ADMINISTRATOR-
HANDBUCH

Administratorhandbuch für Managed Switches der Serie 300 von Cisco Small Business

Inhaltsverzeichnis

1

Erste Schritte

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

- **Starten des webbasierten Switch-Konfigurationsdienstprogramms**
- **Kurzanleitung für die Switch-Konfiguration**
- **Benennungskonventionen für Schnittstellen**
- **Fensternavigation**

Starten des webbasierten Switch-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.

Für Browser gelten die folgenden Einschränkungen:

- Wenn Sie eine ältere Version von Internet Explorer verwenden, können Sie nicht über eine IPv6-Adresse direkt auf den Switch zugreifen. Sie können jedoch den DNS-Server (Domain Name System) einsetzen, um einen Domänennamen mit der IPv6-Adresse zu erstellen, und dann diesen Domänennamen in der Adresszeile anstelle der IPv6-Adresse verwenden.
- 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 den Switch 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 Switch in die Adresszeile des Browsers ein, und drücken Sie die **Eingabetaste**. Die Seite *Anmeldung* wird geöffnet.

HINWEIS Wenn der Switch die werkseitig konfigurierte Standard-IP-Adresse 192.168.1.254 verwendet, blinkt die Betriebs-LED ununterbrochen. Wenn der Switch 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 Switch konfiguriert sind. Wenn der Browser beispielsweise Chinesisch anfordert und Chinesisch im Switch geladen ist, wird die Anmeldeseite automatisch auf Chinesisch angezeigt. Wenn Chinesisch im Switch nicht geladen ist, wird die Anmeldeseite auf Englisch angezeigt.

Die im Switch 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 Switch 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 im

Abschnitt **Einrichten der Kennwortkomplexitätsregeln** im Kapitel **Konfigurieren der Sicherheitsfunktionen** beschrieben.

SCHRITT 2 Wenn Sie nicht Englisch als Sprache verwenden, wählen Sie im Dropdown-Menü *Language* die gewünschte Sprache aus. Im Abschnitt *Firmware/Sprache aktualisieren/sichern* erfahren Sie, wie Sie eine neue Sprache für den Switch 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 *Ändern des Kennworts* geöffnet. Weitere Informationen hierzu finden Sie unter *Kennwort-Ablaufzeit*.

SCHRITT 4 Wählen Sie aus, ob die **Erzwingung der Kennwortkomplexität** deaktiviert werden soll. Weitere Informationen zur Kennwortkomplexität finden Sie im 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 Seite *Anmeldung* angezeigt.

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 *Systemzusammenfassung* 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.

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

Kennwort-Ablaufzeit

Die Seite *Neues Kennwort* wird angezeigt:

- Wenn Sie sich zum ersten Mal bei dem Switch anmelden, verwenden Sie den Standardbenutzernamen **cisco** und das Standardkennwort **cisco**. Es ist erforderlich, dass Sie das werksmäßig 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 diesen Standardwert gemäß der Beschreibung im Abschnitt **Definieren des Timeouts für Sitzungsleerlauf** im Kapitel **Allgemeine Verwaltungsinformationen und -aufgaben ändern**.

VORSICHT Wenn die aktuelle Konfiguration nicht in die Startkonfiguration kopiert wird, gehen beim Neustarten des Switch 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 die Schaltfläche **Blinkendes Speichersymbol deaktivieren** auf der Seite **Konfiguration kopieren/speichern** klicken.

Wenn der Switch automatisch ein Gerät (beispielsweise ein IP-Telefon) erkennt (siehe **Kapitel 10, „Was ist ein Smartport?“**), konfiguriert er den Port entsprechend für das Gerät. Diese Konfigurationsbefehle werden in die aktuelle Konfigurationsdatei geschrieben. Aus diesem Grund beginnt das Speichersymbol bei Ihrer Anmeldung zu blinken, obwohl 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 Switch ab.

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

Die angezeigte Anfangsseite ist von der Option "Diese Seite beim Starten nicht anzeigen" auf der Seite *Erste Schritte* abhängig. Wenn Sie diese Option nicht aktiviert haben, ist die Anfangsseite die Seite *Erste Schritte*. Wenn Sie diese Option aktiviert haben, ist die Anfangsseite die Seite *Systemzusammenfassung*.

Kurzanleitung für die Switch-Konfiguration

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

Links auf der Seite "Erste Schritte"

Kategorie	Link-Name (auf der Seite)	Verlinkte Seite
	Verwaltungsanwendungen und -services ändern	Seite *TCP/UDP-Services*
	Geräte-IP-Adresse ändern	Seite *IPv4-Schnittstelle*
	VLAN erstellen	Seite *VLAN erstellen*
	Porteinstellungen konfigurieren	Seite *Porteinstellungen*
Gerätestatus	Systemzusammenfassung	Seite *Systemzusammenfassung*
	Anschlussstatistik	Seite *Schnittstelle*
	RMON-Statistik	Seite *Statistik*
	Protokoll anzeigen	Seite *RAM-Speicher*
Schnellzugriff	Gerätekennwort ändern	Seite *Benutzerkonten*
	Gerätesoftware aktualisieren	Seite *Firmware/Sprache aktualisieren/sichern*

Links auf der Seite "Erste Schritte" (Fortsetzung)

Kategorie	Link-Name (auf der Seite)	Verlinkte Seite
	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 Switch-Produkte, 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.
  - **LAG (Port-Channel)**: Für diese wird **LAG** angezeigt.
  - **VLAN**: Für diese wird **VLAN** angezeigt.
  - **Tunnel**: Für diese wird **Tunnel** angezeigt.
- **Schnittstellennummer: Port, LAG Tunnel oder VLAN-ID**

Fensternavigation

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

Anwendungsheader

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

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 die Startkonfigurationdatei des Switch kopieren. Nach dem Speichervorgang werden das rote X und der Link zum Speichern nicht mehr angezeigt. Beim Neustart des Switch wird der Startkonfigurations-Dateityp in die aktuelle Konfiguration kopiert und die Switch-Parameter werden entsprechend den Daten in der aktuellen Konfiguration festgelegt.
Benutzername	Zeigt den Namen des beim Switch angemeldeten Benutzers an. Der Standardbenutzername lautet **cisco**. (Das Standardkennwort lautet **cisco**).

Anwendungslinks (Fortsetzung)

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:** Fügen Sie dem Switch eine neue Sprache hinzu. ▪ **Sprache löschen:** Löscht die zweite Sprache aus dem Switch. 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** Zum Aktualisieren einer Sprachdatei verwenden Sie die Seite *Firmware/Sprache aktualisieren/sichern*.
Abmelden	Klicken Sie auf diese Schaltfläche, um sich vom webbasierten Switch-Konfigurationsdienstprogramm abzumelden.
Info	Zeigt den Switch-Namen und die Switch-Versionsnummer an.
Hilfe	Zeigt die Online-Hilfe an.

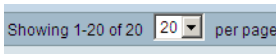
Anwendungslinks (Fortsetzung)

Anwendungslink-Name	Beschreibung
	Das Symbol für den Syslog-Alarmstatus wird angezeigt, wenn eine Syslog-Nachricht 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.

Verwaltungsschaltflächen

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 Startkonfigurations-Dateityp des Switch zu speichern.

Verwaltungsschaltflächen (Fortsetzung)

Schaltflächenname	Beschreibung
Übernehmen	Klicken Sie auf diese Schaltfläche, um die Änderungen in die ausgeführte Konfiguration des Switch zu übernehmen. Wird der Switch neu gestartet, geht die aktuelle Konfiguration verloren, sofern diese nicht im Startkonfigurations-Dateityp oder in einem anderen Dateityp gespeichert wird. Klicken Sie auf **Speichern**, um die Seite *Konfiguration kopieren/speichern* anzuzeigen und die aktuelle Konfiguration im Startkonfigurations-Dateityp des Switch 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.
Schließen	Ruft die Hauptseite auf. Wenn Änderungen vorhanden sind, die nicht in die aktuelle Konfiguration übernommen wurden, wird eine Meldung angezeigt.

Verwaltungsschaltflächen (Fortsetzung)

Schaltflächenname	Beschreibung
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.
Testen	Klicken Sie auf **Testen**, um die entsprechenden Tests auszuführen.

2

Anzeigen von Statistiken

In diesem Abschnitt wird beschrieben, wie Sie Statistiken für den Switch anzeigen.

Die folgenden Themen werden behandelt:

- **Anzeigen der Ethernet-Schnittstellen**
- **Anzeigen der Etherlike-Statistik**
- **Anzeigen der GVRP-Statistik**
- **Anzeigen der 802.1X EAP-Statistik**
- **Anzeigen der TCAM-Auslastung**
- **Verwalten von RMON**

Anzeigen der Ethernet-Schnittstellen

Auf der Seite *Schnittstelle* werden für jeden Port Verkehrsstatistiken 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**. Die Seite *Schnittstelle* wird angezeigt.

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. 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.

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:

- Klicken Sie auf **Schnittstellenzähler löschen**, um die Zähler für die angezeigte Schnittstelle zu löschen.
- Klicken Sie auf **Alle Schnittstellenzähler löschen**, um die Zähler für alle Schnittstellen zu löschen.

Anzeigen der Etherlike-Statistik

Auf der Seite *Etherlike* werden Statistiken pro 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**. Die Seite *Etherlike* wird angezeigt.

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 Empfängerfehler 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 Zähler für die ausgewählte Schnittstelle zu löschen.
- Klicken Sie auf **Alle Schnittstellenzähler löschen**, um die Zähler für alle Schnittstellen zu löschen.

Anzeigen der GVRP-Statistik

Auf der Seite *GVRP* werden Informationen zu Frames des GARP VLAN-Registrierungsprotokolls (GVRP) angezeigt, die von einem Port gesendet oder an diesem 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 hierzu 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**. Die Seite *GVRP* wird angezeigt.

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 Seite *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 Schnittstellenzähler löschen**, um die Zähler für alle Schnittstellen zu löschen.

Anzeigen der 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**. Die Seite *802.1x EAP* wird angezeigt.

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

SCHRITT 3 Legen Sie den Zeitraum (**Aktualisierungsrate**) fest, 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 Zähler für die ausgewählte Schnittstelle zu löschen.
- Klicken Sie auf **Alle Schnittstellenzähler löschen**, um die Zähler für alle Schnittstellen zu löschen.

Anzeigen der TCAM-Auslastung

Die Switch-Architektur nutzt einen TCAM-Speicher (Ternary Content Addressable Memory), um Paketaktionen mit Wire-Speed zu ermöglichen.

Im TCAM sind die von anderen Anwendungen erzeugten Regeln gespeichert, beispielsweise Zugriffssteuerungslisten (Access Control Lists, ACLs), QoS-Regeln (Quality of Service) und von Benutzern erstellte Regeln. Von allen Anwendungen des Geräts können maximal 512 Anwendungen zugewiesen werden.

Manche 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 Seite *TCAM-Auslastung* wird angezeigt. Sie zeigt den Prozentsatz der TCAM-Auslastung des Systems sowie die maximalen TCAM-Einträge an.

Verwalten von RMON

Die SNMP-Spezifikation RMON (Remote Networking Monitoring) ermöglicht es einem SNMP-Agenten im Switch, zu vorbeugenden Zwecken für einen bestimmten Zeitraum eine Verkehrsstatistik zu pflegen und Traps an einen SNMP-Manager zu 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 reduziert den Verkehr zwischen Manager und Switch, da der SNMP-Manager den Switch nicht so oft abfragen muss, weil dieser vom Switch bei Ereignissen rechtzeitig Statusmeldungen erhält.

Mit dieser Funktion können Sie die folgenden Aktionen ausführen:

- Sie können die aktuelle Statistik (seit 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.

Anzeigen der 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**. Die Seite *Statistik* wird angezeigt.

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.

Es wird die Statistik für die ausgewählte Schnittstelle angezeigt.

- **Empfangene Bytes (Oktette)**: Die Anzahl der empfangenen Oktette, einschließlich fehlerhafter Pakete und FCS-Oktette jedoch ausschließlich Frame-Bits.
- **Drop-Ereignisse**: Die Anzahl der gelöschten Pakete.
- **Empfangene Pakete**: Die Zahl der empfangenen gültigen Pakete, einschließlich Multicast- und Broadcast-Paketen.
- **Empfangene Broadcast-Pakete**: Die Zahl der fehlerfrei empfangenen Broadcast-Pakete. Multicast-Pakete sind hier nicht enthalten.
- **Empfangene Multicast-Pakete**: Die Zahl der fehlerfrei empfangenen Multicast-Pakete.
- **CRC- & Ausrichtungsfehler**: Die Zahl der aufgetretenen CRC- und Ausrichtungsfehler.
- **Zu kleine Pakete**: Die Zahl der empfangenen Pakete mit unzureichender Größe (weniger als 64 Oktette).
- **Zu große Pakete**: Die Zahl der empfangenen Pakete mit unzulässiger Größe (mehr als 2000 Oktette).
- **Fragmente**: Die Zahl der empfangenen Fragmente (Pakete mit weniger als 64 Oktetten, ausschließlich Frame-Bits aber einschließlich FCS-Oktette).
- **Jabber**: Die Gesamtzahl der empfangenen Pakete, die mehr als 1632 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). 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 Zahl der empfangenen Kollisionen. Wenn Jumbo Frames aktiviert sind, wird der Schwellenwert für die Jabber Frames auf die maximale Jumbo Frame-Größe erweitert.
- **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 - 127 Byte.
- **Frames mit 128 bis 255 Byte**: Die Zahl der empfangenen Frames mit 128 - 255 Byte.
- **Frames mit 256 bis 511 Byte**: Die Zahl der empfangenen Frames mit 256 - 511 Byte.
- **Frames mit 512 bis 1023 Byte**: Die Zahl der empfangenen Frames mit 512 - 1023 Byte.
- **Frames mit mehr als 1024 Byte**: Die Zahl der empfangenen Frames mit 1024 - 2000 Byte sowie Jumbo-Frames.

So löschen Sie Statistikzähler:

- Klicken Sie auf **Schnittstellenzähler löschen**, um die Zähler für die ausgewählte Schnittstelle zu löschen.
- Klicken Sie auf **Alle Schnittstellenzähler löschen**, um die Zähler für alle Schnittstellen zu löschen.

Konfigurieren des RMON-Verlaufs

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.

Nach der Datenerfassung und -speicherung werden die Daten auf der Seite *Verlaufstabelle* angezeigt, die Sie durch Klicken auf **Verlaufstabelle** anzeigen.

So geben Sie RMON-Steuerungsinformationen ein:

SCHRITT 1 Wählen Sie **Status und Statistik** > **RMON** > **Verlauf**. Die Seite *Verlaufssteuerungstabelle* wird angezeigt. 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 es kann die Zahl der Stichproben pro Anforderung beschränkt werden. 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**. Die Seite *RMON-Verlauf hinzufügen* wird angezeigt.

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**, um die eigentliche Statistik anzuzeigen.

Anzeigen der 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**. Die Seite *Verlauf* wird angezeigt.

SCHRITT 2 Klicken Sie auf **Verlaufstabelle**. Die Seite *Verlaufssteuerungstabelle* wird angezeigt.

SCHRITT 3 Klicken Sie auf **Verlaufstabelle**, um zur Seite *Verlaufstabelle* zu gehen.

SCHRITT 4 Wählen Sie in der Liste **Verlaufseintrags-Nr.** 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.

Definieren der 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**. Die Seite *Ereignisse* wird angezeigt.

Auf dieser Seite werden vordefinierte Ereignisse angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *RMON-Ereignisse hinzufügen* wird angezeigt.

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 (optional).

- **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.
- **Uhrzeit**: Der Zeitpunkt des Ereignisses. (Hierbei handelt es sich um eine schreibgeschützte Tabelle im übergeordneten Fenster, die nicht definiert werden kann).
- **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 die aktuelle Konfigurationsdatei geschrieben.

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

Anzeigen der 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 des Alarms eingetreten sind.

SCHRITT 1 Klicken Sie auf **Status und Statistik > RMON** > **Ereignisse**. Die Seite *Ereignisse* wird angezeigt.

SCHRITT 2 Klicken Sie auf **Ereignisprotokolltabelle.** Die Seite *Ereignisprotokolltabelle* wird angezeigt.

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.

Definieren von RMON-Alarmen

RMON-Alarme bieten die Möglichkeit, Schwellenwerte und Stichprobenintervalle festzulegen, um Ausnahmeereignisse für beliebige 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.

Auf der Seite *Alarme* haben Sie die Möglichkeit, Alarme zu konfigurieren und diese mit Ereignissen zu verbinden. 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**. Die Seite *Alarme* wird angezeigt. Alle bereits definierten Alarme werden angezeigt. Die Felder werden unten auf der Seite *RMON-Alarm hinzufügen* beschrieben. Zusätzlich zu diesen Feldern wird das folgende Feld angezeigt:

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

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *RMON-Alarm hinzufügen* wird angezeigt.

SCHRITT 3 Geben Sie die Parameter ein.

- **Alarmeintrag**: 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.
- **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 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 erstellen Sie auf der Seite *Ereignisse*.
- **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 die aktuelle Konfigurationsdatei geschrieben.

3

Verwalten von Systemprotokollen

In diesem Abschnitt wird die Funktion für Systemprotokolle beschrieben, über die der Switch verschiedene unabhängige Protokolle generieren kann. Die einzelnen Protokolle enthalten Meldungen, die Systemereignisse beschreiben.

Der Switch generiert die folgenden lokalen Protokolle:

- An die Konsolenschnittstelle gesendete Protokolle.
- Protokolle, die in eine zyklische Liste protokollierter Ereignisse in das RAM geschrieben und bei einem Switch-Neustart 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 Nachrichten in Form von SNMP-Traps und Syslog-Nachrichten an Syslog-Remote-Server senden.

In diesem Abschnitt werden die folgenden Themen behandelt:

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

Festlegen der Systemprotokolleinstellungen

Auf der Seite *Protokolleinstellungen* können Sie die Protokollierung aktivieren oder deaktivieren und auswählen, ob Protokollmeldungen aggregiert werden.

Sie können Ereignisse nach Schweregrad auswählen. Für jede Protokollmeldung ist ein Schweregrad angegeben. Die Angabe erfolgt den ersten Buchstabens 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**. Die Seite *Protokolleinstellungen* wird geöffnet.

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.
- **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.

Einstellen der Remote-Protokollierung

Auf der Seite *Remote-Protokoll-Server* können Sie Syslog-Remote-Server definieren, an die Protokollmeldungen gesendet werden (mit dem Syslog-Protokoll). 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**. Die Seite *Remote-Protokoll-Server* wird geöffnet.

Auf dieser Seite wird eine Liste der Remote-Protokoll-Server angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *Remote-Protokoll-Server hinzufügen* wird geöffnet.

SCHRITT 3 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 4 Klicken Sie auf **Übernehmen**. Die Seite *Remote-Protokoll-Server hinzufügen* wird geschlossen, der Syslog-Server wird hinzugefügt und die aktuelle Konfigurationsdatei wird aktualisiert.

Anzeigen von Speicherprotokollen

Der Switch kann Meldungen in die folgenden 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 Nachrichten 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**. Die Seite *RAM-Speicher* wird geöffnet.

Oben auf der Seite wird eine Schaltfläche angezeigt, mit der Sie das blinkende Alarmsymbol deaktivieren können. Klicken Sie auf die Schaltfläche, um zwischen Deaktivieren und Aktivieren zu wechseln.

Auf dieser Seite werden folgende Felder angezeigt:

- **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.

Flash-Speicher

Auf der Seite *Flash-Speicher* werden die im Flash-Speicher abgelegten Nachrichten in chronologischer Reihenfolge angezeigt. Den Mindestschweregrad für die Protokollierung können Sie auf der Seite *Protokolleinstellungen* konfigurieren. Flash-Protokolle bleiben auch bei einem Switch-Neustart erhalten. Sie können die Protokolle manuell löschen.

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

Auf dieser Seite werden folgende Felder angezeigt:

- **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.

4

Verwalten von Systemdateien

In diesem Abschnitt wird die Verwaltung der Systemdateien beschrieben.

Folgende Themen werden behandelt:

- **Systemdateitypen**
- **Firmware/Sprache aktualisieren/sichern**
- **Auswählen des aktiven Image**
- **Herunterladen oder Sichern einer Konfiguration oder eines Protokolls**
- **Anzeigen von Konfigurationsdateieigenschaften**
- **Kopieren von Konfigurationsdateien**
- **Automatische DHCP-Konfiguration**

Systemdateitypen

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

Für diese Dateien können Sie verschiedene Aktionen ausführen, beispielsweise Auswählen der Firmwaredatei, von der der Switch gestartet wird, internes Kopieren verschiedener Arten von Konfigurationsdateien im Switch 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: Verwendet die Funktionen des Browsers.
- TFTP/SCP-Client: Erfordert einen TFTP/SCP-Server.

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

Wenn eine Konfiguration für den Switch referenziert wird, erfolgt die Referenzierung anhand des *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

Der Switch verfügt über die folgenden Typen von Konfigurations- und Betriebsdateien:

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

  Wird der Switch neu gestartet, geht die aktuelle Konfiguration verloren. Die Startkonfiguration im Flash-Speicher überschreibt die im RAM gespeicherte aktuelle Konfiguration.

  Damit am Switch vorgenommene Änderungen 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 Switch-Neustart erhalten. Dabei wird die Startkonfiguration in das RAM kopiert und als aktuelle Konfiguration identifiziert.

- **Spiegelkonfiguration**: Eine Kopie der Startkonfiguration, die der Switch in folgenden Fällen erstellt:
  - Der Switch 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 Switch 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 zurzeit verwendeten Firmware-Images oder Auswählen des beim nächsten Neustart verwendeten Images, wie im Abschnitt **Auswählen des aktiven Image** beschrieben.
- Speichern von Konfigurationsdateien auf dem Switch in einem Speicherort auf einem anderen Gerät, wie im Abschnitt **Herunterladen oder Sichern einer Konfiguration oder eines Protokolls** beschrieben.
- Löschen der Dateitypen "Startkonfiguration" oder "Sicherungskonfiguration", wie im Abschnitt **Anzeigen von Konfigurationsdateieigenschaften** beschrieben.
- Kopieren eines Konfigurationsdateityps in einen anderen Konfigurationsdateityp gemäß der Beschreibung im Abschnitt **Kopieren von Konfigurationsdateien**.
- Aktivieren des automatischen Uploads einer Konfigurationsdatei von einem DHCP-Server auf den Switch gemäß der Beschreibung im Abschnitt **Automatische DHCP-Konfiguration**.

In diesem Abschnitt werden die folgenden Themen behandelt:

- **Firmware/Sprache aktualisieren/sichern**
- **Auswählen des aktiven Image**
- **Herunterladen oder Sichern einer Konfiguration oder eines Protokolls**
- **Anzeigen von Konfigurationsdateieigenschaften**
- **Kopieren von Konfigurationsdateien**
- **Automatische DHCP-Konfiguration**

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.
- SCP: Erfordert einen SCP-Server.

Wenn eine neue Sprachdatei in den Switch geladen wurde, kann die neue Sprache im Dropdown-Menü ausgewählt werden. (Es ist nicht erforderlich, den Switch neu zu starten.)

Im Switch 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 den Switch wird dieser weiterhin mit dem aktiven Image (der alten Version) gestartet, bis Sie das neue Image anhand der im Abschnitt **Auswählen des aktiven Image** beschriebenen Vorgehensweise als aktives Image festlegen. Starten Sie dann den Switch.

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**. Die Seite *Firmware/Sprache aktualisieren/sichern* wird geöffnet.

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 Aktionen aus:

- **Speichermethode "Aktualisieren"**: Gibt an, dass der Dateityp auf dem Switch durch eine neue Version dieses Dateityps ersetzt werden soll, die sich auf einem TFTP-Server befindet.
- **Speichermethode "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 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 (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 Domänennamen 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, ist nur die Option **Aktualisieren** möglich. Geben Sie die Parameter gemäß der Beschreibung in diesem Schritt ein.

- **Dateityp**: Wählen Sie den Typ der Konfigurationsdatei aus. Es können nur gültige Dateitypen ausgewählt werden. (Die Dateitypen werden im Abschnitt **Dateien und Dateitypen** beschrieben). Die folgenden Dateitypen können aktualisiert werden:
  - *Firmware-Image*: Wählen Sie diese Option aus, um das Firmware-Image zu aktualisieren.
  - *Sprache*: 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 **Verwenden der SSH-Clientfunktion** 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-Benutzerauthentifizierung**, um eine SSH-Benutzerauthentifizierungsmethode (Kennwort oder öffentlicher/privater Schlüssel) auszuwählen, einen Benutzernamen und ein Kennwort für den Switch 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 gehen, 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.

- **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 SSH-Serverauthentifizierung aktiviert ist (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.

Auswählen des aktiven Image

Im Switch sind zwei Firmware-Images gespeichert. Eines der Images ist das *aktive Image*, das andere ist das *inaktive Image*. Der Switch startet mit dem Image, das Sie als *aktives Image* festlegen. Sie können das *inaktive Image* als *aktives Image* festlegen. (Sie können den Switch wie in Abschnitt **Neustarten des Switch** beschrieben neu starten.)

So wählen Sie das aktive Image aus:

SCHRITT 1 Wählen Sie **Administration** > **Dateiverwaltung** > **Aktives Image**. Die Seite *Aktives Image* wird geöffnet.

Auf dieser Seite wird Folgendes angezeigt:

- **Aktives Image**: Zeigt die derzeit aktive Image-Datei auf dem Switch 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 Firmware-Version 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 Switch 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 Switch verwendet wird.

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

Herunterladen oder Sichern einer Konfiguration oder eines Protokolls

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

- Sichern von Konfigurationsdateien oder Protokollen vom Switch in einem externen Gerät.
- Wiederherstellen von Konfigurationsdateien von einem externen Gerät im Switch.

HINWEIS

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 Wiederherstellung in einer Startkonfiguration durchführen, müssen Sie den Switch neu starten, damit die wiederhergestellte Startkonfiguration als ausgeführte Konfiguration verwendet wird. Sie können den Switch wie in Abschnitt **Konsoleneinstellungen (Unterstützung für automatische Baudrate)** beschrieben neu starten.

So sichern Sie die Systemkonfigurationsdatei oder stellen diese wieder her:

SCHRITT 1 Klicken Sie auf **Administration** > **Dateiverwaltung** > **Konfiguration/Protokoll herunterladen/sichern**. Die Seite *Konfiguration/Protokoll herunterladen/sichern* wird geöffnet.

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.

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

a. **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. **TFTP-Server**: Geben Sie die IP-Adresse 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).

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

a. **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 Domänennamen 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-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 für **Speichermethode** die Option *Herunterladen* auswählen (Ersetzen der Datei im Switch 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 den Switch 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-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 **Verwenden der SSH-Clientfunktion** 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. Verwenden Sie die Seite **SSH-Serverauthentifizierung**, um eine SSH-Benutzerauthentifizierungsmethode (Kennwort oder öffentlicher/privater Schlüssel) auszuwählen, einen Benutzernamen und ein Kennwort für den Switch 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:

- **SSH-Client verwenden**: Legt permanente SSH-Benutzeranmeldeinformationen fest. Klicken Sie auf **Systemanmeldeinformationen**, um zur Seite *SSH-Benutzerauthentifizierung* zu gehen, 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.
- **SCP-Serverdefinition**: Wählen Sie aus, ob der TFTP-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 TFTP-Servers ein.

Wenn Sie für **Speichermethode** die Option *Herunterladen* auswählen (Ersetzen der Datei im Switch durch eine neue Version von einem anderen Gerät), geben Sie Werte für die folgenden 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-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.

Anzeigen von Konfigurationsdateieigenschaften

Auf der Seite *Konfigurationsdateieigenschaften* können Sie sehen, wann verschiedene Systemkonfigurationsdateien erstellt wurden. Außerdem können Sie die Startkonfigurationsdatei und die Backup-Konfigurationsdatei löschen. Die anderen Konfigurationsdateitypen können Sie nicht löschen.

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**. Die Seite *Konfigurationsdateieigenschaften* wird geöffnet.

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 **Systemdateitypen**.

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.

Auf dieser Seite sind die folgenden Felder verfügbar:

- **Name der Konfigurationsdatei**: Zeigt den Dateityp an.
- **Erstellungszeit**: Zeigt das Datum und die Uhrzeit der letzten Dateibearbeitung an.

Kopieren von Konfigurationsdateien

Wenn Sie in einem Fenster auf **Übernehmen** klicken, werden Ihre Änderungen an den Switch-Konfigurationseinstellungen *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 ausgeführte Konfiguration nicht in die Startkonfiguration oder in eine andere Konfigurationsdatei kopieren, gehen alle Änderungen seit dem letzten Speichern der Datei verloren, wenn der Switch 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 Backup-Konfiguration.
- Kopieren aus der Backup-Konfiguration in die Startkonfiguration.
- Kopieren aus der Spiegelkonfiguration in die Startkonfiguration oder Backup-Konfiguration.

So kopieren Sie einen Konfigurationsdateityp in einen anderen Konfigurationsdateityp:

SCHRITT 1 Wählen Sie **Administration** > **Dateiverwaltung** > **Konfiguration kopieren/speichern**. Die Seite *Konfiguration kopieren/speichern* wird geöffnet.

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.

- Wenn Sie eine Konfigurationsdatei sichern, 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-Regeln**.

SCHRITT 4 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 5 Klicken Sie auf **Übernehmen**. Die Datei wird kopiert.

Automatische DHCP-Konfiguration

Der Switch unterstützt mit der automatischen DHCP-Konfiguration eine Möglichkeit, Konfigurationsinformationen (einschließlich der IP-Adresse eines TFTP oder SCP-Servers und eines Dateinamens) an Hosts in einem TCP/IP-Netzwerk zu übertragen. Auf der Grundlage dieses Protokolls kann ein Switch mit der Funktion für die automatische Konfiguration Konfigurationsdateien von einem TFTP/SCP-Server herunterladen.

Standardmäßig ist der Switch als DHCP-Client konfiguriert, wenn die Funktion für die automatische Konfiguration aktiviert ist.

Die automatische Konfiguration unterstützt außerdem das Herunterladen einer Konfigurationsdatei ohne sensible Informationen oder einer Konfigurationsdatei mit sensiblen Informationen (beispielsweise TACACS+-Schlüssel und SSH/SSL-Schlüssel mit dem SCP-Protokoll (Secured Copy Protocol)).

Auslösen der automatischen DHCP-Konfiguration

Der automatische Konfigurationsprozess wird in folgenden Fällen ausgelöst:

- Nach dem Neustart, wenn eine IP-Adresse dynamisch zugewiesen oder erneuert wird (über DHCP).
- Bei einer expliziten DHCP-Erneuerungsanforderung und wenn Switch und Server entsprechend konfiguriert sind.
- Bei der automatischen Erneuerung der DHCP-Lease.

Servername/-adresse

Sie können die IP-Adresse oder den Namen des TFTP/SCP-Servers angeben. Dieser Server wird verwendet, wenn in der DHCP-Nachricht keine Server-IP-Adresse angegeben wurde. Diese DHCP-Nachricht ist die vom DHCP-Server stammende DHCP-Angebotsnachricht. Mögliche Optionen: BOOTP-Optionen "sname" und "siaddr" und DHCP-Option 150 oder 66. Dies ist ein optionaler Parameter.

Name der Backup-Konfigurationsdatei

Sie können den Namen der Backup-Konfigurationsdatei angeben. Diese Datei wird verwendet, wenn in der DHCP-Nachricht kein Dateiname angegeben wurde. Dies ist ein optionaler Parameter.

Downloadprotokoll für die automatische Konfiguration

Das Downloadprotokoll für die automatische Konfiguration kann wie folgt konfiguriert werden:

Automatisch nach Dateierweiterung: Wenn diese Option ausgewählt ist, können Sie eine Dateierweiterung angeben (die standardmäßige Dateierweiterung ist ".scp"). Dateien mit der angegebenen Dateierweiterung werden mit SCP (über SSH) heruntergeladen, während Dateien mit anderen Erweiterungen mit 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. Der Standardwert lautet "Automatisch nach Dateierweiterung".

- **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-Clientauthentifizierungsparameter

Da die SSH-Remoteserverauthentifizierung standardmäßig deaktiviert ist, akzeptiert das Gerät im Auslieferungszustand jeden SSH-Remoteserver. Sie können die SSH-Remoteserverauthentifizierung aktivieren, um nur Verbindungen von Servern in der Liste der vertrauenswürdigen Server zuzulassen.

SSH-Clientauthentifizierungsparameter sind erforderlich für den Zugriff des Clients (des Switch) auf den SSH-Server. 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 (ein Download, der nicht über die Funktion für die automatische DHCP-Konfiguration ausgeführt wird).

Automatischer Konfigurationsprozess

Wenn ein automatischer Konfigurationsprozess ausgelöst wird, tritt die folgende Ereignissequenz auf:

- Es wird auf den DHCP-Server zugegriffen, um die IP-Adresse des TFTP/SCP-Servers und den Namen der Konfigurationsdatei zu beziehen. Diese Parameter werden an die DHCP-Optionsparameter übergeben.
- Wenn der DHCP-Server keine IP-Adresse bereitgestellt hat, wird die Adresse des Backup-Servers verwendet (falls vom Benutzer konfiguriert).
- Wenn der DHCP-Server die IP-Adresse nicht bereitgestellt hat und der Parameter für die Adresse des Backup-TFTP/SCP-Servers leer ist, wird der automatische Konfigurationsprozess angehalten.

  HINWEIS Bei den beiden vorherigen Aufzählungspunkten ist mit IP-Adresse die IP-Adresse bzw. der Hostname des TFTP- oder SCP-Servers gemeint.

- Wenn der Konfigurationsdateiname vom DHCP-Server bereitgestellt wurde, wird das Kopierprotokoll (SCP/TFTP) gemäß der Beschreibung unter **Automatische DHCP-Konfiguration** ausgewählt.
- 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. Beachten Sie, dass die SSH-Serverauthentifizierung standardmäßig deaktiviert ist, damit Konfigurationsdateien für Geräte mit werkseitiger Standardkonfiguration heruntergeladen werden können (beispielsweise Geräte im Auslieferungszustand).

- 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 vom DHCP-Server kein Konfigurationsdateiname bereitgestellt wurde, wird der Name der Backup-Konfigurationsdatei verwendet.
- Wenn der Konfigurationsdateiname nicht vom DHCP-Server bereitgestellt wurde und der Name der Backup-Konfigurationsdatei leer ist, wird der automatische Konfigurationsprozess angehalten.
- Es wird auf den TFTP/SCP-Server zugegriffen, um die Datei dort herunterzuladen.

  Der Downloadprozess wird nur ausgeführt, wenn sich der neue Konfigurationsdateiname vom aktuellen Konfigurationsdateinamen unterscheidet (auch wenn die aktuelle Konfigurationsdatei leer ist).
- Es wird eine Syslog-Nachricht generiert, in der bestätigt wird, dass der automatische Konfigurationsprozess abgeschlossen ist.

Automatischer Konfigurationsprozess mit Werkseinstellungen

Die automatische Konfiguration mit und ohne sensible Daten wird für Geräte im Auslieferungszustand mit Werkseinstellungen unterstützt. Der Downloadprozess wird im Dokument zur Verwaltung sensibler Daten beschrieben.

