ADMINISTRATOR-HANDBUCH

Cisco Small Business

Serie SG 200 8-Port Smart Switch

Inhalt

1

Erste Schritte

In diesem Kapitel erhalten Sie eine Übersicht über das webbasierte Switch-Konfigurationsdienstprogramm. Es werden die folgenden Themen behandelt:

- **Starten des webbasierten Switch-Konfigurationsdienstprogramms**
- **Kurzanleitung für die Gerätekonfiguration**
- **Fensternavigation**

Starten des webbasierten Switch-Konfigurationsdienstprogramms

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

Für Browser gelten die folgenden Einschränkungen:

- Wenn Sie Internet Explorer 8 verwenden, öffnen Sie ein Browserfenster, und konfigurieren Sie die folgenden Einstellungen:

  Klicken Sie auf **Extras** > **Internetoptionen**, und wählen Sie die Registerkarte **Sicherheit** aus. Wählen Sie **Lokales Intranet** aus, und klicken Sie auf **Sites**. Klicken Sie auf **Erweitert** und auf **Hinzufügen**. Fügen Sie die Intranetadresse des Switch (http://*<IP-Adresse>*) der lokalen Intranetzone hinzu. Die IP-Adresse kann auch als Subnetz-IP-Adresse angegeben werden, sodass alle Adressen im Subnetz der lokalen Intranetzone hinzugefügt werden.

- Wenn Sie Internet Explorer 6 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 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 lokalen IPv6-Link-Adresse, um über den Browser auf den Switch zuzugreifen.

Starten des Dienstprogramms

So öffnen Sie das webbasierte Switch-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.

Anmelden

So melden Sie sich am webbasierte Switch-Konfigurationsdienstprogramm an:

SCHRITT 1 Geben Sie den *Benutzernamen* und das *Kennwort* ein. Der Standardbenutzername lautet **cisco**, das Standardkennwort **cisco**.

Hinweis: Wenn der Switch mit den Werkseinstellungen gestartet wird, wird das webbasierte Switch-Konfigurationsdienstprogramm in der Standardsprache angezeigt. Nach der Anmeldung können Sie über die Seite *Firmware/Sprache aktualisieren/sichern* zusätzliche Sprachen herunterladen.

SCHRITT 2 Wenn Sie sich zum ersten Mal mit dem Standardbenutzernamen (**cisco**) und dem Standardkennwort (**cisco**) anmelden oder Ihr Kennwort abgelaufen ist, wird die Seite *Administrationskennwort ändern* geöffnet. Geben Sie das neue Kennwort ein, bestätigen Sie es, klicken Sie auf **Übernehmen** und dann auf **Schließen**. Das neue Kennwort wird gespeichert.

SCHRITT 3 Klicken Sie auf **Anmeldung**.

Wenn der Anmeldeversuch erfolgreich verläuft, wird die Seite *Erste Schritte* angezeigt.

Wenn Sie einen falschen Benutzernamen oder ein falsches Kennwort eingegeben haben, wird eine Fehlermeldung angezeigt, und auf dem Bildschirm 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.

Abmelden

Standardmäßig werden Sie nach zehn Minuten ohne Aktivität automatisch abgemeldet. Anweisungen zum Ändern des standardmäßigen Timeout-Zeitraums finden Sie unter **Konfigurieren des Timeouts für Sitzungsleerlauf**.

Um sich abzumelden, klicken Sie in der oberen rechten Ecke einer beliebigen Seite auf **Abmelden**.

VORSICHT Wenn Sie die aktuelle Konfiguration nicht in den Startkonfigurations-Dateityp kopieren, gehen alle Änderungen seit dem letzten Speichern des Dateityps verloren, wenn der Switch neu gestartet wird. Es wird empfohlen, die aktuelle Konfiguration vor dem Abmelden als Startkonfiguration zu speichern, um alle während der aktuellen Sitzung durchgeführten Änderungen zu speichern.

Auf der linken Seite der Schaltfläche „Speichern“ weist ein rotes **X** darauf hin, dass Änderungen an der ausgeführten Konfiguration durchgeführt wurden, die Sie noch nicht im Startkonfigurations-Dateityp gespeichert haben.

Wenn Sie auf **Speichern** klicken, wird die Seite angezeigt (siehe **Herunterladen und Sichern der Konfigurations- und Protokolldateien**). Speichern Sie die aktuelle Konfiguration, indem Sie diese in den Startkonfigurations-Dateityp kopieren. Nach dem Speichervorgang werden das rote **X** und die Schaltfläche „Speichern“ nicht mehr angezeigt.

Kurzanleitung für die Gerätekonfiguration

Um die Switch-Konfiguration zu vereinfachen, bietet 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
Ersteinrichtung	Geräte-IP-Adresse ändern	*IPv4-Schnittstelle*
	VLAN erstellen	*VLAN erstellen*
	Porteinstellungen konfigurieren	*Porteinstellungen*
Gerätestatus	Systemzusammenfassung	*Systemzusammenfassung*
	Port-Statistik	*Schnittstelle*
	RMON-Statistik	*Statistik*
	Protokoll anzeigen	*RAM-Speicher*
Schnellzugriff	Gerätekennwort ändern	*Benutzerkonten*
	Gerätesoftware aktualisieren	*Firmware/Sprache aktualisieren/sichern*
	Gerätekonfiguration sichern	*Konfiguration/Protokoll herunterladen/sichern*
	QoS konfigurieren	*QoS-Eigenschaften*
	Port-Spiegelung konfigurieren	*Port-Spiegelung*

Fensternavigation

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

Anwendungsheader

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

Schaltflächen

Schaltflächenname	Beschreibung
	Die Schaltfläche für den SYSLOG-Alarmstatus (roter Kreis mit einem **X**) wird angezeigt, wenn eine neue SYSLOG-Meldung über dem kritischen Schweregrad protokolliert wird. Klicken Sie auf diese Schaltfläche, um die Seite **Status und Statistik** > **Protokoll anzeigen** > *RAM-Speicherprotokoll* zu öffnen. Nachdem Sie auf diese Seite zugegriffen haben, wird die Schaltfläche für den SYSLOG-Alarmstatus nicht mehr angezeigt.
	Links neben der Schaltfläche „Speichern“ weist ein rotes **X** darauf hin, dass Konfigurationsänderungen durchgeführt wurden, die Sie noch nicht in der Startkonfigurationsdatei gespeichert haben. Wenn Sie auf diese Schaltfläche klicken, wird die Seite *Konfiguration/Protokoll herunterladen/sichern* angezeigt. Speichern Sie die aktuelle Konfiguration, indem Sie diese in den Startkonfigurations-Dateityp kopieren. Nach dem Speichervorgang werden das rote X und die Schaltfläche „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.
Benutzer	Der Name des beim Switch angemeldeten Benutzers. Der Standardbenutzername lautet **cisco**.

Schaltflächen (Fortsetzung)

Schaltflächenname	Beschreibung
Sprachmenü	Wählen Sie eine Sprache aus, oder laden Sie eine neue Sprachdatei in das Gerät. Wenn die gewünschte Sprache im Menü angezeigt wird, wählen Sie diese aus. Wählen Sie anderenfalls **Sprache herunterladen** aus. Weitere Informationen zum Hinzufügen einer neuen Sprache finden Sie auf der Seite *Firmware/Sprache aktualisieren/ sichern*.
Abmelden	Klicken Sie auf diese Schaltfläche, um sich vom webbasierten Switch-Konfigurationsdienstprogramms abzumelden.
Info	Klicken Sie auf diese Schaltfläche, um den Switch-Typ und die Switch-Versionsnummer anzuzeigen.
Hilfe	Zeigt die Online-Hilfe an.

Andere Ressourcen

Über die folgenden Links auf der Seite *Erste Schritte* erhalten Sie weitere Informationen und Unterstützung bei der Verwendung des Switch:

- **Support**: Zeigt die Support-Webseite für Cisco Small Business Managed Switches an.
- **Foren**: Zeigt die Webseite der Cisco Small Business Support Community an.

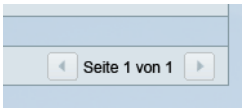
Navigationsfenster

Links auf jeder Seite befindet sich ein Navigationsfenster. Klicken Sie auf eine Kategorie der obersten Ebene, um Links zu verwandten Seiten anzuzeigen. Bei Links mit einem vorangestellten Pfeil handelt es sich um Unterkategorien, die Sie erweitern können, um die zugehörigen Seitenlinks anzuzeigen.

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
	Abhängig von der Anzahl der Seiten und der zurzeit angezeigten Seite können Sie mithilfe dieser Funktionen durch die Seiten der Tabelle navigieren. Klicken Sie auf **I<**, um zur ersten Seite zu gehen, auf **<**, um zur vorherigen Seite zu gehen, auf **>**, um zur nächsten Seite zu gehen oder auf **>I**, um zur letzten Seite zu gehen. Mithilfe der Dropdown-Liste **Seite** *<Zahl>* **von** *<Zahl>* können Sie eine bestimmte Seite auswählen.
	Wählen Sie die Anzahl der Tabelleneinträge aus, die auf jeder Seite angezeigt werden sollen.
	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**. Klicken Sie auf **Schließen**, um zur Hauptseite zurückzukehren. **Hinweis:** Ihre Änderungen werden nur auf die aktuelle Konfiguration angewendet. Wird der Switch neu gestartet, geht die aktuelle Konfiguration verloren. Klicken Sie zum Speichern der Änderungen auf **Speichern**. Weitere Informationen finden Sie unter **Kopieren und Speichern von Konfigurationsdateien**.

Verwaltungsschaltflächen (Fortsetzung)

Schaltflächenname	Beschreibung
Übernehmen	Klicken Sie auf diese Schaltfläche, um die auf der ausgewählten Seite eingegebenen Änderungen zu übernehmen. **Hinweis:** Ihre Änderungen werden nur auf die aktuelle Konfiguration angewendet. Wird der Switch neu gestartet, geht die aktuelle Konfiguration verloren. Klicken Sie zum Speichern der Änderungen auf **Speichern**. Weitere Informationen finden Sie unter **Kopieren und Speichern von Konfigurationsdateien**.
Abbrechen	Klicken Sie auf diese Schaltfläche, um die auf der Seite vorgenommenen Änderungen rückgängig zu machen und die Werte auf die vorher gültigen Einträge zurückzusetzen.
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	Klicken Sie auf diese Schaltfläche, um die Protokollmeldungen zu löschen.
Tabelle löschen	Klicken Sie auf diese Schaltfläche, um die Tabelleneinträge zu löschen.
Schließen	Klicken Sie auf diese Schaltfläche, um zur Hauptseite zurückzukehren. Wenn Sie Änderungen vorgenommen haben, die nicht in der aktuellen Konfiguration übernommen wurden, wird eine Meldung angezeigt.
Einstellungen kopieren	Eine Tabelle enthält normalerweise einen oder mehrere Einträge mit Konfigurationseinstellungen. Anstatt jeden Eintrag einzeln zu ändern, können Sie einen Eintrag ändern und diesen wie folgt in mehrere Einträge kopieren: ▪ Wählen Sie den zu kopierenden Eintrag aus. Klicken Sie auf **Einstellungen kopieren**. ▪ Geben Sie die Nummern der Zieleinträge ein. ▪ Klicken Sie auf **Übernehmen**, um die Änderungen in der aktuellen Konfiguration zu speichern. ▪ Klicken Sie auf **Schließen**, um zur Hauptseite zurückzukehren.

Verwaltungsschaltflächen (Fortsetzung)

Schaltflächenname	Beschreibung
Löschen	Wählen Sie in der Tabelle den zu löschenden Eintrag aus, und klicken Sie auf **Löschen**. Der Eintrag wird gelöscht.
Details	Klicken Sie auf diese Schaltfläche, um Informationen zu dem auf der Hauptseite ausgewählten Eintrag anzuzeigen.
Bearbeiten	Wählen Sie einen Eintrag aus und klicken Sie auf **Bearbeiten**, um den Eintrag zu bearbeiten. Die Seite *Bearbeiten* wird geöffnet, auf der Sie den Eintrag ändern können. ▪ Klicken Sie auf **Übernehmen**, um die Änderungen in der aktuellen Konfiguration zu speichern. ▪ Klicken Sie auf **Schließen**, um zur Hauptseite zurückzukehren.
Testen	Klicken Sie auf **Testen**, um die entsprechenden Tests auszuführen.
Filter löschen	Klicken Sie auf **Filter löschen**, um die Daten auf der Seite wieder gemäß den Standardkriterien anzuzeigen.
Los	Klicken Sie auf **Los**, um die auf einer Seite angezeigten Daten nach den ausgewählten Kriterien zu filtern.
Sortierschaltflächen	Wenn unter eine Tabelle die Meldung *Diese Tabelle ist sortierbar* angezeigt wird, können die einzelnen Spaltenüberschriften als Sortierschaltflächen verwendet werden. Klicken Sie auf eine Spaltenüberschrift, um die Datensätze in aufsteigender Reihenfolge nach dem Inhalt der ausgewählten Spalte zu sortieren. Nach der Anwendung der Sortierung wird in der Spaltenüberschrift ein Pfeil angezeigt. Sie können auf diesen Pfeil klicken, um die Sortierreihenfolge umzukehren.

2

Anzeigen von Statistiken

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

Das Kapitel enthält die folgenden Themen:

Systemzusammenfassung

Auf der Seite *Systemzusammenfassung* werden grundlegende Informationen angezeigt, beispielsweise eine Beschreibung des Hardwaremodells, die Softwareversion und die Systembetriebszeit.

Anzeigen der Systemzusammenfassung

Um Systeminformationen anzuzeigen, klicken Sie im Navigationsfenster auf **Status und Statistik** > **Systemzusammenfassung**. Alternativ können Sie auf der Seite *Erste Schritte* unter **Gerätestatus** auf **Systemzusammenfassung** klicken.

Auf der Seite *Systemzusammenfassung* werden die folgenden Informationen angezeigt:

- **Systembeschreibung**: Eine Beschreibung des Systems.

- **Systemstandort**: Physischer Standort des Switch. Klicken Sie auf **Bearbeiten**, um die Seite *Systemeinstellungen* aufzurufen und diesen Wert einzugeben.
- **Systemkontakt**: Name einer Kontaktperson. Klicken Sie auf **Bearbeiten**, um die Seite *Systemeinstellungen* aufzurufen und diesen Wert einzugeben.
- **Hostname**: Name des Switch. Klicken Sie auf **Bearbeiten**, um die Seite *Systemeinstellungen* aufzurufen und diesen Wert einzugeben. Standardmäßig setzt sich der Switch-Hostname aus dem Wort *switch* und den drei am wenigsten signifikanten Byte der MAC-Adresse des Switch (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.

Hardware-Informationen und Firmware-Version:

Die folgenden Hardware- und Software-Informationen werden für den Switch angezeigt:

- **Seriennummer**: Seriennummer des Switch.
- **PID VID**: Teilenummer und Versions-ID.
- **Maximal verfügbare Leistung (W)**: (nur bei PoE-Switches) Die maximale Leistung, die vom PoE bereitgestellt werden kann.
- **Hauptleistungsaufnahme (W)**: (nur bei PoE-Switches) Die zurzeit für die mit dem Switch verbundenen PoE-Geräte bereitgestellte PoE-Leistung.
- **Firmware-Version**: Firmware-Versionsnummer des aktiven Images.
- **Firmware-MD5-Prüfsumme**: MD5-Prüfsumme des aktiven Images.
- **Boot-Version**: Version des Boot-Codes.
- **Boot-MD5-Prüfsumme**: MD5-Prüfsumme des Boot-Codes.

Außerdem können Sie in der grafischen Ansicht des Switch Einstellungen für die einzelnen Switch-Ports anzeigen. Um die Seite *Porteinstellungen* anzuzeigen, klicken Sie auf den Port.

TCP- und UDP-Services

In dieser Tabelle werden die Informationen für die einzelnen Services aufgeführt, die TCP oder UDP verwenden.

- **Servicename**: Der allgemein verwendete Name des Service, falls verfügbar (beispielsweise HTTP).
- **Typ**: Das für diesen Service verwendete Transportprotokoll (TCP oder UDP).
- **Port**: Die IANA-Port-Nummer (Internet Assigned Numbers Authority) für den Service.
- **IP-Adresse**: Gegebenenfalls die IP-Adresse eines Remote-Geräts, das mit diesem Service auf dem Switch verbunden ist.
- **Remote-Port**: Die IANA-Port-Nummer eines Remote-Geräts, das mit diesem Service kommuniziert.
- **Status**: Der Status des Service. Bei UDP werden nur Verbindungen mit dem Status „Aktiv“ in der Tabelle angezeigt. Beim Status „Aktiv“ ist eine Verbindung zwischen dem Switch und einem Client oder Server hergestellt. Die TCP-Status lauten:
  - **Mithören**: Der Dienst hört Verbindungsanforderungen mit.
  - **Aktiv**: Eine Verbindungssitzung ist hergestellt, und es werden Pakete gesendet und empfangen.
  - **Hergestellt**: Zwischen dem Switch und einem Server oder Client (abhängig von der Rolle des jeweiligen Geräts im Hinblick auf dieses Protokoll) wurde eine Verbindungssitzung hergestellt.

Sprachpakettabelle

In dieser Tabelle werden Informationen zu den im Switch verfügbaren Sprachen angezeigt. Der Administrator kann eine Sprache auswählen, wenn er sich beim Konfigurationsdienstprogramm anmeldet.

Englisch ist als Standardsprache in die Software integriert. Auf der Seite *Firmware/Sprache aktualisieren/sichern* können Sie weitere Sprachpakete herunterladen. Sprachdateien stehen auf der Cisco-Seite für Firmware-Downloads zur Verfügung.

In der Sprachpakettabelle werden folgende Informationen für die einzelnen verfügbaren Sprachen angezeigt:

- **Sprache**: Name der Sprache.
- **Gebietsschema**: Gebietsschemacode der Internet Engineering Task Force (IETF), mit dem die Sprache und das Land bzw. die Region identifiziert wird.

- **Version**: Version der Sprachdatei.
- **MD5-Prüfsumme**: 128-Bit-Hashcode, der zum Überprüfen der Dateiintegrität verwendet wird.
- **Dateityp**: Gibt einen der folgenden Werte an:
  - **Integriert**: In der Software enthaltene Standardsprache, die nicht als separate Datei heruntergeladen werden kann.
  - **Extern**: Eine Sprachdatei, die in den Switch heruntergeladen wurde und bei der Anmeldung ausgewählt werden kann.
- **Dateigröße**: Die Dateigröße in KB.
- **Standard**: **Ja** gibt an, dass die Anmeldeseite für das webbasierte Switch-Konfigurationsdienstprogramm nach jedem Neustart des Switch in dieser Sprache angezeigt wird.
- **Status**: Hier kann **Aktiv** oder **Inaktiv** angezeigt werden. Der Benutzer kann bei der Anmeldung eine Sprache auswählen. Die ausgewählte Sprache ist die aktive Sprache.

Konfigurieren von Systemeinstellungen

So konfigurieren Sie die Systemeinstellungen:

SCHRITT 1 Klicken Sie auf **Status und Statistik** > **Systemzusammenfassung**. Die Seite *Systemeinstellungen* wird geöffnet.

SCHRITT 2 Klicken Sie auf **Bearbeiten**, um die folgenden Parameter zu ändern:

- **Systemstandort**: Geben Sie den Ort ein, an dem der Switch sich physisch befindet.
- **Systemkontakt**: Geben Sie den Namen einer Kontaktperson ein.
- **Hostname**: Geben Sie den Hostnamen ein. Es sind nur Buchstaben, Ziffern und Bindestriche zulässig. Der Hostname darf nicht mit einem Bindestrich beginnen oder enden. Sonderzeichen, Satzzeichen oder Leerzeichen sind nicht zulässig (gemäß RFC1033, RFC1034 und RFC1035). Der Standard-Hostname besteht aus dem Wort *switch* gefolgt von den ersten drei Byte der MAC-Basisadresse. Ein Switch mit der MAC-Adresse 010203040506 beispielsweise hat den Standard-Hostnamen *switch010203*.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Schnittstellenstatistiken

Auf der Seite *Schnittstelle* können Sie Statistiken für empfangene und gesendete Pakete anzeigen. Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **Status und Statistik** > **Schnittstelle** oder auf der Seite *Erste Schritte* unter **Gerätestatus** auf **Portstatistik**.

Wählen Sie die Schnittstelle (Port oder LAG) aus, für die Sie Statistiken anzeigen möchten, und wählen Sie dann eine Aktualisierungsrate für die Statistiken aus. Für die ausgewählte Schnittstelle werden die folgenden Informationen angezeigt:

- **Byte insgesamt (Oktette)**: Die Gesamtanzahl der Oktette, die die ausgewählte Schnittstelle seit der letzten Aktualisierung des Switch gesendet oder empfangen hat.
- **Unicast-Pakete**: Die Gesamtanzahl der Unicast-Pakete, die die ausgewählte Schnittstelle seit der letzten Aktualisierung des Switch gesendet oder empfangen hat.
- **Multicast-Pakete**: Die Gesamtanzahl der Multicast-Pakete, die die ausgewählte Schnittstelle seit der letzten Aktualisierung des Switch gesendet oder empfangen hat.
- **Broadcast-Pakete**: Die Gesamtanzahl der Broadcast-Pakete, die die ausgewählte Schnittstelle seit der letzten Aktualisierung des Switch gesendet oder empfangen hat.
- **Pakete mit Fehlern**: Die Gesamtanzahl der Pakete mit Fehlern, die die ausgewählte Schnittstelle seit der letzten Aktualisierung des Switch gesendet oder empfangen hat.
- **STP-BPDUs**: Die Gesamtanzahl der STP-BPDUs (Spanning Tree Protocol; Bridge Protocol Data Units, Bridge-Protokoll-Dateneinheit), die die ausgewählte Schnittstelle seit der letzten Aktualisierung des Switch gesendet oder empfangen hat.
- **RSTP-BPDUs**: Die Gesamtanzahl der RSTP-BPDUs (Rapid Spanning Tree Protocol), die die ausgewählte Schnittstelle seit der letzten Aktualisierung des Switch gesendet oder empfangen hat.

So löschen Sie Statistikzähler:

- Klicken Sie auf **Schnittstellenzähler löschen**, um alle Zähler für die ausgewählte Schnittstelle auf 0 zurückzusetzen.
- Klicken Sie auf **Alle Schnittstellenzähler löschen**, um die Zähler für alle Schnittstellen auf 0 zurückzusetzen.

Etherlike-Statistik

Das System sammelt und meldet Statistiken für Ports und LAGs gemäß RFC2665.

Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **Status und Statistik** > **Etherlike**.

Wählen Sie die Schnittstelle (Port oder LAG) aus, für die Sie Statistiken anzeigen möchten, und wählen Sie dann eine Aktualisierungsrate für die Statistiken aus. Diese Statistiken wurden seit der letzten Aktualisierung der Seite kumuliert. Für die ausgewählte Schnittstelle werden die folgenden Informationen angezeigt:

- **Fehler bei Frame-Prüfsequenz**: Empfangene FCS Fehler.
- **Einzel-Kollisions-Frames**: Empfangene Fehler bei Einzel-Kollisions-Frames.
- **Verspätete Kollisionen**: Empfangene verspätete Kollisions-Frames.
- **Übermäßige Kollisionen**: Empfangene übermäßige Kollisions-Frames.
- **Mehrfach-Kollisionen**: Empfangene Mehrfach-Kollisions-Frames.
- **Zu große Pakete**: Die empfangenen Pakete waren mehr als 1518 Oktette lang (ausschließlich Frame-Bits und einschließlich FCS-Oktetten) und wiesen ansonsten die korrekte Form auf.
- **Interne MAC-Empfangsfehler**: Von der LAG oder Schnittstelle empfangene interne MAC-Fehler.
- **Ausrichtungsfehler**: Empfangene Pakete mit Ausrichtungsfehlern.
- **Empfangene Pausen-Frames**: Von der LAG oder Schnittstelle empfangene Pausen-Frames.
- **Gesendete Pausen-Frames**: Von der LAG oder Schnittstelle gesendete Pausen-Frames.

So löschen Sie Statistikzähler:

- Klicken Sie auf **Schnittstellenzähler löschen**, um alle Zähler für die ausgewählte Schnittstelle auf 0 zurückzusetzen.
- Klicken Sie auf **Alle Schnittstellenzähler löschen**, um die Zähler für alle Schnittstellen auf 0 zurückzusetzen.

802.1X EAP-Statistik

Sie können die Switch-Ports so konfigurieren, dass der Netzwerkzugriff mithilfe des IEEE 802.1X EAP-Protokolls (Extensible Authentication Protocol) gesteuert wird (siehe **802.1X**). Auf der Seite *802.1X EAP* können Sie Informationen zu den an einem Port empfangenen EAP-Paketen anzeigen.

Um die Seite *802.1X EAP* anzuzeigen, klicken Sie im Navigationsfenster auf **Status und Statistik** > **802.1X EAP**.

SCHRITT 1 Wählen Sie den **Port** aus, für den Sie Statistiken anzeigen möchten.

SCHRITT 2 Wählen Sie eine **Aktualisierungsrate** für die Statistiken aus. Diese Statistiken wurden seit der letzten Aktualisierung der Seite kumuliert.

Für die ausgewählte Schnittstelle werden die folgenden Informationen angezeigt:

- **Empfangene EAPOL-Frames**: Am Port empfangene gültige EAPOL-Frames (Extensible Authentication Protocol).
- **Übertragene EAPOL-Frames**: Vom Port übertragene gültige EAPOL-Frames.
- **Empfangene EAPOL-Start-Frames**: Am Port empfangene EAPOL-Start-Frames.
- **Empfangene EAPOL-Logoff-Frames**: Am Port empfangene EAPOL-Logoff-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.

So löschen Sie Statistikzähler:

- Klicken Sie auf **Schnittstellenzähler löschen**, um alle Zähler für die ausgewählte Schnittstelle auf 0 zurückzusetzen.
- Klicken Sie auf **Alle Schnittstellenzähler löschen**, um die Zähler für alle Schnittstellen auf 0 zurückzusetzen.

IPv6-DHCP-Statistik

Sie können den Switch so konfigurieren, dass dieser über eine IPv6-Schnittstelle verwaltet werden kann und die IPv6-Adresse für die Verwaltung über das DHCP (Dynamic Host Configuration Protocol, DHCPv6) erhält. Informationen zum Konfigurieren von IPv6 und DHCP in der Verwaltungsschnittstelle finden Sie unter **Verwaltungsschnittstelle**. Auf der Seite *IPv6-DHCP-Statistik* können Sie Informationen zu gesendeten und empfangenen DHCPv6-Paketen anzeigen.

Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **Status und Statistik** > **IPv6-DHCP-Statistik**.

Wählen Sie eine Aktualisierungsrate für die Seite aus. Auf der Seite werden die folgenden Statistiken angezeigt, die seit der letzten Aktualisierung der Seite kumuliert wurden.

- Empfangene DHCPv6-Ankündigungspakete
- Empfangene DHCPv6-Antwortpakete
- Empfangene, verworfene DHCPv6-Ankündigungspakete
- Empfangene, verworfene DHCPv6-Antwortpakete
- Empfangene defekte DHCPv6-Pakete
- Insgesamt empfangene DHCPv6-Pakete
- Übertragene DHCPv6-Anfragepakete
- Übertragene DHCPv6-Anforderungspakete
- Übertragene DHCPv6-Erneuerungspakete
- Übertragene DHCPv6-Neuanbindungspakete
- Übertragene DHCPv6-Freigabepakete
- Insgesamt übertragene DHCPv6-Pakete

Klicken Sie auf **Zähler löschen**, um alle Zähler auf 0 zurückzusetzen.

RADIUS-Statistik

Sie können den Switch für die Kommunikation mit einem RADIUS-Server zur Benutzerauthentifizierung konfigurieren. Um die Seite *RADIUS-Statistik* anzuzeigen, klicken Sie im Navigationsfenster auf **Status und Statistik** > **RADIUS-Statistik**.

Wählen Sie einen RADIUS-Server aus der Liste aus, und wählen Sie eine Aktualisierungsrate für die Seite aus. Auf der Seite werden die folgenden Statistiken angezeigt, die seit der letzten Aktualisierung der Seite kumuliert wurden.

- **Zugriffsanfragen**: Die Anzahl der an den RADIUS-Server gesendeten Authentication-Request-Pakete.
- **Zugriffsneuübertragungen**: Die Anzahl der erneut an den RADIUS-Server gesendeten Authentication-Request-Pakete.
- **Akzeptierte Zugriffsversuche**: Die Anzahl der vom RADIUS-Server akzeptierten Authentication-Request-Pakete.
- **Abgelehnte Zugriffsversuche**: Die Anzahl der vom RADIUS-Server abgelehnten Authentication-Request-Pakete.
- **Zugriffsherausforderungen**: Die Anzahl der vom RADIUS-Server an den Switch gesendeten Access-Challenge-Pakete.
- **Zugriffsantworten mit inkorrekter Form**: Die Anzahl der vom RADIUS-Server empfangenen Antwortpakete mit inkorrekter Form.
- **Fehlerhafte Authentifikatoren**: Die Anzahl der Authentication-Request-Pakete, die ungültige Meldungsauthentifikatorattribute enthielten.
- **Ausstehende Anforderungen**: Die Anzahl der an den Server gesendeten Authentication-Request-Pakete, die nicht beantwortet wurden.
- **Timeouts**: Die Anzahl der Authentication-Request-Pakete, bei denen ein Timeout aufgetreten ist, da der Server nicht geantwortet hat.
- **Unbekannte Typen**: Die Anzahl der vom Switch empfangenen RADIUS-Pakete unbekannten Typs.
- **Verworfene Pakete**: Die Anzahl der vom Switch verworfenen RADIUS-Pakete.

Klicken Sie auf **Alle Statistiken löschen**, um alle Zähler auf 0 zurückzusetzen.

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 abgebildet.

So zeigen Sie die Statistik an:

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

SCHRITT 2 Wählen Sie den Port oder die LAG aus, für den bzw. für die Sie Statistiken anzeigen möchten.

SCHRITT 3 Wählen Sie eine Aktualisierungsrate für die Seite aus.

Für die ausgewählte Schnittstelle werden die folgenden Informationen angezeigt:

- **Empfangene Byte**: Die Anzahl der Oktette, die die Schnittstelle seit der letzten Aktualisierung des Switch empfangen hat. Diese Zahl beinhaltet fehlerhafte Pakete und FCS-Oktette, jedoch keine Frame-Bits.
- **Drop-Ereignisse**: Die Anzahl der Fälle, in denen seit der letzten Aktualisierung des Switch Pakete von der Schnittstelle verworfen wurden.
- **Empfangene Pakete**: Die Anzahl der Pakete, die von der Schnittstelle empfangen wurden. Dazu gehören fehlerhafte Pakete, Multicast- und Broadcast-Pakete.
- **Empfangene Broadcast-Pakete**: Die Anzahl der gültigen Broadcast-Pakete, die die Schnittstelle seit der letzten Aktualisierung des Switch empfangen hat. Multicast-Pakete sind hier nicht enthalten.
- **Empfangene Multicast-Pakete**: Die Anzahl der gültigen Multicast-Pakete, die die Schnittstelle seit der letzten Aktualisierung des Switch empfangen hat.
- **CRC- & Ausrichtungsfehler**: Die Anzahl der CRC- und Ausrichtungsfehler, die seit der letzten Aktualisierung des Switch aufgetreten sind.
- **Zu kleine Pakete**: Die Anzahl der zu kleinen Pakete (weniger als 64 Oktette), die die Schnittstelle seit der letzten Aktualisierung des Switch empfangen hat.
- **Zu große Pakete**: Die Anzahl der zu großen Pakete (mehr als 1518 Oktette), die die Schnittstelle seit der letzten Aktualisierung des Switch empfangen hat.
- **Fragmente**: Die Anzahl der Fragmente (Pakete mit weniger als 64 Oktetten, ausschließlich Frame-Bits, jedoch einschließlich Frame-Prüfsequenz-Oktetten), die die Schnittstelle seit der letzten Aktualisierung des Switch empfangen hat.

- **Jabbers**: Die Anzahl der empfangenen Pakete, die mehr als 1518 Oktette lang waren und bei denen während der Stichprobensitzung ein FCS-Fehler aufgetreten ist.
- **Kollisionen**: Die Anzahl der Kollisionen, die die Schnittstelle seit der letzten Aktualisierung des Switch empfangen hat.
- **Frames mit 64 Byte**: Die Anzahl der Frames mit 64 Byte, die die Schnittstelle seit der letzten Aktualisierung des Switch empfangen hat.
- **Frames mit 65 bis 127 Byte**: Die Anzahl der Frames mit 65 bis 127 Byte, die die Schnittstelle seit der letzten Aktualisierung des Switch empfangen hat.
- **Frames mit 128 bis 255 Byte**: Die Anzahl der Frames mit 128 bis 255 Byte, die die Schnittstelle seit der letzten Aktualisierung des Switch empfangen hat.
- **Frames mit 256 bis 511 Byte**: Die Anzahl der Frames mit 256 bis 511 Byte, die die Schnittstelle seit der letzten Aktualisierung des Switch empfangen hat.
- **Frames mit 512 bis 1023 Byte**: Die Anzahl der Frames mit 512 bis 1023 Byte, die die Schnittstelle seit der letzten Aktualisierung des Switch empfangen hat.
- **Frames mit 1024 bis 1518 Byte**: Die Anzahl der Frames mit 1024 bis 1518 Byte, die die Schnittstelle seit der letzten Aktualisierung des Switch empfangen hat.

Protokolle

Der Switch generiert Nachrichten, die den Status des Systems identifizieren und die Diagnose von Problemen beim Betrieb des Switch erleichtern. Nachrichten können als Reaktion auf Ereignisse oder Fehler, die auf der Plattform auftreten, sowie auf Konfigurationsänderungen generiert werden.

Die Protokolle dieser Nachrichten werden im RAM und im Flash-Speicher gespeichert. Die Einträge im Flash-Protokoll werden (im Gegensatz zu denen im RAM) so gespeichert, dass sie auch nach einem Neustart der Plattform erhalten bleiben.

Um auf die Elemente des Protokollmenüs zuzugreifen, klicken Sie im Navigationsfenster auf **Status und Statistik** > **Protokoll anzeigen**. Das Protokollmenü enthält die folgenden Seiten:

- **RAM-Speicherprotokoll**
- **Flash-Speicherprotokoll**

RAM-Speicherprotokoll

Auf der Seite *RAM-Speicher* können Sie Informationen zu bestimmten RAM-Protokolleinträgen (Cache) anzeigen, einschließlich des Zeitpunkts des Protokolleintrags, des Protokollschweregrads und einer Beschreibung des Protokolls.

Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **Status und Statistik** > **Protokoll anzeigen** > **RAM-Speicher**.

HINWEIS Wenn die Tabelle die maximale Anzahl von Einträgen enthält, kann das Laden der Seite bis zu 45 Sekunden dauern.

Die RAM-Speicherprotokolltabelle enthält die folgenden Felder:

- **Protokollindex**: Die numerische ID des Protokolleintrags.
- **Protokollzeit**: Der Zeitpunkt, zu dem das Protokoll in die RAM-Speicherprotokolltabelle aufgenommen wurde.
- **Schweregrad**: Für den Protokollschweregrad sind folgende Werte möglich:
  - **Notfall (0)**: Das System kann nicht verwendet werden.
  - **Alarm (1)**: Es muss sofort eine Aktion ausgeführt werden.
  - **Kritisch (2)**: Kritische Bedingungen.
  - **Fehler (3)**: Fehlerbedingungen.
  - **Warnung (4)**: Warnbedingungen.
  - **Hinweis (5)**: Normale, aber signifikante Bedingungen.
  - **Information (6)**: Informationsnachrichten.
  - **Debugging (7)**: Bietet detaillierte Informationen zu einem Ereignis.

  Auf der Seite *Protokolleinstellungen* können Sie die im Protokoll aufgezeichneten Schweregrade auswählen.

- **Komponente**: Die Softwarekomponente oder der Service, von der bzw. von dem der Protokolleintrag erzeugt wurde.
- **Beschreibung**: Die Protokollbeschreibung.

Sie können auf **Protokolle löschen** klicken, um alle Protokolleinträge aus dem RAM zu entfernen.

Flash-Speicherprotokoll

Die Protokolldatei enthält Informationen zu bestimmten Protokolleinträgen, einschließlich des Zeitpunkts des Protokolleintrags, des Protokollschweregrads und einer Beschreibung des Protokolls. Es werden verschiedene Protokolltypen unterstützt, und im System werden bis zu drei Versionen jedes Typs gespeichert.

So zeigen Sie ein Flash-Protokoll an:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Status und Statistik** > **Protokoll anzeigen** > **Flash-Speicher**.

SCHRITT 2 Wählen Sie einen Protokolltyp aus der Liste aus:

- **Standard**: TBD
- **Start**: Enthält Protokolleinträge, die bei Systemneustart erstellt werden.
- **Operativ**: Enthält Protokolleinträge, die während des Systembetriebs erstellt werden.

SCHRITT 3 Wählen Sie eine Protokollversion zum Anzeigen aus.

Version 1 ist die aktuelle oder zuletzt erstellte Protokolldatei, Version 2 die vorletzte und Version 3 die älteste. Wenn ein neues Protokoll des angegebenen Typs erstellt wird, wird das Protokoll der Version 3 gelöscht, und die Protokolle der Versionen 1 und 2 werden in Version 2 bzw. Version 3 umbenannt.

Wenn eine andere Version und ein anderes Protokoll ausgewählt werden, wird das neue Protokoll automatisch in der Flash-Speicherprotokolltabelle angezeigt. Wenn die Tabelle die maximale Anzahl von Einträgen enthält, kann es bis zu 45 Sekunden dauern, bis die Seite angezeigt wird.

Die Flash-Speicherprotokolltabelle enthält die folgenden Felder:

- **Protokollindex**: Die numerische ID des Protokolleintrags.
- **Protokollzeit**: Der Zeitpunkt der Erstellung des Protokolls in der Flash-Speichertabelle.

- **Schweregrad**: Für den Protokollschweregrad sind folgende Werte möglich:
  - **Alarm (1)**: Es muss sofort eine Aktion ausgeführt werden.
  - **Kritisch (2)**: Kritische Bedingungen.
  - **Fehler (3)**: Fehlerbedingungen.
  - **Warnung (4)**: Warnbedingungen.
  - **Hinweis (5)**: Normale, aber signifikante Bedingungen.
  - **Information (6)**: Informationsnachrichten.
  - **Debugging (7)**: Bietet detaillierte Informationen zu einem Ereignis.

  Auf der Seite *Protokolleinstellungen* können Sie die im Protokoll aufgezeichneten Schweregrade auswählen.
- **Komponente**: Die Softwarekomponente, von der der Protokolleintrag erzeugt wurde.
- **Beschreibung**: Die Protokollbeschreibung.

HINWEIS Sie können auf **Protokolle löschen** klicken, um alle Protokolleinträge aus dem Flash-Speicher zu entfernen. Sie können auf **Protokolle sichern** klicken, um die Seite *Konfiguration/Protokoll herunterladen/sichern* zu öffnen, auf der Sie die Protokolldateien mithilfe von TFTP oder HTTP auf einem TFTP-Server oder in einem Netzwerkspeicherort sichern können. Weitere Informationen finden Sie unter **Sichern der Konfigurationsdatei und der Protokolle**.

3

Administration

In diesem Kapitel wird das Konfigurieren globaler Systemeinstellungen und das Ausführen von Diagnosen beschrieben.

Das Kapitel enthält die folgenden Themen:

- **Konfigurieren von Systemeinstellungen**
- **Verwaltungsschnittstelle**
- **Verwalten von Benutzerkonten**
- **Aktivieren von Verwaltungsdiensten**
- **Konfigurieren des Timeouts für Sitzungsleerlauf**
- **Anmeldesitzungen**
- **Anmeldeverlauf**
- **Zeiteinstellungen**
- **Systemprotokolle**
- **Dateiverwaltung**
- **Neustarten des Switch**
- **Verwenden von Ping für Hosts**
- **Konfigurieren der Weiterleitung von Kontrollpaketen**
- **Diagnose**
- **Aktivieren von Bonjour**
- **LLDP-MED**
- **Konfigurieren von DHCP-Client-Lieferantenoptionen**

Konfigurieren von Systemeinstellungen

Auf der Seite *Systemeinstellungen* können Sie Informationen konfigurieren, die den Switch innerhalb des Netzwerks identifizieren.

So konfigurieren Sie die Systemeinstellungen:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Systemeinstellungen**.

Die Systembeschreibung ist fest in der Firmware codiert.

SCHRITT 2 Geben Sie die Parameter ein:

- **Systemstandort**: Eine Beschreibung des physischen Standorts des Switch.
- **Systemkontakt**: Eine Kontaktperson für den Switch.
- **Hostname**: Der administrativ zugewiesene Name dieses verwalteten Knotens. Konventionsgemäß handelt es sich dabei um den vollständigen Hostnamen des Knotens. Der Standardhostname setzt sich aus dem Wort „switch“ und den sechs letzten Hexadezimalstellen der MAC-Adresse des Switch zusammen. Hostnamen dürfen nur Buchstaben, Ziffern und Bindestriche enthalten. Der Hostname darf nicht mit einen Bindestrich beginnen oder enden. Sonstige Symbole, Satzzeichen oder Leerzeichen sind nicht zulässig.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Verwaltungsschnittstelle

Mithilfe der Switch-Verwaltungsschnittstelle können Sie über eine Verwaltungsstation im Netzwerk auf das webbasierte Switch-Konfigurationsdienstprogramm zugreifen. Der Switch unterstützt die Konfiguration eines Verwaltungs-VLANs, das den Verwaltungsverkehr von anderem Verkehr im Switch trennt.

