Benutzerhandbuch für die Dell™ PowerConnect™ 6200-Reihe

Einführung
Hardwarebeschreibung
Verwenden von Dell™ OpenManage™ Switch Administrator
Informationen zu Kabeln und Anschlüssen
Konfigurieren von Dell™ PowerConnect™
Konfigurieren von Systeminformationen
Konfigurieren der Funktionsmerkmale IP-Telefon und Access Point-Support
Konfigurieren von Switching-Informationen
Anzeigen von Statistiken/RMON
Routingkonfiguration
IPv6-Konfiguration
Konfigurieren von Quality of Service (QoS)
Konfigurieren von IP-Multicast
Wie Sie Hilfe bekommen

Anmerkungen, Hinweise und Vorsichtshinweise

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie das System besser einsetzen können.

HINWEIS: Ein HINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und informiert darüber, wie dies zu vermeiden ist.

VORSICHT: Hiermit werden Sie auf eine potentiell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen könnte.

Modelle PC6224, PC6248, PC6224P, PC6248P und PC6224F

Irrtümer und technische Änderungen vorbehalten.
© 2007 Dell Inc. Alle Rechte vorbehalten.

Die Vervielfältigung oder Wiedergabe in jeglicher Weise ohne vorherige schriftliche Genehmigung von Dell Inc. sind strengstens untersagt.

In diesem Text verwendete Marken: *Dell*, *Dell OpenManage*, das *DELL* Logo, *Inspiron*, *Dell Precision*, *Dimension*, *OptiPlex*, *PowerConnect*, *PowerApp*, *PowerVault*, *Axim*, *DellNet* und *Latitude* sind Marken von Dell Inc.; *Microsoft*, *Windows* und *Windows Vista* sind Marken oder eingetragene Marken von Microsoft Corporation in den USA und/oder anderen Ländern. *Procomm Plus* ist eine eingetragene Marke von Symantec Corporation oder ihren Tochtergesellschaften in den USA und anderen Ländern.

Alle anderen in dieser Dokumentation genannten Marken und Handelsbezeichnungen sind Eigentum der jeweiligen Hersteller und Firmen. Dell Inc. erhebt keinen Anspruch auf Besitzrechte an Marken und Handelsbezeichnungen mit Ausnahme der eigenen.

Modelle PC6224, PC6248, PC6224P, PC6248P und PC6224F

September 2007 Rev. A00

Zurück zum Inhaltsverzeichnis

Informationen zu Kabeln und Anschlüssen

Benutzerhandbuch für die Dell™ PowerConnect™ 6200-Reihe

- 10/100/1000 Ethernet-Schnittstelle
- SFP-Schnittstellen
- Schnittstellen des dualen 10G-Steckplatzes
- Serielle Kabelverbindung
- Gleich- und Wechselstromversorgung

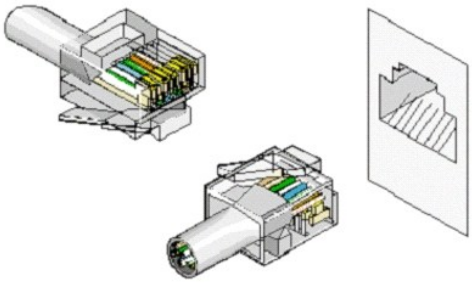
Dieser Abschnitt beschreibt die physischen Schnittstellen des Switch sowie die Kabelverbindungen.

Die Stationen werden über die auf der Vorderseite befindlichen physischen Schnittstellenanschlüsse mit den einzelnen Switch-Ports verbunden. Für jede Station wird der geeignete Modus (Halbduplex-, Vollduplex- bzw. automatischer Modus) eingestellt.

10/100/1000-Ethernet-Schnittstelle

Unter Verwendung von durchgehenden Kabeln kann der Switching-Port mit Stationen verbunden werden, die gemäß dem standardmäßigen Ethernet-Stationsmodus verkabelt sind. Übertragungsgeräte werden mit Hilfe von gekreuzten Kabeln miteinander verbunden. Abbildung 4-1 zeigt den RJ-45-Anschluss.

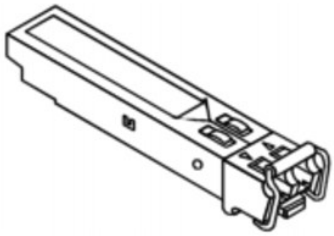
Abbildung 4-1. RJ-45-Anschluss



SFP-Schnittstellen

Die Anschlüsse der SFP-Schnittstellen befinden sich an der Vorderseite der Konsole. Abbildung 4-2 zeigt einen SFP-Anschluss.

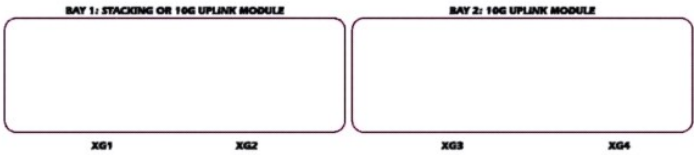
Abbildung 4-2. SFP-Anschluss



Schnittstellen des dualen 10G-Steckplatzes

Die Steckplätze an der Rückseite der Switches der Reihe 6200 unterstützen zwei XAUI-Schnittstellen. Diese Schnittstellen können bei Einsatz eines XFP-Moduls mit 10 Gbit/s betrieben werden, bzw. mit 12 Gbit/s (nur der auf der Gehäuserückseite linke Steckplatz), wenn ein Stack-Modul unterstützt wird. Abbildung 4-3 zeigt die XAUI-Steckplätze.

Abbildung 4-3. XAUI-Steckplätze



Serielle Kabelverbindung

Für das Setup und die Erstkonfiguration kann der Switch über ein serielles Kabel (Nullmodem) mit einem Terminal verbunden werden. (Sie können jedoch auch einen Computer mit einer geeigneten Terminal-Emulationssoftware verwenden.) Bei dem seriellen Kabel des Switch handelt es sich um ein gekreuztes DB-9-Kabel Buchse auf Buchse (siehe Abbildung 4-4).

Abbildung 4-4. Serieller Anschluss

Verbinden des Switch mit einem Terminal

1. Verbinden Sie das serielle Kabel mit dem ASCII-DTE-RS-232-Anschluss am Terminal.
2. Verbinden Sie das Schnittstellenkabel mit dem seriellen Anschluss des Switch (siehe Abbildung 4-5).
3. Wenn Sie einen Stack konfigurieren: Verbinden Sie das Schnittstellenkabel mit dem seriellen Anschluss des Master-Switch.

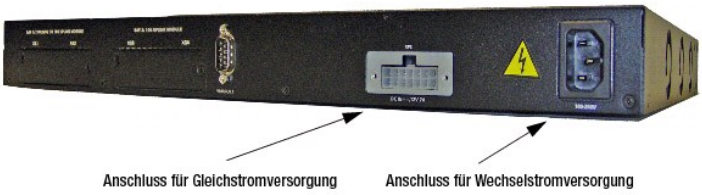
Abbildung 4-5. Serielle Verbindung zu Switch

Gleich- und Wechselstromversorgung

1. Verbinden Sie ein gängiges, ordnungsgemäß geerdetes Netzkabel mit einer Länge von 1,5 m (5 Fuß) mit der Haupt-Netzanschlussbuche an der Geräterückseite (siehe Abbildung 4-6).
2. Verbinden Sie das Stromkabel mit einer geerdeten Netzsteckdose.
3. Wenn Sie ein redundantes Gleichstrom-Netzteil verwenden (z. B. das RPS600 oder EPS470): Verbinden Sie das Gleichstromkabel mit der Gleichstrombuchse an der Geräterückseite (siehe Abbildung 4-6).
4. Überprüfen Sie die LEDs auf der Vorderseite, um sicherzustellen, dass das Gerät angeschlossen ist und korrekt funktioniert.

   Eine vollständige Erläuterung der LEDs finden Sie unter "LED-Definitionen".

Abbildung 4-6. Gleich- und Wechselstromversorgung des Switch



Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Konfigurieren von Systeminformationen

Benutzerhandbuch für die Dell™ PowerConnect™ 6200-Reihe

- Öffnen der Systemseite
- Definieren allgemeiner Geräteinformationen
- Konfigurieren von SNTP-Einstellungen
- Verwalten von Protokollen
- Definieren der IP-Adressierung
- Ausführen der Kabeldiagnose
- Verwalten der Gerätesicherheit
- Definieren von SNMP-Parametern
- Verwalten von Dateien
- Definieren erweiterter Einstellungen
- Definieren der Stacking-Eigenschaften

Öffnen der Systemseite

Über die Menüs auf der Seite **System** können Sie die Beziehung zwischen dem Switch und der übrigen Systemumgebung definieren. Klicken Sie zum Anzeigen der Seite **System** in der Strukturansicht auf **System**. Das **System**-*Menü* enthält Links zu folgenden Funktionen:

- Definieren allgemeiner Geräteinformationen
- Konfigurieren von SNTP-Einstellungen
- Verwalten von Protokollen
- Definieren der IP-Adressierung
- Ausführen der Kabeldiagnose
- Verwalten der Gerätesicherheit
- Definieren von SNMP-Parametern
- Verwalten von Dateien
- Definieren erweiterter Einstellungen
- Definieren der Stacking-Eigenschaften

Definieren allgemeiner Geräteinformationen

Die Menüseite **General** (Allgemein) enthält Links zu Seiten, über die Sie Geräteparameter konfigurieren können. Die Seite bietet Zugriff auf folgende Funktionen:

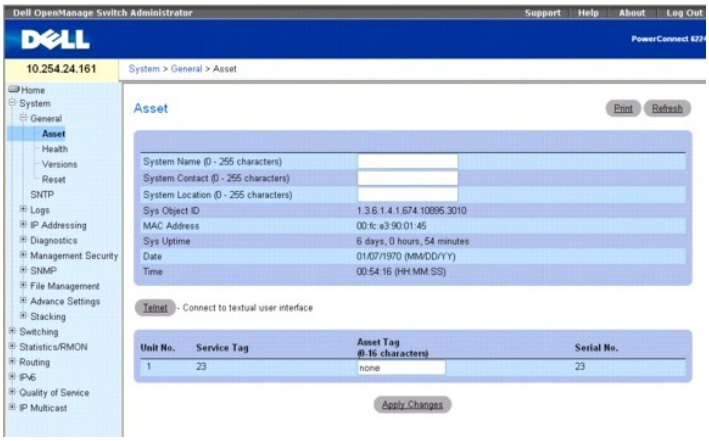
- Bestand
- Systemzustand
- Versionen
- Systemressourcen
- Zeitzonenkonfiguration
- Sommerzeitkonfiguration
- Einstellungsoptionen für die Uhr
- Zurücksetzen

Bestand

Über die Felder der Seite **Asset** (Bestand) können Sie allgemeine Geräteinformationen konfigurieren oder einsehen.

Klicken Sie zum Anzeigen der Seite **Asset** (Bestand) in der Strukturansicht auf **System**→ **General (Allgemein)**→ **Asset (Bestand)**.

Abbildung 6-1. Bestand



Die Seite **Asset** (Bestand) enthält folgende Felder:

System Name (0 – 255 characters) (Systemname, 0 – 255 Zeichen) – Dient der Zuweisung eines gerätespezifischen Systemnamens.

System Contact (0 – 255 characters) (Systemkontakt, 0 – 255 Zeichen) Dient der Zuweisung eines Kontaktperson-Namens.

System Location (0 – 255 characters) (Systemstandort, 0 – 255 Zeichen) – Dient der Spezifikation eines Systemstandorts.

Sys Object ID (Systemobjekt-ID) – Die zugewiesene Systemobjekt-Kennnummer.

MAC Address (MAC-Adresse) – Zeigt die MAC-Adresse des Switch an.

Sys Uptime (Systembetriebszeit) – Zeigt die Anzahl der Tage, Stunden und Minuten seit dem letzten Neustart an.

Date (Datum) – Zeigt das aktuelle Systemdatum an. Das Format lautet: Monat, Tag, Jahr (MM/TT/JJ). Beispiel: 11/01/05 steht für 1. November 2005.

Time (Uhrzeit) – Zeigt die aktuelle Systemzeit an. Das Format lautet: Stunde, Minute, Sekunde (HH:MM:SS). Beispiel: 20:12:03 steht für 8:12:03 PM.

Unit No. (Einheit-Nr.) – Zeigt die Position des Switch im Stack an.

Service Tag (Service-Tag) – Zeigt die bei der Wartung des Geräts verwendete Wartungsreferenznummer an.

Asset Tag (0 – 16 characters) (Asset-Tag, 0-16 Zeichen) – Zeigt die benutzerdefinierte Gerätereferenz an.

Serial No. (Seriennr.) – Zeigt die Seriennummer des Geräts an.

Definieren von Systeminformationen

1. Öffnen Sie die Seite **Asset** (Bestand).
2. Definieren Sie folgende Felder: **System Name** (Systemname), **System Contact** (Systemkontakt), **System Location** (Systemstandort) und **Asset Tag** (Asset-Tag).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Systemparameter werden angewendet, und das Gerät wird aktualisiert.

Starten einer Telnet-Sitzung

1. Öffnen Sie die Seite **Asset** (Bestand).

ANMERKUNG: Die entsprechenden Telnet-Parameter werden VOR dem Start der Telnet-Sitzung gesetzt. Weiter Informationen hierzu finden Sie unter Konfigurieren eines ersten Telnet-Kennworts. Arbeitet der Client in einer Microsoft® Windows®-Umgebung, muss das Programm für Telnet konfiguriert werden. Arbeitet der Client in einer Unix-Umgebung, muss das Telnet-Programm in den Pfad aufgenommen werden.

2. Klicken Sie auf **Telnet**.

   Die Eingabeaufforderung erscheint; das System ist jetzt für weitere Eingaben bereit.

Konfigurieren von Geräteinformationen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in den folgendem Kapiteln:

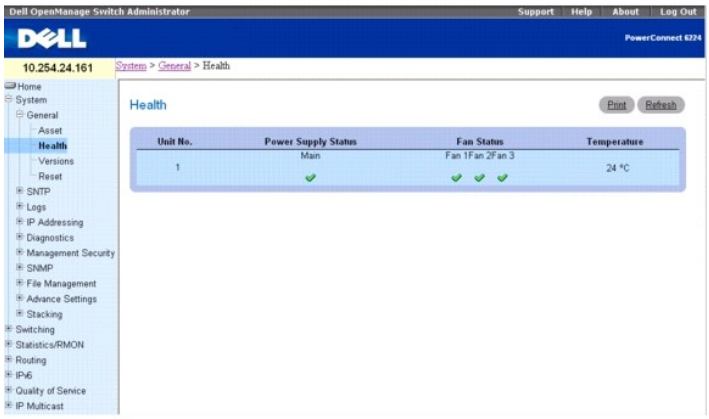
- System Management Commands (System-Management-Befehle)
- SNMP Commands (SNMP-Befehle)
- Clock Commands (Zeit-Befehle)

Systemzustand

Auf der Seite **Health** (Systemzustand) können Sie Informationen zu physikalischen Komponenten des Switch abrufen, beispielsweise den Netzteilen und Lüftern.

Klicken Sie zum Anzeigen der Seite **Health** (Systemzustand) in der Strukturansicht auf **System** → **General (Allgemein)**→ **Health (Systemzustand)**.

Abbildung 6-2. Systemzustand



Die Seite Health enthält folgende Felder:

Unit No. (Einheit-Nr.) – Zeigt die Position der Geräteeinheit im Stack an.

Power Supply Status (Netzteilstatus) – Zeigt den Status des Netzteils an.

– Das Netzteil funktioniert ordnungsgemäß.

– Das Netzteil funktioniert nicht ordnungsgemäß.

Not Present (Nicht vorhanden) – Das Netzteil ist derzeit nicht vorhanden.

Fan Status (Lüfterstatus) – Zeigt den aktuellen Lüfterstatus an. Der PowerConnect 6224 verfügt über drei Lüfter, das Modell 6248 über vier.

– Der Lüfter funktioniert ordnungsgemäß.

– Der Lüfter funktioniert nicht ordnungsgemäß.

Not Present (Nicht vorhanden) – Der Lüfter ist derzeit nicht vorhanden.

Temperature (Temperatur) – Zeigt die aktuelle Gerätetemperatur an.

Anzeigen von Informationen zum Systemzustand mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

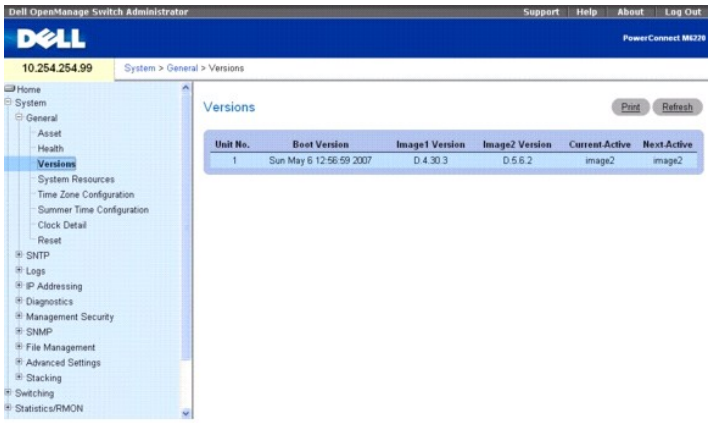
- System Management Commands (System-Management-Befehle)

Versionen

Auf der Seite **Versions** (Versionen) können Sie Informationen zu den Versionen der derzeit ausgeführten Hardware und Software abrufen.

Klicken Sie zum Anzeigen der Seite **Versions** (Versionen) in der Strukturansicht auf **System**→ **General (Allgemein)**→ **Versions (Versionen)**.

Abbildung 6-3. Versionen



Die Seite Versions (Seiten) enthält folgende Felder:

Unit No. (Einheit-Nr.) – Zeigt die Position der Geräteeinheit im Stack an.

Boot Version (Boot-Version) – Zeigt die Boot-Abbild-Version des aktiven Abbilds.

Image1 Version (Abbild1-Version) – Zeigt die Versionsnummer eines der beiden verfügbaren Software-Images.

Image2 Version (Abbild2-Version) – Zeigt die Versionsnummer des anderen der beiden verfügbaren Software-Images.

Current-Active (Derzeit aktiv) – Zeigt die derzeit auf dem Gerät ausgeführte Version der Software.

Next-Active (Als nächstes aktiv) – Zeigt die Softwareversion, die geladen wird, falls die derzeit aktive Version abstürzt.

Anzeigen von Geräteversionen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

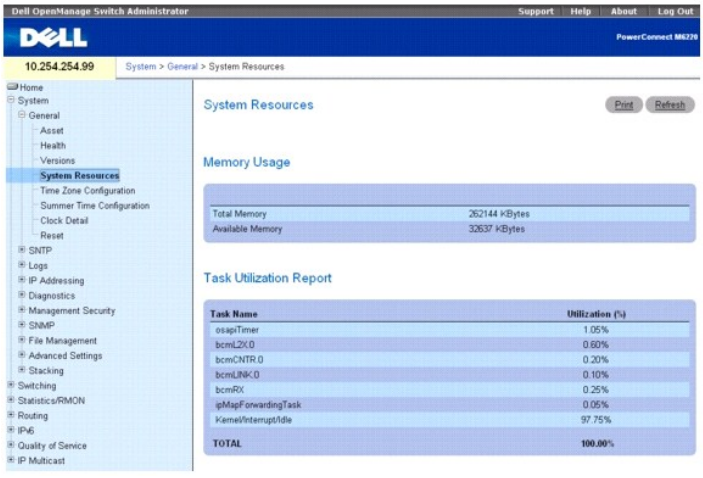
- System Management Commands (System-Management-Befehle)

Systemressourcen

Verwenden Sie die Seite **Systemressourcen** , um Informationen zu Speicherverwendung und Aufgabennutzung anzuzeigen.

Klicken Sie zum Anzeigen der Seite **System Resources** (Systemressourcen) in der Strukturansicht auf **System→ General (Allgemein)→ System Resources (Systemressourcen)**.

Abbildung 6-4. Systemressourcen



Die Seite System Resources (Systemressourcen) enthält folgende Felder:

Total Memory (Speicher insgesamt) – Zeigt den insgesamt vorhandenen Speicher des Switches an.

Available Memory (Verfügbarer Speicher) – Zeigt den verfügbaren (zuweisbaren) Speicher des Switch an.

Task Name (Aufgabenname) – Name der aktiven Aufgabe, die am Switch ausgeführt wird.

Utilization (%) (Nutzung %) – Prozentanteil der Prozessorzeit, die von der betreffenden Aufgabe beansprucht wird. Die Berechnung erfolgt für einen Zeitraum von 2 Sekunden.

Anzeigen der Systemressourcen, die die CLI nutzen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

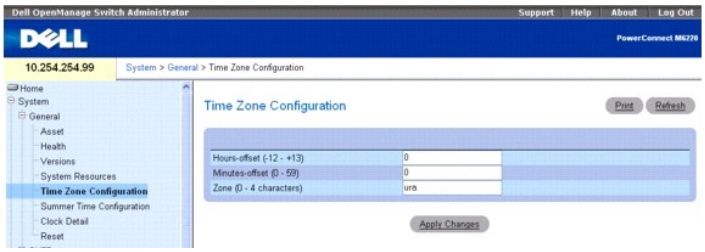
- System Management Commands (System-Management-Befehle)

Zeitzonenkonfiguration

Über die **Zeitzonenkonfiguration** können Sie die Abweichung Ihrer Zeitzone von der UTC-Standardzeit (Coordinated Universal Time) einstellen.

Um die Seite **Time Zone Configuration** (Zeitzonenkonfiguration) anzuzeigen, klicken Sie in der Strukturansicht auf **System**→ **General (Allgemein)**→ **Time Zone Configuration (Zeitzonenkonfiguration)**.

Abbildung 6-5. Zeitzonenkonfiguration



Die Seite Time Zone Configuration (Zeitzonenkonfiguration) enthält folgende Felder:

Hours-offset (Stundendifferenz) – Stellen Sie die Abweichung von der UTC-Standardzeit in Stunden ein. (Bereich: -12 bis +13)

Minutes-offset (Minutendifferenz) – Stellen Sie die Abweichung von der UTC-Standardzeit in Minuten ein. (Bereich: 0–59)

Zone – Geben Sie die Abkürzung für die betreffende Zeitzone ein. (Bereich: 0–4 Zeichen)

Festlegen der Zeitzonenparameter

1. Öffnen Sie die Seite **Time Zone Configuration** (Zeitzonenkonfiguration).
2. Nehmen Sie die erforderlichen Einstellungen vor.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Zeitzoneneinstellungen werden geändert, und das Gerät wird aktualisiert.

Konfiguration der Zeitzoneneinstellungen über die CLI

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

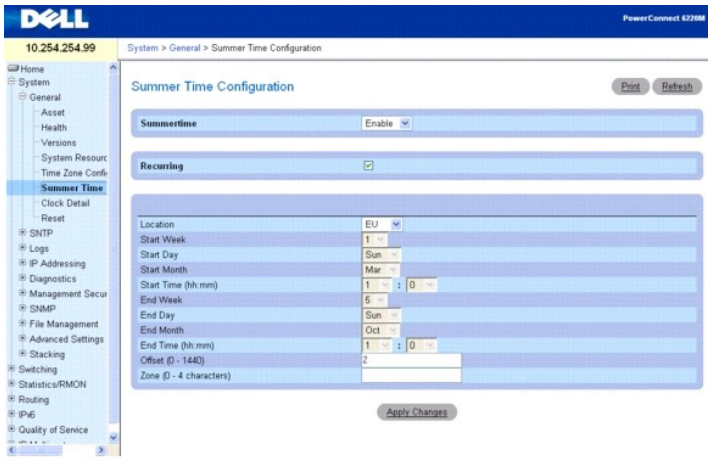
- Clock Commands (Zeit-Befehle)

Sommerzeitkonfiguration

Verwenden Sie die Seite **Sommerzeitkonfiguration** , um Dauer und Zeitverschiebung für die Sommerzeit festzulegen.

Um die Seite **Summer Time Configuration** (Sommerzeitkonfiguration) anzuzeigen, klicken Sie in der Strukturansicht auf **System**→ **General (Allgemein)**→ **Summer Time Configuration (Sommerzeitkonfiguration)**.

Abbildung 6-6. Sommerzeitkonfiguration



Die Felder auf der Seite Summer Time Configuration (Sommerzeitkonfiguration) ändern sich je nachdem, ob Sie das Kontrollkästchen "Recurring" (Wiederkehrend) markieren oder nicht. Die Seite Summer Time Configuration (Sommerzeitkonfiguration) enthält folgende Felder:

Recurring (Wiederkehrend) – Markieren Sie dieses Kontrollkästchen, um festzulegen, dass die Konfiguration jährlich wiederholt wird.

Location (Standort) – Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen "Recurring" markiert ist. Die Sommerzeitkonfigurationen für die USA und die EU sind vordefiniert. Um einen anderen Sommerzeit-Standort als die USA oder die EU festzulegen, wählen Sie "None".

Start Week (Anfangswoche) – Wählen Sie die Nummer der Anfangswoche aus. Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen "Recurring" markiert ist.

Start Day (Anfangstag) – Wählen Sie die Nummer des Anfangstags aus. Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen "Recurring" markiert ist.

Start Month (Anfangsmonat) – Wählen Sie die Nummer des Anfangsmonats aus.

Start Time (Anfangszeit) – Wählen Sie die Uhrzeit für den Anfang aus (im Format hh:mm).

Start Date (Anfangsdatum) – Wählen Sie das Anfangsdatum aus. Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen "Recurring" nicht markiert ist.

Start Year (Anfangsjahr) – Wählen Sie das Anfangsjahr aus. Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen "Recurring" nicht markiert ist.

End Week (Endwoche) – Wählen Sie die Nummer der Endwoche aus. Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen "Recurring" markiert ist.

End Day (Endtag) – Wählen Sie die Nummer des Endtags aus. Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen "Recurring" markiert ist.

End Month (Endmonat) – Wählen Sie die Nummer des Endmonats aus.

End Time (Endzeit) – Wählen Sie die Uhrzeit für das Ende aus (im Format hh:mm).

End Date (Enddatum) – Wählen Sie das Enddatum aus. Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen "Recurring" nicht markiert ist.

End Year (Endjahr). — Wählen Sie das Endjahr aus. Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen "Recurring" nicht markiert ist.

Offset (Verschiebung) – Geben Sie die Anzahl der Minuten an, die während der Sommerzeit hinzugerechnet werden sollen (von 0 bis 1440).

Zone – Geben Sie die Abkürzung für die Zeitzone ein, die angezeigt werden soll, während die Sommerzeit gilt.

Definition der Parameter für die Sommerzeit

1. Öffnen Sie die Seite **Summer Time Configuration** (Sommerzeitkonfiguration).
2. Nehmen Sie die erforderlichen Einstellungen vor.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Sommerzeiteinstellungen werden geändert, und das Gerät wird aktualisiert.

Konfiguration der Sommerzeit-Parameter über die CLI

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

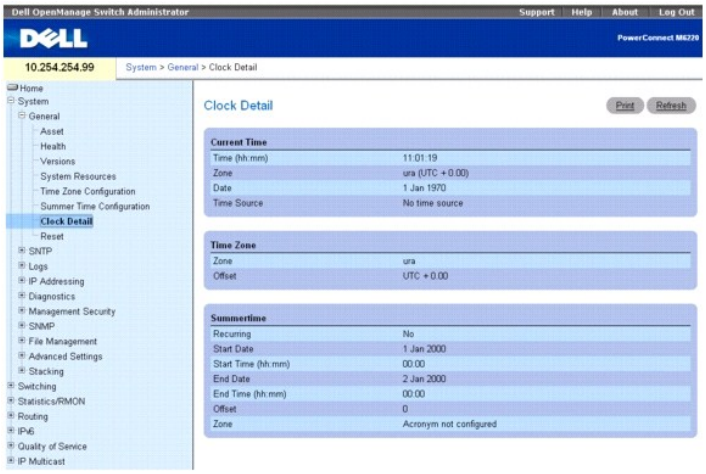
- Clock Commands (Zeit-Befehle)

Einstellungsoptionen für die Uhr

Verwenden Sie die Seite **Clock Detail** (Einstellungsoptionen für die Uhr), um Informationen zu den Einstellungen für die aktuelle Uhrzeit, die Zeitzone und die Sommerzeit anzuzeigen.

Klicken Sie zum Anzeigen der Seite **Clock Detail** (Einstellungsoptionen für die Uhr) in der Strukturansicht auf **System**→ **General (Allgemein)**→ **Clock Detail (Einstellungsoptionen für die Uhr)**.

Abbildung 6-7. Einstellungsoptionen für die Uhr



Die Seite Clock Detail (Einstellungsoptionen für die Uhr) enthält Informationen zu folgenden Uhrzeitfunktionen:

Current Time (Aktuelle Uhrzeit) – In diesem Abschnitt wird die aktuelle Uhrzeit angezeigt.

Time Zone (Zeitzone) – In diesem Abschnitt werden die Einstellungen für die Zeitzone angezeigt.

Summertime (Sommerzeit) – In diesem Abschnitt werden die Einstellungen für die Sommerzeit angezeigt.

Einstellungsoptionen für die Uhr über die CLI anzeigen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

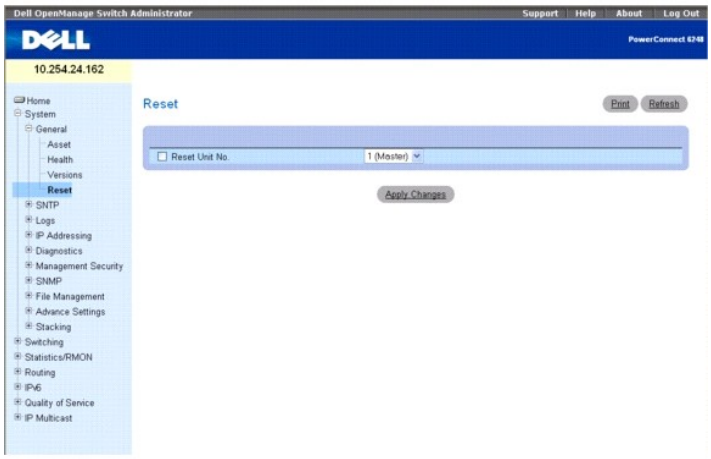
- Clock Commands (Zeit-Befehle)

Zurücksetzen

Auf der Seite **Reset** (Zurücksetzen) können Sie veranlassen, dass das Gerät zurückgesetzt wird.

Klicken Sie zum Anzeigen der Seite **Reset** (Zurücksetzen) in der Strukturansicht auf **System** → **General (Allgemein)**→ **Reset (Zurücksetzen)**.

Abbildung 6-8. Zurücksetzen



Die Seite Reset (Zurücksetzen) enthält folgende Felder:

Reset Unit No. (Einheit Nr. # zurücksetzen) – Dient der Auswahl der Geräteeinheit im Stack, die zurückgesetzt werden muss.

Zurücksetzen des Geräts

1. Öffnen Sie die Seite **Reset** (Zurücksetzen).
2. Klicken Sie auf **Reset Unit No.**

   (Einheit Nr. # zurücksetzen).
3. **Wählen Sie entweder Individual Unit (Bestimmte Einheit) oder All**

   (Alle).
4. Klicken Sie auf die Schaltfläche **Apply Changes (Änderungen übernehmen).**
5. Klicken Sie bei Erscheinen der Bestätigungsmeldung auf **OK**.

   Das ausgewählte Gerät wird zurückgesetzt. Geben Sie nach dem Zurücksetzen des Geräts einen Benutzernamen und das zugehörige Kennwort ein.

Konfigurieren von SNTP-Einstellungen

Das Gerät unterstützt das Simple Network Time Protocol (SNTP). SNTP stellt die genaue Zeitsynchronisierung des Netzwerkgeräts bis auf die Millisekunde sicher. Die Zeitsynchronisierung erfolgt über einen SNTP-Server des Netzwerks. Das Gerät wird nur als SNTP-Client betrieben; es kann keine Zeitdienste für andere Systeme bereitstellen.

Die Zeitquellen werden über entsprechende Strata realisiert. Die Stratum-Werte legen die Genauigkeit der Referenzuhr fest. Je höher das Stratum (wobei Null den höchsten Wert darstellt), desto genauer arbeitet die Uhr. Das Gerät empfängt die Zeit von Stratum 1 (oder höher), dass es sich bei dem Gerät selbst um ein Stratum 2-Gerät handelt.

Im Folgenden ist ein Beispiel für Stratum-Werte gezeigt:

- **Stratum 0** *–Als Zeitquelle wird eine Echtzeituhr verwendet, zum Beispiel ein GPS-System.*
- **Stratum 1** *– Es wird ein Server verwendet, der direkt mit einer Stratum 0-Zeitquelle verbunden ist. Stratum 1-Zeitserver stellen primäre Netzwerk-Zeitstandards bereit.*
- **Stratum 2 –** *Der Stratum 1-Server bezieht die Zeit über einen Netzwerkpfad von der Zeitquelle. Beispielsweise empfängt der Stratum 2-Server die Zeit über eine Netzwerkverbindung und NTP von einem Stratum 1-Server.*

Die von SNTP-Servern empfangenen Informationen werden auf der Grundlage der Zeitebene und des Servertyps ausgewertet.

SNTP-Zeitdefinitionen werden anhand der folgenden Zeitebenen beurteilt und ermittelt:

- **T1** *– Die Zeit, zu der die ursprüngliche Anforderung vom Client gesendet wurde.*
- **T2 –** *Die Zeit, zu der die ursprüngliche Anforderung vom Server empfangen wurde.*
- **T3** *– Die Zeit, zu der der Server eine Antwort gesendet hat.*
- **T4 –** *Die Zeit, zu der der Client die Antwort des Servers empfangen hat.*

Das Gerät kann die Serverzeit von den folgenden Servertypen abfragen: Unicast und Broadcast.

Die Abfrage von Unicast-Informationen wird zur Abfrage eines Servers verwendet, dessen IP-Adresse bekannt ist. Für die Abfrage von Synchronisierungsinformationen werden nur SNTP-Server verwendet, die für das Gerät konfiguriert worden sind. Die Zeitebenen T1 bis T4 werden zur Ermittlung der Serverzeit verwendet. Dies ist das bevorzugte Verfahren für die Synchronisierung der Gerätezeit, da es das sicherste Verfahren ist. Wenn dieses Verfahren ausgewählt ist, werden nur SNTP-Informationen von SNTP-Servern akzeptiert, die über die Seite **SNTP Servers** (SNTP-Server) für das Gerät definiert wurden.

Die Abfrage von Broadcast-Informationen wird verwendet, wenn die IP-Adresse des Servers unbekannt ist. Jede Broadcast-Nachricht, die von einem SNTP-Server gesendet wird, wird vom SNTP-Client empfangen. Wenn die Broadcast-Abfrage aktiviert ist, werden beliebige Synchronisierungsinformationen akzeptiert, auch wenn sie nicht durch das Gerät angefordert wurden. Dieses Verfahren ist am unsichersten.

Das Gerät ruft die Synchronisierungsinformationen entweder durch aktives Anfordern der Daten oder zu einem Zeitpunkt ab, der durch das Abfrageintervall festgelegt ist. Wenn die Unicast- und Broadcast-Abfrage aktiviert ist, werden die Informationen in der folgenden Reihenfolge abgerufen:

- Informationen von Servern, die für das Gerät definiert sind, werden bevorzugt. Wenn die Unicast-Abfrage deaktiviert ist oder keine Server für das Gerät definiert sind, akzeptiert das Gerät Zeitinformationen von einem beliebigen SNTP-Server, der eine Antwort sendet.
- Wenn mehrere Unicast-Geräte eine Antwort senden, werden die Synchronisierungsinformationen des Geräts bevorzugt, das das niedrigste Stratum besitzt.
- Ist das Stratum der Server identisch, werden die Synchronisierungsinformationen des SNTP-Servers akzeptiert, der zuerst eine Antwort gesendet hat.

Pfade zu SNTP-Servern, über die eine Gerätesynchronisierung erfolgt, sind durch MD5-Authentifizierung (Message Digest 5) geschützt. MD5 ist ein Algorithmus, der einen 128 Bit langen Hash-Wert erzeugt. MMD5 ist eine Variante von MD4 und erhöht die MD4-Sicherheit. MD5 überprüft die Integrität der Kommunikation und authentifiziert den Ursprung der Kommunikation.

Die Menüseite **SNTP** enthält Links zu Seiten, auf denen Sie SNTP-Geräteparameter konfigurieren können.

Klicken Sie zum Anzeigen der Seite **SNTP** in der Strukturansicht auf **System → SNTP** .

Die Seite bietet Zugriff auf folgende Funktionen:

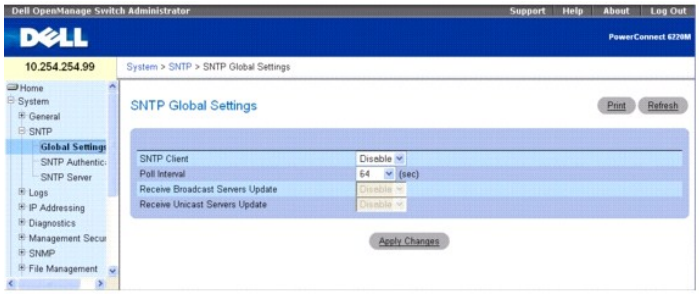
- Globale SNTP-Einstellungen
- SNTP-Authentifizierung
- SNTP-Server

Globale SNTP-Einstellungen

Auf der Seite SNTP Global Settings (Globale SNTP-Einstellungen) können Sie die SNTP-Parameter einsehen und anpassen.

Klicken Sie zum Anzeigen der Seite SNTP Global Settings (Globale SNTP-Einstellungen) in der Strukturansicht auf **System→SNTP→ Global Settings (Globale Einstellungen)**.

Abbildung 6-9. Globale SNTP-Einstellungen



Die Seite SNTP Global Settings (Globale SNTP-Einstellungen) enthält folgende Felder:

SNTP Client (SNTP-Client) – Über diese Dropdown-Liste kann der Client aktiviert bzw. deaktiviert werden. Bei Deaktivierung des Clients werden auch einige der nachstehenden Felder deaktiviert.

Poll Interval (Abfrageintervall) – Definiert das Intervall (in Sekunden) für die Abfrage von Unicast-Informationen des SNTP-Servers. Der Wertebereich liegt zwischen 60 und 1024 Sekunden.

Receive Broadcast Servers Update (Aktualisierungen von Broadcast-Servern empfangen) – Bei Aktivierung dieser Option (Einstellung **Enable**) prüfen die ausgewählten Schnittstellen, ob Broadcast-Server-Zeitinformationen von den SNTP-Servern gesendet werden. Das Gerät wird bei jedem Eingang eines SNTP-Pakets synchronisiert – und zwar auch dann, wenn keine Synchronisierung angefordert wurde.

Receive Unicast Servers Update (Aktualisierungen von Unicast-Servern empfangen) – Bei Aktivierung dieser Option (Einstellung **Enable**) werden Unicast-Server-Zeitinformationen von den geräteseitig definierten SNTP-Servern abgerufen.

Definieren globaler SNTP-Parameter

1. Öffnen Sie die Seite **SNTP Global Settings** (Globale SNTP-Einstellungen).
2. Nehmen Sie die erforderlichen Einstellungen vor.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die globalen SNTP-Einstellungen werden geändert, und das Gerät wird aktualisiert.

Definieren globaler SNTP-Parameter mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

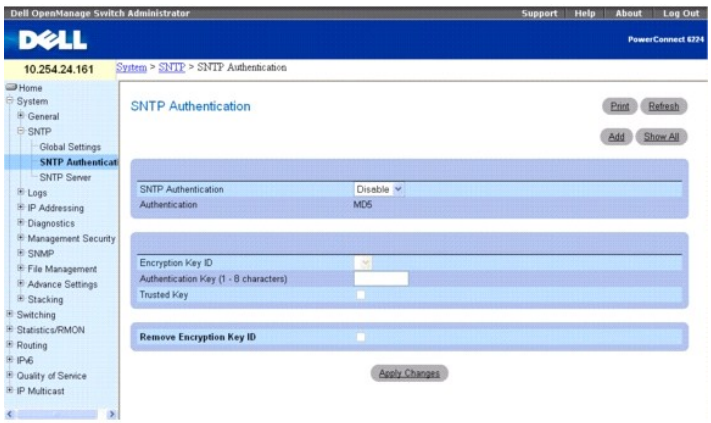
- Clock Commands (Zeit-Befehle)

SNTP-Authentifizierung

Auf der Seite **SNTP Authentication** (SNTP-Authentifizierung) können Sie die SNTP-Authentifizierung zwischen dem Gerät und einem SNTP-Server aktivieren und den gewünschten SNTP-Server auswählen. Nutzen Sie die Seite SNTP Authentication (**SNTP-Authentifizierung**), um die SNTP-Authentifizierung zu aktivieren bzw. deaktivieren, den Authentifizierungsschlüssel (Authentication Key) für eine zuvor ausgewählte Verschlüsselungsschlüssel-ID (Encryption Key ID) zu ändern, den gewählten Authentifizierungsschlüssel als vertrauenswürdigen Schlüssel (Trusted Key) zu vereinbaren und die gewählte Verschlüsselungsschlüssel-Kennung zu entfernen.

Klicken Sie in der Strukturansicht auf **System → SNTP → Authentication** (Authentifizierung), um die Seite **SNTP Authentication** (SNTP-Authentifizierung) anzuzeigen.

Abbildung 6-10. SNTP-Authentifizierung



Die Seite **SNTP Authentication** (SNTP-Authentifizierung) enthält folgende Felder:

SNTP Authentication (SNTP-Authentifizierung) – Bei Aktivierung dieser Option (Einstellung **Enable**) ist für eine SNTP-Sitzung zwischen dem Gerät und einem SNTP-Server eine Authentifizierung erforderlich.

Authentication (Authentifizierung) **–** Authentifizierungstyp. Das System unterstützt nur MD5.

Encryption Key ID (Verschlüsselungsschlüssel-ID) – Enthält eine Liste mit benutzerdefinierten Schlüsselkennungen (IDs) für die Authentifizierung des SNTP-Servers und des Geräts. Mögliche Werte für dieses Feld sind 1 bis 4294767295.

Authentication Key (1-8 Characters) (Authentifizierungsschlüssel, 1-8 Zeichen) – Der für die Authentifizierung verwendete Schlüssel.

Trusted Key (Vertrauenswürdiger Schlüssel) – Bei Aktivierung dieser Option wird ein Verschlüsselungsschlüssel vereinbart (Unicast), bei Deaktivierung erfolgt eine Authentifizierung des SNTP-Servers (Broadcast).

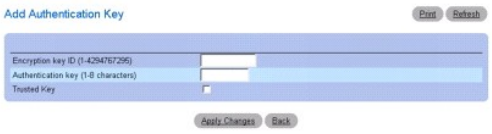
Remove Encryption Key ID (Verschlüsselungsschlüssel-ID entfernen) – Bei Aktivierung dieser Option wird der zuvor ausgewählte Authentifizierungsschlüssel wieder entfernt.

Hinzufügen eines SNTP-Authentifizierungsschlüssels

1. Öffnen Sie die Seite **SNTP Authentication** (SNTP-Authentifizierung).
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add Authentication Key** (Authentifizierungsschlüssel hinzufügen) wird angezeigt:

Abbildung 6-11. Authentifizierungsschlüssel hinzufügen



3. Nehmen Sie die erforderlichen Einstellungen vor.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der SNTP-Authentifizierungsschlüssel wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der Seite Authentication Key Table (Tabelle der Authentifizierungsschlüssel)

1. Öffnen Sie die Seite **SNTP Authentication** (SNTP-Authentifizierung).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **Authentication Key Table** (Tabelle der Authentifizierungsschlüssel) wird angezeigt:

Abbildung 6-12. Tabelle der Authentifizierungsschlüssel

Entfernen eines Authentifizierungsschlüssels

1. Öffnen Sie die Seite **SNTP Authentication** (SNTP-Authentifizierung).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **Authentication Key Table** (Tabelle der Authentifizierungsschlüssel) wird angezeigt.
3. Wählen Sie einen Eintrag der **Authentication Key Table** (Tabelle der Verschlüsselungsschlüssel) aus, indem Sie auf das zugehörigen Kontrollkästchen **Remove** (Entfernen) klicken.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Eintrag wird entfernt und das Gerät aktualisiert.

Definieren von SNTP-Authentifizierungseinstellungen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

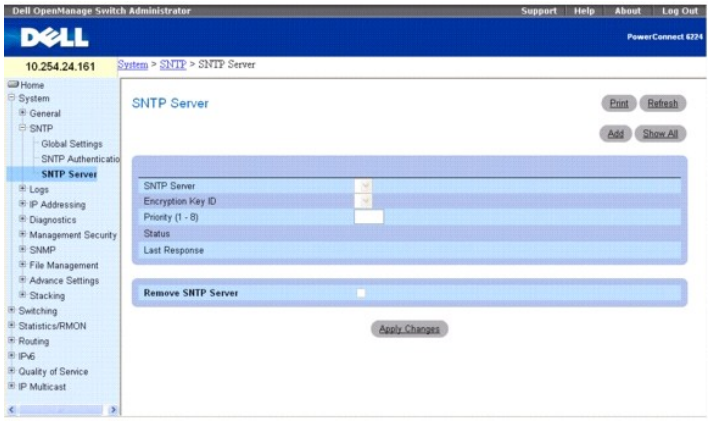
- Clock Commands (Zeit-Befehle)

SNTP-Server

Auf der Seite **SNTP Server** (SNTP-Server) können Sie Informationen zur Aktivierung von SNTP-Servern einsehen oder ändern und bei Bedarf neue SNTP-Server hinzufügen.

Klicken Sie zum Anzeigen der Seite **SNTP Server** (SNTP-Server) in der Strukturansicht auf **System→ SNTP→ SNTP Server**.

Abbildung 6-13. SNTP-Server



Die Seite **SNTP Servers (SNTP-Server) enthält folgende Felder:**

SNTP Server (SNTP-Server) – Öffnet ein Dropdown-Menü mit benutzerdefinierten IP-Adressen für SNTP-Server. Bis zu acht SNTP-Server können hier über die Schaltfläche **Add** (Hinzufügen) definiert werden.

Encryption Key ID (Verschlüsselungsschlüssel-ID) – Legt die für die Kommunikation zwischen dem SNTP-Server und dem Gerät verwendete Schlüssel-ID fest. Die Definition der Verschlüsselungsschlüssel-ID erfolgt auf der Seite **SNTP Authentication** (SNTP-Authentifizierung).

Priority (1-8) (Priorität, 1-8) – Legt die Priorität dieses Server-Eintrags fest; dies geschieht durch Festlegung der Reihenfolge, in der SNTP-Anfragen an die Server übermittelt werden. Gültige Werte sind 1 bis 8, der Standardwert lautet 1. Der Server mit dem niedrigsten Wert hat die höchste Priorität.

Status – Zeigt den Betriebsstatus des SNTP-Servers an. Die für dieses Feld möglichen Werte sind:

Up (In Betrieb) – Der SNTP-Server arbeitet derzeit ordnungsgemäß.

Down (Außer Betrieb) – Gibt an, dass derzeit kein SNTP-Server verfügbar ist. Dies ist beispielsweise der Fall, wenn der SNTP-Server gerade nicht mit

dem Netzwerk verbunden oder nicht betriebsbereit ist.

In progress (Übertragung aktiv) – Der SNTP-Server sendet oder empfängt gerade SNTP-Informationen.

Unknown (Unbekannt) – Der Fortschritt bei der Übertragung von SNTP-Daten ist derzeit unbekannt. Dies ist beispielsweise der Fall, wenn das Gerät gerade nach einer Schnittstelle sucht.

Last Response (Letzte Antwort) – Zeigt den letzten Zeitpunkt an, zu dem eine Antwort vom SNTP-Server empfangen wurde.

Remove (Entfernen) – Bei Auswahl dieser Option wird der betreffende SNTP-Server aus der Liste **SNTP Server** entfernt.

Hinzufügen eines SNTP-Servers

1. Öffnen Sie die Seite **SNTP Servers** (SNTP-Server).
2. Klicken Sie auf **Add**

   (Hinzufügen).

   Die Seite **Add SNTP Server** (SNTP-Server hinzufügen) wird angezeigt.

Abbildung 6-14. SNTP-Server hinzufügen

3. Nehmen Sie die erforderlichen Einstellungen vor.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der SNTP-Server wird hinzugefügt und das Gerät aktualisiert.

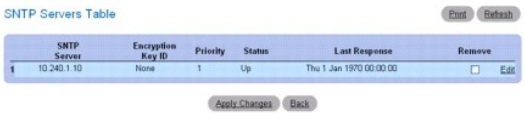
Anzeigen der Seite SNTP Servers Table (Tabelle der SNTP-Server)

1. Öffnen Sie die Seite **SNTP Servers** (SNTP-Server).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die Seite **SNTP Servers Table** (Tabelle der SNTP-Server) wird angezeigt.

Abbildung 6-15. Tabelle der SNTP-Server



Ändern eines SNTP-Servers

1. Öffnen Sie die Seite **SNTP Servers** (SNTP-Server).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die Seite **SNTP Servers Table** (Tabelle der SNTP-Server) wird geöffnet.

3. Klicken Sie neben dem zu ändernden **SNTP Server**-Eintrag auf **Edit** (Bearbeiten).
4. Ändern Sie die relevanten Felder.

5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Informationen zum SNTP-Server werden aktualisiert.

Entfernen eines SNTP-Servers

1. Öffnen Sie die Seite **SNTP Servers** (SNTP-Server).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die Seite **SNTP Servers Table** (Tabelle der SNTP-Server) wird geöffnet.
3. Wählen Sie den Eintrag eines **SNTP-Servers** aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Eintrag wird entfernt und das Gerät aktualisiert.

Definieren von SNTP-Servern mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Clock Commands (Zeit-Befehle)

Verwalten von Protokollen

Der Switch quittiert bestimmte plattformbezogene Ereignisse, Störungen/Ausfälle oder Fehler sowie Konfigurationsänderungen oder anderen Vorkommnisse mit der Ausgabe entsprechender Meldungen. Diese Meldungen werden lokal (d. h. auf der Plattform selbst) gespeichert und zu Überwachungszwecken sowie zur langfristigen Archivierung an einen oder mehrere zentrale Sammelpunkte weitergeleitet. Die lokale Konfiguration und die Fernkonfiguration der Protokollfunktion ermöglicht eine Filterung der protokollierten bzw. weitergeleiteten Meldungen nach Schweregrad und Meldungsquelle (Komponente).

Das *speicherinterne* Protokoll legt – basierend auf den aktuellen Einstellungen für die Meldungskomponente und -dringlichkeit – Meldungen im Speicher ab. Bei stapelbaren Systemen liegt dieses Protokoll nur auf der obersten Plattform vor. Alle anderen Plattformen im Stack leiten ihre Meldungen an das Protokoll dieser (obersten) Plattform weiter. Ein Zugriff auf die speicherinternen Protokolle der übrigen Plattformen ist nicht möglich.

Das *dauerhafte* Protokoll wird im Dauerspeicher abgelegt. Es können zwei Typen von dauerhaften Protokollen konfiguriert werden.

- Der erste Protokolltyp ist ***Systemstart-Protokoll***. Das Systemstart-Protokoll speichert die ersten N Meldungen, die nach einem Neustart des Systems empfangen werden. Bei Erreichen der maximalen Protokollkapazität wird die Meldungsprotokollierung automatisch beendet (Attribut "stop on full"). Das Protokoll kann bis zu 32 Meldungen speichern.
- Der zweite Protokolltyp ist das ***Systembetrieb-Protokoll***. Das Systembetrieb-Protokoll speichert die letzten N Meldungen, die während des Systembetriebs eingehen. Bei Erreichen der maximalen Protokollkapazität werden die aktuellen Protokolleinträge automatisch überschrieben (Attribut "overwrite"). Dieses Protokoll kann bis zu 1000 Meldungen speichern.

Meldungen, die am Protokoll-Subsystem eingehen und die entsprechenden Speicherkriterien erfüllen, werden nicht in beiden, sondern immer nur in einem Protokoll gespeichert: Systemstart-Protokoll ODER Systembetrieb-Protokoll. Mit anderen Worten: Ist das Startprotokoll konfiguriert, werden bei Systemstart so viele Meldungen gespeichert, wie es die Protokollkapazität zulässt. Ist das Betriebsprotokoll konfiguriert, werden weitere Meldungen anschließend in diesem Protokoll gespeichert.

Das System behält maximal drei Versionen der dauerhaften Protokolle bei: <DATEI>0.txt, <DATEI>1.txt und <DATEI>2.txt. Bei Systemstart wird <DATEI>2.txt entfernt, <DATEI>1.txt wird in <DATEI>2.txt umbenannt, <DATEI>0.txt wird in <DATEI>1.txt umbenannt, <DATEI>0.txt wird neu angelegt, und die Protokollierung in <DATEI>0.txt beginnt. (Im obigen Beispiel ist <DATEI> durch olog (für das Betriebsprotokoll) oder slog (für das Startprotokoll) zu ersetzen.)

Die lokalen dauerhaften Protokolle können über die CLI-Schnittstelle, per xmodem über das lokale serielle Kabel oder über TFTP abgerufen werden.

Klicken Sie zum Anzeigen der Menüseite **Logs** (Protokolle) in der Strukturansicht auf **System** → **Logs** (Protokolle). Die Seite bietet Zugriff auf folgende Funktionen:

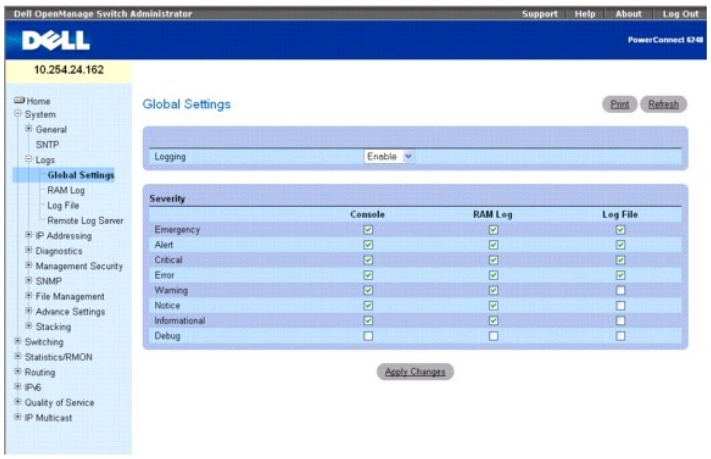
- Globale Einstellungen
- Tabelle der RAM-Protokolleinträge
- Protokolldatei
- Einstellungen von Remote-Protokollservern

Global Settings (Globale Einstellungen)

Auf der Seite **Global Settings** (Globale Einstellungen) können Sie Protokolle global aktivieren und Protokollparameter definieren. Die unter dem **Schweregrad** aufgeführten Protokollmeldungen sind vom höchsten bis zum niedrigsten Schweregrad angeordnet.

Klicken Sie zum Anzeigen der Seite **Global Settings** (Globale Einstellungen) in der Strukturansicht auf **System→ Logs (Protokolle)→ Global Settings (Globale Einstellungen)**.

Abbildung 6-16. Globale Einstellungen



Die Seite Global Settings (Globale SNTP-Einstellungen) enthält folgende Felder:

Logging (Protokolle aufzeichnen) – Ermöglicht die Erstellung globaler Geräteprotokolle in Form von Cache-, Datei- und Serverprotokollen. Alle Protokolle, die an die Konsole ausgegeben werden, werden in Protokolldateien gespeichert. Die für dieses Feld möglichen Werte sind:

Enable (Aktivieren) – Aktiviert die Speicherung von Protokollen im Cache (RAM), in Dateien (FLASH) sowie auf einem externen Server.

Disable – Deaktiviert die Protokollspeicherung. Für Protokolle, die an die Konsole ausgegeben werden, kann die Protokollierungsfunktion nicht deaktiviert werden.

Severity (Schweregrad)

Über die Kontrollkästchen in diesem Abschnitt können Sie die Empfindlichkeit der Konsole, des Dauerspeichers und der Protokolldateien anpassen.

Wenn Sie hier eine bestimmte Empfindlichkeitsebene vereinbaren, werden automatisch auch alle höheren Ebenen ausgewählt. Beispiel: Bei Aktivierung von Error (Fehler) aktiviert das System automatisch Error (Fehler), Critical (Kritisch), Alert (Alarm) und Emergency (Notfall). Bei Deaktivierung von "Error" (Fehler) werden auch alle tieferen Ebenen (z. B. "Error" (Fehler), "Warning" (Warnung), "Notice" (Hinweis), "Informational" (Information), "Debug" (Fehlerbehebung) deaktiviert.

Emergency (Notfall) – Die höchste Warnstufe. Falls keine Verbindung zum Gerät besteht oder das Gerät nicht ordnungsgemäß funktioniert, wird geräteseitig eine Notfall-Protokollmeldung gespeichert.

Alert (Alarm) – Die zweithöchste Warnstufe. Ein Protokoll dieses Typs wird bei einem schwerwiegenden Geräteausfall gespeichert, beispielweise wenn sämtliche Gerätefunktionen ausgefallen sind.

Critical (Kritisch) – Die dritthöchste Warnstufe. Ein Protokoll dieses Typs wird bei einer Gerätefehlfunktion gespeichert, beispielsweise wenn zwei Geräte-Ports nicht arbeiten, während die übrigen Ports weiterhin funktionsfähig sind.

Error (Fehler) – Ein Gerätefehler ist aufgetreten, beispielsweise ein offline geschalteter Port.

Warning (Warnung) – Die niedrigste Gerätewarnstufe.

Notice (Hinweis) – Liefert dem Netzwerkadministrator Geräteinformationen.

Informational (Information) – Zeigt Geräteinformationen an.

Debug (Fehlerbehebung) – Zeigt ausführliche Informationen zum Protokoll an. Der Debug-Modus sollte nur von qualifizierten Support-Mitarbeitern aktiviert werden.

Die Kontrollkästchen erscheinen unter diesen drei Spalten:

Console (Konsole) – Protokolle werden an die Konsole übermittelt.

RAM Logs (RAM-Protokolle) – Protokolle werden an den RAM-Speicher (Cache) übermittelt.

Log File (Protokolldatei) – Protokolle werden in eine Datei ausgegeben (FLASH).

Aktivieren von Protokollen

1. Öffnen Sie die Seite **Global Settings** (Globale Einstellungen).
2. Wählen Sie im **Dropdown-Menü Logging** (Protokolle) die Option **Enable** (Aktivieren) aus.

3. Über die Kontrollkästchen können Sie den Protokolltyp und den Schweregrad auswählen.

ANMERKUNG: Wenn Sie hier einen Schweregrad vereinbaren, werden automatisch auch alle höheren Schweregrade ausgewählt.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Protokolleinstellungen werden gespeichert, und das Gerät wird aktualisiert.

Aktivieren von globalen Protokollen mit Hilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

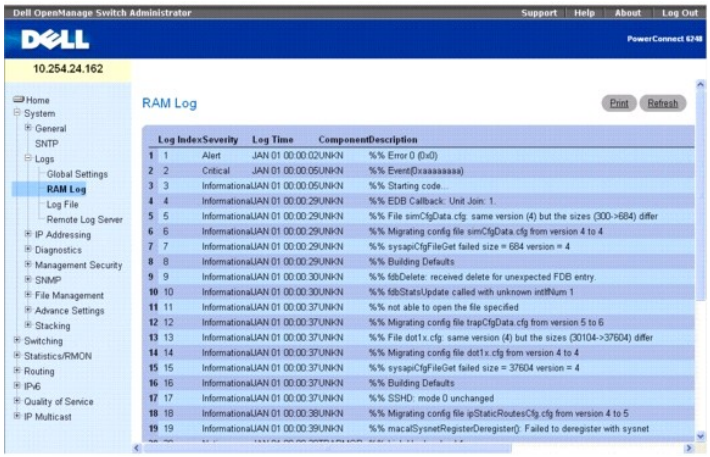
- Syslog-Befehle.

Tabelle der RAM-Protokolleinträge

Auf der Seite **RAM Log Table** (Tabelle der RAM-Protokolleinträge) können Sie Informationen zu bestimmten RAM-(Cache-)Protokolleinträgen einsehen, beispielsweise die Uhrzeit eines Protokolleintrags, den Schweregrad des Protokolls sowie eine Protokollbeschreibung.

Klicken Sie zum Anzeigen der Seite **RAM Log Table** (Tabelle der RAM-Protokolleinträge) in der Strukturansicht auf **System**→ **Logs (Protokolle)**→ **RAM Log (RAM-Protokoll)**.

Abbildung 6-17. Tabelle der RAM-Protokolleinträge



Die Seite RAM Log Table (Tabelle der RAM-Protokolleinträge) enthält folgende Felder:

Log Index (Protokollverzeichnis) – Gibt die Log Number (Protokollnummer) in der Tabelle der RAM-Protokolleinträge an.

Severity (Schweregrad) – Gibt den Schweregrad des Protokolls an.

Log Time (Protokollzeit) – Die Uhrzeit, zu der das Protokoll in die Tabelle der RAM-Protokolleinträge eingefügt wurde.

Component (Komponente) – Die zu protokollierende Komponente.

Description (Beschreibung) – Die Protokollbeschreibung.

Entfernen von Protokollinformationen

1. Öffnen Sie die Seite **RAM Log Table** (Tabelle der RAM-Protokolleinträge).

2. Klicken Sie auf **Clear Log** (Protokoll löschen).

   Die Protokollinformationen werden aus der Tabelle der Protokolldateien entfernt, und das Gerät wird aktualisiert.

Entfernen von Protokollinformationen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

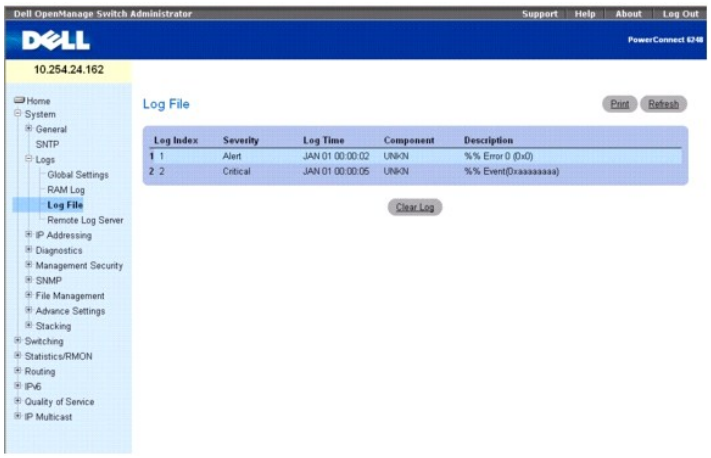
- Syslog-Befehle.

Protokolldatei

Das **Log File** (Protokolldatei) enthält Informationen zu bestimmten Protokolleinträgen, einschließlich der Uhrzeit, zu der das Protokoll aufgezeichnet wurde, des Protokollschweregrads sowie einer Beschreibung des Protokolls.

Klicken Sie zum Anzeigen der Seite **Log File** (Protokolldatei) in der Strukturansicht auf **System**→ **Logs (Protokolle)**→ **Log File (Protokolldatei)**.

Abbildung 6-18. Protokolldatei



Die Seite **Log File Table** (Tabelle der Protokolldateien) enthält folgende Felder:

- **Log Index** (Protokollverzeichnis) – Gibt die Log Number (Protokollnummer) in der Tabelle der Protokolldateien (**Log File Table**) an.
- **Severity** (Schweregrad) – Gibt den Schweregrad des Protokolls an.
- **Log Time** (Protokollzeit) – Die Uhrzeit, zu der das Protokoll in die **Tabelle der Protokolldateien** eingefügt wurde.
- **Component** (Komponente) – Die zu protokollierende Komponente.
- **Description** (Beschreibung) – Die Protokollbeschreibung.

Entfernen von Protokollinformationen

1. Öffnen Sie die Seite **Log File Table** (Tabelle der Protokolldateien).
2. Klicken Sie auf **Clear Log** (Protokoll löschen).

   Die Protokollinformationen werden aus der Tabelle der Protokolldateien entfernt, und das Gerät wird aktualisiert.

Entfernen von Protokollinformationen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

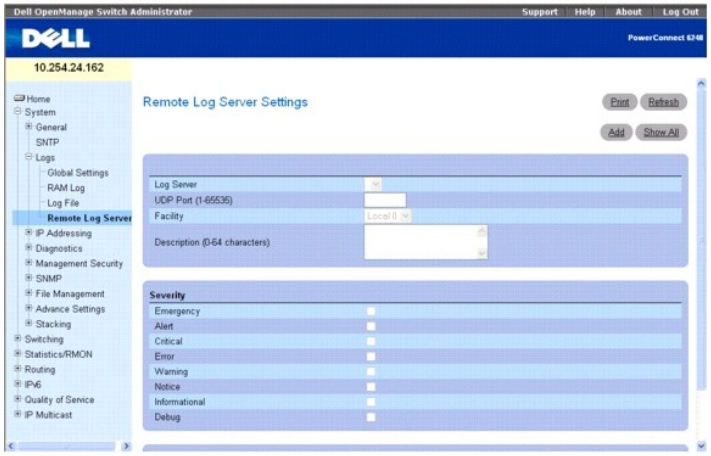
- Syslog-Befehle.

Einstellungen von Remote-Protokollservern

Auf der *Seite* **Remote Log Server Settings** (Einstellungen von Remote-Protokollservern) können Sie die verfügbaren Protokollserver einsehen, neue Protokollserver definieren und den Schweregrad der an den Server übermittelten Protokollereignisse einstellen.

Klicken Sie zum Anzeigen der Seite **Remote Log Server Settings** (Einstellungen von Remote-Protokollservern) auf **System**→ **Logs (Protokolle)**→ **Remote Log Server** (Remote-Protokollserver).

Abbildung 6-19. Einstellungen von Remote-Protokollservern



Die Seite Remote Log Server Settings (Einstellungen von Remote-Protokollservern) enthält folgende Felder:

Log Server (Protokollserver) – Server, an den Protokolle gesendet werden können.

UDP Port (1–65535) (UDP-Port, 1-65535) – Legt fest, von welchem UDP-Port die Protokolle übermittelt werden. Der Standardwert ist 514.

Facility (Anlage) – Eine benutzerdefinierte Anwendung, aus der Systemprotokolle an den Remote-Server gesendet werden. Jedem Server kann nur eine Anlage zugewiesen werden. Wird eine zweite Anlagenebene zugewiesen, wird die erste Anlagenebene aufgehoben. Alle für ein Gerät definierten Anwendungen verwenden dieselbe Anlage auf einem Server. Die möglichen Feldwerte liegen im Bereich **Local 0** bis **Local 7**.

Description (Beschreibung) – Legt die Serverbeschreibung fest. Die maximale Länge beträgt 64 Zeichen.

Severity (Schweregrad) – Vereinbart den Schweregrad des Protokolls. Bei Auswahl eines Schweregrads werden automatisch auch alle höheren Schweregrade ausgewählt.

Remove Log Server (Protokollserver entfernen) – Entfernt einen Server aus der Liste der Protokollserver (**Log Server**). Durch Markieren dieses Kontrollkästchens kann der Server aus der Liste entfernt werden. Wird das Kästchen nicht markiert, verbleibt der Server in der Liste.

Darüber hinaus enthält die Seite **Remote Log Server Settings** (Einstellungen von Remote-Protokollservern) eine Liste der Schweregrade. Die Schweregrad-Definitionen sind identisch mit denen auf der Seite **RAM Log Table** (Tabelle der RAM-Protokolleinträge).

Senden von Protokollen an einen Server

1. Öffnen Sie die Seite **Remote Log Server Settings** (Einstellungen von Remote-Protokollservern).
2. Definieren Sie die Felder **UDP Port** (UDP-Port), **Facility** (Anlage) und **Description** (Beschreibung).
3. Wählen Sie mit Hilfe der Kontrollkästchen auf der Seite **Log Parameters** (Protokollparameter) den Protokolltyp und den Protokollschweregrad aus.

ANMERKUNG: Wenn Sie hier einen Schweregrad vereinbaren, werden automatisch auch alle höheren Schweregrade ausgewählt.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Protokolleinstellungen werden gespeichert, und das Gerät wird aktualisiert.

Hinzufügen eines neuen Servers

1. Öffnen Sie die Seite **Remote Log Server Settings** (Einstellungen von Remote-Protokollservern).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add a Remote Log Server** (Remote-Protokollserver hinzufügen) anzuzeigen.

ANMERKUNG: Bevor Sie einen neuen Server hinzufügen, müssen Sie die IP-Adresse des Remote-Protokollservers bestimmen.

Abbildung 6-20. Einstellungen von Remote-Protokollservern

3. Nehmen Sie im Dialogfeld die erforderlichen Einstellungen und/oder Eingaben vor, und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Auf der Seite **Remote Log Server Settings** (Einstellungen von Remote-Protokollservern) werden die Server in der Liste **Log Server** (Protokollserver) erst angezeigt, nachdem Sie zur Seite **Remote Log Server Settings** (Einstellungen von Remote-Protokollservern) zurückgekehrt sind.

Anzeigen/Entfernen eines Protokollservers

1. Öffnen Sie die Seite **Remote Log Server Settings** (Einstellungen von Remote-Protokollservern).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **Remote Log Servers Table (Remote-Protokollserver-Tabelle) anzuzeigen**.

Abbildung 6-21. Alle Protokollserver anzeigen

3. Markieren Sie ggf. das Kontrollkästchen **Remove** (Entfernen), um den entsprechenden Server zu entfernen.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Server wird entfernt und das Gerät aktualisiert.

Festlegen von Einstellungen für Remote-Protokollserver mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Syslog-Befehle.

Definieren der IP-Adressierung

Auf der Seite **IP Addressing** (IP-Adressierung) können Sie eine Managementschnittstelle sowie Standard-Gateway-IP-Adressen zuweisen, eine Abstimmung mit dem Domänennamen-System vornehmen, einen Standard-Domänennamen vereinbaren, Host-Namen zuweisen sowie ARP- und DHCP-Parameter für die einzelnen Schnittstellen definieren.

Klicken Sie zum Anzeigen der Seite **IP Addressing** (IP-Adressierung) in der Strukturansicht auf **System→ IP Addressing (IP-Adressierung)**. Die Seite bietet Zugriff auf folgende Funktionen:

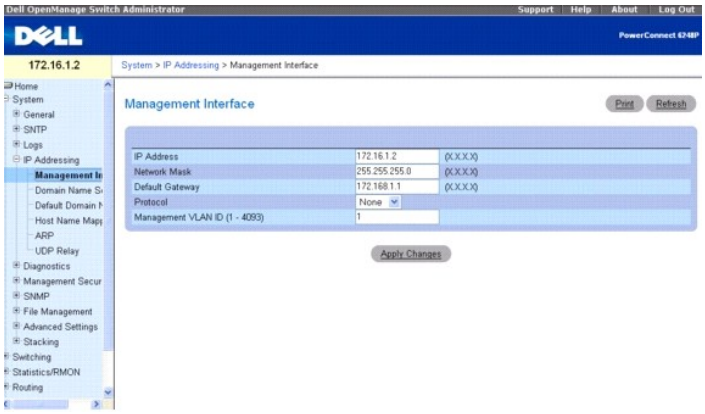
- Managementschnittstelle
- Domänennamen-Server (DNS)
- Standard-Domänenname
- Zuweisung von Host-Namen
- ARP-Tabelle
- UDP-Relais

Managementschnittstelle

Auf der Menüseite **Management Interface** (Managementschnittstelle) können Sie die IP-Adresse der Managementschnittstelle, die Subnetzmaske und die IP-Adresse der Standard-Gateways vereinbaren sowie das Systemstartprotokoll aktivieren bzw. deaktivieren.

