach der Analyse der Kabellänge wird die Stromversorgung an die verschiedenen Kabellängen angepasst. Wenn ein Kabel kürzer als 50 m ist, verbraucht das Gerät beim Senden von Frames über das Kabel weniger Strom. Dadurch wird Energie gespart. Dieser Modus wird nur an RJ45-GE-Ports unterstützt und gilt nicht für Kombinationsports.

  Der Modus ist standardmäßig global deaktiviert. Er kann nicht aktiviert werden, wenn der EEE-Modus aktiviert ist (siehe unten).

Neben den oben genannten Green Ethernet-Funktionen bieten Geräte mit Unterstützung für GE-Ports außerdem die Funktion **802.3az Energy Efficient Ethernet (EEE)**. Mit EEE wird die Leistungsaufnahme reduziert, wenn am Port kein Verkehr vorhanden ist. Weitere Informationen hierzu finden Sie unter **802.3az Energy Efficient Ethernet-Funktion** (nur für GE-Modelle verfügbar).

EEE ist standardmäßig global aktiviert. Wenn EEE aktiviert ist, wird der Modus für kurze Reichweite an einem bestimmten Port deaktiviert. Wenn der Modus für kurze Reichweite aktiviert ist, wird EEE grau dargestellt.

Diese Modi werden pro Port ohne Berücksichtigung der LAG-Mitgliedschaft der Ports konfiguriert.

Die Geräte-LEDs sind Stromverbraucher. Da sich die Geräte meist in einem nicht besetzten Raum befinden, wäre es Energieverschwendung, diese LEDs leuchten zu lassen. Mit der Green Ethernet-Funktion können Sie die Port-LEDs (für Link, Geschwindigkeit und PoE) deaktivieren, wenn sie nicht benötigt werden, und sie bei Bedarf aktivieren (Fehlerbehebung, Herstellen von Verbindungen mit weiteren Geräten usw.).

Auf die LEDs in den Geräteabbildungen auf der Seite „Systemübersicht“ wirkt sich das Deaktivieren der LEDs nicht aus.

Sie können die Stromeinsparungen, den aktuellen Stromverbrauch und die kumulative Energieeinsparung überwachen. Der insgesamt eingesparte Strom kann als Prozentwert im Bezug auf den Strom betrachtet werden, der von den physischen Schnittstellen verbraucht worden wäre, wenn diese nicht im Green Ethernet-Modus betrieben worden wären.

Der eingesparte Strom bezieht sich nur auf Green Ethernet. Wie viel Strom mit EEE gespart wird, wird nicht angezeigt.

Energieeinsparung durch Deaktivieren der Port-LEDs

Die Funktion „Deaktivieren der Port-LEDs“ spart die von Geräte-LEDs verbrauchte Energie ein. Da sich die Geräte meist in einem nicht besetzten Raum befinden, wäre es Energieverschwendung, diese LEDs leuchten zu lassen. Mit der Green Ethernet-Funktion können Sie die Port-LEDs (für Link, Geschwindigkeit und PoE) deaktivieren, wenn sie nicht benötigt werden, und sie bei Bedarf aktivieren (Fehlerbehebung, Herstellen von Verbindungen mit weiteren Geräten usw.).

Auf die LEDs in den Geräteabbildungen auf der Seite „Systemübersicht“ wirkt sich das Deaktivieren der LEDs nicht aus.

Port-LEDs können auf der Seite „Green Ethernet –> Eigenschaften“ deaktiviert werden.

802.3az Energy Efficient Ethernet-Funktion

In diesem Abschnitt wird die EEE-Funktion (802.3az Energy Efficient Ethernet) beschrieben.

Die folgenden Themen werden behandelt:

- **802.3az EEE (Übersicht)**
- **Ankündigen der Aushandlungsfunktionen**
- **Erkennung auf Link-Ebene für 802.3az EEE**
- **Verfügbarkeit von 802.3az EEE**
- **Standardkonfiguration**
- **Interaktionen zwischen Funktionen**
- **Konfigurations-Workflow für 802.3az EEE**

802.3az EEE (Übersicht)

Mit 802.3az EEE kann Strom gespart werden, wenn am Link kein Verkehr vorhanden ist. Bei Green Ethernet wird der Stromverbrauch reduziert, wenn der Port nicht aktiv ist. Bei 802.3az EEE wird der Stromverbrauch reduziert, wenn der Port aktiv ist, ohne dass Verkehr vorhanden ist.

802.3az EEE wird nur für Geräte mit GE-Ports unterstützt.

Bei Verwendung von 802.3az EEE können Systeme auf beiden Seiten des Links Teile ihrer Funktionalität deaktivieren und in Zeiten ohne Verkehr Strom sparen.

802.3az EEE unterstützt den IEEE 802.3-MAC-Betrieb mit 100 MBit/s und 1000 MBit/s:

Die optimalen Parameter für beide Geräte werden mithilfe von LLDP ausgewählt. Wenn LLDP vom Link-Partner nicht unterstützt wird oder deaktiviert ist, kann 802.3az EEE zwar verwendet werden, befindet sich jedoch möglicherweise nicht im optimalen Betriebsmodus.

Die 802.3az EEE-Funktion wird mit einem Portmodus implementiert, der als Energiesparmodus im Leerlauf (Low Power Idle, LPI) bezeichnet wird. Wenn kein Verkehr vorhanden ist und diese Funktion für den Port aktiviert ist, wird der Port in den LPI-Modus versetzt, durch den die Leistungsaufnahme drastisch verringert wird.

Dies ist nur möglich, wenn beide Seiten einer Verbindung (Geräteport und Verbindung herstellendes Gerät) 802.3az EEE unterstützen. Wenn kein Verkehr vorhanden ist, senden beide Seiten Signale, aus denen hervorgeht, dass der Stromverbrauch reduziert wird. Wenn Signale von beiden Seiten empfangen werden, weist das Keep Alive-Signal darauf hin, dass sich die Ports im LPI-Modus befinden (und nicht den Status „Ausgefallen“ haben), und der Stromverbrauch wird reduziert.

Damit die Ports im LPI-Modus bleiben, muss das Keep Alive-Signal ständig von beiden Seiten empfangen werden.

Ankündigen der Aushandlungsfunktionen

Die 802.3az EEE-Unterstützung wird in der Phase der automatischen Aushandlung angekündigt. Mithilfe der automatischen Aushandlung kann ein verbundenes Gerät die vom Gerät auf der anderen Seite unterstützten Funktionen (Betriebsmodi) erkennen, die gemeinsamen Funktionen ermitteln und sich selbst für den gemeinsamen Betrieb konfigurieren. Die automatische Aushandlung wird beim Herstellen der Verbindung, auf Befehl über die Verwaltung oder bei Erkennung eines Verbindungsfehlers ausgeführt. Beim Verbindungsaufbau tauschen beide Link-Partner ihre 802.3az EEE-Funktionen aus. Wenn die automatische Aushandlung für ein Gerät aktiviert ist, funktioniert sie automatisch ohne Eingriff des Benutzers.

> **HINWEIS** Wenn die automatische Aushandlung für einen Port nicht aktiviert ist, wird EEE deaktiviert. Einzige Ausnahme: Bei einer Link-Geschwindigkeit von 1 GB wird EEE aktiviert, obwohl die automatische Aushandlung deaktiviert ist.

Erkennung auf Link-Ebene für 802.3az EEE

Zusätzlich zu den oben beschriebenen Funktionen werden die 802.3az EEE-Funktionen und -Einstellungen mithilfe von Frames angekündigt, die auf den organisationsspezifischen TLVs basieren, die in Anhang G des IEEE Std 802.1AB-Protokolls (LLDP) definiert sind. LLDP wird verwendet, um den 802.3az EEE-Betrieb nach Abschluss der automatischen Aushandlung weiter zu optimieren. Das 802.3az EEE-TLV wird verwendet, um die Dauer der Reaktivierungs- und Aktualisierungsvorgänge des Systems zu optimieren.

Verfügbarkeit von 802.3az EEE

Eine vollständige Liste mit Produkten, die EEE unterstützen, finden Sie in den Versionshinweisen.

Standardkonfiguration

Standardmäßig sind 802.3az EEE und EEE LLDP global und pro Port aktiviert.

Interaktionen zwischen Funktionen

Im Folgenden werden die 802.3az EEE-Interaktionen mit anderen Funktionen beschrieben.

- Wenn die automatische Aushandlung für den Port nicht aktiviert ist, ist der 802.3az EEE-Betrieb deaktiviert. Als Ausnahme zu dieser Regel wird bei einer Link-Geschwindigkeit von 1 GB EEE aktiviert, obwohl die automatische Aushandlung deaktiviert ist.
- Wenn 802.3az EEE aktiviert ist und der Port aktiviert wird, wird sofort der Betrieb gemäß dem Wert für die maximale Aufwachzeit des Ports aufgenommen.
- Auf der grafischen Benutzeroberfläche ist das EEE-Feld für den Port nicht verfügbar, wenn für diesen die Option „Modus für kurze Reichweite“ aktiviert ist.
- Wenn Sie die Portgeschwindigkeit des GE-Ports in 10 MBit/s ändern, wird 802.3az EEE deaktiviert. Dies wird nur bei GE-Modellen unterstützt.

Konfigurations-Workflow für 802.3az EEE

In diesem Abschnitt wird beschrieben, wie Sie die 802.3az EEE-Funktion konfigurieren und die zugehörigen Zähler anzeigen.

SCHRITT 1 Stellen Sie sicher, dass die automatische Aushandlung für den Port aktiviert ist, indem Sie die Seite **Portverwaltung > Porteinstellungen** öffnen.

a. Wählen Sie einen Port aus und öffnen Sie die Seite „Porteinstellung bearbeiten“.

b. Wählen Sie das Feld **Automatisch aushandeln** aus, um sicherzustellen, dass diese Funktion aktiviert ist.

SCHRITT 2 Stellen Sie sicher, dass **802.3 Energy Efficient Ethernet (EEE)** auf der Seite „Portverwaltung > Green Ethernet > Eigenschaften“ aktiviert ist (die Option ist standardmäßig aktiviert). Auf dieser Seite wird außerdem angezeigt, wie viel Strom gespart wurde.

SCHRITT 3 Stellen Sie sicher, dass 802.3az EEE für einen Port aktiviert ist, indem Sie die Seite „Green Ethernet > Porteinstellungen“ öffnen.

a. Wählen Sie einen Port aus und öffnen Sie die Seite „Porteinstellung bearbeiten“.

b. Aktivieren Sie den Modus **802.3 Energy Efficient Ethernet (EEE)** für den Port (die Option ist standardmäßig aktiviert).

c. Wählen Sie auf der Seite **802.3 Energy Efficient Ethernet (EEE) LLDP** aus, ob die Ankündigung der 802.3az EEE-Funktionen über LLDP aktiviert oder deaktiviert werden soll (die Option ist standardmäßig aktiviert).

SCHRITT 4 Zum Anzeigen von Informationen zu 802.3az EEE auf dem lokalen Gerät öffnen Sie die Seite „Administration > Discovery – LLDP > LLDP – Lokale Informationen“ und zeigen die Informationen im Block „802.3az Energy Efficient Ethernet (EEE)“ an.

SCHRITT 5 Um Informationen zu 802.3az EEE auf dem Remote-Gerät anzuzeigen, öffnen Sie die Seite „Administration > Discovery – LLDP > LLDP-Nachbarinformationen“ und zeigen die Informationen im Block „802.3az Energy Efficient Ethernet (EEE)“ an.

Globale Green Ethernet-Eigenschaften

Auf der Seite „Eigenschaften“ können Sie die Konfiguration des Green Ethernet-Modus für das Gerät anzeigen und ändern. Auf der Seite wird auch die aktuelle Stromeinsparung angezeigt.

So aktivieren Sie Green Ethernet und EEE und zeigen Stromeinsparungen an:

SCHRITT 1 Klicken Sie auf **Portverwaltung** > **Green Ethernet** > **Eigenschaften**.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **Energieerkennungsmodus**: (nicht verfügbar bei SG500XG) Standardmäßig deaktiviert. Klicken Sie auf das Kontrollkästchen, um die Funktion zu aktivieren.
- **Kurze Reichweite**: Hier können Sie den Modus für kurze Reichweite global aktivieren oder deaktivieren, falls am Gerät GE-Ports vorhanden sind.

  HINWEIS Wenn „Kurze Reichweite“ aktiviert ist, muss EEE deaktiviert sein.

- **Port-LEDs**: Wählen Sie diese Option aus, um die Port-LEDs zu aktivieren. Wenn sie deaktiviert sind, zeigen sie den Leitungsstatus, Aktivität usw. nicht an.
- **Stromeinsparungen**: Zeigt an, wie viel Strom prozentual durch den Green Ethernet-Modus und „Kurze Reichweite“ gespart wurde. Die angezeigten Stromeinsparungen beziehen sich nur auf den durch die Modi „Kurze Reichweite“ und „Energieerkennung“ gesparten Strom. Die EEE-Stromeinsparungen sind von Natur aus dynamisch, da sie auf der Portauslastung basieren, und werden daher nicht berücksichtigt. Die Berechnung der Energieeinsparung erfolgt durch Vergleichen des maximalen Energieverbrauchs ohne Energieeinsparungen mit dem aktuellen Energieverbrauch.

- **Kumulative Energieeinsparung**: Zeigt an, wie viel Strom seit dem letzten Neustart des Geräts eingespart wurde. Dieser Wert wird bei jedem Ereignis, das sich auf das Stromsparen auswirkt, aktualisiert.
- **802.3 Energy Efficient Ethernet (EEE)**: Hier können Sie den EEE-Modus global aktivieren oder deaktivieren (nur verfügbar, wenn am Gerät GE-Ports vorhanden sind).

SCHRITT 3 Klicken Sie auf **Zähler für Energieeinsparungen zurücksetzen**, um die Daten für „Energieeinsparung summiert“ zurückzusetzen.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Green Ethernet-Eigenschaften werden in die aktuelle Konfigurationsdatei geschrieben.

Green Ethernet-Eigenschaften für Ports

Auf der Seite „Porteinstellungen“ werden die aktuellen Green Ethernet- und EEE-Modi pro Port angezeigt. Auf der Seite „Porteinstellung bearbeiten“ können Sie Green Ethernet für einen Port konfigurieren. Damit die Green Ethernet-Modi für einen Port in Betrieb genommen werden können, müssen die entsprechenden Modi global auf der Seite „Eigenschaften“ aktiviert sein.

EEE-Einstellungen werden nur für Geräte mit GE-Ports angezeigt. EEE funktioniert nur, wenn für die Ports die automatische Aushandlung festgelegt ist. Als Ausnahme ist EEE auch bei deaktivierter automatischer Aushandlung funktionsfähig, sofern der Port 1 GB oder mehr unterstützt.

So legen Sie Green Ethernet-Einstellungen auf Port-Ebene fest:

SCHRITT 1 Klicken Sie auf **Portverwaltung** > **Green Ethernet** > **Porteinstellungen**.

Auf der Seite „Porteinstellungen“ wird Folgendes angezeigt:

- **Status der globalen Parameter**: Beschreibt die aktivierten Funktionen.

Für die einzelnen Ports werden folgende Felder beschrieben:

- **Port**: Die Port-Nummer.
- **Energieerkennung**: Status des Ports im Hinblick auf den Energieerkennungsmodus:
  - *Administrativ*: Zeigt an, ob der Energieerkennungsmodus aktiviert wurde.
  - *Betrieb*: Zeigt an, ob der Energieerkennungsmodus momentan ausgeführt wird.
  - *Grund*: Falls der Energieerkennungsmodus nicht ausgeführt wird, wird hier der Grund angezeigt.

- **Kurze Reichweite**: Status des Ports im Hinblick auf den Modus für kurze Reichweite:
  - *Administrativ*: Zeigt an, ob der Modus für kurze Reichweite aktiviert wurde.
  - *Betrieb*: Zeigt an, ob der Modus für kurze Reichweite momentan ausgeführt wird.
  - *Grund*: Falls der Modus für kurze Reichweite nicht ausgeführt wird, wird hier der Grund angezeigt.
  - *Kabellänge*: Zeigt die von VCT zurückgegebene Kabellänge in Metern an.

  HINWEIS Der Modus für kurze Reichweite wird nur an RJ45-GE-Ports unterstützt und gilt nicht für Kombinationsports.
- **802.3 Energy Efficient Ethernet (EEE)**: Der Status des Ports im Hinblick auf die EEE-Funktion:
  - *Administrativ*: Zeigt an, ob EEE aktiviert wurde.
  - *Operativ*: Zeigt an, ob EEE zurzeit am lokalen Port in Betrieb ist. Dies hängt davon ab, ob die Funktion aktiviert ist (Administrationsstatus), am lokalen Port aktiviert ist und dort in Betrieb ist.
  - *LLDP Administrativ*: Zeigt an, ob die Ankündigung von EEE-Zählern über LLDP aktiviert wurde.
  - *LLDP Operativ*: Zeigt an, ob die Ankündigung von EEE-Zählern über LLDP zurzeit in Betrieb ist.
  - *EEE-Support auf Remote*: Zeigt an, ob EEE vom Link-Partner unterstützt wird. EEE muss vom lokalen Link-Partner und vom Remote-Link-Partner unterstützt werden.

  HINWEIS Im Fenster werden für jeden Port die Einstellungen für kurze Reichweite, Energieerkennung und EEE angezeigt; die Einstellungen werden jedoch nur dann für einen Port aktiviert, wenn sie auch auf der Seite „Eigenschaften“ global aktiviert wurden. Informationen zum globalen Aktivieren von „Kurze Reichweite“ und EEE finden Sie unter **Globale Green Ethernet-Eigenschaften**.

SCHRITT 2 Wählen Sie einen **Port** aus und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Aktivieren oder deaktivieren Sie den **Energieerkennung**smodus für den Port.

SCHRITT 4 Aktivieren oder deaktivieren Sie den Modus für **kurze Reichweite** für den Port, wenn das Gerät über GE-Ports verfügt.

SCHRITT 5 Aktivieren oder deaktivieren Sie den Modus für **802.3 Energy Efficient Ethernet (EEE)** für den Port, wenn das Gerät über GE-Ports verfügt.

SCHRITT 6 Aktivieren oder deaktivieren Sie den Modus für **802.3 Energy Efficient Ethernet (EEE)** LLDP für den Port (Ankündigung von EEE-Funktionen über LLDP), wenn das Gerät über GE-Ports verfügt.

SCHRITT 7 Klicken Sie auf **Übernehmen**. Die Green Ethernet-Porteinstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

12

Portverwaltung: Unidirectional Link Detection

In diesem Abschnitt wird die Arbeitsweise der UDLD-Funktion (Unidirectional Link Detection) beschrieben.

Die folgenden Themen werden behandelt:

- **UDLD – Übersicht**
- **UDLD-Betrieb**
- **Verwendungshinweise**
- **Abhängigkeiten von anderen Funktionen**
- **Standardeinstellungen und Konfiguration**
- **Vorbereitung**
- **Allgemeine UDLD-Aufgaben**
- **Konfigurieren von UDLD**

UDLD – Übersicht

UDLD ist ein Schicht-2-Protokoll, mit dem Geräte, die über Fiber- oder Twisted-Pair-Ethernet-Kabel verbunden sind, unidirektionale Verbindungen erkennen können. Eine unidirektionale Verbindung tritt auf, wenn Datenverkehr von einem benachbarten Gerät auf einem lokalen Gerät eingeht, der Datenverkehr vom lokalen Gerät jedoch nicht auf dem benachbarten Gerät empfangen wird.

Mit UDLD können Ports erkannt werden, auf denen das benachbarte Gerät keinen Datenverkehr vom lokalen Gerät empfängt (unidirektionale Verbindung). Diese Ports werden heruntergefahren.

Alle verbundenen Geräte müssen UDLD unterstützen, damit das Protokoll die unidirektionalen Verbindungen erfolgreich erkennt. Wenn nur das lokale Gerät UDLD unterstützt, kann das Gerät den Status der Verbindung nicht ermitteln. In diesem Fall wird der Status der Verbindung auf „Undefiniert“ gesetzt. Der Benutzer kann konfigurieren, ob Ports im Status „Undefiniert“ heruntergefahren werden oder vielmehr Benachrichtigungen auslösen sollen.

UDLD-Betrieb

UDLD-Status und -Modi

Unter dem UDLD-Protokoll werden Ports die folgenden Status zugewiesen:

- **Erkennung**: Das System versucht zu bestimmen, ob es sich um eine bidirektionale oder unidirektionale Verbindung handelt. Dies ist ein vorübergehender Status.
- **Bidirektional**: Der Datenverkehr, der durch ein lokales Gerät gesendet wird, wird bekanntermaßen auf dem benachbarten Gerät empfangen, und Datenverkehr vom Nachbarn wird auf dem lokalen Gerät empfangen.
- **Herunterfahren**: Es handelt sich um eine unidirektionale Verbindung. Datenverkehr, der durch ein lokales Gerät gesendet wird, wird auf dessen benachbartem Gerät empfangen, Datenverkehr vom benachbarten Gerät wird jedoch nicht auf dem lokalen Gerät empfangen.
- **Undefiniert**: Das System kann den Status des Ports aus einem der folgenden Gründe nicht bestimmen:
  - Auf dem benachbarten Gerät wird UDLD nicht unterstützt.

    und

  - Das benachbarte Gerät empfängt keinen Datenverkehr vom lokalen Gerät.

  In diesem Fall hängt die UDLD-Aktion vom UDLD-Modus des Geräts ab. Siehe Erläuterungen unten.

UDLD unterstützt die folgenden Betriebsmodi:

- **Normal**

  Wurde der Verbindungsstatus des Ports auf „Bidirektional“ gesetzt und die UDLD-Informationen laufen ab, während die Verbindung auf dem Port noch aktiv ist, versucht UDLD, den Status des Ports wiederherzustellen.

- **Aggressiv**

  Wurde der Verbindungsstatus des Ports auf „Bidirektional“ gesetzt und die UDLD-Informationen laufen ab, fährt die UDLD-Funktion den Port nach längerer Zeit herunter, sobald die Fehlerhaftigkeit der Verbindung ermittelt werden kann. Der Port-Status für UDLD ist als „Undefiniert“ gekennzeichnet.

UDLD wird auf dem Port aktiviert, wenn Folgendes zutrifft:

- Der Port ist ein Fiber-Port, und UDLD ist global aktiviert.
- Der Port ist ein Kupfer-Port; in diesem Fall müssen Sie UDLD auf diesem Port implizit aktivieren.

Funktionsweise von UDLD

Wenn UDLD auf einem Port aktiviert ist, werden die folgenden Aktionen ausgeführt:

- UDLD initiiert den Erkennungsstatus auf dem Port.

  In diesem Status sendet UDLD regelmäßige Nachrichten über alle aktiven Schnittstellen an alle Nachbarn. Diese Nachrichten enthalten die Geräte-IDs aller bekannten Nachbarn. Es sendet diese Nachrichten auf Basis eines benutzerdefinierten Zeitplans.

- UDLD empfängt UDLD-Nachrichten von benachbarten Geräten. Es speichert diese Nachrichten, bis die definierte Zeit abgelaufen ist (das Dreifache der Nachrichtenzeit). Wenn eine neue Nachricht vor Ablauf der Zeit eingeht, werden die Informationen in der vorherigen Nachricht durch diese Nachricht überschrieben.

- Nach Ablauf der Zeit führt das Gerät die folgenden Aktionen mit den empfangenen Informationen aus:

  - **Die Nachbarnachricht enthält die lokale Gerät-ID**: Der Verbindungsstatus des Ports wird auf „Bidirektional“ gesetzt.

  - **Die Nachbarnachricht enthält keine lokale Gerät-ID**: Der Verbindungsstatus des Ports wird auf „Unidirektional“ gesetzt, und der Port wird heruntergefahren.

- Wenn UDLD-Nachrichten nicht vor Ablauf des definierten Zeitrahmens von einem benachbarten Gerät eingehen, wird der Verbindungsstatus des Ports auf „Undefiniert“ gesetzt, außerdem werden die folgenden Schritte ausgeführt:

  - **Das Gerät läuft im normalen UDLD-Modus:** Es wird eine Benachrichtigung gesendet.

  - **Das Gerät läuft im aggressiven UDLD-Modus:** Der Port wird heruntergefahren.

Während sich die Schnittstelle im bidirektionalen oder undefinierten Status befindet, sendet das Gerät regelmäßig eine Nachricht. Die oben genannten Schritte werden immer wieder ausgeführt.

Ein Port, der heruntergefahren wurde, kann auf der Seite „Portverwaltung > Wiederherstellungseinstellungen nach Fehlern“ manuell reaktiviert werden. Weitere Informationen finden Sie unter **Reaktivieren eines heruntergefahrenen Ports**.

Wenn eine Schnittstelle ausgefallen und UDLD aktiviert ist, entfernt das Gerät alle Nachbarinformationen und sendet mindestens eine UDLD-Nachricht an die Nachbarn, um diese darüber zu informieren, dass der Port nicht verfügbar ist. Sobald der Port reaktiviert wurde, wird der UDLD-Status in „Erkennung“ geändert.

UDLD wird auf einem Nachbarn nicht unterstützt oder wurde deaktiviert

Wenn UDLD auf einem Nachbarn nicht unterstützt wird oder deaktiviert wurde, werden keine UDLD-Nachrichten von diesem Nachbarn empfangen. In diesem Fall kann das Gerät nicht bestimmen, ob es sich bei der Verbindung um eine unidirektionale oder bidirektionale Verbindung handelt. Der Status der Schnittstelle wird in diesem Fall auf „Undefiniert“ gesetzt.

Reaktivieren eines heruntergefahrenen Ports

Sie können einen Port, der durch UDLD heruntergefahren wurde, wie folgt reaktivieren:

- **Automatisch**: Sie können das System auf der Seite „Portverwaltung > Wiederherstellungseinstellungen nach Fehlern“ so konfigurieren, dass Ports, die durch UDLD heruntergefahren wurden, automatisch reaktiviert werden. Wenn in diesem Fall ein Port durch UDLD heruntergefahren wird, wird er automatisch reaktiviert, wenn das automatische Wiederherstellungsintervall abläuft. UDLD wird anschließend wieder auf dem Port gestartet. Wenn die Verbindung weiterhin unidirektional ist, wird sie von UDLD erneut heruntergefahren, nachdem beispielsweise die UDLD-Ablaufzeit vorüber ist.
- **Manuell**: Sie können einen Port auf der Seite „Portverwaltung > Wiederherstellungseinstellungen nach Fehlern“ reaktivieren.

Verwendungshinweise

Cisco rät von der Aktivierung von UDLD auf Ports ab, die mit Geräten verbunden sind, auf denen UDLD nicht unterstützt wird oder deaktiviert ist. Das Senden von UDLD-Paketen auf einem Port, der mit einem Gerät verbunden ist, auf dem UDLD nicht unterstützt wird, führt zu erhöhtem Datenverkehr auf dem Port, ohne Vorteile zu bewirken.

Außerdem sollten Sie bei der Konfiguration von UDLD Folgendes berücksichtigen:

- Legen Sie das Nachrichtenintervall gemäß der Dringlichkeit fest, nach der Ports mit einer unidirektionalen Verbindung heruntergefahren werden müssen. Je geringer das Nachrichtenintervall, desto mehr UDLD-Pakete werden gesendet und analysiert, allerdings wird der Port auch eher heruntergefahren, wenn es sich um eine unidirektionale Verbindung handelt.
- Wenn Sie UDLD auf einem Kupfer-Port aktivieren möchten, müssen Sie es pro Port aktivieren. Die globale Aktivierung von UDLD ist nur auf Fiber-Ports möglich.
- Setzen Sie den UDLD-Modus auf „Normal“, wenn Ports nicht heruntergefahren werden sollen, es sei denn, Sie sind sich sicher, dass es sich um eine unidirektionale Verbindung handelt.
- Setzen Sie den UDLD-Modus auf „Aggressiv“, wenn sowohl unidirektionale als auch bidirektionale Verbindungen heruntergefahren werden sollen.

Abhängigkeiten von anderen Funktionen

- UDLD und Schicht-1-Protokoll

  Wenn UDLD auf einem Port aktiviert ist, wird UDLD auf diesem Port aktiv ausgeführt, während der Port betriebsbereit ist. Ist der Port nicht verfügbar, wird UDLD in den heruntergefahrenen Status versetzt. In diesem Status entfernt UDLD alle erlernten Nachbarn. Wenn der Port vom heruntergefahrenen Status in den verfügbaren Status wechselt, wird UDLD wieder aktiv ausgeführt.

- UDLD und Schicht-2-Protokolle

  UDLD wird auf einem Port unabhängig von anderen Schicht-2-Protokollen ausgeführt, die auf dem gleichen Port ausgeführt werden, z. B. STP oder LACP. So weist UDLD unabhängig vom STP-Status des Ports und unabhängig davon, ob der Port zu einem LAG gehört oder nicht, dem Port einen Status zu.

Standardeinstellungen und Konfiguration

Die folgenden Standardwerte sind für diese Funktion verfügbar:

- UDLD ist standardmäßig auf allen Ports auf dem Gerät deaktiviert.
- Das Standardnachrichtenintervall ist auf 15 Sekunden eingestellt.
- Die Standardablaufzeit beträgt 45 Sekunden (das Dreifache des Nachrichtenintervalls).
- Standard-Port-UDLD-Status:
  - Die Fiber-Schnittstellen befinden sich im Status „UDLD“.
  - Nicht-Fiber-Schnittstellen befinden sich im Status „Deaktiviert“.

Vorbereitung

Es sind keine Vorarbeiten erforderlich.

Allgemeine UDLD-Aufgaben

In diesem Abschnitt werden einige allgemeine Aufgaben zur Einrichtung von UDLD beschrieben.

Workflow 1: *So aktivieren Sie UDLD global auf Fiber-Ports:*

SCHRITT 1 Öffnen Sie die Seite **Portverwaltung** > **Globale UDLD-Einstellungen**.

a. Geben Sie das **Nachrichtenintervall** ein.

b. Geben Sie in das Feld „Fiber-Port-UDLD-Standardstatus“ entweder **Deaktiviert**, **Normal** oder **Aggressiv** als den globalen Status ein.

SCHRITT 2 Klicken Sie auf **Übernehmen**.

Workflow 2: *So ändern Sie die UDLD-Konfiguration eines Fiber-Ports oder aktivieren UDLD auf einem Kupfer-Port:*

SCHRITT 1 Öffnen Sie die Seite **Portverwaltung > Globale UDLD-Einstellungen**.

a. Wählen Sie einen Port aus.

b. Wählen Sie entweder **Standard**, **Deaktiviert**, **Normal** oder **Aggressiv** als UDLD-Status für den Port aus. Wenn Sie „Standard“ auswählen, empfängt der Port die globale Einstellung.

SCHRITT 2 Klicken Sie auf **Übernehmen**.

Workflow 3: *So reaktivieren Sie einen Port, nachdem er von UDLD heruntergefahren und die automatische Reaktivierung nicht konfiguriert wurde:*

SCHRITT 1 Öffnen Sie die Seite **Portverwaltung** > **Wiederherstellungseinstellungen nach Fehlern**.

a. Wählen Sie einen Port aus.

b. Klicken Sie auf **Reaktivieren**.

Konfigurieren von UDLD

Die UDLD-Funktion kann für alle Fiber-Ports gleichzeitig (auf der Seite „Globale UDLD-Einstellungen“) oder pro Port (auf der Seite „UDLD-Schnittstelleneinstellungen“) konfiguriert werden.

Globale UDLD-Einstellungen

Der Fiber-Port-UDLD-Standardstatus kann nur auf Fiber-Ports angewendet werden.

Das Feld „Nachrichtenintervall“ kann sowohl auf Kupfer- als auch auf Fiber-Ports angewendet werden.

So führen Sie eine globale Konfiguration von UDLD durch:

SCHRITT 1 Klicken Sie auf **Portverwaltung > UDLD** > **Globale UDLD-Einstellungen**.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **Nachrichtenzeit**: Geben Sie das Intervall zwischen zwei gesendeten UDLD-Nachrichten ein. Dieses Feld gilt für Fiber- und Kupfer-Ports.
- **Fiber-Port-UDLD-Standardstatus**: Dieses Feld gilt nur für **Fiber**-Ports. Den UDLD-Status für Kupfer-Ports müssen Sie individuell auf der Seite „UDLD-Schnittstelleneinstellungen“ konfigurieren. Die folgenden Status sind verfügbar:
  - *Deaktiviert*: UDLD ist auf allen Ports auf dem Gerät deaktiviert.
  - *Normal*: Das Gerät fährt eine Schnittstelle herunter, wenn es sich um eine unidirektionale Verbindung handelt. Wenn die Verbindung undefiniert ist, wird eine Nachricht gesendet.
  - *Aggressiv*: Das Gerät fährt eine Schnittstelle herunter, wenn es sich um eine unidirektionale Verbindung handelt. Wenn die Verbindung bidirektional ist, fährt das Gerät herunter, nachdem die UDLD-Informationen abgelaufen sind. Der Port-Status ist als „Undefiniert“ gekennzeichnet.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um die Einstellungen in der aktuellen Konfigurationsdatei zu speichern.

UDLD-Schnittstelleneinstellungen

Auf der Seite „UDLD-Schnittstelleneinstellungen“ können Sie den UDLD-Status für einen speziellen Port ändern. An dieser Stelle kann der Status sowohl für Kupfer- als auch für Fiber-Ports festgelegt werden.

Um einen bestimmten Satz mit Werten auf mehrere Ports zu kopieren, legen Sie den Wert für einen Port fest, und verwenden Sie die Schaltfläche **Kopieren**, um ihn auf die anderen Ports zu kopieren.

So konfigurieren Sie UDLD für eine Schnittstelle:

SCHRITT 1 Klicken Sie auf **Portverwaltung > UDLD** > **UDLD-Schnittstelleneinstellungen**.

Die Informationen werden für alle Ports angezeigt, auf denen UDLD aktiviert ist, oder, wenn Sie nur eine bestimmte Gruppe mit Ports gefiltert haben, werden die Informationen für diese Gruppe mit Ports angezeigt.

- **Port**: Die Port-ID.

- **UDLD-Status**: Die folgenden Status sind möglich:
  - *Deaktiviert*: UDLD ist auf allen Fiber-Ports auf dem Gerät deaktiviert.
  - *Normal*: Das Gerät fährt eine Schnittstelle herunter, wenn es erkennt, dass es sich um eine unidirektionale Verbindung handelt. Es sendet eine Benachrichtigung, wenn die Verbindung den Status „Undefiniert“ aufweist.
  - *Aggressiv*: Das Gerät fährt eine Schnittstelle herunter, wenn es sich um eine unidirektionale Verbindung handelt. Wenn die Verbindung bidirektional ist, fährt das Gerät herunter, nachdem die UDLD-Informationen abgelaufen sind. Der Port-Status ist als „Undefiniert“ gekennzeichnet.
- **Bidirektionaler Status**: Wählen Sie den Wert dieses Feldes für den ausgewählten Port aus. Die folgenden Status sind verfügbar:
  - *Erkennung*: Derzeit wird der letzte UDLD-Status des Ports bestimmt. Die Zeit ist seit der letzten Erkennung (falls eine Ablaufzeit definiert war) oder seit dem Zeitpunkt, an dem die Ausführung von UDLD auf dem Port begann, noch nicht abgelaufen, so dass der Status nicht bestimmt werden konnte.
  - *Bidirektional*: Der Datenverkehr, der durch das lokale Gerät gesendet wird, wird auf dem benachbarten Gerät empfangen, und Datenverkehr vom Nachbarn wird durch das lokale Gerät empfangen.
  - *Undefiniert*: Der Status der Verbindung zwischen dem Port und dessen verbundenen Port kann nicht bestimmt werden, da entweder keine UDLD-Nachricht empfangen wurde oder die UDLD-Nachricht keine lokale Geräte-ID enthielt.
  - *Deaktiviert*: UDLD wurde auf diesem Port deaktiviert.
  - *Herunterfahren*: Der Port wurde heruntergefahren, da es sich bei der Verbindung mit dem verbundenen Gerät um eine undefinierte Verbindung im aggressiven Modus handelt.
- **Anzahl der Nachbarn**: Die Anzahl der erkannten, verbundenen Geräte.

SCHRITT 2 Um den UDLD-Status für einen bestimmten Port zu ändern, wählen Sie ihn aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Ändern Sie den Wert für den UDLD-Status. Wenn Sie **Standard** auswählen, empfängt der Port den Wert des **Fiber-Port-UDLD-Standardstatus** auf der Seite „Globale UDLD-Einstellungen“.

SCHRITT 4 Klicken Sie auf **Übernehmen**, um die Einstellungen in der aktuellen Konfigurationsdatei zu speichern.

UDLD-Nachbarn

So zeigen Sie alle Geräte an, die mit dem lokalen Gerät verbunden sind:

SCHRITT 1 Klicken Sie auf **Portverwaltung > UDLD** > **UDLD-Nachbarn**.

Die folgenden Felder werden für alle UDLD-aktivierten Ports angezeigt:

- **Schnittstellenname**: Der Name des lokalen, UDLD-aktivierten Ports.
- **Nachbarinformationen:**
  - *Geräte-ID*: Die ID des Remote-Geräts.
  - *Geräte-MAC-Adresse*: Die MAC-Adresse des Remote-Geräts.
  - *Gerätename*: Der Name des Remote-Geräts.
  - *Port-ID*: Der Name des Remote-Ports.
- **Status**: Der Status der Verbindung zwischen dem lokalen und dem benachbarten Gerät auf dem lokalen Port. Folgende Werte sind möglich:
  - *Erkennung*: Derzeit wird der letzte UDLD-Status des Ports bestimmt. Die Zeit ist seit der letzten Erkennung (falls eine Ablaufzeit definiert war) oder seit dem Zeitpunkt, an dem die Ausführung von UDLD auf dem Port begann, noch nicht abgelaufen, so dass der Status nicht bestimmt werden konnte.
  - *Bidirektional*: Der Datenverkehr, der durch das lokale Gerät gesendet wird, wird auf dem benachbarten Gerät empfangen, und Datenverkehr vom Nachbarn wird durch das lokale Gerät empfangen.
  - *Undefiniert*: Der Status der Verbindung zwischen dem Port und dessen verbundenen Port kann nicht bestimmt werden, da entweder keine UDLD-Nachricht empfangen wurde oder die UDLD-Nachricht keine lokale Geräte-ID enthielt.
  - *Deaktiviert*: UDLD wurde auf diesem Port deaktiviert.
  - *Herunterfahren*: Der Port wurde heruntergefahren, da es sich bei der Verbindung mit dem verbundenen Gerät um eine undefinierte Verbindung im aggressiven Modus handelt.
- **Ablaufzeit des Nachbarn (Sek.)**: Zeigt die Zeit an, die vergehen muss, bevor der Port-UDLD-Status erkannt wird. Hierbei handelt es sich um das Dreifache des Nachrichtenintervalls.
- **Nachrichtenzeit des Nachbarn (Sek.)**: Zeigt das Intervall zwischen UDLD-Nachrichten an.

13

Smartport

In diesem Dokument wird die Smartport-Funktion beschrieben.

Das Kapitel enthält die folgenden Themen:

Übersicht

Mit der Smartport-Funktion können Sie gemeinsame Konfigurationen bequem speichern und gemeinsam nutzen. Ein Smartport-Makro wird auf mehrere Schnittstellen angewendet, damit diese die gleiche Konfiguration verwenden. Ein Smartport-Makro ist ein Skript mit CLI-Befehlen (Command Line Interface, Kommandozeile).

Ein Smartport-Makro kann anhand des Makronamens oder anhand des dem Makro zugeordneten Smartport-Typs auf eine Schnittstelle angewendet werden. Die Anwendung eines Smartport-Makros anhand des Makronamens ist nur über die CLI möglich. Details hierzu finden Sie im CLI-Handbuch.

Es gibt zwei Möglichkeiten, ein Smartport-Makro anhand des Smartport-Typs auf eine Schnittstelle anzuwenden:

- **Statischer Smartport**: Sie weisen einer Schnittstelle manuell einen Smartport-Typ zu. Daraufhin wird das entsprechende Smartport-Makro auf die Schnittstelle angewendet.
- **Auto-Smartport**: Auto-Smartport wartet mit dem Anwenden einer Konfiguration, bis ein Gerät mit der Schnittstelle verbunden wird. Wenn an einer Schnittstelle ein Gerät erkannt wird, wird automatisch das Smartport-Makro (falls zugewiesen) angewendet, das dem Typ des verbundenen Geräts entspricht.

Die Smartport-Funktion besteht aus verschiedenen Komponenten und arbeitet mit anderen Funktionen des Geräts zusammen. Diese Komponenten und Funktionen werden in den folgenden Abschnitten beschrieben:

- Smartport, Smartport-Typ und Smartport-Makros werden in diesem Abschnitt beschrieben.
- Voice-VLAN und Smartport werden im Abschnitt **Voice-VLAN** beschrieben.
- LLDP/CDP für Smartport wird im Abschnitt **Konfigurieren von LLDP** bzw. **Konfigurieren von CDP** beschrieben.

Außerdem werden im Abschnitt **Allgemeine Smartport-Aufgaben** typische Workflows beschrieben.

Was ist ein Smartport?

Ein Smartport ist eine Schnittstelle, für die ein integriertes (oder benutzerdefiniertes) Makro ausgeführt werden kann. Diese Makros sollen eine schnelle Konfiguration des Geräts ermöglichen, um so die Kommunikationsanforderungen zu unterstützen und die Funktionen verschiedener Arten von Netzwerkgeräten zu nutzen. Die Anforderungen für den Netzwerkzugriff und für QoS hängen davon ab, ob die Schnittstelle mit einem IP-Telefon, einem Drucker oder einem Router und/oder einem Zugriffspunkt (Access Point, AP) verbunden ist.

Smartport-Typen

Smartport-Typen beziehen sich auf die Typen der Geräte, die mit Smartports verbunden werden oder verbunden werden sollen. Das Gerät unterstützt folgende Smartport-Typen:

- Drucker
- Desktop
- Gast
- Server
- Host
- IP-Kamera
- IP-Telefon
- IP-Telefon + Desktop
- Switch
- Router
- WLAN-Zugriffspunkt

Die Namen der Smartport-Typen entsprechen jeweils dem mit der Schnittstelle verbundenen Gerätetyp. Jedem Smartport-Typ sind zwei Smartport-Makros zugeordnet. Ein Makro (auch „das Makro“ genannt) führt die gewünschte Konfiguration aus. Mit dem anderen Makro („Anti-Makro“) kann die durch das Makro vorgenommene Konfiguration rückgängig gemacht werden, wenn sich der Smartport-Typ der Schnittstelle ändert.

Sie können ein Smartport-Makro mit folgenden Methoden ausführen:

- Anhand des zugeordneten Smartport-Typs
- Statisch über ein Smartport-Makro anhand des Namens (nur über die CLI)

Ein Smartport-Makro kann statisch über die CLI und die grafische Benutzeroberfläche anhand des Smartport-Typs und dynamisch über die Auto-Smartport-Funktion angewendet werden. Auto-Smartport leitet die Smartport-Typen von den verbundenen Geräten basierend auf CDP-Funktionen, LLDP-Systemfunktionen und/oder LLDP MED-Funktionen ab.

Nachfolgend werden die Beziehungen zwischen Smartport-Typen und Auto-Smartport beschrieben.

Smartport-Typ	Von Auto-Smartport unterstützt	Standardmäßig von Auto-Smartport unterstützt
Unbekannt	Nein	Nein
Default	Nein	Nein
Drucker	Nein	Nein
Desktop	Nein	Nein
Gast	Nein	Nein
Server	Nein	Nein
Host	Ja	Nein
IP-Kamera	Nein	Nein
IP-Telefon	Ja	Ja
IP-Telefon + Desktop	Ja	Ja
Switch	Ja	Ja
Router	Ja	Nein
WLAN-Zugriffspunkt	Ja	Ja

Spezielle Smartport-Typen

Es gibt zwei spezielle Smartport-Typen: *Standard* und *Unbekannt*. Diesen beiden Typen sind keine Makros zugeordnet. Sie dienen vielmehr zum Angeben des Smartport-Status der Schnittstelle.

Nachfolgend werden diese speziellen Smartport-Typen beschrieben:

- **Default**

  Eine Schnittstelle, der (noch) kein Smartport-Typ zugewiesen ist, hat den Smartport-Status „Standard“.

  Wenn Auto-Smartport einer Schnittstelle einen Smartport-Typ zuweist und die Schnittstelle nicht dauerhaft für Auto-Smartport konfiguriert ist, wird ihr Smartport-Typ in den folgenden Fällen mit dem Status „Standard“ erneut initialisiert:

  - Für die Schnittstelle wird ein Link-Aktivierungs- bzw. Link-Deaktivierungsvorgang ausgeführt.
  - Das Gerät wird neu gestartet.
  - Alle mit der Schnittstelle verbundenen Geräte sind fällig geworden. Dieser Zustand ist als Fehlen von CDP- und/oder LLDP-Ankündigungen vom Gerät über einen vorgegebenen Zeitraum definiert.

- **Unbekannt**

  Wenn ein Smartport-Makro auf eine Schnittstelle angewendet wird und ein Fehler auftritt, wird der Schnittstelle der Status „Unbekannt“ zugewiesen. In diesem Fall können die Funktionen Smartport und Auto-Smartport erst für die Schnittstelle verwendet werden, wenn Sie den Fehler korrigieren und mit der Aktion Zurücksetzen (auf den Seiten für die Schnittstelleneinstellungen) den Smartport-Status zurücksetzen.

  Tipps für die Fehlerbehebung finden Sie im Abschnitt **Allgemeine Smartport-Aufgaben**.

  HINWEIS In diesem Abschnitt wird der Begriff „fällig“ zum Beschreiben der LLDP- und CDP-Nachrichten im Hinblick auf ihre TTL verwendet. Wenn Auto-Smartport aktiviert ist, der dauerhafte Status deaktiviert ist und keine weiteren CDP- oder LLDP-Nachrichten an der Schnittstelle empfangen werden, bevor beide TTLs der neuesten CDP- und LLDP-Pakete auf 0 zurückgehen, wird das Anti-Makro ausgeführt und der Smartport-Typ wird auf den Standardwert zurückgesetzt.

Smartport-Makros

Ein Smartport-Makro ist ein Skript mit CLI-Befehlen, das eine Schnittstelle für ein bestimmtes Netzwerkgerät konfiguriert.

Smartport-Makros sind nicht mit globalen Makros zu verwechseln. Globale Makros konfigurieren das Gerät global, während Smartport-Makros nur für die Schnittstelle gelten, auf der sie ausgeführt werden.

Die Makroquelle kann mit dem Befehl „show parser macro name [Makroname]“ im privilegierten Ausführungsmodus der CLI ermittelt werden oder indem Sie auf der Seite „Smartport-Typ-Einstellungen“ auf die Schaltfläche **Makro-Quelle anzeigen** klicken.

Jedem Smartport-Typ wird ein Paar aus Makro und entsprechendem Anti-Makro zugeordnet. Mit dem Makro wenden Sie die Konfiguration an und mit dem Anti-Makro entfernen Sie sie.

Es gibt zwei Arten von Smartport-Makros:

- **Integriert**: Diese Makros werden vom System bereitgestellt. Mit einem Makro wenden Sie das Konfigurationsprofil an und mit dem anderen entfernen Sie es. Die Makronamen der integrierten Smartport-Makros und der zugeordnete Smartport-Typ lauten wie folgt:
  - makro-name (Beispiel: „printer“)
  - no_macro-name (Beispiel: „no_printer“)

- **Benutzerdefiniert**: Diese Makros werden von den Benutzern geschrieben. Weitere Informationen hierzu finden Sie im *CLI-Referenzhandbuch*. Wenn Sie ein benutzerdefiniertes Makro einem Smartport-Typ zuordnen möchten, müssen Sie auch das Anti-Makro definieren.
  - smartport-type-name (Beispiel: „my_printer“)
  - no_smartport-type-name (Beispiel: „no_my_printer“)

Auf der Seite Smartport-Typeinstellungen bearbeiten können Sie Smartport-Makros an Smartport-Typen binden.

Eine Liste der integrierten Smartport-Makros für die einzelnen Gerätetypen finden Sie unter **Integrierte Smartport-Makros**.

Anwenden eines Smartport-Typs auf eine Schnittstelle

Wenn Sie Smartport-Typen auf Schnittstellen anwenden, werden die Smartport-Typen und die Konfiguration in den zugeordneten Smartport-Makros in der aktuellen Konfigurationsdatei gespeichert. Wenn der Administrator die aktuelle Konfigurationsdatei in der Startkonfigurationsdatei speichert, wendet das Gerät die Smartport-Typen und Smartport-Makros nach dem Neustart wie folgt auf die Schnittstellen an:

- Wenn in der Startkonfigurationsdatei kein Smartport-Typ für eine Schnittstelle angegeben ist, wird der Smartport-Typ auf „Standard“ festgelegt.
- Wenn in der Startkonfigurationsdatei ein statischer Smartport-Typ angegeben ist, wird der Smartport-Typ der Schnittstelle auf diesen statischen Typ festgelegt.
- Wenn in der Startkonfigurationsdatei ein Smartport-Typ angegeben ist, der dynamisch von Auto-Smartport zugewiesen wurde, gilt Folgendes:
  - Wenn der globale Auto-Smartport-Betriebsstatus, der Auto-Smartport-Status der Schnittstelle sowie der dauerhafte Status **aktiviert** sind, wird der Smartport-Typ auf diesen dynamischen Typ festgelegt.
  - Anderenfalls wird das entsprechende Anti-Makro angewendet und der Schnittstellenstatus wird auf „Standard“ festgelegt.

Makrofehler und der Zurücksetzungsvorgang

Bei einem Smartport-Makro können Fehler auftreten, wenn ein Konflikt zwischen der vorhandenen Konfiguration der Schnittstelle und einem Smartport-Makro vorliegt.

Wenn bei einem Smartport-Makro ein Fehler auftritt, wird eine Syslog-Nachricht mit den folgenden Parametern gesendet:

- Portnummer
- Smartport-Typ
- Zeilennummer des fehlgeschlagenen CLI-Befehls im Makro

Wenn bei einem Smartport-Makro Fehler an einer Schnittstelle auftreten, wird der Status der Schnittstelle auf *Unbekannt* festgelegt. Den Grund für den Fehler können Sie auf der Seite Schnittstelleneinstellungen im Popup-Fenster **Diagnose anzeigen** anzeigen.

Wenn Sie die Quelle des Problems ermittelt und die vorhandene Konfiguration oder das Smartport-Makro korrigiert haben, müssen Sie die Schnittstelle zurücksetzen, damit der Smartport-Typ erneut angewendet werden kann (auf den Seiten für die Schnittstelleneinstellungen). Tipps für die Fehlerbehebung finden Sie im Abschnitt **Allgemeine Smartport-Aufgaben**.

Funktionsweise von Smartport

Sie können ein Smartport-Makro anhand des Makronamens oder anhand des mit dem Makro verknüpften Smartport-Typs auf eine Schnittstelle anwenden. Die Anwendung eines Smartport-Makros anhand des Makronamens ist nur über die CLI möglich. Details hierzu finden Sie im CLI-Handbuch.

Da Smartport-Typen unterstützt werden, die Geräten entsprechen, die keine Erkennung über CDP und/oder LLDP zulassen, müssen Sie diese Smartport-Typen den gewünschten Schnittstellen statisch zuweisen. Navigieren Sie hierzu zur Seite Smartport-Schnittstelleneinstellungen, aktivieren Sie das Optionsfeld für die gewünschte Schnittstelle und klicken Sie auf **Bearbeiten**. Wählen Sie dann den zuzuweisenden Smartport-Typ aus und passen Sie die Parameter nach Bedarf an. Klicken Sie dann auf **Übernehmen**.

Es gibt zwei Möglichkeiten, ein Smartport-Makro anhand des Smartport-Typs auf eine Schnittstelle anzuwenden:

- **Statischer Smartport**

  Sie weisen einer Schnittstelle manuell einen Smartport-Typ zu. Das entsprechende Smartport-Makro wird auf die Schnittstelle angewendet. Auf der Seite Smartport-Schnittstelleneinstellungen können Sie einer Schnittstelle manuell einen Smartport-Typ zuweisen.

- **Auto-Smartport**

  Wenn an einer Schnittstelle ein Gerät erkannt wird, wird gegebenenfalls automatisch das Smartport-Makro angewendet, das dem Typ des verbundenen Geräts entspricht. Auto-Smartport ist standardmäßig global und auf Schnittstellenebene aktiviert.

In beiden Fällen wird das zugeordnete Anti-Makro ausgeführt, wenn der Smartport-Typ von der Schnittstelle entfernt wird, und das Anti-Makro wird auf genau die gleiche Weise ausgeführt, sodass die gesamte Schnittstellenkonfiguration entfernt wird.

Auto-Smartport

Damit Auto-Smartport Schnittstellen automatisch Smartport-Typen zuweist, muss die Auto-Smartport-Funktion global und an den Schnittstellen, die mit Auto-Smartport konfiguriert werden sollen, aktiviert sein. Standardmäßig ist Auto-Smartport aktiviert und kann alle Schnittstellen konfigurieren. Der den einzelnen Schnittstellen zugewiesene Smartport-Typ wird durch die an den einzelnen Schnittstellen empfangenen CDP- und LLDP-Pakete bestimmt.

- Wenn mehrere Geräte mit einer Schnittstelle verbunden sind, wird nach Möglichkeit ein für alle Geräte geeignetes Konfigurationsprofil angewendet.
- Wenn ein Gerät fällig ist (keine Ankündigungen von anderen Geräten mehr empfängt), wird die Schnittstellenkonfiguration gemäß dem dauerhaften Status geändert. Wenn der dauerhafte Status aktiviert ist, wird die Schnittstellenkonfiguration beibehalten. Anderenfalls wird der Smartport-Typ auf „Standard“ zurückgesetzt.

Aktivieren von Auto-Smartport

Auf der Seite Eigenschaften haben Sie folgende Möglichkeiten, Auto-Smartport zu aktivieren:

- **Aktiviert**: Mit dieser Option wird Auto-Smartport manuell aktiviert und sofort verwendet.
- **Aktivieren nach Auto-Voice-VLAN**: Mit dieser Option wird Auto-Smartport aktiviert, jedoch nur, wenn Auto-Voice-VLAN aktiviert ist und verwendet wird. „Aktivieren nach Auto-Voice-VLAN“ ist die Standardeinstellung.

HINWEIS Sie müssen Auto-Smartport nicht nur global, sondern auch für die gewünschte Schnittstelle aktivieren. Auto-Smartport ist standardmäßig für alle Schnittstellen aktiviert.

Weitere Informationen zum Aktivieren von Auto-Voice-VLAN finden Sie unter **Voice-VLAN**.

Identifizieren des Smartport-Typs

Wenn Auto-Smartport global (auf der Seite Eigenschaften) und für eine Schnittstelle (auf der Seite Schnittstelleneinstellungen) aktiviert ist, wendet das Gerät ein Smartport-Makro anhand des Smartport-Typs des verbundenen Geräts an. Auto-Smartport leitet die Smartport-Typen der verbundenen Geräte aus den CDP- und/oder LLDP-Ankündigungen der Geräte ab.

Wenn beispielsweise ein IP-Telefon mit einem Port verbunden ist, überträgt es CDP- oder LLDP-Pakete, in denen seine Funktionen angekündigt werden. Nach dem Empfang dieser CDP- und/oder LLDP-Pakete leitet das Gerät den entsprechenden Smartport-Typ für das Telefon ab und wendet das passende Smartport-Makro auf die Schnittstelle an, mit der das IP-Telefon verbunden ist.

Sofern Auto-Smartport nicht dauerhaft für eine Schnittstelle aktiviert ist, werden der Smartport-Typ und die sich ergebende von Auto-Smartport angewendete Konfiguration entfernt, wenn die verbundenen Geräte fällig werden, ihre Verbindungen getrennt werden, die Geräte neu gestartet werden oder widersprüchliche Funktionen empfangen werden. Die Fälligkeitszeiten werden anhand fehlender CDP- und/oder LLDP-Ankündigungen vom Gerät über einen bestimmten Zeitraum bestimmt.

Identifizieren von Smartport-Typen mithilfe von CDP/LLDP-Informationen

Das Gerät erkennt den Typ des mit dem Port verbundenen Geräts anhand der CDP/LLDP-Funktionen.

Diese Zuordnung wird in den folgenden Tabellen gezeigt:

Zuordnung von CDP-Funktionen zu Smartport-Typen

Funktionsname	CDP-Bit	Smartport-Typ
Router	0x01	Router
TB-Bridge	0x02	WLAN-Zugriffspunkt
SR-Bridge	0x04	Ignorieren
Switch	0x08	Switch
Host	0x10	Host
Bedingte IGMP-Filterung	0x20	Ignorieren
Repeater	0x40	Ignorieren
VoIP-Telefon	0x80	IP-Telefon
Remote verwaltetes Gerät	0x100	Ignorieren
CAST-Telefonport	0x200	Ignorieren
2-Port-MAC-Relais	0x400	Ignorieren

Zuordnung von LLDP-Funktionen zu Smartport-Typen

Funktionsname	LLDP-Bit	Smartport-Typ
Sonstige	1	Ignorieren
Repeater IETF RFC 2108	2	Ignorieren
MAC-Bridge IEEE Std. 802.1D	3	Switch
WLAN-Zugriffspunkt IEEE Std. 802.11 MIB	4	WLAN-Zugriffspunkt
Router IETF RFC 1812	5	Router
Telefon IETF RFC 4293	6	IP-Telefon
DOCSIS-Kabelgerät IETF RFC 4639 und IETF RFC 4546	7	Ignorieren
Nur Station IETF RFC 4293	8	Host
C-VLAN-Komponente einer VLAN-Bridge IEEE Std 802.1Q	9	Switch
S-VLAN-Komponente einer VLAN-Bridge IEEE Std 802.1Q	10	Switch
2-Port-MAC-Relais (TPMR) IEEE Std 802.1Q	11	Ignorieren
Reserviert	12-16	Ignorieren

HINWEIS Wenn nur die Bits für IP-Telefon und Host festgelegt sind, entspricht der Smartport-Typ „IP-Telefon + Desktop“.

Mehrere mit dem Port verbundene Geräte

Das Gerät leitet den Smartport-Typ eines verbundenen Geräts von den Funktionen ab, die das Gerät in seinen CDP- und/oder LLDP-Paketen ankündigt.

Wenn mehrere Geräte über eine Schnittstelle mit dem Gerät verbunden sind, betrachtet Auto-Smartport bei der Zuweisung des richtigen Smartport-Typs jede über diese Schnittstelle empfangene Funktionsankündigung. Die Zuweisung basiert auf dem folgenden Algorithmus:

- Wenn alle Geräte an der Schnittstelle die gleiche Funktion ankündigen (kein Konflikt), wird der entsprechende Smartport-Typ auf die Schnittstelle angewendet.
- Wenn eines der Geräte ein Switch ist, wird der Smartport-Typ *Switch* verwendet.
- Wenn eines der Geräte ein Zugriffspunkt ist, wird der Smartport-Typ *WLAN-Zugriffspunkt* verwendet.

- Wenn eines der Geräte ein IP-Telefon und ein anderes Gerät ein Host ist, wird der Smartport-Typ *IP-Telefon + Desktop* verwendet.
- Wenn eines der Geräte ein IP-Telefon-Desktop und das andere ein IP-Telefon oder Host ist, wird der Smartport-Typ *IP-Telefon + Desktop* verwendet.
- In allen anderen Fällen wird der Smartport-Typ „Standard“ verwendet.

Weitere Informationen zu LLDP/CDP finden Sie im Abschnitt **Konfigurieren von LLDP** bzw. **Konfigurieren von CDP**.

Dauerhafte Auto-Smartport-Schnittstelle

Wenn der dauerhafte Status für eine Schnittstelle aktiviert ist, bleiben Smartport-Typ und Konfiguration, die bereits dynamisch von Auto-Smartport zugewiesen wurden, auch dann erhalten, wenn das verbundene Gerät fällig, die Schnittstelle deaktiviert und das Gerät neu gestartet wird (sofern die Konfiguration gespeichert wurde). Der Smartport-Typ und die Konfiguration der Schnittstelle werden erst geändert, wenn Auto-Smartport ein verbundenes Gerät mit einem anderen Smartport-Typ erkennt. Wenn der dauerhafte Status einer Schnittstelle deaktiviert ist, wird die Schnittstelle auf den Standard-Smartport-Typ zurückgesetzt, wenn das verbundene Gerät fällig, die Schnittstelle deaktiviert oder das Gerät neu gestartet wird. Wenn Sie den dauerhaften Status für eine Schnittstelle aktivieren, entfällt die ansonsten auftretende Verzögerung für die Geräteerkennung.

HINWEIS Die Dauerhaftigkeit der auf die Schnittstellen angewendeten Smartport-Typen ist nur dann zwischen Neustarts wirksam, wenn die aktuelle Konfiguration mit dem auf die Schnittstellen angewendeten Smartport-Typ in der Startkonfigurationsdatei gespeichert ist.

Fehlerbehandlung

Wenn ein Smartport-Makro nicht auf eine Schnittstelle angewendet werden kann, können Sie den Fehler auf der Seite Schnittstelleneinstellungen untersuchen, den Port zurücksetzen und das Makro erneut anwenden, sobald Sie den Fehler auf den Seiten Schnittstelleneinstellungen und Schnittstelleneinstellungen bearbeiten behoben haben.

Standardkonfiguration

Smartport ist immer verfügbar. Auto-Smartport wird standardmäßig durch Auto-Voice-VLAN aktiviert, ist darauf angewiesen, dass CDP und LLDP den Smartport-Typ verbundener Geräte erkennen und erkennt die Smartport-Typen „IP-Telefon“, „IP-Telefon + Desktop“, „Switch“ und „WLAN-Zugriffspunkt“.

Eine Beschreibung der Werkseinstellungen für die Sprachfunktionen finden Sie unter **Voice-VLAN**.

Beziehungen zu anderen Funktionen und Abwärtskompatibilität

Auto-Smartport ist standardmäßig aktiviert und kann deaktiviert werden. Telefonie-OUI kann nicht gleichzeitig mit Auto-Smartport und Auto-Voice-VLAN verwendet werden. Sie müssen Auto-Smartport deaktivieren, bevor Sie Telefonie-OUI aktivieren.

Allgemeine Smartport-Aufgaben

In diesem Abschnitt werden einige der allgemeinen Aufgaben zum Einrichten von Smartport und Auto-Smartport beschrieben.

Workflow 1: Um Auto-Smartport global für das Gerät zu aktivieren und einen Port mit Auto-Smartport zu konfigurieren, führen Sie folgende Schritte aus:

SCHRITT 1 Um die Auto-Smartport-Funktion für das Gerät zu aktivieren, öffnen Sie die Seite Smartport > Eigenschaften. Legen Sie **Administrativer Auto-Smartport** auf **Aktivieren** oder **Aktivieren nach Voice-VLAN** fest.

SCHRITT 2 Wählen Sie aus, ob das Gerät CDP- und/oder LLDP-Ankündigungen von verbundenen Geräten verarbeiten soll.

SCHRITT 3 Wählen Sie im Feld **Erkennung für Auto-Smartport-Gerät** aus, welche Gerätetypen erkannt werden sollen.

SCHRITT 4 Klicken Sie auf **Übernehmen**.

SCHRITT 5 Um die Auto-Smartport-Funktion für eine oder mehrere Schnittstellen zu aktivieren, öffnen Sie die Seite Smartport > Schnittstelleneinstellungen.

SCHRITT 6 Wählen Sie die Schnittstelle aus und klicken Sie auf **Bearbeiten**.

SCHRITT 7 Wählen Sie im Feld **Smartport-Anwendung** die Option „Auto-Smartport“ aus.

SCHRITT 8 Aktivieren oder deaktivieren Sie nach Bedarf die Option **Dauerhafter Status**.

SCHRITT 9 Klicken Sie auf **Übernehmen**.

Workflow 2: Um eine Schnittstelle als statischen Smartport zu konfigurieren, führen Sie die folgenden Schritte aus:

SCHRITT 1 Um die Smartport-Funktion für die Schnittstelle zu aktivieren, öffnen Sie die Seite Smartport > Schnittstelleneinstellungen.

SCHRITT 2 Wählen Sie die Schnittstelle aus und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Wählen Sie im Feld **Smartport-Anwendung** den Smartport-Typ aus, den Sie der Schnittstelle zuweisen möchten.

SCHRITT 4 Legen Sie die Makroparameter nach Bedarf fest.

SCHRITT 5 Klicken Sie auf **Übernehmen**.

Workflow 3: Um die Standardeinstellungen für Smartport-Makros anzupassen und/oder ein benutzerdefiniertes Makropaar an einen Smartport-Typ zu binden, führen Sie die folgenden Schritte aus:

Mit diesem Verfahren erreichen Sie Folgendes:

- Sie zeigen die Makroquelle an.
- Sie ändern die Parameterstandardeinstellungen.
- Sie stellen die Werkseinstellungen für die Parameter wieder her.
- Sie binden ein benutzerdefiniertes Makropaar (Makro und zugehöriger Gegenmakro) an einen Smartport-Typ.

1. Öffnen Sie die Seite Smartport > Smartport-Typ-Einstellungen.
2. Wählen Sie den Smartport-Typ aus.
3. Klicken Sie auf **Makro-Quelle anzeigen**, um das aktuelle Smartport-Makro anzuzeigen, das dem ausgewählten Smartport-Typ zugeordnet ist.
4. Klicken Sie auf **Bearbeiten**, um ein neues Fenster zu öffnen, in dem Sie benutzerdefinierte Makros an den ausgewählten Smartport-Typ binden und/oder die Standardwerte der Parameter in den an diesen Smartport-Typ gebundenen Makros ändern können. Diese Parameterstandardwerte werden verwendet, wenn Auto-Smartport den ausgewählten Smartport-Typ (falls zutreffend) auf eine Schnittstelle anwendet.
5. Ändern Sie die Felder auf der Seite Bearbeiten.
6. Klicken Sie auf **Übernehmen**, um das Makro erneut auszuführen, wenn die Parameter geändert wurden, oder auf **Standards wiederherstellen**, um gegebenenfalls die Standardparameterwerte für integrierte Makros wiederherzustellen.

Workflow 4: Um ein fehlgeschlagenes Makro erneut auszuführen, führen Sie die folgenden Schritte aus:

SCHRITT 1 Wählen Sie auf der Seite Schnittstelleneinstellungen eine Schnittstelle mit dem Smartport-Typ Unbekannt aus.

SCHRITT 2 Klicken Sie auf **Diagnose anzeigen**, um das Problem zu finden.

SCHRITT 3 Führen Sie eine Problembehandlung aus und korrigieren Sie das Problem. Einen Tipp für die Fehlerbehebung finden Sie unten.

SCHRITT 4 Klicken Sie auf **Bearbeiten.** Ein neues Fenster wird geöffnet, in dem Sie auf **Zurücksetzen** klicken können, um die Schnittstelle zurückzusetzen.

SCHRITT 5 Kehren Sie zur Hauptseite zurück und wenden Sie das Makro mit **Erneut anwenden** (für Geräte, die keine Switches, Router oder APs sind) oder **Smartport-Makro erneut anwenden** (für Switches, Router oder APs) erneut an, um das Smartport-Makro an der Schnittstelle auszuführen.

Es gibt eine zweite Methode für das Zurücksetzen einzelner oder mehrerer unbekannter Schnittstellen:

SCHRITT 1 Aktivieren Sie auf der Seite Schnittstelleneinstellungen das Kontrollkästchen Porttyp ist gleich.

SCHRITT 2 Wählen Sie die Option *Unbekannt* aus und klicken Sie auf **Los**.

SCHRITT 3 Klicken Sie auf **Alle unbekannten Smartports zurücksetzen**. Wenden Sie dann das Makro wie oben beschrieben erneut an.

TIPP Der Grund für den Makrofehler kann ein Konflikt mit einer Konfiguration der Schnittstelle sein, die vor der Anwendung des Makros vorgenommen wurde (meist im Zusammenhang mit Sicherheits- und Sturmsteuerungseinstellungen), ein falscher Porttyp, ein Tippfehler oder ein falscher Befehl in dem benutzerdefinierten Makro oder eine ungültige Parametereinstellung. Parameter werden vor der Anwendung des Makros weder auf den Typ noch auf die Grenze überprüft. Daher führt eine falsche oder ungültige Eingabe in einem Parameterwert fast zwangsläufig zu einem Fehler bei der Anwendung des Makros.

Konfigurieren von Smartport über die webbasierte Benutzeroberfläche

Die Smartport-Funktion können Sie auf den Seiten Smartport > Eigenschaften, Smartport-Typ-Einstellungen und Schnittstelleneinstellungen konfigurieren.

Informationen zur Voice-VLAN-Konfiguration finden Sie unter **Voice-VLAN**.

Informationen zur LLDP/CDP-Konfiguration finden Sie im Abschnitt **Konfigurieren von LLDP** bzw. **Konfigurieren von CDP**.

Smartport-Eigenschaften

So konfigurieren Sie die Smartport-Funktion global:

SCHRITT 1 Klicken Sie auf **Smartport > Eigenschaften**.

SCHRITT 2 Geben Sie die Parameter ein.

- **Administrativer Auto-Smartport**: Wählen Sie hier aus, ob Auto-Smartport global aktiviert oder deaktiviert sein soll. Folgende Optionen stehen zur Verfügung:
  - *Deaktivieren*: Wählen Sie diese Option aus, um Auto-Smartport auf dem Gerät zu deaktivieren.
  - *Aktivieren*: Wählen Sie diese Option aus, um Auto-Smartport auf dem Gerät zu aktivieren.
  - *Aktivieren nach Auto-Voice-VLAN*: Diese Option aktiviert die Auto-Smartport-Funktion. Sie wird jedoch nur ausgeführt, wenn Auto-Voice-VLAN ebenfalls aktiviert ist und verwendet wird. „Aktivieren nach Auto-Voice-VLAN“ ist die Standardeinstellung.
- **Auto-Smartport für Betrieb**: Zeigt den Auto-Smartport-Status an.
- **Erkennungsmethode für Auto-Smartport-Gerät**: Wählen Sie aus, ob eingehende CDP- und/oder LLDP-Pakete zum Erkennen des Smartport-Typs der verbundenen Geräte verwendet werden. Sie müssen mindestens eine Option aktivieren, damit Auto-Smartport Geräte identifiziert.
- **CDP-Status für Betrieb**: Zeigt den Betriebsstatus von CDP an. Aktivieren Sie CDP, wenn Auto-Smartport den Smartport-Typ basierend auf der CDP-Ankündigung erkennen soll.
- **LLDP-Status für Betrieb**: Zeigt den Betriebsstatus von LLDP an. Aktivieren Sie LLDP, wenn Auto-Smartport den Smartport-Typ basierend auf der LLDP/LLDP MED-Ankündigung erkennen soll.
- **Erkennung für Auto-Smartport-Gerät**: Wählen Sie die einzelnen Gerätetypen aus, für die Auto-Smartport den Schnittstellen Smartport-Typen zuweisen kann. Wenn diese Option nicht aktiviert ist, weist Auto-Smartport diesen Smartport-Typ keiner Schnittstelle zu.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Damit werden die globalen Smartport-Parameter auf dem Gerät eingestellt.

Smartport-Typ-Einstellungen

Auf der Seite Smartport-Typ-Einstellungen können Sie die Smartport-Typ-Einstellungen bearbeiten und die Makroquelle anzeigen.

Standardmäßig ist jeder Smartport-Typ einem Paar aus integrierten Smartport-Makros zugeordnet. Weitere Informationen zu Makros und Anti-Makros finden Sie unter **Smartport-Typen**. Alternativ können Sie einem Smartport-Typ ein eigenes Paar aus benutzerdefinierten Makros mit angepassten Konfigurationen zuordnen. Benutzerdefinierte Makros können Sie nur über die CLI erstellen. Details finden Sie im CLI-Referenzhandbuch.

Integrierte oder benutzerdefinierte Makros können Parameter haben. Die integrierten Makros haben bis zu drei Parameter.

Wenn Sie diese von Auto-Smartport angewendeten Parameter für die Smartport-Typen auf der Seite Smartport-Typ-Einstellungen bearbeiten, werden die Standardwerte für die Parameter konfiguriert. Diese Standardeinstellungen werden von Auto-Smartport verwendet.

HINWEIS Wenn Sie Änderungen an Auto-Smartport-Typen vornehmen, werden die neuen Einstellungen auf Schnittstellen angewendet, denen dieser Typ bereits von Auto-Smartport zugewiesen wurde. In diesem Fall führt die Bindung an ein ungültiges Makro oder das Festlegen eines ungültigen Standardparameters dazu, dass alle Ports dieses Smartport-Typs den Status „Unbekannt“ annehmen.

SCHRITT 1 Klicken Sie auf **Smartport > Smartport-Typ-Einstellungen**.

SCHRITT 2 Zum Anzeigen des einem Smartport-Typ zugeordneten Smartport-Makros wählen Sie einen Smartport-Typ aus und klicken auf **Makro-Quelle anzeigen**.

SCHRITT 3 Um die Parameter eines Makros zu ändern oder ein benutzerdefiniertes Makro zuzuweisen, wählen Sie einen Smartport-Typ aus, und klicken auf **Bearbeiten**.

SCHRITT 4 Geben Sie Werte für die Felder ein.

- **Porttyp**: Wählen Sie einen Smartport-Typ aus.
- **Makroname**: Zeigt den Namen des Smartport-Makros an, das dem Smartport-Typ zurzeit zugeordnet ist.
- **Makrotyp**: Legen Sie fest, ob das diesem Smartport-Typ zugeordnete Paar aus Makro und Gegenmakro integriert oder benutzerdefiniert sein soll.
- **Benutzerdefiniertes Makro**: Wählen Sie gegebenenfalls das benutzerdefinierte Makro aus, das dem ausgewählten Smartport-Typ zugeordnet werden soll. Das Makro muss bereits mit einem Anti-Makro gepaart sein.

Die Makropaare werden anhand des Namens gebildet. Dies wird im Abschnitt „Smartport-Makro“ beschrieben.

- **Makroparameter**: Zeigt die folgenden Felder für drei Parameter in dem Makro an:
  - *Name von Parameter*: Der Name des Parameters in dem Makro.
  - *Wert von Parameter*: Der aktuelle Wert des Parameters in dem Makro. Diesen Wert können Sie hier ändern.
  - *Beschreibung von Parameter*: Die Beschreibung des Parameters.

  Sie können die Standardparameterwerte wiederherstellen, indem Sie auf **Standard wiederherstellen** klicken.

SCHRITT 5 Klicken Sie auf **Übernehmen**, um die Änderungen in der aktuellen Konfiguration zu speichern. Wenn das dem Smartport-Typ zugeordnete Smartport-Makro und/oder seine Parameterwerte geändert werden, wendet Auto-Smartport das Makro automatisch erneut auf die Schnittstellen an, denen der Smartport-Typ zurzeit durch Auto-Smartport zugewiesen ist. Auto-Smartport wendet die Änderungen nicht auf Schnittstellen mit statisch zugewiesenem Smartport-Typ an.

HINWEIS Es gibt keine Methode für die Überprüfung von Makroparametern, da diese nicht über eine Typzuordnung verfügen. Daher ist an dieser Stelle jede Eingabe gültig. Ungültige Parameterwerte können jedoch zu Fehlern führen, wenn der Smartport-Typ einer Schnittstelle zugewiesen wird und damit das zugeordnete Makro angewendet wird.

Smartport-Schnittstelleneinstellungen

Auf der Seite „Schnittstelleneinstellungen“ können Sie die folgenden Aufgaben ausführen:

- Statisches Anwenden eines bestimmten Smartport-Typs auf eine Schnittstelle mit schnittstellenspezifischen Werten für die Makroparameter.
- Aktivieren von Auto-Smartport an einer Schnittstelle.
- Diagnostizieren eines Smartport-Makros, dessen Anwendung fehlgeschlagen ist und aufgrund dessen der Smartport-Typ „Unbekannt“ entspricht.
- Erneutes Anwenden eines Smartport-Makros nach dem Fehlschlagen für einen der folgenden Schnittstellentypen: Switch, Router und Zugriffspunkt. Sie müssen die notwendigen Korrekturen vornehmen, bevor Sie auf **Erneut anwenden** klicken. Tipps für die Fehlerbehebung finden Sie im Abschnitt **Allgemeine Smartport-Aufgaben**.
- Erneutes Anwenden eines Smartport-Makros auf eine Schnittstelle. In manchen Fällen müssen Sie möglicherweise ein Smartport-Makro erneut anwenden, um die Konfiguration einer Schnittstelle auf den aktuellen Stand zu bringen. Wenn Sie beispielsweise ein Smartport-Makro für ein Gerät erneut auf eine Geräteschnittstelle anwenden, wird die Schnittstelle zum Mitglied der VLANs, die seit der

letzten Anwendung des Makros erstellt wurden. Sie müssen mit den aktuellen Konfigurationen des Geräts sowie mit der Definition des Makros vertraut sein, um abschätzen zu können, ob die erneute Anwendung Auswirkungen auf die Schnittstelle hat.

- Zurücksetzen unbekannter Schnittstellen. Damit wird der Modus unbekannter Schnittstellen auf „Standard“ festgelegt.

So wenden Sie ein Smartport-Makro an:

SCHRITT 1 Klicken Sie auf **Smartport > Schnittstelleneinstellungen**.

Wenden Sie das zugeordnete Smartport-Makro wie folgt erneut an:

- Wählen Sie eine Gruppe von Smartport-Typen aus (Switches, Router oder APs) und klicken Sie auf **Smartport-Makro erneut anwenden.** Die Makros werden auf alle ausgewählten Schnittstellentypen angewendet.
- Wählen Sie eine aktive Schnittstelle aus und klicken Sie auf **Erneut anwenden**, um das letzte auf die Schnittstelle angewendete Makro erneut anzuwenden.

  Mit der Aktion **Erneut anwenden** wird die Schnittstelle darüber hinaus allen neu erstellten VLANs hinzugefügt.

SCHRITT 2 Smartport-Diagnose

Wenn bei einem Smartport-Makro Fehler auftreten, entspricht der Smartport-Typ der Schnittstelle „Unbekannt“. Wählen Sie eine Schnittstelle mit dem Typ „Unbekannt“ aus und klicken Sie auf **Diagnose anzeigen**. Daraufhin wird der Befehl angezeigt, bei dem die Anwendung des Makros fehlgeschlagen ist. Tipps für die Fehlerbehebung finden Sie im Abschnitt **Allgemeine Smartport-Aufgaben**. Wenn Sie das Problem korrigiert haben, wenden Sie das Makro erneut an.

SCHRITT 3 Zurücksetzen aller unbekannten Schnittstellen auf den Typ „Standard“.

- Aktivieren Sie das Kontrollkästchen *Porttyp entspricht*.
- Wählen Sie die Option *Unbekannt* aus und klicken Sie auf **Los**.
- Klicken Sie auf **Alle unbekannten Smartports zurücksetzen**. Wenden Sie dann das Makro wie oben beschrieben erneut an. Daraufhin werden alle Schnittstellen mit dem Typ „Unbekannt“ zurückgesetzt, das heißt, für alle Schnittstellen wird wieder der Typ „Standard“ festgelegt. Wenn Sie den Fehler im Makro und/oder in der aktuellen Schnittstellenkonfiguration korrigiert haben, können Sie ein neues Makro anwenden.

HINWEIS Beim Zurücksetzen der Schnittstelle mit dem unbekannten Typ wird nicht die Konfiguration zurückgesetzt, die durch das Makro vorgenommen wurde. Sie müssen die Konfiguration manuell bereinigen.

So weisen Sie einer Schnittstelle einen Smartport-Typ zu oder aktivieren Auto-Smartport für die Schnittstelle:

SCHRITT 1 Wählen Sie eine Schnittstelle aus und klicken Sie auf **Bearbeiten**.

SCHRITT 2 Geben Sie Werte für die Felder ein.

- **Schnittstelle**: Wählen Sie den Port oder die LAG aus.
- **Smartport-Typ**: Zeigt den Smartport-Typ an, der dem Port bzw. der LAG zurzeit zugewiesen ist.
- **Smartport-Anwendung**: Wählen Sie im Pulldown-Menü „Smartport-Anwendung“ den Smartport-Typ aus.
- **Smartport-Anwendungsmethode**: Wenn Auto-Smartport ausgewählt ist, weist Auto-Smartport automatisch den Smartport-Typ basierend auf der CDP- und/oder LLDP-Ankündigung zu, die von verbundenen Geräten empfangen wurde, und wendet das entsprechende Smartport-Makro an. Wählen Sie den gewünschten Smartport-Typ aus, um einen Smartport-Typ statisch zuzuweisen und das entsprechende Smartport-Makro auf die Schnittstelle anzuwenden.
- **Dauerhafter Status**: Wählen Sie diese Option aus, um den dauerhaften Status zu aktivieren. Wenn diese Option aktiviert ist, bleibt die Zuordnung eines Smartport-Typs zu einer Schnittstelle auch dann erhalten, wenn die Schnittstelle deaktiviert oder das Gerät neu gestartet wird. Der dauerhafte Status ist nur möglich, wenn die Smartport-Anwendung der Schnittstelle auf „Auto-Smartport“ festgelegt ist. Wenn Sie den dauerhaften Status an einer Schnittstelle aktivieren, entfällt die ansonsten auftretende Verzögerung für die Geräteerkennung.
- **Makroparameter**: Zeigt die folgenden Felder für bis zu drei Parameter in dem Makro an:
  - *Name von Parameter*: Der Name des Parameters in dem Makro.
  - *Wert von Parameter*: Der aktuelle Wert des Parameters in dem Makro. Diesen Wert können Sie hier ändern.
  - *Beschreibung von Parameter*: Die Beschreibung des Parameters.

SCHRITT 3 Klicken Sie auf **Zurücksetzen**, um eine Schnittstelle, die (aufgrund der nicht erfolgreichen Anwendung eines Makros) den Status „Unbekannt“ aufweist, auf „Standard“ festzulegen. Auf der Hauptseite können Sie das Makro erneut anwenden.

SCHRITT 4 Klicken Sie auf **Übernehmen**, um die Änderungen zu aktualisieren und den Smartport-Typ der Schnittstelle zuzuweisen.

Integrierte Smartport-Makros

Nachfolgend werden die integrierten Makropaare für die einzelnen Smartport-Typen beschrieben. Es gibt für jeden Smartport-Typ ein Makro zum Konfigurieren der Schnittstelle und ein Anti-Makro zum Entfernen der Konfiguration.

Für die folgenden Smartport-Typen wird Makrocode bereitgestellt:

- **Desktop**
- **Drucker**
- **Gast**
- **Server**
- **Host**
- **IP-Kamera**
- **IP-Telefon**
- **IP-Telefon + Desktop**
- **Switch**
- **Router**
- **Zugriffspunkt**

Desktop

```
[desktop]
#interface configuration, for increased network security and reliability when connecting a desktop
device, such as a PC, to a switch port.
#macro description Desktop
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: Ohne Tags betriebenes VLAN, das auf dem Port konfiguriert wird.
#                         $max_hosts: Maximale Anzahl der am Port zulässigen Geräte
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
```

```
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_desktop

```
[no_desktop]
#macro description No Desktop
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

Drucker

```
[printer]
#macro description printer
#macro keywords $native_vlan
#
#macro key description: $native_vlan: Ohne Tags betriebenes VLAN, das auf dem Port konfiguriert wird.
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
```

```
#
@
```

no_printer

```
[no_printer]
#macro description No printer
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

Gast

```
[guest]
#macro description guest
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: Ohne Tags betriebenes VLAN, das auf dem Port konfiguriert
wird.
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_guest

```
[no_guest]
#macro description No guest
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

Server

```
[server]
#macro description server
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: Ohne Tags betriebenes VLAN, das auf dem Port konfiguriert wird.
#                         $max_hosts: Maximale Anzahl der am Port zulässigen Geräte
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_server

```
[no_server]
#macro description No server
```

```
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
#
spanning-tree portfast auto
#
@
```

Host

```
[host]
#macro description host
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: Ohne Tags betriebenes VLAN, das auf dem Port konfiguriert
wird.
#                         $max_hosts: Maximale Anzahl der am Port zulässigen Geräte
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_host

```
[no_host]
#macro description No host
#
no smartport switchport trunk native vlan
```

```
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

IP-Kamera

```
[ip_camera]
#macro description ip_camera
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: Ohne Tags betriebenes VLAN, das auf dem Port konfiguriert
wird.
#Default Values are
#$native_vlan = Default VLAN
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_camera

```
[no_ip_camera]
#macro description No ip_camera
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
```

```
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

IP-Telefon

```
[ip_phone]
#macro description ip_phone
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:   $native_vlan: Ohne Tags betriebenes VLAN, das auf dem Port konfiguriert
wird.
#                         $voice_vlan: Die Voice-VLAN-ID
#                         $max_hosts: Maximale Anzahl der am Port zulässigen Geräte
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone

```
[no_ip_phone]
#macro description no ip_phone
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: Die Voice-VLAN-ID
#
#Default Values are
#$voice_vlan = 1
#
```

```
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

IP-Telefon + Desktop

```
[ip_phone_desktop]
#macro description ip_phone_desktop
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:   $native_vlan: Ohne Tags betriebenes VLAN, das auf dem Port konfiguriert wird.
#                         $voice_vlan: Die Voice-VLAN-ID
#                         $max_hosts: Maximale Anzahl der am Port zulässigen Geräte
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone_desktop

```
[no_ip_phone_desktop]
#macro description no ip_phone_desktop
#macro keywords $voice_vlan
```

```
#
#macro key description:   $voice_vlan: Die Voice-VLAN-ID
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

Switch

```
[switch]
#macro description switch
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: Ohne Tags betriebenes VLAN, das auf dem Port konfiguriert wird.
#                        $voice_vlan: Die Voice-VLAN-ID
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
spanning-tree link-type point-to-point
#
@
```

no_switch

```
[no_switch]
#macro description No switch
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: Die Voice-VLAN-ID
#
no smartport switchport trunk native vlan
```

```
smartport switchport trunk allowed vlan remove all
#
no spanning-tree link-type
#
@
```

Router

```
[router]
#macro description router
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: Ohne Tags betriebenes VLAN, das auf dem Port konfiguriert wird.
#                        $voice_vlan: Die Voice-VLAN-ID
#
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree link-type point-to-point
#
@
```

no_router

```
[no_router]

#macro description No router

#macro keywords $voice_vlan

#

#macro key description:   $voice_vlan: Die Voice-VLAN-ID

#

no smartport switchport trunk native vlan

smartport switchport trunk allowed vlan remove all

#

no smartport storm-control broadcast enable

no smartport storm-control broadcast level
```

```
#
no spanning-tree link-type
#
@
```

Zugriffspunkt

```
[ap]
#macro description ap
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: Ohne Tags betriebenes VLAN, das auf dem Port konfiguriert
wird.
```

14

Portverwaltung: PoE

Die Power-over-Ethernet-Funktion (PoE) steht nur bei PoE-basierten Geräten zur Verfügung. Eine Liste der PoE-basierten Geräte finden Sie im Abschnitt **Gerätemodelle**.

In diesem Abschnitt wird beschrieben, wie Sie die PoE-Funktion verwenden.

HINWEIS Die PoE-Funktion ist auf den SG500XG/ESW2-550X-Geräten nicht verfügbar.

Die folgenden Themen werden behandelt:

- **PoE am Gerät**
- **PoE-Eigenschaften**
- **PoE-Einstellungen**

PoE am Gerät

Ein PoE-Gerät ist ein PSE-Gerät (Power Sourcing Equipment), das über vorhandene Kupferkabel angeschlossene PD-Geräte (Powered Devices) mit elektrischem Strom versorgt, ohne den Netzwerkverkehr zu beeinflussen und ohne das physische Netzwerk zu aktualisieren oder die Netzwerkinfrastruktur zu ändern.

Informationen zur PoE-Unterstützung in verschiedenen Modellen finden Sie unter **Gerätemodelle**.

Vorteile von PoE

PoE bietet folgende Funktionen:

- Es macht die Versorgung aller mit einem LAN verbundenen Geräte mit 110/220 Volt Wechselstrom überflüssig.
- Die Platzierung aller Netzwerkgeräte in der Nähe einer Stromquelle ist nicht erforderlich.
- Es macht doppelte Verkabelungssysteme in Unternehmen überflüssig und reduziert somit die Installationskosten deutlich.

PoE kann in jedem Unternehmensnetzwerk verwendet werden, in dem Geräte mit relativ geringer Stromaufnahme an das Ethernet-LAN angeschlossen sind, wie zum Beispiel:

- IP-Telefone
- Wireless Access Points
- IP-Gateways
- Remote-Geräte für die Audio- und Videoüberwachung

PoE-Betrieb

PoE ist in folgenden Stufen implementiert:

- **Erkennung**: Senden spezieller Impulse durch das Kupferkabel. Befindet sich am anderen Kabelende ein PoE-Gerät, antwortet dieses Gerät auf diese Impulse.
- **Klassifizierung**: Nach der Erkennung erfolgt die Verhandlung zwischen dem PSE-Gerät (Power Sourcing Equipment) und dem PD-Gerät (Powered Device). Während der Verhandlung gibt das PD-Gerät seine Klasse an, d. h. die maximale Leistung, die es verbraucht.
- **Leistungsaufnahme**: Nach Abschluss der Klassifizierung stellt das PSE-Gerät Leistung für das PD-Gerät bereit. Wenn das PD-Gerät PoE unterstützt, jedoch keine Klassifizierung durchführen kann, wird davon ausgegangen, dass es der Klasse 0 (das Maximum) entspricht. Wenn ein PD-Gerät versucht, mehr Leistung als standardmäßig zulässig zu verbrauchen, unterbindet das PSE-Gerät die Leistungsbereitstellung an diesem Port.

PoE unterstützt zwei Modi:

- **Port-Begrenzung**: Die maximale Leistung, die das Gerät bereitstellt, ist auf den vom Systemadministrator konfigurierten Wert begrenzt, unabhängig vom Ergebnis der Klassifizierung.
- **Klassenbegrenzung**: Die vom Gerät maximal bereitgestellte Leistung ist von den Ergebnissen der Klassifizierung abhängig. Das heißt, sie wird entsprechend der Anforderung des Client festgelegt.

Überlegungen zur PoE-Konfiguration

In Bezug auf die PoE-Funktion sind zwei Faktoren zu berücksichtigen:

- Die Leistung, die das PSE-Gerät bereitstellen kann.
- Die Leistung, die das PD-Gerät tatsächlich zu verbrauchen versucht.

Folgendes kann konfiguriert werden:

- Die maximale Leistung, die ein PSE-Gerät für ein PD-Gerät bereitstellen kann.
- Sie können während des Gerätebetriebs zwischen den Modi Klassenbegrenzung und Port-Begrenzung wechseln. Die für den Modus Port-Begrenzung konfigurierten Leistungswerte bleiben erhalten.

  HINWEIS Wenn Sie bei laufendem Gerätebetrieb den Modus von Klassenbegrenzung in Port-Begrenzung oder umgekehrt ändern, führt das zu einem Neustart des PD-Geräts.
- Den maximal zulässigen Port-Wert als numerischen Port-Grenzwert in mW (Port-Begrenzungsmodus).
- Sie können ein Trap generieren, wenn ein PD-Gerät versucht, zu viel Leistung zu verbrauchen. Des Weiteren können Sie den Prozentwert der maximalen Leistung festlegen, bei der das Trap generiert wird.

Die PoE-spezifische Hardware erkennt die PD-Klasse und die Leistungsbegrenzung automatisch basierend auf der Klasse des an jedem einzelnen Port angeschlossenen Geräts (Klassenbegrenzungsmodus).

Wenn ein angeschlossenes PD-Gerät, solange eine Verbindung besteht, mehr Leistung anfordert als in der Konfiguration vorgesehen (unabhängig davon, ob sich das Gerät im Klassenbegrenzungsmodus oder im Port-Begrenzungsmodus befindet), führt das Gerät Folgendes aus:

- Es erhält den aktiven bzw. nicht aktiven Status des PoE-Port-Links.
- Es schaltet die Leistungsbereitstellung für den PoE-Port ab.
- Es protokolliert den Grund für das Abschalten der Leistung.
- Es generiert ein SNMP-Trap.

  HINWEIS Wenn ein PoE-Gerät mit niedrigerer Spannung über PoE an das SG500-Gerät angeschlossen und auf beiden Seiten über PoE-fähige Ports verbunden wird, kann das Niederspannungsgerät keine anderen Geräte mehr mit Strom versorgen. Sie können dies vermeiden, indem Sie die PoE-Unterstützung im SG500 deaktivieren oder einen Nicht-PoE-Port verwenden.

VORSICHT Beachten Sie beim Anschließen von PoE-fähigen Switches Folgendes:

Die PoE-Modelle der Switches der Serien Sx200, Sx300 und SF500 sind PSE-Geräte, die angeschlossene PD-Geräte mit Gleichstrom versorgen können. Dazu gehören VoIP-Telefone, IP-Kameras und drahtlose Zugangspunkte. Der PoE-Switch kann Strom für noch nicht dem Standard entsprechende ältere PoE-PD-Geräte erkennen und liefern. Aufgrund dieser Unterstützung für PoE bei älteren Geräten kann es vorkommen, dass ein PoE-Switch, der als PSE-Gerät fungiert, ein verbundenes PSE-Gerät (beispielsweise einen anderen PoE-Switch) fälschlicherweise als älteres PD-Gerät erkennt und mit Strom versorgt.

In diesem Fall könnte ein PoE-Switch des Typs Sx200/300/500, der als PSE-Gerät eigentlich Wechselstrom benötigt, aufgrund der falschen Erkennung eines anderen PSE-Geräts als älteres PD-Gerät eingeschaltet werden. In diesem Fall funktioniert das PoE-Gerät möglicherweise nicht ordnungsgemäß und kann die angeschlossenen PDs nicht richtig mit Strom versorgen.

Deaktivieren Sie PoE an den für PSEs verwendeten Anschluss der PoE-Switches, um die falsche Erkennung zu verhindern. Außerdem müssen Sie PSE-Geräte einschalten, bevor Sie sie an ein PoE-Gerät anschließen. Wenn ein Gerät fälschlich als PD erkannt wird, trennen Sie das Gerät vom PoE-Port und schalten Sie das Gerät mit Wechselstrom aus und wieder ein, bevor Sie die PoE-Ports wieder verbinden.

PoE-Eigenschaften

Auf der Seite *PoE-Eigenschaften* können Sie den Portbegrenzungsmodus oder den Klassenbegrenzungsmodus für PoE auswählen und die zu generierenden PoE-Traps festlegen.

Diese Einstellungen werden im Voraus festgelegt. Wenn das PD-Gerät eine Verbindung hergestellt hat und Leistung verbraucht, benötigt es möglicherweise deutlich weniger als die maximal zulässige Leistung.

Die Leistungsabgabe wird während des Einschaltens nach dem Neustart, während der Initialisierung und während der Systemkonfiguration deaktiviert, um eine Beschädigung von PD-Geräten zu vermeiden.

So konfigurieren Sie PoE am Gerät und überwachen den aktuellen Stromverbrauch:

SCHRITT 1 Klicken Sie auf **Portverwaltung > PoE > Eigenschaften**.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **Leistungsmodus**: Wählen Sie eine der folgenden Optionen:
  - *Port-Begrenzung*: Die maximale Leistungsbegrenzung für jeden Port wird vom Benutzer konfiguriert.
  - *Klassenbegrenzung*: Die maximale Leistungsbegrenzung pro Port wird von der Geräteklasse bestimmt, die bei der Klassifizierung ermittelt wird.

  HINWEIS Wenn Sie von der Portbegrenzung zur Klassenbegrenzung und umgekehrt wechseln möchten, müssen Sie die PoE-Ports im Vorfeld deaktivieren und nach der Änderung der Konfiguration wieder aktivieren.
- **Traps**: Dient zum Aktivieren oder Deaktivieren von Traps. Wenn Sie Traps aktivieren, müssen Sie auch SNMP aktivieren und mindestens einen SNMP-Benachrichtigungsempfänger konfigurieren.

- **Schwellenwert für Leistungs-Trap**: Geben Sie den Schwellenwert als Prozentwert der Leistungsbegrenzung ein. Es wird ein Alarm ausgegeben, wenn die Leistung diesen Wert überschreitet.

Die folgenden Zähler werden für jedes Gerät oder für alle Einheiten des Stacks angezeigt:

- **Nennleistung**: Die Gesamtleistung, mit der das Gerät alle angeschlossenen PD-Geräte versorgen kann.
- **Verbrauchte Leistung**: Die aktuell von den PoE-Ports verbrauchte Leistung.
- **Verfügbare Leistung**: Nennleistung minus verbrauchte Leistung.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um die PoE-Eigenschaften zu speichern.

PoE-Einstellungen

Auf der Seite *PoE-Einstellungen* werden PoE-Systeminformationen zum Aktivieren der PoE-Funktion an den Schnittstellen und zum Überwachen des aktuellen Stromverbrauchs sowie die maximale Leistung pro Port angezeigt.

HINWEIS PoE kann am Gerät für einen bestimmten Zeitraum konfiguriert werden. Mithilfe dieser Funktion können Sie, für jedes einzelne Gerät, die Wochentage und Zeiten definieren, zu denen PoE aktiviert ist. Außerhalb dieses Zeitbereichs ist PoE deaktiviert. Damit Sie diese Funktion nutzen können, müssen Sie zunächst auf der Seite **Zeitbereich** einen Zeitbereich definieren.

Abhängig vom Leistungsmodus wird auf dieser Seite die Leistung pro Port auf zweierlei Weise beschränkt:

- **Port-Begrenzung:** Die Leistung ist auf die angegebene Wattzahl begrenzt. Damit diese Einstellungen aktiviert werden können, muss sich das System im PoE-Port-Begrenzungsmodus befinden. Diesen Modus können Sie auf der Seite PoE-Eigenschaften konfigurieren.

  Wenn die am Port verbrauchte Leistung den Grenzwert überschreitet, wird die Leistungsversorgung an diesem Port abgeschaltet.

- **Klassenbegrenzung:** Die Leistung wird basierend auf der Klasse des angeschlossenen PD-Geräts bestimmt. Damit diese Einstellungen aktiviert werden können, muss sich das System im PoE-Klassenbegrenzungsmodus befinden. Diesen Modus können Sie auf der Seite PoE-Eigenschaften konfigurieren.

  Wenn die am Port verbrauchte Leistung den Grenzwert für die Klasse überschreitet, wird die Leistungsversorgung an diesem Port abgeschaltet.

Beispiel für PoE-Priorität:

Annahme: Ein Gerät mit 48 Ports stellt insgesamt 375 Watt bereit.

Der Administrator konfiguriert alle Ports, um maximal 30 Watt zuzuweisen. Dadurch ergeben sich 1440 Watt (48 x 30 Ports), was zu viel ist. Das Gerät kann nicht alle Ports mit ausreichend Strom versorgen und stellt den Strom daher nach Priorität bereit.

Der Administrator legt die Priorität der einzelnen Ports fest und weist den Ports jeweils Leistung zu.

Diese Prioritäten können Sie auf der Seite PoE-Einstellungen eingeben.

Eine Beschreibung der Gerätemodelle mit PoE-Unterstützung und der maximalen Leistung, die PoE-Ports zugewiesen werden kann, finden Sie unter **Gerätemodelle**.

So konfigurieren Sie PoE-Porteinstellungen:

SCHRITT 1 Klicken Sie auf **Portverwaltung > PoE > Einstellungen**. Die nachfolgende Liste der Felder gilt für den Leistungsmodus Portbegrenzung. Im Leistungsmodus „Klassenbegrenzung“ weichen die Felder geringfügig ab.

SCHRITT 2 Wählen Sie einen Port aus und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie den Wert in das folgende Feld ein:

- **Schnittstelle**: Wählen Sie den zu konfigurierenden Port aus.
- **PoE-Administrationsstatus**: Aktivieren oder deaktivieren Sie PoE für den Port.
- **Zeitbereich**: Auswählen, um PoE auf dem Port zu aktivieren.
- **Zeitbereichsname**: Wenn Zeitbereich aktiviert ist, wählen Sie den zu verwendenden Zeitbereich aus. Zeitbereiche werden auf der Seite **Zeitbereich** definiert.
- **Leistungsprioritätsstufe**: Legen Sie die Port-Priorität (niedrig, hoch oder kritisch) fest, die verwendet werden soll, wenn die bereitgestellte Leistung nicht ausreicht. Wenn beispielsweise 99 % der Leistung verbraucht werden und Port 1 eine hohe Priorität und Port 3 eine niedrige Priorität besitzt, wird Port 1 mit Leistung versorgt, während keine Bereitstellung an Port 3 erfolgt.
- **Administrative Leistungszuweisung**: Dieses Feld wird nur angezeigt, wenn auf der Seite PoE-Eigenschaften der Leistungsmodus Portbegrenzung festgelegt ist. Wenn der Leistungsmodus „Leistungsbegrenzung“ verwendet wird, geben Sie die dem Port zugewiesene Leistung in Milliwatt ein.
- **Maximale Leistungszuweisung**: Dieses Feld wird nur angezeigt, wenn auf der Seite „PoE-Eigenschaften“ der Leistungsmodus „Leistungslimit“ festgelegt ist. Zeigt die an diesem Port maximal zulässige Leistung an.
- **Leistungsaufnahme**: Zeigt die Leistung in Milliwatt an, die dem angeschlossenen und versorgten Gerät an der ausgewählten Schnittstelle zugewiesen ist.

- **Klasse**: Eine Eingabe in dieses Feld ist nur möglich, wenn auf der Seite PoE-Eigenschaften der Leistungsmodus „Klassenbegrenzung“ festgelegt ist. Die Klasse bestimmt die bereitgestellte Leistung:

Klasse	Maximal vom Geräteport bereitgestellte Leistung
0	15,4 Watt
1	4,0 Watt
2	7,0 Watt
3	15,4 Watt
4	30,0 Watt

- **Zähler für Überlastung**: Zeigt die Gesamtzahl der Ereignisse an, bei denen die Leistungsversorgung überlastet wurde.
- **Zähler für Kurz**: Zeigt die Gesamtzahl der Ereignisse an, bei denen ein Kurzschluss aufgetreten ist.
- **Zähler für Verweigert**: Zeigt an, wie oft dem PD-Gerät die Leistung verweigert wurde.
- **Zähler für Nicht vorhanden**: Zeigt an, wie oft die Leistungsversorgung des PD-Geräts unterbunden wurde, weil dieses nicht mehr erkannt wurde.
- **Zähler für ungültige Signaturen**: Zeigt an, wie oft eine ungültige Signatur empfangen wurde. Signaturen werden von PD-Geräten verwendet, um sich beim PSE zu identifizieren. Signaturen werden bei der PD-Geräteerkennung, Klassifizierung oder Wartung generiert.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die PoE-Einstellungen für den Port werden in die aktuelle Konfigurationsdatei geschrieben.

15

VLAN-Verwaltung

In diesem Abschnitt werden die folgenden Themen behandelt:

- **Übersicht**
- **Reguläre VLANs**
- **Einstellungen für Private VLANs**
- **GVRP-Einstellungen**
- **VLAN-Gruppen**
- **Voice-VLAN**
- **Zugriffsport-Multicast-TV-VLAN**
- **Kundenport-Multicast-TV-VLAN**

Übersicht

Bei einem VLAN handelt es sich um eine logische Gruppe von Ports, mit der die zugeordneten Geräte über die Ethernet-MAC-Schicht miteinander kommunizieren können, und zwar unabhängig vom physischen LAN-Segment des überbrückten Netzwerkes, mit dem sie verbunden sind.

Bei einem VLAN handelt es sich um eine logische Gruppe von Ports, mit der die zugeordneten Geräte über die Ethernet-MAC-Schicht miteinander kommunizieren können, und zwar unabhängig vom physischen LAN-Segment des überbrückten Netzwerkes, mit dem sie verbunden sind.

VLAN-Beschreibung

Jedes VLAN muss mit einer eindeutigen VLAN-ID (VID) mit einem Wert zwischen 1 und 4094 konfiguriert werden. Ein Port eines Gerätes in einem überbrückten Netzwerk ist Mitglied eines VLAN, wenn er Daten an das VLAN senden und Daten von diesem empfangen kann. Ein Port ist ein Mitglied ohne Tag eines VLAN, wenn alle für diesen Port bestimmten Pakete in dem VLAN kein VLAN-Tag besitzen. Ein Port ist ein Mitglied mit Tag eines VLAN, wenn alle für diesen Port bestimmten Pakete in dem VLAN ein VLAN-Tag besitzen. Ein Port kann Mitglied eines VLANs ohne Tag, aber Mitglied mehrerer VLANs mit Tag sein.

Ein Port im VLAN-Zugriffsmodus kann nur Mitglied eines VLAN sein. Befindet er sich im allgemeinen oder Trunk-Modus, kann der Port zu einem oder mehreren VLANs gehören.

Aspekte der VLAN-Adresssicherheit und -Skalierbarkeit. Der Verkehr eines VLAN verbleibt im VLAN und endet an den Geräten innerhalb des VLAN. Es wird darüber hinaus die Netzwerkkonfiguration vereinfacht, da Geräte logisch verbunden werden, ohne dass eine physische Umpositionierung dieser Geräte erforderlich ist.

Wenn ein Frame über ein VLAN-Tag verfügt, wird jedem Ethernet-Frame ein VLAN-Tag mit vier Byte hinzugefügt. Das Tag enthält eine VLAN-ID zwischen 1 und 4094 sowie ein VLAN-Prioritäts-Tag (VPT) zwischen 0 und 7. Details zu VPT finden Sie unter **Quality of Service**.

Wenn ein Frame ein VLAN-fähiges Gerät erreicht, wird es basierend auf dem VLAN-Tag mit vier Byte des Frame als zu einem VLAN zugehörig klassifiziert.

Enthält der Frame kein VLAN-Tag oder besitzt er nur ein Prioritäts-Tag, wird der Frame anhand der PVID (Port VLAN Identifier) für das VLAN klassifiziert, die am Eingangs-Port konfiguriert ist, an dem der Frame empfangen wird.

Der Frame wird am Eingangs-Port verworfen, wenn die Eingangsfilterung aktiviert und der Eingangs-Port kein Mitglied des VLAN ist, zu dem das Paket gehört. Ein Frame wird nur als Frame mit Prioritäts-Tag betrachtet, wenn die VID in seinem VLAN-Tag 0 ist.

Zu einem VLAN gehörende Frames verbleiben in diesem VLAN. Dies wird erreicht, indem ein Frame nur an Ausgangs-Ports gesendet oder weitergeleitet wird, die Mitglieder des Ziel-VLAN sind. Ein Ausgangs-Port kann ein Mitglied mit oder ohne Tag eines VLAN sein.

Der Ausgangs-Port:

- Fügt dem Frame ein VLAN-Tag hinzu, wenn der Ausgangs-Port ein Mitglied mit Tag des Ziel-VLAN ist und der ursprüngliche Frame kein VLAN-Tag besitzt.
- Entfernt das VLAN-Tag aus dem Frame, wenn der Ausgangs-Port ein Mitglied ohne Tag des Ziel-VLAN ist und der ursprüngliche Frame ein VLAN-Tag besitzt.

VLAN-Rollen

VLANs werden im Schicht-2-Systemmodus verwendet. Der gesamte VLAN-Verkehr (Unicast/Broadcast/Multicast) verbleibt in diesem VLAN. An andere VLANs angeschlossene Geräte besitzen über die Ethernet-MAC-Schicht keine direkte Verbindung zueinander. Geräte aus unterschiedlichen VLANs können nur über Router der Schicht 3 miteinander kommunizieren. Ein IP-Router muss beispielsweise den IP-Verkehr zwischen VLANs routen, wenn jedes VLAN ein IP-Subnetz repräsentiert.

Bei dem IP-Router kann es sich um einen traditionellen Router handeln, dessen einzelne Schnittstellen nur mit einem VLAN verbunden sind. Der Verkehr zu und von einem traditionellen IP-Router muss ohne VLAN erfolgen. Der IP-Router kann ein VLAN-fähiger Router sein, dessen einzelne Schnittstellen mit einem oder mehreren VLANs verbunden sind. Der Verkehr von und zu einem VLAN-fähigen IP-Router kann mit oder ohne VLAN-Tag erfolgen.

Angrenzende VLAN-fähige Geräte tauschen VLAN-Informationen über GVRP (Generic VLAN Registration Protocol) aus. Somit werden die VLAN-Informationen durch ein überbrücktes Netzwerk propagiert.

VLANs können für ein Gerät statisch oder dynamisch erstellt werden, basierend auf den von Geräten ausgetauschten GVRP-Informationen. Ein VLAN kann statisch oder dynamisch (in Bezug auf GVRP) sein, jedoch nicht beides. Weitere Informationen zu GVRP finden Sie im Abschnitt „GVRP-Einstellungen“.

Einige VLANs können zusätzliche Rollen besitzen, zum Beispiel:

- Voice-VLAN: Weitere Informationen finden Sie im Abschnitt „Voice-VLAN“.
- Gast-VLAN: Wird auf der Seite „VLAN-Authentifizierung bearbeiten“ festgelegt.
- Standard-VLAN: Weitere Informationen finden Sie im Abschnitt „Konfigurieren der VLAN-Standardeinstellungen“.
- Verwaltungs-VLAN (für Systeme im Schicht-2-Systemmodus): Weitere Informationen finden Sie im Abschnitt „Schicht-2-IP-Adressierung“.

QinQ

QinQ ermöglicht die Isolierung zwischen Netzwerken von Dienstanbietern und denen der Kunden. Das Gerät fungiert als Bridge zum Anbieter und unterstützt portbasierte Dienstschnittstellen mit C-Tag.

Mit QinQ fügt das Gerät ein ID-Tag hinzu (das so genannte Service-Tag (S-Tag)), um Verkehr über das Netzwerk weiterzuleiten. Das S-Tag wird verwendet, um Verkehr zwischen verschiedenen Kunden zu trennen und dabei die VLAN-Tags der Kunden beizubehalten.

Der Verkehr der Kunden wird mit einem S-Tag mit TPID 0x8100 gekapselt, wobei es keine Rolle spielt, ob es sich ursprünglich um Verkehr mit C-Tag oder ohne Tag handelte. Mithilfe des S-Tags kann dieser Datenverkehr innerhalb eines Anbieter-Bridge-Netzwerks als Aggregat behandelt werden, wobei das Bridging nur auf der S-Tag-VID (S-VID) basiert.

Das S-Tag bleibt erhalten, während der Verkehr durch die Infrastruktur des Netzwerkdienstanbieters weitergeleitet wird, und wird später von einem Ausgangsgerät entfernt.

Ein zusätzlicher Vorteil von QinQ besteht darin, dass keine Konfiguration der Edge-Geräte der Kunden erforderlich ist.

QinQ können Sie auf der Seite „VLAN-Verwaltung > Schnittstelleneinstellungen“ aktivieren.

Private VLAN

Die Private VLAN-Funktionalität bietet Schicht-2-Isolierung zwischen Ports. Das bedeutet, dass Ports, die zur selben Broadcast-Domäne gehören, auf der Ebene des Bridgings (im Gegensatz zum IP-Routing) nicht miteinander kommunizieren können. Die Ports in einem Private VLAN können überall im Schicht-2-Netzwerk vorhanden sein, müssen sich also nicht am selben Switch befinden. Ein Private VLAN ist so ausgelegt, dass Datenverkehr ohne Tag oder mit Prioritäts-Tag empfangen und Datenverkehr ohne Tag gesendet wird.

Die folgenden Porttypen können Mitglied eines Private VLAN sein:

- **Promiscuous-Ports**: Ein Promiscuous-Port kann mit allen Ports im selben Private VLAN kommunizieren. Diese Ports werden zum Anschluss von Servern und Routern verwendet.
- **Community-Ports (Host-Ports)**: Community-Ports können eine Gruppe von Ports definieren, die Mitglied derselben Schicht-2-Domäne sind. Sie sind in Schicht 2 von anderen Communitys wie auch von isolierten Ports isoliert. Diese Ports verbinden Host-Ports miteinander.
- **Isolierter Port (Host-Port)**: Ein isolierter Port weist in Schicht 2 eine vollständige Isolierung von anderen isolierten und Community-Ports innerhalb desselben Private VLAN auf. Diese Ports verbinden Host-Ports miteinander.

Folgende Arten von Private VLANs existieren:

- **Primäres VLAN**: Ein primäres VLAN gestattet die Herstellung von Schicht-2-Konnektivität von Promiscuous-Ports mit isolierten und Community-Ports. Je Private VLAN kann es nur ein primäres VLAN geben.
- **Isoliertes VLAN (heißt auch sekundäres VLAN)**: Ein isoliertes VLAN ermöglicht isolierten Ports das Senden von Daten in das primäre VLAN. Je Private VLAN kann es nur ein isoliertes VLAN geben.
- **Community-VLAN (heißt auch sekundäres VLAN)**: Zum Erstellen einer Untergruppe (Community) von Ports in einem VLAN müssen die Ports einem Community-VLAN hinzugefügt werden. Das Community-VLAN wird zum Aktivieren der Schicht-2-Konnektivität von Community-Ports zu Promiscuous-Ports und zu Community-Ports derselben Community verwendet. Für jede Community kann ein einzelnes Community-VLAN vorhanden sein, und es können mehrere Community-VLANs für dasselbe Private VLAN im System koexistieren.

Beispiele für die Verwendung solcher VLANs sind in **Abbildung 1** und **Abbildung 2** gezeigt.

Hostdatenverkehr wird in isolierte und Community-VLANs übertragen, Server- und Router-Datenverkehr hingegen in das primäre VLAN.

Das Erlernen gemeinsam verwendete MAC-Adressen erfolgt zwischen allen VLANs, die Mitglieder desselben Private VLAN sind (auch wenn der Switch das unabhängige Erlernen von VLANs unterstützt). Dies ermöglicht die Übertragung von Unicast-Datenverkehr trotz der Tatsache, dass Host-MAC-Adressen von isolierten und Community-VLANs erlernt werden, während die MAC-Adressen von Routern und Servern vom primären VLAN erlernt werden.

Ein Private VLAN-Port kann nur genau einem Private VLAN hinzugefügt werden. Andere Porttypen wie Zugriffs- oder Trunk-Ports können den einzelnen VLANs hinzugefügt werden, aus denen sich das Private VLAN zusammensetzt (denn es handelt sich hierbei um reguläre 802.1Q-VLANs).

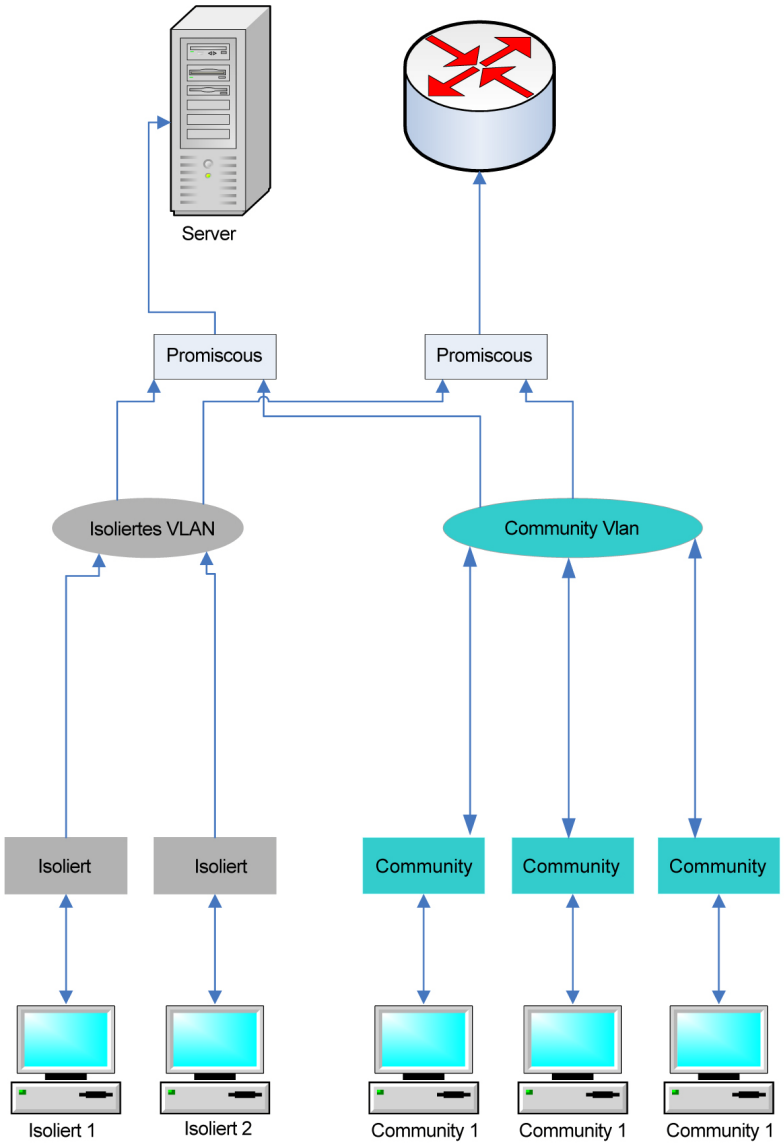
Ein Private VLAN kann so konfiguriert werden, dass es sich über mehrere Switches erstreckt. Hierzu werden Ports zwischen Switches als Trunk-Ports konfiguriert und allen VLANs im Private VLAN hinzugefügt. Trunk-Ports zwischen Switches senden und empfangen getaggten Datenverkehr aus den verschiedenen VLANs des Private VLAN (Primäres VLAN, isolierte VLANs und Communitys).

Der Switch unterstützt 16 primäre und 256 sekundäre VLANs.

Datenfluss

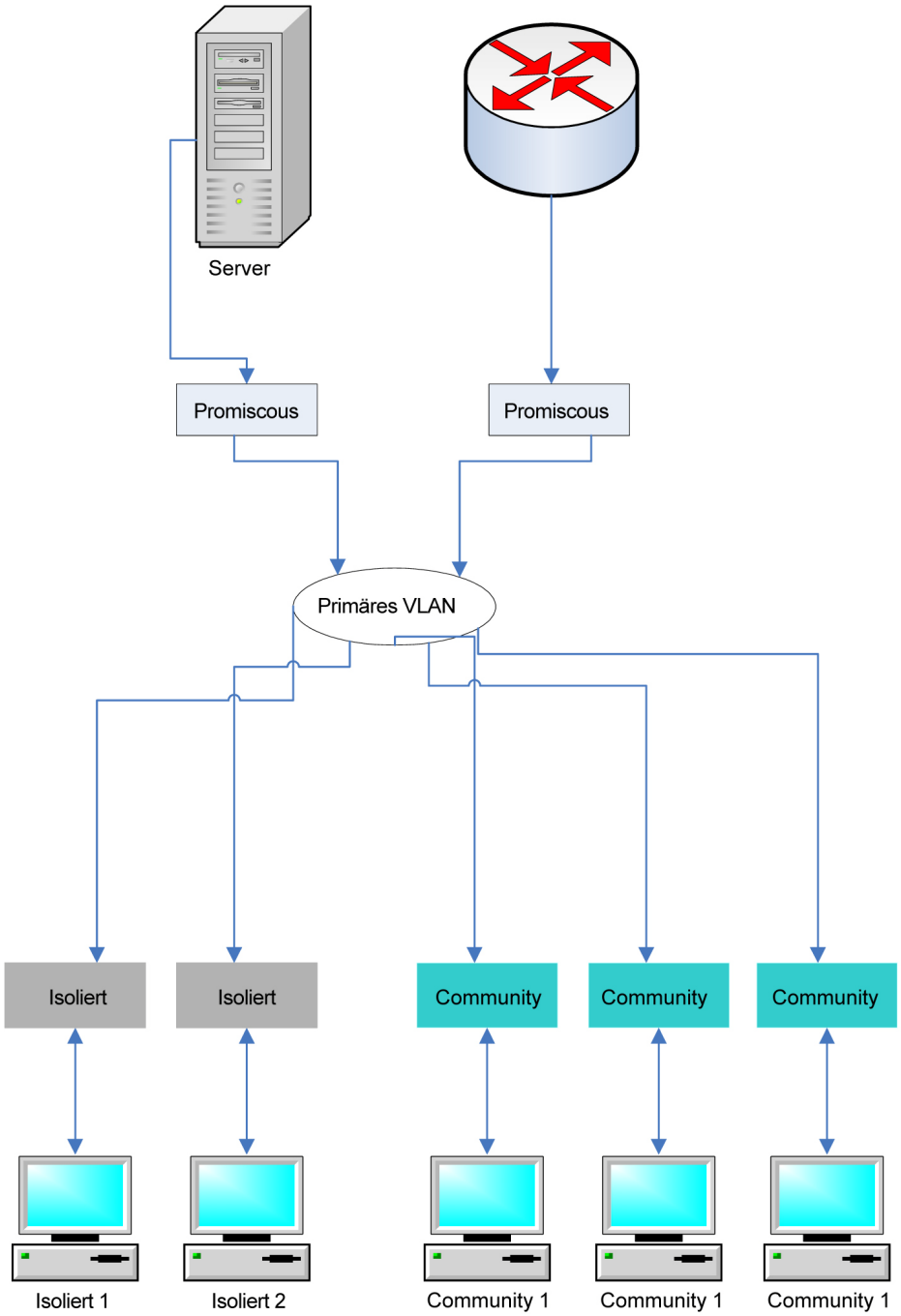
Nachfolgend gezeigt wird der Datenfluss von Hosts zu Servern bzw. Routern oder anderen Hosts.

Abbildung 1 Datenverkehr von Hosts zu Servern/Routern



Nachfolgend gezeigt wird der Datenfluss von Servern bzw. Routern zu Hosts.

Abbildung 2 Datenverkehr von Servern/Routern zu Hosts



Interaktion mit anderen Funktionen

In diesem Abschnitt wird die Interaktion zwischen Private VLANs und anderen Systemfunktionen beschrieben.

Im Private VLAN unterstützte Funktionen

Die folgenden Optionen können nur in einem primären VLAN (also nicht in einem isolierten oder einem Community-VLAN) aktiviert werden, wirken sich allerdings auf alle VLANs im Private VLAN aus.

- IGMP- und MLD-Snooping IGMP-Berichte und -Anfragen werden in allen VLANs im Private VLAN erkannt, jedoch werden die resultierenden Multicast-Einträge nur der FDB des primären VLANs hinzugefügt. Dies ermöglicht es, Multicast-Datenverkehr weiterzuleiten, statt ihn im primären VLAN zu fluten. In isolierten und Community-VLANs wird Multicast-Datenverkehr weiterhin geflutet.
- DHCP-Snooping
- ARP-Prüfung
- IP Source Guard

Das Hinzufügen oder Entfernen von isolierten oder Community-VLANs zu einem Private VLAN wird durch das System unterbunden, solange die oben genannten Funktionen aktiviert sind.

Im Private VLAN nicht unterstützte Funktionen

Die folgenden Funktionen werden weder in Private VLANs noch in VLANs unterstützt, aus denen sich das Private VLAN zusammensetzt:

- Auto-Voice-VLAN
- Standard-VLAN
- DHCP-Relais
- Nach 802.1x nicht authentifiziertes VLAN
- Gast-VLAN
- IPv4 und IPv6. IPv6/IPv6 kann in einem primären VLAN definiert werden. Isolierte und Community-Ports bieten keine IP-Konnektivität. Für IP-Konnektivität ist es erforderlich, dass Datenverkehr in einem primären VLAN übertragen werden kann.

Für Portmodi im Private VLAN nicht unterstützte Funktionen

Die folgenden Funktionen werden für Portmodi im Private VLAN nicht unterstützt:

- GVRP
- Automatische Erkennung von Sprach-VLAN-OUIs

- Gast-VLAN an 802.1x-Port
- Dynamic VLAN Assignment an 802.1x-Port
- Multicast-TV-VLAN

HINWEIS Beachten Sie die folgenden Details:

- Port-Sicherheit: MAC-Einträge in der VLAN-FDB-Tabelle werden geleert, wenn der Port entsperrt wird.
- Die Port-Mitgliedschaft in einem Private VLAN entspricht hinsichtlich der Beschränkungen bei der Funktionsinteraktion der Port-Mitgliedschaft in 802.1Q-VLANs. Beispiele:
  - Ein Port darf keiner LAG/LACP hinzugefügt werden.
  - Ein Port darf nicht als Ziel für einen Port-Monitor konfiguriert werden.

Erforderliche Ressourcen

Da sich ein Private VLAN aus mehreren 802.1Q-VLANs zusammensetzt, benötigt das System für jedes sekundäre VLAN in einem Private VLAN zusätzliche Ressourcen. Die Ressourcen für die folgenden Funktionen werden für jedes VLAN innerhalb des Private VLAN separat zugewiesen.

- **Dynamische MAC-Adressen**: Die in primären VLANs erlernten MAC-Adressen werden in alle Community-VLANs und in das isolierte VLAN kopiert. Im isolierten VLAN und in Community-VLANs erlernte MAC-Adressen werden in das primäre VLAN kopiert.
- **DHCP-Snooping**: Für DHCP-Datenverkehrs-Traps ist eine TCAM-Regel erforderlich.
- **ARP-Prüfung**: Für ARP-Datenverkehrs-Traps ist eine TCAM-Regel erforderlich.
- **IP Source Guard**: Für das Weiterleiten oder Verwerfen von IP-Datenverkehr ist eine TCAM-Regel erforderlich.
- **Sicherheit des ersten Hops**: Für IPv6-Datenverkehrs-Traps ist eine TCAM-Regel erforderlich (sofern IPv6 Source Guard aktiviert ist).

Konfigurationsrichtlinien

Beachten Sie die folgenden Richtlinien für die Konfiguration von Funktionen:

- **MSTP**: Alle VLANs in einen Private VLAN müssen derselben MSTP-Instanz zugewiesen sein.
- **IP Source Guard**: Von der Bindung einer ACL auf IP Source Guard-Ports an ein Private VLAN wird aufgrund der Menge benötigter TCAM-Ressourcen abgeraten.

Reguläre VLANs

In diesem Abschnitt werden die zum Konfigurieren der verschiedenen VLAN-Typen verwendeten GUI-Seiten beschrieben. In diesem Abschnitt werden folgende Prozesse beschrieben:

- **Workflow der VLAN-Konfiguration**
- **VLAN-Standardeinstellungen**
- **VLAN-Einstellungen – Erstellen von VLANs**
- **Schnittstelleneinstellungen**
- **VLAN-Mitgliedschaft**
- **Port zu VLAN**
- **Port-VLAN-Mitgliedschaft**
- **Definieren von GVRP-Einstellungen**

Workflow der VLAN-Konfiguration

So konfigurieren Sie VLANs:

1. Ändern Sie bei Bedarf das Standard-VLAN wie im Abschnitt **VLAN-Standardeinstellungen** beschrieben.
2. Erstellen Sie die erforderlichen VLANs wie im Abschnitt **VLAN-Einstellungen – Erstellen von VLANs** beschrieben.
3. Legen Sie wie im Abschnitt **Schnittstelleneinstellungen** beschrieben die gewünschte VLAN-Konfiguration für Ports fest und aktivieren Sie QinQ für eine Schnittstelle.
4. Weisen Sie den VLANs wie in den Abschnitten **Port zu VLAN** bzw. **Port-VLAN-Mitgliedschaft** beschrieben Schnittstellen zu.
5. Zeigen Sie wie im Abschnitt **Port-VLAN-Mitgliedschaft** beschrieben die aktuelle VLAN-Portmitgliedschaft für alle Schnittstellen an.
6. Konfigurieren Sie bei Bedarf VLAN-Gruppen gemäß der Beschreibung in den Abschnitten **MAC-basierte Gruppen** und **Protokollbasierte VLANs**.
7. Konfigurieren Sie bei Bedarf TV-VLAN gemäß der Beschreibung in den Abschnitten **Zugriffsport-Multicast-TV-VLAN** und **Kundenport-Multicast-TV-VLAN**.

VLAN-Standardeinstellungen

Bei Verwendung der werkseitig festgelegten Standardeinstellungen erstellt das Gerät automatisch VLAN 1 als Standard-VLAN. Der standardmäßige Schnittstellenstatus aller Ports ist „Trunk“, und alle Ports sind als Mitglieder des Standard-VLANs ohne Tag konfiguriert.

Das Standard-VLAN besitzt die folgenden Eigenschaften:

- Es ist individuell, nicht statisch/nicht dynamisch, und alle Ports sind standardmäßig Mitglieder ohne Tag.
- Es kann nicht gelöscht werden.
- Ihm kann keine Bezeichnung zugewiesen werden.
- Es kann nicht für eine spezielle Rolle verwendet werden, beispielsweise als nicht authentifiziertes VLAN oder Voice-VLAN. Dies ist nur für OUI-fähiges Voice-VLAN relevant.
- Ist ein Port nicht mehr Mitglied eines VLAN, konfiguriert das Gerät den Port im Standard-VLAN automatisch als Mitglied ohne Tag. Ein Port ist kein Mitglied eines VLAN, wenn das VLAN gelöscht oder der Port aus dem VLAN entfernt wird.
- RADIUS-Server können das Standard-VLAN mit der dynamischen VLAN-Zuweisung nicht für 802.1x-Anfrager zuweisen.