Sie können die Verwaltungsschnittstelle mit einer IPv4-Adresse oder einer IPv6-Adresse konfigurieren. Die Adressen können statisch konfiguriert oder über DHCP/BOOTP-Server bezogen werden.

Weitere Informationen zu den Konfigurationsseiten im Menü Administration > Verwaltungsschnittstelle finden Sie in den folgenden Themen:

- **Konfigurieren einer IPv4-Verwaltungsschnittstelle**
- **Konfigurieren einer IPv6- Verwaltungsschnittstelle**
- **Anzeigen und Hinzufügen von IPv6-Nachbarn**

Konfigurieren einer IPv4-Verwaltungsschnittstelle

Auf der Seite *IPv4-Schnittstelle* können Sie das Verwaltungs-VLAN und die IPv4-Adresse konfigurieren.

So konfigurieren Sie die IPv4-Verwaltungsschnittstelle:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Verwaltung** > **IPv4-Schnittstelle**.

SCHRITT 2 Wählen Sie ein Verwaltungs-VLAN aus der Liste aus.

Damit ein Port auf das webbasierte Switch-Konfigurationsdienstprogramm zugreifen kann, muss er Mitglied des Verwaltungs-VLANs sein. VLAN 1 ist standardmäßig als Verwaltungs-VLAN konfiguriert, und alle Switch-Ports sind als Mitglieder von VLAN 1 konfiguriert.

Mindestens ein Port muss Mitglied des Verwaltungs-VLANs sein. In der Liste **Mitglieder-Ports** werden alle aktuellen Mitglieder des ausgewählten Verwaltungs-VLANs angezeigt.

Wenn Sie das Verwaltungs-VLAN ändern, müssen Sie alle Mitglieder des vorherigen Verwaltungs-VLANs dem neuen VLAN zuweisen, damit der Verwaltungszugriff weiterhin möglich ist.

SCHRITT 3 Wählen Sie für den IP-Adresstyp eine der folgenden Optionen aus:

- **DHCP**: Die Verwaltungsschnittstelle bezieht ihre IPv4-Adresse von einem DHCP-Server.
- **BOOTP**: Die Verwaltungsschnittstelle bezieht ihre IPv4-Adresse von einem BOOTP-Server.
- **Statisch**: Die im Feld **IP-Adresse** zugewiesene IPv4-Adresse der Verwaltungsschnittstelle.

  Standardmäßig ist DHCP aktiviert, und der Switch fordert eine IP-Adresse von einem DHCP-Server an. Wenn der Switch die IP-Adresse nicht von einem Server beziehen kann, wird die statische IP-Adresse aus den Werkseinstellungen verwendet. Die System-LED blinkt in diesem Fall ununterbrochen. Der Switch versucht weiter, eine IP-Adresse von einem DHCP-Server zu beziehen. Die statische IP-Adresse aus den Werkseinstellungen lautet 192.168.1.254/24 und das Standard-Gateway 192.168.1.1.

  Wenn der IP-Adresstyp auf „Statisch“ festgelegt ist, geben Sie Folgendes an:

  - **IP-Adresse**: Geben Sie eine IPv4-Adresse ein.
  - **Maske**: Geben Sie eine 32-Bit-Netzwerkmaske ein (beispielsweise 255.255.255.0).
    Alternativ wählen Sie **Präfixlänge** aus und geben die Anzahl der Bits (0 – 32) ein, aus denen das Netzwerkpräfix besteht (beispielsweise 24).
  - **Standard-Gateway**: Wählen Sie **Benutzerdefiniert** aus, und geben Sie die IP-Adresse des Standard-Gateways für Verwaltungspakete an. Alternativ wählen Sie **Ohne** aus, um zu verhindern, dass Verwaltungspakete außerhalb des Subnetzes gesendet werden.
- **Betriebsstandard-Gateway**: Das zurzeit verwendete Standard-Gateway.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

VORSICHT Wenn Sie die Verwaltungs-IP-Adresse und den IP-Adresstyp ändern, wird die aktuelle Verwaltungssitzung beendet. Durch die Änderung des Verwaltungs-VLANs und seiner Port-Mitgliedschaften wird möglicherweise die Kommunikation mit dem Switch gestört, sodass die aktuelle Verwaltungssitzung beendet wird.

Konfigurieren einer IPv6- Verwaltungsschnittstelle

Auf der Seite *IPv6-Schnittstelle* können Sie den Zugriff auf das webbasierte Switch-Konfigurationsdienstprogramm über IPv6 aktivieren. Sie können den Switch so konfigurieren, dass dieser seine IPv6-Adressen dynamisch lernt, und Sie können IPv6-Adressen statisch konfigurieren.

So aktivieren Sie den IPv6-Verwaltungszugriff:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Verwaltungsschnittstelle** > **IPv6-Schnittstelle**.

SCHRITT 2 Konfigurieren Sie die folgenden Einstellungen:

- **IPv6-Modus**: Wählen Sie diese Option aus, um den IPv6-Verwaltungszugriff zu aktivieren.
- **Automatische IPv6-Adresskonfiguration**: Wählen Sie diese Option aus, damit der Switch die Link Local-Adressen automatisch im EUI-64-Format konfigurieren kann. Dabei wird die MAC-Adresse der Ports für den Link Local-Teil der Adresse verwendet. Der Switch hört Routerbekanntmachungen mit, um den globalen Teil der Adresse zu erkennen und automatisch zu konfigurieren.
- **DHCPv6**: Wählen Sie diese Option aus, damit der Switch seine IPv6-Adressen von einem DHCPv6-Server beziehen kann.
- **IPv6-Gateway**: Geben Sie die Link Local-Adresse des IPv6-Routers an, an die der Switch IPv6-Pakete senden soll, die für ein Gerät außerhalb des Subnetzes bestimmt sind.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert. Sie können auf **Abbrechen** klicken, um die Änderungen zu löschen.

Hinzufügen von IPv6-Adressen

In der IPv6-Adresstabelle werden die zurzeit im Switch konfigurierten statischen Adressen aufgeführt. Die Tabelle enthält die folgenden Felder:

- **IPv6-Adresse**: IPv6-Adresse im globalen IPv6-Adressformat.

- **DAD-Status**: Der Duplicate Address Detection-Status. Wenn Sie eine IPv6-Adresse im Switch konfigurieren, führt der Switch vor der tatsächlichen Zuweisung der Adresse eine Nachbarerkennung aus, um festzustellen, ob die Adresse bereits im Netzwerk verwendet wird.
  - Wenn die Adresse bereits verwendet wird, entspricht der DAD-Status „Wahr“, und die Adresse kann nicht für den Verwaltungszugriff verwendet werden.
  - Wenn festgestellt wird, dass die Adresse eindeutig ist, entspricht der DAD-Status „Falsch“, und die Adresse kann für den Verwaltungszugriff verwendet werden.

Sie können mehrere IPv6-Adressen konfigurieren. Jede Adresse sollte ein anderes Präfix haben, damit der Switch von Stationen in verschiedenen Subnetzen verwaltet werden kann. Wenn eine Route zu einem Subnetz ausfällt, kann der Switch über ein anderes Subnetz verwaltet werden.

So fügen Sie eine statische IPv6-Adresse hinzu:

SCHRITT 1 Klicken Sie auf **Hinzufügen**.

SCHRITT 2 Geben Sie eine IPv6-Adresse gefolgt von einem Schrägstrich (/) und der Präfixlänge ein.

SCHRITT 3 Wählen Sie **EUI-64** aus, wenn die Adresse dem EUI-64-Format entspricht. Dabei stellen die ersten drei bis fünf Oktette die OUI (Organizationally Unique Identifier) und die verbleibenden Oktette eine eindeutig zugewiesene Adresse dar.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Tabelle der IPv6-Standardrouter

Wenn die IPv6-Verwaltung aktiviert ist, verwendet der Switch die IPv6-Nachbarerkennung, um den Standardrouter für die Kommunikation mit Geräten außerhalb des lokalen IPv6-Subnetzes zu identifizieren. Der Standardrouter in IPv6-Netzwerken ist von der Funktion her vergleichbar mit dem Standardrouter in IPv4-Netzwerken.

In der Tabelle der IPv6-Standardrouter werden die IP-Adressen der Standardrouter für die einzelnen IPv6-Verwaltungsadressen aufgeführt. Eine Standardrouteradresse besteht aus der Link Local-Adresse der IPv6-Schnittstelle im Subnetz.

Anzeigen und Hinzufügen von IPv6-Nachbarn

Wenn die IPv6-Verwaltung aktiviert ist, identifiziert der Switch IPv6-fähige Geräte an verbundenen Links. Der Switch unterstützt die Erkennung von bis zu 1.000 dynamischen IPv6-Nachbarn und die statische Konfiguration von IPv6-Nachbarn.

Auf der Seite *IPv6-Nachbarn* werden dynamisch erkannte und statisch konfigurierte Nachbarn aufgeführt, und Sie können statische Hosts hinzufügen.

Um die IPv6-Nachbartabelle anzuzeigen, klicken Sie im Navigationsfenster auf **Administration** > **Verwaltungsschnittstelle** > **IPv6-Nachbarn**.

In der IPv6-Nachbartabelle werden die folgenden Felder für die einzelnen dynamischen Einträge angezeigt:

- **IPv6-Adresse**: IPv6-Adresse des Nachbarn.
- **MAC-Adresse**: MAC-Adresse des Nachbarn.
- **Status**: Status des Nachbarn. Für dynamische Einträge sind die folgenden Status möglich:
  - **Erreichbar**: Es wurde innerhalb eines vorkonfigurierten Intervalls eine Bestätigung empfangen, dass der Weiterleitungspfad zum Nachbarn ordnungsgemäß funktioniert. Im Status „Erreichbar“ führt das Gerät beim Senden von Paketen keine besonderen Aktionen aus.
  - **Verzögerung**: Seit dem Empfang der letzten Bestätigung der ordnungsgemäßen Funktion des Weiterleitungspfads ist mehr Zeit verstrichen als im Intervall vorkonfiguriert.
- **Alter aktualisiert**: Die Zeit in Sekunden, die seit dem Hinzufügen eines Eintrags zum Cache verstrichen ist.
- **Typ**: Eintragstyp der Nachbarerkennungs-Cache-Informationen (statisch oder dynamisch).

Sie können auf **Dynamische Nachbarn löschen** klicken, um die Tabelle zu löschen.

Hinzufügen von statischen IPv6-Nachbarn

Der Switch unterstützt bis zu 16 Einträge für statische IPv6 Nachbarn. So fügen Sie einen statischen Nachbarn hinzu:

SCHRITT 1 Klicken Sie auf **Hinzufügen**.

SCHRITT 2 Geben Sie eine globale IPv6-Adresse ein (ohne Präfixlänge).

SCHRITT 3 Geben Sie die MAC-Adresse des Nachbarn ein.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Verwalten von Benutzerkonten

Im Switch ist standardmäßig ein Verwaltungsbenutzer konfiguriert.

- Benutzername: **cisco**
- Kennwort: **cisco**

Auf der Seite *Benutzerkonten* können Sie bis zu fünf zusätzliche Benutzer konfigurieren und Benutzerkennwörter ändern.

Hinzufügen eines Benutzers

So fügen Sie einen neuen Benutzer hinzu:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Benutzerkonten**.

In der Benutzerkontentabelle werden die zurzeit konfigurierten Benutzer angezeigt.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie einen Benutzernamen mit 1 bis 32 alphanumerischen Zeichen ein. Für Benutzernamen sind nur die Zahlen 0 - 9 und die Buchstaben a - z (Groß- oder Kleinbuchstaben) zulässig.

SCHRITT 4 Geben Sie ein Kennwort mit 1 bis 64 Zeichen ein (abhängig von der Einstellung **Kennwortsicherheit**), und bestätigen Sie das Kennwort.

Wenn Sie ein Kennwort eingeben, ändert sich die Anzahl und Farbe der vertikalen Balken. Damit wird die Kennwortsicherheit angegeben.

- Rot: Das Kennwort erfüllt nicht die Mindestanforderungen an die Komplexität. Rechts neben der Messanzeige wird der Text **`Unter Minimum`** angezeigt.
- Orange: Das Kennwort erfüllt die Mindestanforderungen an die Komplexität, die Kennwortsicherheit ist jedoch schwach. Rechts neben der Messanzeige wird der Text **`Schwach`** angezeigt.
- Grün: Das Kennwort ist stark. Rechts neben der Messanzeige wird der Text **`Stark`** angezeigt.

Die Schaltfläche „Übernehmen“ ist erst verfügbar, wenn die Messanzeige orange dargestellt wird und das Kennwort bestätigt wurde.

Beim Hinzufügen eines Benutzers können Sie die Funktion für die Überprüfung der Kennwortsicherheit vorübergehend deaktivieren, damit Sie ein Kennwort konfigurieren können, das die Kriterien der Sicherheitsüberprüfung nicht erfüllt. Klicken Sie auf **Durchsetzung der Kennwortkomplexität deaktivieren**, und klicken Sie dann auf **OK**, wenn die Warnung anzeigt wird.

Auf der Seite *Kennwortsicherheit* können Sie die Überprüfung der Kennwortsicherheit für alle Benutzer deaktivieren oder die Merkmale der Überprüfung konfigurieren.

SCHRITT 5 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Ändern eines Benutzerkennworts

So ändern Sie ein Benutzerkennwort:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Benutzerkonten**.

SCHRITT 2 Wählen Sie den zu konfigurierenden Benutzer aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie ein Kennwort mit 1 bis 64 Zeichen ein (abhängig von der Einstellung **Kennwortsicherheit**), und bestätigen Sie das Kennwort.

Wenn Sie ein Kennwort eingeben, ändert sich die Anzahl und Farbe der vertikalen Balken. Damit wird die Kennwortsicherheit angegeben. Rote Balken weisen auf ein schwächeres Kennwort hin. Orangefarbene Balken weisen auf ein stärkeres Kennwort hin, und grüne Balken weisen auf die höchste Kennwortsicherheit hin.

Beim Ändern eines Kennworts können Sie die Funktion für die Überprüfung der Kennwortsicherheit vorübergehend deaktivieren, damit Sie ein Kennwort konfigurieren können, das die Kriterien der Sicherheitsüberprüfung nicht erfüllt. Klicken Sie auf **Durchsetzung der Kennwortkomplexität deaktivieren**, und klicken Sie dann auf **OK**, wenn die Warnung anzeigt wird.

Auf der Seite *Kennwortsicherheit* können Sie die Überprüfung der Kennwortsicherheit für alle Benutzer deaktivieren oder die Merkmale der Überprüfung konfigurieren.

SCHRITT 4 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Löschen eines Benutzers

Sie können alle Benutzer löschen, mit Ausnahme des Standardbenutzers, der normalerweise die Benutzer-ID **cisco** hat.

Um einen Benutzer zu löschen, wählen Sie den Benutzernamen in der Benutzerkontentabelle aus, und klicken Sie auf **Löschen**.

Aktivieren von Verwaltungsdiensten

Auf der Seite *Verwaltungsdienste* können Sie die Nummer des TCP-Ports für HTTP-Verbindungen mit dem webbasierten Switch-Konfigurationsdienstprogramm konfigurieren.

Die Standard-Port-Nummer für HTTP-Verbindungen ist die allgemein bekannte IANA-Port-Nummer 80. So konfigurieren Sie eine andere HTTP-Port-Nummer:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Verwaltungsdienste**.

SCHRITT 2 Geben Sie die zu verwendende logische Port-Nummer ein (1025 bis 65535). Der Standardwert ist Port 80.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren des Timeouts für Sitzungsleerlauf

Nach einer bestimmten Dauer der Inaktivität werden die Benutzer automatisch bei den Verwaltungsschnittstellen abgemeldet. Nach einem Timeout muss sich der Benutzer erneut authentifizieren.

Auf der Seite *Timeout für Sitzungsleerlauf* können Sie den Timeout-Zeitraum konfigurieren. Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **Administration** > **Timeout für Sitzungsleerlauf**.

Das Inaktivitäts-Timeout für HTTP-Sitzungen kann 1 bis 60 Minuten betragen. Der Standardwert beträgt 10 Minuten.

Wenn Sie den Wert ändern, klicken Sie auf **Übernehmen**, um die Änderung in der aktuellen Konfiguration zu speichern.

Anmeldesitzungen

Auf der Seite *Anmeldesitzungen* werden aktive Verwaltungsanmeldesitzungen angezeigt. Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **Administration** > **Anmeldesitzungen**.

Die Seite enthält für jeden zurzeit angemeldeten Benutzer die folgenden Informationen:

- **Benutzername**: Der Name, den der Benutzer bei der Anmeldung verwendet hat.
- **Verbindung von**: Die IP-Adresse des Hosts.
- **Leerlaufzeit**: Die Zeit, die seit der letzten Aktivität des Benutzers verstrichen ist.
- **Sitzungszeit**: Die Zeit, die seit der Anmeldung des Benutzers verstrichen ist.
- **Sitzungstyp**: Das für die Verwaltungssitzung verwendete Protokoll (HTTP).

Anmeldeverlauf

Auf der Seite *Anmeldeverlauf* können Sie Daten zu vorherigen Anmeldungen bei der Verwaltungssoftware anzeigen. Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **Administration** > **Anmeldeverlauf**.

Auf dieser Seite werden folgende Felder angezeigt:

- **Anmeldezeitpunkt**: Die Dauer der Verbindung des Benutzers mit dem Netzwerk.
- **Benutzername**: Der Name, den der Benutzer bei der Anmeldung verwendet hat.
- **Protokoll**: Das vom Benutzer für die Verbindung mit der Konfigurationssoftware verwendete Protokoll (HTTP, Telnet, Seriell, SSH oder SNMP).
- **Standort**: Die IP-Adresse des Hosts.

Zeiteinstellungen

Über eine Systemuhr wird ein mit dem Netzwerk synchronisierter Zeitstempeldienst für Switch-Softwareereignisse wie beispielsweise Nachrichtenprotokolle bereitgestellt. Sie können die Systemuhr manuell konfigurieren oder den Switch als SNTP-Client (Simple Network Time Protocol) konfigurieren, der die Uhrzeitdaten von einem Server bezieht.

Informationen zu den Konfigurationsseiten im Menü „Administration > Zeiteinstellungen“ finden Sie in den folgenden Themen:

- **Festlegen der Systemzeit**
- **Konfigurieren der SNTP-Einstellung**
- **Konfigurieren der SNTP-Authentifizierung**

Festlegen der Systemzeit

Auf der Seite *Systemzeit* können Sie die Systemzeit manuell festlegen oder das System so konfigurieren, dass die Zeiteinstellungen von einem SNTP-Server bezogen werden. Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **Administration** > **Zeiteinstellungen** > **Systemzeit**.

Standardmäßig wird die Uhrzeit lokal im Switch konfiguriert.

HINWEIS Die tatsächlichen Informationen für Systemzeit, Datum, Zeitzone und den Sommerzeitstatus werden unten auf der Seite angezeigt.

Lokales Angeben der Zeiteinstellungen

So konfigurieren Sie die Zeiteinstellungen lokal:

SCHRITT 1 Wählen Sie auf der Seite *Systemzeit* die Option **Lokale Einstellungen verwenden** aus.

SCHRITT 2 Wählen Sie **Zeitzonenquelle: DHCP** aus, wenn der Switch die Zeitzone von einem DHCP-Server beziehen soll.

SCHRITT 3 Wählen Sie **Datum/Zeit von Computer einstellen** aus, wenn der Switch die Zeiteinstellungen von dem Computer abrufen soll, über den Sie auf den Switch zugreifen.

Alternativ können Sie das Feld löschen und die folgenden Zeiteinstellungen konfigurieren:

- **Datum**: Geben Sie das Datum im Format MM/TT/JJJJ ein, beispielsweise 01/01/2010 für den 1. Januar 2010.
- **Lokale Zeit**: Geben Sie die aktuelle Uhrzeit im Format HH:MM:SS ein, beispielsweise 22:00:00 für 22:00 Uhr. (Wenn die Uhrzeit auf dem 24-Stunden-Format basiert, wird im Hinweistext **HH** angezeigt bzw. **hh**, wenn die Uhrzeit auf dem 12-Stunden-Format basiert.)
- **GMT-Zeitzonendifferenz**: Wählen Sie die Differenz zwischen GMT (Greenwich Mean Time) und der lokalen Uhrzeit in Stunden und Minuten aus.

SCHRITT 4 Geben Sie im Feld **Zeitzonenakronym** ein optionales Akronym aus bis zu vier Buchstaben an, das die konfigurierten Einstellungen identifiziert. Dieses Feld dient nur zu Referenzzwecken.

SCHRITT 5 Wählen Sie **Sommerzeit** aus, um Sommerzeiteinstellungen zu konfigurieren, wenn diese für Ihre Zeitzone gelten. Wenn Sie diese Option ausgewählt haben, konfigurieren Sie die folgenden Felder:

- **USA/Europäisch/Andere**: Wählen Sie „USA“ oder „Europäisch“ aus, wenn die Sommerzeitdifferenz mit den Werten für diese Standorte konfiguriert werden soll. Alternativ können Sie **Andere** auswählen, um die Einstellungen manuell zu konfigurieren. Bei der manuellen Konfiguration können Sie nur die Einstellungen für die nächste Sommerzeit konfigurieren, oder Sie können wiederkehrende Einstellungen konfigurieren.
- **Zeitzonenakronym**: Geben Sie ein optionales Akronym aus bis zu vier Buchstaben an, das die konfigurierten Einstellungen identifiziert. Dieses Feld dient nur zu Referenzzwecken.
- **Sommerzeitdifferenz**: Geben Sie die Anzahl der Minuten an, um die die Uhr zu Beginn der Sommerzeit vorgestellt werden soll.
- **Von/Bis**: Geben Sie Datum und Uhrzeit für Beginn und Ende der Sommerzeit an.
- **Wiederkehrend**: Wählen Sie diese Option aus, um wiederkehrende Sommerzeiten anzugeben, indem Sie den Wochentag und die Nummer der Kalenderwoche für Beginn und Ende der Sommerzeit in jedem Jahr angeben.

SCHRITT 6 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren des Switch als SNTP-Client

Sie können den Switch auch so konfigurieren, dass dieser die Zeit von einem SNTP-Server bezieht. Hierzu konfigurieren Sie die SNTP-Einstellungen für den Switch.

So konfigurieren Sie den Switch so, dass dieser die Zeiteinstellungen von einem SNTP-Server bezieht:

SCHRITT 1 Wählen Sie auf der Seite *Systemzeit* die Option **SNTP-Server verwenden** aus.

SCHRITT 2 Konfigurieren Sie den SNTP-Clientbetriebsmodus des Switch:

- **Unicast**: Konfiguriert den Switch so, dass Unicast-SNTP-Anforderungen nur an konfigurierte Unicast-SNTP-Server gesendet werden. Um diese Funktion zu aktivieren, müssen Sie mindestens einen Unicast-SNTP-Server hinzufügen.
- **Broadcast**: Konfiguriert den Switch so, dass dieser die Zeiteinstellungen aus von SNTP-Servern gesendeten SNTP-Nachrichten bezieht.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

SCHRITT 4 Verwenden Sie die Informationen unter **Konfigurieren der SNTP-Einstellung** und **Konfigurieren der SNTP-Authentifizierung** zum Konfigurieren zusätzlicher SNTP-Einstellungen (beispielsweise Abrufintervalle, Adressen von Unicast-Servern und Authentifizierungsinformationen, die der Switch für den Zugriff auf SNTP-Server benötigt).

Konfigurieren der SNTP-Einstellung

Der Switch unterstützt SNTP (Simple Network Time Protocol). SNTP gewährleistet die auf die Millisekunde genaue Zeitsynchronisation von Netzwerkgeräten. Die Zeitsynchronisation wird von einem SNTP-Server im Netzwerk ausgeführt. Der Switch wird nur als SNTP-Client betrieben und kann keine Zeitdienste für andere Systeme leisten.

Um die Seite *SNTP-Einstellung* anzuzeigen, klicken Sie im Navigationsfenster auf **Administration** > **Zeiteinstellungen** > **SNTP-Einstellung.**

Konfigurieren der SNTP-Einstellung

SCHRITT 1 Auf der Seite *Systemzeit* muss die Option „SNTP-Server verwenden“ ausgewählt sein, und je nach Bedarf muss der Unicast- oder Broadcast-Modus ausgewählt sein.

SCHRITT 2 Konfigurieren Sie auf der Seite *SNTP-Einstellung* Folgendes:

- **Client-Port**: Die Nummer des logischen Ports, der für den SNTP-Client auf dem Switch verwendet werden soll. Standardmäßig wird für diesen Dienst die allgemein bekannte IANA-Port-Nummer 123 verwendet.
- **Unicast-Abrufintervall**: Die relative Rate, mit der Synchronisationsnachrichten vom Switch an den SNTP-Server gesendet werden. Dieses Feld kann nur bearbeitet werden, wenn SNTP-Unicast-Empfang ausgewählt ist. Geben Sie einen Wert von 3 bis 16 ein. Das eigentliche Intervall in Sekunden ist der angegebene Wert mit 2 potenziert. Wenn Sie beispielsweise 4 eingeben, beträgt das Abrufintervall 16 Sekunden.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Anzeigen der Eigenschaften und globalen Parameter des aktiven Servers

Auf der Seite *SNTP-Einstellung* werden gegebenenfalls die folgenden Eigenschaften für den SNTP-Server angezeigt, von dem der Switch zuletzt die Zeiteinstellungen bezogen hat: Außerdem werden auf dieser Seite globale (nicht konfigurierbare) Parameter angezeigt.

Aktiver Server:

- **Server-Hostadresse**: IP-Adresse des SNTP-Servers.
- **Servertyp**: Version des vom Server verwendeten IP-Protokolls (IPv4 oder IPv6).
- **Server-Stratum**: Hierarchische Ebene des SNTP-Servers, die dessen Abweichung von einer Referenzuhr identifiziert.
- **Serverreferenz-ID**: 32-Bit-Code, der die vom Server verwendete Referenzuhr identifiziert.
- **Servermodus**: Betriebsmodus des Servers:
  - **Unicast**: Der SNTP-Server hört Unicast-Anforderungen von SNTP-Clients mit.

- **Broadcast**: Der SNTP-Server sendet regelmäßig Broadcast-Nachrichten an SNTP-Clients.
- **Reserviert**: Von einem SNTP-Server wurde keine Antwort empfangen. Bei Empfang einer Antwort von einem Server wird diese mit einem der gültigen Status überschrieben (Broadcast oder Unicast).

Globale Parameter:

- **SNTP-Clientversion**: Die höchste vom Switch unterstützte SNTP-Protokollversion.
- **Zeitpunkt der letzten Aktualisierung**: Der Zeitpunkt, zu dem das letzte SNTP-Update empfangen wurde.
- **Zeitpunkt des letzten Unicast-Versuchs**: Der Zeitpunkt des letzten Versuchs, den Switch mit einem SNTP-Unicast-Server zu synchronisieren.
- **Client-Modus**: Der konfigurierte SNTP-Clientmodus (Unicast oder Broadcast). Informationen zum Konfigurieren dieses Modus finden Sie unter **Festlegen der Systemzeit**.
- **Maximale Anzahl der Servereinträge**: Die maximale Anzahl der Server, die Sie im Switch konfigurieren können.
- **Aktuelle Anzahl der Servereinträge**: Die Anzahl der zurzeit im System konfigurierten SNTP-Server, die in der Unicast-SNTP-Servertabelle aufgeführt sind.
- **Broadcast-Anzahl**: Die Anzahl der SNTP-Broadcast-Pakete, die der Switch von SNTP-Servern empfangen hat.

Hinzufügen und Ändern von SNTP-Servern

In der Unicast-SNTP-Servertabelle werden die folgenden Informationen zu jedem von Ihnen konfigurierten SNTP-Server angezeigt:

- **SNTP-Server**: IP-Adresse oder Hostname des SNTP-Servers.
- **Authentifizierungsschlüssel-ID**: Erforderlicher Verschlüsselungsschlüssel für die Kommunikation mit dem SNTP-Server.
- **Zeitpunkt des letzten Versuchs**: Der Zeitpunkt des letzten Versuchs, den Switch mit einem SNTP-Unicast-Server zu synchronisieren.
- **Status**: Betriebsstatus des SNTP-Servers. Folgende Werte sind möglich:
  - **Erfolgreich**: Der Client konnte die Zeit von diesem Server abrufen.

- **Anforderungszeit überschritten**: Bei der Clientanforderung ist eine Zeitüberschreitung aufgetreten.
- **Fehlerhaftes Datum**: Vom Server wurde ein fehlerhaftes Datumsformat empfangen.
- **Nicht unterstützte Version**: Der Server unterstützt die im Switch konfigurierte SNTP-Version nicht.
- **Nicht synchronisiert**: Die Uhrzeit des Switch wurde nicht mit dem Server synchronisiert.
- **Kiss of Death**: Der SNTP-Server hat mit einem Kiss of Death-Paket geantwortet, in dem der Switch angewiesen wird, aufgrund von Verkehrsspitzen oder anderen Fehlerbedingungen keine Anforderungen mehr an den Server zu senden.
- **Sonstiges**: Der Status konnte nicht bestimmt werden.

- **Letzte Antwort**: Zeitpunkt der letzten Antwort vom SNTP-Server.
- **Version**: Version des vom Server verwendeten SNTP-Protokolls.
- **Port**: Protokoll-Port-Nummer (123 ist eine allgemein bekannte Port-Nummer für SNTP).
- **Abrufmodus**: Gibt an, ob der Switch für das Senden von SNTP-Anforderungen an diesen Server konfiguriert ist (aktiviert oder deaktiviert).
- **Unicast-Anforderungen insgesamt**: Die Gesamtanzahl der Synchronisationsanforderungen, die der Switch an den Unicast-Server gesendet hat.

Um die Einstellungen für einen Server zu bearbeiten, aktivieren Sie das Kontrollkästchen, um den Server auszuwählen, und klicken Sie dann auf **Bearbeiten**. Um einen Server zu entfernen, aktivieren Sie das Kontrollkästchen, um den Server auszuwählen, und klicken Sie dann auf **Löschen**. Um einen neuen Server hinzuzufügen, klicken Sie auf **Hinzufügen**, und geben Sie dann wie unten beschrieben die Einstellungen ein.

So fügen Sie einen SNTP-Server hinzu:

SCHRITT 1 Klicken Sie auf **Hinzufügen**.

SCHRITT 2 Geben Sie die Parameter ein:

- **SNTP-Server**: Geben Sie eine IPv4-Adresse oder einen Domänennamen ein. Wenn Sie einen Domänennamen verwenden möchten, muss der DNS-Dienst im Switch aktiviert sein (siehe **Domain Name System**).
- **Authentifizierungsschlüssel**: Wählen Sie **Aktivieren** aus, wenn für die Kommunikation mit dem SNTP-Server Authentifizierung erforderlich ist.
- **Authentifizierungsschlüssel-ID**: Wenn Authentifizierung verwendet wird, wählen Sie die Authentifizierungsschlüssel-ID aus der Liste aus. Informationen zum Konfigurieren von Authentifizierungsschlüsseln finden Sie unter **Konfigurieren der SNTP-Authentifizierung**.
- **Abrufmodus**: Wählen Sie **Aktivieren** aus, um zuzulassen, dass der Switch Anforderungen an diesen Server sendet.
- **Port**: Geben Sie die Nummer des UDP-Ports an, die in den SNTP-Nachrichten-Headern angegeben werden soll. Standardmäßig wird als Port-Nummer der allgemein bekannte IANA-Wert 123 verwendet.
- **Version**: Geben Sie die höchste SNTP-Version (1 - 4) an, die der Server unterstützt.

SCHRITT 3 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren der SNTP-Authentifizierung

Auf der Seite *SNTP-Authentifizierung* können Sie Verschlüsselungsschlüssel konfigurieren. Diese enthalten die identifizierenden Informationen, die der Switch für die Authentifizierung gegenüber STNP-Servern verwendet. Außerdem können Sie auf dieser Seite den SNTP-Authentifizierungsdienst aktivieren.

Wenn Sie SNTP-Server definieren, die der Switch verwenden kann, geben Sie an, ob ein Server Authentifizierung verwendet und welcher Authentifizierungsschlüssel verwendet wird.

HINWEIS Sie können die SNTP-Authentifizierung erst aktivieren, wenn Sie mindestens einen vertrauenswürdigen Authentifizierungsschlüssel konfiguriert haben. Anderenfalls wird die Nachricht **`SNTP-Authentifizierung konnte nicht aktiviert werden`** angezeigt.

So konfigurieren Sie einen Authentifizierungsschlüssel und aktivieren diesen Dienst:

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

In der SNTP-Authentifizierungstabelle werden alle zurzeit konfigurierten Authentifizierungsschlüssel angezeigt, und es wird angegeben, ob der jeweilige Schlüssel zurzeit für die Verwendung als vertrauenswürdiger Schlüssel aktiviert ist.

SCHRITT 2 Wählen Sie **Aktivieren** aus, damit sich der Switch vor dem Synchronisieren der Uhrzeit gegenüber einem SNTP-Server authentifizieren muss.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

SCHRITT 4 Klicken Sie in der SNTP-Authentifizierungstabelle auf **Hinzufügen**, um der Liste einen Schlüssel hinzuzufügen.

SCHRITT 5 Geben Sie die Parameter ein:

- **Authentifizierungsschlüssel-ID**: Die Schlüsselnummer. Beim Definieren eines SNTP-Servers im System geben Sie an, welcher Schlüssel für die Authentifizierung verwendet werden soll.
- **Authentifizierungsschlüssel**: Der Wert des Schlüssels. Der Wert ist der Kryptographieschlüssel, der zum Verschlüsseln und Entschlüsseln von SNTP-Nachrichten zum und vom Server verwendet wird.
- **Vertrauenswürdiger Schlüssel**: Gibt an, ob es sich bei diesem Schlüssel um einen vertrauenswürdigen Schlüssel handelt. Nur vertrauenswürdige Schlüssel können verwendet werden. Zum Aktivieren des SNTP-Authentifizierungsdiensts muss mindestens ein vertrauenswürdiger Schlüssel konfiguriert sein.

  Schlüssel werden nur für Unicast-SNTP-Server verwendet. Nur als vertrauenswürdig aktivierte Schlüssel werden zum Authentifizieren eines SNTP-Servers verwendet. Ein Schlüssel, der im Switch konfiguriert, aber als nicht vertrauenswürdig angegeben ist, wird nicht verwendet. Ein Administrator kann einen nicht vertrauenswürdigen Schlüssel hinzufügen, um diesen zu einem anderen Zeitpunkt zu verwenden.

SCHRITT 6 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Systemprotokolle

Der Switch generiert Nachrichten als Reaktion auf Ereignisse, Fehler, Änderungen an der Konfiguration und andere Vorkommnisse. Diese Nachrichten werden lokal im Systemspeicher gespeichert und zur Überwachung oder zur langfristigen Archivierung an eine oder mehrere zentrale Sammelstellen weitergeleitet.

Weitere Informationen zu den Konfigurationsseiten im Menü „Administration > Systemprotokoll“ finden Sie in den folgenden Themen:

- **Konfigurieren von Protokolleinstellungen**
- **Konfigurieren von Remote-Protokoll-Servern**

Konfigurieren von Protokolleinstellungen

Auf der Seite *Protokolleinstellungen* können Sie Protokolle global aktivieren und definieren, welche Ereignistypen im temporären Speicher (RAM) und im dauerhaften Speicher (Flash) protokolliert werden sollen. Protokollnachrichten im Flash-Speicher bleiben auch nach einem Neustart erhalten. Wenn das Protokoll voll ist, werden automatisch die ältesten Ereignisse gelöscht und durch die neuen Einträge ersetzt.

So konfigurieren Sie Protokolleinstellungen:

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

SCHRITT 2 Aktivieren Sie die Protokollierungsarten, die im System ausgeführt werden sollen:

- **Protokollaggregation**: Wenn diese Funktion aktiviert ist, werden mehrere Protokolle des gleichen Typs in einer einzigen Protokollnachricht kombiniert. Wenn zwei oder mehr identische Protokollnachrichten nacheinander innerhalb eines konfigurierten Zeitintervalls empfangen werden, werden diese Nachrichten in einer einzigen Protokollnachricht aggregiert.
- **Intervall für Protokollaggregation**: Geben Sie, wenn die Protokollaggregation aktiviert ist, das Intervall in Sekunden an. Innerhalb dieses Intervalls empfangene aufeinander folgende Nachrichten werden in einer einzigen Protokollnachricht aggregiert. Möglich sind Werte im Bereich von 15 bis 120 Sekunden.
- **RAM-Speicherprotokollierung**: Wählen Sie diese Option aus, um die Protokollierung im RAM zu aktivieren.

- **Flash-Speicherprotokollierung**: Wählen Sie diese Option aus, um die Protokollierung im Flash-Speicher zu aktivieren.
- **Flash-Protokollgröße**: Geben Sie die maximale Anzahl von Protokollnachrichten ein, die im Flash-Speicherprotokoll gespeichert werden sollen.

SCHRITT 3 Aktivieren Sie die Ereignisschweregrade, die für die einzelnen Protokolltypen protokolliert werden sollen. Die folgenden Schweregrade stehen 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.
- **Information**: Geräteinformationen.
- **Debugging**: Bietet detaillierte Informationen zu einem Ereignis.

HINWEIS: Wenn Sie einen Schweregrad auswählen, werden automatisch alle Ereignisse mit diesem oder einem höheren Schweregrad für die Protokollierung ausgewählt.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren von Remote-Protokoll-Servern

Sie können einen oder mehrere Remote-Protokoll-Server definieren, an die Syslog-Nachrichten vom Switch gesendet werden. Auf der Seite *Remote-Protokoll-Server* können Sie Protokoll-Server definieren und den Schweregrad der an den Server zu sendenden Protokollereignisse festlegen.

So aktivieren Sie die Syslog-Verwendung und konfigurieren Remote-Protokoll-Server:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Remote-Protokoll-Server**.

SCHRITT 2 Klicken Sie neben dem Syslog-Protokollierungsmodus auf **Aktivieren**, und konfigurieren Sie dann die folgenden Einstellungen:

- **Einrichtung**: Wählen Sie einen Wert aus der Liste aus, der die Klassifizierung der Syslog-Nachrichten von diesem Switch identifiziert. Die Bedeutung der Werte (Lokal 0 bis Lokal 7) bestimmt der Netzwerkadministrator.
- **Lokaler Port**: Geben Sie die IANA-Port-Nummer für den Switch an. Standardmäßig wird die allgemein bekannte Port-Nummer 514 für das Syslog-Protokoll verwendet.

SCHRITT 3 Klicken Sie in der Tabelle für Remote-Protokoll-Server auf **Hinzufügen**.

SCHRITT 4 Geben Sie die Parameter ein:

- **Protokoll-Server**: Die IPv4-Adresse oder der Hostname des Servers, an den die Protokolle gesendet werden sollen.
- **UDP-Port**: Die Nummer des logischen UDP-Ports, der auf dem Remote-Server für das Syslog-Protokoll verwendet wird. Der Standardwert ist die allgemein bekannte IANA-Syslog-Port-Nummer 514.
- **Mindestschweregrad**: Nur Einträge mit diesem oder einem höheren Schweregrad werden an den Remote-Server gesendet. Eine Beschreibung der Schweregrade finden Sie unter **Konfigurieren von Protokolleinstellungen**.

SCHRITT 5 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Dateiverwaltung

Sie können die Dateiverwaltungsfunktionen verwenden, um die Firmware zu aktualisieren oder zu sichern, die Sprachdateien zu aktualisieren, Konfigurationsänderungen zu speichern, Konfigurationsdateien innerhalb des Switch zu kopieren und die Funktion für die automatische Konfiguration einzurichten.

HINWEIS Während eines laufenden Downloads oder Uploads zum bzw. vom Switch ist der Verwaltungszugriff auf den Switch bis zum Abschluss der Übertragung vollständig blockiert. Dies soll den Switch vor unbekannten Änderungen schützen.

Weitere Informationen zu den Konfigurationsseiten im Menü „Administration > Dateiverwaltung“ und den zugehörigen Aufgaben finden Sie in den folgenden Themen:

- **Aktualisieren und Sichern der Firmware und der Sprachdateien**
- **Herunterladen und Sichern der Konfigurations- und Protokolldateien**
- **Konfiguration löschen**
- **Kopieren und Speichern von Konfigurationsdateien**
- **Automatische DHCP-Konfiguration**
- **Firmware-Wiederherstellung über HTTP**

Dateien und Dateitypen

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

- **Aktuelle Konfiguration**: Die aktuellen Switch-Parameter. Dies ist der einzige Dateityp, den Sie ändern, wenn Sie die Parameterwerte über eine der Konfigurationsschnittstellen ändern. Der Dateityp muss manuell unter einem anderen Dateityp, beispielsweise als Startkonfiguration, gespeichert werden, damit er nach einem Neustart erhalten bleibt.

  Wird der Switch neu gestartet, geht die aktuelle Konfiguration verloren. Wenn Sie den Switch neu starten, wird die im Flash-Speicher abgelegte Startkonfiguration in die im RAM gespeicherte aktuelle Konfiguration kopiert.

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

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

- **Backup-Konfiguration**: Eine manuell erstellte Kopie der Parameterdefinitionen 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.

- **Spiegelkonfiguration**: Eine Kopie der Startkonfiguration, die der Switch in folgenden Fällen erstellt:

  - Der Switch war 24 Stunden lang ununterbrochen in Betrieb.
  - In den vergangenen 24 Stunden wurden Änderungen an der aktuellen Konfiguration vorgenommen, die noch nicht gespeichert wurden.

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

- **Firmware**: Das Betriebssystem. Wird meist als *Image* bezeichnet.