Um die Seite **Management Interface** (Managementschnittstelle) anzuzeigen, klicken Sie in der Strukturansicht auf **System→ IP Addressing (IP-Adressierung)→Management Interface (Managementschnittstelle)**.

Abbildung 6-22. Managementschnittstelle



Managementschnittstelle

Die Seite Management Interface (Managementschnittstelle) enthält folgende Felder:

IP Address (IP-Adresse) – Zeigt die IP-Adresse der Managementschnittstelle an.

Network Mask (Netzwerkmaske) – Die Subnetzmaske der IP-Adresse.

ANMERKUNG: Jeder Abschnitt der IP-Adresse muss mit einem numerischen Wert beginnen, der jedoch nicht 0 lauten darf. So sind beispielsweise die IP-Adressen 001.100.192.6 und 192.001.10.3 ungültig.

Default Gateway (Standard-Gateway) – Legt die IP-Adresse des Standard-Gateways fest.

Protocol (Protokoll) — Wählen Sie im Dropdown-Menü eine der Optionen "Bootp", "DCHP" oder "None" (Keines) aus.

Management VLAN ID (1–4093) — Legt die Kennung für das Management-VLAN im Bereich von 1–4093 fest.

HINWEIS: Das Ändern der Kennung für das Management-VLAN bewirkt, dass Ihre Websitzung unterbrochen wird.

Ändern der IP-Adressparameter der Managementschnittstelle

1. Öffnen Sie die Seite **Management Interface** (Managementschnittstelle).
2. Ändern Sie die im Feld **IP Address** angegebene IP-Adresse.
3. Nehmen Sie bei Bedarf weitere Änderungen in den übrigen Feldern vor.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Parameter werden geändert, und das Gerät wird aktualisiert.

Definieren von IP-Schnittstellenparametern mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- IP Routing Commands (IP-Routing-Befehle)

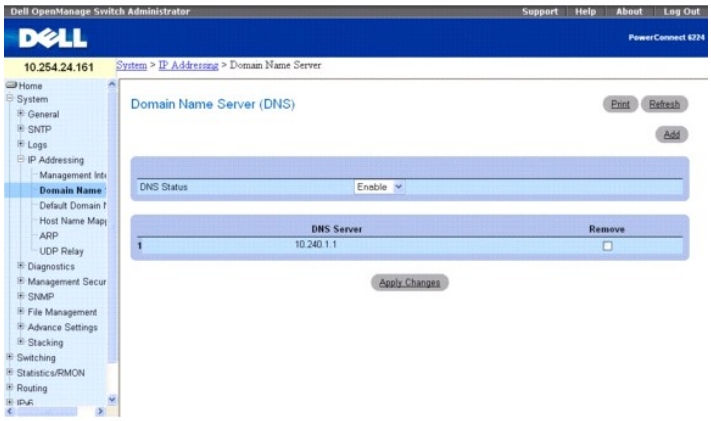
Domänennamen-Server (DNS)

Das Domain Name System (Domänennamen-System, DNS) wandelt benutzerdefinierte Domänennamen in IP-Adressen um. Jedes Mal, wenn ein Domänenname zugewiesen wird, übernimmt dieser Dienst die Umsetzung dieses Namens in eine numerische IP-Adresse. Beispiel: **www.ipexample.com** wird zu 192.87.56.2. DNS-Server pflegen Datenbanken mit Domänennamen sowie den entsprechenden IP-Adressen.

Auf der Seite **Domain Name Server (DNS)** (Domänennamen-Server (DNS)) können Sie bestimmte DNS-Server vereinbaren und aktivieren.

Klicken Sie zum Anzeigen der Seite **Domain Name Server** (Domänennamen-Server) in der Strukturansicht auf **System→IP Addressing (IP-Adressierung)→ Domain Name Server**.

Abbildung 6-23. Domänennamen-Server



Die Seite Domain Name Server (DNS) (Domänennamen-Server (DNS)) enthält folgende Felder:

DNS Status (DNS-Status) – Aktiviert bzw. deaktiviert die Übersetzung von DNS-Namen in IP-Adressen.

DNS Server (DNS-Server) – Enthält eine Liste mit DNS-Servern. DNS-Server werden auf der Seite **Add DNS Server** (DNS-Server hinzufügen) hinzugefügt.

Remove (Entfernen) – Bei Auswahl dieser Option wird der ausgewählte DNS-Server entfernt.

Hinzufügen eines DNS-Servers

1. Öffnen Sie die Seite **Domain Name Server (DNS)** (Domänennamen-Server (DNS)).
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add DNS Server** (DNS-Server hinzufügen) wird angezeigt:

Abbildung 6-24. DNS-Server hinzufügen

3. Definieren Sie die relevanten Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der neue DNS-Server wird definiert und das Gerät aktualisiert.

Konfigurieren von DNS-Servern mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

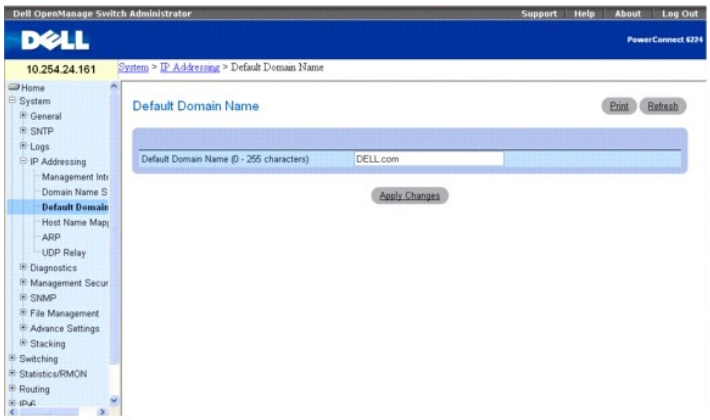
- IP Addressing Commands (IP-Adressierungsbefehle)

Standard-Domänenname

Auf der Seite **Default Domain Name** (Standard-Domänenname) können Sie Standard-DNS-Domänennamen einsehen und definieren.

Klicken Sie zum Anzeigen der Seite **Default Domain Name** (Standard-Domänenname) auf **System→ IP Addressing (IP-Adressierung)→ Default Domain Name** (Standard-Domänenname).

Abbildung 6-25. Standard-Domänenname



Die Seite Default Domain Name (Standard-Domänenname) enthält das folgende Feld:

Default Domain Name (0–255 characters) (Standard-Domänenname, 0-255 Zeichen) – Enthält den benutzerdefinierten Standard-Domänennamen. Wenn ein Standard-Domänenname konfiguriert wurde, wird dieser für alle unvollständigen Host-Namen übernommen.

Definieren von DNS-Domänennamen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

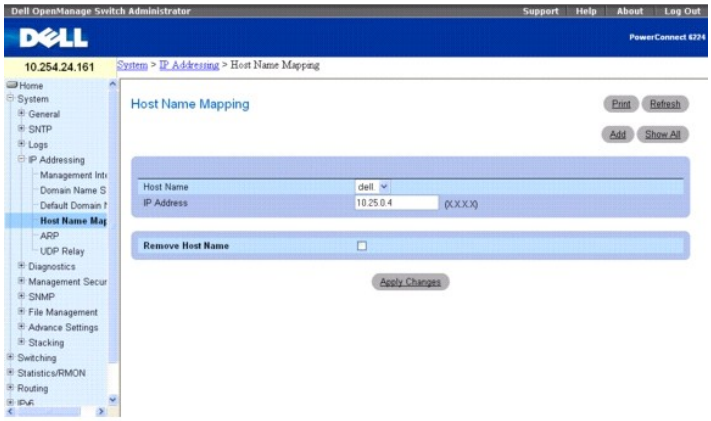
- IP Addressing Commands (IP-Adressierungsbefehle)

Zuweisung von Host-Namen

Auf der Seite **Host Name Mapping** (Zuweisung von Host-Namen) können Sie einem statischen Host-Namen eine IP-Adresse zuweisen. Die Seite **Host Name Mapping** (Zuweisung von Host-Namen) enthält eine IP-Adresse pro Host.

Klicken Sie zum Anzeigen der Seite **Host Name Mapping** (Zuweisung von Host-Namen) auf **System→ IP Addressing (IP-Adressierung)→ Host Name Mapping (Zuweisung von Host-Namen).**

Abbildung 6-26. Zuweisung von Host-Namen



Die Seite Host Name Mapping (Zuweisung von Host-Namen) enthält folgende Felder:

Host Name (Host-Name) – Enthält eine Liste mit Host-Namen. Host-Namen werden auf der Seite **Add Host Name Mapping** (Host-Namen-Zuweisung hinzufügen) definiert. Jedem Host ist eine IP-Adresse zugewiesen.

IP Address (IP-Adresse) – Enthält eine IP-Adresse, die dem angegebenen Host-Namen zugewiesen ist.

Remove Host Name (Host-Name entfernen) – Bei Auswahl dieser Option wird die IP-Zuweisung für den Host-Namen entfernt.

Hinzufügen von Host-Domänennamen

1. Öffnen Sie die Seite **Host Name Mapping** (Zuweisung von Host-Namen).
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add Static Host Name Mapping (Zuweisung für statische Host-Namen hinzufügen) wird angezeigt**:

Abbildung 6-27. Zuweisung für statische Host-Namen hinzufügen

3. Definieren Sie die relevanten Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

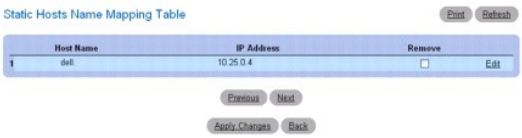
   Die IP-Adresse wird dem Host-Namen zugeordnet und das Gerät aktualisiert.

Anzeigen der Zuweisungstabelle für statische Host-Namen

1. Öffnen Sie die Seite **Host Name Mapping** (Zuweisung von Host-Namen).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **Static Host Name Mapping Table** (Zuweisungstabelle für statische Host-Namen) wird angezeigt:

Abbildung 6-28. Zuweisungstabelle für statische Host-Namen



Entfernen eines Host-Namens aus der IP-Adressen-Zuweisung

1. Öffnen Sie die Seite **Host Name Mapping** (Zuweisung von Host-Namen).
2. Klicken Sie auf **Show All (Alle anzeigen).**

   Die **Host Name Mapping Table** (Zuweisungstabelle für Host-Namen) wird geöffnet:

3. **Wählen Sie einen Eintrag aus der** Host Name Mapping Table **(Zuweisungstabelle für statische Host-Namen) aus.**
4. **Aktivieren Sie das Kontrollkästchen Remove (Entfernen).**
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag in der Host Name Mapping Table (Zuweisungstabelle für Host-Namen) wird gelöscht und das Gerät aktualisiert.

Zuweisen einer IP-Adresse zu Domänen-Host-Namen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

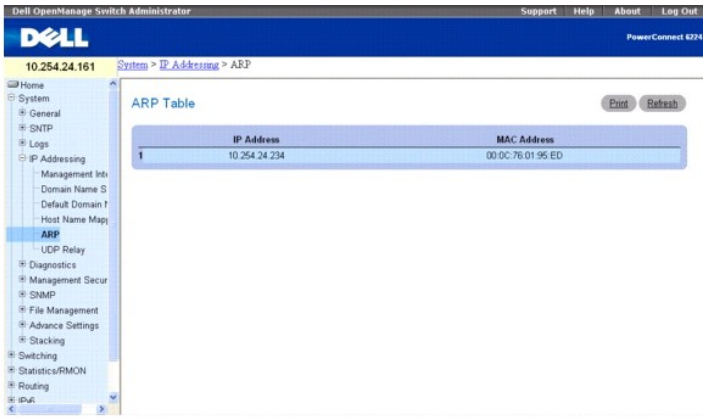
- IP Addressing Commands (IP-Adressierungsbefehle)

ARP-Tabelle

Auf der Seite **ARP Table** (ARP-Tabelle) können Sie ARP-Parameter für IP-Schnittstellen einsehen. Die ARP-Tabelle zeigt die Wechselbeziehung zwischen jeder einzelnen MAC-Adresse und der zugehörigen IP-Adresse.

Klicken Sie zum Anzeigen der Seite **ARP Table** (ARP-Tabelle) in der Strukturansicht auf **System**→ **IP Addressing (IP-Adressierung)**→ **ARP**.

Abbildung 6-29. ARP-Tabelle



Die Seite ARP Table (ARP-Tabelle) enthält folgende Felder:

IP Address (IP-Adresse) – Die Stations-IP-Adresse, die mit der darunter angegebenen MAC-Adresse verknüpft ist.

MAC Address (MAC-Adresse) – Die Stations-MAC-Adresse, die auf der Seite ARP Table (ARP-Tabelle) mit der IP-Adresse verknüpft ist.

Anzeigen der ARP-Tabelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- IP Addressing Commands (IP-Adressierungsbefehle)

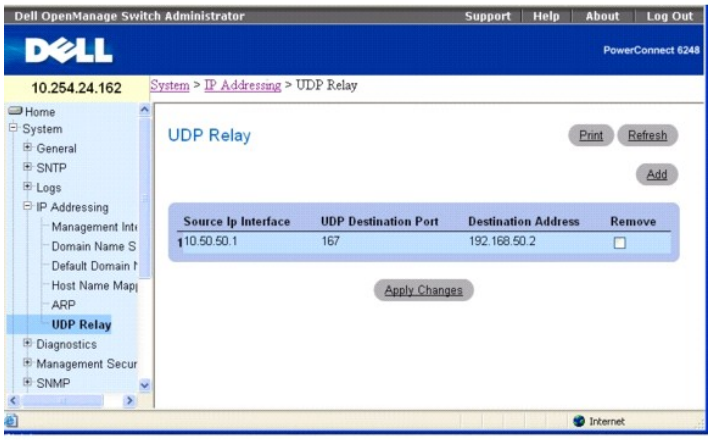
UDP-Relais

Über ein UDP-Relais kann das Gerät bestimmte UDP-Broadcasts von einer Schnittstellen an eine andere übermitteln. In der Regel werden IP-Broadcast-Pakete nicht von einer Schnittstelle an eine andere weitergeleitet, aber einige Anwendungen nutzen UDP-Broadcasts, um die Verfügbarkeit eines Dienstes zu erkennen. Andere Dienste wiederum erfordern ein Routing von UDP-Broadcast-Paketen, um Dienste für Clients bereitstellen zu können, die sich in einem anderen Subnetz befinden. Ein UDP-Relais ermöglicht außerdem Workstation-Suchzugriffe auf Server in anderen Netzwerken.

Auf der Seite UDP Relay (UDP-Relais) können Sie die UDP-Relais-Konfiguration hinzufügen, anzeigen oder löschen.

Klicken Sie zum Anzeigen der Seite **UDP Relay** (UDP-Relais) auf **System**→ **IP Addressing (IP-Adressierung)**→ **UDP Relay** (UDP-Relais).

Abbildung 6-30. UDP-Relais



Die Seite UDP Relay (UDP-Relais) enthält folgende Felder:

Source IP Interface (Quell-IP-Schnittstelle) – Die IP-Eingabeschnittstelle, die UDP-Pakete weiterleitet. Hat dieses Feld den Wert 255.255.255.255, werden UDP-Pakete von allen Schnittstellen weitergeleitet. Folgende Adressbereiche sind ungültig:

0.0.0.0 bis 0.255.255.255

127.0.0.0 bis 127.255.255.255

UDP Destination Port (1–65535) (UDP-Zielport (1-65535)) – Die ID-Nummer des UDP-Zielports, an den UDP-Pakete weitergeleitet werden sollen. Die nachfolgende Tabelle bietet einen Überblick über die Belegung der UDP-Ports.

UDP Port Number (UDP-Port-Nummer)	Akronym	Anwendung
7	Echo	Echo
11	SysStat	Aktiver Benutzer
15	NetStat	NetStat
17	Quote	Zitat des Tages
19	CHARGEN	Zeichengenerator
20	FTP-data	FTP-Daten
21	FTP	FTP
37	Uhrzeit	Uhrzeit
42	NAMESERVER	Host-Namen-Server
43	NICNAME	Wer ist
53	DOMAIN	Domänennamen-Server
69	TFTP	„Trivial File Transfer"-Protokoll
111	SUNRPC	Sun Microsystems Rpc
123	NTP	Netzwerkzeit
137	NetBiosNameService	Verbindungen NT-Server zu Endstelle
138	NetBiosDatagramService	Verbindungen NT-Server zu Endstelle
139	NetBIOS	Verbindungen SessionServiceNT-Server zu Endstelle
161	SNMP	Simple Network Management-Protokoll
162	SNMP-trap	Simple Network Management-Traps
513	who	Unix Rwho Daemon
514	syslog	Systemprotokoll
525	timed	Time Daemon

Destination Address (Zieladresse) – Die IP-Schnittstelle, die UDP-Paket-Relais empfängt. Hat dieses Feld den Wert 0.0.0.0, werden UPD-Pakete verworfen. Hat das Feld jedoch den Wert 255.255.255.255, werden UDP-Pakete an alle IP-Schnittstellen geleitet.

Remove (Entfernen) **–** Aktivieren Sie dieses Kontrollkästchen, um das angegebene UDP-Relais zu entfernen.

Hinzufügen eines UDP-Relais-Eintrags

1. Öffnen Sie die Seite **UDP Relay** (UDP-Relais).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add UDP Relay** (UDP-Relais hinzufügen) anzuzeigen:

Abbildung 6-31. UDP-Relais hinzufügen

3. Füllen Sie die Felder **Source IP Interface** (Quell-IP-Adresse), **UDP Destination Port** (UDP-Zielport) und **Destination Address** (Zieladresse) aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das UDP-Relais wird hinzugefügt und das Gerät aktualisiert.

5. Klicken Sie auf **Back** (Zurück), um zur Seite **UDP Relay** (UDP-Relais) zurückzukehren.

ANMERKUNG: Wird das UDP-Relais aktiviert, aber keine UDP-Port-Nummer angegeben, leitet das Gerät standardmäßig UDP-Broadcast-Pakete für folgende Dienste weiter: IEN-116 Name Service (Port 42), DNS (Port 53), NetBIOS Name Server (Port 137), NetBIOS Datagram Server (Port 138), TACACS Server (Port 49) und Time Service (Port 37).

Entfernen eines UDP-Relais-Eintrags

1. Öffnen Sie die Seite **UDP Relay** (UDP-Relais).
2. Markieren Sie das Kontrollkästchen **Remove** (Entfernen) neben dem zu löschenden Element**.**
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der **UDP Relay**-Eintrag wird entfernt und das Gerät aktualisiert.

Konfiguration der UDP-Relais-Informationen mithilfe der CLI

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- IP Addressing Commands (IP-Adressierungsbefehle)

Ausführen der Kabeldiagnose

Auf der Menüseite **Diagnostics** (Diagnose) können Sie virtuelle Kabeltests für Kupfer- und Glasfaserkabel durchführen.

Klicken Sie zum Anzeigen der Seite **Diagnostics** (Diagnose) in der Strukturansicht auf **System → Diagnostics** (Diagnose).

Die Seite bietet Zugriff auf folgende Funktionen:

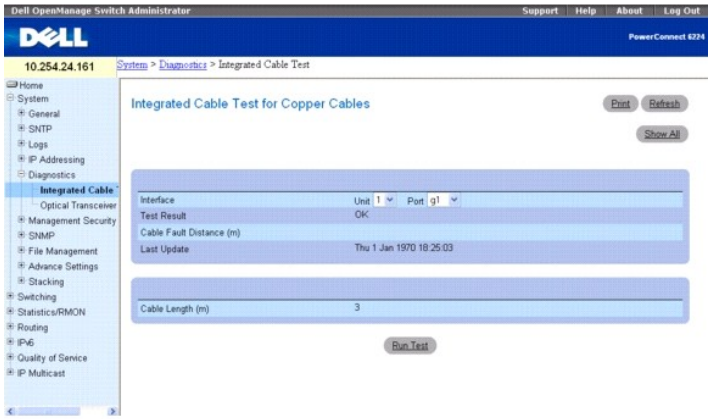
- Integrierter Kabeltest für Kupferkabel
- Diagnose für optische Transceiver

Integrierter Kabeltest für Kupferkabel

Auf der Seite **Integrated Cable Test for Copper Cables** (Integrierter Kabeltest für Kupferkabel) können Sie Tests für Kupferkabel durchführen. Auf dieser Seite finden Sie Informationen über die Stelle im Kabel, an der Fehler aufgetreten sind, den Zeitpunkt der letzten Kabelprüfung und ggf. die Art des Kabelfehlers. Bei den Kabeltests werden mit Hilfe des TDR-Verfahrens (Time Domain Reflectometry) die Qualität und Eigenschaften eines Kupferkabels geprüft, das an einen Port angeschlossen ist. Es lassen sich Kabel mit einer Länge von bis zu 120 Metern prüfen. Kabel werden geprüft, wenn die Ports nicht in Betrieb sind; dies gilt nicht für den Test zur Ermittlung der ungefähren Kabellänge (Approximated Cable Length).

Klicken Sie zum Anzeigen der Seite **Integrated Cable Test for Copper Cables** (Integrierter Kabeltest für Kupferkabel) in der Strukturansicht auf **System→ Diagnostics (Diagnose)→ Integrated Cable Test (Integrierter Kabeltest)**.

Abbildung 6-32. Integrierter Kabeltest für Kupferkabel



Die Seite Integrated Cable Test for Copper Cables (Integrierter Kabeltest für Kupferkabel) enthält folgende Felder:

Interface (Schnittstelle) – Der Schnittstellenport, an dem das Kabel angeschlossen ist.

Test Result (Testergebnis) – Die Ergebnisse des Kabeltests. Mögliche Werte:

No Cable (Kein Kabel) – An den Port ist kein Kabel angeschlossen.

Open Cable (Offenes Kabel) – Die Kabelverbindung ist unterbrochen.

Short Cable (Kurzschluss) – Im Kabel ist ein Kurzschluss vorhanden.

OK – Die Kabelprüfung wurde erfolgreich abgeschlossen.

Fiber Cable (Glasfaserkabel) – An dem Port ist ein Glasfaserkabel angeschlossen.

Cable Fault Distance (Entfernung zum Kabelfehler) – Die Entfernung zwischen dem Port und dem Ort des Kabelfehlers.

Last Update (Letzte Aktualisierung) – Der Zeitpunkt, an dem der Port zuletzt geprüft wurde.

Cable Length (Kabellänge) – Die ungefähre Kabellänge. Dieser Test kann nur durchgeführt werden, wenn der Port aktiv ist und mit einer Geschwindigkeit von 1 Gbit/s arbeitet.

Durchführen einer Kabelprüfung

1. Stellen Sie sicher, dass beide Enden des Kupferkabels an ein Gerät angeschlossen sind.
2. Öffnen Sie die Seite **Integrated Cable Test for Copper Cables** (Integrierter Kabeltest für Kupferkabel).
3. Klicken Sie auf **Run Test** (Test ausführen).

   Der Kupferkabeltest wird durchgeführt, und die Ergebnisse werden auf der Seite **Integrated Cable Test for Copper Cables** (Integrierter Kabeltest für Kupferkabel) angezeigt.

Anzeigen der Ergebnistabelle für die integrierte Kabelprüfung

1. Öffnen Sie die Seite **Integrated Cable Test for Copper Cables** (Integrierter Kabeltest für Kupferkabel).
2. Klicken Sie auf **Show All** (Alle anzeigen).
3. Wählen Sie die gewünschte Einheit aus dem Dropdown-Menü.

   Die Webseite zeigt die Seite **Integrated Cable Test Results Table** (Ergebnistabelle für integrierte Kabelprüfung) mit den Ergebnissen aus früheren Testläufen für jeden einzelnen Port an der gewählten Einheit.

Abbildung 6-33. Ergebnistabelle für integrierte Kabelprüfung

Prüfen von Kupferkabeln mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- PHY Diagnostics Commands (PHY-Diagnose-Befehle)

Diagnose für optische Transceiver

Auf der Seite **Optical Transceiver Diagnostics** (Diagnose für optische Transceiver) können Sie Tests für Glasfaserkabel durchführen.

Klicken Sie zum Anzeigen der Seite **Optical Transceiver Diagnostics** (Diagnose für optische Transceiver) in der Strukturansicht auf **System→ Diagnostics (Diagnose)→ Optical Transceiver Diagnostics (Diagnose für optische Transceiver)**.

ANMERKUNG: Die Diagnose für optische Transceiver kann nur bei vorhandener Verbindung durchgeführt werden.

Abbildung 6-34. Diagnose für optische Transceiver

Die Seite Optical Transceiver Diagnostics (Diagnose für optische Transceiver) enthält folgende Felder:

Port (Port) – Die IP-Adresse des Ports, an den das zu testende Kabel angeschlossen ist.

Temperature (Temperatur) – Die Betriebstemperatur (°C) des Kabels.

Voltage (Spannung) – Die Betriebsspannung des Kabels.

Current (Strom) – Der Betriebsstrom des Kabels.

Output Power (Ausgangsleistung) – Der Übertragungspegel der Ausgangsleistung.

Input Power (Eingangsleistung) – Der Übertragungspegel der Eingangsleistung.

Transmitter Fault (Senderfehler) – Zeigt ggf. das Auftreten eines Fehlers während der Übertragung an.

Loss of Signal (Signalverlust) – Zeigt ggf. einen Signalverlust im Kabel an.

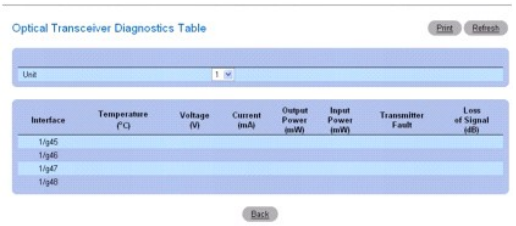
Data Ready (Daten bereit) – Gibt an, dass der Transceiver betriebsbereit ist und Daten bereit stehen.

ANMERKUNG: Finisar-Transceiver unterstützen den Senderfehler-Diagnosetest nicht. Eine Analyse von Glasfaserkabeln kann nur bei SFPs durchgeführt werden, die den Standard SFF-4872 für digitale Diagnosen unterstützen.

Anzeigen der Ergebnistabelle für die Prüfung optischer Transceiver

1. Öffnen Sie die Seite **Optical Transceiver Diagnostics** (Diagnose für optische Transceiver).
2. Klicken Sie auf **Show All** (Alle anzeigen).
3. Wählen Sie die gewünschte Einheit aus dem Dropdown-Menü.

Abbildung 6-35. Ergebnistabelle für die Prüfung optischer Transceiver



Der Test wird durchgeführt, und die Seite **Optical Transceiver Diagnostics Table** (Ergebnistabelle für die Prüfung optischer Transceiver) wird angezeigt.

Prüfen von Glasfaserkabeln mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- PHY Diagnostics Commands (PHY-Diagnose-Befehle)

Verwalten der Gerätesicherheit

Auf der Menüseite **Management Security (Verwalten der Gerätesicherheit)** können Sie Sicherheitsparameter für die Port-, Benutzer- und Serversicherheit einstellen.

Klicken Sie zum Anzeigen der Seite **Management Security** (Verwalten der Gerätesicherheit) in der Strukturansicht auf **System** → **Management Security** (Verwalten der Gerätesicherheit). Die Seite bietet Zugriff auf folgende Funktionen:

- Zugangsprofil
- Authentifizierungsprofile
- Auswählen der Authentifizierung
- Kennwortverwaltung
- Lokale Benutzerdatenbank
- Verbindungskennwörter
- Aktivierungskennwort
- TACACS+-Einstellungen
- RADIUS-Einstellungen
- Telnet-Server
- DoS (Denial of Service)

Zugangsprofil

Auf der Seite **Access Profile** (Zugangsprofil) können Sie ein Profil sowie Regeln für Gerätezugriffe definieren. Hier lassen sich Beschränkungen für den Zugriff auf bestimmte Verwaltungsfunktionen, bestimmte Eintrittsschnittstellen und/oder Quell-IP-Adressen und/oder Quell-IP-Subnetze vereinbaren.

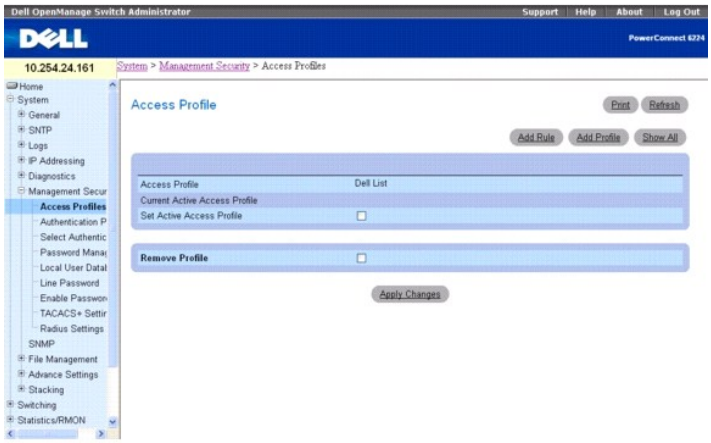
Verwaltungszugriffe können für jede der folgenden Zugriffsmethoden getrennt definiert werden: Webzugriff (HTTP), Sicherer Webzugriff (HTTPS), Telnet, SSH und SNMP.

Management Access Lists (Verwaltungszugriffslisten) enthalten Regeln, über die festgelegt wird, welche Benutzer zur Verwaltung des Gerätes berechtigt sind und welche Methoden hierbei verwendet werden dürfen. Es ist auch möglich, den Gerätezugriff für Benutzer zu sperren.

Auf der Seite **Access Profile** (Zugangsprofil) können Sie Management Lists (Verwaltungslisten) konfigurieren und diese Listen auf bestimmte Schnittstellen anwenden.

Klicken Sie zum Anzeigen der Seite **Access Profile** (Zugangsprofil) in der Strukturansicht auf **System**→ **Management Security (Verwalten der Gerätesicherheit)**→ **Access Profiles (Zugangsprofile)**.

Abbildung 6-36. Zugangsprofil



Access Profile (Zugangsprofil) – Zeigt das Zugangsprofil.

Current Active Access Profile (Derzeit aktives Zugangsprofil) **–** Zeigt das derzeit aktive Zugangsprofil.

Set Active Access Profile (Aktives Zugangsprofil einstellen) – Aktiviert das vereinbarte Zugangsprofil.

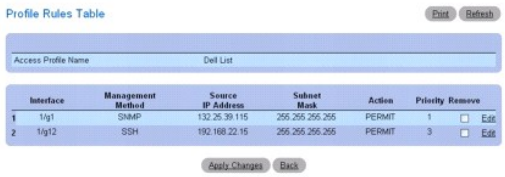
Remove Profile (Profil entfernen) – Bei Auswahl dieser Option wird das Zugangsprofil aus der Liste **Access Profile** (Zugangsprofil) entfernt.

ANMERKUNG: Bei Zuweisung eines Zugangsprofils zu einer Schnittstelle wird der Zugriff über andere Schnittstellen automatisch gesperrt. Ist kein Zugangsprofil aktiviert, kann über alle Schnittstellen auf das Gerät zugegriffen werden.

Anzeigen des Zugangsprofils

1. Öffnen Sie die Seite **Access Profile** (Zugangsprofil).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **Profile Rules Table** (Tabelle der Profilregeln) anzuzeigen.

Abbildung 6-37. Tabelle der Profilregeln

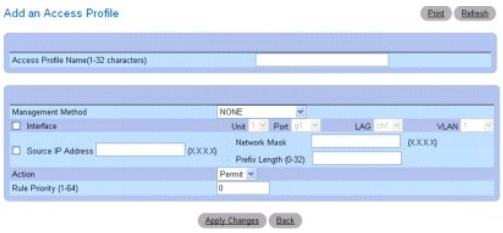


Hinzufügen eines Zugangsprofils

1. Öffnen Sie die Seite **Access Profile** (Zugangsprofil).
2. Klicken Sie auf **Add Profile** (Profil hinzufügen).

   Die Seite **Add an Access Profile** (Zugangsprofil hinzufügen) wird angezeigt.

Abbildung 6-38. Zugangsprofil hinzufügen



3. Geben Sie im Textfeld **Access Profile Name** (Zugangsprofilname) einen Profilnamen ein.
4. Füllen Sie diese Felder aus:

   Management Method (Verwaltungsmethode) **–** Wählen Sie eine Position aus der Dropdown-Liste aus. Die Richtlinie wird durch die vereinbarte Verwaltungsmethode eingeschränkt.

   Interface (Interface) **–** Markieren Sie dieses Kontrollkästchen, wenn die Richtlinie eine schnittstellenbasierte Regel umfassen soll. Bei dieser Schnittstelle kann es sich um eine physikalische Schnittstelle, eine LAG oder ein VLAN handeln.

   Source IP Address (Quell-IP-Adresse) **–** Markieren Sie dieses Kontrollkästchen, wenn die Richtlinie eine Regel umfassen soll, die auf der IP-Adresse des Clients basiert, von dem der Verwaltungsverkehr ausgeht. Geben Sie in den hierfür vorgesehenen Feldern Detailinformationen zur Quell-IP-Adresse und der Netzwerkmaske ein. Hinweis: Die Maske kann in zwei Formaten eingegeben werden: entweder im IP-Format mit Punkten (z. B. 255.255.255.0) oder als Präfixlänge (z. B. 32)

   Action (Aktion) **–** Legen Sie hier fest, welche Aktion ausgeführt werden soll, wenn die weiter oben vereinbarten Regeln entsprochen wird. Öffnen Sie die Dropdown-Liste und wählen Sie **Permit** (Zulassen) oder **Deny** (Ablehnen), um den Zugriff zu gestatten bzw. zu unterbinden.

   Rule Priority (Regelpriorität) **–** Konfigurieren Sie hier Prioritäten für die Regeln. Die Regeln werden – in aufsteigender Reihenfolge der jeweiligen Prioritäten – mit der eingehenden Verwaltungsanforderung abgeglichen. Trifft eine Regel zu, wird die vereinbarte Aktion ausgeführt, und alle nachfolgenden Regeln werden ignoriert. Beispiel: Wenn Sie die Quell-IP-Adresse 10.10.10.10 mit Priorität 1 für **Permit** (Zulassen) konfigurieren und mit Priorität 2 für **Deny** (Ablehnen), wird der Zugriff bei aktivem Profil gestattet; die zweite Regel wird in diesem Fall ignoriert.

5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Das neue Zugangsprofil wird hinzugefügt und das Gerät aktualisiert.

Aktivieren eines Zugangsprofils

1. Öffnen Sie die Seite **Access Profile** (Zugangsprofil).
2. Markieren Sie das Kontrollkästchen **Set Access Profile Active** (Zugangsprofil aktivieren).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Das Zugangsprofil wird für das Gerät aktiviert.

Hinzufügen von Regeln zu einem Zugangsprofil

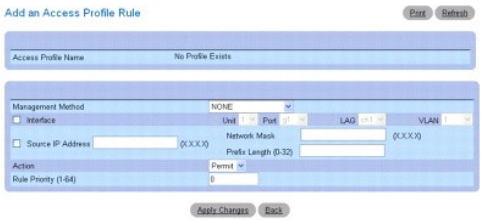
1. Öffnen Sie die Seite **Access Profile** (Zugangsprofil).

   Das Feld **Access Profile** (Zugangsprofil) zeigt das Profil, für das Regeln hinzugefügt werden, wenn die Seite **Add An Access Profile Rule** (Zugangsprofilregel hinzufügen) angezeigt wird.

2. Klicken Sie auf **Add Rule (Regel hinzufügen).**

   Die Seite **Add An Access Profile Rule** (Zugangsprofilregel hinzufügen) wird angezeigt.

Abbildung 6-39. Zugangsprofilregel hinzufügen



3. Nehmen Sie im Dialogfeld die entsprechenden Einstellungen vor.

   Management Method (Verwaltungsmethode) **–** Wählen Sie eine Position aus der Dropdown-Liste aus. Die Richtlinie wird durch die vereinbarte Verwaltungsmethode eingeschränkt.

   Interface (Interface) **–** Markieren Sie dieses Kontrollkästchen, wenn die Richtlinie eine schnittstellenbasierte Regel umfassen soll. Bei dieser Schnittstelle kann es sich um eine physikalische Schnittstelle, eine LAG oder ein VLAN handeln.

   Source IP (Quell-IP-Adresse) **–** Markieren Sie dieses Kontrollkästchen, wenn die Richtlinie eine Regel umfassen soll, die auf der IP-Adresse des Clients basiert, das den Verwaltungsverkehr verursacht. Geben Sie in den hierfür vorgesehenen Textfeldern Detailinformationen zur Quell-IP-Adresse und der Netzwerkmaske ein. Beachten Sie, dass die Maske in zwei Formaten eingegeben werden kann: im IP-Format mit Punkten (z. B. 255.255.255.0) oder als Präfixlänge (z. B. 32)

   Action (Aktion) **–** Legen Sie hier fest, welche Aktion ausgeführt werden soll, wenn die weiter oben vereinbarten Regeln entsprochen wird. Öffnen Sie die Dropdown-Liste und wählen Sie **Permit** (Zulassen) oder **Deny** (Ablehnen), um den Zugriff zu gestatten bzw. zu unterbinden.

   Rule Priority (Regelpriorität) **–** Konfigurieren Sie hier Prioritäten für die Regeln. Die Regeln werden – in aufsteigender Reihenfolge der jeweiligen Prioritäten – mit der eingehenden Verwaltungsanforderung abgeglichen. Trifft eine Regel zu, wird die vereinbarte Aktion ausgeführt, und alle nachfolgenden Regeln werden ignoriert. Beispiel: Wenn Sie die Quell-IP-Adresse 10.10.10.10 mit Priorität 1 für **Permit** (Zulassen) konfigurieren und mit Priorität 2 für **Deny** (Ablehnen), wird der Zugriff bei aktivem Profil gestattet; die zweite Regel wird in diesem Fall ignoriert.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Regel wird zum Zugangsprofil hinzugefügt und das Gerät aktualisiert.

Entfernen einer Regel

1. Öffnen Sie die Seite **Access Profile** (Zugangsprofil).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **Profile Rules Table** (Tabelle der Profilregeln) anzuzeigen.
3. Wählen Sie eine Regel aus.
4. Markieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Regel wird entfernt und das Gerät aktualisiert.

Definieren von Zugangsprofilen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

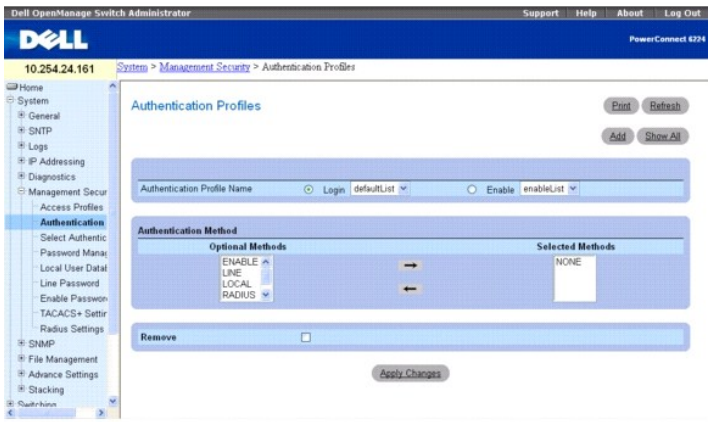
- Management ACL Commands (ACL-Verwaltungsbefehle).

Authentifizierungsprofile

Die Benutzerauthentifizierung erfolgt lokal sowie auf einem externen Server. Auf der Seite **Authentication Profiles** können Sie die Benutzerauthentisierungsmethode für das Gerät auswählen.

Klicken Sie zum Anzeigen der Seite **Authentication Profiles** (Authentifizierungsprofile) in der Strukturansicht auf **System→ Management Security (Verwalten der Gerätesicherheit)→ Authentication Profiles (Authentifizierungsprofile)**.

Abbildung 6-40. Authentifizierungsprofile



Die Seite Authentication Profiles (Authentifizierungsprofile) enthält folgende Felder:

Authentication Profile Name (Authentifizierungsprofilname)

Zeigt Listen, zu denen benutzerdefinierte Authentifizierungsprofile hinzugefügt werden. Vereinbaren Sie über die hierfür vorgesehenen Optionsfelder, ob das Authentifizierungsprofil den Login- oder den Enable-Bereich des Switch-Betriebs regelt, und wählen Sie zusätzlich eine von zwei verfügbaren Listen:

Login (Anmelden) – Bietet die Möglichkeit, sich bei dem Switch anzumelden. Folgende Optionen sind verfügbar: **defaultList**, **networkList** sowie alle benutzerdefinierten Authentifizierungsprofile für die Anmeldung.

Enable (Aktivieren) – Aktiviert den Privileg-Modus.

Authentication Method (Authentifizierungsmethode)

Optional Methods (Optionale Methoden) – Benutzerauthentifizierungsmethoden. Mögliche Optionen:

None (Keine) – Es erfolgt keine Benutzerauthentifizierung.

Local (Lokal) – Die Benutzerauthentifizierung erfolgt auf Geräteebene; Benutzername und Kennwort werden zu Authentifizierungszwecken vom Gerät überprüft.

RADIUS – Die Benutzerauthentifizierung erfolgt auf dem RADIUS-Server. Weitere Information zu RADIUS-Servern finden Sie unter RADIUS-Einstellungen.

TACACS+ — Die Benutzerauthentifizierung erfolgt auf dem TACACS+-Server. Weitere Information zu TACACS+-Servern finden Sie unter TACACS+-Einstellungen.

Line (Verbindung) – Für die Benutzerauthentifizierung wird das Verbindungskennwort verwendet.

Enable (Aktivierung) – Für die Authentifizierung wird das Aktivierungskennwort verwendet.

ANMERKUNG: Die Benutzerauthentifizierung erfolgt in der Reihenfolge, in der die Methoden ausgewählt werden. Falls während der Authentisierung ein Fehler auftritt, wird die nächste ausgewählte Methode verwendet. Wird beispielsweise zunächst **Local** (Lokal) und dann die Option **RADIUS** ausgewählt, wird der Benutzer zuerst lokal und anschließend über einen externen **RADIUS**-Server authentifiziert.

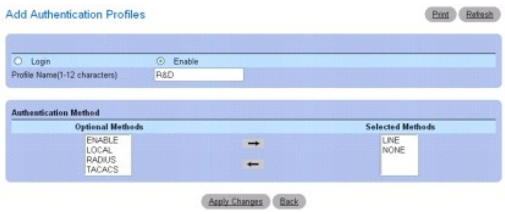
Selected Methods (Ausgewählte Methoden) – Die vereinbarte Authentifizierungsmethode.

Remove (Entfernen) – Entfernt das ausgewählte Profil.

Hinzufügen eines Authentifizierungsprofils

1. Öffnen Sie die Seite **Authentication Profiles** (Authentifizierungsprofile).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add Authentication Profile** (Authentifizierungsprofil hinzufügen) anzuzeigen.

Abbildung 6-41. Authentifizierungsprofil hinzufügen



3. Geben Sie im Feld **Profile Name** (Profilnamen) einen 1 bis 12 Zeichen langen Namen für das Profil ein.

   ANMERKUNG: Der Profilname darf keine Leerstellen enthalten.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Ein Profil wird angelegt. Sie können ein Authentifizierungsprofil über die Webseite **System**→ **Management Security (Verwalten der Gerätesicherheit)**→ **Select Authentication** (Authentifizierung wählen) aktivieren.

Ändern von Authentisierungsprofilen

1. Öffnen Sie die Seite **Authentication Profiles** (Authentifizierungsprofile).
2. Wählen Sie im Feld **Authentication Profile Name** (Authentifizierungsprofilname) ein Element aus.
3. Wählen Sie unter **Optional Methods** (Optionale Methoden) mit Hilfe der Pfeiltasten eine oder mehrere optionale Methoden.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

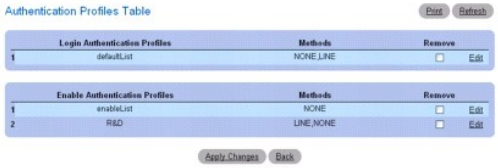
   Das Benutzerauthentifizierungsprofil für das Gerät wird aktualisiert.

Entfernen eines Authentifizierungsprofil-Eintrags

1. Öffnen Sie die Seite **Authentication Profiles** (Authentifizierungsprofile).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Tabelle **Authentication Profiles** (Authentifizierungsprofile) wird geöffnet.

Abbildung 6-42. Tabelle der Authentifizierungsprofile



3. Markieren Sie das Kontrollkästchen **Remove** (Entfernen) neben dem zu löschenden Profil.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der entsprechende Eintrag wird entfernt.

Konfigurieren eines Authentifizierungsprofils mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

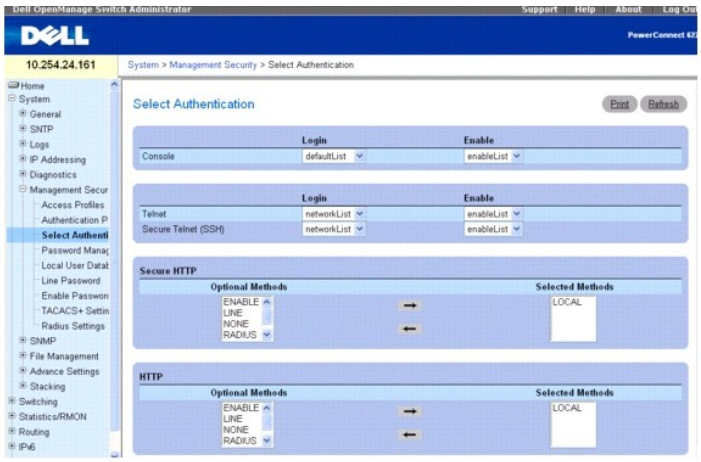
- AAA Commands (AAA-Befehle)

Authentifizierung auswählen

Nach Definition der Authentisierungsprofile können Sie diese Profile auf Verwaltungszugriffsmethoden anwenden. Auf diese Weise lassen sich beispielsweise Konsolenbenutzer durch Authentisierungsprofil-Liste 1 authentisieren, während Telnet-Benutzer durch Authentisierungsprofil-Liste 2 authentisiert werden.

Klicken Sie zum Anzeigen der Seite **Select Authentication** (Authentifizierung auswählen) in der Strukturansicht auf **System→ Management Security (Verwalten der Gerätesicherheit)→ Select Authentication (Authentifizierung auswählen)**.

Abbildung 6-43. Authentifizierung auswählen



Die Seite Select Authentication (Authentifizierung auswählen) enthält folgende Felder:

Console (Konsole) – Authentifizierungsprofile für die Authentifizierung von Konsolenbenutzern.

Telnet – Authentifizierungsprofile für die Authentifizierung von Telnet-Benutzern.

Secure Telnet (SSH) – Authentifizierungsprofile für die Authentifizierung von SSH-Benutzern (Secure Shell). Über SSH können sichere und verschlüsselte Remote-Verbindungen zwischen Clients und einem Gerät hergestellt werden.

Secure HTTP und HTTP – Authentifizierungsmethode für Secure HTTP- bzw. HTTP-Zugriffe. Mögliche Werte für dieses Feld sind:

None (Keine) – Für den Zugriff wird keine Authentifizierungsmethode verwendet.

Local (Lokal) – Die Authentifizierung erfolgt lokal.

RADIUS – Die Authentifizierung erfolgt auf dem RADIUS-Server.

TACACS+ – Die Authentifizierung erfolgt auf dem TACACS+-Server.

Local, None (Lokal, Keine) – Die Authentifizierung erfolgt zunächst lokal.

RADIUS, None (RADIUS, Keine) – Die Authentifizierung erfolgt zunächst auf dem RADIUS-Server. Falls die Authentifizierung nicht überprüft werden kann, wird keine Authentifizierungsmethode verwendet. Die Authentifizierung kann nicht überprüft werden, wenn sich der Remote-Server nicht kontaktieren lässt, um die Benutzerüberprüfung vorzunehmen. Ist jedoch ein Kontakt zum Remote-Server möglich, wird die Antwort des Remote-Servers grundsätzlich akzeptiert.

TACACS+, None (TACACS+, Keine) – Die Authentifizierung erfolgt zunächst auf dem TACACS+-Server. Falls die Authentifizierung nicht überprüft werden kann, wird keine Authentifizierungsmethode verwendet. Die Authentifizierung kann nicht überprüft werden, wenn sich der Remote-Server nicht kontaktieren lässt, um die Benutzerüberprüfung vorzunehmen. Ist jedoch ein Kontakt zum Remote-Server möglich, wird die Antwort des Remote-Servers grundsätzlich akzeptiert.

Local, RADIUS (Lokal, RADIUS) – Die Authentifizierung erfolgt zunächst lokal. Falls die Authentifizierung nicht lokal überprüft werden kann, authentisiert der RADIUS-Server die Verwaltungsmethode. Wenn die Verwaltungsmethode nicht vom RADIUS-Server authentisiert werden kann, wird die Sitzung gesperrt.

Local, TACACS+ (Lokal, TACACS+) – Die Authentifizierung erfolgt zunächst lokal. Falls die Authentifizierung nicht lokal überprüft werden kann, authentisiert der TACACS+-Server die Verwaltungsmethode. Wenn die Verwaltungsmethode nicht vom TACACS+-Server authentisiert werden kann, wird die Sitzung gesperrt.

RADIUS, Local (RADIUS, Lokal) – Die Authentifizierung erfolgt zunächst auf dem RADIUS-Server. Falls die Authentifizierung nicht auf dem RADIUS-Server überprüft werden kann, wird die Sitzung lokal authentisiert. Wenn die Sitzung nicht lokal authentisiert werden kann, wird die Sitzung gesperrt.

TACACS+, Local (TACACS+, Lokal) – Die Authentifizierung erfolgt zunächst auf dem TACACS+-Server. Falls die Authentifizierung nicht auf dem TACACS+-Server überprüft werden kann, wird die Sitzung lokal authentisiert. Wenn die Sitzung nicht lokal authentisiert werden kann, wird die Sitzung gesperrt.

Local, RADIUS, None (Lokal, RADIUS, Keine) – Die Authentifizierung erfolgt zunächst lokal. Falls die Authentifizierung nicht lokal überprüft werden kann, authentisiert der RADIUS-Server die Verwaltungsmethode. Wenn die Verwaltungsmethode nicht vom RADIUS-Server authentisiert werden kann, wird die Sitzung zugelassen.

RADIUS, Local, None (RADIUS, Lokal, Keine) – Die Authentifizierung erfolgt zunächst auf dem RADIUS-Server. Falls die Authentifizierung nicht auf dem RADIUS-Server überprüft werden kann, wird die Sitzung lokal authentisiert. Wenn die Sitzung nicht lokal authentisiert werden kann, wird die Sitzung zugelassen.

Local, TACACS+, None (Lokal, TACACS+, Keine) – Die Authentifizierung erfolgt zunächst lokal. Falls die Authentifizierung nicht lokal überprüft werden kann, authentisiert der TACACS+-Server die Verwaltungsmethode. Wenn die Verwaltungsmethode nicht vom TACACS+-Server authentisiert werden kann, wird die Sitzung zugelassen.

TACACS+, Local, None (TACACS+, Lokal, Keine) – Die Authentifizierung erfolgt zunächst auf dem TACACS+-Server. Falls die Authentifizierung nicht auf dem TACACS+-Server überprüft werden kann, wird die Sitzung lokal authentisiert. Wenn die Sitzung nicht lokal authentisiert werden kann, wird die Sitzung zugelassen.

Zuweisen einer Authentifizierungsmethodenliste zu Konsolensitzungen

1. Öffnen Sie die Seite **Select Authentication** (Authentifizierung auswählen).
2. Wählen Sie im Feld **Console** (Konsole) ein Authentifizierungsprofil aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Konsolensitzungen wird eine Authentifizierungsmethodenliste zugewiesen.

Zuweisen eines Authentifizierungsprofils zu Telnet-Sitzungen

1. Öffnen Sie die Seite **Select Authentication** (Authentifizierung auswählen).
2. Wählen Sie im Feld **Telnet** ein Authentifizierungsprofil aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Konsolensitzungen werden Authentifizierungsprotokolle zugewiesen.

Zuweisen eines Authentifizierungsprofils zu Secure Telnet-(SSH-)Sitzungen

1. Öffnen Sie die Seite **Select Authentication** (Authentifizierung auswählen).
2. Wählen Sie im Feld **Secure Telnet (SSH)** ein Authentifizierungsprofil aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Secure Telnet-(SSH-)Sitzungen werden Authentifizierungsprofile zugewiesen.

Zuweisen einer Authentifizierungssequenz zu HTTP-Sitzungen

1. Öffnen Sie die Seite **Select Authentication** (Authentifizierung auswählen).
2. Wählen Sie unter **HTTP** im Feld **Optional Methods** (Optionale Methoden) eine Authentifizierungsmethode aus und klicken Sie auf die Schaltfläche mit dem nach rechts weisenden Pfeil.

   Die vereinbarte Authentifizierungsmethode wird in das Feld **Selected Methods** (Ausgewählte Methoden) übernommen.
3. Wiederholen Sie diesen Schritt so lange, bis die gewünschte Authentifizierungsreihenfolge im Feld **Selected Methods** (Ausgewählte Methoden) angezeigt wird.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   HTTP-Sitzungen wird die Authentifizierungssequenz zugewiesen.

Zuweisen von Zugriffsmethoden, Authentifizierungsprofilen oder Sequenzen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- AAA Commands (AAA-Befehle)

Zuweisen einer Authentifizierungssequenz zu Secure HTTP-Sitzungen

1. Öffnen Sie die Seite **Select Authentication** (Authentifizierung auswählen).
2. Wählen Sie unter **Secure HTTP** im Feld **Optional Methods** (Optionale Methoden) eine Authentifizierungsmethode aus und klicken Sie auf die Schaltfläche mit dem nach rechts weisenden Pfeil.

   Die vereinbarte Authentifizierungsmethode wird in das Feld **Selected Methods** (Ausgewählte Methoden) übernommen.
3. Wiederholen Sie diesen Schritt so lange, bis die gewünschte Authentifizierungsreihenfolge im Feld **Selected Methods** (Ausgewählte Methoden) angezeigt wird.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Secure HTTP-Sitzungen wird die Authentifizierungssequenz zugewiesen.

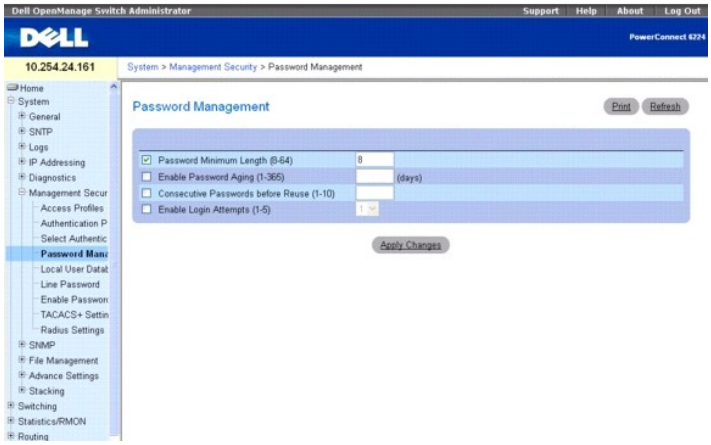
Kennwortverwaltung

Die Kennwortverwaltung sorgt für mehr Netzwerksicherheit sowie eine verbesserte Kennwortkontrolle. Kennwörter für den SSH-, Telnet-, HTTP-, HTTPS- und SNMP-Zugriff verfügen unter anderem über folgende Sicherheitsfunktionen:

- Definieren einer Mindestlänge für Kennwörter
- Festlegung einer Frist für den Ablauf von Kennwörtern
- Verhindern einer häufigen Wiederverwendung derselben Kennwörter
- Sperrung von Benutzern nach fehlgeschlagenen Anmeldeversuchen

Klicken Sie zum Anzeigen der Seite **Password Management** (Kennwortverwaltung) in der Strukturansicht auf **System→ Management Security (Verwalten der Gerätesicherheit)→ Password Management (Kennwortverwaltung)**.

Abbildung 6-44. Kennwortverwaltung



Die Seite Password Management (Kennwortverwaltung) enthält folgende Felder:

Password Minimum Length (8–64) (Kennwort-Mindestlänge, 8-64) – Gibt die Mindestlänge des Kennworts an, wenn das betreffende Kontrollkästchen aktiviert ist. Beispielsweise kann der Administrator festlegen, dass alle Verbindungskennwörter eine Mindestlänge von 10 Zeichen aufweisen müssen.

Enable Password Aging (1–365) (Kennwortalterung aktivieren, 1-365) – Bei Auswahl dieser Option wird angegeben, nach wie vielen Tagen ein Kennwort abläuft. Der Feldwert kann im Bereich 1 bis 365 (Tage) liegen. Die Kennwortalterung funktioniert nur, wenn die Switch-Uhr mit einem SNTP-Server synchronisiert wird. Weitere Informationen finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) unter "Clock Commands" (Zeit-Befehle).

Consecutive Passwords Before Reuse (1–10) (Anzahl anderer Kennwörter vor Wiederverwendung, 1–10) – Gibt an, wie oft ein anderes Kennwort verwendet werden muss, bevor das betreffende Kennwort wiederverwendet werden kann. Die möglichen Feldwerte liegen im Bereich 1 bis 10.

ANMERKUNG: Der Benutzer wird vor Ablauf des Kennworts informiert und aufgefordert, das Kennwort zu ändern. Webbenutzer erhalten diese Benachrichtigung nicht.

Enable Login Attempts (1–5) (Zulässige Anmeldeversuche, 1–5) – Bei Auswahl dieser Option wird dem Benutzer der Gerätezugriff verwehrt, sobald die Anzahl fehlerhafter Kennworteingaben den vereinbarten Wert übersteigt. Beispiel: Wurde für die Anzahl der Anmeldeversuche der Wert 5 vereinbart, kann ein Benutzer fünf Mal versuchen, sich mit einem falschen Kennwort anzumelden. Beim sechsten Mal wird der Benutzer geräteseitig gesperrt. In diesem Fall muss das Benutzerkonto durch einen so genannten "Superuser" reaktiviert werden. Der Wertebereich des Felds reicht von 1 bis 5 (Versuche).

Definieren von Kennworteinschränkungen

1. Öffnen Sie die Seite **Password Management** (Kennwortverwaltung).
2. Definieren Sie die relevanten Felder.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Kennworteinschränkungen werden definiert, und das Gerät wird aktualisiert.

Definieren von Kennworteinschränkungen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

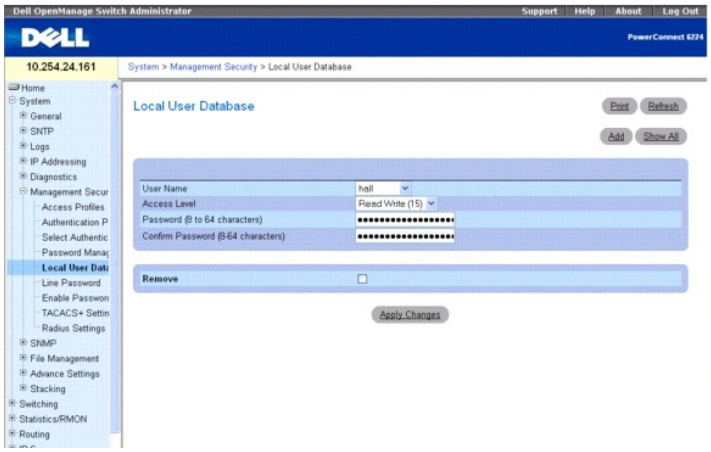
- Password Management Commands (Befehle für die Kennwortverwaltung)

Lokale Benutzerdatenbank

Auf der Seite **Local User Database** (Lokale Benutzerdatenbank) können Sie Kennwörter und Zugangsrechte für Benutzer definieren sowie Benutzer reaktivieren, deren Benutzerkonten vorübergehend deaktiviert wurden.

Klicken Sie zum Anzeigen der Seite **Local User Database** (Lokale Benutzerdatenbank) in der Strukturansicht auf **System→ Management Security (Verwalten der Gerätesicherheit)→ Local User Database (Lokale Benutzerdatenbank)**.

Abbildung 6-45. Lokale Benutzerdatenbank



Die Seite Local User Database (Lokale Benutzerdatenbank) enthält folgende Felder:

User Name (Benutzername) – Die Liste der Benutzer.

Access Level (Zugangsebene) – Die Benutzerzugangsebene. Die niedrigste Benutzerzugangsebene ist **1 (readonly - nur Lesen)** , die höchste **15** (readwrite - Lesen/Schreiben). Bei Bedarf können Sie einen Benutzerzugang vorübergehend sperren, indem Sie hierfür die Zugangsebene 0 vereinbaren (nur Benutzer mit der Zugangsebene 15 haben diese Möglichkeit).

Password (8–64 Characters) (Kennwort, 8-64 Zeichen) – Benutzerdefiniertes Kennwort.

Confirm Password (Kennwort bestätigen) — Bestätigt das benutzerdefinierte Kennwort.

Remove (Entfernen) – Bei Auswahl dieser Option werden Benutzer aus der lokalen Benutzerdatenbank entfernt.

Zuweisen von Zugriffsrechten zu einem Benutzer

1. Öffnen Sie die Seite **Local User Database** (Lokale Benutzerdatenbank).
2. Wählen Sie im Feld **User Name** (Benutzername) einen Benutzer aus.
3. Nehmen Sie die erforderlichen Einstellungen vor.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

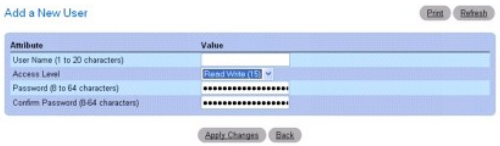
   Die Zugriffsrechte und Kennwörter des Benutzers werden definiert und das Gerät aktualisiert.

Benutzer der lokalen Benutzerdatenbank hinzufügen

1. Öffnen Sie die Seite **Local User Database** (Lokale Benutzerdatenbank).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add User** (Benutzer hinzufügen) anzuzeigen.

   Die Seite **Add a New User** (Einen neuen Benutzer hinzufügen) wird angezeigt.

Abbildung 6-46. Einen neuen Benutzer hinzufügen



3. Füllen Sie die Felder aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der neue Benutzer wird definiert und das Gerät aktualisiert.

ANMERKUNG: Sie können hier bis zu acht lokale Benutzer für das Gerät definieren.

Anzeigen der Benutzer in der lokalen Benutzerdatenbank

1. Öffnen Sie die Seite **Local User Database** (Lokale Benutzerdatenbank).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **Local User Table** (Lokale Benutzertabelle) anzuzeigen.

   Alle Mitglieder der lokalen Benutzerdatenbank werden angezeigt.

Abbildung 6-47. Lokale Benutzertabelle

Entfernen von Benutzern aus der lokalen Benutzerdatenbank

1. Öffnen Sie die Seite **Local User Database** (Lokale Benutzerdatenbank).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **Local User Table (Lokale Benutzertabelle) anzuzeigen**.
3. Wählen Sie unter **User Name** (Benutzername) einen Eintrag aus.
4. Markieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Benutzer wird entfernt und das Gerät aktualisiert.

Zuweisen von Benutzern mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

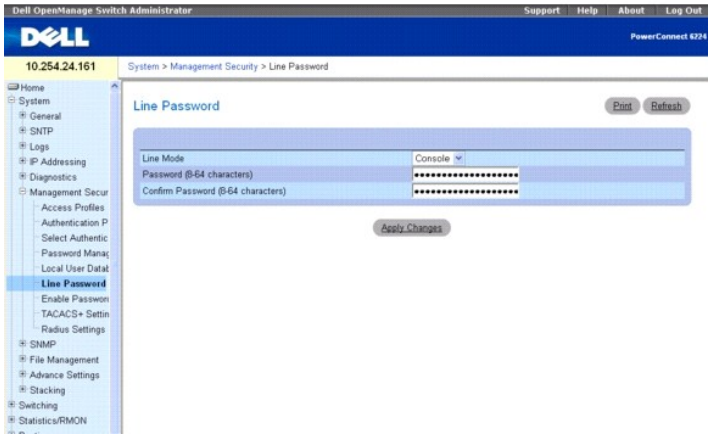
- AAA Commands (AAA-Befehle)

Verbindungskennwörter

Auf der Seite **Line Password** (Verbindungskennwort) können Sie Verbindungskennwörter für Verwaltungsmethoden definieren.

Klicken Sie zum Anzeigen der Seite **Line Password** (Verbindungskennwort) in der Strukturansicht auf **System→ Management Security (Verwalten der Gerätesicherheit)→ Line Password (Verbindungskennwort)**.

Abbildung 6-48. Verbindungskennwort



Die Seite Line Password (Verbindungskennwort) enthält folgende Felder:

Line Mode (Verbindungsmodus) – Dropdown-Menü, in dem der Zugriff auf das Gerät über eine Konsolen-, Telnet- oder Secure Telnet (SSH)-Sitzung festgelegt wird.

Line Password (8–64 characters) (Verbindungskennwort, 8-64 Zeichen) – Das Verbindungskennwort für den Gerätezugriff über eine Konsolen-, Telnet- oder Secure Telnet-Sitzung. Anstelle des Kennworts werden Sternchen (*****) angezeigt.

Confirm Password (8 – 64 characters) (Kennwort bestätigen, 8–64 Zeichen) — Bestätigt das neue Verbindungskennwort. Anstelle des Kennworts werden Sternchen (*****) angezeigt.

Definieren von Verbindungskennwörtern

1. Öffnen Sie die Seite **Line Password** (Verbindungskennwort).
2. Wählen Sie den Zugriff auf das Gerät über eine Konsolen-, Telnet- oder Secure Telnet (SSH)-Sitzung.
3. Definieren Sie das Feld **Line Password** (Verbindungskennwort) für den Sitzungstyp, den Sie für die Anbindung an das Gerät verwenden.
4. Bestätigen Sie das **Line Password** (Verbindungskennwort).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Das Verbindungskennwort für den jeweiligen Sitzungstyp wird definiert und das Gerät aktualisiert.

Zuweisen von Verbindungskennwörtern mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

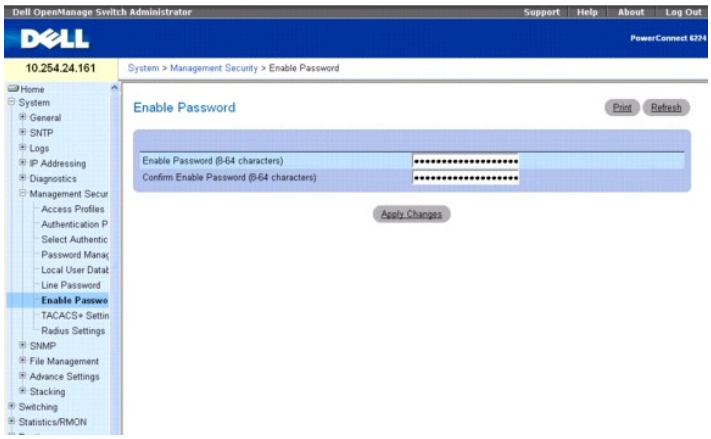
- AAA Commands (AAA-Befehle)

Aktivierungskennwort

Auf der Seite **Enable Password** (Aktivierungskennwort) können Sie eine lokales Kennwort für den Zugang zu normalen und höheren Berechtigungsebene einrichten.

Klicken Sie zum Anzeigen der Seite **Enable Password** (Aktivierungskennwort) in der Strukturansicht auf **System→ Management Security (Verwalten der Gerätesicherheit)→ Enable Password (Aktivierungskennwort)**.

Abbildung 6-49. Aktivierungskennwort



Die Seite Enable Password (Aktivierungskennwort) enthält folgende Felder:

Enable Password (8–64 characters) (Aktivierungskennwort, 8-64 Zeichen) – Das Aktivierungskennwort für die Steuerung des Zugriffs auf normale und privilegierte Zugangsebenen. Anstelle des Kennworts werden Sternchen (*****) angezeigt.

Confirm Enable Password (Aktivierungskennwort bestätigen) – Bestätigt das neue Aktivierungskennwort. Anstelle des Kennworts werden Sternchen (*****) angezeigt.

Definieren von Aktivierungskennwörtern

1. Öffnen Sie die Seite **Enable Password** (Aktivierungskennwort).
2. Vereinbaren Sie ein Aktivierungskennwort.
3. Bestätigen Sie das Aktivierungskennwort.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Das Aktivierungskennwort wird eingerichtet.

Zuweisen von Aktivierungskennwörtern mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- AAA Commands (AAA-Befehle)

TACACS+-Einstellungen

Das Gerät verfügt über Client-Unterstützung für das Terminal Access Controller Access Control System (TACACS+). TACACS+ bietet eine zentrale Sicherheitsfunktionalität für die Validierung von Benutzer(zugriffe)n.

TACACS+ stellt ein zentrales Benutzerverwaltungssystem bereit, das jedoch die Konsistenz zu RADIUS und anderen Authentifizierungsprozessen wahrt. TACACS+ stellt die folgenden Dienste bereit:

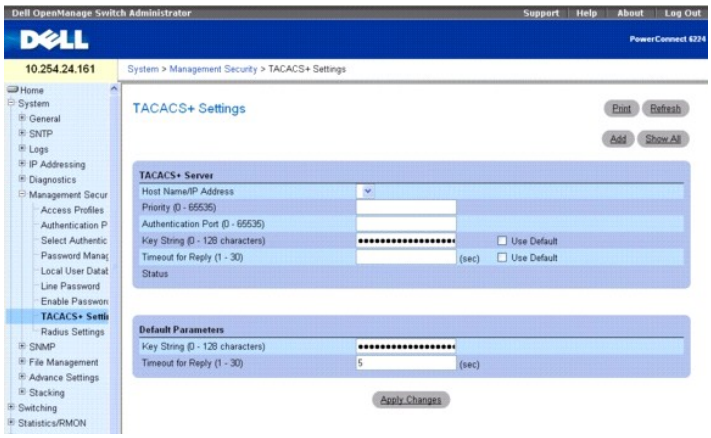
- **Authentication** (Authentifizierung) – Bewirkt die Authentifizierung von Benutzern während der Anmeldung anhand von Benutzernamen und benutzerdefinierten Kennwörtern.
- **Authorization** (Autorisierung) – Erfolgt bei Anmeldung. Nach Beendigung der Authentifizierungssitzung wird eine Autorisierungssitzung unter Verwendung des authentifizierten Benutzernamens gestartet. Der TACACS+-Server prüft die Benutzerrechte.

Das TACACS+-Protokoll gewährleistet die Netzwerksicherheit durch verschlüsselte Protokollaustausche zwischen dem Gerät und dem TACACS+-Server.

Die Seite **TACACS+ Settings** (TACACS+-Einstellungen) enthält benutzerdefinierte und standardmäßige TACACS+-Einstellungen für den Inband-Verwaltungsport.

Klicken Sie zum Anzeigen der Seite **TACACS+ Settings** (TACACS+-Einstellungen) in der Strukturansicht auf **System→ Management Security (Verwalten der Gerätesicherheit)→ TACACS+**.

Abbildung 6-50. TACACS+-Einstellungen



Die Seite **TACACS+ Settings** (TACACS+-Einstellungen) enthält folgende Felder:

Host Name / IP Address (Host-Name / IP-Adresse) – Legt den TACACS+-Server fest.

Priority (0–65535) (Priorität, 0-65636) – Gibt die Reihenfolge an, in der die TACACS+-Server verwendet werden. Der Standardwert ist 0.

Authentication Port (0–65535) (Authentifizierungs-Port, 0-65535) – Die Nummer des Ports, über den die TACACS+-Sitzung eingerichtet wird. Der Standardwert ist Port 49.