Konfigurieren der automatischen DHCP-Konfiguration

Auf der Seite *Automatische DHCP-Konfiguration* können Sie die folgenden Aktionen ausführen, wenn die Informationen nicht in einer DHCP-Nachricht bereitgestellt werden:

- Aktivieren der Funktion für die automatische DHCP-Konfiguration.
- Angeben des Downloadprotokolls.
- Konfigurieren des Switch für den Empfang von Konfigurationsinformationen aus einer bestimmten Datei auf einem bestimmten Server.

Beachten Sie folgende Einschränkungen für die automatische DHCP-Konfiguration:

- 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 die ordnungsgemäße Funktion der Gerätekonfiguration zu gewährleisten und aufgrund der Zuordnung unterschiedlicher IP-Adressen bei jedem DHCP-Erneuerungszyklus wird empfohlen, IP-Adressen in der DHCP-Server-Tabelle an MAC-Adressen zu binden. Dadurch wird sichergestellt, dass jedes Gerät eine eigene IP-Adresse besitzt und dass weitere relevante Informationen bereitgestellt werden können.

So konfigurieren Sie die automatische DHCP-Serverkonfiguration:

SCHRITT 1 Klicken Sie auf **Administration** > **Dateiverwaltung** > **Automatische DHCP-Konfiguration**. Die Seite *Automatische DHCP-Konfiguration* wird geöffnet.

SCHRITT 2 Geben Sie die Werte ein.

- **Automatische Konfiguration über DHCP**: Wählen Sie dieses Feld aus, um die automatische DHCP-Konfiguration zu aktivieren. Die Konfigurationsdatei wird dann automatisch vom DHCP-Server in das Gerät heruntergeladen.
- **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.

- **SSH-Einstellungen für SCP**: Wenn Sie SCP (Secure Copy Protocol) 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.

SCHRITT 3 Geben Sie die folgenden optionalen Informationen ein, die verwendet werden sollen, wenn kein Konfigurationsdateiname vom DHCP-Server empfangen wurde.

- **Backupserverdefinition**: Wählen Sie **Nach IP-Adresse** oder **Nach Name** aus, um den Server zu konfigurieren.

- **Backupserver-IP-Adresse/Name**: Geben Sie die IP-Adresse oder den Namen des Servers ein, der verwendet werden soll, wenn in der DHCP-Nachricht keine IP-Adresse des Servers angegeben wurde.

- **Name der Backup-Konfigurationsdatei**: Geben Sie den Pfad und den Dateinamen der Datei ein, die verwendet werden soll, wenn in der DHCP-Meldung kein Konfigurationsdateiname angegeben wurde.

In diesem Fenster wird Folgendes angezeigt:

- **Letzte IP-Adresse von Server für automatische Konfiguration**: Zeigt die IP-Adresse des Servers an, der zuletzt für die automatische Konfiguration verwendet wurde.

- **Name der letzten Datei für automatische Konfiguration**: Zeigt den letzten Dateinamen an, den der Switch für die automatische Konfiguration verwendet hat.

HINWEIS Der **Name der letzten Datei für automatische Konfiguration** wird mit den von einem DHCP-Server empfangenen Informationen verglichen, wenn eine IP-Adresse für den Switch empfangen wurde. Wenn diese Werte nicht übereinstimmen, überträgt der Switch die Konfigurationsdatei vom durch den DHCP-Server identifizierten Server in die Startkonfigurationsdatei und initiiert einen Neustart. Stimmen die Werte überein, erfolgt keine Aktion.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Funktion für die automatische DHCP-Konfiguration wird in der aktuellen Konfiguration aktualisiert.

5

Allgemeine Verwaltungsinformationen

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

Die folgenden Themen werden behandelt:

- **Switch-Modelle**
- **Systeminformationen**
- **Konsoleneinstellungen (Unterstützung für automatische Baudrate)**
- **Neustarten des Switch**
- **TCAM-Zuweisung**
- **Überwachen des Lüfterstatus und der Temperatur**
- **Definieren des Timeout für Sitzungsleerlauf**
- **Verwenden von Ping für einen Host**
- **Traceroute**

Switch-Modelle

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

Im Schicht-2-Systemmodus leitet der Switch Pakete als VLAN-fähige Bridge weiter. Im Schicht-3-Systemmodus führt der Switch sowohl das IPv4-Routing als auch Bridging mit VLAN-Unterstützung durch.

HINWEIS Den Schicht-3-Systemmodus können Sie auf der Seite *Systemeinstellungen* für die einzelnen Modelle festlegen.

HINWEIS Den Schicht-3-Systemmodus können Sie auf der Seite *Systemmodus und Stack-Verwaltung* für die einzelnen Modelle festlegen,.

Wenn der Switch 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.

HINWEIS Die folgenden Portkonventionen werden verwendet:

- GE wird für Gigabit Ethernet-Ports (10/100/1000) verwendet.
- FE wird für Fast Ethernet-Ports (10/100) verwendet.

In der folgenden Tabelle werden die verschiedenen Modelle, die Anzahl und die Typen der Ports der Modelle sowie Informationen zu Power over Ethernet (PoE) aufgeführt.

Managed Switch-Modelle

Modell-name	Produkt-ID (PID)	Beschreibung der Ports am Gerät	Leistung für PoE	Zahl der Ports mit PoE-Unter-stützung
SG300-10	SRW2008-K9	8 GE-Ports und 2 Kombinationsports für Sonderzwecke (GE/SFP)		
SG300-10MP	SRW2008MP-K9	8 GE-Ports und 2 Kombinationsports für Sonderzwecke (GE/SFP)	124W	8
SG300-10P	SRW2008P-K9	8 GE-Ports und 2 Kombinationsports für Sonderzwecke (GE/SFP)	62W	8
SG300-20	SRW2016-K9	16 GE-Ports und 4 Ports für Sonderzwecke - 2 Uplinks und 2 Kombinationsports		
SG300-28	SRW2024-K9	24 GE-Ports und 4 Ports für Sonderzwecke - 2 Uplinks und 2 Kombinationsports		
SG300-28P	SRW2024P-K9	24 GE-Ports und 4 Ports für Sonderzwecke - 2 Uplinks und 2 Kombinationsports	180 W	24
SG300-52	SRW2048-K9	48 GE-Ports und 4 Ports für Sonderzwecke - 2 Uplinks und 2 Kombinationsports		

Managed Switch-Modelle (Fortsetzung)

Modell-name	Produkt-ID (PID)	Beschreibung der Ports am Gerät	Leistung für PoE	Zahl der Ports mit PoE-Unter-stützung
SF300-08	SRW208-K9	8 FE-Ports		
SF302-08	SRW208G-K9	8 FE-Ports und 2 GE-Ports		
SF302-08MP	SRW208MP-K9	8 FE-Ports und 2 GE-Ports	124W	8
SF302-08P	SRW208P-K9	8 FE-Ports und 2 GE-Ports	62W	8
SF300-24	SRW224G4-K9	24 FE-Ports und 4 GE-Ports für Sonderzwecke - 2 Uplinks und 2 Kombinationsports		
SF300-24P	SRW224G4P-K9	24 FE-Ports und 4 GE-Ports für Sonderzwecke - 2 Uplinks und 2 Kombinationsports	180 W	24
SF300-48	SRW248G4-K9	48 FE-Ports und 4 GE-Ports für Sonderzwecke - 2 Uplinks und 2 Kombinationsports		
SF300-48P	SRW248G4P-K9	48 FE-Ports und 4 GE-Ports für Sonderzwecke - 2 Uplinks und 2 Kombinationsports	375W	48

Systeminformationen

Die Seite *Systemzusammenfassung* bietet eine grafische Übersicht über den Switch und zeigt den Switch-Status, Hardwareinformationen, Informationen zur Firmware-Version, den allgemeinen PoE-Status und weitere Informationen an.

Anzeigen der Systemzusammenfassung

Zum Anzeigen von Systeminformationen klicken Sie auf **Status und Statistik** > **Systemzusammenfassung**. Die Seite *Systemzusammenfassung* wird geöffnet.

Auf der Seite *Systemzusammenfassung* werden System- und Hardwareinformationen angezeigt.

Systembeschreibung:

- **Systembeschreibung**: Eine Beschreibung des Systems.
- **Systemstandort**: Physischer Ort des Switch. Klicken Sie auf **Bearbeiten**, um zur Seite *Systemeinstellungen* zu gehen und diesen Wert einzugeben.
- **Systemkontakt**: Name einer Kontaktperson. Klicken Sie auf **Bearbeiten**, um zur Seite *Systemeinstellungen* zu gehen und diesen Wert einzugeben.
- **Hostname**: Name des Switch. Klicken Sie auf **Bearbeiten**, um zur Seite *Systemeinstellungen* zu gehen und diesen Wert einzugeben. Standardmäßig setzt sich der Switch-Hostname aus dem Wort *switch* und den drei am wenigsten signifikanten Byte der Switch-MAC-Adresse (die sechs ganz rechts befindlichen Hexadezimalstellen) zusammen.
- **Systembetriebszeit**: Die seit dem letzten Neustart verstrichene Zeit.
- **Aktuelle Zeit**: Die aktuelle Systemzeit.
- **MAC-Basisadresse**: MAC-Adresse des Switch. 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 der Switch neu gestartet wurde.

Status der TCP/UDP-Services:

- **HTTP-Service**: Zeigt an, ob HTTP aktiviert oder deaktiviert ist.
- **HTTPS-Service**: Zeigt an, ob HTTPS aktiviert oder deaktiviert ist.
- **SNMP-Service**: Zeigt an, ob SNMP aktiviert oder deaktiviert ist.
- **Telnet-Service**: Zeigt an, ob Telnet aktiviert oder deaktiviert ist.
- **SSH-Service**: Zeigt an, ob SSH aktiviert oder deaktiviert ist.
- **Modellbeschreibung**: Beschreibung des Switch-Modells.
- **Seriennummer**: Seriennummer.
- **PID VID**: Teilenummer und Versions-ID.

PoE-Leistungsinformationen:

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

  HINWEIS Wenn sich das System im Modus "Natives Stacking" befindet, basiert die angezeigte Firmwareversionsnummer auf der Version des Masters.

- **Firmware-MD5-Prüfsumme (aktives Image)**: MD5-Prüfsumme des aktiven Images.
- **Firmware-Version (inaktives Image)**: Firmware-Versionsnummer des nicht aktiven Images. Wenn sich das System im Modus "Natives Stacking" befindet, wird die Version der Mastereinheit angezeigt.
- **Firmware-MD5-Prüfsumme (inaktives Image)**: MD5-Prüfsumme des nicht aktiven 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.

Konfigurieren der Systemeinstellungen

So geben Sie Systemeinstellungen ein:

SCHRITT 1 Wählen Sie **Administration** > **Systemeinstellungen**. Die Seite *Systemeinstellungen* wird geöffnet.

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

- **Systembeschreibung**: Zeigt eine Beschreibung des Switch.
- **Systemstandort**: Geben Sie den Ort ein, an dem der Switch sich physisch befindet.
- **Systemkontakt**: Geben Sie den Namen einer Kontaktperson ein.
- **Hostname**: Wählen Sie den Hostnamen des Switch aus. Dieser Wert wird in der Eingabeaufforderung von CLI-Befehlen verwendet:
  - *Standard verwenden*: Der Hostname (Systemname) dieser Switches lautet standardmäßig: *switch123456*, wobei "123456" die letzten drei Byte der Switch-MAC-Adresse im hexadezimalen Format repräsentiert.
  - *Benutzerdefiniert*: Geben Sie den Host-Namen 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).
- **Systemmodus**: Wählen Sie den Hostnamen des Switch aus. Dieser Wert wird ebenfalls in der Eingabeaufforderung von CLI-Befehlen verwendet:

  HINWEIS Wenn Sie nach dem Klicken auf "Übernehmen" den Systemmodus ändern, muss das System neu gestartet werden. Nach dem Start ist die Startkonfigurationsdatei nicht mehr vorhanden.

  - *L2*: Wählen Sie diese Option aus, um das Gerät in den Schicht-2-Systemmodus zu versetzen.
  - *L3*: Wählen Sie diese Option aus, um das Gerät in den Schicht-3-Systemmodus zu versetzen.

- **Einstellungen für benutzerdef. Anmeldebildschirm**: Wenn auf der Seite *Anmelden* Text angezeigt werden soll, geben Sie diesen in das Textfeld **Anmeldebanner** ein. 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 festzulegen.

Konsoleneinstellungen (Unterstützung für automatische Baudrate)

Die Geschwindigkeit des Konsolen-Ports kann auf einen der folgenden Werte festgelegt werden: "4800", "9600", "19200", "38400", "57600" und "115200" oder "Automatische Erkennung".

Bei der automatischen Erkennung kann das Gerät die Konsolengeschwindigkeit automatisch erkennen, sodass Sie sie nicht explizit festlegen müssen.

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.

Nach der Aktivierung der automatischen Erkennung auf der Seite *Konsoleneinstellungen* 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**. Die Seite *Konsoleneinstellungen* wird angezeigt.

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.

Neustarten des Switch

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

Sie können die Konfiguration 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 **Herunterladen oder Sichern einer Konfiguration oder eines Protokolls** in **Verwalten von Systemdateien**.

So starten Sie den Switch neu:

SCHRITT 1 Wählen Sie **Administration** > **Neustart**. Die Seite *Neustart* wird geöffnet.

SCHRITT 2 Klicken Sie auf die Schaltfläche **Neustart**, um den Switch neu zu starten.

- **Startkonfigurationsdatei löschen**: Aktivieren Sie diese Option, um die Konfiguration im Switch beim nächsten Start zu löschen.
- **Neustart**: Startet den Switch neu. Da beim Neustart des Switch alle nicht gespeicherten Informationen der aktuellen Konfiguration verloren gehen, müssen Sie in der oberen rechten Ecke eines Fensters auf **Speichern** klicken, damit die aktuelle Konfiguration beim Neustart erhalten bleibt. Wenn die Option "Speichern" nicht angezeigt wird, entspricht die aktuelle Konfiguration der Startkonfiguration und es ist keine Aktion erforderlich.
- **Neustart mit Werkseinstellungen**: Startet den Switch mit der werkseitigen Standardkonfiguration neu. Dabei werden die Startkonfigurationsdatei und die Backup-Konfigurationsdatei gelöscht. Wenn Sie diese Aktion auswählen, wird der Systemmodus auf Schicht 2 festgelegt und alle Einstellungen, die

Sie nicht in einer anderen Datei gespeichert haben, werden gelöscht. Die Spiegelkonfigurationsdatei wird beim Wiederherstellen der Werkseinstellungen nicht gelöscht.

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

TCAM-Zuweisung

Auf der Seite *TCAM-Zuweisungseinstellungen* können Sie die angepasste TCAM-Zuweisung anzeigen. TCAM-Einträge werden in die folgenden Gruppen unterteilt:

- **IP-Einträge**: TCAM-Einträge, die für statische IPv4-Routen, IP-Schnittstellen und IP Hosts reserviert sind. Für jeden Typ werden die folgenden TCAM-Einträge generiert:
  - Statische IPv4-Routen: Ein Eintrag pro Route
  - IP-Schnittstelle: Zwei Einträge pro Schnittstelle
  - IP-Hosts: Ein Eintrag pro Host
- **Nicht-IP-Einträge**: TCAM-Einträge, die für andere Anwendungen wie beispielsweise ACL-Regeln, CoS-Überwachungsvorrichtungen und VLAN-Ratenbegrenzungen reserviert sind.

Wenn Ihre TCAM-Zuweisung gültig ist, wird eine Meldung angezeigt, aus der hervorgeht, dass ein Neustart mit den neuen Einstellungen ausgeführt wird. Wenn Sie die TCAM-Zuweisung auf falsche Weise ändern, wird eine Fehlermeldung angezeigt.

Es gibt zwei Möglichkeiten, die TCAM-Zuweisung auf falsche Weise 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.)

SCHRITT 1 Klicken Sie auf **Administration** > **TCAM-Zuweisungseinstellungen**. Die Seite *TCAM-Zuweisungseinstellungen* wird geöffnet.

Die folgenden Felder werden angezeigt:

- **IPv4-Routen**: Zeigt die Anzahl der verwendeten und verfügbaren IPv4-Routen an.
- **IP-Schnittstellen**: Zeigt die Anzahl der verwendeten und verfügbaren IP-Schnittstelleneinträge an.
- **IP-Host**: Zeigt die Anzahl der verwendeten und verfügbaren IP-Host-Einträge an.

Die folgenden Blöcke werden angezeigt:

- **Reservierte TCAM-Größe**: Zeigt die aktuelle Anzahl der TCAM-Einträge an.
  - **IP-Einträge**: Siehe obige Definition.
  - **Nicht-IP-Einträge**: Siehe obige Definition.
  - **Gesamt**: Zeigt die Anzahl der IP-Einträge und Nicht-IP-Einträge an.
- **Aktuelle TCAM-Zuweisung**: Zeigt die aktuelle Anzahl der verwendeten und der noch verfügbaren TCAM-Einträge an.
  - **IPv4-Routen**: Zeigt die Anzahl der verwendeten und verfügbaren IPv4-Routen an.
  - **IP-Schnittstellen**: Zeigt die Anzahl der verwendeten und verfügbaren IP-Schnittstelleneinträge an.
  - **IP-Host**: Zeigt die Anzahl der verwendeten und verfügbaren IP-Host-Einträge an.
  - **Nicht-IP-Einträge**: Siehe obige Definition.

Sie müssen die aktuelle Konfiguration speichern, bevor Sie die TCAM-Zuweisungseinstellungen ändern.

SCHRITT 2 Speichern Sie die neuen Einstellungen, indem Sie auf **Speichern** klicken. Daraufhin wird die Gültigkeit der TCAM-Zuweisung überprüft. Wenn die Zuweisung falsch ist, wird eine Fehlermeldung angezeigt. Wenn die Zuweisung richtig ist, wird sie in die aktuelle Konfigurationsdatei kopiert.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Daraufhin wird ein Neustart mit den neuen Einstellungen ausgeführt.

Überwachen des Lüfterstatus und der Temperatur

Auf der Seite *Integrität* werden Lüfterstatus und Temperatur aller Geräte mit Lüfter angezeigt.

Um die Parameter für den Switch-Zustand anzuzeigen, wählen Sie **Status und Statistik** > **Zustand**. Die Seite *Zustand* wird geöffnet.

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": Die Lüfter-ID gilt für das jeweilige Modell nicht.
- **Temperatur (in Celsius und Fahrenheit)**: Die interne Temperatur des Switch (für Geräte mit Temperaturfühlern).
- **Alarmtemperatur (in Celsius und Fahrenheit)**: Die interne Temperatur der Einheit (für entsprechende Geräte), die einen Alarm auslöst.

Definieren des Timeout für Sitzungsleerlauf

Mit dem *Timeout für Sitzungsleerlauf* konfigurieren Sie die Zeitintervalle, in denen Verwaltungssitzungen im Leerlauf bleiben können, bis eine Zeitüberschreitung ausgelöst wird 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 die unterschiedlichen Sitzungstypen fest:

SCHRITT 1 Klicken Sie auf **Administration** > **Timeout für Sitzungsleerlauf**. Die Seite *Timeout für Sitzungsleerlauf* wird geöffnet.

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 Switch anzuwenden.

Verwenden von Ping für einen Host

Ping ist ein Dienstprogramm, mit dem Sie die Erreichbarkeit eines Remote-Hosts testen und die Umlaufzeit von Paketen messen können, die vom Switch 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**. Die Seite *Ping* wird geöffnet.

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

- **Hostdefinition**: Wählen Sie aus, ob Hosts anhand der IP-Adresse oder anhand des Namens angegeben 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.
- **IPv6-Adresstyp**: Wählen Sie "Link Local" oder "Global" als einzugebenden IPv6-Adresstyp 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**: Wenn der IPv6-Adresstyp "Link Local" entspricht, wählen Sie aus, von wo der Empfang erfolgt.
- **Host-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 der Liste der Meldungen wird eine weitere Meldung 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 den Switch gesendet. Auf der Seite *Traceroute* werden die einzelnen Hops zwischen dem Switch und einem Zielhost sowie die Umlaufzeit zu jedem dieser Hops angezeigt.

SCHRITT 1 Klicken Sie auf **Administration > Traceroute**. Die Seite *Traceroute* wird geöffnet.

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.
- **IPv6-Adresstyp**: Wählen Sie "Link Local" oder "Global" als einzugebenden IPv6-Adresstyp 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**: Wenn der IPv6-Adresstyp "Link Local" entspricht, wählen Sie aus, von wo der Empfang erfolgt.
- **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.

Auf einer Seite werden in den folgenden Feldern die Umlaufzeit (Round Trip Time, RTT) und der Status für jeden Weg angezeigt:

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

6

Systemzeit

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 Der Switch unterstützt SNTP (Simple Network Time Protocol, einfaches Netzwerkzeitprotokoll). Wenn es aktiviert ist, synchronisiert der Switch seine Uhrzeit dynamisch mit der eines SNTP-Servers. Der Switch 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 der Switch 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 Switch kann mit den folgenden Methoden festgelegt werden:

- **Manuell**: Sie müssen 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 Switch. 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 Switch eingestellt werden:

- Dynamische Konfiguration des Switch 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

Der Switch kann die Systemzeit mit einer der folgenden Methoden von einem SNTP-Server empfangen:

- Client-Broadcast-Empfang (passiver Modus)

  Der SNTP-Server überträgt die Uhrzeit und der Switch hört diese Broadcasts mit. Wenn der Switch in diesem Modus arbeitet, muss kein Unicast-SNTP-Server festgelegt werden.

- **Client-Broadcast-Übertragung (aktiver Modus)**: Der Switch fordert als SNTP-Client in regelmäßigen Abständen SNTP-Zeitaktualisierungen an. In diesem Modus wird eine der folgenden Methoden verwendet:
  - **SNTP-Anycast-Client-Modus**: Der Switch überträgt Zeitanforderungspakete an alle SNTP-Server im Subnetz und wartet auf eine Antwort.
  - **Unicast-SNTP-Server-Modus**: Der Switch sendet Unicast-Anfragen an die Liste der manuell konfigurierten SNTP-Server und wartet auf eine Antwort.

Der Switch 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 der Switch 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 Seite *Systemzeit* wird geöffnet.

Die folgenden Felder werden angezeigt:

- **Tatsächliche Zeit (Statisch)**: Die Systemzeit des Geräts.
- **Letzter synchronisierter Server**: Adresse, Stratum und Typ des SNTP-Servers, von dem die Uhrzeit zuletzt bezogen wurde.

SCHRITT 2 Geben Sie diese Parameter ein:

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

- **Hauptuhrzeitquelle (SNTP-Server)**: Wenn Sie diese Option aktivieren, 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 DHCP 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, *müssen Sie auch den DHCP-Client am Switch aktivieren*. Legen Sie dazu auf der Seite *IPv4-Schnittstelle* die Option **IP-Adresstyp** auf **Dynamisch** fest.

  HINWEIS Der DHCP-Client unterstützt Option 100 für die Bereitstellung der dynamischen Zeitzoneneinstellung. Der Switch unterstützt den DHCPv6-Client nicht.
- **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.

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 folgenden 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 acht Unicast-SNTP-Server konfigurieren.

HINWEIS Um einen Unicast-SNTP-Server anhand des Namens anzugeben, müssen Sie zuerst DNS-Server für den Switch konfigurieren (siehe Abschnitt **Definieren von DNS-Servern**). Aktivieren Sie zum Hinzufügen eines Unicast-SNTP-Servers das Kontrollkästchen zum Aktivieren der Option **SNTP-Unicast-Client**.

So fügen Sie einen Unicast-SNTP-Server hinzu:

SCHRITT 1 Klicken Sie auf **Administration** > **Zeiteinstellungen** > **SNTP-Unicast**. Die Seite *SNTP-Unicast* wird geöffnet.

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

- **SNTP-Server**: IP-Adresse des SNTP-Servers. Bis zu acht SNTP-Server können festgelegt werden. 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 Switch 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 Switch 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 aus der letzten empfangenen Antwort vom SNTP-Server.
- **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.

SCHRITT 2 Zum Hinzufügen eines Unicast-SNTP-Servers aktivieren Sie die Option **SNTP-Unicast-Client**.

SCHRITT 3 Klicken Sie auf **Hinzufügen**, um die Seite *SNTP-Server hinzufügen* anzuzeigen.

SCHRITT 4 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 der Switch mit dem Internet verbunden sein und mit einem DNS-Server konfiguriert sein oder so konfiguriert sein, dass ein DNS-Server durch die Verwendung von DHCP identifiziert wird. (Siehe Abschnitt **Definieren von DNS-Servern**.)

- **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 **Sonstige** 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 der Switch 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 erstellen Sie auf der Seite *SNTP-Authentifizierung*.)

SCHRITT 5 Klicken Sie auf **Übernehmen**. Der STNP-Server wird hinzugefügt, und Sie werden zur Hauptseite zurückgeleitet.

Konfigurieren des SNTP-Modus

Der Switch 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**. Die Seite *SNTP-Multicast/-Anycast* wird geöffnet.

SCHRITT 2 Wählen Sie unter den folgenden Optionen aus:

- **SNTP-Multicast-Client-Modus (Client-Broadcast-Empfang)**: Wählen Sie diese Option aus, um die Systemzeit von einem beliebigen SNTP-Server im Subnetz zu empfangen.
- **SNTP-Anycast-Client-Modus (Client-Broadcast-Übertragung)**: Wählen Sie diese Option aus, um SNTP-Broadcast-Synchronisationspakete zum Anfordern von Systemzeitinformationen zu übertragen. Wenn SNTP-Server definiert sind, werden die Pakete an diese Server gesendet. Anderenfalls werden die Pakete 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 SNTP-Empfang/-Übertragung zu öffnen. Die Seite *SNTP-Schnittstelleneinstellungen hinzufügen* wird geöffnet.

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 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**. Die Seite *SNTP-Authentifizierung* wird geöffnet.

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

SCHRITT 3 Klicken Sie auf **Übernehmen**, um den Switch zu aktualisieren.

SCHRITT 4 Klicken Sie auf **Hinzufügen**. Die Seite *SNTP-Authentifizierung hinzufügen* wird geöffnet.

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 den Switch senden.
- **Vertrauensw. Schlüssel**: Wählen Sie diese Option aus, wenn der Switch 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

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. Diesen Zeitbereich definieren Sie auf den Seiten unter *Wiederkehrender Bereich*.

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.

Der Switch unterstützt höchstens 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.

Mit dieser Funktion können Sie den Zugriff auf Computer auf die Geschäftszeiten für das Netzwerk begrenzen. Anschließend werden die Netzwerkports sowie der Zugriff auf das restliche Netzwerk gesperrt.

Absoluter Zeitbereich

So definieren Sie einen absoluten Zeitbereich:

SCHRITT 1 Klicken Sie auf **Administration** > **Zeiteinstellungen** > **Zeitbereich**, um die Seite *Zeitbereich* anzuzeigen.

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**, um die Seite *Wiederkehrender Bereich* anzuzeigen.

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.

7

Verwalten der Gerätediagnose

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:

- **Testen von Kupfer-Ports**
- **Anzeigen des Status des optischen Moduls**
- **Konfigurieren der Port- und VLAN-Spiegelung**
- **Anzeigen der CPU-Auslastung und Secure Core Technology**

Testen von Kupfer-Ports

Auf der Seite *Kupfertest* werden die Ergebnisse der integrierten Kabeltests angezeigt, die von Virtual Cable Tester (VCT) für Kupferkabel 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 Block "Testergebnisse" auf der Seite *Kupfertest* angezeigt.
- DSP-basierte Tests werden an aktiven GE-Verbindungen ausgeführt, um die Kabellänge zu messen. Die Ergebnisse werden im Block "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**. Die Seite *Kupfertest* wird geöffnet.

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 Block **Erweiterte Informationen** die folgenden Informationen angezeigt, die bei jedem Aufrufen 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 Form-factor Pluggable) berichtet wurden. 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**. Die Seite *Status des optischen Moduls* wird geöffnet.

Auf dieser Seite werden folgende Felder angezeigt:

- **Port**: Nummer des Ports, an den der SFP angeschlossen ist.
- **Temperatur**: Betriebstemperatur (Celsius) des SFP.
- **Spannung**: Die Betriebsspannung des SFP.
- **Stromstärke**: Die aktuelle Stromstärke 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 einem Netzwerk-Switch verwendet, um eine Kopie der Netzwerkpakete an einem oder mehreren Switch-Ports oder in einem gesamten VLAN an eine Netzwerk-Überwachungsverbindung oder einen anderen Port am Switch zu senden. Diese Funktion wird normalerweise für Netzwerkgeräte verwendet, bei denen eine Überwachung des Netzwerk-Verkehrs erforderlich ist, beispielsweise ein IDS (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.

Wenn an einem Netzwerk-Port ein Paket empfangen wird, 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. An den Switch gesendete Pakete werden gespiegelt, wenn die Funktion Transmit (Tx) Mirroring aktiviert wird.

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 für manuell erstellte 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 Seite *Port- und VLAN-Spiegelung* wird geöffnet.

Auf dieser Seite werden folgende Felder 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. Die Seite *Port- und VLAN-Spiegelung hinzufügen* wird geöffnet.

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 Analysezielport 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 kommende, der gehende 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

In diesem Abschnitt werden Secure Core Technology (SCT) und das Anzeigen der CPU-Auslastung beschrieben.

Der Switch verarbeitet neben dem Datenverkehr der Endbenutzer die folgenden Verkehrstypen:

- Verwaltungsverkehr
- Protokollverkehr
- Snooping-Verkehr

Übermäßiger Verkehr führt zu einer Belastung der CPU und kann den Betrieb des Switch beeinträchtigen. Der Switch stellt mithilfe der SCT-Funktion (Secure Core Technology) sicher, dass Verwaltungs- und Protokollverkehr unabhängig von der Gesamtmenge des empfangenen Verkehrs 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 Wählen Sie **Administration** > **Diagnose** > **CPU-Auslastung**.

Die Seite *CPU-Auslastung* wird geöffnet.

Auf der Seite **CPU-Eingangsgeschwindigkeit** wird die Rate der pro Sekunde bei der CPU eingehenden Frames angezeigt.

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

SCHRITT 2 Legen Sie die **Aktualisierungsrate** (Zeitraum in Sekunden) fest, die bis zum Aktualisieren der Statistiken verstreichen soll. Für jeden Zeitraum wird ein neues Abbild erstellt.

8

Konfigurieren von Discovery

Dieser Abschnitt enthält Informationen zum Konfigurieren von Discovery.

Die folgenden Themen werden behandelt:

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

Konfigurieren von Bonjour Discovery

Als Bonjour-Client führt der Switch 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.) Der Switch 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 der Switch im Schicht-2-Systemmodus befindet, ist Bonjour Discovery global aktiviert. Die Funktion kann nicht für einzelne Ports oder VLANs deaktiviert werden. Der Switch 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 der Switch sämtliche Servicetyp-Ankündigungen und antwortet auf keinerlei Serviceanforderungen von Netzwerkverwaltungsanwendungen.

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

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – Bonjour**. Die Seite *Discovery – Bonjour* wird geöffnet.

SCHRITT 2 Wählen Sie **Aktivieren** aus, um Bonjour Discovery am Switch global zu aktivieren.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Bonjour wird für den Switch 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 der Switch Bonjour Discovery-Pakete an alle Schnittstellen mit IP-Adresse versenden. Sie können Bonjour einzelnen Ports und/oder VLANs zuweisen. Wenn Bonjour aktiviert ist, kann der Switch Bonjour Discovery-Pakete an Schnittstellen senden, deren IP-Adressen Bonjour in der Tabelle für Bonjour-Discovery-Schnittstellensteuerung zugeordnet sind. (Wenn der Switch 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, wie z. B. ein VLAN, gelöscht wird, werden Goodbye-Pakete gesendet, um die Registrierung der vom Switch 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 der Switch keine Bonjour Discovery-Ankündigungen und hört andere Geräte auch nicht auf gesendete Bonjour Discovery-Ankündigungen ab.

So konfigurieren Sie Bonjour, wenn sich der Switch im Schicht-3-Systemmodus befindet:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – Bonjour**. Die Seite *Discovery – Bonjour* wird geöffnet.

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.

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 untereinander ankündigen. Der Switch sendet standardmäßig regelmäßig eine LLDP/CDP-Ankündigung an alle Schnittstellen und beendet 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 der Switch eingehende CDP/LLDP-Pakete von Ports, für die CDP/LLDP deaktiviert ist.
- Wenn CDP/LLDP global deaktiviert ist, kann der Switch 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 Switch konfigurierten Voice-VLAN basieren, im Switch aktiviert. Details finden Sie in den Abschnitten "Voice-VLAN" und "Auto-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 der Switch nur dann CDP/LLDP-Pakete über die Schnittstelle, wenn diese authentifiziert und autorisiert ist.

Wenn ein Port Ziel einer Spiegelung ist, wird er für CDP/LLDP als deaktiviert betrachtet.

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)**
- **Festlegen von LLDP-Eigenschaften**
- **Bearbeiten von LLDP-Porteinstellungen**
- **LLDP MED**
- **Konfigurieren der LLDP MED-Porteinstellungen**
- **Anzeigen des LLDP-Portstatus**
- **Anzeigen lokaler LLDP-Informationen**
- **Anzeigen von LLDP-Nachbarinformationen**
- **Zugriff auf die 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 der Switch 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**.

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 auf der Seite *Porteinstellungen* LLDP für einzelne Ports. Auf dieser Seite können Sie Schnittstellen für das Senden bzw. Empfangen von LLDP-PDUs, das Senden von SNMP-Benachrichtigungen, das Angeben der anzukündigenden TLVs und das Ankündigen der Verwaltungsadresse des Switch 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.

Festlegen von LLDP-Eigenschaften

Auf der Seite *LLDP-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**. Die Seite *Eigenschaften* wird geöffnet.

SCHRITT 2 Geben Sie die Parameter ein.

- **LLDP-Status**: Wählen Sie diese Option aus, um LLDP für den Switch 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.

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 Switch 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.

Bearbeiten von LLDP-Porteinstellungen

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, und Sie können den TLV für die Verwaltungsadresse des Switch konfigurieren.

So definieren Sie die LLDP-Porteinstellungen:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – LLDP** > **Porteinstellungen**. Die Seite *Porteinstellungen* wird geöffnet.

Auf dieser Seite werden die LLDP-Informationen für den Port angezeigt.

SCHRITT 2 Wählen Sie einen Port aus, und klicken Sie auf **Bearbeiten**. Die Seite *LLDP-Porteinstellungen bearbeiten* wird geöffnet.

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.

  Das Zeitintervall zwischen Benachrichtigungen geben Sie 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*.
- **Verfügbare optionale TLVs**: Wählen Sie die Informationen, die vom Switch veröffentlicht werden sollen, indem Sie das TLV in die Liste **Ausgewählte 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 Switch unterstützten Software ein. Der Wert ist gleich dem sysDescr-Objekt.
- *Systemfunktionen*: Primäre Funktionen des Switch 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.
- *802.3-Maximum-Frame*: Maximale Frame-Größenkapazität der MAC-/PHY-Implementierung.