Wenn Sie die VID des Standard-VLANs ändern, führt das Gerät an allen Ports des VLANs nach dem Konfigurieren und Neustarten des Geräts Folgendes durch:

- Er entfernt die VLAN-Mitgliedschaft der Ports aus dem ursprünglichen Standard-VLAN (wird erst nach einem Neustart wirksam).
- Er ändern die PVID (Port VLAN Identifier) der Ports in die VID des neuen Standard-VLAN.
- Die ursprüngliche Standard-VLAN-ID wird vom Gerät entfernt. Soll sie verwendet werden, müssen Sie diese neu erstellen.
- Er ändert die Ports für das neue Standard-VLAN in VLAN-Mitglieder ohne Tag.

So ändern Sie das Standard-VLAN:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **VLAN-Standardeinstellungen**.

SCHRITT 2 Geben Sie den Wert in das folgende Feld ein:

- **Aktuelle Standard-VLAN-ID**: Zeigt die aktuelle Standard-VLAN-ID an.
- **Standard-VLAN-ID nach Neustart**: Geben Sie eine neue VLAN-ID ein, durch die die Standard-VLAN-ID nach dem Neustart ersetzt werden soll.

SCHRITT 3 Klicken Sie auf **Übernehmen**.

SCHRITT 4 Klicken Sie auf **Speichern** (in der oberen rechten Ecke des Fensters) und speichern Sie die aktuelle Konfiguration als Startkonfiguration.

Die **Standard-VLAN-ID nach Neustart** wird nach dem Neustart des Geräts die **Aktuelle Standard-VLAN-ID**.

VLAN-Einstellungen – Erstellen von VLANs

Sie können ein VLAN erstellen, jedoch wird dieses erst dann aktiv, wenn Sie das VLAN entweder manuell oder dynamisch mit mindestens einem Port verbinden. Ports müssen immer einem oder mehreren VLANs angehören.

Jedes VLAN muss mit einer eindeutigen VID mit einem Wert zwischen 1 und 4094 konfiguriert werden. Das Gerät reserviert die VID 4095 für das Discard-VLAN. Alle für das Discard-VLAN klassifizierten Pakete werden bei Eingang verworfen und nicht an einen Port weitergeleitet.

So erstellen Sie ein VLAN:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **VLAN-Einstellungen**.

Informationen für alle definierten VLANs werden angezeigt. Die Felder werden unten auf der Seite **Hinzufügen** definiert. Das folgende Feld befindet sich nicht auf der Seite **Hinzufügen**.

- **Ersteller**: Gibt an, wie das VLAN erstellt wurde:
  - *GVRP*: Das VLAN wurde mit GVRP (Generic VLAN Registration Protocol) dynamisch erstellt.
  - *Statisch*: Das VLAN ist benutzerdefiniert.
  - *Standard*: Das VLAN ist das Standard-VLAN.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, um ein oder mehrere neue VLANs hinzuzufügen.

Auf dieser Seite können Sie ein einzelnes VLAN oder mehrere VLANs erstellen.

SCHRITT 3 Um ein einzelnes VLAN zu erstellen, wählen Sie das Optionsfeld **VLAN** und geben die **VLAN-ID** und optional den **VLAN-Namen** ein.

Um mehrere VLANs zu erstellen, wählen Sie das Optionsfeld **Bereich** und geben die zu erstellenden VLANs ein, indem Sie die Start-VID und die eingeschlossene End-VID eingeben. Wenn Sie die Funktion **Bereich** verwenden, können Sie jeweils maximal 100 VLANs erstellen.

SCHRITT 4 Fügen Sie die folgenden Felder für die neuen VLANs hinzu.

- **VLAN-Schnittstellenstatus**: Wählen Sie diese Option, um das VLAN zu deaktivieren. In diesem Status kann das VLAN Meldungen weder an übergeordnete Ebenen senden noch von dort empfangen. Wenn Sie beispielsweise ein VLAN deaktivieren, in dem eine IP-Schnittstelle konfiguriert ist, wird das Bridging in das VLAN zwar fortgesetzt, doch kann der Switch IP-Datenverkehr im VLAN weder senden noch empfangen.
- **Leitungsstatus-SNMP-Traps**: Wählen Sie diese Option aus, um die Erzeugung von SNMP-Traps zum Link-Status zu aktivieren.

SCHRITT 5 Klicken Sie auf **Übernehmen**, um das VLAN bzw. die VLANs zu erstellen.

Schnittstelleneinstellungen

Auf der Seite „Schnittstelleneinstellungen“ können Sie die Konfiguration der VLAN-bezogenen Parameter für alle Schnittstellen anzeigen und ändern.

So konfigurieren Sie die VLAN-Einstellungen:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **Schnittstelleneinstellungen**.

SCHRITT 2 Wählen Sie einen Schnittstellentyp aus (Port oder LAG), und klicken Sie auf **Los**. Hier werden Ports oder LAGs und die zugehörigen VLAN-Parameter angezeigt.

SCHRITT 3 Zum Konfigurieren eines Ports oder einer LAG wählen Sie den Port bzw. die LAG aus und klicken Sie auf **Bearbeiten**.

SCHRITT 4 Geben Sie Werte für die folgenden Felder ein:

- **Schnittstelle**: Wählen Sie einen Port bzw. eine LAG aus.
- **Schnittstellen-VLAN-Modus**: Wählen Sie den Schnittstellenmodus für das VLAN. Folgende Optionen sind möglich:
  - *Allgemein*: Die Schnittstelle kann alle Funktionen gemäß der Spezifikation IEEE 802.1q unterstützen. Die Schnittstelle kann ein Mitglied mit oder ohne Tag in einem oder mehreren VLANs sein.
  - *Zugriff*: Die Schnittstelle ist ein Mitglied ohne Tag in einem einzelnen VLAN. Ein in diesem Modus konfigurierter Port wird als Zugriffs-Port bezeichnet.
  - *Trunk*: Die Schnittstelle ist ein Mitglied ohne Tag in höchstens einem VLAN, und sie ist ein Mitglied mit Tag in null oder mehreren VLANs. Ein in diesem Modus konfigurierter Port wird als Trunk-Port bezeichnet.

- *Kunde*: Wenn Sie diese Option auswählen, wird die Schnittstelle in den QinQ-Modus versetzt. Dies ermöglicht es Ihnen, im gesamten Netzwerk des Dienstanbieters Ihre eigene VLAN-Konfiguration (PVID) zu verwenden. Das Gerät befindet sich im QinQ-Modus, wenn es mindestens einen Kundenport hat. Weitere Informationen hierzu finden Sie unter **QinQ**.
- Private VLAN – Host: Wählen Sie diese Option aus, um die Schnittstelle entweder als isolierte oder als Community-Schnittstelle festzulegen. Wählen Sie danach entweder ein isoliertes oder ein Community-VLAN im Feld „Sekundäres VLAN – Host“ aus.
- „Private VLAN – Promiscuous“: Wayne Sie diese Option aus, um die Schnittstelle als Promiscuous-Schnittstelle festzulegen.

- **Administrative PVID**: Geben Sie die Port-VLAN-ID (PVID) des VLANs ein, für das eingehende Frames ohne Tag und Frames mit Prioritäts-Tag klassifiziert werden. Die möglichen Werte sind 1 bis 4094.
- **Frame-Typ**: Wählen Sie den Typ des Frames aus, den die Schnittstelle empfangen kann. Frames, die nicht dem konfigurierten Frame-Typ entsprechen, werden am Eingang verworfen. Diese Frame-Typen stehen nur im allgemeinen Modus zur Verfügung. Folgende Werte sind möglich:
  - *Alle zulassen*: Die Schnittstelle akzeptiert alle Frame-Typen: Frames ohne Tag, Frames mit Tag und Frames mit Prioritäts-Tag.
  - *Nur mit Tag zulassen*: Die Schnittstelle akzeptiert nur Frames mit Tag.
  - *Nur ohne Tag zulassen*: Die Schnittstelle akzeptiert nur Frames ohne Tag und Frames mit Prioritäts-Tag.
- **Eingangsfilterung**: (Nur im allgemeinen Modus verfügbar.) Wählen Sie diese Option, um die Eingangsfilterung zu aktivieren. Ist die Eingangsfilterung für eine Schnittstelle aktiviert, verwirft die Schnittstelle alle eingehenden Frames, die als VLANs klassifiziert sind, denen die Schnittstelle nicht angehört. Die Eingangsfilterung kann für allgemeine Ports deaktiviert oder aktiviert werden. Für Zugriffs-Ports und Trunk-Ports ist sie immer aktiviert.
- **Primäres VLAN**: Wählen Sie das primäre VLAN im Private VLAN aus. Das primäre VLAN gestattet die Herstellung von Schicht-2-Konnektivität von Promiscuous-Ports mit isolierten und Community-Ports.
- **Sekundäres VLAN – Host**: Wählen Sie ein isoliertes oder Community-VLAN für Hosts aus, die nur ein einzelnes sekundäres VLAN benötigen.
- **Ausgewählte sekundäre VLANs**: Verschieben Sie bei Promiscuous-Ports alle sekundären VLANs, die für die normale Paketweiterleitung erforderlich sind, aus der Liste **Verfügbare sekundäre VLANs** hierher. Promiscuous- und Trunk-Ports können Mitglieder mehrerer VLANs sein.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die Parameter werden in die aktuelle Konfigurationsdatei geschrieben.

VLAN-Mitgliedschaft

Auf den Seiten „Port zu VLAN“ und „Port-VLAN-Mitgliedschaft“ werden die VLAN-Mitgliedschaften der Ports in verschiedenen Darstellungen angezeigt. Auf diesen Seiten können Sie Mitgliedschaften für VLANs hinzufügen oder entfernen.

Ist die Standard-VLAN-Mitgliedschaft für einen Port nicht zugelassen, kann dieser Port kein Mitglied in anderen VLANs sein. Dem Port wird die interne VID 4095 zugewiesen.

Um Pakete ordnungsgemäß weiterzuleiten, müssen VLAN-fähige Zwischengeräte, die VLAN-Verkehr zwischen den Endknoten übertragen, entweder manuell konfiguriert werden oder die VLANs und ihre Portmitgliedschaften über GVRP (Generic VLAN Registration Protocol) dynamisch erhalten.

Bei der Mitgliedschaft eines Ports ohne Tag in zwei VLAN-fähigen Geräten ohne eingreifende VLAN-fähige Geräte muss das gleiche VLAN verwendet werden. Mit anderen Worten muss die PVID der Ports zwischen den beiden Geräten gleich sein, wenn die Ports Pakete ohne Tag an das VLAN senden und diese Pakete empfangen sollen. Ansonsten kann der Verkehr zwischen dem einen und dem anderen VLAN verloren gehen.

Frames mit VLAN-Tag können über andere VLAN-fähige oder nicht VLAN-fähige Netzwerkgeräte übertragen werden. Ist ein Ziel-Endknoten nicht VLAN-fähig und erhält seinen Verkehr von einem VLAN, muss das letzte VLAN-fähige Gerät (sofern eines vorhanden ist) die Frames des Ziel-VLAN ohne Tag an den Endknoten übertragen.

Port zu VLAN

Auf der Seite „Port zu VLAN“ können Sie die Ports in einem bestimmten VLAN anzeigen und konfigurieren.

So ordnen Sie einem VLAN Ports oder LAGs zu:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **Port zu VLAN**.

SCHRITT 2 Wählen Sie ein VLAN und den Schnittstellentyp (Port oder LAG) aus und klicken Sie auf **Los**, um die Porteigenschaften für das VLAN anzuzeigen oder zu ändern.

Der Portmodus für jeden Port oder jede LAG wird mit dem aktuellen Portmodus (Zugriffsport, Trunk-Port, allgemeiner Port, Private-Host-Port, Private-Promiscuous-Port oder benutzerdefinierter Port) angezeigt, den Sie auf der Seite „Schnittstelleneinstellungen“ konfiguriert haben.

Jeder Port und jede LAG wird mit der aktuellen Registrierung für das VLAN angezeigt.

SCHRITT 3 Sie ändern die Registrierung einer Schnittstelle für das VLAN, indem Sie den zugehörigen **Schnittstellennamen** auswählen und dann in der folgenden Liste die gewünschte Option wählen:

- **VLAN-Modus**: Porttyp im VLAN.

- **Mitgliedschaftstyp**:
  - *Verboten*: Die Schnittstelle darf dem VLAN nicht hinzugefügt werden, auch nicht über die GVRP-Registrierung. Wenn ein Port nicht Mitglied eines anderen VLAN ist, wird der Port durch das Aktivieren dieser Option Teil des internen VLAN 4095 (mit einer reservierten VID).
  - „Ausgeschlossen“: Die Schnittstelle ist zurzeit kein Mitglied des VLAN. Dies ist die Standardeinstellung für alle Ports und LAGs. Der Port kann dem VLAN über die GVRP-Registrierung hinzugefügt werden.
  - *Mit Tag*: Die Schnittstelle gehört dem VLAN als Mitglied mit Tag an.
  - *Ohne Tag*: Die Schnittstelle gehört dem VLAN als Mitglied ohne Tag an. Frames des VLAN werden ohne Tag an das Schnittstellen-VLAN gesendet.
  - **PVID**: Wählen Sie diese Option, um die PVID der Schnittstelle auf die VID des VLAN einzustellen. Die PVID wird pro Port eingestellt.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Schnittstellen werden dem VLAN zugewiesen und in die aktuelle Konfigurationsdatei geschrieben.

Sie können die Mitgliedschaften eines anderen VLAN anzeigen und/oder konfigurieren, indem Sie eine andere VLAN-ID auswählen.

Port-VLAN-Mitgliedschaft

Auf der Seite „Port-VLAN-Mitgliedschaft“ werden alle Ports des Geräts zusammen mit einer Liste der VLANs angezeigt, zu denen der jeweilige Port gehört.

Wenn die portbasierte Authentifizierungsmethode für eine Schnittstelle auf „802.1x“ und die administrative Portsteuerung auf „Autom.“ festgelegt ist, gilt Folgendes:

- Bis zur Authentifizierung wird der Port von allen VLANs mit Ausnahme von Gast-VLANs und nicht authentifizierten VLANs ausgeschlossen. Auf der Seite „VLAN zu Port“ wird der Port mit dem Großbuchstaben „P“ gekennzeichnet.
- Wenn der Port authentifiziert ist, erhält er die Mitgliedschaft in dem VLAN, in dem er konfiguriert wurde.

So weisen Sie einen Port einem oder mehreren VLANs zu:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **Port-VLAN-Mitgliedschaft**.

SCHRITT 2 Wählen Sie einen Schnittstellentyp (Port oder LAG) aus und klicken Sie auf **Los**. Die folgenden Felder werden für alle Schnittstellen des ausgewählten Typs angezeigt:

- **Schnittstelle**: Port-/LAG-ID.
- **Modus**: Der Schnittstellen-VLAN-Modus, der auf der Seite „Schnittstelleneinstellungen“ ausgewählt wurde.
- **Administrative VLANs**: Dropdown-Liste mit allen VLANs, denen die Schnittstelle möglicherweise als Mitglied angehört.
- **Betriebs-VLANs**: Dropdown-Liste mit allen VLANs, denen die Schnittstelle zurzeit als Mitglied angehört.
- **LAG**: Wenn ein Port als Schnittstelle ausgewählt wurde, wird die LAG angezeigt, der er als Mitglied angehört.

SCHRITT 3 Wählen Sie einen Port aus, und klicken Sie auf die Schaltfläche **Mit VLAN verbinden**.

SCHRITT 4 Geben Sie Werte für die folgenden Felder ein:

- **Schnittstelle**: Wählen Sie einen Port oder eine LAG aus. Wählen Sie die Einheit bzw. den Slot an einem Gerät der Serie 500 aus.
- **Modus**: Zeigt den Port-VLAN-Modus an, der auf der Seite „Schnittstelleneinstellungen“ ausgewählt wurde.
- **VLAN auswählen**: Um einen Port einem oder mehreren VLANs zuzuordnen, bewegen Sie die VLAN-IDs mit den Pfeiltasten von der linken Liste in die rechte Liste. In der rechten Liste wird möglicherweise die Standard-VLAN angezeigt, wenn der Port ein Tag besitzt. Die Auswahl ist jedoch nicht möglich.
- **Tagging**: Wählen Sie eine der folgenden Tagging-/PVID-Optionen:
  - **Verboten**: Die Schnittstelle darf dem VLAN nicht hinzugefügt werden, auch nicht über die GVRP-Registrierung. Wenn ein Port nicht Mitglied eines anderen VLAN ist, wird der Port durch das Aktivieren dieser Option Teil des internen VLAN 4095 (mit einer reservierten VID).
  - **Mit Tag**: Legt fest, ob der Port über ein Tag verfügen soll.
  - **Ausgeschlossen**: Die Schnittstelle ist zurzeit kein Mitglied des VLAN. Dies ist die Standardeinstellung für alle Ports und LAGs. Der Port kann dem VLAN über die GVRP-Registrierung hinzugefügt werden.
  - **Mit Tag**: Legt fest, dass der Port über ein Tag verfügen soll. Für Zugriffs-Ports ist dies nicht relevant.
  - **Ohne Tag**: Legt fest, dass der Port über kein Tag verfügen soll. Für Zugriffs-Ports ist dies nicht relevant.

- **Multicast-TV-VLAN**: Die Schnittstelle, die für Digital-TV mit Multicast-IP verwendet wird. Der Port verbindet das VLAN mit einem VLAN-Tag des Multicast-TV-VLAN. Weitere Informationen finden Sie unter **Zugriffsport-Multicast-TV-VLAN**.
- **PVID**: Die Port-PVID wird auf dieses VLAN eingestellt. Wenn sich die Schnittstelle im Zugriffs-Modus oder Trunk-Modus befindet, richtet das Gerät die Schnittstelle im VLAN automatisch als Mitglied ohne Tag ein. Wenn sich die Schnittstelle im allgemeinen Modus befindet, müssen Sie die VLAN-Mitgliedschaft manuell konfigurieren.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die Einstellungen werden geändert und in die aktuelle Konfigurationsdatei geschrieben.

Um die administrativen VLANs und Betriebs-VLANs an einer Schnittstelle anzuzeigen, klicken Sie auf **Details**.

Einstellungen für Private VLANs

Auf der Seite „Einstellungen für Private VLANs“ werden die definierten Private VLANs angezeigt.

So erstellen Sie ein neues Private VLAN:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **Einstellungen für Private VLANs**.

SCHRITT 2 Klicken Sie auf die Schaltfläche **Hinzufügen**.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **ID des primären VLANs**: Wählen Sie ein VLAN aus, das als primäres VLAN im Private VLAN definiert wird. Das primäre VLAN gestattet die Herstellung von Schicht-2-Konnektivität von Promiscuous-Ports mit isolierten und Community-Ports.
- **ID des isolierten VLAN**: Ein isoliertes VLAN ermöglicht isolierten Ports das Senden von Datenverkehr in das primäre VLAN.
- **Verfügbare Community-VLANs**: Verschieben Sie die VLANs, die als Community-VLANs fungieren sollen, in die Liste **Ausgewählte Community-VLANs**. Community-VLANs ermöglichen Schicht-2-Konnektivität von Community-Ports zu Promiscuous-Ports und zu Community-Ports derselben Community.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Einstellungen werden geändert und in die aktuelle Konfigurationsdatei geschrieben.

GVRP-Einstellungen

Angrenzende VLAN-fähige Geräte können VLAN-Informationen über GVRP (Generic VLAN Registration Protocol) austauschen. GVRP basiert auf dem GARP (Generic Attribute Registration Protocol) und propagiert VLAN-Informationen innerhalb eines gesamten überbrückten Netzwerks.

Da GVRP Tagging-Unterstützung erfordert, muss der Port im Trunk-Modus oder im allgemeinen Modus konfiguriert sein.

Wenn ein Port einem VLAN unter Verwendung von GVRP beitritt, wird er dem VLAN als dynamisches Mitglied hinzugefügt, sofern Sie dies nicht auf der Seite „Port-VLAN-Mitgliedschaft“ ausdrücklich unterbunden haben. Wenn das VLAN nicht existiert, wird es dynamisch erstellt, wenn die dynamische VLAN-Erstellung für diesen Port (auf der Seite „GVRP-Einstellungen“) aktiviert ist.

GVRP muss sowohl global als auch für jeden einzelnen Port aktiviert werden. Ist es aktiviert, werden GPDUs (GARP Packet Data Units) übertragen und empfangen. VLANs, die definiert aber nicht aktiv sind, werden nicht propagiert. Um das VLAN zu propagieren, muss es mindestens an einem Port ausgeführt werden.

Standardmäßig ist GVRP global und für Ports deaktiviert.

Definieren von GVRP-Einstellungen

So definieren Sie GVRP-Einstellungen für eine Schnittstelle:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **GVRP-Einstellungen**.

SCHRITT 2 Wählen Sie **Globaler GVRP-Status** aus, um GVRP global zu aktivieren.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um den globalen GVRP-Status einzustellen.

SCHRITT 4 Wählen Sie einen Schnittstellentyp (Port oder LAG) aus und klicken Sie auf **Los**, um alle Schnittstellen dieses Typs anzuzeigen.

SCHRITT 5 Um die GVRP-Einstellungen für einen Port zu definieren, markieren Sie diesen und wählen **Bearbeiten**.

SCHRITT 6 Geben Sie Werte für die folgenden Felder ein:

- **Schnittstelle**: Dient zum Auswählen der zu bearbeitenden Schnittstelle (Port oder LAG).
- **GVRP-Status**: Dient zum Aktivieren von GVRP für diese Schnittstelle.
- **Dynamische VLAN-Erstellung**: Dient zum Aktivieren der dynamischen VLAN-Erstellung für diese Schnittstelle.
- **GVRP-Registrierung**: Dient zum Aktivieren der VLAN-Registrierung mit GVRP für diese Schnittstelle.

SCHRITT 7 Klicken Sie auf **Übernehmen**. Die GVRP-Einstellungen werden geändert und in die aktuelle Konfigurationsdatei geschrieben.

VLAN-Gruppen

In diesem Abschnitt wird beschrieben, wie Sie VLAN-Gruppen konfigurieren. Die folgenden Prozesse werden beschrieben:

- **MAC-basierte Gruppen**
- **Protokollbasierte VLANs**

VLAN-Gruppen werden für den Lastenausgleich des Verkehrs in einem Schicht-2-Netzwerk verwendet.

Pakete werden anhand verschiedener konfigurierter Klassifizierungen (beispielsweise VLAN-Gruppen) einem VLAN zugewiesen.

Wenn mehrere Klassifizierungsschemas definiert sind, werden Pakete in der folgenden Reihenfolge einem VLAN zugewiesen:

- **TAG**: Wenn das Paket über ein Tag verfügt, wird das VLAN dem Tag entnommen.
- **MAC-basiertes VLAN**: Wenn ein MAC-basiertes VLAN definiert ist, wird das VLAN der Zuordnung von Quell-MAC zu VLAN an der Eingangsschnittstelle entnommen.
- **Protokollbasiertes VLAN**: Wenn ein protokollbasiertes VLAN definiert ist, wird das VLAN der Zuordnung von Protokoll (Ethernet-Typ) zu VLAN an der Eingangsschnittstelle entnommen.
- **PVID**: Das VLAN wird der Standard-VLAN-ID des Ports entnommen.

MAC-basierte Gruppen

Mithilfe der MAC-basierten VLAN-Klassifizierung können Pakete anhand ihrer Quell-MAC-Adresse klassifiziert werden. Sie können dann die MAC-zu-VLAN-Zuordnung auf Schnittstellenbasis vornehmen.

Sie können verschiedene MAC-basierte VLAN-Gruppen definieren, die jeweils verschiedene MAC-Adressen enthalten.

Diese MAC-basierten Gruppen können bestimmten Ports/LAGs zugewiesen werden. MAC-basierte VLAN-Gruppen können keine überlappenden Bereiche von MAC-Adressen am gleichen Port enthalten.

In der folgenden Tabelle wird die Verfügbarkeit von MAC-basierten VLAN-Gruppen in verschiedenen SKUs beschrieben:

Tabelle 5 MAC-basierte VLAN-Gruppenverfügbarkeit

SKU	Systemmodus	Unterstützung von MAC-basierten VLAN-Gruppen
Sx300	**Schicht 2**	Ja
	Schicht 3	Nein
Sx500, Sx500ESW2-550X	**Schicht 2**	Ja
	Schicht 3	Nein
SG500X	**Nativ**	Ja
	Basis-Hybrid – Schicht 2	Ja
	Basis-Hybrid – Schicht 3	Nein
SG500XG	**Wie Sx500**	Ja

Workflow

So definieren Sie eine MAC-basierte VLAN-Gruppe:

1. Weisen Sie die MAC-Adresse einer VLAN-Gruppen-ID zu (auf der Seite „MAC-basierte Gruppen“).
2. Für jede erforderliche Schnittstelle:
   a. Weisen Sie die VLAN-Gruppe einem VLAN zu (auf der Seite „MAC-basierte Gruppen für VLAN“). Die Schnittstellen müssen sich im allgemeinen Modus befinden.
   b. Wenn die Schnittstelle nicht zu einem VLAN gehört, weisen Sie sie manuell auf der Seite „Port zu VLAN“ dem VLAN zu.

MAC-basierte VLAN-Gruppen

Unter **Tabelle 5** finden Sie eine Beschreibung der Verfügbarkeit dieser Funktion.

So weisen Sie einer VLAN-Gruppe eine MAC-Adresse zu:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **VLAN-Gruppen** > **MAC-basierte Gruppen**.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **MAC-Adresse**: Geben Sie eine MAC-Adresse ein, die Sie einer VLAN-Gruppe zuweisen möchten.

  HINWEIS Diese MAC-Adresse kann keiner anderen VLAN-Gruppe zugewiesen werden.

- **Präfixmaske**: Geben Sie eines der folgenden Elemente ein:
  - *Host*: Quell-Host der MAC-Adresse
  - *Länge*: *Präfix* der MAC-Adresse
- **Gruppen-ID**: Geben Sie eine benutzerdefinierte VLAN-Gruppen-ID ein.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die MAC-Adresse wird einer VLAN-Gruppe zugewiesen.

VLAN-Gruppe zu VLAN pro Schnittstelle

Unter **Tabelle 5** finden Sie eine Beschreibung der Verfügbarkeit dieser Funktion.

Ports/LAGs müssen sich im allgemeinen Modus befinden.

So weisen Sie eine MAC-basierte VLAN-Gruppe einem VLAN an einer Schnittstelle zu:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **VLAN-Gruppen** > **MAC-basierte Gruppen für VLAN**.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **Gruppentyp**: Zeigt an, dass die Gruppe MAC-basiert ist.
- **Schnittstelle**: Geben Sie eine Schnittstelle (Port oder LAG) ein, über die Verkehr empfangen wird.
- **Gruppen-ID**: Wählen Sie eine auf der Seite „MAC-basierte Gruppen“ definierte VLAN-Gruppe aus.
- **VLAN-ID**: Wählen Sie das VLAN aus, an das der Verkehr von der VLAN-Gruppe weitergeleitet wird.

SCHRITT 4 Klicken Sie auf **Übernehmen**, um die Zuordnung der VLAN-Gruppe zu diesem VLAN durchzuführen. Durch diese Zuordnung wird die Schnittstelle nicht dynamisch an das VLAN gebunden; Sie müssen die Schnittstelle manuell dem VLAN hinzufügen.

Protokollbasierte VLANs

Sie können Gruppen von Protokollen definieren und diese dann an einen Port binden. Wenn die Protokollgruppe an einen Port gebunden ist, wird jedem Paket, das von einem Protokoll in der Gruppe stammt, das auf der Seite „Protokollbasierte Gruppen“ konfigurierte VLAN zugewiesen.

Workflow

So definieren Sie eine protokollbasierte VLAN-Gruppe:

1. Definieren Sie auf der Seite „Protokollbasierte Gruppen“ eine Protokollgruppe.
2. Weisen Sie auf der Seite „Protokollbasierte Gruppen zu VLAN“ die Protokollgruppe für jede Schnittstelle einem VLAN zu. Die Schnittstellen müssen sich im allgemeinen Modus befinden. Außerdem kann ihnen kein dynamisches VLAN (DVA) zugewiesen sein.

Protokollbasierte Gruppen

So definieren Sie einen Satz mit Protokollen:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **VLAN-Gruppen** > **Protokollbasierte Gruppen**.

Die Seite „Protokollbasierte Gruppen“ enthält die folgenden Felder:

- **Kapselung**: Zeigt das Protokoll an, auf dem die VLAN-Gruppe basiert.
- **Protokoll/DSAP-SSAP**: Zeigt den Protokollwert als Hexadezimalzahlen an.
- **Gruppen-ID**: Zeigt die ID der Protokollgruppe an, der die Schnittstelle hinzugefügt wird.

SCHRITT 2 Klicken Sie auf die Schaltfläche **Hinzufügen**. Die Seite „Protokollbasierte Gruppe hinzufügen“ wird angezeigt.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **Kapselung**: Der Pakettyp des Protokolls. Folgende Optionen stehen zur Verfügung:
  - *Ethernet V2*: Wenn diese Option ausgewählt ist, wählen Sie den **Ethernet-Typ** aus.
  - *LLC-SNAP (RFC 1042)*: Wenn diese Option ausgewählt ist, geben Sie den **Protokollwert** ein.
  - *LLC*: Wenn diese Option ausgewählt ist, wählen Sie die **DSAP-SSAP-Werte** aus.
- **Ethernet-Typ**: Wählen Sie den Ethernet-Typ für die Ethernet-V2-Kapselung aus. Hierbei handelt es sich um ein Feld mit zwei Oktetten im Ethernet-Frame, mit dem angegeben wird, welches Protokoll in der Nutzlast des Ethernet-Pakets für die VLAN-Gruppe gekapselt ist.
- **Protokollwert**: Geben Sie das Protokoll für die LLC-SNAP-Kapselung (rfc 1042) ein.

- **Gruppen-ID**: Geben Sie eine Protokollgruppen-ID ein.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Protokollgruppe wird hinzugefügt und in die aktuelle Konfigurationsdatei geschrieben.

Zuordnung von protokollbasierten Gruppen zu VLANs

Damit Sie eine Protokollgruppe einem Port zuordnen können, muss sich der Port im allgemeinen Modus befinden und DVA darf für den Port nicht konfiguriert sein (siehe **Schnittstelleneinstellungen**).

Sie können mehrere Gruppen an einen einzigen Port binden, wobei jeder Port einem eigenen VLAN zugeordnet ist.

Es ist auch möglich, mehrere Gruppen einem einzigen VLAN zuzuordnen.

So ordnen Sie den Protokollport einem VLAN zu:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **VLAN-Gruppen** > **Protokollbasierte Gruppen zu VLAN**.

Die zurzeit definierten Zuordnungen werden angezeigt.

SCHRITT 2 Um eine Schnittstelle einer protokollbasierten Gruppe und einem VLAN zuzuordnen, klicken Sie auf **Hinzufügen**.

Das Feld **Gruppentyp** zeigt den Typ der zugeordneten Gruppe an.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein.

- **Schnittstelle**: Die anhand einer protokollbasierten Gruppe einem VLAN zugewiesene Portnummer oder LAG-Nummer.
- **Gruppen-ID**: Protokollgruppen-ID.
- **VLAN-ID**: Verbindet die Schnittstelle mit einer benutzerdefinierten VLAN-ID.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Protokollports werden VLANs zugeordnet und in die aktuelle Konfigurationsdatei geschrieben.

Voice-VLAN

In einem LAN werden Sprachgeräte wie beispielsweise IP-Telefone, VoIP-Endpunkte und Sprachsysteme im gleichen VLAN platziert. Dieses VLAN wird als Voice-VLAN bezeichnet. Wenn sich die Sprachgeräte in verschiedenen Voice-VLANs befinden, werden für die Kommunikation IP-Router (Schicht 3) benötigt.

In diesem Abschnitt werden die folgenden Themen behandelt:

- **Voice-VLAN (Übersicht)**
- **Sprach-VLAN-Konfiguration**
- **Telefonie-OUI**

Voice-VLAN (Übersicht)

In diesem Abschnitt werden die folgenden Themen behandelt:

- **Dynamische Voice-VLAN-Modi**
- **Auto-Voice-VLAN, Auto-Smartports, CDP und LLDP**
- **Voice-VLAN-QoS**
- **Voice-VLAN-Beschränkungen**
- **Voice-VLAN-Workflows**

Beispiele für typische Szenarien für die Sprachbereitstellung mit entsprechenden Konfigurationen:

- **Mit UC3xx- oder UC5xx-Host:** Dieses Bereitstellungsmodell wird von allen Telefonen und VoIP-Endpunkten von Cisco unterstützt. Bei diesem Modell befinden sich das UC3xx- bzw. UC5xx-System, die Telefone von Cisco und die VoIP-Endpunkte im gleichen Voice-VLAN. Das Voice-VLAN-ID des UC3xx bzw. UC5xx heißt standardmäßig VLAN 100.
- **Mit IP PBX-Host eines Drittanbieters:** Dieses Bereitstellungsmodell wird vom Cisco SBTG CP-79xx, von SPA5xx-Telefonen und von SPA8800-Endpunkten unterstützt. Bei diesem Modell wird das von den Telefonen verwendete VLAN durch die Netzwerkkonfiguration bestimmt. Getrennte Voice- und Daten-VLANs können verwendet werden, dies muss jedoch nicht der Fall sein. Die Telefone und VoIP-Endpunkte werden bei einem vor Ort installierten IP PBX-System registriert.
- **Mit IP Centrex- oder ITSP-Host:** Dieses Bereitstellungsmodell wird vom Cisco CP-79xx, von SPA5xx-Telefonen und von SPA8800-Endpunkten unterstützt. Bei diesem Modell wird das von den Telefonen verwendete VLAN durch die Netzwerkkonfiguration bestimmt. Getrennte Voice- und Daten-VLANs können verwendet werden, dies muss jedoch nicht der Fall sein. Die Telefone und VoIP-Endpunkte werden bei einem nicht vor Ort installierten SIP-Proxy in der „Cloud“ registriert.

Aus Sicht des VLANs werden die oben beschriebenen Modelle in VLAN-fähigen sowie in nicht VLAN-fähigen Umgebungen betrieben. In der VLAN-fähigen Umgebung ist das Voice-VLAN eines von vielen in einer Installation konfigurierten VLANs. Das nicht VLAN-fähige Szenario ist das Äquivalent einer VLAN-fähigen Umgebung mit nur einem VLAN.

Das Gerät wird immer als VLAN-fähiger Switch betrieben.

Das Gerät unterstützt ein einziges Voice-VLAN. Das Voice-VLAN ist standardmäßig VLAN 1. Sie können manuell ein anderes Voice-VLAN konfigurieren. Das VLAN kann auch dynamisch gelernt werden, wenn die Funktion Auto-Voice-VLAN aktiviert ist.

Sie können dem Voice-VLAN gemäß der im Abschnitt „Konfigurieren der VLAN-Schnittstelleneinstellungen“ beschriebenen VLAN-Basiskonfiguration manuell Ports hinzufügen oder dazu sprachbezogene Smartport-Makros auf die Ports anwenden. Alternativ können die Ports dynamisch hinzugefügt werden, wenn sich das Gerät im Modus „Telefonie-OUI“ befindet oder wenn die Option „Auto-Smartport“ aktiviert ist.

Dynamische Voice-VLAN-Modi

Das Gerät unterstützt zwei dynamische Voice-VLAN-Modi: „Telefonie-OUI“ (Organization Unique Identifier) und „Auto-Voice-VLAN“. Diese beiden Modi beeinflussen die Konfiguration der Portmitgliedschaften für ein VLAN und/oder Voice-VLAN. Die beiden Modi schließen sich gegenseitig aus.

- **Telefonie-OUI**

  Im Telefonie-OUI-Modus muss das Voice-VLAN ein manuell konfiguriertes VLAN sein, bei dem es sich nicht um das Standard-VLAN handeln darf.

  Wenn sich das Gerät im Telefonie-OUI-Modus befindet und ein Port manuell als Beitrittskandidat für das Voice-VLAN konfiguriert ist, fügt das Gerät den Port dynamisch dem Voice-VLAN hinzu, wenn es ein Paket mit einer Quell-MAC-Adresse empfängt, die einer der konfigurierten Telefonie-OUIs entspricht. Bei einer OUI handelt es sich um die ersten drei Byte einer Ethernet-MAC-Adresse. Weitere Informationen zu Telefonie-OUI finden Sie unter **Telefonie-OUI**.

- **Auto-Voice-VLAN**

  Im Auto-Voice-VLAN-Modus kann das Voice-VLAN das Standard-Voice-VLAN sein, manuell konfiguriert werden oder von externen Geräten wie beispielsweise einem UC3xx oder UC5xx und von Switches, die das Voice-VLAN in CDP oder VSDP ankündigen, gelernt werden. VSDP ist ein von Cisco definiertes Protokoll für die Erkennung von Sprachservices.

  Im Gegensatz zum Telefonie-OUI-Modus, in dem Sprachgeräte anhand der Telefonie-OUI erkannt werden, müssen im Auto-Voice-VLAN-Modus die Ports mit Auto-Smartport dem Voice-VLAN dynamisch hinzugefügt werden. Wenn Auto-Smartport aktiviert ist, wird dem Voice-VLAN ein Port hinzugefügt, sobald ein Gerät erkannt wird, das eine Verbindung mit dem Port herzustellen versucht und sich über CDP und/oder LLDP MED als Telefon oder Medienendpunkt ankündigt.

Sprachendpunkte

Um die korrekte Funktionsfähigkeit eines Voice-VLANs zu gewährleisten, müssen die Sprachgeräte wie beispielsweise Telefone von Cisco und VoIP-Endpunkte dem Voice-VLAN zugewiesen werden, über das der Sprachverkehr gesendet und empfangen wird. Beispiele für mögliche Szenarien:

- Ein Telefon oder Endpunkt kann statisch mit dem Voice-VLAN konfiguriert werden.
- Ein Telefon oder Endpunkt kann das Voice-VLAN aus der von einem TFTP-Server heruntergeladenen Boot-Datei beziehen. Die Boot-Datei und der TFTP-Server können vom DHCP-Server angegeben werden, wenn dieser dem Telefon eine IP-Adresse zuweist.
- Ein Telefon oder Endpunkt kann die Informationen zum Voice-VLAN aus CDP- und LLDP MED-Ankündigungen beziehen, die das Telefon bzw. der Endpunkt von benachbarten Sprachsystemen und Switches empfängt.

Das Gerät erwartet, dass die eine Verbindung herstellenden Sprachgeräte Voice-VLAN-Pakete mit Tag senden. An Ports, bei denen das Voice-VLAN gleichzeitig das native VLAN ist, sind Voice-VLAN-Pakete ohne Tag möglich.

Auto-Voice-VLAN, Auto-Smartports, CDP und LLDP

Standardeinstellungen

Gemäß den Werkseinstellungen sind CDP, LLDP und LLDP-MED im Gerät aktiviert, Auto-Smartport ist aktiviert, der QoS-Basismodus mit vertrauenswürdigem DSCP ist aktiviert und alle Ports sind Mitglieder von Standard-VLAN 1, das auch dem Standard-Voice-VLAN entspricht.

Außerdem ist für den Modus „Dynamisches Voice-VLAN“ standardmäßig Auto-Smartport mit auslöserbasierter Aktivierung festgelegt und für Auto-Smartport ist standardmäßig die Aktivierung abhängig von Auto-Voice-VLAN festgelegt.

Voice-VLAN-Auslöser

Wenn für den Modus „Dynamisches Voice-VLAN“ die Einstellung „Auto-Voice-VLAN aktivieren“ festgelegt ist, wird Auto-Voice-VLAN nur bei Vorliegen mindestens eines Auslösers aktiviert. Mögliche Auslöser sind eine statische Voice-VLAN-Konfiguration, in CDP-Ankündigungen von Nachbarn empfangene Voice-VLAN-Informationen und über VSDP (Voice VLAN Discovery Protocol) empfangene Voice-VLAN-Informationen. Bei Bedarf können Sie festlegen, dass Auto-Voice-VLAN ohne Warten auf einen Auslöser sofort aktiviert wird.

Wenn Auto-Smartport abhängig vom Auto-Voice-VLAN-Modus aktiviert ist, wird Auto-Smartport bei Aktivierung von Auto-Voice-VLAN aktiviert. Bei Bedarf können Sie Auto-Smartport unabhängig von Auto-Voice-VLAN verwenden.

HINWEIS Die hier genannte Standardkonfiguration gilt für Switches, deren Firmwareversion Auto-Voice-VLAN sofort ohne Konfiguration unterstützt. Sie gilt auch für nicht konfigurierte Switches, die auf die Firmwareversion mit Unterstützung für Auto-Voice-VLAN aktualisiert wurden.

HINWEIS Die Standardeinstellungen und Voice-VLAN-Auslöser haben keine Auswirkungen auf Installationen ohne Voice-VLAN oder auf bereits konfigurierte Switches. Sie können Auto-Voice-VLAN und/oder Auto-Smartport abhängig von Ihren Bereitstellungsanforderungen deaktivieren oder aktivieren.

Auto-Voice-VLAN

Auto-Voice-VLAN ist für die Verwaltung des Voice-VLANs zuständig, während die Portmitgliedschaften für das Voice-VLAN von Auto-Smartport verwaltet werden. Wenn Auto-Voice-VLAN aktiv ist, werden die folgenden Funktionen ausgeführt:

- Voice-VLAN-Informationen in CDP-Ankündigungen von direkt verbundenen Nachbargeräten werden erkannt.
- Wenn mehrere Nachbar-Switches und/oder -Router (beispielsweise Unified Communications-Geräte (UC) von Cisco) ihr Voice-VLAN ankündigen, wird das Voice-VLAN des Geräts mit der niedrigsten MAC-Adresse verwendet.

  HINWEIS Wenn Sie das Gerät mit einem UC-Gerät von Cisco verbinden möchten, müssen Sie möglicherweise den Port am UC-Gerät mit dem Befehl *`switchport voice vlan`* konfigurieren, um sicherzustellen, dass das UC-Gerät sein Voice-VLAN in CDP am Port ankündigt.
- Die Voice-VLAN-bezogenen Parameter werden über VSDP (Voice Service Discovery Protocol) mit anderen Auto-Voice-VLAN-fähigen Switches synchronisiert. Das Gerät konfiguriert sich selbst immer mit dem Voice-VLAN aus der ihm bekannten Quelle mit höchster Priorität. Die Priorität basiert auf dem Quelltyp und der MAC-Adresse der Quelle, von der die Voice-VLAN-Informationen bereitgestellt werden. Höchste Priorität bei den Quelltypen hat die statische VLAN-Konfiguration, gefolgt von CDP-Ankündigungen, der auf dem geänderten Standard-VLAN basierenden Standardkonfiguration und dem Standard-Voice-VLAN. Eine niedrige numerische MAC-Adresse hat eine höhere Priorität als eine hohe numerische MAC-Adresse.
- Das Voice-VLAN wird beibehalten, bis ein neues Voice-VLAN aus einer Quelle mit höherer Priorität erkannt wird oder die Auto-Voice-VLAN-Funktion vom Benutzer neu gestartet wird. Beim Neustart setzt das Gerät das Voice-VLAN auf das Standard-Voice-VLAN zurück und startet die Auto-Voice-VLAN-Erkennung neu.
- Wenn ein neues Voice-VLAN konfiguriert oder erkannt wird, wird es vom Gerät automatisch erstellt und alle Portmitgliedschaften des vorhandenen Voice-VLANs werden in das neue Voice-VLAN übernommen. Dadurch können bestehende Sprachsitzungen unterbrochen oder beendet werden, was bei Änderungen der Netzwerktopologie zu erwarten ist.

HINWEIS Wenn sich das Gerät im Schicht-2-Systemmodus befindet, kann es mit ausschließlich VSDP-fähigen Switches im selben Verwaltungs-VLAN synchronisieren. Wenn sich das Gerät im Schicht-3-Systemmodus befindet, kann es mit VSDP-fähigen Switches synchronisieren, die sich in den im Gerät konfigurierten direkt verbundenen IP-Subnetzen befinden.

Auto-Smartport verwaltet mithilfe von CDP/LLDP die Portmitgliedschaften des Voice-VLANs, wenn Sprachendpunkte an den Ports erkannt werden:

- Wenn CDP und LLDP aktiviert ist, sendet das Gerät regelmäßig CDP- und LLDP-Pakete, um den Sprachendpunkten das zu verwendende Voice-VLAN anzukündigen.
- Wenn sich ein Gerät, das eine Verbindung mit einem Port herstellt, über CDP und/oder LLDP als Sprachendpunkt ankündigt, wird der Port von Auto-Smartport automatisch dem Voice-VLAN hinzugefügt. Dazu wird das entsprechende Smartport-Makro auf den Port angewendet (wenn keine anderen Geräte am Port vorhanden sind, die eine im Konflikt stehende oder höhere Funktion ankündigen). Wenn sich ein Gerät als Telefon ankündigt, wird standardmäßig das Smartport-Makro „phone“ (Telefon) verwendet. Wenn sich ein Gerät als Telefon und Host oder als Telefon und Bridge ankündigt, wird standardmäßig das Smartport-Makro „phone+desktop“ (Telefon und Desktop) verwendet.

Voice-VLAN-QoS

Voice-VLAN kann die CoS/802.1p- und DSCP-Einstellungen mithilfe von LLDP MED-Netzwerkrichtlinien verbreiten. LLDP MED ist standardmäßig so eingerichtet, dass die Funktion mit der Voice-QoS-Einstellung antwortet, wenn ein Gerät LLDP MED-Pakete sendet. Geräte mit MED-Unterstützung müssen beim Senden von Sprachverkehr die gleichen CoS/802.1p- und DSCP-Werte verwenden, die sie in der LLDP MED-Antwort erhalten haben.

Sie können die automatische Aktualisierung zwischen Voice-VLAN und LLDP MED deaktivieren und eigene Netzwerkrichtlinien verwenden.

Im OUI-Modus kann das Gerät außerdem die Zuordnung und Kommentierung (CoS/802.1p) des Sprachverkehrs auf der Grundlage der OUI konfigurieren.

Standardmäßig sind alle Schnittstellen nach CoS/802.1p vertrauenswürdig. Das Gerät wendet die QoS (Quality of Service) basierend auf dem CoS/802.1p-Wert im Sprachstrom an. Bei Auto-Voice-VLAN können Sie den Wert der Sprachströme mithilfe von erweitertem QoS außer Kraft setzen. Bei Telefonie-OUI-Sprachströmen können Sie QoS außer Kraft setzen und optional die 802.1p-Daten der Sprachströme kommentieren, indem Sie die gewünschten CoS/802.1p-Werte angeben und die Remarking-Option unter „Telefonie-OUI“ verwenden.

Voice-VLAN-Beschränkungen

Es bestehen die folgenden Beschränkungen:

- Es wird nur ein Voice-VLAN unterstützt.
- Ein VLAN, das als Voice-VLAN definiert ist, kann nicht entfernt werden.

Außerdem gelten für Telefonie-OUIs die folgenden Beschränkungen:

- Das Voice-VLAN kann nicht VLAN1 (das Standard-VLAN) sein.
- Für das Voice-VLAN kann Smartport nicht aktiviert sein.
- Das Voice-VLAN unterstützt DVA (Dynamic VLAN Assignment) nicht.
- Das Voice-VLAN kann nicht das Gast-VLAN sein, wenn sich das Voice-VLAN im OUI-Modus befindet. Wenn sich das Voice-VLAN im Modus „Autom." befindet, kann das Voice-VLAN das Gast-VLAN sein.
- Die Voice-VLAN-QoS-Entscheidung hat Priorität vor allen anderen QoS-Entscheidungen, ausgenommen die Richtlinie/ACL QoS-Entscheidung.
- Eine neue VLAN-ID kann für das Voice-VLAN nur konfiguriert werden, wenn das aktuelle Voice-VLAN keine Kandidatenports besitzt.
- Das Schnittstellen-VLAN eines Kandidatenports muss sich im allgemeinen Modus oder im Trunk-Modus befinden.
- Die Voice-VLAN-QoS wird auf Kandidatenports angewendet, die dem Voice-VLAN beigetreten sind, sowie auf statische Ports.
- Der Sprachverkehr wird akzeptiert, wenn die MAC-Adresse von der Weiterleitungsdatenbank erlernt werden kann. (Wenn im FDB kein freier Speicher zur Verfügung steht, erfolgt keine Aktion).

Voice-VLAN-Workflows

Die Standardkonfiguration des Geräts für Auto-Voice-VLAN, Auto-Smartports, CDP und LLDP deckt die gängigsten Szenarien für die Sprachbereitstellung ab. In diesem Abschnitt wird beschrieben, wie Sie Voice-VLAN bereitstellen, wenn die Standardkonfiguration nicht geeignet ist.

Workflow 1: So konfigurieren Sie Auto-Voice-VLAN:

SCHRITT 1 Öffnen Sie die Seite „VLAN-Verwaltung > Voice-VLAN > Eigenschaften".

SCHRITT 2 Wählen Sie die Voice-VLAN-ID aus. Diese kann nicht auf VLAN-ID 1 festgelegt werden (bei dynamischem Voice-VLAN ist dieser Schritt nicht erforderlich).

SCHRITT 3 Legen Sie **Dynamisches Voice-VLAN** auf „Auto-Voice-VLAN aktivieren" fest.

SCHRITT 4 Wählen Sie die Methode für **Auto-Voice-VLAN-Aktivierung** aus.

HINWEIS Wenn sich das Gerät zurzeit im Telefonie-OUI-Modus befindet, müssen Sie diesen deaktivieren, damit Sie Auto-Voice-VLAN konfigurieren können.

SCHRITT 5 Klicken Sie auf **Übernehmen**.

SCHRITT 6 Konfigurieren Sie Smartports gemäß der Beschreibung im Abschnitt **Allgemeine Smartport-Aufgaben**.

SCHRITT 7 Konfigurieren Sie LLDP/CDP gemäß der Beschreibung im Abschnitt **Konfigurieren von LLDP** bzw. **Konfigurieren von CDP**.

SCHRITT 8 Aktivieren Sie die Smartport-Funktion an den relevanten Ports auf der Seite „Smartport > Schnittstelleneinstellungen“.

HINWEIS Schritt 7 und Schritt 8 sind optional, da sie standardmäßig aktiviert sind.

Workflow 2: So konfigurieren Sie die Telefonie-OUI-Methode:

SCHRITT 1 Öffnen Sie die Seite „VLAN-Verwaltung > Voice-VLAN > Eigenschaften“. Legen Sie **Dynamisches Voice-VLAN** auf „OUI-Telefonie aktivieren“ fest.

HINWEIS Wenn sich das Gerät zurzeit im Auto-Voice-VLAN-Modus befindet, müssen Sie diesen deaktivieren, damit Sie Telefonie-OUI aktivieren können.

SCHRITT 2 Konfigurieren Sie Telefonie-OUI auf der Seite „Telefonie-OUI“.

SCHRITT 3 Konfigurieren Sie auf der Seite „Telefonie-OUI-Schnittstelle“ die Telefonie-OUI-VLAN-Mitgliedschaft für Ports.

Sprach-VLAN-Konfiguration

In diesem Abschnitt wird beschrieben, wie Sie Voice-VLAN konfigurieren. Die folgenden Themen werden behandelt:

- **Konfigurieren der Voice-VLAN-Eigenschaften**
- **Auto-Voice-VLAN-Einstellungen**
- **Telefonie-OUI**

Konfigurieren der Voice-VLAN-Eigenschaften

Führen Sie auf der Seite „Voice-VLAN-Eigenschaften“ die folgenden Schritte aus:

- Zeigen Sie an, wie Voice-VLAN zurzeit konfiguriert ist.
- Konfigurieren Sie die VLAN-ID des Voice-VLANs.
- Konfigurieren Sie die Voice-VLAN-QoS-Einstellungen.
- Konfigurieren Sie den Voice-VLAN-Modus (Telefonie-OUI oder Auto-Voice-VLAN).
- Konfigurieren Sie, wie Auto-Voice-VLAN ausgelöst wird.

So können Sie Voice-VLAN-Eigenschaften anzeigen und konfigurieren:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **Voice-VLAN** > **Eigenschaften**.

- Die im Gerät konfigurierten Voice-VLAN-Einstellungen werden im Block **Voice-VLAN-Einstellungen (Administrationsstatus)** angezeigt.
- Die tatsächlich auf die Voice-VLAN-Bereitstellung angewendeten Voice-VLAN-Einstellungen werden im Block **Voice-VLAN-Einstellungen (Betriebsstatus)** angezeigt.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **Voice-VLAN-ID**: Wählen Sie das VLAN aus, das Sie als Voice-VLAN konfigurieren möchten.

  HINWEIS Änderungen an der Voice-VLAN-ID, an CoS/802.1p und/oder DSCP führen dazu, dass das Gerät das administrative Voice-VLAN als statisches Voice-VLAN ankündigt. Wenn für die Option *Auto-Voice-VLAN-Aktivierung* die Auslösung durch ein externes Voice-VLAN ausgewählt ist, müssen Sie die Standardwerte beibehalten.

- **CoS/802.1p**: Wählen Sie einen CoS/802.1p-Wert aus, der von LLDP MED als Netzwerkrichtlinie für Sprachverkehr verwendet werden soll. Weitere Details finden Sie unter *Administration > Discovery > LLDP > LLDP MED-Netzwerkrichtlinien*.
- **DSCP**: Wählen Sie DSCP-Werte aus, die von LLDP MED als Netzwerkrichtlinie für Sprachverkehr verwendet werden sollen. Weitere Details finden Sie unter *Administration > Discovery > LLDP > LLDP MED-Netzwerkrichtlinien*.
- **Dynamisches Voice-VLAN**: Wählen Sie dieses Feld aus, um die Voice-VLAN-Funktion wie folgt zu deaktivieren oder zu aktivieren:
  - *Auto-Voice-VLAN aktivieren*: Aktivieren Sie dynamisches Voice-VLAN im Auto-Voice-VLAN-Modus.
  - *Telefonie-OUI aktivieren*: Aktivieren Sie dynamisches Voice-VLAN im Telefonie-OUI-Modus.
  - *Deaktivieren*: Deaktivieren Sie Auto-Voice-VLAN oder Telefonie-OUI.

- **Auto-Voice-VLAN-Aktivierung**: Wenn Auto-Voice-VLAN aktiviert wurde, wählen Sie eine der folgenden Optionen aus, um Auto-Voice-VLAN zu aktivieren:
  - *Sofort*: Auto-Voice-VLAN wird für das Gerät sofort aktiviert und verwendet, sofern die Option aktiviert ist.
  - *Durch externen Voice-VLAN-Auslöser*: Auto-Voice-VLAN wird nur dann für das Gerät aktiviert und verwendet, wenn das Gerät ein Gerät erkennt, das das Voice-VLAN ankündigt.

HINWEIS Wenn Sie die konfigurierten Standardwerte für Voice-VLAN-ID, CoS/802.1p und/oder DSCP ändern, führt dies zu einem statischen Voice-VLAN, das eine höhere Priorität hat als das von externen Quellen gelernte Auto-Voice-VLAN.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die VLAN-Eigenschaften werden in die aktuelle Konfigurationsdatei geschrieben.

Auto-Voice-VLAN-Einstellungen

Wenn der Auto-Voice-VLAN-Modus aktiviert ist, können Sie auf der Seite „Auto-Voice-VLAN“ die relevanten globalen Parameter und Schnittstellenparameter anzeigen.

Außerdem können Sie auf dieser Seite Auto-Voice-VLAN manuell neu starten, indem Sie auf **Auto-Voice-VLAN neu starten** klicken. Nach einer kurzen Verzögerung wird das Voice-VLAN auf das Standard-Voice-VLAN zurückgesetzt und der Erkennungs- und Synchronisierungsprozess für Auto-Voice-VLAN für alle Auto-Voice-VLAN-fähigen Switches im LAN wird neu gestartet.

HINWEIS Das Voice-VLAN wird nur dann auf das Standard-Voice-VLAN zurückgesetzt, wenn der Quelltyp den Status *Inaktiv* aufweist.

So zeigen Sie Auto-Voice-VLAN-Parameter an:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **Voice-VLAN** > **Auto-Voice-VLAN**.

Auf dieser Seite werden im Block „Betriebsstatus“ Informationen zum aktuellen Voice-VLAN und zu dessen Quelle angezeigt:

- **Auto-Voice-VLAN-Status**: Zeigt an, ob Auto-Voice-VLAN aktiviert ist.
- **Voice-VLAN-ID**: Die Kennung des aktuellen Voice-VLANs.
- **Quelltyp**: Zeigt den Typ der Quelle an, in der das Voice-VLAN vom Root-Gerät erkannt wurde.
- **CoS/802.1p**: Zeigt CoS/802.1p-Werte an, die von LLDP MED als Netzwerkrichtlinie für Sprachverkehr verwendet werden sollen.
- **DSCP**: Zeigt DSCP-Werte an, die von LLDP MED als Netzwerkrichtlinie für Sprachverkehr verwendet werden sollen.

- **MAC-Adresse des Root-Switch**: Die MAC-Adresse des Root-Geräts für Auto-Voice-VLAN, das das Voice-VLAN erkennt bzw. mit dem Voice-VLAN konfiguriert ist, von dem das Voice-VLAN gelernt wird.
- **Switch-MAC-Adresse**: Die MAC-Basisadresse des Geräts. Wenn die Switch-MAC-Adresse des Geräts der MAC-Adresse des Root-Switch entspricht, wird das Gerät als Root-Gerät für Auto-Voice-VLAN verwendet.
- **Änderungszeit für Voice-VLAN-ID**: Der Zeitpunkt der letzten Voice-VLAN-Aktualisierung.

SCHRITT 2 Klicken Sie auf **Auto-Voice-VLAN neu starten**, um das Voice-VLAN auf das Standard-Voice-VLAN zurückzusetzen und die Auto-Voice-VLAN-Erkennung für alle Auto-Voice-VLAN-fähigen Switches im LAN neu zu starten.

Die lokale Tabelle für Voice-VLAN zeigt das im Gerät konfigurierte Voice-VLAN sowie alle von direkt verbundenen Nachbargeräten angekündigten lokalen Voice-VLAN-Konfigurationen an. Die Tabelle enthält die folgenden Felder:

- **Schnittstelle**: Zeigt die Schnittstelle an, an der die Voice-VLAN-Konfiguration empfangen oder konfiguriert wurde. Wenn „n/v“ angezeigt wird, wurde die Konfiguration im Gerät selbst vorgenommen. Wenn eine Schnittstelle angezeigt wird, wurde eine Sprachkonfiguration von einem Nachbarn empfangen.
- **Quell-MAC-Adresse**: MAC-Adresse eines UC, von dem die Sprachkonfiguration empfangen wurde.
- **Quelltyp**: Typ des UC, von dem die Sprachkonfiguration empfangen wurde. Folgende Optionen stehen zur Verfügung:
  - *Standard*: Standard-Voice-VLAN-Konfiguration im Gerät.
  - *Statisch*: Im Gerät definierte benutzerdefinierte Voice-VLAN-Konfiguration.
  - *CDP*: In dem UC, das die Voice-VLAN-Konfiguration angekündigt hat, wird CDP ausgeführt.
  - *LLDP*: In dem UC, das die Voice-VLAN-Konfiguration angekündigt hat, wird LLDP ausgeführt.
  - *Voice-VLAN-ID*: Die Kennung des angekündigten oder konfigurierten Voice-VLANs.
- **Voice-VLAN-ID**: Die Kennung des aktuellen Voice-VLANs.
- **CoS/802.1p**: Die angekündigten oder konfigurierten CoS/802.1p-Werte, die von LLDP MED als Netzwerkrichtlinie für Sprache verwendet werden.
- **DSCP**: Die angekündigten oder konfigurierten DSCP-Werte, die von LLDP MED als Netzwerkrichtlinie für Sprache verwendet werden.
- **Beste lokale Quelle**: Zeigt an, ob dieses Voice-VLAN vom Gerät verwendet wurde. Folgende Optionen stehen zur Verfügung:

- *Ja*: Das Gerät verwendet dieses Voice-VLAN für die Synchronisierung mit anderen Auto-Voice-VLAN-fähigen Switches. Dieses Voice-VLAN wird als Voice-VLAN für das Netzwerk verwendet, sofern nicht ein Voice-VLAN aus einer Quelle mit höherer Priorität erkannt wird. Nur eine lokale Quelle ist die beste lokale Quelle.
- *Nein*: Dieses VLAN ist nicht die beste lokale Quelle.

SCHRITT 3 Klicken Sie auf **Aktualisieren**, um die Informationen auf der Seite zu aktualisieren.

Telefonie-OUI

OUIs werden vom Institute of Electrical and Electronics Engineers, Incorporated (IEEE) zugewiesen, einer Registrierungsstelle. Da die Zahl der IP-Telefonhersteller begrenzt ist und diese bekannt sind, werden die betreffenden Frames anhand der bekannten OUI-Werte bestimmt und der Port, an dem sie auftreten, wird automatisch einem Voice-VLAN zugewiesen.

Die globale OUI-Tabelle kann bis zu 128 OUIs enthalten.

In diesem Abschnitt werden die folgenden Themen behandelt:

- **Telefonie-OUI-Tabelle**
- **Telefon-OUI-Schnittstelle**

Telefonie-OUI-Tabelle

Auf der Seite „Telefonie-OUI“ können Sie QoS-Eigenschaften für Telefonie-OUIs konfigurieren. Außerdem können Sie die Fälligkeitszeit für die automatische Mitgliedschaft konfigurieren. Wenn der angegebene Zeitraum ohne Telefonieaktivitäten verstreicht, wird der Port aus dem Voice-VLAN entfernt.

Auf der Seite „Telefonie-OUI“ können Sie die vorhandenen OUIs anzeigen und neue OUIs hinzufügen.

So konfigurieren Sie Telefonie-OUIs und/oder fügen eine neue Voice-VLAN-OUI hinzu:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **Voice-VLAN** > **Telefonie-OUI**.

Die Seite „Telefonie-OUI“ enthält die folgenden Felder:

- **Telefonie-OUI-Betriebsstatus**: Zeigt an, ob OUIs zum Identifizieren von Sprachverkehr verwendet werden.
- **CoS/802.1p**: Wählen Sie die CoS-Warteschlange aus, die Sprachverkehr zugewiesen werden soll.
- **Remark CoS/802.1p**: Wählen Sie aus, ob Ausgangsverkehr kommentiert werden soll.

- **Fälligkeitszeit für autom. Mitgliedschaft**: Geben Sie ein, wie lange es dauert, bis ein Port aus dem Voice-VLAN entfernt wird, nachdem alle MAC-Adressen der an den Ports erkannten Telefone fällig geworden sind.

SCHRITT 2 Klicken Sie auf **Übernehmen**, um die aktuelle Konfiguration des Geräts mit diesen Werten zu aktualisieren.

Die Telefonie-OUI-Tabelle wird angezeigt:

- **Telefonie-OUI**: Die ersten sechs Ziffern der MAC-Adresse, die für OUIs reserviert sind.
- **Beschreibung**: Benutzerdefinierte OUI-Beschreibung.

SCHRITT 3 Klicken Sie auf **Standard-OUIs wiederherstellen**, um alle benutzerdefinierten OUIs zu löschen und nur die Standard-OUIs in der Tabelle zu belassen. Die OUI-Informationen sind möglicherweise erst korrekt, nachdem die Wiederherstellung abgeschlossen wurde. Dieser Vorgang kann mehrere Sekunden dauern. Warten Sie einige Sekunden, verlassen Sie die Seite und rufen Sie sie erneut auf, um die Darstellung zu aktualisieren.

Um alle OUIs zu löschen, aktivieren Sie das oberste Kontrollkästchen. Alle OUIs werden markiert und können durch Klicken auf **Löschen** gelöscht werden. Wenn Sie anschließend auf **Standard-OUIs wiederherstellen** klicken, stellt das System die bekannten OUIs wieder her.

SCHRITT 4 Zum Hinzufügen einer neuen OUI klicken Sie auf **Hinzufügen**.

SCHRITT 5 Geben Sie Werte für die folgenden Felder ein:

- **Telefonie-OUI**: Geben Sie eine neue OUI ein.
- **Beschreibung**: Geben Sie einen OUI-Namen ein.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die OUI wird der Telefonie-OUI-Tabelle hinzugefügt.

Telefon-OUI-Schnittstelle

QoS-Attribute können Sprachpaketen pro Port in einem der folgenden Modi zugewiesen werden:

- **Alle**: Für das Voice-VLAN konfigurierte QoS-Werte (Quality of Service) werden auf alle eingehenden Frames angewendet, die an der Schnittstelle empfangen und für das Voice-VLAN klassifiziert werden.
- **MAC-Adresse der Telefoniequelle**: Die für das Voice-VLAN konfigurierten QoS-Werte werden auf alle eingehenden Frames angewendet, die für das Voice-VLAN klassifiziert sind und deren Quell-MAC-Adresse eine OUI enthält, die einer konfigurierten Telefonie-OUI entspricht.

Fügen Sie auf der Seite „Telefonie-OUI-Schnittstelle“ dem Voice-VLAN auf der Grundlage der OUI-Kennung eine Schnittstelle hinzu und konfigurieren Sie den OUI-QoS-Modus für das Voice-VLAN.

So konfigurieren Sie die Telefonie-OUI für eine Schnittstelle:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **Voice-VLAN** > **Telefonie-OUI-Schnittstelle**.

Die Seite „Telefonie-OUI-Schnittstelle“ enthält Voice-VLAN-OUI-Parameter für alle Schnittstellen.

SCHRITT 2 Um eine Schnittstelle als Kandidatenport für das Telefonie-OUI-basierte Voice-VLAN zu konfigurieren, klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **Schnittstelle**: Wählen Sie eine Schnittstelle aus.
- **Telefonie-OUI-VLAN-Mitgliedschaft**: Wenn diese Option aktiviert ist, ist die Schnittstelle ein Kandidatenport für das Telefonie-OUI-basierte Voice-VLAN. Wenn Pakete mit einer der konfigurierten Telefonie-OUIs empfangen werden, wird der Port dem Voice-VLAN hinzugefügt.
- **Voice-VLAN-QoS-Modus**: Wählen Sie eine der folgenden Optionen aus:
  - *Alle*: Die QoS-Attribute werden auf alle Pakete angewendet, die für das Voice-VLAN klassifiziert sind.
  - *MAC-Adresse der Telefoniequelle*: Die QoS-Attribute werden nur auf Pakete von IP-Telefonen angewendet.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die OUI wird hinzugefügt.

Zugriffsport-Multicast-TV-VLAN

Multicast-TV-VLANs ermöglichen Multicast-Übertragungen an Teilnehmer, die sich nicht im gleichen Daten-VLAN befinden (Schicht 2, isoliert), ohne die Multicast-Übertragungs-Frames für jedes Teilnehmer-VLAN zu replizieren.

Teilnehmer, die sich nicht im selben Daten-VLAN befinden (Schicht 2, isoliert) und über eine andere VLAN-ID-Mitgliedschaft mit dem Gerät verbunden sind, können den gleichen Multicast-Stream nutzen, indem die Ports derselben Multicast-VLAN-ID hinzugefügt werden.

Der mit dem Multicast-Server verbundene Netzwerkport ist statisch als Mitglied in der Multicast-VLAN-ID konfiguriert.

Die Netzwerkports, über die Teilnehmer mit dem Multicast-Server kommunizieren (durch Senden von IGMP-Nachrichten), empfangen die Multicast-Streams vom Multicast-Server. Das Multicast-TV-VLAN ist dabei im Multicast-Paket-Header enthalten. Aus diesem Grund müssen die Netzwerkports statisch wie folgt konfiguriert sein:

- Porttyp „Trunk“ oder „Allgemein“ (siehe **Schnittstelleneinstellungen**)
- Mitglied des Multicast-TV-VLANs

Die Empfängerports der Teilnehmer können dem Multicast-TV-VLAN nur zugeordnet werden, wenn es mit einem der beiden folgenden Typen definiert ist:

- Zugriffsport
- Kundenport (siehe **Kundenport-Multicast-TV-VLAN**)

Sie können einem Multicast-TV-VLAN eine oder mehrere Multicast-Adressengruppen zuordnen.

Jedes VLAN kann als Multicast-TV-VLAN konfiguriert werden. Ein einem Multicast-TV-VLAN zugewiesener Port:

- Tritt dem Multicast-TV-VLAN bei.
- Pakete, die Egress-Ports im Multicast-TV-VLAN passieren, sind ungetaggt.
- Der Frame-Typ des Ports ist auf **Alle zulassen** festgelegt, sodass ungetaggte Pakete zulässig sind (siehe **Schnittstelleneinstellungen**).

Die Multicast-TV-VLAN-Konfiguration wird pro Port definiert. Kundenports werden auf der Seite „Multicast-TV-VLAN“ als Mitglieder von Multicast-TV-VLANs konfiguriert.

IGMP-Snooping

Multicast-TV-VLAN basiert auf IGMP-Snooping, das heißt:

- Teilnehmer verwenden IGMP-Nachrichten, um einer Multicast-Gruppe beizutreten oder diese zu verlassen.
- Das Gerät führt IGMP-Snooping aus und konfiguriert den Zugriffsport gemäß seiner Multicast-Mitgliedschaft im Multicast-TV-VLAN.

Das Gerät entscheidet für jedes an einem Zugriffsport empfangene IGMP-Paket, ob es dem Zugriffs-VLAN oder dem Multicast-TV-VLAN zugeordnet werden soll. Dabei gelten die folgenden Regeln:

- Wenn eine IGMP-Nachricht an einem Zugriffsport empfangen wird und die Ziel-Multicast-IP-Adresse dem Multicast-TV-VLAN des Ports zugeordnet ist, ordnet die Software das IGMP-Paket dem Multicast-TV-VLAN zu.

- Anderenfalls wird die IGMP-Nachricht dem Zugriffs-VLAN zugeordnet und die IGMP-Nachricht wird nur in diesem VLAN weitergeleitet.
- In folgenden Fällen wird die IGMP-Nachricht verworfen:
  - Der STP/RSTP-Status am Zugriffsport lautet **verwerfen**.
  - Der MSTP-Status für das Zugriffs-VLAN lautet **verwerfen**.
  - Der MSTP-Status für das Multicast-TV-VLAN lautet **verwerfen** und die IGMP-Nachricht ist diesem Multicast-TV-VLAN zugeordnet.

Unterschiede zwischen regulären VLANs und Multicast-TV-VLANs

Merkmale von regulären VLANs im Vergleich zu Multicast-TV-VLANs

	Reguläres VLAN	Multicast-TV-VLAN
VLAN-Mitgliedschaft	Der Quellport und alle Empfängerports müssen statische Mitglieder des gleichen Daten-VLANs sein.	Der Quellport und die Empfängerports können nicht Mitglieder des gleichen Daten-VLANs sein.
Gruppenregistrierung	Die Multicast-Gruppenregistrierung ist immer dynamisch.	Gruppen müssen statisch einem Multicast-VLAN zugeordnet werden, die eigentliche Registrierung der Station erfolgt jedoch dynamisch.
Empfängerports	Das VLAN kann sowohl zum Senden als auch zum Empfangen von Verkehr verwendet werden (Multicast und Unicast).	Das Multicast-VLAN kann nur zum Empfangen von Verkehr durch die Stationen am Port verwendet werden (nur Multicast).
Sicherheit und Isolation	Empfänger des gleichen Multicast-Streams befinden sich im gleichen Daten-VLAN und können miteinander kommunizieren.	Empfänger des gleichen Multicast-Streams befinden sich in verschiedenen Zugriffs-VLANs und sind voneinander isoliert.

Konfiguration

Workflow

Konfigurieren Sie ein TV-VLAN mit den folgenden Schritten:

1. Definieren Sie ein TV-VLAN durch Zuordnen einer Multicast-Gruppe zu einem VLAN (auf der Seite „Multicast-Gruppe zu VLAN“).
2. Geben Sie die Zugriffsports in den einzelnen Multicast-VLANs an (auf der Seite „Port-Multicast-VLAN-Mitgliedschaft“).

Multicast-Gruppe zu VLAN

So definieren Sie die Multicast-TV-VLAN-Konfiguration:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **Zugriffsport-Multicast-TV-VLAN > Multicast-Gruppe zu VLAN**.

Die folgenden Felder werden angezeigt:

- **Multicast-Gruppe**: Die IP-Adresse der Multicast-Gruppe.
- **Multicast-TV-VLAN**: Das VLAN, dem die Multicast-Pakete zugewiesen werden.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, um eine Multicast-Gruppe einem VLAN zuzuordnen. Sie können ein beliebiges VLAN auswählen. Wenn ein VLAN ausgewählt ist, wird es zu einem Multicast-TV-VLAN.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Multicast-TV-VLAN-Einstellungen werden geändert und in die aktuelle Konfigurationsdatei geschrieben.

Port-Multicast-VLAN-Mitgliedschaft

So definieren Sie die Multicast-TV-VLAN-Konfiguration:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **Zugriffsport-Multicast-TV-VLAN > Port-Multicast-VLAN-Mitgliedschaft**.

SCHRITT 2 Wählen Sie im Feld **Multicast-TV-VLAN** ein VLAN.

SCHRITT 3 Wählen Sie unter **Schnittstellentyp** eine Schnittstelle.

SCHRITT 4 Die Liste **Zugriffsports für Kandidaten** enthält alle im Gerät konfigurierten Zugriffsports. Verschieben Sie die gewünschten Ports in das Feld **Zugriffsports für Mitglieder**.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die Multicast-TV-VLAN-Einstellungen werden geändert und in die aktuelle Konfigurationsdatei geschrieben.

Kundenport-Multicast-TV-VLAN

Ein Triple-Play-Service stellt drei Breitbandservices über eine einzige Breitbandverbindung bereit:

- Hochgeschwindigkeits-Internetzugriff
- Video
- Sprache

Der Triple-Play-Service wird für Teilnehmer eines Dienstanbieters bereitgestellt, wobei die Schicht-2-Isolation zwischen den Teilnehmern aufrechterhalten wird.

Jeder Teilnehmer hat eine CPE-MUX-Box. Der MUX hat mehrere Zugriffsports, die mit den Geräten des Teilnehmers verbunden sind (PC, Telefon usw.), sowie einen Netzwerkport, der mit dem Zugriffsgerät verbunden ist.

Die Box leitet die Pakete vom Netzwerkport abhängig vom VLAN-Tag des Pakets an die Geräte des Teilnehmers weiter. Jedes VLAN ist einem der MUX-Zugriffsports zugeordnet.

Pakete von Teilnehmern an den Dienstanbieter werden als Frames mit VLAN-Tag weitergeleitet, um zwischen den Servicetypen zu unterscheiden. Dies bedeutet, dass für jeden Servicetyp eine eindeutige VLAN-ID in der CPE-Box vorhanden ist.

Alle Pakete vom Teilnehmer zum Netzwerk des Dienstanbieters werden vom Zugriffsgerät mit dem als Kunden-VLAN konfigurierten VLAN des Teilnehmers gekapselt (äußeres Tag oder S-VID). Davon ausgenommen sind IGMP-Snooping-Nachrichten von den TV-Empfängern, die dem Multicast-TV-VLAN zugeordnet sind. VOD-Informationen, die ebenfalls von den TV-Empfängern gesendet werden, werden wie jeder andere Verkehrstyp gesendet.

Am Netzwerkport empfangene Pakete vom Netzwerk des Dienstanbieters an den Teilnehmer werden im Netzwerk des Dienstanbieters als Pakete mit doppeltem Tag gesendet, wobei das äußere Tag (Service-Tag oder S-Tag) einen der zwei folgenden VLAN-Typen darstellt:

- VLAN des Teilnehmers (einschließlich Internet und IP-Telefonen)
- Multicast-TV-VLAN

Das innere VLAN (C-Tag) bestimmt das Ziel im Netzwerk des Teilnehmers (über den CPE-MUX).

Workflow

1. Konfigurieren Sie einen Zugriffsport als Kundenport (auf der Seite „VLAN-Verwaltung > Schnittstelleneinstellungen“). Weitere Informationen finden Sie unter **QinQ**.
2. Konfigurieren Sie den Netzwerkport als Trunk-Port oder allgemeinen Port mit Teilnehmer und Multicast-TV-VLAN als VLANs mit Tag. (Verwenden Sie dazu die Seite „VLAN-Verwaltung > Schnittstelleneinstellungen“.)
3. Erstellen Sie ein Multicast-TV-VLAN mit bis zu 4094 verschiedenen VLANs. (Die VLAN-Erstellung erfolgt über die reguläre VLAN-Verwaltungskonfiguration.)
4. Ordnen Sie auf der Seite „Port-Multicast-VLAN-Mitgliedschaft“ den Kundenport einem Multicast-TV-VLAN zu.
5. Ordnen Sie auf der Seite „CPE-VLAN zu VLAN“ das CPE-VLAN (C-Tag) dem Multicast-TV-VLAN (S-Tag) zu.

CPE-VLAN zu VLAN

Zur Unterstützung des CPE-MUX mit ihren VLANs benötigen die Teilnehmer möglicherweise mehrere Videoanbieter, denen jeweils ein anderes externes VLAN zugewiesen wird.

(Interne) CPE-Multicast-VLANs müssen den (externen) VLANs des Multicast-Anbieters zugeordnet werden.

Ein CPE-VLAN, das einem Multicast-VLAN zugeordnet wurde, kann an IGMP-Snooping teilnehmen.

So ordnen Sie CPE-VLANs zu:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **Kundenport-Multicast-TV-VLAN > CPE-VLAN zu VLAN**.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **CPE-VLAN**: Geben Sie das in der CPE-Box definierte VLAN ein.
- **Multicast-TV-VLAN**: Wählen Sie das dem CPE-VLAN zugeordnete Multicast-TV-VLAN aus.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die CPE-VLAN-Zuordnung wird geändert und in die aktuelle Konfigurationsdatei geschrieben.

Port-Multicast-VLAN-Mitgliedschaft

Die den Multicast-VLANs zugeordneten Ports müssen als Kundenports konfiguriert werden (siehe **Schnittstelleneinstellungen**).

So ordnen Sie Multicast-TV-VLANs Ports zu:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **Kundenport-Multicast-TV-VLAN > Port-Multicast-VLAN-Mitgliedschaft**.

SCHRITT 2 Wählen Sie im Feld **Multicast-TV-VLAN** ein VLAN.

SCHRITT 3 Wählen Sie unter **Schnittstellentyp** eine Schnittstelle.

SCHRITT 4 Die Liste **Kundenports für Kandidaten** enthält alle im Gerät konfigurierten Zugriffsports. Verschieben Sie die gewünschten Ports in das Feld **Kundenports für Mitglieder**.

Klicken Sie auf **Übernehmen**. Die neuen Einstellungen werden geändert und in die aktuelle Konfigurationsdatei geschrieben.

16

Spanning Tree

In diesem Abschnitt wird das Spanning Tree-Protokoll (STP) (IEEE802.1D und IEEE802.1Q) beschrieben. Die folgenden Themen werden behandelt:

- **STP-Modi**
- **STP-Status und globale Einstellungen**
- **Spanning Tree-Schnittstelleneinstellungen**
- **Einstellungen für Rapid Spanning Tree**
- **Multiple Spanning Tree**
- **MSTP-Eigenschaften**
- **VLANs zu einer MSTP-Instanz**
- **MSTP-Instanzeinstellungen**
- **MSTP-Schnittstelleneinstellungen**

STP-Modi

STP schützt eine Schicht-2-Broadcast-Domäne vor Broadcast-Stürmen, indem ausgewählte Netzwerkverbindungen zur Vermeidung von Schleifen in den Standby-Modus versetzt werden. Im Standby-Modus werden über diese Netzwerkverbindungen vorübergehend keine Benutzerdaten übertragen. Wenn die Topologie geändert wurde, sodass die Datenübertragung möglich ist, werden die Verbindungen automatisch wieder aktiviert.

Schleifen treten auf, wenn zwischen Hosts alternative Routen bestehen. Schleifen in erweiterten Netzwerken können dazu führen, dass Switches Datenverkehr unbegrenzt weiterleiten. Dadurch wird die Verkehrslast erhöht und die Netzwerkeffizienz verringert.

STP ermöglicht für jede beliebige Anordnung von Switches und verbindenden Links eine Baumtopologie, die für eindeutige Pfade zwischen den Endstationen eines Netzwerks sorgt und somit Schleifen verhindert.

Das Gerät unterstützt die folgenden Versionen des Spanning Tree-Protokolls:

- Classic STP: Sorgt dafür, dass zwischen zwei beliebigen Endstationen immer nur ein einziger Pfad besteht und verhindert dadurch Schleifen.
- Rapid STP (RSTP): Erkennt Netzwerktopologien und bietet auf dieser Grundlage eine schnellere Konvergenz der Spanning Tree-Baumstruktur. Dies ist am wirkungsvollsten, wenn die Netzwerktopologie von vornherein eine Baumstruktur aufweist, da die Konvergenz dadurch möglicherweise beschleunigt werden kann. RSTP ist standardmäßig aktiviert.
- Multiple STP (MSTP): MSTP basiert auf RSTP. MSTP erkennt Schleifen in Schicht 2 und versucht, sie zu verhindern, indem die Übertragung von Datenverkehr am beteiligten Port unterbunden wird. Da Schleifen separat in jeder Schicht-2-Domäne auftreten können, kann folgende Situation entstehen: In VLAN A ist eine Schleife vorhanden und in VLAN B nicht. Wenn beide VLANs über Port X kommunizieren und STP die Schleife verhindern will, stoppt STP den Datenverkehr am gesamten Port, einschließlich des Datenverkehrs von VLAN B.

  MSTP löst dieses Problem durch den Einsatz mehrerer STP-Instanzen, sodass Schleifen in jeder Instanz separat erkannt und verhindert werden können. Durch das Zuweisen von Instanzen zu VLANs wird jeder Instanz eine Schicht-2-Domäne zugeordnet, in der sie Schleifen erkennt und verhindert. Dadurch wird es möglich, dass der Port in einer Instanz gestoppt werden kann (beispielsweise für den Datenverkehr in VLAN A, in dem eine Schleife entstanden ist), während in einer anderen Domäne, in der keine Schleife besteht (zum Beispiel in VLAN B) der Datenverkehr weiterhin aktiv bleiben kann.

STP-Status und globale Einstellungen

Die Seite „STP-Status und globale Einstellungen“ enthält Parameter für die Aktivierung von STP, RSTP oder MSTP.

Auf den Seiten “STP-Schnittstelleneinstellungen“, „RSTP-Schnittstelleneinstellungen“ und „MSTP-Eigenschaften“ können Sie die jeweiligen Modi konfigurieren.

So legen Sie den STP-Status und die globalen Einstellungen fest:

SCHRITT 1 Klicken Sie auf **Spanning Tree** > **STP-Status und globale Einstellungen**.

SCHRITT 2 Geben Sie die Parameter ein.

Globale Einstellungen:

- **Spanning Tree-Status**: Wählen Sie diese Option aus, um Spanning Tree auf dem Gerät zu aktivieren.
- **STP-Loopback-Guard**: Wählen Sie diese Option aus, um Loopback-Guard auf dem Gerät zu aktivieren.
- **STP-Betriebsmodus**: Wählen Sie den STP-Betriebsmodus aus.

- **BPDU-Bearbeitung**: Wählen Sie aus, wie BPDU-Pakete (Bridge Protocol Data Unit) verwaltet werden, wenn STP am Port oder Gerät deaktiviert ist. BPDUs werden für die Übertragung von Spanning Tree-Informationen verwendet.
  - *Filterung*: Filtert BPDU-Pakete, wenn Spanning Tree bei einer Schnittstelle deaktiviert ist.
  - *Überlauf*: Sorgt für den Überlauf der BPDU-Pakete, wenn Spanning Tree bei einer Schnittstelle deaktiviert ist.
- **Standardwerte von Pfadkosten**: Auswahl der Methode für die Zuweisung von Standardpfadkosten zu den STP-Ports. Die einer Schnittstelle zugewiesenen Standardpfadkosten variieren entsprechend der ausgewählten Methode.
  - *Kurz*: Gibt für Port-Pfadkosten den Bereich 1 bis 65.535 an.
  - *Lang*: Gibt für Port-Pfadkosten den Bereich 1 bis 200.000.000 an.

Bridge-Einstellungen:

- **Priorität**: Legt den Prioritätswert der Bridge fest. Nach dem Austausch von BPDUs wird das Gerät mit der niedrigsten Priorität zur Root-Bridge. Falls alle Bridges die gleiche Priorität aufweisen, werden ihre MAC-Adressen für die Ermittlung der Root Bridge verwendet. Der Prioritätswert der Bridge wird als Vielfaches von 4096 angegeben, beispielsweise 4096, 8192, 12288 usw.
- **Hello-Zeit**: Legen Sie das Intervall in Sekunden fest, das eine Root Bridge zwischen Konfigurationsnachrichten abwartet.
- **Maximales Alter**: Legen Sie das Intervall in Sekunden fest, das das Gerät ohne Erhalt einer Konfigurationsnachricht abwarten kann, bevor es versucht, seine eigene Konfiguration neu festzulegen.
- **Weiterleitungsverzögerung**: Legen Sie das Intervall in Sekunden fest, in dem eine Bridge in einem Lernstatus verbleibt, bevor sie Pakete weiterleitet. Weitere Informationen finden Sie unter **Spanning Tree-Schnittstelleneinstellungen**.

Designierte Root:

- **Bridge-ID**: Eine Verkettung aus Bridge-Priorität und MAC-Adresse des Geräts.
- **Root-Bridge-ID**: Eine Verkettung aus Root-Bridge-Priorität und MAC-Adresse des Root-Switches.
- **Root-Port**: Der Port, der den Pfad mit den niedrigsten Kosten von dieser Bridge zur Root-Bridge bietet. (Dies ist von Bedeutung, wenn die Bridge nicht die Root ist.)
- **Root-Pfadkosten**: Die Kosten des Pfads von dieser Bridge zur Root-Bridge.
- **Anzahl der Topologieänderungen**: Die Gesamtanzahl aufgetretener STP-Topologieänderungen.
- **Letzte Topologieänderung**: Das Zeitintervall, das seit der letzten Topologieänderung vergangen ist. Die Zeit wird im Format Tage/Stunden/Minuten/Sekunden angezeigt.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die globalen STP-Einstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Spanning Tree-Schnittstelleneinstellungen

Auf der Seite „STP-Schnittstelleneinstellungen“ können Sie STP auf Port-Ebene konfigurieren und die im Protokoll enthaltenen Informationen anzeigen, beispielsweise die designierte Bridge.

Die definierte Konfiguration ist für alle Arten des STP-Protokolls gültig.

So konfigurieren Sie STP für eine Schnittstelle:

SCHRITT 1 Klicken Sie auf **Spanning Tree** > **STP-Schnittstelleneinstellungen**.

SCHRITT 2 Wählen Sie eine Schnittstelle aus und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Schnittstelle**: Wählen Sie den Port oder die LAG aus, für den bzw. die Spanning Tree konfiguriert wird.
- **STP**: Aktiviert oder deaktiviert STP für den Port.
- **Edge-Port**: Aktiviert oder deaktiviert Fast Link für den Port. Wenn der Fast Link-Modus für einen Port aktiviert ist, wird für den Port automatisch der Weiterleitungsstatus festgelegt, sofern der Port-Link aktiv ist. Durch Fast Link wird die STP-Protokollkonvergenz optimiert. Folgende Optionen sind möglich:
  - *Aktivieren*: Aktiviert Fast Link sofort.
  - *Automatisch*: Aktiviert Fast Link einige Sekunden, nachdem die Schnittstelle aktiv wird. Dadurch können von STP Schleifen aufgelöst werden, bevor Fast Link aktiviert wird.
  - *Deaktivieren*: Deaktiviert Fast Link.

    HINWEIS Es wird empfohlen, den Wert auf „Automatisch“ zu setzen, damit das Gerät den Port auf den Fast Link-Modus festlegt, wenn ein Host mit ihm verbunden ist, bzw. bei Verbindung mit einem anderen Gerät einen regulären STP-Port festlegt. Dadurch können Schleifen verhindert werden.
- **Root Guard**: Aktiviert oder deaktiviert Root Guard für das Gerät. Mit der Option „Root Guard“ können Sie die Root Bridge-Platzierung im Netzwerk erzwingen.

  Root Guard stellt sicher, dass der Port, für den diese Funktion aktiviert ist, der designierte Port ist. Normalerweise sind alle Root Bridge-Ports designierte Ports, es sei denn, mindestens zwei Ports der Root Bridge sind verbunden. Wenn die Bridge an einem Port, an dem Root Guard aktiviert ist, höherrangige BPDUs empfängt, weist Root Guard diesem Port den Status „Root inkonsistent“ zu. Der Status „Root inkonsistent“ entspricht effektiv einem Mithörstatus. Über diesen Port wird kein Verkehr weitergeleitet. Auf diese Weise erzwingt Root die Position der Root Bridge.

- **BPDU Guard**: Aktiviert oder deaktiviert die Funktion BPDU Guard (Bridge Protocol Data Unit) an dem Port.

  Mit BPDU Guard können Sie die STP-Domänengrenzen erzwingen und dafür sorgen, dass die aktive Topologie vorhersehbar bleibt. Die Geräte hinter den Ports, an denen BPDU Guard aktiviert ist, haben keinen Einfluss auf die STP-Topologie. Bei Erhalt von BPDUs deaktiviert der BPDU Guard-Vorgang den Port, für den BPDU konfiguriert ist. In diesem Fall wird eine BPDU-Nachricht empfangen und ein entsprechender SNMP-Trap generiert.

- **BPDU-Bearbeitung**: Wählen Sie aus, wie BPDU-Pakete verwaltet werden, wenn STP am Port oder Gerät deaktiviert ist. BPDUs werden für die Übertragung von Spanning Tree-Informationen verwendet.
  - *Globale Einstellungen verwenden*: Wählen Sie diese Option, um die auf der Seite „STP-Status und globale Einstellungen“ definierten Einstellungen zu verwenden.
  - *Filterung*: Filtert BPDU-Pakete, wenn Spanning Tree bei einer Schnittstelle deaktiviert ist.
  - *Überlauf*: Sorgt für den Überlauf der BPDU-Pakete, wenn Spanning Tree bei einer Schnittstelle deaktiviert ist.
- **Pfadkosten**: Legen Sie den Beitrag des Ports zu den Root-Pfadkosten fest, oder verwenden Sie die vom System erstellten Standardkosten.
- **Priorität**: Legt den Prioritätswert des Ports fest. Der Prioritätswert beeinflusst die Auswahl des Ports, wenn bei einer Bridge zwei Ports mit einer Schleife verbunden sind. Die Priorität kann Werte von 0 bis 240 annehmen, die ein Vielfaches von 16 sind.
- **Port-Status**: Zeigt den aktuellen STP-Status eines Ports an.
  - *Deaktiviert*: STP ist zurzeit für den Port deaktiviert. Der Port leitet Datenverkehr weiter, während er über MAC-Adressen informiert wird.
  - *Blockieren*: Der Port ist derzeit blockiert und kann keinen Datenverkehr weiterleiten (mit Ausnahme von BPDU-Daten) oder über MAC-Adressen informiert werden.
  - *Mithören*: Der Port befindet sich im Mithören-Modus. Der Port kann keinen Datenverkehr weiterleiten und nicht über MAC-Adressen informiert werden.
  - *Lernen*: Der Port befindet sich im Lernen-Modus. Der Port kann keinen Datenverkehr weiterleiten, er kann jedoch über MAC-Adressen informiert werden.
  - *Weiterleitung*: Der Port befindet sich im Weiterleitung-Modus. Der Port kann Datenverkehr weiterleiten und neue MAC-Adressen lernen.
- **Designierte Bridge-ID**: Zeigt die Bridge-Priorität und die MAC-Adresse der designierten Bridge an.
- **Designierte Port-ID**: Zeigt die Priorität und Schnittstelle des ausgewählten Ports an.
- **Designierte Kosten**: Zeigt die Kosten des Ports an, der Bestandteil der STP-Topologie ist. Ports mit niedrigeren Kosten werden mit geringerer Wahrscheinlichkeit blockiert, wenn STP Schleifen entdeckt.

- **Weiterleitungswechsel**: Zeigt an, wie oft der Port vom Status **Blockieren** in den Status **Weiterleitung** gewechselt ist.
- **Geschwindigkeit**: Zeigt die Geschwindigkeit des Ports an.
- **LAG**: Zeigt die LAG an, zu der der Port gehört. Wenn ein Port ein Mitglied einer LAG ist, haben die LAG-Einstellungen Vorrang vor den Porteinstellungen.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Schnittstelleneinstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Einstellungen für Rapid Spanning Tree

Rapid Spanning Tree Protocol (RSTP) ermöglicht eine schnellere STP-Konvergenz ohne Entstehung von Weiterleitungsschleifen.

Auf der Seite „RSTP-Schnittstelleneinstellungen“ können Sie RSTP auf Portebene konfigurieren. Alle auf dieser Seite vorgenommenen Konfigurationen sind aktiv, wenn Sie als globalen STP-Modus „RSTP“ oder „MSTP“ festgelegt haben.

So geben Sie RSTP-Einstellungen ein:

SCHRITT 1 Klicken Sie auf **Spanning Tree** > **STP-Status und globale Einstellungen**. Aktivieren Sie **Rapid STP**.

SCHRITT 2 Klicken Sie auf **Spanning Tree** > **RSTP-Schnittstelleneinstellungen**. Die Seite „RSTP-Schnittstelleneinstellungen“ wird geöffnet.

SCHRITT 3 Wählen Sie einen Port aus.

HINWEIS (Die Option „Protokollmigration aktivieren“ ist erst verfügbar, wenn Sie den Port ausgewählt haben, der mit dem gerade getesteten Bridge-Partnergerät verbunden ist.)

SCHRITT 4 Wenn mittels STP ein Verbindungspartner ermittelt wurde, klicken Sie auf **Protokollmigration aktivieren**, um einen Protokollmigrationstest durchzuführen. Dadurch wird ermittelt, ob der STP verwendende Verbindungspartner noch immer vorhanden ist, und falls ja, ob dieser zu „RSTP“ oder „MSTP“ migriert ist. Falls noch immer eine STP-Verbindung besteht, kommuniziert das Gerät weiterhin über STP mit dieser. Falls die Verbindung zu RSTP oder MSTP migriert ist, kommuniziert das Gerät mit dieser über „RSTP“ bzw. „MSTP“.

SCHRITT 5 Wählen Sie eine Schnittstelle aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 6 Geben Sie die Parameter ein:

- **Schnittstelle**: Legen Sie die Schnittstelle fest, und geben Sie den Port oder die LAG an, für den/die RSTP konfiguriert werden soll.
- **Punkt-zu-Punkt-Administrationsstatus**: Definieren Sie den Punkt-zu-Punkt-Verbindungsstatus. Ports mit Vollduplex werden als Punkt-zu-Punkt-Port-Verbindungen betrachtet.
  - *Aktivieren*: Wenn diese Funktion aktiviert ist, ist dieser Port ein RSTP-Edge-Port und wird schnell (meist innerhalb von zwei Sekunden) in den Weiterleitungsmodus versetzt.
  - *Deaktivieren*: Dieser Port wird nicht als Punkt-zu-Punkt-Verbindung für RSTP betrachtet. Das bedeutet, dass STP bei diesem Port mit normaler Geschwindigkeit arbeitet und nicht mit erhöhter Geschwindigkeit.
  - *Automatisch*: Ermittelt den Gerätestatus automatisch mithilfe von RSTP-BPDUs.
- **Punkt-zu-Punkt-Betriebsstatus**: Zeigt den Punkt-zu-Punkt-Betriebsstatus an, falls Sie für die Option **Punkt-zu-Punkt-Administrationsstatus** den Wert „Autom." ausgewählt haben.
- **Rolle**: Zeigt die Rolle des Ports an, die diesem von STP für das Bereitstellen von STP-Pfaden zugewiesen wurde. Folgende Rollen sind möglich:
  - *Root*: Pfad mit den niedrigsten Kosten für das Weiterleiten von Paketen an die Root-Bridge.
  - *Designiert*: Die Schnittstelle zwischen Bridge und LAN, die den Pfad mit den niedrigsten Kosten vom LAN zur Root Bridge bietet.
  - *Alternativ*: Bietet einen Alternativpfad von der Root-Schnittstelle zur Root-Bridge.
  - *Backup*: Bietet einen Backup-Pfad für den designierten Port-Pfad zu den Spanning Tree-Endelementen. Dadurch entsteht eine Konfiguration, bei der zwei Ports über eine Punkt-zu-Punkt-Verbindung in einer Schleife verbunden sind. Backup-Ports werden auch genutzt, wenn bei einem LAN mindestens zwei Verbindungen mit einem gemeinsam genutzten Segment bestehen.
  - *Deaktiviert*: Der Port ist kein Bestandteil des Spanning Trees.
- **Modus**: Zeigt den aktuellen Spanning Tree-Modus an: Classic STP oder RSTP.
- **Fast Link-Betriebsstatus**: Zeigt an, ob Fast Link (Edge-Port) für die Schnittstelle aktiviert oder deaktiviert ist oder automatisch gesteuert wird. Folgende Werte sind möglich:
  - *Aktiviert*: Fast Link ist aktiviert.
  - *Deaktiviert*: Fast Link ist deaktiviert.
  - *Automatisch*: Der Fast Link-Modus wird einige Sekunden, nachdem die Schnittstelle aktiv wird, aktiviert.

- **Portstatus**: Zeigt den RSTP-Status des jeweiligen Ports an.
  - *Deaktiviert*: STP ist zurzeit für den Port deaktiviert.
  - *Blockieren*: Der Port ist derzeit blockiert und kann keinen Datenverkehr weiterleiten oder über MAC-Adressen informiert werden.
  - *Mithören*: Der Port befindet sich im Mithören-Modus. Der Port kann keinen Datenverkehr weiterleiten und nicht über MAC-Adressen informiert werden.
  - *Lernen*: Der Port befindet sich im Lernen-Modus. Der Port kann keinen Datenverkehr weiterleiten, er kann jedoch über MAC-Adressen informiert werden.
  - *Weiterleitung*: Der Port befindet sich im Weiterleitung-Modus. Der Port kann Datenverkehr weiterleiten und neue MAC-Adressen lernen.

SCHRITT 7 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Multiple Spanning Tree

Multiple Spanning Tree Protocol (MSTP) wird verwendet, um den STP-Portstatus zwischen verschiedenen Domänen (in verschiedenen VLANs) zu trennen. So kann beispielsweise Port A in einer STP-Instanz aufgrund einer Schleife in VLAN A blockiert werden und gleichzeitig in einer anderen STP-Instanz im Weiterleitungsstatus arbeiten. Auf der Seite „MSTP-Eigenschaften“ können Sie die globalen MSTP-Einstellungen definieren.

So konfigurieren Sie MSTP:

1. Legen Sie für den STP-Betriebsmodus die Option „MSTP“ fest wie auf der Seite **STP-Status und globale Einstellungen** beschrieben.
2. Definieren Sie MSTP-Instanzen. Von jeder MSTP-Instanz wird eine schleifenfreie Topologie berechnet und aufgebaut, die als Brücke für die Pakete von dem VLAN dient, das zur jeweiligen Instanz gehört. Weitere Informationen finden Sie im Abschnitt **VLANs zu einer MSTP-Instanz**.
3. Entscheiden Sie, welche MSTP-Instanz in welchem VLAN aktiv ist, und ordnen Sie diese MSTP-Instanzen entsprechend VLANs zu.
4. Konfigurieren Sie die MSTP-Attribute mit folgenden Schritten:
   - **MSTP-Eigenschaften**
   - **MSTP-Instanzeinstellungen**
   - **VLANs zu einer MSTP-Instanz**

MSTP-Eigenschaften

Beim globalen MSTP wird für jede VLAN-Gruppe eine separate Spanning Tree-Baumstruktur erstellt und alle innerhalb der Spanning Tree-Instanz möglichen alternativen Pfade werden bis auf einen blockiert. MSTP ermöglicht die Bildung von MST-Regionen, in denen mehrere MST-Instanzen (MSTI) ausgeführt werden können. Mehrere Regionen und andere STP-Brücken werden über einen einzigen CST (Common Spanning Tree) miteinander verbunden.

MSTP ist insofern mit RSTP-Bridges vollständig kompatibel, als eine MSTP-BPDU von einer RSTP-Bridge als RSTP-BPDU interpretiert werden kann. Dies ermöglicht nicht nur die Kompatibilität mit RSTP-Bridges ohne Konfigurationsänderungen, sondern bewirkt auch, dass alle RSTP-Bridges außerhalb einer MSTP-Region die Region als einzelne RSTP-Bridge betrachten, unabhängig von der Anzahl der innerhalb der Region vorhandenen MSTP-Bridges.

Damit eine MST-Region zwei oder mehr Switches enthalten kann, müssen diese dieselbe Instanzzuordnung zwischen VLANs und MST aufweisen sowie dieselbe Konfigurationsversionsnummer und denselben Regionsnamen.

Switches, die in derselben MST-Region verwendet werden sollen, werden niemals durch Switches einer anderen MST-Region getrennt. Wenn sie getrennt werden, werden aus der Region zwei separate Regionen.

Diese Zuordnung können Sie auf der Seite „VLAN zu MSTP-Instanz“ vornehmen.

Verwenden Sie diese Seite, wenn das System im MSTP-Modus betrieben wird.

So legen Sie MSTP fest:

SCHRITT 1 Klicken Sie auf **Spanning Tree** > **STP-Status und globale Einstellungen**. Aktivieren Sie MSTP.

SCHRITT 2 Klicken Sie auf **Spanning Tree** > **MSTP-Eigenschaften**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Regionsname**: Legen Sie einen MSTP-Regionsnamen fest.
- **Version**: Legen Sie eine unsignierte 16-Bit-Nummer zur Kennzeichnung der Version der aktuellen MST-Konfiguration fest. Die Werte des Felds liegen im Bereich von 0 bis 65535.
- **Max. Hops**: Legen Sie fest, wie viele Hops in einer bestimmten Region höchstens auftreten sollen, bevor die BPDU gelöscht wird. Sobald die BPDU gelöscht wird, sind die Port-Informationen veraltet. Die Werte des Felds liegen im Bereich von 1 bis 40.
- **IST-Master**: Zeigt den Master der Region an.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die MSTP-Eigenschaften werden definiert und die aktuelle Konfigurationsdatei wird aktualisiert.

VLANs zu einer MSTP-Instanz

Auf der Seite „VLAN zu MSTP-Instanz“ können Sie jedes VLAN einer Multiple Spanning Tree-Instanz (MSTI) zuordnen. Damit Geräte zu derselben Region gehören können, müssen sie jeweils dieselbe Zuordnung zwischen VLANs und MSTIs aufweisen.

HINWEIS Einer MSTI können mehrere VLANs zugeordnet werden, aber einem VLAN kann nur eine MST-Instanz zugeordnet werden.

Die Konfiguration auf dieser Seite (und allen anderen MSTP-Seiten) gilt, wenn MSTP als STP-Modus des Systems verwendet wird.

Für Switches der Serie 500 können Sie neben Instanz 0 bis zu 16 MST-Instanzen definieren.

VLANs, die nicht explizit einer der MST-Instanzen zugeordnet sind, werden vom Gerät automatisch der CIST-Instanz (Core und Internal Spanning Tree) zugewiesen. Der CIST-Instanz entspricht die MST-Instanz „0“.

So ordnen Sie VLANs den MST-Instanzen zu:

SCHRITT 1 Klicken Sie auf **Spanning Tree** > **VLAN zu MSTP-Instanz**.

Die Seite „VLAN zu MSTP-Instanz“ enthält die folgenden Felder:

- **MSTP-Instanz-ID**: Alle MST-Instanzen werden angezeigt.
- **VLANs**: Alle zur MST-Instanz gehörenden VLANs werden angezeigt.

SCHRITT 2 Wenn Sie ein VLAN einer MSTP-Instanz hinzufügen möchten, wählen Sie die MST-Instanz aus und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie die Parameter ein:

- **MSTP-Instanz-ID**: Wählen Sie die MST-Instanz aus.
- **VLANs**: Legen Sie die VLANs fest, die dieser MST-Instanz zugeordnet werden.
- **Aktion**: Legen Sie fest, ob Sie das VLAN der MST-Instanz **Hinzufügen** (zuordnen) möchten oder ob Sie es von der MST-Instanz **Entfernen** möchten.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die MSTP-VLAN-Zuordnungen werden definiert und die aktuelle Konfigurationsdatei wird aktualisiert.

MSTP-Instanzeinstellungen

Auf der Seite „MSTP-Instanzeinstellungen“ können Sie Parameter für einzelne MST-Instanzen konfigurieren und anzeigen. Diese Einstellungen sind das instanzspezifische Äquivalent zum Abschnitt *Konfigurieren des STP-Status und der globalen Einstellungen*.

So geben Sie Einstellungen für MSTP-Instanzen ein:

SCHRITT 1 Klicken Sie auf **Spanning Tree** > **MSTP-Instanzeinstellungen**.

SCHRITT 2 Geben Sie die Parameter ein.

- **Instanz-ID**: Wählen Sie eine MST-Instanz aus, die angezeigt und definiert werden soll.
- **Eingeschlossene VLANs**: Zeigt die VLANs an, die der ausgewählten Instanz zugeordnet sind. Gemäß der Standardzuordnung sind alle VLANs der CIST-Instanz (Common and Internal Spanning Tree) zugeordnet (Instanz 0).
- **Bridge-Priorität**: Legen Sie die Priorität dieser Bridge für die ausgewählte MST-Instanz fest.
- **Designierte Root-Bridge-ID**: Zeigt die Priorität und die MAC-Adresse der Root-Bridge für die MST-Instanz an.
- **Root-Port**: Zeigt den Root-Port der ausgewählten Instanz an.
- **Root-Pfadkosten**: Zeigt die Root-Pfadkosten der ausgewählten Instanz an.
- **Bridge-ID**: Zeigt die Bridge-Priorität und die MAC-Adresse dieses Geräts für die ausgewählte Instanz an.
- **Verbleibende Hops**: Zeigt an, wie viele Hops bis zum Erreichen des nächsten Ziels verbleiben.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Konfiguration der MST-Instanz wird definiert und die aktuelle Konfigurationsdatei wird aktualisiert.

MSTP-Schnittstelleneinstellungen

Auf der Seite „MSTP-Schnittstelleneinstellungen“ können Sie die MSTP-Porteinstellungen für die einzelnen MST-Instanzen konfigurieren und Informationen anzeigen, die zurzeit in das Protokoll aufgenommen werden, beispielsweise die designierte Bridge für die jeweilige MST-Instanz.

So konfigurieren Sie die Ports in einer MST-Instanz:

SCHRITT 1 Klicken Sie auf **Spanning Tree** > **MSTP-Schnittstelleneinstellungen**.

SCHRITT 2 Geben Sie die Parameter ein.

- **Instanz ist gleich**: Wählen Sie die zu konfigurierende MSTP-Instanz aus.
- **Schnittstellentyp ist gleich**: Wählen Sie aus, ob die Liste der Ports oder LAGs angezeigt werden soll.

SCHRITT 3 Klicken Sie auf **Los**. Die MSTP-Parameter für die Schnittstellen in der Instanz werden angezeigt.

SCHRITT 4 Wählen Sie eine Schnittstelle aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 5 Geben Sie die Parameter ein.

- **Instanz-ID**: Wählen Sie die zu konfigurierende MST-Instanz aus.
- **Schnittstelle**: Wählen Sie die Schnittstelle aus, für die MSTI-Einstellungen festgelegt werden sollen.
- **Schnittstellenpriorität**: Legen Sie die Portpriorität für die angegebene Schnittstelle und MST-Instanz fest.
- **Pfadkosten**: Geben Sie den Anteil des Ports an den Root-Pfadkosten in das Textfeld **Benutzerdefiniert** ein, oder wählen Sie **Standard verwenden** aus, um den Standardwert zu verwenden.
- **Port-Status**: Zeigt den MSTP-Status des bestimmten Ports in einer bestimmten MST-Instanz an. Folgende Parameter können angegeben werden:
  - *Deaktiviert*: STP ist derzeit deaktiviert.
  - *Blockieren*: Der Port in dieser Instanz ist derzeit blockiert und kann keinen Datenverkehr weiterleiten (mit Ausnahme von BPDU-Daten) oder über MAC-Adressen informiert werden.
  - *Mithören*: Der Port in dieser Instanz befindet sich im Mithören-Modus. Der Port kann keinen Datenverkehr weiterleiten und nicht über MAC-Adressen informiert werden.
  - *Lernen*: Der Port in dieser Instanz befindet sich im Lernen-Modus. Der Port kann keinen Datenverkehr weiterleiten, er kann jedoch über MAC-Adressen informiert werden.
  - *Weiterleiten*: Der Port in dieser Instanz befindet sich im Weiterleiten-Modus. Der Port kann Datenverkehr weiterleiten und neue MAC-Adressen lernen.
  - *Grenze*: Der Port in dieser Instanz ist ein Grenzport. Er erbt seinen Status von Instanz 0 und kann auf der Seite „STP-Schnittstelleneinstellungen“ angezeigt werden.

- **Port-Rolle**: Zeigt an, welche Rolle dem Port oder der LAG in dieser Instanz durch den MSTP-Algorithmus für die Bereitstellung von STP-Pfaden zugewiesen wurde:
  - *Root*: Beim Weiterleiten von Paketen zum Root-Gerät über diese Schnittstelle nutzen Pakete den Pfad mit den niedrigsten Kosten.
  - *Designiert*: Die Schnittstelle zwischen Bridge und LAN, die für die MST-Instanz den Root-Pfad mit den niedrigsten Kosten vom LAN zur Root Bridge bietet.
  - *Alternativ*: Die Schnittstelle bietet einen Alternativpfad von der Root-Schnittstelle zum Root-Gerät.
  - *Backup*: Die Schnittstelle bietet einen Backup-Pfad für den designierten Port-Pfad hin zu den Spanning Tree-Endelementen. Backup-Ports werden genutzt, wenn zwei Ports über eine Punkt-zu-Punkt-Port-Verbindung mit einer Schleife verbunden sind. Backup-Ports werden auch genutzt, wenn bei einem LAN mindestens zwei Verbindungen mit einem gemeinsam genutzten Segment bestehen.
  - *Deaktiviert*: Die Schnittstelle ist kein Bestandteil des Spanning Trees.
  - *Grenze*: Der Port in dieser Instanz ist ein Grenzport. Er erbt seinen Status von Instanz 0 und kann auf der Seite „STP-Schnittstelleneinstellungen“ angezeigt werden.
- **Modus**: Zeigt den aktuellen Spanning Tree-Modus der Schnittstelle an:
  - Wenn der Verbindungspartner MSTP oder RSTP verwendet, lautet der angezeigte Portmodus „RSTP“.
  - Wenn der Verbindungspartner STP verwendet, lautet der angezeigte Portmodus „STP“.
- **Typ**: Zeigt den MST-Typ des Ports an.
  - *Grenze*: Ein Grenzport verknüpft MST-Bridges mit einem LAN in einer Remote-Region. Falls es sich bei dem Port um einen Grenzport handelt, wird auch angezeigt, ob das Gerät auf der anderen Seite der Verknüpfung im RSTP-Modus oder im STP-Modus betrieben wird.
  - *Intern*: Bei dem Port handelt es sich um einen internen Port.
- **Designierte Bridge-ID**: Zeigt die Bridge-ID-Nummer der Bridge an, über die die Verknüpfung oder das gemeinsam genutzte LAN mit der Root verbunden ist.
- **Designierte Port-ID**: Zeigt die Port-ID-Nummer der designierten Bridge an, über die die Verknüpfung oder das gemeinsam genutzte LAN mit der Root verbunden ist.
- **Designierte Kosten**: Zeigt die Kosten des Ports an, der Bestandteil der STP-Topologie ist. Ports mit niedrigeren Kosten werden mit geringerer Wahrscheinlichkeit blockiert, wenn STP Schleifen entdeckt.
- **Verbleibende Hops**: Zeigt an, wie viele Hops bis zum Erreichen des nächsten Ziels verbleiben.
- **Weiterleitungswechsel**: Zeigt an, wie oft der Port vom Status „Weiterleitung“ in den Status „Blockieren“ gewechselt ist.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

17

Verwalten von MAC-Adresstabellen

In diesem Abschnitt wird beschrieben, wie Sie dem System MAC-Adressen hinzufügen. Die folgenden Themen werden behandelt:

- **Statische MAC-Adressen**
- **Dynamische MAC-Adressen**
- **Reservierte MAC-Adressen**

Es gibt zwei MAC-Adresstypen: statisch und dynamisch. MAC-Adressen werden abhängig vom Typ zusammen mit VLAN- und Port-Informationen in der Tabelle *Statische Adressen* oder in der Tabelle *Dynamische Adressen* gespeichert.

Statische Adressen werden vom Benutzer konfiguriert und laufen daher nicht ab.

Eine neue Quell-MAC-Adresse, die in einem am Gerät eingehenden Frame erscheint, wird der Tabelle für dynamische Adressen hinzugefügt. Diese MAC-Adresse wird während eines konfigurierbaren Zeitraums beibehalten. Wenn am Gerät vor Ablauf dieses Zeitraums kein anderer Frame mit der gleichen Quell-MAC-Adresse eingeht, wird der Eintrag aus der Tabelle gelöscht.

Wenn am Gerät ein Frame eingeht, sucht das Gerät in der statischen oder dynamischen Tabelle nach einem entsprechenden Ziel-MAC-Adresseintrag. Wenn eine Übereinstimmung gefunden wird, wird der Frame für den Ausgang an einem bestimmten Port gekennzeichnet. Wenn Frames an eine MAC-Adresse gesendet werden, die in den Tabellen nicht gefunden wird, werden sie an alle Ports im jeweiligen VLAN übertragen. Diese Frames werden als unbekannte Unicast-Frames bezeichnet.

Das Gerät unterstützt maximal 8.000 statische und dynamische MAC-Adressen.

Statische MAC-Adressen

Statische MAC-Adressen werden einer bestimmten physischen Schnittstelle und einem bestimmten VLAN des Geräts zugewiesen. Wenn diese Adresse an einer anderen Schnittstelle erkannt wird, wird sie ignoriert und nicht in die Adresstabelle geschrieben.

So definieren Sie eine statische Adresse:

SCHRITT 1 Klicken Sie auf **MAC-Adresstabellen > Statische Adressen**.

Auf der Seite *Statische Adressen* werden die aktuell definierten statischen Adressen angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie die Parameter ein.

- **VLAN-ID**: Dient zum Auswählen der VLAN-ID für den Port.
- **MAC-Adresse**: Dient zum Auswählen der Schnittstellen-MAC-Adresse.
- **Schnittstelle**: Wählen Sie eine Schnittstelle (Einheit/Slot, Port oder LAG) für den Eintrag aus.
- **Status**: Mit dieser Option wählen Sie, wie der Eintrag behandelt wird. Folgende Optionen sind möglich:
  - *Permanent*: Diese MAC-Adresse wird vom System nie entfernt. Wenn die statische MAC-Adresse in der Startkonfiguration gespeichert ist, bleibt sie nach dem Neustart erhalten.
  - *Bei Zurücksetzen löschen*: Die statische MAC-Adresse wird gelöscht, wenn das Gerät zurückgesetzt wird.
  - *Bei Timeout löschen*: Die MAC-Adresse wird gelöscht, wenn das Fälligkeitsintervall erreicht wird.
  - *Sicher*: Die MAC-Adresse ist sicher, wenn sich die Schnittstelle im klassischen Sperrmodus befindet (siehe **Konfigurieren der Portsicherheit**).

SCHRITT 4 Klicken Sie auf **Übernehmen**. In der Tabelle wird ein neuer Eintrag angezeigt.

Dynamische MAC-Adressen

Die Tabelle der dynamischen Adressen (Bridging-Tabelle) enthält die MAC-Adressen, die durch Überwachen der Quelladressen von am Gerät eingehenden Frames ermittelt werden.

Um das Überlaufen dieser Tabelle zu verhindern und Platz für neue MAC-Adressen freizugeben, wird eine Adresse gelöscht, wenn über einen bestimmten Zeitraum – die so genannte Fälligkeitszeit – kein entsprechender Verkehr empfangen wird.

Konfigurieren der Fälligkeitszeit für dynamische MAC-Adressen

So konfigurieren Sie die Fälligkeitszeit für dynamische Adressen:

SCHRITT 1 Klicken Sie auf **MAC-Adresstabellen > Einstellungen für dynamische Adressen**.

SCHRITT 2 Geben Sie die **Fälligkeitszeit** ein. Die Fälligkeitszeit ist ein Wert zwischen dem benutzerdefinierten Wert und dem Zweifachen des Wertes minus 1. Wenn Sie beispielsweise 300 Sekunden eingegeben haben, beträgt die Fälligkeitszeit 300 bis 599 Sekunden.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Fälligkeitszeit wird aktualisiert.

Abfragen dynamischer Adressen

So fragen Sie dynamische Adressen ab:

SCHRITT 1 Klicken Sie auf **MAC-Adresstabellen > Dynamische Adressen**.

SCHRITT 2 Im Block *Filtern* können Sie die folgenden Abfragekriterien eingeben:

- **VLAN-ID**: Geben Sie die VLAN-ID für die Tabellenabfrage ein.
- **MAC-Adresse**: Geben Sie die MAC-Adresse für die Tabellenabfrage ein.
- **Schnittstelle**: Wählen Sie die Schnittstelle für die Tabellenabfrage aus. Die Abfrage kann nach bestimmten Einheiten/Slots, Ports oder LAGs suchen.

SCHRITT 3 Klicken Sie auf **Los**. Die Tabelle der dynamischen MAC-Adressen wird abgefragt und die Ergebnisse angezeigt.

Zum Löschen aller dynamischen MAC-Adressen klicken Sie auf **Tabelle löschen**.

Reservierte MAC-Adressen

Wenn das Gerät einen Frame mit einer Ziel-MAC-Adresse empfängt, die zu einem reservierten Bereich gehört (gemäß IEEE-Standard), kann der Frame verworfen oder überbrückt werden. Der Eintrag in der Tabelle für reservierte MAC-Adressen kann die reservierte MAC-Adresse oder die reservierte MAC-Adresse und einen Frame-Typ angeben:

So fügen Sie einen Eintrag für eine reservierte MAC-Adresse hinzu:

SCHRITT 1 Klicken Sie auf **MAC-Adresstabellen > Reservierte MAC-Adressen**.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **MAC-Adresse**: Wählen Sie die zu reservierende MAC-Adresse aus.
- **Frame-Typ**: Wählen Sie den Frame-Typ anhand der folgenden Kriterien aus:
  - *Ethernet V2*: Wird für Ethernet V2-Pakete mit dieser bestimmten MAC-Adresse verwendet.
  - *LLC*: Wird für LLC-Pakete (Logical Link Control) mit dieser bestimmten MAC-Adresse verwendet.
  - *LLC-SNAP*: Wird für LLC-SNAP-Pakete (Logical Link Control/Sub-Network Access Protocol) mit dieser bestimmten MAC-Adresse verwendet.
  - *Alle*: Wird für alle Pakete mit der jeweiligen MAC-Adresse verwendet.
- **Aktion**: Wählen Sie eine der folgenden Aktionen aus, die ausgeführt werden soll, wenn das eingehende Paket den ausgewählten Kriterien entspricht:
  - *Bridge*: Weiterleiten des Pakets an alle VLAN-Mitglieder.
  - *Verwerfen*: Löschen des Pakets.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Es wird eine neue MAC-Adresse reserviert.

18

Multicast

In diesem Abschnitt wird die Funktion der Multicast-Weiterleitung beschreiben. Der Abschnitt behandelt folgende Themen:

- **Multicast-Weiterleitung**
- **Multicast-Eigenschaften**
- **MAC-Gruppenadresse**
- **IP-Multicast-Gruppenadressen**
- **IPv4-Multicast-Konfiguration**
- **IPv6-Multicast-Konfiguration**
- **IGMP/MLD-Snooping-IP-Multicast-Gruppe**
- **Multicast-Router-Ports**
- **Alle weiterleiten**
- **Nicht registrierter Multicast**

Multicast-Weiterleitung

Mit der Multicast-Weiterleitung werden Informationen von einem Punkt zu mehreren Teilnehmern übertragen. Multicast-Anwendungen sind für die Übertragung von Informationen an mehrere Clients sinnvoll, wobei die Clients nicht unbedingt den vollständigen Inhalt empfangen müssen. Eine typische Anwendung ist ein dem Kabel-TV ähnlicher Service, bei dem die Clients mitten in der Übertragung einem Kanal beitreten und ihn vor dem Ende wieder verlassen können.

Die Daten werden nur an die relevanten Ports gesendet. Dadurch, dass die Daten nur an die relevanten Ports weitergeleitet werden, werden Bandbreite und Host-Ressourcen für die Verbindungen eingespart.

Standardmäßig werden alle Multicast-Frames an alle Ports im VLAN geflutet. Wenn Sie nur an bestimmte Ports weiterleiten und den Multicast für die verbliebenen Ports ausfiltern (löschen) möchten, aktivieren Sie auf der Seite „Multicast > Eigenschaften“ den Bridge-Multicast-Filterstatus.

Ist die Filterung aktiviert, werden die Multicast-Frames an eine Untergruppe der Ports im entsprechenden VLAN weitergeleitet, die in der MFDB (Multicast Forwarding Data Base, Multicast-Weiterleitungsdatenbank) definiert ist. Die Multicast-Filterung ist für den gesamten Datenverkehr verfügbar.

Eine verbreitete Möglichkeit zur Darstellung einer Multicast-Mitgliedschaft ist die Notation „(S,G)“, wobei „S“ eine einzelne („single“) Quelle ist, die einen Multicast-Datenstrom sendet, und „G“ eine IPv4- oder IPv6-Gruppenadresse. Wenn ein Multicast-Client Multicast-Datenverkehr von einer beliebigen Quelle einer bestimmten Multicast-Gruppe empfängt, wird dies als „(*,G)“ gespeichert.

Sie können eine der folgenden Möglichkeiten für die Weiterleitung von Multicast-Frames konfigurieren:

- **MAC-Gruppenadresse**: Auf der Grundlage der Ziel-MAC-Adresse im Ethernet-Frame.

  HINWEIS Eine oder mehrere IP-Multicast-Gruppen-Adressen können einer MAC-Gruppen-Adresse zugeordnet werden. Die auf der MAC-Gruppenadresse basierende Weiterleitung kann dazu führen, dass ein IP-Multicast-Strom an Ports weitergeleitet wird, die nicht über einen Empfänger für den Strom verfügen.

- **IP-Gruppenadresse**: Auf der Grundlage der Ziel-IP-Adresse des IP-Pakets (*,G).
- **Quellspezifische IP-Gruppenadresse**: Auf der Grundlage sowohl der Ziel-IP-Adresse als auch der Quell-IP-Adresse des IP-Pakets (S,G).

(S,G) wird von IGMPv3 und MLDv2 unterstützt. IGMPv1/2 und MLDv1 unterstützen dagegen nur (*,G), das heißt lediglich die Gruppen-ID.

Das Gerät unterstützt maximal 256 statische und dynamische Multicast-Gruppenadressen.

Nur eine der Filterungsoptionen kann je VLAN konfiguriert werden.

Typisches Multicast-Setup

Während Multicast-Router Multicast-Pakete zwischen IP-Subnetzen übertragen, übertragen Multicast-fähige Schicht-2-Switches Multicast-Pakete an registrierte Knoten in einem LAN oder VLAN.

Ein typisches Setup enthält einen Router, der die Multicast-Ströme zwischen privaten und/oder öffentlichen IP-Netzwerken überträgt, ein Gerät mit IGMP/MLD-Snooping sowie einen Multicast-Client, der einen Multicast-Strom empfangen möchte. In diesem Setup sendet der Router regelmäßig IGMP/MLD-Abfragen.

Multicast-Betrieb

In einem Schicht-2-Multicast-Service empfängt ein Schicht-2-Switch einen einzelnen Frame, der an eine bestimmte Multicast-Adresse gerichtet ist. Er erstellt Kopien des Frames, die an die jeweiligen Ports übertragen werden.

Wenn IGMP/MLD-Snooping für das Gerät aktiviert ist und dieses einen Frame für einen Multicast-Strom empfängt, leitet es den Multicast-Frame an alle Ports weiter, die mithilfe von IGMP/MLD-Beitrittsnachrichten für den Empfang des Multicast-Stroms registriert wurden.

Das System verwaltet Listen mit Multicast-Gruppen für jedes VLAN. Dieses verwaltet die Multicast-Informationen, die die einzelnen Ports empfangen sollen. Die Multicast-Gruppen und die entsprechenden empfangenden Ports können statisch konfiguriert oder mithilfe von IGMP- bzw. MLD-Protokoll Snooping dynamisch gelernt werden.

Multicast-Registrierung (IGMP-/MLD-Snooping)

Die Multicast-Registrierung ist der Prozess, in dem Multicast-Anmeldeprotokolle empfangen und darauf geantwortet wird. Als Protokolle stehen IGMP für IPv4 und MLD für IPv6 zur Verfügung.

Wenn IGMP/MLD-Snooping für ein Gerät in einem VLAN aktiviert ist, analysiert dieses alle IGMP/MLD-Pakete, die es von dem VLAN empfangen hat, mit dem das Gerät und die Multicast-Router im Netzwerk verbunden sind.

Wenn ein Gerät lernt, dass ein Host IGMP/MLD-Nachrichten für die Registrierung zum Empfang eines Multicast-Stroms gegebenenfalls von einer bestimmten Quelle verwendet, fügt das Gerät die Registrierung seiner MFDB hinzu.

Folgende Versionen werden unterstützt:

- IGMP v1/v2/ v3
- MLD v1/v2

HINWEIS Das Gerät unterstützt IGMP/MLD-Snooping nur für statische VLANs. Für dynamische VLANs wird IGMP/MLD-Snooping nicht unterstützt.

Ist das IGMP/MLD-Snooping global oder für ein bestimmtes VLAN aktiviert, werden alle IGMP/MLD-Pakete an die CPU weitergeleitet. Die CPU analysiert die eingehenden Pakete und legt fest,

- welche Ports um Beitritt zu welchen Multicast-Gruppen auf welchem VLAN bitten.
- welche Ports mit Multicast-Routern (MRoutern) verbunden sind, die IGMP/MLD-Abfragen generieren.
- welche Ports PIM-, DVMRP- oder IGMP/MLD-Abfrageprotokolle empfangen.

Diese werden auf der Seite „IGMP/MLD-Snooping“ angezeigt.

Die Ports, die um Beitritt zu einer bestimmten Multicast-Gruppe bitten, geben einen IGMP/MLD-Bericht aus, der festlegt, welcher oder welchen Gruppen der Host beitreten möchte. Daraus wird ein Weiterleitungseintrag in der Multicast-Weiterleitungsdatenbank erstellt.

IGMP-Snooping-Abfrager

Mit dem IGMP/MLD-Snooping-Abfrager wird eine Schicht-2-Multicast-Domäne aus Snooping-Switches unterstützt, wenn kein Multicast-Router vorhanden ist. Dies ist z. B. der Fall, wenn Multicast-Inhalt von einem lokalen Server bereitgestellt wird, der Router (falls vorhanden) im Netzwerk jedoch kein Multicast unterstützt.

Das Gerät kann als IGMP-Abfrager oder, wenn kein normaler IGMP-Abfrager vorhanden ist, als Backup-Abfrager konfiguriert werden. Das Gerät ist kein IGMP-Abfrager mit vollem Funktionsumfang.

Wenn das Gerät als IGMP-Abfrager aktiviert wird, startet es, wenn 60 Sekunden lang kein IGMP-Datenverkehr (Abfragen) von einem Multicast-Router erkannt wurde. Sind andere IGMP-Abfrager vorhanden, kann das Gerät möglicherweise die Übertragung von Abfragen auf der Grundlage der Ergebnisse des Standardauswahlprozesses des Abfragers stoppen.

Die Geschwindigkeit der Aktivität des IGMP/MLD-Abfragers muss auf die Switches abgestimmt sein, bei denen IGMP/MLD-Snooping aktiviert ist. Abfragen müssen mit einer Rate gesendet werden, die der Fälligkeitszeit der Snooping-Tabelle entspricht. Werden die Abfragen mit einer niedrigeren Rate gesendet als die Fälligkeitszeit, kann der Abonnent keine Multicast-Pakete empfangen. Verwenden Sie hierzu die Seite „IGMP/MLD-Snooping bearbeiten“.

Ist der Mechanismus zur Auswahl der IGMP/MLD-Abfrager deaktiviert, dann verzögert der IGMP/MLD-Snooping-Abfrager das Senden von Nachrichten mit allgemeinen Abfragen nach seiner Aktivierung für 60 Sekunden. Ist kein anderer Abfrager vorhanden, dann wird mit dem Senden von Nachrichten mit allgemeinen Abfragen begonnen. Wird hingegen ein anderer Abfrager erkannt, dann wird das Senden von Nachrichten mit allgemeinen Abfragen beendet.

Der IGMP/MLD-Snooping-Abfrager setzt das Senden von Nachrichten mit allgemeinen Abfragen fort, sobald er innerhalb des folgenden Zeitraums einen anderen Abfrager erkennt:

Passives Abfrageintervall = Robustheit · Abfrageintervall + 0,5 · Abfrageantwortintervall.

HINWEIS Es wird empfohlen, den Auswahlmechanismus für IGMP/MLD-Abfrager zu deaktivieren, wenn im VLAN ein IPM-Multicast-Router vorhanden ist.