- **Boot-Code**: Steuert den grundlegenden Systemstart und startet das Firmware-Image.

- **Sprachdatei**: Das Wörterbuch, das die Anzeige von Fenstern in der ausgewählten Sprache ermöglicht.

- **Flash-Protokoll**: Im Flash-Speicher abgelegte SYSLOG-Meldungen.

Aktualisieren und Sichern der Firmware und der Sprachdateien

Auf der Seite *Firmware/Sprache aktualisieren/sichern* können Sie die folgenden Aufgaben ausführen:

- Aktualisieren der Firmware durch Herunterladen eines neuen Images von einem Server.
- Aktualisieren des Boot-Codes durch Herunterladen einer neuen Boot-Datei von einem Server.
- Aktualisieren der Sprachdateien durch Herunterladen einer neuen Datei von einem Server. Die Sprachdateien bestimmen die Sprachoptionen für das webbasierte Switch-Konfigurationsdienstprogramm. Sie können die Anzeigesprache bei der Anmeldung auswählen.
- Sichern des Firmware-Images auf einem Server.

Englisch ist immer die Standardsprache.

HINWEIS Außerdem können Sie die Konfigurationsdateien sichern oder wiederherstellen. Weitere Informationen finden Sie unter **Herunterladen und Sichern der Konfigurations- und Protokolldateien**.

So aktualisieren oder sichern Sie die Firmware oder aktualisieren den Boot-Code oder die Sprachdatei:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Dateiverwaltung** > **Firmware/Sprache aktualisieren/sichern**.

SCHRITT 2 Geben Sie die Parameter ein:

- **Übertragungsmethode**: Wählen Sie das für die Dateiübertragung zu verwendende Protokoll (FTP oder HTTP) aus, das dem Typ des Servers entspricht, auf den Sie Dateien herunterladen bzw. von dem Sie Dateien hochladen.
- **Speichermethode**: Wählen Sie **Aktualisieren** aus, um eine Datei in den Switch herunterzuladen, oder **Sichern**, um eine Datei vom Switch auf den Server zu kopieren.
- **Dateityp**: Wählen Sie den Typ der Datei aus, die aktualisiert oder gesichert werden soll (Sie können nur das Firmware-Image sichern):
  - **Firmware-Image**: Software zum Steuern aller Switch-Funktionen und -Schnittstellen.

- **Boot-Code**: Software zum Steuern des anfänglichen Systemstarts.
- **Sprachdatei**: Die Dateien, mit deren Hilfe die Systemoberfläche in der vom Benutzer auf der Anmeldeseite angegebenen Sprache angezeigt werden kann.

- **IP-Version** (nur TFTP): Wählen Sie die Version des Internetprotokolls aus, das für das Upgrade verwendet werden soll. Der Server muss die ausgewählte Version unterstützen. Alternativ können Sie DNS auswählen, um anstelle der IP-Adresse den Servernamen einzugeben. Wenn Sie einen DNS-Namen verwenden möchten, muss im Switch ein DNS-Server konfiguriert sein (siehe Seite *DNS-Server*).
- **TFTP-Server** (nur TFTP): Geben Sie die IP-Adresse des TFTP-Servers an. Wenn Sie DNS als IP-Version ausgewählt haben, geben Sie den Servernamen an.
- **Name der Quelldatei**: Geben Sie bei Upgrades über TFTP den Dateinamen einschließlich des Pfades ein. Bei Upgrades über HTTP navigieren Sie zur Datei auf dem Computer und wählen diese aus.
- **Name der Zieldatei**: Geben Sie bei Sicherungen über TFTP den Dateinamen einschließlich des Pfades ein. Bei Sicherungen über HTTP wird dieses Feld nicht angezeigt.

SCHRITT 3 Klicken Sie auf **Übernehmen**, um das Upgrade bzw. die Sicherung zu starten. Ein Fortschrittsbalken gibt den Status der Dateiübertragung an. Eine typische Image-Übertragung kann 5 - 6 Minuten dauern.

WARNUNG Die Stromversorgung des Switch darf beim Herunterladen einer Image- oder Boot-Code-Datei nicht unterbrochen werden. Wenn beim Herunterladen einer Datei der Strom ausfällt, geht der Inhalt der Datei im dauerhaften Speicher verloren.

Wenn es beim Herunterladen einer Boot-Code-Datei zu einem Stromausfall kommt, kann der Switch nicht gestartet werden. Bitten Sie das Supportcenter von Cisco Small Business um Unterstützung.

Wenn es beim Herunterladen eines Images zu einem Stromausfall kommt, wird das Image nicht geladen, aber der Boot Loader bleibt betriebsbereit. Anweisungen zum Herunterladen eines funktionsfähigen Images finden Sie unter **Firmware-Wiederherstellung über HTTP**.

Herunterladen und Sichern der Konfigurations- und Protokolldateien

Auf der Seite *Konfiguration/Protokoll herunterladen/sichern* können Sie eine gespeicherte Konfigurationsdatei in den Switch herunterladen, um zuvor gespeicherte Einstellungen wiederherzustellen, oder die aktuelle Konfigurationsdatei in einem Netzwerkspeicherort sichern. Außerdem können Sie diese Seiten zum Sichern von Protokolldateien verwenden.

- *Herunterladen einer Konfigurationsdatei zum Wiederherstellen von Einstellungen*
- *Sichern der Konfigurationsdatei und der Protokolle*

Herunterladen einer Konfigurationsdatei zum Wiederherstellen von Einstellungen

So laden Sie eine Konfigurationsdatei in den Switch herunter, um eine zuvor gesicherte Datei wiederherzustellen:

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

SCHRITT 2 Wählen Sie die **Übertragungsmethode** aus (HTTP oder TFTP).

SCHRITT 3 Wählen Sie **Aktualisieren** als **Speichermethode** aus, um die Datei herunterzuladen, die Sie unten angeben.

SCHRITT 4 Geben Sie die folgenden Parameter ein:

- **IP-Version** (nur TFTP): Wählen Sie die Version des Internetprotokolls aus, das für das Upgrade verwendet werden soll. Der Server muss die ausgewählte Version unterstützen. Alternativ können Sie DNS auswählen, um anstelle der IP-Adresse den Servernamen einzugeben. Wenn Sie einen DNS-Namen verwenden möchten, muss im Switch ein DNS-Server konfiguriert sein (siehe Seite *DNS-Server*).
- **TFTP-Server** (nur TFTP): Geben Sie die IP-Adresse des TFTP-Servers an. Wenn Sie DNS als IP-Version ausgewählt haben, geben Sie den Servernamen an.
- **Name der Quelldatei**: Geben Sie bei TFTP den Dateinamen einschließlich des Pfades ein. Bei HTTP navigieren Sie zur Datei auf dem Computer und wählen diese aus.

- **Typ der Zieldatei**: Wählen Sie eine der folgenden Optionen aus:
  - **Startkonfiguration**: Wenn die angegebene Konfigurationsdatei gültig ist, wird die aktuelle Startkonfigurationsdatei durch sie ersetzt. Diese Datei ist dann beim Neustart die aktive Konfigurationsdatei.
  - **Backup-Konfiguration**: Die angegebene Datei ersetzt die aktuelle Backup-Konfigurationsdatei.

SCHRITT 5 Klicken Sie auf **Übernehmen**, um das Upgrade zu starten. Ein Fortschrittsbalken gibt den Status des Upgrades an.

VORSICHT Die Stromversorgung des Switch darf beim Herunterladen der Konfigurationsdatei nicht unterbrochen werden. Wenn beim Herunterladen der Konfigurationsdatei der Strom ausfällt, geht die Datei verloren, und Sie müssen den Vorgang neu starten.

Sichern der Konfigurationsdatei und der Protokolle

So sichern Sie die Konfigurationsdatei oder das Protokoll:

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

SCHRITT 2 Wählen Sie die Übertragungsmethode aus (HTTP oder TFTP).

SCHRITT 3 Wählen Sie **Sichern** als **Speichermethode** aus.

SCHRITT 4 Geben Sie die Parameter ein:

- **IP-Version** (nur TFTP): Wählen Sie die Version des Internetprotokolls aus, das für das Upgrade verwendet werden soll. Der Server muss die ausgewählte Version unterstützen. Alternativ können Sie DNS auswählen, um anstelle der IP-Adresse den Domänennamen des Servers einzugeben. Wenn Sie einen DNS-Namen verwenden möchten, muss im Switch ein DNS-Server konfiguriert sein (siehe Seite *DNS-Server*).
- **TFTP-Server** (nur TFTP): Geben Sie die IP-Adresse des TFTP-Servers an. Wenn Sie DNS als IP-Version ausgewählt haben, geben Sie den Domänennamen des Servers an.
- **Name der Zieldatei** (nur TFTP): Geben Sie einen Namen für die gespeicherte Datei einschließlich des Pfades auf dem TFTP-Server an.

- **Typ der Quelldatei**: Wählen Sie den Typ der Konfigurationsdatei aus.
  - **Aktuelle Konfiguration**: Die aktuelle Konfiguration einschließlich aller in der aktuellen Verwaltungssitzung angewendeten Änderungen.
  - **Startkonfiguration**: Die im Flash-Speicher abgelegte Konfigurationsdatei. Diese Datei enthält keine angewendeten und im RAM gespeicherten Konfigurationsänderungen, die noch nicht im Switch gespeichert sind.
  - **Backup-Konfiguration**: Eine zusätzliche Konfigurationsdatei, die als Backup im Switch gespeichert ist. Der Administrator kann die Backup-Konfigurationsdatei in den Startkonfigurations-Dateityp kopieren und dann den Switch neu starten, um die Backup-Konfigurationsdatei zu verwenden.
  - **Spiegelkonfiguration**: Wenn die aktuelle Konfiguration mindestens 24 Stunden nicht geändert wurde, wird diese automatisch in einem Spiegelkonfigurations-Dateityp gespeichert. Außerdem wird eine Protokollnachricht mit dem Schweregrad **Warnung** generiert, aus der hervorgeht, dass eine neue Spiegeldatei zur Verfügung steht. Mit dieser Funktion kann der Administrator die vorherige Version der Konfiguration anzeigen, bevor diese im Startkonfigurations-Dateityp gespeichert wird, oder um den Spiegelkonfigurations-Dateityp in einen anderen Konfigurationsdateityp zu kopieren. Wird der Switch neu gestartet, wird die Spiegelkonfiguration auf die werksseitig eingestellten Standardparameter zurückgesetzt.
  - **Flash-Protokoll**: Im Flash-Speicher abgelegtes Ereignisprotokoll.
  - **Betriebsprotokoll**: Im Switch-RAM, aber nicht im Flash-Speicher abgelegtes Ereignisprotokoll.
  - **Startprotokoll**: Protokoll der Startnachrichten.

SCHRITT 5 Klicken Sie auf **Übernehmen**.

Bei HTTP-Sicherungen werden Sie aufgefordert, zu einem Speicherort zu navigieren, in dem die Datei gespeichert werden soll. Ein Fortschrittsbalken gibt den Status der Dateiübertragung an.

Konfiguration löschen

Auf der Seite *Konfiguration löschen* können Sie die Startkonfiguration oder die Backup-Konfiguration löschen. Wenn Sie sowohl die Startkonfigurationsdateien als auch die Backup-Konfigurationsdateien löschen, wird beim Neustart des Switch die Standardkonfigurationsdatei verwendet.

So löschen Sie die Startkonfigurationsdatei oder die Backup-Konfigurationsdatei:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Dateiverwaltung** > **Konfiguration löschen**.

SCHRITT 2 Wählen Sie den Dateityp Startkonfiguration oder Backup-Konfiguration aus.

SCHRITT 3 Klicken Sie auf **Übernehmen**.

Kopieren und Speichern von Konfigurationsdateien

Auf der Seite *Konfiguration kopieren/speichern* können Sie Dateien innerhalb des Dateisystems kopieren. Sie können beispielsweise die Backup-Konfigurationsdatei in die Startkonfigurationsdatei kopieren, damit sie beim nächsten Start des Switch verwendet wird.

So kopieren Sie eine Datei in die Startkonfigurationsdatei oder Backup-Konfigurationsdatei:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Dateiverwaltung** > **Konfiguration kopieren/speichern**.

SCHRITT 2 Wählen Sie den Namen der Quelldatei aus:

- **Aktuelle Konfiguration**: Die aktuelle Konfiguration einschließlich aller in der aktuellen Verwaltungssitzung angewendeten Änderungen.
- **Startkonfiguration**: Der beim letzten Start des Switch verwendete Konfigurationsdateityp. Diese Datei enthält keine angewendeten Konfigurationsänderungen, die noch nicht im Switch gespeichert sind.
- **Backup-Konfiguration**: Der im Switch gespeicherte Backup-Konfigurationsdateityp.
- **Spiegelkonfiguration**: Wenn die aktuelle Konfiguration mindestens 24 Stunden nicht geändert wurde, wird diese automatisch im Spiegelkonfigurations-Dateityp gespeichert. Außerdem wird eine

Protokollnachricht mit dem Schweregrad **Warnung** generiert, aus der hervorgeht, dass eine neue Spiegelkonfigurationsdatei zur Verfügung steht. Sie können die Spiegelkonfigurationsdatei verwenden, wenn beim Starten des Switch mit dem Startkonfigurations- oder Backup-Konfigurationsdateityp Probleme auftreten. In solchen Fällen kann der Administrator die Spiegelkonfiguration in den Startkonfigurations-Dateityp oder Backup-Konfigurationsdateityp kopieren und den Switch neu starten.

SCHRITT 3 Wählen Sie als Namen der Zieldatei den Dateityp aus, den Sie mit der zu kopierenden Datei überschreiben möchten.

- **Startkonfiguration**: Der beim letzten Start des Switch verwendete Konfigurationsdateityp. Diese Datei enthält keine angewendeten Konfigurationsänderungen, die noch nicht im Switch gespeichert sind.
- **Backup-Konfiguration**: Der im Switch gespeicherte Backup-Konfigurationsdateityp.

SCHRITT 4 Klicken Sie auf **Übernehmen**, um den Kopiervorgang zu starten.

Nach Abschluss des Vorgangs wird in einem Fenster die Meldung „Kopiervorgang erfolgreich“ angezeigt.

Automatische DHCP-Konfiguration

Der Switch unterstützt die automatische Konfiguration über DHCP, um die Bereitstellung und Aktualisierung von Konfigurationen zu erleichtern. Bei dieser Funktion wird die Konfiguration eines Switch automatisch aktiviert, wenn beim Startvorgang im Gerätespeicher keine Konfigurationsdatei gefunden wird oder wenn eine neuere Konfigurationsdatei zum Herunterladen zur Verfügung steht.

HINWEIS Voraussetzung für die Funktion für die automatische Konfiguration ist, dass andere Geräte im Netzwerk (beispielsweise ein DHCP- oder BOOTP-Server, ein TFTP-Server und gegebenenfalls ein DNS-Server) richtig konfiguriert sind.

Übersicht

Beim Start versucht der Switch mit einem DCHP-Server zu kommunizieren, um eine IP-Adresse und weitere Informationen abzurufen. Wenn die automatische Konfiguration aktiviert ist, lädt der Switch abhängig vom TFTP-Server und vom Namen der vom DHCP-Server erhaltenen Startkonfigurationsdatei möglicherweise auch eine Startkonfigurationsdatei herunter. Die automatische Konfiguration ist standardmäßig aktiviert.

Die automatische DHCP-Konfiguration wird initiiert, wenn der Switch mit aktivierter automatischer Konfiguration neu gestartet wird und eine der folgenden Bedingungen zutrifft:

1. Es werden Informationen auf dem TFTP-Server und eine Startkonfiguration vom DHCP-Server empfangen, und die Konfigurationsdatei wurde nicht vorher bei der automatischen Konfiguration heruntergeladen.
2. Es werden Informationen auf dem TFTP-Server und eine Startkonfiguration vom DHCP-Server empfangen, und der Name der Konfigurationsdatei stimmt nicht mit dem vorher in einer DHCP-Nachricht bekannt gemachten Dateinamen überein.
3. Die Startkonfigurationsdatei ist nicht vorhanden, und es werden keine Informationen auf dem TFTP-Server oder eine Startkonfiguration vom DHCP-Server empfangen.

Wenn die Bedingungen 1 und 2 vorliegen, wird die Datei im Flash-Speicher des Switch gespeichert. Bei nachfolgenden Starts wird der gespeicherte Dateiname mit dem in Option 66/67 in der aktuellen DHCP-Nachricht angegebenen Namen verglichen. Wenn die Namen nicht übereinstimmen, wird die neue Datei heruntergeladen und in den Flash-Speicher geschrieben.

HINWEIS Beim ersten Start des Systems hat der Switch keinen bestimmten Namen für die vom DHCP-Server empfangene Konfigurationsdatei, da noch keine Startkonfigurationsdatei heruntergeladen wurde. Wenn diese Optionen in der DHCP-Nachricht empfangen werden, wird der Dateiname gespeichert, und der Downloadvorgang beginnt.

Im Fall von Option 3 sucht der Switch den TFTP-Server und die Startkonfigurationsdatei wie unter **Standard-Netzwerkkonfigurationsdatei** beschrieben.

Details der DHCP-Servernachricht

Einige oder alle der folgenden Felder können von einem BOOTP- oder DHCP-Server zurückgegeben und vom Switch verarbeitet werden:

- Der Name der Konfigurationsdatei (Boot-Datei oder Option 67), die vom TFTP-Server heruntergeladen werden soll.
- Die ID des TFTP-Servers, von dem die Boot-Datei bezogen werden soll.

Die IP-Adresse des TFTP-Servers kann aus mehreren Quellen in einer DHCP-Antwort abgeleitet werden. Der Switch nimmt die Auswahl anhand der folgenden Kriterien vor (von der höchsten bis zur niedrigsten Priorität):

1. Feld **sname** in einer DHCP- oder BOOTP-Antwort
2. Feld mit dem Namen des TFTP-Servers **(Option 66)** in einer DHCP-Antwort
3. Feld mit der Adresse des TFTP-Servers **(Option 150)** in einer DHCP-Antwort
4. Feld **siaddr** in einer DHCP- oder BOOTP-Antwort

Wenn nur die Werte für „sname“ oder für „Option 66“ an den Switch zurückgegeben werden, wird zum Auflösen der IP-Adresse des TFTP-Servers ein DNS-Server benötigt. Wenn dem Switch eine IP-Adresse zugewiesen wurde und noch kein Hostname zugewiesen ist, sendet die Funktion für die automatische Konfiguration eine DNS-Anforderung für den entsprechenden Hostnamen.

Alternativer TFTP-Server und Dateiname

Auf der Seite *Automatische DHCP-Konfiguration* können Sie einen alternativen TFTP-Server konfigurieren sowie den Dateinamen, der verwendet werden soll, wenn der vom DHCP-Server angegebene Server oder Dateiname nicht gefunden werden kann. Dies verläuft nach dem folgenden Verfahren:

1. Der Switch sendet Unicast-Nachrichten an den gegebenenfalls über DHCP identifizierten TFTP-Server.
2. Wenn die DHCP-Informationen nicht bereitgestellt werden oder der Server oder Dateiname nicht gefunden werden kann, verwendet der Server die alternativen Informationen, sofern diese konfiguriert sind.
3. Wenn die alternativen Informationen nicht konfiguriert sind oder der Server oder Dateiname nicht gefunden werden können, sendet der Switch Broadcast-Nachrichten an den über DHCP identifizierten TFTP-Server.

Details zum Herunterladen von Konfigurationsdateien

Der Switch versucht zuerst, eine hostspezifische Konfigurationsdatei herunterzuladen. Wenn dies nicht möglich ist und der Modus für die Standard-Netzwerkkonfiguration aktiviert ist, lädt er die Konfigurationsdatei „<Hostname>.cfg“ herunter.

Hostspezifische Konfigurationsdatei

Der Switch versucht, die hostspezifische Konfigurationsdatei herunterzuladen, deren Name als Boot-Dateiname in der Antwort eines DHCP-/BOOTP-Servers angegeben oder als Backup-Konfigurationsdatei für die automatische DHCP-Konfiguration konfiguriert ist. Der Switch sendet drei Unicast-TFTP-Anforderungen für die angegebene Boot-Datei. Wenn die Unicast-Versuche fehlschlagen oder wenn keine Adresse eines TFTP-Servers angegeben wurde, sendet der Switch drei Broadcast-Anforderungen für die angegebene Boot-Datei an alle verfügbaren TFTP-Server. Wenn der Switch die Konfigurationsdatei erhält, wird die Konfiguration auf Fehler überprüft. Nach erfolgreicher Überprüfung kopiert der Switch die Konfiguration in den Startkonfigurations-Dateityp, speichert den Konfigurationsdateinamen im nicht flüchtigen Speicher und startet das Gerät neu.

HINWEIS Der Name der Boot-Datei muss dem Schema **.cfg* entsprechen.

Standard-Netzwerkkonfigurationsdatei

Wenn der Modus für die Standard-Netzwerkkonfiguration aktiviert ist und eine der folgenden Bedingungen zutrifft, lädt der Switch die Konfigurationsdatei „<Hostname>.cfg“ herunter:

- Es ist keine hostspezifische Konfigurationsdatei angegeben oder konfiguriert.
- Auf dem TFTP-Server ist keine hostspezifische Konfigurationsdatei vorhanden.
- Beim Herunterladen tritt ein Fehler auf.

Um den Hostnamen in der Konfigurationsdatei aufzulösen, lädt der Switch zuerst die Datei „fp-net.cfg“ vom TFTP-Server herunter. Die Datei „fp-net.cfg“ wird als Standard-Netzwerkkonfigurationsdatei bezeichnet und enthält eine oder mehrere Zuordnungen zwischen IP-Adressen und Hostnamen. Der Switch ermittelt den Hostnamen anhand der Zuordnungen zur IP-Adresse. Wenn keine Zuordnung vorhanden ist, ermittelt der Switch den Hostnamen mit einem Reverse DNS Lookup.

Beispiel für die Datei „fp-net.cfg“:

```
config
  ...
  ip host switch_to_setup 192.168.1.10
  ip host another_switch 192.168.1.11
  ... <other hostname definitions>
exit
```

Wenn ein Hostname ermittelt wurde, gibt der Switch eine TFTP-Anforderung für eine Datei mit dem Namen „*<Hostname>*.cfg“ aus. Dabei entspricht *<Hostname>* den ersten acht Zeichen des Switch-Hostnamens.

Der Switch verwendet die IP-Adresse für einen DNS Reverse Name Lookup. Wenn die IP-Adresse des Switch beispielsweise 192.168.1.10 lautet, entspricht der Hostname **switch_t.cfg** (den ersten acht Zeichen aus dem oben gezeigten Beispiel).

Der Standard-Switch-Name wird abgeleitet nach dem Schema *Switch+letzte 6 Ziffern der hexadezimalen Adresse*. Die Zuordnungsdatei sollte die Hostnamen enthalten, beispielsweise **ip host switchD99FA5 192.168.1.10**. Dann lautet der Hostname, der für „<Hostname.cfg>“ ermittelt wurde, **switchD9.cfg** für den Switch mit der IP-Adresse **192.168.1.10**.

Wenn der Switch die IP-Adresse nicht einem Hostnamen zuordnen kann, sendet die Funktion für die automatische Konfiguration TFTP-Anforderungen für die Standardkonfigurationsdatei **host.cfg**.

Wenn der Switch die Standardkonfigurationsdatei erhält, wird die Konfiguration auf Fehler überprüft. Nach erfolgreicher Überprüfung kopiert der Switch die Konfiguration in den Startkonfigurations-Dateityp und wird neu gestartet. In diesem Fall wird der Name der Standardkonfigurationsdatei nicht im nicht flüchtigen Speicher abgelegt.

HINWEIS Wenn der Switch die gültige Konfigurationsdatei nicht abrufen kann, wird der oben beschriebene Vorgang alle 20 Minuten wiederholt, bis der Switch eine gültige Konfigurationsdatei erhält. Der Administrator kann eine Startkonfigurationsdatei erstellen, indem er die aktuelle Konfiguration manuell speichert. Der Administrator kann die automatische Konfiguration bei Bedarf auch deaktivieren.

Die folgende Tabelle enthält eine Übersicht über die Konfigurationsdateien, die heruntergeladen werden können, sowie die Reihenfolge, in der nach den Dateien gesucht wird.

Suchreihenfolge	Dateiname	Beschreibung	Letzte gesuchte Datei
1	<Boot-Datei>.cfg	Hostspezifische Konfigurationsdatei mit der Dateinamenerweiterung *.cfg[1]	Ja
2	fp-net.cfg	Standard-Netzwerkkonfigurationsdatei	Nein
3	<Hostname>.cfg	Hostspezifische Konfigurationsdatei, die dem Hostnamen zugeordnet ist	Ja
4	host.cfg	Standardkonfigurationsdatei	Ja

1. Diesen Dateinamen können Sie gemäß der Beschreibung unter **Alternativer TFTP-Server und Dateiname** über DHCP ermitteln oder manuell konfigurieren.

Ein Benutzer kann die automatische Konfiguration jederzeit vor dem Herunterladen der Datei beenden. Dies sollte geschehen, wenn der Switch vom Netzwerk getrennt wird oder wenn Sie die Konfigurationsdateien nicht auf TFTP-Servern eingerichtet haben.

Wenn Sie eine Konfigurationsdatei erfolgreich heruntergeladen und im Startkonfigurations-Dateityp gespeichert haben, protokolliert der Switch vor dem Neustart eine Nachricht mit dem Schweregrad „Alarm“.

Einrichten der automatischen DHCP-Konfiguration

Auf der Seite *Automatische DHCP-Konfiguration* können Sie die Funktion aktivieren und deaktivieren, Einstellungen für den TFTP-Server und für Dateinamen konfigurieren und Statusinformationen anzeigen.

Wenn die automatische DHCP-Konfiguration aktiviert ist, hat die Funktion bis zum Erhalt einer Benachrichtigung vom DHCP-Client den Status **Auf Startoptionen warten**. Der DHCP-Client löst bei Empfang der IP-Adresse vom DHCP-Server den automatischen Installationsvorgang aus. Anschließend wechselt der Status zu **DHCP/BOOTP-Optionen verarbeiten, Voraussetzungen überprüfen**.

Möglicherweise werden außerdem die folgenden Nachrichten angezeigt:

- Auf Startoptionen warten
- DHCP/BOOTP-Optionen verarbeiten, Voraussetzungen überprüfen
- tftp://<TFTP-Adresse>/<Dateiname> herunterladen
- Heruntergeladene Konfiguration anwenden
- Auf Neustart-Timeout warten
- Heruntergeladene Konfiguration speichern
- Gestoppt
- Automatische Installation abgeschlossen
- Automatischer Installationsvorgang beendet: Überprüfung von Datei <Dateiname> fehlgeschlagen.
- Automatischer Installationsvorgang beendet: Die heruntergeladene Konfigurationsdatei <Boot-Datei> konnte nicht in der Startkonfiguration gespeichert werden.
- Automatischer Installationsvorgang beendet: Startkonfiguration wird manuell erstellt.
- Automatischer Installationsvorgang beendet: Boot-Datei ist mit der letzten heruntergeladenen Datei identisch.
- Automatischer Installationsvorgang beendet: Der Name der Boot-Datei konnte nicht aufgelöst werden.

So konfigurieren Sie die automatische DHCP-Konfiguration:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Automatische DHCP-Konfiguration**.

SCHRITT 2 Geben Sie die Parameter ein:

- **Automatische Konfiguration über DHCP**: Wählen Sie **Aktivieren** aus, um diese Funktion im Switch zu aktivieren.
- **Standard-Netzwerkkonfigurationsmodus**: Wählen Sie **Aktivieren** aus, damit der Switch eine Standardkonfigurationsdatei mit dem Namen *fp-net.cfg* herunterlädt, wenn im Switch keine hostspezifische Datei gefunden wird. Weitere Informationen finden Sie unter **Standard-Netzwerkkonfigurationsdatei**.

- **Alternativer TFTP-Server**: Geben Sie die IP-Adresse eines TFTP-Servers an, der als Backup dienen soll. Ein alternativer TFTP-Server wird verwendet, wenn Unicast-Anforderungen an den in Option 66 angegebenen TFTP-Server dreimal fehlschlagen.
- **Alternative Konfigurationsdatei**: Geben Sie den Namen einer alternativen Konfigurationsdatei an, die als Backup dienen soll. Wenn in DHCP-Option 67 keine Startkonfigurationsdatei identifiziert wurde oder wenn die angegebene Datei nicht auf dem TFTP-Server gefunden wird, sucht die automatische Konfiguration nach dem alternativen Dateinamen.
- **Dateiname der letzten autmatischen Konfiguration**: Der Name der Konfigurationsdatei, die bei der letzten Ausführung der automatischen Konfiguration verwendet wurde. Wenn über DHCP ein anderer Dateiname identifiziert wird, beginnt der Dateidownload.
- **Aktueller Status**: Der Status des automatischen Konfigurationsvorgangs. Möglich sind die Werte „Abgeschlossen“ oder „Wird durchgeführt“.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Firmware-Wiederherstellung über HTTP

Der Switch verfügt über eine Firmware-Wiederherstellungsfunktion, mit der Sie nach einem fehlgeschlagenen Download im Switch ein gültiges Image wiederherstellen können. Wenn beim Herunterladen eines Images der Strom ausfällt, können Sie den Switch möglicherweise nicht starten. Obwohl das Image nicht verwendet werden kann, sollte in diesem Fall die Boot Loader-Datei, von der das Firmware-Image aus dem Flash-Speicher in das RAM geladen wird, weiterhin funktionsfähig sein. In die Boot Loader-Datei ist ein HTTP-Server eingebettet, mit dessen Hilfe der Administrator eine Verbindung mit dem Switch über einen Switch-Port herstellen und dann mithilfe eines Webbrowsers ein neues Firmware-Image herunterladen und installieren kann.

Der Switch wechselt in den HTTP-Firmware-Wiederherstellungsmodus, wenn der Switch gestartet wird und der Boot Loader im Flash-Speicher kein gültiges Image findet. In diesem Modus legt der Boot Loader den internen Netzwerk-Port des Switch auf die folgende statische IP-Adresse fest:

- IP-Adresse: 192.168.1.254
- Netzwerkmaske: 255.255.255.0
- Standard-Gateway: 192.168.1.1

Ein HTTP-Server wird gestartet und hört Clientverbindungen an Port 80 mit.

So verwenden Sie die Funktion zum Herunterladen eines neuen Firmware-Images:

SCHRITT 1 Verbinden Sie einen Verwaltungs-PC direkt mit einem beliebigen Switch-Port.

SCHRITT 2 Konfigurieren Sie die IP-Adresse und die Maske auf dem Verwaltungs-PC so, dass sich diese im gleichen Subnetz befinden wie der Switch.

HINWEIS: Sie können über ein Netzwerk auf das System zugreifen, wenn die IP-Adresse des Standard-Gateways 192.168.1.1 lautet.

SCHRITT 3 Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse des Switch (192.168.1.254) in die Adressleiste ein.

HINWEIS: Die HTTP-Firmware-Wiederherstellungsfunktion unterstützt die folgenden Browser:

- Firefox 3.0 und höhere Versionen
- Internet Explorer 6 und höhere Versionen

Es wird eine Firmware-Wiederherstellungsseite angezeigt. Eine Authentifizierung ist nicht erforderlich.

Auf der Webseite werden PIC VID (Produkt-ID und Anbieter-ID), Seriennummer und MAC-Adresse des Switch angezeigt.

SCHRITT 4 Klicken Sie auf **Durchsuchen**, und wählen Sie ein gültiges Firmware-Image zum Herunterladen aus.

Während des Downloads wird ein Fortschrittsbalken angezeigt. Nach dem erfolgreichen Download wird die folgende Nachricht angezeigt:

> **100 % abgeschlossen**
> **Datei erfolgreich heruntergeladen. Bitte warten Sie, während die Datei in den Flash-Speicher geschrieben wird. System wird automatisch neu gestartet.**

Die vom Administrator ausgewählte Datei wird in das RAM heruntergeladen und auf die folgenden Bedingungen überprüft:

- Die CRC der Datei ist gültig.
- Die STK-Datei wurde für diese Plattform erstellt.
- Die Größe der STK-Datei liegt innerhalb der Partitionsgrenzen (für diese Datei sind 4,5 MB reserviert).

Wenn diese Bedingungen erfüllt sind, wird die Datei in den Flash-Speicher geschrieben, und das System wird mit der neuen Firmware neu gestartet.

Wenn eine dieser Überprüfungen fehlschlägt, wird das Image nicht in den Flash-Speicher geschrieben, und der Wiederherstellungsvorgang wird beendet. Sie können den Wiederherstellungsvorgang mit einer korrekten Image-Datei neu starten.

Wenn die Übertragung abgebrochen wird, da das Browserfenster aktualisiert oder geschlossen wurde, wird die Sitzung gelöscht, und es tritt sofort ein Timeout auf. Wenn die Übertragung abgebrochen wird, da das Netzwerk nicht erreichbar ist, tritt nach 45 Sekunden ein Sitzungs-Timeout auf. Nach dem Sitzungs-Timeout können Sie den Wiederherstellungsvorgang erneut beginnen.

Neustarten des Switch

Auf der Seite *Neustart* können Sie den Switch neu starten. So starten Sie den Switch neu:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Neustart**.

SCHRITT 2 Wählen Sie eine der folgenden Optionen aus:

- **Neustart**: Der Switch wird mit der letzten gespeicherten Konfiguration neu gestartet.
- **Neustart mit Werkseinstellungen**: Der Switch wird mit der Standardkonfigurationsdatei mit den Werkseinstellungen neu gestartet. Alle angepassten Einstellungen gehen verloren.

Es wird ein Fenster angezeigt, in dem Sie den Neustart bestätigen oder abbrechen können. Die aktuelle Verwaltungssitzung wird möglicherweise beendet.

SCHRITT 3 Bestätigen Sie den Neustart, oder brechen Sie den Vorgang ab.

Verwenden von Ping für Hosts

Auf der Seite *Ping* können Sie eine Ping-Anforderung vom Switch an eine bestimmte IP-Adresse senden. Mithilfe dieser Funktion können Sie überprüfen, ob die Kommunikation zwischen dem Switch und einem bestimmten Netzwerkhost möglich ist.

So verwenden Sie Ping für einen Netzwerkhost:

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

SCHRITT 2 Wählen Sie **IPv4** oder **IPv6** als Adresstyp aus.

SCHRITT 3 Geben Sie bei einer IPv4-Adresse die folgenden Parameter ein:

- **IP-Adresse/Hostname**: Geben Sie die IP-Adresse oder den Hostnamen der Station ein, an die der Switch den Ping senden soll.
- **Anzahl**: Geben Sie die Anzahl der zu sendenden Pings an.
- **Intervall**: Geben Sie die Anzahl der Sekunden zwischen den gesendeten Pings an.
- **Datagrammgröße**: Geben Sie die Datengröße des zu sendenden Ping-Pakets an.

Geben Sie bei einer IPv6-Adresse die folgenden Parameter ein:

- **Ping-Typ**: Wählen Sie „Global“ aus, um einen Ping an eine Adresse außerhalb des lokalen Subnetzes zu senden. Wählen Sie „Link Local“ aus, um einen Ping an eine Adresse im lokalen Subnetz zu senden.
- **IPv6-Adresse/Hostname**: (nur bei globalen Adressen) Geben Sie die globale 128-Bit-Adresse ein.
- **IPv6 Link Local-Adresse**: (nur bei Link Local-Adressen) Geben Sie die Link Local-Adresse ein, wenn sich die Adresse im gleichen Subnetz befindet wie der Switch.
- **Datagrammgröße**: Geben Sie die Datengröße des zu sendenden Ping-Pakets an (zwischen 48 und 2048 Byte).

SCHRITT 4 Klicken Sie auf **Übernehmen**, um den Ping zu senden. Im Ping-Fenster können Sie den Status anzeigen.

Konfigurieren der Weiterleitung von Kontrollpaketen

Auf der Seite *Weiterleitung des Kontrollpakets* können Sie konfigurieren, wie der Switch Pakete der folgenden Protokolltypen behandelt:

- CPD: Das CDP-Protokoll (Cisco Discovery Protocol), das von vielen Netzwerkgerätetypen von Cisco unterstützt wird. Mit CDP können direkt verbundene Geräte Informationen austauschen, beispielsweise IP-Adressen, Funktionen und Softwareversionen. Obwohl der Switch selbst CDP nicht unterstützt, leitet er standardmäßig CDP-Pakete für verbundene Geräte in einem VLAN weiter.
- Dot1X: Das IEEE 802.1X-Protokoll definiert, wie EAP-Pakete (Extensible Authentication Protocol) über ein LAN gekapselt werden. Mit Dot1X können Sie Benutzer authentifizieren und diesen den Zugriff auf über die Switch-Ports zur Verfügung gestellte Dienste ermöglichen oder verweigern. Informationen zum Konfigurieren der Dot1X-Funktion im Switch finden Sie unter 802.1X.
- LLDP: Netzwerkgeräte verwenden das Link Layer Discovery Protocol, um anderen Geräten ihre Funktionen bekannt zu machen. Informationen zum Konfigurieren der LLDP-Funktion im Switch finden Sie unter LLDP-MED.

So konfigurieren Sie die Weiterleitung von Kontrollpaketen:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Weiterleitung des Kontrollpakets**.

SCHRITT 2 Wählen Sie das Protokoll aus, das Sie konfigurieren möchten (CDP, LLPD oder DOT1x).

SCHRITT 3 Wählen Sie die Aktion aus, die ein Port bei Empfang von Paketen des angegebenen Typs ausführen soll:

- **Löschen**: Alle Pakete des ausgewählten Typs werden gelöscht.
- **Weiterleiten**: Alle Pakete des ausgewählten Typs werden im angegebenen VLAN weitergeleitet.
- **Beenden**: Das Paket wird angenommen und im Switch verarbeitet. Diese Option ist für CPD-Pakete nicht verfügbar.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Diagnose

Auf den Diagnoseseiten können Sie virtuelle Kabeltests für Kupfer- und Glasfaserkabel ausführen, eine Diagnoseüberwachung für einen Port oder ein VLAN einrichten und CPU-Auslastungsdaten anzeigen.

Weitere Informationen zu den Konfigurationsseiten im Menü „Administration > Diagnose“ finden Sie in den folgenden Themen:

- **Testen von Kupfer-Ports**
- **Konfigurieren der Port-Spiegelung**
- **CPU-Auslastung/Speicherauslastung**

Testen von Kupfer-Ports

Auf der Seite *Kupfer-Ports* können Sie Tests für Kupferkabel ausführen. Mithilfe dieser Diagnose der physikalischen Schicht können Sie ermitteln, an welcher Stelle das Kabel möglicherweise gebrochen ist.

In der Tabelle für Kupfer-Ports werden die einzelnen Ports und die folgenden Daten aufgeführt, die aus dem letzten Test hervorgehen (wenn der Port nicht getestet wurde, werden Standarddaten angezeigt):

- **Testergebnis**: Ergebnisse des letzten Kabeltests. Folgende Werte sind möglich:
  - **Normal**: Das Kabel funktioniert ordnungsgemäß.
  - **Offen**: Das Kabel ist getrennt, oder der Stecker ist defekt.
  - **Kurz**: Am Kabel liegt ein Kurzschluss vor.
  - **Nicht getestet**: Es wurde kein Test ausgeführt.
  - **Kabeltest fehlgeschlagen**: Der Kabelstatus konnte mit dem Test nicht ermittelt werden. Möglicherweise ist das Kabel funktionsfähig.
- **Abstand zu Fehler**: Entfernung in Metern von dem Port, an dem der Kabelfehler gegebenenfalls beim letzten Kabeltest festgestellt wurde.
- **Letzte Aktualisierung**: Zeitpunkt des letzten Port-Tests.
- **Kabellänge**: Länge des Kabels in Metern.

So starten Sie einen Kupfer-Port-Test:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Diagnose** > **Kupfer-Ports**.

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

Wenn während des Kabeltests an dem Port eine Verbindung aktiv ist, wird die Verbindung möglicherweise für die Dauer des Tests getrennt. Der Test kann mehrere Sekunden dauern. Nach Abschluss des Tests wird ein Fenster mit den Testergebnissen angezeigt.

Konfigurieren der Port-Spiegelung

Mit der Funktion für die Port-Spiegelung können Sie Netzwerkverkehr an einem Port zur Analyse durch ein Netzwerkanalysegerät an einen anderen Port kopieren.

Eine Spiegelungssitzung umfasst einen *Ziel-Test-Port* und mindestens einen *Quell-Port*. Eine Spiegelkopie des Verkehrs an den zu testenden Quell-Ports wird vom Quell-Port an den Ziel-Test-Port gesendet. Sie können ein Netzwerkanalysegerät mit einem Ziel-Test-Port verbinden, um den Netzwerkverkehr zu analysieren.

Ein als Ziel-Test-Port konfigurierter Port fungiert als Spiegelungs-Port, solange die Sitzung aktiv ist. Wenn die Sitzung nicht aktiv ist, sendet und empfängt der Port Verkehr auf der Grundlage der anderen Konfigurationsparameter.

HINWEIS Wenn ein Port als Test-Port konfiguriert ist, leitet der Switch keinen Verkehr weiter, empfängt keinen Verkehr und antwortet nicht auf einen Ping.

Um die Seite *Port-Spiegelung* anzuzeigen, klicken Sie im Navigationsfenster auf **Administration** > **Diagnose** > **Port-Spiegelung**.