Die folgenden Felder beziehen sich auf die Verwaltungsadresse:

- **Ankündigungsmodus**: Wählen Sie eine der folgenden Arten, die IP-Verwaltungsadresse des Switch anzukündigen:
  - *Automatische Ankündigung*: Gibt an, dass die Software automatisch eine Verwaltungsadresse auswählt, die von allen IP-Adressen des Produkts 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 der Switch im Schicht-3-Modus befindet und mit mehreren IP-Adressen konfiguriert ist.
- **IP-Adresse**: Wenn die manuelle Ankündigung ausgewählt wurde, wählen Sie die IP-Verwaltungsadresse unter den verfügbaren Adressen aus.

SCHRITT 3 Geben Sie die relevanten Informationen ein, und klicken Sie auf **Übernehmen**. Die Porteinstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

LLDP MED

LLDP Media Endpoint Discovery (LLDP MED) ist eine Erweiterung von LLDP, die zusätzliche Funktionen zur Unterstützung von Medien-Endpunktgeräten bietet. Beispiele für die Funktionen von LLDP MED-Netzwerkrichtlinien:

- Ermöglicht die Ankündigung und Erkennung von Netzwerkrichtlinien für Echtzeitanwendungen wie beispielsweise Sprache und/oder Video.
- Bietet 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 den Switch anweisen, automatisch eine Netzwerkrichtlinie für Sprachanwendungen zu generieren und anzukündigen, die auf dem vom Switch verwalteten Voice-VLAN basiert. Im Abschnitt "Auto-Voice-VLAN" finden Sie Details zur Verwaltung des Voice-VLANs auf dem Switch.

So definieren Sie eine LLDP MED-Netzwerkrichtlinie:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – LLDP** > **LLDP MED-Netzwerkrichtlinien**. Die Seite *LLDP MED-Netzwerkrichtlinien* wird angezeigt.

Auf dieser Seite werden die zuvor erstellten Netzwerkrichtlinien angezeigt.

SCHRITT 2 Wählen Sie für LLDP MED-Netzwerkrichtlinien für Sprachanwendungen die Option **Autom.** aus, wenn der Switch 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 Zum Definieren einer neuen Richtlinie klicken Sie auf **Hinzufügen**. Daraufhin wird die Seite *LLDP MED-Netzwerkrichtlinie hinzufügen* geöffnet.

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-Tag**: 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 den Switch 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.

Konfigurieren der 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 der Switch 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 *LLDP MED-Porteinstellungen* wird geöffnet.

Auf dieser Seite werden die LLDP MED-Einstellungen, einschließlich der aktivierten TLVs, für alle Ports angezeigt.

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**. Die Seite *LLDP MED-Porteinstellungen bearbeiten* wird geöffnet.

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.
- **Verfügbare optionale TLVs**: Wählen Sie die TLVs aus, die vom Switch veröffentlicht werden können, indem Sie sie 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 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.

Anzeigen des LLDP-Portstatus

Auf der Seite *Tabelle für LLDP-Portstatus* werden die globalen LLDP-Informationen für jeden Port angezeigt.

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – LLDP** > **LLDP-Portstatus**. Die Seite *LLDP-Portstatus* wird geöffnet.

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 zu 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 Switch angezeigt.
- **Systemname**: Name des Switch.
- **Systembeschreibung**: Beschreibung des Switch (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.

Anzeigen lokaler LLDP-Informationen

So können Sie den angekündigten LLDP-Status des lokalen Ports anzeigen:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – LLDP** > **LLDP – Lokale Informationen**. Die Seite *LLDP – Lokale Informationen* wird geöffnet.

SCHRITT 2 Klicken Sie unten auf der Seite auf **Tabelle für LLDP-Portstatus**.

Klicken Sie auf **LLDP: Details zu lokalen Informationen**, um die Details der LLDP- und LLDP MED-TLVs einzusehen, die an den Nachbarn gesendet wurden.

Klicken Sie auf **LLDP: Details zu Nachbarinformationen**, um Einzelheiten zu den LLDP- und LLDP MED-TLVs einzusehen, die vom Nachbarn empfangen wurden.

SCHRITT 3 Wählen Sie in der **Port**-Liste den gewünschten Port aus.

Auf dieser Seite sind die folgenden Felder verfügbar:

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 Switch angezeigt.
- **Systemname**: Name des Switch.
- **Systembeschreibung**: Beschreibung des Switch (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 Konvertierung digitaler Daten 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-Switch und Verwaltungsfunktionen für Geräteinformationen.
- **PoE-Gerätetyp**: PoE-Typ des Ports, zum Beispiel "powered".
- **PoE-Stromquelle**: Stromquelle des Ports.
- **PoE-Stromprioritä**t: Stromprioritä 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.

Anzeigen von LLDP-Nachbarinformationen

Auf der Seite *LLDP-Nachbarinformationen* werden 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 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**. Die Seite *LLDP-Nachbarinformationen* wird geöffnet.

Auf dieser Seite werden folgende Felder 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 Switch.
- **Time-to-Live**: Zeitraum in Sekunden, nach dem die Informationen über diesen Nachbarn gelöscht werden.

SCHRITT 2 Wählen Sie einen lokalen Port aus, und klicken Sie auf **Details**. Die Seite *Nachbarinformationen* wird geöffnet.

Auf dieser Seite werden folgende Felder angezeigt:

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.
- **Local-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-Stromprioritä**t: Stromprioritä 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.

PPVID-Tabelle

- **VID**: Protokoll-VLAN-ID.
- **Unterstützt**: Unterstützte Port- und Protokoll-VLAN-IDs.
- **Aktiviert**: Aktivierte Port- und Protokoll-VLAN-IDs.

VLAN-IDs

- **VID**: Port- und Protokoll-VLAN-ID.

- **VLAN-Namen**: Angekündigte VLAN-Namen.

Protokoll-IDs

- **Protokoll-ID-Tabelle**: Angekündigte Protokoll-IDs.

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

- **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.

Zugriff auf die 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**. Die Seite *LLDP-Statistik* wird geöffnet.

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**. Die Seite *LLDP-Überlastung* wird geöffnet.

Auf dieser Seite werden für die einzelnen Ports die folgenden Felder angezeigt:

- **Schnittstelle**: Kennung des Ports.
- **Gesamt (Byte)**: Gesamtanzahl der Bytes mit LLDP-Informationen in jedem Paket.

- **Noch zu senden (Byte)**: 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**. Die Seite *LLDP-Überlastungsdetails* wird geöffnet.

Auf dieser Seite werden für die einzelnen vom Port gesendeten TLVs die folgenden Informationen angezeigt:

- **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 MEDLLDP 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 (Byte)**: Gesamtanzahl der Bytes mit LLDP-Informationen in jedem Paket.
- **Noch zu senden (Byte)**: Gesamtanzahl der noch verfügbaren 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:

- **Festlegen von CDP-Eigenschaften**
- **Bearbeiten von CDP-Schnittstelleneinstellungen**
- **Anzeigen lokaler CDP-Informationen**
- **Anzeigen von CDP-Nachbarinformationen**
- **Anzeigen der CDP-Statistik**

Festlegen von 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 Switch. 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*.

Im Abschnitt **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**. Die Seite *Eigenschaften* wird geöffnet.

SCHRITT 2 Geben Sie die Parameter ein.

- **CDP-Status**: Wählen Sie diese Option aus, um CDP für den Switch 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 aus, damit der Switch 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).
- **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.

Bearbeiten von CDP-Schnittstelleneinstellungen

Auf der Seite *Schnittstelleneinstellungen* können Administratoren 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 LLDP-Schnittstelleneinstellungen:

SCHRITT 1 Klicken Sie auf **Administration** > **Discovery – CDP** > **Schnittstelleneinstellungen**. Die Seite *Schnittstelleneinstellungen* wird geöffnet.

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**: Zeigt den Status der Berichterstellungsoptionen an, 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**. Die Seite *CDP-Schnittstelleneinstellungen bearbeiten* wird geöffnet.

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 der Switch so eingerichtet wurde, dass Traps an die Verwaltungsstation gesendet werden.

- **Syslog-Voice-VLAN stimmt nicht überein**: Wählen Sie diese Option aus, um das optionale Senden einer Syslog-Nachricht bei Erkennung einer Nichtübereinstimmung beim Voice-VLAN zu aktivieren. 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**: Wählen Sie diese Option aus, um das optionale Senden einer Syslog-Nachricht bei Erkennung einer Nichtübereinstimmung beim nativen VLAN zu aktivieren. 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 optionale 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.

Anzeigen lokaler CDP-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**. Die Seite *Lokale CDP-Informationen* wird geöffnet.

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.

Anzeigen von 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**. Die Seite *CDP-Nachbarinformationen* wird geöffnet.

Auf dieser Seite werden die folgenden Felder für den Link-Partner (Nachbar) angezeigt:

- **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 2 Wählen Sie ein Gerät aus und klicken Sie auf **Details**. Die Seite *CDP-Nachbardetails* wird geöffnet.

Auf dieser Seite werden folgende Felder für den Nachbarn angezeigt:

- **Geräte-ID**: Die Kennung des Nachbargeräts.
- **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.
- **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.

Anzeigen der CDP-Statistik

Auf der Seite *CDP-Statistik* werden Informationen zu CDP-Frames (Cisco Discovery Protocol) 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. Hierzu verwenden Sie die Seiten *CDP-Eigenschaften* und *CDP-Schnittstelleneinstellungen*.

So zeigen Sie die CDP-Statistik an:

SCHRITT 1 Klicken Sie auf **Administration > Discovery – CDP > CDP-Statistik**. Die Seite *CDP-Statistik* wird geöffnet.

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 **Alle Schnittstellenzähler löschen**.

9

Anschlussverwaltung

In diesem Abschnitt werden die Portkonfiguration, die Link-Aggregation und die Green Ethernet-Funktion beschrieben.

Die folgenden Themen werden behandelt:

- **Konfigurieren von Ports**
- **Festlegen der grundlegenden Portkonfiguration**
- **Konfigurieren von Link-Aggregation**
- **Konfigurieren von Green Ethernet**

Konfigurieren von Ports

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 Switch unterstützt wird und für diesen aktiviert ist, konfigurieren Sie den Switch wie unter **Verwalten von Power-over-Ethernet-Geräten** beschrieben.

Festlegen der grundlegenden Portkonfiguration

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 **Port-Verwaltung** > **Porteinstellungen**. Die Seite *Porteinstellungen* wird geöffnet.

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 der Switch 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 der Switch neu gestartet wurde.

SCHRITT 4 Wählen Sie zum Aktualisieren der Porteinstellungen den gewünschten Port aus, und klicken Sie auf **Bearbeiten**. Die Seite *Porteinstellungen bearbeiten* wird geöffnet.

SCHRITT 5 Ändern Sie die folgenden Parameter:

- **Schnittstelle**: Wählen Sie die Portnummer aus.
- **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.

- **Port-Beschreibung**: Geben Sie den benutzerdefinierten Namen oder einen Kommentar für den Port ein.
- **Administrativer Status**: Wählen Sie aus, ob der Port aktiv oder nicht aktiv sein muss, wenn der Switch neu gestartet wird.
- **Betriebsstatus**: Zeigt an, ob der Port zurzeit aktiv ist.
- **Zeitbereich**: Wählen Sie diese Option aus, 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.
- **Außer Kraft gesetzten Port reaktivieren**: Wählen Sie diese Option aus, wenn Sie einen außer Kraft gesetzten Port reaktivieren möchten. Es gibt verschiedene Möglichkeiten, Ports außer Kraft zu setzen, beispielsweise über die Sicherheitsoption zum Sperren von Ports, einzelne Hostverletzung (DoT1X), Loopback-Erkennung STP-Loopback-Schutz oder ACL-Konfigurationen (Access Control List, Zugriffssteuerungsliste). Beim Reaktivierungsvorgang wird der Port ohne Berücksichtigung der Gründe für seine Außerkraftsetzung wieder aktiviert.
- **Autom. Aushandlung**: 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**: Konfigurieren Sie die Geschwindigkeit des Ports. 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:
  - *Voll*: Die Schnittstelle unterstützt die Übertragung zwischen dem Switch und dem Client in beide Richtungen gleichzeitig.
  - *Halb*: Die Schnittstelle unterstützt die Übertragung zwischen dem Switch und dem Client immer nur in eine Richtung (nicht 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.

- **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 Switch 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**: Der 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 diesen Switch über ein ungekreuztes Kabel mit einer Station zu verbinden.
  - *Automatisch*: Mit dieser Option können Sie den Switch 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.
- **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.

Konfigurieren von Link-Aggregation

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

- **Link-Aggregation (Übersicht)**
- **Workflow von statischen und dynamischen LAGs**
- **Festlegen 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 LACP für sie deaktiviert ist. Bei der Gruppe der Ports, die einer statischen LAG zugewiesen sind, handelt es sich immer um aktive Mitglieder. Nach der manuellen Erstellung einer LAG können Sie die LACP-Option nur dann hinzufügen oder entfernen, wenn Sie die LAG bearbeiten und ein Mitglied entfernen (das Mitglied kann vor der Anwendung

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.

Lastenausgleich

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.

Der Switch 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.

Vom Switch werden acht LAGs unterstützt.

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 dagegen die automatische Aushandlung 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.

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** ziehen.
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.

Festlegen 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**. Die Seite *LAG-Verwaltung* wird geöffnet.

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 die aktuelle Konfigurationsdatei geschrieben.

So definieren Sie die Mitgliedsports oder Kandidatenports in einer LAG:

SCHRITT 1 Wählen Sie die zu konfigurierende LAG aus, und klicken Sie auf **Bearbeiten**. Die Seite *LAG-Mitgliedschaft bearbeiten* wird geöffnet.

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.

- **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.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die LAG-Mitgliedschaft wird in die aktuelle Konfigurationsdatei geschrieben.

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**. Die Seite *LAG-Einstellungen* wird geöffnet.

SCHRITT 2 Wählen Sie eine LAG aus und klicken Sie auf **Bearbeiten**. Die Seite *LAG-Einstellungen bearbeiten* wird geöffnet.

SCHRITT 3 Geben Sie Werte für die folgenden Felder ein:

- **LAG**: Wählen Sie die LAG-ID-Nummer aus.
- **Beschreibung**: Geben Sie den LAG-Namen oder einen Kommentar ein.
- **LAG-Typ**: Zeigt den Port-Typ der LAG an.
- **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.
- **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.
- **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 aus, 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 der Switch 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 am anderen Switch (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.

Festlegen der LACP-Parametereinstellungen für Ports

Auf der Seite *LACP* wird die Konfiguration für die LACP-Systempriorität, das LACP-Timeout und die LACP-Portpriorität angezeigt und Sie können die Konfigurationen auf dieser Seite bearbeiten. Das LACP-Timeout ist ein portspezifischer Parameter. Er bezeichnet das Zeitintervall zwischen dem Senden und Empfangen aufeinander folgender LACP-PDUs. Wenn alle anderen Faktoren gleich sind und für eine LAG mehr potentielle Ports konfiguriert wurden als die zulässige Höchstzahl aktiver Ports, wählt der Switch aus der dynamischen LAG die Ports als aktiv aus, die die höchste Priorität aufweisen.

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**. Die Seite *LACP* wird geöffnet.

SCHRITT 2 Geben Sie die LACP-Systempriorität ein. Weitere Informationen hierzu finden Sie unter **Konfigurieren von LACP**.

SCHRITT 3 Wählen Sie einen Port aus, und klicken Sie auf **Bearbeiten**. Die Seite *LACP bearbeiten* wird geöffnet.

SCHRITT 4 Geben Sie Werte für die folgenden Felder ein:

- **Schnittstelle**: 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 für Ports**.
- **LACP-Timeout**: Wählen Sie aus, ob die periodischen Übertragungen von LACP-PDUs abhängig von der festgelegten LACP-Timeout-Voreinstellung mit einer niedrigen oder mit einer hohen Übertragungsrate ausgeführt werden sollen.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Konfigurieren von Green Ethernet

In diesem Kapitel wird die Green Ethernet-Funktion beschrieben, mit der am Switch Strom gespart werden kann.

Dieses Kapitel umfasst folgende Abschnitte:

- **Green Ethernet (Übersicht)**
- **Festlegen globaler Green Ethernet-Eigenschaften**
- **Einstellen der Green Ethernet-Eigenschaften für Ports**

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 die Gigabyte-Ports.

Mit der Green Ethernet-Funktion kann der Gesamtstromverbrauch auf verschiedene Arten reduziert werden:

- **Energieerkennungsmodus**: 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 der Switch 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 *Systemzusammenfassung* 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.

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 (Switch-Port 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 > *PorteinstellungenPorteinstellungen*" 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 802.3 EEE auf dem lokalen Gerät öffnen Sie die Seite *Administration > Discovery: LLDP > LLDP – Lokale Informationen* und zeigen Sie die Informationen im Block "802.3 Energy Efficient Ethernet (EEE)" an.

SCHRITT 5 Zum Anzeigen von Informationen zu 802.3az EEE auf dem Remote-Gerät öffnen Sie die Seite *Administration > Discovery – LLDP > LLDP-Nachbarinformationen* und zeigen die Informationen im Block "802.3az Energy Efficient Ethernet (EEE)" an.

Festlegen globaler Green Ethernet-Eigenschaften

Auf der Seite *Eigenschaften* können Sie die Konfiguration des Green Ethernet-Modus für den Switch 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**. Die Seite *Eigenschaften* wird geöffnet.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **Energieerkennungsmodus**: 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 Switch GE-Ports vorhanden sind.

  HINWEIS Wenn "Kurze Reichweite" aktiviert ist, muss EEE deaktiviert sein.

- **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.
- **Kumulative Energieeinsparung**: Zeigt an, wie viel Strom seit dem letzten Neustart des Switch 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.
- **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.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Green Ethernet-Eigenschaften werden in die aktuelle Konfigurationsdatei geschrieben.

Einstellen der Green Ethernet-Eigenschaften für Ports

Auf der Seite *Porteinstellungen* werden die aktuellen Green Ethernet- und EEE-Modi pro Port angezeigt und 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.*

Beachten Sie, dass EEE-Einstellungen nur für Geräte mit GE-Ports angezeigt werden. 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**. Die Seite *Porteinstellungen* wird geöffnet.

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 **Festlegen globaler Green Ethernet-Eigenschaften**.

SCHRITT 2 Wählen Sie einen **Port** aus und klicken Sie auf **Bearbeiten**. Die Seite *Porteinstellung bearbeiten* wird geöffnet.

SCHRITT 3 Aktivieren oder deaktivieren Sie den Energieerkennungsmodus 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.

10

Smartports

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. Bei einem Smartport-Makro handelt es sich um ein Skript mit CLI-Befehlen (Command Line Interface, Befehlszeilenschnittstelle).

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 Switch 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, auf die ein integriertes (oder benutzerdefiniertes) Makro angewendet werden kann. Diese Makros sollen die schnelle Konfiguration des Switch im Hinblick auf die Unterstützung der Kommunikationsanforderungen und die Nutzung der Funktionen der verschiedenen Arten von Netzwerkgeräten ermöglichen. 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. Der Switch unterstützt die folgenden 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 ("Makro") dient zum Anwenden der gewünschten Konfiguration. 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 den folgenden Methoden anwenden:

- 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 und Auto-Smartport-Typen

Smartport-Typ	Von Auto-Smartport unterstützt	Standardmäßig von Auto-Smartport unterstützt
Unbekannt	Nein	Nein
Standard	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:

- **Standard**

  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.
  - Der Switch 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 durch Anwenden der Aktion "Zurücksetzen" (auf den Seiten *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 zum Konfigurieren einer Schnittstelle für ein bestimmtes Netzwerkgerät.

Smartport-Makros sind nicht mit globalen Makros zu verwechseln. Mit globalen Makros konfigurieren Sie den Switch global, während das Smartport-Makro nur für die Schnittstelle gilt, auf die es angewendet wird.

Die Makroquelle können Sie ermitteln, indem Sie den Befehl "show parser macro name [Makroname]" im privilegierten Ausführungsmodus der CLI ausführen oder auf die Schaltfläche **Makroquelle anzeigen** auf der Seite *Smartport-Typ-Einstellungen* 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-Typ-Einstellungen bearbeiten* binden Sie Smartport-Makros an Smartport-Typen.

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 der Switch 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 Startup 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 *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 dem Makro zugeordneten 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 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 der Switch ein Smartport-Makro basierend auf dem Smartport-Typ 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 Empfang dieser CDP- und/oder LLDP-Pakete leitet der Switch den entsprechende Smartport-Typ für das Telefon ab und wendet das entsprechende 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

Der Switch 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

Zuordnung von CDP-Funktionen zu Smartport-Typen (Fortsetzung)

Funktionsname	CDP-Bit	Smartport-Typ
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

Der Switch 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 Switch 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 wird, die Schnittstelle deaktiviert wird und der Switch 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 wird, die Schnittstelle deaktiviert wird oder der Switch 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 beim Anwenden eines Smartport-Makros auf eine Schnittstelle ein Fehler aufgetreten ist, können Sie den Fehler auf der Seite *Schnittstelleneinstellungen* untersuchen, den Port zurücksetzen und das Makro erneut anwenden, nachdem Sie den Fehler auf den Seiten *Schnittstelleneinstellungen* und *Schnittstelleneinstellungen bearbeiten* korrigiert 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.

HINWEIS Wenn Sie von einer Firmware-Version ohne Auto-Smartport-Unterstützung auf eine Firmware-Version mit dieser Unterstützung aktualisieren, wird Auto-Voice-VLAN nach dem Upgrade deaktiviert. Wenn Telefonie-OUI vor der Aktualisierung aktiviert war, wird Auto-Smartport nach der Aktualisierung deaktiviert und Telefonie-OUI bleibt aktiviert.

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 den Switch zu aktivieren und einen Port mit Auto-Smartport zu konfigurieren, führen Sie die folgenden Schritte aus:*

SCHRITT 1 Um die Auto-Smartport-Funktion für den Switch 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 der Switch 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 entsprechendes Anti-Makro) 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 Problembehandlung finden Sie unten.

SCHRITT 4 Klicken Sie auf **Bearbeiten.** Es wird ein neues Fenster 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**. Die Seite *Eigenschaften* wird geöffnet.

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 für das Gerät zu deaktivieren.
  - *Aktivieren*: Wählen Sie diese Option aus, um Auto-Smartport für das Gerät zu aktivieren.
  - *Aktivieren nach Auto-Voice-VLAN*: Wenn Sie diese Option auswählen, ist Auto-Smartport aktiviert, wird jedoch nur verwendet, wenn Auto-Voice-VLAN ebenfalls aktiviert ist und verwendet wird. "Aktivieren nach Auto-Voice-VLAN" ist die Standardeinstellung.
- **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 Switch festgelegt.

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**. Die Seite *Smartport-Typ-Einstellungen* wird geöffnet.

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 Zum Ändern der Parameter eines Makros oder zum Zuweisen eines benutzerdefinierten Makros wählen Sie einen Smartport-Typ aus und klicken auf **Bearbeiten**. Die Seite *Smartport-Typ-Einstellungen bearbeiten* wird geöffnet.

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**: Wählen Sie aus, ob das diesem Smartport-Typ zugeordnete Paar aus Makro und Anti-Makro integriert oder benutzerdefiniert ist.

- **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 einen Switch erneut auf eine Switch-Schnittstelle anwenden, wird die Schnittstelle Mitglied der VLANs, die seit der letzten Anwendung des Makros erstellt wurden. Sie müssen mit den aktuellen Konfigurationen des Switch sowie mit der Definition des Makros vertraut sein, um zu bestimmen, 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**. Die Seite *Schnittstelleneinstellungen* wird geöffnet.

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**. Die Seite *Schnittstelleneinstellungen bearbeiten* wird geöffnet.

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 der Switch 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.
#                        $voice_vlan: Die Voice-VLAN-ID
#
#Default Values are
#$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_ap

```
[no_ap]
#macro description No ap
#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
#
@
```

11

Verwalten von Power-over-Ethernet-Geräten

Die Power-over-Ethernet-Funktion (PoE) steht nur bei PoE-basierten Geräten zur Verfügung. Eine Liste der PoE-basierten Geräte finden Sie im Abschnitt **Switch-Modelle**.

In diesem Abschnitt wird beschrieben, wie Sie die PoE-Funktion verwenden.

Die folgenden Themen werden behandelt:

- **PoE am Switch**
- **Konfigurieren von PoE-Eigenschaften**
- **Konfigurieren der PoE-Leistung, Priorität und Klasse**

PoE am Switch

Ein PoE-Switch 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 dass eine Aktualisierung des physischen Netzwerkes oder eine Änderung der Netzwerk-Infrastruktur erforderlich ist.

Informationen zur PoE-Unterstützung in verschiedenen Modellen finden Sie unter **Switch-Modelle**.

Vorteile von PoE

PoE bietet die folgenden Vorteile:

- 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

Betrieb von PoE

PoE wird in den 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 der Switch bereitstellt, ist auf den vom Systemadministrator konfigurierten Wert begrenzt, unabhängig vom Ergebnis der Klassifizierung.
- Klassenbegrenzung: Die vom Switch maximal bereitgestellte Leistung ist von den Ergebnissen der Klassifizierung abhängig. Das heißt, sie wird entsprechend der Anforderung des Clients 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.

Sie können Folgendes festlegen:

- 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.
- Den maximal zulässigen Port-Wert als numerischem 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 bei einer hergestellten Verbindung mehr Leistung als konfiguriert verbrauchen möchte, führt der Switch Folgendes aus (unabhängig davon, ob der Switch sich im Klassenbegrenzungsmodus oder im Port-Begrenzungsmodus befindet):

- Er erhält den aktiven bzw. nicht aktiven Status des PoE-Port-Links.
- Er schaltet die Leistungsbereitstellung für den PoE-Port ab.
- Er protokolliert den Grund für das Abschalten der Leistung.
- Er generiert ein SNMP-Trap.

VORSICHT Berücksichtigen Sie Folgendes, wenn Sie Switches verbinden, die PoE bereitstellen können:

Die PoE-Modelle der Switches der Serien Sx200, Sx300 und Sx500 sind PSE-Geräte (Power Sourcing Equipment), die angeschlossene PD-Geräte (Powered Devices) mit Gleichstrom versorgen können. Dazu gehören VoIP-Telefone, IP-Kamera und drahtlose Zugangspunkte. Der PoE-Switch kann Strom für noch nicht dem Standard entsprechende ältere PoE-PD-Geräte (Powered Devices) erkennen

und liefern. Aufgrund der Unterstützung für ältere PoE-Geräte, besteht die Möglichkeit, dass ein als PSE fungierender PoE-Switch fälschlich ein angeschlossenes PSE (einschließlich anderer PoE-Switches) als älteres PD-Gerät erkennt und mit Strom versorgt.

Obwohl die PoE-Switches Sx200/300/500 PSE-Geräte sind und daher mit Wechselstrom betrieben werden sollten, können sie aufgrund der falschen Erkennung von einem anderen PSE als ältere PD-Geräte mit Strom versorgt werden. In diesem Fall funktioniert der PoE-Switch möglicherweise nicht richtig und kann die angeschlossenen PDs nicht richtig mit Strom versorgen.

Deaktivieren Sie PoE an den für PSEs verwendeten Ports der PoE-Switches, um die falsche Erkennung zu verhindern. Schalten Sie außerdem PSE-Geräte ein, bevor Sie sie mit einem PoE-Switch verbinden. 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.

Konfigurieren von PoE-Eigenschaften

Auf der Seite *PoE-Eigenschaften* können Sie den Portbegrenzungsmodus oder den Klassenbegrenzungsmodus für PoE auswählen und die zu generierenden PoE-Traps angeben.

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 dem Einschalten nach dem Neustart, während der Initialisierung und während der Systemkonfiguration deaktiviert, um eine Beschädigung von PD-Geräten zu vermeiden.

So konfigurieren Sie PoE am Switch und überwachen den aktuellen Leistungsverbrauch:

SCHRITT 1 Klicken Sie auf **Portverwaltung > PoE > Eigenschaften**. Die Seite *PoE-Eigenschaften* wird geöffnet.

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.

- **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.

Für jedes Gerät oder für alle Einheiten des Stacks werden die folgenden Zähler angezeigt:

- **Nennleistung**: Die Gesamtleistung, die der Switch für alle angeschlossenen PD-Geräte bereitstellen 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.

Konfigurieren der PoE-Leistung, Priorität und Klasse

Auf der Seite *PoE-Einstellungen* werden PoE-Systeminformationen zum Aktivieren der PoE-Funktion an den Schnittstellen und zum Überwachen des aktuellen Leistungsverbrauchs sowie die maximale Leistung pro Port angezeigt.

Wählen Sie **Port-Verwaltung > PoE > Einstellungen**. Die Seite *Einstellungen* wird geöffnet.

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 Switch 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. Der Switch kann die einzelnen Ports nicht mit genug 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 Switch-Modelle mit PoE-Unterstützung und der maximalen Leistung, die PoE-Ports zugewiesen werden kann, finden Sie unter **Switch-Modelle**.

So konfigurieren Sie PoE-Porteinstellungen:

SCHRITT 1 Wählen Sie **Port-Verwaltung > PoE > Einstellungen**. Die Seite *Einstellungen* wird geöffnet. Die Liste der folgenden Felder gilt für den Portbegrenzungsmodus. Im Leistungsmodus "Klassenbegrenzung" weichen die Felder geringfügig ab.

SCHRITT 2 Wählen Sie einen Port aus und klicken Sie auf **Bearbeiten**. Die Seite *PoE-Einstellungen bearbeiten* wird geöffnet. Die Liste der folgenden Felder gilt für den Portbegrenzungsmodus. Im Leistungsmodus "Klassenbegrenzung" weichen die Felder geringfügig ab.

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.

- **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**: Zeigt die an diesem Port maximal zulässige Leistung an.
- **Klasse**: Dieses Feld wird nur angezeigt, wenn auf der Seite *PoE-Eigenschaften* der Leistungsmodus "Klassenbegrenzung" festgelegt ist. Die Klasse bestimmt die bereitgestellte Leistung:

Klasse	Maximal vom Switch-Port bereitgestellte Leistung
0	15,4 Watt
1	4,0 Watt
2	7,0 Watt
3	15,4 Watt
4	30,0 Watt

- **Leistungsaufnahme**: Zeigt die Leistung in Milliwatt an, die dem angeschlossenen und versorgten Gerät an der ausgewählten Schnittstelle zugewiesen ist.
- **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-Gerätes 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.

12

VLAN-Verwaltung

In diesem Abschnitt werden die folgenden Themen behandelt:

- VLANs
- Konfigurieren der VLAN-Standardeinstellungen
- Erstellen von VLANs
- Konfigurieren der VLAN-Schnittstelleneinstellungen
- Definieren der VLAN-Mitgliedschaft
- GVRP-Einstellungen
- VLAN-Gruppen
- Voice-VLAN
- Zugriffsport-Multicast-TV-VLAN
- Kundenport-Multicast-TV-VLAN

VLANs

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 wird mit einer eindeutigen VID (VLAN-ID) mit einem Wert von 1 bis 4094 konfiguriert. 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 und 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 **Konfigurieren der 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 in Schicht 2 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. Der Switch fungiert als Bridge zum Anbieter und unterstützt portbasierte Dienstschnittstellen mit C-Tag.

Mit QinQ fügt der Switch ein ID-Tag, das so genannte Service-Tag (S-Tag) hinzu, 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 Verkehr 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.

Workflow der VLAN-Konfiguration

So konfigurieren Sie VLANs:

1. Ändern Sie bei Bedarf das Standard-VLAN anhand der im Abschnitt **Konfigurieren der VLAN-Standardeinstellungen** enthaltenen Informationen.
2. Erstellen Sie die erforderlichen VLANs entsprechend Abschnitt **Erstellen von VLANs**.
3. Legen Sie mithilfe des Abschnitts **Konfigurieren der VLAN-Schnittstelleneinstellungen** die gewünschte VLAN-Konfiguration für Ports fest und aktivieren Sie QinQ für eine Schnittstelle.
4. Weisen Sie den VLANs gemäß Abschnitt **Konfigurieren von Port zu VLAN** oder Abschnitt **Konfigurieren der VLAN-Mitgliedschaft** Schnittstellen zu.
5. Zeigen Sie im Abschnitt **Konfigurieren der VLAN-Mitgliedschaft** die aktuelle VLAN-Portmitgliedschaft für alle Schnittstellen an.

Konfigurieren der VLAN-Standardeinstellungen

Bei Verwendung der werkseitig festgelegten Standardeinstellungen erstellt der Switch 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 der Switch 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 der Switch an allen Ports des VLANs nach dem Konfigurieren und Neustarten des Switch Folgendes durch:

- Er entfernt die VLAN-Mitgliedschaft der Ports aus dem ursprünglichen Standard-VLAN (nur nach dem Neustart möglich).
- Er ändern die PVID (Port VLAN Identifier) der Ports in die VID des neuen Standard-VLAN.
- Die ursprüngliche Standard-VLAN-ID wird aus dem Switch 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**. Die Seite *VLAN-Standardeinstellungen* wird angezeigt.

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 Switch die **Aktuelle Standard-VLAN-ID**.

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.

Der Switch der Serie 300 unterstützt bis zu 4000 VLANs, einschließlich des Standard-VLANs.

Jedes VLAN muss mit einer eindeutigen VID (VLAN-ID) mit einem Wert von 1 bis 4094 konfiguriert werden. Der Switch reserviert die VID 4095 als 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 erstellen**. Die Seite *VLAN erstellen* wird angezeigt.

Auf der Seite *VLAN erstellen* werden für alle VLANs die folgenden Felder angezeigt:

- **VLAN-ID**: Benutzerdefinierte VLAN-ID.
- **VLAN-Name**: Benutzerdefinierter VLAN-Name.
- **Typ**: VLAN-Typ:
  - *Dynamisch*: 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 neues VLAN hinzuzufügen oder ein vorhandenes VLAN auszuwählen, und klicken Sie anschließend auf **Bearbeiten**, um die VLAN-Parameter zu ändern. Die Seite *VLAN hinzufügen/bearbeiten* wird angezeigt.

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 (VID) 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 Klicken Sie auf **Übernehmen**, um das VLAN bzw. die VLANs zu erstellen.

Konfigurieren der VLAN-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**. Die Seite *Schnittstelleneinstellungen* wird angezeigt.

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**. Die Seite *Schnittstelleneinstellung bearbeiten* wird angezeigt.

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. Der Switch befindet sich im QinQ-Modus, wenn er mindestens einen Kundenport hat. Weitere Informationen hierzu finden Sie unter **QinQ**.
- **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.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die Parameter werden in die aktuelle Konfigurationsdatei geschrieben.

Definieren der VLAN-Mitgliedschaft

Auf den Seiten *Port-VLAN* und *Port-VLAN-Mitgliedschaft* werden die VLAN-Mitgliedschaften der Ports in verschiedenen Darstellungen angezeigt. Sie können die Seiten verwenden, um Mitgliedschaften für VLANs hinzuzufügen oder diese zu 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.

Konfigurieren von Port zu VLAN

Auf der Seite *Port-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**. Die Seite *Port-VLAN* wird angezeigt.

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 oder allgemeiner 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 in der folgenden Liste die gewünschte Option wählen:

- **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.
- **Multicast-TV-VLAN**: Die Schnittstelle, die für Digital-TV mit Multicast-IP verwendet wird.
- **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.