Eigenschaften von Multicast-Adressen

Multicast-Adressen haben folgende Eigenschaften:

- Jede IPv4 Multicast-Adresse liegt im Adressbereich von 224.0.0.0 bis 239.255.255.255.
- Die IPv6 Multicast-Adresse lautet FF00:/8.
- So ordnen Sie eine IP-Multicast-Gruppenadresse einer Schicht-2-Multicast-Adresse zu:
  - Bei IPv4 erfolgt die Zuordnung, indem die unteren 23 Bits der IPv4-Adresse dem Präfix 01:00:5e angefügt werden. Standardmäßig werden die oberen neun Bits der IP-Adresse ignoriert und jede IP-Adresse, die sich nur durch die Werte dieser oberen Bits unterscheidet, wird derselben Schicht-2-Adresse zugeordnet, da die verwendeten unteren 23 Bits identisch sind. Die Adresse 234.129.2.3 wird beispielsweise der MAC-Multicast-Gruppenadresse 01:00:5e:01:02:03 zugeordnet. Bis zu 32 IP-Multicast-Gruppenadressen können derselben Schicht-2-Adresse zugeordnet werden.

- Bei IPv6 erfolgt die Zuordnung, indem die unteren 32 Bit der Multicast-Adresse dem Präfix 33:33 angefügt werden. Die IPv6-Multicast-Adresse FF00:1122:3344 wird beispielsweise der Schicht-2-Multicast-Adresse 33:33:11:22:33:44 zugeordnet.

IGMP/MLD-Proxy

IGMP/MLD-Proxy ist ein einfaches IP-Multicast-Protokoll.

Durch die Replikation von Multicast-Datenverkehr auf Geräten wie beispielsweise Edge-Systemen mithilfe von IGMP/MLD-Proxy lassen sich Entwurf und Implementierung solcher Geräte erheblich vereinfachen. Da komplexere Multicast-Routing-Protokolle wie PIM (Protocol Independent Multicast) oder DVMRP (Distance Vector Multicast Routing Protocol) nicht unterstützt werden, werden hierdurch nicht nur die Kosten für die Geräte gesenkt, sondern es wird auch der betriebliche Aufwand verringert. Ein weiterer Vorteil besteht darin, dass die Proxy-Geräte unabhängig von dem auf den Kernnetzwerk-Routern verwendeten Multicast-Routing-Protokoll werden. Aus diesem Grund lassen sich Proxy-Geräte in einem Multicast-Netzwerk unkompliziert bereitstellen.

IGMP/MLD-Proxy-Baumstruktur

IGMP/MLD Proxy funktioniert auf Basis einer einfachen Baumtopologie, in der die Ausführung eines robustesten Multicast-Routing-Protokolls wie etwa PIM nicht erforderlich ist. Ausreichend ist die Verwendung eines einfachen IPM-Routing-Protokolls, mit dem Informationen zu Gruppenmitgliedschaften und Proxy-Gruppenmitgliedschaften erlernt und Multicast-Pakete auf der Grundlage dieser Informationen weitergeleitet werden können.

Die Baumstruktur muss manuell durch Spezifikation von Upstream- und Downstream-Schnittstellen auf jedem Proxy-Gerät konfiguriert werden. Außerdem muss das auf die Proxy-Baumtopologie angewendete IP-Adressierungsschema so konfiguriert sein, dass sichergestellt ist, dass ein Proxy-Gerät die Auswahl des IGMP/MLD-Abfragers gewinnen kann, um Multicast-Datenverkehr weiterleiten zu können. Neben den Proxy-Geräten in der Baumstruktur sollten keine anderen Multicast-Router vorhanden sein. Zudem wird erwartet, dass der Stamm der Baumstruktur mit einer größeren Multicast-Infrastruktur verbunden ist.

Ein Proxy-Gerät, das eine Weiterleitung auf IGMP/MLD-Basis durchführt, verfügt über genau eine Upstream-Schnittstelle und mindestens eine Downstream-Schnittstelle. Diese Angaben werden explizit konfiguriert – es gibt kein Protokoll, mit dem ermittelt werden könnte, welchen Typ die betroffenen Schnittstellen aufweisen. Ein Proxy-Gerät führt die Router-seitigen Aufgaben von IGMP/MLD auf seinen Downstream-Schnittstellen und die Hostaufgaben von IGMP/MLD auf seiner Upstream-Schnittstelle durch.

Es wird nur genau eine Baumstruktur unterstützt

Weiterleitungsregeln und Abfrager

Die folgenden Regeln werden angewendet:

- Ein Multicast-Paket, das an der Upstream-Schnittstelle empfangen wird, wird nur dann über alle das Paket anfordernden Downstream-Schnittstellen weitergeleitet, wenn das Proxy-Gerät der Abfrager für die Schnittstellen ist.
- Ein Proxy-Gerät verwirft auf einer Downstream-Schnittstelle empfangene Multicast-Pakete, wenn es nicht der Abfrager für die Schnittstelle ist.
- Ein Multicast-Paket, das an einer Downstream-Schnittstelle empfangen wird, für die das Proxy-Gerät der Abfrager ist, wird nur dann über die Upstream-Schnittstelle und alle das Paket anfordernden Downstream-Schnittstellen weitergeleitet, wenn das Proxy-Gerät der Abfrager für die Schnittstellen ist.

Schutz von Downstream-Schnittstellen

IP-Multicast-Datenverkehr, der an einer Schnittstelle des IGMP/MLD-Baums eintrifft, wird standardmäßig weitergeleitet. Sie können die Weiterleitung von IP-Multicast-Datenverkehr deaktivieren, der auf Downstream-Schnittstellen empfangen wird. Dies kann global oder für eine gegebene Downstream-Schnittstelle erfolgen.

Multicast-Eigenschaften

Wählen Sie folgende Methode, um die Multicast-Filterung zu aktivieren:

SCHRITT 1 Klicken Sie auf **Multicast > Eigenschaften**.

SCHRITT 2 Geben Sie die Parameter ein.

- **Bridge-Multicast-Filterstatus**: Wählen Sie diese Option aus, um die Filterung zu aktivieren.
- **VLAN-ID**: Wählen Sie die VLAN-ID aus, um die entsprechende Weiterleitungsmethode festzulegen.
- **Weiterleitungsmethode für IPv6**: Legen Sie eine der folgenden Weiterleitungsmethoden für IPv6-Adressen fest: MAC-Gruppenadresse, IP-Gruppenadresse oder Quellspezifische IP-Gruppenadresse.
- **Weiterleitungsmethode für IPv4**: Legen Sie eine der folgenden Weiterleitungsmethoden für IPv4-Adressen fest: MAC-Gruppenadresse, IP-Gruppenadresse oder Quellspezifische IP-Gruppenadresse.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

MAC-Gruppenadresse

Die Seite „MAC-Gruppenadresse“ hat die folgenden Funktionen:

- Abfrage und Anzeige von Informationen aus der Multicast-Weiterleitungsdatenbank (MFDB) zu einer bestimmten VLAN-ID oder einer bestimmten MAC-Gruppenadresse. Diese Daten werden entweder dynamisch über IGMP/MLD-Snooping oder statisch durch manuelle Eingabe generiert.
- Hinzufügen oder Löschen von statischen Einträgen in der Multicast-Weiterleitungsdatenbank, die Informationen zur statischen Weiterleitung über die MAC-Zieladressen enthalten.
- Anzeige einer Liste aller Ports/LAGs, die Mitglied in der VLAN-ID und MAC-Adressengruppe sind, und Eingabe der Information, ob der Datenverkehr weitergeleitet werden soll.

Gehen Sie wie folgt vor, um MAC-Multicast-Gruppen zu definieren und anzuzeigen:

SCHRITT 1 Klicken Sie auf **Multicast > MAC-Gruppenadresse**.

SCHRITT 2 Geben Sie die Filterparameter ein.

- **VLAN-ID ist gleich**: Wählen Sie die VLAN-ID der Gruppe aus, die angezeigt werden soll.
- **MAC-Gruppenadresse ist gleich**: Wählen Sie die MAC-Adresse der Multicast-Gruppe aus, die angezeigt werden soll. Wenn keine MAC-Gruppenadresse festgelegt ist, enthält die Seite alle MAC-Gruppenadressen aus dem ausgewählten VLAN.

SCHRITT 3 Klicken Sie auf **Los**. Die MAC-Multicast-Gruppenadressen werden im unteren Block angezeigt.

Angezeigt werden Einträge, die Sie auf dieser Seite und auf der Seite „IP-Multicast-Gruppenadresse“ erstellt haben. Für die auf der Seite „IP-Multicast-Gruppenadresse“ erstellten Einträge werden die IP-Adressen in MAC-Adressen umgewandelt.

SCHRITT 4 Klicken Sie auf **Hinzufügen**, um eine statische MAC-Gruppenadresse hinzuzufügen.

SCHRITT 5 Geben Sie die Parameter ein.

- **VLAN-ID**: Definiert die VLAN-ID der neuen Multicast-Gruppe.
- **MAC-Gruppenadresse**: Definiert die MAC-Adresse der neuen Multicast-Gruppe.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die MAC-Multicast-Gruppe wird in der aktuellen Konfigurationsdatei gespeichert.

Zum Konfigurieren und Anzeigen der Registrierung der Schnittstellen in der Gruppe, wählen Sie eine Adresse aus, und klicken Sie auf **Details**.

Folgendes wird auf der Seite angezeigt:

- **VLAN-ID**: Die VLAN-ID der Multicast-Gruppe.
- **MAC-Gruppenadresse**: Die MAC-Adresse der Gruppe.

SCHRITT 7 Wählen Sie entweder den Port oder die LAG aus dem Menü **Filter: Schnittstellentyp**.

SCHRITT 8 Klicken Sie auf **Los**, um die Port- oder LAG-Mitgliedschaft des VLAN anzuzeigen.

SCHRITT 9 Wählen Sie die Art aus, nach der die Schnittstellen mit einer Multicast-Gruppe verbunden werden soll:

- **Statisch**: Die Schnittstelle wird als statisches Mitglied an die Multicast-Gruppe angehängt.
- **Dynamisch**: Zeigt an, dass die Schnittstelle der Multicast-Gruppe mit IGMP/MLD-Snooping hinzugefügt wurde.
- **Verboten**: Gibt an, dass der Port dieser Gruppe in diesem VLAN nicht beitreten darf.
- **Ohne**: Legt fest, dass der Port zurzeit kein Mitglied dieser Multicast-Gruppe in diesem VLAN ist.

SCHRITT 10 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

HINWEIS Einträge, die Sie auf der Seite „IP-Multicast-Gruppenadresse“ erstellt haben, können auf dieser Seite nicht gelöscht werden (auch wenn sie ausgewählt sind).

IP-Multicast-Gruppenadressen

Die Seite „IP-Multicast-Gruppenadresse“ ähnelt der Seite „MAC-Gruppenadresse“ mit der Ausnahme, dass Multicast-Gruppen durch IP-Adressen identifiziert werden.

Auf der Seite „IP-Multicast-Gruppenadresse“ können Sie IP-Multicast-Gruppen abfragen und hinzufügen.

Gehen Sie wie folgt vor, um IP-Multicast-Gruppen zu definieren und anzuzeigen:

SCHRITT 1 Klicken Sie auf **Multicast > IP-Multicast-Gruppenadresse**.

Die Seite enthält alle IP-Multicast-Gruppenadressen, die durch Snooping gelernt wurden.

SCHRITT 2 Geben Sie die für die Filterung erforderlichen Parameter ein.

- **VLAN-ID ist gleich**: Definieren Sie die VLAN-ID der Gruppe, die angezeigt werden soll.
- **IP-Version ist gleich**: Wählen Sie IPv6 oder IPv4 aus.
- **IP-Multicast-Gruppenadresse ist gleich**: Definieren Sie die IP-Adresse der Multicast-Gruppe, die angezeigt werden soll. Dies ist nur erforderlich, wenn der Weiterleitungsmodus (S,G) lautet.

- **Quell-IP-Adresse ist gleich**: Definieren Sie die Quell-IP-Adresse des sendenden Geräts. Lautet der Modus (S,G), geben Sie den Sender „S“ ein. Zusammen mit der IP-Gruppenadresse ist dies nun die Multicast-Gruppe-ID (S,G), die angezeigt werden soll. Lautet der Modus (*,G), geben Sie ein * ein, um anzuzeigen, dass die Multicast-Gruppe nur durch das Ziel definiert wird.

SCHRITT 3 Klicken Sie auf **Los**. Die Ergebnisse werden im unteren Block angezeigt. Wenn Bonjour und IGMP auf dem Gerät im Schicht-2-Systemmodus aktiviert sind, wird die IP-Multicast-Adresse von Bonjour angezeigt. Für SG500X/ESW2-550X-Geräte wird die Adresse immer angezeigt.

SCHRITT 4 Klicken Sie auf **Hinzufügen**, um eine statische IP-Multicast-Gruppenadresse hinzuzufügen.

SCHRITT 5 Geben Sie die Parameter ein.

- **VLAN-ID**: Definiert die VLAN-ID der Gruppe, die hinzugefügt werden soll.
- **IP-Version**: Wählen Sie den IP-Adresstyp aus.
- **IP-Multicast-Gruppenadresse**: Definiert die IP-Adresse der neuen Multicast-Gruppe.
- **Quellspezifisch**: Zeigt an, dass der Eintrag eine bestimmte Quelle enthält, und fügt die Adresse im Feld Quell-IP-Adresse ein. Ist dies nicht der Fall, wird der Eintrag als (*,G)-Eintrag mit einer IP-Gruppenadresse einer beliebigen IP-Quelle hinzugefügt.
- **Quell-IP-Adresse**: Definiert die Quelladresse, die eingefügt werden soll.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die IP-Multicast-Gruppe wird hinzugefügt und das Gerät wird aktualisiert.

SCHRITT 7 Zum Konfigurieren und Anzeigen der Registrierung einer IP-Gruppenadresse wählen Sie eine Adresse aus, und klicken Sie auf **Details**.

Oben im Fenster werden VLAN-ID, IP-Version, IP-Multicast-Gruppenadresse und die ausgewählte Quell-IP-Adresse angezeigt. Sie können den Filtertyp auswählen:

- **Schnittstellentyp ist gleich**: Wählen Sie aus, ob Ports oder LAGs angezeigt werden sollen.

SCHRITT 8 Wählen Sie für jede Schnittstelle den entsprechenden Verbindungstyp aus. Verfügbare Optionen sind:

- **Statisch**: Die Schnittstelle wird als statisches Mitglied an die Multicast-Gruppe angehängt.
- **Dynamisch**: Die Schnittstelle wird als dynamisches Mitglied an die Multicast-Gruppe angehängt.
- **Verboten**: Legt fest, dass dieser Port dieser Gruppe in diesem VLAN nicht beitreten darf.
- **Ohne**: Zeigt an, dass der Port zurzeit kein Mitglied dieser Multicast-Gruppe in diesem VLAN ist. Diese Option ist standardmäßig ausgewählt, bis Sie „Statisch“ oder „Verboten“ auswählen.

SCHRITT 9 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

IPv4-Multicast-Konfiguration

Auf den folgenden Seiten wird die IPv4-Multicast-Konfiguration konfiguriert:

- **IGMP-Snooping-Konfiguration**
- **IGMP-VLAN-Einstellungen**

IGMP-Snooping-Konfiguration

Damit die selektive IPv4-Multicast-Weiterleitung unterstützt wird, muss (auf der Seite „Multicast“ > „Eigenschaften“) die Bridge-Multicast-Filterung aktiviert sein. Außerdem muss auf jeder Seite „IGMP-Snooping“ das IGMP-Snooping global und für jedes relevante VLAN aktiviert sein.

Gehen Sie wie folgt vor, um das IGMP-Snooping zu aktivieren und das Gerät als IGMP-Snooping-Abfrager in einem VLAN zu bestimmen:

SCHRITT 1 Klicken Sie auf **Multicast** > **IPv4-Multicast-Konfiguration > IGMP-Snooping**.

Wenn das IGMP-Snooping global aktiviert ist, kann das den Netzwerkverkehr überwachende Gerät erkennen, welche Hosts eine Anfrage zum Empfang von Multicast-Verkehr gestellt haben. Das Gerät führt das IGMP-Snooping nur dann aus, wenn sowohl IGMP-Snooping als auch Bridge-Multicast-Filterung aktiviert sind.

SCHRITT 2 Aktivieren oder deaktivieren Sie die folgenden Funktionen:

- **IGMP-Snooping-Status**: Wählen Sie diese Option aus, um das IGMP-Snooping global für alle Schnittstellen zu aktivieren.
- **IGMP-Abfragerstatus**: Wählen Sie diese Option aus, um den IGMP-Abfrager global für alle Schnittstellen zu aktivieren.

SCHRITT 3 Zum Konfigurieren eines IGMP-Proxys für eine Schnittstelle wählen Sie ein statisches VLAN aus und klicken auf **Bearbeiten**. Geben Sie Werte für die folgenden Felder ein:

- **IGMP-Snooping-Status**: Wählen Sie diese Option aus, um das IGMP-Snooping im VLAN zu aktivieren. Das Gerät überwacht den Netzwerkdatenverkehr und legt damit fest, welche Hosts Multicast-Datenverkehr empfangen möchten. Das Gerät führt das IGMP-Snooping nur dann aus, wenn sowohl IGMP-Snooping als auch Bridge-Multicast-Filterung aktiviert sind.

- **Autom. Lernen MRouter-Ports**: Wählen Sie diese Option aus, um die Funktion zum automatischen Lernen für den Multicast-Router zu aktivieren.
- **Sofortiges Leave**: Wählen Sie diese Option aus, um dem Switch das Entfernen einer Schnittstelle, die eine Leave-Nachricht sendet, aus der Weiterleitungstabelle zu ermöglichen, ohne vorher allgemeine MAC-basierte Abfragen an die Schnittstelle zu senden. Wenn die Nachricht „IGMP Leave Group“ von einem Host empfangen wird, entfernt das System den Host-Port aus dem Tabelleneintrag. Nach dem Weiterleiten der vom Multicast-Router kommenden IGMP-Abfragen werden die Einträge durch den Host regelmäßig gelöscht, sofern er keine Meldungen zu IGMP-Mitgliedschaften von den Multicast-Clients empfängt. Wenn die Option aktiviert ist, verringert dies die zum Blockieren unnötigen IGMP-Datenverkehrs, der an einen Geräte-Port gesendet wurde, erforderliche Zeit.
- **Abfragezähler letztes Mitglied für Betrieb**: Anzahl der gruppenspezifischen IGMP-Abfragen, die gesendet wurden, bevor das Gerät annimmt, dass keine Mitglieder mehr in der Gruppe vorhanden sind, wenn das Gerät der ausgewählte Abfrager ist.
- **IGMP-Abfragerstatus**: Wählen Sie diese Option aus, um die Funktion zu aktivieren. Diese Funktion ist erforderlich, wenn kein Multicast-Router vorhanden ist.
- **Auswahl des IGMP-Abfragers**: Gibt an, ob die Auswahl des IGMP-Abfragers aktiviert oder deaktiviert ist. Wenn der Mechanismus zur Auswahl des IGMP-Abfragers aktiviert ist, unterstützt der IGMP-Snooping-Abfrager den in RFC3810 beschriebenen Standardmechanismus zur Auswahl des IGMP-Abfragers.

  Ist der Mechanismus zur Auswahl des IGMP-Abfragers deaktiviert, dann verzögert der IGMP-Snooping-Abfrager das Senden von Nachrichten mit allgemeinen Abfragen nach seiner Aktivierung für 60 Sekunden; ist kein anderer Abfrager vorhanden, so beginnt er danach mit dem Senden von Nachrichten mit allgemeinen Abfragen. Wird hingegen ein anderer Abfrager erkannt, dann wird das Senden von Nachrichten mit allgemeinen Abfragen beendet. Der IGMP-Snooping-Abfrager setzt das Senden von Nachrichten mit allgemeinen Abfragen fort, sobald er innerhalb des passiven Abfrageintervalls, das wie folgt berechnet wird, einen anderen Abfrager erkennt: Robustheit · Abfrageintervall + 0,5 · Abfrageantwortintervall.
- **IGMP-Abfragerversion**: Wählen Sie die IGMP-Version aus, die verwendet werden soll, wenn das Gerät zum ausgewählten Abfrager wird. Wählen Sie IGMPv3 aus, wenn Switches und/oder Multicast-Router im VLAN vorhanden sind, die quellspezifische IP-Multicast-Weiterleitung ausführen. Wählen Sie anderenfalls IGMPv2 aus.
- **Quell-IP-Adresse von Abfrager**: Wählen Sie die Quellschnittstelle des Geräts aus, die in gesendeten Nachrichten angegeben werden soll. In MLD wird diese Adresse automatisch vom System ausgewählt.

  HINWEIS Wenn Sie die Option „Auto“ auswählen, übernimmt das System die Quell-IP-Adresse aus der IP-Adresse, die auf der ausgehenden Schnittstelle definiert wurde.

SCHRITT 4 Wählen Sie ein VLAN aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 5 Geben Sie die Parameter wie oben beschrieben ein.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

HINWEIS Änderungen an der Konfiguration der IGMP-Snooping-Timer, z. B.: Abfragerobustheit, Abfrageintervall usw. haben keine Auswirkungen auf Timer, die bereits erstellt waren.

IGMP-Schnittstelleneinstellungen

HINWEIS Diese Seite ist nur auf SG500X- und SG500XG-Geräten verfügbar.

Eine Schnittstelle, die als Multicast-Router-Port definiert ist, empfängt alle IGMP-Pakete (Berichte und Abfragen) sowie alle Multicast-Daten.

So definieren Sie IGMP für eine Schnittstelle:

SCHRITT 1 Klicken Sie auf **Multicast** > **IPv4-Multicast-Konfiguration > IGMP-Schnittstelleneinstellungen**.

Die folgenden Felder werden für jede Schnittstelle angezeigt, für die IGMP aktiviert ist:

- **Schnittstellenname**: Schnittstelle, für die das IGMP-Snooping definiert ist.
- **Router-IGMP-Version**: IGMP-Version.
- **Abfragerobustheit**: Geben Sie die Zahl der über einen Link erwarteten Paketverluste ein.
- **Abfrageintervall (Sek)**: Intervall zwischen den allgemeinen Abfragen, das verwendet werden soll, wenn dieses Gerät als Abfrager ausgewählt wurde.
- **Max. Abfrageantwortintervall (Sek)**: Verzögerung, mit der der maximale Antwortcode berechnet werden soll, der in die regelmäßigen allgemeinen Abfragen eingegeben wurde.
- **Abfrageintervall letztes Mitglied**: Wert für die maximale Antwortverzögerung, der verwendet werden soll, wenn das Gerät den Wert für die maximale Reaktionszeit nicht aus den gruppenspezifischen Abfragen ableiten kann, die vom ausgewählten Abfrager gesendet wurden.
- **Multicast-TTL-Grenzwert**: Geben Sie den TTL-Grenzwert (Time-to-Live) für Pakete ein, die über eine Schnittstelle weitergeleitet werden.

  Multicast-Pakete mit einem TTL-Wert, der unter dem Grenzwert liegt, werden über die Schnittstelle nicht weitergeleitet.

  Der Vorgabewert 0 bedeutet, dass alle Multicast-Pakete über die Schnittstelle weitergeleitet werden.

  Der Wert 256 bedeutet, dass keine Multicast-Pakete über die Schnittstelle weitergeleitet werden.

Konfigurieren Sie den TTL-Grenzwert nur auf Border-Routern. Umgekehrt werden Router, auf denen Sie einen TTL-Grenzwert konfigurieren, automatisch zu Border-Routern.

SCHRITT 2 Wählen Sie eine Schnittstelle aus, und klicken Sie auf **Bearbeiten**. Geben Sie die Werte in die oben beschriebenen Felder ein.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

IGMP-VLAN-Einstellungen

So konfigurieren Sie IGMP für ein bestimmtes VLAN

SCHRITT 1 Klicken Sie auf **Multicast** > **IPv4-Multicast-Konfiguration > IGMP-VLAN-Einstellungen**.

Die folgenden Felder werden für jedes VLAN angezeigt, in dem IGMP aktiviert ist:

- **Schnittstellenname**: VLAN, für das das IGMP-Snooping definiert ist.
- **Router-IGMP-Version**: IGMP-Snooping-Version.
- **Abfragerobustheit**: Geben Sie die Zahl der über einen Link erwarteten Paketverluste ein.
- **Abfrageintervall (Sek)**: Intervall zwischen den allgemeinen Abfragen, das verwendet werden soll, wenn dieses Gerät als Abfrager ausgewählt wurde.
- **Max. Abfrageantwortintervall (Sek)**: Verzögerung, mit der der maximale Antwortcode berechnet werden soll, der in die regelmäßigen allgemeinen Abfragen eingegeben wurde.
- **Abfrageintervall letztes Mitglied (ms)**: Geben Sie den Wert für die maximale Antwortverzögerung ein, der verwendet werden soll, wenn das Gerät den Wert für die maximale Reaktionszeit nicht aus den gruppenspezifischen Abfragen ableiten kann, die vom ausgewählten Abfrager gesendet wurden.
- **Multicast-TTL-Grenzwert**: Diese Seite ist nur auf SG500X- und SG500XG-Geräten verfügbar. Geben Sie den Time-to-Live-Grenzwert für Pakete ein, die über eine Schnittstelle weitergeleitet werden.

  Multicast-Pakete mit einem TTL-Wert, der unter dem Grenzwert liegt, werden über die Schnittstelle nicht weitergeleitet.

  Der Vorgabewert 0 bedeutet, dass alle Multicast-Pakete über die Schnittstelle weitergeleitet werden.

  Der Wert 256 bedeutet, dass keine Multicast-Pakete über die Schnittstelle weitergeleitet werden.

  Konfigurieren Sie den TTL-Grenzwert nur auf Border-Routern. Umgekehrt werden Router, auf denen Sie einen TTL-Grenzwert konfigurieren, automatisch zu Border-Routern.

  SCHRITT 2 Wählen Sie eine Schnittstelle aus, und klicken Sie auf **Bearbeiten**. Geben Sie die Werte in die oben beschriebenen Felder ein.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

IGMP-Proxy

HINWEIS Diese Seite ist nur auf SG500X- und SG500XG-Geräten verfügbar.

So konfigurieren Sie IGMP-Proxy:

SCHRITT 1 Klicken Sie auf **Multicast** > **IPv4-Multicast-Konfiguration > IGMP-Proxy**.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **IGMP-Multicast-Routing**: Wählen Sie diese Option aus, um das IPv4-Multicast-Routing zu aktivieren.
- **Schutz von Downstream-Schnittstellen**: Wählen Sie diese Option aus, um Downstream-Pakete zu verwerfen, die nicht für das Gerät erforderlich sind.
- **Source-Specific Multicast**: Wählen Sie diese Option aus, um die Zustellung von Multicast-Paketen zu aktivieren, die von einer bestimmten Quelladresse stammen, die im nächsten Feld definiert wird.
- **SSM-IPv4-Zugriffsliste**: Hier wird die Liste mit den Quelladressen definiert, von denen stammende Multicast-Pakete zugestellt werden:
  - *Standardliste*: Setzt die Zugriffsliste für den SSM-Bereich auf 232.0.0.0/8.
  - *Benutzerdefinierte Zugriffsliste*: Hiermit wählen Sie den Namen der Standard-IPv4-Zugriffsliste aus, die den SSM-Bereich definiert. Diese Zugriffslisten sind in **Zugriffslisten** definiert.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Um Schutz zu einem VLAN hinzuzufügen, klicken Sie auf **Hinzufügen** und geben Werte in die folgenden Felder ein:

- **Upstream-Schnittstelle**: Wählen Sie die Upstream-Schnittstelle aus. Da nur eine einzige Upstream-Schnittstelle vorhanden ist, ist dieses Feld abgeblendet, falls bereits eine Upstream-Schnittstelle ausgewählt wurde.
- **Downstream-Schnittstelle**: Wählen Sie die Downstream-Schnittstelle aus. Es können mehrere Downstream-Schnittstellen vorhanden sein.
- **Schutz für Downstream-Schnittstellen**: Wählen Sie eine der folgenden Optionen aus:
  - *Globale Einstellungen verwenden*: Bei dieser Auswahl wird der im globalen Block festgelegte Status verwendet.
  - *Deaktivieren*: Hiermit wird die Weiterleitung von IPv4-Multicast-Datenverkehr über Downstream-Schnittstellen deaktiviert.
  - *Aktivieren*: Hiermit wird die Weiterleitung über Downstream-Schnittstellen aktiviert.

Folgende Felder werden für jede IP-Multicast-Route angezeigt:

- **Quelladresse**: Unicast-Quell-IPv4-Adresse.
- **Gruppenadresse**: Multicast-Ziel-IPv4-Adresse.
- **Eingehende Schnittstelle**: Schnittstelle, über die der Empfang eines von der Quelle stammenden Multicast-Pakets erwartet wird. Wird das Paket nicht an dieser Schnittstelle empfangen, dann wird es verworfen.
- **Ausgehende Schnittstellen**: Schnittstellen, über die Pakete weitergeleitet werden.
- **Betriebszeit**: Zeitraum in Stunden, Minuten und Sekunden, seit der Eintrag in der IP-Multicast-Routing-Tabelle vorhanden ist.
- **Ablaufzeit**: Zeitraum in Stunden, Minuten und Sekunden, bis der Eintrag aus der IP-Multicast-Routing-Tabelle entfernt wird.

IPv6-Multicast-Konfiguration

Auf den folgenden Seiten wird die IPv6-Multicast-Konfiguration konfiguriert:

- **MLD-Snooping**
- **MLD-VLAN-Einstellungen**
- **MLD-Proxy**

MLD-Snooping

Damit die selektive IPv6-Multicast-Weiterleitung unterstützt wird, muss (auf der Seite „Multicast“ > „Eigenschaften“) die Bridge-Multicast-Filterung aktiviert sein. Außerdem muss auf jeder Seite „MLD-Snooping“ das MLD-Snooping global und für jedes relevante VLAN aktiviert sein.

So aktivieren Sie MLD-Snooping und konfigurieren es auf einem VLAN:

SCHRITT 1 Klicken Sie auf **Multicast** > **IPv6-Multicast-Konfiguration > MLD-Snooping**.

Wenn MLD-Snooping global aktiviert ist, kann das den Netzwerkverkehr überwachende Gerät erkennen, welche Hosts eine Anfrage zum Empfang von Multicast-Verkehr gestellt haben. Das Gerät führt nur dann MLD-Snooping aus, wenn sowohl MLD-Snooping als auch Bridge-Multicast-Filterung aktiviert sind.

SCHRITT 2 Aktivieren oder deaktivieren Sie die folgenden Funktionen:

- **MLD-Snooping-Status**: Wählen Sie diese Option aus, um das MLD-Snooping global für alle Schnittstellen zu aktivieren.

- **MLD-Abfragerstatus**: Wählen Sie diese Option aus, um den MLD-Abfrager global für alle Schnittstellen zu aktivieren.

SCHRITT 3 Zum Konfigurieren eines MLD-Proxys für eine Schnittstelle wählen Sie ein statisches VLAN aus und klicken auf **Bearbeiten**. Geben Sie Werte für die folgenden Felder ein:

- **MLD-Snooping-Status**: Wählen Sie diese Option aus, um das MLD-Snooping im VLAN zu aktivieren. Das Gerät überwacht den Netzwerkdatenverkehr und legt damit fest, welche Hosts Multicast-Datenverkehr empfangen möchten. Das Gerät führt das MLD-Snooping nur dann aus, wenn sowohl MLD-Snooping als auch Bridge-Multicast-Filterung aktiviert sind.
- **Autom. Lernen MRouter-Ports**: Wählen Sie diese Option aus, um die Funktion zum automatischen Lernen für den Multicast-Router zu aktivieren.
- **Sofortiges Leave**: Wählen Sie diese Option aus, um dem Switch das Entfernen einer Schnittstelle, die eine Leave-Nachricht sendet, aus der Weiterleitungstabelle zu ermöglichen, ohne vorher allgemeine MAC-basierte Abfragen an die Schnittstelle zu senden. Wenn die Nachricht „MLD Leave Group“ von einem Host empfangen wird, entfernt das System den Host-Port aus dem Tabelleneintrag. Nach dem Weiterleiten der vom Multicast-Router kommenden MLD-Abfragen werden die Einträge durch den Host regelmäßig gelöscht, sofern er keine Meldungen zu MLD-Mitgliedschaften von den Multicast-Clients empfängt. Wenn die Option aktiviert ist, verringert dies die zum Blockieren unnötigen MLD-Datenverkehrs, der an einen Geräte-Port gesendet wurde, erforderliche Zeit.
- **Abfragezähler letztes Mitglied für Betrieb**: Anzahl der gruppenspezifischen MLD-Abfragen, die gesendet wurden, bevor das Gerät annimmt, dass keine Mitglieder mehr in der Gruppe vorhanden sind, wenn das Gerät der ausgewählte Abfrager ist.
  - *Abfragerobustheit verwenden*: Dieser Wert wird auf der Seite **MLD-Schnittstelleneinstellungen** festgelegt.
  - *Benutzerdefiniert*: Geben Sie einen benutzerdefinierten Wert ein.
- **MLD-Abfragerstatus**: Wählen Sie diese Option aus, um die Funktion zu aktivieren. Diese Funktion ist erforderlich, wenn kein Multicast-Router vorhanden ist.
- **Auswahl des MLD-Abfragers**: Gibt an, ob die Auswahl des MLD-Abfragers aktiviert oder deaktiviert ist. Wenn der Mechanismus zur Auswahl des MLD-Abfragers aktiviert ist, unterstützt der MLD-Snooping-Abfrager den in RFC3810 beschriebenen Standardmechanismus zur Auswahl des MLD-Abfragers.

  Ist der Mechanismus zur Auswahl des MLD-Abfragers deaktiviert, dann verzögert der MLD-Snooping-Abfrager das Senden von Nachrichten mit allgemeinen Abfragen nach seiner Aktivierung für 60 Sekunden; ist kein anderer Abfrager vorhanden, so beginnt er danach mit dem Senden von Nachrichten mit allgemeinen Abfragen. Wird hingegen ein anderer Abfrager erkannt, dann wird das Senden von Nachrichten mit allgemeinen Abfragen beendet. Der MLD-Snooping-Abfrager setzt das Senden von Nachrichten mit allgemeinen Abfragen fort, sobald er innerhalb des passiven Abfrageintervalls, das wie folgt berechnet wird, einen anderen Abfrager erkennt: Robustheit · Abfrageintervall + 0,5 · Abfrageantwortintervall.

- **MLD-Abfragerversion**: Wählen Sie die MLD-Version aus, die verwendet werden soll, wenn das Gerät zum ausgewählten Abfrager wird. Wählen Sie MLDv2 aus, wenn Switches und/oder Multicast-Router im VLAN vorhanden sind, die quellspezifische IP-Multicast-Weiterleitung ausführen. Andernfalls wählen Sie „MLDv1“ aus.

SCHRITT 4 Wählen Sie ein VLAN aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 5 Geben Sie die Parameter wie oben beschrieben ein.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

HINWEIS Änderungen an der Konfiguration der MLD-Snooping-Timer, z. B.: Abfragerobustheit, Abfrageintervall usw. haben keine Auswirkungen auf Timer, die bereits erstellt waren.

MLD-Schnittstelleneinstellungen

HINWEIS Diese Seite ist nur auf SG500X- und SG500XG-Geräten verfügbar.

Eine Schnittstelle, die als Multicast-Router-Port definiert ist, empfängt alle MLD-Pakete (Berichte und Abfragen) sowie alle Multicast-Daten.

So konfigurieren Sie eine Schnittstelle als Multicast-Router-Schnittstelle:

SCHRITT 1 Klicken Sie auf **Multicast** > **IPv6-Multicast-Konfiguration > MLD-Schnittstelleneinstellungen**.

Die folgenden Felder werden für jede Schnittstelle angezeigt, für die MLD aktiviert ist:

- **Router-MLD-Version**: MLD-Version des Multicast-Routers.
- **Abfragerobustheit**: Geben Sie die Zahl der über einen Link erwarteten Paketverluste ein.
- **Abfrageintervall (Sek)**: Intervall zwischen den allgemeinen Abfragen, das verwendet werden soll, wenn dieses Gerät als Abfrager ausgewählt wurde.
- **Max. Abfrageantwortintervall (Sek)**: Verzögerung, mit der der maximale Antwortcode berechnet werden soll, der in die regelmäßigen allgemeinen Abfragen eingegeben wurde.
- **Abfrageintervall letztes Mitglied**: Wert für die maximale Antwortverzögerung, der verwendet werden soll, wenn das Gerät den Wert für die maximale Reaktionszeit nicht aus den gruppenspezifischen Abfragen ableiten kann, die vom ausgewählten Abfrager gesendet wurden.

- **Multicast-TTL-Grenzwert**: Geben Sie den TTL-Grenzwert (Time-to-Live) für Pakete ein, die über eine Schnittstelle weitergeleitet werden.

  Multicast-Pakete mit einem TTL-Wert, der unter dem Grenzwert liegt, werden über die Schnittstelle nicht weitergeleitet.

  Der Vorgabewert 0 bedeutet, dass alle Multicast-Pakete über die Schnittstelle weitergeleitet werden.

  Der Wert 256 bedeutet, dass keine Multicast-Pakete über die Schnittstelle weitergeleitet werden.

  Konfigurieren Sie den TTL-Grenzwert nur auf Border-Routern. Umgekehrt werden Router, auf denen Sie einen TTL-Grenzwert konfigurieren, automatisch zu Border-Routern.

SCHRITT 2 Zum Konfigurieren einer Schnittstelle wählen Sie sie aus und klicken auf **Bearbeiten**. Geben Sie Werte in die oben beschriebenen Felder ein.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

MLD-VLAN-Einstellungen

So konfigurieren Sie MLD für ein bestimmtes VLAN

SCHRITT 1 Klicken Sie auf **Multicast** > **IPv6-Multicast-Konfiguration > MLD-VLAN-Einstellungen**.

Die folgenden Felder werden für jedes VLAN angezeigt, in dem MLD aktiviert ist:

- **Schnittstellenname**: VLAN, für das die MLD-Informationen angezeigt werden sollen.
- **Router-MLD-Version**: Version des MLD-Routers.
- **Abfragerobustheit**: Geben Sie die Zahl der über einen Link erwarteten Paketverluste ein.
- **Abfrageintervall (Sek)**: Intervall zwischen den allgemeinen Abfragen, das verwendet werden soll, wenn dieses Gerät als Abfrager ausgewählt wurde.
- **Max. Abfrageantwortintervall (Sek)**: Verzögerung, mit der der maximale Antwortcode berechnet werden soll, der in die regelmäßigen allgemeinen Abfragen eingegeben wurde.
- **Abfrageintervall letztes Mitglied (ms)**: Geben Sie den Wert für die maximale Antwortverzögerung ein, der verwendet werden soll, wenn das Gerät den Wert für die maximale Reaktionszeit nicht aus den gruppenspezifischen Abfragen ableiten kann, die vom ausgewählten Abfrager gesendet wurden.

- **Multicast-TTL-Grenzwert**: Geben Sie den TTL-Grenzwert (Time-to-Live) für Pakete ein, die über eine Schnittstelle weitergeleitet werden. Nur auf SG500X- und SG500XG-Geräten verfügbar.

  Multicast-Pakete mit einem TTL-Wert, der unter dem Grenzwert liegt, werden über die Schnittstelle nicht weitergeleitet.

  Der Vorgabewert 0 bedeutet, dass alle Multicast-Pakete über die Schnittstelle weitergeleitet werden.

  Der Wert 256 bedeutet, dass keine Multicast-Pakete über die Schnittstelle weitergeleitet werden.

  Konfigurieren Sie den TTL-Grenzwert nur auf Border-Routern. Umgekehrt werden Router, auf denen Sie einen TTL-Grenzwert konfigurieren, automatisch zu Border-Routern.

SCHRITT 2 Zum Konfigurieren eines VLAN wählen Sie es aus und klicken auf **Bearbeiten**. Geben Sie Werte in die oben beschriebenen Felder ein.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

MLD-Proxy

HINWEIS Diese Seite ist nur auf SG500X- und SG500XG-Geräten verfügbar.

So konfigurieren Sie MLD-Proxy:

SCHRITT 1 Klicken Sie auf **Multicast** > **IPv6-Multicast-Konfiguration > MLD-Proxy**.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **MLD-Multicast-Routing**: Wählen Sie diese Option aus, um das IPv6-Multicast-Routing zu aktivieren.
- **Schutz von Downstream-Schnittstellen**: Wählen Sie diese Option aus, um Downstream-Pakete zu verwerfen, die nicht für das Gerät erforderlich sind.
- **Source-Specific Multicast**: Wählen Sie diese Option aus, um die Zustellung von Multicast-Paketen zu aktivieren, die von einer bestimmten Quelladresse stammen, die im nächsten Feld definiert wird.
- **SSM-IPv6-Zugriffsliste**: Hier wird die Liste mit den Quelladressen definiert, von denen stammende Multicast-Pakete zugestellt werden:
  - *Standardliste*: Setzt die Zugriffsliste für den SSM-Bereich auf FF3E::/32.
  - *Benutzerdefinierte Zugriffsliste*: Hiermit wählen Sie den Namen der Standard-IPv6-Zugriffsliste aus, die den SSM-Bereich definiert. Diese Zugriffslisten sind in **IPv6-Zugriffslisten** definiert.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Um Schutz zu einem VLAN hinzuzufügen, klicken Sie auf **Hinzufügen** und geben Werte in die folgenden Felder ein:

- **Upstream-Schnittstelle**: Wählen Sie die ausgehende Schnittstelle aus.
- **Downstream-Schnittstelle**: Wählen Sie die eingehende Schnittstelle aus.
- **Schutz für Downstream-Schnittstellen**: Wählen Sie eine der folgenden Optionen aus:
  - *Globale Einstellungen verwenden*: Bei dieser Auswahl wird der im globalen Block festgelegte Status verwendet.
  - *Deaktivieren*: Hiermit wird die Weiterleitung von IPv6-Multicast-Datenverkehr über Downstream-Schnittstellen deaktiviert.
  - *Aktivieren*: Hiermit wird die Weiterleitung über Downstream-Schnittstellen aktiviert.

Folgende Felder werden für jede IP-Multicast-Route angezeigt:

- **Quelladresse**: Unicast-Quell-IPv4-Adresse.
- **Gruppenadresse**: Multicast-Ziel-IPv4-Adresse.
- **Eingehende Schnittstelle**: Schnittstelle, über die der Empfang eines von der Quelle stammenden Multicast-Pakets erwartet wird. Wird das Paket nicht an dieser Schnittstelle empfangen, dann wird es verworfen.
- **Ausgehende Schnittstellen**: Schnittstellen, über die Pakete weitergeleitet werden.
- **Betriebszeit**: Zeitraum in Stunden, Minuten und Sekunden, seit der Eintrag in der IP-Multicast-Routing-Tabelle vorhanden ist.
- **Ablaufzeit**: Zeitraum in Stunden, Minuten und Sekunden, bis der Eintrag aus der IP-Multicast-Routing-Tabelle entfernt wird.

IGMP/MLD-Snooping-IP-Multicast-Gruppe

Auf der Seite „IGMP/MLD-Snooping-IP-Multicast-Gruppe“ werden die IPv4- und IPv6-Gruppenadressen angezeigt, die das Gerät aus den gesnoopten IGMP/MLD-Nachrichten gelernt hat.

Die Informationen auf dieser Seite unterscheiden sich möglicherweise etwa von denen auf der Seite „MAC-Gruppenadresse“. Ein Beispiel: Wenn das System nach MAC-basierten Gruppen filtert und ein Port vorhanden ist, der den Multicast-Gruppen 224.1.1.1 und 225.1.1.1 beitreten soll, werden beide derselben MAC-Multicast-Adresse 01:00:5e:01:01:01 zugeordnet. In diesem Fall gibt es einen einzigen Eintrag auf der Seite MAC-Multicast, aber zwei Einträge auf dieser Seite.

Gehen Sie wie folgt vor, um eine IP-Multicast-Gruppe abzufragen:

SCHRITT 1 Klicken Sie auf **Multicast** > **IGMP/MLD-Snooping-IP-Multicast-Gruppe**.

SCHRITT 2 Legen Sie den Typ der Snooping-Gruppe fest, nach dem gesucht werden soll: IGMP oder MLD.

SCHRITT 3 Geben Sie einige oder alle der folgenden Abfragefilterkriterien ein:

- **Gruppenadresse ist gleich**: Definiert die MAC-Adresse oder IP-Adresse der Multicast-Gruppe, die abgefragt werden soll.
- **Quelladresse ist gleich**: Definiert die Senderadresse, die abgefragt werden soll.
- **VLAN-ID ist gleich**: Definiert die VLAN-ID, die abgefragt werden soll.

SCHRITT 4 Klicken Sie auf **Los**. Folgende Felder werden für jede Multicast-Gruppe angezeigt:

- **VLAN**: Die VLAN-ID.
- **Gruppenadresse**: Die MAC-Adresse oder IP-Adresse der Multicast-Gruppe.
- **Quelladresse**: Die Senderadresse für alle angegebenen Gruppen-Ports.
- **Eingeschlossene Ports**: Die Liste der Zielports für den Multicast-Strom.
- **Ausgeschlossene Ports**: Liste der Ports, die nicht zur Gruppe gehören.
- **Kompatibilitätsmodus**: Die älteste IGMP/MLD-Version einer Hostregistrierung, die das Gerät für die IP-Gruppenadresse empfängt.

Multicast-Router-Ports

Ein Multicast-Router-Port (MRouter) ist ein Port, der an einen Multicast-Router angeschlossen ist. Das Gerät berücksichtigt die Nummern der Multicast-Router-Ports, wenn es die Multicast-Ströme und IGMP/MLD-Registrierungsnachrichten weiterleitet. Dies ist erforderlich, damit die Multicast-Router ihrerseits die Multicast-Ströme weiterleiten und die Anmeldenachrichten an andere Subnetze verbreiten können.

So können Sie mit dem Multicast-Router verbundene dynamisch erkannte Ports statisch konfigurieren oder anzeigen:

SCHRITT 1 Klicken Sie auf **Multicast** > **Multicast-Router-Port**.

SCHRITT 2 Geben Sie einige oder alle der folgenden Abfragefilterkriterien ein:

- **VLAN-ID ist gleich**: Wählen Sie die VLAN-ID für die beschriebenen Router-Ports aus.

- **IP-Version ist gleich**: Wählen Sie die vom Multicast-Router unterstützte IP-Version aus.
- **Schnittstellentyp ist gleich**: Wählen Sie aus, ob Ports oder LAGs angezeigt werden sollen.

SCHRITT 3 Klicken Sie auf **Los**. Die Schnittstellen, die die Abfragekriterien erfüllen, werden angezeigt.

SCHRITT 4 Wählen Sie für jeden Port bzw. jede LAG den Zuordnungstyp aus. Verfügbare Optionen sind:

- **Statisch**: Der Port wird statisch als Multicast-Router-Port konfiguriert.
- **Dynamisch**: (Nur Anzeige) Der Port wird durch eine MLD/IGMP-Abfrage dynamisch als Multicast-Router-Port konfiguriert. Um das dynamische Lernen von Multicast-Router-Ports zu aktivieren, gehen Sie zur Seite **Multicast** > **IGMP-Snooping** und zur Seite **Multicast** > **MLD-Snooping**.
- **Verboten**: Der Port wird nicht als Multicast-Router-Port konfiguriert, selbst wenn IGMP- oder MLD-Abfragen an diesem Port empfangen wurden. Wenn „Verboten“ an einem Port aktiviert ist, wird MRouter an diesem Port nicht erlernt (das heißt, „MRouter-Ports autom. erlernen“ ist an diesem Port nicht aktiviert).
- **Ohne**: Der Port ist zurzeit kein Multicast-Router-Port.

SCHRITT 5 Klicken Sie auf **Übernehmen**, um das Gerät zu aktualisieren.

Alle weiterleiten

Auf der Seite „Alle weiterleiten“ können Sie die Ports und/oder LAGs konfigurieren, die Multicast-Ströme von einem bestimmten VLAN empfangen sollen. Für diese Funktion muss die Bridge-Multicast-Filterung auf der Seite „Eigenschaften“ aktiviert sein. Wenn die Filterung deaktiviert ist, wird der gesamte Multicast-Verkehr an Ports auf dem Gerät geflutet.

Sie können einen Port statisch (manuell) mit dem Merkmal „Alle weiterleiten“ konfigurieren, wenn die mit dem Port verbundenen Geräte IGMP und/oder MLD nicht unterstützen.

IGMP- oder MLD-Nachrichten, die nicht an die Ports weitergeleitet werden, werden als *Alle weiterleiten* definiert.

HINWEIS Die Konfiguration betrifft nur die Ports, die Mitglied in dem ausgewählten VLAN sind.

Gehen Sie wie folgt vor, um das Multicast-Merkmal „Alle weiterleiten“ zu definieren:

SCHRITT 1 Klicken Sie auf **Multicast** > **Alle weiterleiten**.

SCHRITT 2 Definieren Sie Folgendes:

- **VLAN-ID ist gleich**: Die VLAN-ID, für die die Ports/LAGs angezeigt werden sollen.
- **Schnittstellentyp ist gleich**: Definieren Sie, ob Ports oder LAGs angezeigt werden sollen.

SCHRITT 3 Klicken Sie auf **Los**. Der Status aller Ports/LAGs wird angezeigt.

SCHRITT 4 Wählen Sie mithilfe der folgenden Methoden den Port bzw. die LAG aus, für den bzw. für die „Alle weiterleiten“ definiert werden soll:

- **Statisch**: Der Port empfängt alle Multicast-Ströme.
- **Verboten**: Ports dürfen keine Multicast-Ströme empfangen, selbst wenn IGMP/MLD-Snooping angibt, dass der Port einer Multicast-Gruppe beitritt.
- **Ohne**: Der Port ist zurzeit kein Port mit dem Merkmal „Alle weiterleiten“.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Nicht registrierter Multicast

Mit dieser Funktion kann sichergestellt werden, dass der Kunde nur angefragte (registrierte) Multicast-Gruppen empfängt und keine anderen, die im Netzwerk übertragen werden (also nicht registrierte).

Nicht registrierte Multicast-Frames werden normalerweise an alle Ports im VLAN weitergeleitet.

Sie können einen Port auswählen, der nicht registrierte Multicast-Ströme empfangen oder ablehnen (filtern) soll. Die Konfiguration ist für jedes VLAN gültig, in dem der Port Mitglied ist (oder sein wird).

Gehen Sie wie folgt vor, um die Einstellungen für nicht registriertes Multicast zu definieren:

SCHRITT 1 Klicken Sie auf **Multicast** > **Nicht registriertes Multicast**.

SCHRITT 2 **Schnittstellentyp ist gleich**: Hiermit wählen Sie aus, ob Ports oder LAGs angezeigt werden sollen.

SCHRITT 3 Klicken Sie auf **Los**.

SCHRITT 4 Definieren Sie Folgendes:

- **Port/LAG**: Zeigt die Port- oder LAG-ID an.
- Zeigt den Weiterleitungsstatus der ausgewählten Schnittstelle an. Folgende Werte sind gültig:
  - *Weiterleitung*: Aktiviert die Weiterleitung nicht registrierter Multicast-Frames an die ausgewählte Schnittstelle.
  - *Filterung*: Aktiviert die Filterung (Ablehnung) nicht registrierter Multicast-Frames an der ausgewählten Schnittstelle.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die Einstellungen werden gespeichert und die aktuelle Konfigurationsdatei wird aktualisiert.

19

IP-Konfiguration

IP-Schnittstellenadressen können manuell vom Benutzer oder automatisch von einem DHCP-Server konfiguriert werden. Dieser Abschnitt enthält Informationen zum Definieren der Geräte-IP-Adressen (manuell oder durch Konfigurieren des Geräts als DHCP-Client).

In diesem Abschnitt werden die folgenden Themen behandelt:

- **Übersicht**
- **IPv4-Management und -Schnittstellen**
- **DHCP-Server**
- **IPv6-Verwaltung und -Schnittstellen**
- **Domänenname**

Übersicht

HINWEIS SG500X-Geräte arbeiten immer im L3- und L2-Modus, sofern sie sich nicht im Hybridmodus befinden (siehe **Stack-Einheitenmodus**) und wie Sx500-Geräte fungieren. Die Sx500-Geräte dagegen müssen immer auf den Betrieb entweder im Schicht-2- oder Schicht 3-Systemmodus festgelegt werden. Wenn in diesem Abschnitt von einem Gerät die Rede ist, das im Schicht-3-Systemmodus betrieben wird, sind sowohl alle SG500X-Geräte im Modus „Natives Stacking“ als auch solche Geräte gemeint, die manuell auf den Schicht-3-Systemmodus festgelegt wurden. Wenn in diesem Dokument von einem Gerät die Rede ist, das im Schicht-2-Systemmodus betrieben wird, sind sowohl alle Sx500-Geräte als auch SG500X-Geräte (im Hybridmodus) gemeint, die manuell auf den Schicht-2-Systemmodus festgelegt wurden.

Die MTU für Schicht-3-Datenverkehr auf SG500X, SG500XG und ESW2-550X ist auf 9000 Bytes beschränkt.

Einige Funktionen sind nur im Schicht-2- oder Schicht-3-Systemmodus verfügbar (siehe unten):

- Im Schicht-2-Systemmodus (nur Sx500-Geräte) fungiert das Gerät als VLAN-fähiges Schicht-2-Gerät ohne Routing-Funktionen.
- Im Schicht-3-Systemmodus verfügt das Gerät sowohl über IP-Routing-Funktionen als auch über Funktionen des Schicht-2-Systemmodus. In diesem Systemmodus behält ein Schicht-3-Port einen großen Teil der Schicht-2-Funktionalität, beispielsweise das Spanning Tree-Protokoll und die VLAN-Mitgliedschaft.
- Im Schicht-3-Systemmodus (nur Sx500-Geräte) werden vom Gerät MAC-basiertes VLAN, dynamische VLAN-Zuordnung, VLAN-Ratenbegrenzung, SYN-Raten-DoS-Schutz und erweiterte QoS-Überwachungsvorrichtungen nicht unterstützt.

Informationen zum Konfigurieren des Systemmodus (Schicht-2- oder Schicht-3-Modus) für Sx500-Geräte finden Sie auf der Seite „Systemmodus und Stack-Verwaltung“.

HINWEIS Das Wechseln von einem Systemmodus (Schicht) in einen anderen (Sx500-Geräte) erfordert einen Neustart. Anschließend wird die Startkonfiguration des Geräts gelöscht.

Schicht-2-IP-Adressierung

HINWEIS Dieser Abschnitt ist nur für Sx500-Geräte relevant.

Im Schicht-2-Systemmodus verfügt das Gerät im Management-VLAN über bis zu eine IPv4-Adresse und bis zu zwei IPv6-Schnittstellen (native Schnittstelle oder Tunnel). Diese IP-Adresse und das Standard-Gateway können manuell oder über DHCP konfiguriert werden. Die statische IP-Adresse und das Standard-Gateway für den Schicht-2-Systemmodus können Sie auf den Seiten „IPv4-Schnittstelle“ und „IPv6-Schnittstellen“ konfigurieren. Im Schicht-2-Systemmodus verwendet das Gerät das Standard-Gateway, falls konfiguriert, um mit Geräten zu kommunizieren, die sich nicht im selben Subnetz wie das Gerät befinden. Standardmäßig ist VLAN 1 das Verwaltungs-VLAN, dies kann jedoch geändert werden. Wenn das Gerät im Schicht-2-Systemmodus betrieben wird, ist es nur unter der konfigurierten IP-Adresse über sein Verwaltungs-VLAN erreichbar.

Die werkseitige Standardeinstellung für die IPv4-Adresskonfiguration ist *DHCPv4*. Dies bedeutet, dass das Gerät sich wie ein DHCPv4-Client verhält und während des Hochfahrens eine DHCPv4-Anforderung sendet.

Wenn das Gerät eine DHCPv4-Antwort mit einer IPv4-Adresse vom DHCPv4-Server empfängt, sendet es ARP-Pakete (Address Resolution Protocol), um zu bestätigen, dass die IP-Adresse eindeutig ist. Wenn die ARP-Antwort zeigt, dass die IPv4-Adresse bereits verwendet wird, sendet das Gerät eine DHCPDECLINE-Benachrichtigung sowie ein weiteres DHCPDISCOVER-Paket an den DHCP-Server, der die Adresse angeboten hat, sodass der Prozess von Neuem beginnt.

Wenn das Gerät innerhalb von 60 Sekunden keine DHCPv4-Antwort erhält, sendet es weiterhin DHCPDISCOVER-Anfragen und übernimmt die Standard-IPv4-Adresse: 192.168.1.254/24.

IP-Adresskollisionen erfolgen, wenn dieselbe IP-Adresse im selben IP-Subnetz von mehr als einem Gerät verwendet wird. Adresskollisionen erfordern administrative Maßnahmen am DHCP-Server und/oder an den Geräten, die an der Kollision mit dem Gerät beteiligt sind.

Wenn ein VLAN für die Verwendung dynamischer IPv4-Adressen konfiguriert ist, sendet das Gerät so lange DHCPv4-Anforderungen, bis ihm von einem DHCPv4-Server eine IPv4-Adresse zugewiesen wird. Im Schicht-2-Systemmodus kann nur das Verwaltungs-VLAN mit einer statischen oder dynamischen IP-Adresse konfiguriert werden. Im Schicht-3-Systemmodus können alle Schnittstellentypen (Ports, LAGs und/oder VLANs) mit einer statischen oder dynamischen IP-Adresse auf dem Gerät konfiguriert werden.

Im Folgenden werden die IP-Adresszuweisungsregeln für das Gerät beschrieben:

- Sofern das Gerät nicht mit einer statischen IP-Adresse konfiguriert ist, sendet es im Schicht-2-Systemmodus DHCPv4-Anfragen, bis es eine Antwort vom DHCP-Server empfängt.
- Wenn die IP-Adresse auf dem Gerät geändert wird, sendet das Gerät unaufgefordert ARP-Pakete an das entsprechende VLAN, um auf IP-Adresskollisionen zu prüfen. Diese Regel gilt auch, wenn das Gerät zur Standard-IP-Adresse zurückkehrt.
- Die Systemstatus-LED leuchtet ununterbrochen grün, wenn eine neue eindeutige IP-Adresse vom DHCP-Server empfangen wird. Wenn eine statische IP-Adresse eingerichtet wurde, leuchtet die Systemstatus-LED ebenfalls ununterbrochen grün. Wenn das Gerät eine IP-Adresse abruft und aktuell die werkseitig konfigurierte IP-Standardadresse 192.168.1.254 verwendet, blinkt die LED.
- Dieselben Regeln gelten, wenn ein Client den Mietvertrag vor dessen Ablaufdatum durch eine DHCPREQUEST-Benachrichtigung erneuern muss.
- Mit den Werkseinstellungen wird, wenn keine statisch definierte oder über DHCP erhaltene IP-Adresse verfügbar ist, die Standard-IP-Adresse verwendet. Wenn die anderen IP-Adressen verfügbar werden, werden diese automatisch verwendet. Die Standard-IP-Adresse ist stets im Verwaltungs-VLAN lokalisiert.

Schicht-3-IP-Adressierung

Im Schicht-3-Systemmodus kann das Gerät über mehrere IP-Adressen verfügen. Jede IP-Adresse kann bestimmten Ports, LAGs oder VLANs zugeordnet werden. Diese IP-Adressen werden auf den Seiten „IPv4-Schnittstelle“ und „IPv6-Schnittstellen“ im Schicht-3-Systemmodus konfiguriert. Dies bietet eine größere Netzwerkflexibilität gegenüber dem Schicht-2-Systemmodus, in dem nur eine einzige IP-Adresse konfiguriert werden kann. Wenn das Gerät im Schicht-3-Systemmodus betrieben wird, ist es von den entsprechenden Schnittstellen aus unter allen seinen IP-Adressen erreichbar.

Im Schicht-3-Systemmodus wird keine vordefinierte Standardroute bereitgestellt. Wenn das Gerät standortfern verwaltet werden soll, muss eine Standardroute definiert werden. Alle durch DHCP zugewiesenen Standard-Gateways werden als Standardrouten gespeichert. Zusätzlich können Sie Standardrouten auch manuell definieren. Diese werden auf den Seiten „Statische IPv4-Routen“ und „IPv6-Routen“ definiert.

Alle für das Gerät konfigurierten oder diesem zugewiesenen IP-Adressen werden in diesem Handbuch als „Verwaltungs-IP-Adressen“ bezeichnet.

Wenn die Seiten für Schicht 2 und Schicht 3 voneinander abweichen, werden beide Versionen angezeigt.

Loopback-Schnittstelle

Übersicht

Die Loopback-Schnittstelle ist eine virtuelle Schnittstelle, deren Betriebsstatus immer „Ein“ lautet. Wenn die auf dieser virtuellen Schnittstelle konfigurierte IP-Adresse bei der Kommunikation mit Remote-IP-Anwendungen als die lokale Adresse verwendet wird, wird die Kommunikation nicht abgebrochen, selbst wenn die tatsächliche Route zur Remote-Anwendung geändert wurde.

Der Betriebsstatus einer Loopback-Schnittstelle lautet immer „Ein“. Sie definieren darauf eine IP-Adresse (entweder IPv4 oder IPv6) und verwenden diese IP-Adresse als lokale IP-Adresse für die IP-Kommunikation mit Remote-IP-Anwendungen. Die Kommunikationsfunktion bleibt intakt, solange die Remote-Anwendungen über mindestens eine der aktiven IP-Schnittstellen (d. h. Nicht-Loopback-Schnittstellen) erreichbar sind. Andererseits wird, wenn die IP-Adresse einer IP-Schnittstelle für die Kommunikation mit Remote-Anwendungen verwendet wird, die Kommunikation beendet, wenn die IP-Schnittstelle ausfällt.

Bridging wird auf Loopback-Schnittstellen nicht unterstützt. Die Schnittstelle darf kein Mitglied eines VLAN sein, und es darf kein Schicht-2-Protokoll darauf aktiviert werden.

Die ID für die IPv6-Link-Local-Schnittstelle ist 1.

Wenn sich der Switch im Schicht-2-Systemmodus befindet, werden die folgenden Regeln unterstützt:

- Es wird nur eine Loopback-Schnittstelle unterstützt.
- Es können zwei IPv4-Schnittstellen konfiguriert werden: eine auf einem VLAN- oder Ethernet-Port und eine weitere auf der Loopback-Schnittstelle.
- Wenn die IPv4-Adresse auf dem Standard-VLAN konfiguriert wurde und das Standard-VLAN geändert wird, verschiebt der Switch die IPv4-Adresse auf den neuen Standard-VLAN.

Konfigurieren einer Loopback-Schnittstelle

Führen Sie zum Konfigurieren einer IPv4-Loopback-Schnittstelle die folgenden Schritte aus:

- Aktivieren Sie im Schicht-2-Modus die Loopback-Schnittstelle, und konfigurieren Sie deren Adresse auf der Seite „Administration > Verwaltungsschnittstelle > IPv4-Schnittstelle“. Diese Seite ist auf den folgenden Geräten nicht verfügbar: SG500X, ESW2-550X und SG500XG.
- Fügen Sie im Schicht-3-Modus eine Loopback-Schnittstelle unter „IP-Konfiguration > IPv4-Verwaltung und -Schnittstellen > IPv4-Schnittstelle“ hinzu.

Führen Sie zum Konfigurieren einer IPv6-Loopback-Schnittstelle die folgenden Schritte aus:

- Fügen Sie im Schicht-2-Modus eine Loopback-Schnittstelle auf der Seite „Administration > Verwaltungsschnittstelle > IPv6-Schnittstellen“ hinzu. Konfigurieren Sie die IPv6-Adresse dieser Schnittstelle auf der Seite „Administration > Verwaltungsschnittstelle > IPv6-Adressen“. Diese Seite ist auf den folgenden Geräten nicht verfügbar: SG500X, ESW2-550X und SG500XG.
- Fügen Sie im Schicht-3-Modus eine Loopback-Schnittstelle unter „IP-Konfiguration > IPv6-Verwaltung und -Schnittstellen > IPv6-Schnittstelle“ hinzu. Konfigurieren Sie die IPv6-Adresse dieser Schnittstelle auf der Seite „IP-Konfiguration > IPv6-Verwaltung und -Schnittstellen > IPv6-Adressen“.

IPv4-Management und -Schnittstellen

IPv4-Schnittstelle

IPv4-Schnittstellen können auf dem Gerät definiert werden, wenn es sich im Schicht-2- oder Schicht-3-Systemmodus befindet.

Definieren einer IPv4-Schnittstelle im Schicht-2-Systemmodus

Dieser Abschnitt ist für die folgenden Geräte nicht relevant: SG500X, ESW2-550X oder SG500XG.

Um das Gerät mit dem webbasierten Konfigurationsdienstprogramm zu verwalten, muss die IP-Adresse für die IPv4-Geräteverwaltung definiert und bekannt sein. Die IP-Adresse des Geräts kann manuell konfiguriert oder automatisch von einem DHCP-Server abgerufen werden.

So konfigurieren Sie die IPv4-IP-Adresse des Geräts:

SCHRITT 1 Klicken Sie auf **Administration > Verwaltungsschnittstelle > IPv4-Schnittstelle**.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **Verwaltungs-VLAN**: Wählen Sie das Verwaltungs-VLAN, das für den Zugriff auf das Gerät über Telnet oder die grafische Weboberfläche verwendet wird. Das Standardverwaltungs-VLAN ist VLAN1.
- **IP-Adresstyp**: Wählen Sie eine der folgenden Optionen:
  - *Dynamisch*: Erkennen der IP-Adresse mithilfe von DHCP im Verwaltungs-VLAN.
  - *Statisch*: Manuelle Definition einer statischen IP-Adresse.

  HINWEIS DHCP-Option 12 (Hostnamenoption) wird unterstützt, wenn es sich beim Gerät um einen DHCP-Client handelt. Wenn DHCP-Option 12 von einem DHCP-Server empfangen wird, wird sie als Hostname des Servers gespeichert. DHCP-Option 12 wird nicht vom Gerät angefordert. Damit Sie diese Funktion verwenden können, muss der DHCP-Server unabhängig von der Anforderung für das Senden von Option 12 konfiguriert sein.

Konfigurieren Sie zum Konfigurieren einer statischen IP-Adresse die folgenden Felder:

- **IP-Adresse**: Geben Sie die IP-Adresse ein und konfigurieren Sie jeweils eines der folgenden Felder für die **Maske**:
  - **Netzwerkmaske**: Wählen Sie die IP-Adressmaske, und geben Sie sie ein.
  - **Präfixlänge**: Wählen Sie die IPv4-Präfixlänge, und geben Sie sie ein.
- **Loopback-Schnittstelle**: Wählen Sie diese Option aus, um die Konfiguration einer Loopback-Schnittstelle zu aktivieren (siehe **Loopback-Schnittstelle**).
- **Loopback-IP-Adresse**: Geben Sie die IPv4-Adresse der Loopback-Schnittstelle ein.

Füllen Sie eines der folgenden Felder für die **Loopback-Maske** aus:

- **Netzwerkmaske**: Geben Sie die Maske der IPv4-Adresse für die Loopback-Schnittstelle ein.
- **Präfixlänge**: Geben Sie die Präfixlänge der IPv4-Adresse für die Loopback-Schnittstelle ein.

- **Administratives Standard-Gateway**: Wählen Sie **Benutzerdefiniert** aus und geben Sie die IP-Adresse des Standard-Gateways ein, oder wählen Sie **Ohne** aus, um die ausgewählte IP-Adresse des Standard-Gateways von der Schnittstelle zu entfernen.
- **Betriebsstandard-Gateway**: Der aktuelle Standard-Gateway-Status.

  HINWEIS Wenn das Gerät nicht mit einem Standard-Gateway konfiguriert ist, kann es mit anderen Geräten, die sich nicht im selben IP-Subnetz befinden, nicht kommunizieren.

Wenn eine dynamische IP-Adresse vom DHCP-Server abgerufen wird, wählen Sie die folgenden aktivierten Felder aus:

- **IP-Adresse erneuern**: Die von einem DHCP-Server zugewiesene dynamische IP-Adresse des Geräts kann jederzeit erneuert werden. Abhängig von der Konfiguration des DHCP-Servers kann es vorkommen, dass das Gerät nach der Erneuerung eine neue IP-Adresse erhält, sodass im webbasierten Konfigurationsdienstprogramm die neue IP-Adresse festgelegt werden muss.
- **Automatische Konfiguration über DHCP**: Zeigt den Status der Funktion „Automatische Konfiguration“ an. Sie können dies über *Administration* > *Dateiverwaltung* > *Automatische DHCP-Konfiguration* konfigurieren.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die IPv4-Schnittstelleneinstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Definieren einer IPv4-Schnittstelle im Schicht-3-Systemmodus

Die Seite *IPv4-Schnittstelle* wird verwendet, wenn sich das Gerät im Schicht-3-Systemmodus befindet. In diesem Modus können mehrere IP-Adressen für die Geräteverwaltung konfiguriert werden, und es stehen Routing-Services zur Verfügung.

Die IP-Adresse kann für eine Port-, eine LAG- oder eine VLAN- oder Loopback-Schnittstelle konfiguriert werden.

Beim Betrieb im Schicht-3-Modus routet das Gerät den Datenverkehr zwischen den direkt angeschlossenen IP-Subnetzen, die auf dem Gerät konfiguriert sind. Das Gerät führt weiterhin das Bridging des Datenverkehrs zwischen den Geräten im selben VLAN durch. Zusätzliche IPv4-Routen für das Routing zu nicht direkt angeschlossenen Subnetzen können Sie auf der Seite „Statische IPv4-Routen“ konfigurieren.

HINWEIS Die Gerätesoftware benötigt eine VLAN-ID (VID) für jede für einen Port oder eine LAG konfigurierte IP-Adresse. Das Gerät übernimmt die erste nicht verwendete VID, beginnend mit 4094.

So konfigurieren Sie die IPv4-Adressen:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv4-Verwaltung und -Schnittstellen** > **IPv4-Schnittstelle**.

Nur für SG500X-Geräte: Aktivieren Sie IPv4-Routing, indem Sie das Kontrollkästchen **Aktivieren** aktivieren. Bei Sx500-Geräten wird IP-Routing automatisch aktiviert, wenn Sie den Systemmodus von Schicht 2 in Schicht 3 ändern.

SCHRITT 2 Wählen Sie **IPv4-Routing**, wenn das Gerät als IPv4-Router fungieren soll.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Der Parameter wird in der aktuellen Konfigurationsdatei gespeichert.

Auf dieser Seite werden folgende Felder der IPv4-Schnittstellentabelle angezeigt:

- **Schnittstelle**: Die Schnittstelle, für die die IP-Adresse definiert ist.
- **IP-Adresstyp**: Als statisch oder „DHCP“ definierte IP-Adresse.
  - *DHCP*: Von einem DHCP-Server empfangen.
  - *Statisch*: Manuell eingegeben.
- **IP-Adresse**: Konfigurierte IP-Adresse für die Schnittstelle.
- **Maske**: Konfigurierte IP-Adressmaske.
- **Status**: Ergebnis der Prüfung auf IP-Adressduplikation.
  - *Mit Vorbehalt*: Die Prüfung auf IP-Adressduplikation hat kein endgültiges Resultat ergeben.
  - *Gültig*: Die Prüfung auf IP-Adresskollision wurde durchgeführt, und es wurde keine IP-Adresskollision erkannt.
  - *Gültig-dupliziert*: Die Prüfung auf IP-Adressduplikation wurde durchgeführt, und es wurde eine duplizierte IP-Adresse erkannt.
  - *Dupliziert*: Für die Standard-IP-Adresse wurde eine duplizierte IP-Adresse erkannt.
  - *Verzögert*: Wenn der DHCP-Client beim Start aktiviert ist, wird die Zuweisung der IP-Adresse 60 Sekunden verzögert, um genug Zeit für die Erkennung der DHCP-Adresse zu lassen.
  - *Nicht empfangen*: Relevant für die DHCP-Adresse. Wenn ein DHCP-Client einen Erkennungsprozess startet, weist er eine Dummy-IP-Adresse (0.0.0.0) zu, bevor die tatsächliche Adresse abgerufen wird. Diese Dummy-Adresse hat den Status „Nicht empfangen“.

SCHRITT 4 Klicken Sie auf **Hinzufügen**.

SCHRITT 5 Wählen Sie eines der folgenden Felder aus:

- **Schnittstelle**: Wählen Sie „Port“, „LAG“ oder „VLAN“ als die mit dieser IP-Konfiguration verknüpfte Schnittstelle aus und wählen Sie in der Liste einen Wert für die Schnittstelle aus.
- **IP-Adresstyp**: Wählen Sie eine der folgenden Optionen:
  - *Dynamische IP-Adresse*: Die IP-Adresse wird von einem DHCP-Server empfangen.
  - *Statische IP-Adresse*: Geben Sie die IP-Adresse ein.

SCHRITT 6 Wenn **Statische IP-Adresse** ausgewählt wurde, füllen Sie das Feld **Maske** aus.

- **Netzwerkmaske**: Die IP-Maske für diese Adresse.
- **Präfixlänge**: Länge des IPv4-Präfixes.

SCHRITT 7 Klicken Sie auf **Übernehmen**. Die IPv4-Adresseinstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

VORSICHT Wenn sich das System in einem Stack-Modus befindet und ein Backup-Master vorhanden ist, empfiehlt Cisco das Konfigurieren der IP-Adresse als statische Adresse. Dadurch verhindern Sie, dass bei einem Stacking-Master-Switchover die Netzwerkverbindung getrennt wird. Dies liegt daran, dass der Backup-Master bei der Übernahme der Kontrolle über den Stack bei Verwendung von DHCP möglicherweise eine andere IP-Adresse erhält als die, die er von der ursprünglich als Master des Stacks aktivierten Einheit erhalten hat.

IPv4-Routen

Wenn sich das Gerät im Schicht-3-Systemmodus befindet, können Sie auf dieser Seite statische IPv4-Routen für das Gerät konfigurieren und anzeigen. Beim Routing von Datenverkehr wird der nächste Hop gemäß der längsten Übereinstimmung mit einem Präfix festgelegt (LPM-Algorithmus). Eine IPv4-Zieladresse kann mit vielen Routen in der Tabelle statischer IPv4-Routen übereinstimmen. Das Gerät verwendet die übereinstimmende Route mit der höchsten Subnetzmaske, d. h. mit der längsten Präfix-Übereinstimmung. Werden mehrere Standardgateways definiert, dann wird die niedrigste IPv4-Adresse aller konfigurierten Standardgateways verwendet.

So definieren Sie eine statische IP-Route:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv4-Verwaltung und -Schnittstellen** > **IPv4-Routen**.

Die IPv4-Routing-Tabelle wird angezeigt. Folgende Felder werden für jeden Eintrag angezeigt:

- **IP-Zielpräfix**: Präfix der IP-Zieladresse
- **Präfixlänge**: IP-Routenpräfix für die IP-Zieladresse
- **Routentyp**: Gibt an, ob die Route eine lokale, abgelehnte oder Remote-Route ist.
- **Router-IP-Adresse für nächsten Hop**: IP-Adresse für nächsten Hop oder IP-Alias für die Route
- **Routenbesitzer**: Folgende Optionen sind verfügbar:
  - *Standard*: Die Route wurde durch die Standardkonfiguration des Systems konfiguriert.
  - *Statisch*: Die Route wurde manuell erstellt.
  - *DHCP*: Die Route wurde von einem DHCP-Server empfangen.
- **Metrik**: Die Kosten für diesen Hop (niedrigere Werte werden bevorzugt)
- **Administrative Entfernung**: Administrative Entfernung zum nächsten Hop (niedrigere Werte werden bevorzugt). Für statische Routen ist dies nicht relevant.
- **Ausgehende Schnittstelle**: Ausgehende Schnittstelle dieser Route

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **IP-Zielpräfix**: Geben Sie das Präfix der IP-Zieladresse ein.
- **Maske**: Wählen Sie unter folgenden Optionen aus, und geben Sie die entsprechenden Informationen ein:
  - **Netzwerkmaske**: IP-Routenpräfix für die IP-Zieladresse
  - **Präfixlänge**: IP-Routenpräfix für die IP-Zieladresse
- **Routentyp**: Wählen Sie den Routentyp.
  - *Ablehnen*: Ablehnen der Route und Beenden des Routing zum Zielnetzwerk über alle Gateways. So wird sichergestellt, dass ein Frame gelöscht wird, wenn er mit der IP-Zieladresse dieser Route ankommt.
  - *Remote*: Angabe, dass die Route ein Remote-Pfad ist.
  - *Lokal*: Gibt an, dass die Route ein lokaler Pfad ist. Dieser Typ kann nicht erstellt werden, sondern wird vom System angelegt.

- **Router-IP-Adresse für nächsten Hop**: Geben Sie die IP-Adresse für nächsten Hop oder den IP-Alias für die Route ein.

  HINWEIS Sie können eine statische Route nicht über ein direkt verbundenes IP-Subnetz konfigurieren, in dem das Gerät seine IP-Adresse von einem DHCP-Server erhält.

- **Metrisch**: Geben Sie die administrative Distanz zum nächsten Hop ein. Möglich sind Werte im Bereich von 1 - 255.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die statische IP-Route wird in der aktuellen Konfigurationsdatei gespeichert.

RIPv2

Weitere Informationen hierzu finden Sie unter **IP-Konfiguration: RIPv2**.

Zugriffsliste

Weitere Informationen hierzu finden Sie unter **Zugriffslisten**.

VRRP

Weitere Informationen hierzu finden Sie unter **IP-Konfiguration: VRRP**.

ARP

Das Gerät verwaltet eine ARP-Tabelle (Address Resolution Protocol) für alle bekannten Geräte, die sich in den direkt mit dem Gerät verbundenen IP-Subnetzen befinden. Ein direkt verbundenes IP-Subnetz ist ein Subnetz, mit dem eine IPv4-Schnittstelle des Geräts verbunden ist. Wenn das Gerät ein Paket an ein lokales Gerät senden bzw. routen muss, sucht es in der ARP-Tabelle nach der MAC-Adresse des Geräts. Die ARP-Tabelle enthält sowohl statische als auch dynamische Adressen. Statische Adressen werden manuell konfiguriert und veralten nicht. Das Gerät erstellt dynamische Adressen anhand der ARP-Pakete, die es empfängt. Dynamische Adressen veralten nach einem konfigurierten Zeitraum.

HINWEIS Im Schicht-2-Modus werden die IP- und die MAC-Adresszuordnung in der ARP-Tabelle vom Gerät verwendet, um den vom Gerät stammenden Datenverkehr weiterzuleiten. Im Schicht-3-Modus werden die Zuordnungsinformationen sowohl für das Schicht-3-Routing als auch zum Weiterleiten des generierten Datenverkehrs verwendet.

So definieren Sie ARP-Tabellen:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration > IPv4-Verwaltung und -Schnittstellen** > **ARP**.

SCHRITT 2 Geben Sie die Parameter ein.

- **Fälligkeitszeit für ARP-Einträge**: Geben Sie den Zeitraum in Sekunden ein, den dynamische Adressen in der ARP-Tabelle verbleiben können. Eine dynamische Adresse wird fällig, wenn ihre Aufenthaltszeit in der Tabelle die Fälligkeitszeit für ARP-Einträge überschreitet. Wenn eine dynamische Adresse fällig wird, wird sie aus der Tabelle entfernt und erst wieder aufgenommen, wenn sie erneut gelernt wurde.
- **ARP-Tabelleneinträge löschen**: Wählen Sie die Art der ARP-Einträge aus, die aus dem System entfernt werden sollen.
  - *Alle*: Alle statischen und dynamischen Adressen werden sofort gelöscht.
  - *Dynamische*: Alle dynamischen Adressen werden sofort gelöscht.
  - *Statische*: Alle statischen Adressen werden sofort gelöscht.
  - *Normale Fälligkeit*: Löschen der dynamischen Adressen entsprechend der konfigurierten Fälligkeitszeit für ARP-Einträge.

SCHRITT 3 Klicken Sie auf **Übernehmen.** Die globalen ARP-Einstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

In der ARP-Tabelle werden die folgenden Felder angezeigt:

- **Schnittstelle**: Die IPv4-Schnittstelle des direkt verbundenen IP-Subnetzes, in dem sich das IP-Gerät befindet.
- **IP-Adresse**: Die IP-Adresse des IP-Geräts.
- **MAC-Adresse**: Die MAC-Adresse des IP-Geräts.
- **Status**: Angabe, ob das Gerät manuell eingegeben oder dynamisch gelernt wurde.

SCHRITT 4 Klicken Sie auf **Hinzufügen**.

SCHRITT 5 Geben Sie die Parameter ein:

- **IP-Version**: Das vom Host unterstützte IP-Adressformat. Nur IPv4 wird unterstützt.

  Schnittstelle (Schicht 3): Sie können eine IPv4-Schnittstelle für einen Port, eine LAG oder ein VLAN konfigurieren. Wählen Sie die gewünschte Schnittstelle aus der Liste der für das Gerät konfigurierten IPv4-Schnittstellen aus.

- **Schnittstelle (nur Schicht 2)**: IPv4-Schnittstelle am Gerät.

  Im Fall von Geräten im Schicht-2-Modus gibt es nur ein direkt verbundenes IP-Subnetz, das immer das Management-VLAN ist. Alle statischen und dynamischen Adressen in der ARP-Tabelle befinden sich im Management-VLAN.

- **IP-Adresse**: Geben Sie die IP-Adresse des lokalen Geräts ein.
- **Mac-Adresse**: Geben Sie die MAC-Adresse des lokalen Geräts ein.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Der ARP-Eintrag wird in der aktuellen Konfigurationsdatei gespeichert.

ARP-Proxy

Die Proxy-ARP-Technik wird vom Gerät in einem bestimmten IP-Subnetz verwendet, um ARP-Abfragen nach einer Netzwerkadresse zu beantworten, die sich nicht in diesem Netzwerk befindet.

HINWEIS Die Funktion „ARP-Proxy“ ist nur verfügbar, wenn sich das Gerät im L3-Modus befindet.

Der ARP-Proxy erkennt das Ziel des Datenverkehrs und bietet als Antwort eine weitere MAC-Adresse an. Wenn ein Host als ARP-Proxy für einen anderen Host fungiert, lenkt dies den LAN-Verkehr effektiv zu diesem Host. Der erfasste Verkehr wird dann normalerweise unter Verwendung einer weiteren Schnittstelle oder eines Tunnels vom Proxy zum vorgesehenen Ziel geroutet.

Der Prozess, bei dem eine ARP-Abfrageanforderung zu Proxy-Zwecken für eine andere IP-Adresse dazu führt, dass der Knoten mit seiner eigenen MAC-Adresse antwortet, wird manchmal als Veröffentlichung bezeichnet.

So aktivieren Sie ARP-Proxy an allen IP-Schnittstellen:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration > IPv4-Verwaltung und -Schnittstellen** > **ARP-Proxy**.

SCHRITT 2 Wählen Sie **ARP-Proxy** aus, damit das Gerät auf ARP-Anforderungen für Remote-Knoten mit der MAC-Adresse des Geräts antwortet.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Der ARP-Proxy wird aktiviert und die aktuelle Konfigurationsdatei wird aktualisiert.

UDP-Relay/IP-Helper

Die Funktion „UDP-Relais/IP-Helper“ ist nur verfügbar, wenn sich das Gerät im Schicht-3-Systemmodus befindet. Ein Switch routet normalerweise IP-Broadcast-Pakete nicht zwischen IP-Subnetzen. Wenn diese Funktion aktiviert ist, kann das Gerät jedoch bestimmte UDP-Broadcast-Pakete, die es von seinen IPv4-Schnittstellen empfangen hat, an bestimmte IP-Zieladressen weiterleiten.

Um die Relais-Weiterleitung von UDP-Paketen, die von einer bestimmten IPv4-Schnittstelle erhalten wurden, an einen bestimmen UDP-Ziel-Port zu konfigurieren, müssen Sie ein UDP-Relais hinzufügen:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration > IPv4-Verwaltung und -Schnittstellen** > **UDP-Relais/IP-Helper**.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Wählen Sie die **Quell-IP-Schnittstelle** aus, an die das Gerät basierend auf einem konfigurierten UDP-Zielport UDP-Broadcast-Pakete weiterleiten soll. Die Schnittstelle muss eine der für das Gerät konfigurierten IPv4-Schnittstellen sein.

SCHRITT 4 Geben Sie die Nummer des **UDP-Zielports** für die Pakete ein, die das Gerät weiterleiten soll. Wählen Sie einen bekannten Port in der Dropdown-Liste aus oder klicken Sie auf das Optionsfeld für den Port, um die Nummer manuell einzugeben.

SCHRITT 5 Geben Sie die **IP-Zieladresse** ein, an die die UDP-Pakete weitergeleitet werden sollen. Wenn 0.0.0.0 in das Feld eingegeben ist, werden UDP-Pakete verworfen. Wenn im Feld 255.255.255.255 eingegeben ist, werden UDP-Pakete an alle IP-Schnittstellen verschickt.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die UDP-Relais-Einstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

DHCPv4-Snooping/-Relais

DHCPv4-Snooping

DHCP-Snooping dient als Sicherheitsmechanismus, der den Empfang falscher DHCP-Antwortpakete verhindern und DHCP-Adressen protokollieren soll. Zu diesem Zweck werden Ports auf dem Gerät als vertrauenswürdig oder nicht vertrauenswürdig behandelt.

Ein vertrauenswürdiger Port ist ein Port, der mit einem DHCP-Server verbunden ist und DHCP-Adressen zuweisen darf. An vertrauenswürdigen Ports empfangene DHCP-Nachrichten dürfen das Gerät passieren.

Ein nicht vertrauenswürdiger Port ist ein Port, der keine DHCP-Adressen zuweisen darf. Standardmäßig gelten alle Ports so lange als nicht vertrauenswürdig, bis Sie sie als vertrauenswürdig deklarieren (auf der Seite „DHCP-Snooping-Schnittstelleneinstellungen“).

DHCPv4-Relais

DHCP-Relais leitet DHCP-Pakete an den DHCP-Server weiter.

DHCPv4 in Schicht 2 und Schicht 3

Im Schicht-2-Systemmodus leitet das Gerät DHCP-Nachrichten weiter, die es aus VLANs empfängt, in denen DHCP-Relais aktiviert ist.

Im Schicht-3-Systemmodus kann das Gerät auch DHCP-Nachrichten weiterleiten, die es aus VLANs ohne IP-Adresse empfängt. Wenn DHCP-Relais in einem VLAN ohne IP-Adresse aktiviert ist, wird automatisch Option 82 eingefügt. Diese Einfügung erfolgt im jeweiligen VLAN und hat keinen Einfluss auf den globalen Administrationsstatus der Einfügung von Option 82.

Transparentes DHCP-Relais

Führen Sie für transparentes DHCP-Relais bei Verwendung eines externen DHCP-Relais-Agents die folgenden Schritte aus:

- Aktivieren Sie DHCP-Snooping.
- Aktivieren Sie die Einfügung von Option 82.
- Deaktivieren Sie DHCP-Relais.

Bei regulärem DHCP-Relais:

- Aktivieren Sie DHCP-Relais.
- Die Einfügung von Option 82 muss nicht aktiviert werden.

Option 82

Option 82 (DHCP Relay Agent Information Option) übergibt Informationen zu Port und Agent einem zentralen DHCP-Server und gibt dabei an, wo eine zugewiesene IP-Adresse physisch mit dem Netzwerk verbunden ist.

Option 82 soll vor allem dem DHCP-Server die Auswahl des besten IP-Subnetzes (Netzwerkpool) erleichtern, von dem er eine IP-Adresse bezieht.

Die folgenden Optionen für Option 82 stehen auf dem Gerät zur Verfügung:

- **DHCP-Einfügung**: Fügt Option 82-Informationen Paketen hinzu, die keine fremden Option 82-Informationen enthalten.
- **DHCP-Passthrough**: DHCP-Pakete, die Option 82-Informationen von nicht vertrauenswürdigen Ports enthalten, werden weitergeleitet oder abgelehnt. An vertrauenswürdigen Ports werden DHCP-Pakete mit Option 82-Informationen immer weitergeleitet.

Die folgende Tabelle zeigt den Paketfluss durch die Module DHCP-Relais, DHCP-Snooping und Option 82:

Folgende Fälle sind möglich:

- DHCP-Client und DHCP-Server sind mit dem gleichen VLAN verbunden. In diesem Fall werden die DHCP-Nachrichten zwischen DHCP-Client und DHCP-Server durch reguläres Bridging übergeben.
- DHCP-Client und DHCP-Server sind mit verschiedenen VLANs verbunden. In diesem Fall kann nur DHCP-Relais DHCP-Nachrichten zwischen DHCP-Client und DHCP-Server übertragen. Unicast-DHCP-Nachrichten werden von regulären Routern übergeben. Wenn DHCP-Relais in einem VLAN ohne IP-Adresse aktiviert ist oder wenn das Gerät kein Router ist (Schicht-2-Gerät), wird daher ein externer Router benötigt.

DHCP-Nachrichten werden ausschließlich von DHCP-Relais an einen DHCP-Server weitergeleitet.

Interaktionen zwischen DHCPv4-Snooping, DHCPv4-Relais und Option 82

In der folgenden Tabelle wird das Verhalten des Geräts bei verschiedenen Kombinationen aus DHCP-Snooping, DHCP-Relais und Option 82 beschrieben.

Im Folgenden wird beschrieben, wie DHCP-Anforderungspakete behandelt werden, wenn DHCP-Snooping nicht aktiviert ist und DHCP-Relais aktiviert ist.

	DHCP-Relais **VLAN mit IP-Adresse**		**DHCP-Relais** **VLAN ohne IP-Adresse**	
	Paket geht ohne Option 82 ein.	Paket geht mit Option 82 ein.	Paket geht ohne Option 82 ein.	Paket geht mit Option 82 ein.
Einfügung von Option 82 deaktiviert	Paket wird ohne Option 82 gesendet.	Paket wird mit der ursprünglichen Option 82 gesendet.	Relais: Fügt Option 82 ein. Bridge: Option 82 wird nicht eingefügt.	Relais: Verwirft das Paket. Bridge: Paket wird mit der ursprünglichen Option 82 gesendet.
Einfügung von Option 82 aktiviert	Relais: Wird mit Option 82 gesendet. Bridge: Option 82 wird nicht gesendet.	Paket wird mit der ursprünglichen Option 82 gesendet.	Relais: Wird mit Option 82 gesendet. Bridge: Option 82 wird nicht gesendet.	Relais: Verwirft das Paket. Bridge: Paket wird mit der ursprünglichen Option 82 gesendet.

Im Folgenden wird beschrieben, wie DHCP-Anforderungspakete behandelt werden, wenn sowohl DHCP-Snooping als auch DHCP-Relais aktiviert ist.

	DHCP-Relais VLAN mit IP-Adresse		DHCP-Relais VLAN ohne IP-Adresse	
	Paket geht ohne Option 82 ein.	Paket geht mit Option 82 ein.	Paket geht ohne Option 82 ein.	Paket geht mit Option 82 ein.
Einfügung von Option 82 deaktiviert	Paket wird ohne Option 82 gesendet.	Paket wird mit der ursprünglichen Option 82 gesendet.	Relais: Fügt Option 82 ein. Bridge: Option 82 wird nicht eingefügt.	Relais: Verwirft das Paket. Bridge: Paket wird mit der ursprünglichen Option 82 gesendet.
Einfügung von Option 82 aktiviert	Relais: Wird mit Option 82 gesendet. Bridge: Option 82 wird hinzugefügt. (wenn der Port vertrauenswürdig ist, gleiches Verhalten wie bei nicht aktiviertem DHCP-Snooping)	Paket wird mit der ursprünglichen Option 82 gesendet.	Relais: Wird mit Option 82 gesendet. Bridge: Option 82 wird eingefügt. (wenn der Port vertrauenswürdig ist, gleiches Verhalten wie bei nicht aktiviertem DHCP-Snooping)	Relais: Verwirft das Paket. Bridge: Paket wird mit der ursprünglichen Option 82 gesendet.

Im Folgenden wird beschrieben, wie DHCP-Antwortpakete behandelt werden, wenn DHCP-Snooping deaktiviert ist:

	DHCP-Relais VLAN mit IP-Adresse		DHCP-Relais VLAN ohne IP-Adresse	
	Paket geht ohne Option 82 ein.	Paket geht mit Option 82 ein.	Paket geht ohne Option 82 ein.	Paket geht mit Option 82 ein.
Einfügung von Option 82 deaktiviert	Paket wird ohne Option 82 gesendet.	Paket wird mit der ursprünglichen Option 82 gesendet.	Relais: Verwirft Option 82. Bridge: Paket wird ohne Option 82 gesendet.	Relais: 1. Wenn die Antwort vom Gerät stammt, wird das Paket ohne Option 82 gesendet. 2. Wenn die Antwort nicht vom Gerät stammt, wird das Paket verworfen. Bridge: Paket wird mit der ursprünglichen Option 82 gesendet.
Einfügung von Option 82 aktiviert	Paket wird ohne Option 82 gesendet.	Relais: Paket wird ohne Option 82 gesendet. Bridge: Paket wird mit Option 82 gesendet.	Relais: Verwirft Option 82. Bridge: Paket wird ohne Option 82 gesendet.	Relais: Paket wird ohne Option 82 gesendet. Bridge: Paket wird mit Option 82 gesendet.

Im Folgenden wird beschrieben, wie DHCP-Antwortpakete behandelt werden, wenn sowohl DHCP-Snooping als auch DHCP-Relais aktiviert ist.

	DHCP-Relais VLAN mit IP-Adresse		DHCP-Relais VLAN ohne IP-Adresse	
	Paket geht ohne Option 82 ein.	Paket geht mit Option 82 ein.	Paket geht ohne Option 82 ein.	Paket geht mit Option 82 ein.
Einfügung von Option 82 deaktiviert	Paket wird ohne Option 82 gesendet.	Paket wird mit der ursprünglichen Option 82 gesendet.	Relais: Verwirft Option 82. Bridge: Paket wird ohne Option 82 gesendet.	Relais: 1. Wenn die Antwort vom Gerät stammt, wird das Paket ohne Option 82 gesendet. 2. Wenn die Antwort nicht vom Gerät stammt, wird das Paket verworfen. Bridge: Paket wird mit der ursprünglichen Option 82 gesendet.
Einfügung von Option 82 aktiviert	Paket wird ohne Option 82 gesendet.	Paket wird ohne Option 82 gesendet.	Relais: Verwirft Option 82. Bridge: Paket wird ohne Option 82 gesendet.	Paket wird ohne Option 82 gesendet.

DHCP-Snooping-Bindungsdatenbank

DHCP-Snooping erstellt eine Datenbank (die sogenannte DHCP-Snooping-Bindungsdatenbank), die von Informationen aus DHCP-Paketen abgeleitet wird, die über vertrauenswürdige Ports beim Gerät eingehen.

Die DHCP-Snooping-Bindungsdatenbank enthält die folgenden Daten: Eingabe-Port, Eingabe-VLAN, MAC-Adresse des Clients und gegebenenfalls IP-Adresse des Clients.

Die DHCP-Snooping-Bindungsdatenbank wird außerdem von den Funktionen IP Source Guard und Dynamic ARP Inspection verwendet, um legitime Paketquellen zu ermitteln.

Für DHCP vertrauenswürdige Ports

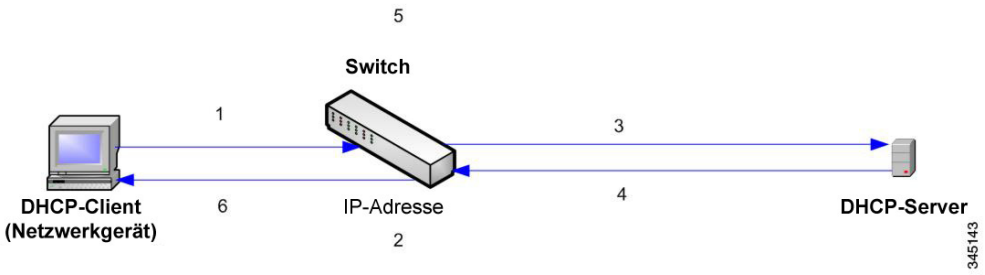
Ports können für DHCP vertrauenswürdig oder nicht vertrauenswürdig sein. Standardmäßig sind alle Ports nicht vertrauenswürdig. Verwenden Sie zum Erstellen eines vertrauenswürdigen Ports die Seite „DHCP-Snooping-Schnittstelleneinstellungen“. Pakete von diesen Ports werden automatisch weitergeleitet. Pakete von vertrauenswürdigen Ports werden verwendet, um die Bindungsdatenbank zu erstellen, und werden wie unten beschrieben behandelt.

Wenn DHCP-Snooping nicht aktiviert ist, sind alle Ports standardmäßig vertrauenswürdig.

Aufbau der DHCP-Snooping-Bindungsdatenbank

Im Folgenden wird beschrieben, wie das Gerät DHCP-Pakete behandelt, wenn DHCP-Client und DHCP-Server vertrauenswürdig sind. Im Rahmen dieses Vorgangs wird die DHCP-Snooping-Bindungsdatenbank erstellt.

Behandlung für DHCP vertrauenswürdiger Pakete



Folgende Aktionen werden ausgeführt:

SCHRITT 1 Das Gerät sendet DHCPDISCOVER, um eine IP-Adresse anzufordern, oder DHCPREQUEST, um eine IP-Adresse und Lease zu akzeptieren.

SCHRITT 2 Das Gerät untersucht das Paket und fügt die IP-MAC-Informationen der DHCP-Snooping-Bindungsdatenbank hinzu.

SCHRITT 3 Das Gerät leitet DHCPDISCOVER- oder DHCPREQUEST-Pakete weiter.

SCHRITT 4 Der DHCP-Server sendet ein DHCPOFFER-Paket, um eine IP-Adresse anzubieten, DHCPACK, um eine IP-Adresse zuzuweisen, oder DHCPNAK, um die Adressenanforderung abzulehnen.

SCHRITT 5 Das Gerät untersucht das Paket. Wenn in der DHCP-Snooping-Bindungstabelle ein dem Paket entsprechender Eintrag vorhanden ist, ersetzt das Gerät diesen bei Erhalt von DHCPACK durch eine IP-MAC-Bindung.

SCHRITT 6 Das Gerät leitet DHCPOFFER, DHCPACK oder DHCPNAK weiter.

Im Folgenden wird zusammengefasst, wie DHCP-Pakete sowohl von vertrauenswürdigen als auch von nicht vertrauenswürdigen Ports behandelt werden. Die DHCP-Snooping-Bindungsdatenbank wird im nicht flüchtigen Speicher gespeichert.

Behandlung von DHCP-Snooping-Paketen

Pakettyp	Von nicht vertrauenswürdiger Eingangsschnittstelle eingehend	Von vertrauenswürdiger Eingangsschnittstelle eingehend
DHCPDISCOVER	Nur an vertrauenswürdige Schnittstellen weiterleiten.	Wird nur an vertrauenswürdige Schnittstellen weitergeleitet.
DHCPOFFER	Filtern.	Paket gemäß DHCP-Informationen weiterleiten. Wenn die Zieladresse unbekannt ist, wird das Paket gefiltert.
DHCPREQUEST	Nur an vertrauenswürdige Schnittstellen weiterleiten.	Nur an vertrauenswürdige Schnittstellen weiterleiten.
DHCPACK	Filtern.	Wie bei DHCPOFFER, außerdem wird der DHCP-Snooping-Bindungsdatenbank ein Eintrag hinzugefügt.
DHCPNAK	Filtern.	Wie bei DHCPOFFER. Entfernen, wenn Eintrag vorhanden.

Pakettyp	Von nicht vertrauenswürdiger Eingangsschnittstelle eingehend	Von vertrauenswürdiger Eingangsschnittstelle eingehend
DHCPDECLINE	Überprüfen, ob in der Datenbank Informationen vorhanden sind. Wenn die Informationen vorhanden sind und nicht der Schnittstelle entsprechen, an der die Nachricht empfangen wurde, wird das Paket gefiltert. Anderenfalls wird das Paket nur an vertrauenswürdige Schnittstellen weitergeleitet und der Eintrag wird aus der Datenbank entfernt.	Nur an vertrauenswürdige Schnittstellen weiterleiten.
DHCPRELEASE	Wie bei DHCPDECLINE.	Wie bei DHCPDECLINE.
DHCPINFORM	Nur an vertrauenswürdige Schnittstellen weiterleiten.	Nur an vertrauenswürdige Schnittstellen weiterleiten.
DHCPLEASEQUERY	Gefiltert.	Weiterleiten.

DHCP-Snooping zusammen mit DHCP-Relais

Wenn DHCP-Snooping und DHCP-Relais global aktiviert sind und im VLAN des Clients DHCP-Snooping aktiviert ist, werden die in der DHCP-Snooping-Bindungsdatenbank enthaltenen DHCP-Snooping-Regeln angewendet. Für weitergeleitete Pakete wird die DHCP-Snooping-Bindungsdatenbank im VLAN des Clients und im VLAN des DHCP-Servers aktualisiert.

DHCP-Standardkonfiguration

Im Folgenden werden die Standardoptionen für DHCP-Snooping und DHCP-Relais beschrieben.

DHCP-Standardoptionen

Option	Standardzustand
DHCP-Snooping	**Aktiviert**
Einfügung von Option 82	**Nicht aktiviert**
Option 82-Passthrough	**Nicht aktiviert**
MAC-Adresse bestätigen	**Aktiviert**
DHCP-Snooping-Bindungsdatenbank sichern	**Nicht aktiviert**
DHCP-Relais	**Deaktiviert**

Konfigurieren des DHCP-Workflows

So konfigurieren Sie DHCP-Relais und DHCP-Snooping:

SCHRITT 1 Aktivieren Sie DHCP-Snooping und/oder DHCP-Relais auf der Seite **IP-Konfiguration > DHCP > Eigenschaften** oder **Sicherheit > DHCP-Snooping > Eigenschaften**.

SCHRITT 2 Definieren Sie auf der Seite **IP-Konfiguration > DHCP > Schnittstelleneinstellungen** die Schnittstellen, an denen DHCP-Snooping aktiviert ist.

SCHRITT 3 Konfigurieren Sie auf der Seite **IP-Konfiguration > DHCP > DHCP-Snooping-Schnittstelle** Schnittstellen als vertrauenswürdig oder nicht vertrauenswürdig.

SCHRITT 4 Optional. Fügen Sie auf der Seite **IP-Konfiguration > DHCP > DHCP-Snooping-Bindungsdatenbank** der DHCP-Snooping-Bindungsdatenbank Einträge hinzu.

DHCP-Snooping/-Relay

In diesem Abschnitt wird die Implementierung der Funktionen „DHCP-Relais“ und „DHCP-Snooping“ über die webbasierte Benutzeroberfläche beschrieben.

Eigenschaften

So konfigurieren Sie DHCP-Relais, DHCP-Snooping und Option 82:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv4-Verwaltung und -Schnittstellen** > **DHCP-Snooping/-Relais > Eigenschaften** oder auf **Sicherheit** > **DHCP-Snooping**.

Geben Sie Werte für die folgenden Felder ein:

- **Option 82**: Wählen Sie **Option 82** aus, um Option 82-Informationen in Pakete einzufügen.
- **DHCP-Relais**: Wählen Sie diese Option aus, um DHCP-Relais zu aktivieren.
- **DHCP-Snooping-Status**: Wählen Sie diese Option aus, um DHCP-Snooping zu aktivieren. Wenn DHCP-Snooping aktiviert ist, können Sie die folgenden Optionen aktivieren:
  - *Option 82-Passthrough*: Wählen Sie diese Option aus, um fremde Option 82-Informationen bei der Weiterleitung von Paketen beizubehalten.
  - *MAC-Adresse bestätigen*: Wählen Sie diese Option aus, um zu überprüfen, ob die Quell-MAC-Adresse des Schicht-2-Headers mit der Hardwareadresse des Clients übereinstimmt, die im DHCP-Header (Teil der Nutzlast) an für DHCP vertrauenswürdigen Ports angezeigt wird.
  - *Backup-Datenbank*: Wählen Sie diese Option aus, um die DHCP-Snooping-Bindungsdatenbank im Flashspeicher des Geräts zu sichern.
  - *Updateintervall für Backup-Datenbank*: Geben Sie ein, wie oft die DHCP-Snooping-Bindungsdatenbank gesichert werden soll (**wenn „Backup-Datenbank“ ausgewählt ist**).

SCHRITT 2 Klicken Sie auf **Übernehmen**. Die Einstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

SCHRITT 3 Zum Definieren eines DHCP-Servers klicken Sie auf **Hinzufügen**.

SCHRITT 4 Geben Sie die IP-Adresse des DHCP-Servers ein und klicken Sie auf **Übernehmen**. Die Einstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Schnittstelleneinstellungen

In Schicht 2 können DHCP-Relais und DHCP-Snooping nur in VLANs mit IP-Adressen aktiviert werden.

In Schicht 3 können DHCP-Relais und DHCP-Snooping an jeder Schnittstelle mit IP-Adresse und in VLANs mit oder ohne IP-Adresse aktiviert werden.

So aktivieren Sie DHCP-Snooping bzw. DHCP-Relais an bestimmten Schnittstellen:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv4-Verwaltung und -Schnittstellen** > **DHCP-Snooping/-Relais > Schnittstelleneinstellungen**.

SCHRITT 2 Klicken Sie zum Aktivieren von DHCP-Relais oder DHCP-Snooping an einer Schnittstelle auf **Hinzufügen**.

SCHRITT 3 Wählen Sie die Schnittstelle und die zu aktivierenden Funktionen aus: **DHCP-Relais** oder **DHCP-Snooping**.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Einstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Vertrauenswürdige DHCP-Snooping-Schnittstellen

Pakete von nicht vertrauenswürdigen Ports/LAGs werden anhand der DHCP-Snooping-Bindungsdatenbank überprüft (siehe Seite „DHCP-Snooping-Bindungsdatenbank“).

Schnittstellen sind standardmäßig vertrauenswürdig.

So deklarieren Sie eine Schnittstelle als nicht vertrauenswürdig:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv4-Verwaltung und -Schnittstellen** > **DHCP-Snooping/-Relais > Vertrauenswürdige DHCP-Snooping-Schnittstellen**.

SCHRITT 2 Wählen Sie die Schnittstelle aus und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Wählen Sie **Vertrauenswürdige Schnittstelle** (**Ja** oder **Nein**) aus.

SCHRITT 4 Klicken Sie auf **Übernehmen**, um die Einstellungen in der aktuellen Konfigurationsdatei zu speichern.

DHCP-Snooping-Bindungsdatenbank

Eine Beschreibung für das Hinzufügen dynamischer Einträge zur DHCP-Snooping-Bindungsdatenbank finden Sie unter **Aufbau der DHCP-Snooping-Bindungsdatenbank**.

Beachten Sie die folgenden Punkte bezüglich der Wartung der DHCP-Snooping-Bindungsdatenbank:

- Das Gerät aktualisiert die DHCP-Snooping-Bindungsdatenbank nicht, wenn eine Station zu einer anderen Schnittstelle wechselt.
- Wenn ein Port nicht aktiv ist, werden die Einträge für diesen Port nicht gelöscht.

- Wenn DHCP-Snooping für ein VLAN deaktiviert ist, werden die für dieses VLAN erfassten Bindungseinträge entfernt.
- Wenn die Datenbank voll ist, leitet DHCP-Snooping weiterhin Pakete weiter, jedoch werden keine neuen Einträge erstellt. Beachten Sie Folgendes: Wenn die Funktionen IP Source Guard und/oder ARP-Prüfung aktiv sind, können die Clients, die nicht in die DHCP-Snooping-Bindungsdatenbank geschrieben wurden, keine Verbindung mit dem Netzwerk herstellen.

So fügen Sie der DHCP-Snooping-Bindungsdatenbank Einträge hinzu:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration > IPv4-Verwaltung und -Schnittstellen** > **DHCP-Snooping/-Relais > DHCP-Snooping-Bindungsdatenbank**.

Um eine Teilmenge der Einträge in der DHCP-Snooping-Bindungsdatenbank anzuzeigen, geben Sie die entsprechenden Suchkriterien ein und klicken Sie auf **Los**.

Es werden die Felder in der DHCP-Snooping-Bindungsdatenbank angezeigt. Mit Ausnahme des Feldes **IP Source Guard** werden die folgenden Felder auf der Seite „Hinzufügen“ beschrieben:

- **Status:**
  - Aktiv **:** IP Source Guard ist auf dem Gerät aktiv.
  - Inaktiv **:** IP Source Guard ist auf dem Gerät nicht aktiv.
- **Grund:**
  - Kein Problem
  - Keine Ressource
  - Kein Snoop-VLAN
  - Vertrauenswürdiger Port

SCHRITT 2 Zum Hinzufügen eines Eintrags klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie Werte für die Felder ein:

- **VLAN-ID:** Das VLAN, in dem ein Paket erwartet wird.
- **MAC-Adresse**: Die MAC-Adresse des Pakets.
- **IP-Adresse**: Die IP-Adresse des Pakets.
- **Schnittstelle**: Die Einheit, der Slot oder die Schnittstelle, an der bzw. dem ein Paket erwartet wird.
- **Typ**: Folgende Feldwerte sind möglich:
  - *Dynamisch*: Der Eintrag hat eine begrenzte Lease-Dauer.
  - *Statisch*: Der Eintrag wurde statisch konfiguriert.

- **Lease-Dauer**: Wenn der Eintrag dynamisch ist, geben Sie ein, wie lange der Eintrag in der DHCP-Datenbank aktiv sein soll. Wenn keine Lease-Dauer vorhanden ist, aktivieren Sie die Option „Unbegrenzt“.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Einstellungen werden definiert und das Gerät wird aktualisiert.

DHCP-Server

Mithilfe der Funktion „DHCPv4-Server“ können Sie das Gerät als DHCPv4-Server konfigurieren. Ein DHCPv4-Server weist einem anderen Gerät (DHCP-Client) eine IPv4-Adresse und weitere Informationen zu.

Der DHCPv4-Server weist IPv4-Adressen aus einem benutzerdefinierten IPv4-Adressenpool zu.

Die folgenden Modi sind möglich:

- **Statische Zuweisung**: Die Hardwareadresse oder Client-ID eines Hosts wird manuell einer IP-Adresse zugeordnet. Verwenden Sie hierzu die Seite „Statische Hosts“.
- **Dynamische Zuweisung**: Ein Client erhält eine Leasing-IP-Adresse für eine angegebene Zeitspanne (auch unbegrenzt möglich). Wenn der DHCP-Client die zugewiesene IP-Adresse nicht erneuert, wird sie am Ende dieser Zeitspanne ungültig und der Client muss eine neue IP-Adresse anfordern. Verwenden Sie hierzu die Seite „Netzwerkpools“.

Abhängigkeiten zwischen Funktionen

- Es ist nicht möglich, einen DHCP-Server und einen DHCP-Client gleichzeitig auf demselben System zu konfigurieren, dies bedeutet: Wenn eine Schnittstelle für den DHCP-Client aktiviert wurde, ist es nicht möglich, den DHCP-Server global zu aktivieren.
- Wenn DHCPv4-Relais aktiviert ist, kann das Gerät nicht als DHCP-Server konfiguriert werden.

Standardeinstellungen und Konfigurationen

- Das Gerät ist standardmäßig nicht als DHCPv4-Server konfiguriert.
- Wenn das Gerät als DHCPv4-Server aktiviert wird, sind standardmäßig keine Netzwerkpools mit Adressen definiert.

Workflow zum Aktivieren der DHCP-Server-Funktion

So konfigurieren Sie das Gerät als DHCPv4-Server:

SCHRITT 1 Aktivieren Sie das Gerät auf der Seite „DHCP-Server > Eigenschaften“ als DHCP-Server.

SCHRITT 2 Wenn bestimmte IP-Adressen nicht zugewiesen werden sollen, geben Sie diese auf der Seite „Ausgeschlossene Adressen“ an.

SCHRITT 3 Definieren Sie auf der Seite „Netzwerkpools“ bis zu 8 Netzwerkpools mit IP-Adressen.

SCHRITT 4 Konfigurieren Sie auf der Seite „Statische Hosts“ Clients, denen eine permanente IP-Adresse zugewiesen werden soll.

SCHRITT 5 Konfigurieren Sie die erforderlichen DHCP-Optionen auf der Seite „DHCP-Optionen“. Auf diese Weise werden die Werte konfiguriert, die für jede relevante DHCP-Option ausgegeben werden sollen.

SCHRITT 6 Fügen Sie auf der Seite „Netzwerkpools“ eine IP-Schnittstelle im Bereich einer der konfigurierten DHCP-Pools hinzu. Das Gerät beantwortet DHCP-Anfragen von dieser IP-Schnittstelle. Beispiel: Wenn der Pool-Bereich 1.1.1.1 - 1.1.1.254 lautet, fügen Sie eine IP-Adresse zu diesem Bereich hinzu, wenn direkt verbundene Clients die IP-Adresse aus dem konfigurierten Pool empfangen sollen. Verwenden Sie dazu die Seite „IP-Konfiguration > IPv4-Schnittstelle“.

SCHRITT 7 Rufen Sie die Seite „Addressbindung“ auf, um die zugewiesenen IP-Adressen anzuzeigen. Auf dieser Seite können IP-Adressen gelöscht werden.

DHCPv4-Server

So konfigurieren Sie das Gerät als DHCPv4-Server:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv4-Verwaltung und -Schnittstellen** > **DHCP-Server > Eigenschaften**, um die Seite „Eigenschaften“ anzuzeigen.

SCHRITT 2 Wählen Sie **Aktivieren**, um das Gerät als DHCP-Server zu konfigurieren.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Das Gerät funktioniert sofort als DHCP-Server. Es kann jedoch erst Clients IP-Adressen zuweisen, wenn ein Pool erstellt wurde.

Netzwerkpool

Wenn das Gerät als DHCP-Server fungiert, muss mindestens ein Pool mit IP-Adressen definiert werden, aus dem das Gerät Clients IP-Adressen zuweisen kann. Jeder Netzwerkpool enthält einen Adressbereich, der zu einem bestimmten Subnetz gehört. Diese Adressen werden verschiedenen Clients in diesem Subnetz zugewiesen.

Wenn ein Client eine IP-Adresse anfordert, weist das Gerät als DHCP-Server wie folgt eine IP-Adresse zu:

- **Direkt angeschlossener Client**: Das Gerät weist eine Adresse aus dem Netzwerkpool zu, dessen Subnetz dem an der IP-Schnittstelle des Geräts konfigurierten Subnetz entspricht, über die die DHCP-Anforderung empfangen wurde.
- **Remote-Client**: Das Gerät weist eine IP-Adresse aus dem Netzwerkpool zu, dessen erstes direkt mit dem Client verbundenes Relais-Subnetz dem an einer der IP-Schnittstellen des Geräts konfigurierten Subnetz entspricht.
  - Wurde die Meldung direkt (d. h. nicht via DHCP-Relais) empfangen, dann ist der Pool ein lokaler Pool und gehört zu einem der IP-Subnetze, die für die eingehende Schicht-2-Schnittstelle definiert wurden. In diesem Fall stimmt die IP-Maske des Pools mit der IP-Maske der IP-Schnittstelle überein, und die niedrigsten und höchsten IP-Adressen des Pools gehören zum IP-Subnetz.
  - Wurde die Meldung via DHCP-Relais empfangen, dann gehört die verwendete Adresse zu dem IP-Subnetz, das durch die niedrigste IP-Adresse und die IP-Maske des Pools angegeben wird, und der Pool ist ein Remote-Pool.

Bis zu acht Netzwerkpools können definiert werden.

So erstellen Sie einen Pool mit IP-Adressen und definieren deren Lease-Dauer:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv4-Verwaltung und -Schnittstellen** > **DHCP-Server** > **Netzwerkpools**, um die Seite „Netzwerkpools“ anzuzeigen.

Die zuvor definierten Netzwerkpools werden angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, um einen neuen Netzwerkpool zu definieren. Beachten Sie, dass Sie entweder IP-Adresse und Maske des Subnetzes oder Maske sowie erste und letzte Adresse des Adresspools eingeben.

SCHRITT 3 Geben Sie Werte für die Felder ein:

- **Poolname**: Geben Sie den Poolnamen ein.
- **Subnetz-IP-Addresse**: Geben Sie die IP-Adresse des Subnetzes an, in dem sich der Netzwerkpool befindet.

- **Maske**: Geben Sie einen der folgenden Werte ein:
  - **Netzwerkmaske**: Aktivieren Sie das Kontrollkästchen und geben Sie die Netzwerkmaske des Pools ein.
  - **Präfixlänge**: Aktivieren Sie das Kontrollkästchen und geben Sie die Anzahl der Bits ein, aus denen das Adresspräfix besteht.
- **Adress-Pool-Anfang**: Geben Sie die erste IP-Adresse im Adressbereich des Netzwerkpools ein.
- **Adress-Pool-Ende**: Geben Sie die letzte IP-Adresse im Adressbereich des Netzwerkpools ein.
- **Lease-Dauer**: Geben Sie die Dauer ein, für die der DHCP-Client eine IP-Adresse aus diesem Pool nutzen kann. Sie können eine Lease-Dauer von bis zu 49.710 Tagen oder eine unbegrenzte Dauer konfigurieren.
  - **Unbegrenzt**: Die Lease-Dauer ist unbegrenzt.
  - **Tage**: Die Lease-Dauer ist in Tagen angegeben. Gültige Werte liegen im Bereich von 0 bis 49710.
  - **Stunden**: Die Anzahl der Stunden im Lease. Bevor ein Stundenwert hinzugefügt werden kann, muss ein Tageswert angegeben werden.
  - **Minuten**: Die Anzahl der Minuten im Lease. Bevor ein Minutenwert hinzugefügt werden kann, müssen ein Tages- und ein Stundenwert angegeben werden.
- **IP-Adresse Standardrouter (Option 3)**: Geben Sie die IP-Adresse des Standardrouters für den DHCP-Client ein.
- **IP-Adresse DNS-Server (Option 6)**: Wählen Sie einen der DNS-Server des Geräts aus (sofern bereits konfiguriert) oder wählen Sie **Sonstiges** und geben Sie die IP-Adresse des DNS-Servers ein, der für den DHCP-Client zur Verfügung steht.
- **Domänenname (Option 15)**: Geben Sie den Domänennamen für einen DHCP-Client ein.
- **NetBIOS-WINS-Server (Option 44):** Geben Sie den NetBIOS-WINS-Namensserver an, der einem DHCP-Client zur Verfügung steht.
- **NetBIOS-Knotentyp (Option 46)**: Wählen Sie aus, wie der NetBIOS-Name aufgelöst werden soll. Gültige Knotentypen:
  - *Hybrid* (H-Knoten): Eine Hybridkombination aus B- und P-Knoten wird verwendet. Wenn ein Computer für die Verwendung von H-Knoten konfiguriert ist, verwendet er grundsätzlich zuerst P-Knoten und weicht nur auf B-Knoten aus, wenn P-Knoten fehlschlägt. Dies ist die Standardeinstellung.
  - *Gemischt* (M-Knoten): Für die Registrierung und Auflösung von NetBIOS-Namen wird eine Kombination aus B- und P-Knoten verwendet. M-Knoten verwendet zuerst B-Knoten und anschließend P-Knoten, falls erforderlich. Die Verwendung von M-Knoten ist für größere Netzwerke in der Regel nicht empfehlenswert, da der bevorzugte Einsatz von Broadcasts (B-Knoten) zu erhöhtem Netzwerkverkehr führt.

- *Peer-to-Peer* (P-Knoten): Die Registrierung und Auflösung von Computernamen in IP-Adressen erfolgt durch Punkt-zu-Punkt-Kommunikation mit einem NetBIOS-Namensserver.
- *Broadcast* (B-Knoten): Die Registrierung und Auflösung von NetBIOS-Namen in IP-Adressen erfolgt mithilfe von IP-Broadcast-Nachrichten.

- **SNTP-Server-IP-Adresse (Option 4)**: Wählen Sie einen der SNTP-Servers des Geräts aus (sofern bereits konfiguriert) oder wählen Sie **Sonstiges** und geben Sie die IP-Adresse des Zeitservers für den DHCP-Client ein.
- **Dateiserver-IP-Adresse (siaddr)**: Geben Sie die IP-Adresse des TFTP/SCP-Servers ein, von dem die Konfigurationsdatei heruntergeladen wird.
- **Dateiserver-Hostname (sname/Option 66):** Geben Sie den Namen des TFTP/SCP-Servers ein.
- **Name der Konfigurationsdatei (file/Option 67):** Geben Sie den Namen der als Konfigurationsdatei verwendeten Datei ein.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Ausgeschlossene Adressen

Standardmäßig geht der DHCP-Server davon aus, dass alle Adressen in einem Pool Clients zugewiesen werden können. Einzelne IP-Adressen oder IP-Adressbereiche können jedoch ausgeschlossen werden. Diese Adressen werden aus allen DHCP-Pools ausgeschlossen.

So definieren Sie einen ausgeschlossenen Adressbereich:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv4-Verwaltung und -Schnittstellen** > **DHCP-Server** > **Ausgeschlossene Adressen**, um die Seite „Ausgeschlossene Adressen“ anzuzeigen.

Die zuvor definierten ausgeschlossenen IP-Adressen werden angezeigt.

SCHRITT 2 Um einen auszuschließenden IP-Adressbereich hinzuzufügen, klicken Sie auf **Hinzufügen** und geben Sie Werte in die folgenden Felder ein:

- **IP-Startadresse**: Erste IP-Adresse im ausgeschlossenen IP-Adressbereich.
- **IP-Endadresse**: Letzte IP-Adresse im ausgeschlossenen IP-Adressbereich.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Statische Hosts

Sie können bestimmten DHCP-Clients eine permanente IP-Adresse zuweisen, die sich nie ändert. Diese Clients werden als statische Hosts bezeichnet.

So weisen Sie einem bestimmten Client manuell eine permanente IP-Adresse zu:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv4-Verwaltung und -Schnittstellen** > **DHCP-Server** > **Statische Hosts**, um die Seite „Statische Hosts“ anzuzeigen.

Die statischen Hosts werden angezeigt.

SCHRITT 2 Um einen statischen Host hinzuzufügen, klicken Sie auf **Hinzufügen** und geben Sie Werte in die folgenden Felder ein:

- **IP-Adresse**: Geben Sie die IP-Adresse ein, die dem Host statisch zugewiesen wurde.
- **Hostname**: Geben Sie den Hostnamen ein. Dieser kann aus einer Symbolfolge und einer Ganzzahl bestehen.
- **Maske**: Geben Sie die Netzwerkmaske des statischen Hosts ein.
  - *Netzwerkmaske*: Aktivieren Sie das Kontrollkästchen und geben Sie die Netzwerkmaske des statischen Hosts ein.
  - *Präfixlänge*: Aktivieren Sie das Kontrollkästchen und geben Sie die Anzahl der Bits ein, aus denen das Adresspräfix besteht.
- **Kennungstyp**: Legen Sie fest, wie der statische Host identifiziert werden soll.
  - *Client-Identifikator*: Geben Sie eine eindeutige Kennung für den Client in hexadezimaler Schreibweise an. Beispiel: 01b60819681172.

  oder:
  - *MAC-Adresse*: Geben Sie die MAC-Adresse des Clients ein.
- **Clientname**: Geben Sie den Namen des statischen Hosts mithilfe eines ASCII-Standardzeichensatzes ein. Der Clientname darf nicht den Domänennamen enthalten.
- **IP-Adresse Standardrouter (Option 3)**: Geben Sie die IP-Adresse des Standardrouters für den statischen Host ein.
- **IP-Adresse DNS-Server (Option 6)**: Wählen Sie einen der DNS-Server des Geräts aus (sofern bereits konfiguriert) oder wählen Sie **Sonstiges** und geben Sie die IP-Adresse des DNS-Servers ein, der für den DHCP-Client zur Verfügung steht.
- **Domänenname (Option 15)**: Geben Sie den Domänennamen für den statischen Host ein.
- **NetBIOS-WINS-Server (Option 44):** Geben Sie den NetBIOS-WINS-Namensserver an, der dem statischen Host zur Verfügung steht.

- **NetBIOS-Knotentyp (Option 46)**: Wählen Sie aus, wie der NetBIOS-Name aufgelöst werden soll. Gültige Knotentypen:
  - *Hybrid* (H-Knoten): Eine Hybridkombination aus B- und P-Knoten wird verwendet. Wenn ein Computer für die Verwendung von H-Knoten konfiguriert ist, verwendet er grundsätzlich zuerst P-Knoten und weicht nur auf B-Knoten aus, wenn P-Knoten fehlschlägt. Dies ist die Standardeinstellung.
  - *Gemischt* (M-Knoten): Für die Registrierung und Auflösung von NetBIOS-Namen wird eine Kombination aus B- und P-Knoten verwendet. M-Knoten verwendet zuerst B-Knoten und anschließend P-Knoten, falls erforderlich. Die Verwendung von M-Knoten ist für größere Netzwerke in der Regel nicht empfehlenswert, da der bevorzugte Einsatz von Broadcasts (B-Knoten) zu erhöhtem Netzwerkverkehr führt.
  - *Peer-to-Peer* (P-Knoten): Die Registrierung und Auflösung von Computernamen in IP-Adressen erfolgt durch Punkt-zu-Punkt-Kommunikation mit einem NetBIOS-Namensserver.
  - *Broadcast* (B-Knoten): Die Registrierung und Auflösung von NetBIOS-Namen in IP-Adressen erfolgt mithilfe von IP-Broadcast-Nachrichten.
- **SNTP-Server-IP-Adresse (Option 4)**: Wählen Sie einen der SNTP-Servers des Geräts aus (sofern bereits konfiguriert) oder wählen Sie **Sonstiges** und geben Sie die IP-Adresse des Zeitservers für den DHCP-Client ein.
- **Dateiserver-IP-Adresse (siaddr)**: Geben Sie die IP-Adresse des TFTP/SCP-Servers ein, von dem die Konfigurationsdatei heruntergeladen wird.
- **Dateiserver-Hostname (sname/Option 66):** Geben Sie den Namen des TFTP/SCP-Servers ein.
- **Name der Konfigurationsdatei (file/Option 67):** Geben Sie den Namen der als Konfigurationsdatei verwendeten Datei ein.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

DHCP-Optionen

Wenn das Gerät als DHCP-Server agiert, können die DHCP-Optionen über die HEX-Option konfiguriert werden. Eine Beschreibung dieser Optionen finden Sie unter „RFC2131“.

Die Konfiguration dieser Optionen definiert, dass die Antwort an die DHCP-Clients gesendet wird, deren Pakete eine Anfrage für die konfigurierten DHCP-Optionen umfassen (über die Option 55).

Beispiel: Die DHCP-Option 66 wird mit dem Namen eines TFTP-Servers auf der Seite „DHCP-Optionen“ konfiguriert. Wenn ein Client-DHCP-Paket mit Option 66 eingeht, wird der TFTP-Server als Wert für Option 66 ausgegeben.

So konfigurieren Sie eine oder mehrere DHCP-Optionen:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv4-Management und -Schnittstellen** > **DHCP-Server** > **DHCP-Optionen**.

Daraufhin werden die zuvor konfigurierten DHCP-Optionen angezeigt.

SCHRITT 2 Um eine Option zu konfigurieren, die noch nicht konfiguriert wurde, geben Sie einen Wert in das folgende Feld ein:

- **DHCP-Server-Poolname ist gleich:** Wählen Sie einen der Pools mit Netzwerkadressen aus, die auf der Seite „Netzwerkpools“ definiert wurden.

SCHRITT 3 Klicken Sie auf **Hinzufügen**, und geben Sie Werte in die folgenden Felder ein:

- **Code**: Geben Sie den DHCP-Optionscode ein.
- **Typ**: Die Optionsschaltflächen für dieses Feld passen sich je nach Typ des Parameters für die DHCP-Option an. Wählen Sie einen der folgenden Codes aus, und geben Sie den Wert für die DHCP-Konfigurationsparameter ein:
  - *Hex*: Wählen Sie diese Option aus, wenn Sie den Hexadezimalwert des Parameters für die DHCP-Option eingeben möchten. Ein Hexadezimalwert kann anstelle jedes anderen Wertetyps eingegeben werden. So können Sie beispielsweise einen Hexadezimalwert einer IP-Adresse statt der IP-Adresse selbst eingeben.

    Der Hexadezimalwert wird nicht überprüft. Wenn Sie also einen Hexadezimalwert eingeben, der nicht korrekt ist, wird keine Fehlermeldung angezeigt, und der Client ist möglicherweise nicht in der Lage, das DHCP-Paket vom Server zu verarbeiten.
  - *IP*: Wählen Sie diese Option aus, wenn Sie eine IP-Adresse eingeben möchten, sollte dies für die ausgewählte DHCP-Option relevant sein.
  - *IP-Liste*: Geben Sie eine Liste der IP-Adressen, getrennt durch Kommas, ein.
  - *Ganzzahl*: Wählen Sie diese Option aus, wenn Sie eine Ganzzahl des ausgewählten Parameters für die DHCP-Option eingeben möchten.
  - *Boolescher Wert*: Wählen Sie diese Option aus, wenn es sich bei dem Parameter für die ausgewählte DHCP-Option um einen booleschen Wert handelt.
- **Boolescher Wert:** Wenn es sich bei dem Typ um einen booleschen Wert handelte, wählen Sie den Wert aus, der ausgegeben werden soll: **Wahr** oder **Falsch**.
- **Wert:** Wenn es sich bei dem Typ nicht um einen booleschen Wert handelt, geben Sie den Wert ein, der für diesen Code gesendet werden soll.
- **Beschreibung:** Geben Sie für Dokumentationszwecke eine Textbeschreibung ein.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Adressbindung

Auf der Seite „Adressbindung“ können Sie die vom Gerät zugewiesenen IP-Adressen und ihre zugehörigen MAC-Adressen anzeigen und entfernen.