Vier standardmäßig deaktivierte Spiegelungssitzungen stehen zur Konfiguration zur Verfügung. In der Tabelle für Port-Spiegelungssitzungen werden für jede Sitzung die folgenden Felder angezeigt:

- **Sitzungs-ID**: Eine ID-Nummer für die Überwachungssitzung.
- **Administrationsmodus**: Gibt an, ob die Port-Spiegelungssitzung aktiviert oder deaktiviert ist.
- **Zielschnittstelle**: Zum Aktivieren der Funktion wählen Sie diese aus und wählen dann den Ziel-Test-Port aus, an dem der Verkehr des Quell-Ports gespiegelt werden soll.
- **Quellschnittstelle**: Liste der Quellschnittstellen, die Sie für die Teilnahme an dieser Spiegelungssitzung ausgewählt haben.

In der Tabelle für die Quellschnittstellen für die Port- Spiegelung werden die den einzelnen Sitzungen zugewiesenen Quellschnittstellen aufgeführt. Sie können auf „Filter“ klicken und eine Sitzungs-ID auswählen, um Daten für nur eine Sitzung anzuzeigen.

Um die Port-Spiegelung einzurichten, weisen Sie zuerst einer Sitzung Quellschnittstellen zu. Dann definieren Sie einen Ziel-Port und aktivieren die Sitzung.

So konfigurieren Sie eine Spiegelungssitzung:

SCHRITT 1 Klicken Sie in der Tabelle für die Quellschnittstellen für die Port-Spiegelung auf **Hinzufügen**.

SCHRITT 2 Wählen Sie eine Sitzungs-ID aus.

SCHRITT 3 Wählen Sie die Quellschnittstelle und den Typ des zu spiegelnden Verkehrs aus.

SCHRITT 4 Geben Sie mithilfe des Optionsfelds „Typ“ die Richtung des Verkehrs an der zu überwachenden Quellschnittstelle an:

- **Nur Rx**: Eingehender Verkehr
- **Nur Tx**: Ausgehender Verkehr
- **Rx und Tx**: Ein- und ausgehender Verkehr

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Sie können den Vorgang wiederholen, um der gleichen Sitzung mehrere Quellschnittstellen zuzuweisen. Eine Quellschnittstelle kann jedoch nur jeweils in einer aktiven Sitzung verwendet werden.

SCHRITT 6 Wählen Sie in der Tabelle für die Port-Spiegelungssitzung die zu aktivierende Sitzung aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 7 Wählen Sie für den Administrationsmodus die Option **Aktivieren** aus.

SCHRITT 8 Wählen Sie für die Zielschnittstelle die Option **Aktivieren** aus, und wählen Sie einen Port zum Spiegeln der Daten aus.

VORSICHT Wenn ein Port als Ziel-Test-Port konfiguriert ist, leitet der Switch keinen Verkehr weiter, empfängt keinen Verkehr und antwortet nicht auf an diesem Port empfangene Pings. Alle bisherigen Konfigurationsparameter für diesen Port werden gelöscht, und Sie müssen den Port neu konfigurieren, wenn Sie die Spiegelung aus der Port-Konfiguration entfernen.

SCHRITT 9 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Testsitzung beginnt.

HINWEIS Um eine Testsitzung zu beenden, wählen Sie die Sitzung in der Tabelle für die Port-Spiegelungssitzung aus, und klicken Sie auf **Bearbeiten**. Deaktivieren Sie das Kontrollkästchen für den Administrationsmodus, und klicken Sie auf **Übernehmen** und dann auf **Schließen**.

CPU-Auslastung/Speicherauslastung

Auf der Seite *CPU-Auslastung/Speicherauslastung* können Sie die CPU-Auslastung und die Speicherauslastung überwachen. Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **Administration** > **Diagnose** > **CPU-Auslastung/Speicherauslastung**.

Auf dieser Seite werden die folgenden Daten angezeigt:

- **Aktualisierungsrate**: Geben Sie an, dass die Seite alle 15, 30 oder 60 Sekunden mit den neuesten Daten aktualisiert werden soll, oder übernehmen Sie die Standardeinstellung „Keine Aktualisierung“.
- **CPU-Auslastungsbericht**: Die prozentuelle Auslastung über Intervalle von 5 Sekunden, 1 Minute und 5 Minuten.
- **Speicherauslastungsbericht**: Die folgenden Daten werden gemeldet:
  - **Reservierter Speicher**: Menge des für das Betriebssystem verfügbaren Speichers.
  - **Freier Speicher**: Menge des für das Betriebssystem verfügbaren Speichers, der zurzeit frei ist.
  - **Gesamtspeicher**: Der gesamte Systemspeicher, einschließlich des reservierten Speichers, des freien Speichers sowie des für die Verwendung durch Code und Datenabschnitte des Software-Images reservierten Speichers.

Aktivieren von Bonjour

Bonjour ermöglicht die Erkennung des Switch und der zugehörigen Dienste mithilfe von Multicast-DNS (mDNS). Bonjour macht Switch-Dienste im Netzwerk bekannt und beantwortet Anfragen für die unterstützten Diensttypen. Dadurch wird die Netzwerkkonfiguration in den Umgebungen kleiner und mittlerer Unternehmen vereinfacht.

Die folgenden Diensttypen werden vom Switch bekannt gemacht:

- **Cisco-spezifische Gerätebeschreibung** (csco-sb): Dieser Dienst ermöglicht Clients die Erkennung von Switches von Cisco und anderen Produkten, die in Netzwerken kleiner und mittlerer Unternehmen bereitgestellt sind.
- **Verwaltungsbenutzeroberflächen**: Dieser Dienst identifiziert die im Switch verfügbaren Verwaltungsschnittstellen (HTTP).

Wenn ein Bonjour-fähiger Switch mit einem Netzwerk verbunden wird, können alle Bonjour-Clients ohne vorherige Konfiguration die Verwaltungsschnittstelle erkennen und auf diese zugreifen.

Ein Systemadministrator kann den Switch mithilfe eines installierten Internet Explorer-Plug-Ins erkennen. Das webbasierte Switch-Konfigurationsdienstprogramm wird als Registerkarte im Browser angezeigt.

Bonjour kann in IPv4- und IPv6-Netzwerken verwendet werden.

So aktivieren Sie die Erkennung des Switch durch Bonjour:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Discovery: Bonjour**.

SCHRITT 2 Wählen Sie die Option „Aktivieren“ aus.

SCHRITT 3 Klicken Sie auf **Übernehmen**.

LLDP-MED

Der IEEE 802.1AB-Standard, Link Layer Discovery Protocol (LLDP), beschreibt eine Methode, mit der Stationen in einem LAN Identifizierungsinformationen, Funktionen und physische Beschreibung bekannt machen. Die Informationen werden in LLDP-Dateneinheiten (LLDP Data Units, LLDPDUs) ausgetauscht, die TLV-Strukturen (Type-Length-Value) enthalten. LLDPDUs können abhängig von den Informationen, für deren Bekanntmachung der Administrator den Port konfiguriert hat, verschiedene TLVs enthalten.

Die aus LLDPDUs hervorgehenden Informationen werden in MIBs gespeichert, und die Informationen sind möglicherweise über ein Netzwerkverwaltungssystem (Network Management System, NMS) wie beispielsweise SNMP zugänglich. Dieses Framework ist erweiterbar und ermöglicht die erweiterte Nutzung in Bereichen wie beispielsweise VoIP-Netzwerken.

HINWEIS LLDPDUs kommunizieren nur Informationen; der Switch wird damit nicht automatisch konfiguriert.

Der Switch unterstützt die LLDP-MED-Erweiterungen (LLDP Media Endpoint Discovery) für das LLDP-Protokoll. LLDP-MED ermöglicht die automatische Erkennung von LAN-Richtlinien, Gerätestandorten sowie anderen Gerätemerkmalen und automatisiert die Verwaltung von PoE-Endpunkten (Power-over-Ethernet).

Weitere Informationen zu den Konfigurationsseiten im Menü „Administration > Erkennung - LLDP“ finden Sie in den folgenden Themen:

- **Konfigurieren von globalen LLDP-MED-Eigenschaften**
- **Konfigurieren von LLDP-MED an einem Port**
- **LLDP-MED-Port-Statusdetails**
- **LLDP-MED-Nachbarinformationen**

Konfigurieren von globalen LLDP-MED-Eigenschaften

Auf der Seite *LLDP-MED-Eigenschaften* können Sie globale Parameter für diese Funktion angeben.

So konfigurieren Sie globale LLDP-MED-Eigenschaften:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Discovery: LLDP-MED** > **Eigenschaften**.

SCHRITT 2 Geben Sie unter **Bestands-ID** die Bestands-ID des Switch ein, die in Bestands-TLVs bekannt gemacht wird.

SCHRITT 3 Geben Sie die Standortparameter an, um für Notrufe den physischen Standort des Switch zu identifizieren:

- **Subtyp**: Wählen Sie eine der folgenden Optionen aus, um zu konfigurieren, wie der Switch-Standort in TLVs identifiziert wird:
  - **Koordinatenbasiert**: Die Switch-URL wird anhand von GPS-Koordinaten im Hexadezimalformat identifiziert.
  - **Hausadresse**: Der Switch-Standort wird anhand einer geografischen Beschreibung des Standorts identifiziert (beispielsweise Stadt, Straße und Gebäude).
  - **ELIN**: Der Switch-Standort wird anhand seiner ELIN (Emergency Location Identification Number) identifiziert.
- **Koordinaten**: GPS-Koordinaten des Switch im Hexadezimalformat.
- **ELIN-Adresse**: Die ELIN-Nummer.
- **Land**: Das Land, in dem sich die Stadt befindet.
- **Stadt**: Die Stadt, in der sich die Straße befindet.
- **Straße**: Die Straße, in der sich das Gebäude befindet.
- **Gebäude**: Das Gebäude, in dem sich der Switch befindet.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren von LLDP-MED an einem Port

Das LLDP-MED-Protokoll (LLDP for Media Endpoint Devices) bietet Erweiterungen für den LLDP-Standard für Netzwerkkonfiguration und -richtlinien, Gerätestandort, Power-over-Ethernet-Verwaltung und Bestandsverwaltung.

Auf der Seite *LLDP-MED-Porteinstellungen* können Sie den LLDP-MED-Betrieb an Ports anzeigen und konfigurieren.

So konfigurieren Sie diese Einstellungen an einem Port:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **Discovery: LLDP-MED** > **LLDP MED-Porteinstellungen**.

In jedem Eintrag in der LLDP-MED-Port-Einstellungstabelle wird die LLDP-MED-Konfiguration für einen Port angezeigt.

SCHRITT 2 Wählen Sie den zu konfigurierenden Port aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie für den ausgewählten Port Folgendes an:

- **LLDP-MED-Status**: Wählen Sie diese Option aus, um den LLDP-MED-Betrieb am Port zu aktivieren.
- **Konfigurationsbenachrichtigung**: Wählen Sie diese Option aus, damit der Switch Benachrichtigungen sendet, wenn Topologie-Änderungen am Netzwerk vorgenommen werden.

SCHRITT 4 Wählen Sie die verfügbaren TLVs aus, die in den LLDP-Bekanntmachungen des Ports enthalten sein sollen:

- **Netzwerkrichtlinie**: Die VLAN-ID, der Wert für die 802.1p-Serviceklasse und der DSCP-Wert (Differentiated Services Code Point). Diese Informationen werden zum Implementieren der Voice-VLAN-Funktion verwendet (siehe **Sprache und Medien**).
- **Standort**: Die GPS-Standortkoordinaten des Switch im Hexadezimalformat.
- **PSE**: Gibt an, ob der Port sich als PSE-Gerät (Power Sourcing Equipment) bekannt macht, das ein angeschlossenes Power-over-Ethernet-Gerät mit Strom versorgen kann. Diese Option wird nur bei SG 200-08p-Geräten angezeigt.
- **PD**: Gibt an, ob sich der Port als PD-Gerät (Powered Device) bekannt macht, das Power-over-Ethernet empfangen kann. Diese Option können Sie nur für Port g1 von SG 200-08-Geräten auswählen.
- **Bestand**: Versionsinformationen für Hardware und Software.
- **Systemfunktionen**: Identifiziert die grundlegende Funktionalität des Switch (beispielsweise Bridging).

SCHRITT 5 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

HINWEIS Sie können auf **Netzwerkrichtlinie konfigurieren** klicken, um die Seite *Medien-VLAN* anzuzeigen. (Sie können auch im Navigationsfenster auf **VLAN-Verwaltung > Sprache und Medien > Medien-VLAN** klicken.) Auf dieser Seite können Sie LLDP-MED-Anwendungen VLANs zuweisen und Prioritätseinstellungen für den zugehörigen Verkehr konfigurieren.

LLDP-MED-Port-Statusdetails

Auf der Seite *LLDP-MED-Port-Statusdetails* wird die LLDP-MED-Konfiguration für alle Ports angezeigt, an denen die Funktion aktiviert ist. Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **Administration** > **Discovery: LLDP-MED** > **LLDP-MED-Port-Statusdetails**.

Wählen Sie einen Port aus der Port-Liste aus. In der Netzwerkrichtlinientabelle werden die Felder für die einzelnen Dienste oder Richtlinien angezeigt, die über LLDP bekannt gemacht werden:

- **Medienrichtlinien-Anwendungstyp**: Der Typ des der LLDP-Netzwerkrichtlinie zugeordneten Dienstes (beispielsweise Sprache).
- **VLAN-ID**: Die der Netzwerkrichtlinie zugeordnete VLAN-ID.
- **Priorität**: Der der Netzwerkrichtlinie zugeordnete 802.1p-Serviceklassenwert.
- **DSCP**: Der DSCP-Wert für die Netzwerkrichtlinie.
- **Mit Tag**: Die Netzwerkrichtlinie ist für VLANs mit Tag definiert.

Die folgenden Switch-Parameter werden in Bestands-TLVs bekannt gemacht.

- **Hardware-Version**: Versions-ID der Switch-Hardware.
- **Firmware-Version**: Die Versionsnummer der Switch-Firmware.
- **Software-Version**: Die Versionsnummer der Switch-Software.
- **Seriennummer**: Die Seriennummer des Switch.
- **Herstellername**: Der Name des Herstellers des Geräts.
- **Modellname**: Der Modellname des Switch.
- **Bestands-ID**: Die LLDP-MED-Bestands-ID für den Switch.

Die folgenden Switch-Parameter werden in System-TLVs bekannt gemacht.

- **Geräte-ID**: Die Hardwareadresse des Switch.
- **Geräte-ID-Subtyp**: Der Typ der Hardwareadresse.
- **Systembeschreibung**: Eine vorkonfigurierte Systembeschreibung.
- **Systemname**: Der vom Benutzer konfigurierte Hostname (siehe Seite *Systemeinstellungen*).
- **Verwaltungsadressen-Subtyp**: Die Protokollversion für die Verwaltungs-IP-Adresse.
- **Verwaltungsadresse**: Die IP-Adresse des Verwaltungs-Ports (siehe Seite *IPv4-Schnittstelle* oder *IPv6-Schnittstelle*).
- **Port-ID-Subtyp**: Der Typ der Port-ID.
- **Port-ID**: Die Port-ID.
- **Port-Beschreibung**: Die Port-Beschreibung.
- **Aktivierte Systemfunktionen**: Die im Switch aktivierten Funktionen.
- **Unterstützte Systemfunktionen**: Die Funktionen, die zurzeit als vom Switch unterstützt bekannt gemacht werden.

Die folgenden Switch-Parameter werden in Standort-TLVs bekannt gemacht.

- **Subtyp**: Der unterstützte Standortinformationstyp (Hausadresse, ELIN oder koordinatenbasiert).
- **Koordinaten**: Die GPS-Koordinaten des Switch im Hexadezimalformat, wenn der koordinatenbasierte Standortinformationstyp verwendet wird.
- **ELIN-Adresse**: Die ELIN-Nummer, wenn dieser Standortinformationstyp verwendet wird.
- **Land**: Das Land, in dem sich die Stadt befindet, wenn der Standortinformationstyp „Hausadresse“ verwendet wird.
- **Stadt**: Die Stadt, in der sich die Straße befindet, wenn der Standortinformationstyp „Hausadresse“ verwendet wird.
- **Straße**: Die Straße, in der sich das Gebäude befindet, wenn der Standortinformationstyp „Hausadresse“ verwendet wird.
- **Gebäude**: Das Gebäude, in dem sich der Switch befindet, wenn der Standortinformationstyp „Hausadresse“ verwendet wird.

LLDP-MED-Nachbarinformationen

Auf der Seite *Nachbarinformationen* werden Informationen angezeigt, die von anderen LLDP-MED-fähigen Geräten im Netzwerk empfangen wurden. Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **Administration** > **Erkennung - LLDP-MED** > **Nachbarinformationen**.

In der Nachbarinformationentabelle werden die folgenden Felder für die einzelnen LLDP-Nachbargeräte angezeigt, für die eine Bekanntmachung empfangen wurde:

- **Lokaler Port**: Die Port-Nummer des lokalen Geräts, an der die LLDP-Bekanntmachung empfangen wurde.
- **Remote-ID**: Die physische Adresse des Ports am Nachbargerät.
- **Geräteklasse**: Die bekannt gemachte Klasse des Remote-Geräts.

Sie können einen Eintrag auswählen und auf **Details** klicken, um zusätzliche Informationen aus der LLDP-MED-Bekanntmachung des Nachbarn anzuzeigen.

Auf der Seite *Details der Nachbarinformationen* werden die folgenden Informationen angezeigt:

MED-Funktionen:

- **Gemeldete Funktionen**: Die bekannt gemachten Funktionen des Geräts.
- **Aktivierte Funktionen**: Die bekannt gemachten im Gerät aktivierten Funktionen.
- **Geräteklasse**: Die bekannt gemachte Klasse des Remote-Geräts.

Netzwerkrichtlinien:

- **Medienrichtlinien-Anwendungstyp**: Der Typ des der LLDP-Netzwerkrichtlinie zugeordneten Dienstes (beispielsweise Sprache).
- **VLAN-ID**: Die der Netzwerkrichtlinie zugeordnete VLAN-ID.
- **Priorität**: Der der Netzwerkrichtlinie zugeordnete 802.1p-Serviceklassenwert.
- **DSCP**: Der DSCP-Wert für die Netzwerkrichtlinie.
- **Unbekannt**: Für diese Netzwerkrichtlinie ist weder der 802.1p-Wert noch der DSCP-Wert konfiguriert.
- **Mit Tag**: Die Netzwerkrichtlinie ist für VLANs mit Tag definiert.

Bestand:

- **Hardware-Version**: Versions-ID der Switch-Hardware.
- **Firmware-Version**: Die Versionsnummer der Switch-Firmware.
- **Software-Version**: Die Versionsnummer der Switch-Software.
- **Herstellername**: Der Name des Herstellers des Geräts.
- **Modellname**: Der Modellname des Switch.
- **Bestands-ID**: Die LLDP-MED-Bestands-ID für den Switch.

Standort:

- **Subtyp**: Wählen Sie eine der folgenden Optionen aus, um zu konfigurieren, wie der Switch-Standort in TLVs identifiziert wird:
  - **Koordinatenbasiert**: Die Switch-URL wird anhand von GPS-Koordinaten im Hexadezimalformat identifiziert.
  - **Hausadresse**: Der Switch-Standort wird anhand einer geografischen Beschreibung des Standorts identifiziert (beispielsweise Stadt, Straße und Gebäude).
  - **ELIN**: Der Switch-Standort wird anhand seiner ELIN (Emergency Location Identification Number) identifiziert.
- **Standortinformationen**: Standortinformationen für den Switch in dem im Feld „Subtyp“ angegebenen Format.

Erweitertes PoE:

- **PoE-Gerätetyp**: Wenn die PoE-Funktionalität bekannt gemacht wird, gibt dieses Feld an, ob es sich bei dem Gerät um ein PD-Gerät (Powered Device) oder um ein PSE-Gerät (Power Sourcing Equipment) handelt.

Erweitertes PoE-PD:

Wenn das Gerät über PoE mit Strom versorgt wird, können die folgenden Eigenschaften bekannt gemacht werden:

- **PoE-Stromwert**: Der vom Gerät angeforderte Netzstrom in Watt.
- **PoE-Stromquelle**: Gibt an, wie das PD-Gerät (Powered Device) mit Strom versorgt wird:
  - **Primär**: Das Gerät ist direkt an eine Stromversorgung angeschlossen.
  - **Backup**: Das Gerät wird über ein PoE-PSE-Gerät mit Strom versorgt.
- **PoE-Stromprioritität**: Gibt mit „Hoch“, „Niedrig“ oder „Kritisch“ an, welche Priorität dem Port zugewiesen wird, wenn nicht so viel PoE-Strom bereitgestellt werden kann wie von allen PD-Geräten angefordert.

Konfigurieren von DHCP-Client-Lieferantenoptionen

Sie können die DHCP-Clientfunktionalität im Switch so konfigurieren, dass die DHCP-Anforderungen Lieferanteninformationen enthalten (DHCP-Option 60). Ein DHCP-Server kann Lieferanteninformationen verwenden, um Clients anhand des Typs oder der Funktionalität der Hardware zu unterscheiden.

So konfigurieren Sie die Zeichenkette für DHCP-Lieferantenoptionen:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Administration** > **DHCP-Optionen**.

Neben der Lieferantenoption und der Zeichenkette wird auf der Seite das Format angezeigt, das der Switch beim Beziehen der Zeitzoneninformationen von einem DHCP-Server verwendet. Außerdem wird angegeben, ob solche Informationen empfangen wurden. Informationen zum Konfigurieren des Switch zum Beziehen der Zeitzone über DHCP finden Sie unter **Zeiteinstellungen**.

SCHRITT 2 Wählen Sie für die Lieferantenoption „Aktivieren“ aus.

SCHRITT 3 Geben Sie in das Textfeld „Zeichenkette für Lieferantenoptionen“ einen Wert ein.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

4

Portverwaltung

In diesem Kapitel wird das Konfigurieren von Switch-Porteinstellungen, das Kombinieren von Ports in Link-Aggregationsgruppen und das Konfigurieren von Funktionen für die Stromversorgung des Ports beschrieben.

Folgende Themen sind enthalten:

- **Konfigurieren von Porteinstellungen**
- **Link-Aggregation**
- **Konfigurieren von PoE**
- **Green Ethernet**

Konfigurieren von Porteinstellungen

Auf der Seite *Porteinstellungen* können Sie administrativ Ports aktivieren und deaktivieren und die automatische Aushandlung der Port-Geschwindigkeit und des Duplex-Modus konfigurieren. Außerdem können Sie auf dieser Seite die Flusskontrolle für den Port konfigurieren.

So konfigurieren Sie Porteinstellungen:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Portverwaltung** > **Porteinstellungen**.

SCHRITT 2 Wählen Sie die zu konfigurierende Schnittstelle aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie für den ausgewählten Port Folgendes an:

- **Administrativer Status**: Wählen Sie „Ein“ aus, um den Port zu aktivieren, oder „Aus“, um den Port zu deaktivieren.

- **Autom. Aushandlung**: Wählen Sie „Aktivieren“ aus, damit der Switch die Port-Geschwindigkeit und den Duplex-Modus mit dem verbundenen Gerät automatisch aushandeln kann. Wenn die automatische Aushandlung aktiviert ist, können Sie die Felder „Geschwindigkeit von Administrations-Port“ und „Duplex-Modus“ nicht bearbeiten.
- **Geschwindigkeit von Administrations-Port**: Wenn die automatische Aushandlung deaktiviert ist, wählen Sie aus, ob der Port den Betrieb mit 10 Mbit/s oder 100 Mbit/s unterstützt.
- **Administrativer Duplex-Modus**: Wenn die automatische Aushandlung deaktiviert ist, wählen Sie „Halb“ für den Betrieb im Halbduplex-Modus oder „Voll“ für den Betrieb im Vollduplex-Modus aus.
- **Administrator-Ankündigung**: Wenn die automatische Aushandlung aktiviert ist, wählen Sie die höchste Port-Geschwindigkeit und Duplex-Einstellung aus, die der Port aushandeln soll. Wenn Sie „Max. Leistungsfähigkeit“ auswählen, handelt der Port automatisch maximal die höchste von der Hardware unterstützte Port-Geschwindigkeit und Duplex-Einstellung aus.
- **Flusssteuerung**: Wählen Sie diese Option aus, um die IEEE 802.3x-Flusskontrolle zu aktivieren. Die Flusskontrolle trägt zur Vermeidung von Datenverlusten bei, wenn der Port mit der Menge der vermittelten Pakete nicht Schritt halten kann. Wenn diese Option aktiviert ist, kann der Switch einen PAUSE-Frame senden, um den Verkehr an einem Port anzuhalten, wenn die von den Paketen am Port verwendete Speichermenge einen vorkonfigurierten Schwellenwert überschreitet. Während des im PAUSE-Frame angegebenen Zeitraums werden von dem angehaltenen Port keine Pakete weitergeleitet. Wenn der im PAUSE-Frame angegebene Zeitraum verstrichen ist oder die Auslastung zu einem angegebenen niedrigen Schwellenwert zurückkehrt, lässt der Switch die Übertragung von Frames durch den Port wieder zu.
- **Mitglied in LAG**: Gibt an, ob der Port Mitglied einer Link-Aggregationsgruppe ist. Informationen zum Konfigurieren von LAGs finden Sie unter **Link-Aggregation**.
- **MTU**: Gibt die MTU-Größe (Maximum Transmission Unit, Maximale Übertragungseinheit) in Byte an. Die Standard-MTU beträgt 1518. Gültig sind Werte im Bereich zwischen 1518 und 9216 Byte.

SCHRITT 4 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Link-Aggregation

Mithilfe von Link-Aggregation können Sie einen oder mehrere Ethernet-Links mit Vollduplex aggregieren, um eine Link-Aggregationsgruppe (Link Aggregation Group, LAG) zu bilden. Die LAG wird vom Switch wie ein einziger physischer Port behandelt und bietet verbesserte Fehlertoleranz und Lastenausgleichsfunktionen.

Eine LAG-Schnittstelle kann statisch oder dynamisch sein.

- **Statische LAG**: Der Administrator weist die Ports direkt einer LAG zu. Die Ports bleiben dedizierte LAG-Mitglieder, bis sie anders konfiguriert werden.
- **Dynamische LAG**: Eine dynamische LAG ist mit einem oder mehreren Kandidaten-Ports konfiguriert. Die LAG wird gebildet durch den Austausch von LACP-Dateneinheiten (Link Aggregation Control Protocol, Link-Aggregationsteuerungsprotokoll) mit dem Remote-Gerät, das eine Verbindung mit den Kandidaten-Ports herstellt. Die so gebildete LAG enthält möglicherweise abhängig von den Port-Einschränkungen für LAGs und anderen Faktoren nur eine Teilmenge der infrage kommenden Ports. Kandidaten-Ports, die nicht als aktive Mitglieder-Ports einer LAG ausgewählt sind, fungieren als Standby-Ports. Ein Standby-Port kann als aktives Mitglied ausgewählt werden, wenn ein aktiver Port in der gleichen LAG ausfällt.

Die folgenden Themen enthalten zusätzliche Informationen zu den Konfigurationsseiten im Menü „Portverwaltung > Link-Aggregation“:

- **Konfigurieren von LAGs**
- **Konfigurieren von LAG-Einstellungen**
- **Konfigurieren von LACP-Einstellungen**

Konfigurieren von LAGs

Der Switch unterstützt bis zu 4 LAGs mit 8 Ports pro LAG. Auf der Seite *LAG-Verwaltung* können Sie LAGs und LACPs Ports zuweisen.

Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **Portverwaltung** > **Link-Aggregation** > **LAG-Verwaltung**.

Standardmäßig sind vier dynamische LAGs mit den Standardnamen *ch1* bis *ch4* vorkonfiguriert. Diese LAGs haben keine Port-Mitglieder und sind deaktiviert.

Sie können einer LAG Ports hinzufügen oder Ports aus einer LAG entfernen, ohne den Verkehr in der LAG zu stören.

Sie können LAGs die Mitgliedschaft in VLANs zuweisen; einzelne Ports verlieren jedoch durch die LAG-Mitgliedschaft ihre individuellen VLAN-Mitgliedschaften. Wenn Sie einen Port aus einer LAG entfernen, tritt dieser wieder den VLANs bei, zu denen er gemäß der Startkonfiguration vorher gehörte.

So konfigurieren Sie eine LAG:

SCHRITT 1 Wählen Sie die zu konfigurierende LAG aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 2 Geben Sie für die ausgewählte LAG Folgendes an:

- **LAG-Name**: Geben Sie bis zu 15 alphanumerische Zeichen ein, um die LAG zu identifizieren.
- **Typ**: Wählen Sie „Statisch“ aus, um der LAG manuell Ports zuzuweisen. Wählen Sie „Dynamisch“ aus, damit die Ports LACPDUs austauschen können, um die LAG dynamisch zu bilden.
- **Port-Liste/LAG-Mitglieder**: Um einer statischen LAG Ports hinzuzufügen bzw. Ports aus einer statischen LAG zu entfernen, wählen Sie die einzelnen Ports aus. Klicken Sie auf den nach links oder nach rechts zeigenden Pfeil, um den Port zwischen der Port-Liste und der LAG-Mitgliederliste zu verschieben.

SCHRITT 3 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren von LAG-Einstellungen

Auf der Seite *LAG-Einstellungen* können Sie eine LAG administrativ aktivieren oder deaktivieren und Einstellungen für den Lastenausgleich konfigurieren.

So konfigurieren Sie LAG-Einstellungen:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Portverwaltung** > **Link-Aggregation** > **LAG-Einstellungen**.

In der LAG-Einstellungstabelle werden alle verfügbaren LAGs aufgeführt.

SCHRITT 2 Wählen Sie die zu konfigurierende LAG aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie für die ausgewählte LAG Folgendes an:

- **Administrativer Status**: Wählen Sie „Ein“ bzw. „Aus“ aus, um die LAG administrativ zu aktivieren oder zu deaktivieren. Wenn eine LAG deaktiviert ist, fungieren die Mitglieder-Ports als eigenständige physische Ports.
- **Lastausgleichslogarithmus**: Wählen Sie eine der Optionen aus, damit der Switch für ausgehende Pakete einen Lastenausgleich zwischen den Mitglieder-Ports einer LAG ausführt. Der Switch wählt einen der Links im Kanal für die Übermittlung eines bestimmten Pakets aus. Die Kriterien für den Lastenausgleich werden in der in der Option aufgelisteten Reihenfolge priorisiert. Folgende Optionen sind möglich:
  - **Quelle/Ziel MAC, VLAN, ETyp, Eingangsport**: Quell- und Ziel-MAC-Adressen, VLAN-Mitgliedschaft, das Ethertype-Feld und der Port, an dem das Paket empfangen wurde.
  - **Felder Quell-/Ziel-IP und TCP/UDP-Port (Quell-IP)**: Quell- und Ziel-IP-Adresse und die TCP- oder UDP-Port-Nummer im IP-Paket.

  Wenn die Option für IP-Pakete ausgewählt ist, wird der Lastenausgleich für am Port empfangene Nicht-IP-Pakete anhand der Quell- und Ziel-MAC-Adresse ausgeführt.
- **MTU**: Gibt die MTU-Größe (Maximum Transmission Unit, Maximale Übertragungseinheit) in Byte an. Die Standard-MTU beträgt 1518. Gültig sind Werte im Bereich zwischen 1518 und 9216 Byte.

SCHRITT 4 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren von LACP-Einstellungen

Der Switch automatisiert die Bildung dynamischer LAGs mithilfe des Link-Aggregationsteuerungsprotokolls (Link Aggregation Control Protocol, LACP). LACP-fähige Ports senden Protokolldateneinheiten (LACPDUs), um sich gegenseitig in einem Netzwerk zu erkennen und eine LAG auszuhandeln.

Auf der Seite *LACP* können Sie die Protokollfunktion anzeigen und konfigurieren.

So konfigurieren Sie LACP-Einstellungen für einzelne Ports:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Portverwaltung** > **Link-Aggregation** > **LACP**.

In der LACP-Schnittstellentabelle werden die lokalen LACP-Konfigurationen (aktiver Port) und Remote-LACP-Konfigurationen (Partner-Port) für die einzelnen Ports am Switch angezeigt. Zu den Einstellungen für den aktiven LACP-Port gehören die Systempriorität für den Switch und der Admininistrationsschlüssel, durch den der Port in LACP-Nachrichten eindeutig identifiziert wird. Diese Werte sind nicht konfigurierbar.

So bearbeiten Sie die LACP-Einstellungen:

SCHRITT 1 Wählen Sie den zu konfigurierenden Port aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 2 Konfigurieren Sie die folgenden Einstellungen für den ausgewählten Port:

- **Modus**: Aktivieren Sie das Kontrollkästchen, um LACP für den Port zu aktivieren.
- **Timeout für aktiven Port**: Die Informationen vom aktiven Port sind nach Ablauf des Timeout-Zeitraums nicht mehr gültig.
  - **Kurz**: Das kurze LACP-Timeout entspricht dem Dreifachen des kurzen periodischen Timers für die Übertragung von LACP-Paketen. Der Standardwert für das kurze LACP-Timeout beträgt 3 Sekunden.
  - **Lang**: Das lange LACP-Timeout entspricht dem Dreifachen des langen periodischen Timers für die Übertragung von LACP-Paketen. Der Standardwert für das lange LACP-Timeout beträgt 90 Sekunden.
- **Partner-Timeout**: Die Informationen vom Partner sind nach Ablauf des Timeout-Zeitraums nicht mehr gültig.
  - **Kurz**: Das kurze LACP-Timeout entspricht dem Dreifachen des kurzen periodischen Timers für die Übertragung von LACP-Paketen. Der Standardwert für das kurze LACP-Timeout beträgt 3 Sekunden.
  - **Lang**: Das lange LACP-Timeout entspricht dem Dreifachen des langen periodischen Timers für die Übertragung von LACP-Paketen. Der Standardwert für das lange LACP-Timeout beträgt 90 Sekunden.

SCHRITT 3 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren von PoE

Beim SG 200-08P können die Ports 1 - 4 als PoE-PSE-Ports betrieben werden. Ein PSE kann angeschlossene PoE-PD-Geräte (Powered Devices) mit Strom versorgen.

Für die Switches SG 200-08P finden Sie Informationen zu den Konfigurationsseiten im Menü „Portverwaltung > PoE“ in den folgenden Themen:

- **Konfigurieren von PoE-Eigenschaften**
- **Konfigurieren von PoE-Porteinstellungen**

HINWEIS Diese Konfigurationsseiten werden für Switches ohne Unterstützung für die PSE-Funktionalität nicht angezeigt.

Konfigurieren von PoE-Eigenschaften

Auf der Seite *Eigenschaften* können Sie konfigurieren, ob der Switch unter bestimmten Umständen Trap-Nachrichten generiert, und die aktuellen Leistungseinstellungen anzeigen.

So konfigurieren Sie PoE-Eigenschaften:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Portverwaltung** > **PoE** > **Eigenschaften**.

SCHRITT 2 Legen Sie die folgenden Parameter fest:

- **Schwellenwert für Leistungs-Trap**: Geben Sie einen Prozentanteil der insgesamt verfügbaren Systemleistung an. Wenn die an PoE-Ports angeforderte Leistung den Schwellenwert übersteigt, wird im Protokoll ein Trap generiert.
- **Energieverwaltungsmodus**: Wählen Sie aus, wie der Switch die an mehreren Ports bereitgestellte Leistung priorisieren soll:
  - **Statisch mit Port-Priorität**: Statisch mit Energieverwaltung und Priorisierung. Dieser Algorithmus weist die Leistung vorab auf der Basis des konfigurierten Leistungslimits und der Priorität des Ports zu.
  - **Dynamisch mit Port-Priorität**: Dynamisch mit Energieverwaltung und Priorisierung. Dieser Algorithmus versorgt Geräte mit Strom, solange der Verbrauch die konfigurierten Werte für Limit und Priorität nicht übersteigt. Eine Vorabzuweisung der Leistung erfolgt nicht.

In beiden Modi hat ein Port mit einer höheren Port-Priorität Vorrang, wenn der Switch mehrere Ports mit Strom versorgt. Wenn zwei oder mehr Port-Prioritäten gleich sind, hat der Port mit der niedrigeren Port-Nummer Vorrang.

- **Modus zurücksetzen**: Wählen Sie „Aktivieren“ aus, damit der Switch den Status der Geräte an allen PoE-Ports initialisieren kann.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

HINWEIS Auf dieser Seite werden die folgenden Daten für die PoE-Leistung des Switch angezeigt:

- **Leistung:** Der aktuelle Leistungsstatus. *Ein*: Der Switch versorgt zurzeit ein angeschlossenes Gerät über PoE mit Strom. *Aus*: Der Switch versorgt zurzeit kein angeschlossenes Gerät über PoE mit Strom.
- **Nennleistung**: Die Gesamtleistung in Watt, die der Switch für alle angeschlossenen PD-Geräte bereitstellen kann.
- **Leistungsschwellenwert**: Wenn dieser Schwellenwert überschritten ist, werden keine weiteren PD-Geräte mehr mit Strom versorgt. Der Schwellenwert wird auf der Basis der Einstellung „Schwellenwert für Leistungs-Trap“ berechnet.
- **Verbrauchte Leistung**: Die insgesamt vom Switch für PoE-Ports bereitgestellte Leistung in Watt.

Konfigurieren von PoE-Porteinstellungen

Auf der Seite *Porteinstellungen* können Sie Einstellungen für als PSEs fungierende Ports anzeigen und konfigurieren.

So konfigurieren Sie PoE-Einstellungen für einen Port:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Portverwaltung** > **PoE** > **Porteinstellungen**.

In der PoE-Einstellungstabelle wird angezeigt, welche Ports für den PoE-Betrieb aktiviert sind. Außerdem sehen Sie für jeden Port die Priorität, die Leistungszuweisung in Milliwatt und weitere Einstellungen.

SCHRITT 2 Wählen Sie den zu konfigurierenden Port aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Konfigurieren Sie die folgenden Einstellungen:

- **PoE**: Aktivieren Sie das Kontrollkästchen „Aktivieren“, um den Port als PSE zu konfigurieren.
- **Leistungsprioritätsstufe**: Wählen Sie „Kritisch“, „Hoch“ oder „Niedrig“ aus, um die Port-Prioritätsstufe für die Stromversorgung eines angeschlossenen Geräts zu konfigurieren.

  Der Switch kann möglicherweise nicht für alle angeschlossenen Geräte die angeforderte Leistung bereitstellen. Wenn die Leistungskapazität nicht für alle aktivierten Ports ausreicht, bestimmt die Port-Priorität, welche Ports Leistung bereitstellen. Bei Ports mit gleicher Prioritätsstufe hat der Port mit der niedrigeren Nummer die höhere Priorität. Wenn bei einem System, das eine bestimmte Anzahl von Geräten mit der Höchstleistung versorgt, ein neues Gerät an einem Port mit hoher Priorität angeschlossen wird, wird die Stromversorgung eines Geräts mit einem Port mit niedrigerer Priorität eingestellt, und das neue Gerät wird mit Strom versorgt.
- **Art der Leistungsbegrenzung**: Wählen Sie eine der folgenden Methoden aus, um die Leistung zu begrenzen, die der Switch einem angeschlossenen Gerät bereitstellt.
  - **Dot3AF**: Die maximale Leistung, die vom Port bereitgestellt werden kann, wird durch die erkannte IEEE 802.3af-Klasse begrenzt.
  - **Benutzerdefiniert**: Der Benutzer gibt die maximale Leistung an, die vom Port bereitgestellt werden kann. Wenn Sie diese Option auswählen, müssen Sie im Feld „Leistungszuweisung“ einen Wert angeben.
  - **LLDP-MED**: Die maximale Leistung, die vom Port bereitgestellt werden kann, wird durch den Wert in den von einem Port-Gerät empfangenen LLDP-MED-TLVs begrenzt. Der vom Gerät angegebene Wert muss sich im Bereich von 3 - 16,2 Watt befinden. Anderenfalls wird der Standardwert 16,2 Watt verwendet.

    Hinweis: Wenn für das Leistungslimit der Typ „LLDP-MED“ ausgewählt ist, wird die Prioritätseinstellung des Remote-Geräts nicht beachtet; stattdessen verwendet der Switch die für den Port konfigurierte Einstellung für die Leistungsprioritätsstufe.
  - **Dot3AF und LLDP-MED**: Die maximale Leistung, die vom Port bereitgestellt werden kann, wird durch den Wert in den von einem Port-Gerät empfangenen LLDP-MED-TLVs begrenzt. Der vom Gerät angegebene Wert muss sich im Bereich von 3 - 16,2 Watt befinden. Anderenfalls wird die maximale Leistung durch die IEEE 802.3AF-Klasse begrenzt.

  - **Benutzerdefiniert und LLDP-MED**: Die maximale Leistung, die vom Port bereitgestellt werden kann, wird durch den Wert in den von einem Port-Gerät empfangenen LLDP-MED-TLVs begrenzt. Der vom Gerät angegebene Wert muss sich im Bereich von 3 - 16,2 Watt befinden. Anderenfalls wird die maximale Leistung durch den Wert begrenzt, den Sie im Feld „Leistungszuweisung“ angeben.

- **Leistungszuweisung**: Wenn Sie für den Typ des Leistungslimits eine benutzerdefinierte Option konfiguriert haben, geben Sie die Leistung in Milliwatt ein, die Sie dem Port zuweisen möchten (zwischen 3000 und 16200 Milliwatt).
- **Erkennungstyp**: Wählen Sie eine der folgenden Methoden aus, um an den Ports angeschlossene über PoE mit Strom versorgte Geräte zu erkennen.
  - **Nur Legacy**: Es werden nur Geräte mit Kapazitäts-Signatur erkannt.
  - **Nur 802.3af 4point**: Mit dem ersten Algorithmus werden nur Geräte mit Widerstands-Signatur erkannt.
  - **802.3af 4point und Legacy**: Mit dem zweiten Algorithmus werden Geräte mit Kapazitäts-Signatur sowie Geräte mit Widerstands-Signatur erkannt.
  - **Nur 802.3af 2point**: Mit dem ersten Algorithmus werden nur Geräte mit Widerstands-Signatur erkannt.
  - **802.3af 2point und Legacy**: Mit dem ersten Algorithmus werden Geräte mit Kapazitäts-Signatur sowie Geräte mit Widerstands-Signatur erkannt.
- **Modus zurücksetzen**: Wählen Sie „Aktivieren“ aus, damit der Switch den Status der Geräte an den PoE-Ports initialisieren kann.