Konfigurieren der VLAN-Mitgliedschaft

Auf der Seite *Port-VLAN-Mitgliedschaft* werden alle Ports des Geräts zusammen mit einer Liste der VLANs, zu denen der jeweilige Port gehört, angezeigt.

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 "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**. Die Seite *Port-VLAN-Mitgliedschaft* wird angezeigt.

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.** Die Seite *Mit VLAN verbinden* wird angezeigt.

SCHRITT 4 Geben Sie Werte für die folgenden Felder ein:

- **Schnittstelle**: Wählen Sie einen Port oder eine LAG 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).
  - **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.
  - **PVID**: Die Port-PVID wird auf dieses VLAN eingestellt. Wenn sich die Schnittstelle im Zugriffs-Modus oder Trunk-Modus befindet, richtet der Switch 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.

SCHRITT 6 Um die administrativen VLANs und Betriebs-VLANs an einer Schnittstelle anzuzeigen, klicken Sie auf **Details**.

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**. Die Seite *GVRP-Einstellungen* wird angezeigt.

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**. Die Seite *GVRP-Einstellung bearbeiten* wird angezeigt.

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

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.
- **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.

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-VLAN* dem VLAN zu.

Zuweisen MAC-basierter VLAN-Gruppen

Diese Funktion ist nur verfügbar, wenn sich der Switch im Schicht-2-Systemmodus befindet.

So weisen Sie einer VLAN-Gruppe eine MAC-Adresse zu:

SCHRITT 1 Klicken Sie auf **VLAN-Verwaltung** > **VLAN-Gruppen** > **MAC-basierte Gruppen**. Die Seite *MAC-basierte Gruppen* wird angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *MAC-basierte Gruppe hinzufügen* wird geöffnet.

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.

Zuordnen von VLAN-Gruppen zu VLANs pro Schnittstelle

Diese Funktion ist nur verfügbar, wenn sich der Switch im Schicht-2-Systemmodus und der Port bzw. die LAG im allgemeinen Modus befindet.

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**. Die Seite *MAC-basierte Gruppen für VLAN* wird angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *Gruppenzuordnung für VLAN hinzufügen* wird geöffnet.

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.

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)**
- **Konfigurieren von Voice-VLAN**

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.

Der Switch wird immer als VLAN-fähiger Switch betrieben.

Der Switch unterstützt ein einziges Voice-VLAN. Das Voice-VLAN heißt 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 der Switch im Modus "Telefonie-OUI" befindet oder wenn die Option "Auto-Smartport" aktiviert ist.

Dynamische Voice-VLAN-Modi

Der Switch 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 der Switch im Telefonie-OUI-Modus befindet und ein Port manuell als Beitrittskandidat für das Voice-VLAN konfiguriert ist, fügt der Switch den Port dynamisch dem Voice-VLAN hinzu, wenn er 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 **Konfigurieren der 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.

Der Switch 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 Switch 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 Firmware-Version Auto-Voice-VLAN sofort ohne Konfiguration unterstützt. Sie gilt auch für nicht konfigurierte Switches, die auf die Firmware-Version 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 den Switch 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. Der Switch 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 der Switch 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 Switch 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 der Switch im Schicht-2-Systemmodus befindet, kann er mit ausschließlich VSDP-fähigen Switches im gleichen Verwaltungs-VLAN synchronisieren. Wenn sich der Switch im Schicht-3-Systemmodus befindet, kann er mit VSDP-fähigen Switches synchronisieren, die sich in den im Switch 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 der Switch 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 der Switch 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. Der Switch 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 kann nicht DVA (Dynamic VLAN Assignment) unterstützen.
- 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 Kandidaten-Ports 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 Switch-Standardkonfiguration 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 die Telefonie-OUI auf der Seite *Telefonie-OUI*.

SCHRITT 3 Konfigurieren Sie auf der Seite *Telefonie-OUI-Schnittstelle* die Telefonie-OUI-VLAN-Mitgliedschaft für Ports.

Konfigurieren von Voice-VLAN

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

- **Konfigurieren der Voice-VLAN-Eigenschaften**
- **Anzeigen von Auto-Voice-VLAN-Einstellungen**
- **Konfigurieren der 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 Seite *Eigenschaften* wird angezeigt.

- Die im Switch 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 der Switch 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 den Switch sofort aktiviert und verwendet, sofern die Option aktiviert ist.
  - *Durch externen Voice-VLAN-Auslöser*: Auto-Voice-VLAN wird nur dann für den Switch aktiviert und verwendet, wenn der Switch 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.

Anzeigen von 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**. Die Seite *Auto-Voice-VLAN* wird angezeigt.

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-Switch 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 Switch. 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 Switch konfigurierte Voice-VLAN sowie alle von direkt verbundenen Nachbargeräten angekündigten lokalen Voice-VLAN-Konfigurationen an. Es werden die folgenden Felder angezeigt:

- **Schnittstelle**: Zeigt die Schnittstelle an, an der die Voice-VLAN-Konfiguration empfangen oder konfiguriert wurde. Wenn *n/v* angezeigt wird, wurde die Konfiguration im Switch 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 Switch.
  - *Statisch*: Im Switch 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 Switch verwendet wurde. Folgende Optionen stehen zur Verfügung:
  - *Ja*: Der Switch 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.

Konfigurieren der 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:

- **Hinzufügen von OUIs zur Telefonie-OUI-Tabelle**
- **Hinzufügen von Schnittstellen zu einem Voice-VLAN auf der Grundlage von OUIs**

Hinzufügen von OUIs zur 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* wird angezeigt.

Auf der Seite *Telefonie-OUI* werden die folgenden Felder angezeigt:

- **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 Switch 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.

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**. Die Seite *Telefonie-OUI hinzufügen* wird angezeigt.

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.

Hinzufügen von Schnittstellen zu einem Voice-VLAN auf der Grundlage von OUIs

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* wird angezeigt.

Auf der Seite *Telefonie-OUI-Schnittstelle* werden Voice-VLAN-OUI-Parameter für alle Schnittstellen angezeigt.

SCHRITT 2 Um eine Schnittstelle als Kandidatenport für das Telefonie-OUI-basierte Voice-VLAN zu konfigurieren, klicken Sie auf **Bearbeiten**. Die Seite *Schnittstelleneinstellungen bearbeiten* wird angezeigt.

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 gleichen Daten-VLAN befinden (Schicht 2, isoliert) und über eine andere VLAN-ID-Mitgliedschaft mit dem Switch verbunden sind, können den gleichen Multicast-Stream nutzen, indem die Ports der gleichen 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 **Konfigurieren der VLAN-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 **Konfigurieren der VLAN-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.
- Der Switch führt IGMP-Snooping aus und konfiguriert den Zugriffsport gemäß seiner Multicast-Mitgliedschaft im Multicast-TV-VLAN.

Der Switch 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 **discard**.
  - Der MSTP-Status für das Zugriffs-VLAN lautet **discard**.
  - Der MSTP-Status für das Multicast-TV-VLAN lautet **discard** 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 Quell-Port und alle Empfängerports müssen statische Mitglieder des gleichen Daten-VLANs sein.	Der Quell-Port 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).

	Reguläres VLAN	Multicast-TV-VLAN
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-TV-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 Seite *Multicast-Gruppe zu VLAN* wird angezeigt.

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**. Die Seite *Port-Multicast-VLAN-Mitgliedschaft* wird angezeigt.

SCHRITT 2 Wählen Sie im Feld **Multicast-TV-VLAN** ein VLAN aus.

SCHRITT 3 Die Liste **Zugriffsports für Kandidaten** enthält alle im Gerät konfigurierten Zugriffsports. Verschieben Sie die gewünschten Ports aus dem Feld **Zugriffsports für Kandidaten** in das Feld **Zugriffsports für Mitglieder**.

SCHRITT 4 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 Access Switch 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 Access Switch 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. (Auf der 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.

Zuordnen von CPE-VLANs zu Multicast-TV-VLANs

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.** Die Seite *CPE-VLAN zu VLAN* wird angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *CPE-VLAN-Zuordnung hinzufügen* wird angezeigt.

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.

CPE-Port-Multicast-VLAN-Mitgliedschaft

Die den Multicast-VLANs zugeordneten Ports müssen als Kundenports konfiguriert werden (siehe **Konfigurieren der VLAN-Schnittstelleneinstellungen**).

Auf der Seite *Port-Multicast-VLAN-Mitgliedschaft* können Sie diese Ports wie unter **Port-Multicast-VLAN-Mitgliedschaft** beschrieben Multicast-TV-VLANs zuordnen.

13

Konfigurieren des Spanning Tree-Protokolls

In diesem Abschnitt wird das Spanning Tree-Protokoll (STP) (IEEE802.1D und IEEE802.1Q) beschrieben. Die folgenden Themen werden behandelt:

- **STP-Modi**
- **Konfigurieren des STP-Status und der globalen Einstellungen**
- **Festlegen von Spanning Tree-Schnittstelleneinstellungen**
- **Konfigurieren der Einstellungen für Rapid Spanning Tree**
- **Multiple Spanning Tree**
- **Festlegen von MSTP-Eigenschaften**
- **Zuordnen von VLANs zu einer MSTP-Instanz**
- **Definieren von MSTP-Instanzeinstellungen**
- **Festlegen von 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.

Der Switch unterstützt die folgenden Spanning Tree-Protokollversionen:

- 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.

Konfigurieren des STP-Status und der globalen 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 einzelnen 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**. Die Seite *STP-Status und globale Einstellungen* wird angezeigt.

SCHRITT 2 Geben Sie die Parameter ein.

Globale Einstellungen:

- **Spanning Tree-Status**: Aktivieren oder deaktivieren Sie STP für den Switch.
- **STP-Betriebsmodus**: Wählen Sie den STP-Betriebsmodus aus.
- **BPDU-Bearbeitung**: Wählen Sie aus, wie BPDU-Pakete (Bridge Protocol Data Unit) verwaltet werden, wenn STP an dem Port oder Switch 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. Die Werte liegen im Bereich von 1 bis 10 Sekunden.
- **Maximales Alter**: Legen Sie das Intervall in Sekunden fest, das der Switch ohne Erhalt einer Konfigurationsnachricht abwarten kann, bevor er 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 **Festlegen von Spanning Tree-Schnittstelleneinstellungen**.

Designierte Root:

- **Bridge-ID**: Eine Verkettung aus Bridge-Priorität und MAC-Adresse des Switch.
- **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.

Festlegen von Spanning Tree-Schnittstelleneinstellungen

Auf der Seite *STP-Schnittstelleneinstellungen* können Sie STP auf Portebene 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**. Die Seite *STP-Schnittstelleneinstellungen* wird angezeigt.

SCHRITT 2 Wählen Sie eine Schnittstelle aus und klicken Sie auf **Bearbeiten**. Die Seite *Schnittstelleneinstellungen bearbeiten* wird angezeigt.

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 Schlaufen aufgelöst werden, bevor Fast Link aktiviert wird.
  - *Deaktivieren*: Deaktiviert Fast Link.

    HINWEIS Es wird empfohlen, den Wert auf "Autom." festzulegen, damit der Switch den Port auf den Fast Link-Modus festlegt, wenn ein Host mit ihm verbunden ist, oder bei Verbindung mit einem anderen Switch einen regulären STP-Port festlegt. Dadurch können Schleifen verhindert werden.
- **Root Guard**: Aktiviert oder deaktiviert Root Guard für den Switch. 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 an dem Port oder Switch deaktiviert ist. BPDUs werden für die Übertragung von Spanning Tree-Informationen verwendet.
  - *Globale Einstellungen verwenden*: Wählen Sie diese Option aus, 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 Schlaufen 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.

Konfigurieren der 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**. Die Seite *STP-Status und globale Einstellungen* wird angezeigt. 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**. Die Seite *RSTP-Schnittstelleneinstellungen bearbeiten* wird angezeigt.

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.
  - *Autom.*: Ermittelt den Switch-Status 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 **Konfigurieren des STP-Status und der globalen 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 **Zuordnen von 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:
   - **Festlegen von MSTP-Eigenschaften**
   - **Definieren von MSTP-Instanzeinstellungen**
   - **Zuordnen von VLANs zu einer MSTP-Instanz**

Festlegen von 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**. Die Seite *STP-Status und globale Einstellungen* wird angezeigt. Aktivieren Sie MSTP.

SCHRITT 2 Klicken Sie auf **Spanning Tree** > **MSTP-Eigenschaften**. Die Seite *MSTP-Eigenschaften* wird angezeigt.

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.

Zuordnen von 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 300 können Sie neben Instanz 0 bis zu sieben MST-Instanzen (vordefiniert von 1 - 7) definieren.

VLANs, die nicht explizit einer der MST-Instanzen zugeordnet sind, werden vom Switch automatisch der CIST-Instanz (Core and 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* wird angezeigt.

Die Seite *VLAN zu MSTP-Instanz* enthält die folgenden Felder:

- **MST-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**. Die Seite *MST-Instanz zu VLAN bearbeiten* wird angezeigt.

SCHRITT 3 Geben Sie die Parameter ein.

- **MST-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.

Definieren von 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**. Die Seite *MSTP-Instanzeinstellungen* wird angezeigt.

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 Switches 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.

Festlegen von 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**. Die Seite *MSTP-Schnittstelleneinstellungen* wird angezeigt.

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**. Die Seite *MSTP-Schnittstelleneinstellungen bearbeiten* wird angezeigt.

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**: Legen Sie den Beitrag des Ports zu den Root-Pfadkosten fest, oder verwenden Sie den Standardwert.
- **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 an:
  - *Classic STP*: Für den Port ist Classic STP aktiviert.
  - *Rapid STP*: Für den Port ist Rapid STP aktiviert.
  - *MSTP*: Für den Port ist MSTP aktiviert.
- **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.

14

Verwalten von MAC-Adresstabellen

In diesem Abschnitt wird beschrieben, wie Sie dem System MAC-Adressen hinzufügen. Die folgenden Themen werden behandelt:

- **Konfigurieren von statischen MAC-Adressen**
- **Verwalten von dynamischen MAC-Adressen**
- **Definieren reservierter MAC-Adressen**

MAC-Adresstypen

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 beim Switch eingehenden Frame erscheint, wird der Tabelle für dynamische Adressen hinzugefügt. Diese MAC-Adresse wird während eines konfigurierbaren Zeitraums beibehalten. Wenn beim Switch vor Ablauf dieses Zeitraums kein anderer Frame mit der gleichen Quell-MAC-Adresse eingeht, wird der Eintrag aus der Tabelle gelöscht.

Wenn beim Switch ein Frame eingeht, sucht der Switch 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.

Der Switch unterstützt maximal 8.000 statische und dynamische MAC-Adressen.

Konfigurieren von statischen MAC-Adressen

Statische MAC-Adressen werden einer bestimmten physischen Schnittstelle und einem bestimmten VLAN des Switch 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**. Die Seite *Statische Adressen* wird geöffnet.

Auf der Seite *Statische Adressen* werden die definierten statischen Adressen angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *Statische Adresse hinzufügen* wird geöffnet.

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 (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.

Verwalten von dynamischen MAC-Adressen

Die Tabelle der dynamischen Adressen (Bridging-Tabelle) enthält die MAC-Adressen, die durch Überwachen der Quelladressen von beim Switch 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 kein entsprechender Verkehr empfangen wird. Dieser Zeitraum wird als Fälligkeitsintervall bezeichnet.

Konfigurieren der Fälligkeitszeit für dynamische MAC-Adressen

So konfigurieren Sie das Fälligkeitsintervall für dynamische Adressen:

SCHRITT 1 Klicken Sie auf **MAC-Adresstabellen > Einstellungen für dynamische Adressen**. Die Seite *Einstellungen für dynamische Adressen* wird geöffnet.

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**. Die Seite *Dynamische Adressen* wird geöffnet.

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 Geben Sie in **Sortierschlüssel für dynamische Adresstabelle** den Schlüssel ein, nach dem die Tabelle sortiert werden soll. Die Adresstabelle kann anhand der VLAN-ID, der MAC-Adresse oder der Schnittstelle sortiert werden.

SCHRITT 4 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**.

Definieren reservierter MAC-Adressen

Wenn der Switch 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**. Die Seite *Reservierte MAC-Adressen* wird geöffnet.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *Reservierte MAC-Adresse hinzufügen* wird geöffnet.

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:
  - *Verwerfen*: Löschen des Pakets.
  - *Bridge*: Weiterleiten des Pakets an alle VLAN-Mitglieder.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Es wird eine neue MAC-Adresse reserviert.

15

Konfigurieren der Multicast-Weiterleitung

In diesem Abschnitt wird die Funktion der Multicast-Weiterleitung beschreiben. Der Abschnitt behandelt folgende Themen:

- **Multicast-Weiterleitung**
- **Definieren von Multicast-Eigenschaften**
- **Hinzufügen von MAC-Gruppenadressen**
- **Hinzufügen von IP-Multicast-Gruppenadressen**
- **Konfigurieren von IGMP-Snooping**
- **MLD-Snooping**
- **Abfragen von IGMP/MLD-IP-Multicast-Gruppen**
- **Definieren von Multicast-Router-Ports**
- **Definieren des Multicast-Merkmals "Alle weiterleiten"**
- **Definieren der Einstellungen für nicht registriertes 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.

Damit die Multicast-Weiterleitung in IP-Subnetzen funktioniert, müssen die Knoten und Router Multicast-fähig sein. Ein Multicast-fähiger Knoten muss folgende Funktionen erfüllen:

- Senden und Empfangen von Multicast-Paketen.
- Registrieren der Multicast-Adressen, die der Knoten mit lokalen Routern abhört, damit lokale und entfernte Router das Multicast-Paket an die Knoten übertragen können.

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, einen Switch mit IGMP-Snooping (IGMP, Internet Group Membership Protocol) oder MLD-Snooping (MLD, Multicast Listener Discovery) sowie einen Multicast-Client, der einen Multicast-Strom empfangen möchte. In diesem Setup sendet der Router regelmäßig IGMP-Abfragen.

HINWEIS MLD für IPv6 wird von IGMP v2 für IPv4 abgeleitet. Obwohl sich die Beschreibung in diesem Kapitel hauptsächlich auf IGMP bezieht, wird auch die Abdeckung von MLD, wo vorhanden, beschrieben.

Diese Abfragen erreichen den Switch, der die Abfragen dann an das VLAN flutet und lernt, an welchem Router sich ein Multicast-Router (MRouter) befindet. Wenn ein Router die IGMP-Abfragenachricht empfängt, antwortet er mit einer IGMP-Beitrittsnachricht, die besagt, dass der Host einen bestimmten Multicast-Strom empfangen möchte, und optional, ob er sie von einer bestimmten Quelle empfangen möchte. Der Switch mit IGMP-Snooping analysiert die Beitrittsnachricht und lernt, dass der Multicast-Strom, der vom Host abgefragt wurde, an diesen bestimmten Port weitergeleitet werden muss. Dann leitet er nur die IGMP-Nachricht über den Beitritt zum MRouter weiter. Wenn der MRouter eine IGMP-Beitrittsnachricht empfängt, lernt er ebenfalls, dass die Schnittstelle, von der er die Beitrittsnachrichten empfängt, einen bestimmten Multicast-Strom empfangen möchte. Der MRouter leitet den angefragten Multicast-Strom an die Schnittstelle weiter.

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 den Switch aktiviert ist und dieser einen Frame für einen Multicast-Strom empfängt, leitet er den Multicast-Frame an alle Ports, die mithilfe von IGMP-Beitrittsnachrichten für den Empfang des Multicast-Stroms registriert wurden.

Der Switch kann Multicast-Ströme mit einer der folgenden Optionen weiterleiten:

- Multicast-MAC-Gruppenadresse
- IP-Multicast-Gruppenadresse (G)
- Eine Kombination der Quell-IP-Adresse (S) und der Ziel-IP-Multicast-Gruppenadresse (G) des Multicast-Pakets.

Eine dieser Optionen kann über VLAN konfiguriert werden.

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

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 einen Switch in einem VLAN aktiviert ist, analysiert dieser alle IGMP/MLD-Pakete, die er von dem VLAN empfangen hat, mit dem der Switch und die Multicast-Router im Netzwerk verbunden sind.

Wenn ein Switch lernt, dass ein Host IGMP/MLD-Nachrichten für die Registrierung zum Empfang eines Multicast-Stroms gegebenenfalls von einer bestimmten Quelle verwendet, fügt der Switch die Registrierung seiner Multicast-Weiterleitungsdatenbank hinzu.

Mit IGMP/MLD-Snooping kann die Übertragung von IP-Anwendungen mit großen Bandbreiten im Multicast-Datenverkehr erheblich reduziert werden. Ein Switch, der IGMP/MLD-Snooping verwendet, leitet nur Multicast-Datenverkehr an die Hosts weiter, die an diesem Datenverkehr interessiert sind. Durch die Reduzierung des Multicast-Datenverkehrs wird auch die Paketverarbeitung am Switch und der Workload der End-Hosts verringert, da diese nicht den gesamten im Netzwerk generierten Multicast-Datenverkehr empfangen und filtern müssen.

Folgende Versionen werden unterstützt:

- IGMP v1/v2/ v3
- MLD v1/v2
- Ein einfacher IGMP-Snooping-Abfrager

Zur Unterstützung des IGMP-Protokolls in einem bestimmten Subnetz ist ein IGMP-Abfrager erforderlich. Im Allgemeinen ist ein Multicast-Router gleichzeitig ein IGMP-Abfrager. Wenn mehrere IGMP-Abfrager in einem Subnetz vorhanden sind, wählen die Abfrager einen einzigen Abfrager als Hauptabfrager aus.

Der Switch kann als IGMP-Abfrager oder, wenn kein normaler IGMP-Abfrager vorhanden ist, als Backup-Abfrager konfiguriert werden. Der Switch ist kein IGMP-Abfrager mit vollem Funktionsumfang.

Wenn der Switch als IGMP-Abfrager aktiviert wird, startet er, wenn 60 Sekunden lang kein IGMP-Datenverkehr (Abfragen) von einem Multicast-Router erkannt wurde. Sind andere IGMP-Abfrager vorhanden, kann der Switch möglicherweise die Übertragung von Abfragen auf der Grundlage der Ergebnisse des Standardauswahlprozesses des Abfragers stoppen.

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.

Definieren von Multicast-Eigenschaften

Auf der Seite *Eigenschaften* können Sie den Bridge-Multicast-Filterstatus konfigurieren.

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 *Eigenschaften* den Bridge-Multicast-Filterstatus.

Wenn die Filterung aktiviert ist, werden die Multicast-Frames an eine Untergruppe der Ports im entsprechenden VLAN weitergeleitet, die in der Multicast-Weiterleitungsdatenbank definiert ist. Die Multicast-Filterung ist für den gesamten Datenverkehr verfügbar. Standardmäßig wird dieser Datenverkehr an alle relevanten Ports geflutet. Sie können die Weiterleitung jedoch auf eine kleinere Untergruppe begrenzen.

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 mit (*,G) notiert.

Es gibt folgende Möglichkeiten zur Weiterleitung von Multicast-Frames:

- **MAC-Gruppenadresse**: Auf der Grundlage der Ziel-MAC-Adresse im Ethernet-Frame.

  HINWEIS Wie bereits erwähnt, können Sie eine oder mehrere IP-Multicast-Gruppenadressen einer MAC-Gruppenadresse zuordnen. 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).

Durch Auswahl des Weiterleitungsmodus können Sie die Methode definieren, die die Hardware zur Erkennung von Multicast-Flow verwendet. Hierzu können Sie eine der folgenden Optionen verwenden: MAC-Gruppenadresse, IP-Gruppenadresse oder Quellspezifische IP-Gruppenadresse.

(S,G) wird von IGMPv3 und MLDv2 unterstützt. IGMPv1/2 und MLDv1 unterstützen dagegen nur (*,G), das heißt lediglich die Gruppen-ID.

Der Switch unterstützt maximal 256 statische und dynamische Multicast-Gruppenadressen.

Wählen Sie folgende Methode, um die Multicast-Filterung zu aktivieren:

SCHRITT 1 Klicken Sie auf **Multicast > Eigenschaften**. Die Seite *Eigenschaften* wird geöffnet.

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.

Hinzufügen von MAC-Gruppenadressen

Der Switch unterstützt die Weiterleitung von eingehendem Multicast-Datenverkehr auf der Grundlage der Multicast-Gruppeninformationen. Diese Informationen werden aus den empfangenen IGMP/MLD-Paketen oder aus der manuellen Konfiguration abgeleitet und in der Multicast-Weiterleitungsdatenbank gespeichert.

Wenn ein Frame von einem VLAN empfangen wird, das für die Weiterleitung von Multicast-Strömen an MAC-Gruppenadressen konfiguriert ist, und die Zieladresse eine Schicht-2-Multicast-Adresse ist, wird der Frame an alle Ports weitergeleitet, die Mitglied der MAC-Gruppenadresse sind.

Die Seite *MAC-Gruppenadresse* hat die folgenden Funktionen:

- Abfrage und Anzeige von Informationen aus der Multicast-Weiterleitungsdatenbank zu einer bestimmten VLAN-ID oder einer bestimmten MAC-Adressengruppe. 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.

Auf der Seite *IP-Multicast-Gruppenadresse* können Sie die Weiterleitungsinformationen im Modus *IP-Adressengruppe* oder *IP- und Quellgruppe* anzeigen.

Gehen Sie wie folgt vor, um MAC-Multicast-Gruppen zu definieren und anzuzeigen:

SCHRITT 1 Klicken Sie auf **Multicast > MAC-Gruppenadresse**. Die Seite *MAC-Gruppenadresse* wird geöffnet.

SCHRITT 2 Geben Sie die Parameter 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, werden auf der Seite alle MAC-Gruppenadressen aus dem ausgewählten VLAN angezeigt.

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. Die Seite *MAC-Gruppenadresse hinzufügen* wird geöffnet.

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 die aktuelle Konfigurationsdatei geschrieben.

Zum Konfigurieren und Anzeigen der Registrierung der Schnittstellen in der Gruppe, wählen Sie eine Adresse aus, und klicken Sie auf **Details**. Die Seite *MAC-Gruppenadresseinstellungen* wird geöffnet.

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 den Port oder die LAG aus, der bzw. die im Menü **Filter: Schnittstellentyp** angezeigt werden soll.

SCHRITT 8 Klicken Sie auf **Los**, um die Port- oder LAG-Mitgliedschaft 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).

Hinzufügen von IP-Multicast-Gruppenadressen

Die Seite *IP-Multicast-Gruppenadresse* hat Ähnlichkeit mit 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 *IP-Multicast-Gruppenadresse* wird geöffnet.

Die Seite zeigt alle IP-Multicast-Gruppenadressen an, 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 einem Switch im Schicht-2-Systemmodus aktiviert sind, wird die IP-Multicast-Adresse von Bonjour angezeigt.

SCHRITT 4 Klicken Sie auf **Hinzufügen**, um eine statische IP-Multicast-Gruppenadresse hinzuzufügen. Die Seite *IP-Multicast-Gruppenadresse hinzufügen* wird geöffnet.

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**. Die Seite *IP-Multicast-Schnittstelleneinstellungen* wird geöffnet.

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.

- **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.

Konfigurieren von IGMP-Snooping

Damit selektive Multicast-Weiterleitung (IPv4) unterstützt wird, muss (auf der Seite *Eigenschaften*) die Bridge-Multicast-Filterung aktiviert sein. Außerdem muss (auf der Seite *IGMP-Snooping*) IGMP-Snooping global und für jedes relevante VLAN aktiviert sein.

Standardmäßig leitet ein Schicht-2-Switch Multicast-Frames an alle Ports des entsprechenden VLAN weiter, wobei der Frame im Wesentlichen wie ein Broadcast behandelt wird. Mit IGMP-Snooping leitet der Switch Multicast-Frames an Ports weiter, an denen Multicast-Clients registriert sind.

HINWEIS Der Switch unterstützt IGMP-Snooping nur für statische VLANs. Für dynamische VLANs unterstützt er kein IGMP-Snooping.

Ist IGMP-Snooping global oder für ein bestimmtes VLAN aktiviert, werden alle IGMP-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 (MRouter) verbunden sind, die IGMP-Abfragen generieren.
- welche Ports PIM-, DVMRP- oder IGMP-Abfrageprotokolle empfangen.

Diese werden auf der Seite *IGMP-Snooping* angezeigt.

Die Ports, die um Beitritt zu einer bestimmten Multicast-Gruppe bitten, geben einen IGMP-Bericht aus, aus dem hervorgeht, welchen Gruppen der Host beitreten möchte. Daraus wird ein Weiterleitungseintrag in der Multicast-Weiterleitungsdatenbank erstellt.

Mit dem IGMP-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.

Die Geschwindigkeit der Aktivität des IGMP-Abfragers muss auf die Switches abgestimmt sein, bei denen IGMP-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. Hierzu verwenden Sie die Seite *IGMP-Snooping bearbeiten*.

Gehen Sie wie folgt vor, um IGMP-Snooping zu aktivieren und den Switch als IGMP-Snooping-Abfrager in einem VLAN zu bestimmen:

SCHRITT 1 Klicken Sie auf **Multicast** > **IGMP-Snooping**. Die Seite *IGMP-Snooping* wird geöffnet.

SCHRITT 2 Aktivieren oder deaktivieren Sie den IGMP-Snooping-Status.

Wenn IGMP-Snooping global aktiviert ist, kann das den Netzwerkverkehr überwachende Gerät erkennen, welche Hosts eine Anfrage zum Empfang von Multicast-Verkehr gestellt haben.

Der Switch führt nur dann IGMP-Snooping aus, wenn sowohl IGMP-Snooping als auch Bridge-Multicast-Filterung aktiviert sind.

SCHRITT 3 Wählen Sie ein VLAN aus, und klicken Sie auf **Bearbeiten**. Die Seite *IGMP-Snooping bearbeiten* wird geöffnet.

In einem Netzwerk kann nur jeweils ein IGMP-Abfrager vorhanden sein. Der Switch unterstützt die standardmäßige Auswahl des IGMP-Abfragers. Einige Werte der Betriebsparameter dieser Tabelle werden vom ausgewählten Abfrager gesendet. Die anderen Werte werden vom Switch abgeleitet.

SCHRITT 4 Geben Sie die Parameter ein.

- **VLAN-ID**: Wählen Sie die VLAN-ID aus, für die IGMP-Snooping definiert ist.
- **IGMP-Snooping-Status**: Aktivieren oder deaktivieren Sie die Überwachung des Netzwerkverkehrs für das ausgewählte VLAN.
- **IGMP-Snooping-Status für Betrieb**: Zeigt den aktuellen IGMP-Snooping-Status für das ausgewählte VLAN an.
- **Autom. Lernen MRouter-Ports**: Aktivieren oder deaktivieren Sie die Funktion zum automatischen Lernen der Ports, an die der MRouter angeschlossen ist.

- **Abfragerobustheit**: Geben Sie den Wert für die Robustheitsvariable ein, der verwendet werden soll, wenn dieser Switch als Abfrager ausgewählt wurde.
- **Abfragerobustheit für Betrieb**: Zeigt die Robustheitsvariable an, die vom ausgewählten Abfrager gesendet wurde.
- **Abfrageintervall**: Geben Sie das Intervall zwischen den allgemeinen Abfragen ein, das verwendet werden soll, wenn dieser Switch als Abfrager ausgewählt wurde.
- **Abfrageintervall für Betrieb**: Das Zeitintervall in Sekunden zwischen den allgemeinen Abfragen, die vom ausgewählten Abfrager gesendet wurden.
- **Max. Abfrageantwortintervall**: Geben Sie die Verzögerung ein, mit der der maximale Antwortcode berechnet werden soll, der in die regelmäßigen allgemeinen Abfragen eingegeben wurde.
- **Max. Abfrageantwortintervall für Betrieb**: Zeigt das maximale Abfrageantwortintervall an, das in den vom ausgewählten Abfrager gesendeten allgemeinen Abfragen enthalten ist.
- **Abfragezähler letztes Mitglied für Betrieb**: Geben Sie die Anzahl der gruppenspezifischen IGMP-Abfragen ein, die gesendet wurden, bevor der Switch annimmt, dass keine Mitglieder mehr in der Gruppe vorhanden sind, wenn der Switch der ausgewählte Abfrager ist.
- **Abfragezähler letztes Mitglied für Betrieb**: Zeigt den Wert für das letzte Mitglied des Abfragezähler für Betrieb an.
- **Abfrageintervall letztes Mitglied**: Geben Sie den Wert für die maximale Antwortverzögerung ein, der verwendet werden soll, wenn der Switch den Wert für die maximale Reaktionszeit nicht aus den vom ausgewählten Abfrager gesendeten gruppenspezifischen Abfragen ableiten kann.
- **Abfrageintervall letztes Mitglied für Betrieb**: Zeigt das Abfrageintervall für das letzte Mitglied an, das vom ausgewählten Abfrager gesendet wurde.
- **Sofortiges Leave**: Aktivieren Sie "Sofortiges Leave", um die Zeit zu erhöhen, die benötigt wird, um einen Multicast-Strom zu blockieren, der von einem teilnehmenden Port gesendet wurde, wenn eine IGMP-Gruppen-Leave-Nachricht an diesem Port empfangen wurde.
- **IGMP-Abfragerstatus**: Aktivieren oder deaktivieren Sie den IGMP-Abfrager.
- **Quell-IP-Adresse von Administrationsabfrager**: Wählen Sie die Quell-IP-Adresse des IGMP-Abfragers aus. Dies kann die IP-Adresse des VLAN oder die Verwaltungs-IP-Adresse sein.

- **Quell-IP-Adresse von Administrationsabfrager für Betrieb**: Zeigt die Quell-IP-Adresse des ausgewählten Abfragers an.
- **IGMP-Abfragerversion**: Wählen Sie die IGMP-Version aus, die verwendet werden soll, wenn der Switch der ausgewählte Abfrager wird. Wählen Sie IGMPv3 aus, wenn Switches und/oder Multicast-Router im VLAN vorhanden sind, die quellspezifische IP-Multicast-Weiterleitung ausführen.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

MLD-Snooping

Hosts verwenden das MLD-Protokoll, um ihre Teilnahme an Multicast-Sitzungen zu melden und der Switch verwendet MLD-Snooping, um Multicast-Mitgliedschaftslisten zu erstellen. Auf der Grundlage dieser Listen werden Multicast-Pakete nur an Switch-Ports weitergeleitet, an denen Hostknoten vorhanden sind, die Mitglieder der Multicast-Gruppen sind. Der Switch unterstützt keine MLD-Abfrager.

Hosts verwenden das MLD-Protokoll, um ihre Teilnahme an den Multicast-Sitzungen zu berichten.

Der Switch unterstützt zwei Versionen des MLD-Snooping:

- MLDv1-Snooping erkennt MLDv1-Kontrollpakete und richtet Bridging für den Datenverkehr auf der Grundlage der IPv6-Ziel-Multicast-Adressen ein.
- MLDv2-Snooping verwendet MLDv2-Kontrollpakete, um Datenverkehr auf der Grundlage der IPv6-Quelladresse und der Ziel-IPv6-Multicast-Adresse weiterzuleiten.

Die aktuelle MLD-Version wird vom Multicast-Router im Netzwerk ausgewählt.