Key String (0–128 Characters) (Schlüsselzeichenkette, 0-128 Zeichen) – Definiert den Schlüssel für die Authentifizierung und Verschlüsselung der TACACS+-Kommunikation zwischen dem Gerät und dem TACACS+-Server. Dieser muss mit der auf dem TACACS+-Server verwendeten Verschlüsselung übereinstimmen. Aktivieren Sie das Kontrollkästchen **Use Default** (Standardeinstellung verwenden), um den Standardwert zu verwenden.

Timeout for Reply (1–30) (Zeitlimit für Antwort (1-30)) – Der Zeitraum bis zum Ablauf des Zeitlimits für die Verbindung zwischen dem Gerät und dem TACACS+-Server. Der Wertebereich des Felds reicht von 1 bis 30 (Sekunden). Aktivieren Sie das Kontrollkästchen **Use Default** (Standardeinstellung verwenden), um den werkseitigen Standardwert auszuwählen.

Status – Der Status der Verbindung zwischen dem Gerät und dem TACACS+-Server. Die für dieses Feld möglichen Werte sind:

Connected (Verbunden) – Zwischen dem Gerät und dem TACACS+-Server ist derzeit eine Verbindung hergestellt.

Not Connected (Nicht verbunden) – Zwischen dem Gerät und dem TACACS+-Server ist derzeit keine Verbindung hergestellt.

Die Felder im Abschnitt Default Parameters (Standardparameter) dieser Seite enthalten Werte, die automatisch auf alle neuen TACACS+-Server angewendet werden.

Key String (0–128 Characters) (Schlüsselzeichenkette, 0-128 Zeichen) – Geben Sie den Standardschlüssel für die Authentifizierung und Verschlüsselung der TACACS+-Kommunikation zwischen dem Gerät und dem TACACS+-Server ein.

Timeout for Reply (1–30) (Zeitlimit für Antwort, 1-30) – Geben Sie hier den Zeitraum gemäß der globalen Benutzerkonfiguration bis zum Ablauf des Zeitlimits für die Verbindung zwischen dem Gerät und dem TACACS+-Server ein.

Definieren von TACACS+-Parametern

1. Öffnen Sie die Seite **TACACS+ Settings** (TACACS+-Einstellungen).
2. Nehmen Sie die erforderlichen Einstellungen vor.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

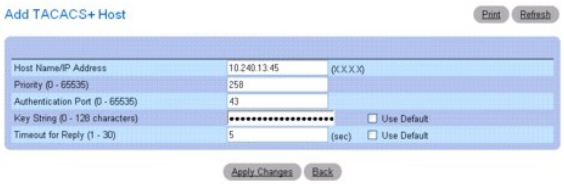
   Die TACACS+-Einstellungen für das Gerät werden aktualisiert.

Hinzufügen eines TACACS+-Servers

1. Öffnen Sie die Seite **TACACS+ Settings** (TACACS+-Einstellungen).
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite Add TACACS+ Host (TACACS+-Host hinzufügen) wird angezeigt.

Abbildung 6-51. TACACS+-Host hinzufügen



3. Nehmen Sie die erforderlichen Einstellungen vor.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der TACACS+-Server wird hinzugefügt und das Gerät aktualisiert.

Anzeigen einer TACACS+-Server-Liste

1. Öffnen Sie die Seite **TACACS+ Settings** (TACACS+-Einstellungen).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **TACACS+ Servers Table (Tabelle der TACACS+-Server) wird angezeigt**.

Abbildung 6-52. Tabelle der TACACS+-Server

Entfernen eines TACACS+-Servers aus der TACACS+- Server-Liste

1. Öffnen Sie die Seite **TACACS+ Settings** (TACACS+-Einstellungen).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **TACACS+ Servers Table (Tabelle der TACACS+-Server) wird angezeigt**.
3. Wählen Sie einen Eintrag aus der **TACACS+-Servertabelle** aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der TACACS+-Server wird entfernt und das Gerät aktualisiert.

Definieren von TACACS+-Parametern mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- TACACS+ Commands (TACACS+-Befehle)

RADIUS-Einstellungen

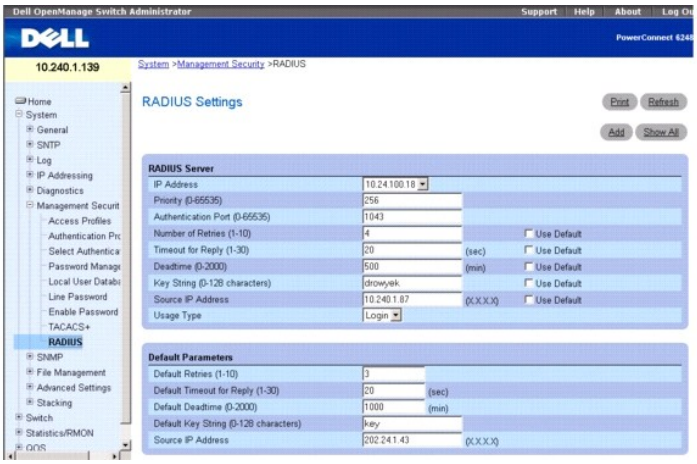
Remote Authorization Dial-In User Service-(RADIUS-)Server bieten zusätzliche Netzwerksicherheit. Der RADIUS-Server pflegt eine Benutzerdatenbank mit benutzerbezogenen Authentifizierungsinformationen. RADIUS-Server stellen eine zentralisierte Authentifizierungsmethode für folgende Zugriffsarten bereit:

- Telnet-Zugriff
- Webzugriff
- Konsolenzugriff auf Switches
- Access Control Port (802.1x)

Die Seite ***RADIUS Settings*** (RADIUS-Einstellungen) enthält benutzerdefinierte und standardmäßige RADIUS-Einstellungen.

Klicken Sie zum Anzeigen der Seite ***RADIUS Settings*** (RADIUS-Einstellungen) in der Strukturansicht auf **System Management (Systemverwaltung)→ Security (Sicherheit)→ RADIUS Settings (RADIUS-Einstellungen)**.

Abbildung 6-53. RADIUS-Einstellungen



Die Seite *RADIUS Settings* *(RADIUS-Einstellungen) enthält folgende Felder:*

IP Address (IP-Adresse) – IP-Adresse des RADIUS-Servers.

Priority (0–65535) (Priorität, 0-65535) – Gibt die Port-Priorität an. Die möglichen Feldwerte liegen im Bereich 0 bis 65535.

Authentication Port (0–65535) (Authentifizierungsport, 0-65535) – Identifiziert den Authentifizierungsport, der für die Überprüfung der RADIUS-Server-Authentifizierung verwendet wird.

Number of Retries (1–10) (Anzahl der Wiederholungsversuche, 1-10) – Die Anzahl der Anforderungen an, die an den RADIUS-Server übermittelt werden, bevor ein Fehler auftritt. Die möglichen Feldwerte liegen im Bereich 1 bis 10. Der Standardwert ist 3. Wird hier kein host-spezifischer Wert angegeben, kommt der Globalwert für jeden Host zur Anwendung. Aktivieren Sie das Kontrollkästchen **Use Default** (Standardeinstellung verwenden), um den benutzerdefinierten Standardwert zu verwenden.

Timeout for Reply (1–30) (Zeitlimit für Antwort, 1-30) – Gibt das Zeitintervall (in Sekunden) an, das ein Gerät auf eine Antwort vom RADIUS-Server wartet, bevor eine Zeitüberschreitung auftritt. Die möglichen Feldwerte liegen im Bereich 1 bis 30. Der Standardwert ist 3. Wird hier kein host-spezifischer Wert angegeben, kommt der Globalwert für jeden Host zur Anwendung. Aktivieren Sie das Kontrollkästchen **Use Default** (Standardeinstellung verwenden), um den benutzerdefinierten Standardwert zu verwenden.

Deadtime (0–2000) (Totzeit, 0-2000) – Gibt das Zeitintervall (in Sekunden) an, für das ein RADIUS-Server bei Dienstanforderungen umgangen wird. Der Wertebereich reicht von 0 bis 2000. Wird hier kein host-spezifischer Wert angegeben, kommt der Globalwert für jeden Host zur Anwendung. Aktivieren Sie das Kontrollkästchen **Use Default** (Standardeinstellung verwenden), um den benutzerdefinierten Standardwert zu verwenden.

Key String (0–128 Characters) (Schlüsselzeichenkette, 0-128 Zeichen) – Die Schlüsselzeichenkette, die für die Authentifizierung und Verschlüsselung der gesamten RADIUS-Kommunikation zwischen dem Gerät und dem RADIUS-Server verwendet wird. Dieser Schlüssel muss mit der RADIUS-Verschlüsselung übereinstimmen. Wird hier kein host-spezifischer Wert angegeben, kommt der Globalwert für jeden Host zur Anwendung. Aktivieren Sie das Kontrollkästchen **Use Default** (Standardeinstellung verwenden), um den benutzerdefinierten Standardwert zu verwenden.

Source IP Address (Quell-IP-Adresse) – Die IP-Adresse eines Geräts, das auf den RADIUS-Server zugreift. Aktivieren Sie das Kontrollkästchen **Use Default** (Standardeinstellung verwenden), um den benutzerdefinierten Standardwert zu verwenden.

Usage Type (Nutzungstyp) – Dropdown-Liste für die Auswahl des RADIUS-Nutzungstyps.

ANMERKUNG: Die Standardwerte auf dieser Seite sind benutzerdefiniert.

Default Retries (1–10) (Standardanzahl der Wiederholungsversuche, 1-10) – Die Standardanzahl der Anforderungen, die an den RADIUS-Server übermittelt werden können, bevor ein Fehler auftritt.

Timeout for Reply (1–30) (Zeitlimit für Antwort, 1-30) – Gibt das Zeitintervall (in Sekunden) an, das ein Gerät auf eine Antwort vom RADIUS-Server wartet, bevor eine Zeitüberschreitung auftritt. Die möglichen Feldwerte liegen im Bereich 1 bis 30.

Default Deadtime (0–2000) (Standard-Totzeit, 0-2000) – Gibt das Standardzeitintervall (in Sekunden) an, für das ein RADIUS-Server bei Dienstanforderungen umgangen wird. Der Wertebereich reicht von 0 bis 2000.

Default Key String (0–128 Characters) (Standardschlüsselzeichenkette, 0-128 Zeichen) – Die Standardschlüsselzeichenkette, die für die Authentifizierung und Verschlüsselung der gesamten RADIUS-Kommunikation zwischen dem Gerät und dem RADIUS-Server verwendet wird. Dieser Schlüssel muss mit der RADIUS-Verschlüsselung übereinstimmen.

Source IP Address (Quell-IP-Adresse) – Die IP-Standardadresse eines Geräts, das auf den RADIUS-Server zugreift.

Hinzufügen eines RADIUS-Servers

1. Öffnen Sie die Seite ***RADIUS Settings*** (RADIUS-Einstellungen).

2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add RADIUS Server** (RADIUS-Server hinzufügen) wird angezeigt.

Abbildung 6-54. RADIUS-Server hinzufügen

3. Nehmen Sie im Dialogfeld die erforderlichen Einstellungen vor.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der neue RADIUS-Server wird hinzugefügt und das Gerät aktualisiert.

Definieren von RADIUS-Parametern

1. Öffnen Sie die Seite ***RADIUS Settings*** (RADIUS-Einstellungen).

2. Nehmen Sie im Dialogfeld die erforderlichen Einstellungen vor.

3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die RADIUS-Einstellungen für das Gerät werden aktualisiert.

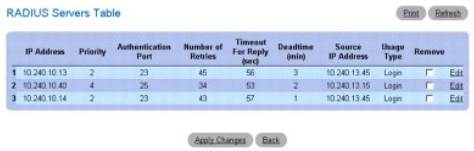
Ändern der RADIUS-Server-Einstellungen

1. Öffnen Sie die Seite ***RADIUS Settings*** (RADIUS-Einstellungen).

2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **RADIUS Servers Table** (Tabelle der RADIUS-Server) wird angezeigt.

Abbildung 6-55. Tabelle der RADIUS-Server



3. Klicken Sie auf den Link **Edit** (Bearbeiten) für den ausgewählten Eintrag.

4. Ändern Sie auf der Seite **RADIUS Settings** (RADIUS-Einstellungen) die Einstellungen für den RADIUS-Server.

5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die RADIUS-Server-Einstellungen werden geändert, und das Gerät wird aktualisiert.

Entfernen eines RADIUS-Servers aus der RADIUS-Server- Liste:

1. Öffnen Sie die Seite ***RADIUS Settings*** (RADIUS-Einstellungen).

2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **RADIUS Servers Table** (Tabelle der RADIUS-Server) wird angezeigt.

3. Wählen Sie einen RADIUS-Server aus und aktivieren Sie die Option **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der RADIUS-Server wird aus der Liste entfernt.

Definieren von RADIUS-Servern mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

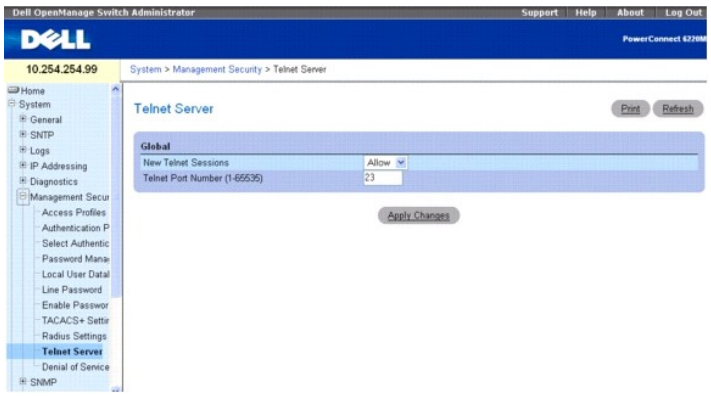
- Radius Commands (RADIUS-Befehle)

Telnet-Server

Verwenden Sie die Seite **Telnet Server** (Telnet-Server), um den Telnet-Service am Switch zu aktivieren und deaktivieren oder den Telnet-Port zu modifizieren.

Um die Seite **Telnet Server** (Telnet-Server) anzuzeigen, klicken Sie auf **System**→ **Management Security (Verwalten der Gerätesicherheit)**→ **Telnet Server** (Telnet-Server).

Abbildung 6-56. Telnet-Server



Die Seite Telnet Server enthält folgende Felder:

New Telnet Sessions (Neue Telnet-Sitzungen) – Dient zum Festlegen des Administrationsmodus für eingehende Telnet-Sitzungen. Wenn Sie den Modus "Block" (Blockieren) auswählen, werden keine neuen Telnet-Sitzungen zugelassen. Bestehende Sitzungen werden jedoch nicht unterbrochen. Der Standardwert ist Allow (Zulassen).

Telnet Port Number (Telnet-Portnummer) – Die Portnummer, an der die Telnet-Sitzung initiiert werden kann. Dieser Port wird für neue eingehende Telnet-Sitzungen am Switch verwendet. Nachdem Sie den Telnet-Serverport geändert haben, verwenden neu eingehende Telnet-Sitzungen den neuen Port. Bestehende Telnet-Sitzungen sind von der Änderung nicht betroffen.

Einstellungen für Telnet-Server ändern

1. Öffnen Sie die Seite **Telnet Server Configuration** (Konfiguration für Telnet-Server).
2. Konfigurieren Sie die relevanten Felder.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Einstellungen werden gespeichert, und das Gerät wird aktualisiert.

Konfigurieren des Telnet-Servers mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

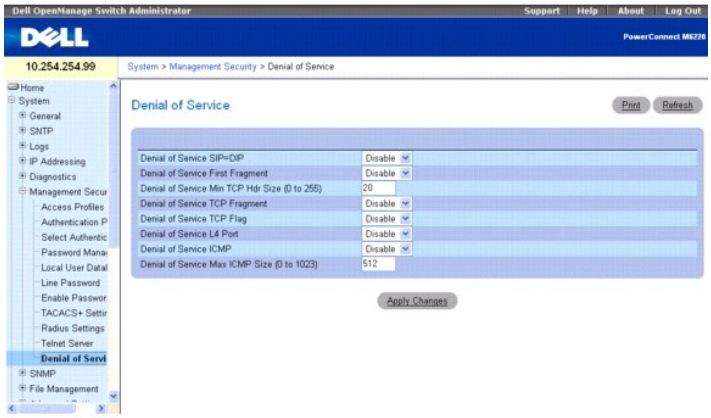
- Telnet-Server Commands (Telnet-Server-Befehle)

DoS (Denial of Service)

Der Ausdruck DoS (Denial of Service) bezieht sich auf die Ausnutzung verschiedener Schwachstellen mit dem Ziel, einen Hostdienst zu unterbrechen oder die Stabilität eines Netzwerks zu beeinträchtigen. Verwenden Sie die Seite **Denial of Service**, um Einstellungen zu konfigurieren, die dazu beitragen, DoS-Attacken zu verhindern.

Um die Seite **Denial of Service** anzuzeigen, klicken Sie in der Strukturansicht auf **System**→ **Management Security (Verwalten der Gerätesicherheit)**→**Denial of Service**.

Abbildung 6-57. DoS (Denial of Service)



Die Seite **Denial of Service** enthält folgende Felder:

Denial of Service SIP=DIP – Die Aktivierung der DoS-Vorbeugeoption SIP=DIP bewirkt, dass der Switch Pakete verwirft, deren Quell-IP-Adresse identisch mit der Ziel-IP-Adresse ist.

Denial of Service First Fragment – Bei Aktivierung dieser Option verwirft der Switch Pakete, deren TCP-Header kleiner ist als die konfigurierte Mindestgröße für TCP-Header (Min TCP Hdr Size).

Denial of Service Min TCP Hdr Size – Legen Sie hier die zulässige Mindestgröße für TCP-Header fest. Wenn die Option "First Fragment DoS prevention" aktiviert ist, verwirft der Switch Pakete, deren TCP-Header kleiner als die hier voreingestellte Mindestgröße ist.

Denial of Service TCP Fragment – Bei Aktivierung dieser Option verwirft der Switch Pakete, deren IP-Fragmentversatz gleich eins ist.

Denial of Service TCP Flag – Bei Aktivierung dieser Option verwirft der Switch Pakete, auf die eine der folgenden Bedingungen zutrifft:

- TCP-Flag SYN ist gesetzt, und der TCP-Quellport ist unter 1024
- TCP-Steuerungsflags und TCP-Sequenznummer sind auf 0 gesetzt
- TCP-Flags FIN, URG und PSH sind gesetzt und TCP-Sequenznummer ist auf 0 gesetzt
- TCP-Flags SYN und FIN sind gesetzt

Denial of Service L4 Port – Bei Aktivierung dieser Option verwirft der Switch Pakete, bei denen der TCP/UDP-Quellport identisch mit dem TCP/UDP-Zielport ist.

Denial of Service ICMP – Bei Aktivierung dieser Option verwirft der Switch ICMP-Pakete, bei denen der Typ auf Echo_REQ (ping) gesetzt ist und die vorkonfigurierte ICMP-Paketgröße (ICMP Pkt Size) überschritten wird.

Denial of Service Max ICMP Pkt Size — Legen Sie hier die maximal zulässige ICMP-Paketgröße fest. Wenn die DoS-Vorbeugemaßnahme ICMP aktiviert ist, verwirft der Switch ICMP-Ping-Pakete, die die hier konfigurierte Größe überschreiten.

Konfigurieren der DoS-Einstellungen

1. Öffnen Sie die Seite **Denial of Service**.
2. Legen Sie die gewünschten Einstellungen fest.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Das Gerät wird auf die neuen Einstellungen aktualisiert.

Konfigurieren der DoS-Einstellungen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Denial of Service Commands (Denial of Service-Befehle).

Definieren von SNMP-Parametern

SNMP (Simple Network Management Protocol) bietet eine Methode zur Verwaltung von Netzwerkgeräten. Das Gerät unterstützt die SNMP-Versionen 1, 2 und 3 (SNMPv1, SNMPv2 und SNMPv3).

ANMERKUNG: Standardmäßig wird geräteseitig automatisch SNMPv2 aktiviert. Um SNMPv3 aktivieren zu können, muss zunächst eine lokale Engine-ID für das Gerät definiert werden. Als lokale Engine-ID wird standardmäßig die MAC-Adresse des Switch eingestellt; wird der Switch jedoch im Stack-Modus betrieben, ist unbedingt eine manuelle Konfiguration der lokalen Engine-ID für den Stack vorzunehmen. Die lokale Engine-ID muss so definiert werden, dass sie im gesamten Netzwerk eindeutig ist. Dies ist besonders wichtig, da als Engine-ID in einem Stack standardmäßig die MAC-Adresse der Mastereinheit verwendet wird; diese Adresse kann sich jedoch ändern, wenn die Mastereinheit ausfällt und eine andere Einheit die Kontrolle über den Stack übernimmt. Weitere Informationen zur Konfiguration der lokalen Engine-ID finden Sie unter "**Globale SNMP-Parameter**".

SNMPv1 und SNMPv2

Der SNMP-Agent verwaltet eine Liste von Variablen, die zur Verwaltung des Geräts verwendet werden. Die Variablen werden in der *Management Information Base* (Management-Informationsbasis, MIB) definiert. Die MIB enthält die vom Agenten gesteuerten Variablen. Der SNMP-Agent definiert das Format für die MIB-Spezifikationen sowie das Format für den Zugriff auf Daten über das Netzwerk. Die Zugriffsrechte auf den SNMP-Agenten werden von Zugriffszeichenketten kontrolliert.

SNMPv3

SNMPv3 wendet ebenfalls Zugriffskontrollverfahren und einen neuen Trap-Mechanismus auf SNMPv1- und SNMPv2-PDUs an. Darüber hinaus ist für SNMPv3 das Benutzersicherheitsmodell (User Security Model, USM) definiert, das folgende Funktionen beinhaltet:

- **Authentication** (Authentifizierung) – Gewährleistet Datenintegrität und authentifiziert den Ursprung von Daten.
- **Privacy** (Datenschutz) – Verhindert die Offenlegung von Nachrichteninhalten. Für die Verschlüsselung wird das Verfahren *Cipher Bock-Chaining* (CBC) verwendet. Für eine SNMP-Nachricht wird entweder nur Authentication (Authentifizierung) oder Authentication (Authentifizierung) und Privacy (Datenschutz) aktiviert. Es ist nicht möglich, für eine Nachricht nur die Funktion Datenschutz zu aktivieren.
- **Timeliness** (Aktualität) – Schützt vor Verzögerungen oder Redundanzen beim Empfang von Nachrichten. Der SNMP-Agent vergleicht die eingehende Nachricht mit dem Zeitstempel der Nachricht.
- **Key Management** (Schlüsselverwaltung) – Legt Einstellungen für die Generierung, Aktualisierung und Verwendung von Schlüsseln fest.

Das Gerät unterstützt SNMP-Benachrichtigungsfilter auf der Grundlage von Objekt-IDs (OID). OIDs werden vom System für die Verwaltung von Gerätefunktionen verwendet. SNMPv3 unterstützt die folgenden Funktionen:

- Sicherheit
- Kontrolle des Zugriffs auf Funktionen
- Traps

Authentifizierungs- und Datenschutzschlüssel werden auf der Seite SNMPv3 User Security Model (USM) (SNMPv3-Benutzersicherheitsmodell) geändert.

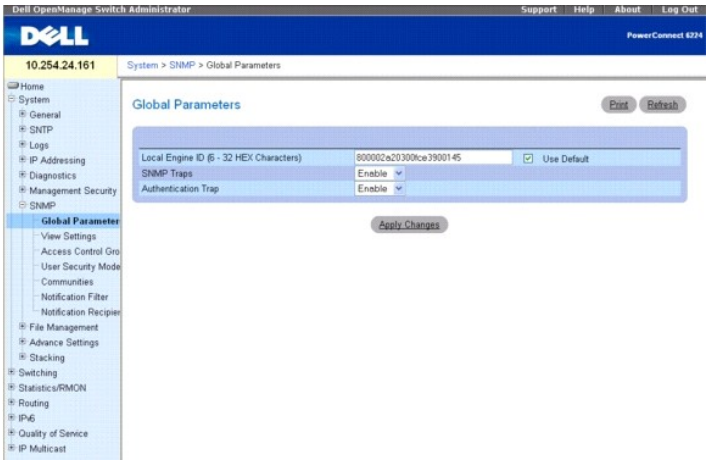
Auf der Seite **SNMP** können Sie SNMP-Parameter definieren. Klicken Sie zum Anzeigen der Seite **SNMP** in der Strukturansicht auf **System** → **SNMP**.

Globale SNMP-Parameter

Auf der Seite **Global Parameters** (Globale Parameter) können Sie SNMP- und Authentifizierungsbenachrichtigungen aktivieren.

Klicken Sie zum Anzeigen der Seite **Global Parameters (Globale Parameter) in der Strukturansicht auf System→ SNMP→ Global Parameters** (Globale Parameter).

Abbildung 6-58. Globale Parameter



Die Seite **Global Parameters (Globale Parameter) enthält folgende Parameter:**

Local Engine ID (6 – 32 hexadecimal characters) (Lokale Engine-ID, 6-32 hexadezimale Zeichen) – Legt die Kennung (ID) der lokalen SNMP-Engine fest.

Use Default (Standardeinstellung verwenden) – Konfiguriert das Gerät für die Verwendung der standardmäßigen SNMP-Engine-ID.

SNMP Traps (SNMP-Traps) – Aktiviert bzw. deaktiviert den geräteseitigen Versand von SNMP-Benachrichtigungen.

Authentication Traps (Authentifizierungs-Traps) – Aktiviert bzw. deaktiviert den geräteseitigen Versand von SNMP-Traps, wenn die Authentifizierung fehlschlägt.

Einstellen der lokalen SNMP-Engine-ID

1. Öffnen Sie die Seite **Global Parameters** (Globale Parameter).
2. Geben Sie im Feld **Local Engine ID** (Lokale Engine-ID) die gewünschte hexadezimale Kennung (ID) ein.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die neue lokale Engine-ID wird hinzugefügt und das Gerät aktualisiert.

Verwenden der lokalen SNMP-Engine-ID

1. Öffnen Sie die Seite **Global Parameters** (Globale Parameter).
2. Markieren Sie das Kontrollkästchen **Use Default** (Standardeinstellung verwenden).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die standardmäßige SNMP-Engine-ID, auf Basis der MAC-Adresse, wird erstellt und das Gerät aktualisiert.

Aktivieren von SNMP-Traps

1. Öffnen Sie die Seite **Global Parameters** (Globale Parameter).
2. Wählen Sie im Feld **SNMP Traps** (SNMP-Traps) die Option **Enable** (Aktivieren) aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Versand von SNMP-Benachrichtigungen wird aktiviert und das Gerät aktualisiert.

Aktivieren von Authentifizierungs-Traps

1. Öffnen Sie die Seite **Global Parameters** (Globale Parameter).
2. Wählen Sie im Feld **Authentication Trap** (Authentifizierungs-Trap) die Option **Enable** (Aktivieren) aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Versand von Authentifizierungs-Benachrichtigungen wird aktiviert und das Gerät aktualisiert.

Aktivieren von SNMP-Benachrichtigungen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- SNMP Commands (SNMP-Befehle)

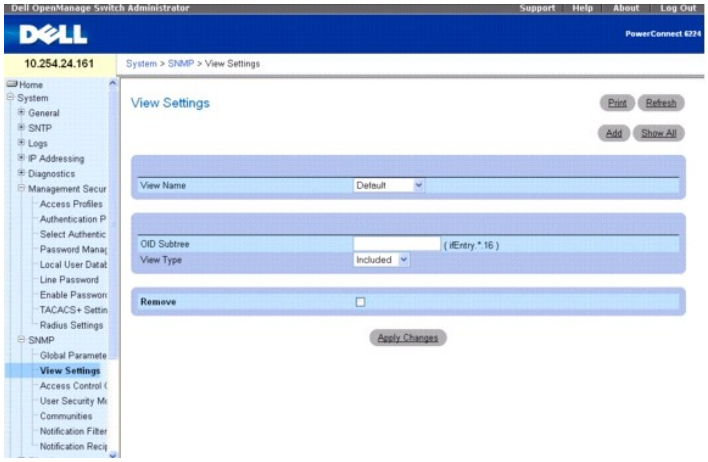
Einstellungen für SNMP-Ansichten

Auf dieser Seite können Sie Ansichten erstellen, die definieren, auf welche Gerätefunktionen zugegriffen werden kann und welche Funktionen gesperrt sind. So kann beispielsweise eine Ansicht erstellt werden, die OIDs für bestimmte Schnittstellen ein- bzw. ausschließt.

Auf der Seite **SNMP View Settings** (Einstellungen für SNMP-Ansichten) können Sie SNMP-Ansichten definieren.

Klicken Sie zum Anzeigen der Seite **SNMP View Settings** (Einstellungen für SNMP-Ansichten) in der Strukturansicht auf **System→ SNMP→ View Settings (Einstellungen für SNMP-Ansichten)**.

Abbildung 6-59. Einstellungen für SNMP-Ansichten



Die Seite **SNMP View Settings** (Einstellungen für SNMP-Ansichten) enthält folgende Felder:

View Name (Ansichtsname) – Enthält eine Liste benutzerdefinierter Ansichten. Der Name einer Ansicht darf aus maximal 30 alphanumerischen Zeichen bestehen.

OID Subtree (OID-Teilstruktur) – Spezifiziert eine gültige SNMP-OID-Zeichenkette, die Metazeichen wie * enthalten kann.

View Type (Ansichtstyp) – Legt fest, ob die Objektkennungen (objectIDs) in der Ansicht erscheinen sollen oder nicht.

Remove (Entfernen) – Markieren Sie diese Option, um die angezeigte Ansicht zu entfernen.

Hinzufügen einer Ansicht

1. Öffnen Sie die Seite **SNMP View Settings (**Einstellungen für SNMP-Ansichten).
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add View** (Ansicht hinzufügen) wird angezeigt:

Abbildung 6-60. Ansicht hinzufügen

3. Definieren Sie die relevanten Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

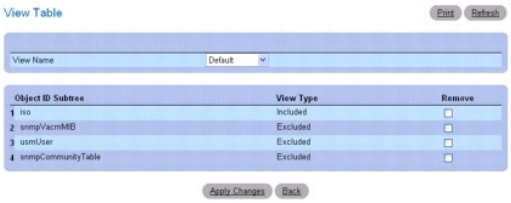
   Die SNMP-Ansicht wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der Seite View Table (Tabelle der Ansichten)

1. Öffnen Sie die Seite **SNMP View Settings (**Einstellungen für SNMP-Ansichten).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **View Table** (Tabelle der Ansichten) wird angezeigt:

Abbildung 6-61. Tabelle der Ansichten



Entfernen von SNMP-Ansichten

1. Öffnen Sie die Seite **SNMP View Settings (**Einstellungen für SNMP-Ansichten).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **View Table** (Tabelle der Ansichten) wird angezeigt.
3. Wählen Sie eine SNMP-Ansicht aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die SNMP-Ansicht wird entfernt und das Gerät aktualisiert.

Definieren von SNMP-Ansichten mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

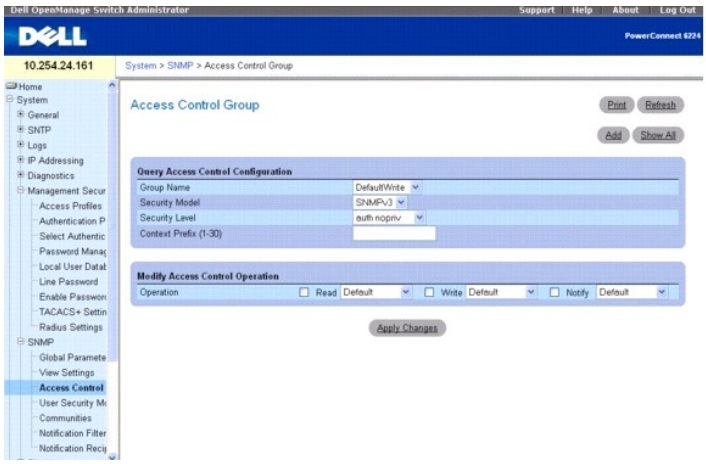
- SNMP Commands (SNMP-Befehle)

Access Control-Gruppe

Auf der Seite **Access Control Group** (Access Control-Gruppe) können Sie Informationen zum Erstellen von SNMP-Gruppen einsehen und SNMP-Zugriffsrechte vereinbaren. Mit Hilfe von Gruppen können Netzwerkverwalter Berechtigungen für den Zugriff auf bestimmte Gerätefunktionen oder -teilfunktionen festlegen.

Klicken Sie zum Anzeigen der Seite **Access Control Group** (Access Control-Gruppe) in der Strukturansicht auf **System**→ **SNMP**→ **Access Control** *(Access Control-Gruppe)*.

Abbildung 6-62. Access Control-Gruppe



Die Seite **Access Control Group** (Access Control-Gruppe) enthält folgende Felder:

Group Name (Gruppenname) – Enthält eine Liste mit benutzerdefinierten Gruppen, für die Zugriffsregeln gelten. Der Name einer Gruppe darf aus maximal 30 alphanumerischen Zeichen bestehen.

Security Model (Sicherheitsmodell) – Legt die SNMP-Version fest, die der Gruppe zugeordnet ist. Die für dieses Feld möglichen Werte sind:

SNMPv1 – Für die Gruppe ist SNMPv1 festgelegt.

SNMPv2 – Für die Gruppe ist SNMPv2 festgelegt.

SNMPv3 – Für die Gruppe ist das Benutzersicherheitsmodell (User Security Model) SNMPv3 definiert.

Security Level (Sicherheitsstufe) – Die der Gruppe zugeordnete Sicherheitsstufe. Sicherheitsstufen können nur SNMPv3-Gruppen zugeordnet werden. Die für dieses Feld möglichen Werte sind:

noauth no priv (Weder Authentifizierung noch Datenschutz) – Der Gruppe ist weder die Sicherheitsstufe Authentication (Authentifizierung) noch die Sicherheitsstufe Privacy (Datenschutz) zugeordnet.

auth nopriv – SNMP-Nachrichten werden authentifiziert, aber nicht verschlüsselt.

auth priv – SNMP-Nachrichten werden authentifiziert und verschlüsselt.

Context Prefix (1–30) – In diesem Feld kann der Kontextname durch Eingabe der (bis zu 30) ersten Zeichen spezifiziert werden.

Operation (Betrieb) – Legt Zugriffsrechte für Gruppen fest. Die für dieses Feld möglichen Werte sind:

Read (Lesen) – Wählen Sie eine Ansicht aus, die den Verwaltungszugang auf das Anzeigen von agentenspezifischen Inhalten beschränkt. Wenn keine Ansicht ausgewählt wurde, können alle Objekte mit Ausnahme der Community-Tabelle, der SNMPv3-Benutzer und der Zugangstabellen angezeigt werden.

Write (Schreiben) – Wählen Sie eine Ansicht aus, die dem Verwaltungszugang Schreib- und Leserechte für die Inhalte des Agenten gewährt.

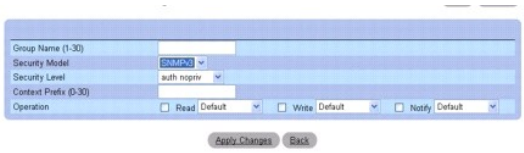
Notify (Benachrichtigen) – Wählen Sie eine Ansicht aus, die das Versenden von SNMP-Traps oder Informationsmeldungen gestattet.

Hinzufügen von SNMP-Gruppen

1. Öffnen Sie die Seite **Access Control Configuration** (Konfiguration der Zugangssteuerung).
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add an Access Control Configuration (Access Control-Konfiguration hinzufügen) wird angezeigt**:

Abbildung 6-63. Access Control-Konfiguration hinzufügen



3. Nehmen Sie die erforderlichen Einstellungen vor.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

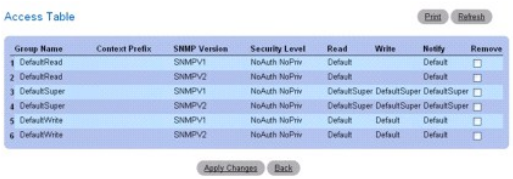
   Die Gruppe wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der Seite Access Table (Zugangstabelle)

1. Öffnen Sie die Seite **Access Control Configuration** (Konfiguration der Zugangssteuerung).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **Access Table** (Zugangstabelle) wird angezeigt:

Abbildung 6-64. Zugangstabelle



Entfernen einer Gruppe

1. Öffnen Sie die Seite **Access Control Configuration** (Konfiguration der Zugangssteuerung).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **Access Table** (Zugangstabelle) wird geöffnet.
3. Wählen Sie eine Gruppe aus.
4. Markieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Gruppe wird entfernt und das Gerät aktualisiert.

Definieren von SNMP-Zugriffsrechten mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

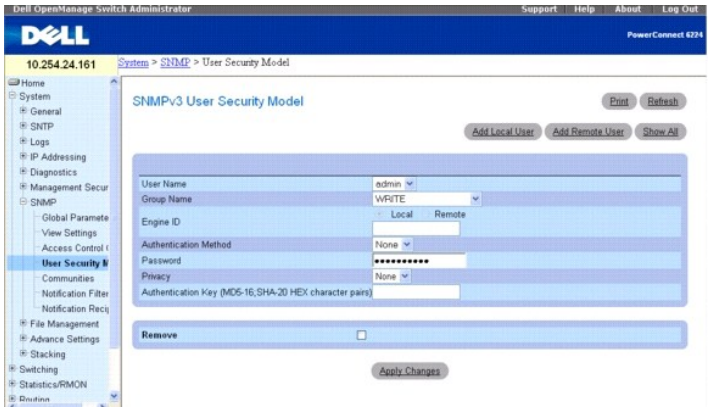
- SNMP Commands (SNMP-Befehle)

SNMPv3-Benutzersicherheitsmodell

Auf der Seite **SNMPv3 User Security Model (USM)** (SNMPv3-Benutzersicherheitsmodell) können Sie SNMP-Gruppen einen oder mehrere Systembenutzer zuweisen und die Benutzerauthentifizierungsmethode definieren.

Klicken Sie zum Anzeigen der Seite **SNMPv3 User Security Model (USM)** (SNMPv3-Benutzersicherheitsmodell) in der Strukturansicht auf **System→ SNMP→ User Security Model**.

Abbildung 6-65. SNMPv3-Benutzersicherheitsmodell



Die Seite **SNMPv3 User Security Model (USM) (SNMPv3-Benutzersicherheitsmodell) enthält folgende Felder:**

User Name (Benutzername) – Enthält eine Liste benutzerdefinierter Benutzernamen.

Group Name (Gruppenname) – Enthält eine Liste benutzerdefinierter SNMP-Gruppen. SNMP-Gruppen werden auf der Seite **Access Control Group (Access Control-Gruppe) eingerichtet**.

Engine ID (Engine ID) – Legt fest, ob der ausgewählte Benutzer mit einem lokalen oder einem bestimmten, für SNMPv3 aktivieren Remote-Gerät verbunden ist.

Remote Engine ID (Remote-Engine-ID) – Gibt an, dass der Benutzer auf einem SNMPv3-fähigen Remote-Gerät konfiguriert ist.

Authentication Method (Authentifizierungsmethode) – Legt die Methode für die Authentifizierung von Benutzern fest. Die für dieses Feld möglichen Werte sind:

None (Keine) – Es erfolgt keine Benutzerauthentifizierung.

MD5 – Die Benutzerauthentifizierung erfolgt mit Hilfe der Authentifizierungsebene HMAC-MD5-96. Der Benutzer sollte ein Kennwort vereinbaren.

SHA – Die Authentifizierung von Benutzern erfolgt mit Hilfe der Authentifizierungsebene HMAC-SHA-96. Der Benutzer muss ein Kennwort eingeben.

Password (Kennwort) – Ändert das benutzerdefinierte Kennwort für die Gruppe. Kennwörter dürfen aus maximal 32 Zeichen bestehen. Kennwörter werden nur dann definiert, wenn die Authentifizierungsmethode MD5 oder SHA Password (SHA-Kennwort) lautet. Das Kennwort wird auf der Seite **Add Local User** (Lokalen Benutzer hinzufügen) festgelegt.

Privacy (Datenschutz) – Legt fest, ob der Authentifizierungsschlüssel verwendet werden soll oder nicht. Wählen Sie einen der folgenden Werte aus:

None (Keiner) – Es wird kein Authentifizierungsschlüssel verwendet.

des — Es wird ein CBC-DES-Kennwort zur symmetrischen Verschlüsselung als Authentifizierungsschlüssel verwendet.

des-key – Es wird ein zuvor erzeugter HMAC-MD5-96-Authentifizierungsschlüssel verwendet.

Authentication Key (MD5-16; SHA-20 HEX character pairs) (Authentifizierungsschlüssel; MD5-16, SHA-20 HEX-Zeichenpaare) – Legen Sie hier den Authentifizierungsschlüssel fest. Ein Authentifizierungsschlüssel wird nur dann definiert, wenn die Authentifizierungsmethode MD5 oder SHA verwendet wird.

Remove (Entfernen) – Bei Auswahl dieser Option wird der angegebene Benutzer aus der betreffenden Gruppe entfernt.

Hinzufügen von lokalen SNMPv3-Benutzern zu einer Gruppe

1. Öffnen Sie die Seite **SNMPv3 User Security Model** (SNMPv3-Benutzersicherheitsmodell).
2. Klicken Sie auf **Add Local User** (Lokalen Benutzer hinzufügen).

   Die Seite **Add Local User** (Lokalen Benutzer hinzufügen) wird angezeigt:

Abbildung 6-66. Lokalen Benutzer hinzufügen

3. Definieren Sie die relevanten Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).
5. Der Benutzer wird zur Gruppe hinzugefügt und das Gerät aktualisiert.

Hinzufügen von SNMPv3-Remote-Benutzern zu einer Gruppe

1. Öffnen Sie die Seite **SNMPv3 User Security Model** (SNMPv3-Benutzersicherheitsmodell).
2. Klicken Sie auf **Add Remote User** (Remote-Benutzer hinzufügen).

   Die Seite **Add Remote User** (Remote-Benutzer hinzufügen) wird angezeigt:

Abbildung 6-67. Remote-Benutzer hinzufügen

3. Definieren Sie die relevanten Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).
5. Der Benutzer wird zur Gruppe hinzugefügt und das Gerät aktualisiert.

Anzeigen der Benutzersicherheitsmodell-Tabelle

1. Öffnen Sie die Seite **SNMPv3 User Security Model (USM)** (SNMPv3-Benutzersicherheitsmodell).

2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **User Security Model Table** (Benutzersicherheitsmodell-Tabelle) wird angezeigt:

Abbildung 6-68. Benutzersicherheitsmodell-Tabelle

Entfernen eines Eintrags aus der Benutzersicherheitsmodell-Tabelle

1. Öffnen Sie die Seite **User Security Model** (Benutzersicherheitsmodell).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **User Security Model Table** (Benutzersicherheitsmodell-Tabelle) wird angezeigt.
3. Wählen Sie einen Eintrag aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Eintrag wird entfernt und das Gerät aktualisiert.

Definieren von SNMP-Benutzern mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

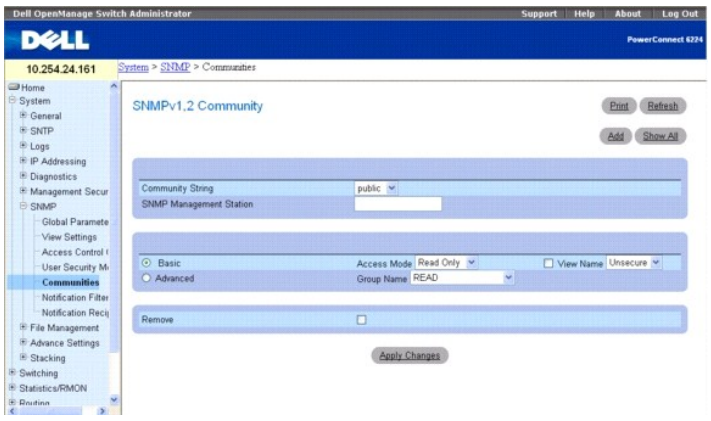
- SNMP Commands (SNMP-Befehle)

Communitys

Die Verwaltung von Zugriffsrechten erfolgt durch die Festlegung von Communitys auf der Seite **SNMPv1, 2 Community**. Sobald der Name einer Community geändert wird, ändern sich auch die Zugriffsrechte. SNMP-Communitys werden nur für SNMPv1 und SNMPv2 definiert.

Klicken Sie zum Anzeigen der Seite **SNMPv1, 2 Community** in der Strukturansicht auf **System** → **SNMP** → **Communities**.

Abbildung 6-69. SNMPv1, 2 Community



Die Seite SNMPv1, 2 Community (SNMPv1,2 Community) enthält folgende Felder:

Community String (Community-Zeichenkette) – Enthält eine Liste mit benutzerdefinierten Community-Zeichenketten, die als Kennwort fungieren und zum Authentifizieren der SNMP-Management-Station gegenüber dem Gerät verwendet werden. Eine Community-Zeichenkette darf aus maximal 20 Zeichen bestehen.

SNMP Management Station (SNMP-Management-Station) – Enthält eine Liste mit IP-Adressen von Management-Stationen, für die Community-Zeichenketten definiert worden sind.

Basic (Standard) – Aktiviert den SNMP-Modus Basic (Standard) für die ausgewählte Community. Die für dieses Feld möglichen Werte sind:

Access Mode (Zugangsmodus) – Definiert die Zugriffsrechte der Community. Die für dieses Feld möglichen Werte sind:

Read-Only (Schreibgeschützt) – Der Community-Zugang zu den in der Ansicht konfigurierten MIB-Objekten ist schreibgeschützt.

Read-Write (Lese-/Schreibzugriff) – Die Community kann Lese- und Schreibzugriffe auf die in der Ansicht konfigurierten MIB-Objekte durchführen.

Super User (Superuser) – Die Community kann Lese- und Schreibzugriffe auf alle MIB-Objekte durchführen.

View Name (Ansichtsname) – Enthält eine Liste mit benutzerdefinierten SNMP-Ansichten.

Advanced (Erweitert) – Enthält eine Liste benutzerdefinierter Gruppen. Bei Auswahl des SNMP-Modus Advanced (Erweitert) werden die SNMP-Zugriffsregeln der Gruppe für die ausgewählte Community aktiviert. Durch den Modus Advanced (Erweitert) werden außerdem SNMP-Gruppen für bestimmte SNMP-Communitys aktiviert. Der SNMP-Modus Advanced (Erweitert) ist nur bei SNMPv3 definiert.

Remove (Entfernen) – Bei Auswahl dieser Option wird die betreffende Community entfernt.

Hinzufügen einer neuen Community

1. Öffnen Sie die Seite **SNMPv1, 2 Community** (SNMPv1 Community).
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite ***Add SNMPv1,2 Community*** (SNMPv1,2 Community hinzufügen) wird angezeigt:

Abbildung 6-70. SNMPv1,2 Community hinzufügen

3. Füllen Sie die relevanten Felder aus.

   Zusätzlich zu den Feldern auf der Seite **SNMPv1, 2 Community** enthält die Seite ***Add SNMPv1,2 Community*** (SNMPv1,2-Community hinzufügen) das Feld **All (0.0.0.0)** (Alle (0.0.0.0)), das angibt, dass die Community von allen Management-Stationen aus verwendet werden kann.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die neue Community wird gespeichert und das Gerät aktualisiert.

Anzeigen von Communitys

1. Öffnen Sie die Seite **SNMPv1, 2 Community** (SNMPv1 Community).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **Basic Table** (Basistabelle) wird angezeigt.

Abbildung 6-71. Basistabelle

Entfernen von Community-Einträgen

1. Öffnen Sie die Seite **SNMPv1, 2 Community** (SNMPv1 Community).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **Basic Table** (Basistabelle) wird angezeigt.
3. Wählen Sie eine Community aus und aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Community-Eintrag wird entfernt und das Gerät aktualisiert.

Konfigurieren von Communitys mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

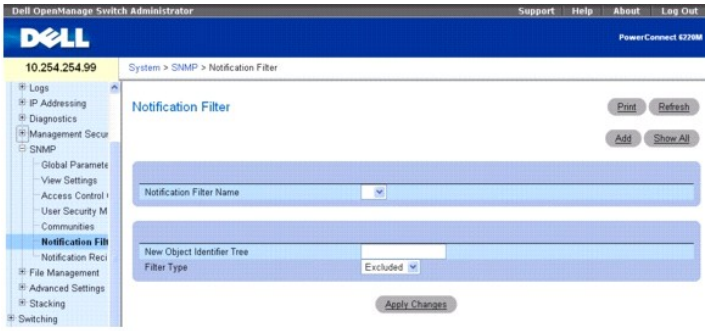
- SNMP Commands (SNMP-Befehle)

Benachrichtigungsfilter

Auf der Seite **Notification Filter** (Benachrichtigungsfilter) können Sie die Filter-Traps auf Basis von OIDs einstellen. Jede OID ist mit einer Gerätefunktion oder -teilfunktion verknüpft. Auf der Seite **Notification Filter** (Benachrichtigungsfilter) können Sie außerdem Benachrichtigungen filtern.

Klicken Sie zum Anzeigen der Seite **Notification Filter** (Benachrichtigungsfilter) in der Strukturansicht auf **System→ SNMP→ Notification Filters** *(Benachrichtigungsfilter)*.

Abbildung 6-72. Benachrichtigungsfilter



Die Seite **Notification Filter (Benachrichtigungsfilter) enthält folgende Felder:**

Notification Filter Name (Name des Benachrichtigungsfilters) – Enthält eine Liste mit benutzerdefinierten Benachrichtigungsfiltern. Der Name eines Benachrichtigungsfilters darf aus maximal 30 alphanumerischen Zeichen bestehen.

New Object Identifier Tree (Neue Objekt-ID-Struktur) – Zeigt die für den ausgewählten Filter konfigurierte Objektkennung (OID). Dieses Feld kann bearbeitet werden.

Notification Filter Type (Benachrichtigungsfiltertyp) – Gibt an, ob Informationsmeldungen oder Traps bezüglich der betreffenden OID an die Trap-Empfänger gesendet werden.

Excluded (Ausgeschlossen) – Schränkt den Versand von OID-Informationsmeldungen oder -Traps ein.

Included (Eingeschlossen) – Aktiviert den Versand von OID-Informationsmeldungen oder -Traps.

Hinzufügen von SNMP-Filtern

1. Öffnen Sie die Seite **Notification Filter** (Benachrichtigungsfilter).
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add Filter** (Filter hinzufügen) wird angezeigt:

Abbildung 6-73. Filter hinzufügen

3. Definieren Sie die relevanten Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der neue Filter wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der Seite Filter Table (Filtertabelle)

1. Öffnen Sie die Seite **Notification Filter** (Benachrichtigungsfilter).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **Filter Table** (Filtertabelle) erscheint; auf dieser Seite werden alle Filter angezeigt, die unter dem ausgewählten Filternamen konfiguriert wurden:

Abbildung 6-74. Benachrichtigung anzeigen

Entfernen eines Filters

1. Öffnen Sie die Seite **Notification Filter** (Benachrichtigungsfilter).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **Show Notification** (Benachrichtigung anzeigen) wird angezeigt.
3. Wählen Sie den Eintrag **Filter Table** (Filtertabelle) aus.
4. Markieren Sie das Kontrollkästchen **Remove** (Entfernen).

   Der Filtereintrag wird entfernt und das Gerät aktualisiert.

Konfigurieren von Benachrichtigungsfiltern mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- SNMP Commands (SNMP-Befehle)

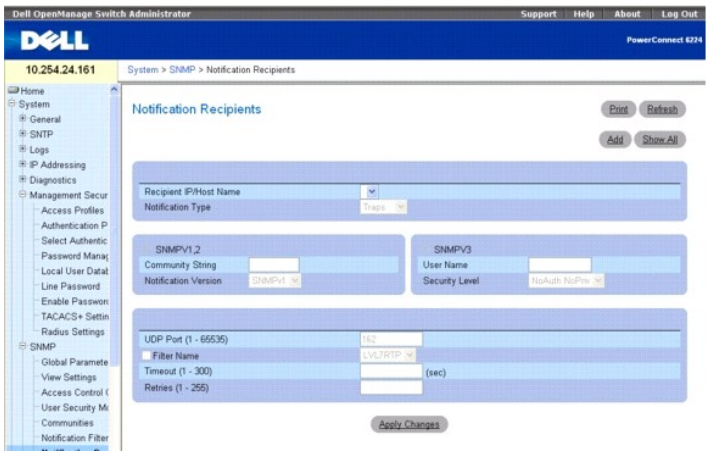
Benachrichtigungsempfänger

Auf der Seite **Notification Recipients** (Benachrichtigungsempfänger) können Sie Informationen zum Definieren von Filtern einsehen, die festlegen, ob Traps an bestimmte Benutzer übermittelt werden und welcher Trap-Typ jeweils gesendet wird. SNMP-Benachrichtigungsfilter stellen folgende Funktionen bereit:

- Identifizierung der Ziele von Verwaltungs-Traps
- Filterung von Traps
- Auswahl von Parametern für die Trap-Erzeugung
- Authentifizierung von Zugriffen

Klicken Sie zum Anzeigen der Seite **Notification Recipients** (Benachrichtigungsempfänger) in der Strukturansicht auf **System** → **SNMP** → **Notification Recipient** (Benachrichtigungsempfänger).

Abbildung 6-75. Benachrichtigungsempfänger



Die Seite Notification Recipients (Benachrichtigungsempfänger) enthält folgende Felder:

Recipient IP (Empfänger-IP) – Enthält eine benutzerdefinierte Liste mit IP-Adressen von Benachrichtigungsempfängern.

Notification Type (Benachrichtigungstyp) – Der Typ der zu übermittelnden Benachrichtigung. Die für dieses Feld möglichen Werte sind:

Trap – Es werden Traps gesendet.

Inform (Informationsmeldung) – Es werden Informationsmeldungen gesendet.

SNMPv1,2 – Für den ausgewählten Empfänger sind die SNMP-Versionen 1 oder 2 aktiviert. Die für dieses Feld möglichen Werte sind:

Community String (Community-Zeichenkette) – Zeigt die Community-Zeichenkette an, die mit der Benachrichtigung übermittelt werden soll.

Notification Version (Benachrichtigungsversion) – Legt die Benachrichtigungsversion fest. Die für dieses Feld möglichen Werte sind:

SNMP V1 – Es werden Traps der SNMP-Version 1 gesendet. Bei Auswahl des Benachrichtigungstyps Inform (Informationsmeldung) ist die Option SNMPv1 nicht verfügbar.

SNMP V2 – Es werden Traps oder Informationsmeldungen der SNMP-Version 2 gesendet.

SNMP v3 – Für den ausgewählten Empfänger ist die SNMP-Version 3 aktiviert. Die für dieses Feld möglichen Werte sind:

User Name (Benutzername) – Wählen Sie den vorhandenen Benutzer aus, um Benachrichtigungen zu erzeugen.

Security Level (Sicherheitsstufe) – Die Benachrichtigungen zugeordnete Sicherheitsstufe. Die für dieses Feld möglichen Werte sind:

NoAu NoPriv (Weder Authentifizierung noch Datenschutz) – Das Paket wird weder authentifiziert noch verschlüsselt.

Auth NoPriv – (Authentifizierung ohne Datenschutz) – Das Paket wird authentifiziert.

Auth Priv (Authentifizierung mit Datenschutz) – Das Paket wird sowohl authentifiziert als auch verschlüsselt.

UDP Port (1–65535) (UDP-Port, 1-65535) – Der für den Versand von Benachrichtigungen verwendete UDP-Port. Der Standardwert ist 162.

Filter Name (Filtername) – Markieren Sie dieses Kontrollkästchen, um einen benutzerdefinierten SNMP-Filter (Filterauswahl über Dropdown-Menü) auf Benachrichtigungen anzuwenden.

Timeout (1–300) (Zeitlimit, 1-300) – Die Zeit (in Sekunden), die das Gerät vor dem erneuten Senden von Informationsmeldungen wartet. Der Standardwert ist 15 Sekunden.

Retries (1–255) (Wiederholungsversuche, 1-255) – Vereinbart, wie oft das Gerät eine Informationsanforderung maximal übermittelt. Der Standardwert ist 3.

Hinzufügen eines neuen Benachrichtigungsempfängers

1. Öffnen Sie die Seite **Notification Recipients** (Benachrichtigungsempfänger).
2. Klicken Sie auf **Add**

   (Hinzufügen).

   Die Seite **Notification Recipients (Benachrichtigungsempfänger)** wird angezeigt:

Abbildung 6-76. Benachrichtigungsempfänger hinzufügen

3. Definieren Sie die relevanten Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

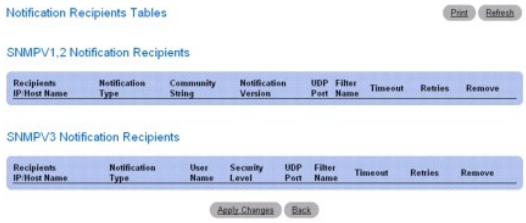
   Der Benachrichtigungsempfänger wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der Seite Notification Recipients Tables (Benachrichtigungsempfänger-Tabellen)

1. Öffnen Sie die Seite **Notification Recipients** (Benachrichtigungsempfänger).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **Notification Recipient Tables (Tabellen der Benachrichtigungsempfänger) wird geöffnet:**

Abbildung 6-77. Tabellen der Benachrichtigungsempfänger



Entfernen von Benachrichtigungsempfängern

1. Öffnen Sie die Seite **Notification Recipients** (Benachrichtigungsempfänger).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **Notification Recipient Tables** (Tabellen der Benachrichtigungsempfänger) wird geöffnet.

3. Aktivieren Sie in der Tabelle **SNMPv1,2 Notification Recipient** (SNMPV1,2-Benachrichtigungsempfänger) und/oder in der Tabelle **SNMPv3 Notification Recipient** (SNMPv3-Benachrichtigungsempfänger) das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Empfänger werden entfernt, und das Gerät wird aktualisiert.

Definieren von SNMP-Benachrichtigungsempfängern mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- SNMP Commands (SNMP-Befehle)

Verwalten von Dateien

Auf der Menüseite **File Management** (Dateiverwaltung) können Sie Gerätesoftware, die Abbilddatei und die Konfigurationsdateien verwalten. Die Dateien können über einen TFTP-Server herunter- oder hochgeladen werden. Das System unterstützt den Einsatz zweier Softwareversionen. Ein System, auf dem eine ältere Softwareversion eingesetzt wird, ignoriert Konfigurationsdateien, die mit einer neueren Softwareversion erstellt wurden (d. h., neuere Konfigurationsdateien werden nicht geladen). Wird eine Konfigurationsdatei, die mit der neueren Softwareversion erstellt wurde, von einem System erkannt, auf dem eine ältere Version dieser Software eingesetzt wird, gibt das System einen entsprechenden Warnhinweis an den Benutzer aus.

Übersicht über die Dateiverwaltung

Die Verwaltungsdateistruktur umfasst die folgenden Dateien:

- **Startup Configuration file** (Startup-Konfigurationsdatei) – Diese Datei speichert die genaue Gerätekonfiguration, wenn das Gerät ausgeschaltet oder neu gestartet wird. In der Startup-Datei werden Konfigurationsbefehle verwaltet. Außerdem können Konfigurationsbefehle aus der aktiven Konfigurationsdatei in der Startup-Datei gespeichert werden.
- **Running Configuration file** (Aktive Konfigurationsdatei) – Diese Datei enthält alle Befehle aus der Startup-Datei sowie alle während der aktuellen Sitzung eingegebenen Befehle. Nach dem Ausschalten oder Neustart des Geräts werden sämtliche in der aktiven Konfigurationsdatei gespeicherten Befehle gelöscht. Während des Startvorgangs werden alle Befehle aus der Startup-Datei in die aktive Konfigurationsdatei kopiert und auf das Gerät angewendet. Während der Sitzung werden alle neu eingegebenen Befehle den in der aktiven Konfigurationsdatei bereits enthaltenen Befehlen hinzugefügt. Befehle werden nicht überschrieben. Um die Startup-Datei zu aktualisieren, muss die aktive Konfigurationsdatei in die Startup-Konfigurationsdatei kopiert werden, bevor das Gerät ausgeschaltet wird. Beim nächsten Gerätestart werden die Befehle von der Startup-Konfigurationsdatei zurück in die aktive Konfigurationsdatei kopiert.
- **Backup Configuration File** (Sicherungskonfigurationsdatei) – Enthält eine Sicherungskopie der Gerätekonfiguration. Die Sicherungsdatei ändert sich, sobald die aktive Konfigurationsdatei oder die Startup-Konfigurationsdatei in die Sicherungsdatei kopiert werden. Die in der Sicherungsdatei enthaltenen Befehle werden durch die in die Datei kopierten Befehle ersetzt. Der Inhalt der Sicherungsdatei kann sowohl in die aktive Konfigurationsdatei als auch in die Startup-Konfigurationsdatei kopiert werden. Sie können aber auch Inhalte von einem Remote-TFTP-Server in die Sicherungsdatei und die Startup-Datei kopieren bzw. Inhalt der Sicherungs- und der Startup-Datei an einen Remote-Server.
- **Image Files** (Abbilddateien) – Systemabbilder werden in zwei Flash-Sektoren gespeichert, die als „Images" (Image 1 und Image 2) bezeichnet werden. Im aktiven Abbild wird die aktive Kopie und im zweiten Abbild eine weitere Kopie gespeichert. Das Gerät wird vom aktiven Abbild aus gestartet und ausgeführt. Falls das aktive Abbild beschädigt ist, startet das System automatisch vom nicht aktiven Abbild aus. Hierbei handelt es sich um eine Sicherheitsfunktion zum Schutz vor Fehlern, die während des Upgrade-Vorgangs bei Systemstart auftreten können.

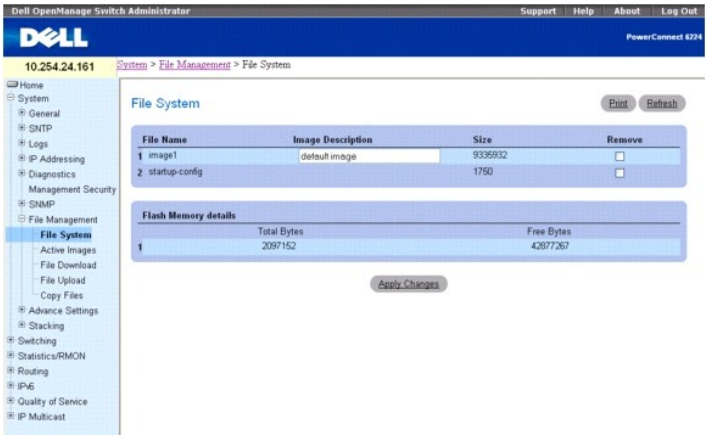
Klicken Sie zum Anzeigen der Seite **File Management** (Dateiverwaltung) in der Strukturansicht auf **System** → **File Management** (Dateiverwaltung).

Dateisystem

Auf der Seite ***File System*** (Dateisystem) können Sie eine Liste aller geräteseitig verfügbaren Dateien einsehen.

Klicken Sie zum Anzeigen der Seite ***File System*** (Dateisystem) in der Strukturansicht auf **System**→ **File Management (Dateiverwaltung)**→ **File System (Dateisystem)**.

Abbildung 6-78. Dateisystem



Die Seite File System (Dateisystem) enthält folgende Felder:

File Name (Dateiname) – Dieses Textfeld enthält eine Liste mit den Namen der Dateien in den einzelnen Dateisystemen.

Image Description (0-128) (Bildbeschreibung, 0-128)– Verwenden Sie dieses Feld, um eine Beschreibung des Abbilds zu konfigurieren und anzuzeigen. Geben Sie bis zu 128 Zeichen für die Beschreibung ein.

Size (Größe) – Zeigt die die Größe der angegebenen Datei an.

Remove (Entfernen) – Aktivieren Sie diese Option, um die angegebene Datei zu entfernen.

Flash Memory Details (Flash-Speicher-Details) – Zeigt den Betriebszustand des Flash-Speichers an.

Total Bytes (Bytes insgesamt) – Zeigt die belegte Flash-Speicher-Kapazität an.

Free Bytes (Freie Bytes) – Zeigt die verfügbare Flash-Speicher-Kapazität an.

Entfernen von Dateien

1. Öffnen Sie die Seite ***File System*** (Dateisystem).
2. Wählen Sie im Feld **File Name** (Dateiname) die zu entfernende Datei aus.
3. Markieren Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Datei wird entfernt.

Anzeigen von Dateien mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

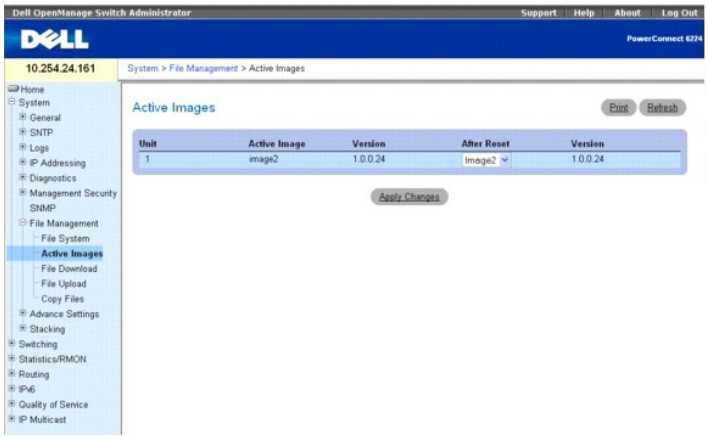
- Configuration and Image File Commands (Konfigurations- und Abbilddatei-Befehle)

Active Images (Aktive Abbilder)

Auf der Seite **Active Image** (Aktives Abbild) können Sie das Boot-Abbild einstellen.

Klicken Sie zum Anzeigen der Seite **Active Image** (Aktives Abbild) in der Strukturansicht auf **System→ File Management (Dateiverwaltung)→ Active Images (Aktive Abbilder)**.

Abbildung 6-79. Aktive Abbilder



Die Seite Active Images (Aktive Abbilder) enthält folgende Felder:

Unit (Einheit) – Zeigt die Einheitennummer des Systems im Stack an.

Active Image (Aktives Abbild) – Zeigt den Namen des derzeit aktiven Abbilds an.

Version – Zeigt die Versionsnummer des aktiven Abbilds an.

After Reset (Nach dem Zurücksetzen) – Ein Dropdown-Menü für die Auswahl einer Abbilddatei, die nach dem nächsten Zurücksetzen aktiviert wird.

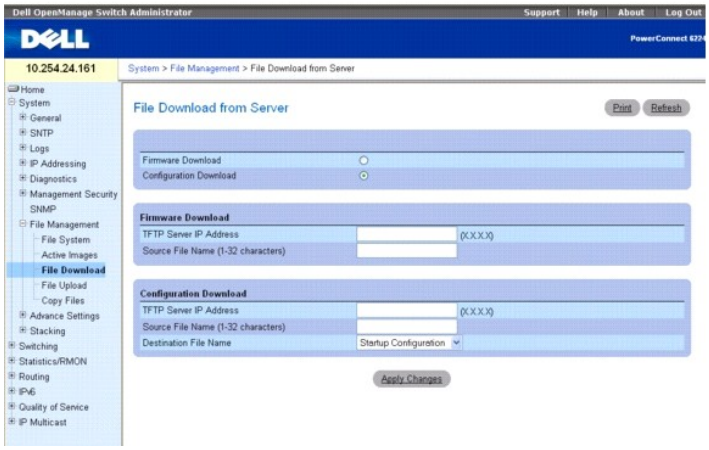
Version – Zeigt die Versionsnummer des Abbilds an, das nach dem nächsten Zurücksetzen aktiviert wird.

File Download From Server (Dateien vom Server herunterladen)

Auf der Seite ***File Download From Server*** (Dateien vom Server herunterladen) können Sie Konfigurations- und Abbilddateien (ASCII bzw. binär) von dem TFTP-Server auf das Gerät herunterladen.

Klicken Sie zum Anzeigen der Seite ***File Download From Server*** (Dateien vom Server herunterladen) in der Strukturansicht auf **System→ File Management (Dateiverwaltung)→ File Download (Datei herunterladen)**.

Abbildung 6-80. Dateien vom Server herunterladen



Die Seite *File Download From Server* *(Dateien vom Server herunterladen) enthält folgende Felder:*

Firmware Download (Firmware herunterladen) – Gibt an, dass die Firmware-Datei heruntergeladen werden soll. Ist diese Option ausgewählt, werden die Felder unter **Configuration Download** (Konfiguration herunterladen) grau dargestellt.

Configuration Download (Konfiguration herunterladen) – Gibt an, dass die Konfigurationsdatei heruntergeladen werden soll. Bei Auswahl von **Configuration Download** (Konfiguration herunterladen) werden die Felder unter **Firmware Download** (Firmware herunterladen) grau dargestellt.

Firmware Download (Firmware herunterladen)

TFTP Server IP Address (IP-Adresse des TFTP-Servers) – Die IP-Adresse des TFTP-Servers, von dem die Firmware-Dateien heruntergeladen werden.

Source File Name (1 – 32 characters) (Name der Quelldatei, 1-32 Zeichen) – Der Name der Datei auf dem TFTP-Server mit Angabe des relativen Pfads zum Verzeichnis tftpboot. Beispiel: Wenn TFTP auf einem Remote-Server konfiguriert ist, das tftpboot-Verzeichnis *e:\tftp*, lautet und die Datei *test.scr* unter *e:\tftp\latest\test.scr* vorliegt, müssen Sie Folgendes eingeben: **\latest\test.scr.**

Configuration Download (Konfiguration herunterladen)

TFTP Server IP Address (IP-Adresse des TFTP-Servers) – Die IP-Adresse des TFTP-Servers, über den die Konfigurationsdateien heruntergeladen werden.

Source File Name (1 – 32 characters) (Name der Quelldatei, 1-32 Zeichen) – Der Name der Datei auf dem TFTP-Server.

Destination File Name (Name der Zieldatei) – Die Zieldatei, in die die Konfigurationsdateien heruntergeladen werden. Mögliche Werte:

Startup Configuration – Lädt die Startup-Konfigurationsdateien herunter.

Backup Configuration (Sicherungskonfiguration) – Lädt die Sicherungskonfigurationsdateien herunter.

Herunterladen von Dateien

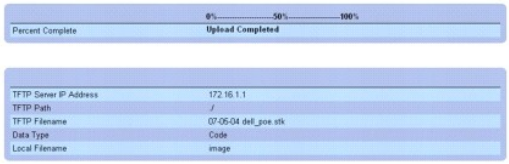
1. Öffnen Sie die Seite ***File Download From Server*** (Dateien vom Server herunterladen).
2. Überprüfen Sie die IP-Adresse des TFTP-Servers und stellen Sie sicher, dass die herunterzuladende Datei (Softwareabbild oder Startdatei) auf dem TFTP-Server verfügbar ist.
3. Füllen Sie die Felder **TFTP Server IP Address** (IP-Adresse des TFTP-Servers) und **Source File Name** (Quelldateiname) (vollständiger Pfad ohne IP-Adresse des TFTP-Servers) aus.

ANMERKUNG: Es wird empfohlen, das aktive Abbild nicht zu überschreiben.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

ANMERKUNG: Nachdem Sie mit dem Herunterladen einer Datei begonnen haben, wird die Seite aktualisiert, und es wird ein Transferstatus-Feld angezeigt, das über die Anzahl der übertragenen Bytes informiert. Die Webschnittstelle ist gesperrt, bis die Datei vollständig heruntergeladen wurde.

Abbildung 6-81. Fortschrittsanzeige für Datei-Download



Die Software wird auf das Gerät heruntergeladen.