Außerdem werden die folgenden Statistiken angezeigt:

- **Leistungsaufnahme**: Die tatsächliche Leistungsaufnahme am Port.
- **Zähler für Überlastung**: Die Gesamtanzahl der Ereignisse, bei denen die Leistungsversorgung überlastet wurde.
- **Zähler für Kurz**: Die Gesamtanzahl der Ereignisse, bei denen ein elektrischer Kurzschluss an einem Port aufgetreten ist.
- **Zähler für Verweigert**: Die Anzahl der Ereignisse, bei denen dem PD-Gerät die Leistung verweigert wurde.

- **Zähler für Nicht vorhanden**: Die Anzahl der Ereignisse, bei denen die Leistungsversorgung des PD-Geräts unterbunden wurde, weil dieses nicht mehr erkannt wurde.
- **Zähler für ungültige Signaturen**: Die Anzahl der Ereignisse, bei denen eine ungültige Signatur empfangen wurde. Signaturen werden von PD-Geräten verwendet, um sich beim PSE zu identifizieren. Eine Signatur wird bei der Erkennung, Klassifizierung oder Wartung eines PD-Geräts generiert.

SCHRITT 4 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Green Ethernet

Über die Gigabit Ethernet-Kupfer-Ports des Switch können die Green Ethernet-Energiesparfunktionen genutzt werden. Zu den Green Ethernet-Funktionen gehören:

- **Energieerkennungsmodus**: Trägt dazu bei, den Stromverbrauch des Chips zu reduzieren, indem ein Port-PHY gezwungen wird, in einen Energiesparmodus zu wechseln, wenn kein Signal von einem Kupfer-Link-Partner vorliegt.

  Bei aktivierter Energieerkennung wechselt der Switch automatisch in den Energiesparmodus, wenn in der Leitung keine Energie vorhanden ist, und nimmt den Normalbetrieb wieder auf, wenn Energie erkannt wird. Wenn sich der Port-PHY im Energiesparmodus befindet, wacht der PHY nach einer bestimmten Zeit auf und überwacht durch Senden von Link-Impulsen, ob Energie vom Link-Partner vorliegt. Wenn Energie erkannt wird, während sich der Port im Aufwachmodus befindet, nimmt der Switch den Normalbetrieb am Port wieder auf. Nach Ablauf des Aufwachzeitraums kehrt der Port in den Energiesparmodus zurück.
- **Automatischer Modus bei kurzer Reichweite**: Wenn diese Funktion aktiviert ist, wird bei Aktivierung eines Links ein Kabeltest ausgeführt. Wenn ein kurzes Kabel erkannt wird, wechselt der Port in den Energiesparmodus. Wenn die Verbindung getrennt wird, wird der Energiesparmodus deaktiviert.

Der Switch unterstützt außerdem die Konfiguration der Funktion „Kurze Reichweite“, mit der die Kabellänge ermittelt wird. Wenn die Kabellänge weniger als 10 Meter beträgt, wird der PHY in den Energiesparmodus versetzt, sodass nur für ein kurzes Kabel ausreichender Strom verbraucht wird. Es gibt zwei Möglichkeiten zum Konfigurieren der Funktion „Kurze Reichweite“:

- **Kurze Reichweite – automatisch**: Der Kabeltest wird automatisch ausgeführt, wenn der Link aktiv wird, und wenn ein kurzes Kabel erkannt wird, wird der Port-PHY in den Energiesparmodus versetzt. Wenn die Verbindung getrennt wird, wird der Energiesparmodus deaktiviert.
- **Kurze Reichweite erzwingen**: Der Port wird administrativ gezwungen, in den Energiesparmodus für Kabel mit kurzer Reichweite zu wechseln.

Die Green Ethernet-Funktionen sind unabhängig davon, ob automatische Aushandlung für den Port aktiviert oder deaktiviert ist, und können vom Administrator aktiviert bzw. deaktiviert werden. Die Eigenschaften des Green Ethernet-Modus können pro Port konfiguriert werden.

Konfigurieren von Green Ethernet-Eigenschaften

Auf der Seite *Green Ethernet-Eigenschaften* können Sie die Green Ethernet-Funktionalität global aktivieren. Die globalen Einstellungen werden auf alle Ports angewendet.

HINWEIS Sie können die globalen Einstellungen außer Kraft setzen, indem Sie diese Funktionen für einzelne Ports konfigurieren (siehe **Konfigurieren von Green Ethernet-Porteinstellungen**); spätere Änderungen an den globalen Eigenschaften setzen jedoch alle individuellen Port-Konfigurationen außer Kraft.

So konfigurieren Sie globale Green Ethernet-Eigenschaften:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Portverwaltung** > **Green Ethernet** > **Eigenschaften**.

Standardmäßig sind der Energieerkennungsmodus und der automatische Modus bei kurzer Reichweite global und für alle Ports aktiviert.

SCHRITT 2 Konfigurieren Sie die folgenden Einstellungen:

- **Energieerkennung**: Wählen Sie „Aktivieren“ aus, um den Energieerkennungsmodus im Switch zu aktivieren. Der Switch wechselt automatisch in den Energiesparmodus, wenn in der Leitung keine Energie vorhanden ist, und nimmt den Normalbetrieb wieder auf, wenn Energie erkannt wird.
- **Kurze Reichweite – automatisch**: Wählen Sie „Aktivieren“ aus, damit automatisch der Kabeltest ausgeführt wird, wenn der Link aktiv wird. Wenn ein kurzes Kabel erkannt wird, wechselt der Port in den Energiesparmodus. Wenn die Verbindung getrennt wird, wird der Energiesparmodus deaktiviert.
- **Kurze Reichweite erzwingen**: Wählen Sie „Aktivieren“ aus, um administrativ zu erzwingen, dass alle Ports standardmäßig in den Energiesparmodus für Kabel mit kurzer Reichweite wechseln. Diese Einstellung kann außer Kraft gesetzt werden.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren von Green Ethernet-Porteinstellungen

Auf der Seite *Green Ethernet-Einstellungen* können Sie die Green Ethernet-Einstellungen für einzelne Ports anzeigen und konfigurieren.

HINWEIS Die Green Ethernet-Porteinstellungen werden außer Kraft gesetzt, wenn die globalen Einstellungen später geändert werden (siehe **Konfigurieren von Green Ethernet-Eigenschaften**).

So konfigurieren Sie Green Ethernet-Porteinstellungen:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Portverwaltung** > **Green Ethernet** > **Porteinstellungen**.

In der Tabelle für Green Ethernet-Einstellungen werden für jeden Port die folgenden Informationen angezeigt:

Felder unter „Energieerkennung“:

- **Administrator**: Gibt an, ob die Energieerkennung für den Port aktiviert ist.
- **Operativ**: Gibt an, ob der Energieerkennungsmodus am Port zurzeit in Betrieb ist („Aktiviert“).

- **Grund**: Gibt an, aus welchem Grund der Betriebsstatus aktiviert oder deaktiviert ist. Der folgende Grund kann angezeigt werden, wenn der Betriebsstatus der Energieerkennung „Aktiviert“ entspricht:
  - **Keine Energie erkannt**: Im Link wird keine Energie erkannt.

  Die folgenden Gründe können angezeigt werden, wenn der Betriebsstatus der Energieerkennung „Deaktiviert“ entspricht:
  - **Port im Glasfasermodus**: Möglicherweise ist der Administrationsstatus aktiv, aber der Port funktioniert im Glasfasermodus. (Die Green Ethernet-Funktionalität gilt nur für Kupfer-Ports.)
  - **Link ist aktiv**: Im Link liegen Aktivitäten vor.
  - **Administrationsmodus deaktiviert**: Der Energieerkennungsmodus wurde administrativ deaktiviert.

Felder unter „Kurze Reichweite“:

- **Automatisch**: Gibt an, ob der Modus „Kurze Reichweite“ administrativ am Port aktiviert ist.
- **Erzwingen**: Gibt an, ob der Modus „Kurze Reichweite erzwingen“ am Port aktiviert ist.
- **Betrieb**: Gibt an, ob der Modus „Kurze Reichweite“ am Port in Betrieb (aktiviert) ist.
- **Grund**: Gibt an, aus welchem Grund der Betriebsstatus „Kurze Reichweite“ aktiv oder inaktiv ist. Der folgende Grund kann angezeigt werden, wenn der Betriebsstatus „Kurze Reichweite“ aktiviert ist:
  - **Kurzes Kabel < 10 m**: Am Port wurden Kabel mit kurzer Reichweite erkannt.
  - **Erzwungen**: Der Modus „Kurze Reichweite“ wurde administrativ am Port erzwungen.

  Die folgenden Gründe können angezeigt werden, wenn der Betriebsstatus „Kurze Reichweite“ deaktiviert ist:
  - **Langes Kabel > 10 m**: Das Kabel ist länger als 10 m.
  - **Link inaktiv**: Der Link ist inaktiv.
  - **Glasfaser**: Der Port befindet sich im Glasfasermodus, und der Green Ethernet-Betrieb ist nicht möglich.

- **Administrationsmodus deaktiviert**: „Kurze Reichweite“ ist administrativ deaktiviert.
- **Keine GIG-Geschwindigkeit**: Der Port arbeitet nicht mit 1G-Geschwindigkeit, daher ist der Green Ethernet-Betrieb nicht möglich.
- **Kabellänge unbekannt**: Die Kabellänge konnte nicht ermittelt werden.

SCHRITT 2 Wählen Sie den zu konfigurierenden Port aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Konfigurieren Sie die folgenden Einstellungen:

- **Energieerkennung**: Wählen Sie diese Option aus, um die Energieerkennung administrativ am Port zu aktivieren.
- **Kurze Reichweite – automatisch**: Wählen Sie diese Option aus, um den Modus „Kurze Reichweite“ am Port zu aktivieren.
- **Kurze Reichweite erzwingen**: Wählen Sie diese Option aus, um den Modus „Kurze Reichweite erzwingen“ am Port zu aktivieren.

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

5

VLAN-Verwaltung

In diesem Kapitel wird das Konfigurieren virtueller VLANs beschrieben.

Das Kapitel enthält die folgenden Themen:

- **Erstellen von VLANs**
- **Konfigurieren der VLAN-Schnittstelleneinstellungen**
- **Konfigurieren der VLAN-Mitgliedschaft**
- **Konfigurieren der Port-VLAN-Mitgliedschaft**
- **Festlegen des Standard-VLAN**
- **Medien-VLAN**
- **Sprache und Medien**

Ein virtuelles LAN (VLAN) an einem Layer 2-Switch bietet einige der Vorteile von Bridging und Routing. Wie eine Bridge leitet ein VLAN-Switch Verkehr basierend auf dem Layer 2-Header weiter, was Geschwindigkeitsvorteile bietet. Wie ein Router unterteilt der VLAN-Switch das Netzwerk in logische Segmente und ermöglicht damit eine bessere Administration, Sicherheit und Verwaltung von Multicast-Verkehr.

Bei einem VLAN handelt es sich um eine Gruppe von Endstationen und die Switch-Ports, über die die Endstationen verbunden sind. Für die logische Unterteilung sind viele Gründe möglich, beispielsweise die Zugehörigkeit zu Abteilungen oder Projekten. Voraussetzung ist lediglich, dass die Endstation und der Port, mit dem die Endstation verbunden ist, zu den gleichen VLANs gehören.

Jedem VLAN in einem Netzwerk ist eine VLAN-ID zugeordnet, die im auch als VLAN-Tag bezeichneten IEEE 802.1Q-Tag im Layer 2-Header von Paketen angezeigt wird, die über ein VLAN übertragen werden. Wenn eine Endstation das Tag oder den VLAN-Teil des Tags weglässt, verwirft der erste Switch-Port, der das Paket empfängt, das Paket oder fügt ein Tag ein, das der VLAN-ID entspricht. Ein Port kann Verkehr für mehrere VLANs verarbeiten, er kann jedoch nur die Port-VLAN-ID (PVID) unterstützen.

Der Switch ist mit der VLAN-ID 1 als Standard-VLAN vorkonfiguriert. Alle Ports sind Mitglieder dieses VLAN und verwenden dessen VLAN-ID (1) als eigene PVID.

Erstellen von VLANs

Auf der Seite *VLAN erstellen* können Sie VLANs im Netzwerk definieren und konfigurieren. Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **VLAN-Verwaltung** > **VLAN erstellen**.

In der VLAN-Tabelle werden die VLAN-ID, gegebenenfalls der Name und der Typ für das vorkonfigurierte VLAN (VLAN-ID 1) sowie alle von Ihnen hinzugefügten VLANs angezeigt. Ein Port muss als Standard-VLAN konfiguriert sein. Der Typ aller Ports ist „Statisch“. Der Switch ist mit der VLAN-ID 1 als Standard-VLAN vorkonfiguriert. Alle Ports sind Mitglieder dieses VLAN und verwenden dessen VLAN-ID (1) als eigene PVID.

Wenn Sie zusätzliche VLANs erstellen, können Sie eines dieser VLANs als Standard-VLAN konfigurieren. (Informationen hierzu finden Sie unter **Festlegen des Standard-VLAN**.) Sie können das konfigurierte Standard-VLAN nicht löschen. Ein statisches VLAN können Sie löschen. VLAN-ID 1 kann jedoch nicht gelöscht werden, auch wenn dieses VLAN als statisches VLAN konfiguriert ist.

Sie können bis zu 16 VLANs erstellen und VLAN-IDs bis 4094 zuweisen. So erstellen Sie ein neues VLAN oder einen VLAN-Bereich:

SCHRITT 1 Klicken Sie auf **Hinzufügen**.

SCHRITT 2 Wählen Sie „VLAN“ aus, und geben Sie eine VLAN-ID ein.

Alternativ können Sie einen VLAN-Bereich erstellen, indem Sie „Bereich“ auswählen und die erste und letzte VLAN-ID des Bereichs eingeben.

SCHRITT 3 Wenn Sie ein einfaches VLAN erstellen, können Sie einen optionalen VLAN-Namen eingeben, an dem Sie das VLAN leicht erkennen.

SCHRITT 4 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren der VLAN-Schnittstelleneinstellungen

Auf der Seite *Schnittstelleneinstellungen* können Sie Port-Funktionen für VLAN-Tagging anzeigen und konfigurieren. Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **VLAN-Verwaltung** > **Schnittstelleneinstellungen**.

In der Schnittstellen-Einstellungstabelle wird die VLAN-Konfiguration der einzelnen Ports angezeigt. Um die VLAN-Konfiguration für Link-Aggregationsgruppen anzuzeigen, wählen Sie aus der Liste „Schnittstellentyp“ die Option „LAG“ aus.

So konfigurieren Sie VLAN-Schnittstelleneinstellungen:

SCHRITT 1 Wählen Sie den Port oder die LAG aus, den bzw. die Sie konfigurieren möchten, und klicken Sie auf **Bearbeiten**.

SCHRITT 2 Konfigurieren Sie die folgenden Einstellungen für den ausgewählten Port bzw. die ausgewählte LAG:

- **Schnittstellen-VLAN-Modus**: Wählen Sie eine Option aus, um den Port-Typ im Hinblick auf die VLAN-Mitgliedschaft und Tagging zu konfigurieren.
  - **Allgemein**: Der Port kann Mitglied eines oder mehrerer VLANs mit oder ohne Tags sein. Dieser Modus lässt sämtliche Funktionen zu, die in der IEEE 802.1Q-Spezifikation unter „VLAN Tagging“ angegeben sind.
  - **Zugriff**: Der Port kann nur Frames ohne Tag annehmen. Ein Zugriffs-Port kann nur Mitglied eines einzigen VLAN sein und verwendet die VLAN-ID als eigene Port-VLAN-ID (PVID). Zugriffs-Ports werden normalerweise zum Verbinden von Hosts verwendet, die durch die physische Verbindung mit dem Port Mitglieder des VLAN werden.
  - **Trunk**: Der Port kann nur Mitglied eines einzigen VLAN ohne Tag sein (das so genannte *native VLAN*) und kann Mitglied beliebig vieler VLANs mit Tag sein (oder Mitglied keines VLAN). Trunk-Ports werden in der Regel verwendet, um Verkehr für mehrere VLANs vom Switch an andere Netzwerkgeräte zu übertragen, beispielsweise an einen Upstream-Router oder einen Edge-Switch.
- **PVID**: Die Port-VLAN-ID gibt das Standard-VLAN an, in dem die Schnittstelle Mitglied ist. Bei Trunk-Ports wird die PVID auf die konfigurierte ID des nativen VLAN festgelegt. Bei allgemeinen Ports können Sie die PVID als beliebige gültige VLAN-ID im Switch konfigurieren. Bei Zugriffs-Ports wird die PVID auf die Zugriffs-VLAN-ID festgelegt.
- **Natives VLAN**: (nur bei Trunk-Ports) Das native VLAN identifiziert die einzige VLAN-Mitgliedschaft ohne Tag für einen Trunk-Port. Wählen Sie „Standard-VLAN“ aus, um diesen Wert auf das Standard-VLAN des Ports festzulegen, oder wählen Sie „Benutzerdefiniert“ aus, um eine andere VLAN-ID anzugeben.
- **PVID**: (nur bei allgemeinen Ports) Die Port-VLAN-ID. Die PVID entspricht der ID des VLAN, in dem ein Port Mitglied ohne Tag ist.
- **Zugriffs-VLAN**: (nur bei Zugriffs-Ports) Ein Zugriffs-Port kann nur Mitglied eines einzigen VLAN sein, das als Zugriffs-VLAN bezeichnet wird. Die Zugriffs-VLAN-ID entspricht der Port-VLAN-ID eines Zugriffs-Ports.

- **Frame-Typ**: Gibt den am Port angenommenen Frame-Typ an:
  - **Nur ohne Tag zulassen**: Nur Frames ohne Tag werden am Port angenommen. Frames mit Tag werden verworfen.
  - **Nur mit Tag zulassen**: Nur Frames mit Tag werden am Port angenommen. Frames ohne Tag werden verworfen.
  - **Alle zulassen**: Am Port werden sowohl Frames mit Tag als auch Frames ohne Tag angenommen.

  Ein Zugriffs-Port kann nur Frames ohne Tag annehmen. Ein Trunk-Port kann Mitglied höchstens eines VLAN ohne Tag und eines oder mehrerer VLANs mit Tag sein. Ein Trunk-Port, der Mitglied sowohl von VLANs ohne Tag als auch von VLANs mit Tag ist, nimmt alle Frame-Typen an. Ein Trunk-Port, der nur Mitglied von VLANs mit Tag ist, nimmt nur Frames mit Tag an.
- **Ingress-Filterung**: Wählen Sie diese Option aus, um die Ingress-Filterung am Port zu aktivieren. Wenn die Ingress-Filterung aktiviert ist, nimmt der Switch nur Frames von den VLANs an, in denen er Mitglied ist. Von anderen VLANs empfangene Frames werden verworfen. Für Ports im Zugriffs- oder Trunk-Modus ist die Ingress-Filterung immer aktiviert. Die Möglichkeit zum Deaktivieren bzw. Aktivieren der Ingress-Filterung ist nur für Ports möglich, für die der allgemeine Modus festgelegt ist.
- **VLAN-Priorität**: Der standardmäßige 802.1p-Prioritätswert für den Port. Der Wert wird basierend auf dem am Port konfigurierten QoS-Vertrauensmodus und den Pakettypen auf die eingehenden Pakete angewendet. Informationen und Anweisungen zum Konfigurieren des Port-Vertrauensmodus finden Sie unter **QoS-Eigenschaften**.

SCHRITT 3 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Ändern des Schnittstellen-VLAN-Modus

Wenn der Schnittstellen-VLAN-Modus eines Ports geändert wird, behandelt der Switch die betroffene VLAN-Mitgliedschaftskonfiguration automatisch wie folgt:

Ändern von Zugriffs-Port in Trunk-Port

Die VLAN-Konfiguration bleibt unverändert. Das Zugriffs-Port-VLAN wird zum nativen VLAN für den Trunk-Port. Für den Port gelten die Einschränkungen für Trunk-Ports.

Ändern von Trunk-Port in Zugriffs-Port

Wenn am ursprünglichen Trunk-Port ein VLAN-Mitglied ohne Tag vorhanden ist, wird der Port aus allen am Port vorhandenen VLANs mit Ausnahme des VLAN ohne Tag entfernt. Die PVID wird auf die VLAN-ID ohne Tag festgelegt.

Wenn am ursprünglichen Trunk-Port kein VLAN-Mitglied ohne Tag vorhanden ist, wird der Port aus allen seinen VLANs entfernt und wird Mitglied des Standard-VLAN. Die PVID des Ports wird auf die Standard-VLAN-ID festgelegt, und der Port wird so eingestellt, dass nur Pakete ohne Tag oder Pakete mit Prioritäts-Tag angenommen werden. Für das Standard-VLAN wird der Port ohne Tag verwendet.

Ändern von Zugriffs-Port in allgemeinen Port

Die VLAN-Konfiguration bleibt unverändert, jedoch kann der Port jetzt alle Frames annehmen. Als allgemeiner Port kann der Port in beliebigen VLANs Mitglied mit Tag oder Mitglied ohne Tag sein.

Ändern von allgemeinem Port in Zugriffs-Port

Wenn am ursprünglichen allgemeinen Port ein VLAN-Mitglied ohne Tag vorhanden ist, wird der Port aus allen seinen VLANs entfernt, mit Ausnahme des VLAN, in dem der Port Mitglied ohne Tag ist. Der Port wird als Mitglied ohne Tag in diesem VLAN konfiguriert.

Wenn am ursprünglichen allgemeinen Port kein VLAN-Mitglied ohne Tag vorhanden ist, wird der Port aus allen seinen VLANs entfernt und wird Mitglied des Standard-VLAN. Die PVID des Ports wird auf die Standard-VLAN-ID festgelegt, und der Port wird so konfiguriert, dass nur Pakete ohne Tag oder Pakete mit Prioritäts-Tag angenommen werden. Für das Standard-VLAN wird der Port ohne Tag verwendet.

Ändern von Trunk-Port in allgemeinen Port

Die VLAN-Konfiguration bleibt unverändert. Als allgemeiner Port kann der Port in beliebigen VLANs Mitglied mit Tag oder Mitglied ohne Tag sein.

Ändern von allgemeinem Port in Trunk-Port

Die VLAN-Konfiguration bleibt unverändert. Das native VLAN des Trunk-Ports wird mit der PVID des allgemeinen Ports konfiguriert. Für den Port gelten die Einschränkungen des Trunk-Ports.

Beispiel: Ein allgemeiner Port ist Mitglied ohne Tag in den VLANs 1, 10 und 20, und die PVID des Ports lautet 1.

Wenn der Port in einen Trunk-Port geändert wird, wird VLAN 1 zum nativen VLAN. Der Trunk-Port bleibt Mitglied der VLANs 10 und 20, jedoch ist jetzt Tagging aktiviert.

Löschen eines VLAN

Beim Löschen eines VLAN werden die folgenden Aktionen ausgeführt:

- Wenn das gelöschte VLAN das native VLAN eines Trunk-Ports war, werden das native VLAN und die PVID des Trunk-Ports in die des Standard-VLAN geändert.
- Wenn ein Zugriffs-Port Mitglied des gelöschten VLAN war, wird der Zugriffs-Port Mitglied des Standard-VLAN, und die PVID des Ports wird in die des Standard-VLAN geändert.
- Wenn ein allgemeiner Port für die Verwendung der VLAN-ID als PVID konfiguriert war, wird die PVID des allgemeinen Ports in die Standard-VLAN-ID geändert. Andere VLAN-Mitgliedschaften werden nicht geändert.

Konfigurieren der VLAN-Mitgliedschaft

Auf diesen Seiten können Sie VLAN-Mitgliedschaften anzeigen und konfigurieren:

- Auf der Seite *Port zu VLAN* können Sie ein VLAN auswählen und dessen Mitglieder-Ports konfigurieren. Informationen hierzu finden Sie unter **Konfigurieren von „Port zu VLAN“**.
- Auf der Seite *Port-VLAN-Mitgliedschaft* können Sie einen Port auswählen und diesen als Mitglied eines oder mehrerer VLANs konfigurieren. Informationen hierzu finden Sie unter **Konfigurieren der Port-VLAN-Mitgliedschaft**.

Alle Ports sind standardmäßig Mitglieder von VLAN 1. Sie können die VLAN-Mitgliedschaft aller Ports ändern. VLAN-Mitgliedschaften können mit Tag oder ohne Tag konfiguriert sein.

- Wenn der Switch einen Frame ohne Tag von einem VLAN empfängt, fügt der Switch ein VLAN-Tag ein, bevor der Frame an die Egress-Ports weitergeleitet wird, die als VLAN-Mitglieder mit Tag konfiguriert sind.
- Wenn der Switch einen Frame ohne Tag von einem VLAN empfängt, leitet der Switch den Frame unverändert an Egress-Ports weiter, die als VLAN-Mitglieder ohne Tag konfiguriert sind.

- Wenn der Switch einen Frame mit Tag von einem VLAN empfängt, entfernt der Switch das VLAN-Tag, bevor der Frame an die Egress-Ports weitergeleitet wird, die als VLAN-Mitglieder ohne Tag konfiguriert sind.
- Wenn der Switch einen Frame mit Tag von einem VLAN empfängt, leitet der Switch den Frame unverändert an Egress-Ports weiter, die als VLAN-Mitglieder mit Tag konfiguriert sind.

Konfigurieren von „Port zu VLAN“

Auf der Seite *Port zu VLAN* können Sie VLANs Ports zuweisen.

SCHRITT 1 Klicken Sie im Navigationsfenster auf **VLAN-Verwaltung** > **Port zu VLAN**.

Auf dieser Seite werden für die ausgewählte VLAN-ID sowie für den ausgewählten Port und die ausgewählte LAG die administrative Konfiguration des Schnittstellen-Port-Modus („Zugriff“, „Trunk“ und „Allgemein“), die Mitgliedschaft, die Tagging-Option und die PVID jedes Ports im Hinblick auf das VLAN angezeigt. (Anweisungen zum Konfigurieren dieser Einstellung finden Sie unter **Konfigurieren der VLAN-Schnittstelleneinstellungen**.)

SCHRITT 2 Wählen Sie die zu konfigurierende VLAN-ID aus, und zeigen Sie mithilfe der Liste „Schnittstellentyp“ entweder Ports oder LAGs an.

SCHRITT 3 Konfigurieren Sie für jede Schnittstelle die folgenden Parameter:

- **Mitglied**: Aktivieren Sie dieses Kontrollkästchen, wenn ein Port Mitglied des VLAN sein soll. Deaktivieren Sie das Kontrollkästchen, wenn ein Port nicht Mitglied des VLAN sein soll. Ein Port ist nicht standardmäßig Mitglied des VLAN.
- **Mit Tag**: Wählen Sie diese Option aus, wenn alle Pakete des VLAN-Regresses zum Port Tags enthalten sollen. Wählen Sie anderenfalls „Ohne Tag“ aus. An einem Trunk-Port werden standardmäßig Tags verwendet. Diese Option ist nur relevant, wenn der Port Mitglied des VLAN ist.
- **Ohne Tag**: Wählen Sie diese Option aus, wenn für die Pakete vom VLAN-Egress an den Port keine Tags verwendet werden sollen. Wählen Sie anderenfalls „Mit Tag“ aus. An einem Zugriffs-Port werden nie Tags verwendet. An einem allgemeinen Port werden standardmäßig keine Tags verwendet. Diese Option ist nur relevant, wenn der Port Mitglied des VLAN ist.

- **PVID**: Aktivieren Sie dieses Kontrollkästchen, wenn ein Port die ausgewählte VLAN-ID als eigene Port-VLAN-ID (PVID) verwenden soll. Deaktivieren Sie das Kontrollkästchen anderenfalls. Wenn für einen Zugriffs- oder Trunk-Port die Option „PVID“ ausgewählt ist, muss der Port VLAN-Mitglied ohne Tag sein. Vom Port empfangene Pakete ohne Tag werden dem entsprechenden VLAN zugewiesen.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren der Port-VLAN-Mitgliedschaft

So konfigurieren Sie VLAN-Einstellungen für Ports:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **VLAN-Verwaltung** > **Port-VLAN-Mitgliedschaft**.

Standardmäßig werden auf der Seite VLAN-Informationen für die einzelnen Ports angezeigt. Mithilfe der Filtereinstellungen können Sie die VLAN-Informationen für LAG-Ports anzeigen. Auf der Seite werden der Schnittstellen-VLAN-Modus („Trunk“ oder „Zugriff“), die PVID und die VLAN-Mitgliedschaften angezeigt. Wenn ein Port Mitglied mehrerer VLANs ist, können Sie den Port auswählen und auf **Detail** klicken, um die Informationen für einen einzigen Port anzuzeigen.

SCHRITT 2 Wählen Sie den Port oder die LAG aus, den bzw. die Sie konfigurieren möchten, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Um eine VLAN-Mitgliedschaft zuzuweisen oder zu entfernen, verwenden Sie die Pfeilschaltflächen wie oben beschrieben.

- So fügen Sie eine VLAN-Mitgliedschaft hinzu: Klicken Sie in der Liste „Verfügbar“ auf ein VLAN, ändern Sie gegebenenfalls dessen Tagging-Eigenschaften (siehe unten), und klicken Sie dann auf die Schaltfläche mit dem Pfeil nach rechts, um das VLAN in die Liste „Ausgewählt“ zu verschieben.
- So entfernen Sie eine VLAN-Mitgliedschaft: Klicken Sie in der Liste „Ausgewählt“ auf ein VLAN, und klicken Sie dann auf die Schaltfläche mit dem Pfeil nach links, um das VLAN in die Liste „Verfügbar“ zu verschieben.

Tagging- und PVID-Eigenschaften

Abhängig vom Schnittstellen-VLAN-Modus („Trunk“, „Zugriff“ oder „Allgemein“) können Sie, wenn Sie ein VLAN aus der Liste „Verfügbar“ auswählen, die folgenden Eigenschaften für die Schnittstelle angeben, bevor Sie das VLAN in die Liste „Ausgewählt“ für die Schnittstelle verschieben.

- **Mitgliedschaft**: Sie können die Schnittstelle als Mitglied mit Tag oder Mitglied ohne Tag im ausgewählten VLAN konfigurieren.
  - **Mit Tag**: Wenn diese Option ausgewählt ist, ist der Port Mitglied mit Tag im ausgewählten VLAN. Wenn der Switch über diese Schnittstelle für dieses VLAN empfangene Pakete weiterleitet, fügt er dem Paket die VLAN-ID hinzu.
  - **Ohne Tag**: Wenn diese Option ausgewählt ist, ist der Port Mitglied ohne Tag im ausgewählten VLAN. Wenn der Switch über diese Schnittstelle Pakete für dieses VLAN weiterleitet, fügt er dem Paket nicht die VLAN-ID hinzu.

  Wenn der Schnittstellen-VLAN-Modus „Allgemein“ entspricht, können Sie für jedes VLAN eine beliebige Option auswählen. Wenn der Schnittstellen-VLAN-Modus „Zugriff“ entspricht, können Sie nur ein VLAN auswählen und müssen für die Schnittstelle die Option „Ohne Tag“ auswählen. Wenn der Schnittstellen-VLAN-Modus „Trunk“ entspricht, können Sie die Schnittstelle als Mitglied ohne Tag in einem VLAN und als Mitglied mit Tag in anderen VLANs angeben.
- **PVID**: Wenn diese Option ausgewählt ist, verwendet der Port die ausgewählte VLAN-ID als eigene Port-VLAN-ID (PVID). Der Port weist die PVID vor der Weiterleitung allen am Port empfangenen Frames ohne Tag zu. Für die Konfiguration gelten die folgenden Regeln:
  - Wenn der Schnittstellen-VLAN-Modus „Allgemein“ entspricht, können Sie jedes VLAN, in dem die Schnittstelle Mitglied mit Tag oder Mitglied ohne Tag ist, zum Bereitstellen der PVID auswählen.
  - Wenn der Schnittstellen-VLAN-Modus „Trunk“ entspricht, wird die PVID auf die ID des VLAN festgelegt, in dem der Port Mitglied ohne Tag ist.
  - Wenn der Schnittstellen-VLAN-Typ „Zugriff“ entspricht, wird die PVID auf die Zugriffs-VLAN-ID festgelegt, und dieses Feld kann nicht geändert werden.

Wenn Sie die Optionen „Ohne Tag“, „Mit Tag“ und „PVID“ auswählen und das VLAN in die Liste „Ausgewählt“ verschieben, wird der VID ein O, M und/oder P angefügt.

SCHRITT 4 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Festlegen des Standard-VLAN

Der Switch erstellt standardmäßig automatisch VLAN 1 als Standard-VLAN für alle Ports und Link-Aggregationsgruppen (LAGs). Ein Port, der keine VLAN-Mitgliedschaften hat, wird vom Switch automatisch als Mitglied des Standard-VLAN konfiguriert.

Auf der Seite *VLAN-Standardeinstellungen* können Sie das Standard-VLAN ändern.

Wenn Sie die VID des Standard-VLAN ändern, gilt Folgendes:

- Ports, die Mitglieder des ursprünglichen Standard-VLAN waren, werden als Mitglieder dieses VLAN entfernt und als Mitglieder des neuen Standard-VLAN konfiguriert.
- Die Port-VLAN-ID (PVID) der Ports, die Mitglieder des ursprünglichen Standard-VLAN waren, wird in die VID des neuen Standard-VLAN geändert.
- Wenn das Verwaltungs-VLAN mit dem des ursprünglichen Standard-VLAN identisch war, wird das Verwaltungs-VLAN so aktualisiert, dass es dem neuen Standard-VLAN entspricht.
- Der Typ des ursprünglichen Standard-VLAN wird von „Standard“ in „Statisch“ geändert, und das Standard-VLAN kann gelöscht werden. Eine Ausnahme ist VLAN 1. Auch wenn VLAN 1 nicht mehr als Standard-VLAN festgelegt ist, können Sie dieses VLAN nicht löschen.

So wählen Sie ein Standard-VLAN aus:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **VLAN-Verwaltung** > **VLAN-Standardeinstellungen**.

SCHRITT 2 Wählen Sie das VLAN aus der Liste aus.

SCHRITT 3 Klicken Sie auf **Übernehmen**.

Sprache und Medien

Mithilfe von VoIP (Voice-over-Internet Protocol) können Sie ein Computerdatennetzwerk für Sprachtelefongespräche verwenden. Angesichts der zunehmenden Bereitstellung verzögerungsempfindlicher Anwendungen wie beispielsweise VoIP in modernen Netzwerken müssen Sie QoS richtig konfigurieren, um hohe Qualität sicherzustellen. Die Funktion „Sprache und Medien“ bietet einen einfachen Klassifizierungsmechanismus für Sprachpakete, sodass diese gegenüber Datenpaketen priorisiert werden können.

Die Funktion „Sprache und Medien“ identifiziert VoIP-Datenströme in Ethernet-Switches und stellt diesen eine bessere Serviceklasse (Class of Service, CoS) bereit als gewöhnlichem Verkehr. Der Switch unterstützt zwei Arten von Sprache und Medien:

- **Protokollbasiert**: Identifiziert eine VoIP-Sitzung mithilfe des SIP-Protokolls (Session Initiation Protocol, SIP) und von H.323-Steuerungsverkehr und weist diesen Paketen die höchste Priorität im Voice-VLAN zu.
- **OUI-basiert**: Ports, für die diese Funktion aktiviert ist, werden automatisch Mitglieder des konfigurierten Voice-VLAN. Der Switch erkennt OUI-Werte (Organizationally Unique Identifier) in den ersten drei Byte der MAC-Adressen in Clientpaketen, um diese im VoIP-VLAN zu klassifizieren und an Ports zu priorisieren, an denen die Option „Autom. VoIP“ aktiviert ist.

In den folgenden Themen finden Sie weitere Informationen zu den Konfigurationsseiten im Menü „VLAN-Verwaltung > Sprache und Medien“:

- **Anzeigen und Hinzufügen von Telefonie-OUI**
- **Konfigurieren von OUI-basierter Sprache und Medien**
- **Konfigurieren von SIP/H.323 basierter Sprache und Medien**

Anzeigen und Hinzufügen von Telefonie-OUI

Auf der Seite *Telefonie-OUI* werden die OUIs (Organizationally Unique Identifiers) aufgeführt, die den verschiedenen Voice-VLANs zugeordnet sind.

Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **VLAN-Verwaltung** > **Autom. VoIP** > **Telefonie-OUI**.

Die Telefonie-OUI-Tabelle ist mit IDs für häufig verwendete Telefoniegeräte vorkonfiguriert. Der Administrator kann OUIs hinzufügen oder entfernen. Wenn „Sprache und Medien“ aktiviert ist, verwenden die Ports die OUI-Ziffern in den Quell- und/oder Ziel-MAC-Adressen eingehender Pakete, um Sprachverkehr automatisch einem Voice-VLAN zuzuweisen. Anweisungen zum Zuordnen einer IEEE 802.1p-Priorität zum VLAN und zum Aktivieren von Ports für Sprache und Medien finden Sie unter **Konfigurieren von OUI-basierter Sprache und Medien**.

So fügen Sie eine neue OUI-Beschreibung hinzu:

SCHRITT 1 Klicken Sie auf **Hinzufügen**.

SCHRITT 2 Geben Sie die folgenden Werte an:

- **Telefonie-OUI**: Geben Sie eine aus drei Oktetten bestehende ID für die Telefonieanwendung ein.
- **Beschreibung**: Geben Sie eine Beschreibung für den Dienst ein, beispielsweise den Namen des Herstellers oder des Telefonieprodukts.

SCHRITT 3 Klicken Sie auf **Übernehmen** und dann auf **Schließen**.

Konfigurieren von OUI-basierter Sprache und Medien

Auf der Seite „Autom. VoIP, OUI-basiert“ können Sie folgende Aufgaben ausführen:

- Konfigurieren Sie eine IEEE 802.1p-Prioritätsstufe für Sprach- und Medienverkehr, der anhand der OUI-Ziffern in MAC-Adressen identifiziert wird.
- Geben Sie das VLAN für OUI-basierte VoIP-Pakete an. Sie können zwar eine noch nicht im Switch erstellte VLAN-ID zuweisen, aber Sie müssen das VLAN anschließend erstellen, damit die Funktion verwendet werden kann (siehe **Erstellen von VLANs**).
- Aktivieren Sie Ports für die Funktion. Wenn die Funktion an einem Port aktiviert ist, wird der Port automatisch Mitglied des konfigurierten Voice-VLAN (das heißt, der Administrator muss den Port nicht manuell als Mitglied des VLAN hinzufügen).

So konfigurieren Sie OUI-basierte Sprache und Medien:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **VLAN-Verwaltung** > **Sprache und Medien** > **OUI-basiert**.

SCHRITT 2 Aktivieren die Sie Option „VLAN“, damit die Felder „VLAN-ID“ und „Priorität“ geändert werden können.

SCHRITT 3 Geben Sie im Feld „VLAN-ID“ das VLAN für die Übertragung von Sprachverkehr an. Dieses VLAN muss bereits im Switch konfiguriert sein (siehe **Erstellen von VLANs**).

SCHRITT 4 Geben Sie im Feld „Priorität“ die Prioritätsstufe der IEEE 802.1p-Serviceklasse für VoIP-Verkehr an.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

SCHRITT 6 Wählen Sie in der Tabelle für die Telefonie-OUI-basierten Schnittstelleneinstellungen die zu konfigurierende Schnittstelle aus, und klicken Sie dann auf **Bearbeiten**.

SCHRITT 7 Wählen Sie für den automatischen VoIP-Modus die Option „Aktivieren“ aus. Der Port wird automatisch als Mitglied des Voice-VLAN hinzugefügt.

SCHRITT 8 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren von SIP/H.323 basierter Sprache und Medien

Auf der Seite *Autom. VoIP, SIP/H.323-basiert* können Sie den Switch so konfigurieren, dass VoIP-Verkehr am Protokoll erkannt wird (beispielsweise SIP (Session Initiation Protocol) und H.323). Der Verkehr wird automatisch auf der Grundlage der Datenverkehrsklasse für den an den Ports konfigurierten VoIP-Verkehr priorisiert.

So konfigurieren Sie SIP/H.323-basierte Sprache und Medien:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **VLAN-Verwaltung** > **Sprache und Medien** > **Autom. VoIP, SIP/H.323-basiert**.

SCHRITT 2 Im Menü „Schnittstellentyp“ können Sie Ports oder LAGs in der Tabelle für protokollbasierte Schnittstelleneinstellungen anzeigen.

SCHRITT 3 Wählen Sie den Port oder die LAG-Schnittstelle aus, den bzw. die Sie konfigurieren möchten, und klicken Sie auf **Bearbeiten**.

SCHRITT 4 Wählen Sie für den automatischen VoIP-Modus die Option „Aktivieren“ aus.