Mit einem dem IGMP-Snooping ähnlichen Verfahren werden die MLD-Frames gesnoopt, wenn sie vom Switch von den Stationen an einen Upstream-Multicast-Router oder umgekehrt weitergeleitet werden. Mit dieser Funktion kann ein Switch erkennen,

- auf welchen Ports Stationen vorhanden sind, die an einem Beitritt zu einer spezifischen Multicast-Gruppe interessiert sind.
- auf welchen Ports Multicast-Router vorhanden sind, die Multicast-Frames senden.

Mit diesem Wissen können irrelevante Ports (Ports, auf denen keine Stationen für den Empfang einer bestimmten Multicast-Gruppe registriert sind) vom Weiterleitungssatz eines eingehenden Multicast-Frames ausgeschlossen werden.

Wenn Sie MLD-Snooping zusammen mit den manuell konfigurierten Multicast-Gruppen aktivieren, ergibt sich ein Zusammenschluss der Multicast-Gruppen und Port-Mitgliedschaften, die von der manuellen Einstellung und der dynamischen Erkennung durch das MLD-Snooping abgeleitet werden. Nur die statischen Definitionen bleiben bei einem Neustart des Systems erhalten.

Gehen Sie wie folgt vor, um MLD-Snooping zu aktivieren:

SCHRITT 1 Klicken Sie auf **Multicast** > **MLD-Snooping**. Die Seite *MLD-Snooping* wird geöffnet.

SCHRITT 2 Aktivieren oder deaktivieren Sie den **MLD-Snooping-Status**. Wenn MLD-Snooping global aktiviert ist, kann das den Netzwerkverkehr überwachende Gerät erkennen, welche Hosts eine Anfrage zum Empfang von Multicast-Verkehr gestellt haben. Der Switch führt nur dann MLD-Snooping aus, wenn sowohl MLD-Snooping als auch Bridge-Multicast-Filterung aktiviert sind.

SCHRITT 3 Wählen Sie ein VLAN aus, und klicken Sie auf **Bearbeiten**. Die Seite *MLD-Snooping bearbeiten* wird geöffnet.

SCHRITT 4 Geben Sie die Parameter ein.

- **VLAN-ID**: Wählen Sie die VLAN-ID aus.
- **MLD-Snooping-Status**: Aktivieren oder deaktivieren Sie MLD-Snooping für das VLAN. Der Switch überwacht den Netzwerkdatenverkehr und legt damit fest, welche Hosts Multicast-Datenverkehr empfangen möchten. Der Switch führt nur dann MLD-Snooping aus, wenn sowohl MLD-Snooping als auch Bridge-Multicast-Filterung aktiviert sind.
- **MLD-Snooping-Betriebsstatus**: Zeigt den aktuellen MLD-Snooping-Status für das ausgewählte VLAN an.
- **MRouter-Ports autom. erlernen**: Aktivieren oder deaktivieren Sie die Funktion zum automatischen Lernen für den Multicast-Router.
- **Abfragerobustheit**: Geben Sie den Wert für die Robustheitsvariable ein, der verwendet werden soll, wenn der Switch den Wert nicht in den Nachrichten lesen kann, die vom Abfrager gesendet wurden.
- **Abfragerobustheit für Betrieb**: Zeigt die Robustheitsvariable an, die vom ausgewählten Abfrager gesendet wurde.

- **Abfrageintervall**: Geben Sie den Wert für das Abfrageintervall ein, der vom Switch verwendet werden soll, wenn der Switch den Wert nicht aus den vom Abfrager gesendeten Nachrichten ableiten kann.
- **Abfrageintervall für Betrieb**: Das Zeitintervall in Sekunden zwischen den allgemeinen Abfragen, die vom ausgewählten Abfrager empfangen wurden.
- **Max. Abfrageantwortintervall**: Geben Sie den Wert für das maximale Abfrageantwortintervall ein, der verwendet werden soll, wenn der Switch den Wert für die maximale Reaktionszeit nicht in den allgemeinen Abfragen lesen kann, die vom ausgewählten Abfrager gesendet wurden.
- **Max. Abfrageantwortintervall für Betrieb**: Geben Sie die Verzögerung ein, mit der der maximale Antwortcode berechnet werden soll, der in den allgemeinen Abfragen eingegeben wurde.
- **Abfragezähler letztes Mitglied**: Geben Sie den Wert für den Abfragezähler für das letzte Mitglied ein, der verwendet werden soll, wenn der Switch den Wert nicht aus den Nachrichten ableiten kann, die vom ausgewählten Abfrager gesendet wurden.
- **Abfragezähler letztes Mitglied für Betrieb**: Zeigt den Wert für das letzte Mitglied des Abfragezähler für Betrieb an.
- **Abfrageintervall letztes Mitglied**: Geben Sie den Wert für die maximale Antwortverzögerung ein, der verwendet werden soll, wenn der Switch den Wert für die maximale Reaktionszeit nicht aus den gruppenspezifischen Abfragen ableiten kann, die vom ausgewählten Abfrager gesendet wurden.
- **Abfrageintervall letztes Mitglied für Betrieb**: Zeigt das Abfrageintervall für das letzte Mitglied an, das vom ausgewählten Abfrager gesendet wurde.
- **Sofortiges Leave**: Wenn diese Option aktiviert ist, reduziert sich die Zeit, die benötigt wird, um unnötigen MLD-Datenverkehr, der an einen Switch-Port gesendet wird, zu blockieren.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Abfragen von IGMP/MLD-IP-Multicast-Gruppen

Auf der Seite *IGMP/MLD-IP-Multicast-Gruppe* werden die IPv4- und IPv6-Gruppenadressen angezeigt, die der Switch aus den gesnoopten IGMP/MLD-Nachrichten gelernt hat.

Die Informationen auf dieser Seite unterscheiden sich möglicherweise zum Beispiel von denen auf der Seite *MAC-Gruppenadresse.* Wenn das System MAC-basierten Gruppen angehört und ein Port vorhanden ist, der den Multicast-Gruppen 224.1.1.1 und 225.1.1.1 beitreten möchte, 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-IP-Multicast-Gruppe**. Die Seite *IGMP/MLD-IP-Multicast-Gruppe* wird geöffnet.

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 Host-Registrierung, die der Switch für die IP-Gruppenadresse empfängt.

Definieren von Multicast-Router-Ports

Ein Multicast-Router-Port (MRouter) ist ein Port, der an einen Multicast-Router angeschlossen ist. Der Switch berücksichtigt die Nummern der Multicast-Router-Ports, wenn er 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**. Die Seite *Multicast-Router-Port* wird geöffnet.

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 den Switch zu aktualisieren.

Definieren des Multicast-Merkmals "Alle weiterleiten"

Auf der Seite *Alle weiterleiten* können Sie die Ports und/oder LAGs konfigurieren, die Multicast-Ströme von einem bestimmten VLAN empfangen sollen, und die Konfiguration anzeigen. 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 am Switch 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**. Die Seite *Alle weiterleiten* wird geöffnet.

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.

Definieren der Einstellungen für nicht registriertes Multicast

Multicast-Frames werden im Allgemeinen an alle Ports im VLAN weitergeleitet. Wenn IGMP/MLD-Snooping aktiviert ist, lernt der Switch das Vorhandensein von Multicast-Gruppen und überwacht, welche Ports welcher Multicast-Gruppe beigetreten sind. Es ist auch möglich, Multicast-Gruppen statisch zu konfigurieren. Multicast-Gruppen, die entweder dynamisch gelernt oder statisch konfiguriert wurden, werden als registriert eingestuft.

Der Switch leitet Multicast-Frames (aus einer registrierten Multicast-Gruppe) nur an Ports weiter, die in dieser Multicast-Gruppe registriert sind.

Auf der Seite *Nicht registriertes Multicast* können Sie die Verarbeitung von Multicast-Frames aktivieren, die zu Gruppen gehören, die dem Switch unbekannt sind (nicht registrierte Multicast-Gruppen). Nicht registrierte Multicast-Frames werden normalerweise an alle Ports im VLAN weitergeleitet.

Sie können einen Port auswählen, der nicht registrierte Multicast-Ströme empfangen oder filtern soll. Die Konfiguration ist für jedes VLAN gültig, in dem er Mitglied ist (oder sein wird).

Mit dieser Funktion kann sichergestellt werden, dass der Kunde nur angefragte Multicast-Gruppen empfängt und keine anderen, die im Netzwerk übertragen werden.

Gehen Sie wie folgt vor, um die Einstellungen für nicht registriertes Multicast zu definieren:

SCHRITT 1 Klicken Sie auf **Multicast** > **Nicht registriertes Multicast**. Die Seite *Nicht registriertes Multicast* wird geöffnet.

SCHRITT 2 Definieren Sie Folgendes:

- **Schnittstellentyp ist gleich**: Definieren Sie, ob alle Ports oder alle LAGs angezeigt werden sollen.
- **Port/LAG**: Zeigt die Port- oder LAG-ID an.
- **Nicht registriertes Multicast**: 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 3 Klicken Sie auf **Übernehmen**. Die Einstellungen werden gespeichert und die aktuelle Konfigurationsdatei wird aktualisiert.

16

Konfigurieren der IP-Informationen

IP-Schnittstellenadressen können manuell vom Benutzer oder automatisch von einem DHCP-Server konfiguriert werden. Dieser Abschnitt enthält Informationen zum Definieren der Switch-IP-Adressen (manuell oder durch Konfigurieren des Switch als DHCP-Client).

In diesem Abschnitt werden die folgenden Themen behandelt:

- **Verwaltungs- und IP-Schnittstellen**
- **Definieren von IPv4-Routen**
- **Konfigurieren von ARP**
- **Aktivieren von ARP-Proxy**
- **Definieren des UDP-Relais**
- **Domain Name Systeme**

Verwaltungs- und IP-Schnittstellen

Einige Funktionen sind nur im Schicht-2- oder Schicht-3-Systemmodus verfügbar (siehe unten):

- Im Schicht-2-Systemmodus fungiert der Switch als VLAN-fähiger Schicht-2-Switch ohne Routing-Funktionen.
- Im Schicht-3-Systemmodus verfügt der Switch 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 werden vom Switch MAC-basiertes VLAN, dynamische VLAN-Zuordnung, VLAN-Ratenbegrenzung, SYN-Raten-DoS-Schutz und erweiterte QoS-Überwachungsvorrichtungen nicht unterstützt.

Auf der Seite *Administration > Systemeinstellungen* können Sie den Switch in einem dieser Modi konfigurieren.

HINWEIS Wenn Sie zwischen den Systemmodi (Schichten) wechseln (bei den Geräten, die dies unterstützen), müssen Sie das Gerät neu starten und die Startkonfiguration des Switch wird gelöscht.

Schicht-2-IP-Adressierung

Im Schicht-2-Systemmodus hat der Switch eine einzelne IP-Adresse im Verwaltungs-VLAN. 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 der Seite *IPv4-Schnittstelle* konfigurieren. Im Schicht-2-Systemmodus verwendet der Switch das Standard-Gateway, falls konfiguriert, um mit Geräten zu kommunizieren, die sich nicht im gleichen Subnetz wie der Switch befinden. Standardmäßig ist VLAN 1 das Verwaltungs-VLAN, dies kann jedoch geändert werden. Wenn der Switch im Schicht-2-Systemmodus betrieben wird, ist er nur unter der konfigurierten IP-Adresse über sein Verwaltungs-VLAN erreichbar.

Die werkseitige Standardeinstellung für die IP-Adresskonfiguration ist *DHCP*. Dies bedeutet, dass der Switch sich wie ein DHCP-Client verhält und während des Hochfahrens eine DHCP-Anforderung sendet.

Wenn der Switch eine DHCP-Antwort mit einer IP-Adresse vom DHCP-Server empfängt, sendet er Address Resolution Protocol-(ARP-)Pakete, um zu bestätigen, dass die IP-Adresse eindeutig ist. Wenn die ARP-Antwort zeigt, dass die IP-Adresse bereits verwendet wird, sendet der Switch eine DHCPDECLINE-Benachrichtigung an den DHCP-Server, der die Adresse angeboten hat, sowie ein weiteres DHCPDISCOVER-Paket, sodass der Prozess von Neuem beginnt.

Wenn der Switch innerhalb von 60 Sekunden keine DHCP-Antwort erhält, sendet er weiterhin DHCPDISCOVER-Anfragen und übernimmt die Standard-IP-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 Switch beteiligt sind.

Wenn ein VLAN für die Verwendung dynamischer IP-Adressen konfiguriert ist, sendet der Switch so lange Anforderungen, bis ihm vom DHCP-Server eine IP-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 bis zu 32 Schnittstellen (Ports, LAGs und/oder VLANs) mit einer statischen oder dynamischen IP-Adresse am Switch konfiguriert werden.

Im Folgenden sind die IP-Adresszuweisungsregeln für den Switch beschrieben:

- Im Schicht-2-Systemmodus sendet der Switch, falls er nicht mit einer statischen IP-Adresse konfiguriert ist, DHCP-Anfragen, bis er eine Antwort vom DHCP-Server empfängt.
- Wenn die IP-Adresse am Switch geändert wird, sendet der Switch unaufgefordert ARP-Pakete an das entsprechende VLAN, um auf IP-Adresskollisionen zu prüfen. Diese Regel gilt auch, wenn der Switch 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 der Switch 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 der Switch mehrere IP-Adressen haben. Jede IP-Adresse kann bestimmten Ports, LAGs oder VLANs zugeordnet werden. Die IP-Adressen können Sie auf der Seite *IPv4-Schnittstelle* im Schicht-3-Systemmodus konfigurieren. Dies bietet eine größere Netzwerkflexibilität gegenüber dem Schicht-2-Systemmodus, in dem nur eine einzige IP-Adresse konfiguriert werden kann. Wenn der Switch im Schicht-3-Systemmodus betrieben wird, ist er von den entsprechenden Schnittstellen aus unter allen seinen IP-Adressen erreichbar.

Im Schicht-3-Systemmodus wird keine vordefinierte Standardroute bereitgestellt. Wenn der Switch 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. Dies können Sie auf der Seite *Statische IPv4-Routen* definieren.

Alle für den Switch 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.

Definieren einer IPv4-Schnittstelle im Schicht-2-Systemmodus

Um den Switch mit dem webbasierten Switch-Konfigurationsdienstprogramm zu verwalten, muss die IP-Adresse für die IPv4-Switch-Verwaltung definiert und bekannt sein. Die IP-Adresse des Switch kann manuell konfiguriert oder automatisch von einem DHCP-Server abgerufen werden.

So konfigurieren Sie die IPv4-IP-Adresse des Switch:

SCHRITT 1 Klicken Sie auf **Administration > Verwaltungsschnittstelle > IPv4-Schnittstelle**. Die Seite *IPv4-Schnittstelle* wird geöffnet.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **Verwaltungs-VLAN**: Wählen Sie das Verwaltungs-VLAN, das für den Zugriff auf den Switch über Telnet oder die Web-GUI 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 Switch angefordert. Damit Sie diese Funktion verwenden können, muss der DHCP-Server unabhängig von der Anforderung für das Senden von Option 12 konfiguriert sein.

Wenn eine statische IP-Adresse verwendet wird, sind die folgenden Felder zu konfigurieren.

- **IP-Adresse**: Geben Sie die IP-Adresse ein, und konfigurieren Sie jeweils eines der folgenden Felder:
  - **Netzwerkmaske**: Wählen Sie die IP-Adressmaske, und geben Sie sie ein.
  - **Präfixlänge**: Wählen Sie die IPv4-Präfixlänge, und geben Sie sie 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 der Switch nicht mit einem Standard-Gateway konfiguriert ist, kann er 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 Switch kann jederzeit erneuert werden. Abhängig von der Konfiguration des DHCP-Servers kann es vorkommen, dass der Switch nach der Erneuerung eine neue IP-Adresse erhält, sodass im webbasierten Switch-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 der Switch im Schicht-3-Modus befindet. In diesem Modus können mehrere IP-Adressen für die Switch-Verwaltung konfiguriert werden, und es stehen Routing-Services zur Verfügung.

Die IP-Adresse kann für eine Port-, eine LAG- oder eine VLAN-Schnittstelle konfiguriert werden.

Beim Betrieb im Schicht-3-Modus routet der Switch den Datenverkehr zwischen den direkt angeschlossenen IP-Subnetzen, die am Switch konfiguriert sind. Der Switch 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 Switch-Software benötigt eine VLAN-ID (VID) für jede für einen Port oder eine LAG konfigurierte IP-Adresse. Der Switch übernimmt die erste nicht verwendete VID, beginnend mit 4094.

So konfigurieren Sie die IPv4-Adressen:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **Verwaltungs- und IP-Schnittstellen** > **IPv4-Schnittstelle.** Die Seite *IPv4-Schnittstelle* wird geöffnet.

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.
  - *Statisch*: Manuell eingegeben.
  - *DHCP*: Von einem DHCP-Server empfangen.
- **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 2 Klicken Sie auf **Hinzufügen**. Die Seite *IPv4-Schnittstelle hinzufügen* wird geöffnet.

SCHRITT 3 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 4 Wenn "Statische IP-Adresse" ausgewählt wurde, geben Sie die **IP-Adresse** für diese Schnittstelle ein.

SCHRITT 5 Geben Sie die Netzwerkmaske oder die Präfixlänge für diese IP-Adresse ein.

- **Netzwerkmaske**: Die IP-Maske für diese Adresse.
- **Präfixlänge**: Länge des IPv4-Präfixes.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die IPv4-Adresseinstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Verwalten von IPv6

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 der ISATAP-Mechanismus verwendet. Dieses Protokoll behandelt das IPv4-Netzwerk als einen virtuellen lokalen IPv6-Link mit Zuordnungen von den einzelnen IPv4-Adressen zu einer Link Local-IPv6-Adresse.

Der Switch erkennt IPv6-Frames durch den IPv6-Ethertype.

Definition der globalen IPv6-Konfiguration

Auf der Seite *Globale IPv6-Konfiguration* können Sie die Häufigkeit der vom Switch generierten IPv6-ICMP-Fehlermeldungen definieren.

So definieren Sie globale IPv6-Parameter:

SCHRITT 1 Im Schicht-2-Systemmodus klicken Sie auf **Administration** > **Verwaltungsschnittstelle** > **Globale IPv6-Konfiguration**.

Im Schicht-3-Systemmodus klicken Sie auf **IP-Konfiguration** > **Verwaltungs- und IP-Schnittstellen** > **Globale IPv6-Konfiguration**.

Die Seite *Globale IPv6-Konfiguration* wird geöffnet.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **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 Switch gesendet werden können.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die globalen IPv6-Parameter werden in die aktuelle Konfigurationsdatei geschrieben.

Definieren einer IPv6-Schnittstelle

Eine IPv6-Schnittstelle kann für eine Port-, eine LAG-, eine VLAN-Schnittstelle oder eine ISATAP-Tunnelschnittstelle konfiguriert werden. Der Switch unterstützt eine IPv6-Schnittstelle als IPv6-Endgerät.

Eine Tunnelschnittstelle wird mit einer IPv6-Adresse auf der Basis von Einstellungen konfiguriert, die auf der Seite *IPv6-Tunnel* definiert werden.

So definieren Sie eine IPv6-Schnittstelle:

SCHRITT 1 Im Schicht-2-Systemmodus klicken Sie auf **Administration** > **Verwaltungsschnittstelle** > **IPv6-Schnittstelle**.

Im Schicht-3-Systemmodus klicken Sie auf **IP-Konfiguration** > **Verwaltungs- und IP-Schnittstellen** > **IPv6-Schnittstelle**.

Die Seite *IPv6-Schnittstelle* wird geöffnet.

Auf dieser Seite werden die bereits konfigurierten IPv6-Schnittstellen angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, um eine neue Schnittstelle hinzuzufügen, für die IPv6 aktiviert ist.

SCHRITT 3 Die Seite *IPv6-Schnittstelle hinzufügen* wird geöffnet.

SCHRITT 4 Geben Sie die Werte ein.

- **IPv6-Schnittstelle**: Wählen Sie einen bestimmten Port, eine LAG, ein VLAN oder einen ISATAP-Tunnel.
- **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.

- **Automatische IPv6-Adresskonfiguration**: Aktiviert die automatische Adresskonfiguration. Nach Aktivieren unterstützt der Switch die statuslose automatische IPv6-Adresskonfiguration von lokalen und globalen IP-Adressen anhand der von der Schnittstelle empfangenen IPv6-Router-Ankündigung. Der Switch unterstützt die statusorientierte automatische Adresskonfiguration nicht. Wenn die automatische Konfiguration nicht aktiviert ist, definieren Sie auf der Seite *IPv6-Adressen* eine IPv6-Adresse.
- **ICMPv6-Nachrichten senden**: Zum Aktivieren von Benachrichtigungen über nicht erreichbare Ziele.

SCHRITT 5 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 6 Klicken Sie auf **IPv6-Adresstabelle**, um der Schnittstelle ggf. manuell IPv6-Adressen hinzuzufügen. Diese Seite wird im Abschnitt **Definieren von IPv6-Adressen** beschrieben.

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-Adressen**.
Klicken Sie im Schicht-3-Systemmodus auf **IP-Konfiguration** > **Verwaltungs- und IP-Schnittstellen** > **IPv6-Adressen**.

Die Seite *IPv6-Adressen* wird geöffnet.

SCHRITT 2 Zum Filtern der Tabelle wählen Sie einen Schnittstellennamen aus und klicken Sie auf **Los**. Die Schnittstelle wird in der IPv6-Adresstabelle angezeigt.

SCHRITT 3 Klicken Sie auf **Hinzufügen**. Die Seite *IPv6-Adresse hinzufügen* wird geöffnet.

SCHRITT 4 Geben Sie Werte für die Felder ein.

- **IPv6-Schnittstelle**: Zeigt die Schnittstelle an, für die die IPv6-Adresse definiert werden soll.
- **IPv6-Adresstyp**: Wählen Sie "Link Local" oder "Global" als hinzuzufügenden IPv6-Adresstyp.
  - *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.
- **IPv6-Adresse**: Der Switch unterstützt 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.

  HINWEIS Für ISATAP-Tunnelschnittstellen können IPv6-Adressen nicht direkt konfiguriert werden.
- **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.

Definieren einer IPv6-Standardrouter-Liste

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 den Switch für nicht lokalen Verkehr sind (die Liste kann leer sein). Der Switch wählt nach dem Zufallsprinzip einen Router aus der Liste aus. Der Switch unterstützt einen statischen IPv6-Standardrouter. Dynamische StandardrouterStandardrouter sind Router, die Router-Ankündigungen an die IPv6-Schnittstelle des Switch 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 der Versuch gemacht wurde, mehr als eine einzelne benutzerdefinierte Adresse einzufügen.
- Eine Alarmmeldung wird angezeigt, wenn der Versuch gemacht wird, eine Adresse, die nicht vom Link Local-Typ ('fe80:') ist, einzufügen.

So definieren Sie einen Standardrouter:

SCHRITT 1 Im Schicht-2-Systemmodus klicken Sie auf **Administration > Verwaltungsschnittstelle > Liste der IPv6-Standardrouter**.
Im Schicht-3-Systemmodus klicken Sie auf **IP-Konfiguration** > **Verwaltungs- und IP-Schnittstellen** > **Liste der IPv6-Standardrouter**.

Die Seite *Liste der IPv6-Standardrouter* wird geöffnet.

Auf dieser Seite werden für die einzelnen Standardrouter die folgenden Felder angezeigt:

- **IPv6-Adresse des Standard-Routers**: Link Local-IP-Adresse des Standard-Routers.
- **Schnittstelle**: Ausgehende IPv6-Schnittstelle, wo der Standardrouter angesiedelt ist.
- **Typ**: Die Standardrouter-Konfiguration, die die folgenden Optionen umfasst:
  - *Statisch*: Der Standardrouter ist über die Schaltfläche **Hinzufügen** manuell zu dieser Tabelle hinzugefügt worden.
  - *Dynamisch*: Der Standardrouter wurde dynamisch konfiguriert.

Status: Die Optionen für den Status des Standard-Routers sind:

- *Unvollständig*: Adressauflösung wird durchgeführt. Der Standardrouter hat noch nicht geantwortet.
- *Erreichbar*: In der *erreichbaren Zeit* wurde eine positive Antwort erhalten.
- *Veraltet*: Ein bekanntes Nachbarnetzwerk ist nicht erreichbar, und es wird keine Maßnahme ergriffen, seine Erreichbarkeit zu verifizieren, bevor Datenverkehr gesendet werden muss.
- *Verzögerung*: Ein bekanntes Nachbarnetzwerk ist nicht erreichbar. Das Gerät hat während einer vordefinierten *Verzögerungszeit* den Status "Verzögerung". Wenn keine Bestätigung empfangen wird, ändert sich der Status nach Test.
- *Test*: Das Nachbarnetzwerk ist nicht erreichbar, und es werden Unicast-Nachbaranfragetests gesendet, um den Status zu überprüfen.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, um einen statischen Standardrouter hinzuzufügen. Die Seite *Standardrouter hinzufügen* wird geöffnet.

Im Fenster wird die Link-Local-Schnittstelle angezeigt. Die Schnittstelle kann ein Port, eine LAG, ein VLAN oder ein Tunnel sein.

SCHRITT 3 Geben Sie die IP-Adresse des statischen Standardrouters in das Feld **IPv6-Standardadresse für Router** ein.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Der Standardrouter wird in die aktuelle Konfigurationsdatei geschrieben.

Konfigurieren von IPv6-Tunneln

Das ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) ermöglicht die Verkapselung von IPv6-Paketen in IPv4-Paketen zur Übermittlung in IPv4-Netzwerken. Zum Konfigurieren eines Tunnels führen Sie die folgenden Schritte aus:

- Aktivieren und konfigurieren Sie manuell einen ISATAP-Tunnel.
- Definieren Sie manuell eine IPv6-Schnittstelle für den ISATAP-Tunnel.

Anschließend konfiguriert der Switch automatisch die Link-Local-IPv6-Adresse für die IPv6-Schnittstelle.

Beachten Sie beim Definieren von ISATAP-Tunneln 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 Host-Zuordnungstabelle 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.

So konfigurieren Sie einen IPv6-Tunnel:

SCHRITT 1 Klicken Sie im Schicht-2-Systemmodus auf **Administration** > **Verwaltungsschnittstelle** > **IPv6-Tunnel**.
Klicken Sie im Schicht-3-Systemmodus auf **IP-Konfiguration** > **Verwaltungs- und IP-Schnittstellen** > **IPv6-Tunnel**.

Die Seite *IPv6-Tunnel* wird geöffnet.

SCHRITT 2 Geben Sie Werte für die folgenden Felder ein:

- **Tunnelnummer**: Die Domänennummer des automatischen Tunnel-Routers.
- **Tunneltyp**: Wird immer als ISATAP angezeigt.
- **Quell-Pv4-Adresse**: Der ISATAP-Tunnel wird über eine IPv4-Schnittstelle deaktiviert oder aktiviert. Die IPv4-Adresse der ausgewählten IPv4-Schnittstelle, die verwendet wird, 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.
  - *Autom.*: Automatische Auswahl der niedrigsten IPv4-Adresse aus allen konfigurierten IPv4-Schnittstellen.
  - *Keine*: Deaktivieren des ISATAP-Tunnels.
  - *Manuell*: Manuelles Konfigurieren einer IPv4-Adresse. Die konfigurierte IPv4-Adresse muss eine der IPv4-Adressen der IPv4-Schnittstellen des Switch sein.

- **Domänenname des Tunnel-Routers**: Eine globale Zeichenfolge, die einen Domänennamen eines bestimmten automatischen Tunnel-Routers repräsentiert. Der Name kann entweder der Standardname (ISATAP) oder ein benutzerdefinierter Name sein.
- **Abfrageintervall**: Der Zeitraum in Sekunden von 10 bis 3600 zwischen DNS-Abfragen (bevor die IP-Adresse des ISATAP-Routers bekannt ist) für diesen Tunnel. Das Intervall kann den Standardwert (10 Sekunden) oder einen benutzerdefinierten Wert haben.
- **ISATAP-Anfrageintervall**: Der Zeitraum in Sekunden von 10 bis 3600 zwischen ISATAP-Router-Anfragebenachrichtigungen, wenn kein aktiver ISATAP-Router verfügbar ist. Das Intervall kann den Standardwert (10 Sekunden) oder einen benutzerdefinierten Wert haben.
- **ISATAP-Robustheit**: Wird verwendet, um das Intervall für die DNS- oder Router-Anfragen zu berechnen. Je größer die Zahl, desto häufiger die Abfragen. Der Standardwert ist 3, der Bereich ist 1 bis 20.

  HINWEIS Der ISATAP-Tunnel ist nicht in Betrieb, wenn die zugrunde liegende IPv4-Schnittstelle nicht in Betrieb ist.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Der Tunnel wird in die aktuelle Konfigurationsdatei geschrieben.

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 befinden wie der Switch. Damit kann die Erreichbarkeit von Nachbarn überprüft werden. Dies ist das IPv6-Äquivalent der IPv4-ARP-Tabelle. Wenn der Switch mit seinen Nachbarn Daten austauschen muss, verwendet er 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** > **Verwaltungs- und IP-Schnittstellen** > **IPv6-Nachbarn**.

Die Seite *IPv6-Nachbarn* wird geöffnet.

SCHRITT 2 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.

SCHRITT 3 Zum Hinzufügen eines Nachbarn zur Tabelle klicken Sie auf **Hinzufügen**. Die Seite *IPv6-Nachbar hinzufügen* wird geöffnet.

SCHRITT 4 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 5 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

SCHRITT 6 Um den Typ einer IP-Adresse von "Dynamisch" in "Statisch" zu ändern, verwenden Sie die Seite *IPv6-Nachbar bearbeiten*.

Anzeigen von IPv6-Routentabellen

Auf der Seite *IPv6-Routen* wird die *IPv6-Routing-Tabelle* angezeigt. Die Tabelle enthält eine einzelne Standardroute (IPv6-Adresse :0), die mithilfe des aus der Liste "IPv6-Standardrouter" ausgewählten Standardrouters Pakete an Zielgeräte sendet, die sich nicht im selben IPv6-Subnetz befinden wie der Switch. 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 Switch verwendete Standardrouter nicht der Router ist, über den Datenverkehr an die IPv6-Subnetze gesendet wird, mit denen der Switch kommuniziert.

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** > **Verwaltungs- und IP-Schnittstellen** > **IPv6-Routen**.

Die Seite *IPv6-Routen* wird geöffnet.

Auf dieser Seite werden folgende Felder angezeigt:

- **IPv6-Adresse**: Die 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. Es muss eine Link Local-Adresse sein.
- **Metrisch**: Wert, der zum Vergleichen dieser Route mit anderen Routen mit demselben Ziel in der IPv6-Routertabelle verwendet wird. Alle Standardrouten haben denselben Wert.
- **Life Time**: 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 Switch 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.

Definieren von IPv4-Routen

Wenn sich der Switch im Schicht-3-Systemmodus befindet, können Sie auf dieser Seite statische IPv4-Routen für den Switch 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. Der Switch verwendet die übereinstimmende Route mit der höchsten Subnetzmaske, d. h. mit der längsten Präfix-Übereinstimmung.

So definieren Sie eine statische IP-Route:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **IPv4-Routen**.

Die Seite *Statische IPv4-Routen* wird geöffnet.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *Statische IP-Route hinzufügen* wird geöffnet.

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**: Das IP-Routenpräfix für die IP-Zieladresse.
  - **Präfixlänge**: Das IP-Routenpräfix für die IP-Zieladresse.
- **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 der Switch seine IP-Adresse von einem DHCP-Server erhält.
- **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.
- **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 die aktuelle Konfigurationsdatei geschrieben.

Konfigurieren von ARP

Der Switch verwaltet eine ARP-Tabelle (Address Resolution Protocol) für alle bekannten Geräte, die sich in seinen direkt verbundenen IP-Subnetzen befinden. Ein direkt verbundenes IP-Subnetz ist ein Subnetz, mit dem eine IPv4-Schnittstelle des Switch verbunden ist. Wenn der Switch ein Paket an ein lokales Gerät senden bzw. routen muss, sucht er 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. Der Switch erstellt dynamische Adressen anhand der ARP-Pakete, die er empfängt. Dynamische Adressen veralten nach einem konfigurierten Zeitraum.

HINWEIS Im Schicht-2-Modus werden die Informationen zur IP- und zur MAC-Adresszuordnung in der ARP-Tabelle vom Switch verwendet, um den vom Switch 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 > ARP.** Die Seite *ARP-Tabelle* wird geöffnet.

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**. Die Seite *ARP hinzufügen* wird geöffnet.

SCHRITT 5 Geben Sie die Parameter ein:

- **IP-Version**: Das vom Host unterstützte IP-Adressformat. Nur IPv4 wird unterstützt.
- **Schnittstelle**: Die IPv4-Schnittstelle am Switch.

Im Fall von Geräten im Schicht-2-Modus gibt es nur ein direkt verbundenes IP-Subnetz, das sich immer im Verwaltungs-VLAN befindet. Alle statischen und dynamischen Adressen in der ARP-Tabelle befinden sich im Verwaltungs-VLAN.

Bei Geräten im Schicht-3-Systemmodus können Sie eine IPv4-Schnittstelle für einen Port, eine LAG oder ein VLAN konfigurieren. Wählen Sie die gewünschte Schnittstelle aus der Liste der für den Switch konfigurierten IPv4-Schnittstellen aus.

- **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 die aktuelle Konfigurationsdatei geschrieben.

Aktivieren von ARP-Proxy

Die Proxy-ARP-Technik wird von einem 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 Datenverkehrsziel 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.

Auf dieser Seite können Sie den Status der ARP-Proxy-Funktion konfigurieren. Nachdem sie auf dieser Seite aktiviert wurde, ist sie für alle IP-Schnittstellen aktiviert.

So aktivieren Sie ARP-Proxy für den Switch:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration > Aktivieren des ARP-Proxys**.

Die Seite *ARP-Proxy* wird geöffnet.

SCHRITT 2 Wählen Sie **ARP-Proxy** aus, damit der Switch auf ARP-Anforderungen für Remote-Knoten mit der MAC-Adresse des Switch antwortet.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Der ARP-Proxy wird aktiviert und die aktuelle Konfigurationsdatei wird aktualisiert.

Definieren des UDP-Relais

Die Funktion UDP-Relais ist nur dann verfügbar, wenn sich der Switch im Schicht-3-Systemmodus befindet. Ein Switch routet normalerweise IP-Broadcast-Pakete nicht zwischen IP-Subnetzen. Nach entsprechender Konfiguration kann der Switch jedoch bestimmte UDP-Broadcast-Pakete, die er 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 > Definieren der UDP-Relais**. Die Seite *UDP-Relais* wird geöffnet.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *UDP-Relais hinzufügen* wird geöffnet.

SCHRITT 3 Wählen Sie die **Quell-IP-Schnittstelle** aus, an die der Switch basierend auf einem konfigurierten UDP-Ziel-Port UDP-Broadcast-Pakete weiterleiten soll. Die Schnittstelle muss eine der für den Switch konfigurierten IPv4-Schnittstellen sein.

SCHRITT 4 Geben Sie die Nummer des **UDP-Ziel-Ports** für die Pakete ein, die der Switch weiterleiten soll. Wählen Sie den 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-Weiterleitungseinstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Domain Name Systeme

Das Domain Name System (DNS) übersetzt benutzerdefinierte Domänennamen in IP-Adressen zum Zweck der Lokalisierung und Adressierung dieser Objekte.