So können Sie Adressbindungen anzeigen und/oder entfernen:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv4-Verwaltung und -Schnittstellen** > **DHCP-Server** > **Adressbindung**, um die Seite „Adressbindung“ anzuzeigen.

Die folgenden Felder für die Adressbindungen werden angezeigt:

- **IP-Adresse**: Die IP-Adressen der DHCP-Clients.
- **Adresstyp**: Gibt an, ob als Adresse des DHCP-Clients die MAC-Adresse oder ein Client-Identifikator verwendet wird.
- **MAC-Adresse/Client-Identifikator**: Eine eindeutige Kennung des Clients, angegeben entweder als MAC-Adresse oder in hexadezimaler Schreibweise (z. B. 01b60819681172).
- **Lease Expiration (Lease-Ablauf)**: Datum und Uhrzeit des Zeitpunkts, an dem die Lease der IP-Adresse abläuft, oder „Unbegrenzt“ (je nach Definition der Lease-Dauer).
- **Typ**: Die Art der Zuweisung der IP-Adresse zum Client. Folgende Optionen sind möglich:
  - *Statisch*: Die Hardwareadresse des Hosts wurde einer IP-Adresse zugeordnet.
  - *Dynamisch*: Die IP-Adresse wurde dynamisch vom Gerät bezogen und ist während einer bestimmten Zeitspanne für den Client gültig. Die IP-Adresse wird am Ende dieser Zeitspanne ungültig und der Client muss eine neue IP-Adresse anfordern.
- **Status**: Folgende Optionen sind möglich:
  - *Zugewiesen*: Die IP-Adresse wurde zugewiesen. Wenn ein statischer Host konfiguriert wird, wird dessen Status zugeordnet.
  - *Abgelehnt*: Die IP-Adresse wurde angeboten, jedoch nicht akzeptiert, daher wird sie nicht zugeordnet.
  - *Abgelaufen*: Die Lease der IP-Adresse ist abgelaufen.
  - *Vorab zugeordnet*: Ein Eintrag befindet zwischen dem Angebot und dem Zeitpunkt des Versands des DHCP ACK durch den Client in einem vorab zugeordneten Status. Anschließend erfolgt die Zuordnung.

SCHRITT 2 Klicken Sie auf **Löschen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

IPv6-Verwaltung und -Schnittstellen

Internetprotokoll Version 6 (IPv6) ist ein Vermittlungsschicht-Protokoll für paketvermittelte Internetzwerke. IPv6 wurde entwickelt, um IPv4, das zuvor vorwiegend bereitgestellte Internetprotokoll, zu ersetzen.

IPv6 bietet größere Flexibilität bei der Zuweisung von IP-Adressen, da die Adressgröße von 32 Bit auf 128 Bit erhöht wurde. IPv6-Adressen werden als acht Gruppen von vier Hexadezimalzeichen geschrieben, z. B. FE80:0000:0000:0000:0000:9C00:876A:130B. Die abgekürzte Form, in der eine Gruppe von Nullen ausgelassen und durch '::' ersetzt wird, ist ebenfalls zulässig, z. B. ::-FE80::9C00:876A:130B.

IPv6-Knoten erfordern einen intermediären Zuordnungsmechanismus, um mit anderen IPv6-Knoten über ein IPv4-Netzwerk kommunizieren zu können. Mithilfe dieses Mechanismus, der als Tunnel bezeichnet wird, können IPv6-Hosts IPv4-Services nutzen und isolierte IPv6-Hosts und -Netzwerke können einen IPv6-Knoten über die IPv4-Infrastruktur erreichen.

Beim Tunneling wird entweder ISATAP oder ein manueller Mechanismus verwendet (siehe **IPv6-Tunnel**). Beim Tunneling wird das IPv4-Netzwerk als virtueller lokaler IPv6-Link mit Zuordnungen von den einzelnen IPv4-Adressen zu einer Link Local-IPv6-Adresse behandelt.

Das Gerät erkennt IPv6-Frames durch den IPv6-Ethertype.

Statisches IPv6-Routing

Wie auch beim IPv4-Routing werden Frames, die nicht an die MAC-Adresse des Geräts, sondern an eine dem Gerät nicht bekannte IPv6-Adresse gerichtet sind, an ein Gerät für den nächsten Hop weitergeleitet. Dieses Gerät kann die Endstation des Ziels oder ein Router in der Nähe des Ziels sein. Der Weiterleitungsmechanismus umfasst die Neuerstellung eines L2-Frames mit der MAC-Adresse des Geräts für den nächsten Hop als Ziel-MAC-Adresse um das empfangene, im Wesentlichen unveränderte L3-Paket herum.

Das System erstellt mithilfe von Nachrichten für statisches Routing und Nachbarerkennung (ähnlich wie IPv4-ARP-Nachrichten) die entsprechenden Weiterleitungstabellen und Adressen für den nächsten Hop.

Eine Route bezeichnet den Pfad zwischen zwei Netzwerkgeräten. Vom Benutzer hinzugefügte Routing-Einträge sind statisch und werden vom System beibehalten und verwendet, bis sie vom Benutzer explizit entfernt werden. Sie werden nicht durch Routing-Protokolle verändert. Eine eventuell erforderliche Aktualisierung einer statischen Route muss explizit durch den Benutzer erfolgen. Der Benutzer ist für die Verhinderung von Routing-Schleifen im Netzwerk verantwortlich.

Typen statischer IPv6-Routen:

- Direkt angeschlossen: Das Ziel ist direkt mit einer Schnittstelle des Geräts verbunden, sodass das Paketziel (die Schnittstelle) als Adresse für den nächsten Hop verwendet wird.
- Rekursiv: Nur der nächste Hop ist angegeben. Die ausgehende Schnittstelle wird vom nächsten Hop abgeleitet.

Ebenso wird die MAC-Adresse der Geräte für den nächsten Hop (einschließlich direkt angeschlossener Endsysteme) mithilfe von Netzwerkerkennung automatisch abgeleitet. Der Benutzer kann dieses Verhalten jedoch außer Kraft setzen, indem er der Nachbartabelle manuell Einträge hinzufügt.

Globale IPv6-Konfiguration

So definieren Sie globale IPv6-Parameter und DHCPv6-Clienteinstellungen:

SCHRITT 1 Klicken Sie im Schicht-2-Systemmodus auf **Administration** > **Verwaltungsschnittstelle** > **Globale IPv6-Konfiguration**.

Klicken Sie im Schicht-3-Systemmodus auf **IP-Konfiguration** > **IPv6-Verwaltung und -Schnittstellen** > **Globale IPv6-Konfiguration**.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **IPv6-Routing** (nur Schicht-3-Systemmodus): Wählen Sie diese Option, um IPv6-Routing zu aktivieren. Wenn diese Option nicht aktiviert ist, fungiert das Gerät als Host (statt als Router) und kann zwar Verwaltungspakete empfangen, aber keine Pakete weiterleiten. Wenn das Routing aktiviert ist, kann das Gerät die IPv6-Pakete weiterleiten.
- **ICMPv6-Ratenbegrenzungsintervall**: Geben Sie ein, wie oft die ICMP-Fehlermeldungen generiert werden.
- **Größe des ICMPv6-Ratenbegrenzungs-Bucket**: Geben Sie ein, wie viele ICMP-Fehlermeldungen maximal pro Intervall vom Gerät gesendet werden können.
- **IPv6-Hop-Limit** (nur Schicht-3-Systemmodus): Geben Sie die maximale Anzahl zwischengeschalteter Router zwischen dem Gerät und dem endgültigen Ziel ein, die ein Paket passieren kann. Bei jeder Weiterleitung eines Pakets an einen weiteren Router wird das Hop-Limit reduziert. Wenn das Hop-Limit den Wert null erreicht, wird das Paket verworfen. Dadurch wird eine endlose Weiterleitung von Paketen verhindert.

DHCPv6-Client-Einstellungen

- **Unique Identifier (DUID) Format**: Dies ist die Kennung des DHCP-Clients, anhand derer der DHCP-Server den Client ermittelt. Folgende Formate sind möglich:
  - *Link-Layer* (Standard). Wenn Sie diese Option wählen, wird die MAC-Adresse des Geräts verwendet.
  - *Enterprise-Nummer*: Wenn Sie diese Option wählen, müssen Sie Werte in die folgenden Felder eingeben.
- **Enterprise-Nummer**: Die bei der IANA registrierte private Enterprise-Nummer des Anbieters.
- **Kennung**: Die vom Anbieter definierte Hexadezimalzeichenfolge (bis zu 64 Hexadezimalzeichen). Wenn die Anzahl der Zeichen ungerade ist, wird an das Ende eine Null angehängt. Dabei kann jedes zweite Hexadezimalzeichen durch einen Punkt oder einen Doppelpunkt abgetrennt werden.

- **DHCPv6 Unique Identifier (DUID)**: Die ausgewählte Kennung.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die globalen IPv6-Parameter und DHCPv6-Clienteinstellungen werden aktualisiert.

IPv6-Schnittstelle

Eine IPv6-Schnittstelle kann für einen Port, eine LAG, ein VLAN, eine Loopback-Schnittstelle oder einen Tunnel konfiguriert werden.

Anders als andere Schnittstellentypen wird eine Tunnelschnittstelle zunächst auf der Seite „IPv6-Tunnel“ erstellt und die IPv6-Schnittstelle dann für den Tunnel auf dieser Seite konfiguriert.

So definieren Sie eine IPv6-Schnittstelle:

SCHRITT 1 Klicken Sie im Schicht-2-Systemmodus auf **Administration** > **Verwaltungsschnittstelle** > **IPv6-Schnittstellen**.
Klicken Sie im Schicht-3-Systemmodus auf **IP-Konfiguration** > **IPv6-Verwaltung und -Schnittstellen** > **IPv6-Schnittstellen**.

SCHRITT 2 Geben Sie die Parameter (in Schicht 3) ein.

- **IPv6-Link Local-Standardzone** (nur Schicht 3): Wählen Sie diese Option, wenn eine Standardzone definiert werden soll. Dabei handelt es sich um eine Schnittstelle, über die Link Local-Pakete weitergeleitet werden, die ohne angegebene Schnittstelle oder mit der Standardzone 0 empfangen werden.
- **IIPv6-Link Local-Standardzone – Schnittstelle** (nur Schicht 3): Wählen Sie eine Schnittstelle, die als Standardzone verwendet werden soll. Dies kann ein zuvor definierter Tunnel oder eine andere Schnittstelle sein.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um die Standardzone zu konfigurieren.

SCHRITT 4 Klicken Sie auf **Hinzufügen**, um eine neue Schnittstelle hinzuzufügen, für die IPv6 aktiviert ist.

SCHRITT 5 Geben Sie Werte für das/die Feld/er ein:

- **IPv6-Schnittstelle**: Wählen Sie einen Port, eine LAG, eine Loopback-Schnittstelle oder ein VLAN für die IPv6-Adresse.

SCHRITT 6 Um die Schnittstelle als DHCPv6-Client zu konfigurieren, sodass sie Informationen vom DHCPv6-Server empfangen kann (z. B. SNTP-Konfigurations- und DNS-Informationen), geben Sie Werte in die folgenden Felder für den **DHCPv6-Client** ein:

- **Statuslos**: Wählen Sie diese Option, um die Schnittstelle als statuslosen DHCPv6-Client zu aktivieren. Damit aktivieren Sie den Empfang der Konfigurationsdaten von einem DHCP-Server.

- **Mindest-Informationsaktualisierungszeit**: Dieser Wert ist die Untergrenze für die Aktualisierungsrate. Wenn der Server eine Option für die Aktualisierung sendet, die unter diesem Wert liegt, wird stattdessen dieser Wert verwendet. Wählen Sie entweder **Unbegrenzt** (Aktualisierung findet nur statt, wenn der Server diese Option sendet) oder **Benutzerdefiniert**, um einen Wert festzulegen.
- **Informationsaktualisierungszeit**: Dieser Wert gibt an, wie oft das Gerät vom DHCPv6-Server empfangene Informationen aktualisiert. Wenn diese Option nicht vom Server empfangen wird, wird der hier eingegebene Wert verwendet. Wählen Sie entweder **Unbegrenzt** (Aktualisierung findet nur statt, wenn der Server diese Option sendet) oder **Benutzerdefiniert**, um einen Wert festzulegen.

SCHRITT 7 Um weitere IPv6-Parameter zu konfigurieren, geben Sie Werte in die folgenden Felder ein:

- **Automatische IPv6-Adresskonfiguration**: Wählen Sie diese Option, um die automatische Adresskonfiguration durch von Nachbarn gesendete Routerankündigungen zu aktivieren.

HINWEIS Das Gerät unterstützt die statusbehaftete automatische Adresskonfiguration über einen DHCPv6-Server nicht.

- **Anzahl der DAD-Versuche**: Geben Sie die Anzahl aufeinanderfolgender Nachbaranfrage-Benachrichtigungen ein, die während der Durchführung der Duplicate Address Detection (DAD) für die Unicast-IPv6-Adressen der Schnittstelle gesendet werden sollen. Mit DAD wird die Eindeutigkeit einer neuen Unicast-IPv6-Adresse überprüft, bevor diese zugewiesen wird. Neue Adressen stehen während der DAD-Prüfung unter Vorbehalt. Durch Eingabe von **0** in dieses Feld wird die DAD-Verarbeitung für die angegebene Schnittstelle deaktiviert. Durch Eingabe von **1** in dieses Feld wird eine einzelne Übertragung ohne Folgeübertragungen angegeben.
- **ICMPv6-Nachrichten senden**: Zum Aktivieren von Benachrichtigungen über nicht erreichbare Ziele.
- **MLD-Version** (nur Schicht-3-Systemmodus): IPv6-MLD-Version.
- **IPv6-Umleitungen** (nur Schicht 3): Wählen Sie diese Option, um ICMP-IPv6-Benachrichtigungen über Umleitungen zu aktivieren. Diese Nachrichten informieren andere Geräte darüber, Datenverkehr statt an dieses an ein anderes Gerät zu senden.

SCHRITT 8 Klicken Sie auf **Übernehmen**, um die IPv6-Verarbeitung für die ausgewählte Schnittstelle zu aktivieren. Bei regulären IPv6-Schnittstellen werden die folgenden Adressen automatisch konfiguriert:

- Link Local-Adresse unter Verwendung einer Schnittstellen-ID im EUI-64-Format, die auf der MAC-Adresse des Geräts basiert.
- Alle Link Local-Multicast-Adressen (FF02::1) des Knotens.
- Angefragte Knoten-Multicast-Adresse (Format FF02::1:FFXX:XXXX).

SCHRITT 9 Klicken Sie auf **IPv6-Adresstabelle**, um der Schnittstelle ggf. manuell IPv6-Adressen hinzuzufügen. Diese Seite wird im Abschnitt **Definieren von IPv6-Adressen** beschrieben.

SCHRITT 10 Um einen Tunnel hinzuzufügen, wählen Sie in der IPv6-Tunneltabelle eine Schnittstelle (die auf der Seite „IPv6-Schnittstellen“ als Tunnel definiert wurde) und klicken auf **IPv6-Tunneltabelle**. Weitere Informationen hierzu finden Sie unter **IPv6-Tunnel**.

SCHRITT 11 Klicken Sie auf die Schaltfläche **Neustart**, um die vom DHCPv6-Server empfangenen statuslosen Informationen zu aktualisieren.

DHCPv6-Clientdetails

Durch Klicken auf die Schaltfläche **Details** werden die über die Schnittstelle von einem DHCPv6-Server empfangenen Informationen angezeigt.

Sie ist aktiv, wenn die ausgewählte Schnittstelle als statusloser DHCPv6-Client definiert ist.

Durch Klicken auf die Schaltfläche werden die folgenden Felder für die vom DHCP-Server empfangenen Informationen angezeigt:

- **DHCPv6-Betriebsmodus**: In diesem Feld wird „Aktiviert“ angezeigt, wenn die folgenden Bedingungen erfüllt sind:
  - Die Schnittstelle ist hochgefahren.
  - IPv6 ist aktiviert.
  - Statusloser DHCPv6-Client ist aktiviert.
- **Statusloser Service**: Gibt an, ob der Client als statuslos definiert ist (d. h. Konfigurationsinformationen von einem DHCP-Server empfängt).
- **DHCPv6-Serveradresse**: Adresse des DHCPv6-Servers.
- **DHCPv6-Server-DUID**: Eindeutige Kennung des DHCPv6-Servers.
- **DHCPv6-Serverpriorität**: Priorität des DHCPv6-Servers.
- **Mindest-Informationsaktualisierungszeit**: Siehe oben.
- **Informationsaktualisierungszeit**: Siehe oben.
- **Empfangene Informationsaktualisierungszeit**: Vom DHCPv6-Server empfangene Aktualisierungsrate.
- **Verbleibende Informationsaktualisierungszeit**: Verbleibende Zeit bis zur nächsten Aktualisierung.
- **DNS-Server**: Vom DHCPv6-Server empfangene Liste der DNS-Server.

- **DNS-Domänen-Suchliste**: Vom DHCPv6-Server empfangene Liste der Domänen.
- **SNTP-Server**: Vom DHCPv6-Server empfangene Liste der SNTP-Server.
- **POSIX-Zeitzonen-String**: Vom DHCPv6-Server empfangene Zeitzone.
- **Konfigurationsserver**: Vom DHCPv6-Server empfangener Server mit der Konfigurationsdatei.
- **Name des Konfigurationspfads**: Pfad zur Konfigurationsdatei auf dem vom DHCPv6-Server empfangenen Konfigurationsserver.

IPv6-Tunnel

Tunnel ermöglichen die Übertragung von IPv6-Paketen über IPv4-Netzwerke. Jeder Tunnel hat eine Quell-IPv4-Adresse und, sofern es sich um einen manuellen Tunnel handelt, auch eine Ziel-IPv4-Adresse. Das IPv6-Paket wird zwischen diesen Adressen gekapselt.

HINWEIS Nur die IPv6-Verwaltungsschnittstelle kann getunnelt werden. Definieren Sie für die Erstellung eines IPv6-Tunnels auf der Seite „IPv6-Schnittstellen“ zunächst eine IPv6-Schnittstelle, und setzen Sie die Konfiguration des Tunnels dann auf der Seite „IPv6-Tunnel“ fort.

Tunneltypen

Auf dem Gerät können die folgenden Tunneltypen konfiguriert werden:

- **ISATAP-Tunnel**

  Beim ISATAP-Tunnel (Intra-Site Automatic Tunnel Addressing Protocol) handelt es sich um einen Punkt-zu-Mehrpunkt-Tunnel. Die Quelladresse ist die IPv4-Adresse (oder eine der IPv4-Adressen) des Geräts.

  Beim Konfigurieren eines ISATAP-Tunnels wird die Ziel-IPv4-Adresse vom Router bereitgestellt. Beachten Sie Folgendes:

  - Der ISATAP-Schnittstelle wird eine IPv6-Link Local-Adresse zugewiesen. Der Schnittstelle wird die initiale IP-Adresse zugewiesen, dann wird die Schnittstelle aktiviert.
  - Wenn eine ISATAP-Schnittstelle aktiv ist, wird die IPv4-Adresse des ISATAP-Routers über DNS unter Verwendung einer ISATAP-zu-IPv4-Zuordnung aufgelöst. Wenn der ISATAP-DNS-Datensatz nicht aufgelöst wird, wird in der Hostzuordnungstabelle nach einer Zuordnung des ISATAP-Host-Namens zu einer Adresse gesucht.
  - Wenn die IPv4-Adresse des ISATAP-Routers nicht über das DNS-Verfahren aufgelöst werden kann, bleibt die ISATAP-IP-Schnittstelle aktiv. Das System hat keinen Standardrouter für ISATAP-Datenverkehr, bis das DNS-Verfahren aufgelöst ist.

- **Manueller Tunnel**

  Hierbei handelt es sich um eine Punkt-zu-Punkt-Definition. Beim Erstellen eines manuellen Tunnels müssen Sie sowohl die Quell-IP-Adresse (eine der IP-Adressen des Geräts) als auch die Ziel-IPv4-Adresse eingeben.

- **6to4-Tunnel**

  6to4 ist ein automatischer Tunneling-Mechanismus, bei dem das zugrunde liegende IPv4-Netzwerk als Sicherungsschicht für IPv6 ohne Broadcast-Funktion, aber mit Mehrfachzugriff genutzt wird. Auf jedem Gerät wird maximal ein 6to4-Tunnel unterstützt.

  Der 6to4-Tunnel wird nur dann unterstützt, wenn die IPv6-Weiterleitung unterstützt wird.

  IPv6-Multicast wird für die 6to4-Tunnelschnittstelle nicht unterstützt.

  Auf dem 6to4-Tunnel erstellt der Switch automatisch das On-Link-Präfix „2002::/16“. Die angeschlossene Route 2002::/16 über den Tunnel wird infolge der Erstellung des On-Link-Präfixes zur Routing-Tabelle hinzugefügt.

  Wird der Tunnel vom 6to4- in einen anderen Modus umgestellt, dann werden das On-Link-Präfix und die angeschlossenen Routen entfernt.

  Handelt es sich bei der zum nächsten Hop ausgehenden Schnittstelle um den 6to4-Tunnel, dann wird die IPv4-Adresse des nächsten Hops, sofern sie global ist, dem Präfix 2002:WWXX:YYZZ::/48 der IPv6-Adresse des nächsten IPv6-Hops entnommen; beim Adresstyp „Link Local“ hingegen wird sie den letzten 32 Bits der Schnittstellenkennung der IPv6-Adresse des nächsten IPv6-Hops entnommen.

Bis zu 16 Tunnel (davon ein ISATAP-Tunnel) können definiert werden.

Konfigurieren von Tunneln

HINWEIS Nach dem Konfigurieren eines Tunnels müssen Sie auf der Seite „IPv6-Schnittstellen“ eine IPv6-Schnittstelle konfigurieren.

So konfigurieren Sie einen IPv6-Tunnel:

SCHRITT 1 Klicken Sie im Schicht-2-Systemmodus auf **Administration > Verwaltungsschnittstelle > IPv6-Tunnel**.

Der Schicht-2-Modus ist auf Sx500- und SG500X-Geräten nur im Stack-Modus „Hybrid“ verfügbar.

SCHRITT 2 Klicken Sie im Schicht-3-Systemmodus auf **IP-Konfiguration** > **IPv6-Verwaltung und -Schnittstellen** > **IPv6-Tunnel**.

SCHRITT 3 Geben Sie die **ISATAP-Parameter** ein.

- **Anfrageintervall**: Die Anzahl an Sekunden zwischen ISATAP-Router-Anfragebenachrichtigungen, wenn kein aktiver ISATAP-Router erkannt wird. Das Intervall kann den Standardwert oder einen benutzerdefinierten Wert haben.
- **Robustheit**: Wird verwendet, um das Intervall für die Router-Anfragen zu berechnen. Je größer die Zahl, desto häufiger die Abfragen.

  HINWEIS Der ISATAP-Tunnel ist nicht in Betrieb, wenn die zugrunde liegende IPv4-Schnittstelle nicht in Betrieb ist.

SCHRITT 4 Klicken Sie auf **Übernehmen**, um die ISATAP-Parameter in der aktuellen Konfigurationsdatei zu speichern.

SCHRITT 5 Um einen Tunnel hinzuzufügen, wählen Sie in der IPv6-Tunneltabelle eine Schnittstelle (die auf der Seite „IPv6-Schnittstellen“ als Tunnel definiert wurde) und klicken auf **Hinzufügen**.

SCHRITT 6 Geben Sie Werte für die folgenden Felder ein:

- **Tunnelname**: Wählen Sie eine Tunnelnummer aus.
- **Tunneltyp**: Zeigt die Tunneltypen an: **Manuell, ISATAP** und **6to4**.
- **Tunnelstatus**: Wählen Sie diese Option, um den Tunnel zu aktivieren. Wird der Tunnel später abgebaut, dann wird dies in diesem Feld angezeigt.
- **Leitungsstatus SNMP-Traps**: Wählen Sie diese Option aus, um die Generierung eines Traps zu aktivieren, wenn der Verbindungsstatus eines Ports geändert wird. Sollten Sie nicht daran interessiert sein, solche Traps auf spezifischen Ports zu empfangen (z. B. benötigt ISP Traps nur auf jenen Ports, die mit dessen Infrastruktur verbunden sind und benötigt keine Traps für Ports, die mit der Ausrüstung des Benutzers verbunden sind), können Sie diese Funktion deaktivieren.
- **Quelle**: Legen Sie die lokale (Quell-)IPv4-Adresse einer Tunnelschnittstelle fest. Die IPv4-Adresse der ausgewählten IPv4-Schnittstelle wird verwendet, um einen Teil der IPv6-Adresse über die ISATAP-Tunnelschnittstelle zu bilden. Die IPv6-Adresse hat ein 64-Bit-Netzwerkpräfix der Form fe80:, wobei der Rest der 64 Bit durch Aneinanderhängen von 0000:5EFE und der IPv4-Adresse gebildet wird.
  - *Automatisch*: Die niedrigste IPv4-Adresse aller konfigurierten IPv4-Schnittstellen wird automatisch als Quelladresse für über die Tunnelschnittstelle gesendete Pakete ausgewählt.
  - *IPv4-Adresse*: Gibt die IPv4-Adresse an, die als Quelladresse für über die Tunnelschnittstelle gesendete Pakete verwendet werden soll. Die lokale Adresse der Tunnelschnittstelle wird nicht geändert, wenn die IPv4-Adresse auf eine andere Schnittstelle übertragen wird.

    HINWEIS Wenn die IPv4-Adresse geändert wird, wird auch die lokale Adresse der Tunnelschnittstelle geändert.
  - *Schnittstelle*: Wählen Sie die Schnittstelle, deren IPv4-Adresse als Quelladresse des Tunnels verwendet werden soll.

Wenn diese Schnittstelle mehrere IPv4-Adressen hat, wird die niedrigste IPv4-Adresse als Quelladresse verwendet. Wenn die niedrigste IPv4-Adresse von der Schnittstelle entfernt wird (vollständig entfernt oder auf eine andere Schnittstelle übertragen), wird die nächst höhere IPv4-Adresse als lokale IPv4-Adresse verwendet.

- **Ziel** (nur manuelle Tunnel): Wählen Sie eine der folgenden Optionen, um die Zieladresse des Tunnels anzugeben:
  - *Hostname*: DNS-Name des Remote-Hosts.
  - *IPv4-Adresse*: IPv4-Adresse des Remote-Hosts.
- **ISATAP-Router-Name** (nur ISATAP-Tunnel): Wählen Sie eine der folgenden Optionen, um eine globale Zeichenfolge zu konfigurieren, die einen Domänennamen eines bestimmten automatischen Tunnel-Routers repräsentiert.
  - *Standard verwenden*: Dies ist immer „ISATAP“.
  - *Benutzerdefiniert*: Geben Sie den Domänennamen des Routers ein.

SCHRITT 7 Klicken Sie auf **Übernehmen**. Der Tunnel wird in der aktuellen Konfigurationsdatei gespeichert.

HINWEIS Zum Abbauen eines Tunnels klicken Sie auf **Bearbeiten** und wählen den „Tunnelstatus“ ab.

Definieren von IPv6-Adressen

So weisen Sie einer IPv6-Schnittstelle eine IPv6-Adresse zu:

SCHRITT 1 Klicken Sie im Schicht-2-Systemmodus auf **Administration** > **Verwaltungsschnittstelle** > **IPv6-Tunnel**.
Klicken Sie im Schicht-3-Systemmodus auf **IP-Konfiguration** > **IPv6-Verwaltung und -Schnittstellen** > **IPv6-Adressen**.

SCHRITT 2 Wählen Sie zum Filtern der Tabelle einen Schnittstellennamen aus, und klicken Sie auf **Los**. Die Schnittstelle wird in der IPv6-Adresstabelle angezeigt.

SCHRITT 3 Klicken Sie auf **Hinzufügen**.

SCHRITT 4 Geben Sie Werte für die Felder ein.

- **IPv6-Schnittstelle**: Zeigt die Schnittstelle an, für die die IPv6-Adresse definiert werden soll. Wenn ein * angezeigt wird, bedeutet dies, dass die IPv6-Schnittstelle nicht aktiviert ist, aber konfiguriert wurde.

- **IPv6-Adresstyp**: Wählen Sie den Typ der hinzuzufügenden IPv6-Adresse.
  - *Link Local*: Eine IPv6-Adresse, die Hosts mit einer einzigen Netzwerkverbindung eindeutig kennzeichnet. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
  - *Global*: Eine IPv6-Adresse, bei der es sich um einen globalen Unicast-IPv6-Typ handelt, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.
  - *Anycast*: Die IPv6-Adresse ist eine Anycast-Adresse. Dabei handelt es sich um eine Adresse, die einer Gruppe von Schnittstellen zugewiesen ist, die in der Regel zu verschiedenen Knoten gehören. An eine Anycast-Adresse gesendete Pakete werden an die gemäß verwendeter Routingprotokolle nächstgelegene Schnittstelle übermittelt, die durch die Anycast-Adresse identifiziert wird.

  HINWEIS Anycast kann nicht verwendet werden, wenn die IPv6-Adresse zu einer ISATAP-Schnittstelle gehört.
- **IPv6-Adresse**: Im Schicht-2-Systemmodus unterstützt das Gerät genau eine IPv6-Schnittstelle. Zusätzlich zu den standardmäßigen Link Local- und Multicast-Adressen fügt das Gerät der Schnittstelle automatisch globale Adressen hinzu, die auf den empfangenen Router-Ankündigungen basieren. Das Gerät unterstützt bis zu 128 Adressen an der Schnittstelle. Alle Adressen müssen gültige IPv6-Adressen sein, die im Hexadezimalformat unter Verwendung von durch Doppelpunkte getrennten 16-Bit-Werten angegeben werden.

  Die folgenden Adresstypen können verschiedenen Tunneltypen hinzugefügt werden:
  - Manuellen Tunneln: Globale oder Anycast-Adresse
  - ISATAP-Tunneln: Globale Adresse mit EUI-6
  - 6to4-Tunneln: Keine
- **Präfixlänge**: Die Länge des globalen IPv6-Präfixes als Wert von 0 bis 128, das die Anzahl der zusammenhängenden Bits höherer Ordnung der Adresse angibt, die das Präfix (den Netzwerkteil der Adresse) bilden.
- **EUI-64**: Der EUI-64-Parameter wird verwendet, um den Schnittstellen-ID-Anteil der globalen IPv6-Adresse unter Verwendung des EUI-Formats basierend auf der MAC-Adresse eines Geräts zu identifizieren.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

IPv6-Router-Konfiguration

In den folgenden Abschnitten wird die Konfiguration von IPv6-Routern beschrieben.

Routerankündigung

IPv6-Router können ihre Präfixe Nachbargeräten gegenüber ankündigen. Diese Funktion kann für jede Schnittstelle wie folgt aktiviert oder unterdrückt werden:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv6-Verwaltung und -Schnittstellen** > **IPv6-Router-Konfiguration > Routerankündigung**.

SCHRITT 2 Um eine in der Routerankündigungstabelle aufgeführte Schnittstelle zu konfigurieren, wählen Sie sie aus und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **Routerankündigung unterdrücken**: Wählen Sie **Ja**, um IPv6-Routerankündigungen an der Schnittstelle zu unterdrücken. Wenn diese Funktion nicht unterdrückt wird, geben Sie Werte in die folgenden Felder ein.
- **Routerpriorität**: Wählen Sie **Niedrig**, **Mittel** oder **Hoch** als Priorität für den Router. Routerankündigungsnachrichten werden mit der in diesem Feld konfigurierten Priorität gesendet. Wenn keine Priorität konfiguriert wird, werden sie mit mittlerer Priorität gesendet.

Die Angabe einer Priorität für einen Router kann beispielsweise nützlich sein, wenn zwei Router in einer Verbindung gleichwertiges Routing zu unterschiedlichen Kosten bieten und Hosts gemäß einer Richtlinie einen der beiden Router bevorzugen sollen.

- **Option Bekanntgabeintervall einschließen**: Wählen Sie diese Option, wenn vom System eine Ankündigungsoption verwendet werden soll. Diese Option informiert mobile Knoten über das Intervall, in dem Routerankündigungen gesendet werden. Diese Informationen können vom Knoten für den Algorithmus zur Bewegungserkennung verwendet werden.
- **Hop-Limit**: Dies ist der Wert, der vom Router angekündigt wird. Wenn dieser Wert nicht null ist, wird er vom Host als Hop-Limit verwendet.
- **Flag für verwaltete Adresskonfiguration**: Wählen Sie dieses Flag, wenn angeschlossene Hosts mithilfe der statusbehafteten automatischen Konfiguration Adressen beziehen sollen. Hosts können gleichzeitig statusbehaftete und statuslose automatische Konfiguration verwenden.
- **Flag für sonstige statusfreie Konfiguration**: Wählen Sie dieses Flag, wenn angeschlossene Hosts mithilfe der statusbehafteten automatischen Konfiguration sonstige Informationen (außer Adressen) beziehen sollen.

HINWEIS Wenn das Flag für verwaltete Adresskonfiguration gesetzt ist, können angeschlossene Hosts sonstige Informationen (außer Adressen) unabhängig von der Einstellung dieses Flags mithilfe der statusbehafteten automatischen Konfiguration beziehen.

- **Neuübertragungsintervall für Nachbaranfragen**: Legen Sie das Intervall zwischen Neuübertragungen von Anfragenachrichten an einen Nachbarn beim Auflösen der Adresse oder beim Prüfen der Erreichbarkeit eines Nachbarn fest.
- **Maximales Routerankündigungsintervall**: Geben Sie an, wie viel Zeit zwischen Routerankündigungen maximal verstreichen darf.

Das Intervall zwischen Übertragungen darf maximal der Gültigkeitsdauer der IPv6-Routerankündigungen entsprechen, wenn der Router über diesen Befehl als Standardrouter konfiguriert wird. Um die Synchronisierung mit anderen IPv6-Knoten zu verhindern, wird als tatsächlich verwendetes Intervall ein zufälliger Wert zwischen Mindest- und Höchstwert ausgewählt.

- **Minimales Routerankündigungsintervall**: Geben Sie an, wie viel Zeit zwischen Routerankündigungen mindestens verstreichen muss (**Benutzerdefiniert**) oder wählen Sie **Standard verwenden**, um den Systemstandardwert zu verwenden.

  HINWEIS Das minimale Routerankündigungsintervall darf maximal 75 % des maximalen Routerankündigungsintervalls und muss mindestens 3 Sekunden betragen.

- **Gültigkeitsdauer der Routerankündigung**: Geben Sie den verbleibenden Zeitraum in Sekunden an, in dem dieser Router weiterhin als Standardrouter verfügbar ist. Der Wert null gibt an, dass er nicht mehr als Standardrouter verfügbar ist.
- **Erreichbare Zeit**: Geben Sie den Zeitraum in Sekunden an, in dem ein Remote-IPv6-Knoten als erreichbar gilt (**Benutzerdefiniert**) oder wählen Sie **Standard verwenden**, um den Systemstandardwert zu verwenden.

SCHRITT 4 Klicken Sie auf **Übernehmen**, um die Konfiguration in der aktuellen Konfigurationsdatei zu speichern.

IPv6-Präfixe

So definieren Sie Präfixe, die an den Schnittstellen des Geräts angekündigt werden sollen:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv6-Verwaltung und -Schnittstellen** > **IPv6-Router-Konfiguration > IPv6-Präfixe**.

SCHRITT 2 Aktivieren Sie bei Bedarf das Feld **Filter** und klicken Sie auf **Los**. Die Gruppe der Schnittstellen, die dem Filter entsprechen, wird angezeigt.

SCHRITT 3 Klicken Sie zum Hinzufügen einer Schnittstelle auf **Hinzufügen**.

SCHRITT 4 Wählen Sie die IPv6-Schnittstelle aus, für die ein Präfix hinzugefügt werden soll.

SCHRITT 5 Geben Sie Werte für die folgenden Felder ein:

- **Präfixadresse**: Das IPv6-Netzwerk. Dieses Argument muss gemäß RFC 4293 im Hexadezimalformat mit durch Doppelpunkte getrennten 16-Bit-Werten angegeben werden.
- **Präfixlänge**: Länge des IPv6-Präfixes. Die Präfixlänge ist ein Dezimalwert, der die Anzahl der zusammenhängenden höherwertigen Bits der Adresse angibt (den Netzwerkteil der Adresse). Diesem Dezimalwert muss ein Schrägstrich vorangestellt werden.
- **Präfixankündigung**: Wählen Sie diese Option, wenn dieses Präfix angekündigt werden soll.
- **Gültige Gültigkeitsdauer**: Verbleibender Zeitraum in Sekunden, in dem dieses Präfix weiterhin gültig ist. Eine aus einem nicht mehr gültigen Präfix generierte Adresse darf nicht als Quell- oder Zieladresse eines Pakets verwendet werden.
  - *Unbegrenzt*: Wählen Sie diese Option, um für das Feld den Wert 4.294.967.295 (entspricht unendlich) zu verwenden.
  - *Benutzerdefiniert*: Geben Sie einen Wert ein.
- **Bevorzugte Gültigkeitsdauer**: Verbleibender Zeitraum in Sekunden, in dem dieses Präfix weiterhin bevorzugt verwendet wird. Nach Ablauf dieses Zeitraums darf das Präfix nicht mehr als Quelladresse in der Kommunikation verwendet werden. An dieser Schnittstelle empfangene Pakete werden jedoch erwartungsgemäß verarbeitet. Die bevorzugte Gültigkeitsdauer darf die Gültigkeitsdauer nicht überschreiten.
  - *Unbegrenzt*: Wählen Sie diese Option, um für das Feld den Wert 4.294.967.295 (entspricht unendlich) zu verwenden.
  - *Benutzerdefiniert*: Geben Sie einen Wert ein.
- **Automatische Konfiguration**: Wählen Sie diese Option, um die automatische Konfiguration von IPv6-Adressen mithilfe der statuslosen automatischen Konfiguration sowie die IPv6-Verarbeitung für die Schnittstelle zu aktivieren. Adressen werden abhängig von den in Routerankündigungsnachrichten empfangenen Präfixen konfiguriert.
- **Präfixstatus**: Wählen Sie eine der folgenden Optionen:
  - *On-Link*: Konfiguriert das angegebene Präfix als On-Link-Präfix. Knoten, die Datenverkehr an Adressen mit dem angegebenen Präfix senden, behandeln das Ziel als lokal über die Verbindung erreichbar. Ein On-Link-Präfix wird als verbundenes Präfix mit gesetztem L-Bit in die Routingtabelle eingefügt.
  - *Nicht-On-Link*: Konfiguriert das angegebene Präfix als Nicht-On-Link-Präfix. Ein Nicht-On-Link-Präfix wird als verbundenes Präfix mit nicht gesetztem L-Bit in die Routingtabelle eingefügt.

- *Off-Link*: Konfiguriert das angegebene Präfix als Off-Link-Präfix. Das Präfix wird mit nicht gesetztem L-Bit angekündigt. Das Präfix wird nicht als verbundenes Präfix in die Routingtabelle eingefügt. Wenn das Präfix bereits als verbundenes Präfix in der Routingtabelle vorhanden ist (weil es beispielsweise auch durch Hinzufügen eines IPv6-Adresse konfiguriert wurde), wird es entfernt.

SCHRITT 6 Klicken Sie auf **Übernehmen**, um die Konfiguration in der aktuellen Konfigurationsdatei zu speichern.

Liste der IPv6-Standardrouter

Auf der Seite „Liste der IPv6-Standardrouter“ können Sie die standardmäßigen IPv6-Routeradressen konfigurieren und anzeigen. Die Liste enthält die Router, die Kandidaten für die Festlegung als Standardrouter für das Gerät für nicht lokalen Datenverkehr sind (die Liste kann leer sein). Das Gerät wählt nach dem Zufallsprinzip einen Router aus der Liste aus. Das Gerät unterstützt einen statischen IPv6-Standardrouter. Dynamische Standardrouter sind Router, die Routerankündigungen an die IPv6-Schnittstelle des Geräts gesendet haben.

Wenn IP-Adressen hinzugefügt oder gelöscht werden, geschieht Folgendes:

- Beim Entfernen einer IP-Schnittstelle werden die IP-Adressen aller Standardrouter entfernt. Dynamische IP-Adressen können nicht entfernt werden.
- Eine Alarmmeldung wird angezeigt, nachdem versucht wurde, mehr als eine einzelne benutzerdefinierte Adresse einzufügen.
- Eine Alarmmeldung wird angezeigt, wenn versucht wird, eine Adresse einzufügen, die nicht vom Link Local-Typ ('fe80:') ist.

So definieren Sie einen Standardrouter:

SCHRITT 1 Im Schicht-2-Systemmodus klicken Sie auf **Administration > Verwaltungsschnittstelle > Liste der IPv6-Standardrouter**.
Klicken Sie im Schicht-3-Systemmodus auf **IP-Konfiguration** > **IPv6-Verwaltung und -Schnittstellen** > **Liste der IPv6-Standardrouter**.

Auf dieser Seite werden für die einzelnen Standard-Router die folgenden Felder angezeigt:

- **Schnittstelle**: Ausgehende IPv6-Schnittstelle, an der der Standardrouter angesiedelt ist.
- **IPv6-Adresse des Standardrouters**: Link Local-IP-Adresse des Standardrouters.
- **Typ**: Die Standardrouter-Konfiguration, die die folgenden Optionen umfasst:
  - *Statisch*: Der Standardrouter wurde über die Schaltfläche **Hinzufügen** manuell dieser Tabelle hinzugefügt.
  - *Dynamisch*: Der Standardrouter wurde dynamisch konfiguriert.

- **Metrik (Schicht 3)**: Die Kosten für diesen Hop.
- **Status**: Angabe des Router-Status Folgende Werte sind möglich:
  - *Erreichbar*: Vom Router ist bekannt, dass er erreichbar ist.
  - *Nicht erreichbar*: Vom Router ist bekannt, dass er nicht erreichbar ist.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, um einen statischen Standardrouter hinzuzufügen.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **Link Local-Schnittstelle (Schicht 2)**: Zeigt die ausgehende Link Local-Schnittstelle an.
- **Nächster Hop – Typ**: Die IP-Adresse des nächsten Ziels, an das das Paket gesendet wird. Dieses Feld besteht aus folgenden Optionen:
  - *Global*: Eine IPv6-Adresse, bei der es sich um einen globalen Unicast-IPv6-Typ handelt, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.
  - *Link Local*: Eine IPv6-Schnittstelle und IPv6-Adresse, die Hosts mit einer einzigen Netzwerkverbindung eindeutig kennzeichnet. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
  - *Point-to-Point*: Ein Punkt-zu-Punkt-Tunnel.
- **Schnittstelle (Schicht 3)**: Zeigt die ausgehende Link Local-Schnittstelle an.
- **IPv6-Adresse des Standardrouters**: IP-Adresse des statischen Standardrouters.
- **Metrik (Schicht 3)**: Geben Sie die Kosten für diesen Hop ein.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Der Standardrouter wird in der aktuellen Konfigurationsdatei gespeichert.

Definieren der IPv6-Nachbarinformationen

Auf der Seite „IPv6-Nachbarn“ können Sie die Liste der IPv6-Nachbarn der IPv6-Schnittstelle konfigurieren und anzeigen. In der IPv6-Nachbartabelle (auch bekannt als IPv6 Neighbor Discovery Cache) sind die MAC-Adressen der IPv6-Nachbarn aufgeführt, die sich im selben IPv6-Subnetz wie das Gerät befinden. Dies ist das IPv6-Äquivalent der IPv4-ARP-Tabelle. Wenn das Gerät mit seinen Nachbarn Daten austauschen muss, verwendet es die IPv6-Nachbartabelle, um die MAC-Adressen auf der Grundlage ihrer IPv6-Adressen zu ermitteln.

Auf dieser Seite werden die Nachbarn angezeigt, die automatisch erkannt oder manuell konfiguriert wurden. Jeder Eintrag gibt an, mit welcher Schnittstelle der Nachbar verbunden ist, die IPv6- und die MAC-Adresse des Nachbarn, den Eintragstyp (statisch oder dynamisch) und den Status des Nachbarn.

So definieren Sie IPv6-Nachbarn:

SCHRITT 1 Klicken Sie im Schicht-2-Systemmodus auf **Administration > Verwaltungsschnittstelle > IPv6-Nachbarn**.
Klicken Sie im Schicht-3-Systemmodus auf **IP-Konfiguration** > **IPv6-Verwaltung und -Schnittstellen** > **IPv6-Nachbarn**.

Sie können unter **Tabelle löschen** eine Option auswählen, um einige oder alle IPv6-Adressen in der IPv6-Nachbartabelle zu löschen.

- **Nur statische**: Zum Löschen der statischen IPv6-Adresseinträge.
- **Nur dynamische**: Zum Löschen der dynamischen IPv6-Adresseinträge.
- **Alle dynamischen und statischen**: Zum Löschen der statischen und der dynamischen IPv6-Adresseinträge.

Für die Nachbarschnittstellen werden die folgenden Felder angezeigt:

- **Schnittstelle**: Typ der Nachbar-IPv6-Schnittstelle.
- **IPv6-Adresse**: IPv6-Adresse eines Nachbarn.
- **MAC-Adresse**: Die der angegebenen IPv6-Adresse zugeordnete MAC-Adresse.
- **Typ**: Eintragstyp der Nachbarerkennungs-Cache-Informationen (statisch oder dynamisch).
- **Status**: Angabe des Status des IPv6-Nachbarn. Folgende Werte sind möglich:
  - *Unvollständig*: Adresserkennung wird ausgeführt. Der Nachbar hat noch nicht geantwortet.
  - *Erreichbar*: Vom Nachbarn ist bekannt, dass er erreichbar ist.
  - *Veraltet*: Ein bekanntes Nachbarnetzwerk ist nicht erreichbar. Es wird keine Maßnahme ergriffen, seine Erreichbarkeit zu verifizieren, bevor Datenverkehr gesendet werden muss.
  - *Verzögerung*: Ein bekanntes Nachbarnetzwerk ist nicht erreichbar. Der Switch ist für eine vordefinierte Verzögerungszeit im Status „Verzögerung“. Wenn keine Bestätigung empfangen wird, ändert sich der Status nach Test.
  - *Probe*: Der Nachbar ist nicht mehr als erreichbar bekannt, und es werden Unicast-Nachbaranfragetests gesendet, um seine Erreichbarkeit zu überprüfen.
- **Router**: Gibt an, ob der Nachbar ein Router ist (**Ja** oder **Nein**).

SCHRITT 2 Zum Hinzufügen eines Nachbarn zur Tabelle klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **Schnittstelle**: Die Nachbar-IPv6-Schnittstelle, die hinzugefügt werden soll.
- **IPv6-Adresse**: Geben Sie die der Schnittstelle zugewiesene IPv6-Netzwerkadresse ein. Die Adresse muss eine gültige IPv6-Adresse sein.
- **MAC-Adresse**: Geben Sie die der angegebenen IPv6-Adresse zugeordnete MAC-Adresse ein.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

SCHRITT 5 Um den Typ einer IP-Adresse von **Dynamisch** in **Statisch** zu ändern, wählen Sie die Adresse aus, klicken Sie auf **Bearbeiten** und ändern Sie den Adresstyp auf der Seite „IPv6-Nachbarn bearbeiten“.

IPv6-Präfix-Liste

Bei der Konfiguration von „Sicherheit des ersten Hops“ ist es möglich, Regeln für das Filtern auf der Basis von IPv6-Präfixen zu definieren. Diese Listen können auf der Seite „IPv6-Präfix-Liste“ definiert werden.

Präfix-Listen werden mit den Stichwörtern **Zulassen** oder **Verweigern** konfiguriert, um ein Präfix, das auf einer Übereinstimmungsbedingung basiert, zuzulassen oder zu verweigern. Eine implizite Verweigerung wird auf Datenverkehr angewendet, der mit keinem Eintrag in der Präfix-Liste übereinstimmt.

Ein Eintrag in einer Präfix-Liste besteht aus einer IP-Adresse und einer Bitmaske. Die IP-Adresse kann sich auf eine Netzklasse, ein Subnetz oder eine einzelne Host-Route beziehen. Die Bitmaske ist eine Zahl von 1 bis 32.

Präfix-Listen werden konfiguriert, um den Datenverkehr auf der Basis einer Übereinstimmung einer exakten Präfixlänge in einem Bereich zu filtern, wenn die Stichwörter „ge“ und „le“ verwendet werden.

Die Parameter **Größer als** und **Kleiner als** werden verwendet, um einen Bereich mit Präfixlängen zu definieren und eine flexiblere Konfiguration zu ermöglichen, die über das Netzwerk-/Längenargument hinausgeht. Eine Präfix-Liste wird über eine genaue Übereinstimmung verarbeitet, wenn keiner der Parameter **Größer als** und **Kleiner als** definiert wurde. Wenn nur der Parameter **Größer als** definiert wurde, erstreckt sich der Bereich vom Wert, der für **Größer als** eingegeben wurde, bis hin zu einer vollen Länge mit 32 Bits. Wurde nur der Parameter **Kleiner als** definiert, erstreckt sich der Bereich vom Wert des Netzwerk-/Längenarguments bis hin zum Parameter **Kleiner als**. Wurde sowohl das Argument für **Größer als** als auch das Argument für **Kleiner als** definiert, bezieht sich der Bereich auf die Werte zwischen **Größer als** und **Kleiner als**.

So erstellen Sie eine Präfix-Liste:

SCHRITT 1 (Im Schicht-3-Systemmodus) Klicken Sie auf **IP-Konfiguration > IPv6-Verwaltung und -Schnittstellen > IPv6-Präfix-Liste**.

oder

(Im Schicht-2-Systemmodus) Klicken Sie auf **Administration > IPv6-Verwaltung und -Schnittstellen > IPv6-Präfix-Liste**.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **Listenname**: Wählen Sie eine der folgenden Optionen aus:
  - *Vorhandene Liste verwenden*: Wählen Sie eine zuvor definierte Liste aus, um sie um ein Präfix zu erweitern.
  - *Neue Liste erstellen*: Geben Sie einen Namen ein, um eine neue Liste zu erstellen.
- **Folgenummer**: Definiert die Stelle des Präfix innerhalb der Präfix-Liste. Wählen Sie eine der folgenden Optionen aus:
  - *Automatische Nummerierung*: Setzt das neue IPV6-Präfix an die Stelle nach dem letzten Eintrag der Präfix-Liste. Die Folgenummer ist mit der letzten Folgenummer identisch und wird um die Ziffer 5 erweitert. Ist die Liste leer, wird dem ersten Eintrag in der Präfix-Liste die Ziffer 5 zugewiesen, bei nachfolgenden Einträgen in der Präfix-Liste wird die Ziffer in 5er-Schritten erhöht.
  - *Benutzerdefiniert*: Setzt das neue IPV6-Präfix an die durch den Parameter definierte Stelle. Wenn bereits eine Nummer vorhanden ist, wird diese durch die neue ersetzt.
- **Regeltyp**: Geben Sie die Regel für die Präfix-Liste ein:
  - *Zulassen*: Lässt Netzwerke zu, die mit der Bedingung übereinstimmen.
  - *Ablehnen*: Lehnt Netzwerke ab, die mit der Bedingung übereinstimmen.
  - *Beschreibung*: Text.
- **IPv6-Präfix**: Das IP-Route-Präfix.
- **Präfixlänge**: Die Länge des IP-Route-Präfix.
- **Größer als**: Die Mindestpräfixlänge, die für Übereinstimmungen verwendet wird. Wählen Sie eine der folgenden Optionen aus:
  - *Kein Limit*: Es muss keine Mindestpräfixlänge für Übereinstimmungen verwendet werden.
  - *Benutzerdefiniert*: Die Mindestpräfixlänge, für die eine Übereinstimmung erzielt werden muss.

- **Kleiner als**: Die Höchstpräfixlänge, die für Übereinstimmungen verwendet wird. Wählen Sie eine der folgenden Optionen aus:
  - *Kein Limit*: Es muss keine Höchstpräfixlänge für Übereinstimmungen verwendet werden.
  - *Benutzerdefiniert*: Die Höchstpräfixlänge, für die eine Übereinstimmung erzielt werden muss.
- **Beschreibung**: Geben Sie eine Beschreibung für die Präfix-Liste ein.

SCHRITT 4 Klicken Sie auf **Übernehmen**, um die Konfiguration in der aktuellen Konfigurationsdatei zu speichern.

IPv6-Zugriffslisten

HINWEIS Diese Seite ist nur auf SG500X- und SG500XG-Geräten verfügbar.

Erstellen Sie auf dieser Seite Zugriffslisten zur Verwendung im MLD-Proxy. Weitere Informationen hierzu finden Sie unter **MLD-Proxy**.

So erstellen Sie eine SSM-Zugriffsliste im Schicht-2-Modus:

SCHRITT 1 Klicken Sie auf **Administration > Verwaltungsschnittstelle > IPv6-Routen**.

oder

So erstellen Sie eine SSM-Zugriffsliste im Schicht-3-Systemmodus:
Klicken Sie auf **IP-Konfiguration** > **IPv6-Verwaltung und -Schnittstellen** > **IPv6-Routen**.

Alle SSM-Zugriffslisten werden angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, und geben Sie Werte in die folgenden Felder ein:

- **Zugriffslistenname**: Wählen Sie eine der folgenden Optionen aus:
  - *Vorhandene Liste verwenden*: Wählen Sie eine zuvor definierte SSM-Zugriffsliste aus.
  - *Neue Liste erstellen*: Geben Sie den Namen einer neuen Liste ein.
- **Schnittstelle**: Die Schnittstelle, die zum Weiterleiten eines Pakets verwendet wird.
- **Quell-IPv6-Adressenliste**: Wählen Sie eine der folgenden Optionen:
  - *Beliebig*: Jede beliebige IPv6-Adresse kann als Quelle fungieren.
  - *Benutzerdefiniert*: Nur die angegebene IPv6-Adresse kann als Quelle fungieren.
- **Präfixlänge**: Geben Sie die Präfixlänge der IPv6-Quelladresse ein.

- Aktion: Wählen Sie eine der folgenden Optionen aus:
  - *Zulassen*: Lässt die Weiterleitung von der Quell-IPv6-Adresse zu.
  - *Verweigern*: Verweigert die Weiterleitung von der Quell-IPv6-Adresse.

SCHRITT 3 Klicken Sie auf **Übernehmen**.

Anzeigen von IPv6-Routentabellen

Die IPv6-Weiterleitungstabelle enthält die verschiedenen konfigurierten Routen. Eine dieser Routen ist eine Standardroute (IPv6-Adresse :0), die mithilfe des aus der Liste „IPv6-Standard-Router“ ausgewählten Standardrouters Pakete an Zielgeräte sendet, die sich nicht im selben IPv6-Subnetz befinden wie das Gerät. Zusätzlich zur Standardroute enthält die Tabelle auch dynamische Routen, bei denen es sich um ICMP-Umleitungsrouten handelt, die von IPv6-Routern unter Verwendung von ICMP-Umleitungsbenachrichtigungen empfangen wurden. Dies kann vorkommen, wenn der vom Gerät verwendete Standardrouter nicht der Router ist, über den Datenverkehr an die IPv6-Subnetze gesendet wird, mit denen das Gerät kommuniziert.

So zeigen Sie IPv6-Routen an oder fügen manuell eine Route hinzu:

So zeigen Sie IPv6-Routing-Einträge im Schicht-2-Systemmodus an:

SCHRITT 1 Klicken Sie auf **Administration > Verwaltungsschnittstelle > IPv6-Routen**.

oder

So zeigen Sie IPv6-Routing-Einträge im Schicht-3-Systemmodus an:
Klicken Sie auf **IP-Konfiguration** > **IPv6-Verwaltung und -Schnittstellen** > **IPv6-Routen**.

Auf dieser Seite werden folgende Felder angezeigt:

- **IPv6-Präfix**: Das IP-Route-Präfix für die Ziel-IPv6-Subnetzadresse.
- **Präfixlänge**: Die Präfixlänge der IP-Route für die IPv6-Subnetz-Zieladresse. Ihr geht ein Schrägstrich voraus.
- **Schnittstelle**: Die Schnittstelle, die zum Weiterleiten eines Pakets verwendet wird.
- **Nächster Hop**: Die Adresse, an die das Paket weitergeleitet wird. Normalerweise ist dies die Adresse eines Nachbar-Routers. Sie kann einen der folgenden Typen aufweisen.
  - *Link Local*: Eine IPv6-Schnittstelle und IPv6-Adresse, die Hosts mit einer einzigen Netzwerkverbindung eindeutig kennzeichnet. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.

  - *Global*: Eine IPv6-Adresse, bei der es sich um einen globalen Unicast-IPv6-Typ handelt, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.
  - *Point-to-Point*: Ein Punkt-zu-Punkt-Tunnel.
- **Metrisch**: Wert, der zum Vergleichen dieser Route mit anderen Routen mit demselben Ziel in der IPv6-Routertabelle verwendet wird. Alle Standardrouten haben denselben Wert.
- **Gültigkeitsdauer**: Zeitraum, in dem ein Paket gesendet und erneut gesendet werden kann, bevor es gelöscht wird.
- **Routentyp**: Methode, wie das Ziel angefügt wird, und die Methode zum Abfragen des Eintrags. Verfügbare Werte sind:
  - *Lokal*: Ein direkt verbundenes Netzwerk, dessen Präfix von der IPv6-Adresse eines manuell konfigurierten Geräts abgeleitet wird.
  - *Dynamisch*: Das Ziel ist eine indirekt angehängte IPv6-Subnetzadresse (remote). Der Eintrag wurde dynamisch über das ND- oder ICMP-Protokoll bezogen.
  - *Statisch*: Der Eintrag wurde manuell von einem Benutzer konfiguriert.

DHCPv6-Relais

DHCPv6-Relais wird zur Weiterleitung von DHCPv6-Nachrichten an DHCPv6-Server verwendet. Es ist in RFC 3315 definiert.

Wenn der DHCPv6-Client nicht direkt mit dem DHCPv6-Server verbunden ist, kapselt ein direkt mit dem DHCPv6-Client verbundener DHCPv6-Relais-Agent (das Gerät) die von ihm empfangenen Nachrichten und leitet sie an den DHCPv6-Server weiter.

In entgegengesetzter Richtung entkapselt der Relais-Agent die vom DHCPv6-Server empfangenen Pakete und leitet sie an den DHCPv6-Client weiter.

Der Benutzer muss die Liste der DHCP-Server konfigurieren, an die Pakete weitergeleitet werden. Es können zwei Gruppen von DHCPv6-Servern konfiguriert werden:

- **Globale Ziele**: Pakete werden immer an diese DHCPv6-Server weitergeleitet.
- **Schnittstellenliste**: Dies ist eine Liste mit DHCPv6-Servern nach Schnittstelle. Wenn ein DHCPv6-Paket an einer Schnittstelle empfangen wird, wird es sowohl an die Server in der Schnittstellenliste (sofern vorhanden) als auch an die Server auf der Liste der globalen Ziele weitergeleitet.

Abhängigkeiten von anderen Funktionen

Die Funktionen „DHCPv6-Client“ und „DHCPv6-Relais“ schließen sich für eine Schnittstelle gegenseitig aus.

Globale Ziele

So konfigurieren Sie eine Liste mit DHCPv6-Servern, an die alle DHCPv6-Pakete weitergeleitet werden:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration > IPv6-Verwaltung und -Schnittstellen > DHCPv6-Relais > Globale Ziele**.

SCHRITT 2 Klicken Sie zum Hinzufügen eines DHCPv6-Standardservers auf **Hinzufügen**.

SCHRITT 3 Geben Sie Werte für die Felder ein:

- **IPv6-Adresstyp**: Geben Sie den Typ der Zieladresse ein, an die Clientnachrichten weitergeleitet werden. Mögliche Adresstypen: **Link Local**, **Global** oder **Multicast** (All_DHCP_Relay_Agents_and_Servers).
- **DHCPv6-Server-IP-Adresse**: Geben Sie die Adresse des DHCPv6-Servers ein, an den Pakete weitergeleitet werden.
- (Ziel-)**IPv6-Schnittstelle**: Geben Sie die Schnittstelle ein, an die Pakete übertragen werden, wenn der Adresstyp des DHCPv6-Servers **Link-Local** oder **Multicast** lautet.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Schnittstelleneinstellungen

So aktivieren Sie die Funktion „DHCPv6-Relais“ für eine Schnittstelle und konfigurieren eine Liste mit DHCPv6-Servern, an die an dieser Schnittstelle empfangene DHCPv6-Pakete weitergeleitet werden:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration > IPv6-Verwaltung und -Schnittstellen > DHCPv6-Relais > Schnittstelleneinstellungen**.

SCHRITT 2 Um für eine Schnittstelle DHCPv6 zu aktivieren und optional einen DHCPv6-Server hinzuzufügen, klicken Sie auf **Hinzufügen**.

Geben Sie Werte für die Felder ein:

- **Quellschnittstelle**: Wählen Sie die Schnittstelle (Port, LAG, VLAN oder Tunnel), für die DHCPv6-Relais aktiviert werden.
- **Nur globale Ziele verwenden**: Wählen Sie diese Option, um Pakete nur an die als globale Ziele definierten DHCPv6-Server weiterzuleiten.
- **IPv6-Adresstyp**: Geben Sie den Typ der Zieladresse ein, an die Clientnachrichten weitergeleitet werden. Mögliche Adresstypen: **Link Local**, **Global** oder **Multicast** (All_DHCP_Relay_Agents_and_Servers).
- **DHCPv6-Server-IP-Adresse**: Geben Sie die Adresse des DHCPv6-Servers ein, an den Pakete weitergeleitet werden.

- (Ziel-)**IPv6-Schnittstelle**: Geben Sie die Schnittstelle ein, an die Pakete übertragen werden, wenn der Adresstyp des DHCPv6-Servers **Link-Local** oder **Multicast** lautet.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Domänenname

Das Domain Name System (DNS) übersetzt Domänennamen in IP-Adressen, damit Hosts lokalisiert und adressiert werden können.

Als DNS-Client löst das Gerät über einen oder mehrere konfigurierte DNS-Server Domänennamen in IP-Adressen auf.

DNS-Einstellungen

Auf der Seite „DNS-Einstellungen“ können Sie die DNS-Funktion aktivieren, die DNS-Server konfigurieren und die vom Gerät verwendete Standarddomäne festlegen.

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **Domain Name System** > **DNS-Einstellungen**.

SCHRITT 2 Geben Sie die Parameter ein.

- **DNS**: Wählen Sie diese Option, um das Gerät als DNS-Client festzulegen, der DNS-Namen über einen oder mehrere konfigurierte DNS-Server in IP-Adressen auflösen kann.
- **Abrufwiederholungen**: Geben Sie an, wie oft eine DNS-Abfrage an einen DNS-Server gesendet werden soll, bis das Gerät den DNS-Server als nicht vorhanden behandelt.
- **Abruf-Timeout**: Geben Sie die Anzahl der Sekunden ein, die das Gerät auf eine Antwort auf die DNS-Abfrage warten soll.
- **Abrufintervall**: Geben Sie an, wie oft (in Sekunden) das Gerät DNS-Abfragepakete senden soll, nachdem die Anzahl der Wiederholungen überschritten wurde.
  - *Standard verwenden*: Wählen Sie diese Option, um den Standardwert zu verwenden.

    Dieser Wert = 2 * (Abrufwiederholungen + 1) * Abruf-Timeout.
  - *Benutzerdefiniert*: Wählen Sie diese Option, um einen benutzerdefinierten Wert einzugeben.
- **Standardparameter**: Geben Sie die folgenden Standardparameter ein:
  - **Standarddomänenname**: Geben Sie den DNS-Domänennamen ein, mit dem nicht qualifizierte Hostnamen vervollständigt werden sollen. Das Gerät fügt diesen Namen allen nicht voll qualifizierten Domänennamen (Non Fully Qualified Domain Names, NFQDNs) an, sodass diese zu FQDNs werden.

HINWEIS Lassen Sie den Punkt weg, der einen nicht qualifizierten Namen vom Domänennamen trennt (wie in „cisco.com“).

- **DNS-Domänen-Suchliste**: Klicken Sie auf **Details**, um die Liste der auf dem Gerät konfigurierten DNS-Server anzuzeigen.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

DNS-Servertabelle: Die folgenden Felder werden für jeden konfigurierten DNS-Server angezeigt:

- **DNS-Server**: Die IP-Adresse des DNS-Servers.
- **Präferenz**: Jeder Server hat einen Prioritätswert. Niedrigere Werte entsprechen einer größeren Verwendungswahrscheinlichkeit.
- **Quelle**: Quelle der IP-Adresse des Servers (statisch, DHCPv4 oder DHCPv6).
- **Schnittstelle**: Schnittstelle der IP-Adresse des Servers.

SCHRITT 4 Bis zu acht DNS-Server können definiert werden. Zum Hinzufügen eines DNS-Servers klicken Sie auf **Hinzufügen**.

Geben Sie die Parameter ein.

- **IP-Version**: Wählen Sie Version 6 für IPv6 oder Version 4 für IPv4.
- **IPv6-Adresstyp**: Wählen Sie den IPv6-Adresstyp aus (falls IPv6 verwendet wird). Folgende Optionen sind möglich:
  - *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
  - *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.
- **Link Local-Schnittstelle**: Wenn der IPv6-Adresstyp „Link Local“ lautet, wählen Sie die Schnittstelle, über die der Empfang erfolgt.
- **DNS-Server-IP-Adresse**: Geben Sie die IP-Adresse des DNS-Servers ein.
- **Präferenz**: Wählen Sie einen Wert aus, der die Reihenfolge vorgibt, in der Domänen verwendet werden (von niedrig zu hoch). Hierdurch wird die Reihenfolge bestimmt, in der nicht qualifizierte Namen bei DNS-Abfragen vervollständigt werden.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Der DNS-Server wird in der aktuellen Konfigurationsdatei gespeichert.

Suchliste

Die Suchliste kann einen vom Benutzer auf der Seite „DNS-Einstellungen“ definierten statischen Eintrag sowie von DHCPv4- und DHCPv6-Servern empfangene dynamische Einträge enthalten.

So zeigen Sie die auf dem Gerät konfigurierten Domänennamen an:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **Domain Name System** > **Suchliste**.

Die folgenden Felder werden für jeden auf dem Gerät konfigurierten DNS-Server angezeigt:

- **Domänenname**: Name der Domäne, die auf dem Gerät verwendet werden kann.
- **Quelle**: Quelle der IP-Adresse des Servers für diese Domäne (statisch, DHCPv4 oder DHCPv6).
- **Schnittstelle**: Schnittstelle der IP-Adresse des Servers für diese Domäne.
- **Präferenz**: Reihenfolge, in der die Domänen verwendet werden (von niedrig zu hoch). Hierdurch wird die Reihenfolge bestimmt, in der nicht qualifizierte Namen bei DNS-Abfragen vervollständigt werden.

Hostzuordnung

Die Zuordnungen von Hostnamen zu IP-Adressen werden in der Hostzuordnungstabelle (DNS-Cache) gespeichert.

Dieser Cache kann die folgenden Eintragstypen enthalten:

- **Statische Einträge**: Hierbei handelt es sich um Zuordnungspaare, die dem Cache manuell hinzugefügt wurden. Bis zu 64 statische Einträge sind möglich.
- **Dynamische Einträge**: Hierbei handelt es sich um Zuordnungspaare, die entweder vom System hinzugefügt wurden, nachdem sie vom Benutzer verwendet wurden, oder die einen Eintrag für jede von DHCP auf dem Gerät konfigurierte IP-Adresse enthalten. 256 dynamische Einträge sind möglich.

Die Auflösung von Namen beginnt immer mit der Prüfung der statischen Einträge, geht dann zur Prüfung der dynamischen Einträge über und endet mit dem Senden von Anforderungen an den externen DNS-Server.

Acht IP-Adressen pro DNS-Server und Hostname werden unterstützt.

So fügen Sie einen Hostnamen und seine IP-Adresse hinzu:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **Domain Name System** > **Host-Zuordnung**.

SCHRITT 2 Wählen Sie ggf. die Option **Tabelle löschen** aus, um einige oder alle Einträge in der Hostzuordnungstabelle zu löschen.

- **Nur statische**: Die statischen Hosts werden gelöscht.
- **Nur dynamische**: Die dynamischen Hosts werden gelöscht.
- **Alle dynamischen und statischen**: Die statischen und dynamischen Hosts werden gelöscht.

In der Hostzuordnungstabelle werden die folgenden Felder angezeigt:

- **Hostname**: Der benutzerdefinierte Hostname oder vollständig qualifizierte Name.
- **IP-Adresse**: Die IP-Adresse des Hosts.
- **IP-Version**: Die Version der Host-IP-Adresse.
- **Typ**: Gibt an, ob der Eintrag im Cache **dynamisch** oder **statisch** ist.
- **Status**: Zeigt die Ergebnisse der Zugriffsversuche auf den Host an.
  - *OK*: Versuch erfolgreich.
  - *Negativer Cache*: Versuch fehlgeschlagen, nicht wiederholen.
  - *Keine Rückmeldung*: Es wurde keine Antwort empfangen, das System kann den Versuch jedoch wiederholen.
- **Lebensdauer (Sek)**: Bei dynamischen Einträgen Verbleibdauer im Cache.
- **Verbleibende Lebensdauer (Sek)**: Bei dynamischen Einträgen zusätzliche Verbleibdauer im Cache.

SCHRITT 3 Zum Hinzufügen einer Hostzuordnung klicken Sie auf **Hinzufügen**.

SCHRITT 4 Geben Sie die Parameter ein.

- **IP-Version**: Wählen Sie **Version 6** für IPv6 oder **Version 4** für IPv4.
- **IPv6-Adresstyp**: Wählen Sie den IPv6-Adresstyp aus (falls IPv6 verwendet wird). Folgende Optionen sind möglich:
  - *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
  - *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.
- **Link Local-Schnittstelle**: Wenn der IPv6-Adresstyp „Link Local“ lautet, wählen Sie die Schnittstelle, über die der Empfang erfolgt.

- **Hostname**: Geben Sie einen benutzerdefinierten Hostnamen oder vollständig qualifizierten Namen ein. Hostnamen dürfen nur die ASCII-Buchstaben A bis Z (Groß-/Kleinschreibung wird nicht beachtet), die Zahlen 0 bis 9 sowie Unterstriche oder Bindestriche enthalten. Die Namen werden durch Punkte (.) getrennt.
- **IP-Adresse**: Geben Sie eine Adresse oder bis zu acht zugeordnete IP-Adressen ein (IPv4 oder IPv6).

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die Einstellungen werden in der aktuellen Konfigurationsdatei gespeichert.

20

IP-Konfiguration: RIPv2

In diesem Abschnitt wird die Funktion des RIP-Protokolls Version 2 (Routing Information Protocol) beschrieben.

Die folgenden Themen werden behandelt:

- **Übersicht**
- **Funktionsweise von RIP im Gerät**
- **Konfigurieren von RIP**

HINWEIS RIP wird auf den folgenden Geräten unterstützt:

- SG500X/SG500XG im Standalone-Stacking-Modus.
- SG500X/SG500XG in den erweiterten Hybrid-Stacking-Modi im Schicht-3-Systemmodus.

Übersicht

Das RIP-Protokoll (Routing Information Protocol) ist eine Implementierung eines Distanzvektorprotokolls für LANs (Local Area Network) und WANs (Wide-Area Networks). Es klassifiziert Router als *aktiv* oder *passiv* (stumm). Aktive Router kündigen anderen ihre Routen an, passive Router hören mit und aktualisieren ihre Routen basierend auf Ankündigungen, kündigen selbst jedoch nicht an. Router führen RIP normalerweise im aktiven Modus aus, während Hosts den passiven Modus verwenden.

Das Standard-Gateway ist ein statischer Router und wird von RIP auf die gleiche Weise angekündigt wie alle anderen statischen Router, wenn dies in der Konfiguration aktiviert ist.

Wenn IP-Routing aktiviert ist, funktioniert RIP vollständig. Wenn IP-Routing deaktiviert ist, funktioniert RIP im passiven Modus, das heißt, es lernt nur Routen aus den empfangenen RIP-Nachrichten, ohne sie zu senden.

HINWEIS Das Steuerelement für IP-Routing steht nur bei den SG500X-/ESW2-550X-Modellen zur Verfügung. Aktivieren Sie das IP-Routing auf der Seite **Konfiguration > Verwaltungs- und IP-Schnittstelle > IPv4-Schnittstelle**.

Das Gerät unterstützt RIP Version 2, das auf folgenden Standards beruht:

- RFC2453 RIP Version 2, November 1998
- RFC2082 RIP-2-MD5-Authentifizierung, Januar 1997
- RFC1724 RIP Version 2 MIB-Erweiterung

Empfangene RIPv1-Pakete werden gelöscht.

Funktionsweise von RIP im Gerät

Im folgenden Abschnitt werden Aktivierung, Offset-Konfiguration, passiver Modus, Authentifizierung, Statistikzähler und Peer-Datenbanken im Rahmen von RIP beschrieben.

Aktivieren von RIP

Aktivieren von RIP

- RIP muss global und für jede Schnittstelle aktiviert werden.
- RIP kann nur konfiguriert werden, wenn es aktiviert ist.
- Wenn Sie RIP global deaktivieren, wird die RIP-Konfiguration im System gelöscht.
- Wenn Sie RIP an einer Schnittstelle deaktivieren, wird die RIP-Konfiguration an der angegebenen Schnittstelle gelöscht.
- Wenn IP-Routing deaktiviert ist, werden keine RIP-Nachrichten gesendet, aber wenn RIP-Nachrichten empfangen werden, werden die Daten der Routing-Tabellen damit aktualisiert.

HINWEIS RIP kann nur für manuell konfigurierte IP-Schnittstellen definiert werden. Das heißt, RIP kann nicht für eine Schnittstelle definiert werden, deren IP-Adresse von einem DHCP-Server empfangen wurde oder der Standard-IP-Adresse entspricht.

Offset-Konfiguration

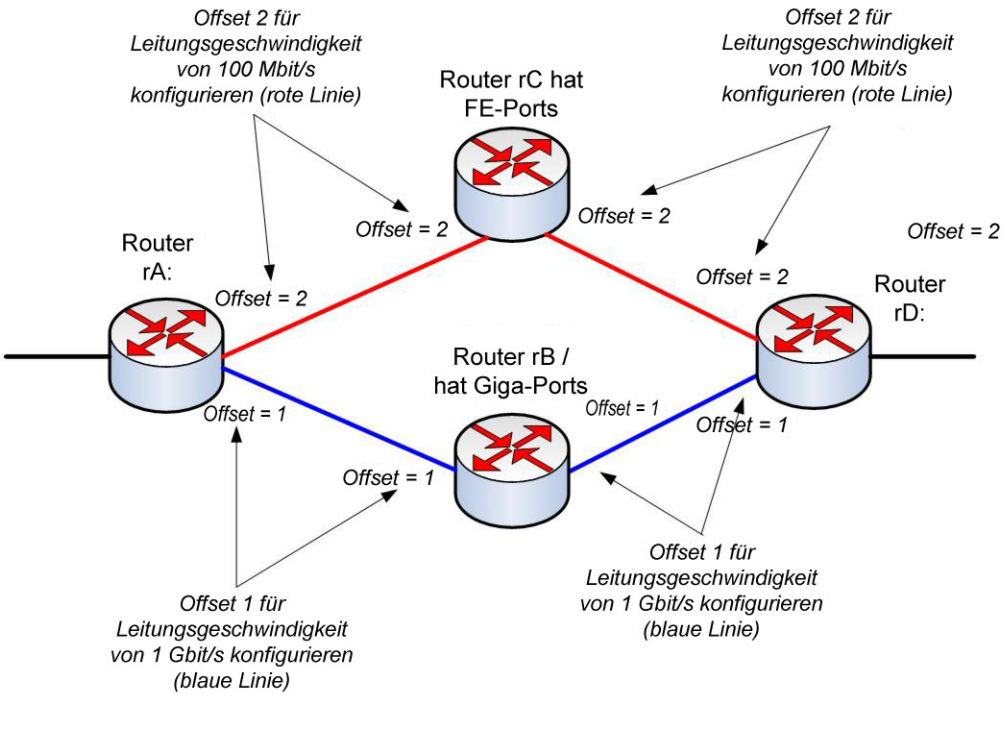
Eine RIP-Nachricht enthält für jede Route eine Metrik (Anzahl der Hops).

Ein Offset ist eine zusätzliche Zahl, die einer Metrik hinzugefügt wird und sich auf die Kosten von Pfaden auswirkt. Der Offset wird pro Schnittstelle festgelegt und kann sich beispielsweise auf die Geschwindigkeit, die Verzögerung oder eine andere Eigenschaft der jeweiligen Schnittstelle beziehen. Auf diese Weise können die relativen Kosten der Schnittstellen nach Bedarf angepasst werden.

Sie müssen den Offset für jede Schnittstelle festlegen (standardmäßig 1).

Die folgende Abbildung veranschaulicht die Konfiguration des Metrik-Offsets für die Portgeschwindigkeit verschiedener Schnittstellen.

Konfiguration des Offsets (für die Portgeschwindigkeit)



Router rD kann Daten an rA über rB oder rC senden. Da rC nur Fast Ethernet-Ports (FE) unterstützt und rB Gigabit Ethernet-Ports (GE) unterstützt, sind die Pfadkosten von Router rD zu Router rA über Router rC höher (Pfadkosten erhöhen sich um 4) als die des Pfads über Router rB (Pfadkosten erhöhen sich um 2). Daher wird die Weiterleitung des Verkehrs über Router rB bevorzugt. Zu diesem Zweck konfigurieren Sie abhängig von der jeweiligen Leitungsgeschwindigkeit für jede Schnittstelle einen anderen Offset (Metrikwert).

Weitere Informationen finden Sie unter **Offset-Konfiguration**.

Passiver Modus

Sie können die Übertragung von Routing-Update-Nachrichten über eine bestimmte Schnittstelle deaktivieren. In diesem Fall ist der Router passiv und empfängt an dieser Schnittstelle nur die aktualisierten RIP-Informationen. Standardmäßig ist die Übertragung von Routing-Updates an einer IP-Schnittstelle aktiviert.

Weitere Informationen finden Sie unter **RIPv2-Einstellungen an IP-Schnittstellen**.

Filtern von Routing-Updates

Sie können eingehende und ausgehende Routen für eine bestimmte IP-Schnittstelle mit zwei Standardzugriffslisten (eine für die Eingabe und eine für die Ausgabe) filtern.

Die Standardzugriffsliste ist eine sortierte Liste mit Namen und Paaren aus IP-Präfix (IP-Adresse und IP-Maskenlänge) und Aktion. Als Aktion ist „Verweigern“ oder „Zulassen“ möglich.

Wenn eine Zugriffsliste definiert ist, wird jede Route aus der RIP-Nachricht anhand der Liste überprüft, beginnend beim ersten Paar: Wenn die Route mit dem ersten Paar übereinstimmt und die Aktion „Zulassen“ entspricht, wird die Route übergeben. Wenn die Aktion „Verweigern“ entspricht, wird die Route nicht übergeben. Wenn die Route nicht übereinstimmt, wird das nächste Paar verglichen.

Wenn die Route mit keinem Paar übereinstimmt, wird die Aktion „Verweigern“ angewendet.

Ankündigen von Standardrouteneinträgen an IP-Schnittstellen

Für die Beschreibung einer Standardroute wird die spezielle Adresse 0.0.0.0 verwendet. Eine Standardroute wird verwendet, um das Mithören jedes möglichen Netzwerks in den Routing-Updates zu verhindern, wenn mindestens ein eng verbundener Router im System bereit ist, Verkehr an die nicht explizit aufgeführten Netzwerke zu übertragen. Diese Router erstellen RIP-Einträge für die Adresse 0.0.0.0, genau wie für ein Netzwerk, mit dem sie verbunden sind.

Sie können die Ankündigung der Standardroute aktivieren und mit einer bestimmten Metrik konfigurieren.

Funktion zur Neuverteilung

Es gibt folgende Arten von Routen, die mithilfe von RIP verteilt werden können:

- **Verbundene**: RIP-Routen, die festgelegten IP-Schnittstellen entsprechen, auf denen RIP nicht aktiviert ist (lokal definiert). Standardmäßig enthält die RIP-Routing-Tabelle nur Routen, die IP-Schnittstellen entsprechen, auf denen RIP aktiviert ist.
- **Statische**: Manuell definierte (Remote) Routen.

Sie können festlegen, ob statische oder verbundene Routen über RIP neu verteilt werden. Konfigurieren Sie dazu wahlweise die Funktion **Statische Route neu verteilen** oder **Verbundene Route neu verteilen**.

Diese Funktionen sind standardmäßig deaktiviert und können global aktiviert werden.

Wenn diese Funktionen aktiviert sind, werden abgelehnte Routen von Routern mit der Metrik 16 angekündigt.

Die Routenkonfigurationen können mit einer der folgenden Optionen verbreitet werden:

- **Standardmetrik**

  RIP verwendet den vordefinierten Standardmetrikwert für die verbreitete Routenkonfiguration.

- **Transparent** (Standard)

  RIP verwendet die Metrik der Routing-Tabelle als RIP-Metrik für die verbreitete Routenkonfiguration.

  Dadurch ergibt sich das folgende Verhalten:

  - Wenn der Metrikwert einer Route kleiner gleich 15 ist, wird bei der Ankündigung dieser Route der Wert im RIP-Protokoll verwendet.
  - Wenn der Metrikwert einer statischen Route größer als 15 ist, wird die Route anderen Routern mit RIP nicht angekündigt.

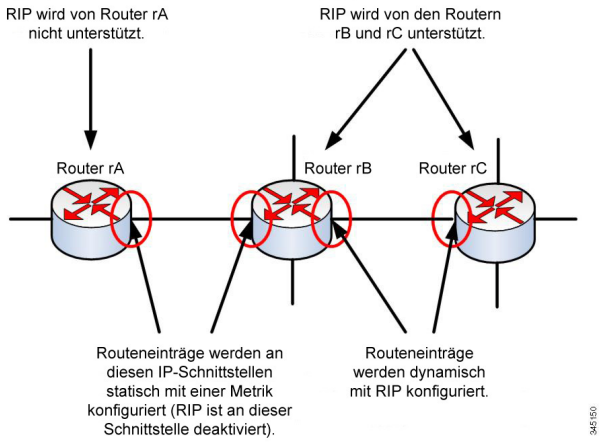
- **Benutzerdefinierte Metrik**

  RIP verwendet den vom Benutzer eingegebenen Metrikwert.

Verwenden von RIP im Netzwerk mit Nicht-RIP-Geräten

Die statische Routenkonfiguration und verbundene Schnittstellen müssen bei der Verwendung von RIP berücksichtigt werden. Dies geht aus der folgenden Abbildung hervor, die ein Netzwerk zeigt, in dem einige Router RIP unterstützen und andere nicht.

Netzwerk mit RIP-Routern und Nicht-RIP-Routern



Router rA unterstützt RIP nicht. Deshalb werden Routing-Einträge mit der entsprechenden Metrik statisch auf diesem Router konfiguriert. Dagegen wird auf dem Router rB die Route zu Router rA als verbundene Route betrachtet. Die Router rB und rC dagegen verwenden RIP zum Ableiten und Verteilen ihrer Routing-Einträge.

Die verbundene Routenkonfiguration von Router rB kann mit der Standardmetrik oder dem transparenten System an Router rC verbreitet werden. Eine statische/verbundene Route wird mit der Metrik der Route (transparente Metrik) oder mit der durch den Befehl für die Standardmetrik definierten Metrik *neu verteilt*.

Weitere Informationen finden Sie unter **Funktion zur Neuverteilung**.

RIP-Authentifizierung

Sie können die Authentifizierung von RIP-Meldungen über die IP-Schnittstelle deaktivieren oder eine der folgenden Authentifizierungsmethoden aktivieren:

- **Unverschlüsselt oder Kennwort**: Verwendet ein Schlüsselkennwort (Zeichenfolge), das zusammen mit der Route an einen anderen Router gesendet wird. Der empfangende Router vergleicht den Schlüssel mit seinem eigenen konfigurierten Schlüssel. Wenn die Schlüssel übereinstimmen, akzeptiert er die Route.
- **MD5**: Verwendet MD5-Digest-Authentifizierung. Jeder Router wird mit einem Satz geheimer Schlüssel konfiguriert. Dieser Satz wird als **Schlüsselkette** bezeichnet. Jede Schlüsselkette besteht aus mindestens einem Schlüssel. Jeder Schlüssel wird durch eine Nummer (**Schlüsselkennung**), eine **Schlüsselzeichenfolge** und optional den Wert **send-lifetime** und **accept-lifetime** identifiziert. Der Wert send-lifetime entspricht dem Zeitraum, in dem ein Authentifizierungsschlüssel in einer Schlüsselkette als gültig gesendet werden kann. Der Wert accept-lifetime entspricht dem Zeitraum, in dem der Authentifizierungsschlüssel in einer Schlüsselkette als gültig empfangen wird.

  Jede übertragene RIP-Nachricht enthält den berechneten MD5-Digest der Nachricht (der die Schlüsselkette enthält) sowie die Schlüsselkennung der verwendeten Schlüsselzeichenfolge. Beim Empfänger ist die Schlüsselkette ebenfalls konfiguriert. Die Schlüsselkennung wird vom Empfänger verwendet, um den Schlüssel für die Überprüfung des MD5-Digests auszuwählen.

RIP-Statistikzähler

Sie können den RIP-Vorgang überwachen, indem Sie die Statistikzähler pro IP-Schnittstelle überprüfen. Eine Beschreibung der Zähler finden Sie unter **Anzeigen von RIPv2-Statistikzählern**.

RIP-Peer-Datenbank

Sie können die RIP-Peer-Datenbank über die IP-Schnittstelle überwachen. Eine Beschreibung der Zähler finden Sie unter **Anzeigen der RIPv2-Peer-Datenbank**.

Konfigurieren von RIP

Die folgenden Aktionen können ausgeführt werden.

- Obligatorische Aktionen:
  - Globales Aktivieren oder Deaktivieren des RIP-Protokolls über die Seite RIPv2-Eigenschaften.
  - Aktivieren oder Deaktivieren des RIP-Protokolls an einer IP-Schnittstelle über die Seite RIPv2-Einstellungen
- Optionale Aktionen (wenn diese Aktionen nicht ausgeführt werden, verwendet das System Standardwerte):
  - Aktivieren oder Deaktivieren von RIP zum Ankündigen von statischen oder verbundenen Routen und deren Metrik an der IP-Schnittstelle über die Seite RIPv2-Eigenschaften.
  - Konfigurieren des Offsets, der der Metrik für eingehende Routen an einer IP-Schnittstelle hinzugefügt wird, über die Seite RIPv2-Einstellungen.
  - Aktivieren des passiven Modus an einer IP-Schnittstelle über die Seite RIPv2-Einstellungen.
  - Steuern der Routen, die bei eingehenden bzw. ausgehenden Routing-Updates verarbeitet werden, durch Angeben einer Liste mit IP-Adressen (siehe **Zugriffslisten**).
  - Ankündigen von Standardrouteneinträgen an der IP-Schnittstelle über die Seite RIPv2-Einstellungen.
  - Aktivieren der RIP-Authentifizierung an einer IP-Schnittstelle über die Seite RIPv2-Einstellungen.

RIPv2-Eigenschaften

So aktivieren oder deaktivieren Sie RIP im Gerät:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv4-Verwaltung und Schnittstellen** > **RIPv2 > Virtuelle Router**.

SCHRITT 2 Wählen Sie nach Bedarf die folgenden Optionen aus:

- **RIP**: Folgende Optionen stehen zur Verfügung:
  - *Aktivieren*: Aktiviert RIP.
  - *Deaktivieren*: Deaktiviert RIP. Wenn Sie RIP deaktivieren, wird die RIP-Konfiguration im System gelöscht.
  - *Herunterfahren*: Legt den globalen RIP-Status auf „Herunterfahren“ fest.

- **RIP-Ankündigung**: Aktiviert das Senden von Routing-Updates an alle RIP-IP-Schnittstellen.
- **Ankündigung Standardroute**: Aktiviert das Senden der Standardroute an die RIP-Domäne. Diese Route dient als Standardrouter.
- **Standardmetrik**: Geben Sie den Wert für die Standardmetrik ein (siehe auch **Funktion zur Neuverteilung**).

SCHRITT 3 **Statische Route neu verteilen**: Wählen Sie diese Option aus, um die Funktion zu aktivieren (Beschreibung siehe **Funktion zur Neuverteilung**).

SCHRITT 4 Wenn **Statische Route neu verteilen** aktiviert ist, wählen Sie eine Option für das Feld **Statische Metrik neu verteilen aus.** Folgende Optionen stehen zur Verfügung:

- **Standardmetrik**: RIP verwendet den vordefinierten Standardmetrikwert für die verbreitete statische Routenkonfiguration (siehe **Funktion zur Neuverteilung**).
- **Transparent**: RIP verwendet die Metrik der Routing-Tabelle als RIP-Metrik für die verbreitete statische Routenkonfiguration. Dadurch ergibt sich das folgende Verhalten:
  - Wenn der Metrikwert einer statischen Route kleiner oder gleich 15 ist, wird bei der Ankündigung der statischen Route der Wert im RIP-Protokoll verwendet.
  - Wenn der Metrikwert einer statischen Route größer als 15 ist, wird die statische Route anderen Routern mit RIP nicht angekündigt.
- **Benutzerdefinierte Metrik**: Geben Sie den Wert der Metrik ein.

SCHRITT 5 **Verbundene Route neu verteilen**: Wählen Sie diese Option aus, um die Funktion zu aktivieren (Beschreibung unter Neuverteilen statischer Routenkonfigurationen).

SCHRITT 6 Wenn **Verbundene Route neu verteilen** aktiviert ist, wählen Sie eine Option für das Feld **Statische Metrik neu verteilen** aus. Folgende Optionen stehen zur Verfügung:

- **Standardmetrik**: RIP verwendet den vordefinierten Standardmetrikwert für die verbreitete statische Routenkonfiguration (siehe **Funktion zur Neuverteilung**).
- **Transparent**: RIP verwendet die Metrik der Routing-Tabelle als RIP-Metrik für die verbreitete statische Routenkonfiguration. Dadurch ergibt sich das folgende Verhalten:
  - Wenn der Metrikwert einer statischen Route kleiner oder gleich 15 ist, wird bei der Ankündigung der statischen Route der Wert im RIP-Protokoll verwendet.
  - Wenn der Metrikwert einer statischen Route größer als 15 ist, wird die statische Route anderen Routern mit RIP nicht angekündigt.
- **Benutzerdefinierte Metrik**: Geben Sie den Wert der Metrik ein.

SCHRITT 7 Klicken Sie auf **Übernehmen**. Die Einstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

RIPv2-Einstellungen an IP-Schnittstellen

So konfigurieren Sie RIP für eine Schnittstelle:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **RIPv2 > RIPv2-Einstellungen**.

SCHRITT 2 Die RIP-Parameter werden pro IP-Schnittstelle angezeigt.

Zum Hinzufügen einer neuen IP-Schnittstelle klicken Sie auf **Hinzufügen**, um die Seite RIPv2-Einstellungen hinzufügen zu öffnen, und füllen Sie folgende Felder aus:

- **IP-Adresse**: Wählen Sie eine in der Schicht-2-Schnittstelle definierte IP-Schnittstelle aus.
- **Herunterfahren**: Aktivieren Sie sogar im heruntergefahrenen Zustand RIP an der Schnittstelle.
- **Passiv**: Gibt an, ob RIP-Meldungen mit Routen-Updates an der angegebenen Schnittstelle gesendet werden dürfen. Wenn das Feld nicht aktiviert ist, werden keine RIP-Updates gesendet (passiv).
- **Versatz**: Gibt die Metriknummer der angegebenen IP-Schnittstelle an. Dieser Wert gibt basierend auf der Geschwindigkeit der Schnittstelle die zusätzlichen Kosten für die Verwendung dieser Schnittstelle an.
- **Ankündigung Standardroute**: Diese Option wird global über die Seite **RIPv2-Eigenschaften** definiert. Sie können die globale Definition verwenden oder dieses Feld für eine bestimmte Schnittstelle definieren. Folgende Optionen stehen zur Verfügung:
  - *Global*: Verwendet die auf der Seite **RIPv2-Eigenschaften** definierten globalen Einstellungen.
  - *Deaktivieren*: Auf dieser RIP-Schnittstelle wird die Standardroute nicht angekündigt.
  - *Aktivieren*: Auf dieser RIP-Schnittstelle wird die Standardroute angekündigt.
- **Ankündigung Standardroute – Metrik**: Geben Sie die Metrik für die Standardroute dieser Schnittstelle ein.
- **Authentifizierungsmodus**: Status der RIP-Authentifizierung (aktivieren/deaktivieren) an einer angegebenen IP-Schnittstelle. Folgende Optionen stehen zur Verfügung:
  - *Keine*: Es wird keine Authentifizierung durchgeführt.
  - *Text*: Das nachstehende Schlüsselkennwort wird für die Authentifizierung verwendet.
  - *MD5*: Der MD5-Digest der unten ausgewählten Schlüsselkette wird für die Authentifizierung verwendet.
- **Schlüsselkennwort**: Wenn Sie den Authentifizierungstyp **Text** ausgewählt haben, geben Sie das zu verwendende Kennwort ein.
- **Schlüsselkette**: Wenn Sie den Authentifizierungsmodus **MD5** ausgewählt haben, geben Sie die zu verwendende Schlüsselkette ein. Diese Schlüsselkette wird gemäß der Beschreibung im Abschnitt **Schlüsselverwaltung** erstellt.

- **Eingangsverteilliste**: Mit dieser Option können Sie Filter für die eingehenden RIP-Routen bestimmter IP-Adressen in einer Zugriffsliste konfigurieren. Wenn dieses Feld aktiviert ist, wählen Sie unten den Namen der Zugriffsliste aus.
- **Name der Zugriffsliste**: Wählen Sie den Namen der Zugriffsliste (die eine Liste mit IP-Adressen enthält) zur Filterung eingehender RIP-Routen an einer bestimmten Schnittstelle aus. Eine Beschreibung der Zugriffslisten finden Sie unter **Erstellen einer Zugriffsliste**.
- **Ausgangsverteilliste**: Mit dieser Option können Sie Filter für ausgehende RIP-Routen an bestimmten IP-Adressen in einer Zugriffsliste konfigurieren. Wenn dieses Feld aktiviert ist, wählen Sie unten den Namen der Zugriffsliste aus.
- **Name der Zugriffsliste**: Wählen Sie den Namen der Zugriffsliste (die eine Liste mit IP-Adressen enthält) zur Filterung ausgehender RIP-Routen an einer bestimmten Schnittstelle aus. Eine Beschreibung der Zugriffslisten finden Sie unter **Erstellen einer Zugriffsliste**.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Einstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Anzeigen von RIPv2-Statistikzählern

So zeigen Sie die RIP-Statistikzähler für die einzelnen IP-Adressen an:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **RIPv2 > RIPv2-Statistik**.

Die folgenden Felder werden angezeigt:

- **IP-Schnittstelle**: In der Schicht-2-Schnittstelle definierte IP-Schnittstelle.
- **Fehlerhafte Pakete empfangen**: Gibt die Anzahl der fehlerhaften Pakete an, die von RIP an der IP-Schnittstelle identifiziert wurden.
- **Fehlerhafte Routen empfangen**: Gibt die Anzahl der empfangenen fehlerhaften Routen an, die von RIP an der IP-Schnittstelle identifiziert wurden. Fehlerhafte Routen sind Routen mit falschen Routenparametern. Beispiel: Das IP-Ziel ist eine Broadcast-Adresse oder die Metrik ist 0 oder größer als 16.
- **Gesendete Updates**: Gibt die Anzahl der Pakete an, die von RIP an der IP-Schnittstelle gesendet wurden.

SCHRITT 2 Zum Löschen aller Schnittstellenzähler klicken Sie auf **Alle Schnittstellenzähler löschen**.

Anzeigen der RIPv2-Peer-Datenbank

So zeigen Sie die RIP-Peer-Datenbank (Nachbarn) an:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **RIPv2 > RIPv2-Peer-Router-Datenbank**.

Für die Peer-Router-Datenbank werden die folgenden Felder angezeigt:

- **IP-Adresse des Routers**: In der Schicht-2-Schnittstelle definierte IP-Schnittstelle.
- **Fehlerhafte Pakete empfangen**: Gibt die Anzahl der fehlerhaften Pakete an, die von RIP an der IP-Schnittstelle identifiziert wurden.
- **Fehlerhafte Routen empfangen**: Gibt die Anzahl der empfangenen fehlerhaften Routen an, die von RIP an der IP-Schnittstelle identifiziert wurden. Fehlerhafte Routen sind Routen mit falschen Routenparametern. Beispiel: Das IP-Ziel ist eine Broadcast-Adresse oder die Metrik ist 0 oder größer als 16.
- **Letzte Aktualisierung**: Gibt an, wann RIP zum letzten Mal RIP-Routen von der Remote-IP-Adresse empfangen hat.

SCHRITT 2 Zum Löschen aller Zähler klicken Sie auf **Alle Schnittstellenzähler löschen**.

Zugriffslisten

Eine Beschreibung der Zugriffslisten finden Sie unter **Filtern von Routing-Updates**.

Zum Erstellen von Zugriffslisten führen Sie die folgenden Schritte aus:

1. Erstellen Sie auf der Seite Zugriffslisteneinstellungen eine Zugriffsliste mit nur einer IP-Adresse.
2. Fügen Sie bei Bedarf über die Seite Quell-IPv4-Adressenliste weitere IP-Adressen hinzu.

Erstellen einer Zugriffsliste

So legen Sie die globale Konfiguration einer Zugriffsliste fest:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv4-Verwaltung und -Schnittstellen > Zugriffsliste** > **Zugriffslisteneinstellungen**.

SCHRITT 2 Zum Hinzufügen einer neuen Zugriffsliste klicken Sie auf **Hinzufügen**, um die Seite Zugriffsliste hinzufügen zu öffnen, und geben Sie Werte für die folgenden Felder ein:

- **Name**: Definieren Sie einen Namen für die Zugriffsliste.

- **Quell-IPv4-Adresse**: Geben Sie die Quell-IPv4-Adresse ein. Folgende Optionen stehen zur Verfügung:
  - *Beliebig*: Alle IP-Adressen sind enthalten.
  - *Benutzerdefiniert*: Geben Sie eine IP-Adresse ein.
- **Quell-IPv4-Maske**: Geben Sie den Maskentyp und Wert für die Quell-IPv4-Adresse ein. Folgende Optionen stehen zur Verfügung:
  - *Netzwerkmaske*: Geben Sie die Netzwerkmaske ein.
  - *Präfixlänge*: Geben Sie die Präfixlänge ein.
- **Aktion**: Wählen Sie eine Aktion für die Zugriffsliste aus. Folgende Optionen stehen zur Verfügung:
  - *Zulassen*: Alle Pakete von den IP-Adressen in der Zugriffsliste werden zugelassen.
  - *Verweigern*: Alle Pakete von den IP-Adressen in der Zugriffsliste werden abgelehnt.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Einstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Auffüllen einer Zugriffsliste

So füllen Sie eine Zugriffsliste mit IP-Adressen:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration > IPv4-Verwaltung und -Schnittstellen > Zugriffsliste** > **Quell-IPv4-Adressenliste**.

SCHRITT 2 Zum Ändern der Parameter einer Zugriffsliste klicken Sie auf **Hinzufügen**, um die Seite Zugriffsliste bearbeiten zu öffnen, und ändern Sie die folgenden Felder:

- **Name der Zugriffsliste**: Name der Zugriffsliste.
- **Quell-IPv4-Adresse**: Quell-IPv4-Adresse. Folgende Optionen stehen zur Verfügung:
  - *Beliebig*: Alle IP-Adressen sind enthalten.
  - *Benutzerdefiniert*: Geben Sie eine IP-Adresse ein.
- **Quell-IPv4-Maske**: Maskentyp und Wert für die Quell-IPv4-Adresse. Folgende Optionen stehen zur Verfügung:
  - *Netzwerkmaske*: Geben Sie die Netzwerkmaske ein (beispielsweise 255.255.0.0).
  - *Präfixlänge*: Geben Sie die Präfixlänge ein.

- **Aktion**: Aktion für die Zugriffsliste. Folgende Optionen stehen zur Verfügung:
  - *Zulassen*: Alle Pakete von den IP-Adressen in der Zugriffsliste werden zugelassen.
  - *Verweigern*: Alle Pakete von den IP-Adressen in der Zugriffsliste werden abgelehnt.

21

IP-Konfiguration: VRRP

In diesem Kapitel wird die Funktionsweise von VRRP (Virtual Router Redundancy Protocol) beschrieben und Sie erfahren, wie Sie virtuelle Router mit VRRP über die grafische Weboberfläche konfigurieren.

HINWEIS Die SF500-Modelle unterstützen die VRRP-Funktion nicht.

Die folgenden Themen werden behandelt:

- **Übersicht**
- **Konfigurierbare Elemente von VRRP**
- **Konfigurieren von VRRP**

Übersicht

VRRP ist ein Auswahl- und Redundanzprotokoll, das dynamisch einem der physischen Router in einem LAN die Aufgaben eines virtuellen Routers zuweist. Dadurch wird die Verfügbarkeit und Zuverlässigkeit von Routing-Pfaden im Netzwerk erhöht.

Bei VRRP wird ein physischer Router in einem virtuellen Router als Master ausgewählt, während der andere physische Router des gleichen virtuellen Routers als Backup für den Fall eines Fehlers beim Master fungiert. Die physischen Router werden als VRRP-Router bezeichnet.

Das Standard-Gateway eines teilnehmenden Hosts wird nicht einem physischen Router, sondern dem virtuellen Router zugewiesen. Wenn bei dem physischen Router, der Pakete im Auftrag des virtuellen Routers weiterleitet, ein Fehler auftritt, wird automatisch ein anderer physischer Router als Ersatz ausgewählt. Der physische Router, der jeweils Pakete weiterleitet, wird als Masterrouter bezeichnet.

VRRP ermöglicht außerdem Lastenausgleich für den Verkehr. Sie können den Verkehr gleichmäßig auf verfügbare Router verteilen, indem Sie VRRP so konfigurieren, dass Verkehr an und von LAN-Clients auf mehrere Router verteilt wird.

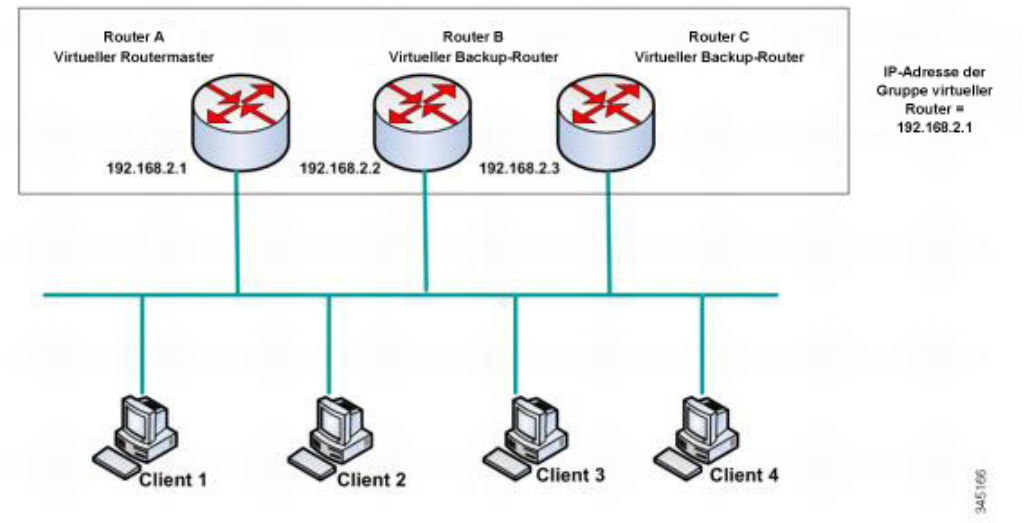
Einschränkungen

VRRP wird nur auf SG500X-/ESW2-550X-Switches unterstützt.

VRRP-Topologie

Die folgende Abbildung zeigt eine LAN-Topologie, in der VRRP konfiguriert ist. In diesem Beispiel verwenden die Router A, B und C VRRP und bilden einen virtuellen Router. Die IP-Adresse des virtuellen Routers ist die gleiche, die Sie für die Ethernet-Schnittstelle von Router A konfiguriert haben (198.168.2.1).

Einfache VRRP-Topologie



Da der virtuelle Router die IP-Adresse der physischen Ethernet-Schnittstelle von Router A verwendet, übernimmt Router A die Rolle des *virtuellen Routermasters* und wird auch als *Besitzer der IP-Adresse* bezeichnet. Als virtueller Routermaster steuert Router A die IP-Adresse des virtuellen Routers und ist für die Weiterleitung von Paketen im Auftrag des virtuellen Routers zuständig. Die Clients 1 bis 3 sind mit der Standard-Gateway-IP-Adresse 198.168.2.1 konfiguriert. Client 4 ist mit der Standard-Gateway-IP-Adresse 198.168.2.2 konfiguriert.

HINWEIS Der VRRP-Router, der Besitzer der IP-Adresse ist, reagiert auf Pakete, deren Ziel die IP-Adresse ist, und verarbeitet sie. Der VRRP-Router, der virtueller Routermaster, aber nicht Besitzer der IP-Adresse ist, reagiert nicht auf diese Pakete bzw. verarbeitet sie nicht.

Router B und C fungieren als *virtuelle Router-Backups*. Wenn beim virtuellen Routermaster ein Fehler auftritt, wird der mit der höchsten Priorität konfigurierte Router zum virtuellen Routermaster und nimmt den Dienst für die LAN-Hosts mit minimaler Unterbrechung auf.

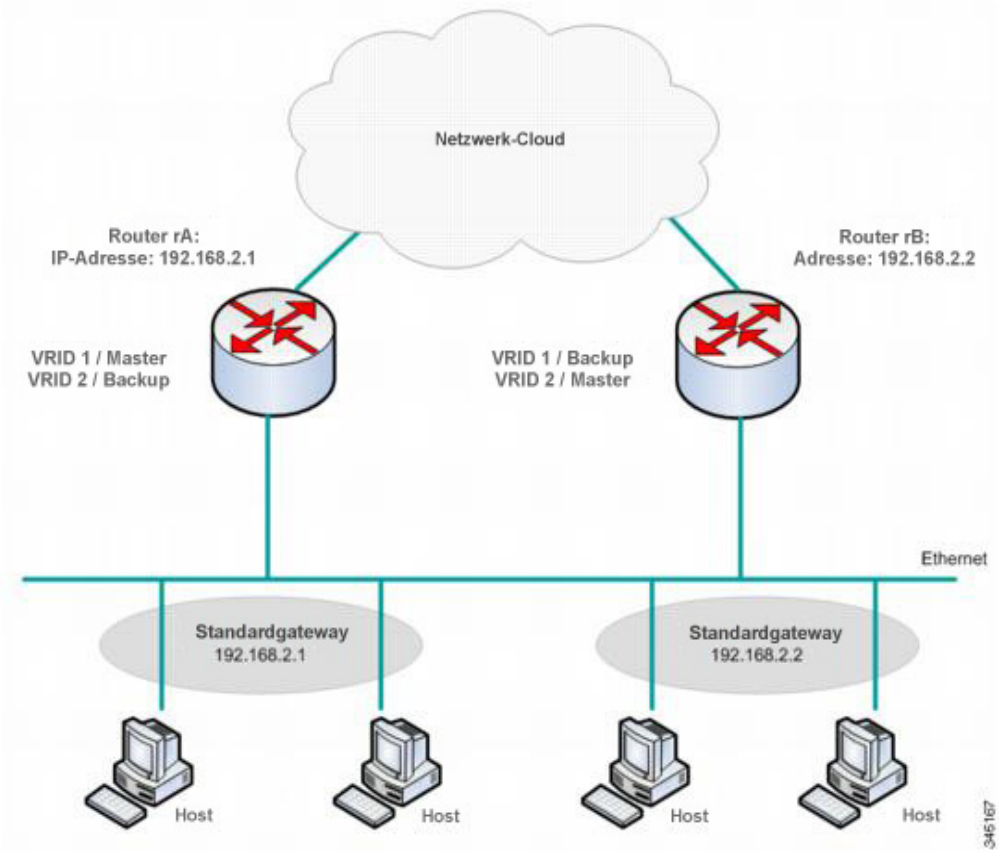
HINWEIS Die Priorität der VRRP-Router hängt von folgenden Faktoren ab: Wenn der VRRP-Router der Besitzer ist, hat er die Priorität 255 (höchste Priorität). Wenn er nicht der Besitzer ist, wird die Priorität manuell konfiguriert (immer niedriger als 255).

Wenn Router A wiederhergestellt ist, wird er wieder zum virtuellen Routermaster. Während der Wiederherstellung des Masters leiten beide Master Pakete weiter. Dadurch entstehen Doppelungen (normales Verhalten), aber keine Unterberechungen.

Weitere Details zu den Rollen von VRRP-Routern und dazu, was bei einem Fehler beim virtuellen Routermaster geschieht, finden Sie unter **Priorität und Vorrang bei VRRP-Routern**.

Die folgende Abbildung zeigt eine LAN-Topologie, in der VRRP konfiguriert ist. Router A und B verarbeiten gemeinsam den Verkehr zu und von den Clients 1 bis 4 und Router A und B fungieren als virtuelle Router-Backups füreinander, falls bei einem der Router ein Fehler auftritt.

VRRP-Topologie für Lastenausgleich



In dieser Topologie sind zwei virtuelle Router konfiguriert. Für den virtuellen Router 1 ist rA der Besitzer der IP-Adresse 192.168.2.1 und der virtuelle Routermaster. rB ist das virtuelle Router-Backup für rA. Die Clients 1 und 2 sind mit der Standard-Gateway-IP-Adresse 192.168.2.1 konfiguriert.

Für den virtuellen Router 2 ist rB der Besitzer der IP-Adresse 192.168.2.2 und der virtuelle Routermaster. rA ist das virtuelle Router-Backup für rB. Die Clients 3 und 4 sind mit der Standard-Gateway-IP-Adresse 192.168.2.2 konfiguriert.

Konfigurierbare Elemente von VRRP

Einem virtuellen Router muss eine unter allen virtuellen Routern im gleichen LAN eindeutige Kennung (Virtual Router Identifier, VRID) zugewiesen werden. Alle VRRP-Router, die den gleichen virtuellen Router unterstützen, müssen mit allen Informationen zu dem virtuellen Router einschließlich seiner VRID konfiguriert sein. Virtuelle Router sollten nur dann im Gerät aktiviert werden, wenn dort auch IP-Routing aktiviert ist.

Sie können einen VRRP-Router als Bestandteil eines oder mehrerer virtueller Router konfigurieren, indem Sie CLI-Befehle oder die grafische Weboberfläche verwenden, wie im Abschnitt **Konfigurieren von VRRP** beschrieben.

Zum Konfigurieren eines virtuellen Routers konfigurieren Sie seine Informationen, beispielsweise die ID und die IP-Adressen des virtuellen Routers, auf allen VRRP-Routern, die den virtuellen Router unterstützen. Sie können die folgenden Elemente konfigurieren und anpassen.

Kennung des virtuellen Routers

Sie müssen eine Kennung (VRID) zuweisen und können eine Beschreibung zuweisen. In den folgenden Abschnitten werden die verschiedenen Attribute des virtuellen Routers beschrieben.

VRRP unterstützt bis zu 255 virtuelle Router (VRRP-Gruppen).

VRRP-Versionen

Das Gerät unterstützt die folgenden VRRP-Versionstypen:

- IPv4-VRRPv3 auf der Grundlage von RFC5798. VRRPv3-Nachrichten werden gesendet.
- IPv4-VRRPv3 und -VRRPv2 auf der Grundlage von RFC5798. VRRPv3- und VRRPv2-Nachrichten werden gesendet.
- IPv4-VRRPv2 auf der Grundlage von RC3768. VRRPv2-Nachrichten werden gesendet.

Sie konfigurieren die VRRP-Version für jeden virtuellen Router einzeln. Standardmäßig ist VRRPv2 festgelegt.

Folgende Situationen sind möglich, wenn Sie einen virtuellen Router konfigurieren:

- Alle vorhandenen VRRP-Router des virtuellen Routers verwenden VRRPv3. Konfigurieren Sie in diesem Fall den neuen VRRP-Router für die Verwendung von VRRPv3.
- Alle vorhandenen VRRP-Router des virtuellen Routers verwenden VRRPv2. Konfigurieren Sie in diesem Fall den neuen VRRP-Router für die Verwendung von VRRPv2.

- Mindestens ein VRRP-Router des virtuellen Routers verwendet VRRPv2 und VRRPv3. Konfigurieren Sie in diesem Fall den VRRP-Router für die Verwendung von VRRPv3, obwohl VRRPv2 ebenfalls kompatibel ist.

  HINWEIS Wenn der virtuelle Router reine VRRPv2-Router und reine VRRPv3-Router enthält, müssen Sie mindestens einen VRRPv2-Router und einen VRRPv3-Router konfigurieren.

  HINWEIS Wenn VRRPv2 und VRRPv3 in einem VRRP-Router aktiviert sind, überträgt der VRRP-Router VRRPv2- und VRRPv3-Pakete. Gemäß dem VRRPv3-Standards sollten Sie VRRPv2 und VRRPv3 aktivieren, wenn Sie von v2 auf v3 aktualisieren. Das Mischen der beiden Versionen ist nicht als Dauerlösung gedacht. Details zum gemeinsamen Betrieb von VRRPv2 und VRRPv3 finden Sie im VRRPv3-Standard.

IP-Adressen des virtuellen Routers

Jedem virtuellen Router wird mindestens eine IP-Adresse zugewiesen, für die der aktuelle Master die Zuständigkeit übernimmt.

Ein VRRP-Router, der einen virtuellen Router unterstützt, benötigt eine IP-Adresse im gleichen IP-Subnetz wie die im virtuellen Router konfigurierten IP-Adressen.

Beim Zuweisen von IP-Adressen zu einem virtuellen Router gelten die folgenden Regeln:

- Alle den virtuellen Router unterstützenden VRRP-Router müssen in ihrer Konfiguration für den virtuellen Router mit den gleichen IP-Adressen des virtuellen Routers konfiguriert sein.
- Keine der IP-Adressen kann für einen anderen virtuellen Router verwendet werden oder für VRRP-Router, die den virtuellen Router nicht unterstützen.
- Einer der VRRP-Router, die den virtuellen Router unterstützen, muss Besitzer aller IP-Adressen des virtuellen Routers sein. Ein VRRP-Router ist Besitzer der IP-Adressen, wenn die Adressen als tatsächliche Adressen an seiner IP-Schnittstelle konfiguriert sind.
- Wenn ein VRRP-Router (der physische Router) Besitzer der IP-Adressen des virtuellen Routers ist, kann die IP-Adresse des virtuellen Routers nicht über DHCP zugewiesen werden, sondern sie muss manuell im VRRP-Router konfiguriert werden.
- Wenn ein VRRP-Router nicht Besitzer der IP-Adressen des virtuellen Routers ist, gilt Folgendes:
  - Die VRRP-Router, die nicht Besitzer sind, müssen mit einer IP-Schnittstelle im gleichen IP-Subnetz konfiguriert werden wie die IP-Adressen des virtuellen Routers.
  - Das entsprechende IP-Subnetz kann nicht über DHCP zugewiesen werden, sondern es muss manuell im VRRP-Router konfiguriert werden.

Alle VRRP-Router, die den gleichen virtuellen Router unterstützen, müssen die gleiche Konfiguration aufweisen. Wenn sich die Konfigurationen unterscheiden, wird die Konfiguration des Masters verwendet. Ein Backup-VRRP-Router protokolliert eine Syslog-Nachricht, wenn seine Konfiguration von der Konfiguration des Masters abweicht.

Quell-IP-Adresse in einem VRRP-Router

Jeder VRRP-Router, der einen virtuellen Router unterstützt, verwendet seine eigene IP-Adresse als Quell-IP-Adresse in seinen ausgehenden VRRP-Nachrichten für den virtuellen Router. VRRP-Router des gleichen virtuellen Routers kommunizieren über VRRP-Nachrichten miteinander. Wenn ein VRRP-Router Besitzer der IP-Adresse des virtuellen Routers ist, ist die IP-Adresse eine der IP-Adressen des virtuellen Routers. Wenn ein VRRP-Router nicht Besitzer der IP-Adresse des virtuellen Routers ist, ist die IP-Adresse die IP-Adresse der Schnittstelle des VRRP-Routers für das gleiche IP-Subnetz des virtuellen Routers.

Wenn die Quell-IP-Adresse manuell konfiguriert wurde, wird die Konfiguration entfernt und die standardmäßige Quell-IP-Adresse verwendet (die niedrigste an der Schnittstelle definierte IP-Adresse des VRRP-Routers). Wenn die Quell-IP-Adresse eine Standardadresse war, wird eine neue standardmäßige Quell-IP-Adresse verwendet.

Priorität und Vorrang bei VRRP-Routern

Ein wichtiger Aspekt des VRRP-Redundanzmodells ist die Möglichkeit, jedem VRRP-Router eine VRRP-Priorität zuzuweisen. Die VRRP-Priorität muss ausdrücken, wie effizient ein VRRP-Router als Backup eines im VRRP-Router definierten virtuellen Routers fungieren würde. Wenn mehrere Backup-VRRP-Router für den virtuellen Router vorhanden sind, bestimmt die Priorität, welcher Backup-VRRP-Router als Master zugewiesen wird, wenn beim aktuellen Master ein Fehler auftritt.

Wenn ein virtueller Router der Besitzer der IP-Adresse ist, wird ihm vom System automatisch die VRRP-Priorität 255 zugewiesen, und der VRRP-Router (dem dieser virtuelle Router zugewiesen wird) fungiert automatisch als virtueller Routermaster, wenn er aktiv ist.

In der **Abbildung** findet ein Auswahlprozess statt, wenn bei Router A, dem virtuellen Routermaster, ein Fehler auftritt. Dabei wird ermittelt, ob die virtuellen Backup-Router B oder C übernehmen müssen. Wenn die Router B und C mit der Priorität 101 bzw. 100 konfiguriert sind, wird Router B als virtueller Routermaster ausgewählt, da er die höhere Priorität hat. Wenn beide die gleiche Priorität haben, wird der Router mit der höheren IP-Adresse als virtueller Routermaster ausgewählt.

Standardmäßig ist eine Vorrangfunktion aktiviert, die Folgendes bewirkt:

- Aktiviert: Wenn ein VRRP-Router aktiv ist, der mit einer höheren Priorität als der aktuelle Master konfiguriert ist, ersetzt er den aktuellen Master.
- Deaktiviert: Auch wenn ein VRRP-Router mit einer höheren Priorität als der aktuelle Master aktiv ist, ersetzt er den aktuellen Master nicht. Nur der ursprüngliche Master ersetzt (wenn er verfügbar wird) den Backup.

VRRP-Ankündigungen

Der virtuelle Routermaster sendet VRRP-Ankündigungen an Router in der gleichen Gruppe (die mit der gleichen Kennung des virtuellen Routers konfiguriert sind).

Die VRRP-Ankündigungen werden in IP-Paketen gekapselt und an die der VRRP-Gruppe zugewiesene IPv4-Multicast-Adresse gesendet. Die Ankündigungen werden standardmäßig jede Sekunde gesendet. Das Bekanntgabeintervall ist konfigurierbar.

Das Bekanntgabeintervall wird in ms angegeben (Bereich: 50 - 40950, Standard: 1000). Ein leerer Wert ist ungültig.

- Bei VRRP-Version 3 wird das betriebsspezifische Bekanntgabeintervall auf 10 ms abgerundet.
- Bei VRRP-Version 2 wird das betriebsspezifische Bekanntgabeintervall auf die nächste Sekunde abgerundet. Minimaler Betriebswert: 1 Sekunde.

Konfigurieren von VRRP

Sie können diese Funktion auf den folgenden Seiten konfigurieren:

Virtuelle Router

Die VRRP-Eigenschaften können Sie auf der Seite „Virtuelle VRRP-Router“ konfigurieren und anpassen.

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv4-Verwaltung und Schnittstellen > VRRP > Virtuelle Router**.

SCHRITT 2 Zum Hinzufügen eines virtuellen Routers klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **Schnittstelle**: Die Schnittstelle, an der der virtuelle Router definiert ist.
- **Kennung des virtuellen Routers**: Eine benutzerdefinierte Nummer zur Identifizierung des virtuellen Routers.
- **Beschreibung**: Eine benutzerdefinierte Zeichenfolge zur Identifizierung des virtuellen Routers.
- **Status**: Wählen Sie diese Option aus, um VRRP für das Gerät zu aktivieren.
- **Version**: Wählen Sie die Version von VRRP aus, die für diesen Router verwendet werden soll.
- **Besitzer der IP-Adresse**: Wenn **Ja** aktiviert ist, bedeutet dies, dass die IP-Adresse des Geräts der IP-Adresse des virtuellen Routers entspricht. Wählen Sie in der Liste **Verfügbare IP-Adresse** die IP-Adressen des Besitzers aus und verschieben Sie sie in die Liste **Besitzer der IP-Adresse**.

- Wenn **Nein** aktiviert ist, müssen Sie die Adressen des virtuellen Routers in das Feld **IP-Adresse des virtuellen Routers** eingeben. Wenn Sie hier mehrere IP-Adressen hinzufügen, trennen Sie sie wie folgt: 1.1.1.1, 2.2.2.2.
- **Quell-IP-Adresse**: Wählen Sie die IP-Adresse aus, die in VRRP-Nachrichten verwendet werden soll. Die standardmäßige Quell-IP-Adresse ist die niedrigste der für die Schnittstelle definierten IP-Adressen.
- **Priorität**: Wenn dieses Gerät der Besitzer ist, erhält dieses Feld den Wert 255, der nicht geändert werden kann. Geben Sie anderenfalls die Priorität des Geräts ein, die von seiner Eignung als Master abhängt. 100 ist der Standardwert für ein Gerät, das nicht Besitzer ist.
- **Vorrangmodus**: Wählen Sie „Wahr“ oder „Falsch“ aus, um den Vorrangmodus zu aktivieren bzw. zu deaktivieren, wie unter **Priorität und Vorrang bei VRRP-Routern** beschrieben.
- **Bekanntgabeintervall**: Geben Sie das unter **VRRP-Ankündigungen** beschriebene Bekanntgabeintervall ein.

  HINWEIS Wenn Sie diese Parameter ändern (**Bearbeiten**), wird der virtuelle Router geändert und es wird eine Nachricht mit den neuen Parametern gesendet.

SCHRITT 4 Zum Anzeigen weiterer Informationen zu einem virtuellen Router klicken Sie auf **Details**.

SCHRITT 5 Für den ausgewählten virtuellen Router werden die folgenden Felder angezeigt:

- **Schnittstelle**: Die Schicht-2-Schnittstelle (Port, LAG oder VLAN), für die der virtuelle Router definiert ist.
- **Kennung des virtuellen Routers**: Die Kennungsnummer des virtuellen Routers.
- **MAC-Adresse des virtuellen Routers**: Die virtuelle MAC-Adresse des virtuellen Routers.
- **Tabelle für IP-Adressen des virtuellen Routers**: Die diesem virtuellen Router zugeordneten IP-Adressen.
- **Beschreibung**: Der Name des virtuellen Routers.
- **Version**: Die Version des virtuellen Routers.
- **Status**: VRRP ist aktiviert.
- **Besitzer der IP-Adresse**: Der Besitzer der IP-Adresse des virtuellen Routers.
- **Master/Backup-Status**: Der virtuelle Router des Masters oder Backups.
- **Versatzzeit**: Die Zeit, die zur Berechnung des Masterdeaktivierungsintervalls verwendet wird.
- **Masterdeaktivierungsintervall**: Das Zeitintervall, gemäß dem das Backup den Master als „Deaktiviert“ erklärt.
- **Vorrangmodus**: Der Vorrangmodus ist aktiviert.

- **Eigene Parameter** des ausgewählten virtuellen Routers:
  - *Priorität*: Die Priorität des Geräts dieses virtuellen Routers, auf der Basis seiner Fähigkeit, als Master zu fungieren.
  - *Bekanntgabeintervall*: Das Zeitintervall, gemäß Beschreibung unter **VRRP-Ankündigungen**.
  - *Quell-IP-Adresse*: IP-Adresse, die in VRRP-Nachrichten verwendet werden soll.
- **Masterparameter** des Mastergeräts:
  - *Priorität*: 255
  - *Bekanntgabeintervall*: Das Zeitintervall, gemäß Beschreibung unter **VRRP-Ankündigungen**.
  - *Quell-IP-Adresse*: IP-Adresse, die in VRRP-Nachrichten verwendet werden soll.

VRRP-Statistik

So zeigen Sie die VRRP-Statistik an und löschen die Schnittstellenzähler:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv4-Verwaltung und Schnittstellen > VRRP > VRRP-Statistik**.

Die folgenden Felder werden für jede Schnittstelle angezeigt, auf der VRRP aktiviert ist:

- **Schnittstelle**: Zeigt die Schnittstelle an, auf der VRRP aktiviert ist.
- **Ungültige Prüfsumme**: Zeigt die Anzahl der Pakete mit ungültigen Prüfsummen an.
- **Ungültige Paketlänge**: Zeigt die Anzahl der Pakete mit ungültigen Paketlängen an.
- **Ungültige TTL**: Zeigt die Anzahl der Pakete mit ungültigen Werten für Time-to-live an.
- **Ungültiger VRRP-Pakettyp**: Zeigt die Anzahl der Pakete mit ungültigen VRRP-Pakettypen an.
- **Ungültige VRRP-ID**: Zeigt die Anzahl der Pakete mit ungültigen VRRP-IDs an.
- **Ungültige Protokoll-ID**: Zeigt die Anzahl der Pakete mit ungültigen Protokollnummern an.
- **Ungültige IP-Liste**: Zeigt die Anzahl der Pakete mit ungültigen IP-Listen an.
- **Ungültiges Intervall**: Zeigt die Anzahl der Pakete mit ungültigen Intervallen an.
- **Ungültige Authentifizierung**: Zeigt die Anzahl der Pakete an, bei denen die Authentifizierung fehlgeschlagen ist.

SCHRITT 2 Wählen Sie eine Schnittstelle aus.

SCHRITT 3 Klicken Sie auf **Schnittstellenzähler löschen**, um die Zähler für die angezeigte Schnittstelle zu löschen.

SCHRITT 4 Klicken Sie auf **Alle Schnittstellenzähler löschen**, um alle Zähler zu löschen.

22

Sicherheit

In diesem Abschnitt werden Sicherheit und Zugriffssteuerung für das Gerät beschrieben. Im System stehen verschiedene Arten von Sicherheitsmaßnahmen zur Verfügung.

In der folgenden Themenliste sind die verschiedenen Arten von Sicherheitsfunktionen aufgeführt, die in diesem Abschnitt beschrieben werden. Einige Funktionen werden bei mehr als einer Art von Sicherheitsmaßnahme oder Kontrolle verwendet, daher erscheinen sie in der Themenliste unten zweimal.

Die Berechtigung zur Verwaltung des Geräts wird in den folgenden Abschnitten beschrieben:

- **Definieren von Benutzern**
- **Konfigurieren von TACACS+**
- **Konfigurieren von RADIUS**
- **Verwaltungszugriffsmethode**
- **Verwaltungszugriffsauthentifizierung**
- **Schlüsselverwaltung**
- **Sicheres Verwalten sensibler Daten (SSD)**
- **SSL-Server**

Der Schutz vor Angriffen auf die CPU des Geräts wird in den folgenden Abschnitten beschrieben:

- **Konfigurieren von TCP-/UDP-Services**
- **Definieren der Sturmsteuerung**
- **Zugriffssteuerung**

Die Steuerung des Zugriffs von Endbenutzern auf das Netzwerk über das Gerät wird in den folgenden Abschnitten beschrieben:

- **Verwaltungszugriffsmethode**
- **Verwaltungszugriffsmethode**
- **Konfigurieren von TACACS+**

- Konfigurieren von RADIUS
- Konfigurieren der Portsicherheit
- 802.1X
- Zeitbereich

Der Schutz vor anderen Netzwerkbenutzern wird in den folgenden Abschnitten beschrieben. Dabei handelt es sich um Angriffe, die das Gerät passieren, aber nicht gegen es gerichtet sind.

- Denial of Service-Sicherung
- DHCP-Snooping
- SSL-Server
- Definieren der Sturmsteuerung
- Konfigurieren der Portsicherheit
- IP Source Guard
- ARP-Prüfung
- Zugriffssteuerung
- Sicherheit des ersten Hops

Definieren von Benutzern

Der Standardbenutzername und das Standardkennwort lauten **cisco/cisco**. Wenn Sie sich das erste Mal mit dem Standardbenutzernamen und dem Standardkennwort anmelden, werden Sie aufgefordert, ein neues Kennwort einzugeben. Die Kennwortkomplexität ist standardmäßig aktiviert. Wenn das ausgewählte Kennwort nicht komplex genug ist (die **Einstellungen für Kennwortkomplexität** können Sie auf der Seite „Kennwortsicherheit“ aktivieren), werden Sie aufgefordert, ein anderes Kennwort zu erstellen.