Herunterladen von Dateien mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

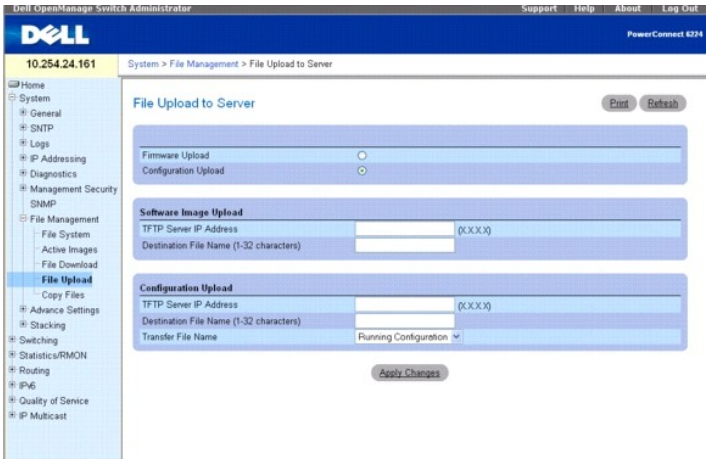
- Configuration and Image File Commands (Konfigurations- und Abbilddatei-Befehle)

Hochladen von Dateien

Auf der Seite ***File Upload to Server*** (Dateien auf den Server hochladen) können Sie Konfigurations- und Abbilddateien (ASCII bzw. binär) vom Gerät auf den TFTP-Server hochladen.

Klicken Sie zum Anzeigen der Seite ***File Upload to Server*** (Dateien auf den Server hochladen) in der Strukturansicht auf **System→ File Management (Dateiverwaltung)→ File Upload (Datei hochladen)**.

Abbildung 6-82. Dateien auf den Server hochladen



Die Seite *File Upload to Server* *(Dateien auf den Server hochladen) enthält folgende Felder:*

Firmware Upload (Firmware hochladen) – Gibt an, dass die Firmware-Datei hochgeladen werden soll. Bei Auswahl von **Firmware Upload** (Firmware hochladen) werden die Felder unter **Configuration Upload** *(Konfiguration hochladen)* grau dargestellt.

Configuration Upload (Konfiguration hochladen) – Gibt an, dass die Konfigurationsdatei hochgeladen wird. Bei Auswahl von **Configuration Upload** (Konfiguration hochladen) werden die Felder unter **Firmware Upload** (Firmware hochladen) grau dargestellt.

Software Image Upload (Softwareabbild hochladen)

TFTP Server IP Address (IP-Adresse des TFTP-Servers) – Die IP-Adresse des TFTP-Servers, auf den das Softwareabbild hochgeladen wird.

Destination File Name (1 – 32 Characters) (Name der Zieldatei, 1-32 Zeichen) – Der Name, den die Datei nach dem Hochladen haben wird.

Transfer File Name (Name der zu übertragenden Datei) – Ermöglicht die Auswahl der hochzuladenden Quelldatei.

Configuration Upload (Konfiguration hochladen)

TFTP Server IP Address (IP-Adresse des TFTP-Servers) – Die IP-Adresse des TFTP-Servers, auf den die Konfigurationsdatei hochgeladen wird.

Destination File Name (1 – 32 Characters) (Name der Zieldatei, 1-32 Zeichen) – Der Name, den die Datei nach dem Hochladen haben wird.

Transfer File Name (Name der zu übertragenden Datei) – Ermöglicht die Auswahl der hochzuladenden Quelldatei. Gültige Werte sind:

Running Configuration (Aktive Konfiguration) – Lädt die aktive Konfigurationsdatei hoch.

Startup Configuration (Startkonfiguration) – Lädt die Startup-Konfigurationsdateien hoch.

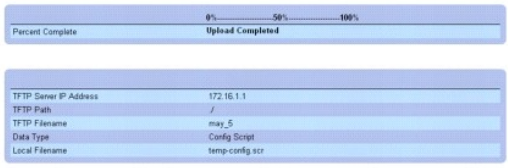
Backup Configuration (Sicherungskonfiguration) – Lädt die Sicherungskonfigurationsdatei hoch.

Hochladen von Dateien

1. Öffnen Sie die Seite ***File Upload to Server*** (Dateien auf den Server hochladen).
2. Definieren Sie alle erforderlichen Felder auf dieser Seite.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

ANMERKUNG: Nachdem Sie mit dem Hochladen einer Datei begonnen haben, wird die Seite aktualisiert, und es wird ein Transferstatus-Feld angezeigt, das über die Anzahl der übertragenen Bytes informiert. Die Webschnittstelle ist gesperrt, bis die Datei vollständig hochgeladen wurde.

Abbildung 6-83. Fortschrittsanzeige für Datei-Upload



Die Software wird auf den Server hochgeladen.

Hochladen von Dateien mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Configuration and Image File Commands (Konfigurations- und Abbilddatei-Befehle)

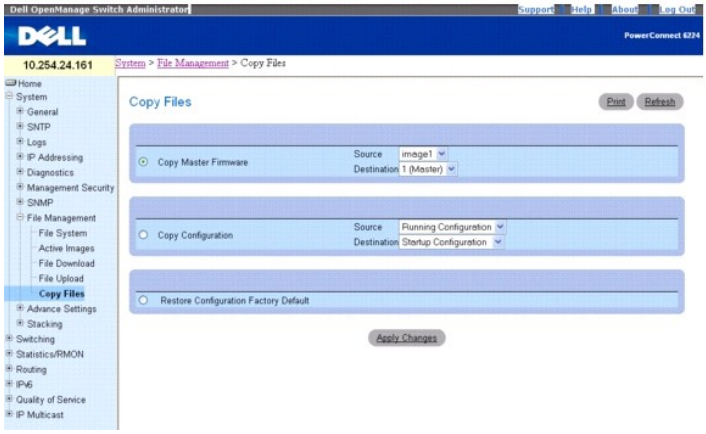
Dateien kopieren

Auf der Webseite Copy Files (Dateien kopieren) können Sie:

- Abbilder innerhalb des Dateisystems kopieren
- Abbilder an und von Remote-Server(n) kopieren.
- Abbilder auf lokalen oder Remote-Systemen sichern
- Abbilder von lokalen oder Remote-Systemen wiederherstellen
- Die Konfigurationsdateien innerhalb des Dateisystems sichern

Klicken Sie zum Anzeigen der Seite **Copy Files** (Dateien kopieren) in der Strukturansicht auf **System→ File Management (Dateiverwaltung)→ Copy (Kopieren)**.

Abbildung 6-84. Dateien kopieren



Die Seite Copy Files (Dateien kopieren) enthält folgende Felder:

Copy Master Firmware (Master-Firmware kopieren) – Gibt an, dass eine Softwareabbild-Datei kopiert werden soll.

Source (Quelle) – Die Quelldatei des Softwareabbilds, von der die Datei kopiert wird.

Destination (Ziel) – Die Zieleinheit, an die die Datei kopiert wird.

Copy Configuration (Konfiguration kopieren) – Gibt an, dass eine Konfigurationsdatei kopiert werden soll.

Source (Quelle) – Die Quellkonfigurationsdatei (aktive, Startup, Sicherung) von der die Datei kopiert wird.

Destination (Ziel) – Die Zielkonfigurationsdatei (aktive, Startup, Sicherung) an die die Datei kopiert wird.

Restore Configuration Factory Default (Werkseitige Standard-Konfigurationseinstellungen wiederherstellen) – Bei Aktivierung dieser Option werden die Dateien mit der werkseitigen Standardkonfiguration wiederhergestellt. Ist die Option deaktiviert, werden die aktuellen Konfigurationseinstellungen beibehalten.

Kopieren von Dateien

1. Öffnen Sie die Seite **Copy Files** (Dateien kopieren).
2. Wählen Sie **Copy** (Kopieren) oder **Restore** (Wiederherstellen) und füllen Sie die entsprechenden Felder aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Datei wird kopiert.

Kopieren von Dateien mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Configuration and Image File Commands (Konfigurations- und Abbilddatei-Befehle)

Definieren erweiterter Einstellungen

Auf der Seite Advanced Settings (Erweiterte Einstellungen) können Sie verschiedene globale Attribute für das Gerät festlegen. Änderungen an diesen Attributen werden erst nach dem Zurücksetzen des Geräts wirksam. Klicken Sie in der Strukturansicht auf **System→ Advanced Settings** (Erweiterte Einstellungen), um die Seite **Advanced Settings** (Erweiterte Einstellungen) anzuzeigen.

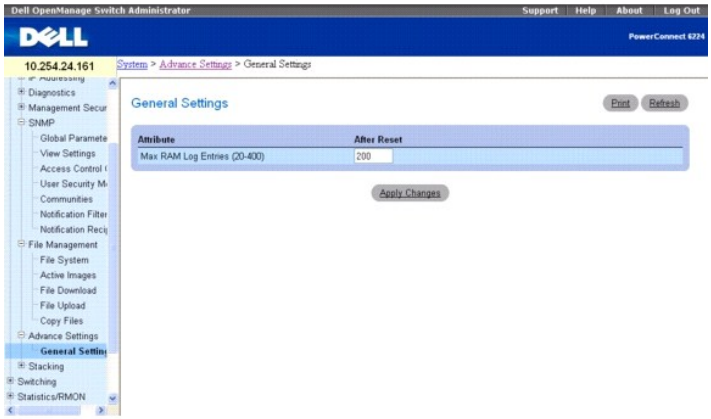
Die Seite **Advanced Settings** (Erweiterte Einstellungen) enthält einen Link zu einer Seite, über die Sie allgemeine Einstellungen konfigurieren können.

Allgemeine Einstellungen

Auf der Seite **General Settings** (Allgemeine Einstellungen) können Sie allgemeine Geräteparameter definieren.

Klicken Sie zum Anzeigen der Seite **General Settings** (Allgemeine Einstellungen) in der Strukturansicht auf **System→ Advanced Settings (Erweiterte Einstellungen)→ General (Allgemein)**.

Abbildung 6-85. Allgemeine Einstellungen



Die Seite General Settings (Allgemeine Einstellungen) enthält folgende Felder:

Attribute (Attribut) – Maximale Anzahl von RAM-Protokolleinträgen. Der Standardwert lautet 200 (Einträge).

After Reset (Nach dem Zurücksetzen) – Maximale Anzahl von Einträgen nach dem Zurücksetzen des Geräts. Bei Eingabe eines Wertes in dieser Spalte wird der Feldtabelle Arbeitsspeicher zugewiesen.

Ändern der zugewiesenen Kapazität für RAM-Protokolleinträge

1. Öffnen Sie die Seite **General Settings** (Allgemeine Einstellungen).
2. Geben Sie im Feld **After Reset** (Nach dem Zurücksetzen) den gewünschten neuen Wert ein.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der für RAM-Protokolleinträge reservierte Speicherplatz wird erst nach dem nächsten Zurücksetzen des Geräts neu zugewiesen.

Anzeigen von allgemeinen Einstellungen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Syslog-Befehle

Definieren der Stacking-Eigenschaften

Über die Stacking-Menüs können Sie die Stacking-Eigenschaften des Geräts einstellen. Änderungen an diesen Attributen werden erst nach dem Zurücksetzen des Geräts wirksam. Klicken Sie in der Strukturansicht auf **System**→ **Stacking,** um die Seite **Stacking** anzuzeigen. Die Seite bietet Zugriff auf folgende Funktionen:

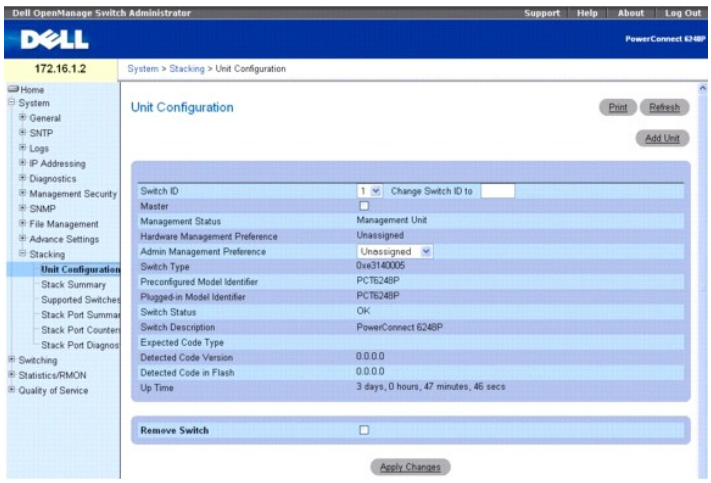
- Einheit-Konfiguration
- Stack-Übersicht
- Unterstützte Switches
- Stack-Port-Übersicht
- Stack-Port-Zähler
- Stack-Port-Diagnose

Einheit-Konfiguration

Auf der Seite **Unit Configuration** (Einheit-Konfiguration) können Sie allgemeine Geräteparameter definieren.

Klicken Sie zum Anzeigen der Seite **Unit Configuration** (Einheit-Konfiguration) in der Strukturansicht auf **System**→ **Stacking** → **Unit Configuration (Einheit-Konfiguration)**.

Abbildung 6-86. Einheit-Konfiguration



Die Seite Unit Configuration (Einheit-Konfiguration) enthält folgende Felder:

Switch ID (Switch-ID) – Gibt die zu konfigurierende Geräteeinheit an.

Change Switch ID to (Switch-ID ändern in) – Ändert die Einheitennummer der ausgewählten Geräteeinheit.

Master (Master) – Vereinbart, dass diese Einheit als Master-Einheit (Verwaltungseinheit) fungiert, die gegenüber anderen Einheiten bevorzugt wird. Der Standardwert für diesen Parameter lautet Unassigned (Nicht zugewiesen).

Management Status (Verwaltungsstatus) – Zeigt, ob die ausgewählte Geräteeinheit den Status Management Unit (Verwaltungseinheit) oder Stack Member (Stack-Komponente) hat.

Hardware Management Preference (Hardware-Verwaltungspräferenz) – Die Verwaltungspräferenz nach Hardwarekonfiguration, die bei der Auswahl als Verwaltungseinheit zu berücksichtigen ist.

Admin Management Preference (Admin-Verwaltungspräferenz) – Legt fest, ob diese Geräteeinheit als Master-Switch fungieren kann. Der Wertebereich reicht von **Disable** (die Geräteeinheit kann nicht als Master-Switch fungieren) bis **Preference 15** (Präferenzstufe 15). Höhere Werte signalisieren, dass die Geräteeinheit gegenüber anderen Einheiten (mit niedrigeren Werten) für die Ausführung der Verwaltungsfunktion bevorzugt wird. Ein weiterer Wert – **Unassigned** (Nicht zugewiesen) – besagt, dass die Präferenzstufe nicht konfiguriert ist und die Auswahl der Master-Einheit den Stack-Einheiten überlassen wird.

Switch Type (Switch-Typ) – Die Hardwarekennung, die an das System übermittelt wird, um den Switch-Typ zu bestimmen.

Preconfigured Model Identifier (Kennung des vorkonfigurierten Modells) – Eine 16 Byte lange Zeichenkette, die es ermöglicht, das vorkonfigurierte Modell der ausgewählten Geräteeinheit zu ermitteln.

Plugged-in Model Identifier (Kennung des Plug-in-Modells) – Eine 16 Byte lange Zeichenkette, die es ermöglicht, das Plug-in-Modell der ausgewählten Geräteeinheit zu ermitteln.

Switch Status (Switch-Status) – Zeigt den Status der ausgewählten Geräteeinheit an. Die möglichen Werte lauten:

OK – Die Geräteeinheit ist vorhanden und in Betrieb.

Unsupported (Nicht unterstützt) – Die Geräteeinheit ist vorhanden, kann jedoch nicht als Stack-Komponente eingesetzt werden.

Code Mismatch (Code-Konflikt) – Die Software des Switches stimmt nicht mit der Software der Master-Einheit überein.

Config Mismatch (Konfigurationskonflikt) – Die Konfiguration des Switches stimmt nicht mit der Konfiguration der Master-Einheit überein.

Not Present (Nicht vorhanden) – Die ausgewählte Geräteeinheit ist nicht vorhanden.

Switch Description (Switch-Beschreibung) – 80 Bytes langes Datenfeld zur Identifizierung des Geräts.

Expected Code Type (Erwarteter Code-Typ) – Zeigt die erwartete Code-Kennung an.

Detected Code Version (Erkannte Code-Version) – Die Freigabenummer und die Versionsnummer der aktiven Code-Version.

Detected Code in Flash (Erkannter Code in Flash) – Freigabenummer und Versionsnummer des im Flash-Speicher erkannten Codes.

Up Time (Betriebszeit) – Zeigt an, wie lange die Geräteeinheit seit dem letzten Zurücksetzen aktiv ist.

Remove Switch (Switch entfernen) – Aktivieren Sie diese Option, um den zugehörigen Switch aus dem Stapel zu entfernen.

Definieren der Einheit-Konfiguration

1. Öffnen Sie die Seite **Unit Configuration** (Einheit-Konfiguration).
2. Geben Sie in den einzelnen Feldern die gewünschten neuen Werte ein.

3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Änderungen werden erst nach dem nächsten Zurücksetzen des Geräts wirksam.

Entfernen eines Switch

1. Öffnen Sie die Seite **Unit Configuration** (Einheit-Konfiguration).
2. Markieren Sie das Kontrollkästchen **Remove Switch** (Switch entfernen).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Änderungen werden erst nach dem nächsten Zurücksetzen des Geräts wirksam.

Hinzufügen einer Einheit

Auf der Seite **Add Unit** (Einheit hinzufügen) können Sie allgemeine Geräteparameter definieren.

Um die Seite **Supported Switches** (Unterstützte Switches) anzuzeigen, klicken Sie in der Strukturansicht auf **System**→ **Stacking**→ **Unit Configuration** (Einheit-Konfiguration) und anschließend auf **Add Unit** (Einheit hinzufügen).

Abbildung 6-87. Einheit hinzufügen

Die Seite Add Unit (Einheit hinzufügen) enthält folgende Felder:

Switch ID (Switch-ID) – Zeigt die Switch-Kennung des ausgewählten Switches im Stack an. Diese Kennung kann von Admin-Benutzern geändert werden, um dem ausgewählten Switch eine neue Switch-ID zuzuweisen. Dieses Feld kann nur von Benutzern mit Berechtigungsstufe 15 über die Webschnittstelle geändert werden.

Switch Type (Switch-Typ) – Zeigt die dem Switch zugewiesene Hardwarekennung an.

Hinzufügen einer Geräteeinheit

1. Öffnen Sie die Seite **Unit Configuration** (Einheit-Konfiguration).
2. Klicken Sie auf **Add Unit** (Einheit hinzufügen).

   Die Seite **Add Unit** (Einheit hinzufügen) erscheint.
3. Geben Sie im Feld **Switch ID** (Switch-ID) den gewünschten neuen Wert ein.
4. Wählen Sie den gewünschten Wert aus der Dropdown-Liste **Switch-Type** (Switch-Typ) aus.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Änderungen werden erst nach dem nächsten Zurücksetzen des Geräts wirksam.

Anzeigen der Einheit-Konfiguration mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

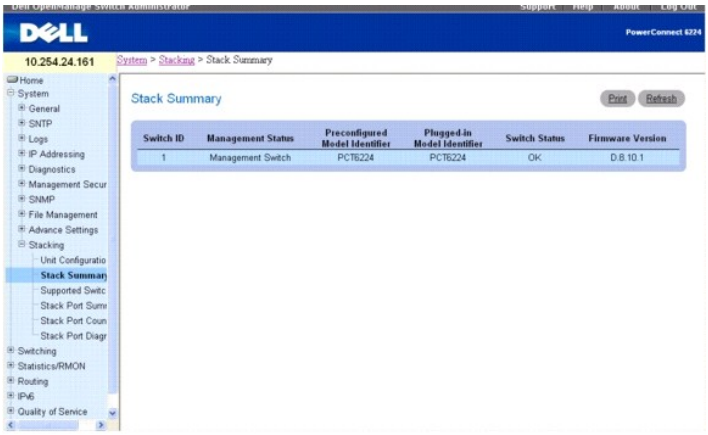
- System Management Commands (System-Management-Befehle)

Stack-Übersicht

Auf der Seite **Stack Summary** (Stack-Übersicht) können Sie eine Übersicht aller Switches einsehen, die Teil eines Stacks sind.

Klicken Sie zum Anzeigen der Seite **Stack Summary** (Stack-Übersicht) in der Strukturansicht auf **System**→ **Stacking**→ **Stack Summary (Stack-Übersicht)**.

Abbildung 6-88. Stack-Übersicht



Die Seite Stacking Summary (Stacking-Übersicht) enthält folgende Felder:

Switch ID (Switch-ID) – Kennung (ID) der Geräteeinheit. Die maximale Anzahl von Geräteeinheiten pro Stack beträgt 8.

Management Status (Management-Status) – Dieses Feld zeigt an, ob es sich bei dem Switch um den Management-Switch, eine Stack-Komponente oder einen Switch ohne Statuszuweisung handelt.

Pre-configured Model Identifier (Kennung des vorkonfigurierten Modells) – Dieses Feld zeigt den Inhalt des 16 Zeichen langen Felds an, das vom Gerätehersteller als eindeutige Kennung für das vorkonfigurierte Gerät vereinbart wurde.

Plugged-in Model Identifier (Kennung des Plug-in-Modells) – Dieses Feld zeigt den Inhalt des 16 Zeichen langen Felds an, das vom Gerätehersteller als eindeutige Kennung für das Plug-in-Gerät vereinbart wurde.

Switch Status (Switch-Status) – Gibt den aktuellen Status der Geräteeinheit an. Es gibt fünf mögliche Statuswerte:

OK – Die Geräteeinheit ist vorhanden und arbeitet fehlerfrei.

Unsupported (Nicht unterstützt) – Die Geräteeinheit kann nicht in den Stack integriert werden.

Code Mismatch (Code-Konflikt) – Das Softwareabbild in dieser Geräteeinheit stimmt nicht mit dem im Master-Switch des Stacks verwendeten Abbild überein.

Config Mismatch (Konfigurationskonflikt) – Die Konfigurationsdatei in dieser Geräteeinheit stimmt nicht mit der im Master-Switch des Stacks verwendeten Datei überein.

Not Present (Nicht vorhanden) – Die Geräteeinheit liegt nicht vor.

Firmware Version (Firmware-Version) – Gibt die erkannte Code-Version für diese Geräteeinheit an.

Anzeigen der Stack-Übersicht mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

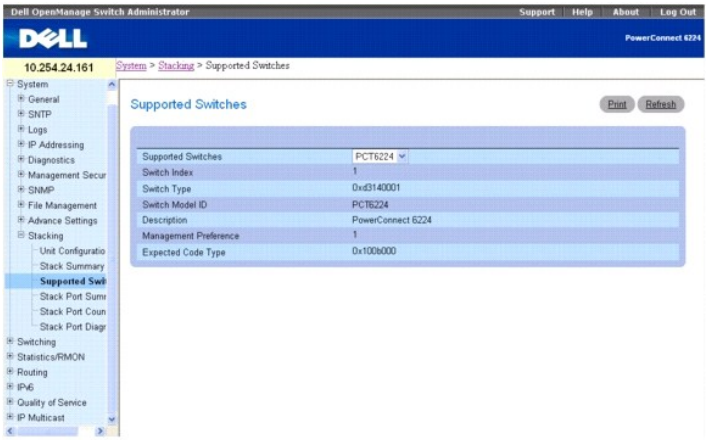
- System Management Commands (System-Management-Befehle)

Unterstützte Switches

Auf der Seite **Supported Switches** (Unterstützte Switches) können Sie Informationen zu jedem Switch-Typ einsehen, der den Stack-Betrieb unterstützt, sowie Informationen zu den unterstützten Switches.

Klicken Sie zum Anzeigen der Seite **Supported Switches** (Unterstützte Switches) in der Strukturansicht auf **System→ Stacking→ Supported Switches (Unterstützte Switches)**.

Abbildung 6-89. Unterstützte Switches



Die Seite Supported Switches (Unterstützte Switches) enthält folgende Felder:

Supported Switches (Unterstützte Switches) – Dropdown-Liste für die Auswahl von unterstützten Switches.

Switch Index (Switch-Index) **–** Legt die Indexnummer in der Datenbank der unterstützten Switch-Typen fest.

Switch Type (Switch-Typ) – Die dem Switch zugewiesene Hardwarekennung.

Switch Model ID (Switch-Modell-ID) – Zeigt eine 16 Byte lange Zeichenkette an, die für die Modellkennung des unterstützten Switches steht.

Description (Beschreibung) – Zeigt ein 256 Bytes langes Datenfeld zur Identifizierung des Geräts an.

Management Preference (Verwaltungspräferenz) – Legt fest, ob diese Geräteeinheit als Master-Switch fungieren kann. Wird hier der Wert 0 vereinbart, kann die Geräteeinheit nicht als Master-Switch fungieren. Höhere Werte signalisieren, dass die Geräteeinheit gegenüber anderen Einheiten (mit niedrigeren Werten) für die Ausführung der Verwaltungsfunktion bevorzugt wird. Der Anfangswert für dieses Feld wird vom Gerätehersteller eingestellt.

Expected Code Type (Erwarteter Code-Typ) – Zeigt die Freigabenummer und die Versionsnummer des erwarteten Codes an.

Anzeigen der Eigenschaften von unterstützten Switches

1. Öffnen Sie die Seite **Supported Switches** (Unterstützte Switches).
2. Wählen Sie den gewünschten Switch aus der Dropdown-Liste **Supported Switches** (Unterstützte Switches).

Anzeigen von unterstützten Switches mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

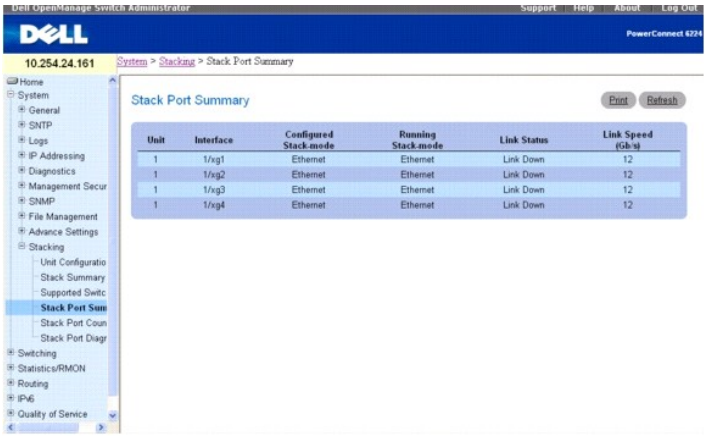
- System Management Commands (System-Management-Befehle)

Stack-Port-Übersicht

Auf der Seite **Stack Port Summary** (Stack-Port-Übersicht) können Sie die vorhandenen stapelbaren Ports einsehen. Dieser Bildschirm zeigt folgende Informationen an: die Geräteeinheit, die stapelbare Schnittstelle, den konfigurierten Schnittstellenmodus, den derzeit aktiven Modus sowie den Verbindungsstatus und die Verbindungsgeschwindigkeit des stapelbaren Ports.

Klicken Sie zum Anzeigen der Seite **Stack Port Summary** (Stack-Port-Übersicht) in der Strukturansicht auf **System** → **Stacking** → **Stack Port Summary** (Stack-Port-Übersicht).

Abbildung 6-90. Stack-Port-Übersicht



Die Seite Stack Port Summary (Stack-Port-Übersicht) enthält folgende Felder:

Unit (Einheit) – Kennnummer (ID) der Geräteeinheit.

Interface (Schnittstelle) – Identifiziert die Stack-Schnittstelle, die der Geräteeinheit zugewiesen ist.

Configured Stack Mode (Konfigurierter Stack-Modus) – Gibt an, ob sich eine Geräteeinheit in den Stack integrieren lässt oder nicht.

Running Stack Mode (Aktiver Stack-Modus) – Gibt an, ob eine Geräteeinheit tatsächlich in den Stack integriert ist oder nicht.

Link Status (Verbindungsstatus) – Gibt an, ob die Stack-Schnittstelle für eine Geräteeinheit derzeit in Betrieb ist oder nicht.

Link Speed (Gb/s) (Verbindungsgeschwindigkeit (Gbit/s)) – Gibt die Nenngeschwindigkeit für die Verbindung einer Geräteeinheit an.

Anzeigen der Stack-Port-Übersicht mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

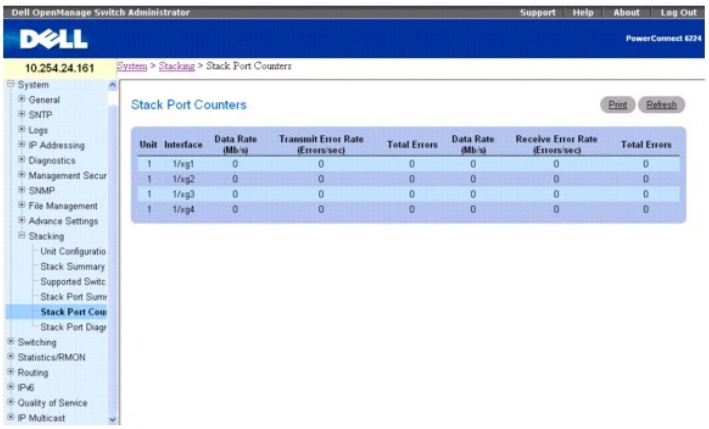
- System Management Commands (System-Management-Befehle)

Stack-Port-Zähler

Auf der Seite **Stack Port Counters** (Stack-Port-Zähler) können Sie die Sende- und Empfangsstatistiken einsehen (Datenrate, Fehlerrate etc.).

Klicken Sie zum Anzeigen der Seite **Stack Port Counters** (Stack-Port-Zähler) in der Strukturansicht auf **System** → **Stacking** → **Stack Point Counters** (Stack-Port-Zähler).

Abbildung 6-91. Stack-Port-Zähler



Die Seite Stack Port Counters (Stack-Port-Zähler) enthält folgende Felder:

Unit (Einheit) – Gibt an, welcher untergeordnete Switch gerade eingesehen wird.

Interface (Schnittstelle) – Gibt den Namen der Schnittstelle an.

Data Rate (Mb/s) (Datenrate, Mbit/s) – Gibt die Geschwindigkeit an, mit der die Daten gesendet werden.

Transmit Error Rate (Errors/sec) (Sendefehlerrate, Fehler/Sek.) – Die Anzahl der Übertragungsfehler pro Sekunde bei Sendevorgängen.

Total Errors (Gesamtfehlerzahl) – Die Gesamtanzahl aller Übertragungsfehler bei Sendevorgängen.

Data Rate (Mb/s) (Datenrate, Mbit/s) – Gibt die Geschwindigkeit an, mit der die Daten empfangen werden.

Receive Error Rate (Errors/sec) (Empfangsfehlerrate, (Fehler/Sek.) – Die Anzahl der Übertragungsfehler pro Sekunde bei Empfangsvorgängen.

Total Errors (Gesamtfehlerzahl) – Die Gesamtanzahl aller Übertragungsfehler bei Empfangsvorgängen.

Anzeigen von Stack-Port-Zählern

1. Öffnen Sie die Seite **Stack Port Counters** (Stack-Port-Zähler).

Anzeigen von Stack-Port-Zählern mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- System Management Commands (System-Management-Befehle)

Stack-Port-Diagnose

Die Seite **Stack Port Diagnostics** (Stack-Port-Diagnose) ist ausschließlich für Field Application Engineers (FAEs) und Entwickler vorgesehen.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Konfigurieren der Funktionsmerkmale IP-Telefon und Access Point-Support

Benutzerhandbuch für die Dell™ PowerConnect™ 6200-Reihe

- Konfigurieren der Stromversorgung über Ethernet (PoE)
- Konfigurieren von LLDP (Link Layer Discovery Protocol) für Medien-Endpoint-Geräte
- Konfigurieren von Ports für Voice-VLAN

Dieser Abschnitt beschreibt die folgenden auf dem System verfügbaren Merkmale für IP-Telefonie und Access-Point-Support:

- Konfigurieren der Stromversorgung über Ethernet (PoE)
- Konfigurieren von LLDP (Link Layer Discovery Protocol) für Medien-Endpoint-Geräte
- Konfigurieren von Ports für Voice-VLAN

Konfigurieren der Stromversorgung über Ethernet (PoE)

Die Stromversorgung über Ethernet (PoE = Power over Ethernet) versorgt Geräte über eine vorhandene LAN-Verkabelung mit Strom, ohne dass eine Aktualisierung oder Änderung der Netzwerkinfrastruktur erforderlich ist. Bei der Nutzung von PoE brauchen Netzwerkgeräte nicht in der Nähe von Stromquellen aufgestellt zu werden. Für die Stromversorgung über Ethernet sind unter anderem folgende Gerätearten geeignet: IP-Telefonie, Wireless Access Points, IP-Gateways, PDAs sowie Geräte zur optischen und akustischen Überwachung über Netzwerk.

Im vorliegenden Abschnitt werden die Optionen erläutert, die auf der Menüseite **System→ General (Allgemein)→ Power Over Ethernet** (Stromversorgung über Ethernet) verfügbar sind. Unter anderem sind dies Optionen für die Konfiguration und Anzeige von PoE-Daten für das System oder für jede Schnittstelle. Von der Menüseite **Power Over Ethernet**(Stromversorgung über Ethernet) aus kann auf diese Optionen über die folgenden Menüseiten zugegriffen werden:

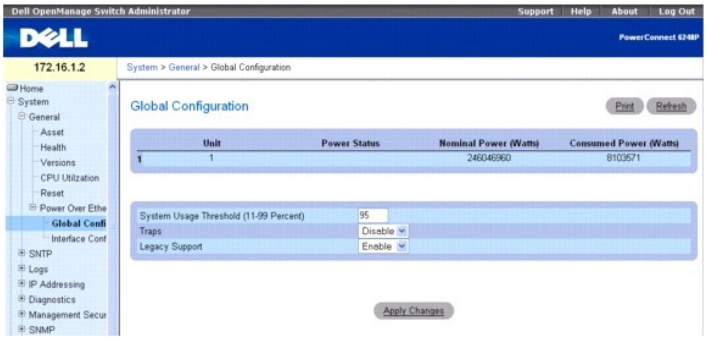
- Konfigurieren der Stromversorgung über Ethernet (PoE)
- Schnittstellenkonfiguration

Globale Konfiguration

Verwenden Sie die Seite **Global Configuration** (Globale Konfiguration), um PoE-Parameter wie Systemnutzung, Traps und PoE-Unterstützung für ältere Geräte systemweit zu konfigurieren und festzulegen.

Um die Seite anzuzeigen, klicken Sie in der Strukturansicht auf **System→ General (Allgemein)→ Power Over Ethernet→ Globale Configuration (Globale Konfiguration)**.

Abbildung 7-1. Globale Konfiguration



Die Seite **Global Configuration** (Globale Konfiguration) enthält folgende Felder:

Unit (Einheit) – Zeigt die Kennung für die Einheit im Stack an.

Power Status (Netzstatus) – Der Betriebsstatus des integrierten Netzteils.

Nominal Power (Nennleistung) – Die Nennleistung des integrierten Netzteils in Watt.

Consumed Power (Stromverbrauch) – Der gemessene Stromverbrauch in Watt.

System Usage Threshold (Verbrauchsgrenze für System) – Der (in Prozent angegebene) Verbrauchsgrenzwert wird mit dem gemessenen Stromverbrauch verglichen. Wenn er überschritten wird, wird eine Alarmnachricht verschickt.

Traps – Gibt an, ob die integrierten Strom-Traps aktiviert oder deaktiviert sind.

Legacy Support (Unterstützung älterer Geräte) – Aktiviert oder deaktiviert die Unterstützung älterer PoE-Geräte.

Konfiguration globaler PoE-Einstellungen

1. Öffnen Sie die Seite **Global Configuration** (Globale Konfiguration).
2. Konfigurieren Sie die Verbrauchsgrenze für das System, Traps oder die Unterstützung älterer PoE-Geräte.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Systemparameter werden angewendet, und das Gerät wird aktualisiert.

Konfigurieren der Stromversorgung über Ethernet mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

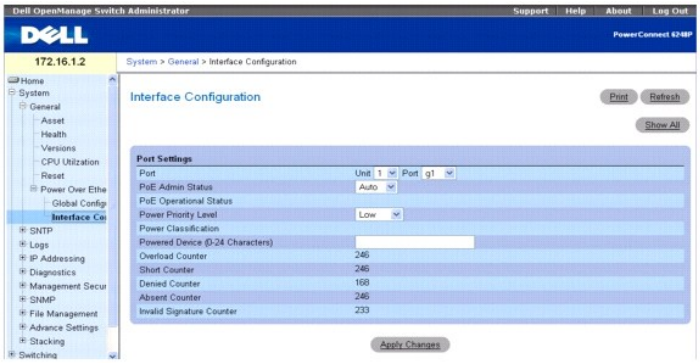
- Power Over Ethernet Commands (PoE-Befehle)

Schnittstellenkonfiguration

Verwenden Sie die Seite **Interface Configuration** (Schnittstellenkonfiguration), um die PoE-Parameter für die einzelnen Ports zu konfigurieren.

Um die Seite anzuzeigen, klicken Sie in der Strukturansicht auf **System→ General (Allgemein)→ Power Over Ethernet→ Interface Configuration (Schnittstellenkonfiguration)**.

Abbildung 7-2. Schnittstellenkonfiguration



Die Seite **Interface Configuration** (Schnittstellenkonfiguration) enthält folgende Felder:

Ports – Legt die Einheit und den Port fest, für die Portparameter definiert werden.

PoE Admin Status – Legt fest, ob die Stromversorgung über diesen Port aktiviert ist.

Auto – Der Port versorgt ein angeschlossenes, PoE-fähige Gerät automatisch mit Strom.

Never (Nie) – Der Port versorgt angeschlossene Geräte nicht mit Strom.

PoE Operational Status (PoE-Betriebsstatus) – Beschreibt den Betriebsstatus der integrierten Stromversorgung des Ports. Dabei kann es sich um eine der folgenden Betriebsstatusangaben handeln:

Off (Aus) – Zeigt an, dass keine Stromversorgung erfolgt.

On (Ein) – Zeigt an, dass das angeschlossene Gerät Strom bezieht.

Test-Fail (Testfehler) – Zeigt an, dass ein Problem am Port vorliegt.

Testing (Test läuft) – Zeigt an, dass sich der Port im Testmodus befindet.

Fault (Ausgefallen) – Zeigt an, dass der Port aufgrund einer Fehlerbedingung inaktiv ist.

Searching (Suche) – Zeigt an, dass keine der oben genannten Statusangaben auf den Port zutrifft.

Power Priority Level (Stromprioritätsstufe) – Die Priorität des Ports von der integrierten Stromverwaltung aus gesehen. Dabei kann es sich um eine der folgenden Stromversorgungs-Prioritätsstufen handeln:

- Critical (Höchste Priorität)
- High (Hohe Priorität)
- Low (Geringe Priorität)

Power Classification (Stromklassifizierung) – Die Stromverbrauchsklasse des versorgten Geräts. Dabei kann es sich um eine der folgenden Stromversorgungsklassen handeln:

- Klasse 0 (0,44–12,95)
- Klasse 1(0,44–3,84)
- Klasse 2(3,84–6,49)
- Klasse 3(6,49–12,95).

Powered Device (Versorgtes Gerät) – Beschreibung des mit Strom versorgten Geräts (bis zu 24 Zeichen).

Overload Counter (Überlast-Zähler) – Zählt die Anzahl der ermittelten Überlast-Bedingungen.

Short Counter (Kurzschluss-Zähler) – Zählt die Anzahl der ermittelten Kurzschluss-Bedingungen.

Denied Counter (Sperrzähler) – Zählt die Fälle, in denen die Stromversorgung gesperrt wurde.

Absent Counter (Ausfallzähler) – Zählt die Fälle, in denen die Stromversorgung unterbrochen wurde, weil ein Ausfall des mit Strom versorgten Gerätes erkannt wurde.

Invalid Signature Counter (Zähler für ungültige Signaturen) – Zählt die Fälle, in denen am versorgten Gerät eine ungültige Signatur erkannt wurde.

Konfigurieren der Stromversorgung über Ethernet (PoE) für eine Schnittstelle

1. Öffnen Sie die Seite **Interface Configuration** *(Schnittstellenkonfiguration)*.
2. Wählen Sie die zu konfigurierende Einheit und den Port aus.
3. Konfigurieren Sie den Administrationsstatus, die Stromversorgungspriorität und den Namen des über den Port mit Strom versorgten Geräts.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

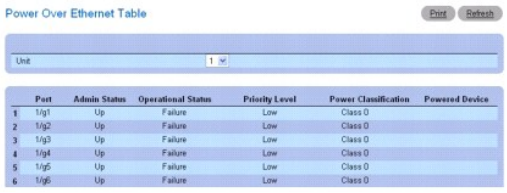
   Die Systemparameter werden angewendet, und das Gerät wird aktualisiert.

Tabelle für Stromversorgung über Ethernet anzeigen

1. Öffnen Sie die Seite **Interface Configuration** (Schnittstellenkonfiguration).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **Power Over Ethernet Table** (Tabelle für Stromversorgung über Ethernet) wird angezeigt. Sie enthält eine Übersicht der PoE-Daten für alle Schnittstellen:

Abbildung 7-3. Tabelle für Stromversorgung über Ethernet



Konfigurieren der Stromversorgung über Ethernet mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Power Over Ethernet Commands (PoE-Befehle)

Konfigurieren von LLDP (Link Layer Discovery Protocol) für Medien-Endpoint-Geräte

Der Standard IEEE 802.1AB, der das LLDP-Protokoll (Link Layer Discovery Protocol) beschreibt, formalisiert die Erkennung und den Abruf der Funktionen der Elemente in einem Datennetzwerk in einer LAN/MAN-Umgebung. Die ausgetauschten Informationen werden in MIBs gespeichert und können von einem Netzwerkmanagementsystem (NMS) wie SNMP abgerufen werden. Dieses Framework ist erweiterbar und kann in Bereichen wie VoIP-Netzwerken umfassend eingesetzt werden.

Das LLPD-MED-Protokoll (Link Layer Discovery Protocol for Media Endpoint Devices) erweitert den LLDP-Standard um Funktionen für Netzwerkkonfiguration und -richtlinien, Geräteaufstellung, Verwaltung der Stromversorgung über Ethernet und Inventarmanagement.

LLDP-MED nutzt die spezifischen, organisatorischen TLV-Erweiterungen von LLDP und definiert neue TLVs, die die Bereitstellung von VoIP-Diensten in verkabelten oder kabellosen LAN/MAN-Umgebungen erleichtern. Zudem sind einige in LLDP optionale TLVs als obligatorisch definiert, und von der Übertragung einiger TLVs wird abgeraten.

Da LLDP-MED das LLDP-Framework nutzt, ist es an die Anforderungen der ursprünglichen Spezifikation gebunden. Rahmenformat, Einschränkungen und Implikationen bleiben unverändert erhalten.

Die TLVs dienen nur zur Weitergabe von Informationen; sie werden nicht automatisch in Konfigurationseinstellungen umgewandelt. Externe Anwendungen können die MED-MIB abfragen und Management-Aktionen zur Funktionskonfiguration durchführen.

Die Menüseite **LLDP-MED** enthält Links zu folgenden Themen:

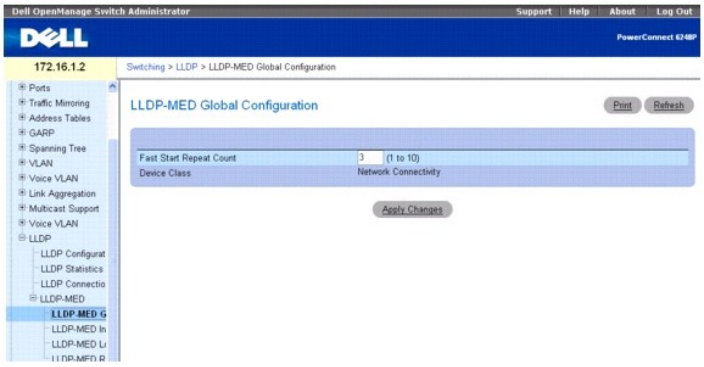
- Globale LLDP-MED-Konfiguration
- LLDP-MED-Schnittstellenkonfiguration
- LLDP-MED-Informationen für lokale Geräte
- LLDP-MED-Informationen für Remote-Geräte

Globale LLDP-MED-Konfiguration

Verwenden Sie die Seite **LLDP-MED Global Configuration** (Globale LLDP-MED-Konfiguration), um die LLDP-MED-Parameter anzuzeigen oder zu ändern, die sich auf das gesamte System auswirken.

Um die Seite **LLDP-MED Global Configuration** (Globale LLDP-MED-Konfiguration) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ LLDP→ *LLDP-MED→ LLDP-MED Global Configuration*** **(Globale LLDP-MED-Konfiguration)**.

Abbildung 7-4. Globale LLDP-MED-Konfiguration



Die Seite ***LLDP-MED Global Configuration*** (Globale LLDP-MED-Konfiguration) enthält folgende Felder:

Fast Start Repeat Count – (Schnellstart-Wiederholungszähler) – Legt die Anzahl der LLDP-PDUs fest, die bei Aktivierung des Protokolls übertragen werden. Der Wertebereich reicht von 1 bis 10. Der Standardwert für den Schnellstart-Wiederholungszähler ist 4.

Device Class (Geräteklasse) – Legt die MED-Klassifizierung des lokalen Geräts fest. Es gibt vier unterschiedliche Gerätearten. Drei davon sind für die tatsächlichen Endpunkte reserviert (Klasse I Allgemein [z. B. IP-Kommunikationscontroller], Klasse II Medien [z. B. Conference Bridge], Klasse III Kommunikation [z. B. IP-Telefone]). Die vierte Geräteart sind Netzwerkkonnektivitätsgeräte. In der Regel handelt es sich dabei um LAN Switches/Router, IEEE 802.1-Bridges, IEEE 802.11 Wireless Access Points usw.

Ändern der globalen LLDP-MED-Konfiguration

1. Öffnen Sie die Seite ***LLDP Configuration*** (LLDP-Konfiguration).
2. Geben Sie unter "Fast Start Repeat Count" (Schnellstart-Wiederholungszähler) einen neuen Wert ein.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die LLDP-MED-Parameter werden im Switch gespeichert.

Konfigurieren globaler LLDP-MED-Einstellungen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

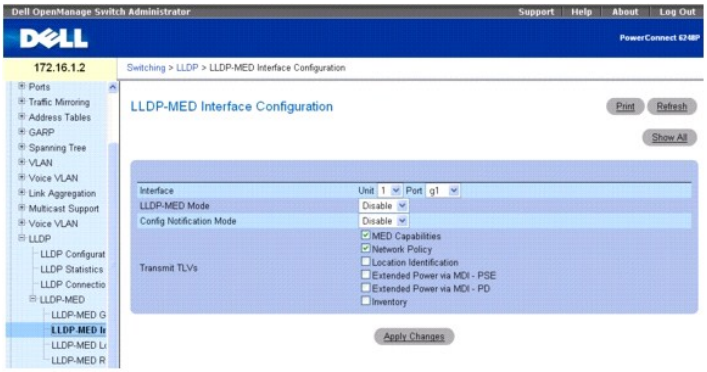
- LLDP Commands (LLDP-Befehle)

LLDP-MED-Schnittstellenkonfiguration

Verwenden Sie die Seite **LLDP-MED Interface Configuration** (LLDP-MED-Schnittstellenkonfiguration), um LLDP-MED-Parameter für eine bestimmte Schnittstelle festzulegen.

Um die Seite **LLDP-MED Interface Configuration** (LLDP-MED-Schnittstellenkonfiguration) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching**→ **LLDP**→ ***LLDP-MED***→ ***LLDP-MED*** **Interface Configuration** ***(LLDP-MED-Schnittstellenkonfiguration)***.

Abbildung 7-5. LLDP-MED-Schnittstellenkonfiguration



Die Seite ***LLDP-MED Interface Configuration*** (LLDP-MED-Schnittstellenkonfiguration) enthält folgende Felder:

Interface (Schnittstelle) – Legt die Liste der Ports fest, an denen LLDP-MED - 802.1AB konfiguriert werden kann. Wählen Sie in der Dropdown-Liste **Ports** die Option **All** (Alle), um für alle Schnittstellen des Systems dieselben LLDP-MED-Einstellungen zu konfigurieren.

ANMERKUNG: Wenn Sie im Feld **Port** die Option **All** (Alle) auswählen, werden der Modus LLDP-MED und der Modus Notification (Benachrichtigung) als "Disabled" (Deaktiviert) angezeigt, und alle "Transmit TLVs"-Kontrollkästchen (TLVs übertragen) werden gelöscht. Dies geschieht selbst dann, wenn Sie für alle Ports dieselben Einstellungen konfigurieren. Um die LLDP-MED-Einstellungen für eine oder alle Schnittstellen anzuzeigen, wählen Sie eine bestimmte Schnittstelle aus, oder klicken Sie auf **Show All** (Alle anzeigen).

LLDP-MED Mode (LLPD-MED-Modus) – Legt den LLDP-MED-Modus für die gewählte Schnittstelle fest. Mit der Aktivierung von MED wird faktisch die Übertragungs- und -Empfangsfunktion von LLDP aktiviert.

Config Notification Mode (Benachrichtigungsmodus konfigurieren) – Legt den LLDP-MED-Topologie-Benachrichtigungsmodus für die ausgewählte Schnittstelle fest.

Transmit TLVs (TLVs übertragen) – Legt fest, welche optionalen Typen/Längen/Wert-Sätze (TLVs = Type Length Values) im LLDP-MED an die LLDP PDU-Frames für die ausgewählte Schnittstelle übertragen werden.

MED Capabilities (MED-Funktionen) – Dient zur Übertragung des Funktionen-TLV in LLDP-Frames.

Network Policy: (Netzwerkrichtlinie) – Dient zur Übertragung der Netzwerkrichtlinie an LLDP-Frames.

Location Identification (Standorterkennung) – Dient zur Übertragung des Standort-TLV in LLDP-Frames.

Extended Power via MDI - PSE (Erweiterte Stromversorgung über MDI - PSE) – Dient zur Übertragung des Erweiterte-PSE-TLV in LLDP-Frames.

Extended Power via MDI - PD (Erweiterte Stromversorgung über MDI - PD) – Dient zur Übertragung des Erweiterte-PD-TLV in LLDP-Frames.

Inventory (Inventar) – Dient zur Übertragung des Inventar-TLV in LLDP-Frames.

Ändern der LLDP-MED-Schnittstellenkonfiguration

1. Öffnen Sie die Seite ***LLDP Configuration*** (LLDP-Konfiguration).
2. Geben Sie die Einheit an, und wählen Sie entweder einen zu konfigurierenden Port aus, oder wählen Sie "All" (Alle), um alle Ports mit denselben Einstellungen zu konfigurieren.
3. Konfigurieren Sie die LLDP-MED-Einstellungen für die Schnittstelle oder die Schnittstellen
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die LLDP-MED-Parameter werden im Switch gespeichert.

   ANMERKUNG: Wenn Sie **All** (Alle) gewählt haben, um alle Ports zu konfigurieren, werden die von Ihnen vorgenommenen Einstellungen nach dem Aktualisieren der Seite nicht angezeigt. Um die LLDP-MED-Einstellungen für eine oder alle Schnittstellen anzuzeigen, wählen Sie eine bestimmte Schnittstelle aus, oder klicken Sie auf **Show All** (Alle anzeigen).

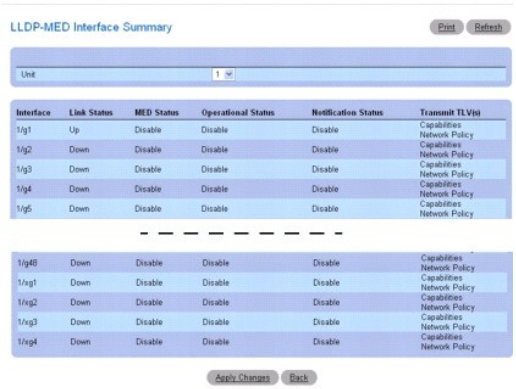
Anzeigen der Schnittstellenzusammenfassung

1. Öffnen Sie die Seite **LLDP-MED Interface Configuration** (LLDP-MED-Schnittstellenkonfiguration).

2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **LLDP-MED Interface Summary** (LLDP-MED-Schnittstellenzusammenfassung) wird angezeigt. Sie enthält zusammenfassende LLDP-MED-Daten zu allen Schnittstellen:

Abbildung 7-6. LLDP-MED-Schnittstellenzusammenfassung



Konfigurieren globaler LLDP-MED-Schnittstelleneinstellungen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

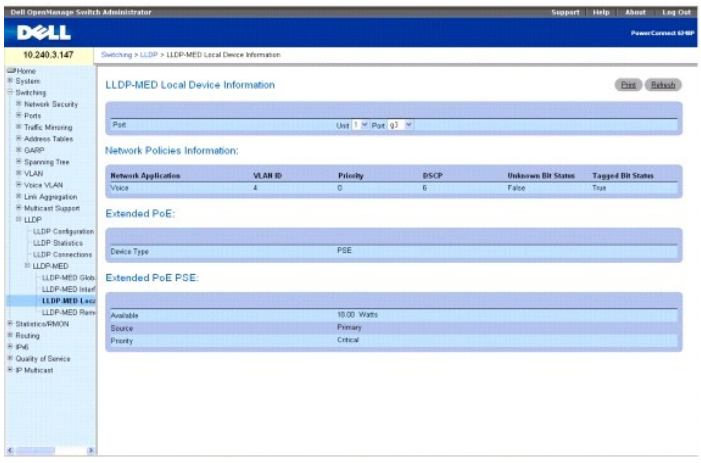
- LLDP Commands (LLDP-Befehle)

LLDP-MED-Informationen für lokale Geräte

Verwenden Sie die Seite **LLDP-MED Local Device Information** (LLDP-MED-Informationen für lokale Geräte), um die angekündigten lokalen LLDP-Daten für jeden Port anzuzeigen.

Um die Seite **LLDP-MED Local Device Information** *(LLDP-MED-Informationen für lokale Geräte)* anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ LLDP→ *LLDP-MED*→ *LLDP-MED* Local Device Information (LLDP-MED-Informationen für lokale Geräte)**.

Abbildung 7-7. LLDP-MED-Informationen für lokale Geräte



Die Seite **LLDP-MED Local Device Information** (LLDP-MED-Informationen für lokale Geräte) enthält folgende Felder:

Port – Wählen Sie die Einheit und den gewünschten Port aus, um die vom Port angekündigten lokalen LLDP-Daten anzuzeigen. Die Dropdown-Liste zur Portauswahl zeigt nur die Ports an, bei denen LLDP-MED aktiviert ist.

Network Policies Information (Informationen zu Netzwerkrichtlinien) – Wenn in den LLDP-Frames ein Netzwerkrichtlinien-TLV vorhanden ist, werden die folgenden Informationen angezeigt:

Network Application (Netzwerkanwendung) – Legt den Typ der vom lokalen Gerät in der Richtlinie festgelegten Medienanwendung fest. Ein Port kann

einen oder mehrere der folgenden Anwendungstypen empfangen:

- unknown
- voicesignaling
- guestvoice
- guestvoicesignalling
- softphonevoice
- videoconferencing
- streamingvideo
- videosignalling

Vlan Id (VLAN-Kennung) – Gibt die mit einem bestimmten Richtlinientyp verknüpfte VLAN-Kennung an.

Priority (Priorität) – Gibt die mit einem bestimmten Richtlinientyp verknüpfte Priorität an.

DSCP (DSCP) – Gibt den mit einem bestimmten Richtlinientyp verknüpften DSCP (Diff Serv Code Point) an.

Unknown Bit Status (Unbekanntes-Bit-Status) – Gibt das mit einem bestimmten Richtlinientyp verknüpfte unbekannte Bit an.

Tagged Bit Status (Tagged-Bit-Status) – Gibt das mit einem bestimmten Richtlinientyp verknüpfte Tagged Bit an.

Inventory(Inventar) – Wenn in LLDP-Frames ein Inventar vorhanden ist, werden folgende Informationen angezeigt:

Hardware Revisions (Hardwareversionen) – Gibt die Hardwareversion an.

Firmware Revisions (Firmwareversionen) – Gibt die Firmwareversion an.

Software Revisions (Softwareversionen) – Gibt die Softwareversion an.

Serial Number (Seriennummer) – Gibt die Seriennummer an.

Manufacturer Name (Herstellername) – Gibt den Herstellernamen an.

Model Name (Modellbezeichnung) – Gibt die Modellbezeichnung an.

Asset ID (Bestandskennung) – Gibt die Bestandskennung an.

Location Information (Standortinformation) – Wenn in LLDP-Frames ein Standort-TLV vorhanden ist, werden folgende Informationen angezeigt:

Sub Type (Untertyp) – Gibt den Typ der Standortinformation an.

Location Information (Standortinformation) – Gibt die Standortinformation als Zeichenkette für den festgelegten Standortkennungstyp an.

Extended PoE (Erweiterte Stromversorgung über Ethernet) – Wenn das lokale Gerät ein PoE-Gerät ist, werden folgende Informationen angezeigt:

Device Type (Gerätetyp) – Gibt den Typ des versorgten Geräts an.

Extended PoE PSE (Erweiterte PoE-PSE) – Wenn im LLDP-Frame ein Erweiterte-PSE-TLV vorhanden ist, werden folgende Informationen angezeigt:

Available (Verfügbar) – Gibt den Stromwert des verfügbaren Netzteils in Zehntelwatt am Port des lokalen Geräts an.

Source (Stromquelle) – Gibt die Stromquelle für den betreffenden Port an.

Priority(Priorität) – Gibt die Strompriorität für den PSE-Port an.

Extended PoE PD (Erweiterte PoE-PD) – Wenn im LLDP-Frame ein Erweiterte-PD-TLV vorhanden ist, werden folgende Informationen angezeigt:

Required (Erforderlich) – Gibt den erforderlichen Netzteil-Stromwert in Zehntelwatt am Port des lokalen Geräts an.

Source (Stromquelle) – Gibt die Stromquelle für den betreffenden Port an.

Priority(Priorität) – Gibt die Strompriorität für den PD-Port an.

LLDP-MED-Informationen für lokale Geräte mithilfe von CLI-Befehlen anzeigen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- LLDP Commands (LLDP-Befehle)

LLDP-MED-Informationen für Remote-Geräte

Verwenden Sie die Seite **LLDP-MED Remote Device Information** (LLDP-MED-Informationen für Remote-Geräte), um die von Remote-Geräten angekündigten LLDP-Daten anzuzeigen.

Um die Seite **LLDP-MED Remote Device Information** *(LLDP-MED-Informationen für Remote-Geräte)* anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ LLDP→ *LLDP-MED*→ *LLDP-MED* Remote Device Information (LLDP-MED-Informationen für Remote-Geräte)**.

Abbildung 7-8. LLDP-MED-Informationen für Remote-Geräte

Die Seite **LLDP-MED Remote Device Information** (LLDP-MED-Informationen für Remote-Geräte) enthält folgende Felder:

Local Interface (Lokale Schnittstelle) – Gibt die Liste aller Ports an, an denen LLDP-MED aktiviert ist.

Capability Information (Funktionsinformationen) – Führt alle unterstützten und aktivierten Funktionen auf, die im MED-TLV an diesem Port empfangen wurden.

Supported Capabilities (Unterstützte Funktionen) – Führt die unterstützten Funktionen auf, die im MED TLV an diesem Port empfangen wurden.

Enabled Capabilities (Aktivierte Funktionen) – Führt die aktivierten Funktionen auf, die im MED TLV an diesem Port empfangen wurden.

Device Class (Geräteklasse) – Gibt die von dem über Remote-Verbindung an den Port angeschlossenen Gerät angekündigte Geräteklasse an.

Network Policy Information (Informationen zu Netzwerkrichtlinien) – Wenn in den LLDP-Frames an diesem Port ein Netzwerkrichtlinien-TLV empfangen wird, werden folgende Informationen angezeigt:

Network Application (Netzwerkanwendung) – Legt den Typ der vom lokalen Gerät in der Richtlinie festgelegten Medienanwendung fest. Ein Port kann einen oder mehrere der folgenden Anwendungstypen empfangen:

- unknown
- voicesignaling
- guestvoice
- guestvoicesignalling
- softphonevoice
- videoconferencing
- streamingvideo
- videosignalling

Vlan Id (VLAN-Kennung) – Gibt die mit einem bestimmten Richtlinientyp verknüpfte VLAN-Kennung an.

Priority (Priorität) – Gibt die mit einem bestimmten Richtlinientyp verknüpfte Priorität an.

DSCP (DSCP) – Gibt den mit einem bestimmten Richtlinientyp verknüpften DSCP (Diff Serv Code Point) an.

Unknown Bit Status (Unbekanntes-Bit-Status) – Gibt das mit einem bestimmten Richtlinientyp verknüpfte unbekannte Bit an.

Tagged Bit Status (Tagged-Bit-Status) – Gibt das mit einem bestimmten Richtlinientyp verknüpfte Tagged Bit an.

Inventory(Inventar) – Wenn in LLDP-Frames ein Inventar vorhanden ist, werden folgende Informationen angezeigt:

Hardware Revisions (Hardwareversionen) – Gibt die Hardwareversion des Remote-Geräts an.

Firmware Revisions (Firmwareversionen) – Gibt die Firmwareversion des Remote-Geräts an.

Software Revisions (Softwareversionen) – Gibt die Softwareversion des Remote-Geräts an.

Serial Number (Seriennummer) – Gibt die Seriennummer des Remote-Geräts an.

Manufacturer Name (Herstellername) – Gibt den Herstellernamen des Remote-Geräts an.

Model Name (Modellbezeichnung) – Gibt die Modellbezeichnung des Remote-Geräts an.

Asset ID (Bestandskennung) – Gibt die Bestandskennung des Remote-Geräts an.

Location Information (Standortinformation) – Wenn in LLDP-Frames ein Standort-TLV vorhanden ist, werden folgende Informationen angezeigt:

Sub Type (Untertyp) – Gibt den Typ der Standortinformation an.

Location Information (Standortinformation) – Gibt die Standortinformation als Zeichenkette für den festgelegten Standortkennungstyp an.

Extended PoE (Erweiterte Stromversorgung über Ethernet) – Gibt an, ob das Remote-Gerät PoE-fähig ist.

Device Type (Gerätetyp) – Gibt den Gerätetyp des mit diesem Port verbundenen Remote-Geräts an.

Extended PoE PSE (Erweiterte PoE-PSE) – Wenn im LLDP-Frame ein Erweiterte-PSE-TLV eingeht, werden folgende Informationen angezeigt:

Available (Verfügbar) – Gibt den PSE-Stromwert des Remote-Ports in Zehntelwatt an.

Source (Stromquelle) – Gibt die PSE-Stromquelle des Remote-Ports an.

Priority (Priorität) – Gibt die PSE-Strompriorität des Remote-Ports an.

Extended PoE PD (Erweiterte PoE-PD) – Wenn im LLDP-Frame ein Erweiterte-PD-TLV eingeht, werden folgende Informationen angezeigt:

Required (Erforderlich) – Gibt die Stromanforderungen des Remote-Ports an.

Source (Stromquelle) – Gibt die Stromquelle des Remote-Ports an.

Priority (Priorität) – Gibt die PD-Strompriorität des Remote-Ports an.

LLDP-MED-Informationen für Remote-Geräte mithilfe von CLI-Befehlen anzeigen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- LLDP Commands (LLDP-Befehle)

Konfigurieren von Ports für Voice-VLAN

Die Voice-VLAN-Funktion ermöglicht Switch-Ports, Telefoniedaten mit einer festgelegten Prioritätsstufe zu übermitteln. Über die Prioritätsstufe kann der am Port eingehende Telefonverkehr separat vom übrigen Datenverkehr behandelt werden. Ein wichtiger Vorteil eines Voice-VLANs besteht darin, dass die Tonqualität eines IP-Telefons bei hohem Datenverkehr am Port nicht beeinträchtigt wird. Das System nutzt die MAC-Quelladresse des durch den Port laufenden Datenverkehrs zur Erkennung der IP-Telefoniedaten.

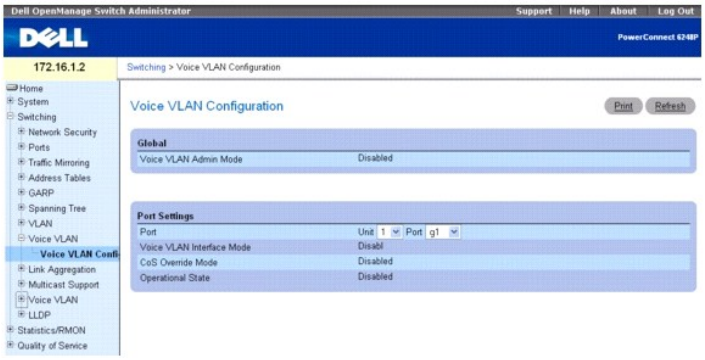
Die Seite **Voice VLAN** (Voice-VLAN) enthält einen Link zur Konfiguration der globalen und portspezifischen Voice-VLAN-Einstellungen.

Voice-VLAN-Konfiguration

Verwenden Sie die Seite **Voice VLAN Configuration** (Voice-VLAN-Konfiguration), um Voice-VLAN-Einstellungen für das gesamte System und für bestimmte Schnittstellen anzuzeigen und zu konfigurieren.

Um die Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Voice VLAN (Voice-VLAN)→ Voice VLAN Configuration (Voice-VLAN-Konfiguration)**.

Abbildung 7-9. Voice-VLAN-Konfiguration



Die Seite **Voice VLAN Configuration** (Voice-VLAN-Konfiguration) enthält folgende Felder:

Voice VLAN Admin Mode (Admin-Modus für Voice-VLAN) – Der Voice-VLAN-Administrationsmodus wird über das Dropdown-Menü ausgewählt. Die Standardeinstellung ist Disable (Deaktivieren).

Port – Wählen Sie die Schnittstelle aus, die angezeigt oder konfiguriert werden soll.

Voice VLAN Interface Mode (Voice-VLAN-Modus für Schnittstelle) – Wählen Sie den Voice-VLAN-Modus für die gewählte Schnittstelle aus. Die Standardeinstellung ist Disable (Deaktivieren). Folgende Modi stehen zur Auswahl:

Disable (Deaktivieren) – Voice-VLAN an diesem Port deaktivieren.

None (Keiner) – Das IP-Telefon kann nicht gekennzeichnete Voice-Daten gemäß seiner eigenen Konfiguration übermitteln.

VLAN ID (VLAN-Kennung) – VLAN-Kennzeichnung für Voice-Datenverkehr konfigurieren. Der VLAN-Kennungsbereich reicht von 1 bis 4093.

dot1p – Voice-VLAN 802.1p-Prioritätskennung für Voice-Datenverkehr konfigurieren. Der Prioritätskennungsbereich reicht von 0 bis 7.

Untagged (Ohne Kennung) – Konfiguriert das Telefon so, dass es nicht gekennzeichneten Datenverkehr übermittelt.

CoS Override Mode (CoS ignorieren) – Aktiviert den Modus "CoS ignorieren" für die gewählte Schnittstelle. Die Standardeinstellung ist Disable (Deaktivieren).

Operational Status (Betriebsstatus) – Der Voice-VLAN-Betriebsstatus an der betreffenden Schnittstelle.

Voice-VLAN-Einstellungen konfigurieren

1. Öffnen Sie die Seite **Voice VLAN Configuration** (Voice-VLAN-Konfiguration).
2. Konfigurieren Sie die Einstellungen für das gesamte System oder für jeden Port einzeln.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Systemparameter werden angewendet, und das Gerät wird aktualisiert.

Konfigurieren des Voice-VLAN mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Voice VLAN Commands (Voice-VLAN-Befehle)

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Konfigurieren von Switching-Informationen

Benutzerhandbuch für die Dell™ PowerConnect™ 6200-Reihe

- Konfigurieren der Netzwerksicherheit
- Konfigurieren von Ports
- Konfigurieren der Datenverkehrsspiegelung
- Konfigurieren von Adresstabellen
- Konfigurieren von GARP
- Konfigurieren des Spanning-Tree-Protokolls
- Konfigurieren von VLANs
- Aggregieren von Ports
- Verwalten der Multicast-Unterstützung
- Konfigurieren von LLDP (Link Layer Discovery Protocol)

In diesem Abschnitt werden alle Systemoperationen sowie allgemeine Informationen im Zusammenhang mit Netzwerksicherheit, Ports, Adresstabellen, GARP, VLANs, Spanning-Tree, Port-Aggregation und Multicast-Unterstützung behandelt.

Die Menüseite **Switching** enthält Links zu folgenden Themen:

- Konfigurieren der Netzwerksicherheit
- Konfigurieren von Ports
- Konfigurieren der Datenverkehrsspiegelung
- Konfigurieren von Adresstabellen
- Konfigurieren von GARP
- Konfigurieren des Spanning Tree-Protokolls
- Konfigurieren von VLANs
- Aggregieren von Ports
- Verwalten der Multicast-Unterstützung
- Konfigurieren von LLDP (Link Layer Discovery Protocol)

Konfigurieren der Netzwerksicherheit

Auf der Menüseite **Network Security** (Netzwerksicherheit) können Sie die Netzwerksicherheit über portbasierte Authentifizierung, gesperrte Ports, Konfiguration von DHCP-Filterung und Zugriffssteuerungslisten einstellen.

Um die Menüseite **Network Security** (Netzwerksicherheit) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Network Security (Netzwerksicherheit)**.

Die Menüseite **Network Security** *(Netzwerksicherheit)* enthält Links zu folgenden Themen:

- Portbasierte Authentifizierung
- Mehrere Hosts
- Authentifizierte Benutzer
- Portsicherheit
- DHCP-Filterung
- Zugriffssteuerungslisten
- Konfiguration von ACL-Verbindungen

Portbasierte Authentifizierung

Im portbasierten Authentifizierungsmodus können, wenn 802.1x global und für den Port aktiviert ist und sich ein beliebiger Bittsteller erfolgreich bei dem Port authentifiziert, alle Benutzer den Port uneingeschränkt nutzen. In diesem Modus kann immer nur ein Bittsteller versuchen, sich zu authentifizieren. In diesem Modus werden die Ports bidirektional gesteuert. Dies ist der Standard-Authentifizierungsmodus.

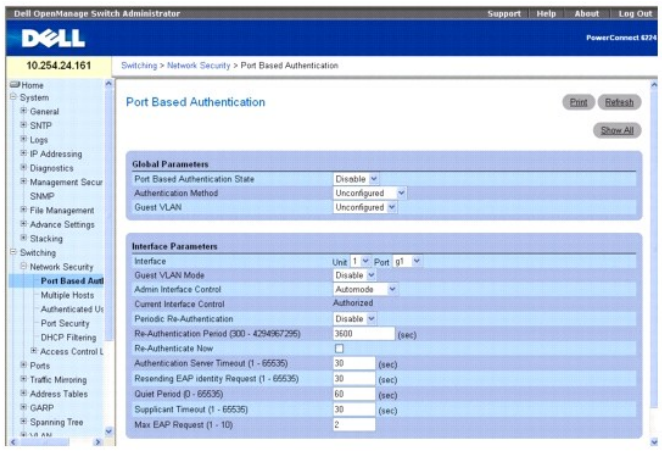
Das 802.1x-Netzwerk besteht aus drei Komponenten:

- **Authentificators** (Authentifizierer) – Bezeichnet den Port, der authentifiziert wird, bevor der Zugriff auf das System zugelassen wird.
- **Supplicants** (Bittsteller) – Bezeichnet den Host, der an den authentifizierten Port angeschlossen ist und den Zugriff auf die Dienste des Systems anfordert.
- **Authentification Server** (Authentifizierungsserver) – Bezeichnet den externen Server, beispielsweise einen RADIUS-Server, der im Namen des Authentifizierers die Authentifizierung durchführt und anzeigt, ob der Benutzer zum Zugriff auf die Dienste des Systems berechtigt ist.