Als DNS-Client löst der Switch über einen oder mehrere konfigurierte DNS-Server Domänennamen zu IP-Adressen auf.

Definieren von DNS-Servern

Auf der Seite *DNS-Server* können Sie die DNS-Funktion aktivieren, die DNS-Server konfigurieren und die vom Switch verwendete Standarddomäne festlegen.

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **Domain Name System** > **DNS-Server**. Die Seite *DNS-Server* wird geöffnet.

SCHRITT 2 Geben Sie die Parameter ein.

- **DNS**: Wählen Sie diese Option aus, um den Switch als DNS-Client festzulegen, der DNS-Namen über einen oder mehrere konfigurierte DNS-Server zu IP-Adressen auflöst.
- **Standarddomänenname**: Geben Sie den Standard-DNS-Domänennamen ein (1 bis 158 Zeichen). Der Switch fügt diesen Namen allen nicht voll qualifizierten Domänennamen (Fully Qualified Domain Names, FQDNs) an, sodass diese zu FQDNs werden.
- **Typ**: Anzeige der Optionen für den Standarddomänentyp:
  - *DHCP*: Der Standarddomänenname wird dynamisch vom DHCP-Server zugewiesen.
  - *Statisch*: Der Standarddomänenname wird vom Benutzer definiert.
  - N. z.: Kein Standarddomänenname.

DNS-Servertabelle:

- **DNS-Server**: Die IP-Adressen der DNS-Server. Bis zu acht DNS-Server können definiert werden.
- **Serverstatus**: Der DNS-Server kann den Status "Aktiv" oder "Inaktiv" aufweisen. Es kann nur einen aktiven Server geben. Jeder statische Server hat eine Priorität, wobei ein niedrigerer Wert eine höhere Priorität bedeutet. Wenn eine Anforderung zum ersten Mal gesendet wird, wird der Server mit der höchsten Priorität ausgewählt. Wenn nach zwei Wiederholungen keine Antwort von diesem Server kommt, wird der Server mit der nächstniedrigeren Priorität ausgewählt. Wenn keiner der statischen Server antwortet, wird der erste dynamische Server in der Tabelle, nach IP-Adresse sortiert (hoch nach niedrig), ausgewählt.

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

SCHRITT 4 Zum Hinzufügen eines DNS-Servers klicken Sie auf **Hinzufügen**. Die Seite *DNS-Server hinzufügen* wird geöffnet.

SCHRITT 5 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**: Falls es sich bei dem IPv6-Adresstyp um Link Local handelt, wählen Sie aus, ob der Empfang über VLAN2 oder ISATAP erfolgt.
- **DNS-Server-IP-Adresse**: Geben Sie die IP-Adresse des DNS-Servers ein.
- **Status des DNS-Servers – Aktiv**: Wählen Sie diese Option, um den neuen DNS-Server zu aktivieren.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Der DNS-Server wird in die aktuelle Konfigurationsdatei geschrieben.

Zuordnen von DNS-Hosts

Der Switch speichert oft abgefragte Domänennamen, die er von den DNS-Servern empfangen hat, in einem lokalen DNS-Cache. Der Cache kann bis zu 64 statische Einträge, 64 dynamische Einträge und einen Eintrag für jede von DHCP am Switch konfigurierte IP-Adresse aufnehmen. 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.

Es werden verschiedene IP-Adressen für einen DNS-Host-Namen unterstützt.

So fügen Sie einen Domänennamen und seine IP-Adresse hinzu:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **Domain Name System** > **Hostzuordnung**. Die Seite *Hostzuordnung* wird geöffnet.

Auf dieser Seite werden folgende Felder angezeigt:

- **Hostname**: Der benutzerdefinierte Hostname, bis zu 158 Zeichnen lang.
- **IP-Adresse**: Die IP-Adresse des Host-Namens.

SCHRITT 2 Zum Hinzufügen einer Hostzuordnung klicken Sie auf **Hinzufügen**. Die Seite *Hostzuordnung hinzufügen* wird geöffnet.

SCHRITT 3 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**: Falls es sich bei dem IPv6-Adresstyp um Link Local handelt, wählen Sie aus, ob der Empfang über VLAN2 oder ISATAP erfolgt.
- **Hostname**: Geben Sie einen Domänennamen ein, bis zu 158 Zeichen lang.
- **IP-Adresse**: Geben Sie eine IPv4-Adresse oder bis zu vier IPv6-Host-IP-Adressen ein. Die Adressen 2 bis 4 sind Reserveadressen.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Der DNS-Host wird in die aktuelle Konfigurationsdatei geschrieben.

17

Konfigurieren der Sicherheitsfunktionen

In diesem Abschnitt werden die Sicherheit und Zugriffssteuerung für den Switch 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 Switch wird in den folgenden Abschnitten beschrieben:

- **Definieren von Benutzern**
- **Konfigurieren von TACACS+**
- **Konfigurieren von RADIUS**
- **Konfigurieren der Verwaltungszugriffsauthentifizierung**
- **Defininieren der Verwaltungszugriffsmethode**
- **Konfigurieren von TCP-/UDP-Services**

Der Schutz vor Angriffen auf die CPU des Switch 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 den Switch wird in den folgenden Abschnitten beschrieben:

- **Konfigurieren der Verwaltungszugriffsauthentifizierung**
- **Defininieren der Verwaltungszugriffsmethode**

- Konfigurieren von TACACS+
- Konfigurieren von RADIUS
- Konfigurieren der Portsicherheit
- Konfigurieren von 802.1X
- Definieren von Zeitbereichen

Der Schutz vor anderen Netzwerkbenutzern wird in den folgenden Abschnitten beschrieben. Dabei handelt es sich um Angriffe, die den Switch passieren, aber nicht gegen ihn gerichtet sind.

- Denial of Service-Sicherung
- Konfigurieren von TCP-/UDP-Services
- Definieren der Sturmsteuerung
- Konfigurieren der Portsicherheit
- IP Source Guard
- Dynamic ARP Inspection
- Zugriffssteuerung

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 den Switch 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**. Die Seite *Benutzerkonten* wird angezeigt.

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. Die Seite *Benutzerkonto hinzufügen (oder bearbeiten)* wird angezeigt.

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 Benutzerkennwort der Richtlinie entsprechen, die im Abschnitt **Einrichten der Kennwortkomplexitätsregeln** konfiguriert wurde.
- **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 Switch-Konfiguration 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 Switch-Konfiguration geändert wird. Weitere Informationen hierzu finden Sie im *CLI-Referenzhandbuch*.
  - *Verwaltungs-Lese-/Schreibzugriff (15)*: Der Benutzer kann auf die grafische Benutzeroberfläche zugreifen und den Switch konfigurieren.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Der Benutzer wird der aktuellen Konfigurationsdatei des Switch hinzugefügt.

Einrichten der Kennwortkomplexitätsregeln

Kennwörter dienen zur Authentifizierung von Benutzern, die auf den Switch 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**. Die Seite *Kennwortsicherheit* wird angezeigt.

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 Zum Konfigurieren der Übereinstimmung von Benutzername und Kennwort sowie der Übereinstimmung von Hersteller und Kennwort können Sie die CLI verwenden. Weitere Anweisungen hierzu finden Sie im *CLI-Referenzhandbuch*.

Konfigurieren von TACACS+

Der Switch ist ein TACACS+-Client *(Terminal Access Controller Access Control System)*, der einen TACACS+-Server verwenden kann, um zentralisierte Sicherheitsfunktionen bereitzustellen.

TACACS+ bietet die folgenden Dienste:

- **Authentifizierung**: Stellt die Authentifizierung für Administratoren bereit, die sich mit Benutzernamen und benutzerdefinierten Kennwörtern beim Switch 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.

Das TACACS+-Protokoll gewährleistet die Netzwerkintegrität durch den Austausch verschlüsselter Protokolle zwischen dem Gerät und dem TACACS+-Server.

TACACS+ wird nur von IPv4 unterstützt.

TACACS+-Server können nicht als 802.1X-Authentifizierungsserver verwendet werden, um Anmeldeinformationen von Netzwerkbenutzern zu verifizieren, die sich über den Switch mit dem Netzwerk verbinden möchten.

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.

Konfigurieren von Standard-TACACS+-Parametern

Auf der Seite *TACACS+* können Sie TACACS+-Server konfigurieren.

Nur Benutzer mit Berechtigungsebene 15 auf dem TACACS+-Server können den Switch 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+**. Die Seite *TACACS+* wird angezeigt.

SCHRITT 2 Geben Sie die standardmäßige **Schlüsselzeichenfolge** ein, die für die Kommunikation mit allen TACACS+-Servern im Modus **Verschlüsselt** oder **Unverschlüsselt** verwendet wird. Der Switch 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.

SCHRITT 3 Geben Sie im Feld **Timeout für Antwort** den Zeitraum ein, der verstreichen soll, bevor die Zeit für die Verbindung zwischen dem Switch 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.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die TACACS+-Einstellungen werden der aktuellen Konfigurationsdatei hinzugefügt.

SCHRITT 5 Zum Hinzufügen eines TACACS+-Servers klicken Sie auf **Hinzufügen**. Die Seite *TACACS+-Server hinzufügen* wird angezeigt.

SCHRITT 6 Geben Sie die Parameter ein.

- **Server-IP-Adresse**: Geben Sie die IP-Adresse 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 der Switch keine Sitzung mit dem Server hoher Priorität aufbauen kann, versucht er dies beim Server mit der nächstniedrigeren Priorität.
- **Quell-IP-Adresse**: (Für SG500X-Geräte und andere Geräte im Schicht-3-Systemmodus). Wählen Sie aus, dass die Standardquelladresse verwendet werden soll, oder wählen Sie eine der verfügbaren IP-Adressen aus.
- **Schlüsselzeichenfolge**: Geben Sie die Standardschlüsselzeichenfolge ein, die zur Authentifizierung und Verschlüsselung zwischen dem Switch 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 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.
- **Timeout für Antwort**: Geben Sie den Zeitraum ein, der verstreichen soll, bevor die Zeit für die Verbindung zwischen dem Switch 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 Zum Anzeigen sensibler Daten in unverschlüsselter Form in der Konfigurationsdatei klicken Sie auf **Sensible Daten unverschlüsselt anzeigen**.

SCHRITT 8 Klicken Sie auf **Übernehmen**. Der TACACS+-Server wird der aktuellen Konfigurationsdatei des Switch hinzugefügt.

Konfigurieren von RADIUS

Remote Authorization Dial-In User Service-(RADIUS-)Server bieten zentralisierte 802.1X- oder MAC-basierte Netzwerkzugriffssteuerung. Der Switch ist ein RADIUS-Client, der einen RADIUS-Server verwenden kann, um zentralisierte Sicherheitsfunktionen bereitzustellen.

So legen Sie die RADIUS-Serverparameter fest:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **RADIUS**. Die Seite *RADIUS* wird angezeigt.

SCHRITT 2 Geben Sie die RADIUS-Abrechnungsoption ein. Folgende Optionen stehen zur Verfügung:

- **Portbasierte Zugriffssteuerung (802.1X, MAC-basiert)**: Gibt an, dass der RADIUS-Server für die 802.1x-Port-Abrechnung verwendet wird.
- **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.

- **IP-Version**: Zeigt die unterstützten IP-Versionen an: IPv6- und/oder IPv4-Subnetz.
- **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 der Switch auf eine Antwort vom RADIUS-Server warten soll, bevor er 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 Switch 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-Adresse**: Geben Sie die zu verwendende Quell-IPv4-Adresse ein.
- **Quell-IPv6-Adresse**: Geben Sie die zu verwendende Quell-IPv6-Adresse ein.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die RADIUS-Standardeinstellungen für den Switch werden in der aktuellen Konfigurationsdatei aktualisiert.

Zum Hinzufügen eines RADIUS-Servers klicken Sie auf **Hinzufügen**. Die Seite *RADIUS-Server hinzufügen* wird angezeigt.

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.

- **IP-Version**: Wenn der RADIUS-Server anhand der IP-Adresse identifiziert werden soll, wählen Sie IPv4 oder IPv6 aus, um anzugeben, dass die IP-Adresse im ausgewählten Format eingegeben wird.
- **IPv6-Adresstyp**: Zeigt an, dass der IPv6-Adresstyp "Global" verwendet wird.
- **IP-Adresse/Name des Servers**: Wählen Sie aus, ob der RADIUS-Server anhand der IP-Adresse oder des Namens angegeben wird.

- **Priorität**: Geben Sie die Priorität des Servers ein. Die Priorität legt die Reihenfolge fest, in der die Server bei der Authentifizierung eines Benutzers vom Switch kontaktiert werden. Der RADIUS-Server mit der höchsten Priorität wird vom Switch zuerst kontaktiert. Null ist die höchste Priorität.
- **Quell-IP-Adresse**: (Für Geräte im Schicht-3-Systemmodus) Wählen Sie aus, dass die Standardquelladresse verwendet werden soll, oder wählen Sie eine der verfügbaren IP-Adressen aus.

  Schlüsselzeichenfolge: Geben Sie die Schlüsselzeichenfolge ein, die zur Authentifizierung und Verschlüsselung der Kommunikation zwischen dem Switch und dem RADIUS-Server verwendet wird. Der Schlüssel muss mit dem auf dem RADIUS-Server konfigurierten Schlüssel übereinstimmen. Wenn **Standard verwenden** ausgewählt ist, versucht der Switch, sich mit der Standardschlüsselzeichenfolge gegenüber dem RADIUS-Server zu authentifizieren.
- **Timeout für Antwort**: Geben Sie ein, wie viele Sekunden lang der Switch auf eine Antwort vom RADIUS-Server wartet, bevor er die Abfrage wiederholt oder (falls die maximale Anzahl der Wiederholungen erreicht ist) zum nächsten Server wechselt. Wenn **Standard verwenden** ausgewählt ist, verwendet der Switch 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**: Geben Sie ein, wie viele Anforderungen an den RADIUS-Server gesendet werden sollen, bevor angenommen wird, dass ein Fehler aufgetreten ist. Wenn **Standard verwenden** ausgewählt ist, verwendet der Switch den Standardwert für die Anzahl der Wiederholungen.
- **Stillstandszeit**: 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 der Switch 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 den Switch verwalten möchten.

- *802.1X*: Der RADIUS-Server wird zur 802.1X-Authentifizierung verwendet.
- *Alle*: Der RADIUS-Server wird zur Authentifizierung von Benutzern verwendet, die den Switch verwalten möchten, und zur 802.1X-Authentifizierung.

SCHRITT 6 Zum Anzeigen sensibler Daten in unverschlüsselter Form in der Konfigurationsdatei klicken Sie auf **Sensible Daten unverschlüsselt anzeigen**.

SCHRITT 7 Klicken Sie auf **Übernehmen**. Die RADIUS-Serverdefinition wird der aktuellen Konfigurationsdatei des Switch hinzugefügt.

Konfigurieren der Verwaltungszugriffsauthentifizierung

Sie können den verschiedenen Verwaltungszugriffsmethoden Authentifizierungsmethoden zuweisen, wie z. B. SSH, Konsole, Telnet, HTTP und HTTPS. Diese Authentifizierung kann lokal oder auf einem TACACS+- oder RADIUS-Server ausgeführt werden.

Damit der RADIUS-Server Zugriff auf das webbasierte Switch-Konfigurationsdienstprogramm gewährt, muss der RADIUS-Server die Zeichenfolge "cisco-avpair = shell:priv-lvl=15" zurückgeben.

Die Benutzerauthentifizierung erfolgt 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 authentifiziert.

Wenn eine Authentifizierungsmethode fehlschlägt oder der Benutzer nicht über die entsprechende Berechtigungsebene verfügt, wird dem Benutzer der Zugriff auf den Switch verweigert. Anders gesagt, wenn die Authentifizierung mit einer Authentifizierungsmethode fehlschlägt, beendet der Switch den Authentifizierungsversuch. Er fährt nicht fort und versucht auch nicht, die nächste Authentifizierungsmethode zu verwenden.

So definieren Sie Authentifizierungsmethoden für Zugriffsmethoden:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Verwaltungszugriffsauthentifizierung**. Die Seite *Verwaltungszugriffsauthentifizierung* wird angezeigt.

SCHRITT 2 Wählen Sie in der Liste **Anwendung** eine Zugriffsmethode aus.

SCHRITT 3 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 authentifiziert. Es muss mindestens ein RADIUS-Server konfiguriert sein.
- *TACACS+*: Der Benutzer wird auf dem TACACS+-Server authentifiziert. Es muss mindestens ein TACACS+-Server konfiguriert sein.
- *Keine*: Der Benutzer kann ohne Authentifizierung auf den Switch zugreifen.
- *Lokal*: Benutzername und Kennwort werden mit den auf dem lokalen Switch 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 4 Klicken Sie auf **Übernehmen**. Die ausgewählten Authentifizierungsmethoden werden der Zugriffsmethode zugeordnet.

Defininieren der Verwaltungszugriffsmethode

Zugriffsprofile bestimmen, wie Benutzer, die über verschiedene Zugriffsmethoden auf den Switch zugreifen, authentifiziert und autorisiert werden. Mithilfe von Zugriffsprofilen kann der Verwaltungszugriff von bestimmten Quellen begrenzt werden.

Nur Benutzer, die beide Methoden, das heißt sowohl die Authentifizierung durch das aktive Zugriffsprofil als auch die Verwaltungszugriffsauthentifizierung, erfolgreich durchlaufen, erhalten Verwaltungszugriff auf den Switch.

Für den Switch 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 den Switch 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 Switch-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 Switch-Modul nur über eine HTTPS-Sitzung erhalten kann, während eine andere Benutzergruppe sowohl über HTTPS- als auch über Telnet-Sitzungen auf das Switch-Modul 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 den Switch zuzugreifen versucht, prüft der Switch, ob das aktive Zugriffsprofil den Verwaltungszugriff auf den Switch mit dieser Methode ausdrücklich zulässt. Wenn keine Übereinstimmung gefunden wird, wird der Zugriff verweigert.

Wenn ein Versuch, auf den Switch zuzugreifen, das aktive Zugriffsprofil verletzt, gibt der Switch 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 Switch 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**. Die Seite *Zugriffsprofile* wird angezeigt.

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 Switch-Konfigurationsdienstprogramm sofort getrennt, und Sie können nur noch über den Konsolen-Port auf den Switch 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 Switch-Konfigurationsdienstprogramm, abhängig vom ausgewählten Zugriffsprofil, u. U. getrennt wird.

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 den Switch 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 den Switch anfordern, der den Kriterien des Telnet-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
  - *Sicheres Telnet*: Benutzern, die Zugriff auf den Switch anfordern, der den Kriterien des SSH-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
  - *HTTP*: Benutzern, die Zugriff auf den Switch anfordern, der den Kriterien des HTTP-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
  - *Sicheres HTTP (HTTPS)*: Benutzern, die Zugriff auf den Switch anfordern, der den Kriterien des HTTPS-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
  - *SNMP*: Benutzern, die Zugriff auf den Switch 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 den Switch wird gewährt, wenn der Benutzer mit den Einstellungen im Profil übereinstimmt.
  - *Verweigern*: Zugriff auf den Switch 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**: 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 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 den Switch 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 den Switch von sämtlichen IP-Adressen aus beschränken, mit Ausnahme von IP-Adressen, die dem IT-Verwaltungszentrum zugeordnet sind. Auf diese Weise kann der Switch 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**. Die Seite *Profilregeln* wird angezeigt.

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. Die Seite *Profilregel hinzufügen* wird angezeigt.

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 den Switch 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 den Switch anfordern, der den Kriterien des Telnet-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
  - *Sicheres Telnet (SSH)*: Benutzern, die Zugriff auf den Switch anfordern, der den Kriterien des SSH-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
  - *HTTP*: Der Regel wird HTTP-Zugriff zugewiesen. Benutzern, die Zugriff auf den Switch anfordern, der den Kriterien des HTTP-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.
  - *Sicheres HTTP (HTTPS)*: Benutzern, die Zugriff auf den Switch anfordern, der den Kriterien des HTTPS-Zugriffsprofils entspricht, wird der Zugriff entweder gewährt oder verweigert.

- *SNMP*: Benutzern, die Zugriff auf den Switch 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 den Switch 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.

Konfigurieren von TCP-/UDP-Services

Auf der Seite *TCP/UDP-Services* können TCP- oder UDP-basierte Services für den Switch aktiviert werden, normalerweise zu Sicherheitszwecken.

Der Switch 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**. Die Seite *TCP/UDP-Services* wird angezeigt.

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.

In der Tabelle für TCP-Services werden die folgenden Felder für die einzelnen Services angezeigt:

- **Servicename**: Die Zugriffsmethode, über die der Switch den TCP-Service anbietet.
- **Typ**: Das IP-Protokoll, das für den Service verwendet wird.
- **Lokale IP-Adresse**: Die lokale IP-Adresse, über die der Switch den Service anbietet.

- **Lokaler Port**: Der lokale Port, über den der Switch 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-Services" werden die folgenden Informationen angezeigt:

- **Servicename**: Die Zugriffsmethode, über die der Switch den UDP-Service anbietet.
- **Typ**: Das IP-Protokoll, das für den Service verwendet wird.
- **Lokale IP-Adresse**: Die lokale IP-Adresse, über die der Switch den Service anbietet.
- **Lokaler Port**: Der lokale UDP-Port, über den der Switch den Service anbietet.
- **Anwendungsinstanz**: Die Serviceinstanz des UDP-Service. (Wenn beispielsweise zwei Absender Daten an das gleiche Ziel senden.)

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

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 Switch eingehen, zu begrenzen und die Typen von Frames zu definieren, die im Hinblick auf diese Begrenzung berücksichtigt werden.

Wenn Sie einen Schwellenwert in das System eingeben, verwirft der Port den Datenverkehr, sobald der Schwellenwert erreicht ist. Der Port bleibt blockiert, bis der Datenverkehr wieder unter diesen Schwellenwert abgesunken ist. Dann wird die normale Weiterleitung wieder aufgenommen.

So definieren Sie die Sturmsteuerung:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Sturmsteuerung**. Die Seite *Sturmsteuerung* wird angezeigt.

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**. Die Seite *Sturmsteuerung bearbeiten* wird angezeigt.

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**: Der Switch lernt MAC-Adressen bis zum konfigurierten Grenzwert erlaubter Adressen. Nach Erreichen des Grenzwerts lernt der Switch 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 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.

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**. Die Seite *Portsicherheit* wird angezeigt.

SCHRITT 2 Wählen Sie die Schnittstelle aus, die geändert werden soll, und klicken Sie auf **Bearbeiten**. Die Seite *Schnittstelleneinstellungen für Portsicherheit bearbeiten* wird angezeigt.

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 heruntergefahren, bis er reaktiviert wird oder bis der Switch 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.

Konfigurieren von 802.1X

Die portbasierte Zugriffssteuerung führt dazu, dass auf die Switch-Ports auf zwei verschiedene Arten zugegriffen werden kann. Ein Zugriffspunkt ermöglicht ungesteuerten Datenaustausch, ungeachtet des Autorisierungszustands (*ungesteuerter Port*). Der andere Zugriffspunkt autorisiert den Datenaustausch zwischen einem Host und dem Switch.

802.1X ist ein IEEE-Standard für die portbasierte Netzwerkzugriffssteuerung. Im 802.1X-Framework kann ein Gerät (der Anfrager) Zugriff auf einen Port von einem Remote-Gerät (dem Authentifikator) anfordern, mit dem es verbunden ist. Nur wenn der Anfrager, von dem Zugriff auf den Port angefordert wird, authentifiziert und autorisiert wurde, können von ihm Daten an den Port gesendet werden. Anderenfalls werden die Daten des Anfragers vom Authentifikator verworfen, es sei denn, die Daten werden an ein Gast-VLAN und/oder ein nicht authentifiziertes VLAN gesendet.

Die Authentifizierung des Anfragers wird über den Authentifikator durch einen externen RADIUS-Server durchgeführt. Der Authentifikator überwacht das Ergebnis der Authentifizierung.

Beim 802.1X-Standard kann ein Gerät gleichzeitig Anfrager und Authentifikator für einen Port sein, also Zugriff auf den Port sowohl anfordern als auch gewähren. Dieses Gerät fungiert jedoch ausschließlich als Authentifikator und übernimmt die Rolle des Anfragers nicht.

Es gibt folgende Varianten von 802.1X:

- **Einzelsitzungs-802.1X**:
  - **Einzelsitzung/Einzelner Host**: In diesem Modus unterstützt der Switch als Authentifikator eine einzige 802.1X-Sitzung und erteilt dem autorisierten Anfrager die Berechtigung, den Port zu verwenden. Alle Zugriffe durch andere Geräte, die über den gleichen Port empfangen werden, werden erst dann erlaubt, wenn der Port nicht mehr vom autorisierten Anfrager verwendet wird oder wenn der Zugriff auf ein nicht authentifiziertes VLAN oder ein Gast-VLAN erfolgt.

- **Einzelsitzung/Mehrere Hosts**: Dies entspricht dem 802.1X-Standard. In diesem Modus gewährt der Switch als Authentifikator jedem Gerät das Recht, einen Port so lange zu verwenden, wie dem Anfrager die Berechtigung dazu erteilt worden ist.

- **Mehrfachsitzungs-802.1X**: Jedes Gerät (Anfrager), das eine Verbindung zu einem Port herstellt, muss durch den Switch (Authentifikator) einzeln in einer eigenen 802.1X-Sitzung authentifiziert und autorisiert werden.

  HINWEIS Dies ist der einzige Modus, der Dynamic VLAN Assignment (DVA) unterstützt.

HINWEIS DVA wird nicht unterstützt, wenn der Switch im Schicht-3-Systemmodus betrieben wird.

Dynamic VLAN Assignment (DVA)

Dynamic VLAN Assignment (DVA) wird in diesem Handbuch auch als RADIUS-VLAN-Zuordnung bezeichnet. Wenn ein Port im Mehrfachsitzungsmodus betrieben wird und DVA aktiviert ist, fügt der Switch den Port automatisch als Mitglied ohne Tag dem VLAN hinzu, dem er vom RADIUS-Server während der Authentifizierung zugewiesen wurde. Der Switch klassifiziert Pakete ohne Tag für das zugewiesene VLAN, wenn die Pakete von authentifizierten und autorisierten Geräten oder Ports stammen.

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.
- Das zugewiesene VLAN darf nicht das Standard-VLAN sein und muss am Switch erstellt worden sein.
- Der Switch darf nicht für die gleichzeitige Verwendung einer DVA- und einer MAC-basierten Gruppe konfiguriert sein.
- 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.

Folgende Authentifizierungsmethoden sind möglich:

- 802.1X: Der Switch unterstützt den Authentifizierungsmechanismus wie im Standard für die Authentifizierung und Autorisierung von 802.1X-Anfragern beschrieben.

- MAC-basiert: Der Switch kann so konfiguriert werden, dass dieser Modus für die Authentifizierung und Autorisierung von Geräten verwendet wird, die 802.1X nicht unterstützen. Der Switch emuliert die Anfragerrolle im Namen des nicht 802.1X-fähigen Geräts und verwendet bei der Kommunikation mit den RADIUS-Servern die MAC-Adresse des Geräts als Benutzername und Kennwort. MAC-Adressen für den Benutzernamen und das Kennwort müssen in Kleinbuchstaben und ohne Trennzeichen eingegeben werden (z. B.: aaccbb55ccff). So verwenden Sie die MAC-basierte Authentifizierung für einen Port:
  - Es muss ein Gast-VLAN definiert sein.
  - Der Port muss für das Gast-VLAN aktiviert sein.
  - Die Pakete vom ersten Anfrager beim Port vor der Autorisierung müssen Pakete ohne Tag sein.

Sie können einen Port so konfigurieren, dass 802.1X-, MAC-basierte oder 802.1X- und MAC-basierte Authentifizierung gleichzeitig verwendet werden. Wenn ein Port für die gleichzeitige Verwendung von 802.1X- und MAC-basierter Authentifizierung konfiguriert ist, hat 802.1X Vorrang vor einem Nicht-802.1X-Gerät.

Nicht authentifizierte VLANs und Gast-VLAN

Nicht authentifizierte und Gast-VLANs stellen Zugriff auf Services bereit, für die eine 802.1X- oder MAC-basierte Authentifizierung und Autorisierung der abonnierenden Geräte oder Ports nicht erforderlich ist.

Ein nicht authentifiziertes VLAN ist ein VLAN, das sowohl autorisierten als auch nicht autorisierten Geräten oder Ports Zugriff gewährt. Sie können in **Erstellen von VLANs** eines oder mehrere VLANs als nicht authentifiziertes VLAN konfigurieren.

Ein nicht authentifiziertes VLAN hat die folgenden Merkmale:

- Es muss ein statisches VLAN sein und kann 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.
- Es ist nur für nicht autorisierte Geräte oder Ports von Geräten automatisch verfügbar, die verbunden sind und die für Gast-VLANs aktiviert sind.
- Wenn ein Port für Gast-VLANs aktiviert ist, fügt der Switch den Port automatisch als Mitglied ohne Tag des Gast-VLANs hinzu, wenn der Port nicht autorisiert ist, und entfernt den Port aus dem Gast-VLAN, wenn der erste Anfrager des Ports autorisiert ist.
- Ein Gast-VLAN kann nicht als Voice-VLAN oder als nicht authentifiziertes VLAN verwendet werden.

Der Switch verwendet das Gast-VLAN auch für die Authentifizierung an Ports, die für den Mehrfachsitzungsmodus und MAC-basierte Authentifizierung konfiguriert sind. Daher müssen Sie ein Gast-VLAN konfigurieren, bevor Sie den MAC-Authentifizierungsmodus verwenden können.

802.1X-Parameter-Workflow

Gehen Sie beim Definieren der 802.1X-Parameter folgendermaßen vor:

- (Optional) Legen Sie auf den Seiten *Zeitbereich* und *Wiederkehrender Bereich* einen oder mehrere Zeitbereiche fest. Diese Bereiche werden auf der Seite *Portauthentifizierung bearbeiten verwendet.*
- (Optional) Definieren Sie eines oder mehrere statische VLANs als nicht authentifiziertes VLAN gemäß der Beschreibung im Abschnitt **Definieren der 802.1X-Eigenschaften**. Autorisierte und nicht autorisierte 802.1X-Geräte oder Ports können immer Pakete von nicht autorisierten VLANs empfangen oder an diese senden.
- Definieren Sie auf der Seite *Portauthentifizierung bearbeiten* 802.1X-Einstellungen für die einzelnen Ports.

Beachten Sie Folgendes:

- Auf dieser Seite können Sie DVA für einen Port aktivieren, indem Sie das Feld "RADIUS-VLAN-Zuordnung" auswählen.
- Sie können das Feld "Gast-VLAN" so einstellen, dass eingehende Frames ohne Tag an das Gast-VLAN gehen.

- Definieren Sie auf der Seite *Portauthentifizierung* die Hostauthentifizierungsparameter für die einzelnen Ports.
- Zeigen Sie auf der Seite *Authentifizierte Hosts* den 802.1X-Authentifizierungsverlauf an.

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 portbasiert Authentifizierung:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **802.1X** > **Eigenschaften**. Die Seite *Eigenschaften* wird angezeigt.

SCHRITT 2 Geben Sie die Parameter ein.

- **portbasiert Authentifizierung**: Aktivieren oder deaktivieren Sie die portbasierte 802.1X-Authentifizierung.
- **Authentifizierungsmethode**: Wählen Sie die Benutzer-Authentifizierungsmethoden. Folgende Optionen sind möglich:
  - *RADIUS, Ohne*: Die Portauthentifizierung 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 *Gast-VLAN-Timeout*-Zeitraum 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.

In der Tabelle VLAN-Authentifizierung werden alle VLANs angezeigt mit der Angabe, ob für sie die Authentifizierung aktiviert ist.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die 802.1X-Eigenschaften werden in die aktuelle Konfigurationsdatei geschrieben.

Konfigurieren nicht authentifizierter VLANs

Wenn 802.1X für einen Port aktiviert ist, können nicht autorisierte Ports oder Geräte nicht auf ein VLAN zugreifen, es sei denn, es handelt sich um ein Gast-VLAN oder ein nicht authentifiziertes VLAN. Sie können ein statisches VLAN mithilfe des im Abschnitt **Definieren der 802.1X-Eigenschaften** beschriebenen Verfahrens zu einem authentifizierten VLAN machen, sodass sowohl autorisierte als auch nicht autorisierte 802.1X-Geräte oder Ports Pakete von nicht authentifizierten VLANs empfangen oder an diese senden können. Sie müssen VLANs auf der Seite *Port zu VLAN* manuell Ports hinzufügen.

SCHRITT 1 Klicken Sie auf **Sicherheit** > **802.1X** > **Eigenschaften**. Die Seite *Eigenschaften* wird angezeigt.

SCHRITT 2 Wählen Sie ein VLAN aus, und klicken Sie auf **Bearbeiten**. Die Seite *VLAN-Authentifizierung bearbeiten* wird angezeigt.

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.

Definieren der 802.1X-Authentifizierung

Auf der Seite *Portauthentifizierung* 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** > **Portauthentifizierung**. Die Seite *Portauthentifizierung* wird angezeigt.

Auf dieser Seite werden die Authentifizierungseinstellungen für alle Ports angezeigt.

SCHRITT 2 Wählen Sie einen Port aus, und klicken Sie auf **Bearbeiten**. Die Seite *Portauthentifizierung bearbeiten* wird angezeigt.

SCHRITT 3 Geben Sie die Parameter ein.

- **Schnittstelle**: Wählen Sie einen Port aus.
- **Benutzername**: Der Benutzername des Ports.
- **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". Der Switch stellt dem Client keine Authentifizierungsservices über die Schnittstelle bereit.

- *Automatisch*: portbasiert Authentifizierung und Autorisierung über den Switch werden aktiviert. Die Schnittstelle wechselt zwischen einem autorisierten und einem nicht autorisierten Status, basierend auf dem Authentifizierungsaustausch zwischen dem Switch und dem Client.
- *Autorisierung erzwingen*: Die Schnittstelle wird ohne Authentifizierung autorisiert.

- **RADIUS-VLAN-Zuweisung**: Wählen Sie diese Option, um die dynamische VLAN-Zuweisung für den ausgewählten Port zu aktivieren. Die dynamische VLAN-Zuweisung ist nur dann möglich, wenn der 802.1X-Modus auf Mehrfachsitzungen eingestellt ist. (Nach der Authentifizierung verbindet sich der Port mit dem Anfrager-VLAN als Port ohne Tag innerhalb dieses VLAN.)
- **Gast-VLAN**: Wählen Sie diese Option, um die Anzeige der Verwendung eines zuvor definierten Gast-VLAN durch den Switch zu aktivieren. Folgende Optionen sind möglich:
  - *Ausgewählt*: Die Verwendung eines Gast-VLAN 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.
- **Authentifizierungsmethode**: Wählen Sie die Authentifizierungsmethode für den Port. Folgende Optionen sind möglich:
  - *Nur 802.1X*: 802.1X-Authentifizierung ist die einzige mögliche Authentifizierungsmethode für den Port.
  - *Nur MAC*: Der Port wird basierend auf der MAC-Adresse des Anfragers authentifiziert. Für den Port können nur 8 MAC-basierte Authentifizierungen verwendet werden.
  - *802.1X und MAC*: Sowohl 802.1X- als auch MAC-basierte Authentifizierungen können vom Switch ausgeführt werden. Die 802.1X-Authentifizierung hat Vorrang.