Einrichten von Benutzerkonten

Auf der Seite „Benutzerkonten“ können Sie weitere Benutzer eingeben, die berechtigt sind, auf das Gerät zuzugreifen (Lesezugriff oder Lese- und Schreibzugriff), oder die Kennwörter vorhandener Benutzer ändern.

Wenn Sie einen Benutzer der Ebene 15 (wie unten beschrieben) hinzugefügt haben, wird der Standardbenutzer aus dem System entfernt.

HINWEIS Sie können nicht alle Benutzer löschen. Wenn alle Benutzer ausgewählt sind, ist die Schaltfläche **Löschen** deaktiviert.

So fügen Sie einen neuen Benutzer hinzu:

SCHRITT 1 Klicken Sie auf **Administration** > **Benutzerkonten**.

Auf dieser Seite werden die im System definierten Benutzer und ihre Berechtigungsebene angezeigt.

SCHRITT 2 Wählen Sie **Kennwortwiederherstellungsservice** aus, um diese Funktion zu aktivieren. Wenn diese Funktion aktiviert ist, kann ein Endbenutzer mit physischem Zugriff auf den Konsolen-Port des Geräts das Startmenü aufrufen und den Kennwortwiederherstellungsprozess auslösen. Wenn der Systemstartprozess beendet ist, können Sie sich ohne Kennwortauthentifizierung bei dem Gerät anmelden. Das Aufrufen des Geräts ist nur über die Konsole möglich und nur, wenn die Konsole mit dem Gerät mit physischem Zugriff verbunden ist.

Wenn der Mechanismus für die Kennwortwiederherstellung deaktiviert ist, können Sie dennoch auf das Startmenü zugreifen und den Kennwortwiederherstellungsprozess auslösen. Der Unterschied besteht darin, dass in diesem Fall alle Konfigurations- und Benutzerdateien während des Systemstartprozesses entfernt werden und im Terminal eine entsprechende Protokollmeldung generiert wird.

SCHRITT 3 Klicken Sie auf **Hinzufügen**, um einen neuen Benutzer hinzuzufügen, oder auf **Bearbeiten**, um einen Benutzer zu ändern.

SCHRITT 4 Geben Sie die Parameter ein.

- **Benutzername**: Geben Sie einen neuen Benutzernamen ein, der aus 0 bis 20 Zeichen besteht. UTF-8-Zeichen sind nicht zulässig.
- **Kennwort**: Geben Sie ein Kennwort ein (UTF-8-Zeichen sind nicht zulässig). Wenn Kennwortsicherheit und -komplexität definiert sind, muss das Kennwort des Benutzers mit der in **Einrichten der Kennwortkomplexitätsregeln** konfigurierten Richtlinie übereinstimmen.
- **Kennwort bestätigen**: Geben Sie erneut das Kennwort ein.
- **Kennwortsicherheitsmessung**: Zur Bestimmung der Kennwortsicherheit. Die Richtlinie für die Kennwortsicherheit und -komplexität wird auf der Seite „Kennwortsicherheit“ konfiguriert.
- **Benutzerebene**: Wählen Sie die Berechtigungsebene des hinzuzufügenden bzw. zu bearbeitenden Benutzers aus.
  - *Schreibgeschützter CLI-Zugriff (1)*: Der Benutzer kann nicht auf die grafische Benutzeroberfläche zugreifen und hat nur Zugriff auf CLI-Befehle, mit denen die Gerätekonfiguration nicht geändert wird.
  - *CLI-Lesezugriff/eingeschränkter Schreibzugriff (7)*: Der Benutzer kann nicht auf die grafische Benutzeroberfläche zugreifen und hat nur Zugriff auf einige CLI-Befehle, mit denen die Gerätekonfiguration geändert wird. Weitere Informationen hierzu finden Sie im *CLI-Referenzhandbuch*.

- *Verwaltungs-Lese-/Schreibzugriff (15)*: Der Benutzer kann auf die grafische Benutzeroberfläche zugreifen und das Gerät konfigurieren.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Der Benutzer wird der aktuellen Konfigurationsdatei des Geräts hinzugefügt.

Einrichten der Kennwortkomplexitätsregeln

Kennwörter dienen zur Authentifizierung von Benutzern, die auf das Gerät zugreifen. Einfache Kennwörter stellen ein potenzielles Sicherheitsrisiko dar. Daher werden Anforderungen an die Kennwortkomplexität standardmäßig erzwungen und können nach Bedarf konfiguriert werden. Anforderungen an die Kennwortkomplexität werden auf der Seite **Kennwortsicherheit** konfiguriert, die Sie über das Dropdown-Menü „Sicherheit“ aufrufen können. Darüber hinaus können Sie auf dieser Seite eine Kennwortfälligkeitszeit konfigurieren.

So definieren Sie Kennwortkomplexitätsregeln:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Kennwortsicherheit**.

SCHRITT 2 Geben Sie die folgenden Parameter für die Fälligkeit von Kennwörtern ein:

- **Kennwortfälligkeit**: Wenn diese Option ausgewählt ist, wird der Benutzer aufgefordert, sein Kennwort zu ändern, wenn die **Kennwortfälligkeitszeit** abgelaufen ist.
- **Kennwortfälligkeitszeit**: Geben Sie ein, nach wie vielen Tagen ein Benutzer aufgefordert wird, sein Kennwort zu ändern.

HINWEIS Die Kennwortfälligkeit gilt auch für Kennwörter, die aus null Zeichen bestehen (kein Kennwort).

SCHRITT 3 Wählen Sie **Einstellungen für Kennwortkomplexität** aus, um die Komplexitätsregeln für Kennwörter zu aktivieren.

Wenn die Kennwortkomplexität aktiviert ist, müssen neue Kennwörter den folgenden Standardeinstellungen entsprechen:

- Sie müssen eine Mindestlänge von acht Zeichen haben.
- Sie müssen Zeichen aus mindestens drei Zeichenklassen enthalten (Großbuchstaben, Kleinbuchstaben, Zahlen und auf einer Standardtastatur verfügbare Sonderzeichen).
- Sie dürfen nicht mit dem aktuellen Kennwort identisch sein.
- Sie dürfen kein Zeichen enthalten, das öfter als dreimal hintereinander wiederholt wird.
- Sie dürfen den Benutzernamen oder eine durch Ändern der Groß-/Kleinschreibung erzielte Variante weder vorwärts noch rückwärts geschrieben enthalten.

- Sie dürfen den Herstellernamen oder eine durch Ändern der Groß-/Kleinschreibung erzielte Variante weder vorwärts noch rückwärts geschrieben enthalten.

SCHRITT 4 Wenn die **Einstellungen für Kennwortkomplexität** aktiviert sind, können die folgenden Parameter konfiguriert werden:

- **Kennwortmindestlänge**: Geben Sie die für Kennwörter erforderliche Mindestanzahl an Zeichen ein.

HINWEIS Ein Kennwort mit null Zeichen (kein Kennwort) ist zulässig und einem solchen Kennwort kann eine Kennwortfälligkeit zugewiesen sein.

- **Zulässige Zeichenwiederholungen**: Geben Sie an, wie oft sich ein Zeichen wiederholen darf.
- **Mindestanzahl an Zeichenklassen**: Geben Sie die Anzahl an Zeichen ein, die in einem Kennwort enthalten sein muss. Zeichenklassen bestehen aus Kleinbuchstaben (1), Großbuchstaben (2), Ziffern (3) und Symbolen oder Sonderzeichen (4).
- **Das neue Kennwort darf nicht mit dem aktuellen identisch sein**: Wenn diese Option ausgewählt ist, muss sich bei einer Kennwortänderung das neue Kennwort vom alten unterscheiden.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die Kennworteinstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

HINWEIS Sie können die CLI zum Konfigurieren der Übereinstimmung von Benutzername und Kennwort sowie der Übereinstimmung von Hersteller und Kennwort verwenden. Weitere Anweisungen hierzu finden Sie im *CLI-Referenzhandbuch*.

Konfigurieren von TACACS+

Eine Organisation kann über einen TACACS+-Server (*Terminal Access Controller Access Control System*) zentralisierte Sicherheitsfunktionen für alle Geräte bereitstellen. So können Authentifizierung und Autorisierung für alle Geräte in der Organisation auf einem Server verarbeitet werden.

Das Gerät kann als TACACS+-Client fungieren, der den TACACS+-Server für die folgenden Services nutzt:

- **Authentifizierung**: Stellt die Authentifizierung für Benutzer bereit, die sich mit Benutzernamen und benutzerdefinierten Kennwörtern beim Gerät anmelden.
- **Autorisierung**: Wird bei der Anmeldung durchgeführt. Nachdem die Authentifizierungssitzung abgeschlossen ist, wird mit dem authentifizierten Benutzernamen eine Autorisierungssitzung gestartet. Der TACACS+-Server überprüft dann die Benutzerrechte.
- **Abrechnung**: Ermöglicht die Abrechnung von Anmeldesitzungen über den TACACS+-Server. So kann ein Systemadministrator über den TACACS+-Server Abrechnungsberichte generieren.

Neben der Bereitstellung von Authentifizierungs- und Autorisierungsservices können mit dem TACACS+-Protokoll verschlüsselte TACACS-Nachrichten generiert werden.

TACACS+ wird nur von IPv4 unterstützt.

Einige TACACS+-Server unterstützen eine einzelne Verbindung, mit der das Gerät alle Informationen über eine einzige Verbindung empfangen kann. Wenn der TACACS+-Server dies nicht unterstützt, kehrt das Gerät zu mehreren Verbindungen zurück.

Abrechnung über einen TACACS+-Server

Der Benutzer kann die Abrechnung von Anmeldesitzungen entweder über einen RADIUS- oder über einen TACACS+-Server aktivieren.

Für die Abrechnung über einen TACACS+-Server wird derselbe benutzerkonfigurierbare TCP-Port verwendet wie für die Authentifizierung und Autorisierung über einen TACACS+-Server.

Die folgenden Informationen werden vom Gerät an den TACACS+-Server gesendet, wenn sich ein Benutzer an- oder abmeldet:

Table 6:

Argument	Beschreibung	In Startnachricht	In Stoppnachricht
task_id	Eine eindeutige ID der Abrechnungssitzung.	Ja	Ja
Benutzer	Eingegebener Benutzername für die Authentifizierung der Anmeldung.	Ja	Ja
rem-addr	IP-Adresse des Benutzers.	Ja	Ja
elapsed-time	Zeigt an, wie lange der Benutzer angemeldet war.	Nein	Ja
reason	Gibt an, warum die Sitzung beendet wurde.	Nein	Ja

Standardeinstellungen

Die folgenden Standardeinstellungen sind für diese Funktion relevant:

- Standardmäßig ist kein TACACS+-Server konfiguriert.
- Wenn Sie einen TACACS+-Server konfigurieren, ist die Abrechnungsfunktion standardmäßig deaktiviert.

Interaktionen mit anderen Funktionen

Die Abrechnungsfunktion kann nicht gleichzeitig auf einem RADIUS- und einem TACACS+-Server aktiviert werden.

Workflow

Gehen Sie wie folgt vor, um einen TACACS+-Server zu verwenden:

SCHRITT 1 Erstellen Sie ein Konto für einen Benutzer auf dem TACACS+-Server.

SCHRITT 2 Konfigurieren Sie diesen Server zusammen mit den anderen Parametern auf den Seiten „TACACS+“ und „TACACS+-Server hinzufügen“.

SCHRITT 3 Wählen Sie auf der Seite „Verwaltungszugriffsauthentifizierung“ die Option **TACACS+**, sodass die Anmeldung eines Benutzers beim Gerät auf dem TACACS+-Server statt in der lokalen Datenbank authentifiziert wird.

HINWEIS Wenn mehrere TACACS+-Server konfiguriert wurden, wählt das Gerät den zu verwendenden TACACS+-Server anhand der konfigurierten Prioritäten der verfügbaren TACACS+-Server aus.

Konfigurieren eines TACACS+-Servers

Auf der Seite „TACACS+“ können Sie TACACS+-Server konfigurieren.

Nur Benutzer mit Berechtigungsebene 15 auf dem TACACS+-Server können das Gerät verwalten. Berechtigungsebene 15 erteilen Sie Benutzern oder Benutzergruppen auf dem TACACS+-Server mit der folgenden Zeichenfolge in der Benutzer- oder Gruppendefinition:

```
service = exec {
priv-lvl = 15
}
```

So konfigurieren Sie TACACS+-Serverparameter:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **TACACS+**.

SCHRITT 2 Aktivieren Sie bei Bedarf die **TACACS+-Abrechnung**. Weitere Informationen finden Sie in Abschnitt **Abrechnung über einen TACACS+-Server**.

SCHRITT 3 Geben Sie die folgenden Standardparameter ein:

- **Schlüsselzeichenfolge**: Geben Sie die standardmäßige **Schlüsselzeichenfolge** ein, die für die Kommunikation mit allen TACACS+-Servern im Modus **Verschlüsselt** oder **Unverschlüsselt** verwendet wird. Das Gerät kann so konfiguriert werden, dass entweder dieser Schlüssel oder ein für einen bestimmten Server eingegebener Schlüssel verwendet wird (dieser wird auf der Seite „TACACS+-Server hinzufügen“ eingegeben).

Wenn Sie keine Schlüsselzeichenfolge in dieses Feld eingeben, muss der auf der Seite „TACACS+-Server hinzufügen“ eingegebene Schlüssel mit dem vom TACACS+-Server verwendeten Verschlüsselungsschlüssel übereinstimmen.

Wenn Sie hier eine Schlüsselzeichenfolge und gleichzeitig eine Schlüsselzeichenfolge für einen einzelnen TACACS+-Server eingeben, dann hat die für den einzelnen TACACS+-Server konfigurierte Schlüsselzeichenfolge Vorrang.

- **Timeout für Antwort**: Geben Sie den Zeitraum ein, der verstreichen soll, bevor die Zeit für die Verbindung zwischen dem Gerät und dem TACACS+-Server überschritten ist. Wenn Sie auf der Seite „TACACS+-Server hinzufügen“ für einen bestimmten Server keinen Wert eingeben, wird der Wert aus diesem Feld übernommen.
- **Quell-IPv4-Schnittstelle**: Wählen Sie die Quell-IPv4-Schnittstelle des Geräts aus, die in Nachrichten im Rahmen der Kommunikation mit dem TACACS+-Server verwendet werden soll.
- **Quell-IPv6-Schnittstelle**: Wählen Sie die Quell-IPv6-Schnittstelle des Geräts aus, die in Nachrichten im Rahmen der Kommunikation mit dem TACACS+-Server verwendet werden soll.

  HINWEIS Wenn Sie die Option „Auto“ auswählen, übernimmt das System die Quell-IP-Adresse aus der IP-Adresse, die auf der ausgehenden Schnittstelle definiert wurde.

  SCHRITT 4 Klicken Sie auf **Übernehmen**. Die TACACS+-Standardeinstellungen werden der aktuellen Konfigurationsdatei hinzugefügt. Diese werden verwendet, wenn die entsprechenden Parameter nicht auf der Seite „Hinzufügen“ definiert werden.

  SCHRITT 5 Zum Hinzufügen eines TACACS+-Servers klicken Sie auf **Hinzufügen**.

  SCHRITT 6 Geben Sie die Parameter ein.

- **Serverdefinition**: Wählen Sie eine der folgenden Methoden zum Identifizieren des TACACS+-Servers:
  - *Nach IP-Adresse*: Wenn Sie diese Option ausgewählt haben, geben Sie in das Feld **Server-IP-Adresse/Name** die IP-Adresse des Servers ein.
  - *Nach Name*: Wenn Sie diese Option ausgewählt haben, geben Sie in das Feld **IP-Adresse/Name des Servers** den Namen des Servers ein.
- **IP-Version**: Wählen Sie die IP-Version, die die Quell-Adresse unterstützt: IPv6 oder IPv4.
- **IPv6-Adresstyp**: Wählen Sie den IPv6-Adresstyp aus (falls IPv6 verwendet wird). Folgende Optionen sind möglich:
  - *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.

  - *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.

- **Link Local-Schnittstelle**: Wählen Sie in der Liste die Link Local-Schnittstelle aus (falls der IPv6-Adresstyp „Link Local“ ausgewählt ist).
- **Server-IP-Adresse/Name**: Geben Sie die IP-Adresse oder den Namen des TACACS+-Servers ein.
- **Priorität**: Geben Sie die Rangfolge für die Verwendung dieses TACACS+-Servers ein. Der Server mit der Priorität Null ist der TACACS+-Server mit der höchsten Priorität und wird als Erster verwendet. Wenn das Gerät keine Sitzung mit dem Server hoher Priorität aufbauen kann, versucht es dies beim Server mit der nächstniedrigeren Priorität.
- **Schlüsselzeichenfolge**: Geben Sie die Standardschlüsselzeichenfolge ein, die zur Authentifizierung und Verschlüsselung zwischen dem Gerät und dem TACACS+-Server verwendet wird. Der Schlüssel muss mit dem auf dem TACACS+-Server konfigurierten Schlüssel übereinstimmen.

  Eine Schlüsselzeichenfolge wird verwendet, um den Datenaustausch unter Verwendung von MD5 zu verschlüsseln. Sie können den Standardschlüssel auf dem Gerät auswählen oder den Schlüssel **verschlüsselt** oder **unverschlüsselt** eingeben. Wenn Sie keine verschlüsselte Schlüsselzeichenfolge (von einem anderen Gerät) haben, geben Sie die Schlüsselzeichenfolge im unverschlüsselten Modus ein und klicken Sie auf **Übernehmen**. Die verschlüsselte Schlüsselzeichenfolge wird generiert und angezeigt.

  Wenn Sie einen Schlüssel eingeben, wird dadurch die Standardschlüsselzeichenfolge überschrieben, sofern diese auf der Hauptseite für das Gerät definiert wurde.
- **Timeout für Antwort**: Wählen Sie **Benutzerdefiniert** aus und geben Sie den Zeitraum ein, der verstreichen soll, bevor die Zeit für die Verbindung zwischen dem Gerät und dem TACACS+-Server überschritten ist. Wählen Sie **Standard verwenden**, um den auf der Seite angezeigten Standardwert zu verwenden.
- **Authentifizierungs-IP-Port**: Geben Sie die Nummer des Ports ein, über den die TACACS+-Sitzung stattfindet.
- **Einzelne Verbindung**: Wählen Sie diese Option aus, um alle Informationen in einer einzigen Verbindung zu empfangen. Wenn der TACACS+-Server dies nicht unterstützt, kehrt das Gerät zu mehreren Verbindungen zurück.

SCHRITT 7 Klicken Sie auf **Übernehmen**. Der TACACS+-Server wird der aktuellen Konfigurationsdatei des Geräts hinzugefügt.

SCHRITT 8 Zum Anzeigen sensibler Daten in unverschlüsselter Form auf dieser Seite klicken Sie auf **Sensible Daten unverschlüsselt anzeigen**.

Konfigurieren von RADIUS

RADIUS-Server (Remote Authorization Dial-In User Service) bieten zentralisierte 802.1X- oder MAC-basierte Netzwerkzugriffssteuerung. Das Gerät ist ein RADIUS-Client, der einen RADIUS-Server verwenden kann, um zentralisierte Sicherheitsfunktionen bereitzustellen.

Eine Organisation kann über einen RADIUS-Server (Remote Authorization Dial-In User Service) zentralisierte 802.1X- oder MAC-basierte Netzwerkzugriffssteuerung für alle Geräte bereitstellen. So können Authentifizierung und Autorisierung für alle Geräte in der Organisation auf einem Server verarbeitet werden.

Das Gerät kann als RADIUS-Client fungieren, der den RADIUS-Server für die folgenden Services nutzt:

- **Authentifizierung**: Stellt die Authentifizierung für normale und 802.1X-Benutzer bereit, die sich mit Benutzernamen und benutzerdefinierten Kennwörtern beim Gerät anmelden.
- **Autorisierung**: Wird bei der Anmeldung durchgeführt. Nachdem die Authentifizierungssitzung abgeschlossen ist, wird mit dem authentifizierten Benutzernamen eine Autorisierungssitzung gestartet. Der RADIUS-Server überprüft dann die Benutzerrechte.
- **Abrechnung**: Ermöglicht die Abrechnung von Anmeldesitzungen über den RADIUS-Server. So kann ein Systemadministrator über den RADIUS-Server Abrechnungsberichte generieren.

Abrechnung über einen RADIUS-Server

Der Benutzer kann die Abrechnung von Anmeldesitzungen über einen RADIUS-Server aktivieren.

Für die Abrechnung über einen RADIUS-Server wird derselbe benutzerkonfigurierbare TCP-Port verwendet wie für die Authentifizierung und Autorisierung über einen RADIUS-Server.

Standardeinstellungen

Die folgenden Standardeinstellungen sind für diese Funktion relevant:

- Standardmäßig ist kein RADIUS-Server konfiguriert.
- Wenn Sie einen RADIUS-Server konfigurieren, ist die Abrechnungsfunktion standardmäßig deaktiviert.

Interaktionen mit anderen Funktionen

Die Abrechnungsfunktion kann nicht gleichzeitig auf einem RADIUS- und einem TACACS+-Server aktiviert werden.

RADIUS-Workflow

Gehen Sie wie folgt vor, um einen RADIUS-Server zu verwenden:

SCHRITT 1 Erstellen Sie ein Konto für das Gerät auf dem RADIUS-Server.

SCHRITT 2 Konfigurieren Sie diesen Server zusammen mit den anderen Parametern auf den Seiten „RADIUS“ und „RADIUS-Server hinzufügen“.

HINWEIS Wenn mehrere RADIUS-Server konfiguriert wurden, wählt das Gerät den zu verwendenden RADIUS-Server anhand der konfigurierten Prioritäten der verfügbaren RADIUS-Server aus.

So legen Sie die RADIUS-Serverparameter fest:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **RADIUS**.

SCHRITT 2 Geben Sie die RADIUS-Abrechnungsoption ein. Folgende Optionen stehen zur Verfügung:

- **Portbasierte Zugriffssteuerung (802.1X, MAC-basiert, Web-Authentifizierung)**: Gibt an, dass der RADIUS-Server für die 802.1x-Port-Abrechnung verwendet wird. Die webbasierte Authentifizierung wird auf Sx300- und SG500-Geräten nur im Schicht-2-Modus unterstützt. Auf SG500XG- und SG500X-Geräten wird sie im nativen Modus sowie im Modus „Erweitertes Hybrid XG“ unterstützt.
- **Verwaltungszugriff**: Gibt an, dass der RADIUS-Server für die Abrechnung im Zusammenhang mit Benutzeranmeldungen verwendet wird.
- **Portbasierte Zugriffssteuerung und Verwaltungszugriff**: Gibt an, dass der RADIUS-Server für die Abrechnung im Zusammenhang mit Benutzeranmeldungen sowie für die 802.1x-Portabrechnung verwendet wird.
- **Keine**: Gibt an, dass der RADIUS-Server nicht für die Abrechnung verwendet wird.

SCHRITT 3 Geben Sie bei Bedarf die RADIUS-Standardparameter ein. Die unter „Standardparameter“ eingegebenen Werte werden auf alle Server angewendet. Wenn Sie für einen bestimmten Server (auf der Seite „RADIUS-Server hinzufügen“) keinen Wert eingeben, werden die Werte aus diesen Feldern übernommen.

- **Wiederholungen**: Geben Sie die Anzahl übermittelter Anfragen an, die an den RADIUS-Server gesendet werden sollen, bevor angenommen wird, dass ein Fehler aufgetreten ist.
- **Timeout für Antwort**: Geben Sie die Zeit in Sekunden ein, die das Gerät auf eine Antwort vom RADIUS-Server warten soll, bevor es die Abfrage erneut startet oder zum nächsten Server umschaltet.

- **Stillstandszeit**: Geben Sie die Zeit in Minuten ein, die verstreichen soll, bevor ein nicht antwortender RADIUS-Server bei Serviceanforderungen umgangen wird. Wenn der Wert 0 ist, wird der Server nicht umgangen.
- **Schlüsselzeichenfolge**: Geben Sie die Standardschlüsselzeichenfolge ein, die zur Authentifizierung und Verschlüsselung zwischen dem Gerät und dem RADIUS-Server verwendet wird. Der Schlüssel muss mit dem auf dem RADIUS-Server konfigurierten Schlüssel übereinstimmen. Eine Schlüsselzeichenfolge wird verwendet, um den Datenaustausch unter Verwendung von MD5 zu verschlüsseln. Sie können den Schlüssel in **verschlüsselter** oder **unverschlüsselter** Form eingeben. Wenn Sie keine verschlüsselte Schlüsselzeichenfolge (von einem anderen Gerät) haben, geben Sie die Schlüsselzeichenfolge im unverschlüsselten Modus ein und klicken Sie auf **Übernehmen**. Die verschlüsselte Schlüsselzeichenfolge wird generiert und angezeigt.

Damit wird gegebenenfalls eine definierte Standardschlüsselzeichenfolge außer Kraft gesetzt.

- **Quell-IPv4-Schnittstelle**: Wählen Sie die Quell-IPv4-Schnittstelle des Geräts aus, die in Nachrichten im Rahmen der Kommunikation mit dem RADIUS-Server verwendet werden soll.
- **Quell-IPv6-Schnittstelle**: Wählen Sie die Quell-IPv6-Schnittstelle des Geräts aus, die in Nachrichten im Rahmen der Kommunikation mit dem RADIUS-Server verwendet werden soll.

HINWEIS Wenn Sie die Option „Auto“ auswählen, übernimmt das System die Quell-IP-Adresse aus der IP-Adresse, die auf der ausgehenden Schnittstelle definiert wurde.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die RADIUS-Standardeinstellungen für das Gerät werden in der aktuellen Konfigurationsdatei aktualisiert.

Zum Hinzufügen eines RADIUS-Servers klicken Sie auf **Hinzufügen**.

SCHRITT 5 Geben Sie die Werte in die Felder für die einzelnen RADIUS-Server ein. Um die auf der Seite „RADIUS“ eingegebenen Standardwerte zu verwenden, wählen Sie **Standard verwenden** aus.

- **Serverdefinition**: Wählen Sie aus, ob der RADIUS-Server anhand der IP-Adresse oder des Namens angegeben wird.
- **IP-Version**: Wählen Sie die Version der IP-Adresse des RADIUS-Servers aus.
- **IPv6-Adresstyp**: Wählen Sie den IPv6-Adresstyp aus (falls IPv6 verwendet wird). Folgende Optionen sind möglich:
  - *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
  - *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.

- **Link Local-Schnittstelle**: Wählen Sie in der Liste die Link Local-Schnittstelle aus (falls der IPv6-Adresstyp „Link Local“ ausgewählt ist).
- **Server-IP-Adresse/Name**: Geben Sie IP-Adresse oder Name des RADIUS-Servers ein.
- **Priorität**: Geben Sie die Priorität des Servers ein. Die Priorität bestimmt die Reihenfolge, in der die Server bei der Authentifizierung eines Benutzers vom Gerät kontaktiert werden. Der RADIUS-Server mit der höchsten Priorität wird vom Gerät zuerst kontaktiert. Null ist die höchste Priorität.

  Schlüsselzeichenfolge: Geben Sie die Schlüsselzeichenfolge ein, die zur Authentifizierung und Verschlüsselung der Kommunikation zwischen dem Gerät und dem RADIUS-Server verwendet wird. Der Schlüssel muss mit dem auf dem RADIUS-Server konfigurierten Schlüssel übereinstimmen. Sie können ihn **verschlüsselt** oder **unverschlüsselt** eingeben. Wenn **Standard verwenden** ausgewählt ist, versucht das Gerät, sich mit der Standardschlüsselzeichenfolge gegenüber dem RADIUS-Server zu authentifizieren.
- **Timeout für Antwort**: Wählen Sie **Benutzerdefiniert** aus und geben Sie ein, wie viele Sekunden lang das Gerät auf eine Antwort vom RADIUS-Server wartet, bevor es die Abfrage wiederholt oder (falls die maximale Anzahl der Wiederholungen erreicht ist) zum nächsten Server wechselt. Wenn **Standard verwenden** ausgewählt ist, verwendet das Gerät den Standard-Timeout-Wert.
- **Authentifizierungsport**: Geben Sie die UDP-Portnummer des RADIUS-Servers für Authentifizierungsanforderungen ein.
- **Abrechnungsport**: Geben Sie die UDP-Portnummer des RADIUS-Servers für Abrechnungsanforderungen ein.
- **Wiederholungen**: Wählen Sie **Benutzerdefiniert** aus und geben Sie die Anzahl der Anfragen ein, die an den RADIUS-Server gesendet werden sollen, bevor angenommen wird, dass ein Fehler aufgetreten ist. Wenn **Standard verwenden** ausgewählt ist, verwendet das Gerät den Standardwert für die Anzahl der Wiederholungen.
- **Stillstandszeit**: Wählen Sie **Benutzerdefiniert** aus und geben Sie die Zeit in Minuten ein, die verstreichen soll, bevor ein nicht antwortender RADIUS-Server bei Serviceanforderungen umgangen wird. Wenn **Standard verwenden** ausgewählt ist, verwendet das Gerät den Standardwert für die Stillstandszeit. Wenn Sie 0 Minuten eingeben, gibt es keine Stillstandszeit.
- **Verwendungstyp**: Geben Sie den Authentifizierungstyp des RADIUS-Servers ein. Folgende Optionen sind möglich:
  - *Anmeldung*: Der RADIUS-Server wird zur Authentifizierung von Benutzern verwendet, die das Gerät verwalten möchten.
  - *802.1X*: Der RADIUS-Server wird zur 802.1X-Authentifizierung verwendet.
  - *Alle*: Der RADIUS-Server wird zur Authentifizierung von Benutzern verwendet, die das Gerät verwalten möchten, sowie zur 802.1X-Authentifizierung.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die RADIUS-Serverdefinition wird der aktuellen Konfigurationsdatei des Geräts hinzugefügt.

SCHRITT 7 Zum Anzeigen sensibler Daten in unverschlüsselter Form auf der Seite klicken Sie auf **Sensible Daten unverschlüsselt anzeigen**.

Schlüsselverwaltung

Schlüsselverwaltung

HINWEIS Diese Funktion ist nur für SG500X/ESW2-550X/500X-Geräte relevant.

In diesem Abschnitt wird beschrieben, wie Sie Schlüsselketten für Anwendungen und Protokolle wie beispielsweise RIP konfigurieren. Unter **RIP-Authentifizierung** wird beschrieben, wie die Schlüsselkette von RIP für die Authentifizierung verwendet wird.

Zum Erstellen einer Schlüsselkette führen Sie die folgenden Schritte aus:

SCHRITT 1 Erstellen Sie auf der Seite „Schlüsselketteneinstellungen“ eine Schlüsselkette mit einem einzigen Schlüssel.

SCHRITT 2 Fügen Sie auf der Seite „Schlüsseleinstellungen“ weitere Schlüssel hinzu.

Erstellen einer Schlüsselkette

Auf der Seite „Schlüsselketteneinstellungen“ können Sie eine neue Schlüsselkette erstellen.

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Schlüsselverwaltung** > **Schlüsselketteneinstellungen**.

SCHRITT 2 Klicken Sie zum Hinzufügen einer neuen Schlüsselkette auf **Hinzufügen**, um die Seite „Schlüsselkette hinzufügen“ zu öffnen, und geben Sie Werte in die folgenden Felder ein:

- **Schlüsselkette**: Name für die Schlüsselkette.
- **Schlüsselkennung**: Aus Ganzzahlen bestehende Kennung für die Schlüsselkette.
- **Schlüsselzeichenfolge**: Wert der Schlüsselzeichenfolge. Wählen Sie eine der folgenden Optionen aus:
  - *Benutzerdefiniert (verschlüsselt)*: Geben Sie eine verschlüsselte Version ein.

- *Benutzerdefiniert (unverschlüsselt)*: Geben Sie eine unverschlüsselte Version ein.

HINWEIS Sie können Werte für **Lebensdauer für Paketempfang** und **Lebensdauer für Paket senden** eingeben. „Lebensdauer für Paketempfang“ gibt an, wann die Schlüsselkennung für das Empfangen von Paketen gültig ist. „Lebensdauer für Paket senden“ gibt an, wann die Schlüsselkennung für das Senden von Paketen gültig ist.

- **Lebensdauer für Paketempfang/Lebensdauer für Paket senden**: Gibt an, wann Pakete mit diesem Schlüssel akzeptiert werden. Wählen Sie eine der folgenden Optionen:
  - *Immer gültig*: Die Lebensdauer der Schlüsselkennung ist nicht begrenzt.
  - *Benutzerdefiniert*: Die Lebensdauer der Schlüsselkette ist begrenzt. Wenn Sie diese Option auswählen, geben Sie Werte in die folgenden Felder ein.

    HINWEIS Wenn Sie „Benutzerdefiniert“ ausgewählt haben, muss die Systemzeit manuell oder über SNTP festgelegt werden. Anderenfalls treten bei „Lebensdauer für Paketempfang“ und „Lebensdauer für Paket senden“ immer Fehler auf.

Die folgenden Felder sind für die Felder „Lebensdauer für Paketempfang“ und „Lebensdauer für Paket senden“ relevant:

- **Anfangsdatum**: Geben Sie das Datum ein, ab dem die Schlüsselkennung gültig ist.
- **Startzeit**: Geben Sie die Uhrzeit ein, ab der die Schlüsselkennung am Anfangsdatum gültig ist.
- **Endzeit**: Geben Sie das Datum ein, bis zu dem die Schlüsselkennung gültig ist. Wählen Sie eine der folgenden Optionen:
  - *Unbegrenzt*: Die Lebensdauer der Schlüsselkennung ist nicht begrenzt.
  - *Dauer*. Die Lebensdauer der Schlüsselkennung ist begrenzt. Wenn Sie diese Option auswählen, geben Sie Werte in die folgenden Felder ein.
- **Dauer**: Die Dauer des Zeitraums, in dem die Schlüsselkennung gültig ist. Geben Sie Werte für die folgenden Felder ein:
  - *Tage*: Die Anzahl der Tage, an denen die Schlüsselkennung gültig ist.
  - *Stunden*: Die Anzahl der Stunden, in denen die Schlüsselkennung gültig ist.
  - *Minuten*: Die Anzahl der Minuten, in denen die Schlüsselkennung gültig ist.
  - *Sekunden*: Die Anzahl der Sekunden, in denen die Schlüsselkennung gültig ist.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Einstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Erstellen von Schlüsseleinstellungen

Auf der Seite „Schlüsselketteneinstellungen“ können Sie einer bereits vorhandenen Schlüsselkette einen Schlüssel hinzufügen.

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Schlüsselverwaltung** > **Schlüsseleinstellungen**.

SCHRITT 2 Klicken Sie zum Hinzufügen einer neuen Schlüsselzeichenfolge auf **Hinzufügen**.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **Schlüsselkette**: Name für die Schlüsselkette.
- **Schlüsselkennung**: Aus Ganzzahlen bestehende Kennung für die Schlüsselkette.
- **Schlüsselzeichenfolge**: Wert der Schlüsselzeichenfolge. Wählen Sie eine der folgenden Optionen aus:
  - *Benutzerdefiniert (verschlüsselt)*: Geben Sie eine verschlüsselte Version ein.
  - *Benutzerdefiniert (unverschlüsselt)*: Geben Sie eine unverschlüsselte Version ein.

  HINWEIS Sie können Werte für **Lebensdauer für Paketempfang** und **Lebensdauer für Paket senden** eingeben. **Lebensdauer für Paketempfang** gibt an, wann die Schlüsselkennung für das Empfangen von Paketen gültig ist. **Lebensdauer für Paket senden** gibt an, wann die Schlüsselkette für das Senden von Paketen gültig ist. Die Felder werden nur für **Lebensdauer für Paketempfang** beschrieben. Die Felder für **Lebensdauer für Paket senden** sind identisch.
- **Lebensdauer für Paketempfang**: Gibt an, wann Pakete mit diesem Schlüssel akzeptiert werden. Wählen Sie eine der folgenden Optionen:
  - *Immer gültig*: Die Lebensdauer der Schlüsselkennung ist nicht begrenzt.
  - *Benutzerdefiniert*: Die Lebensdauer der Schlüsselkette ist begrenzt. Wenn Sie diese Option auswählen, geben Sie Werte in die folgenden Felder ein.
- **Anfangsdatum**: Geben Sie das Datum ein, ab dem die Schlüsselkennung gültig ist.
- **Startzeit**: Geben Sie die Uhrzeit ein, ab der die Schlüsselkennung am Anfangsdatum gültig ist.
- **Endzeit**: Geben Sie das Datum ein, bis zu dem die Schlüsselkennung gültig ist. Wählen Sie eine der folgenden Optionen:
  - *Unbegrenzt*: Die Lebensdauer der Schlüsselkennung ist nicht begrenzt.
  - *Dauer*. Die Lebensdauer der Schlüsselkennung ist begrenzt. Wenn Sie diese Option auswählen, geben Sie Werte in die folgenden Felder ein.

- **Dauer**: Die Dauer des Zeitraums, in dem die Schlüsselkennung gültig ist. Geben Sie Werte für die folgenden Felder ein:
  - *Tage*: Die Anzahl der Tage, an denen die Schlüsselkennung gültig ist.
  - *Stunden*: Die Anzahl der Stunden, in denen die Schlüsselkennung gültig ist.
  - *Minuten*: Die Anzahl der Minuten, in denen die Schlüsselkennung gültig ist.
  - *Sekunden*: Die Anzahl der Sekunden, in denen die Schlüsselkennung gültig ist.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Einstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

SCHRITT 5 Wenn sensible Daten immer unverschlüsselt (als Klartext) angezeigt werden sollen, klicken Sie auf **Sensible Daten unverschlüsselt anzeigen**.

Verwaltungszugriffsmethode

Zugriffsprofile bestimmen, wie Benutzer, die über verschiedene Zugriffsmethoden auf das Gerät zugreifen, authentifiziert und autorisiert werden. Mithilfe von Zugriffsprofilen kann der Verwaltungszugriff von bestimmten Quellen begrenzt werden.

Nur Benutzer, die beide Methoden (d. h. sowohl die Authentifizierung durch das aktive Zugriffsprofil als auch die Verwaltungszugriffsauthentifizierung) erfolgreich durchlaufen, erhalten Verwaltungszugriff auf das Gerät.

Für das Gerät kann nur jeweils ein einziges Zugriffsprofil aktiv sein.

Zugriffsprofile bestehen aus einer oder mehreren Regeln. Die Regeln werden in der Reihenfolge ihrer Priorität innerhalb des Zugriffsprofils (von oben nach unten) angewendet.

Regeln bestehen aus Filtern, die die folgenden Elemente umfassen:

- **Zugriffsmethoden**: Methoden für den Zugriff auf das Gerät und dessen Verwaltung.
  - Telnet
  - Sicheres Telnet (SSH)
  - Hypertext Transfer Protocol (HTTP)
  - Sicheres HTTP (HTTPS)
  - Simple Network Management Protocol (SNMP)
  - Alle obigen
- **Aktion**: Zugriff auf eine Schnittstelle oder Quelladresse zulassen oder verweigern.

- **Schnittstelle**: Ports, LAGs oder VLANs, denen der Zugriff auf das webbasierte Konfigurationsdienstprogramm gewährt oder verweigert wird.
- **Quell-IP-Adresse**: IP-Adressen oder Subnetze. Der Zugriff auf Verwaltungsmethoden kann sich zwischen den Benutzergruppen unterscheiden. Beispielsweise ist es möglich, dass eine Benutzergruppe Zugriff auf das Gerätemodul nur über eine HTTPS-Sitzung erhalten kann, während eine andere Benutzergruppe sowohl über HTTPS- als auch über Telnet-Sitzungen auf das Gerätemodul zugreifen kann.

Aktives Zugriffsprofil

Auf der Seite „Zugriffsprofile“ werden die definierten Zugriffsprofile angezeigt und Sie können ein Zugriffsprofil als aktives Zugriffsprofil auswählen.

Wenn ein Benutzer über eine Zugriffsmethode auf das Gerät zuzugreifen versucht, prüft das Gerät, ob das aktive Zugriffsprofil den Verwaltungszugriff auf das Gerät mit dieser Methode ausdrücklich zulässt. Wenn keine Übereinstimmung gefunden wird, wird der Zugriff verweigert.

Wenn ein Versuch, auf das Gerät zuzugreifen, das aktive Zugriffsprofil verletzt, gibt das Gerät eine SYSLOG-Meldung aus, um den Systemadministrator über den Versuch zu benachrichtigen.

Wenn ein Nur-Konsole-Zugriffsprofil aktiviert wurde, kann es nur über eine direkte Verbindung von der Verwaltungsstation zum physischen Konsolen-Port am Gerät deaktiviert werden.

Weitere Informationen finden Sie unter **Definieren von Profilregeln**.

Verwenden Sie die Seite „Zugriffsprofile“, um ein Zugriffsprofil zu erstellen und die erste Regel hinzuzufügen. Wenn das Zugriffsprofil nur eine einzige Regel enthält, sind keine weiteren Schritte erforderlich. Auf der Seite „Profilregeln“ können Sie dem Profil zusätzliche Regeln hinzufügen.

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Verwaltungszugriffsmethode** > **Zugriffsprofile**.

Auf dieser Seite werden alle aktiven und inaktiven Zugriffsprofile angezeigt.

SCHRITT 2 Wenn Sie das aktive Zugriffsprofil ändern möchten, wählen Sie aus dem Dropdown-Menü **Aktives Zugriffsprofil** ein Profil aus, und klicken Sie auf **Übernehmen**. Dadurch wird das ausgewählte Profil zum aktiven Zugriffsprofil.

HINWEIS Ein Vorsichtshinweis wird angezeigt, wenn Sie „Nur Konsole“ ausgewählt haben. Wenn Sie fortfahren, wird Ihre Verbindung mit dem webbasierten Konfigurationsdienstprogramm sofort getrennt, und Sie können nur noch über den Konsolenport auf das Gerät zugreifen. Dies gilt nur für Gerätetypen mit Konsolen-Port.

Ein Vorsichtshinweis wird angezeigt, wenn Sie ein beliebiges anderes Zugriffsprofil ausgewählt haben. Sie werden gewarnt, dass Ihre Verbindung zum webbasierten Konfigurationsdienstprogramm u. U. getrennt wird (abhängig vom ausgewählten Zugriffsprofil).

SCHRITT 3 Klicken Sie auf **OK**, um das aktive Zugriffsprofil auszuwählen, oder klicken Sie auf **Abbrechen**, um die Aktion abzubrechen.

SCHRITT 4 Klicken Sie auf **Hinzufügen**, um die Seite „Zugriffsprofil hinzufügen“ zu öffnen. Auf dieser Seite können Sie ein neues Profil und eine Regel konfigurieren.

SCHRITT 5 Geben Sie den Wert für **Zugriffsprofilname** ein. Der Name darf aus maximal 32 Zeichen bestehen.

SCHRITT 6 Geben Sie die Parameter ein.

- **Regelpriorität**: Geben Sie die Regelpriorität ein. Wenn ein Paket mit einer Regel abgeglichen wird, wird Benutzergruppen der Zugriff auf das Gerät entweder gewährt oder verweigert. Die Regelpriorität ist beim Abgleich von Paketen mit Regeln ein zentraler Punkt, da Pakete auf First-Match-Basis abgeglichen werden. Eins ist die höchste Priorität.
- **Verwaltungsmethode**: Wählen Sie die Verwaltungsmethode aus, für die die Regel definiert werden soll. Folgende Optionen sind möglich:
  - *Alle*: Der Regel werden alle Verwaltungsmethoden zugewiesen.
  - *Telnet*: Benutzern, die Zugriff auf das Gerät anfordern, das den Kriterien des Telnet-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
  - *Sicheres Telnet*: Benutzern, die Zugriff auf das Gerät anfordern, der den Kriterien des SSH-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
  - *HTTP*: Benutzern, die Zugriff auf das Gerät anfordern, der den Kriterien des HTTP-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
  - *Sicheres HTTP (HTTPS)*: Benutzern, die Zugriff auf das Gerät anfordern, der den Kriterien des HTTPS-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
  - *SNMP*: Benutzern, die Zugriff auf das Gerät anfordern, der den Kriterien des SNMP-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
- **Aktion**: Wählen Sie die Aktion aus, die mit der Regel verbunden werden soll. Folgende Optionen sind möglich:
  - *Zulassen*: Zugriff auf das Gerät wird gewährt, wenn der Benutzer mit den Einstellungen im Profil übereinstimmt.
  - *Verweigern*: Zugriff auf das Gerät wird verweigert, wenn der Benutzer mit den Einstellungen im Profil übereinstimmt.
- **Anwenden für Schnittstelle**: Wählen Sie die Schnittstelle aus, die mit der Regel verbunden werden soll. Folgende Optionen sind möglich:

  - *Alle*: Gilt für alle Ports, VLANs und LAGs.
  - *Benutzerdefiniert*: Gilt für die ausgewählte Schnittstelle.
- **Schnittstelle**: Geben Sie die Schnittstellennummer ein, wenn Sie „Benutzerdefiniert“ ausgewählt haben.
- **Anwenden auf Quell-IP-Adresse**: Wählen Sie den Typ der Quell-IP-Adresse, auf die das Zugriffsprofil angewendet werden soll. Das Feld *Quell-IP-Adresse* ist für ein Subnetzwerk gültig. Wählen Sie unter den folgenden Werten:
  - *Alle*: Gilt für alle Typen von IP-Adressen.
  - *Benutzerdefiniert*: Gilt nur für die Typen von IP-Adressen, die in den Feldern definiert wurden.
- **IP-Version**: Geben Sie die Version der Quell-IP-Adresse ein: Version 6 oder Version 4.
- **IP-Adresse**: Geben Sie die Quell-IP-Adresse ein.
- **Maske**: Wählen Sie das Format der Subnetzmaske für die Quell-IP-Adresse aus, und geben Sie einen Wert in eines der Felder ein:
  - *Netzwerkmaske*: Wählen Sie das Subnetz aus, zu dem die Quell-IP-Adresse gehört, und geben Sie die Subnetzmaske in Dotted-Decimal-Format ein.
  - *Präfixlänge*: Wählen Sie die Präfixlänge aus, und geben Sie die Anzahl der Bits ein, die das Präfix der Quell-IP-Adresse umfasst.

SCHRITT 7 Klicken Sie auf **Übernehmen**. Das Zugriffsprofil wird in die aktuelle Konfigurationsdatei geschrieben. Sie können dieses Zugriffsprofil nun als aktives auswählen.

Definieren von Profilregeln

Zugriffsprofile können bis zu 128 Regeln enthalten, anhand derer entschieden wird, wem Zugriff auf das Gerät und Verwaltungsberechtigung gewährt wird und welche Zugriffsmethoden dabei verwendet werden dürfen.

Alle Regeln in einem Zugriffsprofil enthalten eine Aktion sowie Kriterien (ein oder mehrere Parameter) für den Abgleich. Alle Regeln haben eine Priorität. Regeln mit der höchsten Priorität werden zuerst geprüft. Wenn ein eingehendes Paket mit einer Regel übereinstimmt, wird die mit der Regel verbundene Aktion durchgeführt. Wenn innerhalb des aktiven Zugriffsprofils keine übereinstimmende Regel gefunden wird, wird das Paket gelöscht (Drop).

Beispielsweise können Sie den Zugriff auf das Gerät von sämtlichen IP-Adressen aus beschränken, mit Ausnahme von IP-Adressen, die dem IT-Verwaltungszentrum zugeordnet sind. Auf diese Weise kann das Gerät immer noch verwaltet werden, hat aber eine weitere Sicherheitsschicht hinzugewonnen.

So fügen Sie Profilregeln einem Zugriffsprofil hinzu:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Verwaltungszugriffsmethode** > **Profilregeln**.

SCHRITT 2 Wählen Sie das Feld „Filter“ und ein Zugriffsprofil aus. Klicken Sie auf **Los**.

Das ausgewählte Zugriffsprofil wird in der Tabelle „Profilregeln“ angezeigt.

SCHRITT 3 Klicken Sie auf **Hinzufügen**, um eine Regel hinzuzufügen.

SCHRITT 4 Geben Sie die Parameter ein.

- **Zugriffsprofilname**: Wählen Sie ein Zugriffsprofil aus.
- **Regelpriorität**: Geben Sie die Regelpriorität ein. Wenn ein Paket mit einer Regel abgeglichen wird, wird Benutzergruppen der Zugriff auf das Gerät entweder gewährt oder verweigert. Die Regelpriorität ist beim Abgleich von Paketen mit Regeln ein zentraler Punkt, da Pakete auf First-Fit-Basis abgeglichen werden.
- **Verwaltungsmethode**: Wählen Sie die Verwaltungsmethode aus, für die die Regel definiert werden soll. Folgende Optionen sind möglich:
  - *Alle*: Der Regel werden alle Verwaltungsmethoden zugewiesen.
  - *Telnet*: Benutzern, die Zugriff auf das Gerät anfordern, das den Kriterien des Telnet-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
  - *Sicheres Telnet*: Benutzern, die Zugriff auf das Gerät anfordern, das den Kriterien des Telnet-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
  - *HTTP*: Der Regel wird HTTP-Zugriff zugewiesen. Benutzern, die Zugriff auf das Gerät anfordern, der den Kriterien des HTTP-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
  - *Sicheres HTTP (HTTPS)*: Benutzern, die Zugriff auf das Gerät anfordern, der den Kriterien des HTTPS-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
  - *SNMP*: Benutzern, die Zugriff auf das Gerät anfordern, der den Kriterien des SNMP-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
- **Aktion**: Wählen Sie **Zulassen**, um Benutzer zuzulassen, die unter Verwendung der konfigurierten Zugriffsmethode von der in dieser Regel definierten Schnittstelle bzw. IP-Adresse aus auf das Gerät zugreifen möchten. Sie können auch **Verweigern** wählen, um den Zugriff zu verweigern.

- **Anwenden für Schnittstelle**: Wählen Sie die Schnittstelle aus, die mit der Regel verbunden werden soll. Folgende Optionen sind möglich:
  - *Alle*: Gilt für alle Ports, VLANs und LAGs.
  - *Benutzerdefiniert*: Gilt nur für den Port, das VLAN oder die LAG, der/das/die ausgewählt wurde.
- **Schnittstelle**: Geben Sie die Schnittstellennummer ein.
- **Anwenden auf Quell-IP-Adresse**: Wählen Sie den Typ der Quell-IP-Adresse, auf die das Zugriffsprofil angewendet werden soll. Das Feld *Quell-IP-Adresse* ist für ein Subnetzwerk gültig. Wählen Sie unter den folgenden Werten:
  - *Alle*: Gilt für alle Typen von IP-Adressen.
  - *Benutzerdefiniert*: Gilt nur für die Typen von IP-Adressen, die in den Feldern definiert wurden.
- **IP-Version**: Wählen Sie die IP-Version, die die Quell-Adresse unterstützt: IPv6 oder IPv4.
- **IP-Adresse**: Geben Sie die Quell-IP-Adresse ein.
- **Maske**: Wählen Sie das Format für die Subnetzmaske der Quell-IP-Adresse aus, und geben Sie einen Wert in eines der Felder ein:
  - *Netzwerkmaske*: Wählen Sie das Subnetz aus, zu dem die Quell-IP-Adresse gehört, und geben Sie die Subnetzmaske in Dotted-Decimal-Format ein.
  - *Präfixlänge*: Wählen Sie die Präfixlänge aus, und geben Sie die Anzahl der Bits ein, die das Präfix der Quell-IP-Adresse umfasst.

SCHRITT 5 Klicken Sie auf **Übernehmen**, und die Regel wird dem Zugriffsprofil hinzugefügt.

Verwaltungszugriffsauthentifizierung

Sie können den verschiedenen Verwaltungszugriffsmethoden Autorisierungs- und Authentifizierungsmethoden zuweisen, z. B. SSH, Konsole, Telnet, HTTP und HTTPS. Diese Authentifizierung kann lokal oder auf einem TACACS+- oder RADIUS-Server ausgeführt werden.

Wenn die Autorisierung aktiviert ist, werden sowohl die Identität als auch Lese- und Schreibrechte des Benutzers überprüft. Ist die Autorisierung nicht aktiviert, dann wird nur die Identität des Benutzers überprüft.

Autorisierung und Authentifizierung erfolgen in der Reihenfolge, in der die Authentifizierungsmethoden ausgewählt werden. Wenn die erste Authentifizierungsmethode nicht verfügbar ist, wird die nächste ausgewählte Methode verwendet. Wenn z. B. die ausgewählten Authentifizierungsmethoden „RADIUS“ und „Lokal“ sind und alle konfigurierten RADIUS-Server in der Reihenfolge der Prioritäten angefragt werden und nicht antworten, wird der Benutzer lokal autorisiert bzw. authentifiziert.

Wenn die Autorisierung aktiviert ist und eine Authentifizierungsmethode fehlschlägt oder der Benutzer nicht über die entsprechende Berechtigungsebene verfügt, wird dem Benutzer der Zugriff auf das Gerät verweigert. Wenn also die Authentifizierung mit einer Authentifizierungsmethode fehlschlägt, beendet das Gerät den Authentifizierungsversuch. Es fährt nicht fort und versucht auch nicht, die nächste Authentifizierungsmethode zu verwenden.

Ebenfalls beendet das Gerät den Authentifizierungsversuch, wenn die Autorisierung nicht aktiviert ist und die Authentifizierung fehlschlägt.

So definieren Sie Authentifizierungsmethoden für Zugriffsmethoden:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Verwaltungszugriffsauthentifizierung**.

SCHRITT 2 Geben Sie die **Anwendung** (Typ) der Verwaltungszugriffsmethode ein.

SCHRITT 3 Wählen Sie **Autorisierung** aus, um sowohl Authentifizierung als auch Autorisierung des Benutzers mithilfe der in der nachfolgenden Liste beschriebenen Methoden zu aktivieren. Wenn das Feld nicht ausgewählt ist, wird nur die Authentifizierung durchgeführt. Wenn die Autorisierung aktiviert ist, werden die Lese- und Schreibrechte des Benutzers überprüft. Diese Berechtigungsebene wird auf der Seite „Benutzerkonten“ festgelegt.

SCHRITT 4 Verwenden Sie die Pfeiltasten, um die Autorisierungs- und Authentifizierungsmethode zwischen der Spalte **Optionale Methoden** und der Spalte **Ausgewählte Methoden** zu verschieben. Methoden werden in der hier aufgeführten Reihenfolge angewendet.

SCHRITT 5 Verwenden Sie die Pfeiltasten, um die Authentifizierungsmethode zwischen der Spalte **Optionale Methoden** und der Spalte **Ausgewählte Methoden** zu verschieben. Die erste ausgewählte Methode wird als Erstes angewendet.

- *RADIUS*: Der Benutzer wird auf einem RADIUS-Server autorisiert bzw. authentifiziert. Es muss mindestens ein RADIUS-Server konfiguriert sein. Damit der RADIUS-Server Zugriff auf das webbasierte Konfigurationsdienstprogramm gewährt, muss er die Zeichenfolge „cisco-avpair = shell:priv-lvl=15“ zurückgeben.
- *TACACS+*: Der Benutzer wird auf dem TACACS+-Server autorisiert bzw. authentifiziert. Es muss mindestens ein TACACS+-Server konfiguriert sein.
- *Keine*: Der Benutzer kann ohne Autorisierung bzw. Authentifizierung auf das Gerät zugreifen.
- *Lokal*: Benutzername und Kennwort werden mit den auf dem lokalen Gerät gespeicherten Daten verglichen. Diese Benutzernamen- und Kennwortpaare werden auf der Seite „Benutzerkonten“ definiert.

HINWEIS Die Authentifizierungsmethoden **Lokal** oder **Keine** müssen stets als Letztes ausgewählt werden. Alle nach **Lokal** oder **Keine** ausgewählten Authentifizierungsmethoden werden ignoriert.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die ausgewählten Authentifizierungsmethoden werden der Zugriffsmethode zugeordnet.

Sicheres Verwalten sensibler Daten (SSD)

Weitere Informationen hierzu finden Sie unter **Sicherheit: Sicheres Verwalten sensibler Daten (SSD)**.

SSL-Server

In diesem Abschnitt wird die SSL-Funktion (Secure Socket Layer) beschrieben.

SSL (Übersicht)

Die SSL-Funktion (Secure Socket Layer) wird verwendet, um eine HTTPS-Sitzung mit dem Gerät zu öffnen.

Eine HTTPS-Sitzung kann mit dem im Gerät vorhandenen Standardzertifikat geöffnet werden.

Manche Browser generieren bei Verwendung eines Standardzertifikats Warnungen, da dieses Zertifikat nicht von einer Zertifizierungsstelle (Certification Authority, CA) signiert ist. Es wird empfohlen, ein von einer vertrauenswürdigen Zertifizierungsstelle signiertes Zertifikat zu verwenden.

Um eine HTTPS-Sitzung mit einem von einem Benutzer erstellten Zertifikat zu öffnen, führen Sie die folgenden Aktionen aus:

1. Generieren Sie ein Zertifikat.
2. Legen Sie fest, dass das Zertifikat von einer Zertifizierungsstelle zertifiziert sein muss.
3. Importieren Sie das signierte Zertifikat in das Gerät.

Standardeinstellungen und Konfiguration

Das Gerät enthält standardmäßig ein Zertifikat, das Sie ändern können.

HTTPS ist standardmäßig aktiviert.

Authentifizierungseinstellungen für SSL-Server

Möglicherweise müssen Sie ein neues Zertifikat generieren, um das Standardzertifikat im Gerät zu ersetzen.

So erstellen Sie ein neues Zertifikat:

SCHRITT 1 Klicken Sie auf **Sicherheit > SSL-Server > Authentifizierungseinstellungen für SSL-Server**.

In der SSL-Serverschlüsseltabelle werden Informationen für Zertifikat 1 und 2 angezeigt. Diese Felder definieren Sie mit Ausnahme der folgenden Felder auf der Seite **Bearbeiten**:

- **Gültig ab**: Gibt das Datum an, ab dem das Zertifikat gültig ist.
- **Gültig bis**: Gibt das Datum an, bis zu dem das Zertifikat gültig ist.
- **Zertifikatsquelle**: Gibt an, ob das Zertifikat vom System (automatisch generiert) oder vom Benutzer (benutzerdefiniert) generiert wurde.

SCHRITT 2 Wählen Sie ein aktives Zertifikat aus.

SCHRITT 3 Klicken Sie auf **Zertifikatsanforderung generieren**.

SCHRITT 4 Geben Sie Werte für die folgenden Felder ein:

- **Zertifikats-ID**: Wählen Sie das aktive Zertifikat aus.
- **Allgemeiner Name**: Gibt die voll qualifizierte Geräte-URL oder IP-Adresse an. Wenn nichts angegeben ist, wird (beim Generieren des Zertifikats) standardmäßig die niedrigste IP-Adresse des Geräts verwendet.
- **Organisationseinheit**: Gibt die Organisationseinheit oder den Abteilungsnamen an.
- **Organisationsname**: Gibt den Namen der Organisation an.
- **Ort**: Gibt den Namen des Orts oder der Stadt an.
- **Bundesland**: Gibt den Namen des Bundeslands an.
- **Land**: Gibt den Ländernamen an.
- **Zertifikatsanforderung**: Zeigt den Schlüssel an, der bei Anklicken der Schaltfläche **Zertifikatsanforderung generieren** erstellt wird.

SCHRITT 5 Klicken Sie auf **Zertifikatsanforderung generieren**. Daraufhin wird ein Schlüssel erstellt, der in der Zertifizierungsstelle (Certification Authority, CA) eingegeben werden muss. Kopieren Sie diesen aus dem Feld **Zertifikatsanforderung**.

So importieren Sie ein Zertifikat:

SCHRITT 1 Klicken Sie auf **Sicherheit > SSL-Server > Authentifizierungseinstellungen für SSL-Server**.

SCHRITT 2 Klicken Sie auf **Zertifikat importieren**.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **Zertifikats-ID**: Wählen Sie das aktive Zertifikat aus.
- **Zertifikatsquelle**: Zeigt an, dass das Zertifikat benutzerdefiniert ist.
- **Zertifikat**: Kopieren Sie das empfangene Zertifikat in dieses Feld.
- **RSA-Schlüsselpaar importieren**: Wählen Sie diese Option aus, um das Kopieren des neuen RSA-Schlüsselpaars in dieses Feld zu ermöglichen.
- **Öffentlicher Schlüssel**: Kopieren Sie den öffentlichen RSA-Schlüssel in dieses Feld.
- **Privater Schlüssel (verschlüsselt)**: Wählen Sie den privaten RSA-Schlüssel in verschlüsselter Form aus und kopieren Sie ihn in dieses Feld.
- **Privater Schlüssel (unverschlüsselt)**: Wählen Sie den privaten RSA-Schlüssel in unverschlüsselter Form aus und kopieren Sie ihn in dieses Feld.

SCHRITT 4 Klicken Sie auf **Übernehmen**, um die Änderungen in die aktuelle Konfiguration zu übernehmen.

SCHRITT 5 Klicken Sie auf **Sensible Daten verschlüsselt anzeigen**, um den Schlüssel in verschlüsselter Form anzuzeigen. Wenn Sie auf diese Schaltfläche klicken, werden die privaten Schlüssel in verschlüsselter Form in die Konfigurationsdatei geschrieben (wenn Sie auf „Übernehmen“ klicken). Wenn der Text in verschlüsselter Form angezeigt wird, erhält die Schaltfläche die Beschriftung **Sensible Daten unverschlüsselt anzeigen**, und Sie können den Text erneut in unverschlüsselter Form anzeigen.

Daraufhin wird die Schaltfläche **Details** mit dem Zertifikat und dem RSA-Schlüsselpaar angezeigt. Von hier aus können Sie das Zertifikat und das RSA-Schlüsselpaar in ein anderes Gerät kopieren (mit Kopieren und Einfügen). Wenn Sie auf **Sensible Daten verschlüsselt anzeigen** klicken, werden die privaten Schlüssel in verschlüsselter Form angezeigt.

SSH-Server

Weitere Informationen hierzu finden Sie unter **Sicherheit: SSH-Server**.

SSH-Client

Weitere Informationen hierzu finden Sie unter **Sicherheit: SSH-Client**.

Konfigurieren von TCP-/UDP-Services

Auf der Seite „TCP-/UDP-Services“ können TCP- oder UDP-basierte Services für das Gerät aktiviert werden, normalerweise zu Sicherheitszwecken.

Das Gerät bietet die folgenden TCP-/UDP-Services:

- **HTTP**: Standardmäßig von Herstellerseite aktiviert.
- **HTTPS**: Standardmäßig von Herstellerseite aktiviert.
- **SNMP**: Standardmäßig von Herstellerseite deaktiviert.
- **Telnet**: Standardmäßig von Herstellerseite deaktiviert.
- **SSH**: Standardmäßig von Herstellerseite deaktiviert.

Die aktiven TCP-Verbindungen werden in diesem Fenster ebenfalls angezeigt.

So konfigurieren Sie TCP-/UDP-Services:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **TCP-/UDP-Services**.

SCHRITT 2 Aktivieren oder deaktivieren Sie die folgenden TCP-/UDP-Services für die angezeigten Services.

- **HTTP-Service**: Gibt an, ob der HTTP-Service aktiviert oder deaktiviert ist.
- **HTTPS-Service**: Gibt an, ob der HTTPS-Service aktiviert oder deaktiviert ist.
- **SNMP-Service**: Gibt an, ob der SNMP-Service aktiviert oder deaktiviert ist.
- **Telnet-Service**: Gibt an, ob der Telnet-Service aktiviert oder deaktiviert ist.
- **SSH-Service**: Gibt an, ob der SSH-Server-Service aktiviert oder deaktiviert ist.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Services werden in die aktuelle Konfigurationsdatei geschrieben.

In der Tabelle für TCP-Services werden die folgenden Felder für die einzelnen Services angezeigt:

- **Servicename**: Die Zugriffsmethode, über die das Gerät den TCP-Service anbietet.
- **Typ**: Das IP-Protokoll, das für den Service verwendet wird.
- **Lokale IP-Adresse**: Die lokale IP-Adresse, über die das Gerät den Service anbietet.
- **Lokaler Port**: Der lokale Port, über den das Gerät den Service anbietet.
- **Remote-IP-Adresse**: Die IP-Adresse des standortfernen Geräts, das den Service anfordert.
- **Remote-Port**: Der TCP-Port des standortfernen Geräts, das den Service anfordert.
- **Status**: Status des Service.

In der Tabelle „UDP-Service“ werden die folgenden Informationen angezeigt:

- **Servicename**: Die Zugriffsmethode, über die das Gerät den UDP-Service anbietet.
- **Typ**: Das IP-Protokoll, das für den Service verwendet wird.
- **Lokale IP-Adresse**: Die lokale IP-Adresse, über die das Gerät den Service anbietet.
- **Lokaler Port**: Der lokale UDP-Port, über den das Gerät den Service anbietet.
- **Anwendungsinstanz**: Die Serviceinstanz des UDP-Service. (Wenn beispielsweise zwei Absender Daten an das gleiche Ziel senden.)

Definieren der Sturmsteuerung

Wenn Broadcast-, Multicast- oder unbekannte Unicast-Frames empfangen werden, werden sie dupliziert, und an alle in Frage kommenden Ausgangs-Ports wird eine Kopie gesendet. Dies bedeutet in der Praxis, dass sie an alle Ports gesendet werden, die zum relevanten VLAN gehören. Auf diese Weise entstehen aus einem Eingangs-Frame viele weitere, sodass die Möglichkeit eines Verkehrssturms besteht.

Schutz gegen Sturm erlaubt es Ihnen, die Anzahl der Frames, die beim Gerät eingehen, zu begrenzen und die Typen von Frames zu definieren, die im Hinblick auf diese Begrenzung berücksichtigt werden.

Alle nach Überschreiten des Schwellenwerts empfangenen Broadcast-, Multicast- oder unbekannten Unicast-Frames werden verworfen.

So definieren Sie die Sturmsteuerung:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Sturmsteuerung**.

Alle Felder dieser Seite werden auf der Seite „Sturmsteuerung bearbeiten“ beschrieben. Eine Ausnahme ist das Feld Ratenschwellenwert **Sturmsteuerung (%)**. In diesem Feld wird der Prozentsatz der gesamten Bandbreite angezeigt, der für unbekannte Unicast-, Multicast- und Broadcast-Pakete zur Verfügung stehen soll, bevor die Sturmsteuerung auf den Port angewendet wird. Der Standardwert entspricht 10 % der Maximalrate des Ports. Der Wert wird auf der Seite „Sturmsteuerung bearbeiten“ festgelegt.

SCHRITT 2 Wählen Sie einen Port aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Schnittstelle**: Wählen Sie den Port aus, für den die Sturmsteuerung aktiviert werden soll.
- **Sturmsteuerung**: Aktivieren Sie hiermit die Sturmsteuerung.
- **Ratenschwellenwert Sturmsteuerung**: Geben Sie die Maximalrate für die Weiterleitung unbekannter Pakete ein. Der Standardwert für diesen Schwellenwert entspricht 10.000 für FE-Geräte und 100.000 für GE-Geräte.
- **Sturmsteuerungsmodus**: Wählen Sie einen der folgenden Modi aus:
  - *Unbekanntes Unicast, Multicast und Broadcast*: Zählt unbekannten Unicast-, Multicast- und Broadcast-Verkehr zusammen und vergleicht die Summe mit dem Bandbreiten-Schwellenwert.
  - *Multicast und Broadcast*: Zählt Multicast- und Broadcast-Verkehr zusammen und vergleicht die Summe mit dem Bandbreiten-Schwellenwert.
  - *Nur Broadcast*: Vergleicht nur den Broadcast-Datenverkehr mit dem Bandbreiten-Schwellenwert.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Sturmsteuerung wird geändert und die aktuelle Konfigurationsdatei wird aktualisiert.

Konfigurieren der Portsicherheit

Die Netzwerksicherheit kann erhöht werden, indem der Zugriff auf einen Port auf Benutzer mit bestimmten MAC-Adressen beschränkt wird. Die MAC-Adressen können entweder dynamisch gelernt oder statisch konfiguriert werden.

Durch die Portsicherheitsfunktion werden empfangene und gelernte Pakete überwacht. Der Zugriff auf gesperrte Ports ist beschränkt auf Benutzer mit bestimmten MAC-Adressen.

Es gibt vier Modi der Portsicherheit:

- **Klassische Sperre**: Alle gelernten MAC-Adressen im Port werden gesperrt, und der Port lernt keine neuen MAC-Adressen. Die gelernten Adressen unterliegen keiner Fälligkeit und werden nicht erneut gelernt.
- **Beschränkte dynamische Sperre**: Das Gerät lernt MAC-Adressen bis zum konfigurierten Grenzwert erlaubter Adressen. Nach Erreichen des Grenzwerts lernt das Gerät keine weiteren Adressen. In diesem Modus unterliegen die gelernten Adressen der Fälligkeit und müssen erneut gelernt werden.
- **Permanent sichern**: Behält die aktuellen dem Port zugeordneten dynamischen MAC-Adressen bei und lernt die maximale Anzahl der am Port zulässigen Adressen (festgelegt mit „Maximale Anzahl zulässiger Adressen“). Neulernen und Fälligkeit sind deaktiviert.
- **Bei Zurücksetzen sicher löschen**: Löscht nach dem Zurücksetzen die aktuellen dynamischen MAC-Adressen, die dem Port zugeordnet sind. Es können so viele MAC-Adressen zum Löschen beim Zurücksetzen gelernt werden, wie maximal am Port zulässig sind. Neulernen und Fälligkeit sind deaktiviert.

Wenn ein Frame von einer neuen MAC-Adresse durch einen Port erkannt wird, bei dem er nicht autorisiert ist (der Port ist auf klassische Weise gesperrt, und die MAC-Adresse ist neu, oder der Port ist dynamisch gesperrt, und die Höchstzahl erlaubter Adressen wurde überschritten), wird der Schutzmechanismus ausgelöst, und eine der folgenden Aktionen wird ausgeführt:

- Der Frame wird verworfen.
- Der Frame wird weitergeleitet.
- Der Port wird heruntergefahren.

Wenn die sichere MAC-Adresse von einem anderen Port erkannt wird, wird der Frame weitergeleitet, die MAC-Adresse wird von diesem Port jedoch nicht gelernt.

Zusätzlich zu diesen beiden Aktionen können Sie auch Traps erstellen und deren Frequenz und Anzahl begrenzen, um eine Überlastung der Geräte zu vermeiden.

HINWEIS Wenn Sie 802.1X an einem Port verwenden möchten, muss sich dieser im Mehrfachhostmodus oder Mehrfachsitzungsmodus befinden. Die Portsicherheit an einem Port kann nicht festgelegt werden, wenn sich der Port im Einzelmodus befindet (siehe Seite „802.1X, Host- und Sitzungsauthentifizierung“).

So konfigurieren Sie die Portsicherheit:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Portsicherheit**.

SCHRITT 2 Wählen Sie die Schnittstelle aus, die geändert werden soll, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Schnittstelle**: Wählen Sie den Namen der Schnittstelle.

- **Schnittstellenstatus**: Aktivieren Sie die Sperrung des Ports.
- **Lernmodus**: Wählen Sie die Art der Port-Sperre. Damit dieses Feld konfiguriert werden kann, muss der Status der Schnittstelle „nicht gesperrt“ sein. Der Lernmodus wird nur dann aktiviert, wenn das Feld *Schnittstellenstatus* gesperrt ist. Um den Lernmodus zu ändern, muss die Eingabe unter „Schnittstellenstatus“ gelöscht werden. Nach dem Ändern des Lernmodus kann „Schnittstellenstatus“ wieder eingegeben werden. Folgende Optionen sind möglich:
  - *Klassische Sperre*: Der Port wird sofort gesperrt, ungeachtet der Anzahl bisher gelernter Adressen.
  - *Beschränkte dynamische Sperre*: Der Port wird gesperrt, indem die aktuell mit dem Port assoziierten dynamischen MAC-Adressen gelöscht werden. Der Port lernt Adressen bis zur Höchstzahl erlaubter Adressen. Sowohl erneutes Lernen als auch die Fälligkeit von MAC-Adressen sind aktiviert.
  - *Permanent sichern*: Behält die aktuellen dem Port zugeordneten dynamischen MAC-Adressen bei und lernt die maximale Anzahl der am Port zulässigen Adressen (festgelegt mit **Maximale Anzahl zulässiger Adressen**). Neulernen und Fälligkeit sind aktiviert.
  - *Bei Zurücksetzen sicher löschen*: Löscht nach dem Zurücksetzen die aktuellen dynamischen MAC-Adressen, die dem Port zugeordnet sind. Es können so viele MAC-Adressen zum Löschen beim Zurücksetzen gelernt werden, wie maximal am Port zulässig sind. Neulernen und Fälligkeit sind deaktiviert.
- **Max. Anzahl zulässiger Adressen**: Geben Sie die Höchstzahl an MAC-Adressen ein, die vom Port gelernt werden können, wenn der Lernmodus *Beschränkte dynamische Sperre* aktiviert ist. Die Zahl 0 bedeutet, dass von der Schnittstelle nur statische Adressen unterstützt werden.
- **Aktion bei Verstoß**: Wählen Sie die Aktion, die auf Pakete angewendet werden soll, die bei einem gesperrten Port eingehen. Folgende Optionen sind möglich:
  - *Verwerfen*: Pakete von nicht gelernten Quellen werden verworfen.
  - *Weiterleiten*: Pakete von einer unbekannten Quelle werden weitergeleitet, ohne dass die MAC-Adresse gelernt wird.
  - *Herunterfahren*: Pakete von nicht gelernten Quellen werden verworfen, und der Port wird heruntergefahren. Der Port bleibt geschlossen, bis er wieder aktiviert oder das Gerät neu gestartet wird.
- **Trap**: Wählen Sie die Aktivierung von Traps, wenn ein Paket bei einem gesperrten Port eingeht. Dies ist relevant bei Verstößen gegen Sperren. Bei der klassischen Sperre ist jede empfangene neue Adresse ein Verstoß. Bei der beschränkten dynamischen Sperre ist jede neue Adresse, die die Höchstzahl erlaubter Adressen überschreitet, ein Verstoß.
- **Trap-Frequenz**: Geben Sie die Mindestzeit in Sekunden ein, die zwischen Traps verstreichen soll.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Portsicherheit wird geändert und die aktuelle Konfigurationsdatei wird aktualisiert.

802.1X

Weitere Informationen zur 802.1X-Authentifizierung finden Sie in Kapitel **Sicherheit: 802.1X-Authentifizierung**. Dies beinhaltet auch die MAC-basierte und die webbasierte Authentifizierung.

Denial of Service-Sicherung

Ein DoS-Angriff (Denial of Service) ist der Versuch eines Hackers, ein Gerät für dessen Benutzer nicht mehr verfügbar zu machen.

Bei DoS-Angriffen wird ein Gerät mit externen Kommunikationsanforderungen ausgelastet, sodass es nicht auf legitimen Datenverkehr antworten kann. Solche Angriffe führen in der Regel zu einer CPU-Überlastung des Geräts.

Secure Core Technology (SCT)

Eine vom Gerät eingesetzte Methode zur Abwehr von DoS-Angriffen ist SCT. SCT ist im Gerät standardmäßig aktiviert und kann nicht deaktiviert werden.

Das Cisco-Gerät kann neben Endbenutzer-Datenverkehr (TCP) auch Verwaltungs-, Protokoll- und Snooping-Verkehr verarbeiten.

Mit SCT wird sichergestellt, dass das Gerät unabhängig vom empfangenen Gesamtdatenverkehr auch Verwaltungs- und Protokollverkehr empfängt und verarbeitet. Dies geschieht durch Ratenbegrenzung des TCP-Verkehrs an die CPU.

Es gibt keine Interaktionen mit anderen Funktionen.

SCT kann auf der Seite „Denial of Service > Denial of Service-Sicherung > Security Suite-Einstellungen“ (Schaltfläche **Details**) überwacht werden.

Arten von DoS-Angriffen

Die folgenden Pakettypen oder sonstigen Strategien können bei einem Denial of Service-Angriff eingesetzt werden:

- **TCP-SYN-Pakete**: Diese Pakete haben oft eine falsche Absenderadresse. Jedes dieser Pakete wird wie eine Verbindungsanforderung verarbeitet und veranlasst den Server, durch Zurücksenden eines TCP/SYN-ACK-Pakets (Bestätigung) eine halb offene Verbindung herzustellen und auf ein Antwortpaket auf das ACK-Paket von der Absenderadresse zu warten. Da die Absenderadresse jedoch falsch ist, trifft eine Antwort nie ein. Durch diese halb offenen Verbindungen wird die Anzahl der möglichen Verbindungen durch das Gerät ausgeschöpft, sodass es nicht mehr auf legitime Anforderungen antworten kann.

- **TCP-SYN-FIN-Pakete**: SYN-Pakete werden zum Herstellen einer neuen TCP-Verbindung gesendet. TCP-FIN-Pakete werden zum Trennen einer Verbindung gesendet. In einem Paket sollte nie sowohl das SYN- als auch das FIN-Flag gesetzt sein. Solche Pakete können einen Angriff auf das Gerät bedeuten und sollten daher blockiert werden.
- **Ungültige Adressen**: Ungültige Adressen sind nach Maßgabe des IP-Protokolls unzulässig. Weitere Details finden Sie unter **Ungültige Adressen**.
- **ICMP-Angriff**: Durch das Senden von ICMP-Paketen mit inkorrekter Form oder einer sehr großen Anzahl von ICMP-Paketen an das betroffene Gerät kann ein Systemabsturz verursacht werden.
- **IP-Fragmentierung**: Ungültige IP-Fragmente mit überlappenden und übergroßen Nutzlasten werden an das Gerät gesendet. Dies kann bei verschiedenen Betriebssystemen zu Abstürzen führen, deren Code zum Zusammensetzen von TCP/IP-Fragmenten fehlerhaft ist. Windows 3.1x, Windows 95 und Windows NT sowie Linux-Betriebssysteme bis zu den Versionen 2.0.32 und 2.1.63 sind für solche Angriffe anfällig.
- **Stacheldraht-Distribution**: Der Angreifer stellt mithilfe eines Client-Programms Verbindungen mit kompromittierten Systemen (Handlern) her, über die auf Zombie-Agenten Befehle ausgeführt werden, um den DoS-Angriff einzuleiten. Die Agenten werden über die Handler durch den Angreifer kompromittiert.

  Dabei werden durch automatisierte Routinen Schwachstellen in Programmen ausgenutzt, die Remoteverbindungen auf den Remote-Hosts zulassen, die Ziel des Angriffs sind. Jeder Handler kann bis zu eintausend Agenten kontrollieren.
- **Invasor-Trojaner**: Mithilfe eines Trojaners kann der Angreifer einen Zombie-Agent herunterladen (sofern dieser nicht bereits im Trojaner selbst enthalten ist). Außerdem können Angreifer mithilfe automatisierter Tools in Systeme eindringen. Dabei nutzen diese Tools Fehler in Programmen aus, die Verbindungen von Remote-Hosts abhören. Von diesem Szenario sind in erster Linie Geräte betroffen, die als Server im Internet fungieren.
- **Back Orifice-Trojaner**: Dies ist eine Variante eines Trojaners, der Systeme über die Software „Back Orifice“ infiziert.

Schutz vor DoS-Angriffen

Mithilfe der Funktion DoS-Prävention kann der Systemadministrator solche Angriffe wie folgt abwehren:

- TCP-SYN-Schutz aktivieren. Wenn diese Funktion aktiviert ist, wird jeder ermittelte SYN-Paketangriff gemeldet und der angegriffene Port kann vorübergehend heruntergefahren werden. Ein SYN-Angriff wird ermittelt, wenn die Anzahl der SYN-Pakete pro Sekunde einen vom Benutzer konfigurierten Schwellenwert überschreitet.
- SYN-FIN-Pakete blockieren.

- Pakete mit reservierten ungültigen Adressen blockieren (Seite „Ungültige Adressen“).
- TCP-Verbindungen von bestimmten Schnittstellen aus verhindern (Seite „SYN-Filterung“) und Ratenbegrenzungen für Pakete festlegen (Seite „SYN-Ratenschutz“).
- Blockierung bestimmter ICMP-Pakete konfigurieren (Seite „ICMP-Filterung“).
- Fragmentierte IP-Pakete von einer bestimmten Schnittstelle verwerfen (Seite „IP-Fragmentfilterung“).
- Angriffe durch Stacheldraht-Distribution, Invasor-Trojaner und Back Orifice-Trojaner abwehren (Seite „Security Suite-Einstellungen“).

Abhängigkeiten zwischen Funktionen

Zugriffssteuerungslisten (ACLs) und erweiterte QoS-Richtlinien sind nicht aktiv, wenn für einen Port der DoS-Schutz aktiviert ist. Wenn Sie entweder versuchen, die DoS-Prävention für eine Schnittstelle zu aktivieren, für die eine ACL definiert ist, oder eine ACL für eine Schnittstelle zu definieren, für die die DoS-Prävention aktiviert ist, wird jeweils eine Fehlermeldung angezeigt.

Ein SYN-Angriff kann nicht blockiert werden, wenn eine ACL für eine Schnittstelle aktiv ist.

Standardkonfiguration

Für die Funktion „DoS-Prävention“ gilt die folgende Standardkonfiguration:

- Die Funktion „DoS-Prävention“ ist standardmäßig deaktiviert.
- Der SYN-FIN-Schutz ist standardmäßig aktiviert (auch wenn die DoS-Prävention deaktiviert ist).
- Wenn der SYN-Schutz aktiviert ist, lautet der Standardschutzmodus **Blockieren und melden**. Der Schwellenwert beträgt standardmäßig 30 SYN-Pakete pro Sekunde.
- Alle anderen Funktionen zur DoS-Prävention sind standardmäßig deaktiviert.

Konfigurieren der DoS-Prävention

Auf den folgenden Seiten wird die Konfiguration dieser Funktion beschrieben.

Security Suite-Einstellungen

HINWEIS Vor dem Aktivieren der DoS-Prävention müssen Sie die Bindung aller Zugriffssteuerungslisten (Access Control Lists, ACLs) oder erweiterten QoS-Richtlinien an einen Port aufheben. ACLs und erweiterte QoS-Richtlinien sind nicht aktiv, wenn für einen Port der DoS-Schutz aktiviert ist.

So konfigurieren Sie die globalen Einstellungen für die DoS-Prävention und überwachen SCT:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Denial of Service-Sicherung** > **Security Suite-Einstellungen**. Die Seite *Security Suite-Einstellungen* wird angezeigt.

CPU-Schutzmechanismus: Aktiviert weist darauf hin, dass SCT aktiviert ist.

SCHRITT 2 Klicken Sie neben **CPU-Auslastung** auf **Details**, um die Seite „CPU-Auslastung“ aufzurufen und die Anzeige der CPU-Ressourcenauslastung zu aktivieren.

SCHRITT 3 Klicken Sie neben **TCP-SYN-Schutz** auf **Bearbeiten**, um die Seite „SYN-Schutz“ aufzurufen und diese Funktion zu aktivieren.

SCHRITT 4 Wählen Sie **DoS-Prävention**, um die Funktion zu aktivieren.

- **Deaktivieren**: Deaktivieren der Funktion.
- **Prävention auf Systemebene**: Aktivieren Sie den Teil der Funktion, der Angriffe durch Stacheldraht-Distribution, den Invasor-Trojaner und den Back Orifice-Trojaner verhindert.
- **Prävention auf System- und Schnittstellenebene**: Aktivieren Sie den Teil der Funktion, der Angriffe durch Stacheldraht-Distribution, den Invasor-Trojaner und den Back Orifice-Trojaner verhindert.

SCHRITT 5 Wenn **Prävention auf Systemebene** oder **Prävention auf System- und Schnittstellenebene** ausgewählt ist, können Sie eine oder mehrere der folgenden Optionen für die DoS-Sicherung aktivieren:

- **Stacheldraht-Distribution**: TCP-Pakete, deren Quell-TCP-Port gleich 16660 ist, werden verworfen.
- **Invasor-Trojaner**: TCP-Pakete, deren Ziel-TCP-Port gleich 2140 und deren Quell-TCP-Port gleich 1024 ist, werden verworfen.
- **Back Orifice-Trojaner**: UCP-Pakete, deren Ziel-UCP-Port gleich 31337 und deren Quell-UCP-Port gleich 1024 ist, werden verworfen.

SCHRITT 6 Klicken Sie nach Bedarf auf die folgenden Optionen:

- **Ungültige Adressen**: Klicken Sie auf **Bearbeiten**, um zur Seite „Ungültige Adressen“ zu wechseln.
- **SYN-Filterung**: Klicken Sie auf **Bearbeiten**, um zur Seite „SYN-Filterung“ zu wechseln.
- **SYN-Ratenschutz** (nur in Schicht 2): Klicken Sie auf **Bearbeiten**, um zur Seite „SYN-Ratenschutz“ zu wechseln.
- **ICMP-Filterung**: Klicken Sie auf **Bearbeiten**, um zur Seite „ICMP-Filterung“ zu wechseln.
- **IP fragmentiert**: Klicken Sie auf **Bearbeiten**, um zur Seite „IP-Fragmentfilterung“ zu wechseln.

SYN-Schutz

Die Netzwerkports können von Hackern für SYN-Angriffe auf das Gerät genutzt werden, bei denen TCP-Ressourcen (Puffer) und CPU-Leistung verbraucht werden.

Da die CPU mit SCT geschützt ist, wird der TCP-Verkehr an die CPU begrenzt. Wenn jedoch ein Angriff mit einer großen Anzahl von SYN-Paketen auf einen oder mehrere Ports stattfindet, empfängt die CPU nur die Pakete des Angreifers, wodurch ein Denial of Service entsteht.

Bei aktivierter SYN-Schutzfunktion werden die von jedem Netzwerkport pro Sekunde bei der CPU eingehenden SYN-Pakete gezählt.

Wenn die Anzahl größer als der benutzerdefinierte Schwellenwert ist, wird für den Port eine Regel zur Ablehnung aller SYN-Pakete mit dieser MAC-Adresse angewendet. Die Bindung dieser Regel an den Port wird jeweils nach Ablauf des benutzerdefinierten Intervalls (Zeitspanne für SYN-Schutz) aufgehoben.

So konfigurieren Sie den SYN-Schutz:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Denial of Service-Sicherung** > **SYN-Schutz**.

SCHRITT 2 Geben Sie die Parameter ein.

- **SYN-FIN-Pakete blockieren**: Wählen Sie diese Option, um die Funktion zu aktivieren. Alle TCP-Pakete mit gesetztem SYN- und FIN-Flag werden an allen Ports gelöscht.
- **SYN-Schutzmodus**: Wählen Sie einen von drei Modi aus:
  - *Deaktivieren*: Die Funktion ist für eine bestimmte Schnittstelle deaktiviert.
  - *Bericht*: Eine SYSLOG-Meldung wird generiert. Der Status des Ports wird in **Angegriffen** geändert, wenn der Schwellenwert überschritten wird.
  - *Blockieren und melden*: Wenn ein TCP-SYN-Angriff ermittelt wird, werden für das System bestimmte TCP-SYN-Pakete gelöscht und der Status des Ports wird in **Blockiert** geändert.
- **Schwellenwert SYN-Schutz**: Anzahl der SYN-Pakete pro Sekunde, bevor SYN-Pakete blockiert werden (Regel zur Ablehnung aller SYN-Pakete mit dieser MAC-Adresse wird für den Port angewendet).
- **Zeitspanne SYN-Schutz**: Zeit in Sekunden, bevor die Blockierung der SYN-Pakete aufgehoben wird (Bindung der Regel zur Ablehnung aller SYN-Pakete mit dieser MAC-Adresse an den Port wird aufgehoben).

SCHRITT 3 Klicken Sie auf **Übernehmen**. Der SYN-Schutz wird definiert und die aktuelle Konfigurationsdatei wird aktualisiert.

In der Schnittstellentabelle für den SYN-Schutz werden die folgenden Felder für alle Ports oder LAGs angezeigt (wie vom Benutzer angefordert).

- **Aktueller Status**: Schnittstellenstatus. Folgende Werte sind gültig:
  - *Normal*: Für diese Schnittstelle wurde kein Angriff ermittelt.
  - *Blockiert*: Der Datenverkehr an dieser Schnittstelle wird nicht weitergeleitet.
  - *Angegriffen*: Für diese Schnittstelle wurde ein Angriff ermittelt.
- **Letzter Angriff**: Datum des letzten vom System ermittelten SYN-FIN-Angriffs und der Systemaktion (**Berichtet** oder **Blockiert und berichtet**).

Ungültige Adressen

Auf der Seite „Ungültige Adressen“ können IP-Adressen eingegeben werden, die bei Auftauchen im Netzwerk auf einen Angriff hinweisen. Pakete von diesen Adressen werden verworfen.

Das Gerät unterstützt einen Satz reservierter ungültiger Adressen, die nach Maßgabe des IP-Protokolls ungültig sind. Die unterstützten ungültigen Adressen sind:

- Adressen, die auf der Seite „Ungültige Adressen“ als ungültig definiert wurden.
- Adressen, die nach Maßgabe des Protokolls ungültig sind, wie beispielsweise Loopback-Adressen, einschließlich Adressen aus den folgenden Bereichen:
  - **0.0.0.0/8 (ausgenommen 0.0.0.0/32 als Quelladresse)**: Adressen in diesem Block beziehen sich auf Quell-Hosts in diesem Netzwerk.
  - **127.0.0.0/8**: Wird als Internet-Host-Loopback-Adresse verwendet.
  - **192.0.2.0/24**: Wird als TEST-NET in Dokumentations- und Beispiel-Codes verwendet.
  - **224.0.0.0/4 (als Quell-IP-Adresse)**: Wird für die Zuweisung von IPv4-Multicast-Adressen verwendet und war zuvor als Class D Address Space bekannt.
  - **240.0.0.0/4 (ausgenommen 255.255.255.255/32 als Ziel-IP-Adresse)**: Reservierter Adressbereich; war zuvor als Class E Address Space bekannt.

Sie können auch neue ungültige Adressen für die DoS-Sicherung hinzufügen. Pakete mit ungültigen Adressen werden verworfen.

So definieren Sie ungültige Adressen:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Denial of Service-Sicherung** > **Ungültige Adressen**.

SCHRITT 2 Wählen Sie **Reservierte ungültige Adressen**, und klicken Sie auf **Übernehmen**, um die reservierten ungültigen Adressen in die Liste für die Sicherung auf Systemebene aufzunehmen.

SCHRITT 3 Um eine ungültige Adresse hinzuzufügen, klicken Sie auf **Hinzufügen**.

SCHRITT 4 Geben Sie die Parameter ein.

- **IP-Version**: Die unterstützte IP-Version. Aktuell wird nur IPv4 unterstützt.
- **IP-Adresse**: Geben Sie eine IP-Adresse ein, die abgelehnt werden soll. Folgende Werte sind gültig:
  - *Aus der Liste reservierter Adressen*: Wählen Sie eine bekannte IP-Adresse aus der Liste reservierter Adressen aus.
  - *Neue IP-Adresse*: Geben Sie eine IP-Adresse ein.
- **Maske**: Geben Sie die Maske der IP-Adresse ein, um einen Bereich von IP-Adressen zu definieren, die abgelehnt werden sollen. Folgende Werte sind möglich:
  - *Netzwerkmaske*: Die Netzwerkmaske im Dotted-Decimal-Format.
  - *Präfixlänge*: Geben Sie die Maske der IP-Adresse ein, um den Bereich der IP-Adressen zu definieren, für den die Denial of Service-Sicherung aktiviert werden soll.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die ungültigen Adressen werden in die aktuelle Konfigurationsdatei geschrieben.

SYN-Filterung

Auf der Seite „SYN-Filterung“ können Sie TCP-Pakete filtern, die ein SYN-Flag enthalten und an einen oder mehrere Ports gerichtet sind.

So definieren Sie einen SYN-Filter:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Denial of Service-Sicherung** > **SYN-Filterung**.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Schnittstelle**: Wählen Sie die Schnittstelle aus, für die der Filter definiert werden soll.
- **IPv4-Adresse**: Geben Sie die IP-Adresse ein, für die der Filter definiert werden soll, oder wählen Sie *Alle Adressen*.
- **Netzwerkmaske**: Geben Sie die Netzwerkmaske im IP-Adressformat ein, für die der Filter aktiviert werden soll.
- **TCP-Port**: Geben Sie den Ziel-TCP-Port ein, für den die Filterung aktiviert werden soll:
  - *Bekannte Ports*: Wählen Sie einen Port aus der Liste aus.

- *Benutzerdefiniert*: Geben Sie eine Port-Nummer ein.
- *Alle Ports*: Wählen Sie diese Option, wenn die Filterung für alle Ports aktiviert werden soll.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Der SYN-Filter wird definiert und die aktuelle Konfigurationsdatei wird aktualisiert.

SYN-Ratenschutz

Auf der Seite „SYN-Ratenschutz“ können Sie die Anzahl der am Eingangsport empfangenen SYN-Pakete begrenzen. Dadurch können die Auswirkungen von SYN-Fluten auf Server gemildert werden, indem eine Ratenbegrenzung für neue Verbindungen zur Paketverarbeitung festgelegt wird.

Diese Funktion ist nur verfügbar, wenn sich das Gerät im Falle von Sx300- und SG500-Geräten im Schicht-2-Systemmodus bzw. im Falle von SG500X- und SG500XG-Geräten im nativen Modus befindet.

So definieren Sie den SYN-Ratenschutz:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Denial of Service-Sicherung** > **SYN-Ratenschutz**.

Auf dieser Seite wird der SYN-Ratenschutz angezeigt, der aktuell für die einzelnen Schnittstellen definiert ist:

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Schnittstelle**: Wählen Sie die Schnittstelle aus, für die der Ratenschutz definiert werden soll.
- **IP-Adresse**: Geben Sie die IP-Adresse ein, für die der SYN-Ratenschutz definiert werden soll, oder wählen Sie *Alle Adressen*. Wenn Sie die IP-Adresse eingeben, geben Sie entweder die Maske oder die Präfixlänge ein.
- **Netzwerkmaske**: Wählen Sie das Format für die Subnetzmaske der Quell-IP-Adresse aus, und geben Sie einen Wert in eines der Felder ein:
  - *Maske*: Wählen Sie das Subnetz aus, zu dem die Quell-IP-Adresse gehört, und geben Sie die Subnetzmaske im Dotted-Decimal-Format ein.
  - *Präfixlänge*: Wählen Sie die Präfixlänge aus, und geben Sie die Anzahl der Bits ein, die das Präfix der Quell-IP-Adresse umfasst.
- **SYN-Ratenbegrenzung**: Geben Sie die Anzahl SYN-Pakete ein, deren Empfang zulässig sein soll.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Der SYN-Ratenschutz wird definiert und die aktuelle Konfiguration wird aktualisiert.

ICMP-Filterung

Auf der Seite „ICMP-Filterung“ können Sie die Blockierung von ICMP-Paketen von bestimmten Quellen aktivieren. So kann im Fall eines ICMP-Angriffs die Last für das Netzwerk reduziert werden.

So definieren Sie die ICMP-Filterung:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Denial of Service-Sicherung** > **ICMP-Filterung**.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Schnittstelle**: Wählen Sie die Schnittstelle aus, für die die ICMP-Filterung definiert werden soll.
- **IP-Adresse**: Geben Sie die IPv4-Adresse ein, für die die ICMP-Paketfilterung aktiviert werden soll, oder wählen Sie *Alle Adressen* aus, um ICMP-Pakete von allen Quelladressen zu blockieren. Wenn Sie die IP-Adresse eingeben, geben Sie entweder die Maske oder die Präfixlänge ein.
- **Netzwerkmaske**: Wählen Sie das Format für die Subnetzmaske der Quell-IP-Adresse aus, und geben Sie einen Wert in eines der Felder ein:
  - *Maske*: Wählen Sie das Subnetz aus, zu dem die Quell-IP-Adresse gehört, und geben Sie die Subnetzmaske im Dotted-Decimal-Format ein.
  - *Präfixlänge*: Wählen Sie die Präfixlänge aus, und geben Sie die Anzahl der Bits ein, die das Präfix der Quell-IP-Adresse umfasst.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die ICMP-Filterung wird definiert und die aktuelle Konfiguration wird aktualisiert.

IP-Fragmentfilterung

Auf der Seite „IP-fragmentiert“ können Sie fragmentierte IP-Pakete blockieren.

So konfigurieren Sie die Blockierung fragmentierter IP-Pakete:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Denial of Service-Sicherung** > **IP-Fragmentfilterung**.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Schnittstelle**: Wählen Sie die Schnittstelle aus, für die die IP-Fragmentierung definiert werden soll.
- **IP-Adresse**: Geben Sie ein IP-Netzwerk ein, von dem die fragmentierten IP-Pakete gefiltert werden sollen, oder wählen Sie *Alle Adressen* aus, um fragmentierte IP-Pakete von allen Adressen zu blockieren. Wenn Sie die IP-Adresse eingeben, geben Sie entweder die Maske oder die Präfixlänge ein.

- **Netzwerkmaske**: Wählen Sie das Format für die Subnetzmaske der Quell-IP-Adresse aus, und geben Sie einen Wert in eines der Felder ein:
  - *Maske*: Wählen Sie das Subnetz aus, zu dem die Quell-IP-Adresse gehört, und geben Sie die Subnetzmaske im Dotted-Decimal-Format ein.
  - *Präfixlänge*: Wählen Sie die Präfixlänge aus, und geben Sie die Anzahl der Bits ein, die das Präfix der Quell-IP-Adresse umfasst.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die IP-Fragmentierung wird definiert und die aktuelle Konfigurationsdatei wird aktualisiert.

DHCP-Snooping

Weitere Informationen hierzu finden Sie unter **DHCPv4-Snooping/-Relais**.

IP Source Guard

IP Source Guard ist eine Sicherheitsfunktion, mit der Sie Datenverkehrsangriffe verhindern können, die entstehen, wenn ein Host die IP-Adresse seines Nachbarn zu verwenden versucht.

Wenn IP Source Guard aktiviert ist, überträgt das Gerät IP-Datenverkehr von Clients nur an IP-Adressen, die in der DHCP-Snooping-Bindungsdatenbank enthalten sind. Dazu gehören durch DHCP-Snooping hinzugefügte Adressen sowie manuell hinzugefügte Einträge.

Wenn das Paket einem Eintrag in der Datenbank entspricht, wird es vom Gerät weitergeleitet. Anderenfalls wird es gelöscht.

Interaktionen mit anderen Funktionen

Die folgenden Punkte sind für IP Source Guard relevant:

- DHCP-Snooping muss global aktiviert sein, damit IP Source Guard für eine Schnittstelle aktiviert werden kann.
- IP Source Guard kann nur in folgenden Fällen an einer Schnittstelle aktiv sein:
  - DHCP-Snooping ist in mindestens einem der VLANs des Ports aktiviert.
  - Die Schnittstelle ist für DHCP nicht vertrauenswürdig. Alle Pakete an vertrauenswürdigen Ports werden weitergeleitet.

- Wenn ein Port für DHCP vertrauenswürdig ist, können Sie die Filterung statischer IP-Adressen konfigurieren, obwohl IP Source Guard in diesem Fall nicht aktiv ist. Dazu aktivieren Sie IP Source Guard an dem Port.
- Wenn der Status des Ports von „Für DHCP nicht vertrauenswürdig“ zu „Für DHCP vertrauenswürdig“ wechselt, bleiben die Einträge für die Filterung statischer IP-Adressen als inaktive Einträge in der Bindungsdatenbank.
- Portsicherheit kann nicht aktiviert werden, wenn Quell-IP-Filterung und MAC-Adressfilterung an einem Port konfiguriert sind.
- IP Source Guard verwendet TCAM-Ressourcen und erfordert eine einzige TCAM-Regel pro IP Source Guard-Adresseintrag. Wenn die Anzahl der IP Source Guard-Einträge die Anzahl der verfügbaren TCAM-Regeln überschreitet, sind die überzähligen Adressen inaktiv.

Filterung

Wenn IP Source Guard für einen Port aktiviert ist, gilt Folgendes:

- Aufgrund von DHCP-Snooping zulässige DHCP-Pakete werden zugelassen.
- Wenn die Filterung von Quell-IP-Adressen aktiviert ist, gilt Folgendes:
  - IPv4-Verkehr: Nur Verkehr mit einer dem Port zugeordneten Quell-IP-Adresse ist zulässig.
  - Nicht-IPv4-Verkehr: Zulässig (einschließlich ARP-Paketen).

Konfigurieren des IP Source Guard-Workflows

So konfigurieren Sie IP Source Guard:

SCHRITT 1 Aktivieren Sie DHCP-Snooping auf der Seite „IP-Konfiguration > DHCP > Eigenschaften“ oder auf der Seite „Sicherheit > DHCP-Snooping > Eigenschaften“.

SCHRITT 2 Definieren Sie auf der Seite „IP-Konfiguration > DHCP > Schnittstelleneinstellungen“ die VLANs, in denen DHCP-Snooping aktiviert ist.

SCHRITT 3 Konfigurieren Sie auf der Seite „IP-Konfiguration > DHCP > DHCP-Snooping-Schnittstelle“ Schnittstellen als vertrauenswürdig oder nicht vertrauenswürdig.

SCHRITT 4 Aktivieren Sie IP Source Guard auf der Seite „Sicherheit > IP Source Guard > Eigenschaften“.

SCHRITT 5 Aktivieren Sie auf der Seite „Sicherheit > IP Source Guard > Schnittstelleneinstellungen“ IP Source Guard nach Bedarf für die nicht vertrauenswürdigen Schnittstellen.

SCHRITT 6 Auf der Seite „Sicherheit > IP Source Guard > Bindungsdatenbank“ können Sie Einträge in der Bindungsdatenbank anzeigen.

Aktivieren von IP Source Guard

So aktivieren Sie IP Source Guard global:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **IP Source Guard** > **Eigenschaften**.

SCHRITT 2 Wählen Sie **Aktivieren** aus, um IP Source Guard global zu aktivieren.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um IP Source Guard zu aktivieren.

Konfigurieren von IP Source Guard an Schnittstellen

Wenn IP Source Guard für vertrauenswürdige Ports/LAGs aktiviert ist, werden aufgrund von DHCP-Snooping zulässige DHCP-Pakete übertragen. Wenn die Filterung von Quell-IP-Adressen aktiviert ist, wird die Paketübertragung wie folgt zugelassen:

- **IPv4-Verkehr**: Nur IPv4-Verkehr mit einer dem jeweiligen Port zugeordneten Quell-IP-Adresse ist zulässig.
- **Nicht-IPv4-Verkehr**: Sämtlicher Nicht-IPv4-Verkehr ist zulässig.

Weitere Informationen zum Aktivieren von IP Source Guard an Schnittstellen finden Sie unter **Interaktionen mit anderen Funktionen**.

So konfigurieren Sie IP Source Guard an Schnittstellen:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **IP Source Guard** > **Schnittstelleneinstellungen**.

SCHRITT 2 Wählen Sie „Port/LAG“ im Feld **Filter** aus und klicken Sie auf **Los**. Die Ports/LAGs dieser Einheit werden zusammen mit folgenden Informationen angezeigt:

- **IP Source Guard**: Gibt an, ob IP Source Guard an dem Port aktiviert ist.
- **Vertrauenswürdige DHCP-Snooping-Schnittstellen**: Gibt an, ob es sich um eine für DHCP vertrauenswürdige Schnittstelle handelt.

SCHRITT 3 Wählen Sie den Port oder die LAG aus und klicken Sie auf **Bearbeiten**. Wählen Sie die Option **Aktivieren** im Feld **IP Source Guard** aus, um IP Source Guard an der Schnittstelle zu aktivieren.

SCHRITT 4 Klicken Sie auf **Übernehmen**, um die Einstellung in die aktuelle Konfigurationsdatei zu kopieren.

Bindungsdatenbank

IP Source Guard verwendet die DHCP-Snooping-Bindungsdatenbank, um Pakete von nicht vertrauenswürdigen Ports zu überprüfen. Wenn das Gerät zu viele Einträge in die DHCP-Snooping-Bindungsdatenbank zu schreiben versucht, werden die überzähligen Einträge als inaktive Einträge beibehalten. Einträge werden nach Ablauf ihrer Lease-Dauer gelöscht. Dann können inaktive Einträge aktiviert werden.

Weitere Informationen hierzu finden Sie unter **DHCPv4-Snooping/-Relais**.

HINWEIS Auf der Seite „Bindungsdatenbank“ werden **nur** die Einträge aus der DHCP-Snooping-Bindungsdatenbank angezeigt, die für Ports definiert sind, an denen IP Source Guard aktiviert ist.

Um die DHCP-Snooping-Bindungsdatenbank und die TCAM-Verwendung anzuzeigen, legen Sie **Inaktive einfügen** fest:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **IP Source Guard** > **Bindungsdatenbank**.

SCHRITT 2 Die DHCP-Snooping-Bindungsdatenbank verwendet zum Verwalten der Datenbank TCAM-Ressourcen. Füllen Sie das Feld **Inaktive einfügen** aus, um auszuwählen, wie häufig das Gerät versuchen soll, inaktive Einträge zu aktivieren. Die folgenden Optionen sind verfügbar:

- **Wiederholungsversuche**: Die Häufigkeit, mit der die TCAM-Ressourcen überprüft werden.
- **Nie**: Es wird nie versucht, inaktive Adressen zu reaktivieren.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um die obigen Änderungen in der aktuellen Konfiguration zu speichern, und/oder auf **Jetzt wiederholen**, um die TCAM-Ressourcen zu überprüfen.

Die Einträge in der Bindungsdatenbank werden angezeigt:

- **VLAN-ID:** Das VLAN, in dem ein Paket erwartet wird.
- **MAC-Adresse**: Die MAC-Adresse, die abgeglichen werden soll.
- **IP-Adresse**: Die IP-Adresse, die abgeglichen werden soll.
- **Schnittstelle**: Die Schnittstelle, an der ein Paket erwartet wird.
- **Status**: Zeigt an, ob die Schnittstelle aktiv ist.
- **Typ**: Zeigt an, ob es sich um einen dynamischen oder statischen Eintrag handelt.

- **Grund**: Wenn die Schnittstelle nicht aktiv ist, wird hier der Grund angezeigt. Folgende Gründe sind möglich:
  - *Kein Problem*: Die Schnittstelle ist aktiv.
  - *Kein Snoop-VLAN*: DHCP-Snooping ist im VLAN nicht aktiviert.
  - *Vertrauenswürdiger Port*: Der Port ist vertrauenswürdig.
  - *Ressourcenproblem*: Die TCAM-Ressourcen sind erschöpft.

Zum Anzeigen einer Teilmenge dieser Einträge geben Sie die entsprechenden Suchkriterien ein und klicken Sie auf **Los**.

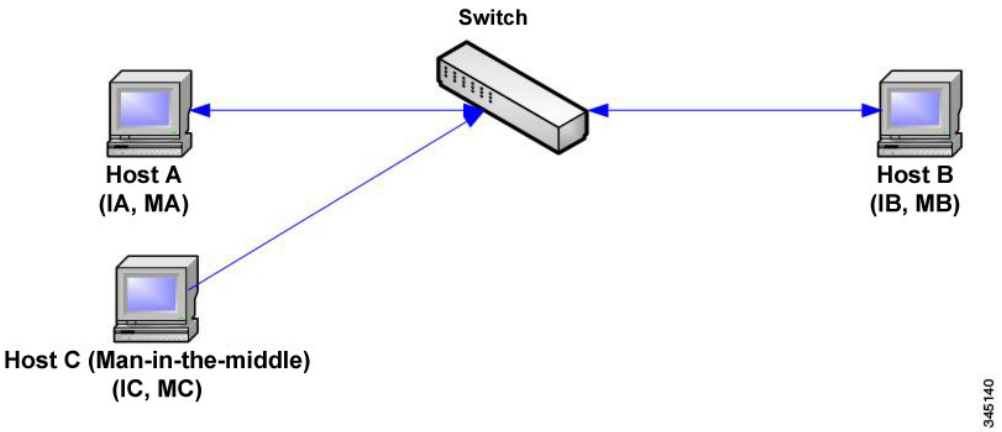
ARP-Prüfung

ARP ermöglicht die IP-Kommunikation innerhalb einer Schicht-2-Broadcast-Domäne durch Zuordnen von IP-Adressen zu MAC-Adressen.

Ein böswilliger Benutzer kann mit einem Schicht-2-Netzwerk verbundene Hosts, Switches und Router angreifen, indem er die ARP-Caches der mit dem Subnetz verbundenen Systeme „vergiftet“ und Verkehr abfängt, der für andere Hosts im Subnetz gedacht ist. Dies ist möglich, da ARP eine unnötige Antwort von einem Host zulässt, auch wenn keine ARP-Anforderung empfangen wurde. Nach dem Angriff fließt der gesamte Verkehr von dem angegriffenen Gerät durch den Computer des Angreifers und dann an den Router, Switch oder Host.

Die folgende Abbildung zeigt ein Beispiel für ARP Cache Poisoning.

ARP Cache Poisoning



Host A, B und C sind mit dem Switch an den Schnittstellen A, B und C verbunden, die sich alle im gleichen Subnetz befinden. Die IP- und MAC-Adressen stehen in Klammern. So verwendet beispielsweise Host A die IP-Adresse IA und die MAC-Adresse MA. Wenn Host A auf der IP-Schicht mit Host B kommunizieren muss, sendet er eine ARP-Anforderung für die MAC-Adresse, die IP-Adresse B zugeordnet ist. Host B antwortet mit einer ARP-Antwort. Der Switch und Host A aktualisieren ihren ARP-Cache mit der MAC- und IP-Adresse von Host B.

Host C kann die ARP-Caches des Switch und von Host A und Host B vergiften, indem er gefälschte ARP-Antworten mit Bindungen für einen Host mit der IP-Adresse IA (oder IB) und der MAC-Adresse MC sendet. Hosts mit vergiftetem ARP-Cache verwenden die MAC-Adresse MC als Ziel-MAC-Adresse für Verkehr, der für IA oder IB gedacht ist. Auf diese Weise kann Host C diesen Verkehr abfangen. Da Host C die IA und IB zugeordneten tatsächlichen MAC-Adressen kennt, kann er den abgefangenen Verkehr an diese Hosts weiterleiten und dabei die richtige MAC-Adresse als Ziel verwenden. Host C hat sich in den Verkehrsstrom von Host A an Host B eingeschaltet, ein klassischer Man-in-the-Middle-Angriff.

So verhindert ARP Cache Poisoning:

Für die ARP-Prüfungsfunktion sind Schnittstellen vertrauenswürdig oder nicht vertrauenswürdig (siehe Seite „Sicherheit > ARP-Prüfung > Schnittstelleneinstellung“).

Schnittstellen werden vom Benutzer wie folgt klassifiziert:

- **Vertrauenswürdig**: Pakete werden nicht überprüft.
- **Nicht vertrauenswürdig**: Pakete werden wie oben beschrieben überprüft.

Die ARP-Prüfung wird nur für nicht vertrauenswürdige Schnittstellen ausgeführt. An der vertrauenswürdigen Schnittstelle empfangene ARP-Pakete werden einfach weitergeleitet.

Beim Eintreffen eines Pakets an nicht vertrauenswürdigen Schnittstellen wird folgende Logik angewendet:

- Die Regeln für ARP-Zugriffssteuerung werden nach der IP- bzw. MAC-Adresse des Pakets durchsucht. Wenn die IP-Adresse gefunden wird und die MAC-Adresse in der Liste mit der MAC-Adresse des Pakets übereinstimmt, ist das Paket gültig. Anderenfalls ist es nicht gültig.
- Wenn die IP-Adresse des Pakets nicht gefunden wurde und DHCP-Snooping für das VLAN des Pakets aktiviert ist, wird die DHCP-Snooping-Bindungsdatenbank nach dem <VLAN/IP-Adresse>-Paar des Pakets durchsucht. Wenn das <VLAN/IP-Adresse>-Paar gefunden wurde und die MAC-Adresse und die Schnittstelle in der Datenbank mit der MAC-Adresse des Pakets und der Eingangsschnittstelle übereinstimmen, ist das Paket gültig.
- Wenn die IP-Adresse des Pakets nicht in den Regeln für ARP-Zugriffssteuerung oder in der DHCP-Snooping-Bindungsdatenbank gefunden wurde, ist das Paket ungültig und wird gelöscht. Es wird eine SYSLOG-Nachricht generiert.
- Wenn ein Paket gültig ist, wird es weitergeleitet und der ARP-Cache wird aktualisiert.

Wenn die Option „ARP-Paketvalidierung“ ausgewählt ist (Seite „Eigenschaften“), werden die folgenden zusätzlichen Überprüfungen ausgeführt:

- **Quell-MAC**: Vergleicht die Quell-MAC-Adresse des Pakets im Ethernet-Header mit der MAC-Adresse des Absenders in der ARP-Anforderung. Diese Überprüfung wird für ARP-Anforderungen und -Antworten ausgeführt.
- **Ziel-MAC**: Vergleicht die Ziel-MAC-Adresse des Pakets im Ethernet-Header mit der MAC-Adresse der Zielschnittstelle. Diese Überprüfung wird für ARP-Antworten ausgeführt.
- **IP-Adressen**: Vergleicht den ARP-Hauptteil auf ungültige und unerwartete IP-Adressen. Zu den Adressen gehören 0.0.0.0, 255.255.255.255 und alle IP-Multicast-Adressen.

Pakete mit ungültigen ARP-Prüfungsbindungen werden protokolliert und gelöscht.

In der ARP-Zugriffssteuerungstabelle können maximal 1024 Einträge definiert werden.

Interaktion zwischen ARP-Prüfung und DHCP-Snooping

Wenn DHCP-Snooping aktiviert ist, verwendet die ARP-Prüfung zusätzlich zu den Regeln für die ARP-Zugriffssteuerung die DHCP-Snooping-Bindungsdatenbank. Wenn DHCP-Snooping nicht aktiviert ist, werden nur die Regeln für die ARP-Zugriffssteuerung verwendet.

ARP-Standardeinstellungen

Die folgende Tabelle beschreibt die ARP-Standardeinstellungen:

Option	Standardzustand
Dynamische ARP-Prüfung	Nicht aktiviert
ARP-Paketvalidierung	Nicht aktiviert
ARP-Prüfung im VLAN aktiviert	Nicht aktiviert
Protokollpufferintervall	SYSLOG-Nachrichten für gelöschte Pakete werden alle fünf Sekunden generiert.

Workflow der ARP-Prüfung

So konfigurieren Sie die ARP-Prüfung:

SCHRITT 1 Verwenden Sie zum Aktivieren der ARP-Prüfung und zum Konfigurieren verschiedener Optionen die Seite „Sicherheit > ARP-Prüfung > Eigenschaften“.

SCHRITT 2 Verwenden Sie zum Konfigurieren von Schnittstellen als für ARP vertrauenswürdig oder nicht vertrauenswürdig die Seite „Sicherheit > ARP-Prüfung > Schnittstelleneinstellung“.

SCHRITT 3 Verwenden Sie zum Hinzufügen von Regeln die Seiten „Sicherheit > ARP-Prüfung > ARP-Zugriffssteuerung und Regeln für ARP-Zugriffssteuerung“.

SCHRITT 4 Verwenden Sie zum Definieren der VLANs, für die die ARP-Prüfung aktiviert ist, und der Zugriffssteuerungsregeln für die einzelnen VLANs die Seite „Sicherheit > ARP-Prüfung > VLAN-Einstellungen“.

Definieren von Eigenschaften der ARP-Prüfung

So konfigurieren Sie die ARP-Prüfung:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **ARP-Prüfung > Eigenschaften**.

Geben Sie Werte für die folgenden Felder ein:

- **ARP-Prüfungsstatus:** Wählen Sie diese Option aus, um die ARP-Prüfung zu aktivieren.

- **ARP-Paketvalidierung**: Wählen Sie diese Option aus, um die folgenden Überprüfungen zu aktivieren:
  - **Quell-MAC**: Vergleicht die Quell-MAC-Adresse des Pakets im Ethernet-Header mit der MAC-Adresse des Absenders in der ARP-Anforderung. Diese Überprüfung wird für ARP-Anforderungen und -Antworten ausgeführt.
  - **Ziel-MAC**: Vergleicht die Ziel-MAC-Adresse des Pakets im Ethernet-Header mit der MAC-Adresse der Zielschnittstelle. Diese Überprüfung wird für ARP-Antworten ausgeführt.
  - **IP-Adressen**: Vergleicht den ARP-Hauptteil auf ungültige und unerwartete IP-Adressen. Zu den Adressen gehören 0.0.0.0, 255.255.255.255 und alle IP-Multicast-Adressen.
- **Protokollpufferintervall**: Wählen Sie eine der folgenden Optionen aus:
  - **Wiederholungsversuche:** Aktiviert das Senden von SYSLOG-Nachrichten für gelöschte Pakete. Geben Sie die Häufigkeit ein, mit der die Nachrichten gesendet werden.
  - **Nie:** Deaktiviert SYSLOG-Nachrichten für gelöschte Pakete.

SCHRITT 2 Klicken Sie auf **Übernehmen**. Die Einstellungen werden definiert und die aktuelle Konfigurationsdatei wird aktualisiert.

Definieren von Einstellungen für Dynamische ARP-Prüfung-Schnittstellen

Pakete von nicht vertrauenswürdigen Ports/LAGs werden anhand der Tabelle der ARP-Zugriffsregeln und der DHCP-Snooping-Bindungsdatenbank (wenn DHCP-Snooping aktiviert ist) überprüft (siehe Seite „DHCP-Snooping-Bindungsdatenbank“).

Ports/LAGs sind standardmäßig für die ARP-Prüfung nicht vertrauenswürdig.

So ändern Sie den ARP-Vertrauensstatus eines Ports bzw. einer LAG:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **ARP-Prüfung** > **Schnittstelleneinstellungen**.

Die Ports/LAGs und der jeweilige Status (für ARP vertrauenswürdig/nicht vertrauenswürdig) werden angezeigt.

SCHRITT 2 Zum Festlegen eines Ports bzw. einer LAG als nicht vertrauenswürdig wählen Sie den Port oder die LAG aus und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Wählen Sie **Vertrauenswürdig** oder **Nicht vertrauenswürdig** aus und klicken Sie auf **Übernehmen**, um die Einstellungen in der aktuellen Konfigurationsdatei zu speichern.

Definieren der Zugriffssteuerung der ARP-Prüfung

So fügen Sie der ARP-Prüfungstabelle Einträge hinzu:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **ARP-Prüfung > ARP-Zugriffssteuerung**.

SCHRITT 2 Zum Hinzufügen eines Eintrags klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie Werte für die Felder ein:

- **ARP-Zugriffssteuerungsname**: Geben Sie einen vom Benutzer erstellten Namen ein.
- **IP-Adresse**: Die IP-Adresse des Pakets.
- **MAC-Adresse**: Die MAC-Adresse des Pakets.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Einstellungen werden definiert und die aktuelle Konfigurationsdatei wird aktualisiert.

Definieren der Regeln für Zugriffssteuerung der ARP-Prüfung

So fügen Sie einer zuvor erstellten ARP-Zugriffssteuerungsgruppe weitere Regeln hinzu:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **ARP-Prüfung > Regeln für ARP-Zugriffssteuerung**.

Die zurzeit definierten Zugriffsregeln werden angezeigt.

SCHRITT 2 Zum Hinzufügen weiterer Regeln zu einer Gruppe klicken Sie auf **Hinzufügen**.

SCHRITT 3 Wählen Sie eine Zugriffssteuerungsgruppe aus und geben Sie Werte für die Felder ein:

- **IP-Adresse**: Die IP-Adresse des Pakets.
- **MAC-Adresse**: Die MAC-Adresse des Pakets.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Einstellungen werden definiert und die aktuelle Konfigurationsdatei wird aktualisiert.

Definieren von VLAN-Einstellungen für die ARP-Prüfung

So aktivieren Sie die ARP-Prüfung für VLANs und ordnen einem VLAN Zugriffssteuerungsgruppen zu:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **ARP-Prüfung > VLAN-Einstellungen**.

SCHRITT 2 Zum Aktivieren der ARP-Prüfung für ein VLAN verschieben Sie das VLAN von der Liste **Verfügbare VLANs** in die Liste **Aktivierte VLANs**.

SCHRITT 3 Zum Zuordnen einer ARP-Zugriffssteuerungsgruppe zu einem VLAN klicken Sie auf **Hinzufügen**. Wählen Sie die VLAN-Nummer sowie eine zuvor definierte **ARP-Zugriffssteuerungsgruppe** aus.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Einstellungen werden definiert und die aktuelle Konfigurationsdatei wird aktualisiert.

Sicherheit des ersten Hops

Sicherheit: IPv6-Sicherheit des ersten Hops

23

Sicherheit: 802.1X-Authentifizierung

In diesem Abschnitt wird die 802.1X-Authentifizierung beschrieben.

Die folgenden Themen werden behandelt:

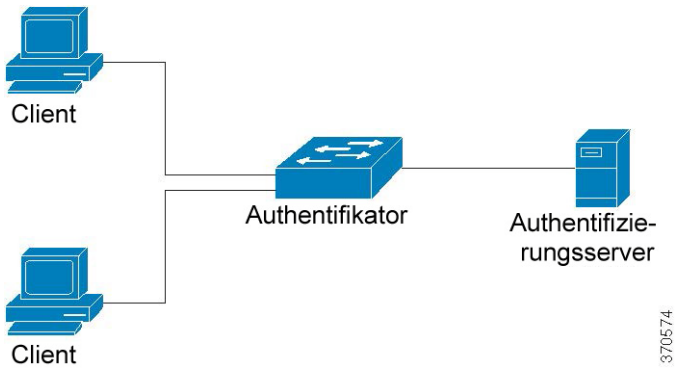
- **802.1X – Überblick**
- **Authentifikator – Übersicht**
- **Allgemeine Aufgaben**
- **802.1X-Konfiguration über die Benutzeroberfläche**
- **Definieren von Zeitbereichen**
- **Unterstützung für Authentifizierungsmethoden und Portmodi**

802.1X – Überblick

Die 802.1X-Authentifizierung verhindert, dass nicht berechtigte Clients über öffentlich zugängliche Ports eine Verbindung zum LAN herstellen können. Die 802.1X-Authentifizierung ist ein Client-Server-Modell. In diesem Modell weisen Netzwerkgeräte die folgenden, spezifischen Rollen auf:

- Client oder Anfrager
- Authentifikator
- Authentifizierungsserver

Dieser wird in der Abbildung unten beschrieben:



Ein Netzwerkgerät kann auf einem Port entweder als Client/Anfrager, als Authentifikator oder als beides auftreten.

Client oder Anfrager

Ein Client oder Anfrager ist ein Netzwerkgerät, das Zugang zum LAN erbittet. Der Client wird mit einem Authentifikator verbunden.

Wenn der Client das 802.1X-Protokoll für die Authentifizierung verwendet, führt es den Anfragerteil des 802.1X-Protokolls und den Client-Teil des EAP-Protokolls aus.

Für die Verwendung der MAC-basierten oder webbasierten Authentifizierung ist keine besondere Software auf dem Client erforderlich.

Authentifikator

Ein Authentifikator ist ein Netzwerkgerät, das Netzwerkdienste bereitstellt und mit dem Anfragerports verbunden sind.

Auf Ports werden die folgenden Authentifizierungsmodi unterstützt (diese Modi werden unter „Sicherheit > 802.1X/MAC/Web-Authentifizierung > Host und Authentifizierung“ definiert):

- **Einzelhost**: Unterstützt die Port-basierte Authentifizierung mit einem einzelnen Client pro Port.
- **Mehrfachhost**: Unterstützt die Port-basierte Authentifizierung mit mehreren Clients pro Port.
- **Mehrfachsitzungen**: Unterstützt die Client-basierte Authentifizierung mit mehreren Clients pro Port.

Weitere Informationen finden Sie unter **Port-Hostmodi**.

Es werden die folgenden Authentifizierungsmethoden unterstützt:

- **802.1X-basiert**: Wird bei allen Authentifizierungsmodi unterstützt.
- **MAC-basiert**: Wird bei allen Authentifizierungsmodi unterstützt.
- **Webbasiert**: Wird nur in den Mehrfachsitzungsmodi unterstützt.

Bei der 802.1X-basierten Authentifizierung extrahiert der Authentifikator die EAP-Nachrichten aus den 802.1X-Nachrichten (EAPOL-Frames) und leitet diese über das RADIUS-Protokoll an den Authentifizierungsserver weiter.

Bei der MAC-basierten oder webbasierten Authentifizierung führt der Authentifikator selbst den EAP-Clientteil der Software aus.

Authentifizierungsserver

Ein Authentifizierungsserver führt die eigentliche Authentifizierung auf dem Client aus. Der Authentifizierungsserver für das Gerät ist ein RADIUS-Authentifizierungsserver mit EAP-Erweiterungen.

Open Access

Die Open-Access-Funktion (Überwachungszugriff) hilft dabei, echte Authentifizierungsfehler von Fehlern zu unterscheiden, die durch eine Fehlkonfiguration und/oder ein Fehlen von Ressourcen in einer 802.1x-Umgebung verursacht wurden.

Open Access erleichtert Systemadministratoren das Nachvollziehen von Konfigurationsproblemen auf mit dem Netzwerk verbundenen Hosts, führt eine Überwachung auf Probleme durch und gestattet die Behebung dieser Probleme.

Wird Open Access auf einer Schnittstelle aktiviert, dann behandelt der Switch alle von einem RADIUS-Server erhaltenen Fehler als erfolgreich und gewährt Stationen, die an Schnittstellen angeschlossen sind, unabhängig von den Authentifizierungsergebnissen Zugriff auf das Netzwerk.

Open Access ändert das normale Verhalten, bei dem an einem Port mit aktivierter Authentifizierung Datenverkehr so lange blockiert wird, bis Authentifizierung und Autorisierung erfolgreich durchgeführt wurden. Zwar besteht das Standardverhalten noch immer darin, den gesamten Datenverkehr mit Ausnahme von EAPoL-Datenverkehr (Extensible Authentication Protocol over LAN) zu blockieren; Open Access bietet dem Administrator jedoch die Möglichkeit, uneingeschränkten Zugriff auf den gesamten Datenverkehr auch bei aktivierter Authentifizierung (auf 802.1X-, MAC- und/oder Webbasis) zu gewähren.

Wenn das RADIUS Accounting aktiviert ist, können Sie Authentifizierungsversuche protokollieren und über einen Prüfpfad Einblick in die Frage gewinnenerhalten, wer oder was Verbindungen mit Ihrem Netzwerk herstellt.

All dies wird ohne Auswirkungen auf die Endbenutzer oder auf mit dem Netzwerk verbundene Hosts erreicht. Open Access kann auf der Seite **802.1X-Portauthentifizierung** aktiviert werden.

Authentifikator – Übersicht

Administrative Port-Authentifizierungsstatus

Der administrative Status des Ports bestimmt, ob der Client Zugang zum Netzwerk erhält.

Der administrative Port-Status kann auf der Seite „Sicherheit > 802.1X/MAC/Web-Authentifizierung > Port-Authentifizierung“ definiert werden.

Die folgenden Werte sind verfügbar:

- **Autorisierung erzwingen**

  Die Port-Authentifizierung wird deaktiviert, und der Port überträgt den gesamten Datenverkehr gemäß seiner statischen Konfiguration, ohne dass eine Authentifizierung erforderlich ist. Der Switch sendet das 802.1X-EAP-Paket mit der integrierten EAP-Erfolgsmeldung, sobald es die 802.1X-EAPOL-Startnachricht erhält.

  Dies ist der Standardstatus.

- **Nicht-Autorisierung erzwingen**

  Die Port-Authentifizierung wird deaktiviert, und der Port überträgt den gesamten Datenverkehr über das Gast-VLAN und nicht authentifizierte VLANs. Weitere Informationen finden Sie unter **Definieren der Host- und Sitzungsauthentifizierung**. Der Switch sendet 802.1X-EAP-Pakete mit integrierten EAP-Fehlermeldungen, sobald es die 802.1X-EAPOL-Startnachrichten erhält.

- **Automatisch**

  Aktiviert die 802.1X-Authentifizierungen gemäß dem konfigurierten Port-Hostmodus und den auf dem Port konfigurierten Authentifizierungsmethoden.

Port-Hostmodi

Ports können in die folgenden Port-Hostmodi versetzt werden (die auf der Seite „Sicherheit > 802.1X/MAC/Web -Authentifizierung > Host und Authentifizierung“ definiert werden):

- **Einzelhost-Modus**

  Ein Port wird autorisiert, wenn ein autorisierter Client verfügbar ist. Pro Port kann nur ein Host autorisiert werden.

  Wenn ein Port nicht autorisiert wurde und das Gast-VLAN aktiviert ist, wird Datenverkehr ohne Tags erneut dem Gast-VLAN zugeordnet. Datenverkehr mit Tags wird nur dann weitergeleitet, wenn er zum Gast-VLAN oder zu einem nicht authentifizierten VLAN gehört. Wenn ein Gast-VLAN auf dem Port nicht aktiviert ist, wird nur Datenverkehr mit Tags überbrückt, der zu nicht authentifizierten VLANs gehört.

Wenn ein Port autorisiert ist, wird Datenverkehr vom autorisierten Host mit und ohne Tags auf Basis der Portkonfiguration für die statische VLAN-Mitgliedschaft überbrückt. Datenverkehr von anderen Hosts wird nicht weitergeleitet.