SCHRITT 5 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Medien-VLAN

Die Funktion „Medien-VLAN“ ermöglicht die Übertragung von Sprach-, Video- und Signalisierungsverkehr mit zugewiesenem Prioritätswert über Switch-Ports. Durch die Zuweisung unterschiedlicher Prioritäten für Verkehr können Sie an einem Port eingehenden Medien- und Datenverkehr trennen. Sie können mithilfe der Funktion „Medien-VLAN“ sicherstellen, dass die Ton- oder Videoqualität eines IP-Telefons oder Videogeräts vor Beeinträchtigungen durch hohes Datenverkehrsaufkommen am Port geschützt wird.

Die durch VLANs bereitgestellte inhärente Verkehrsisolierung stellt sicher, dass der Verkehr zwischen VLANs verwaltet wird und dass mit dem Netzwerk verbundene Clients keinen direkten Angriff auf Sprachkomponenten initiieren können. Der Switch verwendet den IP-DSCP- oder 802.1p-Wert in den Paketen von Mediengeräten, um diesen Verkehr Warteschlangen mit hoher Priorität zuzuweisen.

Der Switch verwendet Medien-VLANs für die Unterstützung von LLDP-MED-Anwendungen. (Informationen zu diesem Protokoll finden Sie unter **LLDP-MED**.) Jedes Medien-VLAN entspricht einer LLDP-MED-Anwendung für einen bestimmten Medienverkehrstyp. Es gibt folgende LLDP-MED-Anwendungen: Voice, Voice-Signalisierung, Gast-Voice, Gast-Voice-Signalisierung, Softphone-Voice, Videokonferenzen, Streaming-Video und Videosignalisierung. Jedem Medien-VLAN sind die folgenden Parameter zugeordnet:

- Ein VLAN mit optionalen VLAN-Tags
- Ein IEEE 802.1p-Prioritätswert
- Ein DSCP-Wert

Wenn an einem Port LLDP-MED mit Netzwerkrichtlinien aktiviert ist, macht der Switch die Medien-VLANs in den an den Port gesendeten LLDP-MED-Netzwerkrichtlinien-TLVs bekannt. Wenn ein LLDP-Medienendpunkt erkannt wird, installiert der Switch das Medien-VLAN am entsprechenden Port. Sie können LLDP-MED und Netzwerkrichtlinien auf den Seiten in „Administration - Erkennung – LLDP“ aktivieren.

Die Funktion „Medien-VLAN“ wird global aktiviert und deaktiviert. Die einzelnen Anwendungen und die zugehörigen Medien-VLANs konfigurieren Sie pro Port. Beispielsweise kann sich „Gast-Voice“ in Medien-VLAN 1 an Schnittstelle g1, aber in Medien-VLAN 10 an Schnittstelle g2 befinden.

In der Tabelle für Medien-VLAN-Schnittstelleneinstellungen werden die einzelnen Medienverkehrstypen angezeigt, die Sie aktivieren können. Außerdem sehen Sie den Status und die Einstellungen des ausgewählten Ports.

So konfigurieren Sie Medien-VLAN-Anwendungen:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **VLAN-Verwaltung > Sprache und Medien > Medien-VLAN**.

SCHRITT 2 Wählen Sie für den Administrationsmodus die Option „Aktivieren“ aus, um die Funktion im Switch global zu aktivieren, und klicken Sie auf **Übernehmen**.

SCHRITT 3 Wählen Sie aus der Schnittstellenliste die Schnittstelle aus, die Sie konfigurieren möchten.

VORSICHT Ports, die Mitglied einer LAG sind, können Sie nicht für Medien-VLAN-Anwendungen aktivieren (siehe **Konfigurieren von LAGs**).

SCHRITT 4 Klicken Sie auf **Bearbeiten**.

SCHRITT 5 Wählen Sie aus der Anwendungsliste den Medienverkehrstyp aus, den Sie konfigurieren möchten:

- Voice
- Voice-Signalisierung
- Gast-Voice
- Gast-Voice-Signalisierung
- Softphone-Voice

- Videokonferenzen
- Streaming-Video
- Videosignalisierung

SCHRITT 6 Wählen Sie unter „Anwendungsstatus“ die Option „Aktivieren“ aus, um die Prioritätszuweisung für die ausgewählte Anwendung zu aktivieren. Deaktivieren Sie das Kontrollkästchen, um die Funktion zu deaktivieren.

SCHRITT 7 Wenn Sie „Anwendungsstatus“ aktiviert haben, aktivieren oder deaktivieren Sie die folgenden Funktionen:

- **Ohne Tag**: Wählen Sie die Option „Aktivieren“ aus, wenn das Mediengerät (LLDP-MED-Endpunkt) Pakete ohne Tags senden soll. Diese Ausnahme muss auch aus dem Netzwerkrichtlinien-TLV des Switch hervorgehen, und ein Mediengerät muss bestätigen, dass es Frames ohne Tag verwendet. Deaktivieren Sie das Kontrollkästchen, um die Funktion zu deaktivieren.
- **VLAN** und **VLAN-ID**: Wählen Sie die Option „Aktivieren“ aus, und wählen Sie dann eine VLAN-ID aus der Liste aus. Deaktivieren Sie das Kontrollkästchen, um die Funktion zu deaktivieren.
- **Priorität** und **Prioritätswert**: Wählen Sie die Option „Aktivieren“ aus, um Pakete der ausgewählten Anwendung zu priorisieren. Geben Sie dann einen Tag-Wert für die IEEE 802.1p-Serviceklassenpriorität für Medien-VLAN-Verkehr ein. Möglich sind Prioritäts-Tags im Bereich von 0 - 7.
- **DSCP** und **DSCP-Wert**: Wählen Sie die Option „Aktivieren“ aus, um einen DSCP für die ausgewählte Anwendung anzugeben. Geben Sie dann einen DSCP-Wert für den Port ein. Möglich sind Werte im Bereich von 0 - 63.

SCHRITT 8 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

SCHRITT 9 An der Schnittstelle muss LLDP-MED aktiviert sein. Anweisungen finden Sie unter **LLDP-MED**.

Autom. VoIP-Sitzungen

Auf der Seite *Autom. VoIP-Sitzungen* werden Informationen zu Quelle, Ziel und Protokoll für die einzelnen VoIP-Sitzungen angezeigt.

6

Spanning Tree

In diesem Kapitel wird das Konfigurieren des STP-Protokolls (Spanning Tree Protocol) im Switch beschrieben.

Das Kapitel enthält die folgenden Themen:

- **Übersicht über Spanning Tree**
- **Konfigurieren des STP-Status und der globalen Einstellungen**
- **Konfigurieren von STP-Schnittstelleneinstellungen**
- **RSTP-Schnittstelleneinstellungen**

Übersicht über Spanning Tree

Das STP-Protokoll ermöglicht die effiziente Kommunikation in Netzwerken mit mehreren Bridges. Die Geräte in diesen Netzwerken können mehrere (das heißt redundante) Pfade zum gleichen Endpunkt lernen. Pfadredundanz ist zwar wünschenswert, um den Verkehrsfluss bei Ausfall bestimmter Links aufrechtzuerhalten, kann jedoch zu Verkehrsschleifen führen, die die Netzwerkleistung beeinträchtigen und Weiterleitungsalgorithmen verwirren.

Jede STP-fähige Bridge tauscht mit anderen Bridges BPDUs (Bridge Protocol Data Units, Bridge-Protokoll-Dateneinheiten) aus. BPDUs identifizieren die MAC-Adressen der Bridge-Ports sowie die den einzelnen Ports zugeordneten Prioritäten und Kosten. STP erstellt anhand dieser Informationen eine Topologie, die einen einzigen aktiven Pfad zwischen zwei beliebigen Stationen im Netzwerk bereitstellt. Doppelte Pfade zwischen diesen Stationen werden in einen Standby-Status versetzt und nur verwendet, wenn der aktive Pfad nicht mehr verfügbar ist.

Ausgetausche BPDU-Nachrichten ermöglichen außerdem die Auswahl einer Root-Bridge und eines Root-Ports für das Netzwerk. Die Root-Bridge wird von den anderen Bridges als Referenz bei der Berechnung des kostengünstigsten Pfads verwendet. Dabei werden die Kosten der Ports in den einzelnen Pfaden summiert, und anschließend wird der Pfad mit der niedrigsten Summe ausgewählt. Der Port, der eine Bridge mit dem kostengünstigsten Pfad verbindet, wird als *Root-Port* der Bridge bezeichnet.

Wenn die Root-Bridge ausgewählt ist und die einzelnen Root-Ports eingerichtet sind, kann jedes Netzwerksegment die Bridge ermitteln, die den kostengünstigsten Pfad zum Root-Port bereitstellt. Der Port, der diesen Pfad bereitstellt, wird als *designierter Port* für das Netzwerksegment bezeichnet. Spanning Tree deaktiviert andere Ports für dieses Netzwerksegment oder legt sie als alternative Ports oder Backup-Ports fest.

Unterstützt werden unter anderem die Spanning Tree-Versionen Common Spanning Tree (CST) Rapid STP (RSTP).

- CST (IEEE 802.1D) ist die ursprüngliche Protokollversion, die einen einzigen Pfad zwischen Endstationen bereitstellt und dadurch Schleifen vermeidet und beseitigt.
- RSTP (IEEE 802.1w) bietet Protokollerweiterungen, mit deren Hilfe Sie in einem Netzwerk schneller die optimale STP-Topologie einrichten können.

Konfigurieren des STP-Status und der globalen Einstellungen

Auf der Seite *STP-Status und globale Einstellungen* können Sie STP aktivieren, den STP-Betriebsmodus auswählen und Bridge-Prioritätseinstellungen konfigurieren. Außerdem können Sie Statusinformationen zur STP-Topologie anzeigen. Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **Spanning Tree** > **STP-Status und globale Einstellungen**.

Auf dieser Seite können Sie globale Einstellungen und Bridge-Einstellungen konfigurieren und Informationen zur designierten Root-Bridge anzeigen.

Konfigurieren von globalen Einstellungen und Bridge-Einstellungen

So konfigurieren Sie globale STP-Einstellungen und Bridge-Einstellungen:

SCHRITT 1 Geben Sie die folgenden globalen Einstellungen an:

- **Spanning Tree-Status**: Wählen Sie diese Option aus, um den STP-Betrieb im Switch zu aktivieren. Sie müssen den STP-Betrieb auch an den einzelnen Ports aktivieren (siehe **Konfigurieren von STP-Schnittstelleneinstellungen**).
- **STP-Betriebsmodus**: Wählen Sie den Modus „Classic STP“ oder „Rapid STP“ aus. Das Rapid Spanning Tree-Protokoll (RSTP) ist eine Weiterentwicklung des Spanning Tree-Protokolls (802.1D-Standard) und bietet eine schnellere Spanning Tree-Konvergenz nach einer Topologieänderung.
- **BPDU-Bearbeitung**: Bridge-Protokoll-Dateneinheiten (Bridge Protocol Data Units, BPDUs) sind Nachrichten, die zwischen Switches ausgetauscht werden, um die STP-Topologie zu berechnen. Wählen Sie die Methode aus, die für die BPDU-Paketbearbeitung verwendet werden soll, wenn Spanning Tree an einer Schnittstelle deaktiviert ist:
  - **Filterung**: Ermöglicht dem Port das Verwerfen von BPDUs, die an Schnittstellen empfangen wurden, für die STP nicht aktiviert ist.
  - **Überlauf**: Ermöglicht den Überlauf von BPDUs, die an Ports ohne Spanning Tree empfangen werden, an alle anderen Ports ohne Spanning Tree.

SCHRITT 2 Geben Sie die folgende Bridge-Einstellung an:

- **Priorität**: Der Prioritätswert der Bridge. Wenn STP von Switches oder Bridges ausgeführt wird, wird jedem Switch bzw. jeder Bridge eine Priorität zugewiesen. Nach dem Austausch von BPDUs wird das Gerät mit der niedrigsten Bridge-ID zur Root-Bridge. Die Bridge-Priorität muss ein Vielfaches von 4096 sein. Wenn Sie eine Priorität angeben, die nicht ein Vielfaches von 4096 ist, wird die Priorität automatisch auf das nächstniedrigere Vielfache von 4096 festgelegt. Wenn Sie beispielsweise versuchen, die Priorität auf einen Wert zwischen 0 und 4095 festzulegen, wird die Priorität auf 0 festgelegt. Die Standardpriorität lautet 32768. Gültig sind Werte im Bereich von 0 - 61440.

In diesem Abschnitt der Seite werden die folgenden Informationen angezeigt:

- **Hello-Zeit**: Das Intervall, in dem eine Bridge Konfigurationsnachrichten sendet.
- **Maximales Alter**: Die Zeit in Sekunden, die eine Bridge wartet, bevor eine Topologieänderung implementiert wird.
- **Max. Hops**: Die Anzahl der Hops, die auftreten, bevor eine BDPU verworfen wird und die Port-Informationen als veraltet gekennzeichnet werden. Die maximale Hop-Anzahl ist auf 20 festgelegt und ist nicht konfigurierbar.
- **Weiterleitungsverzögerung**: Der Zeitraum in Sekunden für den Verbleib einer Bridge im Mithör- und Lernzustand vor dem Weiterleiten von Paketen.
- **Aufbewahrungszeitraum**: Der Zeitraum in Sekunden, der zwischen der Übertragung von Konfigurations-BPDUs über einen Bridge-Port mindestens verstreicht.

Im Abschnitt „Designierte Root“ werden die folgenden Informationen angezeigt:

- **Bridge-ID**: Die Bridge-ID, das heißt eine Verkettung der Bridge-Priorität und der MAC-Basisadresse der Bridge.
- **Root-Bridge-ID**: Die Bridge-ID der Root-Bridge. Die Bridge mit der niedrigsten Bridge-ID aller Bridges wird zur Root-Bridge.
- **Root-Port**: Die Nummer des Ports, der den Pfad mit den niedrigsten Kosten von dieser Bridge zur Root-Bridge bietet. Dies ist wichtig, wenn es sich bei der Bridge nicht um die Root-Bridge handelt. Der Standardwert lautet 0.
- **Root-Pfadkosten**: Die Kosten des Pfads von dieser Bridge zur Root-Bridge.
- **Anzahl der Topologieänderungen**: Die Gesamtanzahl der aufgetretenen STP-Statusänderungen.
- **Letzte Topologieänderung**: Die Zeit, die insgesamt seit der letzten Topologieänderung verstrichen ist.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren von STP-Schnittstelleneinstellungen

Auf der Seite *STP-Schnittstelleneinstellungen* können Sie einzelnen Ports oder LAGs STP-Eigenschaften zuweisen. Diese Einstellungen gelten sowohl für Classic STP als auch für Rapid STP.

So bearbeiten Sie die Einstellungen für einen Port oder eine LAG:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Spanning Tree** > **STP-Schnittstelleneinstellungen**.

In der Tabelle für STP-Schnittstelleneinstellungen werden Konfigurationsinformationen für die einzelnen Ports und LAGs angezeigt. Standardmäßig ist der STP-Betrieb für alle Ports aktiviert.

HINWEIS: Die Liste der Ports und LAGs kann aus mehreren Seiten bestehen. Mithilfe der Seitenliste können Sie die nächste Eintragsgruppe anzeigen.

SCHRITT 2 Wählen Sie den Port oder die LAG aus, den bzw. die Sie konfigurieren möchten, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie die Parameter ein:

- **STP**: Wählen Sie diese Option aus, um den STP-Betrieb für den Port bzw. die LAG zu aktivieren.
- **Autom. Edge**: Wählen Sie die Option „Aktivieren“ aus, damit der Switch automatisch ermitteln kann, ob es sich um einen Edge-Port handelt. Ein Port ist ein Edge-Port, wenn er nicht mit einer Bridge verbunden ist. Die automatische Erkennung beschleunigt den Übergang des Ports in den Weiterleitungsstatus. Ein Port, der sich im Weiterleitungsstatus befindet, kann Verkehr weiterleiten und MAC-Adressen lernen.
- **Edge-Port**: Wählen Sie die Option „Aktivieren“ aus, um den Port manuell als Edge-Port zu konfigurieren.
- **BPDU-Bearbeitung**: Bridge-Protokoll-Dateneinheiten (Bridge Protocol Data Units, BPDUs) sind Nachrichten, die zwischen Switches ausgetauscht werden, um die STP-Topologie zu berechnen. Wählen Sie die Methode aus, die für die BPDU-Paketbearbeitung verwendet werden soll, wenn Spanning Tree an einer Schnittstelle deaktiviert ist:
  - **Filterung**: Ermöglicht dem Port das Verwerfen von BPDUs, die an Schnittstellen empfangen wurden, für die STP nicht aktiviert ist.
  - **Überlauf**: Ermöglicht den Überlauf von BPDUs, die an Ports ohne Spanning Tree empfangen werden, an alle anderen Ports ohne Spanning Tree.

- **Pfadkosten**: Geben Sie die Pfadkosten für den Port an. Bei den Pfadkosten eines Ports handelt es sich um den Anteil des Ports an den Kosten für den Pfad zur Root-Bridge. Die Pfadkosten werden verwendet, um Verkehr weiterzuleiten, wenn ein Pfad umgeleitet wird. Wählen Sie die Option „Standard verwenden“ aus, um die Pfadkosten auf die Port-Geschwindigkeit festzulegen. Wählen Sie alternativ „Benutzerdefiniert“ aus, um einen benutzerdefinierten Wert zwischen 0 und 200.000.000 festzulegen. Der Wert 0 bedeutet, dass die Pfadkosten gemäß der Geschwindigkeit des Ports festgelegt werden.

SCHRITT 4 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Die neue Konfiguration wird zusammen mit den folgenden Informationen zum Port bzw. zur LAG in der STP-Schnittstellentabelle angezeigt.

- **Edge-Betriebsstatus**: Gibt an, ob ein Port zurzeit als Edge-Port betrieben wird. „Aktiviert“ bedeutet, dass sich der Port aufgrund einer der folgenden Konfigurationen im Weiterleitungsstatus befindet:
  - Der Port ist als Edge-Port konfiguriert und befindet sich daher automatisch im Weiterleitungsstatus.
  - Der Port ist als automatischer Edge-Port konfiguriert und hat, da er keine BDPUs empfangen hat, den Weiterleitungsstatus angenommen.
- **Port-Status**: Der aktuelle STP-Status eines Ports. Wenn diese Option aktiviert ist, bestimmt der Port-Status, welche Weiterleitungsaktion für Verkehr ausgeführt wird. Folgende Port-Status sind möglich:
  - **Deaktiviert**: STP ist zurzeit für den Port deaktiviert. Der Port nimmt nicht am Spanning Tree teil, befindet sich jedoch in einem Betriebsstatus, in dem er MAC-Adressen lernt und Verkehr weiterleitet.
  - **Blockieren**: Der Port wird zurzeit blockiert und kann nicht zum Weiterleiten von Verkehr oder zum Lernen von MAC-Adressen verwendet werden.
  - **Mithören**: Der Port befindet sich zurzeit im Mithörmodus. Der Anschluss kann weder Datenverkehr weiterleiten noch MAC-Adressen lernen.
  - **Lernen**: Der Port befindet sich zurzeit im Lernmodus. Der Port kann keinen Verkehr weiterleiten, er kann jedoch neue MAC-Adressen lernen.

  - **Weiterleitung**: Der Port befindet sich zurzeit im Weiterleitungsmodus. Der Port kann Datenverkehr weiterleiten und neue MAC-Adressen lernen.

- **Designierte Bridge-ID**: Die Bridge-ID der Bridge, die den kostengünstigsten Root-Pfad zu einem LAN bietet. Die Bridge-ID ist eine Verkettung der Bridge-Priorität und der MAC-Basisadresse der Bridge.
- **Designierte Port-ID**: Die Port-ID der designierten Bridge, die den kostengünstigsten Root-Pfad zum LAN bietet. Bei der ID handelt es sich um eine Verkettung der Port-Priorität und der Schnittstellennummer des Ports.
- **Designierte Kosten**: Die Root-Pfadkosten von der designierten Bridge zur Root-Bridge. Ports mit niedrigeren designierten Kosten werden mit geringerer Wahrscheinlichkeit blockiert, wenn STP Schleifen erkennt.
- **Geschwindigkeit**: Die Port-Geschwindigkeit.
- **LAG**: Gegebenenfalls die LAG, in der der Port Mitglied ist.

RSTP-Schnittstelleneinstellungen

Mit dem Rapid Spanning Tree-Protokoll (RSTP) können Sie in jedem überbrückten LAN die schnellere Konvergenz eines schleifenfreien Spanning Trees sicherstellen. Um die Seite *RSTP-Schnittstelleneinstellungen* anzuzeigen, klicken Sie im Navigationsfenster auf **Spanning Tree** > **RSTP-Schnittstelleneinstellungen**.

Eine RSTP-Topologie wird automatisch gebildet, wenn RSTP als Spanning Tree-Modus ausgewählt ist. Auf der Seite *STP-Status und globale Einstellungen* können Sie den RSTP-Modus aktivieren.

In der Tabelle für RSTP-Schnittstelleneinstellungen werden standardmäßig Informationen für die einzelnen Ports angezeigt. Mithilfe der Liste „Schnittstellentyp“ können Sie Ports oder LAGs in der Tabelle anzeigen. In der RSTP-Schnittstellentabelle werden die folgenden Informationen für die einzelnen Ports angezeigt:

- **Punkt-zu-Punkt-Betriebsstatus**: Ein physischer Port verfügt über eine Punkt-zu-Punkt-Verbindung mit einem LAN, wenn der Port im Vollduplex-Modus betrieben wird.

- **Portrolle**: Die Port-Rolle, die vom STP-Algorithmus zugewiesen wird, um STP-Pfade bereitzustellen. Folgende Feldwerte sind möglich:
  - **Root**: Bietet von allen Ports im Switch die niedrigsten Kosten für den Root-Pfad zur Root-Bridge.
  - **Designiert**: Bietet die niedrigsten Kosten für den Root-Pfad von einem LAN zur Root-Bridge. Der Switch ist die designierte Bridge im LAN.
  - **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. Backup-Ports werden nur verwendet, wenn zwei Ports mithilfe einer Punkt-zu-Punkt-Verbindung in einer Schleife verbunden sind oder wenn ein LAN zwei oder mehr Verbindungen enthält, die mit einem gemeinsamen Segment verbunden sind.
  - **Deaktiviert**: Der Port nimmt nicht am Spanning-Tree teil.
- **Modus**: Gibt an, ob der RSTP-Administrationsmodus für den Port aktiviert oder deaktiviert ist.
- **Edge-Port-Betriebsstatus**: Wenn diese Option für den Port oder die LAG aktiviert ist, wird der Port automatisch in den Weiterleitungsstatus versetzt. Anweisungen zum Ändern dieser Einstellung finden Sie unter **Konfigurieren von STP-Schnittstelleneinstellungen**.
- **Portstatus**: Der Betriebsstatus des Ports.

Sie können einen Port auswählen und auf **Protokollmigration aktivieren** klicken, damit der Switch RSTP-BPDUs an den Port sendet. Auf diese Weise können Sie testen, ob alle Legacy-Bridges aus dem LAN entfernt wurden.

7

MAC-Adresstabellen

In diesem Kapitel werden die statische Konfiguration und die dynamische Aufnahme von MAC-Adressen (Media Access Control, Medienzugriffssteuerung) in die Filterdatenbank des Switch beschrieben. Der Switch durchsucht seine Filterdatenbank, um zu ermitteln, an welchen Port ein Paket weitergeleitet werden soll. Die Filterdatenbank wird in diesem Dokument auch als Bridging-Tabelle bezeichnet. Die Suche basiert auf dem VLAN und der Ziel-MAC-Adresse des Pakets. Wenn bei der Suche kein übereinstimmender Eintrag gefunden wird, flutet der Switch die Pakete unter Ausschluss des Ingress-Ports an das VLAN.

Das Kapitel enthält die folgenden Themen:

- **Konfigurieren von statischen MAC-Adressen**
- **Konfigurieren der Fälligkeitszeit für dynamische Adressen**
- **Dynamische MAC-Adressen**

Konfigurieren von statischen MAC-Adressen

Auf der Seite *Statische Adressen* wird eine Liste der MAC-Adressen angezeigt, die manuell in der Bridging-Tabelle des Switch konfiguriert sind. Eine statische MAC-Adresse ist außerdem einem VLAN und einem Port zugeordnet.

So fügen Sie statische MAC-Adresseinträge hinzu:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **MAC-Adresstabellen** > **Statische Adressen**.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie die Parameter ein:

- **VLAN-ID**: Wählen Sie das VLAN aus, in dem sich das Gerät mit der statischen MAC-Adresse befindet.
- **Schnittstelle**: Geben Sie den Port bzw. die LAG an, über den bzw. über die die statischen MAC-Adressen erreichbar sind.
- **MAC-Adresse**: Geben Sie die statische MAC-Adresse ein.
- **Status**: Wählen Sie einen Status für diese statische MAC-Adresse aus:
  - **Permanent**: Wenn dieser Status ausgewählt ist, läuft die statische MAC-Adresse nicht ab. Beachten Sie jedoch, dass der Eintrag bei einem Neustart des Switch nur wiederhergestellt wird, wenn Sie den Dateityp der aktuellen Konfiguration in den Startkonfigurations-Dateityp kopiert haben. Informationen hierzu finden Sie unter **Kopieren und Speichern von Konfigurationsdateien**.
  - **Sicher**: Wenn dieser Status ausgewählt ist, wird die MAC-Adresse gesichert und in Verbindung mit der Funktion für die Port-Sicherheit verwendet. Wenn eine MAC-Adresse an einem Port gesichert wird, können Pakete, die von der MAC-Adresse stammen, nur von dem gesicherten Port eingehen. Anderenfalls werden die Pakete verworfen. Wenn Port-Sicherheit für den Port deaktiviert ist, wird die MAC-Adresse aus der Liste der statischen MAC-Adressen gelöscht. Wenn Port-Sicherheit für einen Port aktiviert ist, kann der Port maximal 256 statische und dynamische MAC-Adressen unterstützen. (Weitere Informationen finden Sie unter **Aktivieren der Port-Sicherheit**).
  - **Bei Timeout löschen**: Wenn dieser Status ausgewählt ist, ist die MAC-Adresse statisch, kann aber aufgrund von Inaktivität ablaufen. In dieser Hinsicht wird die Adresse wie eine dynamisch gelernte MAC-Adresse behandelt. Informationen zum Festlegen des Fälligkeitszeitraums finden Sie unter *Einstellungen für dynamische Adressen*.

SCHRITT 4 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

HINWEIS Um eine statische MAC-Adresse zu löschen, wählen Sie diese in der Tabelle aus und klicken Sie auf **Löschen**.

Konfigurieren der Fälligkeitszeit für dynamische Adressen

Auf der Seite *Einstellungen für dynamische Adressen* können Sie eine Fälligkeitszeit festlegen, nach der nicht aktualisierte Adressen aus der Tabelle der dynamischen MAC-Adressen vom System entfernt werden. Die Fälligkeitszeit gilt für dynamisch gelernte Adressen und für statische Adressen, für die das Löschen bei Timeout konfiguriert ist. Die standardmäßige Fälligkeitszeit beträgt 300 Sekunden.

So konfigurieren Sie die Fälligkeitszeit:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **MAC-Adresstabellen** > **Einstellungen für dynamische Adressen**.

SCHRITT 2 Geben Sie eine Fälligkeitszeit von 10 bis 1.000.000 Sekunden an.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Dynamische MAC-Adressen

Wenn der Switch in der Bridging-Tabelle keinen Eintrag findet, der dem VLAN und der MAC-Zieladresse eines eingehenden Pakets entspricht, lernt der Switch die MAC-Adresse, das VLAN und den Ingress-Port des Pakets und fügt der Tabelle der dynamischen Adressen einen Eintrag hinzu.

Um ein Überlaufen der Bridging-Tabelle zu verhindern und Platz für neue Adressen zu schaffen, wird eine Adresse aus der Bridging-Tabelle gelöscht, wenn innerhalb der konfigurierten Fälligkeitszeit kein Verkehr von einer dynamischen MAC-Adresse empfangen wird (siehe **Konfigurieren der Fälligkeitszeit für dynamische Adressen**).

Um die Seite *Dynamische Adressen* anzuzeigen, klicken Sie im Navigationsfenster auf **MAC-Adresstabellen** > **Dynamische Adressen**.

HINWEIS Wenn die Tabelle der dynamischen Adressen die maximale Anzahl von Einträgen enthält, kann das Laden der Seite bis zu 45 Sekunden dauern.

Standardmäßig werden in der Tabelle der dynamischen Adressen alle dynamisch gelernten MAC-Adressen angezeigt. Sie können Filterkriterien eingeben und auf **Los** klicken, um die Anzeige zu filtern. Mit dem Filter *VLAN-ID* können Sie Tabelleneinträge für ein bestimmtes VLAN anzeigen. Mit dem Filter *MAC-Adresse* können Sie Einträge für eine bestimmte MAC-Adresse anzeigen. Mit dem Filter *Schnittstelle* können Sie Einträge für einen bestimmten Port bzw. eine bestimmte LAG anzeigen. Klicken Sie auf **Filter löschen**, um alle Einträge zu löschen.

In der Tabelle der dynamischen Adressen werden für jeden gelernten Eintrag die folgenden Felder angezeigt:

- **VLAN-ID**: Das VLAN, in dem die MAC-Adresse gelernt wurde. Frames werden nur an die Schnittstelle weitergeleitet, wenn sie diesem VLAN zugeordnet sind.
- **MAC-Adresse**: Die dynamisch gelernte MAC-Adresse.
- **Schnittstelle**: Der Port, an dem die MAC-Adresse dynamisch gelernt wurde. Frames, in denen diese MAC-Adresse und dieses VLAN als Ziel angegeben ist, werden an diesen Port weitergeleitet.

Klicken Sie auf **Tabelle löschen**, um alle dynamischen MAC-Adresseinträge aus der Tabelle zu löschen.

8

Multicast

In diesem Kapitel wird das Konfigurieren der Multicast-Protokolle beschrieben, mit denen Pakete von einer Quelle an mehrere Ziele weitergeleitet werden.

Das Kapitel enthält die folgenden Themen:

- **Multicast-Eigenschaften**
- **Konfigurieren von MAC-Gruppenadressen**
- **Konfigurieren von IGMP-Snooping**
- **Konfigurieren von MLD-Snooping**
- **Konfigurieren von IGMP-Multicast-Routerschnittstellen**
- **Konfigurieren von MLD-Multicast-Routerschnittstellen**

Multicast-Protokolle übermitteln Pakete von einer Quelle an mehrere Empfänger. Sie ermöglichen eine bessere Bandbreitenauslastung und tragen dazu bei, die Verarbeitungslast von Hosts und Routern zu reduzieren. Daher sind sie ideal für die Verwendung in Anwendungen wie beispielsweise Video- und Audiokonferenzen, Whiteboard-Tools und Börsenticker.

Der Switch verwaltet eine Multicast-Weiterleitungstabelle, um Weiterleitungsentscheidungen für eingehende Pakete mit einer Multicast-Ziel-MAC-Adresse zu treffen. Wenn Multicasts auf bestimmte Ports beschränkt sind, wird die Weiterleitung des Verkehrs an Netzwerkbereiche ohne Empfänger verhindert. Wenn ein Paket im Switch eintrifft, wird die Ziel-MAC-Adresse mit der VLAN-ID kombiniert, und es wird eine Suche in der Multicast-Weiterleitungstabelle ausgeführt. Wenn keine Übereinstimmung gefunden wird, wird das Paket je nach Switch-Konfiguration entweder an alle Ports im VLAN geflutet oder verworfen. Wenn eine Übereinstimmung gefunden wird, wird das Paket nur an die Ports weitergeleitet, die Mitglieder der jeweiligen Multicast-Gruppe sind.

Multicast-Einträge können durch *Snooping* (Mithören) der Layer 3-Protokolle zur Verwaltung von Multicast-Mitgliedschaften gelernt werden:

- IPv4-Multicast-Gruppenadressen können über das IGMP-Protokoll (Internet Group Management Protocol) gelernt werden.
- IPv6-Multicast-Gruppenadressen können über das MLD-Protokoll (Multicast Listener Discovery) gelernt werden.

Schnittstellen mit IGMP- und MLD-Multicast-Routern für ein bestimmtes VLAN können statisch oder dynamisch konfiguriert sein. Die Multicast-Router verwenden IGMP und MLD zum Verwalten der Mitgliedschaft in den Multicast-Gruppen. Ein Multicast-Router ist außerdem erforderlich, damit der Switch IGMP/MLD-Snooping in einem VLAN richtig unterstützt.

Multicast-Eigenschaften

Auf der Seite *Multicast-Eigenschaften* können Sie angeben, wie Multicast-Pakete innerhalb von VLANs weitergeleitet werden.

Konfigurieren eines Multicast-Weiterleitungsmodus für alle VLANs

Sie können für jedes VLAN einzeln konfigurieren, wie der Switch Multicast-Pakete weiterleitet. Wenn Sie ein VLAN erstellen, wird eine Standardoption für die Multicast-Weiterleitung zugewiesen. Sie können die Einstellung „Globaler Multicast-Modus“ verwenden, um einen ausgewählten Weiterleitungsmodus für alle zurzeit im Switch konfigurierten VLANs festzulegen. Mit der globalen Einstellung wird keine Standardeinstellung für später konfigurierte VLANs erstellt, sondern es wird lediglich sichergestellt, dass alle vorhandenen VLANs mit dem angegebenen Modus konfiguriert sind.

So konfigurieren Sie alle aktuellen VLANs mit einem bestimmten Multicast-Weiterleitungsmodus:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Multicast** > **Eigenschaften**.

SCHRITT 2 Wählen Sie einen globalen Multicast-Modus aus, um diesen auf alle VLANs anzuwenden. Wenn ein VLAN mit einem anderen Modus konfiguriert ist, wird das VLAN auf den folgenden Modus zurückgesetzt:

- **Nicht registrierte weiterleiten**: Wenn ein Paket von einem VLAN mit einer Multicast-Zieladresse empfangen wird und kein Port im VLAN für den Empfang von Multicast-Paketen für diese Adresse registriert ist, wird das Paket an alle Ports im VLAN geflutet. Für das Akzeptieren oder Verwerfen der Pakete sind die Hosts zuständig. Wenn ein Multicast-Paket empfangen wird und Ports für den Empfang des Pakets registriert sind, wird das Paket nur an die registrierten Ports gesendet.
- **Alle weiterleiten**: Alle von einem VLAN empfangenen Multicast-Pakete werden unabhängig von den Port-Registrierungen für Multicast-Adressen an alle Ports im VLAN geflutet.
- **Filter nicht registriert**: Wenn ein Paket von einem VLAN für eine Multicast-Zieladresse empfangen wird und kein Port im VLAN für den Empfang von Multicast-Paketen für diese Adresse registriert ist, werden die Pakete verworfen.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren von Multicast-Eigenschaften für ein VLAN

So konfigurieren Sie ein VLAN mit einem anderen Weiterleitungsmodus als der Einstellung „Globaler Multicast-Modus“:

SCHRITT 1 Wählen Sie im Menü „VLAN-ID“ das VLAN aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 2 Wählen Sie den Multicast-Modus gemäß der Beschreibung in **Konfigurieren eines Multicast-Weiterleitungsmodus für alle VLANs** aus.

SCHRITT 3 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren von MAC-Gruppenadressen

Auf der Seite *MAC-Gruppenadresse* können Sie Zuordnungen zwischen MAC-Adressen von Multicast-Gruppen und VLANs im Switch konfigurieren. Sie können statische Zuordnungen konfigurieren, oder die Zuordnungen können dynamisch über IGMP- oder MLD-Snooping gelernt werden. Wenn ein Paket für eine Multicast-Gruppenadresse empfangen wird, die mit einem Eintrag in der Tabelle für MAC-Gruppenadressen übereinstimmt, wird das Paket nur an Ports gesendet, die Mitglieder des VLAN sind.

Der Switch unterstützt bis zu 32 statische und dynamische Einträge in der Tabelle für MAC-Gruppenadressen. Ein dynamischer Eintrag wird nach Ablauf der Fälligkeitszeit entfernt, wenn während eines konfigurierbaren Zeitraums keine Pakete für die MAC-Gruppenadresse empfangen werden (Informationen zum Konfigurieren der Zeitspanne für die IGMP-Gruppenmitgliedschaft finden Sie im Abschnitt zur Seite *IGMP-Snooping*).

Anzeigen der Tabelle für MAC-Gruppenadressen

Um die Tabelle für MAC-Gruppenadressen anzuzeigen, klicken Sie im Navigationsfenster auf **Multicast** > **MAC-Gruppenadresse**.

Standardmäßig werden in der Tabelle alle Einträge angezeigt. Mit den Filtern „VLAN-ID“ und „MAC-Gruppenadresse“ können Sie nur Einträge anzeigen, die mit den angegebenen Werten übereinstimmen. Die folgenden Felder werden angezeigt:

- **Typ**: Gibt an, ob der Eintrag statisch konfiguriert oder dynamisch gelernt wurde.
- **VLAN-ID**: Die VLAN-ID, an die Multicast-Pakete weitergeleitet werden, die mit der angegebenen Multicast-MAC-Adresse übereinstimmen.
- **MAC-Gruppenadresse**: MAC-Adresse einer Multicast-Gruppe im Hexadezimalformat, die mit der Ziel-MAC-Adresse eines eingehenden Pakets verglichen wird.

Hinzufügen eines statischen Eintrags zur Tabelle für MAC-Gruppenadressen

So fügen Sie eine statische Multicast-MAC-Adresse hinzu und ordnen diese einem VLAN zu:

SCHRITT 1 Klicken Sie auf der Seite *MAC-Gruppenadresse* auf **Hinzufügen**.

SCHRITT 2 Geben Sie die Parameter ein:

- **VLAN-ID**: Wählen Sie ein VLAN aus der Liste aus.
- **Adresstyp**: Wählen Sie „IPv4“ aus, um eine Adresse in der 32-Bit-IPv4-Schreibweise (xxx.xxx.xxx.xxx) anzugeben, oder wählen Sie „MAC“ aus, um die Adresse im 6-Byte-Hexadezimalformat (xx.xx.xx.xx.xx.xx) anzugeben.
- **MAC-Gruppenadresse**: Geben Sie die Adresse im ausgewählten Format ein. Bei einer IPv4-Adresse werden die 23 am wenigsten signifikanten Bit einer Ethernet-MAC-Adresse zugeordnet.

SCHRITT 3 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Der Eintrag wird in der Tabelle für MAC-Gruppenadressen angezeigt.

Konfigurieren der Mitgliedschaft von Ports in MAC-Adressgruppen

Standardmäßig werden an eine Multicast-MAC-Adresse gerichtete Pakete an alle Ports geflutet. Ports können dynamisch durch Austausch von IGMP-Paketen Mitglieder einer bestimmten MAC-Adressgruppe werden. Alternativ können Sie die Ports statisch als Mitglieder konfigurieren.

So zeigen Sie Details an und konfigurieren die Port-Mitglieder einer Multicast-Gruppenadresse:

SCHRITT 1 Wählen Sie auf der Seite *MAC-Gruppenadresse* einen Eintrag aus, und klicken Sie auf **Details**.

Auf der Seite werden die Mitglieder der Multicast-Gruppenadresse an jedem Port angegeben. Der Status „Ohne“ bedeutet, dass der Port keine Mitglieder hat.

SCHRITT 2 Klicken Sie auf **Statisch**, um einen Port als statisches Mitglied der Multicast-MAC-Adresse zu konfigurieren.

SCHRITT 3 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren von IGMP-Snooping

Das IGMP-Protokoll (Internet Group Management Protocol) ist ein Layer 3-Internetprotokoll, mit dem Sie in IPv4-Netzwerken die Mitgliedschaft in Multicast-Gruppen verwalten können. (IPv6-Multicast-Verkehr wird wie unter **Konfigurieren von MLD-Snooping** beschrieben mithilfe des MLD-Protokolls verwaltet.) IGMP-Kommunikation findet zwischen IGMP-Routern und IGMP-fähigen Hosts (Clients) statt. Obwohl der Switch IGMP-Pakete weder initiiert noch beantwortet, können Sie ihn zum Mithören der IGMP-Kommunikation zwischen über den Switch verbundenen Routern und Clients konfigurieren. Außerdem können Sie konfigurieren, dass der Switch Weiterleitungsentscheidungen trifft, mit deren Hilfe nicht notwendiger Netzwerkverkehr reduziert werden kann. Dieses Mithörverhalten wird als IGMP-Snooping bezeichnet. Dies ist besonders vorteilhaft bei Multicast-Netzwerkverkehr mit hoher Bandbreite.

Normalerweise leitet der Switch bei Empfang von Broadcast- oder Multicast-Paketen an jedes der verbleibenden Netzwerksegmente eine Kopie weiter. Diese Methode eignet sich gut für Broadcast-Pakete, die von allen verbundenen Knoten verarbeitet werden sollen. Bei Multicast-Paketen kann diese Methode jedoch zu einer weniger effizienten Nutzung der Netzwerkbandbreite führen, insbesondere wenn das Paket nur für eine kleine Anzahl von Knoten bestimmt ist; die Pakete werden an Netzwerksegmente geflutet, in denen kein Knoten Interesse daran hat, das Paket zu empfangen.

Mithilfe von IGMP-Snooping kann der Switch Mitgliedschaftsberichte von IGMP-Clients und Abfragen von Routern abfangen. Wenn aus der abgefangenen Kommunikation hervorgeht, dass in einem Link kein IGMP-Client für eine bestimmte Multicast-Zieladresse innerhalb eines VLAN vorhanden ist, sendet der Switch keine Kopien dieser Multicast-Pakete an dieses Netzwerksegment.

Sie können IGMP-Snooping für jedes VLAN aktivieren oder deaktivieren. Wenn die Funktion für ein VLAN aktiviert ist, wird IGMP-Snooping an allen Schnittstellen ausgeführt, die Mitglieder dieses VLAN sind.