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 ":" oder "-"-Trennzeichen eingegeben werden, z. B.: 0020aa00bbcc.

- **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:
  - *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 portbasiert Authentifizierung wird überprüft).
- **Zeitbereichsname**: Wählen Sie das Profil, durch das der Zeitbereich spezifiziert wird.
- **Ruhezeit**: Geben Sie den Zeitraum in Sekunden ein, den der Switch nach einem fehlgeschlagenen Authentifizierungsaustausch im Ruhestatus verweilt.

- **EAP wird erneut gesendet**: Geben Sie den Zeitraum in Sekunden ein, den der Switch 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 Authentifizierungs-Server gesendet werden.
- **Grund für Abbruch**: Ggf. Angabe des Grunds für den Abbruch der Portauthentifizierung.

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, und die Aktion, die bei einem Verstoß ausgeführt werden soll.

Die 802.1X-Modi sind:

- **Einzel-Host**: Nur ein einzelner autorisierter Host kann auf den Port zugreifen. (Portsicherheit kann für einen Port im Einzel-Host-Modus nicht aktiviert werden.)
- **Mehrfach-Host (802.1X)**: Es können sich mehrere Hosts mit einem einzelnen 802.1X-aktivierten Port verbinden. Nur der erste Host muss autorisiert werden, dann ist der Port offen für alle Zugriffe auf das Netzwerk. Wenn die Host-Authentifizierung fehlschlägt oder eine EAPOL-Abmeldebenachrichtigung empfangen wird, wird allen verbundenen Clients der Zugriff auf das Netzwerk verweigert.

- **Mehrere Sitzungen**: Die Auswahl dieser Option ermöglicht einer Anzahl bestimmter autorisierter Hosts den Zugriff auf den Port. Jeder Host wird behandelt, als sei er der erste und einzige Benutzer, und muss authentifiziert werden. Die Filterung erfolgt auf der Basis der MAC-Adresse.

So definieren Sie erweiterte 802.1X-Einstellungen für Ports:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **802.1X** > **Host- und Sitzungsauthentifizierung**. Die Seite *Host- und Sitzungsauthentifizierung* wird angezeigt.

802.1X-Authentifizierungsparameter werden für alle Ports beschrieben. Alle Felder mit Ausnahme der folgenden werden auf der Seite *Host- und Sitzungsauthentifizierung bearbeiten* beschrieben.

- **Status**: Zeigt den Host-Status an. Ein Sternchen zeigt an, dass der Port entweder nicht verbunden oder nicht betriebsbereit ist. Folgende Optionen sind möglich:
  - *Nicht autorisiert*: Entweder ist die Port-Steuerung auf *Nicht-Autorisierung erzwingen* gesetzt, und der Port-Link ist nicht betriebsbereit, oder die Port-Steuerung ist auf *Autom.* gesetzt, aber ein Client ist nicht über den Port authentifiziert worden.
  - *Autorisierung erzwingen*: Clients haben vollen Zugriff auf den Port.
  - *Einzel-Host-Sperre*: Die Port-Steuerung ist auf *Autom.* gesetzt, und es ist nur ein einzelner Client über den Port authentifiziert worden.
  - *Kein Einzel-Host*: Die Portsteuerung ist auf *Autom.* festgelegt und der Mehrfach-Host-Modus ist aktiviert. Mindestens ein Client wurde authentifiziert.
  - *Nicht im Modus Autom.*: Die automatische Port-Steuerung ist nicht aktiviert.
- **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**. Die Seite *Host- und Sitzungsauthentifizierung bearbeiten* wird angezeigt.

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 werden oben unter *Definieren der Host- und Sitzungsauthentifizierung* beschrieben.

  HINWEIS Die folgenden Felder sind nur relevant, wenn Sie im Feld "Hostauthentifizierung" die Option "Einzeln" auswählen.

Einstellungen für Einzelhostverstöße:

- **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 heruntergefahren, bis er reaktiviert wird oder der Switch neu gestartet wird.
- **Verletzungsaktion für Einzel-Host**: Wählen Sie diese Option aus, um Traps zu aktivieren.
- **Trap-Frequenz (bei einzelner Hostverletzung)**: 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** > **Authentifizierte Hosts**. Die Seite *Authentifizierte Hosts* wird angezeigt.

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. Folgende Optionen sind möglich:
  - *Keine*: Es wurde keine Authentifizierung angewendet, die Autorisierung erfolgte automatisch.
  - *RADIUS*: Der Benutzer wurde von einem RADIUS-Server authentifiziert.
- **MAC-Adresse**: Die MAC-Adresse des Anfragers.

Definieren von Zeitbereichen

Eine Erläuterung dieser Funktion finden Sie unter **Systemzeit**.

Denial of Service-Sicherung

Denial of Service-(DoS-)Sicherung erhöht die Netzwerksicherheit, indem verhindert wird, dass Pakete mit bestimmten IP-Adressparametern Zugang zum Netzwerk erhalten.

Außerdem eliminiert die DoS-Prävention Pakete mit Headern oder Inhalten, die eine bösartige Absicht signalisieren.

Mithilfe von Denial of Service-Sicherung können Netzwerkmanager:

- Paketen, die reservierte IP-Adressen enthalten, den Zugang verweigern (Seite *Ungültige Adressen*).
- TCP-Verbindungen von bestimmten Schnittstellen aus verhindern (Seite *SYN-Filterung*) und Ratenbegrenzungen für Pakete festlegen (Seite *SYN-Ratenschutz).*
- die 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*).

SCT

Der Cisco-Switch ist ein fortschrittlicher Switch für die Verarbeitung von Endbenutzer-Datenverkehr sowie den folgenden Verkehrstypen:

- Verwaltungsverkehr
- Protokollverkehr
- Snooping-Verkehr

Unerwünschter Verkehr führt zu einer Belastung der CPU und kann den Betrieb des Switch beeinträchtigen.

Der Switch stellt mithilfe der SCT-Funktion (Secure Core Technology) sicher, dass Verwaltungs- und Protokollverkehr unabhängig von der Gesamtmenge des empfangenen Verkehrs empfangen und verarbeitet wird.

SCT ist im Gerät standardmäßig aktiviert und kann nicht deaktiviert werden.

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.

Einstellungen der Denial of Service Security Suite

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 Anzeige der CPU-Ressourcenauslastung zu aktivieren.

SCHRITT 3 Wählen Sie **DoS-Prävention** aus, 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.

SCHRITT 4 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 5 Klicken Sie auf **Übernehmen**. Die Security Suite-Einstellungen für die Denial of Service-Sicherung werden in die aktuelle Konfigurationsdatei geschrieben.

- Wenn "Prävention auf Schnittstellenebene" ausgewählt ist, klicken Sie auf die entsprechende Schaltfläche **Bearbeiten**, und konfigurieren Sie die gewünschte Sicherung.

Definieren ungültiger Adressen

Auf der Seite *Ungültige Adressen* können Sie IP-Adressen eingeben, die bei Auftauchen im Netzwerk auf einen Angriff hinweisen. Pakete von diesen Adressen werden verworfen.

Der Switch 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**. Die Seite *Ungültige Adressen* wird angezeigt.

SCHRITT 2 Wählen Sie "Reservierte ungültige Adressen" aus 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**. Die Seite *Ungültige Adressen hinzufügen* wird angezeigt.

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.

Definieren der 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**. Die Seite *SYN-Filterung* wird angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *SYN-Filterung hinzufügen* wird angezeigt.

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.

Definieren des SYN-Ratenschutzes

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 festgelegt wird.

Diese Funktion ist nur verfügbar, wenn sich das Gerät im Schicht-2-Systemmodus befindet.

So definieren Sie den SYN-Ratenschutz:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **Denial of Service-Sicherung** > **SYN-Ratenschutz**. Die Seite *SYN-Ratenschutz* wird angezeigt.

Auf dieser Seite wird der SYN-Ratenschutz angezeigt, der zurzeit für die einzelnen Schnittstellen definiert ist.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *SYN-Ratenschutz hinzufügen* wird angezeigt.

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.

Definieren der 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**. Die Seite *ICMP-Filterung* wird angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *ICMP-Filterung hinzufügen* wird angezeigt.

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.

Definieren der IP-Fragmentblockierung

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**. Die Seite *IP-Fragmentfilterung* wird angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *IP-Fragmentfilterung hinzufügen* wird angezeigt.

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.

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 der Switch 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 Switch weitergeleitet. Anderenfalls wird es gelöscht.

Interaktionen mit anderen Funktionen

Folgende 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 kan 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 **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**. Die Seite *Eigenschaften* wird angezeigt.

SCHRITT 2 Wählen Sie **Aktivieren** aus, um IP Source Guard global 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.** Die Seite *Schnittstelleneinstellungen* wird angezeigt.

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**. Die Seite *Schnittstelleneinstellungen bearbeiten* wird angezeigt. 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 der Switch 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 **DHCP-Snooping**.

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.** Die Seite *Bindungsdatenbank* wird angezeigt.

SCHRITT 2 Die DHCP-Snooping-Bindungsdatenbank verwendet zum Verwalten der Datenbank TCAM-Ressourcen. Füllen Sie das Feld **Inaktive einfügen** aus, um

auszuwählen, wie häufig der Switch 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**.

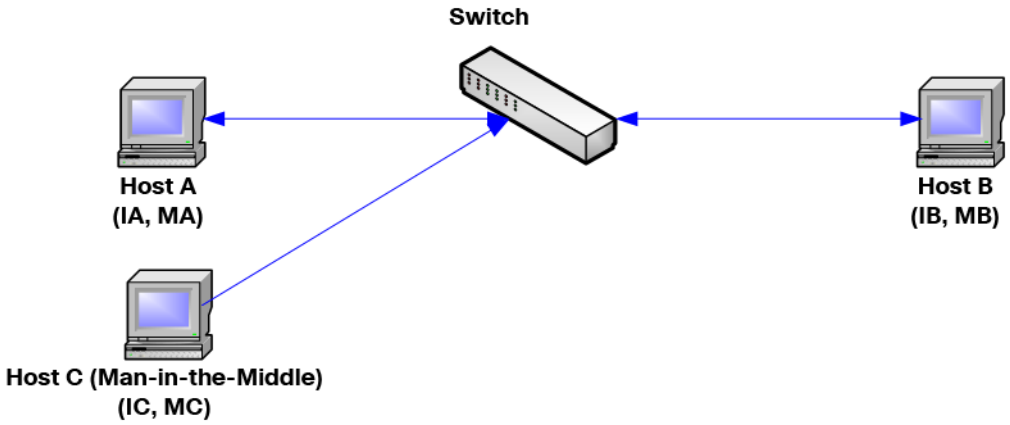
Dynamic ARP Inspection

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

Tabelle für ARP-Standardeinstellungen

Option	Standardzustand
Dynamic ARP Inspection	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 Zum Aktivieren der ARP-Prüfung und Konfigurieren verschiedener Optionen verwenden Sie die Seite **Sicherheit > ARP-Prüfung > Eigenschaften**.

SCHRITT 2 Zum Konfigurieren von Schnittstellen als für ARP vertrauenswürdig oder nicht vertrauenswürdig verwenden Sie die Seite **Sicherheit > ARP-Prüfung > Schnittstelleneinstellung**.

SCHRITT 3 Zum Hinzufügen von Regeln verwenden Sie die Seiten **Sicherheit > ARP-Prüfung > ARP-Zugriffssteuerung und Regeln für ARP-Zugriffssteuerung**.

SCHRITT 4 Zum Definieren der VLANs, für die die ARP-Prüfung aktiviert ist, und der Zugriffssteuerungsregeln für die einzelnen VLANs verwenden Sie 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**. Die Seite *Eigenschaften* wird angezeigt.

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 Dynamic ARP Inspection-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 Seite *Schnittstelleneinstellungen* wird angezeigt.

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**. Die Seite *Schnittstelleneinstellungen bearbeiten* wird angezeigt.

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**. Die Seite *ARP-Zugriffssteuerung* wird angezeigt.

SCHRITT 2 Zum Hinzufügen eines Eintrags klicken Sie auf **Hinzufügen**. Die Seite *ARP-Zugriffssteuerung hinzufügen* wird angezeigt.

SCHRITT 3 Geben Sie Werte für die Felder ein:

- **ARP-Zugriffssteuerungsname**: Geben Sie einen vom Benutzer erstellten Namen ein.
- **MAC-Adresse**: Die MAC-Adresse des Pakets.
- **IP-Adresse**: Die IP-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 Seite *Regeln für ARP-Zugriffssteuerung* wird angezeigt.

Die zurzeit definierten Zugriffsregeln werden angezeigt.

SCHRITT 2 Zum Hinzufügen weiterer Regeln zu einer Gruppe klicken Sie auf **Hinzufügen**. Die Seite *ARP-Zugriffssteuerungsregel hinzufügen* wird angezeigt.

SCHRITT 3 Wählen Sie eine Zugriffssteuerungsgruppe aus und geben Sie Werte für die Felder ein:

- **MAC-Adresse**: Die MAC-Adresse des Pakets.
- **IP-Adresse**: Die IP-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**. Die Seite *VLAN-Einstellungen* wird geöffnet.

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 aus und wählen Sie eine zuvor definierte **ARP-Zugriffssteuerungsgruppe** aus.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Einstellungen werden definiert und die aktuelle Konfigurationsdatei wird aktualisiert.

18

Secure Sensitive Data

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.

Einführung

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 (RADIUS und TACACS) 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 [Sx300-500] 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 [Sx300-500] oder SNMPv1/v2 und 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.

Tabelle 1 Zulässige Leseberechtigungen nach Verwaltungskanal

Verwaltungskanal	Zulässige Optionen für Leseberechtigung
Sicher	Beide, Nur verschlüsselt

Tabelle 1 Zulässige Leseberechtigungen nach Verwaltungskanal

Verwaltungskanal	Zulässige Optionen für Leseberechtigung
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.

Tabelle 2 Standardlesemodi für Leseberechtigungen

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 der jeweiligen 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 FTP als zugrunde liegendes Protokoll 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- und TACACS-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 3 SSD-Standardregeln

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 zeigt sensible Daten in einer Sitzung abhängig von der Leseberechtigung und dem Standardlesemodus des Benutzers in verschlüsselter oder unverschlüsselter Form an.

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 der sensiblen Daten
- Steuerung der Höhe der Sicherheit für Konfigurationsdateien
- Steuerung der Anzeige sensibler Daten innerhalb der aktuellen Sitzung

Passphrase

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 mit der gleichen Passphrase können mit dem anhand 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. (Siehe "Automatische SSD-Konfiguration 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 Konfigurationsdatei-Passphrase

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, auf welche Weise sensible Daten angezeigt werden. Der Lesemodus kann "Unverschlüsselt" entsprechen, 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. Der Benutzer kann die aktuelle Konfiguration ändern, indem er die Backup-Konfigurationsdatei oder die Spiegelkonfigurationsdatei mit anderen Verwaltungsaktionen über CLI, XML, [Sx300-500]SNMP usw. kopiert.

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 mit dem anhand 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 im Auslieferungszustand oder mit Werkseinstellungen verwenden für den Zugriff auf den **[Sx300-500]**SCP-Server den Standardbenutzer "anonymous".

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.

Sicherheit der Verwaltungskanäle

Verwaltungskanäle

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	
[Sx300-500]SNMPv1/v2/v3 ohne Datenschutz	Unsicheres XML-SNMP	Sicheres XML-SNMP
SNMPv3 mit Datenschutz	Sicheres XML-SNMP (Benutzer der Ebene 15)	
TFTP	Unsicher	[Sx300-500]SCP
[Sx300-500]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:

- 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** > **Eigenschaften**. Die Seite *Eigenschaften* wird angezeigt. Das folgende 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 Konfigurationsdatei-Passphrase** 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**).

So ändern Sie die lokale Passphrase:

SCHRITT 4 Klicken Sie auf **Lokale Passphrase ändern** und geben Sie eine neue **Lokale Passphrase** ein:

- **Standard**: Die Standard-Passphrase des Geräts wird verwendet.
- **Benutzerdefiniert (unverschlüsselt)**: Geben Sie eine neue Passphrase ein und bestätigen Sie sie.

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-Regeln**. Die Seite *SSD-Regeln* wird angezeigt.

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, **[Sx300-500]** SCP, SSH und HTTPS), nicht für die Kanäle **[Sx300-500]** SNMP undXML.
  - *Unsicher*: Gibt an, dass die Regel nur für unsichere Kanäle gilt (Telnet, TFTP und HTTP), nicht für die Kanäle **[Sx300-500]** SNMP und XML.
  - *Sicheres XML-SNMP*: Gibt an, dass die Regel nur für XML über HTTPS **[Sx300-500]** und SNMPv3 mit Datenschutz gilt.
  - *Unsicheres XML-SNMP*: Gibt an, dass die Regel nur für XML über HTTP oder **[Sx300-500]** und 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 Die folgenden Aktionen können ausgeführt werden:

▪ **Standard wiederherstellen**: Stellt die ursprüngliche Version einer von einem Benutzer geänderten Standardregel wieder her.

▪ **Standard für alle Regeln wiederherstellen**: Stellt die ursprüngliche Version aller von einem Benutzer geänderten Regeln wieder her und entfernt alle benutzerdefinierten Regeln.

19

Verwenden der SSH-Clientfunktion

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 einen Switch zu übertragen.

Im Hinblick auf SSH ist die im Switch ausgeführte SCP-Anwendung eine SSH-Clientanwendung und der SCP-Server eine SSH-Serveranwendung.

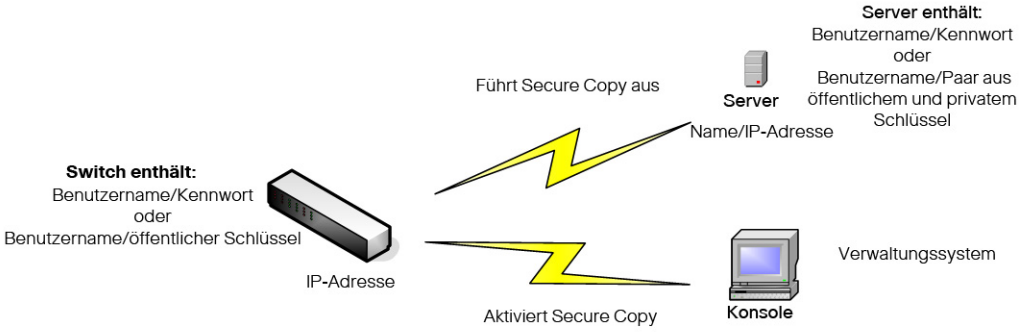
Wenn Dateien über TFTP oder HTTP heruntergeladen werden, ist die Datenübertragung ungeschützt.

Beim Herunterladen von Dateien über SCP werden die Informationen über einen sicheren Kanal vom SCP-Server auf den Switch heruntergeladen. Der Erstellung dieses sicheren Kanals geht eine Authentifizierung voraus, die sicherstellt, dass der Benutzer den Vorgang ausführen darf.

Der Benutzer muss sowohl im Switch 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 einen Switch (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. Dazu verwenden Sie nicht das Verwaltungssystem des Switch. Das Serverkennwort können Sie jedoch über das Verwaltungssystem des Switch ändern, nachdem Sie auf dem Server einen Benutzernamen eingerichtet haben.

Dann müssen Sie den Benutzernamen und das Kennwort im Switch erstellen. Wenn Daten vom Server an den Switch übertragen werden, müssen der vom Switch 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 jeden verwalteten Switch ist ein eigener Benutzername und ein entsprechendes Kennwort erforderlich. Sie können jedoch für mehrere Switches den gleichen Benutzernamen und das gleiche Kennwort verwenden.

Die Kennwortmethode ist die Standardmethode für den Switch.

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 Switch 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.

Beim Starten des Switch werden RSA- und DSA-Standardschlüsselpaare für den Switch 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 Switch kopiert werden kann, gibt es eine Importmethode, mit der Sie private Schlüssel von Switch zu Switch kopieren können (siehe Beschreibung unter **Importieren von Schlüsseln**).

Importieren von Schlüsseln

Bei der Schlüsselmethode müssen Sie für jeden einzelnen Switch individuelle öffentliche und private Schlüssel erstellen. Diese privaten Schlüssel können aus Sicherheitsgründen nicht direkt von einem Switch zu einem anderen 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 in einem Switch 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 Switch nur über einen 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 SSH-Serverauthentifizierung aktiviert ist, authentifiziert der im Switch ausgeführte SSH-Client den SSH-Server mit dem folgenden Authentifizierungsprozess:

- Der Switch berechnet den Fingerprint des empfangenen öffentlichen Schlüssels des SSH-Servers.
- Der Switch sucht in der Tabelle mit vertrauenswürdigen SSH-Servern 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 *Backup-Konfiguration/Protokoll* ein temporäres Kennwort, wenn Sie die sichere Datenübertragung tatsächlich aktivieren.

b. Aktualisieren Sie die Firmware, das Boot-Image oder die Sprachdatei mit 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 Sie können 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 Sie können 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 über die Seite *Benutzerkennwort ändern*. 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 Switch auf einen anderen:

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 > 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* in ein externes Gerät. Kopieren Sie die öffentlichen und privaten Schlüssel getrennt.

SCHRITT 4 Melden Sie sich bei einem anderen Switch 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 den zweiten Switch zu kopieren.

Workflow 3: So definieren Sie einen vertrauenswürdigen Server:

SCHRITT 1 Aktivieren Sie auf der Seite *SSH-Serverauthentifizierung* die SSH-Serverauthentifizierung.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, um einen neuen Server hinzuzufügen und Informationen zu seiner Identifizierung einzugeben.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um den Server der Tabelle mit vertrauenswürdigen SSH-Servern hinzuzufügen.

Workflow 4: *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 Werte für die Felder ein.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um das Kennwort auf dem SSH-Server zu ändern.

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 den Switch 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**. Die Seite *SSH-Benutzerauthentifizierung* wird angezeigt.

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 die 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**. Die Seite *SSH-Serverauthentifizierung* wird angezeigt.

SCHRITT 2 Wählen Sie **Aktivieren** aus, um die SSH-Serverauthentifizierung zu aktivieren.

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.
- **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 ein Kennwort auf einem SSH-Server:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **SSH-Client** > **Benutzerkennwort auf SSH-Server ändern**. Die Seite *Benutzerkennwort auf SSH-Server ändern* wird angezeigt.

SCHRITT 2 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 die entsprechenden Felder ein.

SCHRITT 3 Geben Sie den Wert für **Benutzername** ein. Der Benutzername muss mit dem Benutzernamen auf dem Server übereinstimmen.

SCHRITT 4 Geben Sie den Wert für **Altes Kennwort** ein. Das Kennwort muss mit dem Kennwort auf dem Server übereinstimmen.

SCHRITT 5 Geben Sie den Wert für **Neues Kennwort** ein und bestätigen Sie das Kennwort im Feld **Kennwort bestätigen**.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Das Kennwort auf dem SSH-Server wird geändert.

20

Verwenden der SSH-Serverfunktion

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 mit dem automatisch erstellten (Standard) Schlüssel des Switch eine SSH-Sitzung im Switch aufzubauen, führen Sie die folgenden Schritte aus:*

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 der externen SSH-Clientanwendung (beispielsweise PuTTY) an. Verwenden Sie dabei die IP-Adresse des Switch (es ist nicht notwendig, einen Benutzernamen oder Schlüssel zu verwenden, der dem Gerät bekannt ist).

Workflow 2: *Um einen SSH-Benutzer zu erstellen und sich mit diesem Benutzer beim Switch anzumelden, führen Sie die folgenden Schritte aus:*

SCHRITT 1 Generieren Sie in einer externen SSH-Serveranwendung 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 Fügen Sie auf der Seite *SSH-Benutzerauthentifizierung* einen Benutzer hinzu und kopieren Sie den extern generierten öffentlichen Schlüssel an diese Stelle.

SCHRITT 4 Melden Sie sich bei der externen SSH-Clientanwendung (beispielsweise PuTTY) an. Verwenden Sie dabei die IP-Adresse des Switch und den Benutzernamen des Benutzers.

Workflow 3: *Um einen RSA- oder DSA-Schlüssel von Switch A in Switch B zu importieren, führen Sie die folgenden Schritte aus:*

SCHRITT 1 Wählen Sie in Switch A auf der Seite *SSH-Serverauthentifizierung* einen RSA- oder DSA-Schlüssel aus.

SCHRITT 2 Klicken Sie auf **Bearbeiten** und kopieren Sie den öffentlichen Schlüssel des ausgewählten Schlüssels in Editor oder eine ähnliche Anwendung.

SCHRITT 3 Melden Sie sich bei Switch 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 Switch A ein.

Seiten für die SSH-Serverkonfiguration

In diesem Abschnitt werden die zum Konfigurieren der SSH-Serverfunktion verwendeten Seiten beschrieben.

SSH-Benutzerauthentifizierung

Auf dieser Seite können Sie die SSH-Benutzerauthentifizierung durch öffentlichen Schlüssel aktivieren und 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 einen RSA- oder DSA-Schlüssel für den Benutzer generieren.

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**. Die Seite *SSH-Benutzerauthentifizierung* wird angezeigt.

SCHRITT 2 Wählen Sie die Option **Aktivieren** aus. Wenn diese Option nicht ausgewählt ist, wird keine Authentifizierung für den SSH-Clientbenutzer ausgeführt.

Für die aktuellen 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 3 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.

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**. Die Seite *SSH-Serverauthentifizierung* wird angezeigt.

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.

SCHRITT 4 Wenn neue Schlüssel generiert wurden, klicken Sie auf **Übernehmen**. Die Schlüssel werden in der aktuellen Konfigurationsdatei gespeichert.

21

Verwenden der SSL-Funktion

In diesem Abschnitt wird die SSL-Funktion (Secure Socket Layer) beschrieben.

Das Kapitel enthält die folgenden Themen:

- **SSL (Übersicht)**
- **Standardeinstellungen und Konfiguration**
- **Authentifizierungseinstellungen für SSL-Server**

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

Der Switch 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, ändern ein vorhandenes Zertifikat oder importieren ein Zertifikat:

SCHRITT 1 Klicken Sie auf **Sicherheit** > **SSL-Server** > **Authentifizierungseinstellungen für SSL-Server**. Die Seite *Authentifizierungseinstellungen für SSL-Server* wird angezeigt.

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 Sie können eine der folgenden Aktionen ausführen, indem Sie auf die entsprechende Schaltfläche klicken:

- **Bearbeiten**: Wählen Sie eines der Zertifikate aus und geben Sie Werte für die folgenden Felder ein:
  - **RSA-Schlüssel neu generieren**: Wählen Sie diese Option aus, um den RSA-Schlüssel neu zu generieren.
  - **Schlüssellänge**: Geben Sie die Länge des zu generierenden RSA-Schlüssels ein.

- **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.
- **Dauer**: Gibt die Gültigkeitsdauer eines Zertifikats in Tagen an.

▪ **Zertifikatsanforderung generieren**: Generiert eine von einer Zertifizierungsstelle zu signierende Zertifikatsanforderung.

- Geben Sie Werte für die Felder für das Zertifikat ein (wie die Felder auf der Seite **Bearbeiten**).

SCHRITT 4 Klicken Sie auf **Zertifikatsanforderung generieren**. Daraufhin wird ein Schlüssel erstellt, der in der Zertifizierungsstelle eingegeben werden muss.

▪ **Zertifikat importieren**: Geben Sie nach Erhalt der Genehmigung der Zertifizierungsstelle Folgendes ein:

- **Zertifikats-ID**: Wählen Sie das aktive Zertifikat aus.
- **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.

- **Sensible Daten verschlüsselt anzeigen**: Klicken Sie auf diese Schaltfläche, 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).

- **Details**: Zeigt das Zertifikat und das RSA-Schlüsselpaar an. 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.

SCHRITT 5 Klicken Sie auf **Übernehmen**, um die Änderungen in die aktuelle Konfiguration zu übernehmen.

22

Konfigurieren von DHCP

In diesem Abschnitt wird die Implementierung der Funktionen DHCP-Relais und -Snooping im Switch beschrieben.

Die folgenden Themen werden behandelt:

- **DHCP-Snooping**
- **DHCP-Relais**
- **Option 82**
- **Interaktionen zwischen DHCP-Snooping, DHCP-Relais und Option 82**
- **DHCP-Snooping-Bindungsdatenbank**
- **DHCP-Konfiguration**

DHCP-Snooping

DHCP-Snooping dient als Sicherheitsmechanismus, der den Empfang falscher DHCP-Antwortpakete verhindern und DHCP-Adressen protokollieren soll. Zu diesem Zweck werden Ports am Switch 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 den Switch 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*).

DHCP-Relais

DHCP-Relais leitet DHCP-Pakete an den DHCP-Server weiter.

Im Schicht-2-Systemmodus leitet der Switch DHCP-Nachrichten weiter, die er aus VLANs empfängt, in denen DHCP-Relais aktiviert ist.

Im Schicht-3-Systemmodus kann der Switch auch DHCP-Nachrichten weiterleiten, die er 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.

Option 82

Option 82 (DHCP Relais 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 im Switch zur Verfügung:

- **DHCP Insertion**: 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 der Switch kein Router ist (Schicht-2-Switch), wird daher ein externer Router benötigt.

DHCP-Nachrichten werden ausschließlich von DHCP-Relais an einen DHCP-Server weitergeleitet.

Interaktionen zwischen DHCP-Snooping, DHCP-Relais und Option 82

In der folgenden Tabelle wird das Verhalten des Switch 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.

	DHCP-Relais VLAN mit IP-Adresse		DHCP-Relais VLAN ohne IP-Adresse	
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 ursprüng-lichen 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.

	DHCP-Relais VLAN mit IP-Adresse		DHCP-Relais VLAN ohne IP-Adresse	
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.

	DHCP-Relais VLAN mit IP-Adresse		DHCP-Relais VLAN ohne IP-Adresse	
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 Switch stammt, wird das Paket ohne Option 82 gesendet. 2. Wenn die Antwort nicht vom Switch stammt, wird das Paket verworfen. Bridge: Paket wird mit der ursprüng-lichen 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 sind.

	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 ursprüng-lichen Option 82 gesendet.	Relais: Verwirft Option 82. Bridge: Paket wird ohne Option 82 gesendet.	Relais: 1. Wenn die Antwort vom Switch stammt, wird das Paket ohne Option 82 gesendet. 2. Wenn die Antwort nicht vom Switch 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.

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.

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 Switch 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

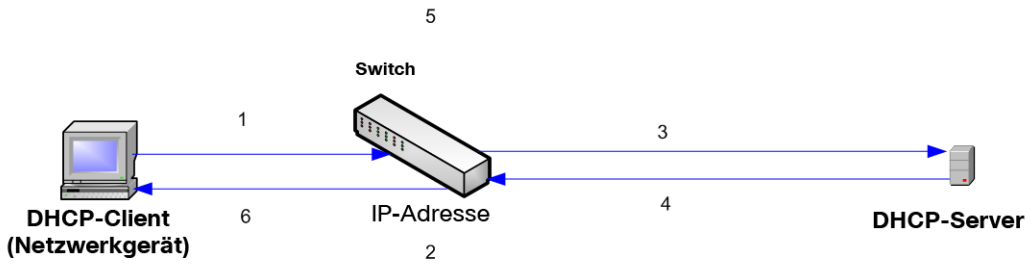
Ports können für DHCP vertrauenswürdig oder nicht vertrauenswürdig sein. Standardmäßig sind alle Ports nicht vertrauenswürdig. Zum Erstellen eines vertrauenswürdigen Ports verwenden Sie die Seite *DHCP-Snooping-Schnittstelleneinstellungen*. Pakete von diesen Ports werden automatisch weitergeleitet. Pakete 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 der Switch 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 Der Switch sendet DHCPDISCOVER, um eine IP-Adresse anzufordern, oder DHCPREQUEST, um eine IP-Adresse und Lease zu akzeptieren.

SCHRITT 2 Der Switch untersucht das Paket und fügt die IP-MAC-Informationen der DHCP-Snooping-Bindungsdatenbank hinzu.

SCHRITT 3 Der Switch 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 Der Switch untersucht das Paket. Wenn in der DHCP-Snooping-Bindungstabelle ein dem Paket entsprechender Eintrag vorhanden ist, ersetzt der Switch diesen bei Erhalt von DHCPACK durch eine IP-MAC-Bindung.

SCHRITT 6 Der Switch 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-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 und 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-Konfiguration

In diesem Abschnitt wird die Implementierung der Funktionen DHCP-Relais und DHCP-Snooping über die webbasierte Benutzeroberfläche beschrieben.

Definieren von DHCP-Eigenschaften

So konfigurieren Sie DHCP-Relais, DHCP-Snooping und Option 82:

SCHRITT 1 Klicken Sie auf **IP-Konfiguration** > **DHCP > Eigenschaften** oder **Sicherheit** > **DHCP-Snooping > Eigenschaften**. Die Seite *Eigenschaften* wird angezeigt.

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 Flash-Speicher 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**. Die Seite *DHCP-Server hinzufügen* wird angezeigt.

SCHRITT 4 Geben Sie die IP-Adresse des DHCP-Servers ein und klicken Sie auf **Übernehmen**. Die Einstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Definieren von DHCP 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** > **DHCP > Schnittstelleneinstellungen**. Die Seite *Schnittstelleneinstellungen* wird angezeigt.

SCHRITT 2 Zum Aktivieren von DHCP-Relais oder DHCP-Snooping an einer Schnittstelle klicken Sie auf **Hinzufügen**.

SCHRITT 3 Wählen Sie die Schnittstelle und die zu aktivierenden Funktionen aus.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Einstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Definieren von DHCP-Snooping-Schnittstelleneinstellungen

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** > **DHCP > Vertrauenswürdige DHCP-Snooping-Schnittstellen**. Die Seite *Vertrauenswürdige DHCP-Snooping-Schnittstellen* wird angezeigt.

SCHRITT 2 Wählen Sie die Schnittstelle aus und klicken Sie auf **Bearbeiten**. Die Seite *Schnittstelleneinstellungen bearbeiten* wird angezeigt.

SCHRITT 3 Wählen Sie **Vertrauenswürdige Schnittstelle** (**Ja** oder **Nein**) aus und klicken Sie auf **Übernehmen**, um die Einstellungen in der aktuellen Konfigurationsdatei zu speichern.

Definieren der 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:

- Der Switch 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 > DHCP > DHCP-Snooping-Bindungsdatenbank**. Die Seite *DHCP-Snooping-Bindungsdatenbank* wird angezeigt.

Um eine Teilmenge der Einträge in der DHCP-Snooping-Bindungsdatenbank anzuzeigen, geben Sie die entsprechenden Suchkriterien ein und klicken Sie auf **Los**.

SCHRITT 2 Zum Hinzufügen eines Eintrags klicken Sie auf **Hinzufügen**. Die Seite *DHCP-Snooping-Eintrag hinzufügen* wird angezeigt.

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.

23

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 **Konfigurieren von QoS – Allgemein**.

ACLs ermöglichen es Netzwerkmanagern, Muster (Filter und Aktionen) für den eingehenden Datenverkehr zu definieren. Paketen, die am Switch über einen Port oder eine LAG mit einer aktiven ACL eingehen, wird der Eingang entweder gewährt oder verweigert.