Ein Benutzer kann festlegen, dass Datenverkehr ohne Tags von einem autorisierten Host erneut einem VLAN zugeordnet wird, der im Rahmen des Authentifizierungsprozesses durch einen RADIUS-Server zugewiesen wurde. Datenverkehr mit Tags wird nur dann weitergeleitet, wenn er zu einem zugewiesenen RADIUS-VLAN oder zu den nicht authentifizierten VLANs gehört. Die RADIUS-VLAN-Zuordnung auf einem Port wird auf der Seite „Sicherheit > 802.1X/MAC/Web-Authentifizierung > Port-Authentifizierung“ definiert.

- **Mehrfachhost-Modus**

  Ein Port wird autorisiert, wenn mindestens ein autorisierter Client vorhanden ist.

  Wenn ein Port nicht autorisiert wurde und ein Gast-VLAN aktiviert ist, wird Datenverkehr ohne Tags erneut dem Gast-VLAN zugeordnet. Datenverkehr mit Tags wird nur dann weitergeleitet, wenn er zum Gast-VLAN oder zu einem nicht authentifizierten VLAN gehört. Wenn ein Gast-VLAN auf einem Port nicht aktiviert ist, wird nur Datenverkehr mit Tags überbrückt, der zu nicht authentifizierten VLANs gehört.

  Wenn ein Port autorisiert wird, wird Datenverkehr mit und ohne Tags von allen Hosts, die mit dem Port verbunden sind, auf Basis der Portkonfiguration für die statische VLAN-Mitgliedschaft überbrückt.

  Sie können festlegen, dass Datenverkehr ohne Tags von einem autorisierten Port erneut einem VLAN zugeordnet wird, der im Rahmen des Authentifizierungsprozesses durch einen RADIUS-Server zugewiesen wurde. Datenverkehr mit Tags wird nur dann weitergeleitet, wenn er zu einem zugewiesenen RADIUS-VLAN oder den nicht authentifizierten VLANs gehört. Die RADIUS-VLAN-Zuordnung auf einem Port wird auf der Seite „Port-Authentifizierung“ festgelegt.

- **Mehrfachsitzungsmodus**

  Im Gegensatz zu den Einzelhost- und Mehrfachhost-Modi weist ein Port im Mehrfachsitzungsmodus keinen Authentifizierungsstatus auf. Dieser Status wird jedem Client zugewiesen, der mit dem Port verbunden ist. Dieser Modus macht eine TCAM-Suche erforderlich. Da Switche im Schicht-3-Systemmodus keiner TCAM-Suche für Mehrfachsitzungen zugewiesen wurden, unterstützen sie nur eine begrenzte Form des Mehrfachsitzungsmodus, bei dem Gast-VLAN- und RADIUS-VLAN-Attribute nicht unterstützt werden. Die maximale Anzahl an autorisierten Hosts, die auf dem Port unterstützt wird, wird auf der Seite „Port-Authentifizierung“ definiert.

  Datenverkehr mit Tags, der zu einem nicht authentifizierten VLAN gehört, wird immer überbrückt, und zwar unabhängig davon, ob der Host autorisiert ist oder nicht.

  Datenverkehr mit und ohne Tags von nicht autorisierten Hosts, die nicht zu einem nicht authentifizierten VLAN gehören, wird dem Gast-VLAN neu zugeordnet, wenn er auf dem VLAN definiert und aktiviert wird, oder er wird gelöscht, wenn das Gast-VLAN nicht auf dem Port aktiviert wird.

Wenn ein autorisierter Host über einen RADIUS-Server einem VLAN zugewiesen wird, wird der gesamte Datenverkehr mit und ohne Tags, der nicht zum nicht authentifizierten VLAN gehört, über das VLAN überbrückt. Wenn das VLAN nicht zugewiesen wurde, wird der gesamte Datenverkehr auf der Basis der Portkonfiguration für die VLAN-Mitgliedschaft überbrückt.

Die folgenden Geräte unterstützen den Mehrfachsitzungsmodus ohne Gast-VLAN und RADIUS-VLAN-Zuordnung:

- Sx500/ESW2-550X im Schicht-3-Routermodus
- SG500X im Basis- und erweiterten Hybrid-Stacking-Modus
- SG500XG

Mehrere Authentifizierungsmethoden

Wenn mehr als ein Authentifizierungsverfahren auf dem Switch aktiviert ist, wird die folgende Hierarchie für Authentifizierungsmethoden angewendet:

- 802.1X-Authentifizierung: Am höchsten
- Webbasierte Authentifizierung
- MAC-basierte Authentifizierung: Am niedrigsten

Es können mehrere Methoden gleichzeitig ausgeführt werden. Sobald eine Methode erfolgreich beendet wurde, wird der Client autorisiert, Methoden mit niedrigerer Priorität werden angehalten, und Methoden mit höherer Priorität werden fortgesetzt.

Wenn eine der gleichzeitig ausgeführten Authentifizierungsmethoden scheitert, werden die übrigen Methoden fortgesetzt.

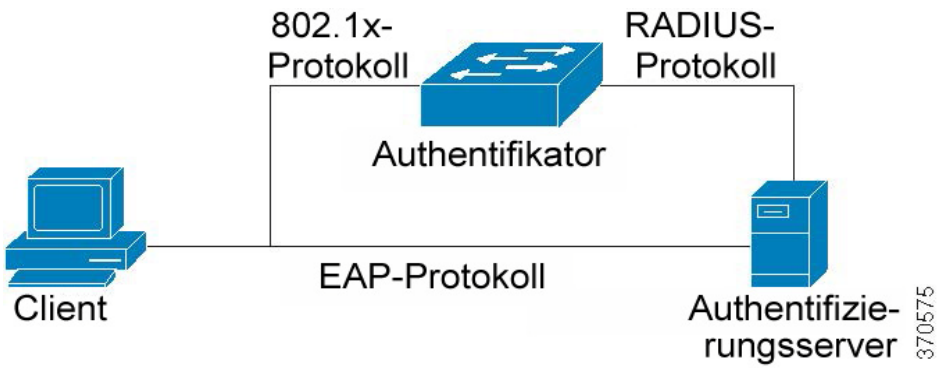
Wenn eine Authentifizierungsmethode für einen Client erfolgreich beendet wird, der durch eine Authentifizierungsmethode mit niedrigerer Priorität authentifiziert wird, werden die Attribute der neuen Authentifizierungsmethode angewendet. Sollte die neue Methode scheitern, wird der Client über die alte Methode autorisiert.

802.1X-basierte Authentifizierung

Der 802.1X-basierte Authentifikator leitet transparente EAP-Nachrichten zwischen 802.1X-Anfragern und Authentifizierungsservern weiter. Die EAP-Nachrichten zwischen Anfragern und dem Authentifikator werden in 802.1X-Nachrichten gekapselt, und die EAP-Nachrichten zwischen dem Authentifikator und den Authentifizierungsservern werden in die RADIUS-Nachrichten gekapselt.

Dies wird im Folgenden beschrieben:

Abbildung 3 802.1X-basierte Authentifizierung

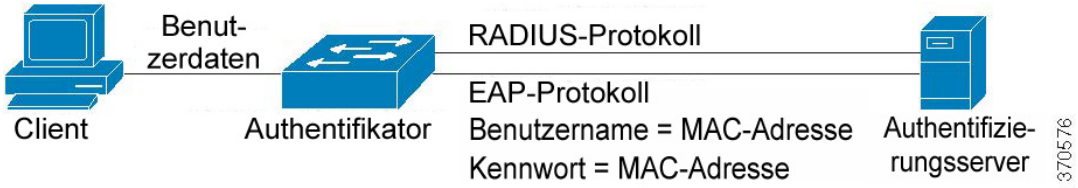


MAC-basierte Authentifizierung

Die MAC-basierte Authentifizierung ist eine Alternative zur 802.1X-Authentifizierung; sie ermöglicht den Netzwerkzugriff für Geräte (z. B. Drucker und IP-Telefone), die nicht mit der 802.1X-Anfragerfunktion ausgestattet sind. Die MAC-basierte Authentifizierung verwendet die MAC-Adresse des verbundenen Geräts, um den Netzwerkzugriff zu genehmigen oder zu verweigern.

In diesem Fall unterstützt der Switch die EAP-MD5-Funktion; hier sind Benutzername und Kennwort gemäß der folgenden Abbildung identisch mit der Client-MAC-Adresse.

Abbildung 4 MAC-basierte Authentifizierung



Diese Methode weist keine spezifische Konfiguration auf.

Webbasierte Authentifizierung

Die webbasierte Authentifizierung wird verwendet, um Endbenutzer zu authentifizieren, die Zugriff auf ein Netzwerk über einen Switch beantragen. Auf diese Weise können Clients, die direkt mit dem Switch verbunden sind, über ein Captive-Portal-Verfahren authentifiziert werden, bevor dem Client der Zugriff auf das Netzwerk eingeräumt wird. Bei der webbasierten Authentifizierung handelt es sich um eine Client-basierte Authentifizierung, die im Mehrfachsitzungsmodus im Schicht-2- und Schicht-3-Systemmodus unterstützt wird.

Diese Authentifizierungsmethode wird pro Port aktiviert, und wenn ein Port aktiviert wird, muss jeder Host sich selbst authentifizieren, um Zugriff auf das Netzwerk zu erhalten. So können auf einem aktivierten Port also sowohl authentifizierte als auch nicht authentifizierte Hosts vorhanden sein.

Wenn die webbasierte Authentifizierung auf einem Port aktiviert ist, ignoriert der Switch den gesamten Datenverkehr, der von nicht authentifizierten Clients am Port eingeht, mit Ausnahme der folgenden Pakete: ARP, DHCP und DNS. Diese Pakete können durch den Switch weitergeleitet werden, so dass selbst nicht autorisierte Clients eine IP-Adresse erhalten können und somit in der Lage sind, Host- oder Domänennamen aufzulösen.

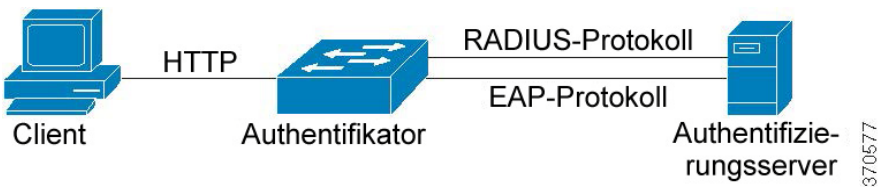
Alle HTTP/HTTPS-über-IPv4-Pakete von nicht autorisierten Clients werden auf der CPU auf dem Switch empfangen. Wenn ein Endbenutzer Zugriff auf das Netzwerk fordert und die webbasierte Authentifizierung auf dem Port aktiviert ist, wird eine Anmeldeseite angezeigt, bevor die angeforderte Seite angezeigt wird. Der Benutzer muss seinen Benutzernamen und das Kennwort eingeben; diese Eingaben werden mithilfe des EAP-Protokolls durch einen RADIUS-Server authentifiziert. War die Authentifizierung erfolgreich, wird der Benutzer darüber informiert.

Der Benutzer verfügt nun über eine authentifizierte Sitzung. Die Sitzung bleibt während ihrer Verwendung geöffnet. Wenn die Sitzung nach Ablauf eines bestimmten Zeitintervalls nicht verwendet wird, wird sie geschlossen. Das Zeitintervall wird durch den Systemadministrator definiert und als „Ruhezeit“ bezeichnet. Wenn die für die Sitzung zulässige Zeit abgelaufen ist, werden Benutzername und Kennwort verworfen, und der Gast muss diese Daten erneut eingeben, um eine neue Sitzung zu öffnen.

Weitere Informationen hierzu finden Sie unter **Authentifizierungsmethoden und Portmodi**.

Sobald die Authentifizierung erfolgreich abgeschlossen wurde, leitet der Switch den gesamten Datenverkehr, der vom Client auf dem Port eingeht, gemäß Abbildung unten weiter.

Abbildung 5 Webbasierte Authentifizierung



Die webbasierte Authentifizierung kann nicht auf einem Port konfiguriert werden, auf dem die Funktion für das Gast-VLAN oder die Funktion „Zugewiesenes RADIUS-VLAN“ aktiviert ist.

Die webbasierte Authentifizierung unterstützt die folgenden Seiten:

- Anmeldeseite
- Seite „Anmeldung erfolgreich“

Es gibt einen vordefinierten, integrierten Satz mit Seiten.

Diese Seiten können auf der Seite „Sicherheit > 802.1X/MAC/Web-Authentifizierung > Anpassung der Web-Authentifizierung“ angepasst werden.

Sie können eine Vorschau für alle angepassten Seiten anzeigen. Die Konfiguration wird in der aktuellen Konfigurationsdatei gespeichert.

In der folgenden Tabelle wird beschrieben, welche SKUs die webbasierte Authentifizierung in welchen Systemmodi unterstützen:

SKU	Systemmodus	WBA unterstützt
Sx300	**Schicht 2**	Ja
	Schicht 3	Nein
Sx500, Sx500ESW2-550X	**Schicht 2**	Ja
	Schicht 3	Nein
SG500X	**Nativ**	Ja
	Basis-Hybrid – Schicht 2	Ja
	Basis-Hybrid – Schicht 3	Nein
SG500XG	**Wie Sx500**	Ja

HINWEIS

- Wenn die webbasierte Authentifizierung nicht unterstützt wird, können VLAN und DVA nicht im Mehrfachsitzungsmodus konfiguriert werden.
- Wenn die webbasierte Authentifizierung unterstützt wird, können VLAN und DVA im Mehrfachsitzungsmodus konfiguriert werden.

Nicht authentifizierte VLANs und Gast-VLAN

Nicht authentifizierte VLANs und Gast-VLANs stellen den Zugriff auf Dienste bereit, für die eine 802.1X- oder MAC-basierte Authentifizierung und -Autorisierung der abonnierenden Geräte oder Ports nicht erforderlich ist.

Das Gast-VLAN ist das VLAN, das einem nicht autorisierten Client zugewiesen ist. Sie können das Gast-VLAN und ein oder mehrere VLANs über die Seite „Sicherheit > 802.1X/MAC/Web-Authentifizierung > Eigenschaften“ so konfigurieren, dass die Authentifizierung aufgehoben wird.

Ein nicht authentifiziertes VLAN ist ein VLAN, das sowohl autorisierten als auch nicht autorisierten Geräten oder Ports Zugriff gewährt.

Ein nicht authentifiziertes VLAN hat die folgenden Charakteristika:

- Es muss ein statisches VLAN sein und darf weder ein Gast- noch ein Standard-VLAN sein.
- Die Mitglieds-Ports müssen manuell als Mitglieder mit Tag konfiguriert werden.
- Der Mitglieds-Port muss ein Trunk- und/oder allgemeiner Port sein. Ein Zugriffs-Port kann nicht Mitglied eines nicht authentifizierten VLAN sein.

Das Gast-VLAN, falls konfiguriert, ist ein statisches VLAN mit den folgenden Charakteristika:

- Es muss von einem vorhandenen statischen VLAN aus definiert sein.
- Ein Gast-VLAN kann nicht als Voice-VLAN oder als nicht authentifiziertes VLAN verwendet werden.

Siehe **VLAN und RADIUS-VLAN-Zuordnung**, um eine Übersicht über die Modi anzuzeigen, in denen das Gast-VLAN unterstützt wird.

Hostmodi mit Gast-VLAN

Die Hostmodi arbeiten wie folgt mit dem Gast-VLAN zusammen:

- **Einzelhost- und Mehrfachhost-Modus**

  Datenverkehr mit und ohne Tags, der zu dem Gast-VLAN gehört und der auf einem nicht autorisierten Port eingeht, wird über das Gast-VLAN überbrückt. Der gesamte übrige Datenverkehr wird verworfen. Der Datenverkehr, der zu einem nicht authentifizierten VLAN gehört, wird über das VLAN überbrückt.

- **Mehrfachsitzungsmodus in Schicht-2-Systemmodus**

  Datenverkehr mit und ohne Tags, der nicht zu den nicht authentifizierten VLANs gehört und von nicht autorisierten Clients eingeht, wird dem Gast-VLAN auf Basis der TCAM-Regel zugewiesen und über das Gast-VLAN überbrückt. Der Datenverkehr mit Tags, der zu einem nicht authentifizierten VLAN gehört, wird über das VLAN überbrückt.

  Dieser Modus kann nicht auf der gleichen Schnittstelle wie die richtlinienbasierten VLANs konfiguriert werden.

- **Mehrfachsitzungsmodus im Schicht-3-Systemmodus**

  Bei diesem Modus wird das Gast-VLAN nicht unterstützt.

RADIUS-VLAN-Zuordnung oder Dynamische VLAN-Zuordnung

Ein autorisierter Client kann über einen RADIUS-Server einem VLAN zugewiesen werden, wenn diese Option auf der Seite „Port-Authentifizierung“ aktiviert wurde. Dies wird entweder als „Dynamische VLAN-Zuweisung“ (DVA) oder „Zugewiesenes RADIUS-VLAN“ bezeichnet. In diesem Handbuch wird die Benennung „Zugewiesenes RADIUS-VLAN“ verwendet.

Wenn ein Port im Mehrfachsitzungsmodus betrieben wird und die Funktion „Zugewiesenes RADIUS-VLAN“ aktiviert ist, fügt das Gerät den Port automatisch als Mitglied ohne Tag dem VLAN hinzu, dem er durch den RADIUS-Server während der Authentifizierung zugewiesen wurde. Das Gerät klassifiziert Pakete ohne Tag für das zugewiesene VLAN, wenn die Pakete von authentifizierten und autorisierten Geräten oder Ports stammen.

Weitere Informationen zum Verhalten der diversen Modi, wenn die Funktion „Zugewiesenes RADIUS-VLAN“ auf dem Gerät aktiviert ist, finden Sie unter **VLAN und RADIUS-VLAN-Zuordnung**.

HINWEIS Die RADIUS-VLAN-Zuordnung wird nur auf den Sx500-Geräten unterstützt, wenn sich das jeweilige Gerät im Schicht-2-Systemmodus befindet. Die SG500X- und SG500XG-Geräte verhalten sich wie Sx500-Geräte, wenn sie sich im Basis- und erweiterten Hybrid-Stacking-Modus befinden.

Für Geräte, die für einen Port mit aktivierter DVA authentifiziert und autorisiert werden sollen, gilt Folgendes:

- Der RADIUS-Server muss das Gerät authentifizieren und ihm dynamisch ein VLAN zuweisen. Sie können das Feld „RADIUS-VLAN-Zuordnung“ auf der Seite „Port-Authentifizierung“ auf „Statisch“ setzen. Damit kann der Host gemäß der statischen Konfiguration überbrückt werden.
- Ein RADIUS-Server muss DVA unterstützen mit den RADIUS-Attributen tunnel-type (64) = VLAN (13), tunnel-media-type (65) = 802 (6) und tunnel-private-group-id = eine VLAN-ID.

Ist die Funktion „Zugewiesenes Radius-VLAN“ aktiviert, verhalten sich die Hostmodi wie folgt:

- **Einzelhost- und Mehrfachhost-Modus**

  Datenverkehr mit und ohne Tags, der zum zugewiesenen RADIUS-VLAN gehört, wird über dieses VLAN überbrückt. Datenverkehr, der nicht zu nicht authentifizierten VLANs gehört, wird verworfen.

- **Vollständiger Mehrfachsitzungsmodus**

  Datenverkehr mit und ohne Tags, der nicht zu nicht authentifizierten VLANs gehört und vom Client eingeht, wird dem zugewiesenen RADIUS-VLAN auf Basis von TCAM-Regeln zugewiesen und über das VLAN überbrückt.

- **Mehrfachsitzungsmodus in Schicht-3-Systemmodus**

In diesem Modus wird das zugewiesene RADIUS-VLAN nicht unterstützt, mit Ausnahme für die Geräte SG500X SG500XG im nativen Stacking-Modus.

In der folgenden Tabelle wird die Unterstützung für die Gast-VLAN- und RADIUS-VLAN-Zuordnung in Abhängigkeit von der Authentifizierungsmethode und dem Port-Modus erläutert.

VLAN und RADIUS-VLAN-Zuordnung

Authentifizierungsverfahren	Einzelhost	Mehrfachhost	Mehrfachsitzungen	
			Gerät im Schicht-3-Systemmodus	Gerät im Schicht-2-Systemmodus
802.1X	†	†	n.u.	†
MAC	†	†	n.u.	†
WEB	n.u.	n.u.	n.u.	n.u.

Legende:

†: Der Port-Modus unterstützt die Gast-VLAN- und RADIUS-VLAN-Zuordnung.

n.u.: Der Port-Modus bietet keine Unterstützung der Authentifizierungsmethode.

Verletzungsmodus

Im Einzelhost-Modus können Sie die Aktion konfigurieren, die ausgeführt wird, wenn ein nicht autorisierter Host auf einem autorisierten Port versucht, auf die Schnittstelle zuzugreifen. Verwenden Sie hierzu die Seite „Host- und Sitzungsauthentifizierung“.

Folgende Optionen stehen zur Verfügung:

- **Beschränken**: Generiert einen Trap, wenn eine Station, bei deren MAC-Adresse es sich nicht um die MAC-Adresse des Anfragers handelt, versucht, auf die Schnittstelle zuzugreifen. Die Mindestdauer zwischen Traps beträgt 1 Sekunde. Diese Frames werden weitergeleitet, die zugehörigen Quelladressen wurden jedoch nicht gelernt.
- **Schützen**: Verwerfen Sie Frames mit Quelladressen, bei denen es sich nicht um die Anfrageradresse handelt.
- **Herunterfahren**: Verwerfen Sie Frames mit Quelladressen, bei denen es sich nicht um die Anfrageradresse handelt, und fahren Sie den Port herunter.

Sie können das Gerät außerdem zum Versenden von SNMP-Traps konfigurieren und dabei eine Mindestzeit zwischen aufeinanderfolgenden Traps konfigurieren. Wenn Sekunden = 0, werden Traps deaktiviert. Wenn keine Mindestzeit definiert wurde, wird im Modus „Beschränken“ ein Standardwert von 1 Sekunde und bei anderen Modi ein Standardwert von 0 Sekunden verwendet.

Ruhezeit

Die Ruhezeit ist ein Zeitraum, in dem der Port (im Einzelhost- oder Mehrfachhost-Modus) oder der Client (im Mehrfachsitzungsmodus) nach einem fehlgeschlagenen Authentifizierungsaustausch nicht versuchen kann, eine Authentifizierung zu erzielen. Im Einzelhost- oder Mehrfachhost-Modus wird der Zeitraum pro Port definiert, während in den Mehrfachsitzungsmodi der Zeitraum pro Client definiert wird. Während der Ruhezeit nimmt der Switch keine Authentifizierungsanforderungen an und initiiert diese nicht.

Der Zeitraum wird nur auf 802.1X-basierte und webbasierte Authentifizierungen angewendet.

Sie können außerdem die maximale Anzahl von Anmeldeversuchen definieren, bevor die Ruhezeit gestartet wird. Mit einem Wert von 0 können Sie eine unbegrenzte Anzahl an Anmeldeversuchen definieren.

Die Dauer der Ruhezeit und die maximale Anzahl an Anmeldeversuchen können Sie auf der Seite „Port-Authentifizierung“ definieren.

Allgemeine Aufgaben

Workflow 1: So aktivieren Sie die 802.1X-Authentifizierung auf einem Port:

SCHRITT 1 Klicken Sie auf **Sicherheit > 802.1X/MAC/Web-Authentifizierung > Eigenschaften**.

SCHRITT 2 Aktivieren Sie die Port-basierte Authentifizierung.

SCHRITT 3 Wählen Sie die **Authentifizierungsmethode** aus.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

SCHRITT 5 Klicken Sie auf Sicherheit > 802.1X/MAC/Web-Authentifizierung > Host und Sitzung.

SCHRITT 6 Wählen Sie den erforderlichen Port aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 7 Definieren Sie den Host-Authentifizierungsmodus.

SCHRITT 8 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

SCHRITT 9 Klicken Sie auf **Sicherheit > 802.1X/MAC/Web-Authentifizierung > Port-Authentifizierung**.

SCHRITT 10 Wählen Sie einen Port aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 11 Setzen Sie das Feld „Administrative Portsteuerung“ auf **Autom.**

SCHRITT 12 Definieren Sie die Authentifizierungsmethoden.

SCHRITT 13 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Workflow 2: So konfigurieren Sie Traps:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **802.1X/MAC/Web-Authentifizierung** > **Eigenschaften**.

SCHRITT 2 Wählen Sie die erforderlichen Traps aus.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Workflow 3: So konfigurieren Sie die 802.1X-basierte oder webbasierte Authentifizierung:

SCHRITT 1 Klicken Sie auf **Sicherheit > 802.1X/MAC/Web-Authentifizierung > Port-Authentifizierung**.

SCHRITT 2 Wählen Sie den erforderlichen Port aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie Werte in die erforderlichen Felder für den Port ein.

Die Felder auf dieser Seite werden unter **802.1X-Portauthentifizierung** näher beschrieben.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Mit der Schaltfläche **Einstellungen kopieren** können Sie Einstellungen von einem Port auf einen anderen kopieren.

Workflow 4: So konfigurieren Sie die Ruhezeit:

SCHRITT 1 Klicken Sie auf **Sicherheit > 802.1X/MAC/Web-Authentifizierung > Port-Authentifizierung**.

SCHRITT 2 Wählen Sie einen Port aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie die Ruhezeit in das Feld „Ruhezeit“ ein.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Workflow 5: So konfigurieren Sie das Gast-VLAN:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **802.1X/MAC/Web-Authentifizierung** > **Eigenschaften**.

SCHRITT 2 Wählen Sie die Option **Aktivieren** im Feld „Gast-VLAN“ aus.

SCHRITT 3 Wählen Sie die Gast-VLAN im Feld „Gast-VLAN-ID“ aus.

SCHRITT 4 Konfigurieren Sie das Gast-VLAN-Timeout entweder auf „Sofort“, oder geben Sie einen Wert in das Feld „Benutzerdefiniert“ ein.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Workflow 6: So konfigurieren Sie nicht authentifizierte VLANs:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **802.1X/MAC/Web-Authentifizierung** > **Eigenschaften**.

SCHRITT 2 Wählen Sie ein VLAN aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Wählen Sie ein VLAN aus.

SCHRITT 4 Wahlweise können Sie **Authentifizierung** deaktivieren, um das VLAN zu einem nicht authentifizierten VLAN zu machen.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

802.1X-Konfiguration über die Benutzeroberfläche

HINWEIS Die webbasierte Authentifizierung wird auf Sx300- und SG500-Geräten nur im Schicht-2-Modus unterstützt. Auf SG500XG- und SG500X-Geräten wird sie im nativen Modus sowie im Modus „Erweitertes Hybrid XG“ unterstützt.

Definieren der 802.1X-Eigenschaften

Auf der Seite „802.1X-Eigenschaften“ können Sie 802.1X global aktivieren und definieren, auf welche Weise Ports authentifiziert werden. Damit das 802.1X-Protokoll ausgeführt werden kann, muss es sowohl global als auch auf jedem Port einzeln aktiviert werden.

So definieren Sie die Port-basierte Authentifizierung:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **802.1X/MAC/Web-Authentifizierung** > **Eigenschaften**.

SCHRITT 2 Geben Sie die Parameter ein.

- **Port-basierte Authentifizierung**: Aktivieren oder deaktivieren Sie die Port-basierte Authentifizierung.

  Wenn dies deaktiviert wird, wird auch die 802.1X-, MAC-basierte und webbasierte Authentifizierung deaktiviert.

- **Authentifizierungsmethode**: Wählen Sie die Benutzer-Authentifizierungsmethoden. Folgende Optionen sind möglich:
  - *RADIUS, Ohne*: Die Port-Authentifizierung zuerst unter Verwendung des RADIUS-Servers durchführen. Wenn keine Antwort von RADIUS erfolgt (z. B. wenn der Server nicht betriebsbereit ist), wird keine Authentifizierung durchgeführt und die Sitzung wird zugelassen. Wenn der Server verfügbar ist, aber die Anmeldeinformationen des Benutzers nicht korrekt sind, wird der Zugriff verweigert und die Sitzung wird beendet.
  - *RADIUS*: Der Benutzer wird auf dem RADIUS-Server authentifiziert. Wenn keine Authentifizierung durchgeführt wird, wird die Sitzung nicht zugelassen.
  - *Ohne*: Der Benutzer wird nicht authentifiziert. Die Sitzung wird zugelassen.
- **Gast-VLAN**: Wählen Sie diese Option, um die Verwendung eines Gast-VLAN für nicht autorisierte Ports zu aktivieren. Wenn ein Gast-VLAN aktiviert ist, verbinden sich alle nicht autorisierten Ports automatisch mit dem im Feld *Gast-VLAN-ID* ausgewählten VLAN. Wenn ein Port später autorisiert wird, wird er aus dem Gast-VLAN entfernt.
- **Gast-VLAN-ID**: Wählen Sie das Gast-VLAN aus der Liste der VLANs aus.
- **Gast-VLAN-Timeout**: Geben Sie einen Zeitraum an:
  - Nach der Verknüpfung, wenn die Software den 802.1X-Anfrager nicht erkennt oder die Authentifizierung fehlgeschlagen ist, wird der Port dem Gast-VLAN nur dann hinzugefügt, wenn der Zeitraum für das *Gast-VLAN-Timeout* abgelaufen ist.
  - Wenn sich der Port-Status von *Autorisiert* in *Nicht autorisiert* ändert, wird der Port dem Gast-VLAN nur dann hinzugefügt, wenn das *Gast-VLAN-Timeout* abgelaufen ist.
- **Trap-Einstellungen**: Um Traps zu aktivieren, wählen Sie mindestens eine der folgenden Optionen aus:
  - *Traps für das Fehlschlagen der 802.1X-Authentifizierung*: Wählen Sie diese Option aus, um einen Trap zu generieren, wenn die 802.1X-Authentifizierung scheitert.
  - *Traps für die erfolgreiche 802.1X-Authentifizierung*: Wählen Sie diese Option aus, um einen Trap zu generieren, wenn die 802.1X-Authentifizierung erfolgreich verläuft.
  - *Traps für das Fehlschlagen der MAC-Authentifiz.*: Wählen Sie diese Option aus, um einen Trap zu generieren, wenn die MAC-Authentifizierung scheitert.
  - *Traps für die erfolgreiche MAC-Authentifizierung*: Wählen Sie diese Option aus, um einen Trap zu generieren, wenn die MAC-Authentifizierung erfolgreich verläuft.
- Gehen Sie, wenn sich der Switch im Schicht-2-Systemmodus befindet, sowie bei SG500XG und SG500X wie folgt vor:
  - *Traps für das Fehlschlagen der Web-Authentifiz.*: Wählen Sie diese Option aus, um einen Trap zu generieren, wenn die Web-Authentifizierung scheitert.

- *Traps für die erfolgreiche Web-Authentifizierung*: Wählen Sie diese Option aus, um einen Trap zu generieren, wenn die Web-Authentifizierung erfolgreich verläuft.
- *Traps für die Ruhezeit der Web-Authentifizierung*: Wählen Sie diese Option aus, um einen Trap zu generieren, wenn die Ruhezeit fortgesetzt wird.

Wenn sich das Gerät im Schicht-3-Routermodus befindet, zeigt die VLAN-Authentifizierungstabelle alle VLANs an und zeigt an, ob die Authentifizierung auf diesen aktiviert wurde.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die 802.1X-Eigenschaften werden in die aktuelle Konfigurationsdatei geschrieben.

802.1X-Portauthentifizierung

Auf der Seite „Port-Authentifizierung“ können Sie die 802.1X-Parameter für die einzelnen Ports konfigurieren. Da einige Konfigurationsänderungen wie beispielsweise die Hostauthentifizierung nur möglich sind, wenn der Port den Status „Autorisierung erzwingen“ hat, wird empfohlen, die Portsteuerung in „Autorisierung erzwingen“ zu ändern, bevor Sie Änderungen vornehmen. Wenn die Konfigurierung abgeschlossen ist, setzen Sie die Port-Steuerung auf ihren vorherigen Status zurück.

HINWEIS Ein Port, für den 802.1X definiert ist, kann kein Mitglied einer LAG werden.

So definieren Sie die 802.1X-Authentifizierung:

SCHRITT 1 Klicken Sie **auf Sicherheit** > **802.1X/MAC/Web-Authentifizierung** > **Port-Authentifizierung**.

Auf dieser Seite werden die Authentifizierungseinstellungen für alle Ports angezeigt.

SCHRITT 2 Wählen Sie einen Port aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Schnittstelle**: Wählen Sie einen Port aus.
- **Aktuelle Port-Steuerung**: Der aktuelle Status der Port-Autorisierung. Wenn der Status *Autorisiert* ist, wird der Port entweder authentifiziert, oder die *Administrations-Port-Steuerung* ist *Autorisierung erzwingen*. Wenn umgekehrt der Status *Nicht autorisiert* ist, wird der Port entweder nicht authentifiziert, oder die *Administrations-Port-Steuerung* ist *Nicht-Autorisierung erzwingen*.
- **Administrations-Port-Steuerung**: Der Status der Administrations-Port-Steuerung. Folgende Optionen sind möglich:
  - *Nicht-Autorisierung erzwingen*: Der Zugang zur Schnittstelle wird verweigert durch Versetzen der Schnittstelle in den Status „Nicht autorisiert“. Das Gerät stellt dem Client keine Authentifizierungsservices über die Schnittstelle bereit.

  - *Automatisch*: Port-basierte Authentifizierung und Autorisierung über das Gerät werden aktiviert. Die Schnittstelle wechselt zwischen einem autorisierten und einem nicht autorisierten Status, basierend auf dem Authentifizierungsaustausch zwischen dem Gerät und dem Client.
  - *Autorisierung erzwingen*: Die Schnittstelle wird ohne Authentifizierung autorisiert.

- **RADIUS-VLAN-Zuordnung**: Wählen Sie diese Option, um die dynamische VLAN-Zuweisung für den ausgewählten Port zu aktivieren.
  - ***Deaktivieren***: Dieses Funktion wurde nicht aktiviert.
  - ***Ablehnen***: Wenn der RADIUS-Server den Anfrager autorisiert hat, jedoch keine Anfrager-VLAN bereitgestellt hat, wird der Anfrager abgelehnt.
  - ***Statisch***: Wenn der RADIUS-Server den Anfrager autorisiert hat, jedoch keine Anfrager-VLAN bereitgestellt hat, wird der Anfrager akzeptiert.
- **Gast-VLAN**: Wählen Sie diese Option aus, um die Anzeige der Verwendung eines zuvor definierten Gast-VLANs durch das Gerät zu aktivieren. Folgende Optionen sind möglich:
  - *Ausgewählt*: Die Verwendung eines Gast-VLANs durch nicht autorisierte Ports ist aktiviert. Wenn ein Gast-VLAN aktiviert ist, verbindet sich der nicht autorisierte Port automatisch mit dem im Feld „Gast-VLAN-ID“ auf der Seite „Port-802.1X-Authentifizierung“ ausgewählten VLAN.
    Nachdem eine Authentifizierung fehlgeschlagen ist und wenn das Gast-VLAN global für einen bestimmten Port aktiviert ist, wird das Gast-VLAN den nicht autorisierten Ports automatisch als VLAN ohne Tag zugewiesen.
  - *Gelöscht*: Gast-VLAN ist für den Port deaktiviert.
- **Open Access**: Der Port wird auch dann erfolgreich authentifiziert, wenn die Authentifizierung fehlschlägt. Weitere Informationen hierzu finden Sie unter **Open Access**.
- **802.1X-basierte Authentifizierung**: Die 802.1X-Authentifizierung ist die einzige mögliche Authentifizierungsmethode für den Port.
- **MAC-basierte Authentifizierung**: Der Port wird basierend auf der MAC-Adresse des Anfragers authentifiziert. Für den Port können nur 8 MAC-basierte Authentifizierungen verwendet werden.

  HINWEIS Damit die MAC-Authentifizierung erfolgreich ausgeführt werden kann, müssen der Benutzername und das Kennwort des RADIUS-Server-Anfragers der MAC-Adresse des Anfragers entsprechen. Die MAC-Adresse muss in Kleinbuchstaben und ohne die Trennzeichen „.“ oder „-“ eingegeben werden. Beispiel: 0020aa00bbcc.
- **Webbasierte Authentifizierung**: Diese Option ist nur im Schicht-2-Switch-Modus oder auf SG500XG bzw. SG500X verfügbar. Wählen Sie diese Option aus, um die webbasierte Authentifizierung auf dem Switch zu aktivieren.

- **Periodische Neuauthentifizierung**: Wählen Sie diese Option, um die Neuauthentifizierung eines Ports nach Ablauf des angegebenen Neuauthentifizierungszeitraums zu aktivieren.
- **Zeitspanne für Neuauthentifizierung**: Geben Sie den Zeitraum in Sekunden ein, nach dem der ausgewählte Port erneut authentifiziert werden soll.
- **Jetzt erneut authentifizieren**: Wählen Sie diese Option, um die sofortige Neuauthentifizierung zu aktivieren.
- **Status des Authentifikators**: Der definierte Port-Autorisierungsstatus. Folgende Optionen sind möglich:
  - *Initialisieren*: Wird hochgefahren.
  - *Autorisierung erzwingen*: Der Status des kontrollierten Ports wird auf „Autorisierung erzwingen“ gesetzt (weitergeleiteter Datenverkehr).
  - *Nicht-Autorisierung erzwingen*: Der Status des kontrollierten Ports wird auf „Nicht-Autorisierung erzwingen“ gesetzt (zu löschender Datenverkehr).

    HINWEIS Wenn der Port nicht den Status „Autorisierung erzwingen“ oder „Nicht-Autorisierung erzwingen“ aufweist, befindet er sich im automatischen Modus und der Authentifikator zeigt den Status der ausgeführten Authentifizierung an. Nachdem der Port authentifiziert ist, wird der Status als „Authentifiziert“ angezeigt.
- **Zeitbereich**: Hier können Sie einen Grenzwert für den Zeitbereich eingeben, in dem ein bestimmter Port zur Verwendung autorisiert ist, wenn 802.1X aktiviert ist (die portbasierte Authentifizierung wird überprüft).
- **Zeitbereichsname**: Wählen Sie das Profil, durch das der Zeitbereich spezifiziert wird.
- **Maximale WBA-Anmeldeversuche**: Nur im Schicht-2-Switch-Modus oder auf SG500XG bzw. SG500X verfügbar. Geben Sie die maximale Anzahl an Anmeldeversuchen ein, die auf dieser Schnittstelle zulässig sind. Wählen Sie **Unbegrenzt** für „Kein Limit“ oder **Benutzerdefiniert** aus, um ein Limit zu setzen.
- **Maximale WBA-Ruhezeit**: Nur im Schicht-2-Switch-Modus oder auf SG500XG bzw. SG500X verfügbar. Geben Sie die maximale Länge der Ruhezeit ein, die auf dieser Schnittstelle zulässig ist. Wählen Sie **Unbegrenzt** für „Kein Limit“ oder **Benutzerdefiniert** aus, um ein Limit zu setzen.
- **Max. Hosts**: Geben Sie die maximale Anzahl an autorisierten Hosts ein, die auf der Schnittstelle zulässig sind. Wählen Sie **Unbegrenzt** für „Kein Limit“ oder **Benutzerdefiniert** aus, um ein Limit zu setzen.

  HINWEIS Setzen Sie diesen Wert auf 1, um den Einzelhost-Modus für die webbasierte Authentifizierung im Mehrfachsitzungsmodus zu simulieren.
- **Ruhezeit**: Geben Sie den Zeitraum in Sekunden ein, den das Gerät nach einem fehlgeschlagenen Authentifizierungsaustausch im Ruhestatus verweilt.
- **EAP wird erneut gesendet**: Geben Sie den Zeitraum in Sekunden ein, den das Gerät auf eine Antwort auf eine/n Extensible Authentication Protocol-(EAP-)Anforderung/-Identitäts-Frame vom Anfrager (Client) wartet, bevor die Anforderung erneut gesendet wird.

- **Max. EAP-Anforderungen**: Geben Sie die Höchstzahl der EAP-Anforderungen an, die gesendet werden können. Wenn nach dem definierten Zeitraum keine Antwort empfangen wird (Anfrager-Timeout), wird die Authentifizierung erneut gestartet.
- **Anfrager-Timeout**: Geben Sie den Zeitraum in Sekunden ein, der verstreichen soll, bevor EAP-Anforderungen erneut an den Anfrager gesendet werden.
- **Server-Timeout**: Geben Sie den Zeitraum in Sekunden ein, der verstreichen soll, bevor EAP-Anforderungen erneut an den Authentifizierungsserver gesendet werden.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Porteinstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Definieren der Host- und Sitzungsauthentifizierung

Auf der Seite „Host- und Sitzungsauthentifizierung“ können Sie den Modus definieren, in dem 802.1X am Port ausgeführt wird, sowie die Aktion, die bei einem Verstoß ausgeführt werden soll.

Unter **Port-Hostmodi** finden Sie eine Erläuterung dieser Modi.

So definieren Sie erweiterte 802.1X-Einstellungen für Ports:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **802.1X/MAC/Web-Authentifizierung** > **Host- und Sitzungsauthentifizierung**.

802.1X-Authentifizierungsparameter werden für alle Ports beschrieben. Alle Felder mit Ausnahme der folgenden werden auf der Seite **Bearbeiten** beschrieben.

- **Anzahl der Verstöße**: Die Anzahl der Pakete, die an der Schnittstelle im Einzel-Host-Modus von einem Host ankommen, dessen MAC-Adresse nicht die MAC-Adresse des Anfragers ist.

SCHRITT 2 Wählen Sie einen Port aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Schnittstelle**: Geben Sie eine Portnummer ein, für die die Hostauthentifizierung aktiviert ist.
- **Hostauthentifizierung**: Wählen Sie einen der Modi aus. Diese Modi sind oben unter **Port-Hostmodi** beschrieben.

Einstellungen für Einzelhostverstöße (wird nur angezeigt, wenn „Einzelhost“ als Hostauthentifizierung festgelegt ist):

- **Aktion bei Verstoß**: Wählen Sie die Aktion, die auf Pakete angewendet werden soll, die an der Schnittstelle im Einzel-Sitzungs-/Einzel-Host-Modus von einem Host ankommen, dessen MAC-Adresse nicht die MAC-Adresse des Anfragers ist. Folgende Optionen sind möglich:
  - *Schützen (Verwerfen)*: Die Pakete werden verworfen.

- *Beschränken (Weiterleiten)*: Die Pakete werden weitergeleitet.
- *Herunterfahren*: Die Pakete werden verworfen, und der Port wird heruntergefahren. Der Port bleibt geschlossen, bis er wieder aktiviert oder das Gerät neu gestartet wird.

- **Traps**: Wählen Sie diese Option, um Traps zu aktivieren.
- **Trap-Frequenz**: Definiert, wie oft Traps an den Host gesendet werden. Dieses Feld kann nur definiert werden, wenn der Mehrfach-Host-Modus deaktiviert ist.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Einstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Anzeigen authentifizierter Hosts

So können Sie Details zu den authentifizierten Benutzern anzeigen:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **802.1X/MAC/Web-Authentifizierung** > **Authentifizierte Hosts**.

Auf dieser Seite werden folgende Felder angezeigt:

- **Benutzername**: Namen von Anfragern, die bei den jeweiligen Ports authentifiziert wurden.
- **Port**: Die Nummer des Ports.
- **Sitzungszeit (TT:HH:MM:SS)**: Der Zeitraum in Sekunden, in dem der Benutzer am Port angemeldet war.
- **Authentifizierungsmethode**: Die Methode, mit der die letzte Sitzung authentifiziert wurde.
- **Authentifizierungsserver**: Der RADIUS-Server.
- **MAC-Adresse**: Die MAC-Adresse des Anfragers.
- **VLAN-ID**: Das Port-VLAN.

Gesperrte Clients

So zeigen Sie Clients an, die aufgrund fehlgeschlagener Anmeldeversuche gesperrt wurden, und heben die Sperre für gesperrte Clients auf:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **802.1X/MAC/Web-Authentifizierung** > **Gesperrte Clients**.

Die folgenden Felder werden angezeigt:

- **Schnittstelle**: Der gesperrte Port.

- **MAC-Adresse**: Der aktuelle Status der Port-Autorisierung. Wenn der Status *Autorisiert* ist, wird der Port entweder authentifiziert, oder die *Administrations-Port-Steuerung* ist *Autorisierung erzwingen*. Wenn umgekehrt der Status *Nicht autorisiert* ist, wird der Port entweder nicht authentifiziert, oder die *Administrations-Port-Steuerung* ist *Nicht-Autorisierung erzwingen*.
- **Verbleibende Zeit (Sek)**: Die Zeit bis zur Sperre des Ports.

SCHRITT 2 Wählen Sie einen Port aus.

SCHRITT 3 Klicken Sie auf **Entsperren**.

Anpassung der Web-Authentifizierung

Auf dieser Seite können Sie Seiten für die webbasierte Authentifizierung in verschiedenen Sprachen aktivieren.

Sie können bis zu vier Sprachen hinzufügen.

HINWEIS Bis zu fünf HTTP-Benutzer und ein HTTPS-Benutzer können gleichzeitig eine webbasierte Authentifizierung anfordern. Wenn diese Benutzer authentifiziert werden, können weitere Benutzer eine Authentifizierung anfordern.

So fügen Sie eine Sprache für die webbasierte Authentifizierung hinzu:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **802.1X/MAC/Web-Authentifizierung** > **Anpassung der Web-Authentifizierung**.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Wählen Sie eine Sprache in der Dropdown-Liste **Sprache** aus.

SCHRITT 4 Wählen Sie **Als Standard-Anzeigesprache festlegen** aus, wenn diese Sprache die Standardsprache ist. Die Seiten für die Standardsprache werden angezeigt, wenn der Endbenutzer keine Sprache auswählt.

SCHRITT 5 Klicken Sie auf **Übernehmen**, um diese Einstellung in die aktuelle Konfigurationsdatei zu speichern.

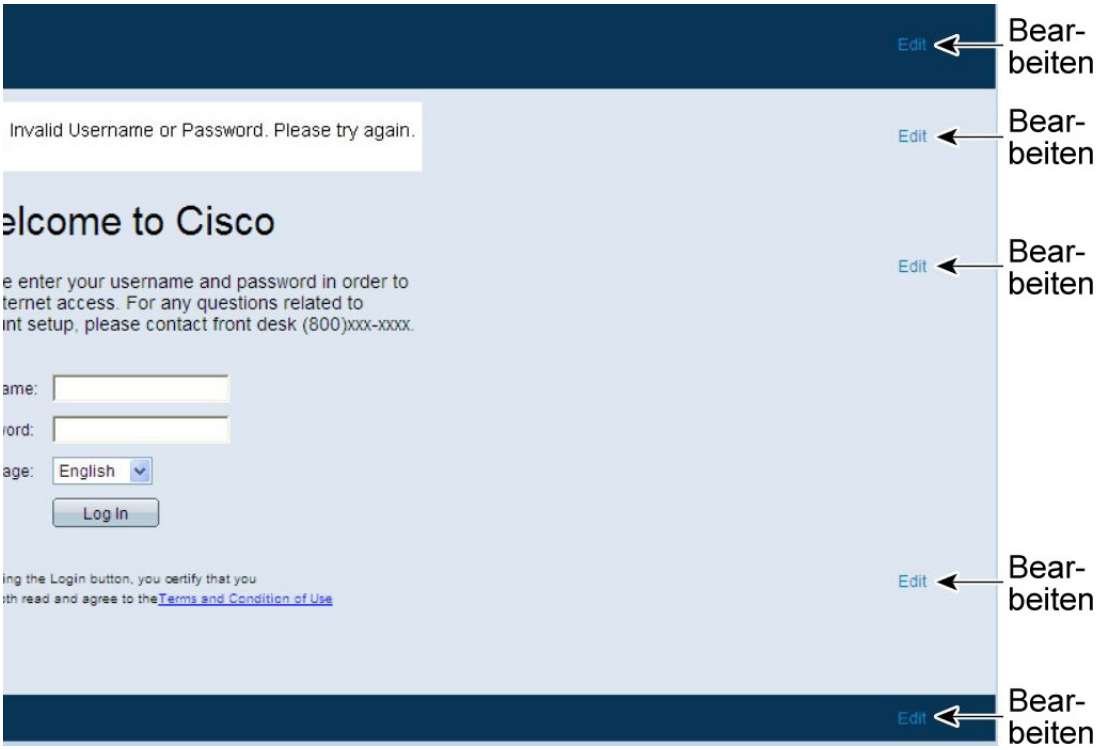
So passen Sie die Seiten für die Web-Authentifizierung an:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **802.1X/MAC/Web-Authentifizierung** > **Anpassung der Web-Authentifizierung.**

Diese Seite zeigt die Sprachen an, die angepasst werden können.

SCHRITT 2 Klicken Sie auf **Anmeldeseite bearbeiten**.

Abbildung 6 Daraufhin wird die folgende Seite angezeigt:



SCHRITT 3 Klicken Sie auf **Bearbeiten1**. Die folgenden Felder werden angezeigt:

- **Sprache**: Zeigt die Sprache der Seite an.
- **Farbschema**: Wählen Sie eine der Kontrastoptionen aus:

  Wenn das Farbschema **Benutzerdefiniert** ausgewählt wurde, sind die folgenden Optionen verfügbar:

  - *Hintergrundfarbe der Seite*: Geben Sie den ASCII-Code der Hintergrundfarbe ein. Die ausgewählte Farbe wird im Feld „Text“ angezeigt.
  - *Hintergrundfarbe von Kopf- und Fußzeilen*: Geben Sie den ASCII-Code für die Hintergrundfarbe für die Kopf- und Fußzeile ein. Die ausgewählte Farbe wird im Feld „Text“ angezeigt.
  - *Textfarbe von Kopf- und Fußzeilen*: Geben Sie den ASCII-Code für die Textfarbe für die Kopf- und Fußzeile ein. Die ausgewählte Farbe wird im Feld „Text“ angezeigt.
  - *Hyperlink-Farbe*: Geben Sie den ASCII-Code der Hyperlink-Farbe ein. Die ausgewählte Farbe wird im Feld „Text“ angezeigt.
- **Aktuelles Logobild**: Wählen Sie eine der folgenden Optionen:
  - *Kein*: Kein Logo.
  - *Standard*: Verwenden Sie das Standardlogo.
  - *Sonstiges*: Wählen Sie diese Option aus, um ein benutzerdefiniertes Logo einzugeben.

Wenn Sie die Logooption **Sonstiges** auswählen, sind die folgenden Optionen verfügbar:

- *Dateiname des Logobildes*: Geben Sie den Namen der Logodatei ein, oder suchen Sie das Bild, indem Sie auf **Durchsuchen** klicken.
- *Anwendungstext*: Geben Sie einen Begleittext für das Logo ein.
- *Fenstertiteltext*: Geben Sie einen Titel für die Anmeldeseite ein.

SCHRITT 4 Klicken Sie auf **Übernehmen**, um diese Einstellung in die aktuelle Konfigurationsdatei zu speichern.

SCHRITT 5 Klicken Sie auf **Bearbeiten2**. Die folgenden Felder werden angezeigt:

- **Ungültige Benutzeranmeldeinformationen**: Geben Sie den Text der Nachricht ein, die angezeigt werden soll, wenn der Endbenutzer einen ungültigen Benutzernamen oder ein ungültiges Kennwort eingibt.
- **Dienst nicht verfügbar**: Geben Sie den Text der Nachricht ein, die angezeigt wird, wenn der Authentifizierungsdienst nicht verfügbar ist.

SCHRITT 6 Klicken Sie auf **Übernehmen**, um diese Einstellung in die aktuelle Konfigurationsdatei zu speichern.

SCHRITT 7 Klicken Sie auf **Bearbeiten3**. Die folgenden Felder werden angezeigt:

- **Begrüßungsmeldung**: Geben Sie den Text der Nachricht ein, die angezeigt wird, wenn sich der Endbenutzer anmeldet.
- **Nachricht mit Anweisungen**: Geben Sie Anweisungen ein, die dem Endbenutzer angezeigt werden.
- **RADIUS-Authentifizierung**: Zeigt an, ob die RADIUS-Authentifizierung aktiviert ist. Ist dies der Fall, müssen der Benutzername und das Kennwort auf die Anmeldeseite eingefügt werden.
- **Textfeld „Benutzername“**: Wählen Sie diese Option aus, um das Textfeld „Benutzername“ anzuzeigen.
- **Bezeichnung d. Textfeldes „Benutzername“**: Wählen Sie diese Option aus, um die Bezeichnung auszuwählen, die vor dem Textfeld „Benutzername“ angezeigt wird.
- **Textfeld „Kennwort“**: Wählen Sie diese Option aus, um ein Textfeld für das Kennwort anzuzeigen.
- **Bezeichnung des Textfeldes „Kennwort“**: Wählen Sie diese Option aus, um die Bezeichnung auszuwählen, die vor dem Textfeld „Kennwort“ angezeigt wird.
- **Sprachauswahl**: Wählen Sie diese Option aus, damit der Endbenutzer eine Sprache auswählen kann.
- **Bezeichnung des Dropdowns „Sprache“**: Geben Sie die Bezeichnung für die Dropdown-Liste „Sprachauswahl“ ein.

- **Bezeichnung der Schaltfläche „Anmelden“**: Geben Sie die Bezeichnung der Schaltfläche „Anmelden“ ein.
- **Bezeichnung des Anmeldeverlaufs**: Geben Sie den Text ein, der während der Anmeldung angezeigt wird.

SCHRITT 8 Klicken Sie auf **Übernehmen**, um diese Einstellung in die aktuelle Konfigurationsdatei zu speichern.

SCHRITT 9 Klicken Sie auf **Bearbeiten4**. Die folgenden Felder werden angezeigt:

- **Geschäftsbedingungen**: Wählen Sie diese Option aus, um ein Textfeld mit den Geschäftsbedingungen aufzurufen.
- **Geschäftsbedingungen – Warnung**: Geben Sie den Text der Nachricht ein, die als Anweisung für die Eingabe der Geschäftsbedingungen angezeigt werden soll.
- **Geschäftsbedingungen – Inhalt**: Geben Sie den Text der Nachricht ein, die als Geschäftsbedingungen angezeigt werden soll.

SCHRITT 10 Klicken Sie auf **Übernehmen**, um diese Einstellung in die aktuelle Konfigurationsdatei zu speichern.

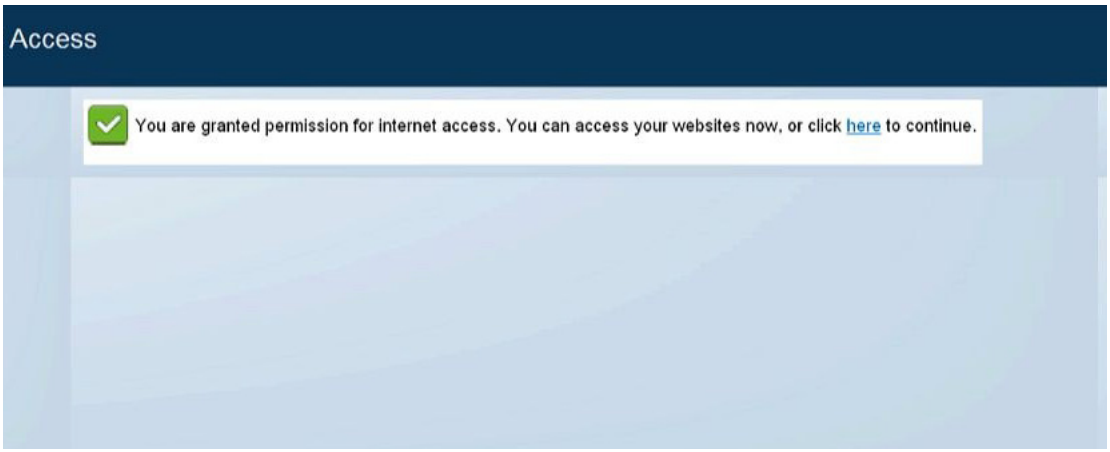
SCHRITT 11 Klicken Sie auf **Bearbeiten5**. Die folgenden Felder werden angezeigt:

- **Copyright**: Wählen Sie diese Option aus, um einen Copyright-Text anzuzeigen.
- **Copyright – Text**: Geben Sie den Copyright-Text ein.

SCHRITT 12 Klicken Sie auf **Übernehmen**, um diese Einstellung in die aktuelle Konfigurationsdatei zu speichern.

SCHRITT 13 Klicken Sie auf **Erfolgreich-Seite bearbeiten**.

Abbildung 7 Daraufhin wird die folgende Seite angezeigt:



SCHRITT 14 Klicken Sie auf die Schaltfläche **Bearbeiten** im rechten Bereich der Seite.

SCHRITT 15 Geben Sie die **Erfolgsmeldung** ein. Hierbei handelt es sich um den Text, der angezeigt wird, nachdem sich der Endbenutzer erfolgreich angemeldet hat.

SCHRITT 16 Klicken Sie auf **Übernehmen**, um diese Einstellung in die aktuelle Konfigurationsdatei zu speichern.

Um eine Vorschau auf die Anmelde- oder Erfolgsmeldung anzuzeigen, klicken Sie auf **Vorschau**.

Um die Standardsprache der grafischen Oberfläche als Standardsprache für die webbasierte Authentifizierung festzulegen, klicken Sie auf **Standard-Anzeigesprache festlegen**.

Definieren von Zeitbereichen

Eine Erläuterung dieser Funktion finden Sie unter **Zeitbereich**.

Unterstützung für Authentifizierungsmethoden und Portmodi

In der folgenden Tabelle werden die Kombinationen der unterstützten Authentifizierungsmethoden und Portmodi erläutert.

Authentifizierungsmethoden und Portmodi

Authentifizierungsverfahren	Einzelhost	Mehrfachhost	Mehrfachsitzungen	
			Gerät im Schicht-3-Systemmodus	Gerät im Schicht-2-Systemmodus
802.1X	†	†	†	†
MAC	†	†	†	†
WEB	n.u.	n.u.	n.u.	†

Legende:

†: Der Port-Modus unterstützt auch die Gast-VLAN- und RADIUS-VLAN-Zuordnung.

n.u.: Die Authentifizierungsmethode bietet keine Unterstützung des Portmodus.

HINWEIS Für die webbasierte Authentifizierung benötigen Sie die TCAM-Unterstützung für die Klassifizierung des eingehenden Datenverkehrs, und die webbasierte Authentifizierung kann nur durch den vollständigen Mehrfachsitzungsmodus unterstützt werden. Sie können den Einzelhostmodus simulieren, indem Sie den Parameter „Max. Hosts“ auf der Seite „Port-Authentifizierung“ auf „1“ setzen.

Modusverhalten

In der folgenden Tabelle wird erläutert, wie authentifizierter und nicht authentifizierter Datenverkehr in verschiedenen Szenarios behandelt wird.

	Nicht authentifizierter Datenverkehr				Authentifizierter Datenverkehr			
	Mit Gast-VLAN		Ohne Gast-VLAN		Mit Radius-VLAN		Ohne Radius-VLAN	
	Ungetaggt	Getaggt	Ungetaggt	Getaggt	Ungetaggt	Getaggt	Ungetaggt	Getaggt
Einzelhost	Frames werden dem Gast-VLAN erneut zugewiesen.	Frames werden ignoriert, wenn sie nicht zum Gast-VLAN oder zu nicht authentifizierten VLANs gehören.	Frames werden ignoriert.	Frames werden ignoriert, wenn sie nicht zu den nicht authentifizierten VLANs gehören.	Frames werden dem dem RADIUS zugewiesenen VLAN erneut zugeordnet.	Frames werden ignoriert, wenn sie nicht zum RADIUS-VLAN oder zu nicht authentifizierten VLANs gehören.	Frames werden auf Basis der statischen VLAN-Konfiguration überbrückt.	Frames werden auf Basis der statischen VLAN-Konfiguration überbrückt.
Mehrfachhost	Frames werden dem Gast-VLAN erneut zugewiesen.	Frames werden ignoriert, wenn sie nicht zum Gast-VLAN oder zu nicht authentifizierten VLANs gehören.	Frames werden ignoriert.	Frames werden ignoriert, wenn sie nicht zu den nicht authentifizierten VLANs gehören.	Frames werden dem dem RADIUS zugewiesenen VLAN erneut zugeordnet.	Frames werden ignoriert, wenn sie nicht zum RADIUS-VLAN oder zu nicht authentifizierten VLANs gehören.	Frames werden auf Basis der statischen VLAN-Konfiguration überbrückt.	Frames werden auf Basis der statischen VLAN-Konfiguration überbrückt.
Nicht vollständige Mehrfachsitzungen	n.u.	n.u.	Frames werden ignoriert.	Frames werden ignoriert, wenn sie nicht zu den nicht authentifizierten VLANs gehören.	n.u.	n.u.	Frames werden auf Basis der statischen VLAN-Konfiguration überbrückt.	Frames werden auf Basis der statischen VLAN-Konfiguration überbrückt.

	Nicht authentifizierter Datenverkehr				Authentifizierter Datenverkehr			
	Mit Gast-VLAN		Ohne Gast-VLAN		Mit Radius-VLAN		Ohne Radius-VLAN	
	Ungetaggt	Getaggt	Ungetaggt	Getaggt	Ungetaggt	Getaggt	Ungetaggt	Getaggt
Vollständige Mehrfachsitzungen	Frames werden dem Gast-VLAN erneut zugewiesen.	Frames werden dem Gast-VLAN erneut zugeordnet, wenn sie nicht authentifizierten VLANs angehören.	Frames werden ignoriert.	Frames werden ignoriert, wenn sie nicht zu den nicht authentifizierten VLANs gehören.	Frames werden dem dem RADIUS zugewiesenen VLAN erneut zugeordnet.	Frames werden dem RADIUS-VLAN erneut zugeordnet, wenn sie nicht authentifizierten VLANs angehören.	Frames werden auf Basis der statischen VLAN-Konfiguration überbrückt.	Frames werden auf Basis der statischen VLAN-Konfiguration überbrückt.

24

Sicherheit: IPv6-Sicherheit des ersten Hops

In diesem Abschnitt wird beschrieben, wie die Funktion „IPv6-Sicherheit des ersten Hops“ (FHS) arbeitet und wie Sie sie auf der Benutzeroberfläche konfigurieren.

Die folgenden Themen werden behandelt:

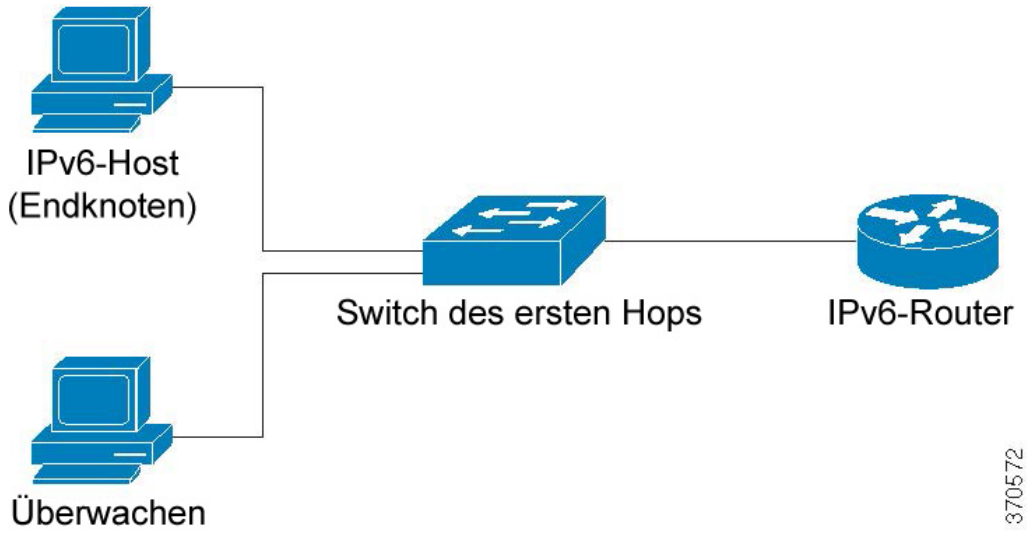
- **IPv6-Sicherheit des ersten Hops – Übersicht**
- **Routerankündigungs-Guard**
- **Nachbarerkennungsprüfung**
- **DHCPv6 Guard**
- **Integrität der Nachbarbindung**
- **IPv6 Source Guard**
- **Schutz vor Angriffen**
- **Richtlinien, globale Parameter und Systemstandardeinstellungen**
- **Allgemeine Aufgaben**
- **Standardeinstellungen und Konfiguration**
- **Standardeinstellungen und Konfiguration**
- **Konfigurieren der IPv6-Sicherheit des ersten Hops über die grafische Weboberfläche**

IPv6-Sicherheit des ersten Hops – Übersicht

„IPv6-FHS“ ist ein Funktionspaket, das entwickelt wurde, um die Verbindungsvorgänge in einem IPv6-aktivierten Netzwerk zu sichern. Es basiert auf den Meldungen zum NDP-Protokoll (Neighbor Discovery Protocol) und DHCPv6.

Mit dieser Funktion werden NDP-Protokoll-Nachrichten, DHCPv6-Nachrichten sowie Benutzerdaten-Nachrichten auf Basis einer Anzahl verschiedener Regeln durch einen Schicht-2-Switch-Modus (siehe **Abbildung 8**) gefiltert.

Abbildung 8 IPv6-Sicherheit des ersten Hops – Konfiguration



Auf jedem VLAN, auf dem diese Funktion aktiviert ist, wird eine separate und unabhängige Instanz der IPv6-Sicherheit des ersten Hops ausgeführt.

Abkürzungen

Name	Beschreibung
CPA-Nachricht	Zertifikatpfadankündigungsnachricht
CPS-Nachricht	Zertifikatpfadanfragenachricht
DAD-NS-Nachricht	Nachbaranfragenachricht für Duplicate Address Detection (DAD)
FCFS-SAVI	Reihenfolge des Eingangs der Anforderung – Verbesserung der Quelladressvalidierung
NA-Nachricht	Nachbarbekanntgabenachricht
NDP	NDP-Protokoll (Neighbor Discovery Protocol)
NS-Nachricht	Nachbaranfragenachricht
RA-Nachricht	Router-Ankündigungsnachricht
RS-Nachricht	Router-Anfragenachricht
SAVI	Verbesserung der Quelladressvalidierung

IPv6-Sicherheit des ersten Hops – Komponenten

Die IPv6-Sicherheit des ersten Hops umfasst die folgenden Funktionen:

- IPv6-Sicherheit des ersten Hops – Allgemeines
- RA Guard
- ND-Prüfung
- Integrität der Nachbarbindung
- DHCPv6 Guard
- IPv6 Source Guard

Diese Komponenten können auf VLANs aktiviert und deaktiviert werden.

Es gibt zwei leere, vorab definierte Richtlinien pro Funktion mit den folgenden Namen: vlan_default und port_default. Die erste Richtlinie wird an jedes VLAN angefügt, das nicht mit einer benutzerdefinierten Richtlinie verknüpft ist, und die zweite ist mit jeder einzelnen Schnittstelle und jedem VLAN verknüpft, die nicht mit einer benutzerdefinierten Richtlinie verknüpft sind. Diese Richtlinien können nicht explizit durch den Benutzer verknüpft werden. Weitere Informationen hierzu finden Sie unter **Richtlinien, globale Parameter und Systemstandardeinstellungen**.

IPv6-Sicherheit des ersten Hops – Pipe

Wenn die IPv6-Sicherheit des ersten Hops auf einem VLAN aktiviert ist, leitet der Switch die folgenden Nachrichten weiter:

- Router-Ankündigungsnachrichten
- Router-Anfragenachrichten
- Nachbarankündigungsnachrichten
- Nachbaranfragenachrichten
- ICMPv6-Umleitungsnachrichten
- CPA-Nachrichten
- Zertifikatpfadanfragenachrichten
- DHCPv6-Nachrichten

Weitergeleitete RA-, CPA- und ICMPv6-Weiterleitungsnachrichten werden an die RA Guard-Funktion weitergeleitet. RA Guard validiert diese Nachrichten, löscht ungültige Nachrichten und leitet zulässige Nachrichten an die ND-Prüffunktion weiter.

Die ND-Prüfung validiert diese Nachrichten, löscht ungültige Nachrichten und leitet zulässige Nachrichten an die IPv6 Source Guard-Funktion weiter.

Weitergeleitete DHCPv6-Nachrichten werden an die DHCPv6 Guard-Funktion weitergeleitet. DHCPv6 Guard validiert diese Nachrichten, löscht ungültige Nachrichten und leitet zulässige Nachrichten an die IPv6 Source Guard-Funktion weiter.

Weitergeleitete Datennachrichten werden an die IPv6 Source Guard-Funktion weitergeleitet. IPv6 Source Guard validiert eingehende Nachrichten (weitergeleitete Datennachrichten, NDP-Nachrichten aus der ND-Prüfung und DHCPv6-Nachrichten von DHCPv6 Guard) über die Tabelle zur Nachbarbindung, löscht unzulässige Nachrichten und leitet zulässige Nachrichten zur Weiterleitung weiter.

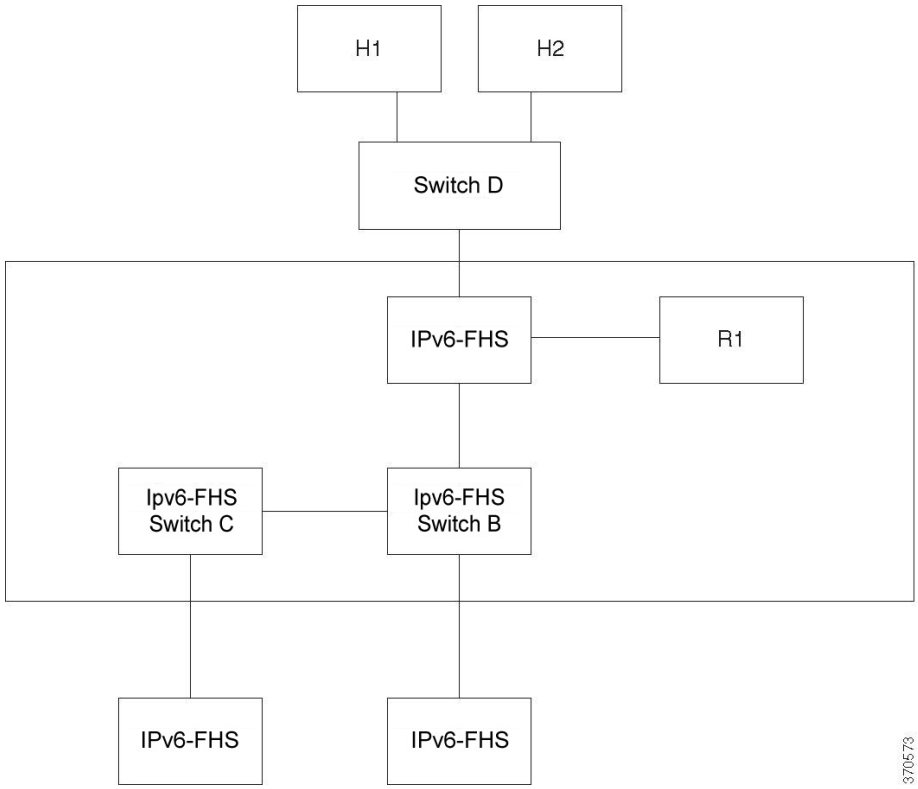
Die Integrität der Nachbarbindung ruft Nachbarn aus den eingehenden Nachrichten (NDP- und DHCPv6-Nachrichten) ab und speichert diese in die Tabelle für die Nachbarbindung. Außerdem können statische Einträge manuell hinzugefügt werden. Nach der Ermittlung der Adressen leitet die NBI-Funktion die Frames zur Weiterleitung weiter.

Weitergeleitete RS-, CPS-, NS- und NA-Nachrichten werden ebenfalls an die ND-Prüffunktion weitergeleitet. Die ND-Prüfung validiert diese Nachrichten, löscht ungültige Nachrichten und leitet zulässige Nachrichten an die IPv6 Source Guard-Funktion weiter.

IPv6-Sicherheit des ersten Hops – Umkreis

Switches für die IPv6-Sicherheit des ersten Hops können einen Umkreis formen, der nicht vertrauenswürdige Bereiche von vertrauenswürdigen Bereichen trennt. Alle Switches innerhalb des Umkreises unterstützen die IPv6-Sicherheit des ersten Hops, und Hosts und Router innerhalb dieses Umkreises gelten als vertrauenswürdige Geräte. In **Abbildung 9** sind beispielsweise Switch B und Switch C innere Links innerhalb des geschützten Bereichs.

Abbildung 9 IPv6-Sicherheit des ersten Hops – Umkreis



Der Befehl **device-role** auf dem Richtlinienkonfigurationsbildschirm für die Nachbarbindung gibt den Umkreis an.

Jeder Switch für die IPv6-Sicherheit des ersten Hops baut Bindungen für Nachbarn auf Basis einer Edge-Partitionierung auf. Auf diese Weise werden Bindungseinträge auf Geräten für die IPv6-Sicherheit des ersten Hops erstellt, die den Umkreis bilden. Die Geräte für die IPv6-Sicherheit des ersten Hops können daraufhin die Bindungsintegrität für das Innere des Umkreises bereitstellen, ohne Bindungen für alle Adressen auf jeden einzelnen Gerät einzurichten.

Routerankündigungs-Guard

Der Routerankündigungs-Guard ist die erste FHS-Funktion, die weitergeleitete RA-Nachrichten verarbeitet. RA Guard unterstützt die folgenden Szenarios:

- Filtern empfangener RA-, CPA- und ICMPv6-Umleitungsnachrichten
- Validieren empfangener RA-Nachrichten

Filtern empfangener RA-, CPA- und ICMPv6-Umleitungsnachrichten

RA Guard verwirft RA- und CPA-Nachrichten, die auf Schnittstellen eingehen, die nicht die Rolle eines Routers ausführen. Die Schnittstellenrolle wird auf der Seite „Sicherheit > IPv6-Sicherheit des ersten Hops > RA Guard-Einstellungen“ konfiguriert.

Validieren von RA-Nachrichten

RA Guard validiert RA-Nachrichten mithilfe von Filtern auf Basis der RA Guard-Richtlinie, die an die Schnittstelle angefügt ist. Diese Richtlinien können auf der Seite „RA Guard-Einstellungen“ konfiguriert werden.

Falls eine Nachricht die Prüfung nicht besteht, wird sie gelöscht. Falls die Konfiguration für die Protokollierung des Paketlöschens auf der bekannten FHS-Komponente aktiviert ist, wird eine Datenratenbegrenzungs-SYSLOG-Nachricht gesendet.

Nachbarerkennungsprüfung

Die Nachbarerkennungsprüfung unterstützt die folgenden Funktionen:

- Prüfung der empfangenen Nachrichten für das Nachbarerkennungsprotokoll.
- Ausgangsfilterung

Nachrichtenvalidierung

Die ND-Prüfung überprüft die Nachrichten des Nachbarerkennungsprotokolls auf Basis einer ND-Prüfungsrichtlinie, die an die Schnittstelle angefügt ist. Diese Richtlinie kann auf der Seite „ND-Prüfungseinstellungen“ definiert werden.

Wenn eine Meldung die in der Richtlinie definierte Prüfung nicht besteht, wird sie gelöscht, und es wird eine Datenratenbegrenzungs-SYSLOG-Nachricht versendet.

Ausgangsfilterung

Die ND-Prüfung blockiert die Weiterleitung von RS- und CPS-Nachrichten auf Schnittstellen, die als Hostschnittstellen konfiguriert wurden.

DHCPv6 Guard

DHCPv6 Guard verarbeitet die weitergeleiteten DHCPv6-Nachrichten. DHCPv6 Guard unterstützt die folgenden Funktionen:

- Filtern eingehender DHCPv6-Nachrichten

  DHCP Guard verwirft DHCPv6-Antwortnachrichten, die auf Schnittstellen eingegangen sind, denen die Client-Rolle zugewiesen wurde. Die Schnittstellenrolle wird auf der Seite „DHCP Guard-Einstellungen“ konfiguriert.

- Validieren eingehender DHCPv6-Nachrichten

  DHCPv6 Guard validiert DHCPv6-Nachrichten, die mit dem Filter übereinstimmen, und zwar auf Basis der DHCPv6 Guard-Richtlinie, die an die Schnittstelle angefügt ist.

Falls eine Nachricht die Prüfung nicht besteht, wird sie gelöscht. Falls die Konfiguration für die Protokollierung des Paketlöschens auf der bekannten FHS-Komponente aktiviert ist, wird eine Datenratenbegrenzungs-SYSLOG-Nachricht gesendet.

Integrität der Nachbarbindung

Die Nachbarbindungsintegrität baut Bindungen mit Nachbarn auf.

Auf jedem VLAN, auf dem diese Funktion aktiviert ist, wird eine separate, unabhängige Instanz der NB-Integrität ausgeführt.

Erlernen von angekündigten IPv6-Präfixes

Die NB-Integrität lernt die in RA-Nachrichten angekündigten IPv6-Präfixe und speichert diese in die Tabelle „Nachbarpräfix“. Die Präfixe werden für die Validierung zugewiesener, globaler IPv6-Adressen verwendet.

Standardmäßig ist diese Validierung deaktiviert. Ist diese Funktion aktiviert, werden Adressen gegen die Präfixe auf der Seite „Bindungseinstellungen der Nachbarn“ validiert.

Statische Präfixe, die für die Adressprüfung verwendet werden, können auf der Seite mit der Tabelle „Nachbarpräfix“ hinzugefügt werden.

Validieren globaler IPv6-Adressen

Die NB-Integrität führt die folgenden Validierungen aus:

- Wenn es sich bei der Zieladresse in einer NS- oder NA-Nachricht um eine globale IPv6-Adresse handelt, muss sie zu einem der Präfixe gehören, die in der RA-Präfixtabelle definiert wurden.
- Eine globale IPv6-Adresse, die durch einen DHCPv6-Server bereitgestellt wird, muss zu einem der Präfixe gehören, die in der IPv6-Präfix-Liste (auf der Seite „IP-Konfiguration > IPv6-Präfix-Liste“) definiert wurden.

Wenn eine Meldung diese Validierung nicht besteht, wird sie gelöscht, und es wird eine Datenratenbegrenzungs-SYSLOG-Nachricht versendet.

Tabelle zur Nachbarbindung – Overflow

Wenn zur Erstellung eines neuen Eintrags kein Platz mehr vorhanden ist, wird kein Eintrag erstellt und eine SYSLOG-Nachricht gesendet.

Aufbauen von Nachbarbindungen

Ein Switch der IPv6-Sicherheit des ersten Hops kann Bindungsinformationen auf Basis der folgenden Methoden ermitteln und erfassen:

- **NBI-NDP-Methode**: Erlernen von IPv6-Adressen aus den Nachrichten für das Snoop-Nachbarerkennungsprotokoll
- **NBI-DHCP-Methode**: Durch das Erlernen von IPv6-Adressen aus den Snoop-DHCPv6-Nachrichten
- **Manuelle NBI-Methode:** Durch die manuelle Konfiguration

Eine IPv6-Adresse ist an eine Verbindungsschichteigenschaft des Netzwerkanhangs des Hosts gebunden. Diese Eigenschaft, die als „Bindungsanker“ bezeichnet wird, besteht aus der Schnittstellen-ID (ifIndex), über die der Host verbunden ist, und der MAC-Adresse des Hosts.

Der Switch für die IPv6-Sicherheit des ersten Hops baut Bindungen nur auf perimetrischen Schnittstellen auf (siehe **IPv6-Sicherheit des ersten Hops – Umkreis**).

Die Bindungsinformationen werden in der Tabelle zur Nachbarbindung gespeichert.

NBI-NDP-Methode

Die verwendete NBI-NDP-Methode basiert auf der unter RFC6620 angegebenen FCFS-SAVI-Methode, jedoch mit den folgenden Abweichungen:

- Im Gegensatz zu FCFS-SAVI, das ausschließlich Bindungen für lokale IPv6-Adressen bietet, unterstützt NBI-NDP darüber hinaus Bindungen von globalen IPv6-Adressen.
- NBI-NDP unterstützt IPv6-Adressbindungen nur bei IPv6-Adressen, die aus NDP-Nachrichten erlernt wurden. Die Quelladressvalidierung für Datennachrichten wird über den IPv6-Quelladress-Guard bereitgestellt.
- Bei NBI-NDP basiert der Nachweis des Adressbesitzes auf dem Prinzip der Reihenfolge des Eingangs der Anforderung (First-Come, First-Served). Der erste Host, der eine vorhandene Quelladresse beansprucht, ist bis auf Weiteres der Besitzer dieser Adresse. Da Änderungen an Hosts nicht akzeptabel sind, muss ein Weg gefunden werden, um den Adressbesitz zu bestätigen, ohne dass ein neues Protokoll benötigt wird. Aus diesem Grund bindet der Switch, wenn eine IPv6-Adresse erstmals von der NDP-Nachricht erlernt wird, die Adresse an die Schnittstelle. Nachfolgende NDP-Nachrichten, die diese IPV6-Adresse enthalten, können gegen den gleichen Bindungsanker geprüft werden, um zu bestätigen, dass der Ersteller der Eigentümer der Quell-IP-Adresse ist.

  Es gibt eine Ausnahme von dieser Regel, wenn ein IPv6-Host in der Schicht-2-Domäne verwendet werden kann oder wenn dieser seine MAC-Adresse ändert. In diesem Fall ist der Host weiterhin der Besitzer der IP-Adresse, der zugewiesene Bindungsanker ist jedoch möglicherweise nicht mehr der ursprüngliche. Um ein solches Szenario aufzufangen, impliziert das definierte NBI-NDP-Verhalten die Prüfung, ob der Host weiterhin erreichbar ist. Dazu werden DAD-NS-Nachrichten an die vorherige Bindungsschnittstelle gesendet. Wenn der Host am zuvor erfassten Bindungsanker nicht mehr erreichbar ist, geht NBI-NDP davon aus, dass der neue Anker gültig ist und passt den Bindungsanker entsprechend an. Sollte der Host nach wie vor über den zuvor erfassten Bindungsanker erreichbar sein, wird die Bindungsschnittstelle nicht geändert.

Um die Größe der Tabelle zur Nachbarbindung zu reduzieren, baut NBI-NDP Bindungen ausschließlich auf Schnittstellen auf, die zum Umkreis gehören (siehe **IPv6-Sicherheit des ersten Hops – Umkreis**), und verteilt die Bindungsinformationen mit NS- und NA-Nachrichten über interne Schnittstellen. Vor der Erstellung einer lokalen NBI-NDP-Bindung sendet das Gerät eine DAD-NS-Nachricht, um die betroffene Adresse abzufragen. Wenn ein Host mit einer NA-Nachricht auf diese Nachricht antwortet, geht das Gerät, dass die DAD-NS-Nachricht gesendet hat, davon aus, dass eine Bindung für diese Adresse in einem anderen Gerät existiert und erstellt daher keine lokale Bindung für diese Adresse. Ist keine NA-Nachricht als Antwort auf die DAD-NS-Nachricht eingegangen, geht das lokale Gerät davon aus, dass keine Bindung für diese Adresse auf anderen Geräten existiert und erstellt daher die lokale Bindung für diese Adresse.

NBI-NDP unterstützt einen Timer für die gesamte Lebensdauer. Die Werte des Timers können auf der Seite „Bindungseinstellungen der Nachbarn“ konfiguriert werden. Der Timer wird immer dann neu gestartet, wenn die eingehende IPv6-Adresse bestätigt wird. Wenn der Timer abläuft, sendet das Gerät zur Prüfung des Nachbarn bis zu zwei DAD-NS-Nachrichten innerhalb kurzer Intervalle.

NBI-DHCP-Methode

Die NBI-NDP-Methode basiert auf der SAVI-DHCP-Methode, die in der SAVI-Lösung für DHCP mit der Bezeichnung „draft-ietf-savi-dhcp-15“ vom 11. September 2012 näher beschrieben wird.

Wie bei NBI-NDP unterstützt NBI-DHCP perimetrische Bindungen zum Zweck einer besseren Skalierbarkeit. Die NBI-DHCP-Methode weicht wie folgt von der NBI-FCFS-Methode ab: NBI-DHCP folgt dem Status, der in den DHCPv6-Nachrichten angekündigt wurde, daher ist es nicht erforderlich, den Status über NS/NA-Nachrichten zu verteilen.

NB-Integritätsrichtlinie

Wie bei anderen Funktionen der IPv6-Sicherheit des ersten Hops wird das Verhalten der NB-Integrität auf einer Schnittstelle durch eine NB-Integritätsrichtlinie definiert, die mit einer Schnittstelle verknüpft ist. Diese Richtlinien werden auf der Seite „Bindungseinstellungen der Nachbarn“ konfiguriert.

IPv6 Source Guard

Wenn die Integrität der Nachbarbindung (NB-Integrität) aktiviert ist, validiert IPv6 Source Guard die Quell-IPv6-Adressen von NDP- und DHCPv6-Nachrichten unabhängig davon, ob IPv6 Source Guard aktiviert ist. Wenn IPv6 Source Guard und NB-Integrität aktiviert sind, konfiguriert IPv6 Source Guard den TCAM-Speicher mit der Angabe, welche IPv4-Daten-Frames weitergeleitet, gelöscht oder in der CPU abgefangen werden, und validiert die Quell-IPv6-Adresse der mittels Trap aufgefangenen IPv6-Datennachrichten. Bei nicht aktivierter NB-Integrität ist auch IPv6 Source Guard nicht aktiviert, unabhängig davon, ob es aktiviert wurde oder nicht.

Wenn im TCAM-Speicher kein freier Speicher mehr vorhanden ist, um eine neue Regel hinzuzufügen, wird der TCAM-Zähler für Überlastung erhöht und eine SYSLOG-Nachricht mit Ratenbegrenzung gesendet, die die Schnittstellen-ID, die MAC-Adresse des Hosts und die IPv6-Adresse des Hosts enthält.

IPv6 Source Guard validiert die Quelladressen aller empfangenen IPv6-Nachrichten anhand der Tabelle zur Nachbarbindung. Davon ausgenommen bleiben die folgenden Nachrichten, die ohne Überprüfung weitergeleitet werden:

- RS-Nachrichten, wenn die Quell-IPv6-Adresse der nicht angegebenen IPv6-Adresse entspricht.
- NS-Nachrichten, wenn die Quell-IPv6-Adresse der nicht angegebenen IPv6-Adresse entspricht.
- NA-Nachrichten, wenn die Quell-IPv6-Adresse der Zieladresse entspricht.

IPv6 Source Guard löscht alle anderen IPv6-Nachrichten, deren Quell-IPv6-Adresse der nicht angegebenen IPv6-Adresse entspricht.

IPv6 Source Guard wird nur auf nicht vertrauenswürdigen, zum Umkreis gehörenden Schnittstellen ausgeführt.

Eine IPv6-Nachricht wird in folgenden Fällen von IPv6 Source Guard gelöscht:

- Die IPv6-Adresse ist nicht in der Tabelle zur Nachbarbindung enthalten.
- Die IPv6-Adresse ist in der Tabelle enthalten, aber an eine andere Schnittstelle gebunden.

Die IPv6 Source Guard-Funktion initiiert den Prozess zur Nachbarwiederherstellung, indem sie DAD_NS-Nachrichten für die unbekannten Quell-IPv6-Adressen sendet.

Schutz vor Angriffen

In diesem Abschnitt wird der Schutz vor Angriffen beschrieben, der durch die IPv6-Sicherheit des ersten Hops bereitgestellt wird.

Schutz vor IPv6-Router-Spoofing

Ein IPv6-Host kann die eingegangenen RA-Nachrichten für Folgendes verwenden:

- IPv6-Routererkennung
- Statusfreie Adresskonfiguration

Ein böswilliger Host könnte RA-Nachrichten versenden, sich damit selbst als IPv6-Router ausgeben und gefälschte Präfixe für die statusfreie Adresskonfiguration bereitstellen.

RA Guard bietet Schutz vor solchen Angriffen, indem die Schnittstellenrolle für alle Schnittstellen, mit denen IPv6-Router verbunden werden können, als Hostschnittstelle konfiguriert wird.

Schutz vor IPv6-Adressauflösungs-Spoofing

Ein böswilliger Host könnte NA-Nachrichten versenden und sich selbst als IPv6-Host mit der jeweiligen IPv6-Adresse ausgeben.

Die NB-Integrität bietet wie folgt Schutz gegen solche Angriffe:

- Wenn die jeweilige IPv6-Adresse nicht bekannt ist, wird die NS-Nachricht (Nachbaranfragenachricht) nur auf innere Schnittstellen weitergeleitet.
- Ist die jeweilige IPv6-Adresse bekannt, wird die NS-Nachricht nur an die Schnittstelle weitergeleitet, an die die IPv6-Adresse gebunden ist.
- Eine NA-Nachricht (Nachbarankündigungsnachricht) wird gelöscht, wenn die IPv6-Zieladresse an eine andere Schnittstelle gebunden ist.

Schutz vor Spoofing beim Erkennen doppelter IPv6-Adressen

Ein IPv6-Host muss die Erkennung doppelter Adressen für jede zugewiesene IPv6-Adresse durchführen, indem er eine spezielle NS-Nachricht versendet (Nachbaranfragenachricht für Duplicate Address Detection (DAD_NS)).

Ein böswilliger Host könnte eine Antwort auf eine DAD_NS-Nachricht versenden und sich damit selbst als IPv6-Host mit der jeweiligen IPv6-Adresse ausgeben.

Die NB-Integrität bietet wie folgt Schutz gegen solche Angriffe:

- Wenn die jeweilige IPv6-Adresse nicht bekannt ist, wird die DAD_NS-Nachricht nur auf innere Schnittstellen weitergeleitet.
- Ist die jeweilige IPv6-Adresse bekannt, wird die DAD_NS-Nachricht nur an die Schnittstelle weitergeleitet, an die die IPv6-Adresse gebunden ist.
- Eine NA-Nachricht wird gelöscht, wenn die IPv6-Zieladresse an eine andere Schnittstelle gebunden ist.

Schutz vor DHCPv6-Server-Spoofing

Ein IPv6-Host kann das DHCPv6-Protokoll für Folgendes verwenden:

- Statusfreie Informationskonfiguration
- Statushaltige Adresskonfiguration

Ein böswilliger Host könnte Antworten auf DHCPv6-Nachrichten versenden, sich damit als DHCPv6-Server ausgeben und gefälschte statusfreie Informationen und IPv6-Adressen bereitstellen. DHCPv6 Guard bietet Schutz vor solchen Angriffen, indem die Schnittstellenrolle für alle Ports, mit denen sich DHCPv6-Server nicht verbinden können, als Client-Port konfiguriert wird.

Schutz vor NBD-Cache-Spoofing

Ein IPv6-Router unterstützt den Cache für das Nachbarerkennungsprotokoll (NDP), das die IPv6-Adresse für das letzte Hop-Routing mit der MAC-Adresse verknüpft.

Ein böswilliger Host könnte IPv6-Nachrichten mit einer abweichenden IPv6-Zieladresse für die Weiterleitung des letzten Hops versenden und damit einen Overflow des NBD-Cache bewirken.

Ein eingebettetes Verfahren in der NDP-Implementierung begrenzt die Anzahl der zulässigen Einträge mit dem Status „Unvollständig“ (INCOMPLETE) im Nachbarerkennungs-Cache. Auf diese Weise wird die Tabelle vor einem Flooding durch Hacker geschützt.

Richtlinien, globale Parameter und Systemstandardeinstellungen

Jede Funktion von FHS kann einzeln aktiviert und deaktiviert werden. Keine Funktion wird standardmäßig aktiviert.

Die Funktionen müssen anfänglich auf spezifischen VLANs aktiviert werden. Wenn Sie diese Funktion aktivieren, können Sie außerdem globale Konfigurationswerte für die Prüfregeln dieser Funktion definieren. Wenn Sie keine Richtlinie mit abweichenden Werten für diese Prüfregeln definieren, werden die globalen Werte verwendet, um die Funktion auf die Pakete anzuwenden.

Richtlinien

Richtlinien enthalten die Prüfregeln, die auf Eingabepaketen ausgeführt werden. Sie können an VLANs, Ports und LAGs angehängt werden. Sollte die Funktion auf einem VLAN nicht aktiviert sein, haben die Richtlinien keine Wirkung.

Richtlinien können entweder durch den Benutzer definiert werden, oder es handelt sich um Standardrichtlinien (siehe unten).

Standardrichtlinien

Für jede FHS-Funktion sind leere Standardrichtlinien vorhanden, die standardmäßig auf alle VLANs und Schnittstellen angewendet werden. Die Standardrichtlinien werden wie folgt benannt: „vlan_default“ und „port_default“ (für jede Funktion):

- Sie können diese Standardrichtlinien um Regeln erweitern. Es ist jedoch nicht möglich, Standardrichtlinien manuell an Schnittstellen anzuhängen. Sie werden standardmäßig angehängt.
- Standardrichtlinien können nicht gelöscht werden. Sie können nur die durch den Benutzer hinzugefügte Konfiguration löschen.

Benutzerdefinierte Richtlinien

Sie können Richtlinien definieren, die von den Standardrichtlinien abweichen.

Wenn eine benutzerdefinierte Richtlinie an eine Schnittstelle angehängt wird, wird die Standardrichtlinie von dieser Schnittstelle gelöst. Wenn die benutzerdefinierte Richtlinie von der Schnittstelle gelöst wird, wird wieder die Standardrichtlinie angehängt.

Richtlinien wirken sich erst aus, nachdem:

- die Funktion in der Richtlinie auf dem VLAN mit der Schnittstelle aktiviert wurde.
- die Richtlinie an die Schnittstelle angehängt wurde (VLAN, Port oder LAG).

Wenn Sie eine Richtlinie anhängen, wird die Standardrichtlinie von dieser Schnittstelle gelöst. Wenn Sie die Richtlinie von der Schnittstelle entfernen, wird erneut die Standardrichtlinie angehängt.

Sie können nur eine Richtlinie (für eine spezifische Funktion) an ein VLAN anhängen.

Sie können mehrere Richtlinien (für eine spezifische Funktion) an eine Schnittstelle anhängen, wenn sie sich auf verschiedene VLANs beziehen.

Prüfregelebenen

Der finale Regelsatz, der auf ein Eingabepaket auf einer Schnittstelle angewendet wird, wird wie folgt aufgebaut:

- Die Regeln, die in Richtlinien konfiguriert und an die Schnittstelle (Port oder LAG) angehängt sind, bei der das Paket eingegangen ist, werden zu dem Satz hinzugefügt.
- Die Regeln, die in der Richtlinie konfiguriert wurden, die an das VLAN angehängt wurden, werden dem Satz hinzugefügt, wenn sie nicht auf Portebene hinzugefügt wurden.
- Die globalen Regeln werden dem Satz hinzugefügt, wenn sie nicht auf VLAN- oder Portebene hinzugefügt wurden.

Regeln, die auf Portebene definiert wurden, überschreiben die Regeln, die auf der VLAN-Ebene definiert wurden. Regeln, die auf der VLAN-Ebene definiert wurden, überschreiben die global konfigurierten Regeln. Die global konfigurierten Regeln überschreiben die Systemstandardeinstellungen.

Allgemeine Aufgaben

IPv6-Sicherheit des ersten Hops – Allgemeiner Workflow

SCHRITT 1 Geben Sie auf der Seite „FHS-Einstellungen“ die Liste der VLANs ein, auf denen diese Funktion aktiviert ist.

SCHRITT 2 Legen Sie auf der gleichen Seite die Funktion „Globale Protokollierung des Paketlöschens“ fest.

SCHRITT 3 Konfigurieren Sie ggf. entweder eine benutzerdefinierte Richtlinie, oder fügen Sie Regeln zu den Standardrichtlinien für die Funktion hinzu.

SCHRITT 4 Fügen Sie die Richtlinie an ein VLAN, einen Port oder ein LAG an; gehen Sie dazu entweder auf die Seite „Richtlinienanlage (VLAN)“ oder auf die Seite „Richtlinienanlage (Port)“.

Routerankündigungs-Guard-Workflow

SCHRITT 1 Geben Sie auf der Seite „RA Guard-Einstellungen“ die Liste der VLANs ein, auf denen diese Funktion aktiviert ist.

SCHRITT 2 Auf dieser Seite können Sie auch die globalen Konfigurationswerte festlegen, die verwendet werden, wenn in einer Richtlinie keine Werte definiert wurden.

SCHRITT 3 Konfigurieren Sie ggf. entweder eine benutzerdefinierte Richtlinie, oder fügen Sie Regeln zu den Standardrichtlinien für die Funktion hinzu.

SCHRITT 4 Fügen Sie die Richtlinie an ein VLAN, einen Port oder ein LAG an; gehen Sie dazu entweder auf die Seite „Richtlinienanlage (VLAN)“ oder auf die Seite „Richtlinienanlage (Port)“.

DHCPv6 Guard-Workflow

SCHRITT 1 Geben Sie auf der Seite „DHCPv6 Guard-Einstellungen“ die Liste der VLANs ein, auf denen diese Funktion aktiviert ist.

SCHRITT 2 Auf dieser Seite können Sie auch die globalen Konfigurationswerte festlegen, die verwendet werden, wenn in einer Richtlinie keine Werte definiert wurden.

SCHRITT 3 Konfigurieren Sie ggf. entweder eine benutzerdefinierte Richtlinie, oder fügen Sie Regeln zu den Standardrichtlinien für die Funktion hinzu.

SCHRITT 4 Fügen Sie die Richtlinie an ein VLAN, einen Port oder ein LAG an; gehen Sie dazu entweder auf die Seite „Richtlinienanlage (VLAN)“ oder auf die Seite „Richtlinienanlage (Port)“.

Nachbarerkennungsprüfungs-Workflow

SCHRITT 1 Geben Sie auf der Seite „ND-Prüfungseinstellungen“ die Liste der VLANs ein, auf denen diese Funktion aktiviert ist.

SCHRITT 2 Auf dieser Seite können Sie auch die globalen Konfigurationswerte festlegen, die verwendet werden, wenn in einer Richtlinie keine Werte definiert wurden.

SCHRITT 3 Konfigurieren Sie ggf. entweder eine benutzerdefinierte Richtlinie, oder fügen Sie Regeln zu den Standardrichtlinien für die Funktion hinzu.

SCHRITT 4 Fügen Sie die Richtlinie an ein VLAN, einen Port oder ein LAG an; gehen Sie dazu entweder auf die Seite „Richtlinienanlage (VLAN)“ oder auf die Seite „Richtlinienanlage (Port)“.

Nachbarbindungs-Workflow

SCHRITT 1 Geben Sie auf der Seite „Bindungseinstellungen der Nachbarn“ die Liste der VLANs ein, auf denen diese Funktion aktiviert ist.

SCHRITT 2 Auf dieser Seite können Sie auch die globalen Konfigurationswerte festlegen, die verwendet werden, wenn in einer Richtlinie keine Werte definiert wurden.

SCHRITT 3 Konfigurieren Sie ggf. entweder eine benutzerdefinierte Richtlinie, oder fügen Sie Regeln zu den Standardrichtlinien für die Funktion hinzu.

SCHRITT 4 Fügen Sie alle erforderlichen manuellen Einträge auf der Seite „Nachbarbindung“ hinzu.

SCHRITT 5 Fügen Sie die Richtlinie an ein VLAN, einen Port oder ein LAG an; gehen Sie dazu entweder auf die Seite „Richtlinienanlage (VLAN)“ oder auf die Seite „Richtlinienanlage (Port)“.

IPv6 Source Guard-Workflow

SCHRITT 1 Geben Sie auf der Seite „IPv6 Source Guard-Einstellungen“ die Liste der VLANs ein, auf denen diese Funktion aktiviert ist.

SCHRITT 2 Konfigurieren Sie ggf. entweder eine benutzerdefinierte Richtlinie, oder fügen Sie Regeln zu den Standardrichtlinien für die Funktion hinzu.

SCHRITT 3 Fügen Sie die Richtlinie an ein VLAN, einen Port oder ein LAG an; gehen Sie dazu entweder auf die Seite „Richtlinienanlage (VLAN)“ oder auf die Seite „Richtlinienanlage (Port)“.

Standardeinstellungen und Konfiguration

Wenn die IPv6-Sicherheit des ersten Hops auf einem VLAN aktiviert ist, leitet der Switch die folgenden Nachrichten standardmäßig weiter:

- Router-Ankündigungsnachrichten
- Router-Anfragenachrichten
- Nachbarankündigungsnachrichten
- Nachbaranfragenachrichten
- ICMPv6-Umleitungsnachrichten

- CPA-Nachrichten
- Zertifikatpfadanfragenachricht
- DHCPv6-Nachrichten

Die FHS-Funktionen werden standardmäßig deaktiviert.

Vorbereitung

Es sind keine Vorarbeiten erforderlich.

Konfigurieren der IPv6-Sicherheit des ersten Hops über die grafische Weboberfläche

Allgemeine FHS-Einstellungen

Auf der Seite „FHS-Einstellungen“ können Sie die allgemeine FHS-Funktion auf einer definierten Gruppe von VLANs aktivieren und den globalen Konfigurationswert für die Protokollierung gelöschter Pakete festlegen. Falls erforderlich, können Sie eine Richtlinie hinzufügen. Alternativ können Sie die Protokollierung des gelöschten Pakets zur durch das System definierten Standardrichtlinie hinzufügen.

So konfigurieren Sie die allgemeinen Parameter für die IPv6-Sicherheit des ersten Hops:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **IPv6-Sicherheit des ersten Hops** > **FHS-Einstellungen**.

Die zurzeit definierten Richtlinien werden angezeigt.

SCHRITT 2 Geben Sie Werte in die Felder für die globale Konfiguration ein:

- **FHS-VLAN-Liste**: Geben Sie mindestens ein VLAN ein, auf dem die IPv6-Sicherheit des ersten Hops aktiviert ist.
- **Protokollierung des Paketlöschens**: Wählen Sie diese Option aus, um ein SYSLOG zu erstellen, wenn ein Paket durch eine Richtlinie des Typs „Sicherheit des ersten Hops“ gelöscht wird. Hierbei handelt es sich um den globalen Standardwert, wenn keine Richtlinie definiert wurde.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um die Einstellungen der aktuellen Konfigurationsdatei hinzuzufügen.

SCHRITT 4 Erstellen Sie, falls erforderlich, eine FHS-Richtlinie, indem Sie auf **Hinzufügen** klicken.

Geben Sie Werte für die folgenden Felder ein:

- **Richtlinienname**: Geben Sie einen benutzerdefinierten Richtliniennamen ein.
- **Protokollierung des Paketlöschens**: Wählen Sie diese Option aus, um ein SYSLOG zu erstellen, wenn ein Paket infolge einer Funktion der Sicherheit des ersten Hops innerhalb dieser Richtlinie gelöscht wurde.
  - *Geerbt*: Verwenden Sie den Wert aus dem VLAN oder der globalen Konfiguration.
  - *Aktivieren*: Erstellen Sie ein SYSLOG, wenn ein Paket infolge der Sicherheit des ersten Hops gelöscht wurde.
  - *Deaktivieren*: Erstellen Sie kein SYSLOG, wenn ein Paket infolge der Sicherheit des ersten Hops gelöscht wurde.

So fügen Sie diese Richtlinie an eine Schnittstelle an:

- **Richtlinie an VLAN anfügen**: Klicken Sie auf diese Option, um auf die Seite **Richtlinienanlage (VLAN)** zu wechseln und diese Richtlinie an ein VLAN anzufügen.
- **Richtlinie an Schnittstelle anfügen**: Klicken Sie auf diese Option, um auf die Seite **Richtlinienanlage (Port)** zu wechseln und diese Richtlinie an einen Port anzufügen.

RA Guard-Einstellungen

Auf der Seite „RA Guard-Einstellungen“ können Sie die RA Guard-Funktion auf einer definierten Gruppe mit VLANs aktivieren und die globalen Konfigurationswerte für diese Funktion festlegen. Falls erforderlich, können Sie eine Richtlinie hinzufügen, oder Sie können die durch das System definierten RA Guard-Standardrichtlinien auf dieser Seite konfigurieren.

So konfigurieren Sie RA Guard:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **IPv6-Sicherheit des ersten Hops** > **RA Guard-Einstellungen**.

SCHRITT 2 Geben Sie Werte in die Felder für die globale Konfiguration ein:

- **RA Guard-VLAN-Liste**: Geben Sie mindestens ein VLAN ein, auf dem RA Guard aktiviert ist.
- **Geräterolle**: Zeigt eine der folgenden Optionen an, mit denen die Rolle des mit dem Port für RA Guard verbundenen Geräts definiert wird.
  - *Geerbt*: Die Rolle des Geräts wird entweder vom VLAN oder den Systemstandardeinstellungen (Client) übernommen.

- *Router*: Die Rolle des Geräts lautet „Router“.
- *Host*: Die Rolle des Geräts lautet „Host“.

- **Minimales Hop-Limit**: Dieses Feld zeigt an, ob die RA Guard-Richtlinie das minimale Hop-Limit des eingegangenen Pakets überprüft.
  - *Keine Überprüfung*: Deaktiviert die Prüfung der unteren Grenze des Limits für die Hop-Anzahl.
  - *Benutzerdefiniert*: Verifiziert, dass das Limit für die Anzahl der Hops größer oder gleich diesem Wert ist.
- **Maximales Hop-Limit**: Dieses Feld zeigt an, ob die RA Guard-Richtlinie das maximale Hop-Limit des eingegangenen Pakets überprüft.
  - *Keine Überprüfung*: Deaktiviert die Prüfung der oberen Grenze des Limits für die Hop-Anzahl.
  - *Benutzerdefiniert*: Verifiziert, dass das Limit für die Anzahl der Hops kleiner oder gleich diesem Wert ist. Der Wert der oberen Grenze muss größer als der Wert auf der unteren Grenze oder damit identisch sein.
- **Flag für verwaltete Konfiguration**: Dieses Feld definiert die Überprüfung des bekannt gemachten Flag für die verwaltete Adresskonfiguration innerhalb einer IPv6 RA Guard-Richtlinie.
  - *Keine Überprüfung*: Deaktiviert die Überprüfung des bekannt gemachten Flag für die verwaltete Adresskonfiguration.
  - *Ein*: Aktiviert die Überprüfung des bekannt gemachten Flag für die verwaltete Adresskonfiguration.
  - *Aus*: Der Wert des Flag muss 0 sein.
- **Flag für andere Konfiguration**: Dieses Feld definiert die Überprüfung des bekannt gemachten Flag für andere Konfigurationen innerhalb einer IPv6-RA Guard-Richtlinie.
  - *Keine Überprüfung*: Deaktiviert die Überprüfung des bekannt gemachten Flag für andere Konfigurationen.
  - *Ein*: Aktiviert die Überprüfung des bekannt gemachten Flag „Verwaltete sonstige“.
  - *Aus*: Der Wert des Flag muss 0 sein.
- **Minimale Routerpriorität**: Dieses Feld zeigt an, ob die RA Guard-Richtlinie den Wert für die minimale bekannt gemachte Standard-Routerpriorität in RA-Nachrichten innerhalb einer RA Guard-Richtlinie überwacht.
  - *Keine Überprüfung*: Deaktiviert die Prüfung der unteren Grenze der bekannt gemachten Standard-Routerpriorität.

  - *Niedrig*: Legt den zulässigen Mindestwert für die bekannt gemachte Standard-Routerpriorität fest. Die folgenden Werte sind zulässig: Niedrig, Mittel und Hoch (siehe RFC4191).
  - *Mittel*: Legt den zulässigen Mindestwert für die bekannt gemachte Standard-Routerpriorität fest. Die folgenden Werte sind zulässig: Niedrig, Mittel und Hoch (siehe RFC4191).
  - *Hoch*: Legt den zulässigen Mindestwert für die bekannt gemachte Standard-Routerpriorität fest. Die folgenden Werte sind zulässig: Niedrig, Mittel und Hoch (siehe RFC4191).
- **Maximale Routerpriorität**: Dieses Feld zeigt an, ob die RA Guard-Richtlinie den Wert für die maximal bekannt gemachte Standard-Routerpriorität in RA-Nachrichten innerhalb einer RA Guard-Richtlinie überwacht.
  - *Keine Überprüfung*: Deaktiviert die Prüfung der oberen Grenze der bekannt gemachten Standard-Routerpriorität.
  - *Niedrig*: Legt den zulässigen Maximalwert für die bekannt gemachte Standard-Routerpriorität fest. Die folgenden Werte sind zulässig: Niedrig, Mittel und Hoch (siehe RFC4191).
  - *Mittel*: Legt den zulässigen Maximalwert für die bekannt gemachte Standard-Routerpriorität fest. Die folgenden Werte sind zulässig: Niedrig, Mittel und Hoch (siehe RFC4191).
  - *Hoch*: Legt den zulässigen Maximalwert für die bekannt gemachte Standard-Routerpriorität fest. Die folgenden Werte sind zulässig: Niedrig, Mittel und Hoch (siehe RFC4191).

Zum Erstellen einer RA Guard-Richtlinie klicken Sie auf **Hinzufügen** und geben die oben genannten Parameter ein. Um die systemdefinierten Standardrichtlinien oder eine benutzerdefinierten Richtlinie zu konfigurieren, wählen Sie die Richtlinie in der Richtlinientabelle aus und klicken Sie auf **Bearbeiten**.

So fügen Sie diese Richtlinie an eine Schnittstelle an:

- **Richtlinie an VLAN anfügen**: Klicken Sie auf diese Option, um auf die Seite **Richtlinienanlage (VLAN)** zu wechseln und diese Richtlinie an ein VLAN anzufügen.
- **Richtlinie an Schnittstelle anfügen**: Klicken Sie auf diese Option, um auf die Seite **Richtlinienanlage (Port)** zu wechseln und diese Richtlinie an einen Port anzufügen.

DHCPv6 Guard-Einstellungen

Auf der Seite „DHCPv6 Guard-Einstellungen“ können Sie die DHCPv6 Guard-Funktion auf einer definierten Gruppe mit VLANs aktivieren und die globalen Konfigurationswerte für diese Funktion festlegen. Falls erforderlich, können Sie eine Richtlinie hinzufügen, oder Sie können die durch das System definierten DHCPv6 Guard-Standardrichtlinien auf dieser Seite konfigurieren.

So konfigurieren Sie DHCPv6 Guard:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **IPv6-Sicherheit des ersten Hops** > **DHCPv6 Guard-Einstellungen**.

SCHRITT 2 Geben Sie Werte in die Felder für die globale Konfiguration ein:

- **DHCPv6 Guard VLAN-Liste**: Geben Sie mindestens ein VLAN ein, auf dem DHCPv6 Guard aktiviert ist.
- **Geräterolle**: Zeigt die Geräterolle an. Eine Definition hierzu finden Sie auf der Seite **Hinzufügen**.
- **Minimale Priorität**: Dieses Feld zeigt an, ob die DHCPv6 Guard-Richtlinie den minimalen bekannt gemachten Prioritätswert des eingegangenen Pakets überprüft.
  - *Geerbt*: Die minimale Präferenz wird entweder vom VLAN oder aus den Systemstandardeinstellungen (Client) übernommen.
  - *Keine Überprüfung*: Deaktivieren Sie die Überprüfung des minimalen bekannt gemachten Prioritätswerts des eingegangenen Pakets.
  - *Benutzerdefiniert*: Überprüft, dass der bekannt gemachte Prioritätswert größer ist als dieser Wert oder mit diesem Wert identisch ist. Dieser Wert muss kleiner sein als der Wert für „Maximale Priorität“.
- **Maximale Priorität**: Dieses Feld zeigt an, ob die DHCPv6 Guard-Richtlinie den maximalen bekannt gemachten Prioritätswert des eingegangenen Pakets überprüft. Dieser Wert muss größer sein als der Wert für „Minimale Priorität“.
  - *Geerbt*: Die maximale Präferenz wird entweder vom VLAN oder aus den Systemstandardeinstellungen (Client) übernommen.
  - *Keine Überprüfung*: Deaktiviert die Prüfung der unteren Grenze des Limits für die Hop-Anzahl.
  - *Benutzerdefiniert*: Überprüft, dass der bekannt gemachte Prioritätswert kleiner ist als dieser Wert oder mit diesem Wert identisch ist.

SCHRITT 3 Klicken Sie zum Erstellen einer DHCPv6-Richtlinie ggf. auf **Hinzufügen**.

SCHRITT 4 Geben Sie Werte für die folgenden Felder ein:

- **Richtlinienname**: Geben Sie einen benutzerdefinierten Richtliniennamen ein.
- **Geräterolle**: Wählen Sie entweder **Server** oder **Client** aus, um die Rolle des mit dem Port für DHCPv6 Guard verbundenen Geräts zu definieren.
  - *Geerbt*: Die Rolle des Geräts wird entweder vom VLAN oder den Systemstandardeinstellungen (Client) übernommen.
  - *Client*: Die Rolle des Geräts lautet „Client“.
  - *Server*: Die Rolle des Geräts lautet „Server“.

- **Antwortpräfixe zuordnen**: Wählen Sie diese Option aus, um die Prüfung der bekannt gemachten Präfixe in den eingegangenen DHCP-Antwortnachrichten innerhalb einer DHCPv6 Guard-Richtlinie zu aktivieren.
  - *Geerbt*: Der Wert wird entweder vom VLAN oder den Systemstandardeinstellungen übernommen (keine Prüfung).
  - *Keine Überprüfung*: Bekannt gemachte Präfixe werden nicht geprüft.
  - *Liste der Übereinstimmungen*: Die IPv6-Präfixliste für die Übereinstimmung.
- **Serveradresse zuordnen**: Wählen Sie diese Option aus, um die Prüfung der IPv6-Adresse des DHCP-Servers und des Relais in eingegangenen DHCP-Antwortnachrichten innerhalb einer DHCPv6 Guard-Richtlinie zu aktivieren.
  - *Geerbt*: Der Wert wird entweder vom VLAN oder den Systemstandardeinstellungen übernommen (keine Prüfung).
  - *Keine Überprüfung*: Deaktiviert die Überprüfung der IPv6-Adresse des DHCP-Servers und des Relais.
  - *Liste der Übereinstimmungen*: Die IPv6-Präfixliste für die Übereinstimmung.
- **Minimale Priorität**: Siehe oben.
- **Maximale Priorität**: Siehe oben.

SCHRITT 5 Klicken Sie auf **Übernehmen**, um die Einstellungen der aktuellen Konfigurationsdatei hinzuzufügen.

So fügen Sie diese Richtlinie an eine Schnittstelle an:

- **Richtlinie an VLAN anfügen**: Klicken Sie auf diese Option, um auf die Seite **Richtlinienanlage (VLAN)** zu wechseln und diese Richtlinie an ein VLAN anzufügen.
- **Richtlinie an Schnittstelle anfügen**: Klicken Sie auf diese Option, um auf die Seite **Richtlinienanlage (Port)** zu wechseln und diese Richtlinie an einen Port anzufügen.

Nachbarerkennungsprüfung – Einstellungen

Auf der Seite „Nachbarerkennungprüfung – Einstellungen“ können Sie die Funktion für die ND-Prüfung auf einer definierten Gruppe mit VLANs aktivieren und die globalen Konfigurationswerte für diese Funktion festlegen. Falls erforderlich, können Sie eine Richtlinie hinzufügen, oder Sie können die durch das System definierten ND-Prüfungsrichtlinien auf dieser Seite konfigurieren.

So konfigurieren Sie die ND-Prüfung:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **IPv6-Sicherheit des ersten Hops** > **ND-Prüfungseinstellungen**.

SCHRITT 2 Geben Sie Werte in die Felder für die globale Konfiguration ein:

- **ND-Prüfung – VLAN-Liste**: Geben Sie mindestens ein VLAN ein, auf dem die ND-Prüfung aktiviert ist.
- **Geräterolle**: Zeigt die Rolle des Geräts an, die nachstehend erläutert wird.
- **Ungesicherte löschen**: Wählen Sie diese Option aus, um das Löschen von Nachrichten ohne CGA- oder RSA-Signaturoption innerhalb einer IPv6 ND-Prüfungsrichtlinie zu aktivieren.
- **Minimale Sicherheitsstufe**: Wenn unsichere Nachrichten nicht gelöscht werden, wählen Sie die unten genannte Sicherheitsstufe aus, um anzugeben, welche Nachrichten nicht weitergeleitet werden.
  - *Keine Überprüfung*: Deaktiviert die Überprüfung der Sicherheitsstufe.
  - *Benutzerdefiniert*: Definieren Sie die Sicherheitsstufe der Nachricht, die weitergeleitet werden soll.
- **Quell-MAC überprüfen**: Legen Sie fest, ob die globale Prüfung der Quell-MAC-Adresse gegen die Verbindungsschichtadresse aktiviert werden soll:
  - *Geerbt*: Der geerbte Wert aus dem VLAN oder den Systemstandardeinstellungen (deaktiviert).
  - *Aktivieren*: Aktivieren Sie die Prüfung der Quell-MAC-Adresse gegen die Verbindungsschichtadresse.
  - *Deaktivieren*: Deaktivieren Sie die Prüfung der Quell-MAC-Adresse gegen die Verbindungsschichtadresse.

SCHRITT 3 Klicken Sie zum Erstellen einer ND-Prüfungsrichtlinie ggf. auf **Hinzufügen**.

SCHRITT 4 Geben Sie Werte für die folgenden Felder ein:

- **Richtlinienname**: Geben Sie einen benutzerdefinierten Richtliniennamen ein.
- **Geräterolle**: Wählen Sie entweder **Server** oder **Client** aus, um die Rolle des mit dem Port für die ND-Prüfung verbundenen Geräts zu definieren.
  - *Geerbt*: Die Rolle des Geräts wird entweder vom VLAN oder den Systemstandardeinstellungen (Client) übernommen.
  - *Host*: Die Rolle des Geräts lautet „Host“.
  - *Router*: Die Rolle des Geräts lautet „Router“.
- **Ungesicherte löschen**: Siehe oben.
- **Minimale Sicherheitsstufe**: Siehe oben.

- **Quell-MAC überprüfen**: Siehe oben.

SCHRITT 5 Klicken Sie auf **Übernehmen**, um die Einstellungen der aktuellen Konfigurationsdatei hinzuzufügen.

So fügen Sie diese Richtlinie an eine Schnittstelle an:

- **Richtlinie an VLAN anfügen**: Klicken Sie auf diese Option, um auf die Seite **Richtlinienanlage (VLAN)** zu wechseln und diese Richtlinie an ein VLAN anzufügen.
- **Richtlinie an Schnittstelle anfügen**: Klicken Sie auf diese Option, um auf die Seite **Richtlinienanlage (Port)** zu wechseln und diese Richtlinie an einen Port anzufügen.

Bindungseinstellungen der Nachbarn

Die Tabelle zur Nachbarbindung ist eine Datenbanktabelle mit IPv6-Nachbarn, die mit einem Gerät verbunden sind. Sie wird aus Informationsquellen wie dem NDP-Snooping erstellt. Diese Datenbank- oder Bindungstabelle wird von verschiedenen IPv6 Guard-Funktionen verwendet, um Spoofing und Umleitungsangriffe zu verhindern.

Auf der Seite „Bindungseinstellungen der Nachbarn“ können Sie die Nachbarbindungsfunktion auf einer definierten Gruppe mit VLANs aktivieren und die globalen Konfigurationswerte für diese Funktion festlegen. Falls erforderlich, können Sie eine Richtlinie hinzufügen, oder Sie können die durch das System definierten Nachbarbindungsrichtlinien auf dieser Seite konfigurieren.

So konfigurieren Sie die Nachbarbindung:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **IPv6-Sicherheit des ersten Hops** > **Bindungseinstellungen der Nachbarn**.

SCHRITT 2 Geben Sie Werte in die Felder für die globale Konfiguration ein:

- **Bindung der Nachbarn – VLAN-Liste**: Geben Sie mindestens ein VLAN ein, auf dem die Nachbarbindung aktiviert ist.
- **Geräterolle**: Zeigt die globale Standardrolle des Geräts (Umkreis) an.
- **Gültigkeitsdauer für die Nachbarbindung**: Geben Sie die Dauer ein, die Adressen in der Tabelle „Nachbarbindungen“ verbleiben.
- **Protokollierung der Nachbarbindung**: Wählen Sie diese Option aus, um die Protokollierung wichtiger Ereignisse in der Tabelle zur Nachbarbindung zu aktivieren.
- **Adresspräfixprüfung**: Wählen Sie diese Option aus, um die IPv6 Source Guard-Prüfung von Adressen zu aktivieren.

Globale Konfiguration der Adressbindungen:

- **Bindung über NDP-Nachrichten**: Um die globale Konfiguration der zulässigen Konfigurationsmethoden für globale IPv6-Adressen innerhalb einer IPv6-Nachbarbindungsrichtlinie zu ändern, wählen Sie eine der folgenden Optionen aus:
  - *Beliebig*: Für globales, an NDP-Nachrichten gebundenes IPv6 sind beliebige Konfigurationsmethoden (statusfreie und manuelle) zulässig.
  - *Statusfrei*: Für globales, an NDP-Nachrichten gebundenes IPv6 ist nur eine statusfreie automatische Konfiguration zulässig.
  - *Deaktivieren*: Die Bindung über NDP-Nachrichten ist deaktiviert.
- **Bindung über DHCPv6-Nachrichten**: Die Bindung über DHCPv6 ist zulässig.

Eintragslimits für Nachbarbindung: Wählen Sie diese Option aus, um die maximale Anzahl von Einträgen für die Nachbarbindung pro Schnittstellen- oder Adresstyp festzulegen:

- **Einträge pro VLAN**: Legen Sie das Limit für die Nachbarbindung pro VLAN fest. Wählen Sie entweder **Kein Limit** aus oder geben Sie einen benutzerdefinierten Wert ein.
- **Einträge pro Schnittstelle**: Legen Sie das Limit für die Nachbarbindung pro Schnittstelle fest. Wählen Sie entweder **Kein Limit** aus oder geben Sie einen benutzerdefinierten Wert ein.
- **Einträge pro MAC-Adresse**: Legen Sie das Limit für die Nachbarbindung pro MAC-Adresse fest. Wählen Sie entweder **Kein Limit** aus oder geben Sie einen **benutzerdefinierten** Wert ein.

SCHRITT 3 Klicken Sie zum Erstellen einer Nachbarbindungsrichtlinie ggf. auf **Hinzufügen**.

SCHRITT 4 Geben Sie Werte für die folgenden Felder ein:

- **Richtlinienname**: Geben Sie einen benutzerdefinierten Richtliniennamen ein.
- **Geräterolle**: Wählen Sie **eine** der folgenden Optionen aus, um die Rolle des mit dem Port für RA Guard verbundenen Geräts zu definieren.
  - *Geerbt*: Die Rolle des Geräts wird entweder vom VLAN oder den Systemstandardeinstellungen (Client) übernommen.
  - *Umkreis*: Der Port ist mit Geräten verbunden, die keine Unterstützung für die IPv6-Sicherheit des ersten Hops bieten.
  - *Intern*: Der Port ist mit Geräten verbunden, die Unterstützung für die IPv6-Sicherheit des ersten Hops bieten.
- **Protokollierung der Nachbarbindung**: Wählen Sie eine der folgenden Optionen aus, um die Protokollierung anzugeben:
  - *Geerbt*: Die Protokollierungsoption entspricht dem globalen Wert.

- *Aktivieren*: Aktivieren Sie die Protokollierung wichtiger Ereignisse in der Bindungstabelle.
- *Deaktivieren*: Deaktivieren Sie die Protokollierung wichtiger Ereignisse in der Bindungstabelle.

- **Adresspräfixprüfung**: Wählen Sie eine der folgenden Optionen aus, um die Prüfung von Adressen zu definieren:
  - *Geerbt*: Die Überprüfungsoption entspricht dem globalen Wert.
  - *Aktivieren*: Aktivieren Sie die Überprüfung von Adressen.
  - *Deaktivieren*: Deaktivieren Sie die Überprüfung von Adressen.

Globale Konfiguration der Adressbindungen:

- *Einstellungen für Adressbindungen erben*: Aktivieren Sie diese Option, um die globalen Einstellungen für Adressbindungen zu verwenden.
- *Bindung über NDP-Nachrichten*: Um die globale Konfiguration der zulässigen Konfigurationsmethoden für globale IPv6-Adressen innerhalb einer IPv6-Nachbarbindungsrichtlinie zu ändern, wählen Sie eine der folgenden Optionen aus:
  - *Beliebig*: Für globales, an NDP-Nachrichten gebundenes IPv6 sind beliebige Konfigurationsmethoden (statusfreie und manuelle) zulässig.
  - *Statusfrei*: Für globales, an NDP-Nachrichten gebundenes IPv6 ist nur eine statusfreie automatische Konfiguration zulässig.
  - *Deaktivieren*: Die Bindung über NDP-Nachrichten ist deaktiviert.

    Bindung über DHCPv6-Nachrichten: Wählen Sie diese Option aus, um die Bindung über DHCPv6 zu aktivieren.

Eintragslimits für die Nachbarbindung:Siehe oben.

- **Einträge pro VLAN**: Wählen Sie **Geerbt** aus, um den globalen Wert zu verwenden, **Kein Limit**, um die Anzahl der Einträge nicht zu begrenzen, und **Benutzerdefiniert**, um einen speziellen Wert für diese Richtlinie festzulegen.
- **Einträge pro Schnittstelle**: Wählen Sie **Geerbt** aus, um den globalen Wert zu verwenden, **Kein Limit**, um die Anzahl der Einträge nicht zu begrenzen, und **Benutzerdefiniert**, um einen speziellen Wert für diese Richtlinie festzulegen.
- **Einträge pro MAC-Adresse**: Wählen Sie **Geerbt** aus, um den globalen Wert zu verwenden, **Kein Limit**, um die Anzahl der Einträge nicht zu begrenzen, und **Benutzerdefiniert**, um einen speziellen Wert für diese Richtlinie festzulegen.

SCHRITT 5 Klicken Sie auf **Übernehmen**, um die Einstellungen der aktuellen Konfigurationsdatei hinzuzufügen.

So fügen Sie diese Richtlinie an eine Schnittstelle an:

- **Richtlinie an VLAN anfügen**: Klicken Sie auf diese Option, um auf die Seite **Richtlinienanlage (VLAN)** zu wechseln und diese Richtlinie an ein VLAN anzufügen.
- **Richtlinie an Schnittstelle anfügen**: Klicken Sie auf diese Option, um auf die Seite **Richtlinienanlage (Port)** zu wechseln und diese Richtlinie an einen Port anzufügen.

IPv6 Source Guard-Einstellungen

Die Seite „IPv6 Source Guard-Einstellungen“ verwenden Sie, um die Funktion „IPv6 Source Guard“ für einen angegebene Gruppe von VLANs zu aktivieren. Falls erforderlich, können Sie eine Richtlinie hinzufügen, oder Sie können die durch das System definierten IPv6 Source Guard-Standardrichtlinien auf dieser Seite konfigurieren.

So konfigurieren Sie IPv6 Source Guard:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **IPv6-Sicherheit des ersten Hops** > **IPv6 Source Guard-Einstellungen**.

SCHRITT 2 Geben Sie Werte in die Felder für die globale Konfiguration ein:

- **IPv6 Source Guard VLAN-Liste**: Geben Sie mindestens ein VLAN ein, auf dem IPv6 Source Guard aktiviert ist.
- **Port-Vertrauensstellung**: Zeigt an, dass die Richtlinien standardmäßig für nicht vertrauenswürdige Ports gedacht sind. Dies kann für jede Richtlinie einzeln geändert werden.

SCHRITT 3 Klicken Sie ggf. auf **Hinzufügen**, um eine Richtlinie „Sicherheit des ersten Hops“ zu erstellen.

SCHRITT 4 Geben Sie Werte für die folgenden Felder ein:

- **Richtlinienname**: Geben Sie einen benutzerdefinierten Richtliniennamen ein.
- **Port-Vertrauensstellung**: Wählen Sie den Port-Vertrauensstellungsstatus der Richtlinie aus:
  - *Geerbt*: Wird die Richtlinie an einen Port angefügt, ist sie nicht vertrauenswürdig.
  - *Vertrauenswürdig*: Wird die Richtlinie an einen Port anfügt, ist sie vertrauenswürdig.

SCHRITT 5 Klicken Sie auf **Übernehmen**, um die Richtlinie anzufügen.

So fügen Sie diese Richtlinie an eine Schnittstelle an:

- **Richtlinie an VLAN anfügen**: Klicken Sie auf diese Option, um auf die Seite **Richtlinienanlage (VLAN)** zu wechseln und diese Richtlinie an ein VLAN anzufügen.
- **Richtlinie an Schnittstelle anfügen**: Klicken Sie auf diese Option, um auf die Seite **Richtlinienanlage (Port)** zu wechseln und diese Richtlinie an einen Port anzufügen.

Richtlinienanlage (VLAN)

So hängen Sie eine Richtlinie an ein oder mehrere VLANs an:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **IPv6-Sicherheit des ersten Hops** > **Richtlinienanlage (VLAN)**.

Die Liste der bereits angehängten Richtlinien wird mit dem jeweiligen **Richtlinientyp**, dem **Richtliniennamen** und der **VLAN-Liste** angezeigt.

SCHRITT 2 Um eine Richtlinie an ein VLAN anzuhängen, klicken Sie auf **Hinzufügen**, und geben Sie Werte in die folgenden Felder ein:

- **Richtlinientyp**: Wählen Sie diese Option aus, um den Richtlinientyp auszuwählen, der an die Schnittstelle angehängt werden soll.
- **Richtlinienname**: Wählen Sie den Namen der Richtlinie aus, die an die Schnittstelle angehängt werden soll.
- **VLAN-Liste**: Wählen Sie die VLANs aus, an die die Richtlinie angehängt wird. Wählen Sie entweder **Alle VLANs** oder einen Bereich mit VLANs aus.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um die Einstellungen der aktuellen Konfigurationsdatei hinzuzufügen.