Auf der Seite **Port Based Authentication** (Portbasierte Authentifizierung) können Sie allgemeine 802.1x-Parameter für einen Port konfigurieren.

Um die Seite **Port Based Authentication** (Portbasierte Authentifizierung) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Network Security (Netzwerksicherheit)→ Port Based Authentication (Portbasierte Authentifizierung)**.

Abbildung 8-1. Portbasierte Authentifizierung



Die Seite Port Based Authentication (Portbasierte Authentifizierung) enthält folgende Felder:

Globale Parameter

Port Based Authentication State (Zustand der portbasierten Authentifizierung) – Lässt die portbasierte Authentifizierung für den Switch zu. Die für dieses Feld möglichen Werte sind:

Enable (Aktivieren) – Aktiviert die portbasierte Authentifizierung für den Switch.

Enable (Deaktivieren) – Deaktiviert die portbasierte Authentifizierung für den Switch.

Authentication Method (Authentifizierungsmethode) – Wählt die verwendete Authentifizierungsmethode. Die für dieses Feld möglichen Werte sind:

Unconfigured (Nicht konfiguriert) – Gibt an, dass keine Authentifizierungsmethode gewählt wurde.

None (Keine) – Gibt an, dass keine Authentifizierungsmethode verwendet wird.

RADIUS – Gibt an, dass die Authentifizierung auf dem RADIUS-Server erfolgt.

RADIUS, None (RADIUS, keine) – Gibt an, dass die Authentifizierung auf dem RADIUS-Server erfolgt. Wenn der RADIUS-Server nicht verfügbar ist, wird keine Authentifizierungsmethode verwendet.

None, RADIUS (Keine, RADIUS) – Gibt an, dass keine Authentifizierungsmethode verwendet wird. Wenn eine Authentifizierung erforderlich ist, erfolgt sie auf dem RADIUS-Server.

Guest VLAN (Gast-VLAN) – Spezifiziert ein Gast-VLAN für alle Ports. Die für dieses Feld möglichen Werte sind:

Unconfigured (Nicht konfiguriert) – Gast-VLAN ist nicht für alle Ports konfiguriert.

VLAN ID (VLAN-ID) – Zeigt die ID der im System konfigurierten VLANs. Wählen Sie das als Gast-VLAN für alle Ports zu verwendende VLAN.

Interface Parameters (Schnittstellenparameter)

Interface (Schnittstelle) – Wählt die betroffene Einheit und den betroffenen Port.

Guest VLAN Mode (Gast-VLAN-Modus) – Aktiviert und deaktiviert den Gast-VLAN-Modus für diese Schnittstelle.

Admin Interface Control (Administrierte Schnittstellensteuerung) – Legt den Autorisierungszustand des Ports fest. Die für dieses Feld möglichen Werte sind:

Automode (Automodus) – Erkennt automatisch den Modus der Schnittstelle.

Authorized (Autorisiert) – Versetzt die Schnittstelle ohne Authentifizierung in einen autorisierten Zustand. Die Schnittstelle sendet und empfängt normalen Verkehr, ohne eine portbasierte Authentifizierung des Clients vorzunehmen.

Unauthorized (Nicht autorisiert) – Verweigert der ausgewählten Schnittstelle den Zugang zum System, indem die Schnittstelle in den nicht autorisierten Zustand versetzt wird. Der Switch kann dem Client durch die Schnittstelle keine Authentifizierungsdienste zur Verfügung stellen.

Current Interface Control (Aktuelle Schnittstellensteuerung) – Zeigt den aktuellen Autorisierungszustand des Ports an.

Periodic Re-Authentication (Periodische Reauthentifizierung) – Reauthentifiziert den gewählten Port periodisch.

Reauthentication Period (300-4294967295) (Reauthentifizierungsperiode, 300-4294967295) – Gibt die Zeitspanne an, in der der gewählte Port reauthentifiziert wird. Der Wert des Feldes wird in Sekunden angegeben. Der Standardwert für dieses Feld ist 3600 Sekunden.

Re-Authenticate Now (Jetzt reauthentifizieren) – Erzwingt die sofortige Reauthentifizierung.

Authentication Server Timeout (1-65535) (Zeitüberschreitung für Authentifizierungsserver, 1-65535) – Legt fest, nach welcher Zeitspanne der Switch erneut eine Anfrage an den Authentifizierungsserver versendet. Der Wert des Feldes wird in Sekunden angegeben. Der Standardwert für dieses Feld ist 30

Sekunden.

Resending EAP Identity Request (1-65535) (Erneutes Senden der EAP-Identitätsanforderung, 1-65535) – Legt fest, nach welcher Zeitspanne EAP-Identitätsanforderungen erneut versendet werden. Der Wert des Feldes wird in Sekunden angegeben. Der Standardwert für dieses Feld ist 30 Sekunden.

Quiet Period (0-65535) (Ruheperiode, 0-65535) – Legt fest, nach welcher Zeitspanne der Switch nach einem fehlgeschlagenen Authentifizierungsaustausch im Ruhezustand wartet. Der mögliche Wertebereich für das Feld ist 0 bis 65535. Der Wert wird in Sekunden angegeben. Der Standardwert für dieses Feld ist 60 Sekunden.

Supplicant Timeout (0-65535) (Zeitüberschreitung für Bittsteller, 0-65535) – Gibt an, nach welcher Zeitspanne erneut EAP-Anfragen an den Benutzer versendet werden. Der Wert des Feldes wird in Sekunden angegeben. Der Standardwert für dieses Feld ist 30 Sekunden.

Max EAP Requests (1-10) (Max. EAP-Anfragen, 1-10) – Gibt die maximale Anzahl der EAP-Anfragen an, die der Switch senden kann, bis der Authentifizierungsprozess neu gestartet wird, wenn er keine Antwort erhält. Der mögliche Wertebereich für das Feld ist 1 bis 10. Der Standardwert sind 2 Neuversuche.

Anzeigen der portbasierten Authentifizierungstabelle

1. Öffnen Sie die Seite **Port Based Authentication** (Portbasierte Authentifizierung).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **Port Based Authentication Table** (Portbasierte Authentifizierungstabelle) wird geöffnet, und die linke Seite der Tabelle wird angezeigt:

Abbildung 8-2. Portbasierte Authentifizierungstabelle

3. Um die rechte Seite der Tabelle anzuzeigen, verwenden Sie die horizontale Bildlaufleiste oder klicken Sie auf den Pfeil nach rechts am unteren Bildschirmrand.
4. Über das Dropdown-Menü **Unit** (Einheit) können Sie die **Port Based Authentication Table** (Portbasierte Authentifizierungstabelle) für andere ggf. im Stack vorhandene Einheiten anzeigen.

Reauthentifizieren eines Ports

1. Öffnen Sie die Seite **Port Based Authentication** (Portbasierte Authentifizierung).
2. Markieren Sie **Edit** (Bearbeiten), um die Einheit/den Port für die Reauthentifizierung auszuwählen.
3. Aktivieren Sie **Reauthenticate Now** (Jetzt reauthentifizieren).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der angegebene Port wird reauthentifiziert, und das Gerät wird aktualisiert.

Reauthentifizieren mehrerer Ports in der portbasierten Authentifizierungstabelle

1. Öffnen Sie die Seite **Port Based Authentication** (Portbasierte Authentifizierung).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **Port Based Authentication Table** (Portbasierte Authentifizierungstabelle) wird angezeigt.

3. Markieren Sie **Edit** (Bearbeiten), um die Einheiten/Ports für die Reauthentifizierung auszuwählen.

4. Zur periodischen Reauthentifizierung aktivieren Sie **Periodic Re-Authentication** (Regelmäßige Reauthentifizierung), und legen Sie für alle gewünschten Ports eine **Re-Authentication Period** (Reauthentifizierungsperiode) fest.

5. Zur sofortigen Reauthentifizierung aktivieren Sie für alle gewünschten Ports **Reauthenticate Now** (Jetzt reauthentifizieren).

6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die angegebenen Ports werden (entweder sofort oder periodisch) reauthentifiziert, und das Gerät wird aktualisiert.

Ändern der administrativen Portsteuerung

1. Öffnen Sie die Seite **Port Based Authentication** (Portbasierte Authentifizierung).

2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **Port Based Authentication Table** (Portbasierte Authentifizierungstabelle) wird angezeigt.

3. Blättern Sie zur rechten Seite der Tabelle, und aktivieren Sie für jeden zu konfigurierenden Port das Kontrollkästchen **Edit** (Bearbeiten). Setzen Sie **Admin Port Control** (Administrative Portsteuerung) für die gewählten Ports je nach Bedarf auf **Authorized** (Autorisiert), **Unauthorized** (Nicht autorisiert) oder **Automode** (Automodus). Nur bei Wahl von **Automode** (Automodus) wird dot1x zur Authentifizierung verwendet. Bei Wahl von **Authorized** (Autorisiert) und **Unauthorized** (Nicht autorisiert) wird manuell überschrieben.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die administrative Portsteuerung für die gewählten Ports wird eingestellt, und das Gerät wird aktualisiert.

Aktivieren der portbasierten Authentifizierung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- 802.1X Commands (802.1X-Befehle)

Mehrere Hosts

Für einen Port im Modus **Multiple Hosts** (Mehrere Hosts) muss nur ein einziger Switch authentifiziert werden, damit jeder Switch auf das Netzwerk zugreifen kann. Wenn der Port aus irgendeinem Grund auf **Unauthorized** (Nicht autorisiert) gesetzt wird, verlieren alle Switches ihren Netzwerkzugriff, und der Authentifizierungsprozess muss neu gestartet werden.

Die Seite **Multiple Hosts** (Mehrere Hosts) enthält Angaben zur Definition von erweiterten portbasierten Authentifizierungseinstellungen für bestimmte Ports.

Um die Menüseite **Multiple Hosts** (Mehrere Hosts) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Network Security (Netzwerksicherheit)** → **Multiple Host (Mehrere Hosts)**.

Abbildung 8-3. Mehrere Hosts

Die Seite **Multiple Hosts (Mehrere Hosts) enthält folgende Felder:**

Interface (Schnittstelle) – Gibt die Einheit- und Port-Nummern an, für die erweiterte portbasierte Authentifizierungseinstellungen vorzunehmen sind.

Multiple Hosts (Mehrere Hosts) – Lässt zu oder verhindert, dass ein einzelner Host mehrere Hosts für den Systemzugriff autorisieren kann. Diese Einstellung muss aktiviert sein, damit auf dem gewählten Port Ingress-Filterung deaktiviert oder Portsperren zur Sicherheit verwendet werden können.

Action on Single Host Violation (Aktion bei Verletzung durch einzelnen Host) – Legt fest, wie verfahren wird, wenn im Einzelhostmodus Pakete von einem Host empfangen werden, dessen MAC-Adresse nicht die MAC-Adresse des Clients (Bittstellers) ist. Die für dieses Feld möglichen Werte sind:

Forward (Weiterleiten) – Leitet die von einer unbekannten Quelle stammenden Pakete weiter. Die MAC-Adresse wird jedoch nicht erfasst.

Discard (Ablehnen) – Verwirft die aus einer unbekannten Quelle stammenden Pakete. Dies ist der Standardwert.

Shutdown (Herunterfahren) – Verwirft das aus einer unbekannten Quelle stammende Paket und fährt den Port herunter. Ports bleiben heruntergefahren, bis sie aktiviert werden oder der Switch zurückgesetzt wird.

Traps – Aktiviert oder deaktiviert das Senden von Traps an den Host im Falle einer Sicherheitsverletzung.

Trap Frequency (1-1000000) (Traphäufigkeit, 1-1000000) – Legt das Zeitintervall in Sekunden fest, mit dem Traps an den Host gesendet werden. Der Standardwert ist 10 Sekunden. Das Sicherheitstrap mit Angabe der Anzahl von Verletzungen wird alle 10 Sekunden gesendet.

Status – Zeigt den Hoststatus an. Die für dieses Feld möglichen Werte sind:

Authorized (Autorisiert) – Gibt an, dass der Port sich derzeit im Automodus befindet und Clients vollen Zugriff auf den Port haben.

Unauthorized (Nicht autorisiert) – Gibt an, dass die Portsteuerung auf *Force Unauthorized* (Nicht autorisierten Betrieb erzwingen) steht, keine Verbindung am Port besteht oder die Portsteuerung auf Auto (Automatisch) steht, aber kein Client über den Port authentifiziert wurde.

Not in Auto Mode (Nicht im Automodus) – Gibt an, dass die Portsteuerung auf *Forced Authorized* (Autorisierter Betrieb erzwingen) steht und Clients vollen Zugriff auf den Port haben.

Single-host Lock (Sperre auf einzelnen Host) – Gibt an, dass die Portsteuerung auf *Auto* (Automatisch) steht und über den Port ein einzelner Client authentifiziert wurde.

No Single Host (Kein Einzelhostbetrieb) – Gibt an, dass der Multihostmodus aktiviert ist.

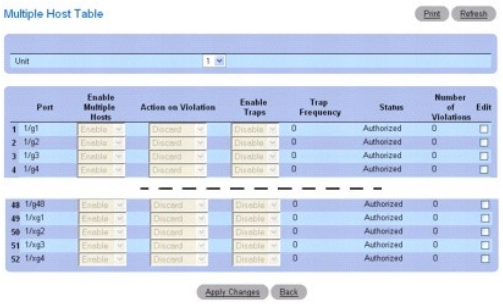
Number of Violations (Anzahl von Verletzungen) – Zeigt die Anzahl der Pakete an, die im Einzelhostmodus an der Schnittstelle eingegangen sind und von einem Host stammen, dessen MAC-Adresse nicht die MAC-Adresse des Clients (Bittstellers) ist.

Anzeigen der Multihosttabelle

1. Öffnen Sie die Seite **Multiple Hosts** (Mehrere Hosts).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **Multiple Host Table** (Multihosttabelle) wird angezeigt.

Abbildung 8-4. Multihosttabelle



3. Über das Dropdown-Menü **Unit** (Einheit) können Sie die **Multiple Host Table** (Multihosttabelle) für andere ggf. im Stack vorhandene Einheiten anzeigen.

Aktivieren/Deaktivieren mehrerer Hosts für einen Port

1. Öffnen Sie die Seite **Multiple Hosts** (Mehrere Hosts).
2. Wählen Sie unter **Interface** (Schnittstelle) die betroffene Einheit und den betroffenen Port.
3. Definieren Sie Variablen je nach Bedarf.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Für den gewählten Port wird der Multihostmodus aktiviert, und das Gerät wird aktualisiert.

Aktivieren/Deaktivieren mehrerer Hosts für mehrere Port

1. Öffnen Sie die Seite **Multiple Hosts** (Mehrere Hosts).

2. Klicken Sie auf **Show All** (Alle anzeigen), um die **Multiple Host Table** (Multihosttabelle) anzuzeigen.
3. Aktivieren Sie für jeden zu konfigurierenden Port das Kontrollkästchen **Edit** (Bearbeiten).
4. Ändern Sie die Variablen der Ports je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die bearbeiteten Ports und das Gerät werden aktualisiert.

Konfigurieren der erweiterten portbasierten Authentifizierung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

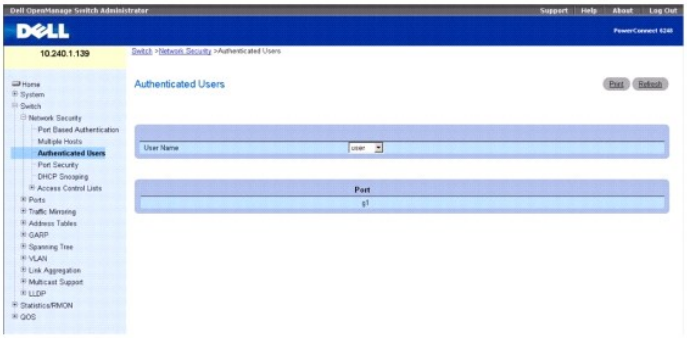
- 802.1X Commands (802.1X-Befehle)

Authentifizierte Benutzer

Die Seite **Authenticated Users** (Authentifizierte Benutzer) zeigt nach Ports aufgeschlüsselte Benutzerzugriffslisten.

Um die Seite **Authenticated Users** (Authentifizierte Benutzer) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Network Security (Netzwerksicherheit)→ Authenticated Users (Authentifizierte Benutzer)**.

Abbildung 8-5. Authentifizierte Benutzer



Die Seite **Authenticated Users** (Authentifizierte Benutzer) enthält folgende Felder:

User Name (Benutzername) – Spezifiziert einen der aufgelisteten Benutzer, die über den RADIUS-Server autorisiert sind.

Port – Listet den zur Authentifizierung verwendeten Port auf.

Anzeigen authentifizierter Benutzer mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- 802.1X Commands (802.1X-Befehle)

Portsicherheit

Portsicherheit kann für einzelne Ports aktiviert werden. Wenn ein Port gesperrt ist, können nur Pakete mit zulässigen MAC-Quelladressen weitergeleitet werden. Alle anderen Pakete werden abgelehnt. Es gibt zwei Methoden, um eine MAC-Adresse als zulässig zu definieren: dynamisch oder statisch. Wenn ein Port gesperrt ist, werden beide Methoden gleichzeitig verwendet.

Beim dynamischen Sperren wird zur Portsicherheit ein First-Arrival-Mechanismus implementiert. Sie legen fest, wie viele Adressen auf dem gesperrten Port erfasst werden können. Solange die Grenze nicht erreicht ist, wird ein Paket mit unbekannter MAC-Quelladresse normal erfasst und weitergeleitet. Sobald die Grenze erreicht ist, werden auf dem Port keine Adressen mehr erfasst. Pakete mit nicht erfassten MAC-Quelladressen werden verworfen. Beachten Sie, dass dynamisches Sperren effektiv deaktiviert werden kann, indem Sie die Anzahl der zulässigen dynamischen Eingaben auf Null setzen.

Durch statisches Sperren können Sie eine Liste der für einen Port zulässigen MAC-Adressen festlegen. Die Pakete verhalten sich wie beim dynamischen Sperren: Nur Pakete mit zulässiger MAC-Quelladresse können weitergeleitet werden.

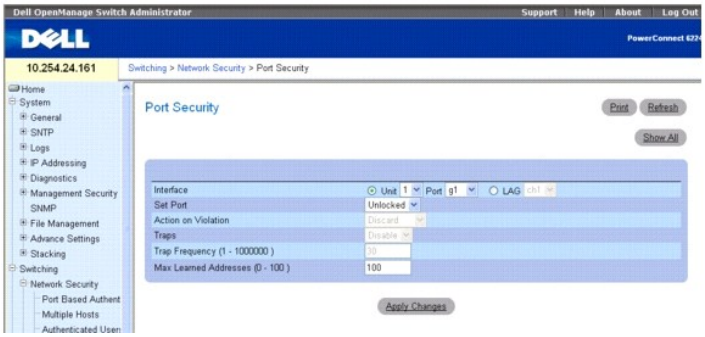
Weitere Informationen zum Anzeigen der auf einem Port erfassten MAC, zum Hinzufügen einer statischen MAC zu einem Port und zum Löschen statischer MAC-Einträge finden Sie unter Konfigurieren von Adresstabellen.

Deaktivierte Ports können nur über die Seite ***Konfigurieren von Ports*** aktiviert werden.

Um die Seite ***Port Security***(Portsicherheit) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Network Security (Netzwerksicherheit)→ Port**

Security (Portsicherheit).

Abbildung 8-6. Portsicherheit



Interface (Schnittstelle) – Wählt die Einheit und den Port oder die LAG, für die Portsicherheitseinstellungen konfiguriert werden sollen.

Set Port (Port einstellen) – Aktiviert die Sperrung des Port / der LAG. Wenn ein Port gesperrt wird, werden alle vom Switch dynamisch auf dem Port erfassten aktuellen Adressen aus der Datenbank gelöscht

Action on Violation (Aktion bei Verletzung) – Gibt an, wie verfahren wird, wenn Pakete auf dem Port bzw. der LAG eingehen. Wenn der Port bzw. die LAG freigegeben ist, ist das Feld grau unterlegt. Mögliche Werte:

Discard (Ablehnen) – Verwirft die aus einer unbekannten Quelle stammenden Pakete. Dies ist der Standardwert.

Forward (Weiterleiten) – Leitet die von einer unbekannten Quelle stammenden Pakete weiter. Die MAC-Adresse wird nicht erfasst.

Shutdown (Herunterfahren) – Verwirft das aus einer beliebigen unbekannten Quelle stammende Paket und sendet ein Trap. Außerdem wird der Ingress-Port deaktiviert.

Traps – Aktiviert oder deaktiviert das Senden eines Traps, wenn ein Paket auf einem gesperrten Port bzw. einer gesperrten LAG empfangen wird.

Trap Frequency (1-1000000) (Traphäufigkeit, 1-1000000) – Legt das zwischen Traps liegende Zeitintervall in Sekunden fest.

Max Learned Addresses (0-100) (Max. erfasste Adressen, 0-100) – Gibt die maximale Anzahl sicherer MAC-Adressen an, die auf einem Port erfasst werden können.

Festlegen einer Portsperre

1. Öffnen Sie die Seite ***Port Security*** (Portsicherheit).
2. Wählen Sie den Typ und die Nummer einer Schnittstelle aus.
3. Wählen Sie im Dropdown-Menü **Set Port** (Port einstellen) **Locked** (Gesperrt).
4. Füllen Sie die übrigen Felder aus.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der gesperrte Port bzw. die gesperrte LAG wird der Portsicherheitstabelle hinzugefügt, und das Gerät wird aktualisiert.

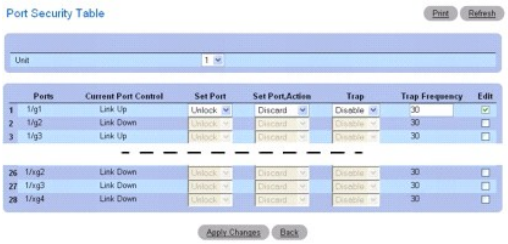
Anzeigen der Portsicherheitstabelle

1. Öffnen Sie die Seite ***Port Security*** (Portsicherheit).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die ***Port Security*** **Table** (Portsicherheitstabelle) wird angezeigt.

Abbildung 8-7. Portsicherheitstabelle



3. Über das Dropdown-Menü **Unit** (Einheit) können Sie die **Port Security Table** (Portsicherheitstabelle) für andere ggf. im Stack vorhandene Einheiten anzeigen.

Festlegen mehrerer Portsperren

1. Öffnen Sie die Seite ***Port Security*** Portsicherheit).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die ***Port Security*** **Table** (Portsicherheitstabelle) wird angezeigt.
3. Klicken Sie für jeden Port, dessen Parameter geändert werden sollen, auf **Edit** (Bearbeiten).
4. Die Felder für diese Ports können jetzt je nach Bedarf bearbeitet werden.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Portsicherheitstabelle wird entsprechend geändert, und das Gerät wird aktualisiert.

Konfigurieren der Portsicherheit mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

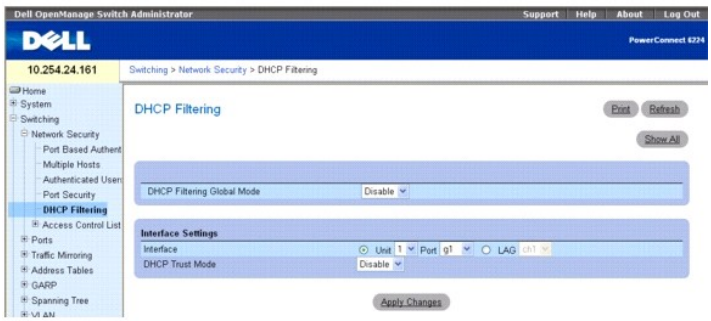
- Address Table Commands (Adresstabellenbefehle)

DHCP-Filterung

Die DHCP-Filterung ist eine nützliche Funktion, die als Sicherheitsmaßnahme gegen nicht autorisierte DHCP-Server verwendet werden kann. Ein bekannter Angriff besteht darin, dass ein nicht autorisierter DHCP-Server einem Client antwortet, der eine IP-Adresse anfordert. Der Server konfiguriert das Gateway für den Client entsprechend der IP-Adresse des Servers. Der Client sendet dann seinen gesamten IP-Datenverkehr, der für andere Netzwerke bestimmt ist, an das nicht autorisierte Gerät. Dadurch kann der Angreifer den Datenverkehr auf Kennwörter durchsuchen oder einen Man-in-the-Middle-Angriff ausführen. Bei der DHCP-Filterung hat der Administrator die Möglichkeit, jeden Port als vertrauenswürdigen oder nicht vertrauenswürdigen Port zu konfigurieren. Der Port mit dem autorisierten DHCP-Server sollte als vertrauenswürdig konfiguriert werden. Auf einem vertrauenswürdigen Port empfangene DHCP-Antworten werden weitergeleitet. Alle anderen Ports sollten als nicht vertrauenswürdig konfiguriert werden. Von DHCP (oder BootP) empfangene Antworten werden abgelehnt.

Um die Seite ***DHCP Filtering*** (DHCP-Filterung) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Network Security (Netzwerksicherheit)→ DHCP Filtering (DHCP-Filterung)**.

Abbildung 8-8. DHCP-Filterung



Die Seite DHCP-Filtering (DHCP-Filterung) enthält folgende Felder:

DHCP Filtering Global Mode (Globaler DHCP-Filterungsmodus) – Schaltet die DHCP-Filterung ein und aus. Die Standardeinstellung ist **Disabled** (Deaktiviert).

Interface (Schnittstelle) – Gibt die betroffene Einheit und den Port oder die betroffene LAG an. Wählen Sie in den Dropdown-Menüs die gewünschte Einheit und den Port für die LAG.

DHCP Trust Mode (Trust-Modus für DHCP) – Aktiviert oder deaktiviert den Trust-Modus. Der Standardwert ist **Disable** (Deaktivieren).

Hinzufügen der DHCP-Filterung

1. Öffnen Sie die Seite **DHCP-Filtering** (DHCP-Filterung).
2. Legen Sie die betroffene **Interface** (Schnittstelle) oder **LAG** fest.
3. Legen Sie die gewünschten Einstellungen für **DHCP Filtering Global Mode** (Globaler DHCP-Filterungsmodus) und **DHCP Filtering Trust Mode** (Trust-Modus für DHCP-Filterung) fest.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Das Gerät wird aktualisiert.

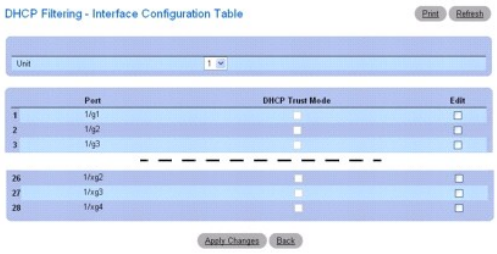
Anzeigen der Schnittstellenkonfigurationstabelle für DHCP-Filterung

1. Öffnen Sie die Seite **DHCP-Filtering** (DHCP-Filterung).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Auf der Seite **DHCP Filtering Table** (DHCP-Filterungstabelle) werden alle Ports, die Einheiten, auf denen sich die Ports befinden, und ihr jeweiliger **DHCP-Trust-Modus** angezeigt.

Abbildung 8-9. Schnittstellenkonfigurationstabelle für DHCP-Filterung



3. Über das Dropdown-Menü **Unit** (Einheit) können Sie die **DHCP Filtering Table** (DHCP-Filterungstabelle) für andere ggf. im Stack vorhandene Einheiten anzeigen.

Konfigurieren von DHCP-Filterung für mehrere Ports

1. Öffnen Sie die Seite ***DHCP-Filtering*** (DHCP-Filterung).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die ***DHCP Filtering Interface Configuration*** **Table** (Schnittstellenkonfigurationstabelle für DHCP-Filterung) wird angezeigt.
3. Klicken Sie für jeden zu konfigurierenden Port auf **Edit** (Bearbeiten).
4. Aktivieren oder deaktivieren Sie das Feld **DHCP Trust Mode** (DHCP-Trust-Modus) für diese Ports je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Schnittstellenkonfigurationstabelle für DHCP-Filterung wird entsprechend geändert, und das Gerät wird aktualisiert.

Konfigurieren von DHCP-Filterung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- DHCP Filtering Commands (Befehle zur DHCP-Filterung)

Konfigurieren von IP-ACLs

Über Zugriffssteuerungslisten (ACL) können Netzwerkverwalter Klassifikationsaktionen und -regeln für bestimmte Ingress-Ports festlegen. Der Switch unterstützt bis zu 100 ACLs. Die Hardwareressourcen sind jedoch begrenzt und können 100 komplett belegte ACLs nicht voll unterstützen.

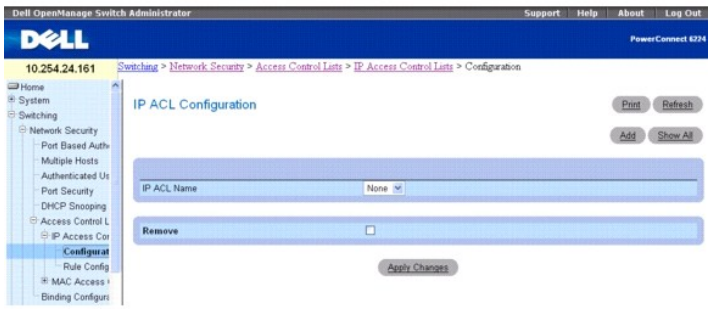
Pakete können auf Ingress gefiltert werden. Wenn die Filterregeln erfüllt sind, können Aktionen wie Verwerfen des Pakets oder Deaktivieren des Ports ausgeführt werden. Beispielsweise definiert ein Netzwerkadministrator eine ACL-Regel, laut der Port-Nummer 20 TCP-Pakete empfangen kann. Wenn jedoch ein UDP-Paket empfangen wird, wird das Paket abgelehnt.

ACLs bestehen aus Zugriffssteuerungseinträgen (ACE) oder Regeln auf Basis der Filter zur Bestimmung von Datenverkehrklassifizierungen. Die Gesamtzahl der Regeln, die für jede ACL definiert werden können, beträgt 10.

Auf der Seite **IP ACL Configuration** (Konfiguration von IP-ACLs) können Sie IP-basierte ACLs hinzufügen und entfernen.

Um die Seite **IP ACL Configuration** (IP-ACL-Konfiguration) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Network Security (Netzwerksicherheit) → Access Control Lists (Zugriffssteuerungslisten)→ IP Access Control Lists (IP-Zugriffssteuerungslisten)→ Configuration (Konfiguration)**.

Abbildung 8-10. Konfiguration von IP-ACLs



Die Seite IP ACL Configuration (Konfiguration von IP-ACLs) enthält folgende Felder:

IP ACL Name (IP-ACL-Name) – Spezifiziert einen benutzerdefinierten Namen für die ACL.

Remove (Entfernen) – Entfernt die im Feld IP ACL gewählte IP-ACL.

Hinzufügen einer IP-basierten ACL

1. Öffnen Sie die Seite **IP ACL Configuration** (Konfiguration von IP-ACLs).
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add IP ACL** (IP-ACL hinzufügen) wird angezeigt.

Abbildung 8-11. IP-ACL hinzufügen

3. Geben Sie im Feld **ACL Name den ACL-Namen ein**.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die IP-basierte ACL wird hinzugefügt, und das Gerät wird aktualisiert.

Entfernen einer IP-basierten ACL

1. Öffnen Sie die Seite **IP ACL Configuration** (Konfiguration von IP-ACLs), und wählen Sie im Dropdown-Menü **IP ACL** die zu löschende ACL.

2. Aktivieren Sie das Kontrollkästchen **Remove ACL** (ACL entfernen).

3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die IP-basierte ACL wird entfernt, und das Gerät wird aktualisiert.

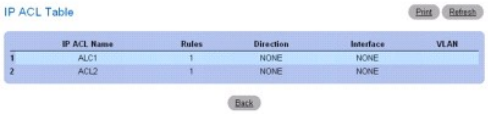
Anzeigen von IP-ACLs

1. Öffnen Sie die Seite **IP ACL Configuration** (Konfiguration von IP-ACLs).

2. Klicken Sie auf **Show All** (Alle anzeigen).

   Alle IP-ACLs und ihre zugehörigen Daten werden in der **IP ACL Table** (IP-ACL-Tabelle) angezeigt.

Abbildung 8-12. IP-ACL-Tabelle



Hinzufügen einer IP-basierten ACL mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- ACL Commands (ACL-Befehle)

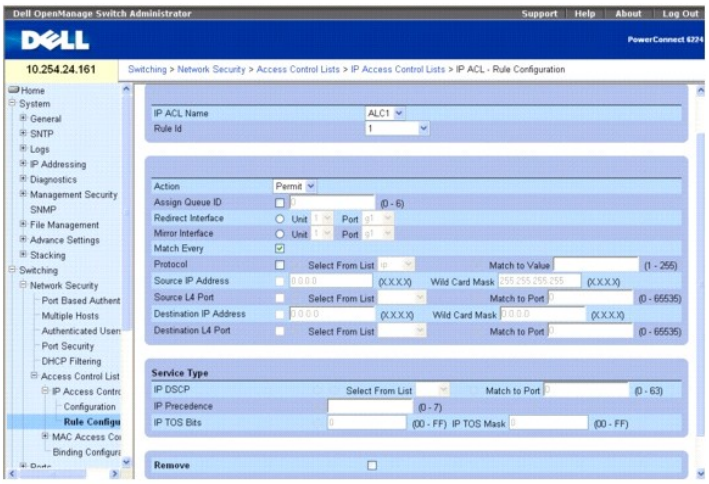
Konfigurieren von IP-ACL-Regeln

Auf der Seite **IP ACL Rule Configuration** (Konfiguation von IP-ACL-Regeln) können Sie Regeln für IP-basierte ACLs festlegen. Die Zugriffslistendefinition enthält Regeln, die festlegen, ob Datenverkehr, der die Kriterien erfüllt, normal weitergeleitet oder abgelehnt wird. Zusätzlich können Sie festlegen, dass Datenverkehr einer bestimmten Warteschlange zugeordnet wird, Datenverkehr filtern, VLAN-Kennungen ändern, Ports herunterfahren und/oder den Datenverkehr zu einem bestimmten Port umleiten.

HINWEIS: Am Ende der Liste steht eine implizite Deny-All-Regel (Alle verweigern). D. h. wenn eine ACP für ein Paket angewandt wird und keine der expliziten Regeln erfüllt ist, wird die Deny-All-Regel am Ende der Liste angewandt, und das Paket wird abgelehnt.

Um die Seite **IP ACL Rule Configuration** (Konfiguration von IP-ACL-Regeln) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Network Security (Netzwerksicherheit) → Access Control Lists (Zugriffssteuerungslisten)→ IP Access Control Lists (IP-Zugriffssteuerungslisten)→ Rule Configuration (Konfiguration von Regeln)**.

Abbildung 8-13. Konfigurieren von IP-ACL-Regeln (Standard)



Die Seite IP ACL Rule Configuration (Konfiguration von IP-ACL-Regeln) enthält folgende Felder:

IP ACL Name (IP-ACL-Name) – Gibt eine vorhandene IP-ACL an. Auf der Seite IP ACL Configuration (Konfiguration von IP-ACLs) können Sie eine neue IP-ACL einrichten.

Rule ID (Regel-ID) – Wählt oder erstellt benutzerdefinierte ACLs. Geben Sie eine vorhandene Regel-ID ein, oder erstellen Sie eine neue, indem Sie im Dopdown-Menü **Create** (Erstellen) wählen und im zugehörigen Feld die gewünschte neue Regel-ID eingeben. Sobald Sie auf Apply Changes (Änderungen übernehmen) klicken, wird die neue ID erstellt. Für jede ACL können bis zu 10 Regeln erstellt werden.

Action (Aktion) – Wählt die ACL-Weiterleitungsaktion aus. Wählen Sie im Dropdown-Menü Optionen zur Anwendung einer Weiterleitungsaktion. Mögliche Werte:

Permit (Zulassen) – Leitet Pakete weiter, die die ACL-Kriterien erfüllen.

Deny (Verweigern) – Lehnt Pakete ab, die die ACL-Kriterien erfüllen.

Assign Queue ID (Warteschlangen-ID zuweisen) – Aktivieren Sie das Kontrollkästchen, um dieses Kriterium anzuwenden, und geben Sie dann eine Kennnummer von 0 bis 6 ein.

Redirect Interface (Schnittstelle umleiten) – Wählt aus der Schnittstellen-Dropdown-Liste eine Schnittstelle aus, zu der Pakete weitergeleitet werden können, auf die diese Regel zutrifft.

Mirror Interface (Schnittstelle spiegeln) – Wählt aus der Schnittstellen-Dropdown-Liste eine Schnittstelle aus, auf die Pakete gespiegelt werden können, auf die diese Regel zutrifft.

Logging (Protokollierung) – Wenn das Kontrollkästchen markiert ist, wird die Protokollierung für eine bestimmte ACL ausgewählt. Die Protokollierung wird nur für die Aktion "Deny" (Verweigern) unterstützt.

Match Every (Alle erfüllen) – Bedeutet, dass ein Paket die Kriterien dieser ACL erfüllen muss. Aktivieren Sie das Kontrollkästchen, um diese Kriterien anzuwenden. Wenn diese Option aktiviert ist, sind die anderen Filterregeln auf dem Bildschirm nicht zugänglich.

Protocol (Protokoll) – Das Protokoll eines Pakets muss mit dem hier angegebenen Protokoll übereinstimmen. Aktivieren Sie das Kontrollkästchen, um diese Kriterien anzuwenden, und wählen Sie dann eine der folgenden Optionen:

Select from List (Aus Liste wählen) – Wählen Sie aus der Dropdown-Liste das Protokoll, auf dem die Regel basieren kann.

Match to Value (Wert zuweisen) – Klicken Sie, um eine benutzerdefinierte Protokoll-ID hinzuzufügen, anhand der Pakete der Regel zugewiesen werden.

Source IP Address (Quelle IP-Adresse) – Die IP-Adresse des Quell-Ports eines Pakets muss mit der hier angegebenen Adresse übereinstimmen. Aktivieren Sie das Kontrollkästchen, und geben Sie eine Adresse ein, um diese Kriterien anzuwenden.

Wild Card Mask (Platzhaltermaske) – Gibt die Platzhaltermaske der IP-Quelladresse an. Durch Platzhaltermasken wird festgelegt, welche Bits verwendet und welche ignoriert werden. Die Platzhaltermaske 255.255.255.255 gibt an, dass kein Bit von Bedeutung ist. Der Platzhalter 0.0.0.0 gibt an, dass alle Bits berücksichtigt werden. Dieses Feld ist erforderlich, wenn **Source IP Address** (IP-Quelladresse) aktiviert ist.

Source L4 Port (Quelle L4-Port) – Der TCP/UDP-Quell-Port eines Pakets muss mit dem hier angegebenen Port übereinstimmen. Aktivieren Sie das Kontrollkästchen, um diese Kriterien anzuwenden, und wählen Sie dann im Dropdown-Menü eine der folgenden Optionen:

Select From List (Aus Liste wählen) – Klicken Sie, um aus einer Liste den Quellport zu wählen, auf dem die Regel basieren kann.

Match to Port (Port zuweisen) – Klicken Sie, um eine benutzerdefinierte Port-ID hinzuzufügen, anhand der Pakete der Regel zugewiesen werden.

Destination IP Address (Ziel IP-Adresse) – Die IP-Adresse des Ziel-Ports eines Pakets muss mit der hier angegebenen Adresse übereinstimmen. Aktivieren Sie das Kontrollkästchen, und geben Sie eine Adresse ein, um diese Kriterien anzuwenden.

Wild Card Mask (Platzhaltermaske) – Gibt die Platzhaltermaske der IP-Zieladresse an. Dieses Feld ist erforderlich, wenn **Destination IP Address** (IP-Zieladresse) aktiviert ist.

Destination L4 Port (Ziel L4-Port) – Der TCP/UDP-Ziel-Port eines Pakets muss mit dem hier angegebenen Port übereinstimmen. Aktivieren Sie das Kontrollkästchen, um diese Kriterien anzuwenden, und wählen Sie dann eine der folgenden Optionen:

Select From List (Aus Liste wählen) – Wählen Sie aus einer Liste den Zielport, auf dem die Regel basieren kann.

Match to Port (Port zuweisen) – Klicken Sie, um eine benutzerdefinierte Port-ID hinzuzufügen, anhand der Pakete der Regel zugewiesen werden.

Diensttyp-Felder

Wählen Sie eines der folgenden drei Zuordnungsfelder, die beim Zuweisen von Paketen zu ACLs verwendet werden sollen:

IP DSCP (IP-DSCP) – Weist der Regel den DSCP-Wert des Pakets zu. Um ACLs Pakete zuzuweisen, wird entweder der DSCP-Wert oder der IP-Precedence-Wert verwendet.

Select From List (Aus Liste wählen) – Wählen Sie aus einer Liste von DSCP-Stichworten einen Wert.

Match to Port (Port zuweisen) – Klicken Sie, um eine benutzerdefinierte Port-ID hinzuzufügen.

IP Precedence (IP-Vorrang) – Weist den IP-Precedence-Wert des Pakets der Regel zu. Geben Sie den zuzuweisenden IP-Precedence-Wert ein. Um ACLs Pakete zuzuweisen, wird entweder der DSCP-Wert oder der IP-Precedence-Wert verwendet.

IP TOS Bits (IP-TOS-Bits) – Sorgt für Zuweisung zu Diensttyp-Bits im IP-Header.

TOS Bits (TOS-Bits) – Bedeutet, dass die Bits im TOS-Feld eines Pakets der hier eingegebenen zweistelligen Hexadezimalzahl entsprechen müssen.

TOS Mask (TOS-Maske) – Gibt die Bitpositionen an, die zum Vergleich mit dem IP-TOS-Feld in einem Paket verwendet werden.

Remove (Entfernen) – Entfernt eine Regel-ID, sobald **Remove** markiert ist und Sie auf **Apply Changes** (Änderungen übernehmen) klicken.

Ändern einer IP-basierten Regel

ANMERKUNG: Regeln können nur geändert werden, wenn die ACL, zu der sie gehören, nicht an eine Schnittstelle gebunden sind.

1. Öffnen Sie die Seite **IP ACL Configuration** (Konfiguration von IP-ACLs).
2. Wählen Sie **im Dropdown-Menü IP ACL die gewünschte ACL**.
3. Wählen Sie im Dropdown-Menü **Rule ID** (Regel-ID) die gewünschte Regel.
4. Ändern Sie die übrigen Felder je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die IP-basierte Regel wird geändert, und das Gerät wird aktualisiert.

Hinzufügen einer neuen Regel zu einer IP-basierten ACL

1. Öffnen Sie die Seite **IP ACL Configuration** (Konfiguration von IP-ACLs).
2. Wählen Sie **im Dropdown-Menü IP ACL die gewünschte ACL**.
3. Wählen Sie im Dropdown-Menü **Rule ID** (Regel-ID) die Option **Create Rule** (Regel erstellen), und geben Sie eine neue ID-Nummer ein.
4. Definieren Sie die übrigen Felder je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der neue Regel wird der spezifizierten IP-basierten ACL zugewiesen.

Festlegen einer IP-basierten ACL-Regel mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

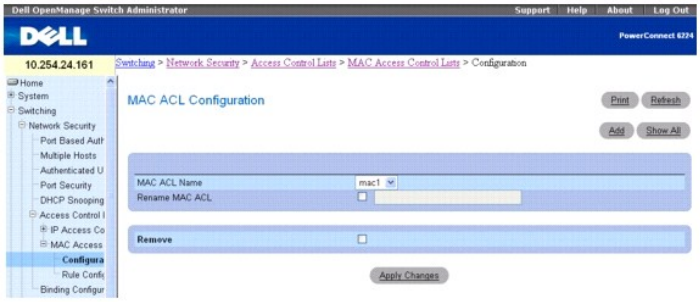
- ACL Commands (ACL-Befehle)

Konfigurieren von MAC-ACLs

Auf der Seite **MAC ACL Configuration** (Konfiguration von MAC-ACLs) können Netzwerkadministratoren eine MAC-basierte ACL festlegen. Weitere Informationen über ACLs finden Sie unter Konfigurieren von ACLs.

Um die Seite **MAC ACL Configuration** (Konfiguration von MAC-ACLs) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Network Security (Netzwerksicherheit) → Access Control Lists (Zugriffssteuerungslisten)→ MAC Access Control Lists (MAC-Zugriffssteuerungslisten)→ Configuration (Konfiguration)**.

Abbildung 8-14. Konfiguration von MAC-ACLs



Die Seite MAC ACL Configuration (Konfiguration von MAC-ACLs) enthält folgende Felder:

MAC ACL Name (MAC-ACL-Name) – Benutzerdefinierter ACL-Name.

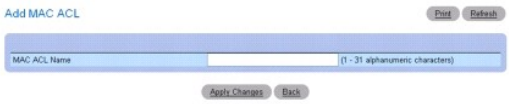
Rename MAC ACL (MAC-ACL umbenennen) – Um die MAC-ACL umzubenennen, aktivieren Sie das Kontrollkästchen, und geben Sie einen neuen MAC-ACL-Namen ein.

Remove (Entfernen) – Klicken Sie auf dieses Feld und dann auf die Schaltfläche "Apply Changes" (Änderungen übernehmen), um die im Feld MAC ACL aufgeführte MAC-ACL zu löschen.

Hinzufügen einer MAC-basierten ACL

1. Öffnen Sie die Seite **MAC ACL Configuration** (Konfiguration von MAC-ACL).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add MAC ACL** (MAC-ACL hinzufügen) anzuzeigen.

Abbildung 8-15. MAC-ACL hinzufügen



3. Geben Sie im Feld MAC **ACL Name den gewünschten MAC-ACL-Namen ein**.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die MAC-basierte ACL wird hinzugefügt, und das Gerät wird aktualisiert.

Entfernen einer MAC-basierten ACL

1. Öffnen Sie die Seite **MAC ACL Configuration** (Konfiguration von MAC-ACL), und wählen Sie im Dropdown-Menü **MACACL** die zu entfernende ACL.
2. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die MAC-basierte ACL wird entfernt, und das Gerät wird aktualisiert.

Anzeigen von MAC-ACLs

1. Öffnen Sie die Seite **MAC ACL Configuration** (Konfiguration von MAC-ACLs).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Alle MAC-ACLs und ihre zugehörigen Daten werden auf dem Bildschirm angezeigt.

Abbildung 8-16. MAC-ACL-Tabelle

Konfigurieren MAC-basierter ACLs mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

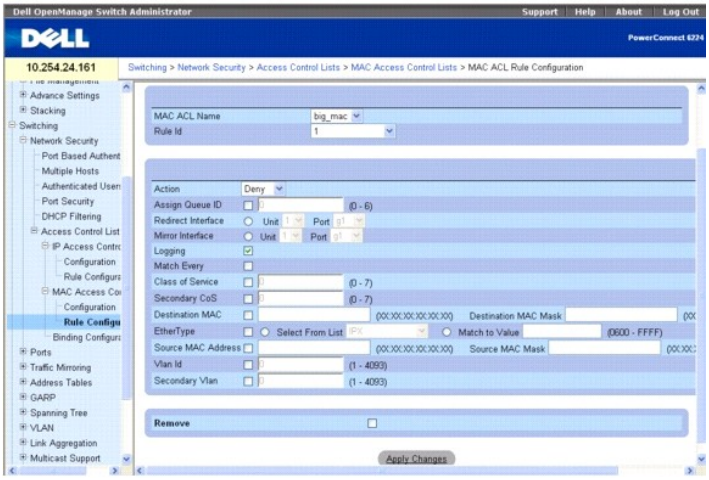
- ACL Commands (ACL-Befehle)

Konfigurieren von MAC-ACL-Regeln

Auf der Seite **MAC ACL Rule Configuration** (Konfiguation von MAC-ACL-Regeln) können Sie Regeln für MAC-basierte ACLs festlegen. Die Zugriffslistendefinition enthält Regeln, die festlegen, ob Datenverkehr, der die Kriterien erfüllt, normal weitergeleitet oder abgelehnt wird. Eine Deny-All-Regel (Alle verweigern) ist standardmäßig die letzte Regel in jeder Liste.

Um die Seite **MAC ACL Configuration** (Konfiguration von MAC-ACLs) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Network Security (Netzwerksicherheit) → Access Control Lists (Zugriffssteuerungslisten)→ MAC Access Control Lists (MAC-Zugriffssteuerungslisten)→ Rule Configuration (Konfiguration von Regeln)**.

Abbildung 8-17. Konfiguration von MAC-ACL-Regeln



Die Seite MAC ACL Rule Configuration (Konfiguration von MAC-ACL-Regeln) enthält folgende Felder:

MAC ACL Name (MAC-ACL-Name) – Gibt eine vorhandene MAC-ACL an. Auf der Seite MAC ACL Configuration (Konfiguration von MAC-ACLs) können Sie eine neue MAC-ACL einrichten.

Rule ID (Regel-ID) – Wählt oder erstellt benutzerdefinierte ACLs. Geben Sie eine vorhandene Regel-ID ein, oder erstellen Sie eine neue, indem Sie im Dopdown-Menü **Create** (Erstellen) wählen und im zugehörigen Feld die gewünschte neue Regel-ID eingeben. Sobald Sie auf Apply Changes (Änderungen übernehmen) klicken, wird die neue ID erstellt.

Action (Aktion) – Wählt die ACL-Weiterleitungsaktion aus. Dabei stehen folgende Optionen zur Auswahl:

Permit (Zulassen) – Leitet Pakete weiter, die die ACL-Kriterien erfüllen.

Deny (Verweigern) – Lehnt Pakete ab, die die ACL-Kriterien erfüllen.

Assign Queue ID (Warteschlangen-ID zuweisen) – Aktivieren Sie das Kontrollkästchen, um dieses Kriterium anzuwenden, und geben Sie dann eine Kennnummer von 0 bis 6 ein.

Redirect Interface (Schnittstelle umleiten) – Wählt aus der Schnittstellen-Dropdown-Liste eine Schnittstelle aus, zu der Pakete weitergeleitet werden können, auf die diese Regel zutrifft.

Mirror Interface (Schnittstelle spiegeln) – Wählt aus der Schnittstellen-Dropdown-Liste eine Schnittstelle aus, auf die Pakete gespiegelt werden können, auf die diese Regel zutrifft.

Logging (Protokollieren) – Markieren Sie das Kontrollkästchen, um die Protokollierung für diese ACL zu aktivieren. Diese Funktion wird nur für die Aktion "Deny" (Verweigern) unterstützt.

Match Every (Alle erfüllen) – Bedeutet, dass ein Paket die Kriterien dieser ACL erfüllen muss. Aktivieren Sie das Kontrollkästchen, um diese Kriterien anzuwenden.

Class of Service (Dienstklasse) – Bedeutet, dass die CoS eines Pakets dem hier aufgeführten CoS-Wert entsprechen muss. Aktivieren Sie das Kontrollkästchen, und geben Sie einen CoS-Wert zwischen 0 und 7 ein, um diese Kriterien anzuwenden.

Secondary CoS (Sekundäre Dienstklasse) – Bedeutet, dass die CoS eines Pakets dem hier aufgeführten CoS-Wert entsprechen muss. Aktivieren Sie das Kontrollkästchen, und geben Sie einen CoS-Wert zwischen 0 und 7 ein, um diese Kriterien anzuwenden.

Destination MAC Address (MAC-Zieladresse) – Bedeutet, dass die Zielport-MAC-Adresse eines Pakets der hier aufgeführten Adresse entsprechen muss. Aktivieren Sie das Kontrollkästchen, und geben Sie eine Adresse ein, um diese Kriterien anzuwenden.

Destination MAC Mask (MAC-Zielmaske) – Geben Sie bei Bedarf die MAC-Maske für die entsprechende Ziel-MAC ein.

EtherType – Bedeutet, dass der EtherType eines Pakets dem hier aufgeführten EtherType entsprechen muss. Aktivieren Sie das Kontrollkästchen, und wählen Sie die EtherType-ID aus einer Liste, oder geben Sie sie ein:

Select from List (Aus Liste wählen) – Wählen Sie im Dropdown-Menü den gewünschten EtherType.

Match to Port (Port zuweisen) – Geben Sie die gewünschte entsprechende Portnummer ein.

Source MAC Address (MAC-Quelladresse) – Bedeutet, dass die Quellport-MAC-Adresse eines Pakets der hier aufgeführten Adresse entsprechen muss. Aktivieren Sie das Kontrollkästchen, und geben Sie eine Adresse ein, um diese Kriterien anzuwenden.

Source MAC Mask (MAC-Quellmaske) – Geben Sie bei Bedarf die MAC-Maske für die entsprechende Quell-MAC-Adresse ein.

VLAN-ID – Bedeutet, dass die VLAN-ID eines Pakets der hier aufgeführten ID entsprechen muss. Aktivieren Sie das Kontrollkästchen, und geben Sie die VLAN-ID ein, um diese Kriterien anzuwenden. Mögliche Werte für dieses Feld sind 1–4093.

Secondary VLAN (Sekundär-VLAN) – Bedeutet, dass die Sekundär-VLAN-ID eines Pakets der hier aufgeführten ID entsprechen muss. Aktivieren Sie das Kontrollkästchen, und geben Sie die Sekundär-VLAN-ID ein, um diese Kriterien anzuwenden. Mögliche Werte für dieses Feld sind 1–4093.

Remove (Entfernen) – Entfernt die MAC-ACL-Regel, sobald Sie auf **Apply Changes** (Änderungen übernehmen) klicken.

Ändern einer MAC-basierten Regel:

ANMERKUNG: Regeln können nur geändert werden, wenn die ACL, zu der sie gehören, nicht an eine Schnittstelle gebunden sind.

1. Öffnen Sie die Seite **MAC ACL Rule Configuration** (Konfiguration von MAC-ACL-Regeln).
2. Wählen Sie **im Dropdown-Menü MAC ACL die gewünschte ACL**.
3. Wählen Sie im Dropdown-Menü **Rule ID** (Regel-ID) die gewünschte Regel.
4. Ändern Sie die übrigen Felder je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der MAC-basierte Regel wird geändert, und das Gerät wird aktualisiert.

Hinzufügen einer neuen Regel zu einer MAC-basierten ACL

1. Öffnen Sie die Seite **MAC ACL Rule Configuration** (Konfiguration von MAC-ACL-Regeln).
2. Wählen Sie **im Dropdown-Menü MAC ACL die gewünschte ACL**.
3. Wählen Sie unter **Rule ID** (Regel-ID) die Option **Create New Rule** (Neue Regel erstellen).
4. Geben Sie eine neue ID-Nummer ein.
5. Definieren Sie die übrigen Felder je nach Bedarf.
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der neue Regel wird der spezifizierten MAC-basierten ACL zugewiesen.

Entfernen einer Regel aus einer MAC-basierten ACL

1. Wählen Sie eine ACL.
2. Wählen Sie im Dropdown-Menü **Rule ID** (Regel-ID) eine Regel.
3. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die MAC-basierte ACL wird entfernt, und das Gerät wird aktualisiert.

Festlegen einer MAC-basierten ACL-Regel mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- ACL Commands (ACL-Befehle)

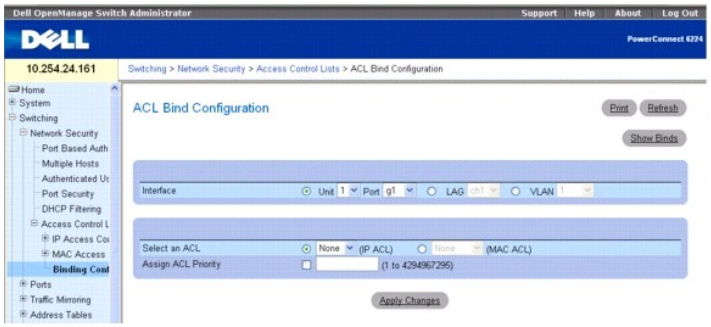
Konfiguration von ACL-Verbindungen

Wenn eine ACL an eine Schnittstelle gebunden ist, werden alle definierten Regeln auf die gewählte Schnittstelle angewandt. Auf der Seite **ACL Bind Configuration** (Konfiguration von ACL-Verbindungen) können Sie ACL-Listen ACL-Prioritäten und Schnittstellen zuweisen.

Über die Webschnittstelle können Sie die ACL-Regel in Ingress-Richtung konfigurieren, so dass sie auf Pakete angewandt wird, die am Port eintreffen. Über die CLI können Sie die ACL-Regel entweder in Ingress- oder in Egress-Richtung konfigurieren. Egress-ACLs wenden Sicherheitsregeln auf den Datenverkehr an, der über den Port nach außen gelangt. ACLs können auf jede physische Schnittstelle, LAG oder Port (einschließlich 10G) angewandt werden.

Um die Seite **ACL Bind Configuration** (Konfiguration von ACL-Verbindungen) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Network Security (Netzwerksicherheit)→ Access Control Lists (Zugriffssteuerungslisten)→ Binding Configuration (Konfiguration von Verbindungen)**.

Abbildung 8-18. Konfiguration von ACL-Verbindungen



Die Seite ACL Bind Configuration (Konfiguration von ACL-Verbindungen) enthält folgende Felder:

Interface (Schnittstelle) – Über die Optionsschaltflächen kann die Schnittstelle nach Einheit/Port, LAG oder VLAN ausgewählt werden.

Select an ACL (ACL auswählen) – Wählt den Typ der ACL, der eingehende Pakete zugewiesen werden. Pakete können entweder IP- oder MAC-basierten ACLs zugewiesen werden.

Assign ACL Priority (ACL-Priorität zuweisen) – Bestimmt die Priorität dieser ACL. Wenn mehr als eine ACL auf eine Schnittstelle angewandt wird, werden erst die Zuweisungskriterien für die ACLs mit der höchsten Priorität geprüft.

Zuweisen einer ACL an eine Schnittstelle

1. Öffnen Sie die Seite **ACL Bind Configuration** (Konfiguration von ACL-Verbindungen).
2. Geben Sie im Feld **Interface** (Schnittstelle) die Einheit/Port-Kombination, die LAG oder das VLAN an, für die die Konfiguration vorgenommen werden soll.
3. Wählen Sie im Feld **Select an ACL** (Wählen Sie eine ACL) die IP oder MAC-ACL.

   ANMERKUNG: Bei Zuweisung einer ACL zu einem Port, einer LAG oder einem VLAN wird für Datenflüsse von der Ingress-Schnittstelle, die der ACL nicht entsprechen, die Standardregel angewandt, gemäß der nicht entsprechende Pakete abgelehnt werden.

4. Legen Sie in **Assign ACL Priority** (ACL-Priorität zuweisen) die Priorität fest.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die ACL wird mit der festgelegten Schnittstelle verknüpft.

Entfernen einer Schnittstelle aus einer ACL

1. Öffnen Sie die Seite **ACL Bind Configuration** (Konfiguration von ACL-Verbindungen).
2. Klicken Sie auf **Show All** (Alle anzeigen).
3. Geben Sie im Feld "Interface" (Schnittstelle) die Einheit und den Port, die LAG oder das VLAN an, um die ACL-Bindings für die betreffende Schnittstelle zu sehen.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen), um eine oder mehrere ACLs zu entfernen.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die festgelegten ACLs werden von der Schnittstelle entfernt.

Zuweisen von ACL-Mitgliedschaften mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- ACL Commands (ACL-Befehle)

Konfigurieren von Ports

Die Menüseite **Ports** enthält Links zur Konfiguration von Portfunktionen einschließlich erweiterter Merkmale wie z. B. Sturmkontrolle und Portspiegelung sowie zum Testen virtueller Ports.

Um die Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Switching**→ **Ports**. Die Menüseite **Ports** enthält Links zu folgenden Themen:

- Globale Parameter
- Portkonfiguration
- Konfiguration geschützter Ports
- LAG-Konfiguration
- Sturmkontrolle

Globale Parameter

Über die globalen Parameter können Sie die **Flow Control** (Flusskontrolle) konfigurieren. Sie erlaubt das Regulieren von Datenverkehr für eine festgelegte Zeitspanne und wird für direkt verbundene Switches definiert. Flow Control kann nur für Ports eingestellt werden, für die der Vollduplex-Betriebsmodus konfiguriert ist. Da auf Autoverhandlung gesetzte Ports keinem LAG-Mitglied hinzugefügt werden können, kann für LAG-Mitglieder keine automatische Flusskontrolle eingestellt werden.

ANMERKUNG: Flow Control ist mit dem Unterdrückungsmodus Head-of-Line-Blocking nicht kompatibel. Der Switch kann in jedem Modus ausgeführt werden, jedoch nicht gleichzeitig.

Um die Seite **Global Parameters** (Globale Parameter) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching**→ **Ports**→ **Global Parameters (Globale Parameter)**.

Abbildung 8-19. Globale Port-Parameter

Die Seite Global Parameters (Globale Parameter) enthält das folgende Feld:

Flow Control (Flusskontrolle) – Wählen Sie im Drowdown-Menü "Enabled" (Aktiviert) oder "Disabled" (Deaktiviert). Dieser Befehl gilt für alle im Stack enthaltenen Ports. Diese Option ist standardmäßig aktiviert.

Enable (Aktivieren) – Schaltet den Ingress-Backpressure-Mechanismus am Switch ein.

Disable (Deaktivieren) – Setzt den Switch wieder in den Modus zur Unterdrückung durch Head-of-Line-Blocking.

Aktivieren von Ingress-Backpressure

1. Öffnen Sie die Seite **Ports Global Parameters** (Globale Portparameter).
2. Wählen Sie im Dropdown-Menü unter **Flow Control** (Flusskontrolle) die Option **Enable** (Aktivieren).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).
4. Ingress-Backpressure wird aktiviert.

Konfigurieren der Flusskontrolle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Ethernet Configuration Commands (Befehle zur Ethernet-Konfiguration)

Portkonfiguration

Auf der Seite **Port Configuration** (Portkonfiguration) können Sie Portparameter festlegen.

Um die Seite **Port Configuration** (Portkonfiguration) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching**→ **Ports**→ **Port Configuration** (Portkonfiguration).

Abbildung 8-20. Portkonfiguration

Die Seite Port Configuration (Portkonfiguration) enthält folgende Felder:

Port – Legt die Einheit und den Port fest, für die Portparameter definiert werden.

Description (0-64 Characters) (Beschreibung, 0-64 Zeichen) – Gibt eine kurze Beschreibung der Schnittstelle, z. B. Ethernet.

Admin Status (Administrierter Status) – Aktiviert (oben) oder deaktiviert (unten) die Weiterleitung von Datenverkehr über den Port.

Current Port Status (Aktueller Portstatus) – Zeigt an, ob der Port gerade in Betrieb oder außer Betrieb ist.

Current Port Speed (Aktuelle Portgeschwindigkeit) – Zeigt die derzeit synchronisierte Geschwindigkeit des Ports in Bit/s an.

Admin Port Speed (Administrierte Portgeschwindigkeit) – Erzwingt als Portgeschwindigkeit den gewählten Wert – 10M, 100M, 1000M oder 10000M.

Maximum Frame Size (1518-9216) (Maximale Frame-Länge) – Legt die Schwelle fest, ab der Pakete verworfen werden, die diesen Wert überschreiben. Der Standardwert ist 1518.

Admin Duplex (Administrierte Duplexeinstellung) – Legt den Duplexmodus für den Port fest. Mögliche Einstellungen sind Voll- und Halbduplex.

Full (Vollduplex) – Bedeutet, dass die Schnittstelle die gleichzeitige Übertragung in beide Richtungen zwischen Switch und Client unterstützt.

Half (Halbduplex) – Bedeutet, dass die Schnittstelle die Übertragung zwischen Switch und Client immer nur eine Richtung unterstützt.

Current Duplex Mode (Aktueller Duplexmodus) – Gibt den Duplexmodus für den synchronisierten Port an.

Auto Negotiation (Auto-Verhandlung) – Aktiviert den Auto-Verhandlungsmodus für den Port.
Dies ist ein Protokoll zwischen zwei Verbindungspartnern, mit dem ein Port dem jeweils anderen Port seine Fähigkeiten bezüglich Datenübertragungsrate, Duplexmodus und Flusskontrolle mitteilen kann.

Current Auto Negotiation (Aktuelle Auto-Verhandlung) – Gibt die aktuelle Einstellung für die Auto-Verhandlung an.

Admin Advertisement (Administrierte Bekanntmachung) – Legt die vom Port mitgeteilten Fähigkeiten fest. Mögliche Wert für dieses Feld sind:

Max Capability (Max. Fähigkeit) – Gibt an, dass alle Portgeschwindigkeiten und Duplexmodi akzeptiert werden.

10 Half (10 Halbduplex) – Gibt an, dass der Port eine Portgeschwindigkeit von 10 Mbit/s im Halbduplexmodus mitteilt.

10 Full (10 Vollduplex) – Gibt an, dass der Port eine Portgeschwindigkeit von 10 Mbit/s im Vollduplexmodus mitteilt.

100 Half (100 Halbduplex) – Gibt an, dass der Port eine Portgeschwindigkeit von 100 Mbit/s im Halbduplexmodus mitteilt.

100 Full (100 Vollduplex) – Gibt an, dass der Port eine Portgeschwindigkeit von 100 Mbit/s im Vollduplexmodus mitteilt.

1000 Full (1000 Vollduplex) – Gibt an, dass der Port eine Portgeschwindigkeit von 1000 Mbit/s im Vollduplexmodus mitteilt.

MDI/MDIX – Ermöglicht dem Switch die Erkennung gekreuzter und durchgehender Kabel.

Die Ports von Hubs und Switches sind im Vergleich zu den Ports von Endstationen absichtlich umgekehrt belegt, so dass zum Anschluss eines Hubs oder Switches an eine Endstation ein ungekreuztes 1:1-Kabel verwendet werden kann und die Adernpaare dabei richtig miteinander verbunden werden. Wenn zwei Hubs/Switches bzw. zwei Endstationen miteinander verbunden werden, wird ein gekreuztes Kabel verwendet, um eine korrekte Verbindung der Adernpaare sicherzustellen.

Mögliche Werte:

On (Ein) – Der Switch kann den Verbindungstyp erkennen.

Off (Aus) – Erfordert den richtigen Kabeltyp zur Verbindung mit dem Switch.

Auto – Der Wert wird automatisch eingestellt.

Current MDI/MDX (Aktuelle MDI/MDX) – Gibt die aktuellen MDX-Einstellungen des Switches an. Mögliche Werte für dieses Feld sind:

MDI – Die aktuelle MDI-Einstellung ist MDI.

MDX – Die aktuelle MDI-Einstellung ist MDX.

Auto – Der Wert wird automatisch eingestellt.

LAG – Zeigt die LAG-Nummer an, wenn dieser Port Mitglied einer LAG ist.

Festlegen von Portparametern

1. Öffnen Sie die Seite **Port Configuration** (Portkonfiguration).
2. Wählen Sie in den Feldern **Unit** und **Port** eine Einheit und einen Port.
3. Legen Sie die verfügbaren Einstellungen auf dem Bildschirm fest.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Portparameter werden im Switch gespeichert.

Anzeigen der Porttabelle

1. Öffnen Sie die Seite **Port Configuration** (Portkonfiguration).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die **Port Configuration Table** (Portkonfigurationstabelle) wird angezeigt.

Abbildung 8-21. Portkonfigurationstabelle

3. Über das Dropdown-Menü **Unit** (Einheit) können Sie die **Port Configuration Table** (Portkonfigurationstabelle) für andere ggf. im Stack vorhandene Einheiten anzeigen.

Kopieren von Portkonfigurationseinstellungen

1. Öffnen Sie die Seite **Port Configuration** (Portkonfiguration).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **Port Configuration Table** (Portkonfigurationstabelle) wird angezeigt.

3. Legen Sie in **Copy Parameters From** (Parameter kopieren aus) die Einheit und den Port fest, aus denen kopiert werden soll.
4. Klicken Sie für jeden Port, der diese Parameter erhalten soll, auf **Copy To** (Kopieren zu).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Portkonfigurationseinstellungen werden kopiert, und das Gerät wird aktualisiert.

Ändern der Portkonfigurationseinstellungen für mehrere Ports

1. Öffnen Sie die Seite **Port Configuration** (Portkonfiguration).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **Port Configuration Table** (Portkonfigurationstabelle) wird angezeigt.
3. Klicken Sie für jeden zu ändernden Port auf **Edit** (Bearbeiten).
4. Bearbeiten Sie die Felder zur Portkonfiguration je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Portkonfigurationseinstellungen werden geändert, und das Gerät wird aktualisiert.

Konfigurieren von Ports mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

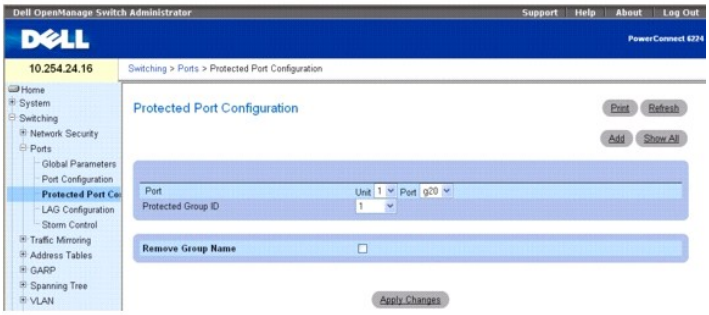
- Ethernet Configuration Commands (Befehle zur Ethernet-Konfiguration)

Konfiguration geschützter Ports

Verwenden Sie die Seite **Protected Port Configuration** (Konfiguration geschützter Ports), um das Layer-2-Sicherheitsmerkmal PVE (Private VLAN Edge)-Ports zu konfigurieren. PVE bietet Sicherheitsfunktionen auf Port-Ebene für die Kommunikation zwischen Ports, die demselben VLAN angehören. Der Datenverkehr von geschützten Ports wird nur an die Uplink-Ports gesendet und kann nicht an andere Ports innerhalb des VLAN gesendet werden.

Um die Seite **Port Configuration** (Portkonfiguration) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Ports→ Protected Port Configuration** (Konfiguration geschützter Ports).

Abbildung 8-22. Konfiguration geschützter Ports



Die Seite Protected Port Configuration (Konfiguration geschützter Ports) enthält folgende Felder:

Port – Legt die Einheit und den Port fest, für die Portparameter definiert werden.

Protected Group ID (Kennung für geschützte Gruppe) – Dropdown-Menü für die Zuweisung eines Ports zur Gruppe 0, 1 oder 2.

Remove Group Name (Gruppenbezeichnung entfernen) – Aktivieren Sie dieses Kontrollkästchen, um den gewählten Port aus der geschützten Gruppe zu entfernen.

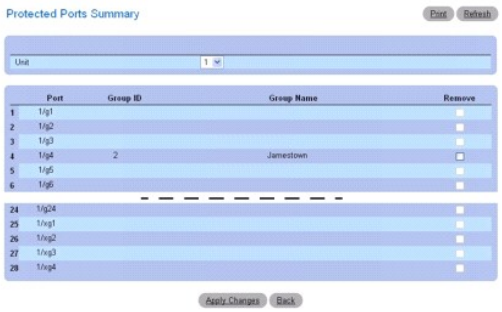
Anzeigen der Tabelle geschützter Ports

1. Öffnen Sie die Seite **Protected Port Configuration** (Konfiguration geschützter Ports).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die Tabelle **Protected Ports Summary** (Übersicht über geschützte Ports) wird angezeigt.

Abbildung 8-23. Übersichttabelle für geschützte Ports



3. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen), und klicken Sie auf **Apply Changes**, um einen Port aus einer geschützten Gruppe herauszunehmen.