Der Abschnitt enthält die folgenden Themen:

- **Zugriffssteuerungslisten**
- **Definieren MAC-basierter ACLs**
- **IPv4-basierte ACLs**
- **IPv6-basierte ACLs**
- **Definieren einer 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.

Der Switch 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 zuzulassen, der direkt an den Switch selbst gerichtet ist, einschließlich Verwaltungsdatenverkehr wie z. B. Telnet, HTTP oder SNMP. 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 mit Bindung an eine ACL aktiviert ist, fügen Sie der ACL ACE-Filter zum Weiterleiten der IGMP-/MLD-Pakete an den Switch 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 einem Port mehrere ACLs zuzuordnen, müssen Sie eine Richtlinie mit mindestens einer Klassenzuordnung verwenden (siehe **Konfigurieren einer Richtlinie** *in* **Erweiterter QoS-Modus**).

Sie können die folgenden Arten von ACLs definieren (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 "Flow" mit dem Namen dieser ACL definiert. Bei der erweiterten QoS kann der Flow-Name verwendet werden, um auf diese Frames zu verweisen, und auf diese Frames kann QoS angewendet werden (siehe **Erweiterter QoS-Modus**).

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-basiertes ACE*
   c. IPv6-basierte ACL auf den Seiten *IPv6-basierte ACL* und *IPv6-basiertes ACE*
2. Auf der Seite *ACL-Bindung* können Sie der 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 nicht zu einer Klassenzuordnung des erweiterten QoS-Modus gehört, 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 den Unterabschnitten dieses Abschnitts geändert werden.

Definieren MAC-basierter 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 definieren Sie auf der Seite *MAC-basiertes ACE*.

So definieren Sie eine MAC-basierte ACL:

SCHRITT 1 Klicken Sie auf **Zugriffssteuerung** > **MAC-basierte ACL**. Die Seite *MAC-basierte ACL* wird angezeigt.

Auf dieser Seite wird eine Liste aller zurzeit definierten MAC-basierten ACLs angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *MAC-basierte ACL hinzufügen* wird angezeigt.

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 geschrieben.

Hinzufügen von Regeln zu einer MAC-basierten ACL

So fügen Sie einer ACL Regeln (ACEs) hinzu:

SCHRITT 1 Klicken Sie auf **Zugriffssteuerung** > **MAC-basiertes ACE**. Die Seite *MAC-basiertes ACE* wird angezeigt.

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**. Die Seite *MAC-basiertes ACE hinzufügen* wird angezeigt.

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 *Porteinstellungen* wieder aktiviert werden.
- **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 **Zeitbereich**.
- **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**. Der MAC-basierte ACE wird in die aktuelle Konfigurationsdatei geschrieben.

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 (siehe **Erweiterter QoS-Modus**).

Auf der Seite *IPv4-basierte ACL* können Sie dem System ACLs hinzufügen. Die Regeln definieren Sie auf der Seite *IPv4-basiertes ACE*.

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**. Die Seite *IPv4-basierte ACL* wird angezeigt.

Auf dieser Seite werden alle zurzeit definierten IPv4-basierten ACLs angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *IPv4-basierte ACL hinzufügen* wird angezeigt.

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 geschrieben.

Hinzufügen von Regeln (ACEs) zu einer IPv4-basierten ACL

So fügen Sie einer IPv4-basierten ACL Regeln (ACEs) hinzu:

SCHRITT 1 Klicken Sie auf **Zugriffssteuerung** > **IPv4-basiertes ACE**. Die Seite *IPv4-basiertes ACE* wird 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**. Die Seite *IPv4-basiertes ACE hinzufügen* wird angezeigt.

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.
  - *Shutdown*: Drop-Paket, das die ACE-Kriterien erfüllt und den Port deaktiviert, an den das Paket adressiert war. Ports können von der Seite *Port-Verwaltung* aus wieder aktiviert werden.
- **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 **Zeitbereich**.
- **Protokoll**: Sie können ein ACE auf der Grundlage entweder 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:
  - *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*: 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**. Der IPv4-basierte ACE wird in die aktuelle Konfigurationsdatei geschrieben.

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 (siehe **Erweiterter QoS-Modus**).

Definieren einer IPv6-basierten ACL

So definieren Sie eine IPv6-basierte ACL:

SCHRITT 1 Klicken Sie auf **Zugriffssteuerung** > **IPv6-basierte ACL**. Die Seite *IPv6-basierte ACL* wird angezeigt.

In diesem Fenster werden die Liste definierter ACLs und deren Inhalt angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *IPv6-basierte ACL hinzufügen* wird angezeigt.

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 geschrieben.

Hinzufügen von Regeln (ACEs) für eine IPv6-basierte ACL

SCHRITT 1 Klicken Sie auf **Zugriffssteuerung** > **IPv6-basiertes ACE**. Die Seite *IPv6-basiertes ACE* wird angezeigt.

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**. Die Seite *IPv6-basiertes ACE hinzufügen* wird angezeigt.

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 von der Seite *Port-Verwaltung* aus wieder aktiviert werden.
- **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 **Zeitbereich** 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*: 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 eine 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**.

Definieren einer ACL-Bindung

Wenn eine ACL an eine Schnittstelle gebunden ist, 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 Sie können einen Port an eine Richtlinie oder an eine ACL binden, jedoch nicht an beide.

So binden Sie eine ACL an eine Schnittstelle:

SCHRITT 1 Klicken Sie auf **Zugriffssteuerung** > **ACL-Bindung**. Die Seite *ACL-Bindung* wird angezeigt.

SCHRITT 2 Wählen Sie einen Schnittstellentyp aus: **Ports/LAGs** (Port oder LAG).

SCHRITT 3 Klicken Sie auf **Los**. Die Liste der Ports/LAGs wird angezeigt. Für jeden ausgewählten Schnittstellentyp werden alle Schnittstellen dieses Typs mit einer Liste ihrer aktuellen ACLs angezeigt:

- **Schnittstelle**: Kennung der Schnittstelle.
- **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).

  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**. Die Seite *ACL-Bindung bearbeiten* wird angezeigt.

SCHRITT 5 Wählen Sie die **Schnittstelle** aus, an die die ACLs gebunden werden sollen.

SCHRITT 6 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.
- **Alle zulassen**: Wählen Sie eine der folgenden Optionen aus:

- *Deaktivieren (alle verweigern)*: Wenn das Paket nicht einer ACL entspricht, wird es verweigert (gelöscht).
- *Aktivieren*: Wenn das Paket nicht einer ACL entspricht, wird es zugelassen (weitergeleitet).

HINWEIS "Alle zulassen" können Sie nur definieren, wenn IP Source Guard für die Schnittstelle nicht aktiviert ist.

SCHRITT 7 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/waren.

24

Konfigurieren der 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.
- **Sonstiges Attribut für die Bearbeitung von Datenverkehrsklassen**: Wendet QoS-Mechanismen auf verschiedene Klassen an, einschließlich der Bandbreitenverwaltung.

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 in Schicht 3 um den DSCP-

Wert (Differentiated Service Code Point) für IPv4 oder den TC-Wert (Traffic Class, Datenverkehrsklasse) für IPv6 handeln. Beim Betrieb im Basismodus vertraut der Switch diesem extern zugewiesenen QoS-Wert. Der extern zugewiesene QoS-Wert eines Pakets bestimmt dessen Datenverkehrsklasse und QoS.

Das Header-Feld, dem vertraut werden soll, geben Sie auf der Seite *Globale Einstellungen* ein. 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 folgende Aktionen durch:

SCHRITT 1 Wählen Sie auf der Seite *QoS-Eigenschaften* den QoS-Modus ("Basismodus", "Erweiterter Modus" oder "Deaktiviert" wie im Abschnitt **QoS-Modi** beschrieben) für das System aus. 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 der Switch 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 der Switch im CoS/802.1-Vertrauensmodus betrieben wird, werden alle eingehenden Pakete entsprechend ihrer CoS/802.1p-Priorität in die zugehörigen Ausgangswarteschlangen eingereiht. Hierzu verwenden Sie 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.

c. Legen Sie auf der Seite *VLAN-Eingangsratenbegrenzung* die VLAN-Eingangsratenbegrenzung 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**. Die Seite *QoS-Eigenschaften* wird angezeigt.

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 nur falls das System im Basismodus betrieben wird und die Option *CoS vertrauen* auf der Seite *Globale Einstellungen* ausgewählt wurde.

Wählen Sie **Standards wiederherstellen** aus, um die standardmäßige CoS-Werkseinstellung für diese Schnittstelle wiederherzustellen.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die aktuelle Konfigurationsdatei wird aktualisiert.

Zum Festlegen von QoS für eine Schnittstelle wählen Sie diese aus und klicken Sie auf **Bearbeiten**. Die Seite *Schnittstellen-CoS-Konfiguration bearbeiten* wird angezeigt.

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). Die Werte "0" bis "7" sind möglich.

SCHRITT 2 Klicken Sie auf **Übernehmen**. Der CoS-Standardwert für die Schnittstelle wird in die aktuelle Konfigurationsdatei geschrieben.

Konfigurieren von QoS-Warteschlangen

Der Switch unterstützt vier Warteschlangen für jede Schnittstelle. Die Warteschlange Nummer vier 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 alle vier Warteschlangen im WRR-Modus betrieben werden und 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 Sie auf der Seite *Warteschlange* auswählen. Wenn als Warteschlangenmodus die strikte Priorität verwendet wird, werden die Warteschlangen gemäß der Priorität bedient. Dabei wird zunächst Warteschlange 4 (die Warteschlange mit der höchsten Priorität) bearbeitet und sobald diese abgeschlossen wurde, kommt die nächstniedrigere Warteschlange an die Reihe.

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**. Die Seite *Warteschlange* wird angezeigt.

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.

Standardzuordnungswarteschlangen

802.1p-Werte (0 - 7, wobei 7 der höchste Wert ist)	Warteschlange (Warteschlangen 1 - 4, wobei 4 die höchste Priorität hat)	Warteschlange (2 Warteschlangen: "Normal" und "Hoch")	Hinweise
0	1	Normal	Hintergrund
1	1	Normal	Beste Leistung
2	2	Normal	Ausgezeichnete Leistung
3	3	Normal	Wichtige Anwendung LVS-Telefon mit SIP

802.1p-Werte (0 - 7, wobei 7 der höchste Wert ist)	Warteschlange (Warteschlangen 1 - 4, wobei 4 die höchste Priorität hat)	Warteschlange (2 Warteschlangen: "Normal" und "Hoch")	Hinweise
4	3	Normal	Video
5	4	Hoch	Voice Cisco IP-Telefonstandard
6	4	Hoch	Interwork-Steuerelement LVS-Telefon mit RTP
7	4	Hoch	Netzwerk-Steuerelement

Durch das Ändern der Zuordnung unter "CoS/802.1p zu Warteschlange" sowie der Warteschlangenplanungsmethode und der Bandbreitenzuweisung kann in einem Netzwerk die gewünschte Servicequalität erreicht werden.

Die Zuordnung "CoS/802.1p zu Warteschlange" gilt nur, falls eine der folgenden Bedingungen erfüllt ist:

- Der Switch wird im QoS-Basismodus und CoS/802.1p-Vertrauensmodus betrieben.
- Der Switch 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 die höchste Priorität.

So ordnen Sie CoS-Werte Ausgangswarteschlangen zu:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Allgemein** > **CoS/802.1p zu Warteschlange**. Die Seite *CoS/802.1p zu Warteschlange* wird angezeigt.

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 vier Ausgangswarteschlangen unterstützt, wobei Warteschlange 4 die höchste Priorität besitzt und Warteschlange 1 die niedrigste Priorität.

SCHRITT 3 Wählen Sie für jede 802.1p-Priorität die Ausgabewarteschlange aus, der die Priorität zugeordnet werden soll.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die 802.1p-Prioritätswerte werden den Warteschlangen zugeordnet und die aktuelle Konfigurationsdatei wird aktualisiert.

Zuordnen von DSCP zu Warteschlange

Auf der Seite *DSCP zu Warteschlange* (IP Differentiated Services Code Point) können Sie DSCP 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 gilt für IP-Pakete, falls Folgendes zutrifft:

- Der Switch wird im QoS-Basismodus und DSCP-Vertrauensmodus betrieben.
- Der Switch 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.

So ordnen Sie DSCP Warteschlangen zu:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Allgemein** > **DSCP zu Warteschlange**. Die Seite *DSCP zu Warteschlange* wird angezeigt.

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 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) legt fest, welche durchschnittliche Datenmenge (gemessen in Bit/s) höchstens über die Ausgangsschnittstelle gesendet werden darf.
- Die CBS (Committed Burst Size) bestimmt, wie hoch die Datenspitzen der gesendeten Daten höchstens sein dürfen. 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**. Die Seite *Bandbreite* wird angezeigt.

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**. Die Seite *Bandbreite bearbeiten* wird angezeigt.

SCHRITT 3 Wählen Sie die **Port- oder LAG-** Schnittstelle aus.

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.

- **Ausgangskontrollrate**: Wählen Sie diese Option aus, um die Ausgangskontrollrate für die Schnittstelle zu aktivieren.
- **Committed Information Rate (CIR)**: Geben Sie die zulässige Höchstbandbreite für die Ausgangsschnittstelle ein.
- **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.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die Bandbreiteneinstellungen werden in die aktuelle Konfigurationsdatei geschrieben.

Konfigurieren der Ausgangskontrolle auf Warteschlangen-Ebene

Zusätzlich zur Begrenzung der Übertragungsrate pro Port, die Sie auf der Seite *Bandbreite* vornehmen, kann durch den Switch auch die Übertragungsrate ausgewählter ausgehender Frames auf Warteschlangen- und Portebene begrenzt werden. Die Ausgangsratenbegrenzung wird durch die Kontrolle der Ausgabelast erreicht.

Durch den Switch 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**. Die Seite *Ausgangskontrolle pro Warteschlange* wird angezeigt.

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**. Die Liste der Ports/LAGs wird angezeigt.

SCHRITT 3 Wählen Sie einen Port oder eine LAG aus und klicken Sie auf **Bearbeiten**. Die Seite *Ausgangskontrolle pro Warteschlange bearbeiten* wird angezeigt.

Diese Seite ermöglicht die Ausgangskontrolle für bis zu vier 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.

Konfigurieren der VLAN-Ratenbegrenzung

HINWEIS Die Funktion für die VLAN-Ratenbegrenzung ist nicht verfügbar, wenn der Switch im Schicht-3-Modus 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 Switch 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.

So definieren Sie die VLAN-Eingangsratenbegrenzung:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Allgemein** > **VLAN-Eingangsratenbegrenzung**. Die Seite *VLAN-Eingangsratenbegrenzung* wird angezeigt.

Auf dieser Seite wird die Tabelle für VLAN-Eingangsratenbegrenzung angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *VLAN-Eingangsratenbegrenzung hinzufügen* wird angezeigt.

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-Überlastungsvermeidung

Auf der Seite *TCP-Überlastungsvermeidung* können Sie einen Algorithmus für die TCP-Überlastungsvermeidung aktivieren. Wenn verschiedene Quellen Pakete mit derselben Byteanzahl senden und dadurch ein Datenstau entsteht, sorgt der Algorithmus bei den Knoten mit Datenstau 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**. Die Seite *TCP-Überlastungsvermeidung* wird angezeigt.

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. Der Switch 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 den Switch (siehe im Folgenden das Feld *Vertrauensmodus*). 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**. Die Seite *Globale Einstellungen* wird angezeigt.

SCHRITT 2 Wählen Sie den **Vertrauensmodus** aus, während sich der Switch 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 der Switch 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. Die Seite *DSCP-Überschreibungstabelle* wird angezeigt.

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 Switch 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**. Die Seite *Schnittstelleneinstellungen* wird angezeigt.

SCHRITT 2 Wählen Sie **Port** oder **LAG** aus, um die Liste der Ports bzw. LAGs anzuzeigen.

Die Liste der Ports/LAGs wird angezeigt. Unter **QoS-Status** wird angezeigt, ob QoS für die Schnittstelle aktiviert ist.

SCHRITT 3 Wählen Sie eine Schnittstelle aus, und klicken Sie auf **Bearbeiten**. Die Seite *QoS-Schnittstelleneinstellungen bearbeiten* wird angezeigt.

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 Switch 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 Einzel-Überwachungsvorrichtung und die Aggregat-Überwachungsvorrichtung. Jede Überwachungsvorrichtung wird mit einer QoS-Spezifikation konfiguriert. Bei einer Einzel-Überwachungsvorrichtung wird basierend auf deren QoS-Spezifikation die QoS auf eine einzelne Klassenzuordnung und somit auf einen einzelnen Datenfluss angewendet. Bei einer Aggregat-Überwachungsvorrichtung wird die QoS auf eine oder mehrere Klassenzuordnungen angewendet und somit auf einen oder mehrere Datenflüsse. Eine Aggregat-Überwachungsvorrichtung 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 Einzel-Überwachungsvorrichtung und die Aggregat-Überwachungsvorrichtung sind verfügbar, wenn der Switch 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 Einzel-Überwachungsvorrichtung an mehrere Ports gebunden wird, besitzt jeder Port seine eigene Instanz der Einzel-Überwachungsvorrichtung; jede dieser Vorrichtungen wendet die QoS auf die Klassenzuordnung (den Klassenzuordnungsdatenfluss) bei dem jeweiligen Port an, unabhängig von den anderen Ports.
- Eine Aggregat-Überwachungsvorrichtung 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 die internen DSCP-Werte sich 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 unter *Erstellen von ACL-Workflows* 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 *Richtlinienklassenzuordnung* 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.
   - **Einzel-Überwachungsvorrichtung**: Erstellen Sie eine Richtlinie, durch die einer Klassenzuordnung eine Einzel-Überwachungsvorrichtung zugewiesen wird. Verwenden Sie dazu die Seiten *Richtlinientabelle* und *Klassenzuordnung*. Definieren Sie innerhalb der Richtlinie die Einzel-Überwachungsvorrichtung.

- **Aggregat-Überwachungsvorrichtung**: Erstellen Sie auf der Seite *Aggregat-Überwachungsvorrichtung* für jeden Datenfluss eine QoS-Aktion, durch die alle übereinstimmenden Frames an dieselbe Überwachungsvorrichtung (Aggregat-Überwachungsvorrichtung) gesendet werden. Erstellen Sie auf der Seite *Richtlinientabelle* eine Richtlinie, durch die einer Klassenzuordnung die Aggregat-Überwachungsvorrichtung zugewiesen wird.

5. Binden Sie auf der Seite *Richtlinienbindung* die Richtlinie an eine Schnittstelle.

Konfigurieren der globalen Einstellungen

Die Seite *Globale Einstellungen* enthält Informationen zum Aktivieren der Vertrauensfunktion für den Switch. 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**. Die Seite *Globale Einstellungen* wird angezeigt.

SCHRITT 2 Wählen Sie den **Vertrauensmodus** aus, während sich der Switch 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 für die Priorisierung des an der Schnittstelle eingehenden Verkehrs die für die Schnittstelle konfigurierten CoS-Standardwerte verwendet. 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 der Switch 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 *DSCP-Überschreibungstabelle*.

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 der Switch den ursprünglichen DSCP-Wert der profilexternen IP-Pakete basierend auf der Tabelle "Profilexterne DSCP-Zuordnung" durch einen neuen Wert. Anhand der neuen Werte weist der Switch diesen Paketen Ressourcen und die Ausgangswarteschlange zu. Außerdem ersetzt der Switch 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**. Die Seite *Profilexterne DSCP-Zuordnung* wird angezeigt. Auf dieser Seite können Sie den DSCP-Wert für Datenverkehr ändern, der beim Switch 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.

Festlegen von Klassenzuordnungen

Eine Klassenzuordnung definiert einen Datenverkehrsfluss mithilfe von ACLs (Access Control Lists, Zugangskontrolllisten). 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**. Die Seite *Klassenzuordnung* wird angezeigt.

Auf dieser Seite werden die bereits festgelegten Klassenzuordnungen angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *Klassenzuordnung hinzufügen* wird angezeigt.

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

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.

HINWEIS QoS-Überwachungsvorrichtungen werden nicht unterstützt, wenn der Switch im Schicht-3-Systemmodus betrieben wird.

Eine Überwachungsvorrichtung wird mit einer QoS-Spezifikation konfiguriert. Es gibt zwei Arten von Überwachungsvorrichtungen:

- **(Reguläre) Einzel-Überwachungsvorrichtung**: Eine Einzel-Überwachungsvorrichtung wendet die QoS basierend auf der QoS-Spezifikation der Überwachungsvorrichtung auf eine einzige Klassenzuordnung und einen einzigen Datenfluss an. Wenn eine Klassenzuordnung mit Einzel-Überwachungsvorrichtung an mehrere Ports gebunden wird, besitzt jeder Port seine eigene Instanz der Einzel-Überwachungsvorrichtung; jede dieser Vorrichtungen wendet die QoS auf die Klassenzuordnung (den Klassenzuordnungsdatenfluss) bei dem jeweiligen Port an, unabhängig von den anderen Ports. Eine Einzel-Überwachungsvorrichtung können Sie auf der Seite *Richtlinientabelle* erstellen.

- **Aggregat-Überwachungsvorrichtung**: Bei einer Aggregat-Überwachungsvorrichtung wird die QoS auf eine oder mehrere Klassenzuordnungen angewendet und somit auf einen oder mehrere Datenflüsse. Eine Aggregat-Überwachungsvorrichtung kann Klassenzuordnungen von verschiedenen Richtlinien unterstützen. Eine Aggregat-Überwachungsvorrichtung wendet die QoS aggregiert auf alle zugehörigen Datenflüsse an, unabhängig von Richtlinien und Ports. Eine Aggregat-Überwachungsvorrichtung können Sie auf der Seite *Aggregat-Überwachungsvorrichtung* erstellen.

  Eine Aggregat-Überwachungsvorrichtung 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 Aggregat-Überwachungsvorrichtung handelt, müssen Sie diese auf der Seite *Aggregat-Überwachungsvorrichtung* erstellen.

Definieren von Aggregat-Überwachungsvorrichtung

Bei einer Aggregat-Überwachungsvorrichtung wird die QoS auf eine oder mehrere Klassenzuordnungen angewendet und somit auf einen oder mehrere Datenflüsse. Eine Aggregat-Überwachungsvorrichtung kann Klassenzuordnungen von verschiedenen Richtlinien unterstützen und wendet die QoS unabhängig von Richtlinien und Ports aggregiert auf alle zugehörigen Datenflüsse an.

HINWEIS Der Switch unterstützt Aggregat-Überwachungsvorrichtungen und Einzel-Überwachungsvorrichtungen nur dann, wenn er im Schicht-2-Modus betrieben wird.

So legen Sie eine Aggregat-Überwachungsvorrichtung fest:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **Erweiterter QoS-Modus** > **Aggregat-Überwachungsvorrichtung**. Die Seite *Aggregat-Überwachungsvorrichtung* wird angezeigt.

Auf dieser Seite werden die vorhandenen Aggregat-Überwachungsvorrichtung angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *Aggregat-Überwachungsvorrichtung. hinzufügen* wird angezeigt.

SCHRITT 3 Geben Sie die Parameter ein.

- **Name der Aggregat-Überwachungsvorrichtung**: Geben Sie den Namen der Aggregat-Überwachungsvorrichtung 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 *Richtlinienklassenzuordnung* wird die Liste der erweiterten QoS-Richtlinien angezeigt, die im System definiert 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 Aggregat-Überwachungsvorrichtungen, 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**. Die Seite *Richtlinientabelle* wird angezeigt.

Auf dieser Seite werden die definierten Richtlinien angezeigt.

SCHRITT 2 Klicken Sie auf **Tab. für Richtlinienklassenzuordnungen**, um die Seite *Richtlinienklassenzuordnungen* 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.

Richtlinienklassenzuordnungen

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 der Switch im Schicht-3-Modus betrieben wird. Der Switch 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** > **Richtlinienklassenzuordnungen**. Die Seite *Richtlinienklassenzuordnungen* wird angezeigt.

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**. Die Seite *Richtlinienklassenzuordnung hinzufügen* wird angezeigt.

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 der Switch dem CoS/802.1p- und DSCP-Wert des übereinstimmenden Pakets. Im Fall von IP-Paketen leitet der Switch 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.

    Andernfalls verwenden Sie den neuen Wert ("0" bis "4") 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 Einzel-Überwachungsvorrichtung für die Richtlinie verwendet.
  - *Aggregat*: Es wird eine Aggregat-Überwachungsvorrichtung für die Richtlinie verwendet.

- **Aggregat-Überwachungsvorrichtung**: Nur im Schicht-2-Systemmodus verfügbar. Wenn der **Richtlinientyp** auf *Aggregat* festgelegt ist, wählen Sie eine zuvor (auf der Seite *Aggregat-Überwachungsvorrichtung*) definierte Aggregat-Überwachungsvorrichtung 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**. Die Seite *Richtlinienbindung* wird angezeigt.

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.

Verwalten der QoS-Statistik

Auf diesen Seiten können Sie die Einzel-Überwachungsvorrichtung und die Aggregat-Überwachungsvorrichtung verwalten und Warteschlangenstatistiken anzeigen.

Überwachungsvorrichtungsstatistik

Eine Einzel-Überwachungsvorrichtung wird an eine Klassenzuordnung einer einzigen Richtlinie gebunden. Eine Aggregat-Überwachungsvorrichtung wird an eine oder mehrere Klassenzuordnungen einer oder mehrerer Richtlinien gebunden.

Anzeigen der Statistik für Einzel-Überwachungsvorrichtungen

Auf der Seite *Statistik für Einzel-Überwachungsvorrichtung* 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 der Switch 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 Einzel-Überwachungsvorrichtung**. Die Seite *Statistik für Einzel-Überwachungsvorrichtung* wird angezeigt.

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**. Die Seite *Statistik für Einzel-Überwachungsvorrichtung hinzufügen* wird angezeigt.

SCHRITT 3 Geben Sie die Parameter ein.

- **Schnittstelle**: Wählen Sie die Schnittstelle aus, für die statistische Daten gesammelt werden.
- **Richtliniennname**: 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 Aggregat-Überwachungsvorrichtungen an:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **QoS-Statistik** > **Statistik für Aggregat-Überwachungsvorrichtung**. Die Seite *Statistik für Aggregat-Überwachungsvorrichtung* wird angezeigt.

Auf dieser Seite werden folgende Felder angezeigt:

- **Name der Aggregat-Überwachungsvorrichtung**: 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**. Die Seite *Statistik für Aggregat-Überwachungsvorrichtung hinzuf.* wird angezeigt.

SCHRITT 3 Wählen Sie unter **Name der Aggregat-Überwachungsvorrichtung** einen Namen aus (eine der zuvor erstellten Aggregat-Überwachungsvorrichtung), 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 weitergeleitetete und gelöschte Pakete. Die Daten sind nach Schnittstelle, Warteschlange und Löschpriorität geordnet.

HINWEIS Die QoS-Statistik wird nur angezeigt, wenn der Switch im erweiterten QoS-Modus betrieben wird. Diese Änderung können Sie unter **Allgemein** > **QoS-Eigenschaften** vornehmen.

So zeigen Sie die Warteschlangenstatistik an:

SCHRITT 1 Klicken Sie auf **Quality of Service** > **QoS-Statistik** > **Warteschlangenstatistik**. Die Seite *Warteschlangenstatistik* wird angezeigt.

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**. Die Seite *Warteschlangenstatistik hinzufügen* wird angezeigt.

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:
  - *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.

25

Konfigurieren von SNMP

In diesem Abschnitt wird die SNMP-Funktion (Simple Network Management Protocol) beschrieben, mit der Sie Netzwerkgeräte verwalten können.

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**
- **Festlegen von SNMP-Communitys**
- **Festlegen von Trap-Einstellungen**
- **Benachrichtigungsempfänger**
- **SNMP-Benachrichtigungsfilter**

SNMP-Versionen und -Workflow

Der Switch 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 Switch 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. Der Switch 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 den Switch 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 definieren Sie auf der Seite *Ansichten*.)
- **Erweiterter Modus**: Die Zugriffsrechte einer Community werden durch eine Gruppe definiert (Gruppen definieren Sie auf der Seite *Gruppen*). 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 (*Objekt-IDs*) von Switches lauten wie folgt: :

Modellname	Beschreibung	Objekt-ID
<Variable>SG300-10	8 GE-Ports und 2 Kombinationsports für Sonderzwecke (GE/SFP)	9.6.1.83.10.1
SG300-10MP	8 GE-Ports und 2 Kombinationsports für Sonderzwecke (GE/SFP)	9.6.1.83.10.3
SG300-10P	8 GE-Ports und 2 Kombinationsports für Sonderzwecke (GE/SFP)	9.6.1.83.10.2

Modellname	Beschreibung	Objekt-ID
SG300-20	16 GE-Ports und 4 Ports für Sonderzwecke - 2 Uplinks und 2 Kombinationsports	9.6.1.83.20.1
SG300-28	24 GE-Ports und 4 Ports für Sonderzwecke - 2 Uplinks und 2 Kombinationsports	9.6.1.83.28.1
SG300-28P	24 GE-Ports und 4 Ports für Sonderzwecke - 2 Uplinks und 2 Kombinationsports	9.6.1.83.28.2
SG300-52	48 GE-Ports und 4 Ports für Sonderzwecke - 2 Uplinks und 2 Kombinationsports	9.6.1.83.52.1
SF300-08	8 FE-Ports	9.6.1.82.08.4
SF302-08	8 FE-Ports und 2 GE-Ports	9.6.1.82.08.1
SF302-08MP	8 FE-Ports und 2 GE-Ports	9.6.1.82.08.3
SF302-08P	8 FE-Ports und 2 GE-Ports	9.6.1.82.08.2
SF300-24	24 FE-Ports und 4 GE-Ports für Sonderzwecke - 2 Uplinks und 2 Kombinationsports	9.6.1.82.24.1
SF300-24P	24 FE-Ports und 4 GE-Ports für Sonderzwecke - 2 Uplinks und 2 Kombinationsports	9.6.1.82.24.2
SF300-48	48 FE-Ports und 4 GE-Ports für Sonderzwecke - 2 Uplinks und 2 Kombinationsports	9.6.1.82.48.1
SF300-48P	48 FE-Ports und 4 GE-Ports für Sonderzwecke - 2 Uplinks und 2 Kombinationsports	9.6.1.82.48.2

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**. Die Seite *Engine-ID* wird angezeigt.

SCHRITT 2 Wählen Sie aus, welche ID als **Lokale Engine-ID** verwendet werden soll.

- **Standard verwenden**: Wählen Sie diese Option aus, um die vom Gerät erzeugte Engine-ID zu verwenden. Die Standard-Engine-ID basiert auf der MAC-Adresse des Switch 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 Switch.
- **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 - 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 und auf der Seite *Communitys* können Sie Ansichten einer Community im Basiszugriffsmodus zuordnen.

So definieren Sie SNMP-Ansichten:

SCHRITT 1 Klicken Sie auf **SNMP** > **Ansichten**. Die Seite *Ansichten* wird angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, um die neuen Ansichten festzulegen. Die Seite *Ansicht hinzufügen* wird angezeigt.

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 festgelegte 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**: Der Switch 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**. Die Seite *Gruppen* wird angezeigt.

Auf dieser Seite werden die vorhandenen SNMP-Gruppen und ihre Sicherheitsstufen angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *Gruppe hinzufügen* wird angezeigt.

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**: Indem Sie eine Ansicht den Lese-, Schreib- und Benachrichtigungsberechtigungen der Gruppe zuordnen, beschränken Sie den Umfang der MIB-Struktur, für die die Gruppe über Lese-, Schreib- und Benachrichtigungszugriff verfügt.

- *Anzeigen*: Wählen Sie eine zuvor definierte Ansicht für "Lesen", "Schreiben" und "Benachrichtigen" aus.
- *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 die aktuelle Konfigurationsdatei geschrieben.

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 den Switch konfiguriert sein. Hierzu verwenden Sie 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**. Die Seite *Benutzer* wird angezeigt.

Auf dieser Seite werden die vorhandenen Benutzer angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *Benutzer hinzufügen* wird angezeigt.

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 Switch verbunden.
  - *Remote IP-Adresse*: Der Benutzer ist neben dem lokalen Switch 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-Kennwort*: Ein Kennwort, das zum Generieren eines Schlüssels durch die MD5-Authentifizierungsmethode verwendet wird.
  - *SHA-Kennwort*: 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.

Festlegen 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* können Sie Communitys Zugriffsrechte zuweisen, 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 definieren Sie auf der Seite *SNMP-Ansichten*.)
- **Erweiterter Modus**: Die Zugriffsrechte einer Community werden durch eine Gruppe definiert (Gruppen definieren Sie auf der Seite *Gruppen*). 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**. Die Seite *Communitys* wird angezeigt.

Auf dieser Seite wird eine Tabelle mit den konfigurierten SNMP-Communitys und ihren Eigenschaften angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *SNMP-Community hinzufügen* wird angezeigt.

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.

Festlegen von Trap-Einstellungen

Auf der Seite *Trap-Einstellungen* können Sie konfigurieren, ob und in welchen Fällen SNMP-Benachrichtigungen vom Switch 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**. Die Seite *Trap-Einstellungen* wird angezeigt.

SCHRITT 2 Wählen Sie **Aktivieren** für **SNMP-Benachrichtigungen** aus, um anzugeben, dass der Switch 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 Switch 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 Switch 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**. Die Seite *Benachrichtigungsempfänger SNMPv1, 2* wird angezeigt.

Auf dieser Seite werden die Empfänger für SNMPv1 und SNMPv2 angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *SNMP-Benachrichtigungsempfänger hinzufügen* wird angezeigt.

SCHRITT 3 Geben Sie die Parameter ein.

- **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 an, an die 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 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 erstellen Sie auf der Seite *Benachrichtigungsfilter*.
- **Filtername**: Wählen Sie den SNMP-Filter aus, der bestimmt, welche Informationen in Traps enthalten sein sollen. (Den Filter definieren Sie auf der Seite *Benachrichtigungsfilter*.)

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Einstellungen für SNMP-Benachrichtigungsempfänger werden in die aktuelle Konfigurationsdatei geschrieben.

Festlegen von Benachrichtigungsempfängern bei SNMPv3

So legen Sie einen Empfänger in SNMPv3 fest:

SCHRITT 1 Klicken Sie auf **SNMP** > **Benachrichtigungsempfänger SNMPv3**. Die Seite *Benachrichtigungsempfänger SNMPv3* wird angezeigt.

Auf dieser Seite werden die Empfänger für SNMPv3 angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *SNMP-Benachrichtigungsempfänger hinzufügen* wird angezeigt.

SCHRITT 3 Geben Sie die Parameter ein.

- **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 an, an die 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 erstellen Sie auf der Seite *Benachrichtigungsfilter*.

▪ **Filtername**: Wählen Sie den SNMP-Filter aus, der bestimmt, welche Informationen in Traps enthalten sein sollen. (Den Filter definieren Sie auf der Seite *Benachrichtigungsfilter*.)

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* wird angezeigt.

Auf der Seite *Benachrichtigungsfilter* werden Benachrichtigungsinformationen für die einzelnen Filter angezeigt. In der Tabelle können Benachrichtigungseinträge nach dem Filternamen gefiltert werden.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Die Seite *Benachrichtigungsfilter hinzufügen* wird angezeigt.

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.