Richtlinienanlage (Port)

So hängen Sie eine Richtlinie an einen oder mehrere Ports oder LAGs an:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **IPv6-Sicherheit des ersten Hops** > **Richtlinienanlage (Port)**.

Die Liste der Richtlinien, die bereits angehängt wurden, wird mit der jeweiligen **Schnittstellen**nummer, dem **Richtlinientyp**, dem **Richtliniennamen** und der **VLAN-Liste** angezeigt.

SCHRITT 2 Um eine Richtlinie an einen Port oder ein LAG anzuhängen, klicken Sie auf **Hinzufügen**, und geben Sie Werte in die folgenden Felder ein:

- **Schnittstelle**: Wählen Sie die Schnittstelle aus, an die die Richtlinie angehängt werden soll.
- **Richtlinientyp**: Wählen Sie diese Option aus, um den Richtlinientyp auszuwählen, der an die Schnittstelle angehängt werden soll.
- **Richtlinienname**: Wählen Sie den Namen der Richtlinie aus, die an die Schnittstelle angehängt werden soll.
- **VLAN-Liste**: Wählen Sie die VLANs aus, an die die Richtlinie angehängt wird. Wählen Sie entweder **Alle VLANs** oder einen Bereich mit VLANs aus.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um die Einstellungen der aktuellen Konfigurationsdatei hinzuzufügen.

Tabelle zur Nachbarbindung

So zeigen Sie Einträge in der Tabelle zur Nachbarbindung an:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **IPv6-Sicherheit des ersten Hops** > **Tabelle zur Nachbarbindung.**

SCHRITT 2 Wählen Sie eine der folgenden Optionen zum Löschen der Tabelle aus:

- **Nur statische**: Löschen Sie alle statischen Einträge in der Tabelle.
- **Nur dynamische**: Löschen Sie alle dynamischen Einträge in der Tabelle.
- **Alle dynamischen und statischen**: Löschen Sie alle dynamischen und statischen Einträge in der Tabelle.

Geben Sie Werte für die folgenden Felder ein:

- **VLAN-ID**: VLAN-ID des Eintrags.
- **IPv6-Adresse**: Die Quell-IPv6-Adresse des Eintrags.
- **Schnittstellenname**: Der Port, auf dem das Paket eingeht.
- **MAC-Adresse**: Die Nachbar-MAC-Adresse des Nachbarn.

- **Ursprung**: Das Protokoll, dass die IPv6-Adresse hinzugefügt hat (nur für dynamische Einträge verfügbar):
  - *Statisch*: Manuell hinzugefügt.
  - *NDP*: Aus Nachrichten für das Nachbarerkennungsprotokoll gelernt.
  - *DHCP*: Aus DHCPv6-Protokollnachrichten gelernt.
- **Status**: Status des Eintrags:
  - *Mit Vorbehalt*: Die neue Host-IPv6-Adresse wird gerade der Prüfung unterzogen. Da ihre Lebensdauer kürzer als 1 Sekunde ist, wird ihre Ablaufzeit nicht angezeigt.
  - *Gültig*: Die Host-IPv6-Adresse wurde gebunden.
- **Ablaufzeit (Sek.)**: Die verbleibende Zeit in Sekunden, bis der Eintrag entfernt wird, sofern keine Bestätigung erfolgt.
- **TCAM-Überlastung**: Mit **Nein** markierte Einträge wurden aufgrund einer TCAM-Überlastung nicht zum TCAM-Speicher hinzugefügt.

Tabelle „Nachbarpräfix“

In der Tabelle „Nachbarpräfix“ können Sie statische Präfixe für globale IPv6-Adressen hinzufügen, die über NDP-Nachrichten gebunden sind. Dynamische Einträge werden wie unter **Erlernen von angekündigten IPv6-Präfixes** beschrieben gelernt.

So fügen Sie der Tabelle „Nachbarpräfix“ Einträge hinzu:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **IPv6-Sicherheit des ersten Hops** > **Tabelle „Nachbarpräfix“.**

SCHRITT 2 Wählen Sie eine der folgenden Optionen zum Löschen der Tabelle „Nachbarpräfix“ aus:

- **Nur statische**: Löschen Sie nur die statischen Einträge.
- **Nur dynamische**: Löschen Sie nur die dynamischen Einträge.
- **Alle dynamischen und statischen**: Löschen Sie sowohl statische als auch dynamische Einträge.

SCHRITT 3 Für die vorhandenen Einträge werden die folgenden Felder angezeigt:

- **VLAN-ID**: Das VLAN, auf dem die Präfixe relevant sind.
- **IPv6-Präfix**: Das IPv6-Präfix.
- **Präfixlänge:** Die IPv6-Präfixlänge.
- **Ursprung**: Der Eintrag ist dynamisch (gelernt) oder statisch (manuell konfiguriert).

- **Automatische Konfiguration**: Das Präfix kann für die statusfreie Konfiguration verwendet werden.
- **Ablaufzeit (Sek.)**: Die Dauer, für die der Eintrag erhalten bleibt, bis er gelöscht wird.

SCHRITT 4 Klicken Sie auf **Hinzufügen**, um der Tabelle einen neuen Eintrag hinzuzufügen und die obigen Felder für den neuen Eintrag auszufüllen.

FHS-Status

So zeigen Sie die globale Konfiguration für die FHS-Funktionen an:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **IPv6-Sicherheit des ersten Hops** > **FHS-Status.**

SCHRITT 2 Wählen Sie einen Port, ein LAG oder ein VLAN aus, für das/den der FHS-Status gemeldet wird.

SCHRITT 3 Es werden die folgenden Felder für die ausgewählte Schnittstelle angezeigt:

- **FHS-Status**
  - *FHS-Status in aktuellem VLAN*: „FHS“ ist auf dem aktuellen aktiviert.
  - *Protokollierung des Paketlöschens*: Diese Funktion ist für die aktuelle Schnittstelle aktiviert (und zwar auf der Ebene der globalen Konfiguration oder in einer Richtlinie, die mit der Schnittstelle verbunden ist).
- **RA Guard-Status**
  - *RA Guard-Status in aktuellem VLAN*: „RA Guard“ ist auf dem aktuellen VLAN aktiviert.
  - *Geräterolle*: Die RA-Geräterolle.
  - *Flag für verwaltete Konfiguration*: Die Prüfung der Flag für die verwaltete Konfiguration ist aktiviert.
  - *Flag für andere Konfiguration*: Die Prüfung der Flag für die andere Konfiguration ist aktiviert.
  - *RA-Adressenliste*: Die abzugleichende RA-Adressenliste.
  - *RA-Präfixliste*: Die abzugleichende RA-Präfixliste.
  - *Minimales Hop-Limit*: Die Prüfung für das minimale RA-Hop-Limit ist aktiviert.
  - *Maximale Hop-Limit*: Die Prüfung für das maximale RA-Hop-Limit ist aktiviert.
  - *Minimale Routerpriorität*: Die Prüfung der minimalen Routerpriorität ist aktiviert.
  - *Maximale Routerpriorität*: Die Prüfung der maximalen Routerpriorität ist aktiviert.

- **DHCPv6 Guard-Status**
  - *DHCPv6 Guard-Status in aktuellem VLAN*: Die Funktion „DHCPv6“ ist auf dem aktuellen VLAN aktiviert.
  - *Geräterolle*: Die DHCP-Geräterolle.
  - *Antwortpräfixe zuordnen*: Die Prüfung von DHCP-Antwortpräfixes ist aktiviert.
  - *Serveradresse zuordnen*: Die Prüfung von DHCP-Serveradressen ist aktiviert.
  - *Minimale Priorität*: Die Prüfung der minimalen Priorität ist aktiviert.
  - *Maximale Priorität*: Die Prüfung der maximalen Priorität ist aktiviert.
- **ND-Prüfungsstatus**
  - *ND-Prüfungsstatus in aktuellem VLAN*: Die Funktion „ND-Prüfung“ ist auf dem aktuellen VLAN aktiviert.
  - *Geräterolle*: Die Geräterolle lautet „ND-Prüfung“.
  - *Ungesicherte löschen*: Diese Option gibt an, ob unsichere Nachrichten gelöscht werden.
  - *Minimale Sicherheitsstufe*: Wenn unsichere Nachrichten nicht gelöscht werden, müssen Sie die minimale Sicherheitsstufe für weiterzuleitende Pakete festlegen.
  - *Quell-MAC überprüfen*: Die Prüfung der Quell-MAC-Adresse ist aktiviert.
- **Status der Nachbarbindung**
  - *Status der Nachbarbindung im aktuellen VLAN*: Die Funktion „ND-Bindung“ ist auf dem aktuellen VLAN aktiviert.
  - *Geräterolle*: Die Geräterolle lautet „Nachbarbindung“.
  - *Bindung protokollieren*: Gibt an, ob die Protokollierung der Ereignisse in der Tabelle zur Nachbarbindung aktiviert ist.
  - *Adresspräfixprüfung*: Gibt an, ob die Adresspräfixprüfung aktiviert ist.
  - *Globale Adresskonfiguration*: Welche Nachrichten geprüft werden.
  - *Max. Einträge pro VLAN*: Die maximale Anzahl der zulässigen dynamischen Einträge in der Tabelle zur Nachbarbindung pro VLAN.
  - *Max. Einträge pro Schnittstelle*: Die maximale Anzahl der zulässigen Einträge in der Tabelle zur Nachbarbindung pro Schnittstelle.
  - *Max. Einträge pro MAC-Adresse*: Die maximale Anzahl der zulässigen Einträge in der Tabelle zur Nachbarbindung pro MAC-Adresse.

- **IPv6 Source Guard-Status:**
  - *IPv6 Source Guard-Status in aktuellem VLAN*: Gibt an, ob die Funktion „IPv6 Source Guard“ auf dem aktuellen VLAN aktiviert ist.
  - *Port-Vertrauensstellung*: Gibt an, ob der Port vertrauenswürdig ist und wie er seinen vertrauenswürdigen Status erhalten hat.

FHS-Statistik

So zeigen Sie die FHS-Statistik an:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **IPv6-Sicherheit des ersten Hops** > **FHS-Statistik.**

SCHRITT 2 Wählen Sie die **Aktualisierungsrate** aus, d. h. den Zeitraum, der bis zum Aktualisieren der Statistik verstreichen soll.

SCHRITT 3 Es werden die folgenden globalen Zähler für Überlastung angezeigt:

- **Tabelle zur Nachbarbindung**: Die Anzahl der Einträge, die dieser Tabelle nicht hinzugefügt werden konnten, weil die Tabelle ihre maximale Größe erreicht hat.
- **Tabelle „Nachbarpräfix“**: Die Anzahl der Einträge, die dieser Tabelle nicht hinzugefügt werden konnten, weil die Tabelle ihre maximale Größe erreicht hat.
- **TCAM**: Die Anzahl der Einträge, die aufgrund einer TCAM-Überlastung nicht hinzugefügt werden konnten.

SCHRITT 4 Wählen Sie eine Schnittstelle aus. Daraufhin werden die folgenden Felder angezeigt:

- **Nachrichten für das Nachbarerkennungsprotokoll**: Die Anzahl der eingegangenen und gelöschten Nachrichten wird für die folgenden Nachrichtentypen angezeigt:
  - *RA*: Router-Ankündigungsnachrichten
  - *REDIR*: Umleitungsnachrichten
  - *NS*: Nachbaranfragenachrichten
  - *NA*: Nachbarbekanntgabenachrichten.
  - *RS*: Router-Anfragenachrichten

- **DHCPv6-Nachrichten**: Die Anzahl der eingegangenen und gelöschten Nachrichten wird für die folgenden DHCPv6-Nachrichtentypen angezeigt.
  - *ADV*: Bekanntgabenachrichten
  - *REP*: Antwortnachrichten
  - *REC*: Konfigurationsänderungsnachrichten
  - *REL-REP*: Relay-Antwortnachrichten
  - *LEAS-REP*: Antwortnachrichten zu Lease-Abfragen
  - *RLS*: Freigegebene Nachrichten
  - *DEC*: Ablehnungsnachrichten

Die folgenden Felder werden in der Tabelle „Gelöschte FHS-Nachricht“ angezeigt.

- **Funktion**: Der Typ der gelöschten Nachricht (DHCPv6 Guard, RA Guard usw.).
- **Anzahl**: Die Anzahl der gelöschten Nachrichten.
- **Grund**: Der Grund für das Löschen der Nachricht.

25

Sicherheit: SSH-Client

In diesem Abschnitt wird die SSH-Clientfunktion des Geräts beschrieben.

Die folgenden Themen werden behandelt:

- **Secure Copy (SCP) und SSH**
- **Schutzmethoden**
- **SSH-Serverauthentifizierung**
- **SSH-Clientauthentifizierung**
- **Vorbereitung**
- **Allgemeine Aufgaben**
- **SSH-Clientkonfiguration über die grafische Oberfläche**

Secure Copy (SCP) und SSH

Secure Shell (SSH) ist ein Netzwerkprotokoll, das den Datenaustausch über einen sicheren Kanal zwischen einem SSH-Client (in diesem Fall das Gerät) und einem SSH-Server ermöglicht.

Der SSH-Client erleichtert dem Benutzer die Verwaltung eines aus mindestens einem Switch bestehenden Netzwerks, in dem verschiedene Systemdateien auf einem zentralen SSH-Server gespeichert sind. Wenn Konfigurationsdateien über ein Netzwerk übertragen werden, gewährleistet Secure Copy (SCP), eine Anwendung, die das SSH-Protokoll nutzt, dass sensible Daten wie beispielsweise Benutzernamen und Kennwörter nicht abgefangen werden können.

Secure Copy (SCP) wird verwendet, um Firmware, Boot-Images, Konfigurationsdateien, Sprachdateien und Protokolldateien von einem zentralen SCP-Server sicher an ein Gerät zu übertragen.

Im Hinblick auf SSH ist die auf dem Gerät ausgeführte SCP-Anwendung eine SSH-Clientanwendung und der SCP-Server eine SSH-Serveranwendung.

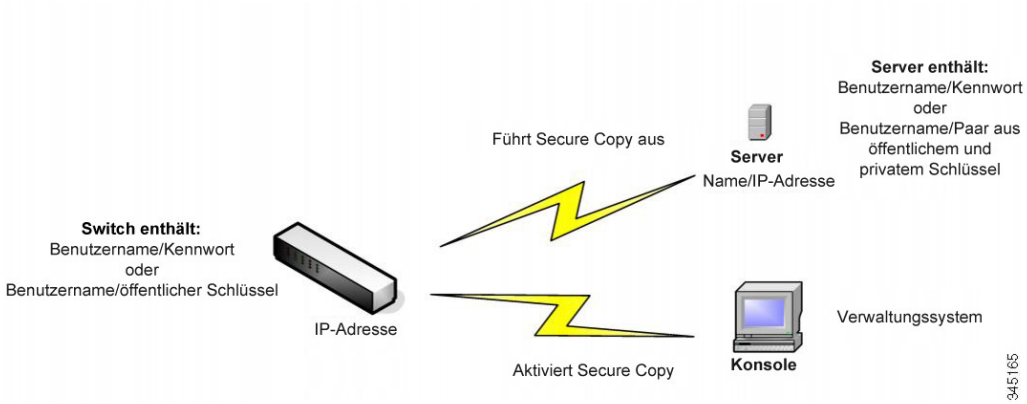
Wenn Dateien über TFTP oder HTTP heruntergeladen werden, ist die Datenübertragung ungeschützt.

Beim Herunterladen von Dateien über SCP werden die Informationen über einen sicheren Kanal vom SCP-Server auf das Gerät heruntergeladen. Der Erstellung dieses sicheren Kanals geht eine Authentifizierung voraus, die sicherstellt, dass der Benutzer den Vorgang ausführen darf.

Benutzer müssen sowohl im Gerät als auch auf dem SSH-Server Authentifizierungsinformationen eingeben. In diesem Handbuch werden die Servervorgänge jedoch nicht beschrieben.

Die folgende Abbildung zeigt eine typische Netzwerkkonfiguration, in der die SCP-Funktion verwendet werden kann.

Typische Netzwerkkonfiguration



Schutzmethoden

Wenn Daten von einem SSH-Server an ein Gerät (Client) übertragen werden, verwendet der SSH-Server für die Clientauthentifizierung verschiedene Methoden. Diese Methoden werden unten beschrieben.

Kennwörter

Wenn Sie die Kennwortmethode verwenden möchten, stellen Sie zuerst sicher, dass auf dem SSH-Server ein Benutzername und ein Kennwort eingerichtet ist. Verwenden Sie dazu nicht das Verwaltungssystem des Geräts, auch wenn das Serverkennwort über das Verwaltungssystem des Geräts geändert werden kann, nachdem Sie auf dem Server einen Benutzernamen eingerichtet haben.

Dann müssen Sie den Benutzernamen und das Kennwort auf dem Gerät erstellen. Wenn Daten vom Server auf das Gerät übertragen werden, müssen der vom Gerät angegebene Benutzername und das entsprechende Kennwort mit dem Benutzernamen und Kennwort auf dem Server übereinstimmen.

Die Daten können mit einem während der Sitzung ausgehandelten einmaligen symmetrischen Schlüssel verschlüsselt werden.

Für jedes verwaltete Gerät ist ein eigener Benutzername und ein entsprechendes Kennwort erforderlich. Sie können jedoch für mehrere Geräte den gleichen Benutzernamen und das gleiche Kennwort verwenden.

Die Kennwortmethode ist die Standardmethode für das Gerät.

Öffentliche/private Schlüssel

Zum Verwenden der Methode mit öffentlichen und privaten Schlüsseln erstellen Sie auf dem SSH-Server einen Benutzernamen und einen öffentlichen Schlüssel. Der öffentliche Schlüssel wird wie unten beschrieben im Gerät generiert und dann auf den Server kopiert. Die Aktionen zum Erstellen eines Benutzernamens auf dem Server und zum Kopieren des öffentlichen Schlüssels auf den Server werden in diesem Handbuch nicht beschrieben.

Die RSA- und DSA-Standardschlüsselpaare für das Gerät werden beim Starten generiert. Einer dieser Schlüssel wird zum Verschlüsseln der vom SSH-Server heruntergeladenen Daten verwendet. Standardmäßig wird der RSA-Schlüssel verwendet.

Wenn der Benutzer einen oder beide dieser Schlüssel löscht, werden sie erneut generiert.

Die öffentlichen und privaten Schlüssel sind verschlüsselt und im Speicher des Geräts gespeichert. Die Schlüssel sind Bestandteil der Gerätekonfigurationsdatei und der private Schlüssel kann dem Benutzer in verschlüsselter oder unverschlüsselter Form angezeigt werden.

Da der private Schlüssel nicht direkt in den privaten Schlüssel eines anderen Geräts kopiert werden kann, gibt es eine Importmethode, mit der Sie private Schlüssel von Gerät zu Gerät kopieren können (Beschreibung unter **Importieren von Schlüsseln**).

Importieren von Schlüsseln

Bei der Schlüsselmethode müssen Sie für jedes Gerät einzeln öffentliche und private Schlüssel erstellen. Diese privaten Schlüssel können aus Sicherheitsgründen nicht direkt von einem Gerät auf ein anderes kopiert werden.

Wenn im Netzwerk mehrere Switches vorhanden sind, kann die Erstellung öffentlicher und privater Schlüssel für alle Switches Zeit raubend sein, da Sie jeden einzelnen öffentlichen und privaten Schlüssel erstellen und dann auf den SSH-Server laden müssen.

Eine zusätzliche Funktion erleichtert diesen Prozess durch die Möglichkeit, den verschlüsselten privaten Schlüssel sicher an alle Switches im System zu übertragen.

Wenn Sie auf einem Gerät einen privaten Schlüssel erstellen, können Sie auch eine zugehörige *Passphrase* erstellen. Dieser Passphrase wird verwendet, um den privaten Schlüssel zu verschlüsseln und ihn in den übrigen Switches zu importieren. Auf diese Weise kann für alle Switches der gleiche öffentliche und private Schlüssel verwendet werden.

SSH-Serverauthentifizierung

Als SSH-Client kommuniziert ein Gerät nur mit einem vertrauenswürdigen SSH-Server. Wenn SSH-Serverauthentifizierung deaktiviert ist (Standardeinstellung), gilt jeder SSH-Server als vertrauenswürdig. Wenn SSH-Serverauthentifizierung aktiviert ist, muss der Benutzer der Tabelle mit vertrauenswürdigen SSH-Servern einen Eintrag für die vertrauenswürdigen Server hinzufügen. In dieser Tabelle werden die folgenden Informationen für jeden vertrauenswürdigen SSH-Server gespeichert (maximal 16 Server):

- IP-Adresse/Hostname des Servers
- Fingerprint des öffentlichen Schlüssels des Servers

Wenn die SSH-Serverauthentifizierung aktiviert ist, authentifiziert der auf dem Gerät ausgeführte SSH-Client den SSH-Server mithilfe des folgenden Authentifizierungsprozesses:

- Das Gerät berechnet den Fingerprint des empfangenen öffentlichen Schlüssels des SSH-Servers.
- Das Gerät durchsucht die Tabelle der vertrauenswürdigen SSH-Server nach der IP-Adresse bzw. dem Hostnamen des SSH-Servers. Eines der folgenden Ereignisse kann auftreten:
  - Wenn eine Übereinstimmung für die IP-Adresse bzw. den Hostnamen des Servers und seinen Fingerprint gefunden wurde, wird der Server authentifiziert.
  - Wenn eine übereinstimmende IP-Adresse bzw. ein übereinstimmender Hostname, aber kein übereinstimmender Fingerprint gefunden wurde, wird die Suche fortgesetzt. Wenn kein übereinstimmender Fingerprint gefunden wurde, wird die Suche abgeschlossen und die Authentifizierung schlägt fehl.
  - Wenn keine übereinstimmende IP-Adresse bzw. kein übereinstimmender Hostname gefunden wurde, wird die Suche abgeschlossen und die Authentifizierung schlägt fehl.
- Wenn der Eintrag für den SSH-Server in der Liste der vertrauenswürdigen SSH-Server nicht gefunden wurde, schlägt der Prozess fehl.

SSH-Clientauthentifizierung

Die SSH-Clientauthentifizierung durch Kennwort ist standardmäßig aktiviert. Benutzername und Kennwort lauten „anonymous“.

Der Benutzer muss die folgenden Informationen für die Authentifizierung konfigurieren:

- Die zu verwendende Authentifizierungsmethode
- Den Benutzernamen und das Kennwort oder das Paar aus öffentlichem und privatem Schlüssel

Zur Unterstützung der automatischen Konfiguration von Geräten im Auslieferungszustand (Geräte mit werkseitiger Konfiguration) ist die SSH-Serverauthentifizierung standardmäßig deaktiviert.

Unterstützte Algorithmen

Wenn die Verbindung zwischen einem Gerät (als SSH-Client) und einem SSH-Server hergestellt ist, tauschen der Client und der SSH-Server Daten aus, um die Algorithmen zu ermitteln, die in der SSH-Transportschicht verwendet werden sollen.

Die folgenden Algorithmen werden auf der Clientseite unterstützt:

- Diffie-Hellman-Schlüsselaustauschalgorithmus
- Verschlüsselungsalgorithmen
  - aes128-cbc
  - 3des-cbc
  - arcfour
  - aes192-cbc
  - aes256-cbc
- Algorithmen für den Nachrichtenauthentifizierungscode
  - hmac-sha1
  - hmac-md5

HINWEIS Kompressionsalgorithmen werden nicht unterstützt.

Vorbereitung

Vor der Verwendung der SCP-Funktion müssen Sie die folgenden Aktionen ausführen:

- Wenn Sie die Authentifizierungsmethode mit Kennwort verwenden, müssen Sie auf dem SSH-Server einen Benutzernamen und ein Kennwort einrichten.
- Wenn Sie die Authentifizierungsmethode mit öffentlichen und privaten Schlüsseln verwenden, müssen Sie den öffentlichen Schlüssel auf dem SSH-Server speichern.

Allgemeine Aufgaben

In diesem Abschnitt werden einige allgemeine Aufgaben beschrieben, die Sie mit dem SSH-Client ausführen. Alle genannten Seiten befinden sich im SSH-Clientzweig der Menüstruktur.

Workflow 1: Um den SSH-Client zu konfigurieren und Daten an einen bzw. von einem SSH-Server zu übertragen, führen Sie die folgenden Schritte aus:

SCHRITT 1 Entscheiden Sie, welche Methode verwendet werden soll: Kennwort oder öffentlicher und privater Schlüssel Verwenden Sie die Seite SSH-Benutzerauthentifizierung.

SCHRITT 2 Wenn Sie die Kennwortmethode ausgewählt haben, führen Sie die folgenden Schritte aus:

a. Erstellen Sie auf der Seite SSH-Benutzerauthentifizierung ein globales Kennwort oder erstellen Sie auf der Seite Firmware/Sprache aktualisieren/sichern oder Konfiguration/Protokoll sichern ein temporäres Kennwort, wenn Sie die sichere Datenübertragung tatsächlich aktivieren.

b. Aktualisieren Sie die Firmware, das Boot-Image oder die Sprachdatei über SCP, indem Sie die Option **über SCP (über SSH)** auf der Seite Firmware/Sprache aktualisieren/sichern auswählen. Sie können das Kennwort auf dieser Seite direkt eingeben oder das auf der Seite SSH-Benutzerauthentifizierung eingegebene Kennwort verwenden.

c. Laden Sie mit SCP die Konfigurationsdatei herunter bzw. sichern Sie diese, indem Sie die Option **über SCP (über SSH)** auf der Seite Konfiguration/Protokoll herunterladen/sichern auswählen. Sie können das Kennwort auf dieser Seite direkt eingeben oder das auf der Seite SSH-Benutzerauthentifizierung eingegebene Kennwort verwenden.

SCHRITT 3 Richten Sie auf dem SSH-Server einen Benutzernamen und ein Kennwort ein oder ändern Sie das Kennwort auf dem SSH-Server. Diese Aktivität hängt vom Server ab und wird hier nicht beschrieben.

SCHRITT 4 Wenn Sie die Methode mit öffentlichen und privaten Schlüsseln verwenden, führen Sie die folgenden Schritte aus:

a. Wählen Sie aus, ob ein RSA- oder DSA-Schlüssel verwendet werden soll, erstellen Sie einen Benutzernamen und generieren Sie dann die öffentlichen und privaten Schlüssel.

b. Zeigen Sie den generierten Schlüssel an, indem Sie auf die Schaltfläche **Details** klicken. Übertragen Sie den Benutzernamen und den öffentlichen Schlüssel an den SSH-Server. Diese Aktion hängt vom Server ab und wird in diesem Handbuch nicht beschrieben.

c. Aktualisieren bzw. sichern Sie die Firmware oder die Sprachdatei mit SCP, indem Sie die Option **über SCP (über SSH)** auf der Seite Firmware/Sprache aktualisieren/sichern auswählen.

d. Laden Sie mit SCP die Konfigurationsdatei herunter bzw. sichern Sie diese, indem Sie die Option **über SCP (über SSH)** auf der Seite Konfiguration/Protokoll herunterladen/sichern auswählen.

Workflow 2: So importieren Sie die öffentlichen und privaten Schlüssel von einem Gerät auf ein anderes:

SCHRITT 1 Generieren Sie auf der Seite SSH-Benutzerauthentifizierung einen öffentlichen oder privaten Schlüssel.

SCHRITT 2 Legen Sie auf der Seite Sicheres Verwalten sensibler Daten (SSD) > Eigenschaften die SSD-Eigenschaften fest und erstellen Sie eine neue lokale Passphrase.

SCHRITT 3 Klicken Sie auf **Details**, um die generierten verschlüsselten Schlüssel anzuzeigen, und kopieren Sie sie (einschließlich der Fußzeilen Begin und End) von der Seite Details auf ein externes Gerät. Kopieren Sie die öffentlichen und privaten Schlüssel getrennt.

SCHRITT 4 Melden Sie sich bei einem anderen Gerät an und öffnen Sie die Seite SSH-Benutzerauthentifizierung. Wählen Sie den Typ des gewünschten Schlüssels aus und klicken Sie auf **Bearbeiten**. Fügen Sie die öffentlichen und privaten Schlüssel ein.

SCHRITT 5 Klicken Sie auf **Übernehmen**, um die öffentlichen und privaten Schlüssel auf das zweite Gerät zu kopieren.

Workflow 3: So ändern Sie das Kennwort auf einem SSH-Server:

SCHRITT 1 Identifizieren Sie den Server auf der Seite Benutzerkennwort auf SSH-Server ändern.

SCHRITT 2 Geben Sie das neue Kennwort ein.

SCHRITT 3 Klicken Sie auf **Übernehmen**.

SSH-Clientkonfiguration über die grafische Oberfläche

In diesem Abschnitt werden die zum Konfigurieren der SSH-Clientfunktion verwendeten Seiten beschrieben.

SSH-Benutzerauthentifizierung

Auf dieser Seite können Sie eine SSH-Benutzerauthentifizierungsmethode auswählen, einen Benutzernamen und ein Kennwort für das Gerät festlegen, wenn die Kennwortmethode ausgewählt ist, oder einen RSA- oder DSA-Schlüssel generieren, wenn die Methode mit öffentlichen und privaten Schlüsseln ausgewählt ist.

So wählen Sie eine Authentifizierungsmethode aus und legen Benutzername und Kennwort bzw. Schlüssel fest:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **SSH-Client** > **SSH-Benutzerauthentifizierung**.

SCHRITT 2 Wählen Sie eine **SSH-Benutzerauthentifizierungsmethode** aus. Dies ist die für Secure Copy (SCP) definierte globale Methode. Wählen Sie eine der Optionen aus:

- **Nach Kennwort**: Dies ist die Standardeinstellung. Wenn Sie diese Option ausgewählt haben, geben Sie ein Kennwort ein oder behalten Sie das Standardkennwort bei.
- **Durch öffentlichen RSA-Schlüssel**: Wenn Sie diese Option ausgewählt haben, erstellen Sie im Block **SSH-Benutzerschlüsseltabelle** einen öffentlichen und einen privaten RSA-Schlüssel.
- **Durch öffentlichen DSA-Schlüssel**: Wenn Sie diese Option ausgewählt haben, erstellen Sie im Block **SSH-Benutzerschlüsseltabelle** einen öffentlichen und einen privaten DSA-Schlüssel.

SCHRITT 3 Geben Sie unter **Benutzername** den Benutzernamen ein (unabhängig von der ausgewählten Methode) oder verwenden Sie den Standardbenutzernamen. Der Benutzername muss mit dem auf dem SSH-Server definierten Benutzernamen übereinstimmen.

SCHRITT 4 Wenn Sie die Methode *Nach Kennwort* ausgewählt haben, geben Sie ein Kennwort (**Verschlüsselt** oder **Unverschlüsselt**) ein oder behalten Sie das verschlüsselte Standardkennwort bei.

SCHRITT 5 Führen Sie eine der folgenden Aktionen aus:

- **Übernehmen**: Die ausgewählten Authentifizierungsmethoden werden der Zugriffsmethode zugeordnet.
- **Standardanmeldeinformationen wiederherstellen**: Der Standardbenutzername und das Standardkennwort („anonymous“) werden wiederhergestellt.
- **Sensible Daten unverschlüsselt anzeigen**: Sensible Daten für die aktuelle Seite werden in unverschlüsselter Form angezeigt.

In der **SSH-Benutzerschlüsseltabelle** werden folgende Felder für die einzelnen Schlüssel angezeigt:

- **Schlüsseltyp**: RSA oder DSA.
- **Schlüsselquelle**: Automatisch generiert oder benutzerdefiniert.
- **Fingerprint**: Der anhand des Schlüssels generierte Fingerprint.

SCHRITT 6 Wählen Sie für einen RSA- oder DSA-Schlüssel RSA oder DSA aus und führen Sie eine der folgenden Aktionen aus:

- **Generieren**: Generiert einen neuen Schlüssel.
- **Bearbeiten**: Zeigt die Schlüssel an, die Sie kopieren und auf einem anderen Gerät einfügen können.

- **Löschen**: Löscht den Schlüssel.
- **Details**: Zeigt die Schlüssel an.

SSH-Serverauthentifizierung

So aktivieren Sie die SSH-Serverauthentifizierung und definieren die vertrauenswürdigen Server:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **SSH-Client** > **SSH-Serverauthentifizierung**.

SCHRITT 2 Wählen Sie **Aktivieren** aus, um die SSH-Serverauthentifizierung zu aktivieren.

- **Informiert IPv4-Quellschnittstelle**: Wählen Sie die Quellschnittstelle aus, deren IPv4-Adresse als Quell-IPv4-Adresse für die Kommunikation mit IPv4-SSH-Servern verwendet wird.
- **Informiert IPv6-Quellschnittstelle**: Wählen Sie die Quellschnittstelle aus, deren IPv6-Adresse als Quell-IPv6-Adresse für die Kommunikation mit IPv6-SSH-Servern verwendet wird.

HINWEIS Wenn Sie die Option „Auto“ auswählen, übernimmt das System die Quell-IP-Adresse aus der IP-Adresse, die auf der ausgehenden Schnittstelle definiert wurde.

SCHRITT 3 Klicken Sie auf **Hinzufügen**, und geben Sie Werte für die folgenden Felder für den vertrauenswürdigen SSH-Server ein:

- **Serverdefinition**: Wählen Sie eine der folgenden Methoden zum Identifizieren des SSH-Servers aus:
  - *Nach IP-Adresse*: Wenn Sie diese Option ausgewählt haben, geben Sie unten in die Felder die IP-Adresse des Servers ein.
  - *Nach Name*: Wenn Sie diese Option ausgewählt haben, geben Sie in das Feld **IP-Adresse/Name des Servers** den Namen des Servers ein.
- **IP-Version**: Wenn Sie den SSH-Server über die IP-Adresse festlegen, können Sie hier angeben, ob die IP-Adresse eine IPv4- oder eine IPv6-Adresse ist.
- **IP-Adresstyp**: Wenn die IP-Adresse des SSH-Servers eine IPv6-Adresse ist, wählen Sie als Adresstyp IPv6 aus. Folgende Optionen sind möglich:
  - *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix FE80, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
  - *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.
- **Link Local-Schnittstelle**: Wählen Sie aus der Schnittstellenliste die Link Local-Schnittstelle aus.

- **Server IP-Adresse/Name**: Geben Sie entweder die IP-Adresse oder den Namen des SSH-Servers ein, je nachdem, was Sie unter **Serverdefinition** ausgewählt haben.
- **Fingerprint**: Geben Sie den (vom Server kopierten) Fingerprint des SSH-Servers ein.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Definition für den vertrauenswürdigen Server wird in der aktuellen Konfigurationsdatei gespeichert.

Ändern des Benutzerkennworts auf dem SSH-Server

So ändern Sie das Kennwort auf dem SSH-Server:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **SSH-Client** > **Benutzerkennwort auf SSH-Server ändern**.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **Serverdefinition**: Definieren Sie den SSH-Server, indem Sie **Nach IP-Adresse** oder **Nach Name** auswählen. Geben Sie den Servernamen oder die IP-Adresse des Servers in das Feld **Server-IP-Adresse/Name** ein.
- **IP-Version**: Wenn Sie den SSH-Server über die IP-Adresse festlegen, können Sie hier angeben, ob die IP-Adresse eine IPv4- oder eine IPv6-Adresse ist.
- **IP-Adresstyp**: Wenn die IP-Adresse des SSH-Servers eine IPv6-Adresse ist, wählen Sie als Adresstyp IPv6 aus. Folgende Optionen sind möglich:
  - *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix FE80, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
  - *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.
- **Link Local-Schnittstelle**: Wählen Sie aus der Schnittstellenliste die Link Local-Schnittstelle aus.
- **Server IP-Adresse/Name**: Geben Sie entweder die IP-Adresse oder den Namen des SSH-Servers ein, je nachdem, was Sie unter **Serverdefinition** ausgewählt haben.
- **Benutzername**: Muss mit dem Benutzernamen auf dem Server übereinstimmen.
- **Altes Kennwort**: Muss mit dem Kennwort auf dem Server übereinstimmen.
- **Neues Kennwort**: Geben Sie das neue Kennwort ein und bestätigen Sie es im Feld **Kennwort bestätigen**.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Das Kennwort auf dem SSH-Server wird geändert.

26

Sicherheit: SSH-Server

In diesem Abschnitt wird beschrieben, wie Sie eine SSH-Sitzung im Gerät aufbauen.

Die folgenden Themen werden behandelt:

- **Übersicht**
- **Allgemeine Aufgaben**
- **Seiten für die SSH-Serverkonfiguration**

Übersicht

Mit der SSH-Serverfunktion können Benutzer eine SSH-Sitzung im Gerät erstellen. Dies ist vergleichbar mit dem Aufbauen einer Telnet-Sitzung. Der Unterschied ist jedoch, dass die Sitzung geschützt ist.

Öffentliche und private Schlüssel werden automatisch im Gerät generiert. Diese Schlüssel können vom Benutzer geändert werden.

Die SSH-Sitzung wird mit einer speziellen SSH-Clientanwendung wie beispielsweise PuTTY geöffnet.

Der SSH-Server kann in einem der folgenden Modi verwendet werden:

- **Durch intern generierte RSA-/DSA-Schlüssel (Standardeinstellung)**: Es werden ein RSA-Schlüssel und ein DSA-Schlüssel generiert. Benutzer melden sich bei der SSH-Serveranwendung an und werden automatisch für das Öffnen einer Sitzung im Gerät authentifiziert, wenn sie die IP-Adresse des Geräts angeben.
- **Modus mit öffentlichem Schlüssel**: Benutzer werden im Gerät definiert. Ihre RSA-/DSA-Schlüssel werden in einer externen SSH-Serveranwendung wie beispielsweise PuTTY generiert. Die öffentlichen Schlüssel werden im Gerät eingegeben. Die Benutzer können dann über die externe SSH-Serveranwendung eine SSH-Sitzung im Gerät öffnen.

Allgemeine Aufgaben

In diesem Abschnitt werden einige allgemeine Aufgaben beschrieben, die Sie mit der SSH-Serverfunktion ausführen.

Workflow 1: Um sich mit dem vom Gerät automatisch erstellten (Standard-)Schlüssel über SSH beim Gerät anzumelden, gehen Sie folgendermaßen vor:

SCHRITT 1 Aktivieren Sie den SSH-Server auf der Seite TCP/UDP-Services und vergewissern Sie sich auf der Seite SSH-Benutzerauthentifizierung, dass die SSH-Benutzerauthentifizierung durch öffentlichen Schlüssel deaktiviert ist.

SCHRITT 2 Melden Sie sich bei einer externen SSH-Clientanwendung (beispielsweise PuTTY) an. Verwenden Sie dabei die IP-Adresse des Geräts (Sie müssen keinen Benutzernamen oder Schlüssel verwenden, der dem Gerät bekannt ist).

Workflow 2: Um einen SSH-Benutzer zu erstellen und sich mit diesem Benutzer über SSH beim Gerät anzumelden, führen Sie die folgenden Schritte aus:

SCHRITT 1 Generieren Sie in einer externen SSH-Clientanwendung wie beispielsweise PuTTY einen RSA- oder DSA-Schlüssel.

SCHRITT 2 Aktivieren Sie auf der Seite SSH-Benutzerauthentifizierung die SSH-Benutzerauthentifizierung durch öffentlichen Schlüssel.

SCHRITT 3 Aktivieren Sie bei Bedarf die automatische Anmeldung (siehe **Automatische Anmeldung** unten).

SCHRITT 4 Fügen Sie auf der Seite SSH-Benutzerauthentifizierung einen Benutzer hinzu und kopieren Sie den extern generierten öffentlichen Schlüssel an diese Stelle.

SCHRITT 5 Melden Sie sich bei der externen SSH-Clientanwendung (beispielsweise PuTTY) an. Verwenden Sie dabei die IP-Adresse des Geräts und den Benutzernamen des Benutzers.

Workflow 3: Um einen RSA- oder DSA-Schlüssel von Gerät A nach Gerät B zu importieren, führen Sie die folgenden Schritte aus:

SCHRITT 1 Wählen Sie auf Gerät A über die Seite SSH-Serverauthentifizierung einen RSA- oder DSA-Schlüssel aus.

SCHRITT 2 Klicken Sie auf **Details** und kopieren Sie den öffentlichen Schlüssel des ausgewählten Schlüsseltyps in den Editor oder ein ähnliches Textverarbeitungsprogramm.

SCHRITT 3 Melden Sie sich bei Gerät B an und öffnen Sie die Seite SSH-Serverauthentifizierung. Wählen Sie den RSA-Schlüssel oder den DSA-Schlüssel aus, klicken Sie auf **Bearbeiten** und fügen Sie den Schlüssel von Gerät A ein.

Seiten für die SSH-Serverkonfiguration

In diesem Abschnitt werden die zum Konfigurieren der Funktion **SSH-Server** verwendeten Seiten beschrieben.

SSH-Benutzerauthentifizierung

Auf dieser Seite können Sie die SSH-Benutzerauthentifizierung durch öffentlichen Schlüssel und/oder Kennwort aktivieren und (sofern Sie die Authentifizierung durch öffentlichen Schlüssel nutzen) einen SSH-Clientbenutzer hinzufügen, der verwendet wird, um eine SSH-Sitzung in einer externen SSH-Anwendung (beispielsweise PuTTY) zu erstellen.

Vor dem Hinzufügen eines Benutzers müssen Sie in der externen SSH-Schlüsselgenerierungsanwendung bzw. SSH-Clientanwendung (wie PuTTY) einen RSA- oder DSA-Schlüssel für den Benutzer generieren.

Automatische Anmeldung

Wenn Sie die Seite „SSH-Benutzerauthentifizierung“ für die Erstellung eines SSH-Benutzernamens für einen Benutzer verwenden, der bereits in der lokalen Benutzerdatenbank konfiguriert wurde. Sie können zusätzliche Authentifizierungen verhindern, wenn Sie die Funktion **Automatisches Login** konfigurieren, die wie folgt funktioniert:

- **Aktiviert**: Wenn ein Benutzer in der lokalen Datenbank angelegt ist, und sich über SSH mit einem öffentlichen Schlüssel authentifiziert hat, wird die Authentifizierung mit dem Benutzernamen und Kennwort in der lokalen Datenbank übersprungen.

  HINWEIS Die für diese spezielle Verwaltungsmethode konfigurierte Authentifizierungsmethode (Console, Telnet, SSH usw.) muss *Lokal* sein (d. h. nicht *RADIUS* oder *TACACS+*). Weitere Informationen finden Sie unter **Verwaltungszugriffsmethode**.

- **Nicht aktiviert**: Nach der erfolgreichen Authentifizierung mit öffentlichem SSH-Schlüssel wird der Benutzer, abhängig von den auf der Seite Verwaltungszugriffsauthentifizierung konfigurierten Authentifizierungsmethoden, erneut authentifiziert.

Diese Seite ist optional. Sie müssen in SSH nicht mit Benutzerauthentifizierung arbeiten.

So aktivieren Sie die Authentifizierung und fügen einen Benutzer hinzu:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **SSH-Server** > **SSH-Benutzerauthentifizierung**.

SCHRITT 2 Aktivieren Sie folgende Felder:

- **SSH User Authentication by Password**: Aktivieren, um den SSH-Clientbenutzer mithilfe des Benutzernamens/Kennworts aus der lokalen Datenbank zu authentifizieren (siehe **Definieren von Benutzern**).
- **SSH User Authentication by Public Key**: Aktivieren, um den SSH-Clientbenutzer mit dem öffentlichen Schlüssel zu authentifizieren.
- **Automatic Login**: Kann aktiviert werden, wenn die Option **SSH User Authentication by Public Key** ausgewählt ist. Weitere Informationen hierzu finden Sie unter **Automatische Anmeldung**.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Einstellungen werden in der aktuellen Konfigurationsdatei gespeichert.

Für die konfigurierten Benutzer werden die folgenden Felder angezeigt:

- **SSH-Benutzername**: Benutzername des Benutzers.
- **Schlüsseltyp**: Gibt an, ob es sich um einen RSA- oder DSA-Schlüssel handelt.
- **Fingerprint**: Der anhand der öffentlichen Schlüssel generierte Fingerprint.

SCHRITT 4 Klicken Sie auf **Hinzufügen**, um einen neuen Benutzer hinzuzufügen, und geben Sie Werte für die Felder ein:

- **SSH-Benutzername**: Geben Sie einen Benutzernamen ein.
- **Schlüsseltyp**: Wählen Sie **RSA** oder **DSA** aus.
- **Öffentlicher Schlüssel**: Kopieren Sie den von einer externen SSH-Clientanwendung (beispielsweise PuTTY) generierten öffentlichen Schlüssel in dieses Textfeld.

SCHRITT 5 Klicken Sie auf **Übernehmen**, um den neuen Benutzer zu speichern.

Für alle konfigurierten Benutzer werden die folgenden Felder angezeigt:

- **IP-Adresse**: Die IP-Adresse des aktiven Benutzers.
- **SSH-Benutzername**: Der Benutzername des aktiven Benutzers.
- **SSH-Version**: Die vom aktiven Benutzer verwendete SSH-Version.
- **Verschlüsselung**: Die Verschlüsselung des aktiven Benutzers.
- **Authentifizierungscode**: Der Authentifizierungscode des aktiven Benutzers.

SSH-Serverauthentifizierung

Beim Starten des Geräts mit Werkseinstellungen werden automatisch öffentliche und private RSA- und DSA-Schlüssel generiert. Die einzelnen Schlüssel werden auch automatisch erstellt, wenn der entsprechende von einem Benutzer konfigurierte Schlüssel vom Benutzer gelöscht wird.

So generieren Sie einen RSA- oder DSA-Schlüssel erneut oder kopieren einen auf einem anderen Gerät generierten RSA- oder DSA-Schlüssel:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **SSH-Server** > **SSH-Serverauthentifizierung**.

Folgende Felder werden für jeden Schlüssel angezeigt:

- **Schlüsseltyp**: RSA oder DSA.
- **Schlüsselquelle**: Automatisch generiert oder benutzerdefiniert.
- **Fingerprint**: Der anhand des Schlüssels generierte Fingerprint.

SCHRITT 2 Wählen Sie einen RSA-Schlüssel oder einen DSA-Schlüssel aus.

SCHRITT 3 Sie können folgende Aufgaben ausführen:

- **Generieren**: Generiert einen Schlüssel des ausgewählten Typs.
- **Bearbeiten**: Mit dieser Option können Sie einen Schlüssel von einem anderen Gerät kopieren.
- **Entfernen**: Mit dieser Option können Sie einen Schlüssel löschen.
- **Details**: Mit dieser Option können Sie den generierten Schlüssel anzeigen. Im Fenster „Details“ können Sie außerdem auf **Sensible Daten unverschlüsselt anzeigen** klicken. Wenn Sie auf diese Option klicken, werden die Schlüssel in unverschlüsselter Form und nicht in verschlüsselter Form angezeigt. Wenn der Schlüssel bereits unverschlüsselt angezeigt wird, können Sie auf **Sensible Daten verschlüsselt anzeigen** klicken, um den Text in verschlüsselter Form anzuzeigen.

27

Sicherheit: Sicheres Verwalten sensibler Daten (SSD)

Secure Sensitive Data (SSD) ist eine Architektur, die den Schutz sensibler Daten (beispielsweise Kennwörter und Schlüssel) auf einem Gerät ermöglicht. Die Funktion nutzt Passphrases, Verschlüsselung, Zugriffssteuerung und Benutzerauthentifizierung, um eine sichere Lösung für die Verwaltung sensibler Daten bereitzustellen.

Die Funktion schützt darüber hinaus die Integrität von Konfigurationsdateien und den Konfigurationsprozess und unterstützt die automatische SSD-Konfiguration ohne Benutzereingriff.

Einleitung

SSD schützt sensible Daten auf einem Gerät wie beispielsweise Kennwörter und Schlüssel und verweigert den Zugriff auf verschlüsselte und unverschlüsselte sensible Daten auf der Grundlage von Benutzeranmeldeinformationen und SSD-Regeln. Außerdem werden Konfigurationsdateien, die sensible Daten enthalten, vor Manipulationen geschützt.

Des Weiteren ermöglicht SSD das sichere Sichern und Freigeben von Konfigurationsdateien, die sensible Daten enthalten.

SSD bietet Benutzern die Flexibilität, die gewünschte Schutzstufe für ihre sensiblen Daten zu konfigurieren. Die Möglichkeiten reichen von sensiblen Daten in unverschlüsselter Form ohne Schutz über minimalen Schutz mit Verschlüsselung auf der Grundlage der Standard-Passphrase bis zum besseren Schutz mit Verschlüsselung auf der Grundlage einer benutzerdefinierten Passphrase.

SSD erteilt Leseberechtigungen für sensible Daten nur authentifizierten und autorisierten Benutzern und gemäß SSD-Regeln. Ein Gerät authentifiziert und autorisiert den Verwaltungszugriff für Benutzer durch den Benutzerauthentifizierungsprozess.

Unabhängig von der Verwendung von SSD sollten Administratoren den Authentifizierungsprozess schützen, indem sie die lokale Authentifizierungsdatenbank verwenden und/oder die Kommunikation mit dem beim Benutzerauthentifizierungsprozess verwendeten externen Authentifizierungsserver schützen.

Zusammengefasst schützt SSD sensible Daten auf einem Gerät mit SSD-Regeln, SSD-Eigenschaften und Benutzerauthentifizierung. Die Konfigurationen für SSD-Regeln, SSD-Eigenschaften und Benutzerauthentifizierung des Geräts stellen selbst sensible Daten dar, die mit SSD geschützt werden.

SSD-Verwaltung

Die SSD-Verwaltung umfasst eine Sammlung von Konfigurationsparametern, die die Behandlung und Sicherheit sensibler Daten definieren. Auch die SSD-Konfigurationsparameter selbst sind sensible Daten und werden mit SSD geschützt.

Die gesamte Konfiguration von SSD wird auf SSD-Seiten ausgeführt, die ausschließlich Benutzern mit den entsprechenden Berechtigungen zur Verfügung stehen (siehe **SSD-Regeln**).

SSD-Regeln

SSD-Regeln definieren die Leseberechtigungen und den Standardlesemodus für eine Benutzersitzung in einem Verwaltungskanal.

Eine SSD-Regel wird anhand des Benutzers und des SSD-Verwaltungskanals eindeutig identifiziert. Es ist möglich, dass für den gleichen Benutzer unterschiedliche SSD-Regeln für unterschiedliche Kanäle vorhanden sind. Umgekehrt sind Regeln für den gleichen Kanal, aber für unterschiedliche Benutzer möglich.

Leseberechtigungen bestimmen, auf welche Weise sensible Daten angezeigt werden können: nur in verschlüsselter Form, nur in unverschlüsselter Form, sowohl in verschlüsselter als auch in unverschlüsselter Form oder überhaupt nicht. Die SSD-Regeln selbst werden als sensible Daten geschützt.

Ein Gerät kann insgesamt 32 SSD-Regeln unterstützen.

Ein Gerät erteilt einem Benutzer die SSD-Leseberechtigung der SSD-Regel, die der Identität bzw. den Anmeldeinformationen des Benutzers sowie dem Typ des Verwaltungskanals, über den der Benutzer auf die sensiblen Daten zugreifen möchte, am genauesten entspricht.

Ein Gerät verfügt über einen Satz SSD-Standardregeln. Ein Administrator kann nach Bedarf SSD-Regeln hinzufügen, löschen und ändern.

HINWEIS Ein Gerät unterstützt möglicherweise nicht alle durch SSD definierten Kanäle.

Elemente einer SSD-Regel

Eine SSD-Regel enthält die folgenden Elemente:

- **Benutzertyp**: Die unterstützten Benutzertypen in der Reihenfolge von der höchsten bis zur niedrigsten Priorität lauten wie folgt: (Wenn ein Benutzer mehreren SSD-Regeln entspricht, wird die Regel für den Benutzertyp mit der höchsten Priorität angewendet).
  - **Spezifisch**: Die Regel gilt für einen bestimmten Benutzer.
  - **Standardbenutzer (cisco)**: Die Regel gilt für den Standardbenutzer (cisco).
  - **Ebene 15**: Die Regel gilt für Benutzer mit Berechtigungsebene 15.
  - **Alle**: Die Regel gilt für alle Benutzer.
- **Benutzername**: Für den Benutzertyp „Spezifisch“ ist ein Benutzername erforderlich.
- **Kanal:** Der Typ des SSD-Verwaltungskanals, auf den die Regel angewendet werden soll. Folgende Kanaltypen werden unterstützt:
  - **Sicher**: Gibt an, dass die Regel nur für sichere Kanäle gilt. Je nach Gerät werden möglicherweise einige oder alle der folgenden sicheren Kanäle unterstützt: Konsolen-Port-Schnittstelle, SCP, SSH und HTTPS.
  - **Unsicher**: Gibt an, dass die Regel nur für unsichere Kanäle gilt. Je nach Gerät werden möglicherweise einige oder alle der folgenden unsicheren Kanäle unterstützt: Telnet, TFTP und HTTP.
  - **Sicheres XML-SNMP**: Gibt an, dass die Regel nur für XML über HTTPS oder SNMPv3 mit Datenschutz gilt. Ein Gerät unterstützt möglicherweise nicht alle sicheren XML- und SNMP-Kanäle.
  - **Unsicheres XML-SNMP**: Gibt an, dass die Regel nur für XML über HTTP oder SNMPv1/v2 sowie SNMPv3 ohne Datenschutz gilt. Ein Gerät unterstützt möglicherweise nicht alle sicheren XML- und SNMP-Kanäle.

- **Leseberechtigung**: Die den Regeln zugeordneten Leseberechtigungen. Die folgenden Einstellungen sind möglich:
  - (Am niedrigsten) **Ausschließen**: Die Benutzer dürfen nicht auf sensible Daten in irgendeiner Form zugreifen.
  - (Mittel) **Nur verschlüsselt**: Die Benutzer dürfen nur auf sensible Daten in verschlüsselter Form zugreifen.
  - (Höher) **Nur unverschlüsselt**: Die Benutzer dürfen nur auf sensible Daten in unverschlüsselter Form zugreifen. Außerdem erhalten die Benutzer Lese- und Schreibberechtigungen für SSD-Parameter.
  - (Am höchsten) **Beide**: Die Benutzer verfügen über die Berechtigungen „Verschlüsselt“ und „Unverschlüsselt“ und dürfen auf sensible Daten in verschlüsselter Form und in unverschlüsselter Form zugreifen. Außerdem erhalten die Benutzer Lese- und Schreibberechtigungen für SSD-Parameter.

  Jeder Verwaltungskanal lässt bestimmte Leseberechtigungen zu. Diese werden nachfolgend zusammengefasst.

Verwaltungskanal	Zulässige Optionen für Leseberechtigung
Sicher	Beide, Nur verschlüsselt
Unsicher	Beide, Nur verschlüsselt
Sicheres XML-SNMP	Ausschließen, Nur unverschlüsselt
Unsicheres XML-SNMP	Ausschließen, Nur unverschlüsselt

- **Standardlesemodus**: Für alle Standardlesemodi gilt die Leseberechtigung der Regel. Die folgenden Optionen sind vorhanden. Einige werden jedoch möglicherweise abhängig von der Leseberechtigung abgelehnt. Wenn die benutzerdefinierte Leseberechtigung für einen Benutzer beispielsweise „Ausschließen“ lautet und der Standardlesemodus „Verschlüsselt“ entspricht, hat die benutzerdefinierte Leseberechtigung Vorrang.
  - **Ausschließen**: Das Lesen sensibler Daten ist nicht zulässig.
  - **Verschlüsselt**: Sensible Daten werden in verschlüsselter Form angezeigt.
  - **Unverschlüsselt**: Sensible Daten werden in unverschlüsselter Form angezeigt.

Jeder Verwaltungskanal lässt bestimmte Leseberechtigungen zu. Diese werden nachfolgend zusammengefasst.

Leseberechtigung	Zulässiger Standardlesemodus
Ausschließen	Ausschließen
Nur verschlüsselt	*Verschlüsselt
Nur unverschlüsselt	*Unverschlüsselt
Beide	*Unverschlüsselt, Verschlüsselt

*Der Lesemodus einer Sitzung kann auf der Seite SSD-Eigenschaften vorübergehend geändert werden, wenn der neue Lesemodus nicht gegen die Leseberechtigung verstößt.

HINWEIS Beachten Sie Folgendes:

- Der Standardlesemodus für die Verwaltungskanäle Sicheres XML-SNMP und Unsicheres XML-SNMP muss mit deren Leseberechtigung identisch sein.
- Die Leseberechtigung „Ausschließen“ ist nur für die Verwaltungskanäle „Sicheres XML-SNMP“ und „Unsicheres XML-SNMP“ zulässig, für reguläre sichere und unsichere Kanäle ist „Ausschließen“ nicht zulässig.
- Das Ausschließen sensibler Daten in sicheren und unsicheren XML-SNMP-Verwaltungskanälen bedeutet, dass die sensiblen Daten als 0 (Zeichenfolgen „null“ oder numerische 0) angezeigt werden. Wenn der Benutzer sensible Daten anzeigen möchte, muss die Regel in „Unverschlüsselt“ geändert werden.
- Ein SNMPv3-Benutzer mit Datenschutz und Berechtigungen für XML über sichere Kanäle gilt als Benutzer der Ebene 15.
- SNMP-Benutzer in den Kanälen „Unsicheres XML“ und „Unsicheres SNMP“ (SNMPv1, v2 und v3 ohne Datenschutz) gelten als zu „Alle Benutzer“ gehörend.
- SNMP-Community-Namen werden nicht als Benutzernamen für den Abgleich mit SSD-Regeln verwendet.
- Sie können den Zugriff durch einen bestimmten SNMPv3-Benutzer steuern, indem Sie eine SSD-Regel mit einem Benutzernamen konfigurieren, der dem SNMPv3-Benutzernamen entspricht.
- Es muss immer mindestens eine Regel mit Leseberechtigung vorhanden sein: „Nur unverschlüsselt“ oder „Beide“, da nur Benutzer mit diesen Berechtigungen auf die SSD-Seiten zugreifen können.
- Änderungen am Standardlesemodus und an Leseberechtigungen einer Regel werden sofort wirksam und auf die betreffenden Benutzer und den betreffenden Kanal aller aktiven Verwaltungssitzungen angewendet. Davon ausgenommen ist die Sitzung, in der die Änderungen vorgenommen werden, auch wenn die Regel zutrifft. Wenn eine Regel geändert wird (durch Hinzufügen, Löschen oder Bearbeiten), aktualisiert das System alle betroffenen CLI/GUI-Sitzungen.

HINWEIS Wenn die auf die Sitzungsanmeldung angewendete SSD-Regel in der jeweiligen Sitzung geändert wird, muss sich der Benutzer ab- und wieder anmelden, um die Änderung zu sehen.

HINWEIS Bei einer durch einen XML- oder SNMP-Befehl initiierten Dateiübertragung wird als zugrunde liegendes Protokoll TFTP verwendet. Daher werden die SSD-Regeln für unsichere Kanäle angewendet.

SSD-Regeln und Benutzerauthentifizierung

SSD erteilt SSD-Berechtigungen nur authentifizierten und autorisierten Benutzern und gemäß den SSD-Regeln. Ein Gerät ist darauf angewiesen, dass sein Benutzerauthentifizierungsprozess den Verwaltungszugriff authentifiziert und autorisiert. Zum Schutz eines Geräts und seiner Daten einschließlich sensibler Daten und SSD-Konfigurationen vor nicht autorisiertem Zugriff wird empfohlen, den Benutzerauthentifizierungsprozess auf einem Gerät zu schützen. Zum Schützen des Benutzerauthentifizierungsprozesses können Sie die lokale Authentifizierungsdatenbank verwenden und die Kommunikation über externe Authentifizierungsserver, wie beispielsweise RADIUS-Server, schützen. Die Konfiguration der sicheren Kommunikation mit den externen Authentifizierungsservern enthält sensible Daten, die durch SSD geschützt werden.

HINWEIS Die Benutzeranmeldeinformationen in der lokalen Authentifizierungsdatenbank werden bereits durch einen von SSD unabhängigen Mechanismus geschützt.

Wenn ein Benutzer aus einem Kanal eine Aktion ausführt, bei der ein alternativer Kanal verwendet wird, wendet das Gerät die Leseberechtigung und den Standardlesemodus aus der SSD-Regel an, die den Benutzeranmeldeinformationen und dem alternativen Kanal entspricht. Wenn sich beispielsweise ein Benutzer über einen sicheren Kanal anmeldet und eine TFTP-Upload-Sitzung startet, wird die SSD-Leseberechtigung des Benutzers für den unsicheren Kanal (TFTP) angewendet.

SSD-Standardregeln

Das Gerät verfügt über die folgenden werkseitig konfigurierten Standardregeln:

Tabelle 7

Regelschlüssel		Regelaktion	
Benutzer	**Kanal**	**Leseberechtigung**	**Standardlesemodus**
Ebene 15	Sicheres XML-SNMP	Nur unverschlüsselt	Unverschlüsselt
Ebene 15	Sicher	Beide	Verschlüsselt
Ebene 15	Unsicher	Beide	Verschlüsselt
Alle	Unsicheres XML-SNMP	Ausschließen	Ausschließen
Alle	Sicher	Nur verschlüsselt	Verschlüsselt
Alle	Unsicher	Nur verschlüsselt	Verschlüsselt

Die Standardregeln können Sie ändern, aber nicht löschen. Wenn die SSD-Standardregeln geändert wurden, können sie wiederhergestellt werden.

Außerkraftsetzung des SSD-Standardlesemodus für Sitzungen

Das System enthält sensible Daten in einer Sitzung. Diese sind abhängig von der Leseberechtigung und dem Standardlesemodus des Benutzers verschlüsselt oder unverschlüsselt.

Der Standardlesemodus kann vorübergehend außer Kraft gesetzt werden, solange dadurch kein Konflikt mit der SSD-Leseberechtigung der Sitzung entsteht. Diese Änderung wird in der aktuellen Sitzung sofort wirksam, bis eines der folgenden Ereignisse eintritt:

- Der Benutzer ändert den Modus erneut.
- Die Sitzung wird beendet.
- Die Leseberechtigung der auf den Sitzungsbenutzer angewendeten SSD-Regel wird geändert und ist nicht mehr mit dem aktuellen Lesemodus der Sitzung kompatibel. In diesem Fall kehrt der Sitzungslesemodus zum Standardlesemodus der SSD-Regel zurück.

SSD-Eigenschaften

Bei SSD-Eigenschaften handelt es sich um einen Satz von Parametern, die in Verbindung mit den SSD-Regeln die SSD-Umgebung eines Geräts definieren und steuern. Die SSD-Umgebung besteht aus diesen Eigenschaften:

- Steuerung der Art der Verschlüsselung sensibler Daten
- Steuerung der Sicherheitsstufe für Konfigurationsdateien
- Steuerung der Anzeige sensibler Daten innerhalb der aktuellen Sitzung

Kennsatz

Eine Passphrase bildet die Grundlage für den Sicherheitsmechanismus der SSD-Funktion und wird verwendet, um den Schlüssel für die Ver- und Entschlüsselung sensibler Daten zu generieren. Switches der Serien Sx200, Sx300, Sx500 und SG500x/SG500XG/ESW2-550X mit derselben Passphrase können mit dem aus der Passphrase generierten Schlüssel gegenseitig ihre sensiblen Daten entschlüsseln.

Eine Passphrase muss den folgenden Regeln entsprechen:

- **Länge**: Zwischen 8 und 16 Zeichen.
- **Zeichenklassen**: Die Passphrase muss mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen (z. B. # oder $) enthalten.

Standard-Passphrases und benutzerdefinierte Passphrases

Alle Geräte verfügen im Auslieferungszustand über eine für Benutzer transparente Standard-Passphrase. Die Standard-Passphrase wird nie in der Konfigurationsdatei oder in der CLI/GUI angezeigt.

Wenn höhere Sicherheit und besserer Schutz gewünscht werden, sollte ein Administrator SSD auf einem Gerät so konfigurieren, dass eine benutzerdefinierte Passphrase anstelle der Standard-Passphrase verwendet wird. Eine benutzerdefinierte Passphrase sollte als gut gehütetes Geheimnis behandelt werden, damit die Sicherheit der sensiblen Daten im Gerät nicht gefährdet wird.

Eine benutzerdefinierte Passphrase kann manuell in unverschlüsselter Form konfiguriert werden. Sie kann auch von einer Konfigurationsdatei abgeleitet werden. (Weitere Informationen hierzu finden Sie unter **Automatische Konfiguration sensibler Daten ohne Benutzereingriff**.) Benutzerdefinierte Passphrases werden von einem Gerät immer in verschlüsselter Form angezeigt.

Lokale Passphrase

Ein Gerät verwaltet eine lokale Passphrase als Passphrase für seine aktuelle Konfiguration. SSD verwendet für die Verschlüsselung und Entschlüsselung sensibler Daten normalerweise den anhand der lokalen Passphrase generierten Schlüssel.

Die lokale Passphrase kann als Standard-Passphrase oder benutzerdefinierte Passphrase konfiguriert werden. Standardmäßig sind lokale Passphrase und Standard-Passphrase identisch. Sie können die Passphrase durch administrative Aktionen über die Befehlszeilenschnittstelle (falls verfügbar) oder über die webbasierte Benutzeroberfläche ändern. Sie wird automatisch in die Passphrase in der Startkonfigurationsdatei geändert, wenn die Startkonfiguration zur aktuellen Konfiguration des Geräts wird. Beim Zurücksetzen eines Geräts auf die Werkseinstellungen wird die lokale Passphrase auf die Standard-Passphrase zurückgesetzt.

Steuerung der Konfigurationsdateipassphrase

Die Steuerung der Datei-Passphrase bietet zusätzlichen Schutz für eine benutzerdefinierte Passphrase und die sensiblen Daten in textbasierten Konfigurationsdateien, die mit dem anhand der benutzerdefinierten Passphrase generierten Schlüssel verschlüsselt werden.

Es gibt folgende Steuerungsmodi für die Passphrase:

- **Unbeschränkt** (Standard): Das Gerät schließt seine Passphrase beim Erstellen einer Konfigurationsdatei ein. So kann jedes Gerät, das die Konfigurationsdatei akzeptiert, die Passphrase der Datei entnehmen.
- **Beschränkt**: Das Gerät beschränkt das Exportieren seiner Passphrase in eine Konfigurationsdatei. Der Modus „Beschränkt“ schützt die verschlüsselten sensiblen Daten in einer Konfigurationsdatei von Geräten, die die Passphrase nicht kennen. Dieser Modus sollte verwendet werden, wenn ein Benutzer die Passphrase nicht in einer Konfigurationsdatei verfügbar machen möchte.

Nach dem Zurücksetzen eines Geräts auf die Werkseinstellungen wird seine lokale Passphrase auf die Standard-Passphrase zurückgesetzt. Daher kann das Gerät keine sensiblen Daten entschlüsseln, die anhand einer benutzerdefinierten Passphrase verschlüsselt wurden, die in einer Verwaltungssitzung (GUI/CLI) eingegeben wurde, oder die sich in einer Konfigurationsdatei mit dem Modus „Beschränkt“ befinden. Dazu gehören auch die Dateien, die das Gerät selbst erstellt hat, bevor es auf die Werkseinstellungen zurückgesetzt wurde. Dies gilt, bis das Gerät manuell mit der benutzerdefinierten Passphrase neu konfiguriert wird oder die benutzerdefinierte Passphrase aus einer Konfigurationsdatei erfährt.

Steuerung der Konfigurationsdateiintegrität

Ein Benutzer kann eine Konfigurationsdatei vor Manipulationen oder Änderungen schützen, indem er die Konfigurationsdatei mit Steuerung der Konfigurationsdateiintegrität erstellt. Es wird empfohlen, die Steuerung der Konfigurationsdateiintegrität zu aktivieren, wenn ein Gerät eine benutzerdefinierte Passphrase mit unbeschränkter Steuerung der Konfigurationsdatei-Passphrase verwendet.

VORSICHT Jede Änderung an einer Konfigurationsdatei mit Integritätsschutz gilt als Manipulation.

Ein Gerät ermittelt, ob die Integrität einer Konfigurationsdatei geschützt ist, indem es den Befehl für die Steuerung der Dateiintegrität im SSD-Steuerungsblock der Datei untersucht. Wenn die Integrität einer Datei geschützt ist und das Gerät feststellt, dass die Integrität der Datei nicht intakt ist, lehnt das Gerät die Datei ab. Anderenfalls wird die Datei zur weiteren Verarbeitung akzeptiert.

Ein Gerät überprüft die Integrität einer textbasierten Konfigurationsdatei, wenn die Datei in die Startkonfigurationsdatei heruntergeladen oder kopiert wird.

Lesemodus

Jede Sitzung hat einen Lesemodus. Dieser bestimmt, wie sensible Daten angezeigt werden. Der Lesemodus kann Unverschlüsselt lauten, sodass sensible Daten als normaler Text angezeigt werden, oder Verschlüsselt, sodass sensible Daten in verschlüsselter Form angezeigt werden.

Konfigurationsdateien

Eine Konfigurationsdatei enthält die Konfiguration eines Geräts. Ein Gerät hat eine aktuelle Konfigurationsdatei, eine Startkonfigurationsdatei, eine Spiegelkonfigurationsdatei (optional) und eine Backup-Konfigurationsdatei. Ein Benutzer kann manuell eine Konfigurationsdatei auf einen Remote-Dateiserver hochladen bzw. von einem solchen Server herunterladen. Ein Gerät kann seine Startkonfigurationsdatei in der Phase der automatischen Konfiguration automatisch über DHCP von einem Remote-Dateiserver herunterladen. Auf Remote-Dateiservern gespeicherte Konfigurationsdateien werden als Remote-Konfigurationsdateien bezeichnet.

Eine aktuelle Konfigurationsdatei enthält die Konfiguration, die zurzeit von einem Gerät verwendet wird. Die Konfiguration in einer Startkonfigurationsdatei wird nach dem Neustart zur aktuellen Konfiguration. Die aktuelle Konfigurationsdatei und die Startkonfigurationsdatei liegen in einem internen Format vor. Die Spiegelkonfigurationsdatei, die Backup-Konfigurationsdatei und die Remote-Konfigurationsdatei sind textbasierte Dateien, die in der Regel zu Archivierungs-, Aufzeichnungs- oder Wiederherstellungszwecken aufbewahrt werden. Beim Kopieren, Hochladen und Herunterladen einer Quellkonfigurationsdatei wandelt ein Gerät den Quellinhalt automatisch in das Format der Zieldatei um, wenn die beiden Dateien unterschiedlich formatiert sind.

SSD-Indikator für Dateien

Beim Kopieren der aktuellen Konfigurationsdatei oder der Startkonfigurationsdatei in eine textbasierte Konfigurationsdatei generiert das Gerät den SSD-Indikator der Datei und platziert ihn in der textbasierten Konfigurationsdatei. Dadurch wird angegeben, ob die Datei verschlüsselte sensible Daten, unverschlüsselte sensible Daten oder keine sensiblen Daten enthält.

- Wenn der SSD-Indikator vorhanden ist, muss er sich in der Header-Datei der Konfiguration befinden.
- Bei einer textbasierten Konfiguration ohne SSD-Indikator wird davon ausgegangen, dass sie keine sensiblen Daten enthält.
- Der SSD-Indikator wird verwendet, um SSD-Leseberechtigungen für textbasierte Konfigurationsdateien zu erzwingen. Er wird jedoch ignoriert, wenn die Konfigurationsdateien in die aktuelle Konfigurationsdatei oder die Startkonfigurationsdatei kopiert werden.

Der SSD-Indikator in einer Datei wird gemäß den Anweisungen des Benutzers (Einschließen verschlüsselter sensibler Daten, Einschließen unverschlüsselter sensibler Daten oder Ausschließen sensibler Daten in einer Datei) beim Kopieren festgelegt.

SSD-Steuerungsblock

Wenn ein Gerät eine textbasierte Konfigurationsdatei aus seiner Startkonfigurationsdatei oder seiner aktuellen Konfigurationsdatei erstellt und der Benutzer entscheidet, dass die Datei sensible Daten enthalten soll, schließt es einen SSD-Steuerungsblock in die Datei ein. Der vor Manipulationen geschützte SSD-Steuerungsblock enthält SSD-Regeln und SSD-Eigenschaften des Geräts, das die Datei erstellt. Ein SSD-Steuerungsblock beginnt mit „ssd-control-start“ und endet mit „ssd-control-end“.

Startkonfigurationsdatei

Das Gerät unterstützt zurzeit das Kopieren aus der aktuellen Konfigurationsdatei, der Backup-Konfigurationsdatei, der Spiegelkonfigurationsdatei und der Remote-Konfigurationsdatei in eine Startkonfigurationsdatei. Die Konfigurationen in der Startkonfiguration sind wirksam und werden nach dem Neustart zur aktuellen Konfiguration. Ein Benutzer kann die sensiblen Daten in verschlüsselter oder unverschlüsselter Form aus einer Startkonfigurationsdatei abrufen. Dabei gelten die SSD-Leseberechtigung und der aktuelle SSD-Lesemodus der Verwaltungssitzung.

Lesezugriff auf sensible Daten in der Startkonfigurationsdatei ist in jeder Form ausgeschlossen, wenn die Passphrase in der Startkonfigurationsdatei und die lokale Passphrase unterschiedlich sind.

SSD fügt beim Kopieren der Backup-Konfigurationsdatei, der Spiegelkonfigurationsdatei und der Remote-Konfigurationsdatei in die Startkonfigurationsdatei die folgenden Regeln hinzu:

- Nach dem Zurücksetzen eines Geräts auf die Werkseinstellungen wird seine gesamte Konfiguration, einschließlich der SSD-Regeln und -Eigenschaften auf die Standard-Passphrase zurückgesetzt.
- Wenn eine Quellkonfigurationsdatei verschlüsselte sensible Daten enthält, ohne dass ein SSD-Steuerungsblock vorhanden ist, lehnt das Gerät die Quelldatei ab und der Kopiervorgang schlägt fehl.
- Wenn in der Quellkonfigurationsdatei kein SSD-Steuerungsblock vorhanden ist, wird die SSD-Konfiguration in der Startkonfigurationsdatei auf die Standardeinstellungen zurückgesetzt.
- Wenn der SSD-Steuerungsblock der Quellkonfigurationsdatei eine Passphrase enthält und die Datei verschlüsselte sensible Daten enthält, die nicht mit dem anhand der Passphrase im SSD-Steuerungsblock generierten Schlüssel verschlüsselt sind, lehnt das Gerät die Quelldatei ab, und der Kopiervorgang schlägt fehl.
- Wenn die Quellkonfigurationsdatei einen SSD-Steuerungsblock enthält und die SSD-Integritätsprüfung der Datei nicht erfolgreich war, lehnt das Gerät die Quelldatei ab und der Kopiervorgang schlägt fehl.
- Wenn der SSD-Steuerungsblock der Quellkonfigurationsdatei keine Passphrase enthält, müssen alle verschlüsselten sensiblen Daten in der Datei entweder mit dem anhand der lokalen Passphrase generierten Schlüssel oder mit dem anhand der Standard-Passphrase generierten Schlüssel verschlüsselt sein. Sie können jedoch nicht mit beiden Schlüsseln verschlüsselt sein. Anderenfalls wird die Quelldatei abgelehnt und der Kopiervorgang schlägt fehl.

- Das Gerät konfiguriert in der Startkonfigurationsdatei die Passphrase, die Passphrase-Steuerung und die Dateiintegrität gegebenenfalls anhand des SSD-Steuerungsblocks in der Quellkonfigurationsdatei. Es konfiguriert die Startkonfigurationsdatei mit der Passphrase, die zum Generieren des Schlüssels für die Entschlüsselung der sensiblen Daten in der Quellkonfigurationsdatei verwendet wird. Nicht gefundene SSD-Konfigurationen werden auf die Standardeinstellung zurückgesetzt.
- Wenn die Quellkonfigurationsdatei einen SSD-Steuerungsblock enthält und die Datei unverschlüsselte sensible Daten mit Ausnahme der SSD-Konfigurationen im SSD-Steuerungsblock enthält, wird die Datei akzeptiert.

Aktuelle Konfigurationsdatei

Eine aktuelle Konfigurationsdatei enthält die Konfiguration, die zurzeit vom Gerät verwendet wird. Ein Benutzer kann die sensiblen Daten in verschlüsselter oder unverschlüsselter Form aus einer aktuellen Konfigurationsdatei abrufen. Dabei gelten die SSD-Leseberechtigung und der aktuelle SSD-Lesemodus der Verwaltungssitzung. Benutzer können die aktuelle Konfiguration ändern, indem sie die Backup-Konfigurationsdatei oder die Spiegelkonfigurationsdatei mit anderen Verwaltungsaktionen über CLI, XML, SNMP usw. kopieren.

Ein Gerät wendet die folgenden Regeln an, wenn ein Benutzer die SSD-Konfiguration in der aktuellen Konfiguration direkt ändert:

- Wenn der Benutzer, der die Verwaltungssitzung geöffnet hat, keine SSD-Berechtigungen (das heißt Leseberechtigungen für „Beide“ oder „Nur unverschlüsselt“) besitzt, lehnt das Gerät alle SSD-Befehle ab.
- Beim Kopieren aus einer Quelldatei werden der SSD-Indikator der Datei, die SSD-Steuerungsblockintegrität und die SSD-Dateiintegrität weder überprüft noch erzwungen.
- Beim Kopieren aus einer Quelldatei schlägt der Kopiervorgang fehl, wenn die Passphrase in der Quelldatei unverschlüsselt vorliegt. Wenn die Passphrase verschlüsselt ist, wird sie ignoriert.
- Beim direkten Konfigurieren der Passphrase (kein Dateikopiervorgang) in der aktuellen Konfiguration muss die Passphrase im Befehl unverschlüsselt eingegeben werden. Anderenfalls wird der Befehl abgelehnt.
- Konfigurationsbefehle mit verschlüsselten sensiblen Daten, die über einen aus der lokalen Passphrase generierten Schlüssel verschlüsselt sind, werden in die aktuelle Konfiguration übernommen. Anderenfalls tritt bei dem Konfigurationsbefehl ein Fehler auf und der Befehl wird nicht in die aktuelle Konfigurationsdatei aufgenommen.

Backup-Konfigurationsdatei und Spiegelkonfigurationsdatei

Ein Gerät generiert regelmäßig seine Spiegelkonfigurationsdatei aus der Startkonfigurationsdatei, wenn der Service für die automatische Spiegelkonfiguration aktiviert ist. Die Spiegelkonfigurationsdatei wird immer mit verschlüsselten sensiblen Daten generiert. Daher gibt der SSD-Indikator für Dateien in einer Spiegelkonfigurationsdatei immer an, dass die Datei verschlüsselte sensible Daten enthält.

Der Service für die automatische Spiegelkonfiguration ist standardmäßig aktiviert. Um die automatische Spiegelkonfiguration als aktiviert oder deaktiviert zu konfigurieren, klicken Sie auf **Administration > Dateiverwaltung > Konfigurationsdateieigenschaften**.

Ein Benutzer kann die vollständigen Spiegelkonfigurationsdateien und Backup-Konfigurationsdateien abhängig von der SSD-Leseberechtigung, dem aktuellen Lesemodus der Sitzung und dem SSD-Indikator der Datei in der Quelldatei wie folgt anzeigen, kopieren und hochladen:

- Wenn eine Spiegelkonfigurationsdatei oder Backup-Konfigurationsdatei keinen SSD-Indikator für Dateien enthält, können alle Benutzer auf die Datei zugreifen.
- Ein Benutzer mit der Leseberechtigung „Beide“ kann auf alle Spiegelkonfigurationsdateien und Backup-Konfigurationsdateien zugreifen. Wenn jedoch der aktuelle Lesemodus der Sitzung nicht mit dem SSD-Indikator der Datei übereinstimmt, wird dem Benutzer eine Meldung angezeigt, aus der hervorgeht, dass diese Aktion nicht zulässig ist.
- Ein Benutzer mit der Berechtigung „Nur unverschlüsselt“ kann auf Spiegelkonfigurationsdateien und Backup-Konfigurationsdateien zugreifen, wenn der SSD-Indikator der Dateien auf sensible Daten der Kategorien „Ausschließen“ oder „Nur unverschlüsselt“ hinweist.
- Ein Benutzer mit der Berechtigung „Nur verschlüsselt“ kann auf Spiegelkonfigurationsdateien und Backup-Konfigurationsdateien zugreifen, wenn der SSD-Indikator der Dateien auf sensible Daten der Kategorien „Ausschließen“ oder „Verschlüsselt“ hinweist.
- Ein Benutzer mit der Berechtigung „Ausschließen“ kann nicht auf Spiegelkonfigurationsdateien und Backup-Konfigurationsdateien zugreifen, wenn der SSD-Indikator der Dateien auf sensible Daten der Kategorien „Verschlüsselt“ oder „Unverschlüsselt“ hinweist.

Der Benutzer sollte den SSD-Indikator der Datei nicht manuell ändern, wenn dieser auf einen Konflikt mit den sensiblen Daten in der Datei hinweist. Anderenfalls werden möglicherweise unverschlüsselte sensible Daten unerwartet verfügbar gemacht.

Automatische Konfiguration sensibler Daten ohne Benutzereingriff

Bei der automatischen SSD-Konfiguration ohne Benutzereingriff werden Zielgeräte mit verschlüsselten sensiblen Daten automatisch konfiguriert, ohne dass die Zielgeräte manuell mit der Passphrase vorkonfiguriert werden müssen, deren Schlüssel zum Verschlüsseln der sensiblen Daten verwendet wird.

Das Gerät unterstützt zurzeit die automatische Konfiguration, die standardmäßig aktiviert ist. Wenn die automatische Konfiguration auf einem Gerät aktiviert ist und das Gerät DHCP-Optionen empfängt, die einen Dateiserver und eine Boot-Datei angeben, lädt das Gerät die Boot-Datei (Remote-Konfigurationsdatei) von einem Dateiserver in die Startkonfigurationsdatei herunter und wird dann neu gestartet.

HINWEIS Der Dateiserver kann in den BOOTP-Feldern „siaddr“ und „sname“ angegeben sein oder als DHCP-Option 150 angegeben und statisch im Gerät konfiguriert sein.

Der Benutzer kann Zielgeräte sicher und automatisch mit sensiblen Daten konfigurieren, indem er zuerst anhand eines Geräts, das die entsprechenden Konfigurationen enthält, die Konfigurationsdatei erstellt, die in der automatischen Konfiguration verwendet werden soll. Das Gerät muss für folgende Aufgaben konfiguriert und entsprechend angewiesen werden:

- Verschlüsseln der sensiblen Daten in der Datei
- Erzwingen der Integrität des Dateiinhalts
- Einschließen der sicheren Authentifizierungskonfigurationsbefehle und SSD-Regeln, die den Zugriff auf Geräte und sensible Daten ordnungsgemäß steuern und schützen

Wenn die Konfigurationsdatei mit einer Benutzer-Passphrase generiert wurde und die SSD-Steuerung für die Datei-Passphrase auf „Beschränkt“ festgelegt ist, kann die sich ergebende Konfigurationsdatei in den gewünschten Zielgeräten automatisch konfiguriert werden. Damit die automatische Konfiguration mit einer benutzerdefinierten Passphrase ausgeführt werden kann, müssen die Zielgeräte jedoch manuell mit der Passphrase des Geräts vorkonfiguriert werden, das die Dateien generiert. Das heißt, hier ist ein Benutzereingriff erforderlich.

Wenn das Gerät, das die Konfigurationsdatei erstellt, sich im Passphrase-Steuerungsmodus „Unbeschränkt“ befindet, schließt das Gerät die Passphrase in die Datei ein. Daher kann der Benutzer die Zielgeräte, einschließlich Geräten im Auslieferungszustand oder mit Werkseinstellungen, automatisch mit der Konfigurationsdatei konfigurieren, ohne die Zielgeräte manuell mit der Passphrase vorzukonfigurieren. In diesem Fall ist kein Benutzereingriff erforderlich, da die Zielgeräte die Passphrase direkt aus der Konfigurationsdatei erhalten.

HINWEIS Geräte, die sofort einsatzbereit sind oder die Werkseinstellungen verwenden, greifen mithilfe des Standardbenutzers anonymous auf den SCP-Server zu.

SSD-Verwaltungskanäle

Geräte können über Verwaltungskanäle wie beispielsweise Telnet, SSH und das Internet verwaltet werden. SSD teilt die Kanäle abhängig von ihrer Sicherheit und/oder ihren Protokollen in die folgenden Kategorien ein: sicher, unsicher, sicheres XML-SNMP und unsicheres XML-SNMP.

Nachfolgend wird beschrieben, welche Verwaltungskanäle SSD als sicher bzw. unsicher betrachtet. Bei unsicheren Kanälen wird der parallele sichere Kanal angegeben.

Verwaltungskanal	SSD-Verwaltungskanaltyp	Paralleler sicherer Verwaltungskanal
Konsole	Sicher	
Telnet	Unsicher	SSH
SSH	Sicher	
GUI/HTTP	Unsicher	GUI/HTTPS
GUI/HTTPS	Sicher	
XML/HTTP	Unsicheres XML-SNMP	XML/HTTPS
XML/HTTPS	Sicheres XML-SNMP	
SNMPv1/v2/v3 ohne Datenschutz	Unsicheres XML-SNMP	Sicheres XML-SNMP
SNMPv3 mit Datenschutz	Sicheres XML-SNMP (Benutzer der Ebene 15)	
TFTP	Unsicher	SCP
SCP (Secure Copy)	Sicher	
HTTP-basierte Dateiübertragung	Unsicher	HTTPS-basierte Dateiübertragung
HTTPS-basierte Dateiübertragung	Sicher	

Menü-CLI und Kennwortwiederherstellung

Die Oberfläche der Menü-CLI kann nur von Benutzern verwendet werden, die über die Leseberechtigung „Beide“ oder „Nur unverschlüsselt“ verfügen. Andere Benutzer werden abgelehnt. In der Menü-CLI werden sensible Daten immer in unverschlüsselter Form angezeigt.

Die Kennwortwiederherstellung wird zurzeit über das Startmenü aktiviert und ermöglicht dem Benutzer die Anmeldung am Terminal ohne Authentifizierung. Wenn SSD unterstützt wird, ist diese Option nur zulässig, wenn die lokale Passphrase mit der Standard-Passphrase identisch ist. Wenn ein Gerät mit einer benutzerdefinierten Passphrase konfiguriert ist, kann der Benutzer die Kennwortwiederherstellung nicht aktivieren.

Konfigurieren von SSD

Die SSD-Funktion können Sie auf den folgenden Seiten konfigurieren:

- Die SSD-Eigenschaften legen Sie auf der Seite Eigenschaften fest.
- SSD-Regeln definieren Sie auf der Seite SSD-Regeln.

SSD-Eigenschaften

Nur Benutzer mit der SSD-Leseberechtigung „Nur unverschlüsselt“ oder „Beide“ können SSD-Eigenschaften festlegen.

So konfigurieren Sie globale SSD-Eigenschaften:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Sicheres Verwalten sensibler Daten (SSD)** > **Eigenschaften**. Folgendes Feld wird angezeigt:

- **Aktueller Typ der lokalen Passphrase**: Zeigt an, ob zurzeit die Standard-Passphrase oder eine benutzerdefinierte Passphrase verwendet wird.

SCHRITT 2 Geben Sie Werte für die folgenden Felder unter **Dauerhafte Einstellungen** ein:

- **Steuerung der Konfigurationsdateipassphrase**: Wählen Sie gemäß der Beschreibung unter **Steuerung der Konfigurationsdateipassphrase** eine Option aus.
- **Steuerung der Konfigurationsdateiintegrität**: Wählen Sie diese Option aus, um die Funktion zu aktivieren. Weitere Informationen hierzu finden Sie unter **Steuerung der Konfigurationsdateiintegrität**.

SCHRITT 3 Wählen Sie einen Lesemodus für die aktuelle Sitzung aus (siehe **Elemente einer SSD-Regel**).

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Einstellungen werden in der aktuellen Konfigurationsdatei gespeichert.

So ändern Sie die lokale Passphrase:

SCHRITT 1 Klicken Sie auf **Lokale Passphrase ändern** und geben Sie eine neue **Lokale Passphrase** ein:

- **Standard**: Verwendet die Standard-Passphrase des Geräts.
- **Benutzerdefiniert (unverschlüsselt)**: Geben Sie eine neue Passphrase ein.
- **Passphrase bestätigen**: Bestätigen Sie die neue Passphrase.

SCHRITT 2 Klicken Sie auf **Übernehmen**. Die Einstellungen werden in der aktuellen Konfigurationsdatei gespeichert.

Konfiguration der SSD-Regeln

Nur Benutzer mit der SSD-Leseberechtigung „Nur unverschlüsselt“ oder „Beide“ können SSD-Regeln festlegen.

So konfigurieren Sie SSD-Regeln:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Sicheres Verwalten sensibler Daten (SSD)** > **SSD-Regeln**.

Die zurzeit definierten Regeln werden angezeigt.

SCHRITT 2 Zum Hinzufügen einer Regel klicken Sie auf **Hinzufügen**. Geben Sie Werte für die folgenden Felder ein:

- **Benutzer**: Definiert die Benutzer, für die die Regel gilt: Wählen Sie eine der folgenden Optionen aus:
  - *Einzelner Benutzer*: Wählen Sie diese Option aus und geben Sie den Benutzernamen ein, für den diese Regel gilt (dieser Benutzer muss nicht zwangsläufig definiert werden).
  - *Standardbenutzer (cisco)*: Gibt an, dass die Regel für den Standardbenutzer gilt.
  - *Ebene 15*: Gibt an, dass die Regel für alle Benutzer mit Berechtigungsebene 15 gilt.
  - *Alle*: Gibt an, dass die Regel für alle Benutzer gilt.

- **Kanal**: Diese Option definiert die Sicherheitsstufe des Eingabekanals, für den die Regel gilt: Wählen Sie eine der folgenden Optionen aus:
  - *Sicher*: Gibt an, dass die Regel nur für sichere Kanäle gilt (Konsole, SCP, SSH und HTTPS), nicht für die Kanäle SNMP und XML.
  - *Unsicher*: Gibt an, dass die Regel nur für unsichere Kanäle gilt (Telnet, TFTP und HTTP), außer den Kanälen SNMP und XML.
  - *Sicheres XML-SNMP*: Gibt an, dass die Regel nur für XML über HTTPS und SNMPv3 mit Datenschutz gilt.
  - *Unsicheres XML-SNMP*: Gibt an, dass die Regel nur für XML über HTTP oder SNMPv1 /v2 und SNMPv3 ohne Datenschutz gilt.
- **Leseberechtigung**: Die der Regel zugeordneten Leseberechtigungen. Die folgenden Einstellungen sind möglich:
  - *Ausschließen*: Niedrigste Leseberechtigung. Die Benutzer dürfen nicht auf sensible Daten in irgendeiner Form zugreifen.
  - *Nur unverschlüsselt*: Höhere Leseberechtigung als die oben genannte. Die Benutzer dürfen nur auf sensible Daten in unverschlüsselter Form zugreifen.
  - *Nur verschlüsselt*: Mittlere Leseberechtigung. Die Benutzer dürfen nur auf sensible Daten in verschlüsselter Form zugreifen.
  - *Beide (unverschlüsselt und verschlüsselt)*: Höchste Leseberechtigung. Die Benutzer verfügen über die Berechtigungen „Verschlüsselt“ und „Unverschlüsselt“ und dürfen auf sensible Daten in verschlüsselter Form und in unverschlüsselter Form zugreifen.
- **Standardlesemodus**: Für alle Standardlesemodi gilt die Leseberechtigung der Regel. Die folgenden Optionen sind vorhanden. Einige werden jedoch möglicherweise abhängig von der Leseberechtigung der Regel abgelehnt.
  - *Ausschließen*: Das Lesen der sensiblen Daten ist nicht zulässig.
  - *Verschlüsselt*: Sensible Daten werden in verschlüsselter Form angezeigt.
  - *Unverschlüsselt*: Sensible Daten werden in unverschlüsselter Form angezeigt.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Einstellungen werden in der aktuellen Konfigurationsdatei gespeichert.

SCHRITT 4 Für die ausgewählten Regeln können folgende Aktionen ausgeführt werden:

- **Hinzufügen**, **Bearbeiten** oder **Löschen** von Regeln.
- **Standard wiederherstellen**: Stellt die ursprüngliche Version einer von einem Benutzer geänderten Standardregel wieder her.

28

Zugriffssteuerung

Die Funktion Zugriffssteuerungsliste (Access Control List, ACL) ist Teil des Sicherheitsmechanismus. ACL-Definitionen dienen als einer der Mechanismen zur Definition von Datenverkehrsflüssen, die eine bestimmte Quality of Service (Servicequalität, QoS) erhalten. Weitere Informationen finden Sie unter **Quality of Service**.

ACLs ermöglichen es Netzwerkmanagern, Muster (Filter und Aktionen) für den eingehenden Datenverkehr zu definieren. Paketen, die am Gerät über einen Port oder eine LAG mit einer aktiven ACL eingehen, wird der Zugang entweder gewährt oder verweigert.

Der Abschnitt enthält die folgenden Themen:

- **Zugriffssteuerungslisten**
- **MAC-basierte ACLs**
- **IPv4-basierte ACLs**
- **IPv6-basierte ACLs**
- **ACL-Bindung**

Zugriffssteuerungslisten

Eine Zugriffssteuerungsliste (Access Control List, ACL) ist eine geordnete Liste von Klassifikationsfiltern und -aktionen. Eine einzelne Klassifikationsregel plus die dazugehörige Aktion wird als Zugriffssteuerungselement (Access Control Element, ACE) bezeichnet.

Jedes ACE besteht aus Filtern, die zwischen Datenverkehrsgruppen und zugehörigen Aktionen unterscheiden. Eine einzelne ACL kann eines oder mehrere ACEs enthalten, die auf den Inhalt eingehender Frames angewendet werden. Auf Frames, deren Inhalt mit dem Filter übereinstimmt, wird entweder die Aktion VERWEIGERN oder die Aktion ZULASSEN angewendet.

Das Gerät unterstützt maximal 512 ACLs und maximal 512 ACEs.

Wenn ein Paket mit einem ACE-Filter übereinstimmt, wird die ACE-Aktion durchgeführt und die Verarbeitung dieser ACL gestoppt. Wenn das Paket nicht mit dem ACE-Filter übereinstimmt, wird das nächste ACE verarbeitet. Wenn alle ACEs einer ACL abgearbeitet worden sind, ohne dass eine Übereinstimmung gefunden wurde, und wenn eine weitere ACL vorhanden ist, wird diese in ähnlicher Weise abgearbeitet.

HINWEIS Wenn mit keinem der ACEs in keiner der relevanten ACLs eine Übereinstimmung gefunden wird, erfolgt eine Drop-Aktion für das Paket (als Standardaktion). Wegen dieser standardmäßigen Drop-Aktion müssen Sie in der ACL ausdrücklich ACEs hinzufügen, um den gewünschten Datenverkehr, einschließlich Verwaltungsverkehr wie z. B. Telnet, HTTP oder SNMP, zuzulassen, der direkt an das Gerät selbst gerichtet ist. Wenn Sie beispielsweise nicht alle Pakete verwerfen möchten, die nicht den Bedingungen in einer ACL entsprechen, müssen Sie in der ACL, die den gesamten Verkehr zulässt, explizit ein ACE mit der niedrigsten Priorität hinzufügen.

Wenn IGMP-/MLD-Snooping an einem Port aktiviert ist, der mit einer ACL verknüpft ist, fügen Sie der ACL ACE-Filter zum Weiterleiten der GMP-/MLD-Pakete an das Gerät hinzu. Anderenfalls schlägt das IGMP-/MLD-Snooping am Port fehl.

Die Reihenfolge der ACEs innerhalb der ACL ist von Bedeutung, da jeweils das erste passende ACE angewendet wird. Die ACEs werden nacheinander verarbeitet, beginnend mit dem ersten.

ACLs können zu Sicherheitszwecken angewendet werden, z. B. indem bestimmten Datenverkehrsflüssen Zugang gewährt oder verweigert wird, oder auch zur Klassifikation und Priorisierung von Datenverkehr im erweiterten QoS-Modus.

HINWEIS Ein Port kann entweder durch eine ACL gesichert oder mit einer erweiterten QoS-Richtlinie konfiguriert werden, beides gleichzeitig ist jedoch nicht möglich.

Pro Port kann es nur eine ACL geben, jedoch ist es ausnahmsweise möglich, einem einzelnen Port sowohl eine IP-basierte als auch eine IPv6-basierte ACL zuzuordnen.

Um mehrere ACLs mit einem Port zu verknüpfen, müssen Sie eine Richtlinie mit mindestens einer Klassenzuordnung verwenden.

Es können die folgenden Arten von ACLs definiert werden (abhängig davon, welcher Teil des Frame-Headers geprüft wird):

- MAC-ACL: Nur Felder der Schicht 2 werden geprüft, wie in *Definieren MAC-basierter ACLs* beschrieben.
- IP-ACL: Schicht 3 von IP-Frames wird geprüft, wie in *IPv4-basierte ACLs* beschrieben.
- IPv6-ACL: Schicht 3 von IPv4-Frames wird geprüft, wie in *Definieren einer IPv6-basierten ACL* beschrieben.

Wenn ein Frame mit einem Filter in einer ACL übereinstimmt, wird er als ein „Flow“ mit dem Namen dieser ACL definiert. Bei der erweiterten QoS kann für den Verweis auf diese Frames der Flow-Name verwendet werden und QoS kann auf diese Frames angewendet werden.

ACL-Protokollierung

Mit dieser Funktion kann eine Protokollierungsoption zu ACEs hinzugefügt werden. Bei aktivierter Funktion erzeugt jedes vom ACE zugelassene oder verweigerte Paket eine diesbezügliche SYSLOG-Nachricht zur Information.

Wenn die ACL-Protokollierung aktiviert ist, kann sie für jede Schnittstelle einzeln festgelegt werden, indem die ACL an die jeweilige Schnittstelle gebunden wird. In diesem Fall werden SYSLOGs für Pakete generiert, die mit den Zulassen- oder Verweigern-ACEs übereinstimmen, die mit der Schnittstelle verknüpft sind.

„Flow“ bezeichnet einen Strom von Paketen mit folgenden identischen Merkmalen:

- **Schicht-2-Pakete** besitzen identische Quell- und Ziel-MAC-Adressen.
- **Schicht-3-Pakete** besitzen identische Quell- und Ziel-IP-Adressen.
- **Schicht-4-Pakete** besitzen identische Quell- und Ziel-IP- und L4-Ports.

Bei jedem neuen Flow verursacht das erste Paket, das von einer bestimmten Schnittstelle aufgefangen wird, die Generierung einer SYSLOG-Nachricht zur Information. Zusätzliche Pakete aus demselben Flow werden an die CPU weitergeleitet, wobei die Anzahl der SYSLOG-Nachrichten für diesen Flow auf eine Nachricht alle 5 Minuten begrenzt ist. Dieses SYSLOG zeigt an, dass mindestens ein Paket in den vergangenen 5 Minuten aufgefangen wurde.

Nach der Verarbeitung des aufgefangenen Pakets werden die Pakete bei „Zulassen“ weitergeleitet und bei „Verweigern“ verworfen.

Für jede Einheit eines Stacks werden 150 Flows unterstützt.

SYSLOGs

Vom Schweregrad her entsprechen SYSLOG-Nachrichten einer Information und geben Aufschluss darüber, ob es beim Paket eine Übereinstimmung mit einer Verweigern-Regel oder einer Zulassen-Regel gab.

- Bei Schicht-2-Paketen enthält das SYSLOG folgende Informationen (sofern zutreffend): Quell-MAC-Adresse, Ziel-MAC-Adresse, Ethertype, VLAN-ID und CoS-Warteschlange.
- Bei Schicht-3-Paketen enthält das SYSLOG folgende Informationen (sofern zutreffend): Quell-IP-Adresse, Ziel-IP-Adresse, Protokoll, DSCP-Wert, ICMP-Typ, ICMP-Code und IGMP-Typ.
- Bei Schicht-4-Paketen enthält das SYSLOG folgende Informationen (sofern zutreffend): Quell-Port, Ziel-Port und TCP-Flag.

Nachstehend sind Beispiele möglicher SYSLOGs gezeigt:

- Für ein Nicht-IP-Paket:
  - 06-Jun-2013 09:49:56 %3SWCOS-I-LOGDENYMAC: gi0/1: deny ACE 00:00:00:00:00:01 -> ff:ff:ff:ff:ff:ff, Ethertype-2054, VLAN-20, CoS-4, trapped

- Für ein IP-Paket (v4 und v6):
  - 06-Jun-2013 12:38:53 %3SWCOS-I-LOGDENYINET: gi0/1: deny ACE IPv4(255) 1.1.1.1 -> 1.1.1.10, protocol-1, DSCP-54, ICMP Type-Echo Reply, ICMP code-5, trapped
- Für ein L4-Paket:
  - 06-Jun-2013 09:53:46 %3SWCOS-I-LOGDENYINETPORTS: gi0/1: deny ACE IPv4(TCP) 1.1.1.1(55) -> 1.1.1.10(66), trapped

Konfigurieren von ACLs

In diesem Abschnitt wird beschrieben, wie ACLs erstellt und Regeln (ACEs) hinzugefügt werden.

Workflow zum Erstellen von ACLs

Gehen Sie beim Erstellen von ACLs und bei deren Zuordnung zu einer Schnittstelle folgendermaßen vor:

1. Erstellen Sie eine oder mehrere der folgenden Arten von ACLs:
   a. MAC-basierte ACL auf den Seiten MAC-basierte ACL und MAC-basiertes ACE
   b. IP-basierte ACL auf den Seiten IPv4-basierte ACL und IPv4-basierter ACE
   c. IPv6-basierte ACL auf den Seiten IPv6-basierte ACL und IPv6-basierter ACE
2. Auf der Seite ACL-Bindung können Sie die ACL Schnittstellen zuordnen.

Ändern des ACL-Workflow

Eine ACL kann nur geändert werden, wenn Sie nicht verwendet wird. Im Folgenden wird beschrieben, wie die Bindung einer ACL aufgehoben wird, damit sie geändert werden kann:

1. Wenn die ACL keiner Klassenzuordnung des erweiterten QoS-Modus angehört, aber einer Schnittstelle zugeordnet ist, heben Sie auf der Seite *ACL-Bindung* die Bindung an die Schnittstelle auf.
2. Wenn die ACL Teil der Klassenzuordnung und nicht an eine Schnittstelle gebunden ist, kann sie geändert werden.
3. Wenn die ACL Teil einer Klassenzuordnung ist, die in einer an eine Schnittstelle gebundenen Richtlinie enthalten ist, müssen Sie die Bindung folgendermaßen aufheben:
   - Heben Sie auf der Seite *Richtlinienbindung* die Bindung der Richtlinie, die die Klassenzuordnung enthält, an die Schnittstelle auf.
   - Löschen Sie auf der Seite *Konfigurieren einer Richtlinie* (**Bearbeiten**) die Klassenzuordnung, die die ACL enthält, aus der Richtlinie.
   - Löschen Sie auf der Seite *Definieren von Klassenzuordnungen* die Klassenzuordnung, die die ACL enthält.

Erst dann kann die ACL gemäß der Beschreibung in diesem Abschnitt geändert werden.

MAC-basierte ACLs

MAC-basierte ACLs werden verwendet, um den Datenverkehr auf der Grundlage von Schicht-2-Feldern zu filtern. Anhand von MAC-basierten ACLs werden alle Frames auf Übereinstimmung geprüft.

MAC-basierte ACLs werden auf der Seite MAC-basierte ACL definiert. Die Regeln werden auf der Seite *MAC-basierter ACE* definiert.

So definieren Sie eine MAC-basierte ACL:

SCHRITT 1 Klicken Sie auf **Zugriffssteuerung** > **MAC-basierte ACL**.

Diese Seite enthält eine Liste aller aktuell definierten MAC-basierten ACLs.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie den Namen der neuen ACL in das Feld **ACL-Name** ein. Bei ACL-Namen muss Groß- und Kleinschreibung beachtet werden.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die MAC-basierte ACL wird in die aktuelle Konfigurationsdatei gespeichert.

Hinzufügen von Regeln zu einer MAC-basierten ACL

HINWEIS Jede MAC-basierte Regel verbraucht eine TCAM-Regel. Beachten Sie, dass die TCAM-Zuweisung in Paaren erfolgt; dies bedeutet, dass für die erste ACE zwei TCAM-Regeln zugewiesen werden. Die zweite TCAM-Regel wird der nächsten ACE zugewiesen usw.

So fügen Sie einer ACL Regeln (ACEs) hinzu:

SCHRITT 1 Klicken Sie auf **Zugriffssteuerung** > **MAC-basiertes ACE**.

SCHRITT 2 Wählen Sie eine ACL aus, und klicken Sie auf **Los**. Die ACEs in der ACL werden aufgelistet.

SCHRITT 3 Klicken Sie auf **Hinzufügen**.

SCHRITT 4 Geben Sie die Parameter ein.

- **ACL-Name**: Zeigt den Namen der ACL an, zu der ein ACE hinzugefügt wird.
- **Priorität**: Geben Sie die Priorität der ACE ein. ACEs mit höherer Priorität werden zuerst verarbeitet. Eins ist die höchste Priorität.

- **Aktion**: Wählen Sie die Aktion aus, die bei einer Übereinstimmung ausgeführt werden soll. Folgende Optionen sind möglich:
  - *Zulassen*: Pakete weiterleiten, die die ACE-Kriterien erfüllen.
  - *Verweigern*: Pakete löschen (Drop), die die ACE-Kriterien erfüllen.
  - *Herunterfahren*: Pakete löschen (Drop), die die ACE-Kriterien erfüllen und den Port deaktivieren, von dem die Pakete empfangen wurden. Solche Ports können auf der Seite Port-Einstellungen wieder aktiviert werden.
- **Protokollierung**: Wählen Sie diese Option aus, um die Protokollierung von ACL-Flows zu aktivieren, die mit der ACL-Regel übereinstimmen.
- **Zeitbereich**: Wählen Sie diese Option aus, um die Verwendung der ACL auf einen bestimmten Zeitbereich zu beschränken.
- **Zeitbereichsname**: Wenn **Zeitbereich** ausgewählt ist, wählen Sie den zu verwendenden Zeitbereich aus. Zeitbereiche definieren Sie im Abschnitt **Konfigurieren der Systemzeit**.
- **Ziel-MAC-Adresse**: Wählen Sie *Jede beliebige*, wenn alle Zieladressen akzeptabel sind, oder *Benutzerdefiniert*, um eine Zieladresse oder einen Bereich von Zieladressen einzugeben.
- **Wert von Ziel-MAC-Adresse**: Geben Sie die MAC-Adresse ein, mit der die Ziel-MAC-Adresse abgeglichen werden soll, sowie gegebenenfalls deren Maske.
- **Ziel-MAC-Platzhaltermaske**: Geben Sie die Maske zur Definition einer Reihe von MAC-Adressen ein. Beachten Sie, dass diese Maske sich von Masken, die sonst verwendet werden, z. B. Subnetzmasken, unterscheidet. Hier zeigt das Setzen eines Bits als **1** „indifferent“ an, und **0** bedeutet, dass dieser Wert maskiert werden soll.

  HINWEIS Geben Sie die Maske 0000 0000 0000 0000 0000 0000 1111 1111 ein (damit gleichen Sie Bits mit der Ziffer 0 ab, während Bits mit der Ziffer 1 nicht abgeglichen werden). Sie müssen die Ziffer 1 in eine dezimale Ganzzahl umwandeln und schreiben für vier Nullen jeweils 0. Da in diesem Beispiel gilt 1111 1111 = 255, wird die folgende Maske geschrieben: 0.0.0.255.
- **Quell-MAC-Adresse**: Wählen Sie *Beliebig*, wenn alle Quelladressen akzeptabel sind, oder *Benutzerdefiniert*, um eine Quelladresse oder einen Bereich von Quelladressen einzugeben.
- **Wert von Quell-MAC-Adresse**: Geben Sie die MAC-Adresse ein, mit der die Quell-MAC-Adresse abgeglichen werden soll, sowie gegebenenfalls deren Maske.
- **Quell-MAC-Platzhaltermaske**: Geben Sie die Maske zur Definition einer Reihe von MAC-Adressen ein.
- **VLAN-ID**: Geben Sie den VLAN-ID-Abschnitt des VLAN-Tags ein, mit dem Übereinstimmung bestehen soll.
- **802.1p**: Wählen Sie **Einschließen**, um 802.1p zu verwenden.

- **802.1p-Wert**: Geben Sie den 802.1p-Wert ein, der dem VPT-Tag hinzugefügt werden soll.
- **802.1p-Maske**: Geben Sie die Platzhaltermaske ein, die auf das VPT-Tag angewendet werden soll.
- **Ethertype**: Geben Sie den Ethertype des Frames ein, mit dem Übereinstimmung bestehen soll.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die MAC-basierte ACE wird in die aktuelle Konfigurationsdatei gespeichert.

IPv4-basierte ACLs

IPv4-basierte ACLs werden verwendet, um IPv4-Pakete zu überprüfen, wobei andere Arten von Frames, z. B. ARPs, nicht überprüft werden.

Die folgenden Felder können abgeglichen werden:

- IP-Protokoll (nach Namen bekannter Protokolle oder direkt nach Wert)
- Quell- bzw. Ziel-Ports für TCP-/UDP-Datenverkehr
- Flag-Werte für TCP-Frames
- ICMP- und IGMP-Typ und -Code
- Quell- bzw. Ziel-IP-Adresse (einschließlich Platzhalter)
- DSCP- bzw. IP-Prioritätswert

HINWEIS ACLs werden außerdem als Bauelemente von Flow-Definitionen für die Pro-Flow-Behandlung bei QoS verwendet.

Auf der Seite IPv4-basierte ACL können Sie dem System ACLs hinzufügen. Die Regeln werden auf der Seite IPv4-basiertes ACE definiert.

IPv6-ACLs werden auf der Seite IPv6-basierte ACL definiert.

Definieren einer IPv4-basierten ACL

So definieren Sie eine IPv4-basierte ACL:

SCHRITT 1 Klicken Sie auf **Zugriffssteuerung** > **IPv4-basierte ACL**.

Diese Seite enthält alle aktuell definierten IPv4-basierten ACLs.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie den Namen der neuen ACL in das Feld **ACL-Name** ein. Bei den Namen muss Groß- und Kleinschreibung beachtet werden.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die IPv4-basierte ACL wird in die aktuelle Konfigurationsdatei gespeichert.

Hinzufügen von Regeln (ACEs) zu einer IPv4-basierten ACL

HINWEIS Jede IPv4-basierte Regel verbraucht eine TCAM-Regel. Beachten Sie, dass die TCAM-Zuweisung in Paaren erfolgt; dies bedeutet, dass für die erste ACE zwei TCAM-Regeln zugewiesen werden. Die zweite TCAM-Regel wird der nächsten ACE zugewiesen usw.

So fügen Sie einer IPv4-basierten ACL Regeln (ACEs) hinzu:

SCHRITT 1 Klicken Sie auf **Zugriffssteuerung** > **IPv4-basiertes ACE**.

SCHRITT 2 Wählen Sie eine ACL aus, und klicken Sie auf **Los**. Für die ausgewählte ACL werden alle aktuell definierten IP-ACEs angezeigt.

SCHRITT 3 Klicken Sie auf **Hinzufügen**.

SCHRITT 4 Geben Sie die Parameter ein.

- **ACL-Name**: Zeigt den Namen der ACL an.
- **Priorität**: Geben Sie die Priorität ein. ACEs mit höherer Priorität werden zuerst verarbeitet.
- **Aktion**: Wählen Sie die Aktion aus, die dem mit dem ACE übereinstimmenden Paket zugewiesen werden soll. Verfügbare Optionen sind:
  - *Zulassen*: Pakete weiterleiten, die die ACE-Kriterien erfüllen.
  - *Verweigern*: Pakete löschen (Drop), die die ACE-Kriterien erfüllen.
  - *Herunterfahren*: Paket löschen (Drop), das die ACE-Kriterien erfüllt und den Port deaktivieren, an den das Paket adressiert war. Ports können über die Seite Port-Verwaltung wieder aktiviert werden.

- **Protokollierung**: Wählen Sie diese Option aus, um die Protokollierung von ACL-Flows zu aktivieren, die mit der ACL-Regel übereinstimmen.
- **Zeitbereich**: Wählen Sie diese Option aus, um die Verwendung der ACL auf einen bestimmten Zeitbereich zu beschränken.
- **Zeitbereichsname**: Wenn **Zeitbereich** ausgewählt ist, wählen Sie den zu verwendenden Zeitbereich aus. Zeitbereiche definieren Sie im Abschnitt **Konfigurieren der Systemzeit**.
- **Protokoll**: Sie können ein ACE entweder auf der Grundlage eines Protokolls oder einer Protokoll-ID erstellen. Wählen Sie *Beliebig (IPv4)*, um alle IP-Protokolle zu akzeptieren. Andernfalls wählen Sie eines der folgenden Protokolle aus der Dropdown-Liste **Aus Liste auswählen** aus:
  - *ICMP*: Internet Control Message Protocol
  - *IGMP*: Internet Group Management Protocol
  - *IP in IP*: IP-in-IP-Verkapselung
  - *TCP*: Transmission Control Protocol
  - *EGP*: Exterior Gateway Protocol
  - *IGP*: Interior Gateway Protocol
  - *UDP*: User Datagram Protocol
  - *HMP*: Host Mapping Protocol
  - *RDP*: Reliable Datagram Protocol
  - *IDPR*: Inter-Domain Policy Routing Protocol
  - *IPV6*: IPv6- über IPv4-Tunneling
  - *IPV6:ROUT*: Abgleich von Paketen, die zur IPv6-über-IPv4-Route durch ein Gateway gehören
  - *IPV6:FRAG*: Abgleich von Paketen, die zum IPv6-über-IPv4-Fragment-Header gehören
  - *IDPR*: Inter-Domain Routing Protocol
  - *RSVP*: ReSerVation Protocol
  - *AH*: Authentication Header
  - *IPV6:ICMP*: Internet Control Message Protocol
  - *EIGRP*: Enhanced Interior Gateway Routing Protocol
  - *OSPF*: Open Shortest Path First
  - *IPIP*: IP in IP
  - *PIM*: Protocol Independent Multicast

- *L2TP*: Layer 2 Tunneling Protocol
- *ISIS*: IGP-spezifisches Protokoll
- *Abzugleichende Protokoll-ID*: Geben Sie anstatt den Namen auszuwählen die Protokoll-ID ein.

- **Quell-IP-Adresse**: Wählen Sie *Beliebig*, wenn alle Quelladressen akzeptabel sind, oder *Benutzerdefiniert*, um eine Quelladresse oder einen Bereich von Quelladressen einzugeben.
- **Wert der Quell-IP-Adresse**: Geben Sie die IP-Adresse ein, mit der die Quell-IP-Adresse abgeglichen werden soll.
- **Quell-IP-Platzhaltermaske**: Geben Sie die Maske zur Definition einer Reihe von IP-Adressen ein. Beachten Sie, dass diese Maske sich von Masken, die sonst verwendet werden, z. B. Subnetzmasken, unterscheidet. Hier bedeutet das Festlegen eines Bits auf 1 „indifferent“ und 0 bedeutet, dass dieser Wert maskiert werden soll.

  HINWEIS Geben Sie die Maske 0000 0000 0000 0000 0000 0000 1111 1111 ein (damit gleichen Sie Bits mit der Ziffer 0 ab, während Bits mit der Ziffer 1 nicht abgeglichen werden). Sie müssen die Ziffer 1 in eine dezimale Ganzzahl umwandeln und schreiben für vier Nullen jeweils 0. Da in diesem Beispiel gilt 1111 1111 = 255, wird die folgende Maske geschrieben: 0.0.0.255.
- **Ziel-IP-Adresse**: Wählen Sie *Beliebig*, wenn alle Zieladressen akzeptabel sind, oder *Benutzerdefiniert*, um eine Zieladresse oder einen Bereich von Zieladressen einzugeben.
- **Wert der Ziel-IP-Adresse**: Geben Sie die IP-Adresse ein, mit der die Ziel-IP-Adresse abgeglichen werden soll.
- **Ziel-IP-Platzhaltermaske**: Geben Sie die Maske zur Definition einer Reihe von IP-Adressen ein.
- **Quell-Port**: Wählen Sie eine der folgenden Optionen aus:
  - *Beliebig*: Abgleich mit allen Quell-Ports.
  - *Einzeln nach Liste*: Wählen Sie einen einzelnen TCP-/UDP-Quell-Port aus, mit dem die Pakete abgeglichen werden sollen. Dieses Feld ist nur aktiv, wenn TCP oder UDP im Listen-Dropdown-Menü ausgewählt ist.
  - *Einzeln nach Nummer*: Geben Sie einen einzelnen TCP-/UDP-Quell-Port ein, mit dem die Pakete abgeglichen werden sollen. Dieses Feld ist nur aktiv, wenn TCP oder UDP im Listen-Dropdown-Menü ausgewählt ist.
  - *Bereich*: Geben Sie einen Bereich von TCP-/UDP-Quell-Ports ein, mit denen die Pakete abgeglichen werden sollen. Es können acht verschiedene Port-Bereiche konfiguriert werden (für Quell- und Ziel-Ports gemeinsam). TCP- und UDP-Protokolle haben jeweils acht Port-Bereiche.
- **Ziel-Port**: Wählen Sie einen der verfügbaren Werte aus, die mit den oben für das Feld „Quell-Port“ beschriebenen identisch sind.

  HINWEIS Sie müssen das IP-Protokoll für das ACE angeben, bevor Sie den Quell- und/oder den Ziel-Port eingeben können.

- **TCP-Flags**: Wählen Sie eines oder mehrere TCP-Flags zum Filtern von Paketen aus. Gefilterte Pakete werden entweder weitergeleitet oder gelöscht (Drop). Das Filtern von Paketen anhand von TCP-Flags verbessert die Paketkontrolle, was die Netzwerksicherheit erhöht.
- **Servicetyp**: **Der Servicetyp des IP-Pakets.**
  - *Beliebig*: Jeder beliebige Servicetyp.
  - *Abzugleichender DSCP*: Differentiated Serves Code Point (DSCP), mit dem Übereinstimmung bestehen soll.
  - *Abzugleichende IP-Priorität*: Die IP-Priorität ist ein TOS-Modell (Type of Service), mit dessen Hilfe das Netzwerk die entsprechenden QoS-Zusagen bereitstellt. Bei diesem Modell werden gemäß der Beschreibung in RFC 791 und RFC 1349 die drei signifikantesten Bits des Servicetyps im IP-Header verwendet.
- **ICMP**: Wenn das IP-Protokoll der ACL ICMP ist, wählen Sie den zu Filterzwecken verwendeten ICMP-Meldungstyp aus. Wählen Sie den Meldungstyp entweder anhand des Namens aus, oder geben Sie die Nummer des Meldungstyps ein:
  - *Beliebig*: Alle Meldungstypen werden akzeptiert.
  - *Aus Liste auswählen*: Wählen des Meldungstyps anhand des Namens.
  - *Abzugleichender ICMP-Typ*: Nummer des Meldungstyps, der zu Filterzwecken verwendet werden soll.
- **ICMP-Code**: Die ICMP-Meldungen können ein Code-Feld aufweisen, das angibt, wie mit der Meldung zu verfahren ist. Durch Auswahl einer der folgenden Optionen können Sie konfigurieren, ob anhand dieses Codes gefiltert werden soll:
  - *Beliebig*: Alle Codes akzeptieren.
  - *Benutzerdefiniert*: Geben Sie einen ICMP-Code zu Filterzwecken ein.
- **IGMP**: Wenn die ACL auf IGMP basiert, wählen Sie den zum Filtern zu verwendenden IGMP-Meldungstyp aus. Wählen Sie den Meldungstyp entweder anhand des Namens aus, oder geben Sie die Nummer des Meldungstyps ein:
  - *Beliebig*: Alle Meldungstypen werden akzeptiert.
  - *Aus Liste auswählen*: Wählen des Meldungstyps anhand des Namens.
  - *Abzugleichender IGMP-Typ*: Nummer des Meldungstyps, der zu Filterzwecken verwendet werden soll.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die IPv4-basierte ACE wird in die aktuelle Konfigurationsdatei gespeichert.

IPv6-basierte ACLs

Auf der Seite IPv6-basierte ACL können Sie IPv6-ACLs anzeigen und erstellen, mit denen ausschließlich auf IPv6 basierender Datenverkehr überprüft wird. Mit IPv6-ACLs können keine IPv6-über-IPv4- oder ARP-Pakete überprüft werden.

HINWEIS ACLs werden außerdem als Bauelemente von Flow-Definitionen für die Pro-Flow-Behandlung bei QoS verwendet.

Definieren einer IPv6-basierten ACL

So definieren Sie eine IPv6-basierte ACL:

SCHRITT 1 Klicken Sie auf **Zugriffssteuerung** > **IPv6-basierte ACL**.

In diesem Fenster wird die Liste definierter ACLs mitsamt ihres Inhalts angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie den Namen einer neuen ACL in das Feld **ACL-Name** ein. Bei den Namen muss Groß- und Kleinschreibung beachtet werden.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die IPv6-basierte ACL wird in die aktuelle Konfigurationsdatei gespeichert.

Hinzufügen von Regeln (ACEs) für eine IPv6-basierte ACL

HINWEIS Jede IPv6-basierte Regel verbraucht zwei TCAM-Regeln.

SCHRITT 1 Klicken Sie auf **Zugriffssteuerung** > **IPv6-basiertes ACE**.

In diesem Fenster werden die ACEs (Regeln) für eine bestimmte ACL (Gruppe von Regeln) angezeigt.

SCHRITT 2 Wählen Sie eine ACL aus, und klicken Sie auf **Los**. Für die ausgewählte ACL werden alle aktuell definierten IP-ACEs angezeigt.

SCHRITT 3 Klicken Sie auf **Hinzufügen**.

SCHRITT 4 Geben Sie die Parameter ein.

- **ACL-Name**: Zeigt den Namen der ACL an, zu der ein ACE hinzugefügt wird.
- **Priorität**: Geben Sie die Priorität ein. ACEs mit höherer Priorität werden zuerst verarbeitet.

- **Aktion**: Wählen Sie die Aktion aus, die dem mit dem ACE übereinstimmenden Paket zugewiesen werden soll. Verfügbare Optionen sind:
  - *Zulassen*: Pakete weiterleiten, die die ACE-Kriterien erfüllen.
  - *Verweigern*: Pakete löschen (Drop), die die ACE-Kriterien erfüllen.
  - *Herunterfahren*: Pakete löschen (Drop), die die ACE-Kriterien erfüllen und den Port deaktivieren, an den die Pakete adressiert waren. Ports können über die Seite Port-Verwaltung wieder aktiviert werden.
- **Protokollierung**: Wählen Sie diese Option aus, um die Protokollierung von ACL-Flows zu aktivieren, die mit der ACL-Regel übereinstimmen.
- **Zeitbereich**: Wählen Sie diese Option aus, um die Verwendung der ACL auf einen bestimmten Zeitbereich zu beschränken.
- **Zeitbereichsname**: Wenn **Zeitbereich** ausgewählt ist, wählen Sie den zu verwendenden Zeitbereich aus. Zeitbereiche werden im Abschnitt **Konfigurieren der Systemzeit** beschrieben.
- **Protokoll**: Wählen Sie diese Option, um ein ACE auf der Grundlage eines bestimmten Protokolls zu erstellen. Wählen Sie *Beliebig (IPv6)*, um alle IP-Protokolle zu akzeptieren. Wählen Sie andernfalls unter den folgenden Optionen:
  - *TCP*: Transmission Control Protocol. Ermöglicht die Kommunikation und den Austausch von Datenströmen zwischen zwei Hosts. TCP garantiert die Zustellung von Paketen und deren Übermittlung und Empfang in der Reihenfolge, in der sie gesendet wurden.
  - *UDP*: User Datagram Protocol. Übermittelt Pakete, garantiert aber nicht deren Zustellung.
  - *ICMP*: Gleicht Pakete nach dem Internet Control Message Protocol (ICMP) ab.
- **Abzugleichende Protokoll-ID**: Geben Sie die ID des abzugleichenden Protokolls ein.
- **Quell-IP-Adresse**: Wählen Sie *Beliebig*, wenn alle Quelladressen akzeptabel sind, oder *Benutzerdefiniert*, um eine Quelladresse oder einen Bereich von Quelladressen einzugeben.
- **Wert der Quell-IP-Adresse**: Geben Sie die IP-Adresse ein, mit der die Quell-IP-Adresse abgeglichen werden soll, sowie gegebenenfalls deren Maske.
- **Länge des Quell-IP-Präfixes**: Geben Sie die Präfixlänge der IP-Quelladresse ein.
- **Ziel-IP-Adresse**: Wählen Sie *Beliebig*, wenn alle Zieladressen akzeptabel sind, oder *Benutzerdefiniert*, um eine Zieladresse oder einen Bereich von Zieladressen einzugeben.
- **Wert der Ziel-IP-Adresse**: Geben Sie die IP-Adresse ein, mit der die Ziel-IP-Adresse abgeglichen werden soll, sowie gegebenenfalls deren Maske.
- **Länge des Ziel-IP-Präfixes**: Geben Sie die Präfixlänge der IP-Adresse ein.

- **Quell-Port**: Wählen Sie eine der folgenden Optionen aus:
  - *Beliebig*: Abgleich mit allen Quell-Ports.
  - *Einzeln nach Liste*: Wählen Sie einen einzelnen TCP-/UDP-Quell-Port aus, mit dem die Pakete abgeglichen werden sollen. Dieses Feld ist nur aktiv, wenn TCP oder UDP im Dropdown-Menü „Aus Liste auswählen“ ausgewählt ist.
  - *Einzeln nach Nummer*: Geben Sie einen einzelnen TCP-/UDP-Quell-Port ein, mit dem die Pakete abgeglichen werden sollen. Dieses Feld ist nur aktiv, wenn TCP oder UDP im Dropdown-Menü „Aus Liste auswählen“ ausgewählt ist.
  - *Bereich*: Geben Sie einen Bereich von TCP-/UDP-Quell-Ports ein, mit denen die Pakete abgeglichen werden sollen.
- **Ziel-Port**: Wählen Sie einen der verfügbaren Werte aus. (Sie sind mit den oben für den Quell-Port beschriebenen identisch).

  HINWEIS Sie müssen das IPv6-Protokoll für die ACL angeben, bevor Sie den Quell- und/oder den Ziel-Port konfigurieren können.
- **TCP-Flags**: Wählen Sie eines oder mehrere TCP-Flags zum Filtern von Paketen aus. Gefilterte Pakete werden entweder weitergeleitet oder gelöscht (Drop). Das Filtern von Paketen anhand von TCP-Flags verbessert die Paketkontrolle, was die Netzwerksicherheit erhöht.
  - Gesetzt: Übereinstimmung, wenn das Flag GESETZT ist.
  - Nicht gesetzt: Übereinstimmung, wenn das Flag NICHT GESETZT ist.
  - Indifferent: TCP-Flag ignorieren.
- **Servicetyp**: Der Servicetyp des IP-Pakets.
- **ICMP**: Wenn die ACL auf ICMP basiert, wählen Sie den ICMP-Meldungstyp aus, der zum Filtern verwendet werden soll. Wählen Sie den Meldungstyp entweder anhand des Namens aus, oder geben Sie die Nummer des Meldungstyps ein. Wählen Sie *Beliebig*, wenn alle Meldungstypen akzeptiert werden sollen.
  - *Beliebig*: Alle Meldungstypen werden akzeptiert.
  - *Aus Liste auswählen*: Wählen des Meldungstyps aus der Dropdown-Liste anhand des Namens.
  - *Abzugleichender ICMP-Typ*: Nummer des Meldungstyps, der zu Filterzwecken verwendet werden soll.
- **ICMP-Code**: Die ICMP-Meldungen können ein Code-Feld aufweisen, das angibt, wie mit der Meldung zu verfahren ist. Durch Auswahl einer der folgenden Optionen können Sie konfigurieren, ob anhand dieses Codes gefiltert werden soll.
  - *Beliebig*: Alle Codes akzeptieren.
  - *Benutzerdefiniert*: Geben Sie einen ICMP-Code zu Filterzwecken ein.

SCHRITT 5 Klicken Sie auf **Übernehmen**.

ACL-Bindung

Wenn eine ACL an eine Schnittstelle gebunden ist (Port, LAG oder VLAN), werden ihre ACE-Regeln auf Pakete angewendet, die an dieser Schnittstelle ankommen. Pakete, die mit keinem der ACEs in der ACL übereinstimmen, werden mit einer Standard-Regel abgeglichen, deren Aktion darin besteht, Pakete ohne Übereinstimmung zu löschen (Drop).

Zwar kann eine Schnittstelle jeweils nur an eine ACL gebunden werden, jedoch können mehrere Schnittstellen an dieselbe ACL gebunden werden, indem die letzteren in eine Richtlinienzuordnung gruppiert werden und diese Richtlinienzuordnung an die Schnittstelle gebunden wird.

Nachdem eine ACL an eine Schnittstelle gebunden wurde, kann sie nicht bearbeitet, geändert oder gelöscht werden, es sei denn, sie wird von allen Ports entfernt, an die sie gebunden ist oder wo sie verwendet wird.