Obwohl IGMP auf IP-Multicast-Adressen basiert, erfolgt die eigentliche Multicast-Weiterleitung im Switch auf der Grundlage der äquivalenten MAC-Adressen.

So konfigurieren Sie IGMP-Snooping:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Multicast** > **IGMP-Snooping**.

SCHRITT 2 Wählen Sie für den IGMP-Snooping-Status die Option „Aktivieren“ aus.

SCHRITT 3 Klicken Sie in der IGMP-Snooping-Tabelle auf **Hinzufügen**.

SCHRITT 4 Wählen Sie unter **VLAN-ID** das VLAN aus, das IGMP-Snooping unterstützen soll.

SCHRITT 5 Konfigurieren Sie die folgenden Einstellungen:

- **IGMP Fast Leave**: Wählen Sie „Aktivieren“ aus, damit der Switch einen Port (oder eine LAG) sofort aus der Multicast-Weiterleitungstabelle entfernen kann, wenn er eine IGMP-Leave-Nachricht für diese Multicast-Gruppe empfängt. Wenn die Option aktiviert ist, entfernt der Switch den Port, ohne vorher allgemeine Abfragen an die Schnittstelle zu senden. Aktivieren Sie den Fast Leave-Modus nur für VLANs, in denen mit jedem Port nur ein Host verbunden ist. Dadurch verhindern Sie das versehentliche Verwerfen der anderen Hosts, die mit dem gleichen Port verbunden sind und weiterhin Interesse daran haben, an diese Gruppe gerichteten Multicast-Verkehr zu empfangen.
- **IGMP: Zeitspanne für Gruppenmitgliedschaft**: Geben Sie an, wie viele Sekunden der Switch auf einen IGMP-Mitgliedschaftsbericht von einer bestimmten Gruppe an einer bestimmten Schnittstelle wartet, bevor die Schnittstelle aus dem Eintrag in der Multicast-Weiterleitungsdatenbank gelöscht wird. Wählen Sie „Standard“ aus, um 260 Sekunden anzugeben, oder wählen Sie „Benutzerdefiniert“ aus, und geben Sie einen Wert im Bereich von 2 bis 3600 Sekunden ein.
- **IGMP: maximale Reaktionszeit**: Geben Sie an, wie viele Sekunden der Switch auf eine Antwort wartet, nachdem er eine Abfrage an eine Schnittstelle gesendet hat, da er für eine bestimmte Gruppe an dieser Schnittstelle keinen Bericht erhalten hat. Dieser Wert muss kleiner sein als der Wert für „IGMP: Zeitspanne für Gruppenmitgliedschaft“. Wählen Sie „Standard“ aus, um 10 Sekunden anzugeben, oder wählen Sie „Benutzerdefiniert“ aus, und geben Sie einen Wert im Bereich von 1 bis 25 Sekunden ein.
- **IGMP: MRouter-Ablaufzeit**: Geben Sie an, wie viele Sekunden der Switch auf den Empfang einer Abfrage an einer dynamischen MRouter-Schnittstelle wartet, bevor die Schnittstelle aus dem VLAN entfernt wird. Der Wert 0 gibt ein unbegrenztes Timeout an (das heißt kein Ablauf). Wählen Sie „Standard“ aus, um 0 Sekunden anzugeben, oder wählen Sie „Benutzerdefiniert“ aus, und geben Sie einen Wert im Bereich von 0 bis 3600 Sekunden ein.

SCHRITT 6 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Der neue VLAN-Eintrag wird in der IGMP-Snooping-Tabelle angezeigt.

SCHRITT 7 Für dieses VLAN (oder für alle VLANs) muss eine IGMP-Mrouter-Schnittstelle konfiguriert sein. Informationen hierzu finden Sie unter **Konfigurieren von IGMP-Multicast-Routerschnittstellen**.

Konfigurieren von MLD-Snooping

MLD ist ein Protokoll, das von IPv6-Multicast-Routern verwendet wird, um die Anwesenheit von Multicast-Listenern (Knoten, die IPv6-Multicast-Pakete empfangen sollen) an den direkt verbundenen Links zu erkennen und zu erkennen, welche Multicast-Pakete für Nachbarknoten von Interesse sind. MLD wurde von IGMP abgeleitet, das eine ähnliche Funktion für IPv4-Multicast-Verkehr ausübt (siehe **Konfigurieren von IGMP-Snooping**).

Wenn MLD-Snooping aktiviert ist, leitet der Switch selektiv IPv6-Multicast-Pakete an eine Liste von Ports weiter, die die Daten empfangen sollen, anstatt die Pakete an alle Ports im VLAN zu fluten. Die Liste wird durch Snooping von IPv6-Multicast-Kontrollpaketen erstellt.

HINWEIS Der Switch unterstützt MLD-Snooping von Paketen der MLD-Versionen 1 und 2. Sie können den Switch so konfigurieren, dass MLD-Snooping und IGMP-Snooping gleichzeitig ausgeführt werden.

Sie können MLD-Snooping für jedes VLAN getrennt aktivieren oder deaktivieren. Obwohl MLD auf IPv6-Adressen basiert, erfolgt die eigentliche Multicast-Weiterleitung im Switch auf der Grundlage der äquivalenten MAC-Adressen.

So aktivieren und konfigurieren Sie MLD-Snooping:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Multicast** > **MLD-Snooping**.

In der MLD-Snooping-Tabelle werden die einzelnen VLANs aufgeführt, in denen die Funktion aktiviert ist.

SCHRITT 2 Wählen Sie für den MLD-Snooping-Status die Option „Aktivieren“ aus.

SCHRITT 3 Klicken Sie in der MLD-Snooping-Tabelle auf **Hinzufügen**.

SCHRITT 4 Wählen Sie unter **VLAN-ID** das VLAN aus, das MLD-Snooping unterstützen soll.

SCHRITT 5 Geben Sie die Parameter ein:

- **MLD Fast Leave**: Wählen Sie „Aktivieren“ aus, damit der Switch einen Port (oder eine LAG) sofort aus der Multicast-Weiterleitungstabelle entfernen kann, wenn er eine MLD-Leave-Nachricht für diese Multicast-Gruppe empfängt. Wenn die Option aktiviert ist, entfernt der Switch den Port, ohne vorher allgemeine MAC-basierte Abfragen an die Schnittstelle zu senden. Aktivieren Sie den Fast Leave-Modus nur für VLANs, in denen mit jedem Port nur ein Host verbunden ist. Dadurch verhindern Sie das versehentliche Verwerfen der anderen Hosts, die mit dem gleichen Port verbunden sind und weiterhin Interesse daran haben, an diese Gruppe gerichteten Multicast-Verkehr zu empfangen.
- **MLD: Zeitspanne für Gruppenmitgliedschaft**: Geben Sie an, wie viele Sekunden der Switch auf einen MLD-Mitgliedschaftsbericht von einer bestimmten Gruppe an einer bestimmten Schnittstelle wartet, bevor die Schnittstelle aus dem Eintrag in der Multicast-Weiterleitungsdatenbank gelöscht wird. Wählen Sie „Standard“ aus, um 260 Sekunden anzugeben, oder wählen Sie „Benutzerdefiniert“ aus, und geben Sie einen Wert im Bereich von 2 bis 3600 Sekunden ein.
- **MLD: maximale Reaktionszeit**: Geben Sie an, wie viele Sekunden der Switch auf eine Antwort wartet, nachdem er eine Abfrage an eine Schnittstelle gesendet hat, da er für eine bestimmte Gruppe an dieser Schnittstelle keinen Bericht erhalten hat. Dieser Wert muss kleiner sein als der Wert für „MLD: Zeitspanne für Gruppenmitgliedschaft“. Wählen Sie „Standard“ aus, um 10 Sekunden anzugeben, oder wählen Sie „Benutzerdefiniert“ aus, und geben Sie einen Wert im Bereich von 1 bis 65 Sekunden ein.

- **MLD: Mrouter-Ablaufzeit**: Geben Sie an, wie viele Sekunden der Switch auf den Empfang einer Abfrage an einer Schnittstelle wartet, bevor die Schnittstelle aus der Liste der Schnittstellen mit angeschlossenem MLD-Multicast-Router entfernt wird. Der Wert 0 gibt ein unbegrenztes Timeout an (das heißt kein Ablauf). Wählen Sie „Standard“ aus, um 0 Sekunden anzugeben, oder wählen Sie „Benutzerdefiniert“ aus, und geben Sie einen Wert im Bereich von 0 bis 3600 Sekunden ein.

SCHRITT 6 Klicken Sie auf **Übernehmen** und dann auf **Schließen**.

Der neue VLAN-Eintrag wird in der MLD-Snooping-Tabelle angezeigt.

SCHRITT 7 Für dieses VLAN muss eine MLD-Mrouter-Schnittstelle konfiguriert sein. Informationen hierzu finden Sie unter **Konfigurieren von MLD-Multicast-Routerschnittstellen**.

Konfigurieren von IGMP-Multicast-Routerschnittstellen

Zum Verwalten der IGMP-Clients in einem VLAN muss ein IGMP-Router vorhanden sein. Der Switch muss für jedes VLAN, das IGMP-Snooping unterstützt, statisch mit mindestens einer Schnittstelle mit einem IGMP-Router konfiguriert sein oder eine solche Schnittstelle dynamisch lernen. Eine Schnittstelle mit einem IGMP-Router wird als IGMP-Multicast-Routerschnittstelle bezeichnet. Ein VLAN, für das IGMP-Snooping aktiviert ist, muss über mindestens eine IGMP-Multicast-Routerschnittstelle verfügen. Ein IGMP-Multicast-Router kann ein oder mehrere VLANs bedienen.

So aktivieren Sie einen Switch-Port oder eine LAG als IGMP-Mrouter-Schnittstelle und konfigurieren die zugehörigen Einstellungen:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Multicast** > **IGMP-Mrouter**.

Standardmäßig werden in der IGMP-MRouter-Tabelle alle Switch-Ports aufgeführt. Um LAGs anzuzeigen, wählen Sie in der Liste der Schnittstellentypen den Typ „LAG“ aus.

SCHRITT 2 Wählen Sie den Port oder die LAG aus, den bzw. die Sie konfigurieren möchten, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Wählen Sie für den Modus die Option „Aktivieren“ aus.

SCHRITT 4 Um die VLANs anzugeben, in denen diese Schnittstelle als IGMP-Mrouter-Schnittstelle verwendet wird, verschieben Sie das VLAN wie unten beschrieben in die Liste „Ausgewählt“.

- So wählen Sie ein VLAN aus: Klicken Sie in der Liste „Verfügbar“ auf ein VLAN, und klicken Sie dann auf die Schaltfläche mit dem Pfeil nach rechts, um das VLAN in die Liste „Ausgewählt“ zu verschieben.
- So entfernen Sie ein VLAN: Klicken Sie in der Liste „Ausgewählt“ auf ein VLAN, und klicken Sie dann auf die Schaltfläche mit dem Pfeil nach links, um das VLAN in die Liste „Verfügbar“ zu verschieben.

SCHRITT 5 Klicken Sie auf **Übernehmen** und dann auf **Schließen**.

In der IGMP-Mrouter-Tabelle wird für die Schnittstelle in der Spalte „Modus“ die Option *Aktivieren* angezeigt, und die ausgewählten VLANs werden aufgeführt.

Konfigurieren von MLD-Multicast-Routerschnittstellen

Zum Verwalten der MLD-Clients in einem VLAN muss ein MLD-Multicast-Router vorhanden sein. Der Switch muss für jedes VLAN, das MLD-Snooping unterstützt, statisch mit mindestens einer Schnittstelle mit einem MLD-Multicast-Router konfiguriert sein oder eine solche Schnittstelle dynamisch lernen. Die Schnittstelle mit einem MLD-Multicast-Router wird als MLD-Multicast-Routerschnittstelle bezeichnet. Ein VLAN, für das MLD-Snooping aktiviert ist, muss über mindestens eine MLD-Multicast-Routerschnittstelle verfügen. Ein MLD-Multicast-Router kann ein oder mehrere VLANs bedienen.

So aktivieren Sie einen Switch-Port oder eine LAG als MLD-Mrouter-Schnittstelle:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Multicast** > **IGMP-Mrouter**.

Standardmäßig werden in der MLD-MRouter-Tabelle alle Switch-Ports aufgeführt. Um LAGs anzuzeigen, wählen Sie in der Liste der Schnittstellentypen den Typ „LAG“ aus.

SCHRITT 2 Wählen Sie den Port oder die LAG aus, den bzw. die Sie konfigurieren möchten, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Wählen Sie für den Modus die Option „Aktivieren“ aus.

SCHRITT 4 Verwenden Sie den nach links bzw. nach rechts zeigenden Pfeil, um VLAN-IDs zwischen den Listen „Verfügbar“ und „Ausgewählt“ zu verschieben. Die VLANs in der Liste „Ausgewählt“ verwenden diesen Port bzw. diese LAG als MLD-Mrouter-Schnittstelle.

SCHRITT 5 Klicken Sie auf **Übernehmen** und dann auf **Schließen**.

In der MLD-Mrouter-Tabelle wird für die Schnittstelle in der Spalte „Modus“ die Option „Aktivieren“ angezeigt, und die enthaltenen VLANs werden aufgeführt.

9

IP-Konfiguration

In diesem Kapitel werden die Clientfunktionen für das Address Resolution Protocol (ARP) und das Domain Name System (DNS) beschrieben.

Das Kapitel enthält die folgenden Themen:

- **ARP-Tabelle**
- **Domain Name System**

ARP-Tabelle

Im Switch wird eine ARP-Tabelle (Address Resolution Protocol) verwaltet. Jeder Eintrag in der Tabelle enthält die IP-Adresse und die MAC-Adressen eines Geräts, das bereits mit dem Switch kommuniziert hat.

Auf der Seite *ARP* können Sie die aus dem Verwaltungs-VLAN bezogenen ARP-Einträge anzeigen. Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **IP-Konfiguration** > **ARP**.

Sie können auf **ARP löschen** klicken, um alle Einträge mit Ausnahme der IP-Adresse und der MAC-Adresse des Verwaltungs-Ports aus der Tabelle zu löschen.

Domain Name System

Der Switch unterstützt IPv4-DNS-Clientfunktionen. Wenn der Switch als DNS-Client aktiviert ist, stellt er für andere Anwendungen im Switch (beispielsweise Ping, RADIUS, Syslog, automatische Konfiguration und TFTP) einen Suchdienst für Hostnamen bereit. Sie können den Switch mit DNS-Servern konfigurieren, die Hostnamen in IP-Adressen auflösen. Außerdem können Sie den Switch mit statischen Zuordnungen zwischen Hostnamen und IP-Adressen konfigurieren, um den DNS-Server zu umgehen.

Weitere Informationen zu den Konfigurationsseiten im Menü „IP-Konfiguration > Domain Name System“ finden Sie in den folgenden Themen:

- **Konfigurieren von DNS-Servern**
- **Zuordnung von Hostnamen**

Konfigurieren von DNS-Servern

Um einen Hostnamen in eine IP-Adresse aufzulösen, stellt der Client eine Verbindung mit einem oder mehreren DNS-Servern her. DNS-Server können dynamisch gelernt werden, wenn die Verwaltungsschnittstelle ebenfalls als DHCP-Client konfiguriert ist (siehe **Verwaltungsschnittstelle**). Sie können DNS-Server auch auf der Seite *DNS-Server* statisch konfigurieren.

Die DNS-Clientfunktionalität ist standardmäßig aktiviert.

Konfigurieren von globalen DNS-Einstellungen

So konfigurieren Sie den DNS-Servermodus und globale Einstellungen:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **IP-Konfiguration** > **Domain Name System** > **DNS-Server**.

SCHRITT 2 Wählen Sie gegebenenfalls die Option „Aktivieren“ aus, um die DNS-Clientfunktionalität im Switch zu implementieren.

SCHRITT 3 Geben Sie die folgenden Parameter ein:

- **Standarddomänenname**: Geben Sie einen Domänennamen an, mit dem nicht qualifizierte Hostnamen vervollständigt werden sollen. *finance.yahoo.com* ist beispielsweise ein vollständiger Hostname. Wenn nur der nicht qualifizierte Hostname *finance* angegeben ist , wird der Standarddomänenname *yahoo.com* mit einem Punkt dazwischen angefügt.

Lassen Sie in Ihrem Eintrag den Punkt weg, der den nicht qualifizierten Hostnamen vom Domänennamen trennt. Gültig sind alphanumerische Zeichen im Bereich von 1 - 255.

- **Domäne: erneuter Versuch**: Gibt die Anzahl der erneuten Versuche zum Senden von DNS-Abfragen an. Gültig sind Werte im Bereich von 0 - 100, und der Standardwert lautet 2.
- **Domänen-Timeout**: Geben Sie an, wie viele Sekunden der Switch auf eine Antwort auf eine DNS-Abfrage wartet. Gültig sind Werte im Bereich von 0 - 3600 Sekunden. Der Standardwert lautet 3 Sekunden.

Hinweis: Wenn die Standarddomänennamen aus DHCP-Antwortnachrichten gelernt werden, werden die Namen in der Liste mit den Standarddomänennamen angezeigt.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Hinzufügen von DNS-Servern

In der DNS-Servertabelle werden die konfigurierten Server aufgeführt.

So fügen Sie einen DNS-Server hinzu:

SCHRITT 1 Klicken Sie auf **Hinzufügen**.

SCHRITT 2 Geben Sie die IPv4- oder IPv6-Adresse des DNS-Servers an.

SCHRITT 3 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Änderungen werden in der aktuellen Konfiguration gespeichert und der Server wird in der DNS-Servertabelle angezeigt.

Zuordnung von Hostnamen

Auf der Seite *Host-Zuordnung* können Sie Zuordnungen zwischen Hostnamen und IP-Adressen anzeigen und konfigurieren. Sie können einen Hostnamen statisch einer IP-Adresse zuordnen. Außerdem können Sie Hostnamen anzeigen, die dynamisch über Anwendungen gelernt wurden, die den DNS-Suchdienst verwenden.

Konfigurieren von statischen DNS-Zuordnungen

In der Host-Zuordnungstabelle werden Hostnamen aufgeführt, die IP-Adressen auf dem Switch statisch zugewiesen sind. So konfigurieren Sie eine statische Hostnamenzuordnung:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **IP-Konfiguration** > **Domain Name System** > **Host-Zuordnung**.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie einen Hostnamen aus 1 - 255 alphanumerischen Zeichen ein. Der Hostname muss mit einem Buchstaben beginnen.

SCHRITT 4 Geben Sie eine IPv4- oder IPv6-Adresse ein, die dem Hostnamen zugeordnet werden soll.

SCHRITT 5 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Anzeigen und Löschen von dynamischen DNS-Einträgen

In der Tabelle für dynamische DNS-Einträge werden Hostnamen angezeigt, die von Anwendungen gelernt wurden, die DNS-Suchdienste verwenden. Wenn Sie beispielsweise einen Ping an einen Hostnamen senden, wird der DNS-Suchdienst aufgerufen, und eine zugeordnete IP-Adresse wird gelernt und der Tabelle hinzugefügt.

In der Tabelle für dynamische DNS-Einträge werden die folgenden Felder angezeigt:

- **Hostname**: Der der IP-Adresse zugewiesene Hostname (oder ein offizieller Hostname).
- **Gesamt**: Die Anzahl von Minuten der Reservierung des Hostnamens für diese Zuweisung.
- **Verstrichen**: Die Anzahl der Minuten, die seit der Zuweisung des Hostnamens verstrichen sind.
- **Typ**: Identifiziert den Hostnamen als einen der folgenden Typen:
  - **IP**: Der zugewiesene Hostname ist einer IP-Adresse zugeordnet.
  - **Autorisiert**: Der zugewiesene Hostname ist ein Alias oder Ersatzname für einen ordnungsgemäß angegebenen (offiziellen) Hostnamen. Beispielsweise kann *www.google.com* ein Hostnamenalias sein, das dem offiziellen Hostnamen *www.l.google.com* zugewiesen ist.

- **Adressen**: Wenn der Typ „IP“ entspricht, wird in diesem Feld die dem Hostnamen zugeordnete IPv4- oder IPv6-Adresse angezeigt. Wenn der Typ „Autorisiert“ entspricht, wird in diesem Feld der dem Alias zugeordnete autorisierte Hostname angezeigt. Einer autorisierten DNS-Adresse können mehrere Hostnamenaliase zugeordnet sein.

Um einen dynamischen Eintrag zu löschen, wählen Sie diesen aus, und klicken Sie auf **Löschen**. Um alle dynamischen Einträge aus der Tabelle zu löschen, klicken Sie auf **Alle dynamischen Einträge löschen**.

10

Sicherheit

In diesem Kapitel werden die Sicherheitsfunktionen für den Port, den Benutzer und den Server beschrieben.

Das Kapitel enthält die folgenden Themen:

- **RADIUS**
- **Kennwortsicherheit**
- **Regeln für Verwaltungszugriffsprofile**
- **Authentifizierungsmethoden**
- **Sturmsteuerung**
- **Portsicherheit**
- **802.1X**

RADIUS

Der Switch unterstützt die RADIUS-Clientfunktionalität (Remote Authorization Dial-In User Service). RADIUS ist bei Administratoren großer zugriffsbereiter Netzwerke das bevorzugte Protokoll für die Authentifizierung von Benutzern vor dem Zugriff. Zur sicheren Authentifizierung von Benutzern konfigurieren Sie einen RADIUS-Client und einen RADIUS-Server mit dem gleichen gemeinsamen Kennwort oder *geheimen Schlüssel*. Mithilfe dieses geheimen Schlüssels werden unidirektionale verschlüsselte Authentifikatoren erstellt, die in allen RADIUS-Paketen enthalten sind. Wenn ein böswilliger Benutzer den geheimen Schlüssel nicht kennt, ist die Wahrscheinlichkeit sehr gering, dass ihm das Spoofing von Paketen gelingt.

Der RADIUS-Client im Switch wird für die Authentifizierung des Verwaltungszugriffs und für die Port-Zugriffssteuerung nach IEEE 802.1X („dot1X“) verwendet (siehe **Regeln für Verwaltungszugriffsprofile** und **802.1X**).

Auf der Seite *RADIUS* können Sie globale RADIUS-Einstellungen konfigurieren und RADIUS-Server hinzufügen.

Konfigurieren von globalen RADIUS-Einstellungen

So konfigurieren Sie die globalen Einstellungen:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Sicherheit** > **RADIUS**.

SCHRITT 2 Geben Sie die Parameter ein:

- **Wiederholungen**: Die maximale Anzahl der Neuübertragungen von Anforderungen vom RADIUS-Client an den RADIUS-Server. Der Bereich lautet 1 bis 10. Der Standardwert ist 3.
- **Timeout für Antwort**: Geben Sie an, wie viele Sekunden der Switch auf die Antwort eines RADIUS-Servers auf eine Serveranforderung wartet, bevor er eine weitere Anforderung sendet. Der Bereich lautet 1 bis 30. Der Standardwert ist 3.
- **Stillstandszeit**: Geben Sie an, wie lange ein RADIUS-Server umgangen wird, der vom Switch für nicht verfügbar befunden wird. Durch die Umgehung nicht verfügbarer Switches können Sie die Switch-Antwortzeiten verbessern. Der Bereich lautet 0 bis 2000. Der Standardwert ist 0.
- **RADIUS-Attribut 4** (NAS-IP-Adresse): Wählen Sie diese Option aus, damit der Switch das NAS-Attribut (Network Access Server, Netzwerkzugangsserver) in Access Request-Pakete für den RADIUS-Server einschließt. Wenn diese Option deaktiviert ist, verwendet der RADIUS-Client die Adresse des Switch-Verwaltungs-Ports als NAS-IP-Adresse.
- **NAS-IP-Adresse**: Die in Access Request-Pakete einzuschließende IP-Adresse. Dieses Feld kann nur bearbeitet werden, wenn das RADIUS-Attribut 4 aktiviert ist. Die Adresse muss im Bereich des RADIUS-Servers für den NAS eindeutig sein.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Hinzufügen eines RADIUS-Servers

Sie können mehrere RADIUS-Server konfigurieren und Prioritätsstufen konfigurieren, die die Reihenfolge bestimmen, in der Verbindungen mit den Servern hergestellt werden.

VORSICHT Alle Verwaltungsbenutzer werden mit Lese-/Schreibberechtigungen erstellt. Sie müssen RADIUS-Serverbenutzer mit den gleichen Berechtigungsstufen konfigurieren; anderenfalls wird diesen Benutzern der Zugriff auf den Switch nicht gewährt.

So fügen Sie der RADIUS-Tabelle einen RADIUS-Server hinzu:

SCHRITT 1 Klicken Sie auf **Hinzufügen**

SCHRITT 2 Geben Sie die Parameter ein:

- **RADIUS-IP-Adresse/-Hostname**: Die IP-Adresse oder der Hostname des Servers.
- **Priorität**: Je niedriger der Prioritätswert, umso höher die tatsächliche Priorität des Servers. So hat beispielsweise ein mit dem Prioritätswert 1 konfigurierter Server eine höhere Priorität als ein mit dem Prioritätswert 2 konfigurierter Server. Wenn alle Server mit dem gleichen Prioritätswert oder mit dem Standardprioritätswert konfiguriert sind, versucht der Switch, die Verbindung mit den RADIUS-Servern in der Reihenfolge des Eingangs der Anforderung herzustellen. Der Bereich lautet 1 bis 65535. Der Standardwert ist 8.
- **Schlüsselzeichenfolge**: Eine Zeichenfolge für einen gemeinsamen geheimen Schlüssel, der für die Authentifizierung und Verschlüsselung der gesamten RADIUS-Kommunikation zwischen dem Switch und dem RADIUS-Server verwendet wird. Dieser geheime Schlüssel muss mit dem auf dem RADIUS-Server konfigurierten geheimen Schlüssel übereinstimmen. Sie können den geheimen Schlüssel bearbeiten, indem Sie den Eintrag löschen und einen neuen Eintrag mit dem gewünschten geheimen Schlüssel erstellen. Dabei muss es sich um einen alphanumerischen ASCII-Wert aus 32 bis 176 Zeichen handeln.
- **Authentifizierungs-Port**: Die für RADIUS-Authentifizierungsanforderungen und -antworten verwendete Port-Nummer. Der Standard-Port 1812 ist die allgemein bekannte IANA-Port-Nummer für RADIUS-Authentifizierungsdienste. Der Bereich lautet 1025 bis 65535. Der Standardwert ist 1812.

- **Meldungsauthentifikator**: Dieses Feld ist standardmäßig ausgewählt. Wenn diese Option aktiviert ist, ist das Meldungsauthentifikator-Attribut in RADIUS-Anforderungsnachrichten an den Server enthalten. Mit diesem Attribut werden die RADIUS-Nachrichten vor Spoofing und Manipulationen geschützt. Als Schlüssel wird der gemeinsame geheime Schlüssel verwendet. Wenn das RADIUS-Meldungsauthentifikator-Attribut im Paket enthalten ist, wird es vom Server überprüft. Wenn die Überprüfung nicht erfolgreich ist, verwirft der Server das Anforderungspaket.

SCHRITT 3 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Kennwortsicherheit

Auf der Seite *Kennwortsicherheit* können Sie die Merkmale sicherer Kennwörter für Verwaltungsbenutzer konfigurieren.

So konfigurieren Sie Kennwortsicherheitseinstellungen:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Sicherheit** > **Kennwortsicherheit**.

SCHRITT 2 Geben Sie die folgenden Parameter ein:

- **Kennwort-Mindestlänge**: Die Mindestanzahl an Zeichen, die für das Kennwort eines Verwaltungsbenutzers erforderlich ist. Geben Sie 0 an, um die Kennwortlänge auf einen Bereich von 1 - 7 Zeichen festzulegen. Alternativ können Sie eine konkrete Kennwortlänge festlegen, indem Sie einen Wert im Bereich von 8 - 64 Zeichen verwenden.
- **Kennwortfälligkeitszeit**: Aktivieren Sie das Kontrollkästchen, und geben Sie ein, nach welcher Zeit ein Kennwort abläuft (1 - 365 Tage). Wenn das Kennwort abläuft, kann der Benutzer den Vorgang erst fortsetzen, wenn er ein neues Kennwort eingegeben hat.

SCHRITT 3 Wählen Sie für das Feld „Sicherheitsüberprüfung“ die Option „Aktivieren“ aus, um die Typen der auszuführenden Überprüfungen zu konfigurieren.

- **Schlüsselwort-Ausschlussüberprüfung für Kennwort**: Wählen Sie „Aktivieren“ aus, damit der Switch beim Versuch des Benutzers, das Kennwort zu erstellen oder zu ändern, überprüft, ob in einem Kennwort vorkonfigurierte Schlüsselwörter vorkommen. Die vorkonfigurierten Schlüsselwörter lauten *cisco* und *ocsic*.

- **Benutzernamenüberprüfung für Kennwort**: Wählen Sie „Aktivieren“ aus, um zu verhindern, dass Benutzer beim Erstellen oder Ändern von Kennwörtern ihren Benutzernamen im Kennwort verwenden.
- **Zeichen kann maximal dreimal hintereinander wiederholt werden**: Wählen Sie „Aktivieren“ aus, damit der Switch überprüft, ob ein Zeichen im Kennwort mehr als dreimal hintereinander wiederholt wird.
- **Mindestanzahl an Zeichenklassen**: Aktivieren Sie das Kontrollkästchen, und geben Sie die Mindestanzahl an Zeichenklassen ein, die in der Kennwortzeichenfolge enthalten enthalten sein müssen. Folgende vier Zeichenklassen sind möglich: Großbuchstaben, Kleinbuchstaben, Zahlen und auf einer Standardtastatur verfügbare Sonderzeichen.

SCHRITT 4 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Regeln für Verwaltungszugriffsprofile

Auf der Seite *Regeln für Verwaltungszugriffsprofile* können Sie ein Profil und Regeln für den Zugriff auf das Gerät zu Verwaltungszwecken definieren.

Sie können den Zugriff auf bestimmte Benutzernamen, Ingress-Ports oder LAGs und Quell-IP-Adressen beschränken.

Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **Sicherheit** > **Regeln für Verwaltungszugriffsprofile**.

In der Zugriffsprofiltabelle wird der Profilname des zurzeit konfigurierten Profils (falls vorhanden) angegeben. In der Profilregeltabelle werden die vorhandenen Regeln für das Profil angezeigt. Standardmäßig sind im Switch keine Zugriffsprofile oder Regeln konfiguriert. Sie können nur ein Profil erstellen und aktivieren, und alle Regeln, die Sie erstellen, werden diesem Profil zugewiesen.

Konfigurieren von Zugriffsprofilen und Regeln

So erstellen Sie ein Zugriffsprofil und weisen diesem Regeln zu:

SCHRITT 1 Klicken Sie in der Zugriffsprofiltabelle auf **Hinzufügen**.

SCHRITT 2 Geben Sie den Zugriffsprofilnamen an, und wählen Sie die Option „Aktivieren“ aus.

SCHRITT 3 Klicken Sie auf **Übernehmen** und dann auf **Schließen**.

Das neue Profil wird in der Zugriffsprofiltabelle angezeigt. Nun können Sie dem Profil Regeln hinzufügen.

SCHRITT 4 Klicken Sie in der Profilregeltabelle auf **Hinzufügen**.

SCHRITT 5 Geben Sie beliebige der folgenden Parameter an, um den Zugriff einzuschränken oder zuzulassen:

- **Regelpriorität**: Die Regeln werden nach aufsteigender Priorität mit der eingehenden Verwaltungsanforderung verglichen. Wenn eine Regel übereinstimmt, wird die angegebene Aktion ausgeführt, und die Regeln mit niedrigerer Priorität werden ignoriert. Wenn Sie beispielsweise für die Quell-IP-Adresse 10.10.10.10 mit Priorität 1 die Option „Zulassen“ konfigurieren und für die Quell-IP-Adresse 10.10.10.10 mit Priorität 2 die Option „Verweigern“ konfigurieren und das Profil aktiv ist, wird dieser IP-Adresse der Zugriff gewährt, und die zweite Regel wird ignoriert. Der Bereich lautet 1 bis 16, wobei 1 der höchsten Priorität entspricht.
- **Verwaltungsmethode**: Die für den Zugriff auf die Switch-Konfiguration verwendete Methode. Standardmäßig ist HTTP-Zugriff zugelassen, sodass alle Benutzer das webbasierte Switch-Konfigurationsdienstprogramm verwenden können. Wenn Sie beispielsweise nur bestimmte Benutzer zulassen möchten, können Sie eine Regel erstellen, mit der allen Benutzern HTTP-Zugriff verweigert wird, und dann eine weitere Regel erstellen, in der bestimmte Benutzer zugelassen werden. Die Regel, die bestimmte Benutzer zulässt, muss eine höhere Regelpriorität haben als die Regel, die allen Benutzern den Zugriff verweigert.

  HINWEIS: Da HTTP die einzige Methode für den Verwaltungszugriff ist, sind die Optionen „HTTP“ und „Alle“ gleichwertig.
- **Aktion**: Wählen Sie die Aktion aus, die ausgeführt werden soll, wenn eine Übereinstimmung mit den Regelkriterien vorliegt.

- **Zulassen**: Die angegebene Schnittstelle, der angegebene Benutzer oder die angegebene IP-Adresse kann auf den Switch zugreifen, obwohl dies ansonsten durch eine Verweigerungsregel explizit nicht zulässig ist.
- **Verweigern**: Der angegebenen Schnittstelle, dem angegebenen Benutzer oder der angegebenen IP-Adresse wird der Zugriff auf den Switch verweigert.

- **Anwenden für Schnittstelle**: Wählen Sie „Alle“ aus, um diese Regel auf alle Schnittstellen (Ports und LAGs) anzuwenden. Wählen Sie alternativ „Benutzerdefiniert“ aus, und wählen Sie einen Port oder eine LAG aus, auf den bzw. auf die die Regel angewendet werden soll.
- **Anwenden für Benutzer**: Wählen Sie „Aktivieren“ aus, und wählen Sie den konfigurierten Benutzer aus, auf den die Regel angewendet werden soll. Auf diese Weise können Sie einen Verwaltungsbenutzer im System behalten und gleichzeitig verhindern, dass er auf den Switch zugreift, während diese Regel für das Zugriffsprofil gilt.
- **Anwenden auf Quell-IP-Adresse**: Wählen Sie „Alle“ aus, um die Regel auf alle Quell-IP-Adressen anzuwenden. Wählen Sie alternativ „Benutzerdefiniert“ aus, und geben Sie eine Quell-IPv4-Adresse und Maske an, auf die diese Regel angewendet werden soll.

SCHRITT 6 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Die neue Regel wird in der Profilregeltabelle angezeigt. Sie können die Regel auswählen und auf **Bearbeiten** klicken, um sie zu bearbeiten, oder auf **Löschen** klicken, um die Regel aus dem Zugriffsprofil zu entfernen.

HINWEIS Dem Benutzer **cisco** wird der Verwaltungszugriff nicht verweigert.

VORSICHT Wenn ein Profil aktiviert ist, das den Zugriff auf ein Intranet oder eine Domäne mit einer zurzeit aktiven Internetverwaltungssitzung verweigert, bleibt die Sitzung bis zur Abmeldung oder bis zum Timeout aktiv. Zukünftige Sitzungen werden durch das Profil blockiert. Aktive Sitzungen, in denen Internet Explorer 8 verwendet wird, werden sofort beendet, sofern die Verwaltungs-IP-Adresse des Switch nicht der Liste der lokalen Intranetsites in Internet Explorer hinzugefügt wird. Anweisungen finden Sie unter **Starten des webbasierten Switch-Konfigurationsdienstprogramms**.

Ändern und Löschen von Zugriffsprofilen und Regeln

Bevor Sie ein Zugriffsprofil löschen oder Regeln ändern können, müssen Sie das Profil deaktivieren.

So deaktivieren Sie ein Zugriffsprofil:

SCHRITT 1 Wählen Sie das Profil in der Zugriffsprofiltabelle aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 2 Deaktivieren Sie das Kontrollkästchen „Aktivieren“.

SCHRITT 3 Klicken Sie auf **Übernehmen** und dann auf **Schließen**.

Wenn Sie mit den Änderungen fertig sind, aktivieren Sie das Zugriffsprofil wieder.

So löschen Sie ein Zugriffsprofil (nachdem Sie dieses deaktiviert haben):

SCHRITT 1 Wählen Sie das Profil in der Zugriffsprofiltabelle aus.

SCHRITT 2 Klicken Sie auf **Löschen**.

So löschen Sie eine Profilregel (nachdem Sie das Zugriffsprofil deaktiviert haben):

SCHRITT 1 Wählen Sie die Regel in der Profilregeltabelle aus.

SCHRITT 2 Klicken Sie auf **Löschen**.

So ändern Sie eine Profilregel (nachdem Sie das Zugriffsprofil deaktiviert haben):

SCHRITT 1 Wählen Sie die Regel in der Profilregeltabelle aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 2 Geben Sie die neuen Einstellungen ein.

SCHRITT 3 Klicken Sie auf **Übernehmen** und dann auf **Schließen**.

So aktivieren Sie ein Zugriffsprofil (nachdem Sie alle Änderungen vorgenommen haben):

SCHRITT 1 Wählen Sie das Profil in der Zugriffsprofiltabelle aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 2 Aktivieren Sie das Kontrollkästchen „Aktivieren“.

SCHRITT 3 Klicken Sie auf **Übernehmen** und dann auf **Schließen**.

Authentifizierungsmethoden

Auf der Seite *Klicken Sie im Navigationsfenster auf Sicherheit > Authentifizierungsmethoden.Authentifizierungsmethoden* können Sie angeben, wie Benutzern der Zugriff auf Switch-Ports gewährt wird.

So wählen Sie die Authentifizierungsmethode aus:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Sicherheit** > **Authentifizierungsmethoden**.

SCHRITT 2 Wählen Sie aus der Methodenliste eine Authentifizierungsmethode aus:

- **Lokal**: Eine Kombination aus Benutzer-ID und Kennwort des Anfragers wird mit einer lokal gespeicherten Benutzerdatenbank im Switch verglichen.
- **Ohne**: Es wird keine Authentifizierungsmethode verwendet.
- **RADIUS**: Der Switch gibt Authentifizierungsanforderungen an einen RADIUS-Server weiter, der mit RADIUS-Access-Accept- oder -Access-Reject-Frames antwortet.
- **RADIUS, Ohne**: Der Switch gibt Authentifizierungsanforderungen an einen RADIUS-Server weiter. Wenn er den Server nicht erreicht, wird keine Authentifizierung verwendet.
- **RADIUS, Lokal**: Der Switch gibt Authentifizierungsanforderungen an einen RADIUS-Server weiter. Wenn er den Server nicht erreicht, wird die lokale Benutzerdatenbank verwendet.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Sturmsteuerung

Ein Verkehrssturm ist das Ergebnis einer übermäßig hohen Anzahl von Broadcast-Nachrichten, Multicast-Nachrichten oder unbekannten Unicast-Nachrichten, die gleichzeitig von einem einzigen Port in einem Netzwerk übertragen werden. Weitergeleitete Antworten auf Nachrichten können die Netzwerkressourcen überlasten und zu Timeouts im Netzwerk führen.

Der Switch misst die Rate der pro Port eingehenden Broadcast-Pakete, Multicast-Pakete und unbekannten Unicast-Pakete und verwirft Pakete, wenn die Rate einen definierten Wert überschreitet. Die Sturmsteuerung kann pro Schnittstelle aktiviert oder deaktiviert werden.

Auf der Seite *Sturmsteuerung* können Sie die Sturmsteuerung für Switch-Schnittstellen aktivieren und konfigurieren. Um diese Seite anzuzeigen, klicken Sie im Navigationsfenster auf **Sicherheit** > **Sturmsteuerung**.

Die Sturmsteuerung ist standardmäßig an allen Ports für alle Pakettypen deaktiviert. So bearbeiten Sie Sturmsteuerungseinstellungen für einen Port:

SCHRITT 1 Wählen Sie den zu konfigurierenden Port aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 2 Geben Sie für Broadcast-, Multicast- und Unicast-Verkehr die folgenden Parameter für den ausgewählten Port an:

- **Sturmsteuerung**: Wählen Sie „Aktivieren“ aus, um den Sturmsteuerungsschutz für den Verkehrstyp zu aktivieren.
- **Ratenschwellenwerttyp**: Wählen Sie aus, wie der Switch bestimmt, ob Verkehr den Schwellenwert überschreitet:
  - **Prozent**: Der Verkehr wird verworfen, wenn ein Prozentanteil der Link-Kapazität überschritten ist.
  - **pps**: Pakete pro Sekunde. Der Verkehr wird verworfen, wenn beim Link ein Schwellenwert für Pakete pro Sekunde überschritten ist.
- **Ratenschwellenwert Sturmsteuerung**: Geben Sie die maximale Rate an, mit der Pakete weitergeleitet werden. Wenn Sie den Ratenschwellenwerttyp „Prozent“ ausgewählt haben, geben Sie einen Prozentanteil der gesamten Port-Kapazität ein (0 % - 100 %). Wenn Sie den Ratenschwellenwerttyp „pps“ ausgewählt haben, geben Sie eine Rate für die Pakete pro Sekunde ein (0 - 14880000). Ports, die mit 10 MbPS, 100 MbPS und 1000 MbPS betrieben werden, haben einen maximalen Durchsatz von 14880, 148800 bzw. 1488000 Paketen pro Sekunde.

HINWEIS: Die tatsächlich zum Aktivieren der Sturmsteuerung erforderliche Rate des Ingress-Verkehrs basiert auf der Größe der eingehenden Pakete und der fest codierten durchschnittlichen Paketgröße (512 Byte). Die Rate für die Pakete pro Sekunde wird berechnet, da die Hardware anstelle einer absoluten Rate in kBps einen pps-Wert benötigt. Wenn das konfigurierte Limit beispielsweise 10 % beträgt, wird dies in ~25000 pps (für einen 100M-Port) konvertiert, und dieses pps-Limit wird in der Hardware festgelegt.