4. Über das Dropdown-Menü **Unit** (Einheit) können Sie die Tabelle **Protected Port Summary (Übersicht über geschützte Ports)** für andere ggf. im Stack vorhandene Einheiten anzeigen.

Hinzufügen geschützter Portgruppen

1. Öffnen Sie die Seite **Protected Port Configuration** (Konfiguration geschützter Ports).

2. Klicken Sie auf **Add** (Hinzufügen).

   Die Option **Add Protected Group** (Geschützte Gruppe hinzufügen) wird angezeigt.

Abbildung 8-24. Geschützten Port hinzufügen

3. Weisen Sie über das Dropdown-Menü unter **Protected Group ID** (Kennung für geschützte Gruppe) die Nummernkennung 0, 1 oder 2 zu.

4. Geben Sie unter **Protected Group Name (1–32 characters)** (Bezeichnung für geschützte Gruppe, 1–32 Zeichen) eine Bezeichnung ein.

5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Einstellungen für geschützte Gruppen werden kopiert, und das Gerät wird aktualisiert.

Konfigurieren geschützter Ports mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

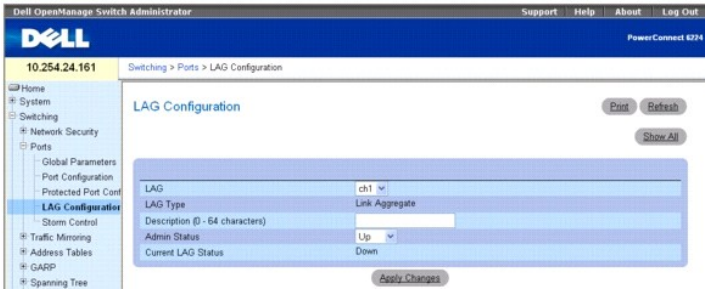
- switchport protected Commands (Switchport-Schutz-Befehle)

LAG-Konfiguration

Bei der Link-Aggregation können ein oder mehrere Fullduplex-Ethernet-Links zu einer Link Aggregation Group (LAG) aggregiert werden. Der Switch kann eine LAG wie eine einzige Verbindung behandeln.

Um die Seite **LAG Configuration** (LAG-Konfiguration) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Ports→ LAG Configuration** (LAG-Konfiguration).

Abbildung 8-25. LAG-Konfiguration



Die Seite LAG Configuration (LAG-Konfiguration) enthält folgende Felder:

LAG – Enthält eine Liste der LAG-Nummern.

LAG Type (LAG-Typ) – Die Porttypen, aus denen die LAG besteht.

Description (0-64 Characters) (Beschreibung, 0 bis 64 Zeichen) – Beschreibung des Ports.

Admin Status (Administrierter Status) – Aktiviert oder deaktiviert die Weiterleitung von Datenverkehr durch die ausgewählte LAG.

Current LAG Status (Aktueller LAG-Status) – Gibt an, ob die ausgewählte LAG den Status "Up" (Aktiv) oder "Down" (Inaktiv) hat.

Festlegen von LAG-Parametern

1. Öffnen Sie die Seite **LAG Configuration** (LAG-Konfiguration).
2. Wählen Sie im Feld **LAG** eine LAG.
3. Legen Sie die verfügbaren Einstellungen auf dem Bildschirm fest.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die LAG-Parameter werden im Switch gespeichert.

Anzeigen der LAG-Konfigurationstabelle

1. Öffnen Sie die Seite **LAG Configuration** (LAG-Konfiguration).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).
3. Die **LAG Configuration Table** (LAG-Konfigurationstabelle) wird angezeigt.

Abbildung 8-26. LAG-Konfigurationstabelle

Bearbeiten von LAG-Parametern

1. Öffnen Sie die Seite **LAG Configuration** (LAG-Konfiguration).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).
3. Die **LAG Configuration Table** (LAG-Konfigurationstabelle) wird angezeigt.
4. Wählen Sie für alle zu ändernden LAGs **Edit** (Bearbeiten).

5. **Admin Status** (Administrierter Status) und **Description** (Beschreibung) können nun nach Bedarf bearbeitet werden.

6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die LAG-Parameter werden im Switch gespeichert.

Konfigurieren von LAGs mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Port Channel Commands (Portkanal-Befehle)

Sturmkontrolle

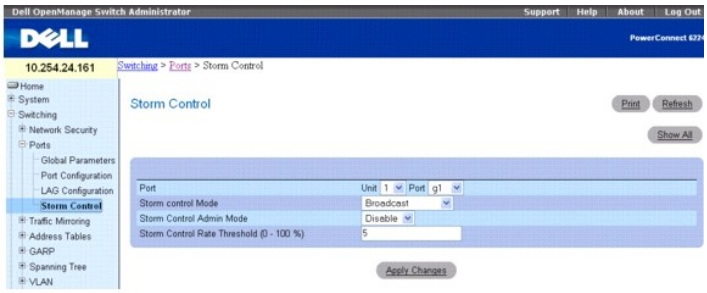
Ein Broadcaststurm entsteht durch eine übermäßig hohe Anzahl von Broadcast-Nachrichten, die von einem einzelnen Port gleichzeitig über ein Netzwerk übertragen werden. Antworten auf weitergeleitete Meldungen können Netzwerkressourcen überlasten und/oder zu einer Zeitüberschreitung des Netzwerks führen.

Der Switch misst die Rate der eingehenden Broadcast-/Multicast-/Unknown Unicast-Pakete nach Port und lehnt überzählige Pakete ab, wenn die Rate den festgelegten Wert übersteigt. Die Sturmkontrolle wird für jede Schnittstelle individuell aktiviert, indem der Pakettyp und die Übertragungsrate der Pakete definiert wird.

Auf der Seite **Storm Control** können Sie die Sturmkontrolle aktivieren und deaktivieren.

Um die Seite **Storm Control** (Sturmkontrolle) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching**→ **Ports**→ **Storm Control** (Sturmkontrolle).

Abbildung 8-27. Sturmkontrolle



Die Seite Storm Control (Sturmkontrolle) enthält folgende Felder:

Port – Legt die **Unit** (Einheit) und den **Port** fest, für die die Sturmkontrolle aktiviert wird.

Storm Control Mode (Sturmkontrollmodus) – Legt den Broadcast-Modus fest, der von der Sturmkontrolle betroffen ist.

Broadcast – Wenn die Übertragungsrate von L2-Broadcast-Datenverkehr bei Ingress an einer Schnittstelle den konfigurierten Schwellenwert überschreitet, wird der Datenverkehr verworfen.

Multicast – Wenn die Übertragungsrate von L2-Multicast-Datenverkehr bei Ingress an einer Schnittstelle den konfigurierten Schwellenwert überschreitet, wird der Datenverkehr verworfen.

Unknown Unicast – Wenn die Übertragungsrate von unbekanntem L2-Unicast-Datenverkehr (erfolglose Zielsuche) bei Ingress an einer Schnittstelle den konfigurierten Schwellenwert überschreitet, wird der Datenverkehr verworfen.

Storm Control Admin Mode (Administrierter Sturmkontrollmodus) – Aktiviert oder deaktiviert die Sturmkontrolle.

Storm Control Rate Threshold (0-100%) (Schwellenwert für Übertragungsrate bei Sturmkontrolle) – Legt die maximale Übertragungsrate fest, mit der Pakete weitergeleitet werden. Der Bereich wird in Prozent vom gesamten Schwellenwert angegeben.

Festlegen von Portparametern für die Sturmkontrolle

1. Öffnen Sie die Seite **Storm Control** (Sturmkontrolle).

2. Bearbeiten Sie die Felder auf dem Bildschirm.

3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Portparameter für die Sturmkontrolle werden im Switch gespeichert.

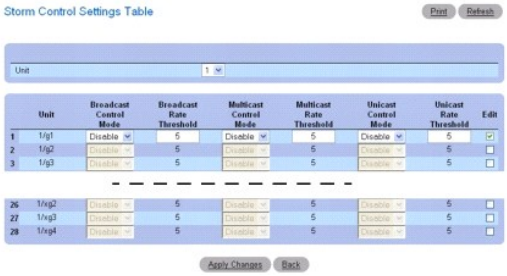
Anzeigen der Tabelle mit Einstellungen für die Sturmkontrolle

1. Öffnen Sie die Seite **Storm Control** (Sturmkontrolle).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die **Storm Control Settings Table** (Tabelle mit Einstellungen für die Sturmkontrolle) wird angezeigt.

Abbildung 8-28. Tabelle mit Einstellungen für die Sturmkontrolle



3. Über das Dropdown-Menü **Unit** (Einheit) können Sie die **Storm Control Settings Table** (Tabelle mit Einstellungen für die Sturmkontrolle) für andere ggf. im Stack vorhandene Einheiten anzeigen.

Ändern der Broadcast-Kontrolle

1. Öffnen Sie die Seite **Storm Control** (Sturmkontrolle).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die **Storm Control Settings Table** (Tabelle mit Einstellungen für die Sturmkontrolle) wird angezeigt.
3. Wählen Sie für jeden Port, für den **Broadcast Control** (Broadcast-Kontrolle) geändert werden soll, **Edit** (Bearbeiten).
4. Bearbeiten Sie die **Broadcast Control** (Broadcast-Kontrolle) je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Portparameter für die Sturmkontrolle werden im Switch gespeichert.

Konfigurieren der Sturmkontrolle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Ethernet Configuration Commands (Befehle zur Ethernet-Konfiguration)

Konfigurieren der Datenverkehrsspiegelung

Bei der Datenverkehrsspiegelung kann der Benutzer den Switch so konfigurieren, dass er Kopien von Paketen auf einem gespiegelten Port an den Spiegelungsport sendet. Die Spiegelung kann port- oder flussbasiert sein.

Auf der Seite **Traffic Mirroring** (Datenverkehrsspiegelung) können Sie Portspiegelungssitzungen definieren und flussbasierte Spiegelung konfigurieren.

Um die Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Traffic Mirroring (Datenverkehrsspiegelung)**. Die Menüseite **Traffic Mirroring** (Datenverkehrsspiegelung) enthält Links zu folgenden Themen:

- Port-Spiegelung
- Flussbasierte Spiegelung

Port-Spiegelung

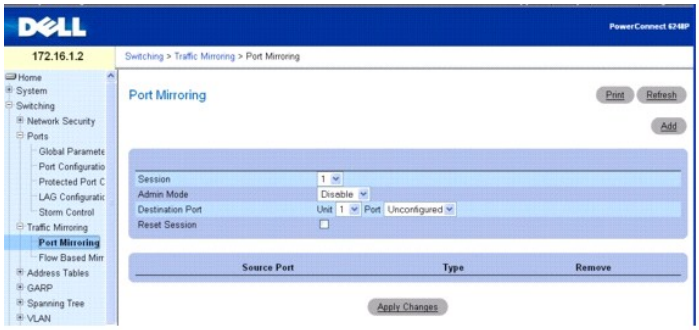
Bei der Portspiegelung wird der Netzwerk-Datenverkehr zur Analyse durch einen Netzwerkanalysator gewählt. Dies geschieht für bestimmte Ports des Switches. Dabei werden viele Switch-Ports als Quellports und einer als Zielport konfiguriert. Sie können einstellen, wie der Datenverkehr eines Quellports

gespiegelt werden soll. Es können Pakete auf den Zielport gespiegelt werden, die auf einem Quellport empfangen, gesendet oder empfangen und gesendet werden.

Das auf den Zielport kopierte Paket hat das gleiche Format wie das übertragene Originalpaket. D. h., wenn der Spiegel ein empfangenes Paket kopiert, hat das kopierte Paket ebenfalls eine VLAN-Kennung, wenn es am Quellport mit einer solchen empfangen wurde. Wenn der Spiegel ein gesendetes Paket kopiert, hat das kopierte Paket auch eine VLAN-Kennung, wenn es am Quellport mit einer solchen gesendet wurde.

Um die Seite **Port Mirroring** (Portspiegelung) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching**→ **Traffic Mirroring (Datenverkehrsspiegelung)**→ **Port Mirroring (Portspiegelung)**.

Abbildung 8-29. Portspiegelung



Die Seite Port Configuration (Portkonfiguration) enthält folgende Felder:

Session (Sitzung) – Legt die Überwachungssitzung fest.

Admin Mode (Administrierter Modus) – Aktiviert oder deaktiviert die Portspiegelung.

Destination Port (Zielport) – Wählt den Port, auf den der Datenverkehr von Ports kopiert werden kann.

Reset Session (Sitzung zurücksetzen) – Bietet die Möglichkeit, die Portüberwachungssitzung zurückzusetzen.

Source Port (Quellport) – Listet die hinzugefügten Quellports von der Seite "Add Source Port" (Quellport hinzufügen) auf.

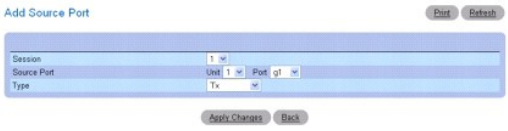
Type (Typ) – Zeigt den Typ des Datenverkehrs an, der auf dem Quellport überwacht wird.

Hinzufügen einer Portspiegelungssitzung

ANMERKUNG: Ein Port wird aus einem VLAN bzw. einer LAG entfernt, wenn er zum Zielport wird.

1. Öffnen Sie die Seite **Port Mirroring** (Portspiegelung).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add Source Port** (Quellport hinzufügen) anzuzeigen.

Abbildung 8-30. Quellport hinzufügen



3. Konfigurieren Sie folgende Felder:

   Session (Sitzung) – Wählt die Überwachungssitzung.

   Source Port (Quellport) – Wählt die Einheit und den Port, deren Datenverkehr gespiegelt werden soll. Bis zu vier Quellports können auf einen Zielport gespiegelt werden.

   Type (Typ) – Legt den Typ des zu überwachenden Datenverkehrs fest. Mögliche Werte für dieses Feld sind:

   TX – Nur gesendete Pakete werden überwacht.

   RX – Nur empfangene Pakete werden überwacht.

   TX and RX (TX und RX) – Gesendete und empfangene Pakete werden überwacht.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die neue Portspiegelungssitzung für die Einheit und den Port wird aktiviert, und das Gerät wird aktualisiert. Der Quellport wird auf der Seite **Port Mirroring** (Portspiegelung) in der Quellporttabelle angezeigt.

Ändern einer Portspiegelungssitzung

1. Öffnen Sie die Seite **Port Mirroring** (Portspiegelung).
2. Ändern Sie die Felder je nach Bedarf.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Felder für die Portspiegelungssitzung werden geändert, und das Gerät wird aktualisiert.

Entfernen einer Portspiegelungssitzung

1. Öffnen Sie die Seite **Port Mirroring** (Portspiegelung).
2. Markieren Sie das Kontrollkästchen **Reset Session** (Sitzung zurücksetzen).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die gewählte Portspiegelungssitzung wird entfernt, und das Gerät wird aktualisiert.

Konfigurieren einer Portspiegelungssitzung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Port Monitor Commands (Portüberwachungsbefehle)

Flussbasierte Spiegelung

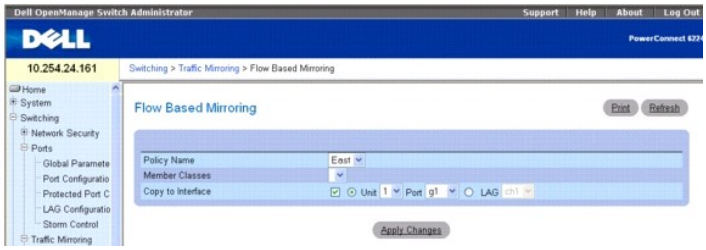
Die flussbasierte Spiegelung basiert auf der Diffserv-Komponente in QoS. In QoS erstellt der Benutzer Datenverkehrsklassen, um Entsprechungskriterien zu definieren, und dann Richtlinien, um die Aktion für die Datenverkehrsklasse festzulegen.

Bei der flussbasierten Spiegelung kann der Benutzer bestimmte Datenverkehrstypen auf einen einzigen Zielport kopieren. Dies sorgt für Flexibilität – anstatt den gesamten Ingress- oder Egress-Datenverkehr auf einem Port zu spiegeln, kann der Switch die Spiegelung auf bestimmte Teile des Datenverkehrs beschränken. Sie können den Switch so konfigurieren, dass er Flüsse auf Basis von Layer 2-, Layer 3- und Layer 4-Informationen spiegelt.

Auf der Seite **Flow Based Mirroring** (Flussbasierte Spiegelung) können Sie Ports für die flussbasierte Spiegelung festlegen.

Um die Seite **Flow Based Mirroring** (Flussbasierte Spiegelung) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Traffic Mirroring (Datenverkehrsspiegelung)→ Flow Based Mirroring (Flussbasierte Spiegelung)**.

Abbildung 8-31. Flussbasierte Spiegelung



Die Seite Flow Based Mirroring (Flussbasierte Spiegelung) enthält folgende Felder:

Policy Name (Richtlinienname) – Wählt die mit einer Datenverkehrsklasse zu verbindende Richtlinie. Der Richtlinienname wird auf der Webseite zur Diffserv Konfiguration von Richtlinien festgelegt.

Member Classes (Mitgliedsklassen) – Wählt die mit dieser Richtlinie verbundene Datenverkehrsklasse. Die Mitgliedsklasse auf der Webseite zur Diffserv Konfiguration von Richtlinien festgelegt.

Copy to Interface (Auf Schnittstelle kopieren) – Wenn diese Option aktiviert ist, können Pakete auf eine Einheit/Schnittstelle oder LAG kopiert werden.

Kopieren der Spiegelung auf einen Zielport

1. Öffnen Sie die Seite **Flow Based Mirroring** (Flussbasierte Spiegelung).

2. Legen Sie den **Policy Name** (Richtliniennamen) und die **Member Class** (Mitgliedsklasse) fest, und wählen Sie in **Copy to Interface** (Auf Schnittstelle kopieren) die gewünschte Zieleinheit und den Port.

3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Einstellungen für die flussbasierte Spiegelung werden auf den festgelegten Port kopiert, und das Gerät wird aktualisiert.

Konfigurieren der flussbasierten Spiegelung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- QOS Commands (QOS-Befehle)

Konfigurieren von Adresstabellen

MAC-Adressen sind entweder in der statischen oder dynamischen Adresstabelle gespeichert. Statische Adressen werden von Ihnen definiert. Dynamische Adressen werden vom System erfasst und nach einer Zeitüberschreitung gelöscht. Ein Paket, das an eine Zieladresse in einer der Tabellen adressiert ist, wird sofort an die Ports weitergeleitet. Die statischen und dynamischen Adresstabellen können nach Schnittstelle, VLAN-ID oder VLAN-Name sortiert werden. Den statischen und dynamischen Adresstabellen können auch Adressen hinzugefügt werden.

Um die Menüseite **Address Tables** (Adresstabellen) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Address Tables** (Adresstabellen). Die Menüseite **Address Tables** (Adresstabellen) enthält Links zu folgenden Themen:

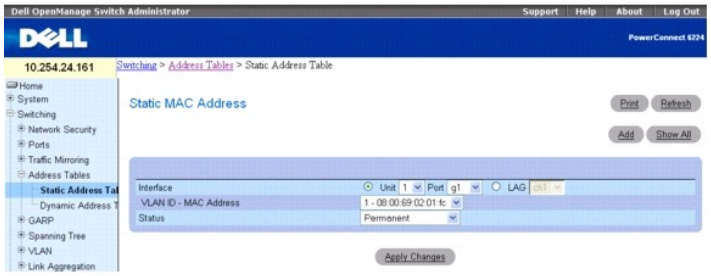
- Statische Adresstabelle
- Dynamische Adresstabelle

Statische Adresstabelle

Die Seite **Static MAC Address** enthält eine Liste statischer MAC-Adressen. Über die statische MAC-Adresstabelle können statische Adressen hinzugefügt und entfernt werden.

Um die Seite **Static MAC Address** (Statische MAC-Tabelle) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Address Tables (Adresstabellen)→ Static Address Table (Statische Adresstabellen)**.

Abbildung 8-32. Statische MAC-Adresse



Die Seite Static MAC Address (Statische MAC-Adresse) enthält folgende Felder:

Interface (Schnittstelle) – Legt die Einheit und den Port bzw. die LAG fest, auf die die statische MAC-Adresse angewandt wird. Um Informationen zu anderen Einheiten/Ports oder LAGs anzuzeigen, wechseln Sie die hier aufgeführte Schnittstelle.

VLAN ID - MAC Address (VLAN-ID - MAC-Adresse) – Bestimmt die VLAN-ID, die der MAC-Adresse zugewiesen ist, und die MAC-Adresse(n) in der aktuellen statischen Adressliste.

ANMERKUNG: Es werden nur MAC-Adressen angezeigt, die der festgelegten Schnittstelle und dem VLAN zugewiesen sind.

Status – Legt den Status der MAC-Adresse fest. Mögliche Werte:

Permanent – Es handelt sich um eine permanente MAC-Adresse.

Secure (Sicher) – Stellt sicher, dass eine MAC-Adresse mit gesperrtem Anschluss nicht gelöscht wird.

Delete on Reset (Bei Zurücksetzen löschen) – Die MAC-Adresse wird gelöscht, wenn der Switch zurückgesetzt wird.

Delete on Timeout (Bei Zeitüberschreitung löschen) – Die MAC-Adresse wird bei einer Zeitüberschreitung gelöscht.

Hinzufügen einer statischen MAC-Adresse

1. Öffnen Sie die Seite **Static MAC Address** (Statische MAC-Adresse).
2. Klicken Sie auf **Add**

   (Hinzufügen).

   Die Seite **Add Static MAC Address** (Statische MAC-Adresse hinzufügen) wird angezeigt.

Abbildung 8-33. Statische MAC-Adresse hinzufügen

3. Füllen Sie die Felder je nach Bedarf aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die neue statische Adresse wird der statischen MAC-Adresstabelle (**Static MAC Address Table**) hinzugefügt, und das Gerät wird aktualisiert.

Ändern einer statischen Adresse in der statischen MAC-Adresstabelle

1. Öffnen Sie die Seite **Static MAC Address** (Statische MAC-Adresse).
2. Ändern Sie die Felder je nach Bedarf.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die statische MAC-Adresse wird geändert, und das Gerät wird aktualisiert.

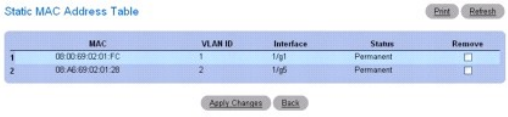
Anzeigen der statischen MAC-Adresstabelle

1. Öffnen Sie die Seite **Static MAC Address** (Statische MAC-Adresse).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die **Static MAC Address Table** (Statische MAC-Adresstabelle) zeigt alle vorhandenen statischen MAC-Adressen an.

Abbildung 8-34. Statische MAC-Adresstabelle



Entfernen einer statischen Adresse aus der statischen Adresstabelle

1. Öffnen Sie die Seite **Static MAC Address** (Statische MAC-Adresse).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **Static MAC Address Table** (Statische MAC-Adresstabelle) anzuzeigen.
3. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen) für die zu entfernende Adresse.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die statische Adresse wird gelöscht, und das Gerät wird aktualisiert.

Konfigurieren von Parametern statischer Adressen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Address Table Commands (Adresstabellenbefehle)

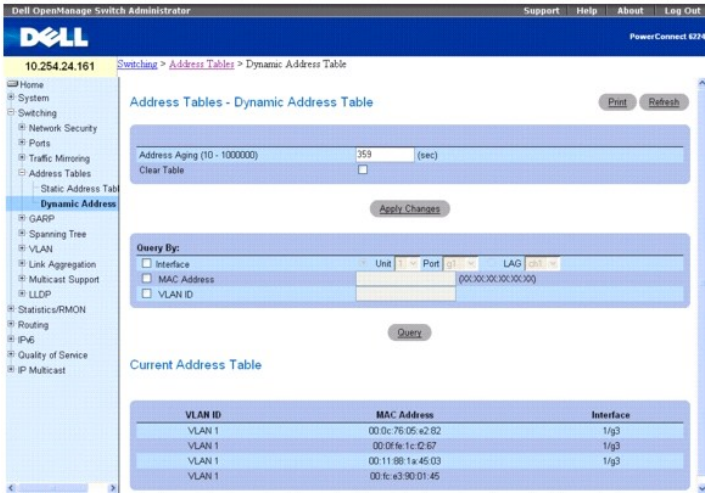
Dynamische Adresstabelle

Die Seite **Dynamic Address Table** (Dynamische Adresstabelle) enthält Felder zur Abfrage von Informationen in der dynamischen Adresstabelle, einschließlich Schnittstellentyp, MAC-Adressen, VLAN und Sortierschlüssel der Tabelle. Pakete, die an eine in der Adresstabelle gespeicherte Adresse gerichtet sind, werden direkt an die entsprechenden Ports weitergeleitet.

Die **Dynamic Address Table** (Dynamische Adresstabelle) enthält auch Informationen zur Speicherdauer, nach der eine dynamische MAC-Adresse aus der Tabelle entfernt wird.

Um die Seite **Dynamic Address Table** (Dynamische Adresstabelle) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Address Tables (Adresstabellen)→ Dynamic Address Table (Dynamische Adresstabellen)**.

Abbildung 8-35. Dynamische Adresstabelle



Die Seite **Dynamic Address Table** (Dynamische Adresstabelle) enthält folgende Felder:

Address Aging (10-1000000) (Adressspeicherdauer, 10-100000) – Legt die Speicherdauer in Sekunden fest, nach der eine dynamische MAC-Adresse gelöscht wird. Der Standardwert ist 300 Sekunden.

Clear Table (Tabelleneinträge löschen) – Löscht alle dynamischen MAC-Adressdaten aus der Tabelle, sobald Sie auf **Apply Changes** (Änderungen übernehmen) klicken.

In der Dynamic Address Table **(Dynamische Adresstabelle) können abgefragt werden:**

Interface (Schnittstelle) – Gibt die Einheit und den Port an, die für eine Adresse abgefragt werden.

LAG – Gibt die LAG an, die für eine Adresse abgefragt wird.

MAC Address (MAC-Adresse) – Gibt die MAC-Adresse an, die für eine Adresse abgefragt wird.

VLAN ID – Gibt die VLAN-Nummer an (der die MAC-Adresse zugewiesen ist), die für eine Adresse abgefragt wird.

Die **Current Address Table** (Aktuelle Adresstabelle) enthält dynamische Adressparameter, anhand derer Pakete direkt an die Ports weitergeleitet werden. Die Seite **Current Address Table** (Aktuelle Adresstabelle) enthält folgende Felder:

VLAN ID – Gibt den Wert der VLAN-Kennung an.

MAC Address (MAC-Adresse) – Gibt die MAC-Adresse an.

Interface (Schnittstelle) – Gibt die Portnummer an.

Festlegen der Speicherdauer

1. Öffnen Sie die Seite **Dynamic Address Table** (Dynamische Adresstabelle).
2. Legen Sie im Feld **Address Aging** die Adressspeicherdauer fest.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Speicherdauer wird geändert, und das Gerät wird aktualisiert.

Abfragen der dynamischen Adresstabelle

1. Öffnen Sie die Seite **Dynamic Address Table** (Dynamische Adresstabelle).
2. Definieren Sie die Parameter, nach denen die **Dynamic Address Table** (Dynamische Adresstabelle) abgefragt werden soll.

   Die Einträge können nach **Interface (Schnittstelle), LAG**, **MAC Address** (MAC-Adresse) oder **VLAN ID** (VLAN-ID) abgefragt werden.
3. Klicken Sie zum Abfragen der dynamischen Adresstabelle auf **Query** (Abfrage).

Entfernen von Daten aus der dynamischen Adresstabelle

1. Öffnen Sie die Seite **Dynamic Address Table** (Dynamische Adresstabelle).
2. Aktivieren Sie **Clear Table** (Tabelleneinträge löschen).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Alle Daten werden aus der dynamischen Adresstabelle gelöscht.

Abfragen und Sortieren von dynamischen Adressen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Address Table Commands (Adresstabellenbefehle)

Konfigurieren von GARP

Das Generic Attribute Registration Protocol (GARP) ist ein universell einsetzbares Protokoll, das beliebige Informationen zur Netzwerkkonnektivität oder über Mitgliedschaften registriert. GARP definiert eine Gruppe von Switches, die an einem bestimmten Netzwerkattribut interessiert sind, beispielsweise an einer VLAN- oder Multicast-Adresse. Die Seite **GARP Timers** (GARP-Zeitgeber) kann über die Menüseite **GARP** aufgerufen werden.

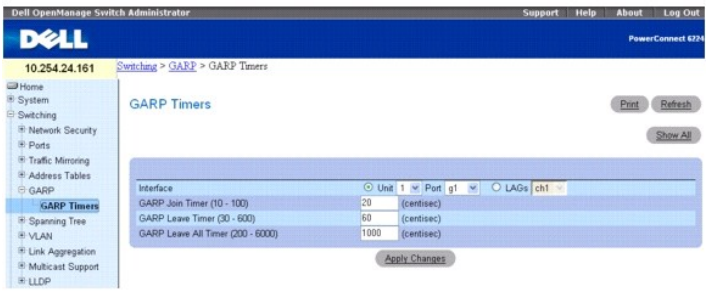
Um die Menüseite **GARP** *anzuzeigen*, klicken Sie in der Strukturansicht auf **Switching**→ **GARP**.

GARP-Zeitgeber

Die Seite **GARP Timers** (GARP-Zeitgeber) enthält Felder zur GARP-Aktivierung für den Switch.

Um die Seite **GARP Timers** (GARP-Zeitgeber) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching**→ **GARP**→ **GARP Timers** (GARP-Zeitgeber).

Abbildung 8-36. GARP-Zeitgeber



Die Seite **GARP Timers** (GARP-Zeitgeber) enthält folgende Felder:

Interface (Schnittstelle) – Legt die Einheit und den Port oder die LAG fest, für die der GARP-Zeitgeber aktiviert ist.

GARP Join Timer (10 - 100) (GARP-Join-Zeitgeber, 10-100) – Gibt die Zeit in Hundertstelsekunden an, in der PDUs übertragen werden. Mögliche Werte für dieses Feld sind 10 bis 100. Der Standardwert ist 100 Hundertstelsekunden.

GARP Leave Timer (30 - 600) (GARP-Leave-Zeitgeber, 30-600) – Gibt die Zeit in Hundertstelsekunden an, nach der der Switch seinen GARP-Zustand verlässt. Die Leave-Zeit wird durch eine gesendete/empfangene Leave-all-Zeit-Nachricht aktiviert und durch die empfangene Join-Nachricht beendet. Die

Leave-Zeit muss größer oder gleich der dreifachen Join-Zeit sein. Mögliche Werte für dieses Feld sind 30 bis 600. Der Standardwert ist 60 Hundertstelsekunden.

GARP Leave All Timer (200 - 6000) (GARP-Leave-All-Zeitgeber, 200-6000) – Gibt die Zeit in Hundertstelsekunden an, nach der alle Switches den GARP-Zustand verlassen. Die Leave-all-Zeit muss größer als die Leave-Zeit sein. Mögliche Werte für dieses Feld sind 200 bis 6000. Der Standardwert ist 1000 Hundertstelsekunden.

Festlegen von GARP-Zeitgebern

1. Öffnen Sie die Seite **GARP Timers** (GARP-Zeitgeber).
2. Füllen Sie die Felder aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Parameter werden auf die gewählten Ports oder LAGs in der GARP-Zeitgeber-Tabelle kopiert, und das Gerät wird aktualisiert.

Anzeigen von Parametern in der GARP-Zeitgeber-Tabelle

1. Öffnen Sie die Seite **GARP Timers** (GARP-Zeitgeber).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **GARP Timers Table** (GARP-Zeitgeber-Tabelle) wird angezeigt.

Abbildung 8-37. GARP-Zeitgeber-Tabelle

3. Über das Dropdown-Menü **Unit** (Einheit) können Sie die **GARP Timers Table** (GARP-Zeitgeber-Tabelle) für andere ggf. im Stack vorhandene Einheiten anzeigen.

Kopieren von GARP-Zeitgeber-Einstellungen

1. Öffnen Sie die Seite **GARP Timers** (GARP-Zeitgeber).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **GARP Timers Table** (GARP-Zeitgeber-Tabelle) wird angezeigt.

3. Legen Sie in **Copy Parameters From** (Parameter kopieren aus) die Einheit und den Port fest, aus denen kopiert werden soll.
4. Klicken Sie für jede Schnittstelle, die diese Parameter erhalten soll, auf **Copy To** (Kopieren zu).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die GARP-Zeitgeber-Einstellungen werden kopiert, und das Gerät wird aktualisiert.

Ändern der GARP-Zeitgeber-Einstellungen für mehrere Ports

1. Öffnen Sie die Seite **GARP Timers** (GARP-Zeitgeber).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **GARP Timers Table** (GARP-Zeitgeber-Tabelle) wird angezeigt.
3. Klicken Sie für jede zu ändernde Schnittstelle auf **Edit** (Bearbeiten).
4. Bearbeiten Sie die GARP-Zeitgeber-Felder je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die GARP-Zeitgeber-Einstellungen werden geändert, und das Gerät wird aktualisiert.

Festlegen von GARP-Zeitgebern mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- GVRP Commands (GVRP-Befehle)

Konfigurieren des Spanning Tree-Protokolls

Das Spanning Tree-Protokoll (STP) stellt eine Baumstruktur-Topologie für jede Brückenanordnung bereit. STP stellt auch einen Pfad zwischen Endstationen im Netzwerk bereit und eliminiert dadurch Schleifen. Zu den unterstützten Spanning Tree-Versionen gehören Classic STP, Multiple STP und Rapid STP.

Classic STP stellt zwischen zwei beliebigen Endstationen jeweils genau einen Pfad bereit und vermeidet bzw. eliminiert so Netzwerkschleifen. Weitere Informationen zur Konfiguration von Classic STP finden Sie unter **Globale STP-Einstellungen**.

Das Multiple Spanning Tree-Protokoll (MSTP) unterstützt mehrere Spanning Tree-Instanzen, um VLAN-Datenverkehr effizient über verschiedene Schnittstellen zu leiten. Jede Spanning Tree-Instanz verhält sich wie in IEEE 802.1w Rapid Spanning Tree (RSTP) spezifiziert, mit leichten Abweichungen bei der Funktionsweise, nicht jedoch im Endeffekt (der wichtigste Effekt ist der schnelle Übergang des Ports zur Weiterleitung). Das RSTP unterscheidet sich vom traditionellen STP (IEEE 802.1d) in der Fähigkeit zur Konfiguration und Erkennung von Vollduplexkonnektivität und von Ports, die mit Endstationen verbunden sind, was zu einem schnellen Übergang des Ports zum Weiterleitungszustand und zur Unterdrückung der Topologieänderungsbenachrichtigung führt. Diese Merkmale sind durch die Parameter pointtopoint und edgeport dargestellt. MSTP ist mit RSTP und STP kompatibel. Es verhält sich STP- und RSTP-Brücken entsprechend. Eine MSTP-Brücke kann so konfiguriert werden, dass sie sich genau wie eine RSTP- oder STP-Brücke verhält.

Um die Menüseite **Spanning Tree** anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Spanning Tree**. Die Seite **Spanning Tree** enthält links zu folgenden STP-Verfahren:

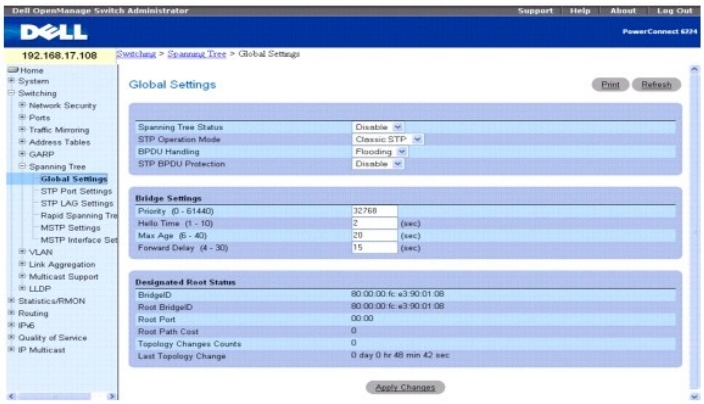
- Globale STP-Einstellungen
- STP Port Settings (STP-Porteinstellungen)
- STP-LAG-Einstellungen
- Rapid Spanning Tree
- MSTP-Einstellungen
- MSTP-Schnittstelleneinstellungen

Globale STP-Einstellungen

Die Seite **STP Global Settings** (Globale STP-Einstellungen) enthält Felder zur STP-Aktivierung für den Switch.

Um die Seite **STP Global Settings** (Globale STP-Einstellungen) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Spanning Tree→ Global Settings** (Globale Einstellungen).

Abbildung 8-38. Globale Spanning Tree-Einstellungen



Die Seite STP Global Settings (Globale STP-Einstellungen) enthält folgende Felder:

Spanning Tree Status (Spanning Tree-Status) – Aktiviert oder deaktiviert auf dem Switch RSTP, STP oder MSTP.

STP Operation Mode (STP-Betriebsmodus) – Gibt den STP-Modus an, gemäß dem STP auf dem Switch aktiviert wird. Mögliche Werte für dieses Feld sind: **Classic STP**, **Rapid STP und Multiple STP**.

BPDU Handling (BPDU-Behandlung) – Legt fest, wie BPDU (Bridge Protocol Data Unit)-Pakete behandelt werden, wenn auf einer Schnittstelle Spanning Tree deaktiviert ist. Mögliche Werte für dieses Feld sind Filtering (Filterung) und Flooding (Fluten). Der Standardwert ist Flooding.

STP BPDU Protection (STP-BPDU-Schutz) – Deaktiviert einen Port, falls ein neuer Switch versucht, die bereits vorhandene STP-Topologie einzugeben. Dadurch können Switches, die nicht ursprünglich zu einem STP gehören, die STP-Topologie nicht beeinflussen.

Wenn ein auf Enable (Aktivieren) gesetzter Endport eine BPDU empfängt, wird der Port deaktiviert und kann anschließend nur manuell wieder aktiviert werden.

Bridge-Einstellungen

Priority (0-61440) (Priorität, 0-61440) – Legt den Wert für die Bridge-Priorität fest. Wenn auf Switches oder Bridges STP ausgeführt wird, wird jedem Switch und jeder Bridge eine Priorität zugewiesen. Nach Auswechseln der BPDUs wird der Switch mit der niedrigsten Priorität zur Root-Bridge.

Hello Time (1-10) (Hello-Zeit, 1-10) – Legt die Hello-Zeitdauer in Sekunden fest, die eine Root-Bridge zwischen Konfigurationsmeldungen wartet. Der Standardwert ist 2.

Max Age (6-40) (Max. Speicherdauer, 6-40) – Legt die maximale Speicherdauer in Sekunden fest, die eine Bridge bis zum Implementieren einer Topologieänderung wartet. Der Standardwert ist 20.

Forward Delay (4-30) (Weiterleitungsverzögerung, 4-30) – Legt die Switch-Weiterleitungsverzögerung in Sekunden fest, die eine Bridge bis zur Weiterleitung von Paketen im Lausch- und Erfassungszustand bleibt. Der Standardwert ist 15.

Designierter Root-Status

Bridge ID (Bridge-ID) – Zeigt die Bridge-ID an.

Root Bridge ID (Root-Bridge-ID) – Gibt die Root-Bridge-ID an.

Root Port (Root-Port) – Zeigt die Nummer des Ports mit den niedrigsten Pfadkosten von dieser Bridge zur Root-Bridge an. Dies ist von Bedeutung, wenn es sich bei der Bridge nicht um die Root-Bridge handelt. Der Standardwert ist 0.

Root Path Cost (Root-Pfadkosten) – Zeigt die Kosten des Pfads von dieser Bridge bis zum Root-Gerät an.

Topology Changes Counts (Zähler für Topologieänderungen) – Zeigt die Gesamtanzahl der aufgetretenen STP-Zustandsänderungen an.

Last Topology Change (Letzte Topologieänderung) – Zeigt die Zeit seit der letzten Topologieänderung an. Die Zeit wird im Format Tag/Stunde/Minute/Sekunde angezeigt, z. B. 5 Stunden 10 Minuten und 4 Sekunden.

Festlegen globaler STP-Parameter

1. Öffnen Sie die Seite **STP Global Settings** (Globale STP-Einstellungen).
2. Wählen Sie im Feld **Spanning Tree State** (Spanning Tree-Zustand) **Enable** (Aktivieren).
3. Wählen Sie im Feld **STP Operation Mode** (STP-Betriebsmodus) den **STP**-Modus, und legen Sie die übrigen Einstellungen fest.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

STP wird auf dem Switch aktiviert.

Ändern globaler STP-Parameter:

1. Öffnen Sie die Seite **STP Global Settings** (Globale STP-Einstellungen).
2. Ändern Sie die Felder auf dieser Seite je nach Bedarf.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die STP-Parameter werden geändert und das Gerät aktualisiert.

Festlegen globaler STP-Parameter mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

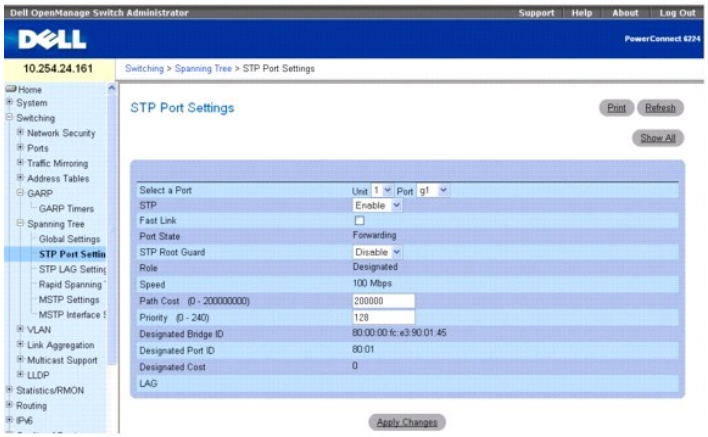
- Spanning Tree Commands (Spanning Tree-Befehle)

STP Port Settings (STP-Porteinstellungen)

Auf der Seite **STP Port Settings** (STP-Porteinstellungen) können Sie einzelnen Ports STP-Eigenschaften zuweisen.

Um die Seite **STP Port Settings** (STP-Porteinstellungen) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Spanning Tree→ STP Port Settings** (STP-Porteinstellungen).

Abbildung 8-39. STP-Porteinstellungen



Die Seite STP Port Settings (STP-Porteinstellungen) enthält folgende Felder:

Select a Port (Port auswählen) – Legt die Einheit und den Port fest, für die STP aktiviert ist.

STP – Aktiviert oder deaktiviert STP auf dem Port.

Fast Link (Schnelle Verbindung) – Aktiviert den Fast Link-Modus für den Port. Wenn der Fast-Link-Modus für einen Port aktiviert ist, wird der **Port State** (Portzustand) automatisch in den Zustand **Forwarding** (Weiterleitung) versetzt, sobald auf dem Port eine Verbindung besteht. Bis zum Konvergieren des STP können in großen Netzwerken zwischen 30 und 60 Sekunden vergehen.

Port State (Portzustand) – Gibt den aktuellen STP-Zustand eines Ports an. Falls aktiviert, legt der Portzustand fest, wie der Port mit Datenverkehr umgeht. Folgende Portzustände sind möglich:

Disabled (Deaktiviert) – STP ist derzeit auf dem Port deaktiviert. Der Port leitet Datenverkehr weiter und erfasst dabei MAC-Adressen.

Blocking (Blockieren) – Der Port ist derzeit blockiert und kann nicht für die Weiterleitung von Datenverkehr oder die Erfassung von MAC-Adressen verwendet werden.

Listening (Lauschen) – Der Port befindet sich derzeit im Lauschmodus. Der Port kann weder Datenverkehr weiterleiten noch MAC-Adressen erfassen.

Learning (Erfassen) – Der Port befindet sich derzeit im Erfassungsmodus. Der Port kann keinen Datenverkehr weiterleiten, er kann jedoch neue MAC-Adressen erfassen.

Forwarding (Weiterleiten) – Der Port befindet sich derzeit im Weiterleitungsmodus. Der Port kann Datenverkehr weiterleiten und neue MAC-Adressen erfassen.

STP Root Guard (STP-Root-Schutz) – Verhindert unerwartete Root-Änderungen einer Spanning Tree-Instanz. Wenn diese Funktion für eine Root-Bridge aktiviert ist und eine höhere BPDU ankommt, wechselt der Port in einen Root-Inkonsistenz-Zustand, der dem Lauschzustand entspricht. Die Root-Bridge wird erzwungen.

Role (Funktion) – Zeigt die Funktion des Ports in der STP-Topologie an.

Speed (Geschwindigkeit) – Zeigt die Geschwindigkeit an, mit der der Port betrieben wird.

Path Cost (0-200000000) (Pfadkosten, 0-200000000) – Gibt den Anteil dieses Ports an den Root-Pfadkosten an. Wenn der Leitweg eines Pfads geändert wird, werden die Kosten für den Pfad auf einen höheren oder niedrigen Wert gesetzt und entsprechend zur Weiterleitung von Datenverkehr herangezogen. Der Wert 0 bedeutet, dass die Pfadkosten auf den der Portgeschwindigkeit entsprechenden Wert gesetzt wurden. Der Standardwert ist 0.

Priority (0-240) (Priorität, 0-240) – Legt den Wert für die Port-Priorität fest. Der Prioritätswert beeinflusst die Portwahl, wenn eine Brücke zwei Ports in einer Schleifenkonfiguration aufweist. Der Standardwert ist 128.

Designated Bridge ID (ID der designierten Bridge) – Zeigt die ID der designierten Bridge an.

Designated Port ID (ID des designierten Ports) – Zeigt die ID des gewählten Ports an.

Designated Cost (Designierte Kosten) – Zeigt die Kosten des an der STP-Topologie teilnehmenden Ports an. Wenn STP eine Schleifenkonfiguration entdeckt, werden Ports mit niedrigeren Kosten mit geringerer Wahrscheinlichkeit blockiert.

LAG – Zeigt die LAG an, mit der der Port verknüpft ist.

Aktivieren von STP auf einem Port

1. Öffnen Sie die Seite **STP Port Settings** (STP-Porteinstellungen).
2. Legen Sie im Feld **Select a Port** (Port auswählen) die Einheit und den Port fest, die aktiviert werden sollen.
3. Wählen Sie im Feld **STP** die Option **Enable** (Aktivieren).
4. Bearbeiten Sie die Felder **Fast Link** *(Schnelle Verbindung)*, ***STP Root Guard*** *(STP-Root-Schutz)*, **Path Cost** (Pfadkosten) und **Priority** (Priorität) je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   STP wird auf dem Port aktiviert.

Ändern der STP-Porteigenschaften

1. Öffnen Sie die Seite **STP Port Settings** (STP-Porteinstellungen).
2. Ändern Sie die Felder **Fast Link** (Schnelle Verbindung), **STP Root Guard** (STP-Root-Schutz), **Path Cost** (Pfadkosten) und **Priority** (Priorität) je nach Bedarf.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

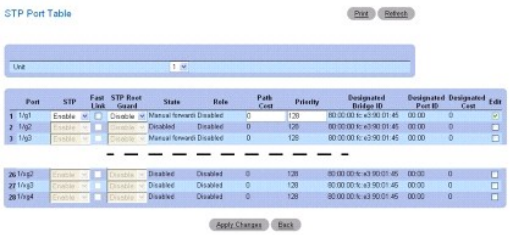
   Die STP-Portparameter werden geändert und das Gerät aktualisiert.

Anzeigen der STP Port Table (STP-Porttabelle)

1. Öffnen Sie die Seite **STP Port Settings** (STP-Porteinstellungen).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **STP Port Table** (STP-Porttabelle) wird angezeigt.

Abbildung 8-40. STP-Porttabelle



3. Über das Dropdown-Menü **Unit** (Einheit) können Sie die **STP Port Table** (STP-Porttabelle) für andere ggf. im Stack vorhandene Einheiten anzeigen

Ändern der STP-Porteinstellungen für mehrere Ports

1. Öffnen Sie die Seite **STP Port Settings** (STP-Porteinstellungen).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **STP Port Table** (STP-Porttabelle) wird geöffnet.
3. Klicken Sie für jeden zu ändernden Port auf **Edit** (Bearbeiten).
4. Bearbeiten Sie die STP-Porteinstellungen je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die STP-Porteinstellungen werden geändert, und das Gerät wird aktualisiert.

Anwenden von Fast Link auf einen Port

1. Öffnen Sie die Seite **STP Port Settings** (STP-Porteinstellungen).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **STP Port Table** (STP-Porttabelle) wird angezeigt.
3. Klicken Sie für jeden zu ändernden Port auf **Edit** (Bearbeiten).
4. Aktivieren Sie den Modus **Fast Link** (Schnelle Verbindung) für einen Port. Wenn der Fast-Link-Modus für einen Port aktiviert ist, wird der **Port State** (Portzustand) automatisch in den Zustand **Forwarding** (Weiterleitung) versetzt, sobald auf dem Port eine Verbindung besteht.
5. Klicken Sie auf **Apply Changes**

   (Änderungen übernehmen).

   Die STP-Portparameter werden für die gewählten Ports geändert, und das Gerät wird aktualisiert.

Festlegen von STP-Porteinstellungen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Spanning Tree Commands (Spanning Tree-Befehle)

STP-LAG-Einstellungen

Auf der Seite **STP LAG Settings** (STP-LAG-Einstellungen) können Sie STP-Parameter für aggregierte Ports zuweisen.

Um die Seite **STP LAG Settings** (STP-LAG-Einstellungen) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching**→ **Spanning Tree**→ **STP LAG Settings (STP-LAG-Einstellungen)**.

Abbildung 8-41. STP-LAG-Einstellungen

Die Seite STP LAG Settings (STP-LAG-Einstellungen) enthält folgende Felder:

Select a LAG (LAG auswählen) – Gibt die LAG-Nummer an, deren STP-Einstellungen Sie ändern möchten.

STP – Aktiviert oder deaktiviert STP für die LAG. In der Standardeinstellung ist STP aktiviert.

Fast Link (Schnelle Verbindung) – Aktiviert den Fast-Link-Modus für die LAG. Wenn der Fast-Link-Modus für eine LAG aktiviert ist, wird der **Port State** (Portzustand) automatisch in den Zustand **Forwarding** (Weiterleitung) versetzt, sobald auf der LAG eine Verbindung besteht. Der Fast-Link-Modus optimiert die Zeit, die benötigt wird, bis das STP-Protokoll konvergiert. Bis zum Konvergieren des STP können in großen Netzwerken zwischen 30 und 60 Sekunden vergehen.

Port State (Portzustand) – Gibt den aktuellen STP-Zustand einer LAG an. Falls aktiviert, legt der LAG-Zustand fest, wie die LAG mit Datenverkehr umgeht. Wenn die Bridge eine fehlerhaft arbeitende LAG entdeckt, wird diese in den Zustand **Broken** (Defekt) versetzt. Folgende LAG-Zustände sind möglich:

Disabled (Deaktiviert) – STP ist derzeit für die LAG deaktiviert. Die LAG leitet Datenverkehr weiter und erfasst dabei MAC-Adressen.

Blocking (Blockieren) – Die LAG ist blockiert und kann nicht für die Weiterleitung von Datenverkehr oder die Erfassung von MAC-Adressen verwendet werden.

Listening (Lauschen) – Die LAG ist im Lauschmodus und kann weder Datenverkehr weiterleiten noch MAC-Adressen erfassen.

Learning (Erfassen) – Die LAG ist im Erfassungsmodus und kann keinen Datenverkehr weiterleiten, jedoch neue MAC-Adressen erfassen.

Forwarding (Weiterleiten) – Die LAG ist derzeit im Weiterleitungsmodus und kann Datenverkehr weiterleiten und neue MAC-Adressen erfassen.

Broken (Defekt) – Die LAG funktioniert derzeit nicht korrekt und kann nicht zur Weiterleitung von Datenverkehr verwendet werden.

Role (Funktion) – Zeigt die Funktion des Ports in der STP-Topologie an.

Path Cost (0-200000000) (Pfadkosten, 0-200000000) – Legt den Anteil dieser LAG an den Root-Pfadkosten fest. Wenn der Leitweg eines Pfads geändert wird, werden die Kosten für den Pfad auf einen höheren oder niedrigen Wert gesetzt und entsprechend zur Weiterleitung von Datenverkehr herangezogen. Der Standardwert ist 0.

Priority (0-240) (Priorität, 0-240) – Legt den Wert für die LAG-Priorität fest. Der Prioritätswert beeinflusst die LAG-Wahl, wenn eine Brücke zwei Ports in einer Schleifenkonfiguration aufweist. Der Prioritätswert liegt zwischen 0 und 240.

Designated Bridge ID (Designierte Bridge-ID) – Zeigt die designierte Bridge-ID an.

Designated Port ID (Designierte Port-ID) – Zeigt die designierte Port-ID an.

Designated Cost (Designierte Kosten) – Zeigt die Kosten des an der STP-Topologie teilnehmenden Ports an. Wenn STP eine Schleifenkonfiguration entdeckt, werden Ports mit niedrigeren Kosten mit geringerer Wahrscheinlichkeit blockiert.

Ändern der LAG-STP-Parameter für eine LAG

1. Öffnen Sie die Seite **STP LAG Settings** (STP-LAG-Einstellungen).
2. Wählen Sie im Dropdown-Menü **Select a LAG** (LAG auswählen) eine LAG.
3. Ändern Sie die Felder je nach Bedarf.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die STP-Parameter für die LAG werden geändert, und das Gerät wird aktualisiert.

Anzeigen der STP-LAG-Tabelle

1. Öffnen Sie die Seite **STP LAG Settings** (STP-LAG-Einstellungen).

2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **STP LAG Table** (STP-LAG-Tabelle) wird angezeigt.

Abbildung 8-42. STP-LAG-Tabelle

3. Über die Tabelle können Fast Verbindung und STP Root Guard für eine individuelle LAG aktiviert oder deaktiviert werden. Klicken Sie dazu auf **Fast Link**, wählen Sie die entsprechenden Optionen aus, und klicken Sie dann auf **Apply Changes** (Änderungen übernehmen).

Ändern der LAG-STP-Parameter für mehrere LAGs

1. Öffnen Sie die Seite **STP LAG Settings** (STP-LAG-Einstellungen).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **STP LAG Table** (STP-LAG-Tabelle) wird angezeigt.
3. Wählen Sie für alle zu ändernden LAGs **Edit** (Bearbeiten).
4. Ändern Sie die Felder je nach Bedarf.
5. Klicken Sie auf **Apply Changes**

   (Änderungen übernehmen).

   Die STP-LAG-Parameter werden für die gewählten LAGs geändert, und das Gerät wird aktualisiert.

Festlegen von STP-LAG-Einstellungen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

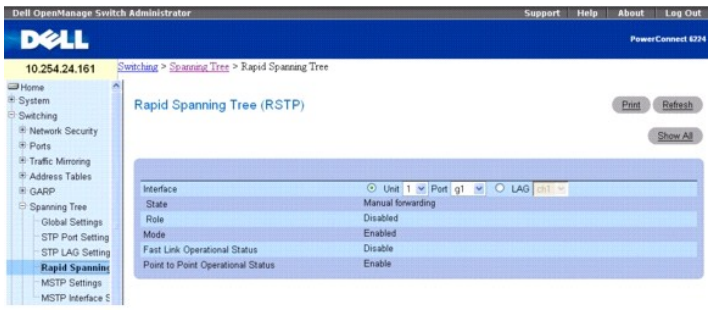
- Spanning Tree Commands (Spanning Tree-Befehle)

Rapid Spanning Tree

Das Rapid Spanning Tree Protocol (RSTP) erkennt und verwendet Netzwerktopologien, die ein schnelleres Konvergieren des Spanning Tree ermöglichen, ohne dabei Weiterleitungsschleifen zuzulassen.

Um die Seite **Rapid Spanning Tree** anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Spanning Tree→ Rapid Spanning Tree**.

Abbildung 8-43. Rapid Spanning Tree



Die Seite **Rapid Spanning Tree** enthält folgende Felder:

Interface (Schnittstelle) – Legt fest, ob RSTP für eine Einheit und einen Port oder eine LAG aktiviert ist. Klicken Sie auf **Unit/Port** (Einheit/Port) oder **LAG** , um den Typ der Schnittstelle festzulegen. Wählen Sie dann im Dropdown-Menü die Einheit und den Port oder die LAG, die Sie konfigurieren möchten.

State (Zustand) – Zeigt den Spanning Tree-Zustand für den Port an.

Role (Funktion) – Zeigt die Spanning Tree-Funktion des Ports in der STP-Topologie an.

Mode (Modus) – Zeigt den Verwaltungsmodus an und ob er aktiviert oder deaktiviert ist.

Fast Link Operational Status (Fast-Link-Betriebsstatus) – Zeigt an, ob der Fast-Link-Modus auf dem Port bzw. der LAG aktiviert oder deaktiviert ist. Wenn Fast Link für eine LAG aktiviert ist, wird der Port automatisch in den Weiterleitungszustand versetzt. Diese Einstellung kann auf der Seite STP Port Settings (STP-Porteinstellungen) oder STP LAG Settings (STP-LAG-Einstellungen) geändert werden.

Point-to-Point Operational Status (Punkt-zu-Punkt-Betriebsstatus) – Gibt den Betriebsstatus der Punkt-zu-Punkt-Verbindung an.

Um die Datenübertragung über eine Punkt-zu-Punkt-Verbindung herzustellen, sendet das Ursprungs-PPP zunächst LCP-Pakete (Link Control Protocol), um die Datenverbindung zu konfigurieren und zu testen. Wenn die Verbindung hergestellt ist und vom LCP benötigte optionale Merkmale ausgehandelt worden sind, sendet das Ursprungs-PPP NCP-Pakete (Network Control Protocols), um ein oder mehrere Layer 3-Protokolle auszuwählen und zu konfigurieren. Nach Konfiguration der einzelnen gewählten Layer 3-Protokolle können Pakete der einzelnen Layer 3-Protokolle über die Verbindung gesendet werden. Die Verbindung verbleibt für die Datenübertragung konfiguriert, bis sie explizit durch LCP- oder NCP-Pakete geschlossen wird oder ein externes Ereignis auftritt. Dies ist der tatsächliche Verbindungstyp des Switch-Ports.

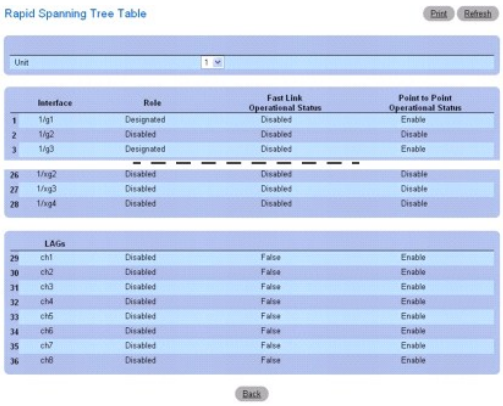
Anzeigen der Rapid Spanning Tree-Tabelle (RSTP)

1. Öffnen Sie die Seite **Rapid Spanning Tree (RSTP)**.

2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **Rapid Spanning Tree Table** (Rapid Spanning Tree-Tabelle) wird angezeigt.

Abbildung 8-44. Rapid-Spanning Tree-Tabelle



3. Über das Dropdown-Menü **Unit** (Einheit) können Sie die **Rapid-Spanning Tree Table** (Rapid Spanning Tree-Tabelle) für andere ggf. im Stack vorhandene Einheiten anzeigen.

Festlegen von Rapid STP-Parametern mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

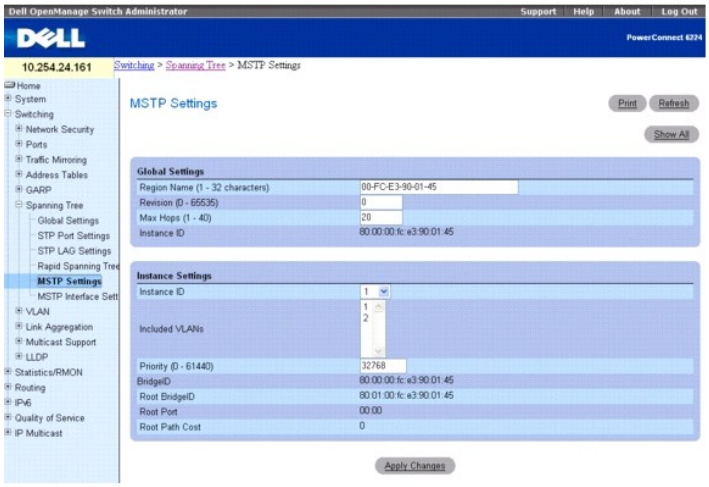
- Spanning Tree Commands (Spanning Tree-Befehle)

MSTP-Einstellungen

Das Multiple Spanning Tree-Protokoll (MSTP) unterstützt mehrere Spanning Tree-Instanzen, um VLAN-Datenverkehr effizient über verschiedene Schnittstellen zu leiten. MSTP ist mit RSTP sowie STP kompatibel. Eine MSTP-Bridge kann so konfiguriert werden, dass sie sich genau wie eine RSTP- oder STP-Brücke verhält.

Um die Seite **MSTP Settings** (MSTP-Einstellungen) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Spanning Tree→ MSTP Settings** (MSTP-Einstellungen).

Abbildung 8-45. MSTP-Einstellungen



Die Seite **MSTP Settings** (MSTP-Einstellungen) ist in zwei Bereiche unterteilt, **Global Settings** (Globale Einstellungen) und **Instance Settings** (Instanz-Einstellungen), und enthält folgende Felder:

Region Name (1–32 Characters) (Regionsname, 1-32 Zeichen) – Legt den benutzerdefinierten Namen der MSTP-Region fest.

Revision (0–65535) – Legt eine 16-Bit-Zahl ohne Vorzeichen fest, die die Revision der aktuellen MST-Konfiguration bezeichnet. Die Revisionsnummer ist ein erforderlicher Bestandteil der MST-Konfiguration. Der Standardwert ist 0.

Max Hops (1–40) (Max. Sprünge, 1-40) – Legt die Gesamtzahl der in einer spezifischen Region zulässigen Sprünge fest, nach denen die BPDU abgelehnt wird. Bei Ablehnung der BPDU verfallen die Portinformationen. Der Standardwert ist 20.

Instance ID (Instanz-ID) – Legt die ID der Spanning Tree-Instanz fest. Der Wertebereich für das Feld ist 1 bis 15. Der Standardwert ist 1.

Included VLANs (Eingeschlossene VLANs) – Weist die gewählten VLANs der gewählten Schnittstelle zu. Jedes VLAN gehört nur zu einer Instanz.

Priority (0–61440) (Priorität, 0-61440) – Legt die Switch-Priorität für die gewählte Spanning Tree-Instanz fest. Der Standardwert ist 32768.

Bridge ID (Bridge-ID) – Gibt die Bridge-ID der gewählten Instanz an.

Root Bridge ID der Root-Bridge mit den geringsten Pfadkosten.

Root Port (Root-Port) – Gibt den Root-Port der gewählten Instanz an.

Root Path Cost (Root-Pfadkosten) – Gibt die Pfadkosten der gewählten Instanz an.

Ändern der MSTP-Einstellungen:

1. Öffnen Sie die Seite **MSTP Settings** (MSTP-Einstellungen).
2. Ändern Sie die Felder unter **Global Settings** (Globale Einstellungen) und **Instance Settings** (Instanz-Einstellungen) je nach Bedarf.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

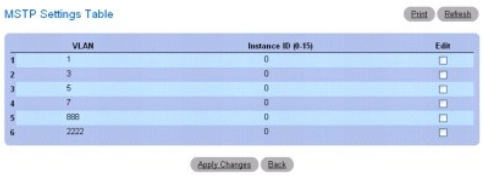
   Die MSTP-Parameter werden geändert, und das Gerät wird aktualisiert.

Anzeigen der Zuordnungstabelle für MSTP-VLANs zu Instanzen

1. Öffnen Sie die Seite **MSTP Settings** (MSTP-Einstellungen).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **MSTP Settings Table** (Tabelle mit MSTP-Einstellungen) wird angezeigt.

Abbildung 8-46. Tabelle mit MSTP-Einstellungen



3. Um die Instanz-ID für ein oder mehrere VLANs zu ändern, aktivieren Sie für die gewünschten VLANs **Edit** (Bearbeiten).
4. Ändern Sie die Instanz-IDs je nach Bedarf. Um die VLAN-Instanz-Zuordnung aufzuheben, geben Sie den Wert 0 ein.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Instanz-IDs werden für die gewählten VLANs geändert, und das Gerät wird aktualisiert.

Festlegen von MST-Instanzen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Spanning Tree Commands (Spanning Tree-Befehle)

MSTP-Schnittstelleneinstellungen

Auf der Seite **MSTP Interface Settings** (MSTP-Schnittstelleneinstellungen) können Sie Schnittstellen MSTP-Einstellungen zuweisen.

Um die Seite **MSTP Interface Settings** (MSTP-Schnittstelleneinstellungen) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching**→ **Spanning Tree**→ **MSTP Interface Settings** (MSTP-Schnittstelleneinstellungen).

Abbildung 8-47. MSTP-Schnittstelleneinstellungen

Die Seite **MSTP Interface Settings** (MSTP-Schnittstelleneinstellungen) enthält folgende Felder:

Instance ID (Instanz-ID) – Wählt die auf dem Switch konfigurierten MSTP-Instanzen aus. Der mögliche Wertebereich für das Feld liegt zwischen 1 und 15.

Interface (Schnittstelle) – Wählt entweder eine Einheit und einen Port oder eine LAG für diese MSTP-Instanz aus.

Port State (Portzustand) – Gibt an, ob der Port in der gegebenen Instanz aktiviert oder deaktiviert ist.

Port Type (Porttyp) – Gibt an, ob MSTP den Port als Punkt-zu-Punkt-Port oder an einen Hub angeschlossenen Port behandelt und ob es ein interner Port der MST-Region oder ein Boundary-Port (Grenz-Port) ist. Bei einem Boundary-Port wird auch angegeben, ob der Switch am anderen Ende der Verbindung im RSTP- oder STP-Modus arbeitet.

Role (Funktion) – Gibt die Funktion an, die der STP-Algorithmus dem Port zugewiesen hat, um STP-Pfade bereitstellen. Die für dieses Feld möglichen Werte sind:

Root (Wurzel) – Stellt den kostengünstigsten Pfad für die Weiterleitung von Paketen zum Root-Switch bereit.

Designated (Designiert) – Gibt den Port bzw. die LAG an, über den/die der designierte Switch an das LAN angeschlossen ist.

Alternate (Alternativ) – Stellt für die Weiterleitung von Paketen zum Root-Switch einen zur Weiterleitung über die Schnittstelle alternativen Pfad bereit.

Backup (Reserve) – Stellt einen Reservepfad zum designierten LAN bereit. Reserveports treten nur auf, wenn zwei Ports durch eine Punkt-zu-Punkt-Verbindung in einer Schleife miteinander verbunden sind. Reserveports treten auch auf, wenn ein LAN zwei oder mehr Verbindungen zu einem gemeinsamen Segment aufweist.

Disabled (Deaktiviert) – Gibt an, dass der Port nicht an dem Spanning Tree teilnimmt.

Priority (Priorität) – Legt die Schnittstellenpriorität für die angegebene Instanz fest. Der Prioritätswert liegt zwischen 0 und 240 und wird in 16er-Schritten angegeben. Der Standardwert ist 128.

Path Cost (0–200000000) (Pfadkosten) – Gibt den Anteil dieses Ports an der Spanning-Tree-Instanz an. Der Wert sollte stets zwischen 0 und 200.000.000 liegen. Der Standardwert wird durch die Portgeschwindigkeit und die Pfadkostenmethode bestimmt. Der Standardwert ist:

- Portkanal bis 20.000
- 1.000 Mbit/s (Giga) bis 20.000
- 100 Mbit/s bis 200.000
- 10 Mbit/s bis 2.000.000

Designated Bridge ID (ID der designierten Bridge) – Zeigt die ID-Nummer der Bridge an, die die Verbindung oder das gemeinsame LAN mit dem Root-Gerät verbindet.

Designated Port ID (ID des designierten Ports) – Zeigt die ID-Nummer des Ports auf der designierten Bridge an, die die Verbindung oder das gemeinsame LAN mit dem Root-Gerät verbindet.

Designated Cost (Designierte Kosten) – Zeigt die Kosten des Pfads von der Verbindung oder dem gemeinsamen LAN zum Root-Gerät an.

Zuordnen von MSTP-Schnittstelleneinstellungen

1. Öffnen Sie die Seite **MSTP Interface Settings** (MSTP-Schnittstelleneinstellungen).
2. Wählen Sie im Dropdown-Menü **Instance ID** eine Instanz-ID.
3. Wählen Sie im Dropdown-Menü **Port** oder **LAG** die gewünschte Schnittstelle.
4. Legen Sie die **Interface Priority** (Schnittstellenpriorität) und die **Path Cost** (Pfadkosten) fest.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

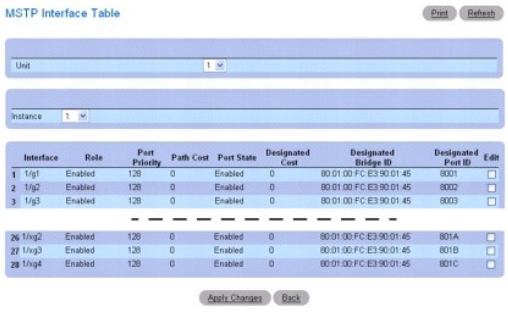
   Die Schnittstelleneinstellungen werden gespeichert, und das Gerät wird aktualisiert.

Anzeigen der Tabelle mit den MSTP-Schnittstelleneinstellungen

1. Öffnen Sie die Seite **MSTP Settings** (MSTP-Einstellungen).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **MSTP Interface Table** (MSTP-Schnittstellentabelle) wird angezeigt.

Abbildung 8-48. MSTP-Schnittstellentabelle



3. Über das Dropdown-Menü **Unit** (Einheit) können Sie die **MSTP Interface Table** (MSTP-Schnittstellentabelle) für andere ggf. im Stack vorhandene Einheiten anzeigen.
4. Um die Portpriorität oder Pfadkosten für eine oder mehrere Schnittstellen zu ändern, aktivieren Sie für die gewünschten Schnittstellen **Edit** (Bearbeiten).
5. Ändern Sie die Werte in den Spalten **Port Priority** (Portpriorität) oder **Path Cost** (Pfadkosten) nach Bedarf.
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Felder werden für die gewählten Schnittstellen geändert, und das Gerät wird aktualisiert.

Festlegen von MSTP-Schnittstellen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Spanning Tree Commands (Spanning Tree-Befehle)

Konfigurieren von VLANs

Durch zusätzliche Virtual LAN (VLAN)-Unterstützung eines Layer 2-Switches können einige Vorteile des Bridging sowie Routing genutzt werden. Wie eine Bridge leitet ein VLAN-Switch Datenverkehr auf Basis des Layer 2-Headers weiter, was die Geschwindigkeit erhöht, und wie ein Router unterteilt er das Netzwerk in logische Segmente und sorgt damit für verbesserte Administration, Sicherheit und Verwaltung von Multicast-Datenverkehr.

Ein VLAN umfasst Endstationen und Switch-Ports zu deren Verbindung. Für eine logische Unterteilung, wie z. B. nach Abteilung oder Projektteilnehmern, kann es viele Gründe geben. Die einzige Hardwarevoraussetzung ist, dass die Endstation und der Port, mit dem sie verbunden ist, zum selben VLAN gehören.