HINWEIS Es ist möglich, eine Schnittstelle (Port, LAG oder VLAN) mit einer Richtlinie oder einer ACL zu finden, eine Bindung an eine Richtlinie und eine ACL ist jedoch nicht möglich.

So binden Sie eine ACL an ein VLAN:

SCHRITT 1 Klicken Sie auf **Zugriffssteuerung** > **ACL-Bindung (VLAN)**.

SCHRITT 2 Wählen Sie ein VLAN aus, und klicken Sie auf **Bearbeiten**.

Wenn das von Ihnen benötigte VLAN nicht angezeigt wird, fügen Sie ein neues VLAN hinzu.

SCHRITT 3 Wählen Sie eine der folgenden Optionen aus:

- **MAC-basierte ACL auswählen**: Wählen Sie eine MAC-basierte ACL aus, die an die Schnittstelle gebunden werden soll.
- **IPv4-basierte ACL auswählen**: Wählen Sie eine IPv4-basierte ACL aus, die an die Schnittstelle gebunden werden soll.
- **IPv6-basierte ACL auswählen**: Wählen Sie eine IPv6-basierte ACL aus, die an die Schnittstelle gebunden werden soll.
- **Standardaktion**: Wählen Sie eine der folgenden Optionen:
  - *Alle verweigern*: Wenn das Paket nicht einer ACL entspricht, wird es verweigert (gelöscht).
  - *Alle zulassen*: Wenn das Paket nicht einer ACL entspricht, wird es zugelassen (weitergeleitet).

  HINWEIS Die Standardaktion können Sie nur definieren, wenn IP Source Guard für die Schnittstelle nicht aktiviert ist.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die ACL-Bindung wird geändert und die aktuelle Konfigurationsdatei wird aktualisiert.

HINWEIS Wenn keine ACL ausgewählt wird, wird die Bindung der ACL aufgehoben, die zuvor an das VLAN gebunden war.

So binden Sie eine ACL an einen Port oder eine LAG:

SCHRITT 1 Klicken Sie auf **Zugriffssteuerung** > **ACL-Bindung (Port)**.

SCHRITT 2 Wählen Sie einen Schnittstellentyp aus: **Ports/LAGs** (Port oder LAG).

SCHRITT 3 Klicken Sie auf **Los**. Für jeden ausgewählten Schnittstellentyp werden alle Schnittstellen dieses Typs mit einer Liste ihrer aktuellen ACLs angezeigt:

- **Schnittstelle**: Identifikator der Schnittstelle, für die eine ACL definiert ist.
- **MAC-ACL**: ACLs des Typs MAC, die an die Schnittstelle gebunden sind (falls vorhanden).
- **IPv4-ACL**: ACLs des Typs IPv4, die an die Schnittstelle gebunden sind (falls vorhanden).
- **IPv6-ACL**: ACLs des Typs IPv6, die an die Schnittstelle gebunden sind (falls vorhanden).
- **Standardaktion**: Eine Aktion der ACL-Regeln (Alle löschen/Alle zulassen).

HINWEIS Um die Bindung aller ACLs an eine Schnittstelle aufzuheben, wählen Sie die Schnittstelle aus, und klicken Sie auf **Löschen**.

SCHRITT 4 Wählen Sie eine Schnittstelle aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 5 Wählen Sie eine der folgenden Optionen aus:

- **MAC-basierte ACL auswählen**: Wählen Sie eine MAC-basierte ACL aus, die an die Schnittstelle gebunden werden soll.
- **IPv4-basierte ACL auswählen**: Wählen Sie eine IPv4-basierte ACL aus, die an die Schnittstelle gebunden werden soll.
- **IPv6-basierte ACL auswählen**: Wählen Sie eine IPv6-basierte ACL aus, die an die Schnittstelle gebunden werden soll.
- **Standardaktion**: Wählen Sie eine der folgenden Optionen:
  - *Alle verweigern*: Wenn das Paket nicht einer ACL entspricht, wird es verweigert (gelöscht).
  - *Alle zulassen*: Wenn das Paket nicht einer ACL entspricht, wird es zugelassen (weitergeleitet).

HINWEIS Die Standardaktion können Sie nur definieren, wenn IP Source Guard für die Schnittstelle nicht aktiviert ist.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die ACL-Bindung wird geändert und die aktuelle Konfigurationsdatei wird aktualisiert.

HINWEIS Wenn keine ACL ausgewählt wird, wird die Bindung der ACL aufgehoben, die zuvor an die Schnittstelle gebunden war.

29

Quality of Service

Die Funktion Quality of Service (QoS, Servicequalität) wird auf das gesamte Netzwerk angewendet, damit der Netzwerkverkehr entsprechend den erforderlichen Kriterien priorisiert wird, also der gewünschte Datenverkehr bevorzugt behandelt wird.

In diesem Abschnitt werden die folgenden Themen behandelt:

- **Funktionen und Komponenten von QoS**
- **Konfigurieren von QoS – Allgemein**
- **QoS-Basismodus**
- **Erweiterter QoS-Modus**
- **Verwalten der QoS-Statistik**

Funktionen und Komponenten von QoS

Die QoS-Funktion dient zur Optimierung der Netzwerkleistung.

QoS bietet Folgendes:

- Klassifizierung des eingehenden Datenverkehrs in Datenverkehrsklassen, basierend auf Attributen wie:
  - Gerätekonfiguration
  - Eingangsschnittstelle
  - Paketinhalt
  - Kombination dieser Attribute

QoS beinhaltet Folgendes:

- **Klassifizierung des Datenverkehrs**: Jedes eingehende Paket wird basierend auf dem Paketinhalt und/oder dem Port als Bestandteil eines bestimmten Verkehrsflusses klassifiziert. Die Klassifizierung erfolgt anhand von Zugriffssteuerungslisten (Access Control Lists, ACLs), und nur der Datenverkehr, der die ACL-Kriterien erfüllt, wird gemäß CoS oder QoS klassifiziert.
- **Zuweisung zu Hardware-Warteschlangen**: Weist eingehende Pakete Weiterleitungswarteschlangen zu. Die Pakete werden entsprechend der Datenverkehrsklasse, der sie angehören, zur Bearbeitung an eine bestimmte Warteschlange gesendet. Weitere Informationen hierzu finden Sie unter **Konfigurieren von QoS-Warteschlangen**.
- **Sonstiges Attribut für die Bearbeitung von Datenverkehrsklassen**: Wendet QoS-Mechanismen auf verschiedene Klassen an, einschließlich der Bandbreitenverwaltung.

QoS-Betrieb

Das Header-Feld, dem vertraut werden soll, wird auf der Seite „Globale Einstellungen“ eingegeben. Jedem Wert in diesem Feld wird eine Ausgangswarteschlange zugewiesen, an die der Frame gesendet wird. Je nachdem, ob der Vertrauensmodus CoS/802.1p oder DSCP verwendet wird, verwenden Sie für die Zuweisung die Seite „CoS/802.1p zu Warteschlange“ oder die Seite „DSCP zu Warteschlange“.

QoS-Modi

Der ausgewählte QoS-Modus wird auf alle Schnittstellen im System angewendet.

- **Basismodus**: Serviceklasse (Class of Service, CoS).

  Der gesamte Datenverkehr derselben Klasse wird gleich behandelt, und zwar wird als einzige QoS-Aktion die Ausgangswarteschlange am Ausgangsport bestimmt. Diese richtet sich nach dem angegebenen QoS-Wert im eingehenden Frame. Hierbei kann es sich in Schicht 2 um den Wert des VLAN-Prioritäts-Tags (VPT) nach 802.1p und um den DSCP-Wert (Differentiated Service Code Point) für IPv4 oder den TC-Wert (Traffic Class, Datenverkehrsklasse) für IPv6 handeln.
  Schicht 3. Beim Betrieb im Basismodus, vertraut das Gerät diesem extern zugewiesenen QoS-Wert. Der extern zugewiesene QoS-Wert eines Pakets bestimmt dessen Datenverkehrsklasse und QoS.

  Das Header-Feld, dem vertraut werden soll, wird auf der Seite „Globale Einstellungen“ eingegeben. Jedem Wert in diesem Feld wird eine Ausgangswarteschlange zugewiesen, an die der Frame gesendet wird. Je nachdem, ob der Vertrauensmodus CoS/802.1p oder DSCP verwendet wird, verwenden Sie für die Zuweisung die Seite „CoS/802.1p zu Warteschlange“ oder die Seite „DSCP zu Warteschlange“.

- **Erweiterter Modus**: Quality of Service (QoS) auf Datenflussebene.

  Im erweiterten Modus besteht eine datenflussspezifische QoS aus einer Klassenzuordnung und/oder einer Überwachungsvorrichtung:

  - Eine Klassenzuordnung legt die Art des Datenverkehrs fest und enthält eine oder mehrere ACLs. Pakete, die mit den ACLs übereinstimmen, gehören zum Datenfluss.
  - Eine Überwachungsvorrichtung wendet die konfigurierte QoS auf einen Datenfluss an. Die QoS-Konfiguration eines Datenflusses kann die Ausgangswarteschlange, den DSCP- oder CoS/802.1p-Wert sowie Aktionen für profilexternen (exzessiven) Datenverkehr umfassen.

- **Deaktivierungsmodus**: In diesem Modus wird der gesamte Datenverkehr einer einzigen Warteschlange, mit der die beste Leistung erzielt wird, zugewiesen, sodass kein Datenverkehrstyp gegenüber einem anderen Datenverkehrstyp priorisiert wird.

Es kann immer nur jeweils ein Modus aktiv sein. Wenn das System so konfiguriert ist, dass es im erweiterten QoS-Modus arbeitet, sind die Einstellungen für den QoS-Basismodus nicht aktiv und umgekehrt.

Wenn der Modus geändert wird, tritt Folgendes ein:

- Wenn Sie vom erweiterten QoS-Modus in einen beliebigen anderen Modus wechseln, werden die Richtlinienprofildefinitionen und Klassenzuordnungen gelöscht. ACLs, die direkt an Schnittstellen gebunden sind, bleiben gebunden.
- Wenn Sie vom QoS-Basismodus in den erweiterten Modus wechseln, bleibt die Konfiguration des QoS-Vertrauensmodus im Basismodus nicht erhalten.

- Wenn Sie QoS deaktivieren, werden die Einstellungen für Kontrolle und Warteschlange (WRR/SP-Bandbreiteneinstellung) auf die Standardwerte zurückgesetzt.

Alle anderen Konfigurationen bleiben intakt.

QoS-Workflow

Führen Sie zum Konfigurieren der allgemeinen QoS-Parameter die folgenden Aktionen durch:

SCHRITT 1 Wählen Sie auf der Seite „QoS-Eigenschaften“ den QoS-Modus für das System aus (Basismodus, erweiterter Modus oder Deaktiviert, wie im Abschnitt **QoS-Modi** beschrieben). Bei den folgenden Schritten des Workflows wird davon ausgegangen, dass Sie QoS aktiviert haben.

SCHRITT 2 Weisen Sie auf der Seite „QoS-Eigenschaften“ jeder Schnittstelle eine CoS-Standardpriorität zu.

SCHRITT 3 Weisen Sie den Ausgangswarteschlangen auf der Seite „Warteschlange“ eine Planungsmethode (strikte Priorität oder WRR) und die Bandbreitenzuweisung für WRR zu.

SCHRITT 4 Weisen Sie auf der Seite „DSCP zu Warteschlange“ jedem IP-DSCP/TC-Wert eine Ausgangswarteschlange zu. Wenn das Gerät im DSCP-Vertrauensmodus betrieben wird, werden die eingehenden Pakete basierend auf ihrem DSCP/TC-Wert in die Ausgangswarteschlangen eingereiht.

SCHRITT 5 Weisen Sie jeder CoS/802.1p-Priorität eine Ausgangswarteschlange zu. Wenn das Gerät im CoS/802.1-Vertrauensmodus betrieben wird, werden alle eingehenden Pakete entsprechend ihrer CoS/802.1p-Priorität in die zugehörigen Ausgangswarteschlangen eingereiht. Verwenden Sie hierzu die Seite „CoS/802.1p zu Warteschlange“.

SCHRITT 6 Gilt nur für Schicht 3: Weisen Sie falls erforderlich auf der Seite „DSCP zu Warteschlange“ jedem DSCP/TC-Wert eine Warteschlange zu.

SCHRITT 7 Geben Sie auf den folgenden Seiten die Bandbreiten- und Ratenbegrenzungen ein:

a. Legen Sie auf der Seite „Ausgangskontrolle pro Warteschlange“ die Ausgangskontrolle für die einzelnen Warteschlangen fest.

b. Legen Sie auf der Seite „Bandbreite“ die Eingangsratenbegrenzung und die Ausgangskontrollrate für die einzelnen Ports fest.

SCHRITT 8 Konfigurieren Sie den ausgewählten Modus, indem Sie einen der folgenden Schritte durchführen:

a. Konfigurieren Sie den Basismodus wie unter *Workflow für das Konfigurieren des QoS-Basismodus* beschrieben.

b. Konfigurieren Sie den erweiterten Modus wie unter *Workflow für das Konfigurieren des erweiterten QoS-Modus* beschrieben.

Konfigurieren von QoS – Allgemein

Die Seite „QoS-Eigenschaften“ enthält Felder zum Festlegen des QoS-Modus für das System (Basismodus, erweiterter Modus oder Deaktiviert, wie im Abschnitt **QoS-Modi** beschrieben). Zusätzlich kann die CoS-Standardpriorität für die einzelnen Schnittstellen festgelegt werden.

Festlegen von QoS-Eigenschaften

So wählen Sie den QoS-Modus aus:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Allgemein** > **QoS-Eigenschaften**.

SCHRITT 2 Legen Sie den QoS-Modus fest. Folgende Optionen stehen zur Verfügung:

- **Deaktivieren**: QoS ist für das Gerät deaktiviert.
- **Einfach**: QoS ist im Basismodus für das Gerät aktiviert.
- **Erweitert**: QoS ist im erweiterten Modus für das Gerät aktiviert.

SCHRITT 3 Wählen Sie die Option **Port/LAG** aus und klicken Sie auf **Los**, um alle Ports/LAGs des Geräts und ihre CoS-Informationen anzuzeigen und zu bearbeiten.

Die folgenden Felder werden für alle Ports/LAGs angezeigt:

- **Schnittstelle**: Schnittstellentyp.
- **Standard-CoS**: VPT-Standardwert für eingehende Pakete, die kein VLAN-Tag besitzen. Der CoS-Standardwert ist „0“. Der Standardwert ist nur für Frames ohne Tags relevant und auch nur, falls das System im Basismodus betrieben wird und auf der Seite „Globale Einstellungen“ die Option „CoS vertrauen“ ausgewählt wurde.

Wählen Sie **Standards wiederherstellen** aus, um die standardmäßige CoS-Werkseinstellung für diese Schnittstelle wiederherzustellen.

Zum Festlegen von QoS für eine Schnittstelle wählen Sie diese aus und klicken Sie auf **Bearbeiten**.

SCHRITT 1 Geben Sie die Parameter ein.

- **Schnittstelle**: Wählen Sie den Port oder die LAG aus.
- **Standard-CoS**: Wählen Sie den CoS-Standardwert aus, der eingehenden Paketen zugewiesen werden soll (die kein VLAN-Tag besitzen).

SCHRITT 2 Klicken Sie auf **Übernehmen**. Der CoS-Standardwert für die Schnittstelle wird in der aktuellen Konfigurationsdatei gespeichert.

Konfigurieren von QoS-Warteschlangen

Das Gerät unterstützt entweder vier oder acht Warteschlangen für jede Schnittstelle (wird auf der Seite „Systemmodus und Stack-Verwaltung“ ausgewählt). Die Warteschlange Nummer vier oder acht besitzt die höchste Priorität. Die Warteschlange Nummer eins besitzt die niedrigste Priorität.

Für die Behandlung des Datenverkehrs in Warteschlangen gibt es zwei Möglichkeiten: nach strikter Priorität oder WRR (Weighted Round Robin).

- **Strikte Priorität**: Der Ausgangsverkehr der Warteschlange mit der höchsten Priorität wird zuerst übertragen. Der Datenverkehr der Warteschlangen mit niedrigerer Priorität wird erst dann verarbeitet, nachdem die Daten der prioritären Warteschlange übermittelt wurden. Der Datenverkehr der Warteschlange mit der höchsten Nummer erhält also die höchste Priorität.
- **WRR (Weighted Round Robin)**: Im WRR-Modus ist die Anzahl der von der Warteschlange gesendeten Pakete proportional zur Gewichtung der Warteschlange (je höher die Gewichtung, desto mehr Frames werden gesendet). Wenn beispielsweise maximal vier Warteschlangen möglich sind und alle vier Warteschlangen im WRR-Modus betrieben werden sowie die Standardgewichtungen verwendet werden, erhält die Warteschlange 1 1/15 der Bandbreite (vorausgesetzt, dass alle Warteschlangen belegt sind und ein Datenstau vorliegt), Warteschlange 2 erhält 2/15, Warteschlange 3 erhält 4/15 und Warteschlange 4 erhält 8/15 der Bandbreite. Vom Gerät wird nicht der standardmäßige DWRR-Algorithmus (Deficit WRR) verwendet, sondern der SDWRR-Algorithmus (Shaped Deficit WRR).

Die Warteschlangenmodi können auf der Seite „Warteschlange“ ausgewählt werden. Wenn als Warteschlangemodus die strikte Priorität verwendet wird, werden die Warteschlangen gemäß der Priorität bedient. Dabei wird zunächst Warteschlange 4 oder Warteschlange 8 (die Warteschlange mit der höchsten Priorität) bearbeitet. Sobald diese abgeschlossen wurde, wird mit der nächstniedrigeren Warteschlange fortgefahren.

Wenn als Warteschlangenmodus WRR (Weighted Round Robin) verwendet wird, wird eine Warteschlange so lange bedient, bis ihr Anteil aufgebraucht wurde, dann kommt die nächste Warteschlange an die Reihe.

Es ist auch möglich, einigen weniger wichtigen Warteschlangen WRR zuzuweisen und die wichtigeren Warteschlangen über die strikte Priorität zu steuern. In diesem Fall wird der Datenverkehr der Warteschlangen mit strikter Priorität immer vor dem Datenverkehr der WRR-Warteschlangen gesendet. Erst nachdem die Warteschlangen mit strikter Priorität vollständig abgearbeitet wurden, wird der Datenverkehr von den WRR-Warteschlangen weitergeleitet. (Der relative Anteil der einzelnen WRR-Warteschlangen hängt von deren Gewichtung ab.)

So wählen Sie die Prioritätsmethode aus und geben die WRR-Daten ein:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Allgemein** > **Warteschlange**.

SCHRITT 2 Geben Sie die Parameter ein.

- **Warteschlange**: Zeigt die Warteschlangennummer an.
- **Planungsmethode:** Wählen Sie eine der folgenden Optionen aus:
  - *Strikte Priorität*: Die Datenverkehrsplanung für die ausgewählte Warteschlange und alle Warteschlangen mit höherer Priorität richtet sich streng nach der Warteschlangenpriorität.
  - *WRR*: Die Datenverkehrsplanung für die ausgewählte Warteschlange richtet sich nach WRR. Der Zeitraum wird auf die WRR-Warteschlangen aufgeteilt, die nicht leer sind, das heißt sie haben Deskriptoren für den Ausgang. Dies kommt nur dann vor, wenn die Warteschlangen mit strikter Priorität leer sind.
  - *WRR-Gewichtung*: Wenn WRR ausgewählt ist, geben Sie die WRR-Gewichtung ein, die der Warteschlange zugewiesen ist.
  - *% der WRR-Bandbreite*: Zeigt an, wie viel Bandbreite der Warteschlange zugewiesen wurde. Die Werte stellen den prozentualen Anteil im Bezug auf die WRR-Gewichtung dar.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Warteschlangen werden konfiguriert und die aktuelle Konfigurationsdatei wird aktualisiert.

Zuordnen von CoS/802.1p zu einer Warteschlange

Auf der Seite „CoS/802.1p zu Warteschlange“ können Sie 802.1p-Prioritäten Ausgangswarteschlangen zuordnen. In der Tabelle CoS/802.1p zu Warteschlange werden die Ausgangswarteschlangen der eingehenden Pakete basierend auf der in ihren VLAN-Tags angegebenen 802.1p-Priorität bestimmt. Bei eingehenden Paketen ohne Tag wird die CoS/802.1p-Standardpriorität, die den Eingangsports zugewiesen wurde, als 802.1p-Priorität verwendet.

In der folgenden Tabelle wird die Standardzuordnung bei vier Warteschlangen beschrieben:

802.1p-Werte (0–7, wobei 7 der höchste Wert ist)	Warteschlange (4 Warteschlangen 1 - 4, wobei 4 die höchste Priorität besitzt)	Hinweise
0	1	Hintergrund
1	1	Beste Leistung
2	2	Ausgezeichnete Leistung
3	3	Wichtige Anwendung – LVS-Telefon mit SIP
4	3	Video
5	4	Voice – Cisco IP-Telefonstandard
6	4	Interwork-Steuerelement – LVS-Telefon mit RTP
7	4	Netzwerk-Steuerelement

In der folgenden Tabelle wird die Standardzuordnung bei acht Warteschlangen beschrieben:

802.1p-Werte (0–7, wobei 7 der höchste Wert ist)	Warteschlange (acht Warteschlangen 1 bis 8, wobei 8 die höchste Priorität hat) Standalone	7 Warteschlangen (8 ist die höchste Priorität für Datenverkehr zur Stacking-Steuerung) Stack	Hinweise
0	1	1	Hintergrund
1	2	1	Beste Leistung
2	3	2	Ausgezeichnete Leistung
3	6	5	Wichtige Anwendung – LVS-Telefon mit SIP
4	5	4	Video
5	8	7	Voice – Cisco IP-Telefonstandard
6	8	7	Interwork-Steuerelement LVS-Telefon mit RTP
7	7	6	Netzwerk-Steuerelement

Durch das Ändern der Zuordnung von CoS/802.1p zu einer Warteschlange (Seite „CoS/802.1p zu Warteschlange“) sowie der Warteschlangenplanungsmethode und der Bandbreitenzuweisung (Seite „Warteschlange“) kann in einem Netzwerk die gewünschte Quality of Service erreicht werden.

Die Zuordnung von CoS/802.1p zu einer Warteschlange ist nur anwendbar, wenn eine der folgenden Bedingungen erfüllt ist:

- Das Gerät wird im QoS-Basismodus und CoS/802.1p-Vertrauensmodus betrieben.
- Das Gerät wird im erweiterten QoS-Modus betrieben und die Pakete gehören zu Datenflüssen, denen nach CoS/802.1p vertraut wird.

Warteschlange 1 hat die niedrigste, Warteschlange 4 oder 8 die höchste Priorität.

So ordnen Sie CoS-Werte Ausgangswarteschlangen zu:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Allgemein** > **CoS/802.1p zu Warteschlange**.

SCHRITT 2 Geben Sie die Parameter ein.

- **802.1p**: Zeigt die Werte der 802.1p-Prioritäts-Tags an, die einer Ausgangswarteschlange zugewiesen werden sollen, wobei „0“ für die niedrigste und „7“ für die höchste Priorität steht.
- **Ausgabewarteschlange**: Wählen Sie die Ausgangswarteschlange aus, der die 802.1p-Priorität zugeordnet wird. Es werden entweder vier oder acht Ausgangswarteschlangen unterstützt, wobei Warteschlange 4 oder 8 die höchste und Warteschlange 1 die niedrigste Priorität hat.

SCHRITT 3 Wählen Sie für jede 802.1p-Priorität die Ausgabewarteschlange aus, der die Priorität zugeordnet werden soll.

SCHRITT 4 Klicken Sie auf **Übernehmen, Abbrechen** oder auf **Standard wiederherstellen**. Die 802.1p-Prioritätswerte werden den Warteschlangen zugeordnet und die aktuelle Konfigurationsdatei wird aktualisiert, die eingegebenen Änderungen werden abgebrochen bzw. die vorher definierten Werte wiederhergestellt.

Zuordnen von DSCP zu Warteschlange

Auf der Seite „DSCP zu Warteschlange“ (IP Differentiated Services Code Point) können Sie DSCP-Werte Ausgangswarteschlangen zuordnen. In der Tabelle DSCP zu Warteschlange werden die Ausgangswarteschlangen der eingehenden IP-Pakete basierend auf ihrem jeweiligen DSCP-Wert bestimmt. Das ursprüngliche VPT (VLAN-Prioritäts-Tag) des Pakets bleibt unverändert.

Durch das Ändern der Zuordnung unter „DSCP zu Warteschlange“ sowie der Warteschlangenplanungsmethode und der Bandbreitenzuweisung kann in einem Netzwerk die gewünschte Servicequalität erreicht werden.

Die Zuordnung von DSCP zu Warteschlangen kann nur auf IP-Pakete angewendet werden, wenn folgende Bedingungen erfüllt sind:

- Das Gerät wird im QoS-Basismodus und DSCP-Vertrauensmodus betrieben.
- Das Gerät wird im erweiterten QoS-Modus betrieben und die Pakete gehören zu Datenflüssen, denen nach DSCP vertraut wird.

Nicht-IP-Pakete werden immer für die Warteschlange mit der besten Leistung klassifiziert.

In den folgenden Tabellen wird die Standardzuordnung von DSCP zu Warteschlangen für Systeme mit vier und acht Warteschlangen beschrieben:

DSCP	63	55	47	39	31	23	15	7
Warteschlange	3	3	4	3	3	2	1	1
DSCP	62	54	46	38	30	22	14	6
Warteschlange	3	3	4	3	3	2	1	1
DSCP	61	53	45	37	29	21	13	5
Warteschlange	3	3	4	3	3	2	1	1
DSCP	60	52	44	36	28	20	12	4
Warteschlange	3	3	4	3	3	2	1	1
DSCP	59	51	43	35	27	19	11	3
Warteschlange	3	3	4	3	3	2	1	1
DSCP	58	50	42	34	26	18	10	2
Warteschlange	3	3	4	3	3	2	1	1
DSCP	57	49	41	33	25	17	9	1
Warteschlange	3	3	4	3	3	2	1	1
DSCP	56	48	40	32	24	16	8	0
Warteschlange	3	3	4	3	3	2	1	1

In den folgenden Tabellen wird die Standardzuordnung von DSCP zu Warteschlangen für ein System mit acht Warteschlangen beschrieben, bei dem 7 die höchste Stufe ist und 8 zur Stack-Kontrolle verwendet wird.

DSCP	63	55	47	39	31	23	15	7
Warteschlange	6	6	7	5	4	3	2	1
DSCP	62	54	46	38	30	22	14	6
Warteschlange	6	6	7	5	4	3	2	1
DSCP	61	53	45	37	29	21	13	5
Warteschlange	6	6	7	5	4	3	2	1
DSCP	60	52	44	36	28	20	12	4
Warteschlange	6	6	7	5	4	3	2	1

DSCP	59	51	43	35	27	19	11	3
Warteschlange	6	6	7	5	4	3	2	1
DSCP	58	50	42	34	26	18	10	2
Warteschlange	6	6	7	5	4	3	2	1
DSCP	57	49	41	33	25	17	9	1
Warteschlange	6	6	7	5	4	3	2	1
DSCP	56	48	40	32	24	16	8	0
Warteschlange	6	6	6	7	6	6	1	1

In den folgenden Tabellen wird die Standardzuordnung von DSCP zu Warteschlangen für Systeme mit acht Warteschlangen beschrieben, bei dem 8 die höchste Stufe ist:

DSCP	63	55	47	39	31	23	15	7
Warteschlange	7	7	8	6	5	4	3	1
DSCP	62	54	46	38	30	22	14	6
Warteschlange	7	7	8	6	5	4	3	1
DSCP	61	53	45	37	29	21	13	5
Warteschlange	7	7	8	6	5	4	3	1
DSCP	60	52	44	36	28	20	12	4
Warteschlange	7	7	8	6	5	4	3	1
DSCP	59	51	43	35	27	19	11	3
Warteschlange	7	7	8	6	5	4	3	1
DSCP	58	50	42	34	26	18	10	2
Warteschlange	7	7	8	6	5	4	3	1
DSCP	57	49	41	33	25	17	9	1
Warteschlange	7	7	8	6	5	4	3	1
DSCP	56	48	40	32	24	16	8	0
Warteschlange	7	7	7	8	7	7	1	2

So ordnen Sie DSCP Warteschlangen zu:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Allgemein** > **DSCP zu Warteschlange**.

Die Seite „DSCP zu Warteschlange“ enthält die Option **Eingangs-DSCP**. Der DSCP-Wert im eingehenden Paket und die zugehörige Klasse werden angezeigt.

SCHRITT 2 Wählen Sie die **Ausgabewarteschlange** (Warteschlange zur Weiterleitung des Datenverkehrs) aus, der der DSCP-Wert zugeordnet wird.

SCHRITT 3 Wählen Sie **Standards wiederherstellen**, um die standardmäßige CoS-Werkseinstellung für diese Schnittstelle wiederherzustellen.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Konfigurieren der Bandbreite

Auf der Seite „Bandbreite“ können Benutzer zwei Werte (Eingangsratenbegrenzung und Ausgangskontrollrate) definieren, durch die bestimmt wird, wie viel Datenverkehr das System senden und empfangen kann.

Die Eingangsratenbegrenzung gibt an, wie viele Bit pro Sekunde von der Eingangsschnittstelle empfangen werden können. Exzessive Bandbreite oberhalb dieser Begrenzung wird verworfen.

Die folgenden Werte werden für die Ausgangskontrolle eingegeben:

- Die **CIR (Committed Information Rate)** bestimmt die maximale durchschnittliche Datenmenge (gemessen in Bit/s), die über die Ausgangsschnittstelle gesendet werden darf.
- Die **CBS (Committed Burst Size)** bestimmt die maximalen Datenspitzen der gesendeten Daten. Dieser Wert darf über dem CIR-Wert liegen und wird als Anzahl von Datenbytes angegeben.

So geben Sie die Bandbreitenbegrenzung ein:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Allgemein** > **Bandbreite**.

Auf der Seite „Bandbreite“ werden Bandbreiteninformationen für die einzelnen Schnittstellen angezeigt.

Der Prozentwert in Spalte % berechnet sich aus der Eingangsratenbegrenzung geteilt durch die gesamte Port-Bandbreite.

SCHRITT 2 Wählen Sie eine Schnittstelle aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Wählen Sie die **Port- oder LAG-**Schnittstelle aus. Switches der 500-Serie verfügen außerdem über eine Option zum Auswählen der Einheit bzw. des Ports.

SCHRITT 4 Geben Sie Werte in die Felder für die ausgewählte Schnittstelle ein:

- **Eingangsratenbegrenzung**: Wählen Sie diese Option aus, um die Eingangsratenbegrenzung zu aktivieren; der zugehörige Wert wird im folgenden Feld festgelegt.
- **Eingangsratenbegrenzung**: Geben Sie die zulässige Höchstbandbreite für die Schnittstelle ein.

  HINWEIS Die beiden Felder **Eingangsratenbegrenzung** werden nicht angezeigt, wenn der Schnittstellentyp LAG entspricht.
- **Eingangs-CBS (Committed Burst Size)**: Geben Sie die maximal zulässigen Datenspitzen für die Eingangsschnittstelle ein (in Byte). Diese Datenmenge darf selbst dann gesendet werden, wenn dadurch kurzfristig die erlaubte Höchstbandbreite überschritten wird. Dieses Feld ist nur verfügbar, wenn es sich bei der Schnittstelle um einen Port handelt.
- **Ausgangskontrollrate**: Wählen Sie diese Option aus, um die Ausgangskontrollrate für die Schnittstelle zu aktivieren.

  HINWEIS Im Feld „Ausgangskontrollrate“ können Sie für die folgenden Switches eine Mindest-CIR von 2 Mbit/s anstelle von 64 kbit/s konfigurieren: SF500 Ports GE1 – GE4 und SG500 Ports GE49 – GE52.
- **Committed Information Rate (CIR)**: Geben Sie die zulässige Höchstbandbreite für die Ausgangsschnittstelle ein.
- **Ausgangs-CBS (Committed Burst Size)**: Geben Sie die maximal zulässigen Datenspitzen für die Ausgangsschnittstelle ein (in Byte). Diese Datenmenge darf selbst dann gesendet werden, wenn dadurch kurzfristig die erlaubte Höchstbandbreite überschritten wird.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die Bandbreiteneinstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Konfigurieren der Ausgangskontrolle pro Warteschlange

Zusätzlich zur Begrenzung der Übertragungsrate pro Port, die auf der Seite „Bandbreite“ vorgenommen werden kann, kann durch das Gerät auch die Übertragungsrate ausgewählter ausgehender Frames pro Warteschlange an einem Port begrenzt werden. Die Ausgangsratenbegrenzung wird durch die Kontrolle der Ausgabelast erreicht.

Durch das Gerät werden alle Frames außer Verwaltungsframes begrenzt. Alle Frames, die nicht begrenzt werden, werden bei der Berechnung der Rate ignoriert, das heißt ihr Volumen wird nicht in den zu begrenzenden Gesamtwert einberechnet.

Die Ausgangsratenkontrolle auf Warteschlangenebene kann deaktiviert werden.

So legen Sie die Ausgangskontrolle auf Warteschlangenebene fest:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Allgemein** > **Ausgangskontrolle pro Warteschlange**.

Auf der Seite „Ausgangskontrolle pro Warteschlange“ werden die Ratenbegrenzung und die maximalen Datenspitzen für die einzelnen Warteschlangen angezeigt.

SCHRITT 2 Wählen Sie einen Schnittstellentyp aus (Port oder LAG), und klicken Sie auf **Los**.

SCHRITT 3 Wählen Sie einen Port oder eine LAG aus und klicken Sie auf **Bearbeiten**.

Diese Seite ermöglicht die Ausgangskontrolle für bis zu acht Warteschlangen an jeder Schnittstelle.

SCHRITT 4 Wählen Sie die **Schnittstelle** aus.

SCHRITT 5 Geben Sie für jede erforderliche Warteschlange Werte in die folgenden Felder ein:

- **Aktivieren**: Wählen Sie diese Option aus, um die Ausgangskontrolle für diese Warteschlange zu aktivieren.
- **Committed Information Rate (CIR)**: Geben Sie die Höchstrate (CIR) in KBit/s ein. Die CIR gibt an, wie hoch die durchschnittlich gesendete Datenmenge höchstens sein darf.
- **Committed Burst Size (CBS)**: Geben Sie die maximal zulässigen Datenspitzen ein (in Bytes). Die CBS gibt die maximal zulässigen Datenspitzen an, die beim Senden erreicht werden dürfen; der Wert darf die CIR übersteigen.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die Bandbreiteneinstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

VLAN-Eingangsratenbegrenzung

HINWEIS Die Funktion zur VLAN-Ratenbegrenzung ist nicht verfügbar, wenn das Gerät im Schicht-3-Systemmodus betrieben wird.

Die Ratenbegrenzung auf VLAN-Ebene können Sie auf der Seite „VLAN-Eingangsratenbegrenzung“ festlegen. Sie ermöglicht die Begrenzung des Datenverkehrs in VLANs. Wenn eine VLAN-Eingangsratenbegrenzung konfiguriert wurde, wird dadurch der aggregierte Datenverkehr aller Ports am Gerät begrenzt.

Für die Ratenbegrenzung pro VLAN gelten die folgenden Einschränkungen:

- Die Begrenzung hat eine niedrigere Priorität als andere im System definierte Verkehrsüberwachungen. Wenn für ein Paket beispielsweise eine QoS-Ratenbegrenzung, aber auch eine VLAN-Ratenbegrenzung festgelegt wurde und die Ratenbegrenzungen miteinander in Konflikt stehen, hat die QoS-Ratenbegrenzung Vorrang.
- Sie wird auf Geräteebene und innerhalb des Geräts auf Paketverarbeitungsebene angewendet. Wenn das Gerät mehrere Paketprozessoren enthält, wird der konfigurierte VLAN-Ratenbegrenzungswert unabhängig voneinander auf jeden einzelnen Paketprozessor angewendet. Geräte mit bis zu 24 Ports haben einen einzigen Paketprozessor, während Geräte mit mindestens 48 Ports über zwei Paketprozessoren verfügen.

Die Ratenbegrenzung wird für jeden Paketprozessor einer Einheit und für jede Einheit eines Stacks getrennt berechnet.

So definieren Sie die VLAN-Eingangsratenbegrenzung:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Allgemein** > **VLAN-Eingangsratenbegrenzung**.

Auf dieser Seite wird die Tabelle für VLAN-Eingangsratenbegrenzung angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie die Parameter ein.

- **VLAN-ID**: Wählen Sie ein VLAN aus.
- **Committed Information Rate (CIR)**: Geben Sie ein, welche durchschnittliche Datenmenge höchstens im VLAN akzeptiert werden kann (in Kilobytes pro Sekunde).
- **Committed Burst Size (CBS)**: Geben Sie die maximal zulässigen Datenspitzen für die Ausgangsschnittstelle ein (in Bytes). Diese Datenmenge darf selbst dann gesendet werden, wenn dadurch kurzfristig die erlaubte Höchstbandbreite überschritten wird. Dieser Wert kann nicht für LAGs eingegeben werden.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die VLAN-Ratenbegrenzung wird hinzugefügt und die aktuelle Konfigurationsdatei wird aktualisiert.

TCP-Stauvermeidung

Auf der Seite „TCP-Überlastungsvermeidung“ können Sie einen TCP-Algorithmus zur Überlastungsvermeidung aktivieren. Wenn verschiedene Quellen Pakete mit derselben Byteanzahl senden und dadurch eine Datenüberlastung entsteht, sorgt der Algorithmus bei den Knoten mit Datenüberlastung dafür, dass die globale TCP-Synchronisierung vermieden oder aufgelöst wird.

So konfigurieren Sie die TCP-Überlastungsvermeidung:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Allgemein** > **TCP-Überlastungsvermeidung**.

SCHRITT 2 Klicken Sie auf **Aktivieren**, um die TCP-Überlastungsvermeidung zu aktivieren, und klicken Sie dann auf **Übernehmen**.

QoS-Basismodus

Im QoS-Basismodus kann eine bestimmte Domäne im Netzwerk als vertrauenswürdig konfiguriert werden. Innerhalb dieser Domäne werden die Pakete zur Signalisierung des erforderlichen Servicetyps mit 802.1p-Priorität und/oder DSCP gekennzeichnet. Mithilfe dieser Felder werden die Pakete durch die Knoten in dieser Domäne einer bestimmten Ausgabewarteschlange zugewiesen. Die ursprüngliche Paket-Klassifizierung und Kennzeichnung dieser Felder wird am Eingang der vertrauenswürdigen Domäne durchgeführt.

Workflow für das Konfigurieren des QoS-Basismodus

Führen Sie zum Konfigurieren des QoS-Basismodus folgende Aktionen durch:

1. Wählen Sie auf der Seite „QoS-Eigenschaften“ den Basismodus für das System aus.
2. Wählen Sie auf der Seite „Globale Einstellungen“ das Vertrauensverhalten aus. Das Gerät unterstützt den CoS/802.1p-Vertrauensmodus und den DSCP-Vertrauensmodus. Der CoS/802.1p-Vertrauensmodus verwendet die 802.1p-Priorität im VLAN-Tag. Der DSCP-Vertrauensmodus verwendet den DSCP-Wert im IP-Header.

Falls ein Port ausnahmsweise nicht der eingehenden CoS-Kennzeichnung vertrauen soll, deaktivieren Sie auf der Seite „Schnittstelleneinstellungen“ den QoS-Status für diesen Port.

Aktivieren oder deaktivieren Sie auf der Seite „Schnittstelleneinstellungen“ den global ausgewählten Vertrauensmodus der Ports. Wenn ein Port ohne Vertrauensmodus deaktiviert ist, werden alle Eingangspakete des Ports nach dem Prinzip der besten Leistung weitergeleitet. Es wird empfohlen, dass Sie bei den Ports, bei denen die CoS/802.1p-Werte und/oder die DSCP-Werte in den eingehenden Paketen nicht vertrauenswürdig sind, den Vertrauensmodus deaktivieren. Andernfalls kann die Netzwerkleistung möglicherweise negativ beeinflusst werden.

Konfigurieren der globalen Einstellungen

Die Seite „Globale Einstellungen“ enthält Informationen zum Aktivieren der Vertrauensfunktion für das Gerät (siehe Feld „Vertrauensmodus“ unten). Diese Konfiguration ist aktiv, wenn für die QoS der Basismodus festgelegt wurde. In eine QoS-Domäne eingehende Pakete werden an der Grenze der QoS-Domäne klassifiziert.

So legen Sie die Vertrauenskonfiguration fest:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **QoS-Basismodus** > **Globale Einstellungen**.

SCHRITT 2 Wählen Sie den **Vertrauensmodus** aus, während sich das Gerät im Basismodus befindet. Wenn die CoS-Ebene und das DSCP-Tag verschiedenen Warteschlangen zugeordnet werden, richtet sich die Warteschlangenzuweisung des Pakets nach dem Vertrauensmodus:

- **CoS/802.1p**: Die Zuordnung des Datenverkehrs zu Warteschlangen erfolgt auf der Grundlage des VPT-Felds im VLAN-Tag oder des portspezifischen CoS/802.1p-Standardwerts (falls das eingehende Paket kein VLAN-Tag aufweist). Die tatsächliche Zuordnung der VPTs zu Warteschlangen können Sie auf der Seite „CoS/802.1p zu Warteschlange“ konfigurieren.
- **DSCP**: Der gesamte IP-Datenverkehr wird basierend auf dem DSCP-Feld im IP-Header Warteschlangen zugeordnet. Die tatsächliche Zuordnung des DSCP zu Warteschlangen können Sie auf der *Seite DSCP zu Warteschlange* konfigurieren. Falls es sich bei dem Datenverkehr nicht um IP-Datenverkehr handelt, wird dieser der Warteschlange für die beste Leistung zugeordnet.
- **CoS/802.1p-DSCP**: Je nachdem, welche Option festgelegt ist, CoS/802.1p oder DSCP.

SCHRITT 3 Wählen Sie **Eingangs-DSCP überschreiben**, um die ursprünglichen DSCP-Werte in den eingehenden Paketen mit den neuen Werten entsprechend der DSCP-Überschreibungstabelle zu überschreiben. Wenn die Option „Eingangs-DSCP außer Kraft setzen“ aktiviert ist, verwendet das Gerät die neuen DSCP-Werte für die Ausgangswarteschlangen. Außerdem ersetzt der Switch die ursprünglichen DSCP-Werte in den Paketen durch die neuen DSCP-Werte.

HINWEIS Der Frame wird basierend auf dem neuen, umgeschriebenen Wert und nicht nach dem ursprünglichen DSCP-Wert einer Ausgangswarteschlange zugeordnet.

SCHRITT 4 Falls **Eingangs-DSCP überschreiben** aktiviert war, klicken Sie auf **DSCP-Überschreibungstabelle**, um DSCP neu zu konfigurieren.

DSCP eingehend: Zeigt den DSCP-Wert des eingehenden Pakets an, der in einen alternativen Wert geändert werden soll (Remarking).

SCHRITT 5 Wählen Sie unter **DSCP ausgehend** den Wert aus, der dem Ausgangswert zugeordnet werden soll.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird mit den neuen DSCP-Werten aktualisiert.

QoS-Schnittstelleneinstellungen

Auf der Seite „Schnittstelleneinstellungen“ können Sie QoS für die einzelnen Ports des Geräts wie folgt konfigurieren:

QoS-Status an Schnittstelle deaktiviert: Der gesamte am Port eingehende Datenverkehr wird der Warteschlange für die beste Leistung zugeordnet, und es findet keine Klassifizierung/Priorisierung statt.

QoS-Status des Ports ist aktiviert: Die Priorisierung des am Port eingehenden Datenverkehrs basiert auf dem systemweit konfigurierten Vertrauensmodus; hierbei kann es sich entweder um den CoS/802.1p-Vertrauensmodus oder den DSCP-Vertrauensmodus handeln.

So geben Sie die QoS-Einstellungen auf Schnittstellenebene ein:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **QoS-Basismodus** > **Schnittstelleneinstellungen**.

SCHRITT 2 Wählen Sie **Port** oder **LAG** aus, um die Liste der Ports bzw. LAGs anzuzeigen.

Unter **QoS-Status** wird angezeigt, ob QoS für die Schnittstelle aktiviert ist.

SCHRITT 3 Wählen Sie eine Schnittstelle aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 4 Wählen Sie die **Port**- oder **LAG**-Schnittstelle aus.

SCHRITT 5 Aktivieren oder deaktivieren Sie den **QoS-Status** für diese Schnittstelle durch Anklicken.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Erweiterter QoS-Modus

Frames, die mit einer ACL übereinstimmen und denen der Eingang erlaubt wurde, werden implizit mit dem Namen der ACL markiert, die diese Erlaubnis erteilt hat. Auf diese Datenflüsse können dann Aktionen des erweiterten QoS-Modus angewendet werden.

Im erweiterten QoS-Modus werden vom Gerät Richtlinien zur Unterstützung von QoS auf Datenflussebene eingesetzt. Eine Richtlinie und ihre Komponenten weisen die folgenden Merkmale und Beziehungen auf:

- Eine Richtlinie enthält eine oder mehrere Klassenzuordnungen.
- In einer Klassenzuordnung wird ein Datenfluss mit einer oder mehreren gehörigen ACLs festgelegt. Pakete, die nur mit den ACL-Regeln (ACE) in einer Klassenzuordnung mit der Aktion „Zulassen“ (Weiterleiten) übereinstimmen, werden als Bestandteile dieses Datenflusses betrachtet und erhalten dieselbe Servicequalität. Eine Richtlinie beinhaltet also einen oder mehrere Datenflüsse, von denen jeder eine benutzerdefinierte QoS aufweist.

- Die QoS einer Klassenzuordnung (genauer gesagt eines Klassenzuordnungsflusses) wird durch die zugehörige Überwachungsvorrichtung durchgesetzt. Es gibt zwei Typen von Überwachungsvorrichtungen, die Einzelüberwachungsvorrichtung und die Gesamtüberwachungsvorrichtung. Jede Überwachungsvorrichtung wird mit einer QoS-Spezifikation konfiguriert. Bei einer Einzelüberwachungsvorrichtung wird basierend auf deren QoS-Spezifikation die QoS auf eine einzelne Klassenzuordnung und somit auf einen einzelnen Datenfluss angewendet. Bei einer Gesamtüberwachungsvorrichtung wird die QoS auf eine oder mehrere Klassenzuordnungen angewendet und somit auf einen oder mehrere Datenflüsse. Eine Gesamtüberwachungsvorrichtung kann Klassenzuordnungen von verschiedenen Richtlinien unterstützen.
- Die datenflussspezifische QoS wird auf Datenflüsse angewendet, indem die Richtlinien an die gewünschten Ports gebunden werden. Eine Richtlinie und ihre zugehörigen Klassenzuordnungen können an einen oder mehrere Ports gebunden werden, aber jeder einzelne Port kann nur mit einer einzigen Richtlinie verbunden sein.

Hinweise:

- Die Einzelüberwachungsvorrichtung und die Gesamtüberwachungsvorrichtung sind verfügbar, wenn das Gerät im Schicht-2-Modus betrieben wird.
- Eine ACL kann für eine oder mehrere Klassenzuordnungen konfiguriert werden, unabhängig von den Richtlinien.
- Eine Klassenzuordnung kann nur zu einer Richtlinie gehören.
- Wenn eine Klassenzuordnung mit Einzelüberwachungsvorrichtung an mehrere Ports gebunden wird, besitzt jeder Port seine eigene Instanz der Einzelüberwachungsvorrichtung; jede dieser Vorrichtungen wendet die QoS auf die Klassenzuordnung (den Klassenzuordnungsdatenfluss) bei dem jeweiligen Port an, unabhängig von den anderen Ports.
- Eine Gesamtüberwachungsvorrichtung wendet die QoS unabhängig von Richtlinien und Ports aggregiert auf alle zugehörigen Datenflüsse an.

Die erweiterten QoS-Einstellungen bestehen aus drei Teilen:

- Definitionen der Regeln, mit denen die Frames übereinstimmen müssen; alle Frames, die mit einer einzelnen Gruppe von Regeln übereinstimmen, werden als *Datenfluss* betrachtet.
- Definition der Aktionen, die auf die regelkonformen Frames in den einzelnen Datenflüssen angewendet werden sollen.
- Verbindung der Kombinationen von Regeln und Aktionen mit einer oder mehreren Schnittstellen.

Workflow für das Konfigurieren des erweiterten QoS-Modus

Führen Sie zum Konfigurieren des erweiterten QoS-Modus folgende Aktionen durch:

1. Wählen Sie auf der Seite „QoS-Eigenschaften“ den erweiterten Modus für das System aus. Wählen Sie auf der Seite „Globale Einstellungen“ den Vertrauensmodus aus. Wenn die CoS-Ebene und das DSCP-Tag verschiedenen Warteschlangen zugeordnet werden, richtet sich die Warteschlangenzuweisung des Pakets nach dem Vertrauensmodus:
   - Falls sich die internen DSCP-Werte von denen der eingehenden Pakete unterscheiden, ordnen Sie auf der Seite „Profilexterne DSCP-Zuordnung“ die externen Werte den internen Werten zu. Daraufhin wird die Seite „DSCP-Remarking“ geöffnet.
2. Erstellen Sie ACLs, wie im Workflow zum Erstellen von ACLs beschrieben.
3. Falls Sie ACLs definiert haben, erstellen Sie Klassenzuordnungen und ordnen Sie diesen auf der Seite „Klassenzuordnung“ die ACLs zu.
4. Erstellen Sie auf der Seite „Richtlinientabelle“ eine Richtlinie und weisen Sie der Richtlinie auf der Seite „Richtlinien-Klassenzuordnungen“ eine oder mehrere Klassenzuordnungen zu. Sie können bei Bedarf auch die QoS angeben. Weisen Sie dazu beim Zuordnen der Richtlinie zur Klassenzuordnung dieser Klassenzuordnung eine Überwachungsvorrichtung zu.
   - **Einzelüberwachungsvorrichtung**: Erstellen Sie eine Richtlinie, durch die einer Klassenzuordnung eine Einzelüberwachungsvorrichtung zugewiesen wird. Verwenden Sie dazu die Seiten „Richtlinientabelle“ und „Klassenzuordnung“. Definieren Sie innerhalb der Richtlinie die Einzelüberwachungsvorrichtung.
   - **Gesamtüberwachungsvorrichtung**: Erstellen Sie auf der Seite „Gesamtüberwachungsvorrichtung“ für jeden Datenfluss eine QoS-Aktion, durch die alle übereinstimmenden Frames an dieselbe Überwachungsvorrichtung (Gesamtüberwachungsvorrichtung) gesendet werden. Erstellen Sie auf der Seite „Richtlinientabelle“ eine Richtlinie, durch die einer Klassenzuordnung die Gesamtüberwachungsvorrichtung zugewiesen wird.
5. Verbinden Sie auf der Seite „Richtlinienbindung“ die Richtlinie mit einer Schnittstelle.

Konfigurieren der globalen Einstellungen

Die Seite „Globale Einstellungen“ enthält Informationen zum Aktivieren der Vertrauensfunktion für das Gerät. In eine QoS-Domäne eingehende Pakete werden an der Grenze der QoS-Domäne klassifiziert.

So legen Sie die Vertrauenskonfiguration fest:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Erweiterter QoS-Modus** > **Globale Einstellungen**.

SCHRITT 2 Wählen Sie den **Vertrauensmodus** aus, während sich das Gerät im erweiterten Modus befindet. Wenn die CoS-Ebene und das DSCP-Tag verschiedenen Warteschlangen zugeordnet werden, richtet sich die Warteschlangenzuweisung des Pakets nach dem Vertrauensmodus:

- **CoS/802.1p**: Die Zuordnung des Datenverkehrs zu Warteschlangen erfolgt auf der Grundlage des VPT-Felds im VLAN-Tag oder des portspezifischen CoS/802.1p-Standardwerts (falls das eingehende Paket kein VLAN-Tag aufweist). Die tatsächliche Zuordnung der VPTs zu Warteschlangen können Sie auf der Seite „CoS/802.1p zu Warteschlange“ konfigurieren.
- **DSCP**: Der gesamte IP-Datenverkehr wird basierend auf dem DSCP-Feld im IP-Header Warteschlangen zugeordnet. Die tatsächliche Zuordnung des DSCP zu Warteschlangen können Sie auf der *Seite DSCP zu Warteschlange* konfigurieren. Falls es sich bei dem Datenverkehr nicht um IP-Datenverkehr handelt, wird dieser der Warteschlange für die beste Leistung zugeordnet.
- **CoS/802.1p-DSCP**: Wählen Sie diese Option aus, um für Nicht-IP-Verkehr den CoS-Vertrauensmodus und für IP-Verkehr den DSCP-Vertrauensmodus zu verwenden.

SCHRITT 3 Wählen Sie im Feld **Standardmodus-Status** den standardmäßigen Vertrauensmodus für den erweiterten QoS-Modus aus („Vertrauenswürdig“ oder „Nicht vertrauenswürdig“). Damit wird die QoS-Basisfunktionalität für erweitertes QoS bereitgestellt, sodass Sie CoS/DSCP für erweitertes QoS standardmäßig vertrauen können (ohne eine Richtlinie erstellen zu müssen).

Wenn in **Erweiterter QoS-Modus** der Standardmodus-Status auf „Nicht vertrauenswürdig“ festgelegt ist, werden die für die Schnittstelle konfigurierten CoS-Standardwerte ignoriert und der gesamte Verkehr an die Warteschlange 1 geleitet. Details hierzu finden Sie auf der Seite „Quality of Service > Erweiterter QoS-Modus > Globale Einstellungen“.

Wenn Sie für eine Schnittstelle eine Richtlinie haben, ist der Standardmodus irrelevant, die Aktion entspricht der Richtlinienkonfiguration und nicht übereinstimmender Verkehr wird verworfen.

SCHRITT 4 Wählen Sie **Eingangs-DSCP überschreiben**, um die ursprünglichen DSCP-Werte in den eingehenden Paketen mit den neuen Werten entsprechend der DSCP-Überschreibungstabelle zu überschreiben. Wenn die Option „Eingangs-DSCP außer Kraft setzen“ aktiviert ist, verwendet das Gerät die neuen DSCP-Werte für die Ausgangswarteschlangen. Außerdem ersetzt der Switch die ursprünglichen DSCP-Werte in den Paketen durch die neuen DSCP-Werte.

HINWEIS Der Frame wird basierend auf dem neuen, umgeschriebenen Wert und nicht nach dem ursprünglichen DSCP-Wert einer Ausgangswarteschlange zugeordnet.

SCHRITT 5 Falls **Eingangs-DSCP überschreiben** aktiviert war, klicken Sie auf **DSCP-Überschreibungstabelle**, um DSCP neu zu konfigurieren. Details hierzu finden Sie auf der Seite „Tabelle für DSCP-Überschreibung“.

Konfigurieren der profilexternen DSCP-Zuordnung

Beim Zuweisen einer Überwachungsvorrichtung zu einer Klassenzuordnung (bzw. zu einem Klassenzuordnungsdatenfluss) können Sie angeben, welche Aktion ausgeführt werden soll, wenn die Menge des Datenverkehrs in den Datenflüssen die für die QoS-angegebenen Grenzwerte erreicht hat. Der Teil des Datenverkehrs, der den QoS-Grenzwert des Datenflusses überschreitet, wird als *profilexterne Pakete* bezeichnet.

Wenn die Aktion bei Überschreitung „Profilexternes DSCP“ ist, ersetzt das Gerät den ursprünglichen DSCP-Wert der profilexternen IP-Pakete basierend auf der Tabelle „Profilexterne DSCP-Zuordnung“ durch einen neuen Wert. Anhand der neuen Werte weist das Gerät diesen Paketen Ressourcen und die Ausgangswarteschlange zu. Außerdem ersetzt das Gerät den ursprünglichen DSCP-Wert der profilexternen Pakete physisch durch den neuen DSCP-Wert.

Damit Sie die Überschreitungsaktion „Profilexternes DSCP“ verwenden können, müssen Sie den DSCP-Wert in der Tabelle „Profilexterne DSCP-Zuordnung“ neu zuordnen. Andernfalls wird keine Aktion durchgeführt, weil bei der werkseitigen Standardeinstellung den Paketen in der Tabelle derselbe DSCP-Wert zugeordnet wird, den sie bereits aufweisen.

Durch diese Funktion werden die DSCP-Tags für eingehenden Datenverkehr geändert, der durch Switches zwischen vertrauenswürdigen QoS-Domänen weitergeleitet wird. Durch das Ändern der in einer Domäne verwendeten DSCP-Werte wird für die Priorität dieses Datenverkehrstyps der DSCP-Wert eingestellt, der in der anderen Domäne zur Identifikation von Datenverkehr desselben Typs verwendet wird.

Diese Einstellungen werden aktiv, wenn das System im QoS-Basismodus betrieben wird; sobald sie aktiviert wurden, sind sie global aktiv.

Beispiel: Gehen wir einmal von den drei Serviceebenen Silber, Gold und Platin aus, und die DSCP-Eingangswerte zum Kennzeichnen dieser Ebenen sind 10, 20 und 30. Wenn dieser Datenverkehr an einen anderen Dienstanbieter weitergeleitet wird, der dieselben Serviceebenen besitzt, aber die DSCP-Werte 16, 24 und 48 verwendet, werden durch die **Profilexterne DSCP-Zuordnung** die Eingangswerte entsprechend ihrer Zuordnung zu den Ausgangswerten geändert.

So ordnen Sie DSCP-Werte zu:

SCHRITT 1 Klicken Sie auf **Quality of Service > Erweiterter QoS-Modus > Profilexterne DSCP-Zuordnung**. Auf diese Seite können Sie den DSCP-Wert für Datenverkehr ändern, der beim Gerät ein- oder ausgeht.

„DSCP eingehend“: Zeigt den DSCP-Wert des eingehenden Pakets an, der in einen alternativen Wert geändert werden soll (Remarking).

SCHRITT 2 Wählen Sie unter **DSCP ausgehend** den Wert aus, der dem Eingangswert zugeordnet werden soll.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird mit der neuen DSCP-Zuordnungstabelle aktualisiert.

SCHRITT 4 Wählen Sie **Standards wiederherstellen** aus, um die standardmäßige CoS-Werkseinstellung für diese Schnittstelle wiederherzustellen.

Definieren von Klassenzuordnungen

Eine Klassenzuordnung definiert einen Datenverkehrsfluss mithilfe von ACLs (Access Control Lists, Zugriffskontrolllisten). Eine Klassenzuordnung kann auf einer Kombination von MAC-ACL, IP-ACL und IPv6-ACL basieren. Klassenzuordnungen können so konfiguriert sein, dass entweder beliebige oder alle Paketkriterien erfüllt werden müssen. Beim Vergleich mit den Paketen wird die Methode der ersten Übereinstimmung angewendet, das heißt diejenige Aktion, die der zuerst übereinstimmenden Klassenzuordnung entspricht, wird vom System ausgeführt. Die Pakete, die mit derselben Klassenzuordnung übereinstimmen, werden als Bestandteil desselben Datenflusses behandelt.

HINWEIS Das Festlegen von Klassenzuordnungen wirkt sich nicht auf die QoS aus; es handelt sich hierbei um einen Zwischenschritt, der die spätere Verwendung der Klassenzuordnungen ermöglicht.

Falls komplexere Gruppen von Regeln erforderlich sind, können Sie mehrere Klassenzuordnungen in einer Supergruppe kombinieren. Diese wird als Richtlinie bezeichnet (siehe **Konfigurieren einer Richtlinie**).

Auf der Seite „Klassenzuordnung“ wird die Liste der definierten Klassenzuordnungen sowie der jeweils zugehörigen ACLs angezeigt. Auf dieser Seite können Sie auch Klassenzuordnungen hinzufügen oder löschen.

So definieren Sie eine Klassenzuordnung:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Erweiterter QoS-Modus** > **Klassenzuordnung**.

Auf dieser Seite werden die bereits festgelegten Klassenzuordnungen angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

Eine neue Klassenzuordnung fügen Sie hinzu, indem Sie eine oder zwei ACLs auswählen und der Klassenzuordnung einen Namen geben. Wenn eine Klassenzuordnung zwei ACLs besitzt, können Sie festlegen, dass ein Frame mit einer beliebigen oder einer bestimmten der beiden ACLs übereinstimmen muss oder mit beiden ACLs.

SCHRITT 3 Geben Sie die Parameter ein.

- **Klassenzuordnungsname**: Geben Sie den Namen der neuen Klassenzuordnung ein.
- **Übereinstimmung mit ACL-Typ**: Die Kriterien, mit denen ein Paket übereinstimmen muss, damit es als Bestandteil des in der Klassenzuordnung definierten Datenflusses betrachtet wird. Folgende Optionen sind möglich:
  - *IP*: Ein Paket muss mit einer der beiden IP-basierten ACLs in der Klassenzuordnung übereinstimmen.
  - *MAC*: Ein Paket muss mit der MAC-basierten ACL in der Klassenzuordnung übereinstimmen.
  - *IP und MAC*: Ein Paket muss mit der IP-basierten ACL und der MAC-basierten ACL in der Klassenzuordnung übereinstimmen.
  - *IP oder MAC*: Ein Paket muss entweder mit der IP-basierten ACL oder mit der MAC-basierten ACL in der Klassenzuordnung übereinstimmen.
- **IP**: Wählen Sie die IPv4-basierte ACL oder die IPv6-basierte ACL für die Klassenzuordnung aus.
- **MAC**: Wählen Sie die MAC-basierte ACL für die Klassenzuordnung aus.
- **Bevorzugte ACL**: Wählen Sie aus, ob die Pakete zuerst mit einer IP-basierten ACL oder mit einer MAC-basierten ACL verglichen werden.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

QoS-Überwachungsvorrichtungen

HINWEIS QoS-Überwachungsvorrichtungen werden auf Sx500-Geräten im Schicht-3-Systemmodus nicht unterstützt. Auf SG500X-Geräten werden sie immer unterstützt.

Sie können die Rate des Datenverkehrs messen, der einer voreingestellten Gruppe von Regeln entspricht, und Begrenzungen hierfür durchsetzen, etwa die Rate des Dateiübertragungsverkehrs für einen bestimmten Port begrenzen.

Dazu wird mithilfe der ACLs in den Klassenzuordnungen der gewünschte übereinstimmende Datenverkehr ermittelt und mithilfe einer Überwachungsvorrichtung die QoS auf diesen übereinstimmenden Datenverkehr angewendet.

Eine Überwachungsvorrichtung wird mit einer QoS-Spezifikation konfiguriert. Es gibt zwei Arten von Überwachungsvorrichtungen:

- **(Reguläre) Einzelüberwachungsvorrichtung**: Eine Einzelüberwachungsvorrichtung wendet die QoS basierend auf der QoS-Spezifikation der Überwachungsvorrichtung auf eine einzige Klassenzuordnung und einen einzigen Datenfluss an. Wenn eine Klassenzuordnung mit Einzelüberwachungsvorrichtung an mehrere Ports gebunden wird, besitzt jeder Port seine eigene Instanz der Einzelüberwachungsvorrichtung; jede dieser Vorrichtungen wendet die QoS auf die Klassenzuordnung (den Klassenzuordnungsdatenfluss) bei dem jeweiligen Port an, unabhängig von den anderen Ports. Eine Einzelüberwachungsvorrichtung können Sie auf der Seite „Richtlinientabelle“ erstellen.
- **Gesamtüberwachungsvorrichtung**: Bei einer Gesamtüberwachungsvorrichtung wird die QoS auf eine oder mehrere Klassenzuordnungen angewendet und somit auf einen oder mehrere Datenflüsse. Eine Gesamtüberwachungsvorrichtung kann Klassenzuordnungen von verschiedenen Richtlinien unterstützen. Eine Gesamtüberwachungsvorrichtung wendet die QoS aggregiert auf alle zugehörigen Datenflüsse an, unabhängig von Richtlinien und Ports. Eine Gesamtüberwachungsvorrichtung können Sie auf der Seite „Gesamtüberwachungsvorrichtung“ erstellen.

  Eine Gesamtüberwachungsvorrichtung wird definiert, wenn die Überwachungsvorrichtung von mehreren Klassen gemeinsam genutzt werden soll. Überwachungsvorrichtungen an einem Port können nicht gemeinsam mit anderen Überwachungsvorrichtungen in einem anderen Gerät genutzt werden.

Jede Überwachungsvorrichtung wird mit ihrer eigenen QoS-Spezifikation definiert. Dabei wird eine Kombination der folgenden Parameter verwendet:

- Eine zulässige Höchstrate mit der Bezeichnung CIR (Committed Information Rate), gemessen in KBit/s.
- Eine Datenmenge mit der Bezeichnung CBS (Committed Burst Size), gemessen in Bytes. Diese gibt an, wie hoch temporäre Datenverkehrsspitzen maximal sein dürfen; der Wert darf die festgelegte Höchstdurchschnittsrate übersteigen.

- Eine Aktion, die auf Frames angewendet wird, die den Grenzwert überschreiten (so genannter profilexterner Datenverkehr); dabei können solche Frames in ihrem aktuellen Zustand weitergeleitet werden, gelöscht werden oder mit einem neuen DSCP-Wert weitergeleitet werden, durch den sie für die gesamte nachfolgende Verarbeitung im Gerät als Frames mit einer niedrigeren Priorität gekennzeichnet sind.

Die Zuweisung einer Überwachungsvorrichtung zu einer Klassenzuordnung erfolgt beim Hinzufügen einer Klassenzuordnung zu einer Richtlinie. Falls es sich bei der Überwachungsvorrichtung um eine Gesamtüberwachungsvorrichtung handelt, müssen Sie diese auf der Seite „Gesamtüberwachungsvorrichtung“ erstellen.

Definieren von Aggregat-Überwachungsvorrichtungen

Bei einer Gesamtüberwachungsvorrichtung wird die QoS auf eine oder mehrere Klassenzuordnungen und somit auf einen oder mehrere Datenflüsse angewendet. Eine Gesamtüberwachungsvorrichtung kann Klassenzuordnungen von verschiedenen Richtlinien unterstützen und wendet die QoS unabhängig von Richtlinien und Ports aggregiert auf alle zugehörigen Datenflüsse an.

HINWEIS Das Gerät unterstützt Gesamtüberwachungsvorrichtungen und Einzelüberwachungsvorrichtungen nur dann, wenn es in Geräten, die einen separaten Schicht-2-Systemmodus unterstützen, im Schicht-2-Modus betrieben wird.

So legen Sie eine Gesamtüberwachungsvorrichtung fest:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Erweiterter QoS-Modus** > **Gesamtüberwachungsvorrichtung**.

Auf dieser Seite werden die vorhandenen Gesamtüberwachungsvorrichtungen angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Name der Gesamtüberwachungsvorrichtung**: Geben Sie den Namen der Gesamtüberwachungsvorrichtung ein.
- **Eingangs-CIR**: Geben Sie die zulässige Höchstrate in Bit/s ein. Eine Beschreibung hierzu finden Sie auf der Seite „Bandbreite“.
- **Eingangs-CBS**: Geben Sie die maximal zulässigen Datenspitzen ein (in Bytes); der Wert darf über dem CIR-Wert liegen. Eine Beschreibung hierzu finden Sie auf der Seite „Bandbreite“.
- **Aktion bei Überschreitung**: Wählen Sie die Aktion aus, die bei eingehenden Paketen ausgeführt werden soll, die die CIR überschreiten. Folgende Werte sind möglich:
  - *Weiterleiten*: Pakete, die den festgelegten CIR-Wert überschreiten, werden weitergeleitet.
  - *Löschen*: Pakete, die den festgelegten CIR-Wert überschreiten, werden gelöscht.

- *Profilexternes DSCP*: Die DSCP-Werte von Paketen, die den festgelegten CIR-Wert überschreiten, werden basierend auf der Tabelle Profilexterne DSCP-Zuordnung in einen neuen Wert geändert.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Konfigurieren einer Richtlinie

Auf der Seite „Richtlinien-Klassenzuordnungen“ wird die Liste der erweiterten QoS-Richtlinien angezeigt, die im System festgelegt sind. Auf der Seite können Sie auch Richtlinien erstellen und löschen. Nur die Richtlinien, die an eine Schnittstelle gebunden sind, sind aktiv (siehe Seite „Richtlinienbindung“).

Jede Richtlinie besteht aus Folgendem:

- Eine oder mehrere auf ACLs beruhende Klassenzuordnungen, durch die die Datenverkehrsflüsse in der Richtlinie festgelegt werden.
- Eine oder mehrere Gesamtüberwachungsvorrichtungen, die die QoS auf die Datenverkehrsflüsse in der Richtlinie anwenden.

Nachdem Sie eine Richtlinie hinzugefügt haben, können Sie auf der Seite „Richtlinientabelle“ Klassenzuordnungen hinzufügen.

So fügen Sie eine QoS-Richtlinie hinzu:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Erweiterter QoS-Modus** > **Richtlinientabelle**.

Auf dieser Seite werden die definierten Richtlinien angezeigt.

SCHRITT 2 Klicken Sie auf **Tab. für Richtlinien-Klassenzuordnungen**, um die Seite „Richtlinien-Klassenzuordnungen“ anzuzeigen.
oder
Klicken Sie auf **Hinzufügen**, um die Seite „Richtlinientabelle hinzufügen“ zu öffnen.

SCHRITT 3 Geben Sie in das Feld **Neuer Richtlinienname** den Namen der neuen Richtlinie ein.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Das QoS-Richtlinienprofil wird hinzugefügt und die aktuelle Konfigurationsdatei wird aktualisiert.

Richtlinien-Klassenzuordnungen

Einer Richtlinie können eine oder mehrere Klassenzuordnungen hinzugefügt werden. In einer Klassenzuordnung werden die Pakettypen festgelegt, die als Bestandteil desselben Datenverkehrsflusses betrachtet werden.

HINWEIS Sie können für eine Klassenzuordnung keine Überwachungsvorrichtung konfigurieren, wenn das Gerät im Schicht-3-Modus betrieben wird. Das Gerät unterstützt Überwachungsvorrichtungen nur im Schicht-2-Modus.

So fügen Sie einer Richtlinie eine Klassenzuordnung hinzu:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Erweiterter QoS-Modus** > **Richtlinien-Klassenzuordnungen**.

SCHRITT 2 Wählen Sie im Filter eine Richtlinie aus und klicken Sie auf **Los**. Alle Klassenzuordnungen in dieser Richtlinie werden angezeigt.

SCHRITT 3 Klicken Sie zum Hinzufügen einer neuen Klassenzuordnung auf **Hinzufügen**.

SCHRITT 4 Geben Sie die Parameter ein.

- **Richtlinienname**: Zeigt die Richtlinie an, der die Klassenzuordnung hinzugefügt wird.
- **Klassenzuordnungsname**: Wählen Sie eine vorhandene Klassenzuordnung aus, die der Richtlinie zugewiesen werden soll. Klassenzuordnungen werden auf der Seite „Klassenzuordnung“ erstellt.
- **Aktionstyp**: Wählen Sie die Aktion für die CoS/802.1p- und/oder DSCP-Eingangswerte aller übereinstimmenden Pakete aus.
  - *Standardmodus für Vertrauen verwenden*: Der CoS/802.1p- und/oder DSCP-Eingangswert wird ignoriert. Die übereinstimmenden Pakete werden nach dem Prinzip der besten Leistung gesendet.
  - *Immer vertrauen*: Wenn diese Option ausgewählt ist, vertraut das Gerät dem CoS/802.1p- und DSCP-Wert des übereinstimmenden Pakets. Im Fall von IP-Paketen leitet das Gerät das Paket basierend auf dessen DSCP-Wert und der Tabelle „DSCP zu Warteschlange“ an die Ausgangswarteschlange weiter. Bei allen anderen Pakettypen richtet sich die Ausgangswarteschlange des Pakets nach dessen CoS/802.1p-Wert und der Tabelle CoS/802.1p zu Warteschlange.
  - *Einst.*: Wenn diese Option ausgewählt ist, bestimmen Sie mithilfe des im Feld **Neuer Wert** eingegebenen Werts die Ausgangswarteschlange der übereinstimmenden Pakete wie folgt:

    Wenn es sich bei dem neuen Wert („0“ bis „7“) um eine CoS/802.1p-Priorität handelt, können Sie mithilfe des Prioritätswerts und der Tabelle CoS/802.1p zu Warteschlange die Ausgangswarteschlange aller übereinstimmenden Pakete bestimmen.

    Wenn es sich bei dem neuen Wert („0“ bis „63“) um eine DSCP handelt, können Sie mithilfe der neuen DSCP und der Tabelle DSCP zu Warteschlange die Ausgangswarteschlange der übereinstimmenden IP-Pakete bestimmen.

Verwenden Sie anderenfalls den neuen Wert („1“ bis „8“) als Ausgangswarteschlangennummer für alle übereinstimmenden Pakete.

- **Richtlinientyp**: Nur im Schicht-2-Systemmodus verfügbar. Wählen Sie den Typ der Überwachungsvorrichtung für die Richtlinie aus. Folgende Optionen sind möglich:
  - *Keine*: Es wird keine Richtlinie verwendet.
  - *Einzeln*: Es wird eine Einzelüberwachungsvorrichtung für die Richtlinie verwendet.
  - *Gesamt*: Es wird eine Gesamtüberwachungsvorrichtung für die Richtlinie verwendet.
- **Gesamtüberwachungsvorrichtung**: Nur im Schicht-2--Systemmodus verfügbar. Wenn der **Richtlinientyp** *Gesamt* lautet, wählen Sie eine zuvor (auf der Seite „Gesamtüberwachungsvorrichtung“) definierte Gesamtüberwachungsvorrichtung aus.

Wenn für den **Richtlinientyp** die Option *Einzeln* verwendet wird, geben Sie die folgenden QoS-Parameter ein:

- **Eingangs-CIR**: Geben Sie die CIR (Committed Information Rate) in KBit/s ein. Eine Beschreibung hierzu finden Sie auf der Seite „Bandbreite“.
- **Eingangs-CBS**: Geben Sie die maximal zulässigen Datenspitzen (CBS, Committed Burst Size) in Bytes ein. Eine Beschreibung hierzu finden Sie auf der Seite „Bandbreite“.
- **Aktion bei Überschreitung**: Wählen Sie die Aktion aus, die eingehenden Paketen zugewiesen werden soll, die die CIR überschreiten. Folgende Werte sind möglich:
  - *Keine*: Keine Aktion.
  - *Löschen*: Pakete, die den festgelegten CIR-Wert überschreiten, werden gelöscht.
  - *Profilexternes DSCP*: IP-Pakete, die den festgelegten CIR-Wert überschreiten, werden mit einem neuen DSCP-Wert weitergeleitet, der aus der Tabelle „Profilexterne DSCP-Zuordnung“ abgeleitet wurde.

SCHRITT 5 Klicken Sie auf **Übernehmen**.

Richtlinienbindung

Auf der Seite „Richtlinienbindung“ wird angezeigt, welches Richtlinienprofil an welchen Port gebunden ist. Wenn ein Richtlinienprofil an einen bestimmten Port gebunden ist, ist es an diesem Port aktiv. An einem Port kann immer nur ein einziges Richtlinienprofil konfiguriert werden, aber eine Richtlinie kann an mehrere Ports gebunden werden.

Wenn eine Richtlinie an einen Port gebunden ist, filtert dieser den eingehenden Datenverkehr, der zu den in der Richtlinie festgelegten Datenflüssen gehört, und wendet QoS auf diesen Datenverkehr an. Die Richtlinie gilt nicht für den ausgehenden Datenverkehr an diesem Port.

Damit Sie eine Richtlinie bearbeiten können, muss diese zunächst von allen Ports, an die sie gebunden ist, entfernt werden (die Bindung muss aufgehoben werden).

HINWEIS Sie können einen Port an eine Richtlinie oder an eine ACL binden, jedoch nicht an beide.

So legen Sie die Richtlinienbindung fest:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Erweiterter QoS-Modus** > **Richtlinienbindung**.

SCHRITT 2 Wählen Sie einen **Richtliniennamen** und bei Bedarf einen **Schnittstellentyp** aus.

SCHRITT 3 Klicken Sie auf **Los**. Die Richtlinie wird ausgewählt.

SCHRITT 4 Wählen Sie die folgenden Optionen für die Richtlinie/Schnittstelle aus:

- **Bindung**: Wählen Sie diese Option aus, um die Richtlinie an die Schnittstelle zu binden.
- **Alle zulassen**: Wählen Sie diese Option aus, um Pakete an der Schnittstelle, die keiner Richtlinie entsprechen, weiterzuleiten.

  HINWEIS „Alle zulassen“ können Sie nur definieren, wenn IP Source Guard für die Schnittstelle nicht aktiviert ist.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die QoS-Richtlinienbindung wird definiert und die aktuelle Konfigurationsdatei wird aktualisiert.

SCHRITT 6 Klicken Sie auf **Richtlinienbindung pro Port anzeigen**, um die Schnittstellentypen (Port von Einheit 1/1 oder LAG) pro Schnittstelle anzuzeigen:

Die folgenden Felder werden für alle Ports/LAGs angezeigt:

- Richtlinienname
- Alle zulassen

Verwalten der QoS-Statistik

Auf diesen Seiten können Sie die Einzelüberwachungsvorrichtung und die Gesamtüberwachungsvorrichtung verwalten und Warteschlangenstatistiken anzeigen.

Statistik für Überwachungsvorrichtung

Eine Einzelüberwachungsvorrichtung wird an eine Klassenzuordnung einer einzigen Richtlinie gebunden. Eine Gesamtüberwachungsvorrichtung wird an eine oder mehrere Klassenzuordnungen einer oder mehrerer Richtlinien gebunden.

Anzeigen der Statistik für Einzelüberwachungsvorrichtungen

Auf der Seite „Statistik für Einzelüberwachungsvorrichtung“ wird die Anzahl der von einer Schnittstelle empfangenen profilinternen und profilexternen Pakete angezeigt, die die Bedingungen erfüllen, die in der Klassenzuordnung einer Richtlinie definiert sind.

HINWEIS Diese Seite wird nicht angezeigt, wenn das Gerät im Schicht-3-Modus betrieben wird.

So zeigen Sie die Statistik für Überwachungsvorrichtungen an:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **QoS-Statistik** > **Statistik für Einzelüberwachungsvorrichtung**.

Auf dieser Seite werden folgende Felder angezeigt:

- **Schnittstelle**: Die Statistik für diese Schnittstelle wird angezeigt.
- **Richtlinie**: Die Statistik für diese Richtlinie wird angezeigt.
- **Klassenzuordnung**: Die Statistik für diese Klassenzuordnung wird angezeigt.
- **Profilinterne Byte**: Anzahl der empfangenen profilinternen Bytes.
- **Profilexterne Byte**: Anzahl der empfangenen profilexternen Bytes.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Schnittstelle**: Wählen Sie die Schnittstelle aus, für die statistische Daten gesammelt werden.
- **Richtlinienname**: Wählen Sie den Richtliniennamen aus.
- **Klassenzuordnungsname**: Wählen Sie den Klassennamen aus.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Eine zusätzliche Anforderung für statistische Daten wird erstellt und die aktuelle Konfigurationsdatei wird aktualisiert.

Anzeigen der Statistik für Aggregat-Überwachungsvorrichtungen

So zeigen Sie die Statistik für Gesamtüberwachungsvorrichtungen an:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **QoS-Statistik** > **Statistik für Gesamtüberwachungsvorrichtung**.

Auf dieser Seite werden folgende Felder angezeigt:

- **Name der Gesamtüberwachungsvorrichtung**: Die Überwachungsvorrichtung, auf der die Statistik basiert.
- **Profilinterne Byte**: Anzahl der empfangenen profilinternen Pakete.
- **Profilexterne Byte**: Anzahl der empfangenen profilexternen Pakete.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Wählen Sie unter **Name der Gesamtüberwachungsvorrichtung** einen Namen aus (eine der zuvor erstellten Gesamtüberwachungsvorrichtungen), für den die Statistik angezeigt wird.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Eine zusätzliche Anforderung für statistische Daten wird erstellt und die aktuelle Konfigurationsdatei wird aktualisiert.

Anzeigen der Warteschlangenstatistik

Auf der Seite „Warteschlangenstatistik“ wird die Warteschlangenstatistik angezeigt, einschließlich der Statistik über weitergeleitete und gelöschte Pakete. Die Daten sind nach Schnittstelle, Warteschlange und Löschpriorität geordnet.

So zeigen Sie die Warteschlangenstatistik an:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **QoS-Statistik** > **Warteschlangenstatistik**.

Auf dieser Seite werden folgende Felder angezeigt:

- **Aktualisierungsrate**: Legen Sie den Zeitraum fest, der bis zum Aktualisieren der Ethernet-Statistik für die Schnittstelle verstreichen soll. Es stehen folgende Optionen zur Verfügung:
  - *Keine Aktualisierung*: Die Statistik wird nicht aktualisiert.
  - *15 Sek*: Die Statistik wird alle 15 Sekunden aktualisiert.
  - *30 Sek*: Die Statistik wird alle 30 Sekunden aktualisiert.
  - *60 Sek*: Die Statistik wird alle 60 Sekunden aktualisiert.

- **Zählersatz**: Folgende Optionen sind möglich:
  - *Satz 1*: Zeigt die Statistik für Satz 1 an, die alle Schnittstellen und Warteschlangen mit hoher Löschpriorität (DP, Drop Precedence) enthält.
  - *Satz 2*: Zeigt die Statistik für Satz 2 an, die alle Schnittstellen und Warteschlangen mit niedriger Löschpriorität enthält.
- **Schnittstelle**: Für diese Schnittstelle wird die Warteschlangenstatistik angezeigt.
- **Warteschlange**: Von dieser Warteschlange wurden die Pakete weitergeleitet oder gelöscht.
- **Löschpriorität**: Die Daten mit der niedrigsten Löschpriorität werden am unwahrscheinlichsten gelöscht.
- **Pakete insgesamt**: Anzahl der weitergeleiteten oder gelöschten Pakete.
- **Gelöschte Pakete**: Prozentualer Anteil der gelöschten Pakete.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Zählersatz**: Wählen Sie den Zählersatz aus:
  - *Satz 1*: Zeigt die Statistik für Satz 1 an, die alle Schnittstellen und Warteschlangen mit hoher Löschpriorität (DP, Drop Precedence) enthält.
  - *Satz 2*: Zeigt die Statistik für Satz 2 an, die alle Schnittstellen und Warteschlangen mit niedriger Löschpriorität enthält.
- **Schnittstelle**: Wählen Sie die Ports aus, für die statistische Daten angezeigt werden. Folgende Optionen sind möglich:
  - *Einheit Nr.*: Wählt die Einheitennummer aus.
  - *Port*: Wählen Sie den Port an der ausgewählten Einheitennummer aus, für den statistische Daten angezeigt werden.
  - *Alle Ports*: Legt fest, dass die Statistik für alle Ports angezeigt werden soll.
- **Warteschlange**: Wählen Sie die Warteschlange aus, für die statistische Daten angezeigt werden.
- **Löschpriorität**: Geben Sie die Löschpriorität für das Löschen von Daten ein.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Der Zähler für die Warteschlangenstatistik wird hinzugefügt und die aktuelle Konfigurationsdatei wird aktualisiert.

30

SNMP

In diesem Abschnitt wird die SNMP-Funktion (Simple Network Management Protocol) beschrieben. Mit dieser Funktion können Netzwerkgeräte verwaltet werden.

Die folgenden Themen werden behandelt:

- **SNMP-Versionen und -Workflow**
- **Modell-OIDs**
- **SNMP-Engine-ID**
- **Konfigurieren von SNMP-Ansichten**
- **Erstellen von SNMP-Gruppen**
- **Verwalten von SNMP-Benutzern**
- **Definieren von SNMP-Communitys**
- **Definieren von Trap-Einstellungen**
- **Benachrichtigungsempfänger**
- **SNMP-Benachrichtigungsfilter**

SNMP-Versionen und -Workflow

Das Gerät dient als SNMP-Agent und unterstützt SNMPv1, SNMPv2 und SNMPv3. Außerdem werden Systemereignisse an Trap-Empfänger berichtet. Dabei werden die Traps verwendet, die in der vom Switch unterstützten Managementinformationsbasis (MIB) festgelegt sind.

SNMPv1 und SNMPv2

Für die Steuerung des Zugangs zum System wird eine Liste von Community-Einträgen festgelegt. Jeder Community-Eintrag besteht aus einer *Community-Zeichenfolge* und der zugehörigen Zugriffsberechtigung. Das System reagiert nur auf SNMP-Nachrichten, in denen die Community angegeben ist, die über die richtigen Berechtigungen verfügt und sich im richtigen Betriebsmodus befindet.

SNMP-Agents verwalten eine Liste von Variablen, die zum Verwalten des Geräts verwendet werden. Diese Variablen werden in der *Managementinformationsbasis* (MIB) definiert.

HINWEIS Aufgrund der Sicherheitsschwachstellen anderer Versionen wird die Verwendung von SNMPv3 empfohlen.

SNMPv3

Zusätzlich zu den Funktionen, die von SNMPv1 und SNMPv2 bereitgestellt werden, wendet SNMPv3 die Zugriffssteuerung und neue Trap-Mechanismen auf SNMPv1- und SNMPv2-PDUs an. Mit SNMPv3 wird außerdem ein USM (User Security Model, Benutzersicherheitsmodell) definiert, das Folgendes umfasst:

- **Authentifizierung**: Sorgt für die Integrität der Daten und die Authentifizierung des Datenursprungs.
- **Datenschutz**: Schützt gegen die Offenlegung des Inhalts von Nachrichten. Die Verschlüsselung erfolgt mithilfe von *Cipher Block-Chaining* (CBC-DES). Bei einer SNMP-Nachricht kann entweder nur die Authentifizierung oder sowohl die Authentifizierung als auch der Datenschutz aktiviert sein. Der Datenschutz kann nicht separat, sondern nur zusammen mit der Authentifizierung aktiviert werden.
- **Aktualität**: Schützt vor Nachrichtenverzögerung und Playback-Angriffen. Der SNMP-Agent vergleicht den Zeitstempel der eingehenden Nachricht mit der Eingangszeit der Nachricht.
- **Schlüsselverwaltung**: Bestimmt die Erstellung, Aktualisierung und Verwendung von Schlüsseln. Das Gerät unterstützt SNMP-Benachrichtigungsfilter auf der Grundlage von *Objekt-IDs* (OIDs). OIDs werden vom System für die Verwaltung von Gerätefunktionen verwendet.

SNMP-Workflow

HINWEIS Aus Sicherheitsgründen ist SNMP standardmäßig deaktiviert. Damit Sie das Gerät über SNMP verwalten können, müssen Sie SNMP auf der Seite „Sicherheit > TCP/UDP-Services“ aktivieren.

Zum Konfigurieren von SNMP wird folgende Vorgehensweise empfohlen:

Falls Sie sich für die Verwendung von SNMPv1 oder SNMPv2 entschieden haben:

SCHRITT 1 Navigieren Sie zur Seite „SNMP > Communitys“ und klicken Sie auf **Hinzufügen**. Sie können der Community im Basismodus Zugriffsrechte und eine Ansicht oder im erweiterten Modus eine Gruppe zuordnen. Es gibt zwei Möglichkeiten, um Zugriffsrechte für eine Community zu definieren:

- **Basismodus**: Die Zugriffsrechte einer Community können nur als „Schreibgeschützt“, „Lesen/Schreiben“ oder „SNMP-Administration“ konfiguriert werden. Zusätzlich können Sie den Zugriff auf die Community mithilfe von Ansichten auf bestimmte MIB-Objekte beschränken (Ansichten werden auf der Seite „Ansichten“ definiert).
- **Erweiterter Modus**: Die Zugriffsrechte einer Community werden durch eine Gruppe definiert (Gruppen werden auf der Seite „Gruppen“ definiert). Sie können die Gruppe mit einem bestimmten Sicherheitsmodell konfigurieren. Die Zugriffsrechte einer Gruppe lauten „Lesen“, „Schreiben“ und „Benachrichtigen“.

SCHRITT 2 Wählen Sie aus, ob die SNMP-Verwaltungsstation auf eine Adresse beschränkt werden soll oder die SNMP-Verwaltung über alle Adressen möglich sein soll. Wenn die SNMP-Verwaltung auf eine Adresse beschränkt sein soll, geben Sie die Adresse des SNMP-Verwaltungs-PCs in das Feld „IP-Adresse“ ein.

SCHRITT 3 Geben Sie in das Feld „Community-Zeichenfolge“ die eindeutige Community-Zeichenfolge ein.

SCHRITT 4 Aktivieren Sie optional Traps auf der Seite **Trap-Einstellungen**.

SCHRITT 5 Definieren Sie optional auf der Seite **Benachrichtigungsfilter** einen oder mehrere Benachrichtigungsfilter.

SCHRITT 6 Konfigurieren Sie auf der Seite „Benachrichtigungsempfänger SNMPv1, 2“ die Benachrichtigungsempfänger.

Falls Sie sich für die Verwendung von SNMPv3 entschieden haben:

SCHRITT 1 Definieren Sie auf der Seite „Engine-ID“ die SNMP-Engine. Erstellen Sie eine eindeutige Engine-ID oder verwenden Sie die Standard-Engine-ID. Beim Anwenden einer Engine-ID-Konfiguration wird die SNMP-Datenbank gelöscht.

SCHRITT 2 Definieren Sie optional auf der Seite „Ansichten“ SNMP-Ansichten. Dadurch wird der Bereich der für eine Community oder Gruppe verfügbaren OIDs begrenzt.

SCHRITT 3 Definieren Sie auf der Seite „Gruppen“ Gruppen.

SCHRITT 4 Definieren Sie auf der Seite „SNMP-Benutzer“ Benutzer, die Sie auf dieser Seite auch einer Gruppe zuordnen können. Wenn Sie die SNMP-Engine-ID nicht festgelegt haben, können Sie keine Benutzer erstellen.

SCHRITT 5 Aktivieren oder deaktivieren Sie optional Traps auf der Seite „Trap-Einstellungen“.

SCHRITT 6 Definieren Sie optional auf der Seite **Benachrichtigungsfilter** einen oder mehrere Benachrichtigungsfilter.

SCHRITT 7 Definieren Sie auf der Seite „Benachrichtigungsempfänger SNMPv3“ einen oder mehrere Benachrichtigungsempfänger.

Unterstützte MIBs

Eine Liste der unterstützten MIBs finden Sie unter der folgenden URL. Navigieren Sie dort zum Downloadbereich **Cisco MIBS**:

www.cisco.com/cisco/software/navigator.html

Modell-OIDs

Die *Modell-OIDs* (ObjektIDs) von Geräten lauten wie folgt:

Modellname	Beschreibung	Objekt-ID
SF500-24	10/100 Stackable Managed Switch mit 24 Ports	9.6.1.80.24.1
SF500-24P	10/100 PoE Stackable Managed Switch mit 24 Ports	9.6.1.80.24.2
SF500-48	10/100 Stackable Managed Switch mit 48 Ports	9.6.1.80.48.1
SF500-48P	10/100 PoE Stackable Managed Switch mit 48 Ports	9.6.1.80.48.2
SG500-28	Stackable Managed Switch mit 28 Gigabit-Ports	9.6.1.81.28.1
SG500-28P	PoE Stackable Managed Switch mit 28 Gigabit-Ports	9.6.1.81.28.2
SG500-52	Stackable Managed Switch mit 52 Gigabit-Ports	9.6.1.81.52.1
SG500-52P	PoE Stackable Managed Switch mit 52 Gigabit-Ports	9.6.1.81.52.2
SG500X-24	Stackable Managed Switch mit 24 Gigabit-Ports und 4 10-Gigabit-Ports	9.6.1.85.24.1

Modellname	Beschreibung	Objekt-ID
SG500X 24P	PoE Stackable Managed Switch mit 24 Gigabit-Ports und 4 10-Gigabit-Ports	9.6.1.85.24.2
SG500X-48	Stackable Managed Switch mit 48 Gigabit-Ports und 4 10-Gigabit-Ports	9.6.1.85.48.1
SG500X-48P	PoE Stackable Managed Switch mit 48 Gigabit-Ports und 4 10-Gigabit-Ports	9.6.1.85.48.2
ESW2-550X-48	Stackable Managed Switch mit 48 Gigabit-Ports und 4 10-Gigabit-Ports	9.6.1.86.48.1
ESW2-550X-48DC	Stackable Managed Switch mit 48 Gigabit-Ports und 4 10-Gigabit-Ports	9.6.1.86.48.6
SG500-52MP	Gigabit-Max-PoE-Managed Switch mit 52 Ports	9.6.1.81.5.3.0
ESW2-550X-48DC	Stackable Managed Switch mit 48 Gigabit-Ports und 4 10-Gigabit-Ports	9.6.1.86.48.6

Die privaten Objekt-IDs befinden sich unter: enterprises(1).cisco(9).otherEnterprises(6).ciscosb(1).switch001(101).

SNMP-Engine-ID

Die Engine-ID wird von SNMPv3-Einheiten zu deren eindeutiger Identifizierung verwendet. Ein SNMP-Agent gilt als autoritative SNMP-Engine. Das bedeutet, dass der Agent auf eingehende Nachrichten (Get, GetNext, GetBulk, Set) reagiert und Trap-Nachrichten an einen Manager sendet. Die lokalen Informationen des Agents sind in Feldern innerhalb der Nachricht eingeschlossen.

Jeder SNMP-Agent verwaltet lokale Informationen, die beim SNMPv3-Nachrichtenaustausch verwendet werden. Die standardmäßige SNMP-Engine-ID setzt sich aus der Enterprise-Nummer und der Standard-MAC-Adresse zusammen. Die Engine-ID muss für die administrative Domäne eindeutig sein, sodass zwei Geräte in einem Netzwerk nie dieselbe Engine-ID aufweisen können.

Lokale Informationen werden in vier schreibgeschützten MIB-Variablen gespeichert (snmpEngineId, snmpEngineBoots, snmpEngineTime und snmpEngineMaxMessageSize).

VORSICHT Wenn sich die Engine-ID ändert, werden alle konfigurierten Benutzer und Gruppen gelöscht.

So legen Sie die SNMP-Engine-ID fest:

SCHRITT 1 Klicken Sie auf **SNMP** > **Engine-ID**.

SCHRITT 2 Wählen Sie aus, welche ID als **Lokale Engine-ID** verwendet werden soll.

- **Standard verwenden**: Wählen Sie diese Option, um die vom Gerät erzeugte Engine-ID zu verwenden. Die Standard-Engine-ID basiert auf der MAC-Adresse des Geräts und wird standardmäßig wie folgt definiert:
  - *Erste 4 Oktette*: Erstes Bit = 1, der Rest ist die IANA-Enterprise-Nummer.
  - *Fünftes Oktett*: Setzen Sie diesen Wert auf „3“, um zu verdeutlichen, dass die MAC-Adresse folgt.
  - *Letzte 6 Oktette*: MAC-Adresse des Geräts.
- **Ohne**: Es wird keine Engine-ID verwendet.
- **Benutzerdefiniert**: Geben Sie die Engine-ID des lokalen Geräts ein. Der Wert des Felds ist eine hexadezimale Zeichenfolge **(Bereich: 10 bis 64)**. Jedes Byte in der hexadezimalen Zeichenfolge wird durch zwei hexadezimale Ziffern dargestellt.

Alle Remote-Engine-IDs und die zugehörigen IP-Adressen werden in der Remote-Engine-ID-Tabelle angezeigt.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

In der Remote-Engine-ID-Tabelle wird die Zuordnung zwischen den IP-Adressen der Engine und der Engine-ID angezeigt. So fügen Sie die IP-Adresse einer Engine-ID hinzu:

SCHRITT 4 Klicken Sie auf **Hinzufügen**. Geben Sie Werte für die folgenden Felder ein:

- **Serverdefinition**: Wählen Sie aus, ob der Engine-ID-Server anhand der IP-Adresse oder des Namens angegeben wird.
- **IP-Version**: Wählen Sie das unterstützte IP-Format aus.
- **IPv6-Adresstyp**: Wählen Sie den IPv6-Adresstyp aus (falls IPv6 verwendet wird). Folgende Optionen sind möglich:
  - *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
  - *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.
- **Link Local-Schnittstelle**: Wählen Sie in der Liste die Link Local-Schnittstelle aus (falls der IPv6-Adresstyp „Link Local“ ausgewählt ist).

- **IP-Adresse/Name des Servers**: Geben Sie die IP-Adresse oder den Domänennamen des Protokollservers ein.
- **Engine-ID**: Geben Sie die Engine-ID ein.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Konfigurieren von SNMP-Ansichten

Eine Ansicht ist eine benutzerdefinierte Bezeichnung für eine Sammlung von MIB-Unterstrukturen. Jede Unterstruktur-ID wird durch die *Objekt-ID* (OID) des Stammverzeichnisses der zugehörigen Unterstrukturen bestimmt. Für die Angabe des Stammverzeichnisses der gewünschten Unterstruktur können Sie bekannte Namen verwenden oder eine OID eingeben (siehe **Modell-OIDs**).

Die einzelnen Unterstrukturen werden beim Festlegen der Ansicht entweder eingeschlossen oder ausgeschlossen.

Auf der Seite „Ansichten“ können Sie SNMP-Ansichten erstellen oder bearbeiten. Die Standardansichten („Standard“, „Standard von Superuser“) können nicht geändert werden.

Auf der Seite „Gruppen“ können Sie Ansichten Gruppen zuordnen. Auf der Seite „Communitys“ können Sie Ansichten einer Community im Basiszugriffsmodus zuordnen.

So definieren Sie SNMP-Ansichten:

SCHRITT 1 Klicken Sie auf **SNMP** > **Ansichten**.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, um die neuen Ansichten festzulegen.

SCHRITT 3 Geben Sie die Parameter ein.

- **Ansichtsname**: Geben Sie einen Ansichtsnamen ein, der aus 0 - 30 Zeichen besteht.
- **Objekt-ID-Unterstruktur**: Wählen Sie den Knoten innerhalb der MIB-Struktur aus, der in den ausgewählten Benachrichtigungsfilter eingeschlossen oder von ihm ausgeschlossen werden soll. Für die Auswahl des Objekts bestehen folgende Optionen:
  - *Aus Liste auswählen*: Hiermit können Sie in der MIB-Struktur navigieren. Klicken Sie auf den *Nach-Oben*-Pfeil, um zur Ebene der übergeordneten und gleichrangigen Elemente des ausgewählten Knotens zu gelangen; klicken Sie auf den *Nach-Unten*-Pfeil, um zur Ebene der untergeordneten Objekte des ausgewählten Knotens zu gelangen. Klicken Sie auf einen Knoten der Ansicht, um zu einem anderen gleichrangigen Knoten zu gelangen. Mit der Scrollleiste können Sie gleichrangige Knoten in den sichtbaren Bereich bewegen.

- *Benutzerdefiniert*: Geben Sie eine OID ein, die nicht in der Option *Aus Liste auswählen* enthalten ist.

SCHRITT 4 Wählen Sie die Option **„In Ansicht einschließen“** aus oder heben Sie deren Auswahl auf. Wenn diese Option ausgewählt ist, sind die ausgewählten MIBs in der Ansicht enthalten, anderenfalls sind sie nicht enthalten.

SCHRITT 5 Klicken Sie auf **Übernehmen**.

SCHRITT 6 Um die Ansichtskonfiguration zu überprüfen, wählen Sie die benutzerdefinierten Ansichten in der Liste **Filter: Ansichtsname** aus. Die folgenden Ansichten sind standardmäßig vorhanden:

- **Default**: Standard-SNMP-Ansicht für Lesen- und Lesen/Schreiben-Ansichten.
- **DefaultSuper**: Standard-SNMP-Ansicht für Administrator-Ansichten.

Weitere Ansichten können hinzugefügt werden.

- **Objekt-ID-Unterstruktur**: Zeigt die Unterstruktur an, die in die SNMP-Ansicht eingeschlossen oder von ihr ausgeschlossen werden soll.
- **Objekt-ID-Unterstrukturansicht**: Zeigt an, ob die definierte Unterstruktur in der ausgewählten SNMP-Ansicht eingeschlossen ist oder ob sie von ihr ausgeschlossen ist.

Erstellen von SNMP-Gruppen

In SNMPv1 und SNMPv2 wird eine Community-Zeichenfolge zusammen mit den SNMP-Frames gesendet. Die Community-Zeichenfolge dient als Kennwort für den Zugriff auf einen SNMP-Agent. Allerdings werden weder die Frames noch die Community-Zeichenfolge verschlüsselt. Insofern sind SNMPv1 und SNMPv2 keine sicheren Protokolle.

In SNMPv3 können die folgenden Sicherheitsmechanismen konfiguriert werden:

- **Authentifizierung**: Das Gerät überprüft, ob es sich bei dem SNMP-Benutzer um einen autorisierten Systemadministrator handelt. Diese Überprüfung wird für jeden einzelnen Frame durchgeführt.
- **Datenschutz**: SNMP-Frames können verschlüsselte Daten transportieren.

SNMPv3 enthält also drei Sicherheitsstufen:

- Keine Sicherheit (keine Authentifizierung und kein Datenschutz)
- Authentifizierung (Authentifizierung und kein Datenschutz)
- Authentifizierung und Datenschutz

Mithilfe von SNMPv3 können Sie steuern, welche Inhalte die einzelnen Benutzer lesen oder schreiben können und welche Benachrichtigungen sie erhalten. Mit einer Gruppe können Sie Lese- bzw. Schreibberechtigungen und eine Sicherheitsstufe definieren. Eine Gruppe ist aktiv, wenn sie einem SNMP-Benutzer oder einer SNMP-Community zugewiesen wird.

HINWEIS Um einer Gruppe eine nicht standardmäßige Ansicht zuzuordnen, erstellen Sie zuerst auf der Seite „Ansichten“ die Ansicht.

So erstellen Sie eine SNMP-Gruppe:

SCHRITT 1 Klicken Sie auf **SNMP** > **Gruppen**.

Diese Seite enthält die vorhandenen SNMP-Gruppen und ihre Sicherheitsstufen.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Gruppenname**: Geben Sie einen neuen Gruppennamen ein.
- **Sicherheitsmodell**: Wählen Sie die SNMP-Version für die Gruppe aus (SNMPv1, SNMPv2 oder SNMPv3).

Sie können drei Ansichtsarten mit verschiedenen Sicherheitsstufen definieren. Wählen Sie für jede Sicherheitsstufe die Ansichten für „Lesen“, „Schreiben“ und „Benachrichtigen“ aus, indem Sie die folgenden Felder auswählen:

- **Aktivieren**: Wählen Sie diese Option aus, um die Sicherheitsstufe zu aktivieren.
- **Sicherheitsstufe**: Legen Sie die Sicherheitsstufe für die Gruppe fest. SNMPv1 und SNMPv2 unterstützen weder Authentifizierung noch Datenschutz. Wenn SNMPv3 ausgewählt ist, wählen Sie eine der folgenden Optionen aus:
  - *Keine Authentifizierung und kein Datenschutz*: Der Gruppe wird keine der Sicherheitsstufen „Authentifizierung“ oder „Datenschutz“ zugewiesen.
  - *Authentifizierung und kein Datenschutz*: Authentifiziert SNMP-Nachrichten und stellt sicher, dass der Ursprung der SNMP-Nachrichten authentifiziert ist, ohne die Nachrichten zu verschlüsseln.
  - *Authentifizierung und Datenschutz*: Authentifiziert und verschlüsselt SNMP-Nachrichten.
- **Anzeigen**: Wählen Sie diese Option aus, um den Lese-, Schreib- und/oder Benachrichtigungsberechtigungen der Gruppe eine Ansicht zuzuordnen. Hierdurch beschränken Sie den Umfang der MIB-Struktur, für die die Gruppe über Lese-, Schreib- und Benachrichtigungszugriff verfügt.
  - *Lesen*: Für die ausgewählte Ansicht besteht ein schreibgeschützter Verwaltungszugriff. Anderenfalls können Benutzer oder Communitys, die dieser Gruppe zugeordnet sind, alle MIBs lesen, außer denjenigen, die SNMP steuern.
  - *Schreiben*: Für die ausgewählte Ansicht besteht der Verwaltungszugriff „Schreiben“. Anderenfalls können Benutzer oder Communitys, die dieser Gruppe zugeordnet sind, alle MIBs schreiben, außer denjenigen, die SNMP steuern.

- *Benachrichtigen*: Beschränkt den verfügbaren Inhalt der Traps auf die in der ausgewählten Ansicht enthaltenen. Andernfalls gelten für den Inhalt der Traps keine Einschränkungen. Diese Option kann nur für SNMPv3 ausgewählt werden.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die SNMP-Gruppe wird in der aktuellen Konfigurationsdatei gespeichert.

Verwalten von SNMP-Benutzern

Ein SNMP-Benutzer wird durch die Anmeldeinformationen (Benutzername, Kennwörter und Authentifizierungsmethode) definiert sowie durch die ihm zugewiesene Gruppe und Engine-ID, die der Art und dem Umfang seiner Arbeit im System entsprechen.

Der konfigurierte Benutzer hat dann die Attribute seiner Gruppe und die in der zugeordneten Ansicht konfigurierten Zugriffsberechtigungen.

Gruppen bieten Netzwerkmanagern die Möglichkeit, Zugriffsrechte einer gesamten Gruppe von Benutzern zuzuweisen anstatt nur einem einzigen Benutzer.

Ein Benutzer kann nur zu einer einzigen Gruppe gehören.

Damit Sie einen SNMPv3-Benutzer erstellen können, muss zunächst Folgendes vorhanden sein:

- Eine Engine-ID muss zunächst für das Gerät konfiguriert werden. Verwenden Sie hierzu die Seite „Engine-ID“.
- Eine SNMPv3-Gruppe muss verfügbar sein. Auf der Seite „Gruppen“ können Sie eine SNMPv3-Gruppe definieren.

So zeigen Sie SNMP-Benutzer an und erstellen neue:

SCHRITT 1 Klicken Sie auf **SNMP** > **Benutzer**.

Diese Seite enthält die vorhandenen Benutzer.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

Die Seite enthält Informationen für das Zuweisen von SNMP-Zugriffssteuerungsberechtigungen zu SNMP-Benutzern.

SCHRITT 3 Geben Sie die Parameter ein.

- **Benutzername**: Geben Sie einen Namen für den Benutzer ein.

- **Engine-ID**: Wählen Sie entweder die lokale SNMP-Einheit oder die Remote-SNMP-Einheit aus, mit der der Benutzer verbunden ist. Durch das Ändern oder Entfernen der lokalen SNMP-Engine-ID wird die SNMPv3-Benutzerdatenbank gelöscht. Um sowohl Informationsnachrichten als auch Anfrageinformationen zu erhalten, müssen Sie sowohl einen lokalen Benutzer als auch einen Remote-Benutzer definieren.
  - *Lokal*: Der Benutzer ist mit dem lokalen Gerät verbunden.
  - *Remote IP-Adresse*: Der Benutzer ist neben dem lokalen Gerät mit einer anderen SNMP-Einheit verbunden. Wenn die Remote-Engine-ID festgelegt ist, empfangen Remote-Geräte Informationsnachrichten, können jedoch keine Informationsanfragen durchführen.

    Geben Sie die Remote-Engine-ID ein.
- **Gruppenname**: Wählen Sie die SNMP-Gruppe aus, der der SNMP-Benutzer angehört. SNMP-Gruppen werden auf der Seite „Gruppe hinzufügen“ definiert.

  HINWEIS Benutzer, die gelöschten Gruppen angehören, bleiben erhalten, sind jedoch inaktiv.
- **Authentifizierungsmethode**: Wählen Sie die Authentifizierungsmethode für den zugewiesenen Gruppennamen aus. Wenn für die Gruppe keine Authentifizierung erforderlich ist, kann der Benutzer keine Authentifizierung konfigurieren. Folgende Optionen sind möglich:
  - *Keine*: Es wird keine Authentifizierung verwendet.
  - *MD5*: Ein Kennwort, das zum Generieren eines Schlüssels durch die MD5-Authentifizierungsmethode verwendet wird.
  - *SHA*: Ein Kennwort, das zum Generieren eines Schlüssels durch die SHA-Authentifizierungsmethode (Secure Hash Algorithm) verwendet wird.
- **Authentifizierungskennwort**: Falls die Authentifizierung über ein MD5- oder SHA-Kennwort erfolgt, geben Sie das Kennwort des lokalen Benutzers ein (**Verschlüsselt** oder **Unverschlüsselt**). Die Kennwörter der lokalen Benutzer werden mit der lokalen Datenbank verglichen. Sie können bis zu 32 ASCII-Zeichen umfassen.
- **Datenschutzmethode**: Wählen Sie eine der folgenden Optionen aus:
  - *Keine*: Das Datenschutzkennwort wird nicht verschlüsselt.
  - *DES*: Das Datenschutzkennwort wird gemäß DES (Data Encryption Standard) verschlüsselt.
- **Datenschutzkennwort**: Wenn Sie die DES-Datenschutzmethode ausgewählt haben, sind 16 Bytes erforderlich. Dieses Feld muss genau 32 Hexadezimalzeichen enthalten. Sie können den Modus **Verschlüsselt** oder **Unverschlüsselt** auswählen.

SCHRITT 4 Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Definieren von SNMP-Communitys

Zur Verwaltung der Zugriffsrechte bei SNMPv1 und SNMPv2 können Sie auf der Seite „Communitys“ Communitys definieren. Der Community-Name dient als eine Art Kennwort, das von der SNMP-Verwaltungsstation und dem Gerät gemeinsam genutzt wird. Es wird zur Authentifizierung der SNMP-Verwaltungsstation verwendet.

Communitys werden nur in SNMPv1 und SNMPv2 definiert, da SNMPv3 nicht mit Communitys, sondern mit Benutzern arbeitet. Die Benutzer gehören Gruppen an, denen Zugriffsrechte zugewiesen wurden.

Auf der Seite „Communitys“ werden Communitys Zugriffsrechte zugewiesen, entweder direkt (Basismodus) oder über Gruppen (erweiterter Modus):

- **Basismodus**: Die Zugriffsrechte einer Community können nur als „Schreibgeschützt“, „Lesen/Schreiben“ oder „SNMP-Administration“ konfiguriert werden. Zusätzlich können Sie den Zugriff auf die Community mithilfe von Ansichten auf bestimmte MIB-Objekte beschränken (Ansichten werden auf der Seite „SNMP-Ansichten“ definiert).
- **Erweiterter Modus**: Die Zugriffsrechte einer Community werden durch eine Gruppe definiert (Gruppen werden auf der Seite „Gruppen“ definiert). Sie können die Gruppe mit einem bestimmten Sicherheitsmodell konfigurieren. Die Zugriffsrechte einer Gruppe lauten „Lesen“, „Schreiben“ und „Benachrichtigen“.

So definieren Sie SNMP-Communitys:

SCHRITT 1 Klicken Sie auf **SNMP** > **Communitys**.

Diese Seite enthält eine Tabelle mit den konfigurierten SNMP-Communitys und ihren Eigenschaften.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

Auf dieser Seite können Netzwerkmanager neue SNMP-Communitys definieren und konfigurieren.

SCHRITT 3 **SNMP-Verwaltungsstation**: Klicken Sie auf **Benutzerdefiniert**, um die IP-Adresse der Verwaltungsstation einzugeben, die auf die SNMP-Community zugreifen kann. Klicken Sie auf **Alle**, um anzugeben, dass alle IP-Geräte auf die SNMP-Community zugreifen können.

- **IP-Version**: Wählen Sie entweder IPv4 oder IPv6 aus.
- **IPv6-Adresstyp**: Wählen Sie den unterstützten IPv6-Adresstyp aus (falls IPv6 verwendet wird). Folgende Optionen sind möglich:
  - *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.

  - *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.

- **Link Local-Schnittstelle**: Falls es sich bei dem IPv6-Adresstyp um „Link Local“ handelt, wählen Sie aus, ob der Empfang über VLAN oder ISATAP erfolgt.
- **IP-Adresse**: Geben Sie die IP-Adresse der SNMP-Verwaltungsstation ein.
- **Community-Zeichenfolge**: Geben Sie den Community-Namen ein, der zur Authentifizierung der Verwaltungsstation gegenüber dem Gerät verwendet wird.
- **Basismodus**: Wählen Sie diesen Modus für eine ausgewählte Community aus. In diesem Modus ist keine Verbindung zu einer Gruppe vorhanden. Sie können lediglich die Zugriffsstufe für die Community festlegen („Schreibgeschützt“, „Lesen/Schreiben“ oder „SNMP-Administration“) und optional eine bestimmte Ansicht erlauben. Der Geltungsbereich ist standardmäßig die gesamte MIB. Falls Sie diese Option auswählen, geben Sie Werte in die folgenden Felder ein:
  - *Zugriffsmodus*: Wählen Sie die Zugriffsrechte der Community aus. Folgende Optionen sind möglich:

    Nur Lesen: Es besteht ein schreibgeschützter Verwaltungszugriff. Es können keine Änderungen an der Community vorgenommen werden.

    Lesen/Schreiben: Der Verwaltungszugriff erlaubt das Lesen und Schreiben. Es können Änderungen an der Gerätekonfiguration vorgenommen werden, jedoch nicht an der Community.

    SNMP-Administration: Der Benutzer hat Zugriff auf alle Optionen für die Gerätekonfiguration und darf Änderungen an der Community vornehmen. „SNMP-Administration“ entspricht der Option „Lesen/Schreiben“ für alle MIBs außer für die SNMP-MIBs. „SNMP-Administration“ ist für den Zugriff auf die SNMP-MIBs erforderlich.
  - *Ansichtsname*: Wählen Sie eine SNMP-Ansicht aus (eine Sammlung von MIB-Unterverzeichnissen, auf die Zugriff gewährt wird).
- **Erweiterter Modus**: Wählen Sie diesen Modus für eine ausgewählte Community aus.
  - *Gruppenname*: Wählen Sie eine SNMP-Gruppe aus, über die die Zugriffsrechte gesteuert werden.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die SNMP-Community wird definiert und die aktuelle Konfigurationsdatei wird aktualisiert.

Definieren von Trap-Einstellungen

Auf der Seite „Trap-Einstellungen“ können Sie konfigurieren, ob und in welchen Fällen SNMP-Benachrichtigungen vom Gerät gesendet werden. Die Empfänger der SNMP-Benachrichtigungen können Sie auf der Seite „Benachrichtigungsempfänger SNMPv1, 2“ oder „Benachrichtigungsempfänger SNMPv3“ konfigurieren.

So legen Sie Trap-Einstellungen fest:

SCHRITT 1 Klicken Sie auf **SNMP** > **Trap-Einstellungen**.

SCHRITT 2 Wählen Sie **Aktivieren** für **SNMP-Benachrichtigungen** aus, um anzugeben, dass das Gerät SNMP-Benachrichtigungen senden kann.

SCHRITT 3 Wählen Sie **Aktivieren** für **Authentifizierungsbenachrichtigungen**, um eine Benachrichtigung im Fall einer nicht erfolgreichen SNMP-Authentifizierung zu aktivieren.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die SNMP-Trap-Einstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Benachrichtigungsempfänger

Trap-Nachrichten werden erzeugt, damit Systemereignisse berichtet werden, entsprechend der Norm RFC 1215. Das System kann Traps erzeugen, die in der unterstützten MIB festgelegt sind.

Die Trap-Empfänger (Benachrichtigungsempfänger) sind Netzwerkknoten, an die die Trap-Nachrichten vom Gerät gesendet werden. Es wird eine Liste der Benachrichtigungsempfänger festgelegt, die die Ziele der Trap-Nachrichten enthält.

Ein Trap-Empfänger-Eintrag enthält die IP-Adresse des Knotens sowie die SNMP-Anmeldeinformationen, die der Version entsprechen, die in der Trap-Nachricht enthalten ist. Wenn ein Ereignis eintritt, für das eine Trap-Nachricht gesendet werden soll, wird diese Nachricht an alle Knoten gesendet, die in der Tabelle für Benachrichtigungsempfänger aufgeführt sind.

Auf den Seiten „Benachrichtigungsempfänger SNMPv1, 2“ und „Benachrichtigungsempfänger SNMPv3“ können Sie die Ziele konfigurieren, an die SNMP-Benachrichtigungen gesendet werden, sowie die Arten der SNMP-Benachrichtigungen, die an das jeweilige Ziel gesendet werden (Traps oder Informationen). In den Popup-Fenstern „Hinzufügen“ und „Bearbeiten“ können Sie die Attribute der Benachrichtigungen konfigurieren.

Eine SNMP-Benachrichtigung ist eine Nachricht, die vom Gerät zur SNMP-Verwaltungsstation gesendet wird und die über ein bestimmtes aufgetretenes Ereignis informiert, beispielsweise über den Betrieb oder Ausfall einer Verbindung.

Es ist auch möglich, bestimmte Benachrichtigungen herauszufiltern. Dazu können Sie auf der Seite „Benachrichtigungsfilter“ einen Filter erstellen und diesen mit einem SNMP-Benachrichtigungsempfänger verknüpfen. Mithilfe des Benachrichtigungsfilters kann der Typ von SNMP-Benachrichtigungen herausgefiltert werden, die an die Verwaltungsstation gesendet werden sollen. Dies geschieht auf Grundlage der OID der zu sendenden Benachrichtigung.

Festlegen von Benachrichtigungsempfängern für SNMPv1 und -v2

So legen Sie einen Empfänger in SNMPv1 und -v2 fest:

SCHRITT 1 Klicken Sie auf **SNMP** > **Benachrichtigungsempfänger SNMPv1, 2**.

Auf dieser Seite werden die Empfänger für SNMPv1 und SNMPv2 angezeigt.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **Informiert IPv4-Quellschnittstelle**: Wählen Sie die Quellschnittstelle aus, deren IPv4-Adresse als Quell-IPv4-Adresse in Informationsnachrichten für die Kommunikation mit IPv4-SNMP-Servern verwendet wird.
- **Erfasst IPv4-Quellschnittstelle**: Wählen Sie die Quellschnittstelle aus, deren IPv6-Adresse als Quell-IPv6-Adresse in Informationsnachrichten für die Kommunikation mit IPv6-SNMP-Servern verwendet wird.
- **Informiert IPv6-Quellschnittstelle**: Wählen Sie die Quellschnittstelle aus, deren IPv4-Adresse als Quell-IPv4-Adresse in Informationsnachrichten für die Kommunikation mit IPv4-SNMP-Servern verwendet wird.
- **Erfasst IPv6-Quellschnittstelle**: Wählen Sie die Quellschnittstelle aus, deren IPv6-Adresse als Quell-IPv6-Adresse in Informationsnachrichten für die Kommunikation mit IPv6-SNMP-Servern verwendet wird.

  HINWEIS Wenn Sie die Option „Auto“ auswählen, übernimmt das System die Quell-IP-Adresse aus der IP-Adresse, die auf der ausgehenden Schnittstelle definiert wurde.

  SCHRITT 3 Klicken Sie auf **Hinzufügen**.

  SCHRITT 4 Geben Sie die Parameter ein.

- **Serverdefinition**: Wählen Sie aus, ob der Remote-Protokollserver anhand der IP-Adresse oder des Namens angegeben wird.
- **IP-Version**: Wählen Sie entweder IPv4 oder IPv6 aus.

- **IPv6-Adresstyp**: Wählen Sie *Link Local* oder *Global* aus.
  - *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
  - *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.
- **Link Local-Schnittstelle**: Falls es sich bei dem IPv6-Adresstyp um „Link Local“ handelt, wählen Sie aus, ob der Empfang über VLAN oder ISATAP erfolgt.
- **IP-Adresse des Empfängers**: Geben Sie die IP-Adresse oder den Namen des Servers ein, an den die Traps gesendet werden.
- **UDP-Port**: Geben Sie den UDP-Port ein, der beim Empfängergerät für Benachrichtigungen verwendet wird.
- **Benachrichtigungstyp**: Wählen Sie aus, ob Traps oder Informationen gesendet werden sollen. Falls beides benötigt wird, müssen zwei Empfänger erstellt werden.
- **Timeout**: Geben Sie an, wie viele Sekunden das Gerät wartet, bis es die Informationen erneut sendet.
- **Wiederholungen**: Geben Sie an, wie oft das Gerät Informationsanforderungen erneut sendet.
- **Community-Zeichenfolge**: Wählen Sie in der Pulldown-Liste die Community-Zeichenfolge des Trap-Managers aus. Die Namen von Community-Zeichenfolgen werden aus den auf der Seite „Community“ aufgeführten Zeichenfolgen generiert.
- **Benachrichtigungsversion**: Wählen Sie die SNMP-Version der Traps aus.
  Als Trap-Version kann SNMPv1 oder SNMPv2 verwendet werden. Es kann immer nur eine der beiden Versionen aktiviert sein.
- **Benachrichtigungsfilter**: Hiermit können die SNMP-Benachrichtigungen, die an die Verwaltungsstation gesendet werden, nach dem Typ gefiltert werden. Die Filter werden auf der Seite „Benachrichtigungsfilter“ erstellt.
- **Filtername**: Wählen Sie den SNMP-Filter aus, der bestimmt, welche Informationen in Traps enthalten sein sollen (der Filter wird auf der Seite „Benachrichtigungsfilter“ definiert).

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die Einstellungen für SNMP-Benachrichtigungsempfänger werden in die aktuelle Konfigurationsdatei geschrieben.

Definieren von Benachrichtigungsempfängern bei SNMPv3

So legen Sie einen Empfänger in SNMPv3 fest:

SCHRITT 1 Klicken Sie auf **SNMP** > **Benachrichtigungsempfänger SNMPv3**.

Auf dieser Seite werden die Empfänger für SNMPv3 angezeigt.

- **Informiert IPv4-Quellschnittstelle**: Wählen Sie die Quellschnittstelle aus, deren IPv4-Adresse als Quell-IPv4-Adresse in Informationsnachrichten für die Kommunikation mit IPv4-SNMP-Servern verwendet wird.
- **Erfasst IPv4-Quellschnittstelle**: Wählen Sie die Quellschnittstelle aus, deren IPv6-Adresse als Quell-IPv6-Adresse in Informationsnachrichten für die Kommunikation mit IPv6-SNMP-Servern verwendet wird.
- **Informiert IPv6-Quellschnittstelle**: Wählen Sie die Quellschnittstelle aus, deren IPv4-Adresse als Quell-IPv4-Adresse in Informationsnachrichten für die Kommunikation mit IPv4-SNMP-Servern verwendet wird.
- **Erfasst IPv6-Quellschnittstelle**: Wählen Sie die Quellschnittstelle aus, deren IPv6-Adresse als Quell-IPv6-Adresse in Informationsnachrichten für die Kommunikation mit IPv6-SNMP-Servern verwendet wird.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Serverdefinition**: Wählen Sie aus, ob der Remote-Protokollserver anhand der IP-Adresse oder des Namens angegeben wird.
- **IP-Version**: Wählen Sie entweder IPv4 oder IPv6 aus.
- **IPv6-Adresstyp**: Wählen Sie den IPv6-Adresstyp aus (falls IPv6 verwendet wird). Folgende Optionen sind möglich:
  - *Link Local*: Die IPv6-Adresse kennzeichnet eindeutig Hosts mit einer einzigen Netzwerkverbindung. Link Local-Adressen besitzen das Präfix **FE80**, können nicht weitergeleitet und nur für die Kommunikation im lokalen Netzwerk verwendet werden. Es wird nur eine Link Local-Adresse unterstützt. Falls bei der Schnittstelle eine Link Local-Adresse vorhanden ist, ersetzt dieser Eintrag die Adresse in der Konfiguration.
  - *Global*: Bei der IPv6-Adresse handelt es sich um einen globalen Unicast-IPv6-Typ, der in anderen Netzwerken sichtbar und von diesen aus erreichbar ist.
- **Link Local-Schnittstelle**: Wählen Sie in der Pulldown-Liste die Link Local-Schnittstelle aus (falls der IPv6-Adresstyp „Link Local“ ausgewählt ist).

- **IP-Adresse des Empfängers**: Geben Sie die IP-Adresse oder den Namen des Servers ein, an den die Traps gesendet werden.
- **UDP-Port**: Geben Sie den UDP-Port ein, der beim Empfängergerät für Benachrichtigungen verwendet wird.
- **Benachrichtigungstyp**: Wählen Sie aus, ob Traps oder Informationen gesendet werden sollen. Falls beides benötigt wird, müssen zwei Empfänger erstellt werden.
- **Timeout**: Geben Sie an, wie lange (in Sekunden) das Gerät wartet, bis es die Informationen bzw. Traps erneut sendet. Timeout: Wertebereich 1 bis 300, Standard 15.
- **Wiederholungen**: Geben Sie an, wie oft das Gerät Informationsanforderungen erneut sendet. Wiederholungen: Wertebereich 1 bis 255, Standard 3.
- **Benutzername**: Wählen Sie in der Dropdown-Liste den Benutzer aus, an den SNMP-Benachrichtigungen gesendet werden. Um Benachrichtigungen zu empfangen, müssen Sie den Benutzer auf der Seite **SNMP-Benutzer** definieren und eine Remote-Engine-ID auswählen.
- **Sicherheitsstufe**: Wählen Sie aus, welches Maß an Authentifizierung auf das Paket angewendet wird.

  HINWEIS Die Sicherheitsstufe hängt vom ausgewählten Benutzernamen ab. Wenn für den Benutzernamen „Keine Authentifizierung“ konfiguriert ist, entspricht die Sicherheitsstufe nur „Keine Authentifizierung“. Wenn Sie dem Benutzernamen jedoch auf der Seite „Benutzer“ die Option „Authentifizierung und Datenschutz“ zugewiesen haben, kann die Sicherheitsstufe auf diesem Bildschirm „Keine Authentifizierung“, nur „Authentifizierung“ oder „Authentifizierung und Datenschutz“ lauten.

  Folgende Optionen sind möglich:

  - *Keine Authentifizierung*: Gibt an, dass das Paket weder authentifiziert noch verschlüsselt wird.
  - *Authentifizierung*: Gibt an, dass das Paket authentifiziert, aber nicht verschlüsselt wird.
  - *Datenschutz*: Gibt an, dass das Paket sowohl authentifiziert als auch verschlüsselt wird.
- **Benachrichtigungsfilter**: Hiermit können die SNMP-Benachrichtigungen, die an die Verwaltungsstation gesendet werden, nach dem Typ gefiltert werden. Die Filter werden auf der Seite „Benachrichtigungsfilter“ erstellt.
- **Filtername**: Wählen Sie den SNMP-Filter aus, der bestimmt, welche Informationen in Traps enthalten sein sollen (der Filter wird auf der Seite „Benachrichtigungsfilter“ definiert).

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Einstellungen für SNMP-Benachrichtigungsempfänger werden in die aktuelle Konfigurationsdatei geschrieben.

SNMP-Benachrichtigungsfilter

Auf der Seite „Benachrichtigungsfilter“ können Sie SNMP-Benachrichtigungsfilter und zu überprüfende Objekt-IDs (OIDs) konfigurieren. Wenn Sie einen Benachrichtigungsfilter erstellt haben, können Sie diesen auf den Seiten „Benachrichtigungsempfänger SNMPv1, 2“ und „Benachrichtigungsempfänger SNMPv3“ mit einem Benachrichtigungsempfänger verknüpfen.

Mithilfe des Benachrichtigungsfilters kann der Typ von SNMP-Benachrichtigungen herausgefiltert werden, die an die Verwaltungsstation gesendet werden sollen. Dies geschieht auf Grundlage der OID der zu sendenden Benachrichtigung.

So legen Sie einen Benachrichtigungsfilter fest:

SCHRITT 1 Klicken Sie auf **SNMP** > **Benachrichtigungsfilter**.

Die Seite „Benachrichtigungsfilter“ enthält Benachrichtigungsinformationen für die einzelnen Filter. In der Tabelle können Benachrichtigungseinträge nach dem Filternamen gefiltert werden.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie die Parameter ein.

- **Filtername**: Geben Sie einen Namen ein, der aus 0 - 30 Zeichen besteht.
- **Objekt-ID-Unterstruktur**: Wählen Sie den Knoten innerhalb der MIB-Struktur aus, der in den ausgewählten SNMP-Filter eingeschlossen oder von ihm ausgeschlossen werden soll. Für die Auswahl des Objekts bestehen folgende Optionen:
  - *Aus Liste auswählen*: Hiermit können Sie in der MIB-Struktur navigieren. Klicken Sie auf den *Nach-Oben*-Pfeil, um zur Ebene der übergeordneten und gleichrangigen Elemente des ausgewählten Knotens zu gelangen; klicken Sie auf den *Nach-Unten*-Pfeil, um zur Ebene der untergeordneten Objekte des ausgewählten Knotens zu gelangen. Klicken Sie auf einen Knoten der Ansicht, um zu einem anderen gleichrangigen Knoten zu gelangen. Mit der Scrollleiste können Sie gleichrangige Knoten in den sichtbaren Bereich bewegen.
  - Wenn Sie die Option *Objekt-ID* verwenden, wird die **eingegebene Objekt-ID** in die Ansicht eingeschlossen, je nachdem, ob Sie die Option **In Filter einschließen** ausgewählt haben.

SCHRITT 4 Wählen Sie die Option **In Filter einschließen** aus oder heben Sie deren Auswahl auf. Wenn diese Option ausgewählt ist, sind die ausgewählten MIBs im Filter enthalten, anderenfalls sind sie nicht enthalten.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die SNMP-Ansichten werden definiert und die aktuelle Konfiguration wird aktualisiert.