SCHRITT 3 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Portsicherheit

Sie können die Port-Sicherheit pro Port aktivieren. Wenn ein Port gesichert (gesperrt) ist, leitet der Switch nur Pakete weiter, deren Quell-MAC-Adresse am Port gesichert wird. Alle anderen Pakete werden verworfen. Der Switch verwirft außerdem Pakete von Ports, deren Quell-MAC-Adresse an einem anderen Port gesichert wird.

Eine sichere MAC-Adresse kann statisch konfiguriert oder dynamisch gelernt werden. An einem gesicherten Port sind maximal 256 sichere MAC-Adressen möglich. Statische sichere MAC-Adressen können Sie auf der Seite *Statische Adressen* konfigurieren. Für statische und dynamische sichere MAC-Adressen gelten Fälligkeitslimits (siehe **Konfigurieren der Fälligkeitszeit für dynamische Adressen**).

Um die Seite *Port-Sicherheit* anzuzeigen, klicken Sie im Navigationsfenster auf **Sicherheit** > **Portsicherheit**.

In der Port-Sicherheitstabelle wird die aktuelle Sicherheitskonfiguration der einzelnen Ports angezeigt. Sie können aus der Liste *Schnittstellentyp* die Option „LAG“ auswählen, um nur Daten für LAGs anzuzeigen. Standardmäßig ist die Port-Sicherheit global und für jede Schnittstelle deaktiviert.

Aktivieren der Port-Sicherheit

So konfigurieren Sie die Port-Sicherheit:

SCHRITT 1 Wählen Sie auf der Seite *Port-Sicherheit* für den globalen Administrationsmodus die Option „Aktivieren“ aus, und klicken Sie auf **Übernehmen**.

SCHRITT 2 Wählen Sie den Port oder die LAG aus, den bzw. die Sie konfigurieren möchten, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Konfigurieren Sie die folgenden Einstellungen:

- **Schnittstellenstatus**: Wählen Sie „Sperren“ aus, um die Port-Sicherheit für die Schnittstelle zu aktivieren. Wenn eine Schnittstelle vom nicht gesperrten in den gesperrten Modus wechselt, werden alle vom Switch an diesem Port dynamisch gelernten Adressen aus der MAC-Adressliste gelöscht.
- **Max. Anzahl der statischen MAC-Adressen**: Geben Sie die maximale Anzahl der statischen sicheren MAC-Adressen am Port bzw. in der LAG an. Statische sichere MAC-Adressen können Sie auf der Seite *Statische Adressen* konfigurieren. Die Gesamtanzahl der sichereren Adressen darf nicht 256 überschreiten.
- **Max. Anzahl der dynamischen MAC-Adressen**: Geben Sie die maximale Anzahl der dynamischen sicheren MAC-Adressen an, die vom Port bzw. von der LAG gelernt werden können. Die Gesamtanzahl der sichereren Adressen darf nicht 256 überschreiten.

  Wenn die Port-Sicherheit für einen Port aktiviert ist und für statische oder dynamische Limits neue Werte festgelegt werden, gelten folgende Regeln:

  - Wenn der neue Wert größer ist als der alte Wert, werden für die dynamischen oder statischen Adressen keine Aktionen ausgeführt.
  - Wenn der neue Wert kleiner ist als der alte Wert, werden die folgenden Aktionen ausgeführt:

    Dynamische Adressen: Der Switch initiiert die Löschung aller gelernten Adressen im Port.

    Statische Adressen: Der Switch behält die statischen Adressen bei (bis zum Limit für statische Adressen). Dabei spielt es keine Rolle, ob die Adressen als sicher, permanent oder zum Löschen bei Timeout konfiguriert sind. Dann werden die verbleibenden statischen Adressen aus der MAC-Adresstabelle gelöscht.

- **Aktion bei Verstoß**: Wählen Sie aus, wie der Switch eingehende Pakete behandelt, die am gesperrten Port nicht zulässig sind:
  - **Verwerfen**: Die Pakete werden verworfen.
  - **Weiterleiten**: Die Pakete werden weitergeleitet, aber die Quell-MAC-Adressen werden nicht der Weiterleitungsdatenbank hinzugefügt.
  - **Herunterfahren**: Die Pakete werden verworfen, und der Port wird heruntergefahren.
- **Dynamische Adressen in statische konvertieren**: Wählen Sie „Aktivieren“ aus, um alle dynamischen sicheren MAC-Adressen in statische sichere MAC-Adressen zu konvertieren.
- **Port zurücksetzen**: Wählen Sie diese Option aus, um den Port zurückzusetzen, wenn dieser von der Funktion für die Port-Sicherheit heruntergefahren wurde.

SCHRITT 4 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Anzeigen und Konfigurieren von sicheren MAC-Adressen

Um die aktuelle Liste der sicheren MAC-Adressen und der zugeordneten Ports und VLANs anzuzeigen, klicken Sie auf der Seite *Port-Sicherheit* auf **Tabelle für sichere Adressen**.

In der Tabelle für sichere Adressen werden für jede Schnittstelle die gesicherten statisch konfigurierten MAC-Adressen angezeigt. Dabei spielt es keine Rolle, ob der Port gesperrt ist. Außerdem werden in der Tabelle die dynamisch gelernten MAC-Adressen für gesperrte Ports aufgeführt. Dynamische Einträge für einen Port werden gelöscht, wenn der Status des Ports von „Gesperrt“ in „Nicht gesperrt“ geändert wird oder wenn der Link deaktiviert wird.

Sie können auf **Tabelle für statische Adressen** klicken, um die Seite zum Konfigurieren statischer Adressen anzuzeigen. Informationen hierzu finden Sie unter **Konfigurieren von statischen MAC-Adressen**. Sie müssen das Feld „Status“ für den Eintrag auf „Sicher“ festlegen.

Sie können auf **Port-Sicherheitstabelle** klicken, um wieder die Seite *Port-Sicherheit* anzuzeigen.

802.1X

Lokale Netzwerke (Local Area Networks, LANs) werden oft in Umgebungen bereitgestellt, in denen nicht autorisierte Geräte physisch mit der LAN-Infrastruktur verbunden werden können oder nicht autorisierte Benutzer versuchen können, über bereits verbundene Geräte auf das LAN zuzugreifen. In einer derartigen Umgebung ist es möglicherweise wünschenswert, den Zugriff auf die vom LAN angebotenen Dienste auf diejenigen Benutzer und Geräte zu beschränken, denen die Verwendung dieser Dienste erlaubt ist.

Mithilfe der Port-basierten Zugriffssteuerung können Sie in Netzwerken steuern, ob Hosts auf an einem verbundenen Port bereitgestellte Dienste zugreifen können. Sie können den Switch für die Verwendung der Port-basierten Netzwerkzugriffssteuerung auf der Grundlage des IEEE 802.1x-Protokolls konfigurieren.

Im 802.1x-Protokoll werden drei Arten von Einheiten definiert:

- Anfrager: Eine Einheit, die Zugriff auf einen Port auf der Remote-Seite des Links anfordert. Der Anfrager präsentiert dem Netzwerk Anmeldeinformationen, die der andere Knoten im Netzwerk (der Authentifikator) verwendet, um bei einem Server die Authentifizierung anzufordern.
- Authentifikator: Eine Einheit, die die Authentifizierung des Anfragers auf der Remote-Seite eines Links ermöglicht. Ein Authentifikator gewährt einem Anfrager Zugriff auf den Port, wenn die Authentifizierung erfolgreich war.
- Authentifizierungsserver: Ein Server, beispielsweise ein RADIUS-Server, der die Authentifizierung im Auftrag des Authentifikators ausführt und angibt, ob der Anfrager autorisiert ist, auf die über den authentifizierenden Port bereitgestellten Dienste zuzugreifen.

Beim Authentifizierungsvorgang unterstützt 802.1X den Austausch von EAPOL-Nachrichten (Extensible Authentication Protocol over LAN) zwischen Anfragern und Authentifikatoren.

Ein Switch-Port kann als Authentifikator oder Anfrager konfiguriert sein, aber nicht beides.

Definieren der 802.1X-Eigenschaften

Auf der Seite *802.1X-Eigenschaften* können Sie den globalen 802.1X-Administrationsmodus für den Switch konfigurieren.

So aktivieren Sie die 802.1X-Sicherheit global:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Sicherheit** > **802.1X** > **Eigenschaften**.

SCHRITT 2 Wählen Sie unter „Port-basierter Authentifizierungsstatus“ die Option „Aktivieren“ aus, um die Port-basierte 802.1X-Authentifizierung global für den Switch zuzulassen.

SCHRITT 3 Wählen Sie aus der Liste der Authentifizierungsmethoden eine Authentifizierungsmethode aus:

- **Ohne**: Es wird keine Authentifizierungsmethode verwendet.
- **Lokal**: Der Switch authentifiziert einen Remote-Anfrager lokal auf der Grundlage von EAP-MD5. Der Anfrager muss sich als einer der im Switch konfigurierten Verwaltungsbenutzer identifizieren (siehe **Verwalten von Benutzerkonten**).
- **RADIUS**: Der Switch verwendet für die Ausführung der Authentifizierung einen oder mehrere externe RADIUS-Server. Sie müssen die Identität und Authentifizierung des Anfragers direkt auf den Servern konfigurieren. (Informationen hierzu finden Sie unter **RADIUS**.)
- **RADIUS, Ohne**: Der Switch verwendet für die Ausführung der Authentifizierung einen oder mehrere externe RADIUS-Server. (Weitere Informationen finden Sie weiter oben in der Beschreibung von RADIUS.) Wenn der Switch keinen Server erreichen kann, wird keine Authentifizierung verwendet.
- **RADIUS, Lokal**: Der Switch verwendet für die Ausführung der Authentifizierung einen oder mehrere externe RADIUS-Server (siehe Beschreibung von RADIUS weiter oben). Wenn der Switch keinen Server erreichen kann, wird die Authentifizierung lokal ausgeführt (siehe Beschreibung von „Lokal“ weiter oben).

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

HINWEIS Anweisungen zum Auswählen der Rollen für die einzelnen Ports finden Sie unter **Ändern von Port-PAE-Funktionen**, und Anweisungen zum Konfigurieren der Authentifizierung für einzelne Ports finden Sie unter **Konfigurieren der Port-Authentifizierung**.

Ändern von Port-PAE-Funktionen

Auf der Seite *Port-PAE-Funktionen* können Sie die 802.1X-Rolle der einzelnen Ports als Authentifikator oder Anfrager anzeigen und konfigurieren.

So ändern Sie die Rolle eines Ports als Authentifikator oder Anfrager:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Sicherheit** > **802.1X** > **Eigenschaften**.

SCHRITT 2 Wählen Sie den zu konfigurierenden Port aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Wählen Sie die Rolle für den Port aus:

- **Authentifikator**: Wählen Sie diese Option aus, wenn der Port den Remote-Anfrager authentifizieren muss, bevor er den Zugriff auf einen lokalen Port gewährt.
- **Anfrager**: Wählen Sie diese Option aus, wenn der Port vor dem Zugriff auf einen Remote-Port die Genehmigung des Remote-Authentifikators einholen muss.

SCHRITT 4 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren der Port-Authentifizierung

Auf der Seite *Port-Authentifizierung* können Sie die Port-Zugriffssteuerung für Ports konfigurieren, die als Authentifikatoren dienen. Informationen zum Aktivieren eines Ports als Authentifikator finden Sie unter **Ändern von Port-PAE-Funktionen**.

So bearbeiten Sie die Einstellungen eines Port-Authentifikators:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Sicherheit** > **802.1X** > **Portauthentifizierung**.

In der Port-Authentifizierungstabelle wird die aktuelle Konfiguration der einzelnen Ports angezeigt.

SCHRITT 2 Wählen Sie den zu konfigurierenden Port aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 3 Geben Sie die Parameter ein:

- **Name des lokalen Datenbankbenutzers**: Verwenden Sie den nach links bzw. nach rechts zeigenden Pfeil, um die konfigurierten Verwaltungsbenutzer zwischen den Listen „Verfügbar“ und „Ausgewählt“ zu verschieben. Nur Benutzer aus der Liste „Ausgewählt“ haben (nach Authentifizierung) Zugriff auf den Port. Diese Liste gilt nur für die lokale Authentifizierung und nicht, wenn für die Authentifizierung ein RADIUS-Server verwendet wird.
- **Aktueller Port-Steuerungsstatus**: Der aktuelle Autorisierungsstatus des Ports („Autorisiert“ oder „Nicht autorisiert“).
- **Port-Steuerung**: Wählen Sie den Port-Autorisierungsmodus aus. Folgende Werte sind gültig:
  - **Nicht-Autorisierung erzwingen**: Wählen Sie diese Option aus, um den Port-Zugriff durch Anfrager, die sich mit dem Port verbinden, immer zu verweigern. Wenn diese Option ausgewählt ist, nimmt die Port-Steuerung den Status „Nicht autorisiert“ an.
  - **Automatisch**: Wählen Sie diese Option aus, wenn die Port-Steuerung auf dem Ergebnis des Authentifizierungsvorgangs basiert. Wenn der Anfrager authentifiziert wurde, nimmt die Port-Steuerung den Status „Autorisiert“ an, das heißt, dem Anfrager wird Zugriff auf den Port gewährt. Wenn der Anfrager nicht authentifiziert wurde, nimmt die Port-Steuerung den Status „Nicht autorisiert“ an, das heißt, dem Anfrager wird der Zugriff verweigert.
  - **Autorisierung erzwingen**: Wählen Sie diese Option aus, um den Port-Zugriff immer zuzulassen, wenn die Authentifizierung von Remote-Anfragern nicht erforderlich ist. Wenn diese Option ausgewählt ist, nimmt die Port-Steuerung den Status „Autorisiert“ an.

- **Periodische Neuauthentifizierung**: Wählen Sie diese Option aus, wenn der Port den Anfrager regelmäßig erneut authentifizieren soll. Der Port authentifiziert den Anfrager gemäß dem geplanten Intervall erneut, auch wenn der Anfrager noch authentifiziert ist.
- **Zeitspanne für Neuauthentifizierung**: Das Intervall zwischen Neuauthentifizierungsversuchen. Der Bereich lautet 300 - 4294967295 Sekunden. Der Standardwert beträgt 3600 Sekunden.
- **Jetzt erneut authentifizieren**: Erzwingt die sofortige Port-Neuauthentifizierung, wenn die Option ausgewählt ist.
- **Status des Authentifikators**: Der aktuelle Status der Port-Autorisierung. Folgende Status sind möglich: „Initialisieren“, „Getrennt“, „Wird verbunden“, „Wird authentifiziert“, „Authentifiziert“, „Wird abgebrochen“, „Gehalten“, „Authentifizierung erzwingen“ und „Nicht-Authentifizierung erzwingen“.
- **Back-End-Status**: Der aktuelle Status des Computers für die Back-End-Authentifizierung. Folgende Werte sind möglich: „Anforderung“, „Antwort“, „Erfolgreich“, „Fehler“, „Timeout“, „Leerlauf“ und „Initialisieren“.
- **Ruhezeit**: Geben Sie den Zeitraum ein, den der Switch nach einem fehlgeschlagenen Authentifizierungsaustausch im Ruhestatus verweilt. Während der Ruhezeit nimmt der Switch keine Authentifizierungsanforderungen an und initiiert diese nicht. Ändern Sie den Standardwert für diesen Befehl nur, wenn ungewöhnliche Umstände vorliegen, beispielsweise unzuverlässige Links oder konkrete Verhaltensprobleme bei bestimmten Clients und Authentifizierungsservern. Wenn Sie den Benutzern kürzere Reaktionszeiten bieten möchten, geben Sie einen kleineren Wert als den Standardwert (60 Sekunden) ein. Der Bereich lautet 0 - 65535 Sekunden.
- **EAP wird erneut gesendet**: Die Zeit, die verstreicht, bevor EAP-Anforderungen erneut gesendet werden. Gültig sind Werte im Bereich von 1 - 65535 Sekunden, und der Standardwert lautet 30 Sekunden.
- **Anfrager-Timeout**: Die Zeit, die verstreicht, bevor EAP-Anforderungen erneut an Anfrager gesendet werden. Ändern Sie den Standardwert (30 Sekunden) für diesen Befehl nur, wenn ungewöhnliche Umstände vorliegen, beispielsweise unzuverlässige Links oder konkrete Verhaltensprobleme bei bestimmten Clients und Authentifizierungsservern. Wenn Sie den Benutzern kürzere Reaktionszeiten bieten möchten, geben Sie einen kleineren Wert als den Standardwert ein. Der Bereich lautet 1 - 65535 Sekunden.

- **Server-Timeout**: Der Zeitraum, der verstreicht, bevor EAP-Anforderungen erneut an den Authentifizierungsserver gesendet werden. Gültig sind Werte im Bereich von 1 - 65535 Sekunden, und der Standardwert lautet 30 Sekunden.
- **Max. EAP-Anforderungen**: Die vorkonfigurierte maximale Anzahl der EAP-Anforderungen, die ein Switch, wenn er keine Antwort erhält, senden kann, bevor der Authentifizierungsvorgang neu gestartet wird.
- **Grund für Abbruch**: Der Grund für den Abbruch.

SCHRITT 4 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Konfigurieren der Anfrager-Port-Authentifizierung

Auf der Seite *Anfrager-Portauthentifizierung* können Sie die Port-Zugriffssteuerung für Ports konfigurieren, die mit der Rolle des Anfragers konfiguriert sind. Informationen zum Aktivieren eines Ports als Anfrager finden Sie unter **Ändern von Port-PAE-Funktionen**.

So konfigurieren Sie die Anfrager-Port-Authentifizierung:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Sicherheit** > **802.1X** > **Anfrager-Portauthentifizierung**.

SCHRITT 2 Wählen Sie den zu konfigurierenden Port aus, und klicken Sie auf **Bearbeiten**.

Im Feld „Aktuelle Port-Steuerung“ wird der aktuelle Autorisierungsmodus des Ports angezeigt.

SCHRITT 3 Konfigurieren Sie die folgenden Felder:

- **Administrative Port-Steuerung**: Wählen Sie den Port-Autorisierungsmodus aus. Folgende Werte sind gültig:
  - **Nicht-Autorisierung erzwingen**: Der ausgewählten Schnittstelle wird durch Versetzen in den Status „Nicht autorisiert“ der Zugriff auf das System verweigert.
  - **Automatisch**: Der Switch erkennt den Modus der Schnittstelle anhand des Ergebnisses des Authentifizierungsaustausches zwischen Anfrager, Authentifikator und Authentifizierungsserver.

- **Autorisierung erzwingen**: Der Port wird in den Status „Autorisiert“ versetzt, ohne dass eine Authentifizierung gegenüber dem Authentifizierungsserver erforderlich ist. Die Schnittstelle sendet und empfängt normalen Verkehr ohne Port-basierte Authentifizierung des Clients.

- **Benutzername**: Wählen Sie den Benutzer aus, den der Port verwenden soll, um sich als Anfrager zu identifizieren. Der Benutzer muss einer der im Switch konfigurierten Verwaltungsbenutzer sein. Bei der Authentifizierung wird das für den Benutzer konfigurierte Kennwort verwendet. Als Anfrager unterstützt der Switch die EAP-MD5-Authentifizierungsmethode. (Informationen zum Einrichten der Benutzer finden Sie unter **Verwalten von Benutzerkonten**.)

SCHRITT 4 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Anzeigen von authentifizierten Hosts

Um auf der Seite *Authentifizierte Hosts* Ports mit authentifizierten Benutzern anzuzeigen, klicken Sie im Navigationsfenster auf **Sicherheit** > **802.1X** > **Authentifizierte Hosts**.

In der Tabelle für authentifizierte Hosts werden für jeden Host die folgenden Informationen angezeigt:

- **Port**: Der für die Authentifizierung verwendete Port.
- **Benutzername**: Der Benutzername des Hosts.
- **Anfrager-MAC-Adresse**: Die MAC-Adresse des Anfragergeräts.
- **Sitzungszeit**: Die seit der Anmeldung des Benutzers verstrichene Zeit in Sekunden.
- **Sitzungs-Timeout**: Die Gültigkeitsdauer der jeweiligen Sitzung. Der Zeitraum in Sekunden wird vom RADIUS-Server bei der Authentifizierung des Ports zurückgegeben.

11

Quality of Service

Dieses Kapitel enthält eine Übersicht über Quality of Service (QoS, Servicequalität) und Erläuterungen der QoS-Funktionen im Menü „Quality of Service“.

- **QoS-Eigenschaften**
- **Definieren von Warteschlangen**
- **Zuordnen von CoS/802.1p-Prioritäten zu Warteschlangen**
- **Zuordnen der IP-Priorität zu Warteschlangen**
- **Zuordnen von DSCP-Werten zu Warteschlangen**
- **Definieren von Ratenbegrenzungsprofilen**
- **Anwenden von Ratenbegrenzungsprofilen auf Schnittstellen**
- **Verkehrsgestaltung**

In einem typischen Switch besteht jeder physische Port aus einer oder mehreren Warteschlangen für die Übertragung von Paketen im verbundenen Netzwerk. Oft werden pro Port mehrere Warteschlangen konfiguriert, um bestimmten Paketen auf der Grundlage benutzerdefinierter Kriterien den Vorzug vor anderen zu geben. Wenn ein Paket zur Übertragung an einem Port in eine Warteschlange eingereiht wird, hängt die Verarbeitungsrate von der Konfiguration der Warteschlange und möglicherweise vom in den anderen Warteschlangen des Ports vorhandenen Verkehr ab. Wenn eine Verzögerung notwendig ist, bleiben Pakete in der Warteschlange, bis das Planungsmodul die Übertragung der Warteschlange autorisiert. Wenn die Warteschlangen voll sind, ist kein Platz für die Aufbewahrung der zu übertragenden Pakete vorhanden, und die Pakete werden möglicherweise vom Switch verworfen.

Mit QoS können Sie eine konsistente, vorhersehbare Datenübermittlung ermöglichen, bei der Pakete mit strikten zeitlichen Anforderungen von verzögerungstoleranteren Paketen unterschieden werden. Pakete mit strikten zeitlichen Anforderungen werden in einem QoS-fähigen Netzwerk bevorzugt behandelt.

In Netzwerken, in denen der QoS-Betrieb aktiviert ist, müssen alle Elemente des Netzwerks QoS-fähig sein. Das Vorhandensein mindestens eines Knotens, der nicht QoS-fähig ist, führt zu einem Fehler im Netzwerkpfad, und die Leistung des gesamten Pakets ist beeinträchtigt.

Der Switch unterstützt vier Egress-Warteschlangen pro Port oder LAG. Warteschlange 1 hat die niedrigste und Warteschlange 4 die höchste Priorität.

Auf den Seiten im Menü „Quality of Service“ können Sie Eigenschaften der Warteschlangen definieren und diesen Verkehr zuordnen, der bestimmte Merkmale aufweist oder an bestimmten Schnittstellen eingeht. Außerdem können Sie Ratenbegrenzungsprofile erstellen, in denen Kriterien definiert werden, anhand derer ermittelt wird, ob ein Port mehr Verkehr empfängt als er verarbeiten kann. Anschließend können Sie die Ratenbegrenzungsprofile Ports zuweisen.

QoS-Eigenschaften

Sie können Switch-Ports konfigurieren, um Verkehr basierend auf den in Ethernet-Frames oder IP-Paket-Headern codierten Prioritätsinformationen Egress-Warteschlangen zuzuweisen. Alternativ kann für den Verkehr ein Standardprioritätswert verwendet werden, der für den Port konfiguriert ist, an dem der Verkehr eingeht. Wenn ein Port für die Verwendung des codierten Prioritätswerts (beispielsweise 802.1p, IP-Priorität oder DSCP-Wert) konfiguriert ist, wird der Port als *vertrauenswürdig* betrachtet. Ein Port, der für die Verwendung eines eigenen Prioritätswerts anstelle des im Frame oder Paket codierten Werts konfiguriert ist, wird bei Entscheidungen über die Warteschlangenzuweisung als *nicht vertrauenswürdig* betrachtet.

Wenn ein Port als vertrauenswürdig konfiguriert ist, während der Frame oder das Paket keine Prioritätsinformationen aufweisen, wird dem Paket die Standard-Port-Priorität zugewiesen. Die Standard-Port-Priorität entspricht null.

Auf der Seite *VLAN-Verwaltung* > *Schnittstelleneinstellungen* können Sie den Wert der VLAN-Priorität ändern.

Auf der Seite *QoS-Eigenschaften* können Sie einen Port als vertrauenswürdig oder nicht vertrauenswürdig definieren und konfigurieren, welchen Prioritätswerten der Port vertraut.

So konfigurieren Sie den Vertrauensmodus für einen Port oder eine LAG:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Quality of Service** > **QoS-Eigenschaften**.

SCHRITT 2 Im Menü „Schnittstellentyp“ können Sie Ports oder LAGs in der Tabelle für die Vertrauensmoduskonfiguration anzeigen.

SCHRITT 3 Wählen Sie die zu konfigurierende Schnittstelle aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 4 Um den Typ der Prioritätswerte anzugeben, mit deren Hilfe die Egress-Warteschlangen der Pakete ermittelt werden sollen, wählen Sie einen der folgenden Vertrauensmodi aus:

- **Nicht vertrauenswürdig**: Der Port weist eine eigene standardmäßige 802.1p-Priorität zu (0).
- **dot1p vertrauen**: Der Port verwendet in Ethernet-Frames mit VLAN-Tag den 802.1p-Prioritätswert. Für Frames ohne Tag wird die Standardpriorität des Ports zugewiesen.
- **ip-precedence vertrauen**: Der Port verwendet den IP-Prioritätswert im IP-Paket-Header. Wenn kein Wert angegeben ist, wird die Standardpriorität des Ports zugewiesen. Nicht-IP-Frames mit VLAN-Tag und Frames ohne Tag wird die Standardpriorität des Ports zugewiesen.
- **ip-dscp vertrauen**: Der Port verwendet die DSCP-Markierung im IP-Paket-Header sowohl für IP-Pakete mit VLAN-Tag als auch für IP-Pakete ohne Tag. Nicht-IP-Frames mit VLAN-Tag und Frames ohne Tag wird die Standardpriorität des Ports zugewiesen.
- **Allen vertrauen**: Der Port verwendet für IP-Pakete die DSCP-Markierung, um die Priorität zu ermitteln. Für Nicht-IP-Frames verwendet der Port die 802.1p-Priorität, wenn der Frame über VLAN-Tags verfügt, und die Standardpriorität des Ports, wenn der Frame nicht über VLAN-Tags verfügt.

SCHRITT 5 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Definieren von Warteschlangen

Auf der Seite *Warteschlange* können Sie konfigurieren, wie das Verkehrsplanungsmodul bestimmt, welche Warteschlange auf den Egress-Port zugreifen kann. Sie können eine Warteschlange im strikten Prioritätsmodus oder im WRR-Modus (Weighted Round-Robin) konfigurieren. Standardmäßig sind alle Warteschlangen als Warteschlangen mit strikter Priorität konfiguriert.

Pakete werden nach den folgenden Prinzipien übermittelt:

- Pakete aus der Warteschlange mit der höchsten Priorität werden zuerst übermittelt.
- Wenn sich eine Warteschlange im strikten Prioritätsmodus befindet, darf sie übertragen, bis keine Pakete mehr vorhanden sind oder bis eine Warteschlange mit einer höheren Priorität zu sendende Pakete enthält.
- Wenn sich eine Warteschlange im WRR-Modus befindet, ist die Anzahl der Pakete, die sie übermitteln darf, proportional zu ihrem konfigurierbaren Gewichtungswert. Die Gewichtung wird für jeden Port als Prozentanteil der Gesamtbandbreite ausgedrückt.

Sie können für einen Port eine Kombination aus einer strikten Warteschlange und WRR-Warteschlangen konfigurieren.

Empfehlungen für die Warteschlangenkonfiguration

Sie sollten Warteschlangen mit höheren Nummern mit höherer Priorität und Gewichtung und mit Einstellungen für die Mindestbandbreite konfigurieren.

Die folgenden Szenarien werden für strikte Priorität (SP) und WRR in den Warteschlangen 1 - 4 empfohlen:

- **Alle vier Warteschlangen im SP-Modus** (Q4 > Q3 > Q2 > Q1). Q4 wird Bandbreite zugewiesen, solange in Q4 Pakete zur Verarbeitung vorhanden sind. Dann wird Q3 verarbeitet, gefolgt von Q2 und dann Q1.
- **Alle 4 Warteschlangen im WRR-Modus** (Q4:Q3:Q2:Q1 = A:B:C:D). In diesem Modus wird jeder Warteschlange eine Mindestbandbreite zugewiesen, die der jeweils konfigurierten Gewichtung entspricht.
- **Eine Warteschlange im SP-Modus und drei Warteschlangen im WRR-Modus** (Q4 > Q3/Q2/Q1; Q3:Q2:Q1 = A:B:C). In diesem Szenario wird empfohlen, Q4 im SP-Modus und Q3, Q2 und Q1 im WRR-Modus zu konfigurieren.
- **Zwei Warteschlangen im SP-Modus und zwei Warteschlangen im WRR-Modus** (q4 > q3 > q2/q1; q2:q1 = A:B): In diesem Szenario wird empfohlen, Q4 und Q3 im strikten Modus und Q2 und Q1 im WRR-Modus zu konfigurieren.

Diese Szenarien veranschaulichen, dass es in einem System, in dem mehr Ingress-Ports mit für verschiedene Warteschlangen an Egress-Ports bestimmtem Verkehr vorhanden sind, zu Head of Line Blocking (HOL) kommen kann. HOL kann dazu führen, dass Warteschlangen mit höheren Nummern mehr Bandbreite erhalten, obwohl Warteschlangen mit höheren Nummern mit einer niedrigen Mindestbandbreite und Gewichtung konfiguriert sind. Es wird empfohlen, Warteschlangen mit höheren Nummern immer im SP-Modus zu konfigurieren, damit auch bei Auftreten von HOL die gewünschte Egress-Trennung zwischen den Warteschlangen erfolgt.

Konfigurieren von Warteschlangen

So konfigurieren Sie QoS-Eigenschaften:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Quality of Service** > **Warteschlange**.

SCHRITT 2 Wählen Sie den zu konfigurierenden Port bzw. die zu konfigurierende LAG aus.

SCHRITT 3 Wählen Sie für jede Warteschlange an der ausgewählten Schnittstelle einen der folgenden Modi aus.

- **Strikte Priorität**: Wählen Sie diesen Modus aus, damit das Planungsmodul den Verkehr strikt auf der Grundlage der Prioritätsstufen in den Warteschlangen weiterleitet. Die Warteschlange mit dem Verkehr mit der höchsten Priorität kann auf den Egress-Port zugreifen, bis dieser Verkehr vollständig weitergeleitet ist. Sie können den Modus „Strikte Priorität“ verwenden, um für Verkehrsklassen mit höherer Priorität niedrige Latenz bereitzustellen.
- **WRR**: Wählen Sie diesen Modus aus, damit das Planungsmodul die Warteschlange basierend auf dem relativen Bandbreitenprozentanteil gegenüber anderen WRR-Warteschlangen abwechselnd mit anderen WRR-Warteschlangen verarbeitet. Strikte Warteschlangen werden weiter verarbeitet, solange sie Verkehr mit höherer Priorität enthalten.

SCHRITT 4 Wenn Sie den WRR-Modus für eine Warteschlange auswählen, geben Sie in das Feld „Prozentanteil der WRR-Bandbreite“ einen Bandbreitenprozentanteil ein. Die Summe aller Bandbreitenprozentanteile für alle Warteschlangen darf nicht 100 % überschreiten.

SCHRITT 5 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Um diese Warteschlangeneigenschaften auf alle Schnittstellen des Switch anzuwenden, klicken Sie auf **Einstellungen in alle Schnittstellen kopieren**.

Zuordnen von CoS/802.1p-Prioritäten zu Warteschlangen

Die Priorität eines an einer Schnittstelle eingehenden Pakets kann möglicherweise durch einen IEEE 802.1p-Prioritätswert im Header des Ethernet-Frames identifiziert werden. 802.1p gibt acht Prioritätsstufen an (0 - 7). Auf der Seite *CoS/802.1p zu Warteschlange* können Sie diese Prioritätsstufen den vier CoS-Warteschlangen zuordnen, um Pakete in die entsprechende ausgehende Warteschlange zu leiten. Warteschlange 1 hat die niedrigste und Warteschlange 4 die höchste Priorität.

HINWEIS Die Zuordnung von CoS/802.1p-Prioritätsstufen zu Warteschlangen wird pro Schnittstelle konfiguriert. Konfigurieren Sie diese Zuordnungswerte für die eingehende Schnittstelle.

So ordnen Sie Warteschlangen 802.1p-Prioritätswerte zu:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Quality of Service** > **CoS/802.1p zu Warteschlange**.

SCHRITT 2 Wählen Sie den zu konfigurierenden Port bzw. die zu konfigurierende LAG aus.

SCHRITT 3 Wählen Sie für jede 802.1p-Serviceklasse eine Warteschlange aus der Liste der Ausgabewarteschlangen aus. Warteschlange 1 hat die niedrigste und Warteschlange 4 die höchste Priorität.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

SCHRITT 5 Um diese Zuordnungen auf alle Schnittstellen des Switch anzuwenden, klicken Sie auf **Einstellungen in alle Schnittstellen kopieren**.

HINWEIS Wenn Sie auf **Standards wiederherstellen** klicken, werden die folgenden Zuordnungen auf alle Schnittstellen angewendet.

802.1p-Priorität	Ausgabewarteschlange
0	1
1	1
2	2
3	3
4	3
5	4
6	4
7	4

Zuordnen der IP-Priorität zu Warteschlangen

Die Priorität eines an einer Schnittstelle eingehenden Pakets kann anhand des ToS-Felds (Type of Service) in einem IP-Paket-Header identifiziert werden. Es gibt acht definierte Prioritätsstufen (0 - 7). Auf der Seite *IP-Priorität zu Warteschlange* können Sie diese Werte den vier CoS-Warteschlangen zuordnen, um Pakete in die entsprechende ausgehende Warteschlange zu leiten. Warteschlange 1 hat die niedrigste und Warteschlange 4 die höchste Priorität.

HINWEIS Die Zuordnung von IP-Prioritätsstufen zu Warteschlangen wird pro Schnittstelle konfiguriert. Konfigurieren Sie diese Zuordnungswerte für die eingehende Schnittstelle.

So ordnen Sie die IP-Prioritätswerte Warteschlangen zu:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Quality of Service** > **IP-Priorität zu Warteschlange**.

SCHRITT 2 Wählen Sie den zu konfigurierenden Port bzw. die zu konfigurierende LAG aus.

SCHRITT 3 Wählen Sie für jeden IP-Prioritätswert eine Warteschlange aus der Liste der Ausgabewarteschlangen aus. Warteschlange 1 hat die niedrigste und Warteschlange 4 die höchste Priorität.

SCHRITT 4 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Um diese Zuordnungen auf alle Schnittstellen des Switch anzuwenden, klicken Sie auf **Einstellungen in alle Schnittstellen kopieren**.

HINWEIS Wenn Sie auf **Standards wiederherstellen** klicken, werden die folgenden Zuordnungen auf alle Schnittstellen angewendet.

IP-Priorität	Ausgabewarteschlange
0	1
1	1
2	2
3	3
4	3
5	4
6	3
7	3

Zuordnen von DSCP-Werten zu Warteschlangen

Die Priorität eines an einer Schnittstelle eingehenden Pakets kann anhand des DSCP-Werts (Differentiated Service Code Point) in einem IP-Paket-Header identifiziert werden. Das IP-DSCP-Feld kann einen der 64 Werte enthalten (0 - 63). Auf der Seite *DSCP zu Warteschlange* können Sie diese Werte den vier Egress-Warteschlangen zuordnen. Warteschlange 1 hat die niedrigste und Warteschlange 4 die höchste Priorität.

DSCP-Zuordnungseinstellungen werden global auf alle Ports angewendet.

So ordnen Sie DSCP-Werte Warteschlangen zu:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Quality of Service** > **DSCP zu Warteschlange**.

SCHRITT 2 Wählen Sie für jeden Ingress-DSCP-Wert eine Warteschlange aus der Liste der Ausgabewarteschlangen aus. Warteschlange 1 hat die niedrigste und Warteschlange 4 die höchste Priorität.

SCHRITT 3 Klicken Sie auf **Übernehmen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

HINWEIS Wenn Sie auf **Standards wiederherstellen** klicken, werden die folgenden Zuordnungen auf alle Schnittstellen angewendet.

DSCP-Wert	Ausgabewarteschlange
00-07	1
08-15	1
16-23	2
24-31	3
32-39	3
40-47	4
48-55	3
56-63	3

Definieren von Ratenbegrenzungsprofilen

Mithilfe der Ratenbegrenzungsfunktion können Sie eine maximale Rate für den an einem Port eingehenden Verkehr festlegen. Wenn die Datenrate die konfigurierte Rate überschreitet, verwirft der Switch sämtlichen weiteren Verkehr von diesem Port. Ratenbegrenzungen werden pro Port angewendet.

Um Ratenbegrenzungen anzuwenden, erstellen Sie zunächst auf dieser Seite mindestens ein Ratenbegrenzungsprofil. In Profilen geben Sie die Kriterien an, anhand derer bestimmt wird, wann die Ratenbegrenzung überschritten ist. Dann weisen Sie Ratenbegrenzungsprofile Schnittstellen zu (siehe **Anwenden von Ratenbegrenzungsprofilen auf Schnittstellen**).

So fügen Sie der Ratenbegrenzungsprofil-Tabelle einen Eintrag hinzu:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Quality of Service** > **Ratenbegrenzungsprofil**.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie die Parameter ein:

- **Profil-ID**: Geben Sie eine Zahl von 1 - 64 an, um das Profil zu identifizieren.
- **CIR**: Geben Sie die vereinbarte Übertragungsrate (Committed Information Rate, CIR) an, das heißt die Rate, mit der Daten übermittelt werden. Für die Datenrate wird über ein Mindestzeitintervall ein Durchschnittswert ermittelt. Der Bereich lautet 64 - 1048576 kBps.
- **CBS**: Geben Sie eine vereinbarte Burst-Größe (Committed Burst Size, CBS) an, das heißt die garantierte Bandbreitenmenge für diskontinuierlichen Verkehr am Port. Der Bereich lautet 4 - 16384 KB.

SCHRITT 4 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Anwenden von Ratenbegrenzungsprofilen auf Schnittstellen

Wenn Sie ein oder mehrere Ratenbegrenzungsprofile erstellt haben, können Sie diese auf dieser Seite Schnittstellen zuordnen. Anweisungen zum Erstellen von Profilen finden Sie unter **Definieren von Ratenbegrenzungsprofilen**.

So wenden Sie ein Ratenbegrenzungsprofil auf eine Schnittstelle an:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Quality of Service** > **Schnittstellen-Ratenbegrenzung**.

SCHRITT 2 Mithilfe der Liste „Schnittstellentyp“ können Sie Ports oder LAGs in der Tabelle für die Schnittstellen-Ratenbegrenzung anzeigen.

SCHRITT 3 Wählen Sie die zu konfigurierende Schnittstelle aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 4 Fügen Sie ein Profil hinzu, oder entfernen Sie ein Profil:

- Um dieser Schnittstelle ein Profil zuzuweisen, klicken Sie in der Liste „Verfügbar“ auf die Profil-ID und dann auf die Schaltfläche mit dem Pfeil nach rechts, um das Profil in die Liste „Ausgewählt“ zu verschieben. In der Liste „Verfügbar“ werden keine Profile mehr angezeigt, da einem Port nur ein Profil zugewiesen sein kann.
- Um ein Profil zu entfernen, klicken Sie in der Liste „Ausgewählt“ auf die Profil-ID und dann auf die Schaltfläche mit dem Pfeil nach links, um das Profil in die Liste „Verfügbar“ zu verschieben. In der Liste „Ausgewählt“ werden alle Profile angezeigt.

SCHRITT 5 Klicken Sie auf **Übernehmen** und dann auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

Verkehrsgestaltung

Auf der Seite *Verkehrsgestaltung* können Sie die Paketausgaberate optimieren. Sie können für jeden Port und jede LAG die als Prozentanteil der Bandbreite ausgedrückte maximale Ausgaberate konfigurieren. Wenn die Verkehrsrate diesen Grenzwert erreicht, werden überschüssige Pakete in eine Warteschlange eingereiht und später nach einem Zeitplan inkrementell übertragen.

So konfigurieren Sie die Verkehrsgestaltung für einen Port oder eine LAG:

SCHRITT 1 Klicken Sie im Navigationsfenster auf **Quality of Service** > **Verkehrsgestaltung**.

SCHRITT 2 Im Menü „Schnittstellentyp“ können Sie Ports oder LAGs in der Tabelle für die Verkehrsgestaltungseinstellungen anzeigen.

SCHRITT 3 Wählen Sie die zu konfigurierende Schnittstelle aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 4 Geben Sie für den ausgewählten Port bzw. die ausgewählte LAG die Ausgaberatenbegrenzung als Prozentanteil der Gesamtbandbreite ein. Klicken Sie auf **Übernehmen**.

SCHRITT 5 Wiederholen Sie diesen Schritt nach Bedarf, um die Bandbreitenauslastung anderen Ports und LAGs zuzuweisen.

SCHRITT 6 Wenn Sie fertig sind, klicken Sie auf **Schließen**. Die Änderungen werden in der aktuellen Konfiguration gespeichert.

 78-19562-01