Jedes VLAN in einem Netzwerk hat eine eigene VLAN-ID, die im IEEE 802.1Q-Tag im Layer 2-Header der Pakete angegeben ist, die über das VLAN übertragen werden. Eine Endstation kann den Tag oder den VLAN-Teil des Tags übergehen. In diesem Fall kann der erste Switch-Port, der das Paket erhalten soll, es entweder ablehnen oder einen Tag einfügen, der auf seiner Standard-VLAN-ID basiert. Ein Port kann Datenverkehr für mehr als ein VLAN handhaben, doch nur eine VLAN-ID unterstützen.

Um die Seite VLAN *anzuzeigen*, klicken Sie in der Strukturansicht auf **Switching→ VLAN**. Die Seite **VLAN** enthält Links zu folgenden Themen:

- VLAN-Mitgliedschaft
- VLAN-Porteinstellungen
- VLAN-LAG-Einstellungen
- Binden von MAC an VLAN
- Binden von IP-Subnetz an VLAN
- Protokollgruppe
- GVRP-Parameter

VLAN-Mitgliedschaft

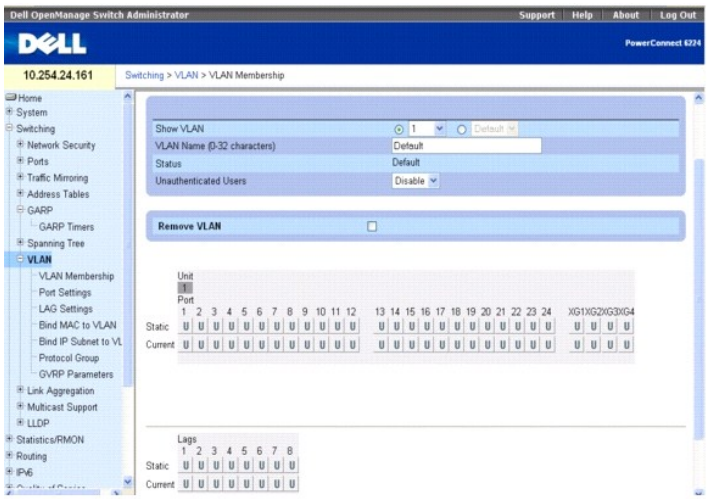
Auf der Seite **VLAN Membership** (VLAN-Mitgliedschaft) können Sie VLAN-Gruppen festlegen, die in der VLAN-Mitgliedschaftstabelle gespeichert werden. Ihr Switch unterstützt bis zu 4094 VLANs. Tatsächlich können Sie jedoch nur 4092 VLANs erstellen, weil:

- VLAN 1 das Standard-VLAN ist, dem alle Ports angehören, und
- VLAN 4095 als Discard-VLAN definiert ist

Es können VLANS mit den Nummern 2–4093 erstellt werden. VLAN 4094 ist reserviert.

Um die Seite **VLAN Membership** (VLAN-Mitgliedschaft) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ VLAN→ VLAN Membership (VLAN-Mitgliedschaft)**.

Abbildung 8-49. VLAN-Mitgliedschaft



Die Seite **VLAN Membership** (VLAN-Mitgliedschaft) ist in zwei Bereiche unterteilt. Der obere Bereich enthält die Felder zum Festlegen aller VLAN-Mitgliedschaften. Der untere Bereich enthält Tabellen zum Festlegen der Mitgliedschaftseinstellungen für bestimmte Ports und LAGs in dem VLAN. Unter **VLAN Membership** (VLAN-Mitgliedschaft) können folgende Felder ausgefüllt werden:

Show VLAN (VLAN anzeigen) – Wählt das anzuzeigende VLAN. Wählen Sie das VLAN entweder im Dropdown-Menü **VLAN ID** (VLAN-ID) oder **VLAN Name** (VLAN-Name).

VLAN Name (0–32) (VLAN-Name, 0-32) – Gibt den benutzerdefinierten VLAN-Namen an. Das Feld wird über die Schaltfläche **Add** (Hinzufügen) definiert. Gültige Namen können zwischen 0 und 32 Zeichen lang sein.

Status – Gibt den VLAN-Typ an. Mögliche Werte:

Dynamic (Dynamisch) – Gibt an, dass das VLAN dynamisch über GVRP erstellt wurde.

Static (Statisch) – Gibt an, dass das VLAN benutzerdefiniert ist und geändert werden kann.

Default (Standard) – Gibt an, dass es sich bei dem VLAN um das Standard-VLAN handelt.

Unauthenticated Users (Nicht authentifizierte Benutzer) – Ermöglicht nicht autorisierten Switches für den Zugriff auf dieses VLAN, wenn "Enable" (Aktiviert) gewählt ist.

Remove VLAN (VLAN entfernen) – Entfernt das angezeigte VLAN aus der VLAN-Mitgliedschaftstabelle.

Die Tabellen **VLAN Membership** (VLAN-Mitgliedschaft) zeigen an, welche Ports und LAGs Mitglieder des VLAN sind, sowie den Status T (Mit Kennung), U (Ohne Kennung) oder F (Nicht zulässig). Die Tabellen enthalten zwei Zeilen: **Static** (Statisch) und **Current** (Aktuell). Über diese Seite ist nur die Zeile **Static** (Statisch) zugänglich. Die Zeile **Current** (Aktuell) wird entweder dynamisch über GVRP aktualisiert oder nach Änderung der Zeile **Static** (Statisch) und Klicken auf **Apply Changes** (Änderungen übernehmen).

Dieser Bereich der Seite enthält zwei Tabellen:

Ports – Weist Ports VLAN-Mitgliedschaften zu und zeigt diese an. Um eine Mitgliedschaft zuzuweisen, klicken Sie für den gewünschten Port auf **Static** (Statisch). Mit jedem Mausklick wird zwischen U, T und Leer umgeschaltet. Die Zustände sind in folgender Tabelle definiert.

LAGs – Weist LAGs VLAN-Mitgliedschaften zu und zeigt diese an. Um eine Mitgliedschaft zuzuweisen, klicken Sie für die gewünschte LAG auf **Static** (Statisch). Mit jedem Mausklick wird zwischen U, T und Leer umgeschaltet. Die Zustände sind in folgender Tabelle definiert.

Tabelle 8-1. Definitionen für VLAN-Portmitgliedschaft

Portsteuerung	Definition
T	Tagged (Mit Kennung): Die Schnittstelle gehört einem VLAN an. Alle über die Schnittstelle weitergeleiteten Pakete haben eine Kennung. Die Pakete enthalten VLAN-Informationen.
U	Untagged (Ohne Kennung): Die Schnittstelle gehört einem VLAN an. Über die Schnittstelle weitergeleitete Pakete haben keine Kennung.
F	Forbidden (Nicht zulässig): Gibt an, dass eine VLAN-Mitgliedschaft für diese Schnittstelle nicht zulässig ist.
Leer	Keine Eingabe: Die Schnittstelle gehört keinem VLAN an. Mit der Schnittstelle verknüpfte Pakete werden nicht weitergeleitet.

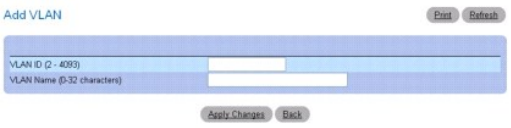
Hinzufügen neuer VLANs

1. Öffnen Sie die Seite **VLAN Membership** (VLAN-Mitgliedschaft).
2. Klicken Sie auf **Add**

   (Hinzufügen).

   Die Seite **Add VLAN** (VLAN hinzufügen) wird angezeigt.

Abbildung 8-50. VLAN hinzufügen



3. Geben Sie eine neue VLAN-ID und einen VLAN-Namen ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Das neue VLAN wird hinzugefügt und das Gerät aktualisiert.

Zuweisen einer VLAN-Mitgliedschaft zu einem Port oder einer LAG

1. Öffnen Sie die Seite **VLAN Membership** (VLAN-Mitgliedschaft).
2. Wählen Sie im Dropdown-Menü **VLAN ID** oder **VLAN Name** ein VLAN.

3. Zum Zuweisen eines Werts in der **VLAN Port Membership Table** (VLAN-Portmitgliedschaftstabelle) klicken Sie für den gewünschten Port oder die gewünschte LAG in die Zeile **Static** (Statisch). Mit jedem Mausklick wird zwischen U, T und Leer (kein Mitglied) umgeschaltet.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Port bzw. die LAG wird dem VLAN mit der gewählten Bezeichnung zugewiesen, in der Zeile **Current** (Aktuell) erscheint die aktuelle Bezeichnung, und das Gerät wird aktualisiert.

Modifizieren von VLAN-Mitgliedschaftsgruppen

1. Öffnen Sie die Seite **VLAN Membership** (VLAN-Mitgliedschaft).

2. Wählen Sie im Dropdown-Menü **VLANID (VLAN-ID) oder VLAN Name** (VLAN-Name) ein VLAN.

3. Ändern Sie die Felder je nach Bedarf.

4. Zum Ändern eines Port- oder LAG-Werts in der **VLAN Port Membership Table** (VLAN-Portmitgliedschaftstabelle) klicken Sie für den gewünschten Port oder die gewünschte LAG in die Zeile **Static** (Statisch). Mit jedem Mausklick wird zwischen U, T und Leer (kein Mitglied) umgeschaltet.

5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die VLAN-Mitgliedschaftsinformation wird geändert, in der Zeile **Current** (Aktuell) erscheint die geänderte Bezeichnung, und das Gerät wird aktualisiert.

Entfernen eines VLAN

1. Öffnen Sie die Seite **VLAN Membership** (VLAN-Mitgliedschaft).

2. Wählen Sie im Dropdown-Menü **VLAN ID** oder **VLAN Name** ein VLAN.

3. Aktivieren Sie das Kontrollkästchen **Remove VLAN** (VLAN entfernen).

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Das gewählte VLAN wird entfernt und das Gerät aktualisiert.

Festlegen von VLAN-Mitgliedschaftsgruppen und Zuweisen von Ports/LAGs mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- VLAN Commands (VLAN-Befehle)

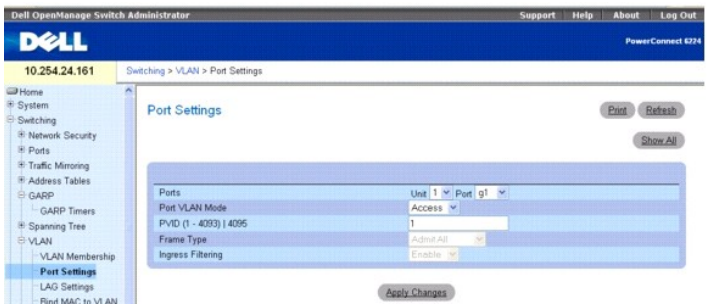
VLAN-Porteinstellungen

In einem portbasierten VLAN wird Datenverkehr ohne Kennung über spezifizierte Ports auf Basis der Empfangsport-PVID übertragen. Portbasierte VLANs können helfen, Netzwerk-Datenverkehrsmuster zu optimieren, da Broadcast-, Multicast- und Unknown-Unicast-Pakete nur an Ports gesendet werden, die Mitglieder des VLAN sind. Mit einer VLAN-Kennung empfangene Pakete verwenden die VLAN-ID für den Switching-Prozess.

Auf der Seite **VLAN Port Settings** (VLAN-Porteinstellungen) können Sie einen Port als Teil eines VLAN identifizieren sowie VLAN-Portparameter festlegen und ändern.

Um die Seite **VLAN Port Settings** (VLAN-Porteinstellungen) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ VLAN→ Port Settings** (Porteinstellungen).

Abbildung 8-51. VLAN-Porteinstellungen



Die Seite **VLAN Port Settings** (VLAN-Porteinstellungen) enthält folgende Felder:

Ports – Legt die Einheit und den Port fest, die im VLAN integriert sind.

Port VLAN Mode (Port-VLAN-Modus) – Gibt den Anschlussmodus an. Mögliche Werte:

General (Allgemeiner Modus) – Der Port gehört zu einem oder mehreren VLANs, die jeweils vom Benutzer als VLAN mit oder ohne Kennung definiert wurden (voller 802.1Q-Modus).

Access (Zugriffsmodus) – Der Port gehört zu einem einzigen VLAN ohne Kennung. Wenn sich ein Port im Zugriffsmodus befindet, können die auf dem Port akzeptierten Pakettypen nicht angegeben werden. Außerdem lässt sich für einen Port im Zugriffsmodus keine Ingress-Filterung aktivieren/deaktivieren.

Trunk – Der Port gehört zu mehr als einem VLAN, und alle Ports haben Kennungen (mit Ausnahme eines optionalen einfachen nativen VLAN).

PVID (1-4093) | 4095 – Weist Paketen ohne Kennung eine VLAN-ID zu. Mögliche Werte sind 1 bis 4093 und 4095.

Frame Type (Frame-Typ) – Gibt den auf dem Port akzeptierten Pakettyp an. Standardwert ist **Admit All** (Alle zulassen). Mögliche Werte:

Admit Tag Only (Nur mit Kennung zulassen) – Gibt an, dass nur Frames mit Kennung auf dem Port akzeptiert werden.

Admit All (Alle zulassen) – Gibt an, dass Frames mit und ohne Kennung auf dem Port akzeptiert werden.

Ingress Filtering (Ingress-Filterung) – Aktiviert oder deaktiviert die Ingress-Filterung auf dem Port. Bei der Ingress-Filterung werden Frames abgelehnt, bei denen die VLAN-Kennung nicht der Port-VLAN-Mitgliedschaft entspricht.

Zuweisen von Porteinstellungen

1. Öffnen Sie die Seite **VLAN Port Settings** (VLAN-Porteinstellungen).
2. Wählen Sie den Port, dem Sie Einstellungen zuordnen möchten, in den Dropdown-Menüs **Unit** (Einheit) und **Port**.
3. Füllen Sie die übrigen Felder auf der Seite aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die VLAN-Porteinstellungen werden definiert, und das Gerät wird aktualisiert.

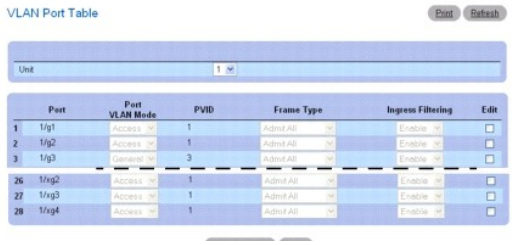
Anzeigen der VLAN-Porttabelle

1. Öffnen Sie die Seite **VLAN Port Settings** (VLAN-Porteinstellungen).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die **VLAN Port Table** (VLAN-Porttabelle) wird geöffnet.

Abbildung 8-52. VLAN-Porttabelle



ANMERKUNG: Bei Wahl von **Access** (Zugriffsmodus) für einen Port können die auf dem Port akzeptierten Pakettypen nicht angegeben werden. Außerdem lässt sich für einen Port im Zugriffsmodus keine Ingress-Filterung aktivieren oder deaktivieren.

3. Über das Dropdown-Menü **Unit** (Einheit) können Sie die **VLAN Port Table** (VLAN-Porttabelle) für andere ggf. im Stack vorhandene Einheiten anzeigen.

Ändern der Einstellungen für mehrere Ports

1. Öffnen Sie die Seite **VLAN Port Settings** (VLAN-Porteinstellungen).

2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die **VLAN Port Table** (VLAN-Porttabelle) wird geöffnet.

3. Klicken Sie für jeden zu ändernden Port auf **Edit** (Bearbeiten).

4. Bearbeiten Sie die Felder je nach Bedarf.

5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die VLAN-Porteinstellungen werden geändert, und das Gerät wird aktualisiert.

Zuweisen von Ports zu VLAN-Gruppen mit Hilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

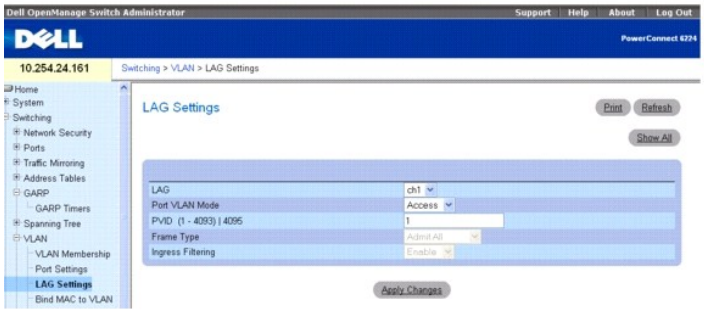
- VLAN Commands (VLAN-Befehle)

VLAN-LAG-Einstellungen

Auf der Seite **VLAN LAG Settings** (VLAN-LAG-Einstellungen) können Sie einem VLAN eine LAG zuweisen. Auf dem Switch eingehende Pakete ohne Kennung erhalten als Kennung die durch die PVID festgelegte LAG-ID.

Um die Seite **VLAN LAG Settings** (VLAN-LAG-Einstellungen) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching**→ **Ports**→ **LAG Settings** (LAG-Einstellungen).

Abbildung 8-53. VLAN-LAG-Einstellungen



Die Seite **VLAN LAG Settings** (VLAN-LAG-Einstellungen) enthält folgende Felder:

LAG – Gibt die Nummer der im VLAN enthaltenen LAG an.

Port VLAN Mode (Port-VLAN-Modus) – Gibt den Port-VLAN-Modus für die LAG an. Mögliche Werte:

General (Allgemeiner Modus) – Die LAG gehört zu einem oder mehreren VLANs, die jeweils vom Benutzer als VLAN mit oder ohne Kennung definiert wurden (voller 802.1Q-Modus).

Access (Zugriffsmodus) – Die LAG gehört zu einem einzigen VLAN ohne Kennung.

Trunk – Die LAG gehört zu mehr als einem VLAN, und alle Ports haben Kennungen (mit Ausnahme eines optionalen einfachen nativen VLAN).

PVID (1-4093) | 4095 – Weist Paketen ohne Kennung eine VLAN-ID zu. Mögliche Werte für das Feld sind 1 bis 4093 und 4095.

Frame Type (Frame-Typ) – Legt den von der LAG akzeptierten Pakettyp fest. Die Standardeinstellung ist **Admit Tag Only** (Nur mit Kennung zulassen). Mögliche Werte:

Admit Tag Only (Nur mit Kennung zulassen) – Die LAG akzeptiert nur Pakete mit Kennung.

Admit All (Alle zulassen) – Die LAG akzeptiert sowohl Pakete mit als auch ohne Kennung.

Ingress Filtering (Ingress-Filterung) – Aktiviert oder deaktiviert Ingress-Filterung durch die LAG. Bei der Ingress-Filterung werden Pakete abgelehnt, bei denen die VLAN-Kennung nicht der LAG-VLAN-Mitgliedschaft entspricht.

Zuweisen von VLAN-Einstellungen für LAGs

1. Öffnen Sie die Seite **VLAN LAG Settings** (VLAN-LAG-Einstellungen).

2. Wählen Sie im Dropdown-Menü **LAG** eine LAG
3. Füllen Sie die übrigen Felder auf der Seite aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die VLAN-Parameter für die LAG werden definiert und das Gerät aktualisiert.

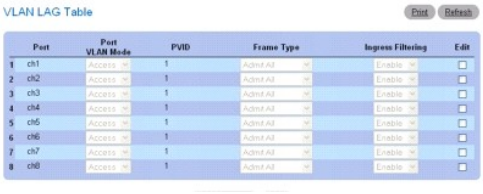
Anzeigen der VLAN-LAG-Tabelle

1. Öffnen Sie die Seite **VLAN LAG Settings** (VLAN-LAG-Einstellungen).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die **VLAN LAG Table** (VLAN-LAG-Tabelle) wird angezeigt.

Abbildung 8-54. VLAN-LAG-Tabelle



Ändern der Einstellungen für mehrere LAGs

1. Öffnen Sie die Seite **VLAN LAG Settings** (VLAN-LAG-Einstellungen).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die **VLAN LAG Table** (VLAN-LAG-Tabelle) wird angezeigt.
3. Klicken Sie für jede zu ändernde LAG auf **Edit** (Bearbeiten).
4. Bearbeiten Sie die Felder je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die VLAN-LAG-Einstellungen werden geändert, und das Gerät wird aktualisiert.

Zuweisen von LAGs zu VLAN-Gruppen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- VLAN Commands (VLAN-Befehle)

Binden von MAC an VLAN

Auf der Seite **Bind MAC to VLAN** (MAC an VLAN binden) können Sie der VLAN-Tabelle MAC-Einträge zuweisen. Nach Festlegen der MAC-Quelladresse und der VLAN-ID werden die MAC-VLAN-Konfigurationen von allen Ports des Switch gemeinsam verwendet. Die Tabelle zum Binden von MAC an VLAN unterstützt bis zu 128 Einträge.

Um die Seite **Bind MAC to VLAN** (MAC an VLAN binden) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ VLAN→ Bind MAC to VLAN (MAC an VLAN binden)**.

Abbildung 8-55. MAC an VLAN binden

Die Seite **Bind MAC to VLAN** (MAC an VLAN binden) enthält folgende Felder:

MAC Address (MAC-Adresse) – Legt die MAC-Adresse für ein VLAN fest.

Bind to VLAN (1-4093) (An VLAN binden) – Legt das VLAN fest, an das die MAC-Adresse gebunden wird.

Zuweisen von Einstellungen zum Binden von MAC an VLAN

1. Öffnen Sie die Seite **Bind MAC to VLAN** (MAC an VLAN binden).
2. Geben Sie die MAC-Adresse ein, die an das VLAN gebunden wird.
3. Geben Sie das VLAN ein, an das die MAC-Adresse gebunden wird.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

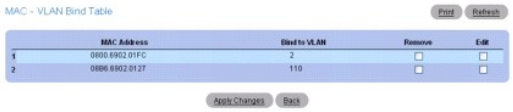
   Die angegebene MAC-Adresse und das VLAN werden verbunden, und das Gerät wird aktualisiert.

Anzeigen der VLAN-LAG-Tabelle

1. Öffnen Sie die Seite **Bind MAC to VLAN** (MAC an VLAN binden).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **MAC - VLAN Bind Table** (Tabelle zum Binden von MAC an VLAN) wird angezeigt.

Abbildung 8-56. Tabelle zum Binden von MAC an VLAN



Ändern von VLAN für mehrere MAC-Adressen

1. Öffnen Sie die Seite **Bind MAC to VLAN** (MAC an VLAN binden).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die **MAC - VLAN Bind Table** (Tabelle zum Binden von MAC an VLAN) wird angezeigt.
3. Klicken Sie für jede MAC-Adresse, dessen VLAN geändert werden soll, auf **Edit** (Bearbeiten).
4. Bearbeiten Sie die Felder **Bind to VLAN** (An VLAN binden).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die MAC-VLAN-Einstellungen werden geändert, und das Gerät wird aktualisiert.

Entfernen eines MAC-VLAN-Eintrags

1. Öffnen Sie die Seite **Bind MAC to VLAN** (MAC an VLAN binden).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **MAC - VLAN Bind Table** (Tabelle zum Binden von MAC an VLAN) wird angezeigt.
3. Aktivieren Sie für jeden zu entfernenden Eintrag **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Einträge werden entfernt, und das Gerät wird aktualisiert.

Binden von MACs an VLANs mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- VLAN Commands (VLAN-Befehle)

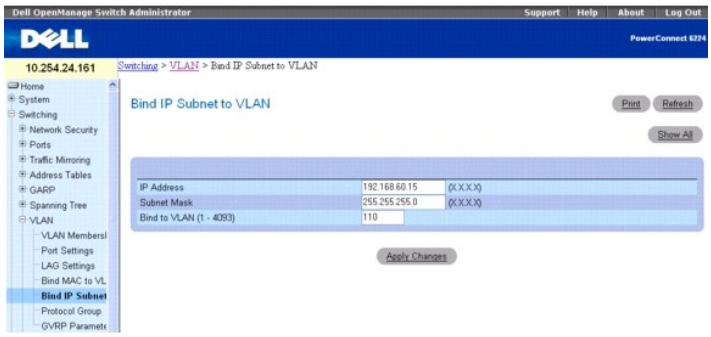
Binden von IP-Subnetz an VLAN

Zum Zuweisen eines IP-Subnetzes zu einem VLAN wird ein Eintrag in der IP-Subnetz-VLAN-Tabelle konfiguriert. Ein Eintrag wird über eine IP-Quelladresse, Netzwerkmaske und die gewünschte VLAN-ID festgelegt. Die IP-Subnetz-VLAN-Konfigurationen werden von allen Ports des Switches gemeinsam verwendet. In dieser Tabelle können bis zu 64 Einträge konfiguriert werden.

Auf der Seite **Bind IP Subnet to VLAN** (IP-Subnetz an VLAN binden) können Sie ein IP-Subnetz an ein VLAN binden.

Um die Seite **Bind IP Subnet to VLAN** (IP-Subnetz an VLAN binden) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ VLAN→ Bind IP Subnet to VLAN** (IP-Subnetz an VLAN binden).

Abbildung 8-57. IP-Subnetz an VLAN binden



Die Seite **Bind IP Subnet to VLAN** (IP-Subnetz an VLAN binden) enthält folgende Felder:

IP Address (IP-Adresse) – Legt die IP-Quelladresse des Pakets fest.

Subnet Mask (Subnetzmaske) – Legt die Quelladresse der IP-Subnetzmaske des Pakets fest.

Bind to VLAN (1–4093) (An VLAN binden, 1-4093) – Legt das VLAN fest, dem die IP-Adresse zuzuordnen ist.

Binden von IP-Subnetz an ein VLAN

1. Öffnen Sie die Seite **Bind IP Subnet to VLAN** (IP-Subnetz an VLAN binden).
2. Geben Sie die IP-Adresse ein, die an das VLAN gebunden werden soll.
3. Geben Sie das mit der IP-Adresse verbundene IP-Subnetz ein.
4. Geben Sie die VLAN-ID ein, der die IP-Adresse und Subnetzmaske zugewiesen werden.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das angegebene VLAN und IP-Subnetz werden verbunden, und das Gerät wird aktualisiert.

Anzeigen der Tabelle zum Binden von IP-Subnetz an VLAN

1. Öffnen Sie die Seite **Bind IP Subnet to VLAN** (IP-Subnetz an VLAN binden).
2. Klicken Sie auf **Show All** (Alle anzeigen).
3. Die **IP Subnet - VLAN Bind Table** (Tabelle zum Binden von IP-Subnetz an VLAN) wird angezeigt.

Abbildung 8-58. Tabelle zum Binden von IP-Subnetz an VLAN

Ändern der VLAN-Bindung für mehrere IP-Adressen

1. Öffnen Sie die Seite **Bind IP Subnet to VLAN** (IP-Subnetz an VLAN binden).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die **IP Subnet - VLAN Bind Table** (Tabelle zum Binden von IP-Subnetz an VLAN) wird angezeigt.
3. Klicken Sie für jeden zu ändernden Eintrag auf **Edit** (Bearbeiten).
4. Bearbeiten Sie die Felder je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die VLAN-Bindungseinstellungen werden geändert, und das Gerät wird aktualisiert.

Entfernen eines MAC-IP-Subnetz-Eintrags

1. Öffnen Sie die Seite **Bind IP Subnet to VLAN** (IP-Subnetz an VLAN binden).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **IP Subnet - VLAN Bind Table** (Tabelle zum Binden von IP-Subnetz an VLAN) wird angezeigt.
3. Aktivieren Sie für jeden zu entfernenden Eintrag **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Einträge werden entfernt, und das Gerät wird aktualisiert.

Binden von IP-Subnetzen an VLANs mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- VLAN Commands (VLAN-Befehle)

Protokollgruppe

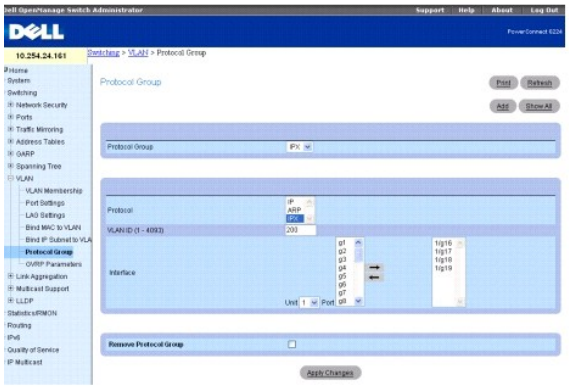
In einem protokollbasierten VLAN wird der Verkehr über festgelegte Ports auf Basis des VLAN-Protokolls übertragen. Benutzerdefinierte Paketfilter bestimmen, ob ein bestimmtes Paket zu einem bestimmten VLAN gehört. Protokollbasierte VLANs werden meist in Situationen verwendet, in denen Netzwerksegmente Hosts enthalten, auf denen mehrere Protokolle ausgeführt werden.

Auf der Seite **Protocol Group** (Protokollgruppe) können Sie konfigurieren, welche EtherTypes an welche VLANs gehen, und dann bestimmte Ports aktivieren,

so dass sie diese Einstellungen verwenden.

Um die Seite **Protocol Group** (Protokollgruppe) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching**→ **VLAN**→ **Protocol Group** (Protokollgruppe).

Abbildung 8-59. Protokollgruppe



Die Seite **Protocol Group** (Protokollgruppe) enthält folgende Felder:

Protocol Group (Protokollgruppe) – Zeigt den mit der Protokollgruppen-ID verknüpften Namen an. Um eine neue Gruppe zu erstellen, klicken Sie auf **Add** (Hinzufügen).

Protocol (Protokoll) – Legt das mit dieser Gruppe verbundene Protokoll fest.

VLAN ID (1-4093) – Legt die mit dieser Gruppe verbundene VLAN-ID fest.

Interface (Schnittstelle) – Wählt die Schnittstellen, die dieser Gruppe hinzugefügt oder daraus entfernt werden sollen. Markieren Sie die Schnittstellen, die in der Protokollgruppe enthalten sein sollen, und klicken Sie auf den Pfeil nach rechts. In der rechten Spalte werden die Schnittstellen angezeigt, die zu der Protokollgruppe gehören.

Remove Protocol Group (Protokollgruppe entfernen) – Entfernt die auf dem Bildschirm angezeigte Protokollgruppe, sobald Sie auf **Apply Changes** (Änderungen übernehmen) klicken. Um mehrere Gruppen gleichzeitig zu entfernen, klicken Sie auf **Show All** (Alle anzeigen), und markieren Sie in der **Protocol Group Table** (Protokollgruppentabelle) die Kontrollkästchen **Remove** (Entfernen).

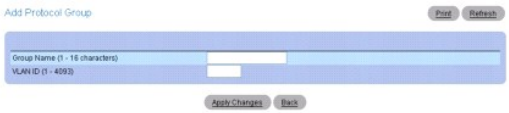
Hinzufügen einer Protokollgruppe

1. Öffnen Sie die Seite **Protocol Group** (Protokollgruppe).
2. Klicken Sie auf **Add**

   (Hinzufügen).

   Die Seite **Add Protocol Group** (Protokollgruppe hinzufügen) wird angezeigt.

Abbildung 8-60. Protokollgruppe hinzufügen



3. Geben Sie einen neuen Protokollgruppennamen und eine VLAN-ID für diese Gruppe ein.
4. Kehren Sie zur Seite **Protocol Group** (Protokollgruppe) zurück.
5. Wählen Sie die hinzugefügte Protokollgruppe und dann das Protokoll.
6. Markieren Sie in der ersten Spalte **Interface** (Schnittstelle) die der Protokollgruppe hinzuzufügenden Schnittstellen. Um mehrere Schnittstellen zu wählen, halten Sie dabei (für aufeinander folgende Schnittstellen) die Umschalttaste bzw. (für nicht aufeinander folgende Schnittstellen) die Strg-Taste gedrückt.
7. Klicken Sie auf den Nach-rechts-Pfeil.

   Gewählte Schnittstellen werden in die zweite Spalte verschoben. Alle Schnittstellen in dieser Spalte gehören zu der Protokollgruppe.

8. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Protokollgruppe wird hinzugefügt und das Gerät aktualisiert.

Ändern der VLAN-Protokollgruppeneinstellungen

1. Öffnen Sie die Seite **Protocol Group** (Protokollgruppe).
2. Legen Sie im Dropdown-Menü **Protocol Group ID** (Protokollgruppen-ID) das zu ändernde Protokoll fest.
3. Ändern Sie das Protokoll oder die VLAN-ID je nach Bedarf.
4. Um der Gruppe eine Schnittstelle hinzuzufügen, markieren Sie die gewünschte Schnittstelle in der ersten Spalte. Um mehrere Schnittstellen zu wählen, halten Sie dabei (für aufeinander folgende Schnittstellen) die Umschalttaste bzw. (für nicht aufeinander folgende Schnittstellen) die Strg-Taste gedrückt.
5. Klicken Sie auf den Nach-rechts-Pfeil.

   Gewählte Schnittstellen werden in die zweite Spalte verschoben. Alle Schnittstellen in dieser Spalte gehören zu der Protokollgruppe.
6. Um eine Schnittstelle aus der Gruppe zu entfernen, markieren Sie die gewünschte Schnittstelle in der zweiten Spalte.
7. Klicken Sie auf den Pfeil nach links.

   Die gewählte Schnittstelle wird aus der zweiten Spalte entfernt.
8. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die VLAN-Protokollgruppenparameter werden geändert, und das Gerät wird aktualisiert.

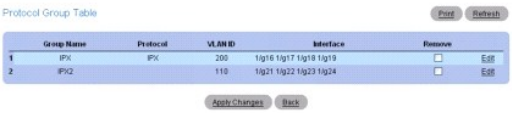
Removing Multiple Protocols From the Protocol Group Table

1. Öffnen Sie die Seite **Protocol Group** (Protokollgruppe).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die Seite **Protocol Group** (Protokollgruppe) wird geöffnet.

Abbildung 8-61. Protokollgruppentabelle



3. Markieren Sie für die zu entfernenden Protokollgruppen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Das Protokoll wird entfernt und das Gerät aktualisiert.

Konfigurieren von Protokollgruppen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- VLAN Commands (VLAN-Befehle)

GVRP-Parameter

Mit dem GARP-VLAN-Registrierungsprotokoll können Netzwerk-Switches dynamisch VLAN-Mitgliedschaftsinformationen bei den MAC-Netzwerk-Switches registrieren (und abmelden), die mit demselben Segment verbunden sind, damit diese Informationen auf alle Netzwerk-Switches in dem Bridged-LAN verteilt werden, die GVRP unterstützen.

Die Funktion von GVRP hängt von den Diensten ab, die vom Generic Attribute Registration Protocol (GARP) bereitgestellt werden. GVRP kan bis zu 1.024 VLANs erzeugen.

Auf der Seite **GVRP Global Parameters** (Globale GVRP-Parameter) können Sie GVRP global aktivieren. Sie können GVRP auch für einzelne Schnittstellen aktivieren.

Um die Seite **GVRP Global Parameters** (Globale GVRP-Parameter) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ VLAN→ GVRP Parameters**.

Abbildung 8-62. Globale GVRP-Parameter

Die Seite **GVRP Global Parameters** (Globale GVRP-Parameter) enthält folgende Felder:

GVRP Global Status (Globaler GVRP-Status) – Aktiviert oder deaktiviert GVRP auf dem Switch. GVRP ist standardmäßig deaktiviert.

Interface (Schnittstelle) – Legt die Einheit und den Port oder die LAG fest, für die GVRP aktiviert ist.

GVRP State (GVRP-Zustand) – Aktiviert oder deaktiviert GVRP auf der gewünschten Schnittstelle.

Dynamic VLAN Creation (Dynamische VLAN-Erstellung) – Aktiviert oder deaktiviert die VLAN-Erstellung über GVRP.

GVRP Registration (GVRP-Registrierung) – Aktiviert oder deaktiviert die GVRP-Registrierung.

Aktivieren von GVRP auf dem Switch

1. Öffnen Sie die Seite **GVRP Global Parameters** (Globale GVRP-Parameter).
2. Wählen im Feld **GVRP Global Status** (Globaler GVRP-Status) **Enable** (Aktivieren).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   GVRP wird auf dem Switch aktiviert.

Aktivieren der VLAN-Registrierung durch GVRP

1. Öffnen Sie die Seite **GVRP Global Parameters** (Globale GVRP-Parameter).
2. Wählen Sie im Feld **Global GVRP State** (Globaler GVRP-Zustand) für das gewünschte Gerät **Enable** (Aktivieren).
3. Wählen im Feld **GVRP Registration** (GVRP-Registrierung) **Enable** (Aktivieren).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

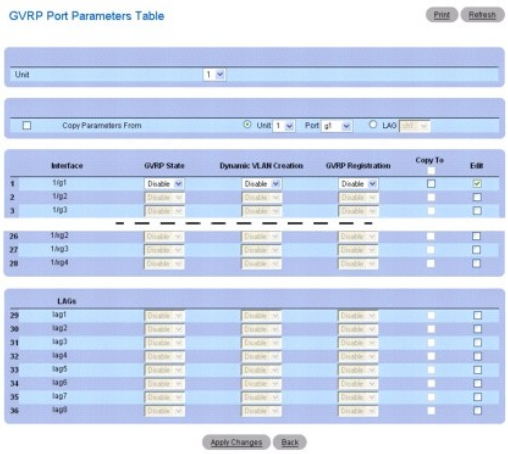
   Die GVRP-VLAN-Registrierung wird auf dem Port aktiviert, und das Gerät wird aktualisiert.

Anzeigen der GVRP-Portparametertabelle

1. Öffnen Sie die Seite **GVRP Global Parameters** (Globale GVRP-Parameter).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **GVRP Port Parameters Table** (GVRP-Portparametertabelle) wird angezeigt.

Abbildung 8-63. GVRP-Portparametertabelle



3. Über das Dropdown-Menü **Unit** (Einheit) können Sie die **GVRP Port Table** (GVRP-Porttabelle) für andere ggf. im Stack vorhandene Einheiten anzeigen.

Kopieren von GVRP-Parametern

1. Öffnen Sie die Seite **GVRP Global Parameters** (Globale GVRP-Parameter).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **GVRP Port Parameters Table** (GVRP-Portparametertabelle) wird angezeigt.
3. Legen Sie in **Copy Parameters From** (Parameter kopieren aus) die Einheit oder LAG fest, aus der kopiert werden soll.
4. Klicken Sie für jede Schnittstelle, die diese Parameter erhalten soll, auf **Copy To** (Kopieren zu).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die GVRP-Portparametereinstellungen werden kopiert, und das Gerät wird aktualisiert.

Ändern der GVRP-Parameter für mehrere Ports

1. Öffnen Sie die Seite **GVRP Global Parameters** (Globale GVRP-Parameter).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **GVRP Port Parameters Table** (GVRP-Portparametertabelle) wird angezeigt.
3. Klicken Sie für jede zu ändernde Schnittstelle/LAG auf **Edit** (Bearbeiten).
4. Bearbeiten Sie die GVRP-Portparameter-Felder je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die GVRP-Portparametereinstellungen werden geändert, und das Gerät wird aktualisiert.

Konfigurieren von GVRP mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- GVRP Commands (GVRP-Befehle)

Aggregieren von Ports

Bei der Link-Aggregation können ein oder mehrere Fullduplex (FDX)-Ethernet-Links zu einer Link Aggregation Group (LAG) aggregiert werden. Dadurch kann der Netzwerk-Switch die LAG wie eine einzige Verbindung behandeln.

Statische LAGs werden unterstützt. Wenn ein Port einer LAG als statisches Mitglied hinzugefügt wird, sendet und empfängt er keine LACPDUs.

Um die Menüseite **Link Aggregation** (Link-Aggregation) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Link Aggregation** (Link-Aggregation). Die Seite **Link Aggregation** (Link-Aggregation) enthält Links zu folgenden Themen:

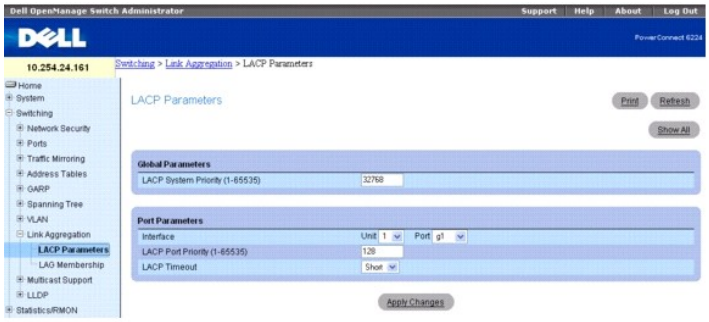
- LACP-Parameter
- LAG-Mitgliedschaft
- LAG-Hash-Konfiguration
- LAG-Hash-Übersicht

LACP-Parameter

Link-Aggregation wird durch die periodischen Änderungen der LACPDUs initiiert und gewartet. Auf der Seite **LACP Parameters** (LACP-Parameter) können Sie LACP-LAGs konfigurieren.

Um die Seite **LACP Parameters** (LACP-Parameter) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Link Aggregation (Link-Aggregation)→ LACP Parameters (LACP-Parameter)**.

Abbildung 8-64. LACP-Parameter



Die Seite **LACP Parameters** (LACP-Parameter) ist in zwei Bereiche unterteilt, **Global Parameters** (Globale Parameter) und **Port Parameters** (Portparameter), und enthält folgende Felder:

Globale Parameter

LACP System Priority (1-65535) (LACP-Systempriorität, 1-65535) – Gibt den LACP-Prioritätswert für globale Einstellungen an. Der Standardwert ist 1.

Portparameter

Interface (Schnittstelle) – Legt die Nummer der Einheit und des Ports fest, denen Zeitüberschreitungs- und Prioritätswerte zugewiesen sind.

LACP Port Priority (1-65535) (LACP-Portpriorität, 1-65535) – Legt den LACP-Prioritätswert für den gewünschten Port fest. Der Standardwert ist 1.

LACP Timeout (LACP-Zeitüberschreitung) – Legt die administrierte LACP-Zeitüberschreitung fest. Mögliche Werte:

Short (Kurz) – Legt eine kurze Zeitüberschreitung fest.

Long (Lang) – Legt eine lange Zeitüberschreitung fest. Dies ist die Standardeinstellung.

Festlegen von Link-Aggregation-Parametern

1. Öffnen Sie die Seite **LACP Parameters** (LACP-Parameter).
2. Füllen Sie die Felder je nach Bedarf aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Parameter werden festgelegt, und das Gerät wird aktualisiert.

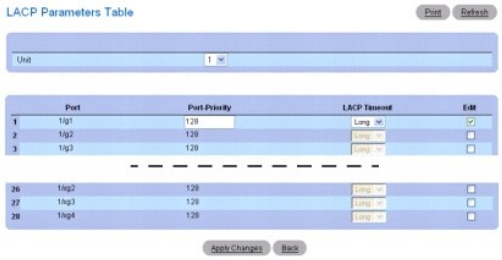
Anzeigen der LACP-Parametertabelle

1. Öffnen Sie die Seite ***LACP Parameters*** (LACP-Parameter).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die ***LACP Parameters Table*** (LACP-Parametertabelle) wird angezeigt.

Abbildung 8-65. LACP-Parametertabelle



3. Über das Dropdown-Menü **Unit** (Einheit) können Sie die **LACP Port Table** (LACP-Porttabelle) für andere ggf. im Stack vorhandene Einheiten anzeigen.

Ändern der LACP-Parameter für mehrere Ports

1. Öffnen Sie die Seite ***LACP Parameters*** (LACP-Parameter).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die ***LACP Parameters Table*** (LACP-Parametertabelle) wird angezeigt.
3. Klicken Sie für jeden zu ändernden Port auf **Edit** (Bearbeiten).
4. Bearbeiten Sie die Felder je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die LACP-Parametereinstellungen werden geändert, und das Gerät wird aktualisiert.

Konfigurieren von LACP-Parametern mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

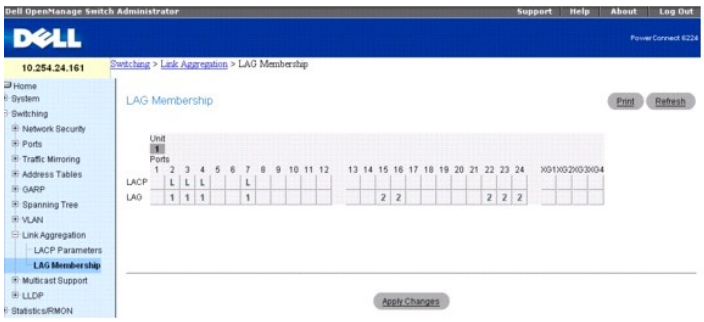
- LACP Commands (LACP-Befehle)

LAG-Mitgliedschaft

Der Switch unterstützt 18 LAGs pro System und acht Ports pro LAG. Auf der Seite **LAG Membership** (LAG-Mitgliedschaft) können Sie Ports bestimmten LAGs und LACPs zuweisen.

Um die Seite **LAG Membership** (LAG-Mitgliedschaft) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Link Aggregation (Link-Aggregation)→ LAG Membership (LAG-Mitgliedschaft)**.

Abbildung 8-66. LAG-Mitgliedschaft



Die Seite **LAG Membership** (LAG-Mitgliedschaft) enthält eine Tabelle mit folgenden Feldern:

LACP – Weist einen LAG-Port einer LACP-Mitgliedschaft zu. Für Ports mit einer Nummer in der Zeile LAG können Sie LACP durch Klicken in die Zeile **LACP** einschalten. Mit jedem Mausklick wird zwischen L (LACP) und Leer (keine LACP) umgeschaltet.

LAG – Fügt den Port einer LAG hinzu und gibt die spezifische LAG an, zu der der Port gehören soll. Für die LAG-Nummern lässt sich durch Klicken ein Wert von 1 bis 18 und anschließend Leer (keine LAG zugewiesen) einstellen.

Einer LAG einen Port hinzufügen

1. Öffnen Sie die Seite **LAG Membership** (LAG-Mitgliedschaft).
2. Klicken Sie in die Zeile **LAG**, um den Port in die gewünschte LAG zu schalten.

   Die LAG-Nummer für den Port wird angezeigt. Für die LAG-Nummer lässt sich durch Klicken ein Wert von 1 bis 18 und anschließend Leer (keine LAG zugewiesen) einstellen.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Port wird der gewählten LAG hinzugefügt und das Gerät aktualisiert.

Hinzufügen eines LAG-Ports zu einem LACP

1. Öffnen Sie die Seite **LAG Membership** (LAG-Mitgliedschaft).
2. Klicken Sie in die Zeile **LACP**, um den gewünschten LAG-Port auf **L** zu setzen.

ANMERKUNG: Der Port muss erst einer LAG zugewiesen werden, damit er zu einer LACP aggregiert werden kann.

3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der LAG-Port wird zu der LACP aggregiert und das Gerät aktualisiert.

Zuweisen von Anschlüssen zu LAGs und LACPs mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

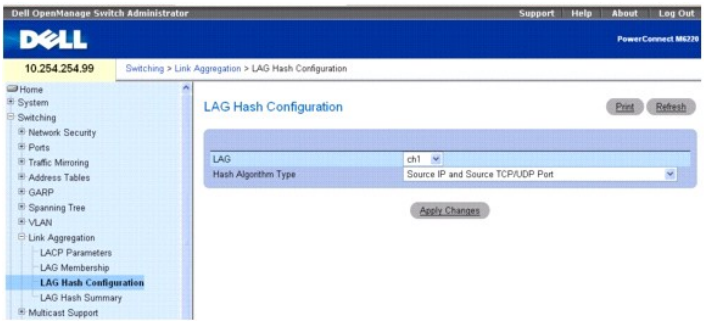
- Port Channel Commands (Portkanal-Befehle)

LAG-Hash-Konfiguration

Der LAG-HASH-Algorithmus dient zum Einstellen des Distributionsmodus für den Datenverkehr am Aggregator-Link. Sie können den HASH-Typ für jeden Trunk individuell einstellen.

Um die Seite **LAG Hash Configuration** (LAG-Hash-Konfiguration) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Link Aggregation (Link-Aggregation)→ LAG Hash Configuration (LAG-Hash-Konfiguration)**.

Abbildung 8-67. LAG-Hash-Konfiguration



Die Seite **LAG Hash Configuration** (LAG-Hash-Konfiguration) enthält folgende Felder:

LAG – Im Dropdown-Menü sind die LAG-Nummern aufgeführt.

Hash Algorithm Type (Hash-Algorithmus-Typ) – Es wird zwischen folgenden HASH-Algorithmus-Typen für Unicast-Datenflüsse unterschieden:

- Quell-MAC, VLAN, EtherType, SourceModule und Port-ID
- Ziel-MAC, VLAN, EtherType, SourceModule und Port-ID
- Quell-IP und Quell-TCP/UDP-Port (Standard)
- Ziel-IP und Ziel-TCP/UDP-Port
- Quell/Ziel-MAC, VLAN, EtherType, Quell-MODID/Port
- Quell/Ziel-IP und Quell/Ziel-TCP/UDP-Port

Konfigurieren des LAG-Hash

1. Öffnen Sie die Seite **LAG Hash Configuration** (LAG-Hash-Konfiguration).
2. Wählen Sie die zu konfigurierende LAG und den Hash-Algorithmus, den Sie der LAG zuweisen wollen.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Parameter werden geändert, und das Gerät wird aktualisiert.

Konfigurieren des LAG-Hash mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

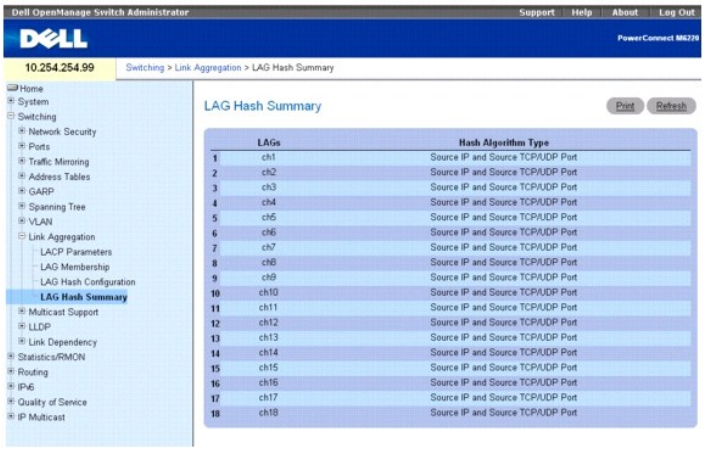
- Port Channel Commands (Portkanal-Befehle)

LAG-Hash-Übersicht

Auf der Seite **LAG Hash Summary** (LAG-Hash-Übersicht) sind die Kanäle des Systems und die ihnen zugewiesenen Hash-Alogorithmustypen aufgeführt.

Um die Seite **LAG Hash Summary** (LAG-Hash-Übersicht) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Link Aggregation (Link-Aggregation) → LAG Hash Summary (LAG-Hash-Übersicht)**.

Abbildung 8-68. LAG-Hash-Übersicht



Die Seite **LAG Hash Summary** (LAG-Hash-Übersicht) enthält eine Tabelle mit folgenden Feldern:

LAGs – Listet die LAG-Nummern auf.

Hash Algorithm Type – Zeigt den Typ des mit der LAG verknüpften HASH-Algorithmus für Unicast-Datenverkehr an.

Anzeigen der Hash-Algorithmus-Übersicht mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Port Channel Commands (Portkanal-Befehle)

Verwalten der Multicast-Unterstützung

Die **Layer 2 Multicast Forwarding Database** (Datenbank zur L2-Multicast-Weiterleitung) wird vom Switch verwendet, um Entscheidungen zur Weiterleitung von Paketen zu treffen, die mit einer Multicast-MAC-Zieladresse eingehen. Durch Beschränken von Multicasts auf bestimmte Ports im Switch gelangt der Datenverkehr nicht in Teile des Netzwerks, in denen er unnötig ist.

Beim Eintreffen eines Pakets im Switch wird die MAC-Zieladresse mit der VLAN-ID kombiniert und in der **Layer 2 Forwarding Database** (Datenbank zur L2-Weiterleitung) eine Suche ausgeführt. Wenn keine Entsprechung gefunden wird, wird das Paket je nach Switch-Konfiguration entweder an alle Ports im VLAN gesendet oder abgelehnt. Wenn eine Entsprechung gefunden wird, wird das Paket nur an die Ports weitergeleitet, die Mitglied der Multicast-Gruppe sind.

Um die Menüseite **Multicast Support** *(Multicast-Unterstützung)* anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Multicast Support (Multicast-Unterstützung)**. Die Seite **Multicast Support** (Multicast-Unterstützung) enthält Links zu folgenden Themen:

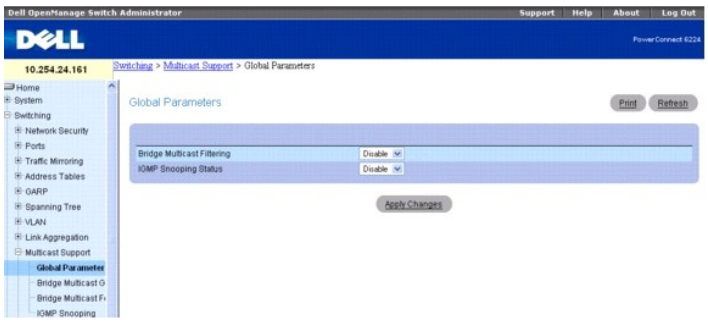
- Globale Multicast-Parameter
- Bridge-Multicast-Gruppe
- Bridge-Multicast-Weiterleitung
- IGMP-Snooping

Globale Multicast-Parameter

Auf der Seite **Multicast Global Parameters** (Globale Multicast-Parameter) können Sie die Bridge-Multicast-Filterung oder IGMP-Snooping für den Switch aktivieren. Die Parameter dieser Funktionen können auf den Webseiten **Bridge Multicast Forward** (Bridge-Multicast-Weiterleitung) und **IGMP Snooping** geändert werden.

Um die Seite **Multicast Global Parameters** (Globale Multicast-Parameter) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Multicast Support (Multicast-Unterstützung)→ Global Parameters (Globale Parameter)**.

Abbildung 8-69. Globale Multicast-Parameter



Die Seite **Multicast Global Parameters** (Globale Multicast-Parameter) enthält folgende Felder:

Bridge Multicast Filtering (Bridge-Multicast-Filterung) – Aktiviert oder deaktiviert die Bridge-Multicast-Filterung. Der Standardwert ist **Disabled** (Deaktiviert).

IGMP Snooping Status (IGMP-Snooping-Status) – Aktiviert oder deaktiviert IGMP-Snooping. Der Standardwert ist **Disabled** (Deaktiviert).

Aktivieren von Bridge-Multicast-Filterung auf dem Switch

1. Öffnen Sie die Seite **Multicast Global Parameters** (Globale Multicast-Parameter).
2. Wählen Sie im Feld **Bridge Multicast Filtering** (Bridge-Multicast-Filterung) **Enable** (Aktivieren).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Bridge Multicast-Filterung wird für den Switch aktiviert.

Aktivieren von Multicast-Weiterleitung und/oder IGMP-Snooping mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

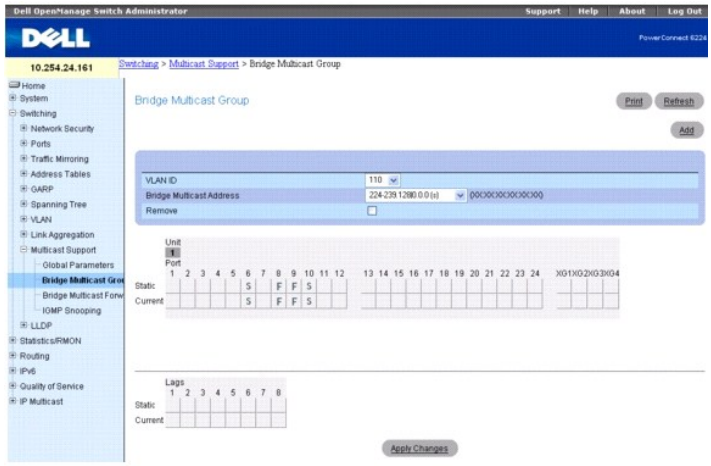
- Address Table Commands (Adresstabellenbefehle)

Bridge-Multicast-Gruppe

Auf der Seite ***Bridge Multicast Group*** (Bridge-Multicast-Gruppe) *können Sie neue Multicast-Servicegruppen erstellen oder Ports und LAGs* ändern, die vorhandenen Multicast-Servicegruppen zugewiesen sind. Die verbundenen Schnittstellen werden in den Tabellen **Port** und **LAG** angezeigt und geben Aufschluss über die Art Ihrer Zugehörigkeit zu der Multicast-Gruppe.

Um die Seite ***Bridge Multicast Group*** (Bridge-Multicast-Gruppe) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching**→ **Multicast Support**→ ***Bridge Multicast Group (Bridge-Multicast-Gruppe)***.

Abbildung 8-70. Bridge-Multicast-Gruppe



Die Seite ***Bridge Multicast Group*** enthält folgende Felder:

VLAN ID (VLAN-ID) – Wählt die VLAN, der eine Multicast-Gruppe hinzugefügt werden soll, oder zum Ändern von Ports in einer vorhandenen Multicast-Gruppe.

Bridge Multicast Address (Bridge-Multicast-Adresse) – Gibt die MAC/IP-Adresse der Multicast-Gruppe an, die der gewählten VLAN-ID zugewiesen ist. Über die Schaltfläche **Add** (Hinzufügen) können Sie einer VLAN-ID eine neue Adresse zuordnen.

Remove (Entfernen) – Entfernt eine Bridge-Multicast-Adresse.

Port- und LAG-Mitgliedstabellen

Die Tabellen ***Bridge Multicast Group*** (Bridge-Multicast-Gruppe) zeigen an, welche Ports und LAGs zur Multicast-Gruppe gehören und ob sie statisch (S), dynamisch (D) oder nicht zulässig (F) sind. Die Tabellen enthalten zwei Zeilen: **Static** (Statisch) und **Current** (Aktuell). Über diese Seite ist nur die Zeile **Static** (Statisch) zugänglich. Die Zeile **Current** (Aktuell) wird nach Änderung der Zeile **Static** (Statisch) und Klicken auf **Apply Changes** (Änderungen übernehmen) aktualisiert.

Die Seite ***Bridge Multicast Group*** (Bridge-Multicast-Gruppe) enthält zwei Tabellen, die bearbeitet werden können:

Units and Ports (Einheiten und Ports) – Weist Ports Multicast-Gruppen-Mitgliedschaften zu und zeigt diese an. Um eine Mitgliedschaft zuzuweisen, klicken Sie für den gewünschten Port auf **Static** (Statisch). Mit jedem Mausklick wird zwischen S, F und Leer Die Zustände sind in folgender Tabelle definiert.

LAGs – Weist LAGs Multicast-Gruppen-Mitgliedschaften zu und zeigt diese an. Um eine Mitgliedschaft zuzuweisen, klicken Sie für die gewünschte LAG auf **Static** (Statisch). Mit jedem Mausklick wird zwischen S, F und Leer Die Zustände sind in folgender Tabelle definiert.

Folgende Tabelle enthält Definitionen für Port/LAG-IGMP-Verwaltungseinstellungen.

Tabelle 8-2. LAG-IGMP-Verwaltungseinstellungen

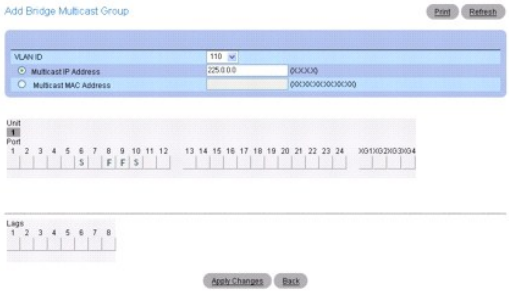
Portsteuerung	Definition
D	Dynamisch: Gibt in der Zeile *Current* (Aktuell) an, dass der Port bzw. die LAG der Multicast-Gruppe dynamisch beigetreten ist.
S	Statisch: Verknüpft den Port in der Zeile *Static* (Statisch) als statisches Mitglied mit der Multicast-Gruppe. Zeigt die Zeile *Current* (Aktuell) an, sobald auf **Apply Changes** (Änderungen übernehmen) geklickt wird.
Leer	Keine Eingabe: Gibt an, dass der Port mit keiner Multicast-Gruppe verknüpft ist.

Hinzufügen von Bridge-Multicast-Adressen

1. Öffnen Sie die Seite ***Bridge Multicast Group*** (Bridge-Multicast-Gruppe).
2. Klicken Sie auf **Add (Hinzufügen).**

   Die Seite **Add *Bridge Multicast Group*** (Bridge-Multicast-Gruppe hinzufügen) wird angezeigt.

Abbildung 8-71. Bridge-Multicast-Gruppe hinzufügen



3. Wählen Sie im Dropdown-Menü **VLAN ID** eine ID.
4. Definieren Sie die **IP- oder MAC-Adresse** für **New Bridge Multicast** (Neuer Bridge-Multicast).
5. Zum Zuweisen einer Einstellung in den ***Bridge Multicast Group Tables*** (Bridge-Multicast-Gruppen-Tabellen) klicken Sie für den gewünschten Port oder die gewünschte LAG in die Zeile **Static** (Statisch). Mit jedem Mausklick wird zwischen S, F und Leer (kein Mitglied) umgeschaltet.
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Bridge-Multicast-Adresse wird der Multicast-Gruppe zugewiesen und die Ports/LAGs der Gruppe, wobei die Zeilen **Current** (Aktuell) auf die Einstellungen von **Static** (Statisch) abgestimmt werden, und das Gerät wird aktualisiert.

Zuweisen einer Schnittstelle zu einer Multicast-Gruppe

1. Öffnen Sie die Seite ***Bridge Multicast Group*** (Bridge-Multicast-Gruppe).

2. Wählen Sie im Dropdown-Menü **VLAN ID** eine ID.

   Die zugehörige **Bridge Multicast Address** (Bridge-Multicast-Adresse) wird angezeigt.

3. Zum Zuweisen einer Einstellung in den ***Bridge Multicast Group Tables*** (Bridge-Multicast-Gruppen-Tabellen) klicken Sie für den gewünschten Port oder die gewünschte LAG in die Zeile **Static** (Statisch). Mit jedem Mausklick wird zwischen S, F und Leer (kein Mitglied) umgeschaltet.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Schnittstelle wird der Multicast-Gruppe zugewiesen, die Zeile **Current** (Aktuell) wird auf die Einstellung von **Static** (Statisch) abgestimmt, und das Gerät wird aktualisiert.

Entfernen einer Bridge-Multicast-Gruppe

1. Öffnen Sie die Seite ***Bridge Multicast Group*** (Bridge-Multicast-Gruppe).

2. Wählen Sie im Dropdown-Menü die **VLAN ID**, die der zu entfernenden Bridge-Multicast-Gruppe zugeordnet ist.

   Die **Bridge Multicast Address** (Bridge-Multicast-Adresse) und die zugewiesenen Ports/LAGs werden angezeigt.

3. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die gewählte Bridge-Multicast-Gruppe wird entfernt und das Gerät aktualisiert.

Verwalten von Multicast-Dienst-Mitgliedern mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

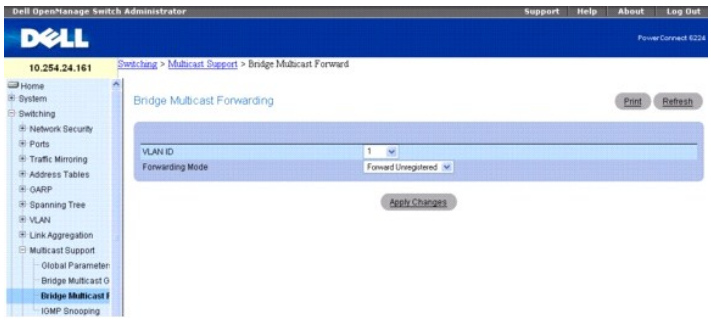
- Address Table Commands (Adresstabellenbefehle)

Bridge-Multicast-Weiterleitung

Auf der Seite ***Bridge Multicast Forward*** (Bridge-Multicast-Weiterleitung) können Sie das Anbinden von Ports oder LAGs an einen Switch aktivieren, der mit einem benachbarten Multicast-Switch verbunden ist. Nach Aktivieren von IGMP-Snooping werden die Multicast-Pakete an den entsprechenden Port bzw. das entsprechende VLAN weitergeleitet.

Um die Seite ***Bridge Multicast Forward*** (Bridge-Multicast-Weiterleitung) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching**→ **Multicast Support (Multicast-Unterstützung)**→ ***Bridge Multicast Forward (Bridge-Multicast-Weiterleitung)***.

Abbildung 8-72. Bridge-Multicast-Weiterleitung



Die Seite ***Bridge Multicast Forward*** (Bridge-Multicast-Weiterleitung) enthält folgende Felder und zwei Tabellen, die bearbeitet werden können:

VLAN ID – Wählt das betreffende VLAN.

Forwarding Mode (Weiterleitungsmodus) – Legt den Multicast-Weiterleitungsmodus für das gewählte VLAN fest. Mögliche Werte:

Forward Unregistered (Unregistrierte weiterleiten) – Erlaubt die Weiterleitung von IPv4-Multicast-Paketen mit einer Zieladresse, die keiner der zuvor in "IGMP Membership Reports" (IGMP-Mitgliedschaftsberichte) angekündigten Gruppen entspricht.

Forward All (Alle weiterleiten) – Erlaubt die Weiterleitung registrierter und unregistrierter Multicast-Pakete.

Filter Unregistered (Unregistrierte filtern) – Verhindert die Weiterleitung von IPv4-Multicast-Paketen mit einer Zieladresse, die keiner der zuvor in "IGMP

Membership Reports" (IGMP-Mitgliedschaftsberichte) angekündigten Gruppen entspricht.

Ändern des Bridge-Multicast-Weiterleitungsmodus

1. Öffnen Sie die Seite ***Bridge Multicast Forward*** (Bridge-Multicast-Weiterleitung).
2. Wählen Sie im Dropdown-Menü **VLAN ID** eine ID.
3. Wählen Sie im Dropdown-Menü den **Forwarding Mode** (Weiterleitungsmodus), der dem VLAN zugewiesen werden soll.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Das VLAN wechselt in den gewählten **Forwarding Mode** (Weiterleitungsmodus), und das Gerät wird aktualisiert.

Verwalten von mit Multicast-Routern verbundenen LAGs und Ports mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

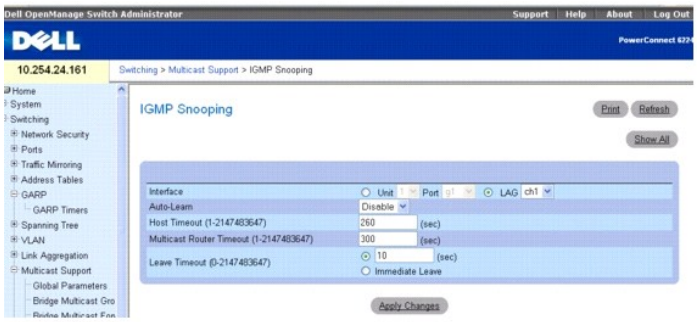
- Address Table Commands (Adresstabellenbefehle)

IGMP-Snooping

Auf der Seite ***IGMP Snooping*** können Sie IGMP-Mitglieder hinzufügen.

Um die Seite ***IGMP Snooping*** (IGMP-Snooping) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ Multicast Support (Multicast-Unterstützung)→ *IGMP Snooping*** (IGMP- Snooping).

Abbildung 8-73. IGMP-Snooping



Die Seite ***IGMP Snooping*** enthält folgende Felder:

Interface (Schnittstelle) – Wählt die betroffene Einheit und den betroffenen Port.

Auto Learn (Autom. Erfassen) – Aktiviert oder deaktiviert das automatische Erfassen auf dem Switch.

Host Timeout (Host-Zeitüberschreitung) – Legt die Speicherdauer eines IGMP-Snooping-Eintrags fest. Der Standardwert ist 260 Sekunden.

Multicast Router Timeout (Multicast-Router-Zeitüberschreitung) – Legt die Speicherdauer eines Multicast-Routereintrags fest. Der Standardwert ist 300 Sekunden.

Leave Timeout (Leave-Zeitüberschreitung) – Legt die Speicherdauer einer eingegangenen Leave-Nachricht in Sekunden fest. **Geben Sie einen Wert für** die Zeitüberschreitung ein, oder klicken Sie auf **Immediate Leave** (Sofortiges Leave-Zeitlimit). Der Standardwert ist 10 Sekunden.

Aktivieren von IGMP-Snooping auf dem Switch

1. Öffnen Sie die Seite ***IGMP Snooping*** (IGMP-Snooping).
2. Wählen Sie im Feld **Interface** (Schnittstelle) die zu konfigurierende Einheit und den zu konfigurierenden Port.
3. Füllen Sie die Felder auf dieser Seite je nach Bedarf aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

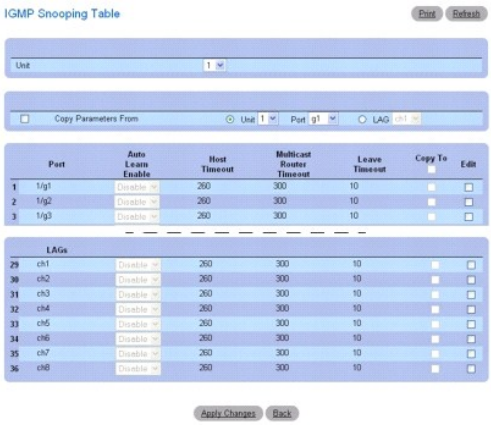
   IGMP-Snooping wird auf dem Switch aktiviert.

Anzeigen der IGMP-Snooping-Tabelle

1. Öffnen Sie die Seite **IGMP Snooping** (IGMP-Snooping).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **IGMP Snooping Table** (IGMP-Snooping-Tabelle) wird angezeigt.

Abbildung 8-74. IGMP-Snooping-Tabelle



3. Über das Dropdown-Menü **Unit** (Einheit) können Sie die **IGMP Snooping Table** (IGMP-Snooping-Tabelle) für andere ggf. im Stack vorhandene Einheiten anzeigen.

Ändern der IGMP-Snooping-Einstellungen für mehrere Ports oder LAGs

1. Öffnen Sie die Seite **IGMP Snooping** (IGMP-Snooping).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **IGMP Snooping Table** (IGMP-Snooping-Tabelle) wird angezeigt.
3. Klicken Sie für jede(n) zu ändernde(n) Port/LAG auf **Edit** (Bearbeiten).
4. Bearbeiten Sie die IGMP-Snooping-Felder je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die IGMP-Snooping-Einstellungen werden geändert, und das Gerät wird aktualisiert.

Kopieren der IGMP-Snooping-Einstellungen auf mehrere Ports oder LAGs

1. Öffnen Sie die Seite **IGMP Snooping** (IGMP-Snooping).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **IGMP Snooping Table** (IGMP-Snooping-Tabelle) wird angezeigt.
3. Klicken Sie auf **Copy Parameters From** (Kopiere Parameter von).
4. Wählen Sie eine Einheit/Port-Kombination oder LAG, die als Quelle der gewünschten Parameter dienen soll.
5. Klicken Sie bei den Einheit/Port-Kombinationen oder LAG, auf die die Parameter kopiert werden sollen, auf **Copy To** (Kopiere nach).
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die IGMP-Snooping-Einstellungen werden geändert, und das Gerät wird aktualisiert.

Konfigurieren von IGMP-Snooping mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- IGMP Snooping Commands (IGMP-Snooping-Befehle)

Konfigurieren von LLDP (Link Layer Discovery Protocol)

Mit dem Link Layer Discovery Protocol (LLDP) gemäß IEEE 802.1AB können Stationen auf einem 802-AN bedeutende Fähigkeiten und Systembeschreibungen mitteilen. Diese Informationen werden von einem Netzwerkmanager überprüft, um die Systemtopologie zu bestimmen und fehlerhafte Konfigurationen im LAN zu erkennen.

Das LLDP ist ein in eine Richtung verlaufendes Protokoll, das keine Abfrage/Antwort-Abfolgen enthält. Die Informationen werden von Stationen mit Übertragungsfunktion übermittelt und von Stationen mit Empfangsfunktion empfangen und verarbeitet. Die Übertragungs- und Empfangsfunktionen können für jeden Port separat aktiviert/deaktiviert werden. Die Übertragungs- und Empfangsfunktionen sind standardmäßig auf allen Ports deaktiviert. Die Anwendung ist dafür zuständig, jedes Gerät je nach konfiguriertem Status und Betriebszustand des Ports im Übertragungs- bzw. Empfangsstatus zu starten.

Die Menüseite **LLDP** *enthält* Links zu folgenden Themen:

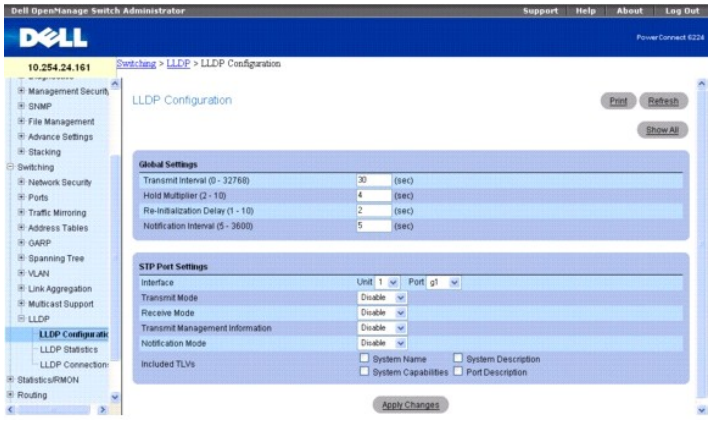
- LLDP-Konfiguration
- LLDP-Statistik
- LLDP-Verbindungen

LLDP-Konfiguration

Auf der Seite **LLDP Configuration** (LLDP-Konfiguration) können Sie LLDP-Parameter festlegen. Hier können Parameter für das gesamte System oder für eine bestimmte Schnittstelle eingestellt werden.

Um die Seite ***LLDP Configuration*** (LLDP-Konfiguration) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ LLDP→ *LLDP Configuration (LLDP-Konfiguration)***.

Abbildung 8-75. LLDP-Konfiguration



Die Seite ***LLDP Configuration*** (LLDP-Konfiguration) enthält folgende Felder:

Global Settings (Globale Einstellungen)

Transmit Interval (1-32768) (Übertragungsintervall, 1-32768) – Legt fest, in welchem Intervall Frames gesendet werden. Der Standardwert ist 30 Sekunden.

Hold Multiplier (2-10) (Hold-Multiplikator, 2-10) – Legt den Multiplikator des Übertragungsintervalls für die Zuweisung zur Laufzeit fest. Der Standardwert ist 4.

Re-Initialization Delay (1-10) (Verzögerung für Neuinitialisierung, 1-10) – Legt die Verzögerung bis zur Neuinitialisierung fest. Der Standardwert ist 2 Sekunden.

Notification Interval (5-3600) (Benachrichtigungsintervall, 5-3600) – Schränkt das Senden von Benachrichtigungen ein. Der Standardwert ist 5 Sekunden.

Port-Einstellungen

Interface (Schnittstelle) – Legt den Port fest, für den die Parameter gelten sollen.

Transmit Mode (Übertragungsmodus) – Aktiviert oder deaktiviert die Übertragungsfunktion. Diese Funktion ist standardmäßig deaktiviert.

Receive Mode (Empfangsmodus) – Aktiviert oder deaktiviert die Empfangsfunktion. Diese Funktion ist standardmäßig deaktiviert.

Transmit Management Information (Verwaltungsinformationen übertragen) – Aktiviert oder deaktiviert die Übertragung von Verwaltungsadressinstanzen. Diese Funktion ist standardmäßig deaktiviert.

Notification Mode (Benachrichtigungsmodus) – Aktiviert oder deaktiviert Remote-Änderungsbenachrichtigungen. Diese Funktion ist standardmäßig deaktiviert.

Included TLVs (Eingeschlossene TLVs) – Wählt zu sendende TLV-Informationen. Systemname, Systemfähigkeiten, Systembeschreibung und Portbeschreibung können gewählt werden.

Ändern der LLDP-Konfiguration

1. Öffnen Sie die Seite ***LLDP Configuration*** (LLDP-Konfiguration).
2. Nehmen Sie die erforderlichen Einstellungen vor.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die LLDP-Parameter werden im Switch gespeichert.

Anzeigen der Tabelle mit den LLDP-Schnittstelleneinstellungen

1. Öffnen Sie die Seite ***LLDP Configuration*** (LLDP-Konfiguration).
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die **LLDP Interface Settings Table** (Tabelle mit LLDP-Schnittstelleneinstellungen) wird angezeigt.

Abbildung 8-76. Tabelle mit LLDP-Schnittstelleneinstellungen

3. Über das Dropdown-Menü **Unit** (Einheit) können Sie die **LLDP Interface Settings Table** (Tabelle mit LLDP-Schnittstelleneinstellungen) für andere ggf. im Stack vorhandene Einheiten anzeigen.

Kopieren von LLDP-Schnittstelleneinstellungen

1. Öffnen Sie die Seite ***LLDP Configuration*** (LLDP-Konfiguration).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **LLDP Interface Settings Table** (Tabelle mit LLDP-Schnittstelleneinstellungen) wird angezeigt.

3. Legen Sie in **Copy Parameters From** (Parameter kopieren aus) die Einheit und den Port fest, aus denen kopiert werden soll.
4. Klicken Sie für jede Einheit bzw. jeden Port, die diese Parameter erhalten sollen, auf **Copy To** (Kopieren zu).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die LLDP-Schnittstelleneinstellungen werden kopiert, und das Gerät wird aktualisiert.

Ändern der LLDP-Schnittstelleneinstellungen für mehrere Ports

1. Öffnen Sie die Seite ***LLDP Configuration*** (LLDP-Konfiguration).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **LLDP Interface Settings Table** (Tabelle mit LLDP-Schnittstelleneinstellungen) wird angezeigt.
3. Klicken Sie für jede zu ändernde Einheit bzw. jeden zu ändernden Port auf **Edit** (Bearbeiten).
4. Bearbeiten Sie die LLDP-Schnittstellenfelder je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die LLDP-Schnittstelleneinstellungen werden geändert, und das Gerät wird aktualisiert.

Einstellen der LLDP-Konfiguration mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

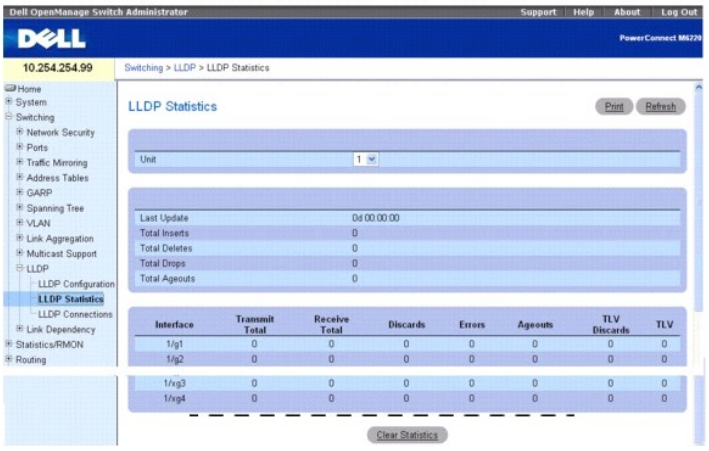
- LLDP Commands (LLDP-Befehle)

LLDP-Statistik

Auf der Seite **LLDP Statistics** (LLDP-Statistik) können Sie LLPD-bezogene Statistiken anzeigen.

Um die Seite ***LLDP Statistics*** (LLDP-Statistik) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ LLDP→ *LLDP Statistics*** .

Abbildung 8-77. LLDP-Statistik



Die Seite ***LLDP Statistics*** (LLDP-Statistik) enthält folgende Statistiken:

Statistiken für das gesamte System

Last Update (Letzte Aktualisierung) – Zeigt den Wert der Systembetriebszeit beim letzten Erstellen, Ändern oder Löschen einer Remote-Eingabe von Daten.

Total Inserts (Einfügungen gesamt) – Zeigt an, wie oft ein von einem Remote-Switch mitgeteilter vollständiger Satz von Informationen in die Tabelle eingefügt wurde.

Total Deletes (Löschungen gesamt) – Zeigt an, wie oft ein von einem Remote-Switch mitgeteilter vollständiger Satz von Informationen aus der Tabelle gelöscht wurde.

Total Drops (Fehlschläge gesamt) – Zeigt an, wie oft ein von einem Remote-Switch mitgeteilter vollständiger Satz von Informationen aus der Tabelle wegen nicht ausreichender Ressourcen nicht eingefügt werden konnte.

Total Ageouts (Zeitüberschreitungen gesamt) – Zeigt an, wie oft eine Remote-Dateneingabe wegen Überschreitung der Laufzeit gelöscht wurde.

Port-Statistiken

Interface (Schnittstelle) – Zeigt die Einheit und den Port, auf die sich die Statistik für die Leitung bezieht.

Transmit Total (Übertragen gesamt) – Zeigt die Gesamtzahl der an den angegebenen Port gesendeten LLDP-Frames.

Receive Total (Empfangen gesamt) – Zeigt die Gesamtzahl der am angegebenen Port empfangenen gültigen LLDP-Frames.

Discards (Ablehnungen) – Zeigt die Anzahl der am angegebenen Port empfangenen und aus irgendeinem Grund abgelehnten LLDP-Frames.

Errors (Fehler) – Zeigt die Anzahl der am angegebenen Port empfangenen ungültigen LLDP-Frames.

Ageouts (Zeitüberschreitungen) – Zeigt an, wie oft eine Remote-Dateneingabe am angegebenen Port wegen Überschreitung der Laufzeit gelöscht wurde.

TLV Discards (TLV-Ablehnungen) – Zeigt die Anzahl der am angegebenen Port empfangenen und aus irgendeinem Grund vom LLDP-Agent abgelehnten LLDP-TLVs (Typ/Länge/Wert-Sätze) an.

TLV Unknowns (Unbekannte TLVs) – Zeigt die Anzahl der am angegebenen Port empfangenen LLDP-TLVs für einen vom LLDP-Agent nicht erkannten Typ.

Über das Dropdown-Menü **Unit** (Einheit) können Sie die **LLDP Statistics** (LLDP-Statistik) für andere ggf. im Stack vorhandene Einheiten anzeigen.

Über die Schaltfläche **Clear Statistics** (Statistiken löschen) können Sie alle LLDP-Statistiken auf Null zurücksetzen.

Anzeigen von LLDP-Statistiken mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

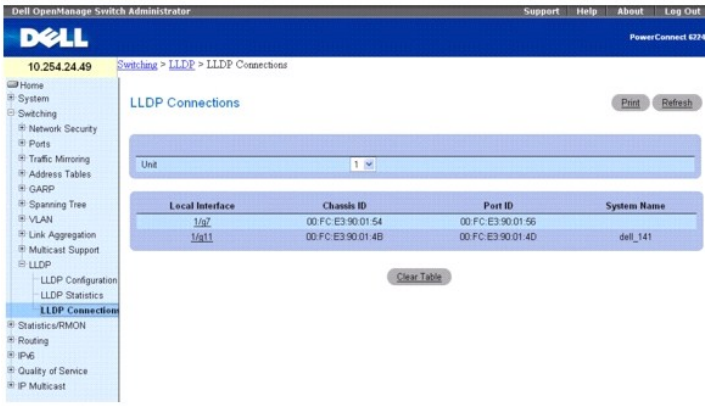
- LLDP Commands (LLDP-Befehle)

LLDP-Verbindungen

Auf der Seite **LLDP Connections** (LLDP-Verbindungen) können Sie die Liste der Ports mit LLDP-Aktivierung anzeigen. Die grundlegenden Verbindungsinformationen werden angezeigt.

Um die Seite **LLDP Connections** (LLDP-Verbindungen) anzuzeigen, klicken Sie in der Strukturansicht auf **Switching→ LLDP→ LLDP Connections (LLDP-Verbindungen)**.

Abbildung 8-78. Tabelle der LLDP-Verbindungen



Die Seite **LLDP Connections** (LLDP-Verbindungen) enthält folgende Port-Informationen:

Local Interface (Lokale Schnittstelle) – Bezeichnet eine Einheit und einen Port in dem Stack.

Chassis ID (Gehäuse-ID) — Gibt das Gehäuse des 802 LAN-Geräts an.

Port ID (Port-ID) – Gibt die Nummer des Ports an, von dem die LLDPDU übertragen wird.

System Name (Systemname) – Gibt den mit dem Remote-Gerät verbundenen Systemnamen an.

Über das Dropdown-Menü **Unit** (Einheit) können Sie die **LLDP Connections** (LLDP-Verbindungen) für andere ggf. im Stack vorhandene Einheiten anzeigen.

Über die Schaltfläche **Clear Table** (Tabelle löschen) können Sie alle Informationen aus der Tabelle **LLDP Connections** (LLDP-Verbindungen) löschen.

Anzeigen von LLDP-Verbindungsinformationen

1. Öffnen Sie die Seite ***LLDP Connections*** (LLDP-Verbindungen).
2. Klicken Sie im Feld **Local Interface** (Lokale Schnittstelle) auf das Gerät, zu dem Sie Informationen anzeigen möchten**.**

   Die Seite **LLDP Connections - Detailed** (LLDP-Verbindungen - Detailliert) für das Gerät wird angezeigt.

Abbildung 8-79. Detaillierte LLDP-Verbindungen

3. Über die Schaltfläche **Back** (Zurück) kehren Sie auf die Seite **LLDP Connections** (LLDP-Verbindungen) zurück.

Anzeigen von LLDP-Verbindungen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- LLDP Commands (LLDP-Befehle)

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Routingkonfiguration

Benutzerhandbuch für die Dell™ PowerConnect™ 6200-Reihe

- ARP
- IP
- OSPF
- BOOTP/DHCP Relay Agent
- RIP
- Routersuche
- Router
- VLAN-Routing
- VRRP
- Tunnel
- Loopbacks

Die 6200-Reihe unterstützt die IP-Routingfunktion. Über die Menüseite **Routing** können Sie VLAN-Routing konfigurieren.

Beim Eintreffen eines Pakets im Switch wird die Ziel-MAC-Adresse überprüft, um festzustellen, ob sie mit einer der konfigurierten Routingschnittstellen übereinstimmt. Ist dies der Fall, durchsucht der Switch die Hosttabelle nach einer entsprechenden Ziel-IP-Adresse. Wird ein Eintrag gefunden, wird das Paket an den betreffenden Host weitergeleitet. Ist kein entsprechender Eintrag vorhanden, wird die Ziel-IP-Adresse durch die Suche nach dem längsten übereinstimmenden Präfix ermittelt. Wird ein Eintrag gefunden, wird das Paket an den nächsten Hop weitergeleitet. Ist kein Treffer vorhanden, wird das Paket an den nächsten Hop weitergeleitet, der in der Standardroute angegeben ist. Wurde keine Standardroute konfiguriert, wird das Paket an die Software der 6200-Reihe übergeben, die es entsprechend weiterverarbeitet.

Einträge können der Routingtabelle entweder statisch durch den Administrator oder dynamisch über RIP oder OSPF hinzugefügt werden. Der Hosttabelle können Einträge entweder statisch durch den Administrator oder dynamisch über ARP hinzugefügt werden.

Die Menüseite **Routing** enthält Links zu den folgenden Merkmalen:

- ARP
- IP
- OSPF
- BOOTP/DHCP Relay Agent
- RIP
- Routersuche
- Router
- VLAN-Routing
- VRRP
- Tunnel
- Loopback-Schnittstellen

ANMERKUNG: CLI-Befehle sind nicht für alle Routingseiten verfügbar.

ARP

Die 6200-Reihe verwendet das ARP-Protokoll für die Zuordnung von Layer 2-MAC-Adressen zu Layer 3-IPv4-Adressen. Darüber hinaus kann der Administrator der ARP-Tabelle Einträge auch statisch hinzufügen.

ARP ist ein wesentlicher Teil des Internetprotokolls (IP) und wird für die Umsetzung von IP-Adressen in MAC-Adressen verwendet, die durch das lokale Netzwerk (LAN), wie beispielsweise Ethernet, vorgegeben sind. Damit eine Station ein IP-Paket senden kann, muss es die MAC-Adresse des IP-Ziels oder, wenn sich das Ziel nicht in demselben Subnetz befindet, des nächsten Hoprouters kennen. Diese Adresse wird durch Aussenden eines ARP-Anforderungspakets ermittelt, auf das der Empfänger durch Rücksendung einer ARP-Antwort mit der eigenen MAC-Adresse reagiert. Ist die MAC-Adresse bekannt, wird sie in das Zieladressfeld des Layer 2-Headers eingefügt, der dem IP-Paket vorangestellt ist.

Der ARP-Cache ist eine Tabelle, die in den einzelnen Stationen in einem Netzwerk lokal verwaltet wird. Für den Aufbau oder die Verwaltung dieses Cache gibt es keine besonderen Vorgaben, allerdings muss er zumindest die Informationen enthalten, die durch die Verarbeitung von ARP-Protokollpaketen ermittelt wurden und die sich für Ethernet im Feld **0x0806 EtherType** befinden. Einträge im ARP-Cache werden durch Überprüfung der Quellinformationen in den ARP-Paketfeldern mit den Nutzdaten (der "Payload") ermittelt; dabei spielt es keine Rolle, ob es sich um eine ARP-Anforderung oder eine ARP-Antwort handelt. Beim Senden einer ARP-Anforderung an alle Stationen in einem LAN-Segment oder in einem virtuellen LAN (VLAN) hat daher jeder Empfänger die Möglichkeit, die IP- und MAC-Adresse des Senders im eigenen ARP-Cache zu speichern. Die ARP-Antwort, bei der es sich um ein Unicast-Paket handelt, ist in der Regel nur für die Station sichtbar, die die ursprüngliche ARP-Anforderung gesendet hat, und wird von dieser im eigenen ARP-Cache gespeichert. Dabei wird der Inhalt des ARP-Cache immer durch neuere Informationen überschrieben.

Der ARP-Cache kann 896 Einträge enthalten, obwohl seine Größe auch auf einen beliebigen Wert zwischen 256 und 896 gesetzt werden kann. Werden von einem Gerät mehrere Netzwerkschnittstellen unterstützt, wie dies typischerweise bei einem Router der Fall ist, wird für sämtliche Schnittstellen entweder ein einziger ARP-Cache verwendet oder für jede Schnittstelle ein eigener Cache verwaltet. Letztere Option ist sinnvoll, wenn die Netzwerkadressierung nicht eindeutig pro Schnittstelle erfolgt; dies trifft nicht auf die Ethernet-MAC-Adresszuordnung zu, daher wird hier ein einziger ARP-Cache verwendet.

Geräte können aus einem Netzwerk entfernt werden, d. h. die IP-Adresse, die einmal einer bestimmten MAC-Adresse zugeordnet war, wird anschließend für eine andere MAC-Adresse verwendet oder ist gar nicht mehr im Netzwerk vorhanden (wenn sie beispielsweise neu konfiguriert, abgetrennt oder abgeschaltet wird). Der ARP-Cache kann daher unter anderem in den folgenden Fällen veraltete Informationen enthalten: wenn die Einträge nicht anhand neu ermittelter Informationen im Netzwerk aktualisiert werden; wenn der ARP-Cache nicht regelmäßig aktualisiert wird, um festzustellen, ob eine Adresse immer noch vorhanden ist; wenn Einträge nicht entfernt werden, die im Verlauf eines Ablaufintervalls (Ageout) nicht als Sender eines ARP-Pakets identifiziert wurden (dieses Ablaufintervall wird in der Regel über die Konfiguration vorgegeben).

Die Menüseite **ARP** enthält Links zu Webseiten, auf denen ARP-Details konfiguriert und angezeigt werden können. Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ ARP**. Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

- ARP-Eintrag erstellen

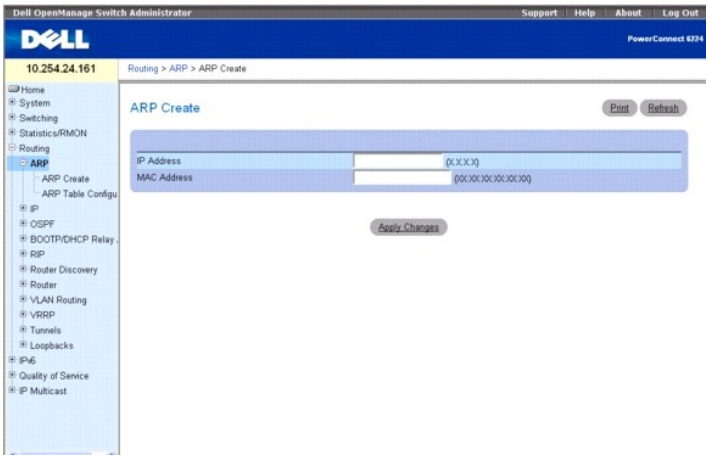
- ARP-Tabellenkonfiguration

ARP-Eintrag erstellen

Über die Seite **ARP Create** (ARP-Eintrag erstellen) können der ARP-Tabelle (Address Resolution Protocol) Einträge hinzugefügt werden.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ ARP→ ARP Create (ARP-Eintrag erstellen)**.

Abbildung 10-1. ARP-Eintrag erstellen



Die Seite **ARP Create** (ARP-Eintrag erstellen) enthält folgende Felder:

IP Address (IP-Adresse) – Geben Sie die IP-Adresse ein, die hinzugefügt werden soll. Es muss sich um die IP-Adresse eines Geräts in einem Subnetz handeln, das mit einer der Routingschnittstellen des Switch verbunden ist.

MAC Address (MAC-Adresse) – Die Unicast-MAC-Adresse des Geräts. Geben Sie die Adresse in Form von sechs zweistelligen Zahlen ein, die durch Doppelpunkt getrennt werden (Beispiel: 00:06:29:32:81:40).

Einfügen von Einträgen in die ARP-Tabelle

1. Öffnen Sie die Seite **ARP Create** (ARP-Eintrag erstellen).
2. Geben Sie die Adressen an, die zugeordnet werden sollen.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Adressen sind jetzt im ARP-Cache enthalten.

Einfügen von Einträgen in die ARP-Tabelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

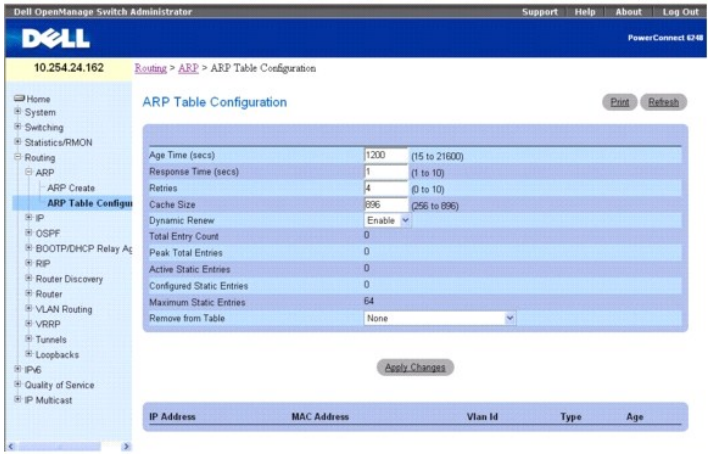
- ARP Commands (ARP-Befehle)

ARP-Tabellenkonfiguration

Über diese Seite können Sie die Konfigurationsparameter für die ARP-Tabelle ändern. Außerdem können Sie auf dieser Seite auch den Inhalt der Tabelle anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ ARP→ ARP Table Configuration (ARP-Tabellenkonfiguration)**.

Abbildung 10-2. ARP-Tabellenkonfiguration



Die Seite **ARP Table Configuration** (ARP-Tabellenkonfiguration) enthält folgende Felder:

Age Time (secs) (Alterungszeit) – Geben Sie den Zeitraum (in Sekunden) an, den der Switch als Ablaufintervall für ARP-Einträge verwenden soll. Hier muss eine gültige ganze Zahl eingegeben werden, die die Anzahl der Sekunden angibt, nach denen ein ARP-Eintrag als veraltet gilt. In diesem Feld sind Angaben zwischen 15 und 21600 Sekunden möglich. Der Standardwert für die Alterungszeit ist 1200 Sekunden.

Response Time (sec) (Antwortzeit) – Geben Sie hier den Zeitraum in Sekunden an, den der Switch als Zeitlimitüberschreitung für ARP-Antworten verwenden soll. Hier muss eine gültige ganze Zahl eingegeben werden, die die Anzahl der Sekunden angibt, die der Switch auf eine Antwort auf eine ARP-Anforderung hin wartet. In diesem Feld sind Angaben zwischen 1 und 10 Sekunden möglich. Der Standardwert für die Antwortzeit ist 1 Sekunde.

Retries (Wiederholungsversuche) – Geben Sie eine ganze Zahl ein; sie gibt an, wie oft eine ARP-Anforderung maximal wiederholt wird. In diesem Feld können Werte zwischen 0 und 10 eingegeben werden; der Standardwert ist 4.

Cache Size (Cache-Größe) – Geben Sie eine ganze Zahl ein; sie gibt die Anzahl Einträge an, die der ARP-Cache maximal enthalten kann. In diesem Feld können Werte zwischen 256 und 896 eingegeben werden; der Standardwert ist 896.

Dynamic Renew (Dynamische Aktualisierung) – Gibt an, ob die ARP-Komponente ARP-Einträge des Typs "Dynamisch" automatisch erneuert, wenn sie ablaufen. Die Standardeinstellung ist **Enable** (Aktivieren).

Total Entry Count (Gesamtzahl Einträge) – Die Gesamtzahl der Einträge in der ARP-Tabelle.

Peak Total Entries (Gesamtzahl erreicht) – Gibt an, dass im Feld "Total Entry Count" (Gesamtzahl Einträge) der höchstmögliche Wert erreicht wurde. Dieser Zählerwert wird zurückgesetzt, sobald die Cache-Größe für die ARP-Tabelle geändert wird.

Active Static Entries (Aktive statische Einträge) – Die Gesamtzahl aktiver statischer Einträge in der ARP-Tabelle.

Configured Static Entries (Konfigurierte statische Einträge) – Die Gesamtzahl konfigurierter statischer Einträge in der ARP-Tabelle.

Maximum Static Entries (Max. Anzahl statischer Einträge) – Die Anzahl statischer Einträge, die maximal definiert werden kann.

Remove from Table (Aus Tabelle entfernen) – Über diesen Parameter können Sie bestimmte Einträge aus der ARP-Tabelle entfernen. Die aufgeführten Optionen geben an, welche ARP-Einträge gelöscht werden sollen:

- Alle dynamischen Einträge
- Alle dynamischen Einträge und Gateway-Einträge
- Bestimmte dynamische Gateway-Einträge
- Bestimmte statische Einträge

Die ARP-Tabelle wird im unteren Teil der Seite angezeigt; sie enthält die folgenden Felder:

IP Address (IP-Adresse) – Die IP-Adresse des Geräts in einem Subnetz, das mit einer der Routingschnittstellen des Switch verbunden ist.

MAC Address (MAC-Adresse) – Die Unicast-MAC-Adresse des Geräts. Die Adresse ist in Form von sechs zweistelligen Zahlen angegeben, die durch Doppelpunkt getrennt werden (Beispiel: 00:06:29:32:81:40).

VLAN ID (VLAN-ID) – Die Routingschnittstelle, die dem ARP-Eintrag zugeordnet ist.

Type (Typ) – Der Typ des ARP-Eintrags.

Age (Alter) – Gibt an, wann der Eintrag zuletzt in der ARP-Tabelle aktualisiert wurde. Wird im Format hh:mm:ss angegeben.

Konfigurieren der ARP-Tabelle

1. Öffnen Sie die Seite **ARP Table Configuration** (ARP-Tabellenkonfiguration).
2. Ändern Sie die Parameter nach Bedarf.

3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Änderungen werden gespeichert, und die ARP-Tabelle wird entsprechend aktualisiert.

Konfigurieren der ARP-Tabelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) im folgenden Kapitel :

- ARP Commands (ARP-Befehle)

IP

Die Menüseite **IP** enthält Links zu Webseiten, auf denen IP-Routingdaten konfiguriert und angezeigt werden können. Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ IP**. Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

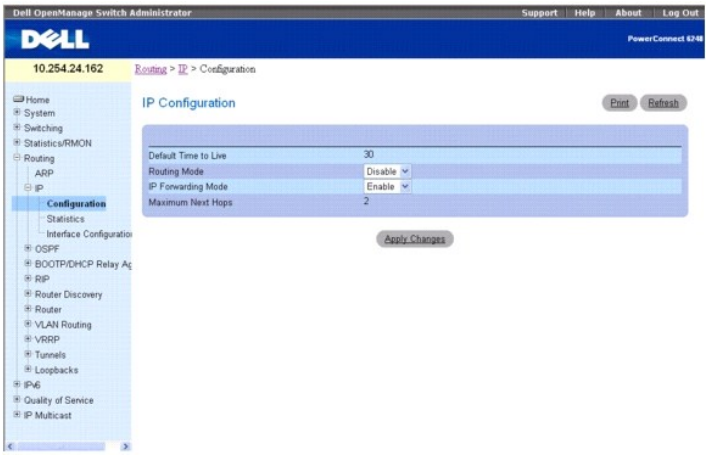
- IP-Konfiguration
- IP-Statistik
- IP-Schnittstellenkonfiguration

IP-Konfiguration

Über die Seite **IP Configuration** (IP-Konfiguration) können Sie die Routingparameter für den Switch (im Gegensatz zu einer Schnittstelle) konfigurieren.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ IP→ Configuration (Konfiguration)**.

Abbildung 10-3. IP-Konfiguration



Die Seite **IP Configuration** (IP-Konfiguration) enthält folgende Felder:

Default Time to Live (Standardlebensdauer) – Der Standardwert, der in das Feld "Time-To-Live" (Lebensdauer) des IP-Headers der vom Switch gesendeten Datagramme eingefügt wird, wenn vom Transportschichtprotokoll kein TTL-Wert zur Verfügung gestellt wird.

Routing Mode (Routingmodus) – Wählen Sie "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus dem Dropdown-Menü. Ein Routing über die Schnittstellen ist nur möglich, wenn die Routingfunktion für den Switch aktiviert wurde. Routing kann auch über die VLAN-Schnittstelle aktiviert bzw. deaktiviert werden. Der Standardwert ist **Disable** (Deaktivieren).

IP Forwarding Mode (IP-Weiterleitungsmodus) – Wählen Sie "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus dem Dropdown-Menü. Über diesen Parameter wird die Weiterleitung von IP-Frames aktiviert bzw. deaktiviert. Der Standardwert ist **Enable** (Aktivieren).

Maximum Next Hops (Max. Anzahl Hops) – Die Anzahl an Hops, die vom Switch maximal unterstützt wird. Dies ist eine Konstante, die bei der Kompilierung festgelegt wird (Compile-Time-Konstante).

Konfigurieren der IP-Routingparameter

1. Öffnen Sie die Seite **IP Configuration** (IP-Konfiguration).
2. Ändern Sie die Parameter nach Bedarf.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Änderungen werden gespeichert und die Routingparameter entsprechend aktualisiert.

Konfigurieren der IP-Routingparameter mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide (CLI-Referenzhandbuch) in den folgendem Kapiteln:*

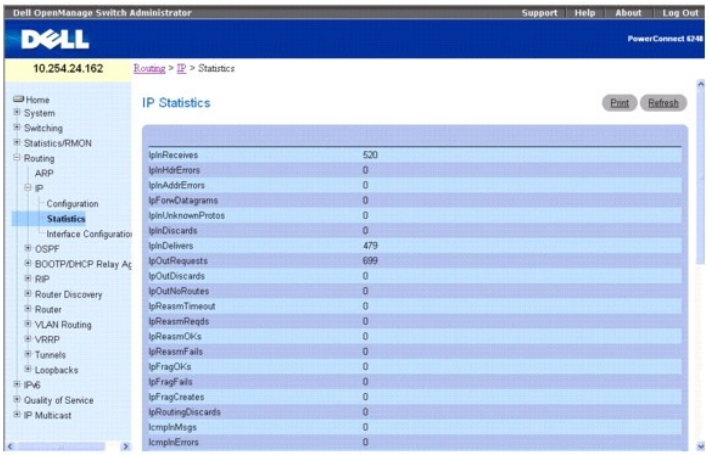
- IP Routing Commands (IP-Routingbefehle)
- VLAN Commands (VLAN-Befehle)

IP-Statistik

Die Statistikdaten auf der Seite **IP Statistics** (IP-Statistik) entsprechen den RFC-1213-Empfehlungen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ IP→ Statistics (Statistik)**.

Abbildung 10-4. IP-Statistik



Die Seite **IP Statistics** (IP-Statistik) enthält folgende Felder:

IpInReceives – Die Gesamtzahl der Eingabedatagramme, die von Schnittstellen empfangen wurden, einschließlich der fehlerhaft empfangenen Datagramme.

IpInHdrErrors – Die Gesamtzahl der Eingabedatagramme, die auf Grund von Fehlern in den IP-Headern abgelehnt wurden (fehlerhafte Prüfsumme, nicht übereinstimmende Versionen, Formatfehler, Überschreitung der Lebensdauer, Fehler bei der Verarbeitung der IP-Optionen usw.).

IpInAddrErrors – Die Anzahl der Eingabedatagramme, die abgelehnt wurden, weil das Zielfeld im IP-Header keine gültige IP-Adresse für den Empfang in dieser Einheit enthielt. Dazu gehören ungültige Adressen (z. B. 0.0.0.0) sowie Adressen nicht unterstützter Klassen (z. B. Klasse E). Bei Geräten, bei denen es sich nicht um IP-Gateways handelt, die also keine Datagramme weiterleiten, zählen hierzu auch Datagramme, die abgelehnt wurden, weil die Zieladresse keine lokale Adresse war.

IpForwDatagrams – Die Anzahl der Eingabedatagramme, für die diese Einheit nicht das endgültige IP-Ziel ist und für die deshalb der Versuch unternommen wurde, sie an das entsprechende endgültige Ziel weiterzuleiten. Für Geräte, bei denen es sich nicht um IP-Gateways handelt, zählen hierzu nur die Pakete, die per Quellrouting (Routenbestimmung durch den Sender) über diese Einheit gesendet wurden und bei denen die Quellroutingverarbeitung erfolgreich war.

IpInUnknownProtos – Die Anzahl der lokal adressierten Datagramme, die zwar erfolgreich empfangen, aber auf Grund eines unbekannten oder nicht unterstützten Protokolls abgelehnt wurden.

IpInDiscards – Die Anzahl der IP-Eingabedatagramme, die zwar problemlos weiterverarbeitet werden konnten, jedoch abgelehnt wurden (weil beispielsweise nicht genügend Pufferspeicher vorhanden war). Datagramme, die beim Warten auf ihre Zusammensetzung abgelehnt wurden, werden hier nicht berücksichtigt.

IpInDelivers – Die Gesamtzahl der erfolgreich an IP-Benutzerprotokolle (einschließlich ICMP) übermittelten Eingabedatagramme.

IpOutRequests – Die Gesamtzahl der IP-Datagramme, die von lokalen IP-Benutzerprotokollen (einschließlich ICMP) auf IP-Übertragungsanforderungen hin an IP übergeben wurden. Die Anzahl der über **ipForwDatagrams** ermittelten Datagramme wird hier nicht berücksichtigt.

IpOutDiscards – Die Anzahl der IP-Ausgabedatagramme, die zwar problemlos an das entsprechende Ziel weitergeleitet werden konnten, jedoch abgelehnt wurden (weil beispielsweise nicht genügend Pufferspeicher vorhanden war). Dazu gehören auch Datagramme, die über **ipForwDatagrams** ermittelt wurden (wenn sie dieses (optionale) Kriterium für ihre Ablehnung erfüllt haben).

IpOutNoRoutes – Die Anzahl der IP-Datagramme, die abgelehnt wurden, weil keine Route für die Übertragung an ihr Ziel gefunden wurde. Dazu gehören alle über "ipForwDatagrams" ermittelten Datagramme, die dieses 'NoRoutes'-Kriterium erfüllen und alle Datagramme, die vom Host nicht übertragen werden können, weil alle ihre Standard-Gateways ausgefallen sind.

IpReasmTimeout – Die Zeit in Sekunden, die empfangene Fragmente, die auf die Zusammensetzung in dieser Einheit warten, maximal beibehalten werden.

IpReasmReqds – Die Anzahl der empfangenen IP-Fragmente, die in dieser Einheit wieder zusammengesetzt werden müssen.

IpReasmOKs – Die Anzahl der erfolgreich wieder zusammengesetzten IP-Datagramme.

IpReasmFails – Die Anzahl der vom Algorithmus für die IP-Wiederzusammensetzung festgestellten Fehler (unabhängig von der Fehlerursache: Zeitüberschreitung, Fehler usw.). Einige Algorithmen verlieren die Übersicht über die Anzahl der Fragmente, da diese gleich beim Empfang zusammengesetzt werden; daher entspricht der Wert hier nicht unbedingt der Anzahl der abgelehnten IP-Fragmente.

IpFragOKs – Die Anzahl der IP-Datagramme, die in dieser Einheit erfolgreich fragmentiert wurden.

IpFragFails – Die Anzahl der IP-Datagramme, die abgelehnt wurden, da sie in dieser Einheit fragmentiert werden sollten, dies aber nicht möglich war (beispielsweise weil das Flag "Nicht fragmentieren" gesetzt war).

IpFragCreates – Die Anzahl der IP-Datagrammfragmente, die bei der Fragmentierung in dieser Einheit generiert wurden.

IpRoutingDiscards – Die Anzahl der Routingeinträge, die abgelehnt wurden, obwohl sie gültig waren. Ein möglicher Grund für die Ablehnung eines Eintrags ist beispielsweise die Freigabe von Pufferspeicher für weitere Routingeinträge.

IcmpInMsgs – Die Gesamtzahl der von der Einheit empfangenen ICMP-Meldungen. Dazu gehören auch alle über **icmpInErrors** ermittelten ICMP-Meldungen.

IcmpInErrors – Die Anzahl der von der Einheit empfangenen ICMP-Meldungen, bei denen ICMP-spezifische Fehler (fehlerhafte Prüfsumme, falsche Länge usw.) festgestellt wurden.

IcmpInDestUnreachs – Die Anzahl der empfangenen ICMP-Meldungen, die darauf hinweisen, dass das Ziel nicht erreicht werden konnte.

IcmpInTimeExcds – Die Anzahl der empfangenen ICMP-Meldungen, die auf eine Überschreitung des Zeitlimits hinweisen.

IcmpInParmProbs – Die Anzahl der empfangenen ICMP-Meldungen, die auf Parameterfehler hinweisen.

IcmpInSrcQuenchs – Die Anzahl der empfangenen ICMP-Meldungen, die auf eine durch den Sender verursachte Überlastung hinweisen.

IcmpInRedirects – Die Anzahl der empfangenen ICMP-Meldungen, die eine Umleitung anfordern.

IcmpInEchos – Die Anzahl der empfangenen ICMP-Meldungen, die eine Echoanforderung enthalten.

IcmpInEchoReps – Die Anzahl der empfangenen ICMP-Meldungen, die als Antwort auf eine Echoanforderung gesendet wurden.

IcmpInTimestamps – Die Anzahl der empfangenen ICMP-Meldungen, die eine Zeitmarke anfordern.

IcmpInTimestampReps – Die Anzahl der empfangenen ICMP-Meldungen, die als Antwort auf eine Zeitmarkenanforderung gesendet wurden.

IcmpInAddrMasks – Die Anzahl der empfangenen ICMP-Adressen, die eine Adressmaske anfordern.

IcmpInAddrMaskReps – Die Anzahl der empfangenen ICMP-Meldungen, die als Antwort auf eine Adressmaskenanforderung gesendet wurden.

IcmpOutMsgs – Die Gesamtzahl der ICMP-Meldungen, die diese Einheit versucht hat zu senden. Dazu gehören auch alle über **icmpOutErrors** ermittelten ICMP-Meldungen.

IcmpOutErrors – Die Anzahl der ICMP-Meldungen, die von dieser Einheit auf Grund von ICMP-spezifischen Problemen nicht gesendet wurden (beispielsweise weil nicht genügend Pufferspeicher vorhanden war). Fehler, die außerhalb der ICMP-Schicht festgestellt wurden (wenn beispielsweise das Datagramm von IP nicht weitergeleitet werden kann), sollten in diesem Wert nicht berücksichtigt werden. In einigen Implementierungen gibt es unter Umständen keine Fehlertypen für diesen Zähler.

IcmpOutDestUnreachs – Die Anzahl der gesendeten ICMP-Meldungen, die darauf hinweisen, dass das Ziel nicht erreicht werden konnte.

IcmpOutTimeExcds – Die Anzahl der gesendeten ICMP-Meldungen, die auf eine Überschreitung des Zeitlimits hinweisen.

IcmpOutParmProbs – Die Anzahl der gesendeten ICMP-Meldungen, die auf Parameterfehler hinweisen.

IcmpOutSrcQuenchs – Die Anzahl der gesendeten ICMP-Meldungen, die auf eine Überlastung durch den Sender hinweisen.

IcmpOutRedirects – Die Anzahl der gesendeten ICMP-Meldungen, die eine Umleitung anfordern. Für Hosts ist dieses Objekt immer Null, da Hosts keine Umleitungsanforderungen senden.

IcmpOutEchos – Die Anzahl der gesendeten ICMP-Meldungen, die eine Echoanforderung enthalten.

IcmpOutEchoReps – Die Anzahl der gesendeten ICMP-Meldungen, die als Antwort auf eine Echoanforderung gesendet werden.

IcmpOutTimestamps – Die Anzahl der gesendeten ICMP-Meldungen, die eine Zeitmarke anfordern.

IcmpOutTimestampReps – Die Anzahl der ICMP-Meldungen, die als Antwort auf eine Zeitmarkenanforderung gesendet wurden.

IcmpOutAddrMasks – Die Anzahl der gesendeten ICMP-Adressen, die eine Adressmaske anfordern.

IcmpOutAddrMaskReps – Die Anzahl der ICMP-Adressen, die als Antwort auf eine Adressmaskenanforderung gesendet wurden.

Aktualisieren der IP-Statistik

1. Öffnen Sie die Seite **IP Statistics** (IP-Statistik).
2. Klicken Sie auf **Refresh** (Aktualisieren).

   Die Anzeige enthält den aktuellen Datenstatus im Switch.

Anzeigen der IP-Statistik mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide (CLI-Referenzhandbuch) in folgendem Kapitel:*

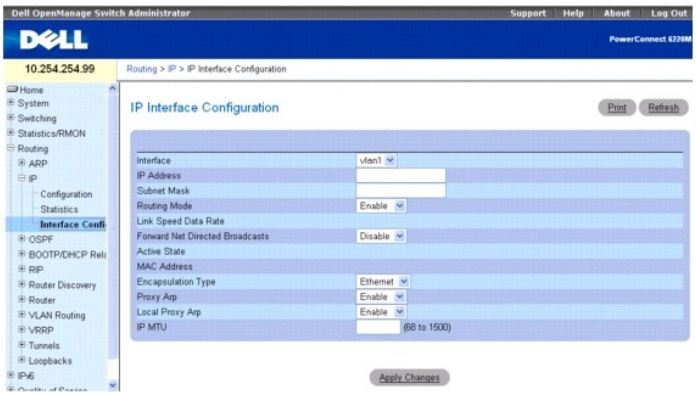
- IP Routing Commands (IP-Routingbefehle)

IP-Schnittstellenkonfiguration

Über die Seite **IP Interface Configuration** (IP-Schnittstellenkonfiguration) können Sie die IP-Schnittstellendaten für den Switch aktualisieren.

Um diese Seite in der Strukturansicht anzuzeigen, klicken Sie auf **Routing→ IP→ Interface Configuration (Schnittstellenkonfiguration)**.

Abbildung 10-5. IP-Schnittstellenkonfiguration



Die Seite **IP Interface Configuration** (IP-Schnittstellenkonfiguration) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie aus dem Dropdown-Menü die Schnittstellennummer. Das Dropdown-Menü enthält Loopback-Schnittstellen und VLANs, die über die Seite **Switching→ VLAN→ VLAN Membership (VLAN-Mitgliedschaft)→ Add (Hinzufügen)** erstellt wurden.

IP Address (IP-Adresse) – Geben Sie die IP-Adresse für die Schnittstelle ein.

Subnet Mask (Subnetzmaske) – Geben Sie die Subnetzmaske für die Schnittstelle ein. Sie wird auch als Subnetz-/Netzwerkmaske bezeichnet und stellt den Teil der Schnittstellen-IP-Adresse dar, der das verbundene Netzwerk kennzeichnet.

Routing Mode (Routingmodus) – Über dieses Feld wird die Routingfunktion für eine Schnittstelle aktiviert bzw. deaktiviert. Der Standardwert ist **Enable** (Aktivieren).

Link Speed Data Rate (Übertragungsrate der Verbindung) – Eine ganze Zahl, die die Datenübertragungsrate der physikalischen Verbindung der angegebenen Schnittstelle angibt. Dieser Wert gilt nur für physikalische Schnittstellen und wird in Megabit pro Sekunde (Mbit/s) angegeben.

Forward Net Directed Broadcasts (Übers Netzwerk geleitete Broadcasts weiterleiten) – Geben Sie an, wie über ein Netzwerk geleitete Broadcast-Pakete gehandhabt werden sollen. Bei Auswahl von "Enable" (Aktivieren) im Dropdown-Menü werden solche Broadcast-Pakete weitergeleitet. Bei Auswahl von **Disable** (Deaktivieren) werden sie abgelehnt. Der Standardwert ist **Disable** (Deaktivieren).

Active State (Aktiver Status) – Der Status der angegebenen Schnittstelle ist "Active" (Aktiv) oder "Inactive" (Inaktiv). Eine Schnittstelle gilt als aktiv, wenn die Verbindung hergestellt und im Weiterleitungsstatus ist.

MAC Address (MAC-Adresse) – Die übertragene physikalische Adresse der angegebenen Schnittstelle. Die Adresse ist in Form von sechs zweistelligen Zahlen angegeben, die durch Doppelpunkt getrennt werden (Beispiel: 00:06:29:32:81:40). Dieser Wert gilt für physikalische Schnittstellen. Für logische Schnittstellen, wie beispielsweise VLAN-Routingschnittstellen, wird in diesem Feld die System-MAC-Adresse angezeigt.

Encapsulation Type (Verkapselungstyp) – Wählen Sie im Dropdown-Menü den Verkapselungstyp der Verbindungsschicht für Pakete aus, die von der angegebenen Schnittstelle übertragen werden. Mögliche Werte sind Ethernet und SNAP. Die Standardeinstellung ist Ethernet.

Proxy ARP (Proxy-ARP) – Geben Sie über das Dropdown-Menü an, ob Proxy-ARP für die angegebene Schnittstelle aktiviert oder deaktiviert werden soll.

Local Proxy ARP (Lokales Proxy-ARP) – Geben Sie über das Dropdown-Menü an, ob lokales Proxy-ARP für die angegebene Schnittstelle aktiviert oder deaktiviert werden soll.

IP MTU (IP-MTU) – Gibt die maximale Größe der Übertragungseinheiten (MTU) für IP-Pakete an, die über eine Schnittstelle gesendet werden. (Zulässiger Bereich: 68 bis 1500.) Standardwert ist 1500.

Ändern einer IP-Schnittstelle

1. Öffnen Sie die Seite **IP Interface Configuration** (IP-Schnittstellenkonfiguration).
2. Ändern Sie die Werte nach Bedarf.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Änderungen werden gespeichert, und die IP-Schnittstelle wird entsprechend aktualisiert.

Konfigurieren der IP-Schnittstelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide (CLI-Referenzhandbuch) in den folgendem Kapiteln:*

- IP Addressing Commands (IP-Adressierungsbefehle)
- IP Routing Commands (IP-Routingbefehle)
- ARP Commands (ARP-Befehle)

OSPF

Das OSPF-Protokoll (Open Shortest Path First) ist ein internes Gateway-Protokoll (IGP). Jeder OSPF-Router erstellt eine Struktur mit den kürzesten Pfaden aller Router und Netzwerke innerhalb der Domäne. Die Routinginformationen werden in LSU-Paketen (Link-State Update) in regelmäßigen Abständen und bei Änderungen an der Netzwerktopologie weitergeleitet. Diese Informationen werden in der OSPF-Datenbank der einzelnen Router empfangen, angeglichen und gespeichert. Eine wesentliche Information bei diesem Datenbankaustausch sind die Nummern und IP-Adressen der Schnittstellen, die dem Router zugeordnet sind. OSPF interpretiert sekundäre IP-Adressen als Netzwerke der untersten hierarchischen Ebene (Stub Networks), die dem Router zugeordnet sind. Obwohl diese Netzwerke in der OSPF-Routingdomäne mitgeteilt werden, werden für sekundäre Adressen keine Nachbarschaftsbeziehungen eingerichtet. Hier muss noch angemerkt werden, dass sich alle sekundären IP-Adressen in demselben Bereich wie die primäre IP-Adresse befinden müssen, damit sie von OSPF mitgeteilt werden. Dies gilt für die Implementierung der 6200-Reihe immer, da die Bereichskonfiguration pro Schnittstelle und nicht pro Netzwerk erfolgt.

Die Menüseite **OSPF** enthält Links zu Webseiten, auf denen OSPF-Parameter und -Daten konfiguriert und angezeigt werden können. Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ OSPF**. Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

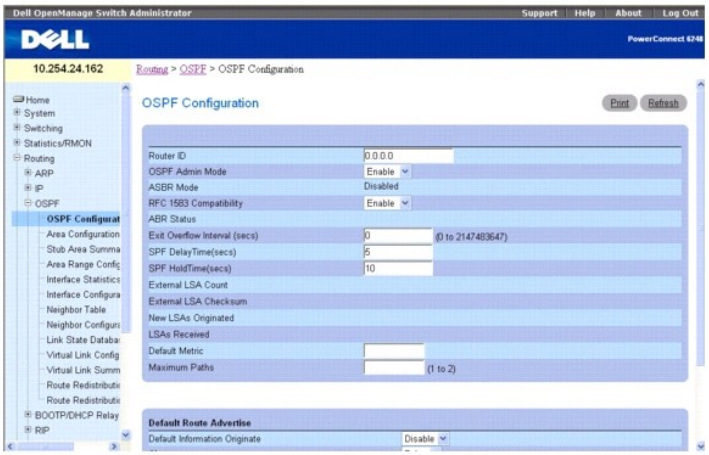
- OSPF-Konfiguration
- Bereichskonfiguration
- Zusammenfassende Daten zu Stub Areas
- Konfiguration des Adressbereichs eines Bereichs
- Schnittstellenstatistiken
- Schnittstellenkonfiguration
- Nachbarschaftstabelle
- Nachbarschaftskonfiguration
- Verbindungsstatusdatenbank
- Konfiguration virtueller Verbindungen
- Zusammenfassende Daten zu virtuellen Verbindungen
- Konfiguration der Routenumverteilung
- Zusammenfassende Daten zur Routenumverteilung

OSPF-Konfiguration

Auf der Seite **OSPF Configuration** (OSPF-Konfiguration) können Sie OSPF auf einem Router aktivieren und die entsprechenden OSPF-Einstellungen vornehmen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ OSPF→ Configuration (Konfiguration)**.

Abbildung 10-6. OSPF-Konfiguration



Die Seite **OSPF Configuration** (OSPF-Konfiguration) enthält folgende Felder:

Router ID (Router-ID) – Ein 32-Bit-Integer in der Schreibweise mit Trennzeichen, das den Router im autonomen System (AS) eindeutig kennzeichnet. Soll die Router-ID geändert werden, müssen Sie zunächst OSPF deaktivieren. Nachdem die neue Router-ID gesetzt wurde, müssen Sie OSPF wieder aktivieren, damit die Änderung wirksam wird. Standardwert ist 0.0.0.0, obwohl es sich hier nicht um eine gültige Router-ID handelt.

OSPF Admin Mode (OSPF-Verwaltungsmodus) – Wählen Sie "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus dem Dropdown-Menü. Bei Auswahl von **Enable** (Aktivieren) wird OSPF für den Switch aktiviert. Der Standardwert ist **Disable** (Deaktivieren). Damit OSPF verwendet werden kann, müssen Sie zunächst eine Router-ID konfigurieren.

ANMERKUNG: OSPF bleibt nach der Initialisierung auf dem Router so lange aktiv, bis der Router zurückgesetzt wird.

ASBR Mode (ASBR-Modus) – Gibt an, ob der ASBR-Modus aktiviert oder deaktiviert ist. Eine Aktivierung bedeutet, dass es sich um einen Router handelt, der Routen aus fremden Netzen über AS importiert (ASBR). Ein Router wird automatisch zu einem ASBR-Router, wenn er für die Umverteilung von Routen konfiguriert wird, die er von anderen Protokollen erhält.

RFC 1583 Compatibility (RFC-1583-Kompatibilität) – Wählen Sie im Dropdown-Menü "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus, um die bevorzugten Regeln für die Auswahl unter mehreren AS-external-LSAs anzugeben, die dasselbe Ziel mitteilen. Bei Auswahl von **Enable** (Aktivieren) wird den von RFC 1583 definierten Regeln Priorität gegeben, bei Auswahl von **Disable** (Deaktivieren) den im Abschnitt 16.4.1 des OSPF-2-Standards (RFC 2328) definierten Regeln. Dadurch werden Routingschleifen verhindert, wenn AS-external-LSAs für dasselbe Ziel aus unterschiedlichen Bereichen stammen. Der Standardwert ist **Enable** (Aktivieren). Um Routingschleifen zu verhindern, sollten Sie **Disable** (Deaktivieren) auswählen, allerdings nur, wenn alle OSPF-Router in der Routingdomäne entsprechend dem RFC-2328-Standard arbeiten.

ABR Status (ABR-Status) – Hier kann "Enabled" (Aktiviert) oder "Disabled" (Deaktiviert) angegeben werden. Eine Aktivierung bedeutet, dass es sich um einen ABR (Area Border Router) handelt. Eine Deaktivierung bedeutet, dass es sich nicht um einen ABR handelt.

Exit Overflow Interval (sec) (Überlaufstatus beenden) – Geben Sie die Zeit in Sekunden ein, die der Router bei Auftreten eines Überlaufs warten soll, bevor er versucht, den Überlaufstatus zu beenden. Der Router erhält dadurch die Möglichkeit, fehlerfreie AS-external-LSAs erneut zu senden. Bei Angabe von 0 verlässt der Router den Überlaufstatus erst bei einem Neustart. Der Wertebereich liegt zwischen 0 und 2147483647 Sekunden.

SPF DelayTime (secs) (SPF-Verzögerungszeit) – Geben Sie die Zeit in Sekunden ein; bei der Verzögerungszeit handelt es sich um den Zeitraum zwischen dem Empfang einer Topologieänderung durch OSPF und dem Start einer SPF-Berechnung durch OSPF. Hier kann eine ganze Zahl zwischen 0 und 65535 eingegeben werden. Die Standardzeit ist 5 Sekunden. Die Angabe von 0 bedeutet, dass es keine Verzögerung gibt, d. h. die SPF-Berechnung wird unverzüglich gestartet.

SPF HoldTime(secs) (SPF-Wartezeit) – Geben Sie die Zeit in Sekunden ein; dieser Wert gibt die Mindestwartezeit zwischen zwei aufeinander folgenden SPF-Berechnungen an. Hier kann eine ganze Zahl zwischen 0 und 65535 angegeben werden. Der Standardwert ist 10 Sekunden. Die Angabe von 0 bedeutet, dass es keine Verzögerung gibt, d. h. zwei SPF-Berechnungen werden unmittelbar hintereinander durchgeführt.

External LSA Count (Anzahl externer LSAs) – Die Anzahl externer LSAs (LS-Typ 5) in der Verbindungsstatusdatenbank (Link-State Database).

External LSA Checksum (Prüfsumme externer LSAs) – Die Summe der LS-Prüfsummen externer LSAs in der Verbindungsstatusdatenbank. Anhand dieser Summe kann festgestellt werden, ob es in der Verbindungsstatusdatenbank Änderungen gab; außerdem kann sie für den Vergleich der Verbindungsstatusdatenbanken zweier Router herangezogen werden. Hier wird ein hexadezimaler Wert angegeben.

New LSAs Originated (Neue gesendete LSAs) – In einem OSPF-Bereich sendet ein Router mehrere LSAs. Jeder Router sendet eine Router-LSA. Handelt es sich bei dem Router außerdem um den designierten Router für eines der Bereichsnetzwerke, sendet er Network-LSAs für die betreffenden Netzwerke. Dieser Wert entspricht der Anzahl der von diesem Router gesendeten LSAs.

LSAs Received (Empfangene LSAs) – Die Anzahl der empfangenen LSAs, die als neue Instanziierungen festgelegt wurden. Dieser Wert umfasst keine neueren Instanziierungen selbst gesendeter LSAs.

Default Metric (Standardmetrik) – Gibt die Standardmetrik für umverteilte Routen an. Die Standardmetrik wird in diesem Feld nur angezeigt, wenn bereits ein Wert gesetzt wurde; wurde kein Wert konfiguriert, ist dieses Feld leer. Mögliche Werte sind 1 bis 16777214.

Maximum Paths (Max. Anzahl Pfade) – Gibt die maximale Anzahl an Pfaden an, über die OSPF Meldungen an ein gegebenes Ziel senden kann. Mögliche Werte sind 1 bis 2.

Default Route Advertise (Standardroute mitteilen)

Default Information Originate (Standardinformationen senden) – Aktivieren oder deaktivieren Sie "Default Route Advertise" (Standardroute mitteilen).

Always (Immer) – Setzt bei Angabe von "True" die Routermitteilung auf 0.0.0.0/0.0.0.0.

Metric (Metrik) – Gibt die Metrik der Standardroute an. Mögliche Werte sind 1 bis 16777214.

Metric Type (Metriktyp) – Gibt den Metriktyp der Standardroute an. Möglich sind die Angaben **External Type 1** (Externer Typ 1) und **External Type 2** (Externer Typ 2). **External Type 2** ist der Standardwert.

Ändern der OSPF-Konfiguration

1. Öffnen Sie die Seite **OSPF Configuration** (OSPF-Konfiguration).
2. Ändern Sie die Werte nach Bedarf.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Änderungen werden gespeichert, und die OSPF-Schnittstelle wird entsprechend aktualisiert.

Konfigurieren von OSPF mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:*

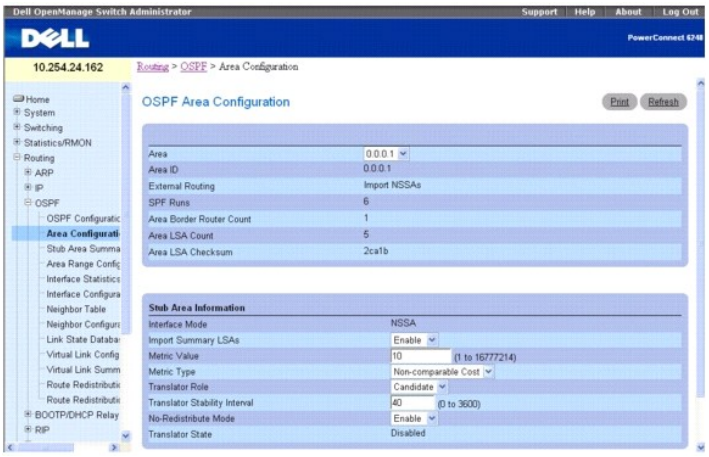
- OSPF Commands (OSPF-Befehle)

Bereichskonfiguration

Auf der Seite **OSPF Area Configuration** (OSPF- Bereichskonfiguration) können Sie eine Stub Area-Konfiguration und eine NSSA-Konfiguration erstellen, sobald Sie OSPF in einer Schnittstelle über **Routing→ OSPF→ Interface Configuration (Schnittstellenkonfiguration)** aktiviert haben. Diese Webseite wird nur angezeigt, wenn OSPF für mindestens einen Router aktiviert wurde.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ OSPF→ Area Configuration (Bereichskonfiguration)**.

Abbildung 10-7. OSPF-Bereichskonfiguration



Die Seite **OSPF Area Configuration** (OSPF-Bereichskonfiguration) enthält folgende Felder:

Area (Bereich) – Wählen Sie im Dropdown-Menü den Bereich aus, der konfiguriert werden soll. Nach Auswahl eines Bereichs werden in **Stub Area Information** (Stub Area-Informationen) Felder angezeigt.

Area ID (Bereichs-ID) – Der OSPF-Bereich. Bei der Bereichs-ID handelt es sich um ein 32-Bit-Integer in der Schreibweise mit Trennzeichen, das den Bereich, mit dem eine Routerschnittstelle verbunden ist, eindeutig kennzeichnet.

External Routing (Externes Routing) – Eine Definition des Routerleistungsspektrums für den Bereich, unter anderem ob AS-external-LSAs in den Bereich/in den gesamten Bereich geflutet werden. Handelt es sich um eine Stub Area, sind dies die möglichen Optionen für die Konfiguration der externen Routingfunktionen; andernfalls steht nur die Option **Import External LSAs** (Externe LSAs importieren) zur Verfügung.

SPF Runs (SPF-Läufe) – Gibt an, wie oft die Tabelle mit Routen innerhalb eines Bereichs unter Verwendung der Verbindungsstatusdatenbank des betreffenden Bereichs berechnet wurde. Die Berechnung erfolgt in der Regel mit Hilfe des Dijkstra-Algorithmus.

Area Border Router Count (Anzahl ABRs) – Die Gesamtzahl der ABRs, die innerhalb dieses Bereichs erreicht werden können. Dieses Feld ist ursprünglich auf Null gesetzt und wird bei jedem SPF-Durchlauf neu berechnet.

Area LSA Count (Anzahl Area-LSAs) – Die Gesamtzahl der LSAs in der Verbindungsstatusdatenbank des Bereichs; AS-external-LSAs werden nicht berücksichtigt.

Area LSA Checksum (Prüfsumme der Area-LSAs) – Die 32-Bit-Summe (ohne Vorzeichen) der LS-Prüfsummen der LSAs, die in der Verbindungsstatusdatenbank des Bereichs enthalten sind. Externe LSAs des LS-Typs 5 sind nicht in diesem Wert berücksichtigt. Anhand dieser Summe kann festgestellt werden, ob es in der Verbindungsstatusdatenbank Änderungen gab; außerdem kann sie für den Vergleich der Verbindungsstatusdatenbanken zweier Router herangezogen

werden. Hier wird ein hexadezimaler Wert angegeben.

Stub Area Information (Stub Area-Informationen)

Import Summary LSAs (Summary-LSAs importieren) – Wählen Sie im Dropdown-Menü "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus. Bei Auswahl von **Enable** (Aktivieren) werden Summary-LSAs in die Stub Areas importiert.

Metric Value (Metrikwert) – Geben Sie den Metrikwert an, der für alle Standardrouten übernommen werden soll, die in der Stub Area mitgeteilt werden. Zulässig sind Werte zwischen 1 und 16.777.215.

Metric Type (Metriktyp) – Wählen Sie den Typ der im Feld "Metric Value" (Metrikwert) angegebenen Metrik aus.

Translator Role (Übersetzerrolle) – Geben Sie für die NSSA-Übersetzerrolle "always/candidate" (immer/Kandidat) an.

Translator Stability Interval (Übersetzerstabilitätsintervall) – Geben Sie das Übersetzerstabilitätsintervall für die ausgewählte NSSA an.

No-Redistribute Mode (Keine Umverteilung) – Geben Sie die Routenumverteilung für die ausgewählte NSSA an.

Translator State (Übersetzerstatus) – Zeigt den aktuellen Status des Übersetzers an.

Konfigurieren eines OSPF-Bereichs

1. Öffnen Sie die Seite **OSPF Area Configuration** (OSPF-Bereichskonfiguration).
2. Geben Sie den Bereich an, der konfiguriert werden soll.
3. Geben Sie in den Feldern je nach Bedarf die entsprechenden Werte an.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der OSPF-Bereich wird definiert und konfiguriert.

Anzeigen einer OSPF-Bereichskonfiguration

1. Öffnen Sie die Seite **OSPF Area Configuration** (OSPF-Bereichskonfiguration).
2. Wählen Sie im Dropdown-Menü den OSPF-Bereich aus, der angezeigt werden soll.

   Die OSPF-Bereichskonfiguration für diesen Bereich wird angezeigt.

Löschen einer OSPF-Bereichskonfiguration

So löschen Sie eine NSSA- oder Stub Area-Konfiguration:

1. Öffnen Sie die Seite **OSPF Area Configuration** (OSPF-Bereichskonfiguration).
2. Wählen Sie im Dropdown-Menü die OSPF-Bereichskonfiguration aus, die gelöscht werden soll.

   Die Konfiguration wid angezeigt.
3. Klicken Sie auf **Delete** (Löschen).

   Die OSPF-Bereichskonfiguration wird entfernt.

Konfigurieren von OSPF-Bereichen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:*

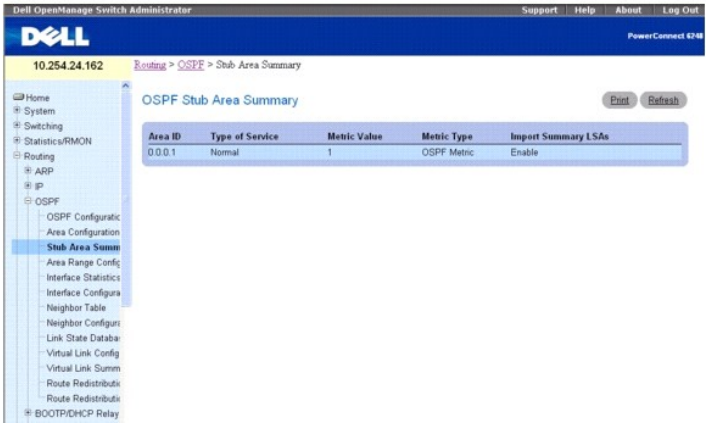
- OSPF Commands (OSPF-Befehle)

Zusammenfassende Daten zu Stub Areas

Über die Seite **OSPF Stub Area Summary** (Zusammenfassende Daten zu OSPF-Stub Areas) können Sie detaillierte Informationen zu OSPF-Stub Areas anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ OSPF→ Stub Area Summary (Zusammenfassende Daten zu Stub Areas)**.

Abbildung 10-8. Zusammenfassende Daten zu OSPF-Stub Areas



Die Seite **OSPF Stub Area Summary** (Zusammenfassende Daten zu OSPF-Stub Areas) enthält folgende Felder:

Area ID (Bereichs-ID) – Die Bereichs-ID der Stub Area.

Type of Service (Dienstart) – Die Dienstart, die der Stub Area-Metrik zugeordnet ist. Der Switch unterstützt nur die Einstellung **Normal** .

Metric Value (Metrikwert) – Zeigt die konfigurierte Metrik an.

Metric Type (Metriktyp) – Der Metriktyp für die Stub Area; gültige Typen sind:

- **OSPF Metric** (OSPF-Metrik) – Die normale OSPF-Metrik
- **Comparable Cost** (Vergleichbarer Aufwand) – Metriken des Typs 1, die mit der OSPF-Metrik vergleichbar sind
- **Non-comparable Cost** (Nicht vergleichbarer Aufwand) – Externe Metriken des Typs 2, von denen angenommen wird, dass ihr Aufwand über dem der OSPF-Metrik liegt

Import Summary LSAs (Summary-LSAs importieren) – Gibt an, ob der Import von Summary-LSAs aktiviert oder deaktiviert ist.

Anzeigen von OSPF-Stub Areas mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide (CLI-Referenzhandbuch) in folgendem Kapitel:*

- OSPF Commands (OSPF-Befehle)

Konfiguration des Adressbereichs eines Bereichs

Über die Seite **OSPF Area Range Configuration** (Konfiguration des Adressbereichs eines OSPF-Bereichs) können Sie den Adressbereich des Bereichs für einen angegebenen NSSA konfigurieren und festlegen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ OSPF→ Area Range Configuration (Konfiguration des Adressbereichs eines Bereichs)**.

Abbildung 10-9. Konfiguration des Adressbereichs eines OSPF-Bereichs

Die Seite **OSPF Area Range Configuration** (Konfiguration des Adressbereichs eines OSPF-Bereichs) enthält folgende Felder:

Area ID (Bereichs-ID) – Wählen Sie im Dropdown-Menü den Bereich aus, für den Daten konfiguriert werden sollen.

IP Address (IP-Adresse) – Geben Sie die IP-Adresse für den Adressbereich des ausgewählten Bereichs ein.

Subnet Mask (Subnetzmaske) – Geben Sie die Subnetzmaske für den Adressbereich des ausgewählten Bereichs ein.

LSDB Type (LSDB-Typ) – Wählen Sie den Typ der Verbindungsmitteilung aus, der dem angegebenen Bereich und dem Adressbereich zugeordnet ist. Standardtyp ist **Network Summary** (Zusammenfassende Daten zum Netzwerk).

Advertisement (Mitteilung) – Wählen Sie "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus dem Dropdown-Menü. Bei Auswahl von "Enable" (Aktivieren) wird der Adressbereich außerhalb des Bereichs über eine Network-Summary-LSA mitgeteilt. Der Standardwert ist **Enable** (Aktivieren).

Add (Hinzufügen) – Aktivieren Sie das Kontrollkästchen "Add" (Hinzufügen), wenn der Adressbereich eines Bereichs hinzugefügt werden soll.

OSPF Area Range Table (Tabelle für den Adressbereich eines OSPF-Bereichs)

Area ID (Bereichs-ID) – Zeigt den OSPF-Bereich an.

IP Address (IP-Adresse) – Zeigt die IP-Adresse eines Adressbereichs für den Bereich an.

Subnet Mask (Subnetzmaske) – Zeigt die Subnetzmaske eines Adressbereichs für den Bereich an.

LSDB Type (LSDB-Typ) – Zeigt den Typ der Verbindungsmitteilung für den Adressbereich und den Bereich an.

Advertisement (Mitteilung) – Zeigt den Mitteilungsmodus für den Adressbereich und den Bereich an.

Remove (Entfernen) – Entfernt den angegebenen Bereichseintrag.

Definieren des Adressbereichs eines OSPF-Bereichs

1. Öffnen Sie die Seite **OSPF Area Range Configuration** (Konfiguration des Adressbereichs eines OSPF-Bereichs).
2. Geben Sie die Bereichs-ID, die IP-Adresse, die Subnetzmaske, den LSDB-Typ und den Mitteilungsmodus ein.
3. Klicken Sie auf das Kontrollkästchen **Add** (Hinzufügen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Adressbereich des OSPF-Bereichs wird definiert und konfiguriert. Alle konfigurierten Adressbereiche eines OSPF-Bereichs werden in der Tabelle auf der Seite **OSPF Area Range Configuration** (Konfiguration des Adressbereichs eines OSPF-Bereichs) angezeigt.

Entfernen der Konfiguration des Adressbereichs eines OSPF-Bereichs

1. Öffnen Sie die Seite **OSPF Area Range Configuration** (Konfiguration des Adressbereichs eines OSPF-Bereichs).
2. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen) in der Zeile **Area ID to be deleted** (Zu löschende Bereichs-ID).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Adressbereich wird aus der Bereichskonfiguration entfernt.

Konfigurieren eines Adressbereichs für einen OSPF-Bereich mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:*

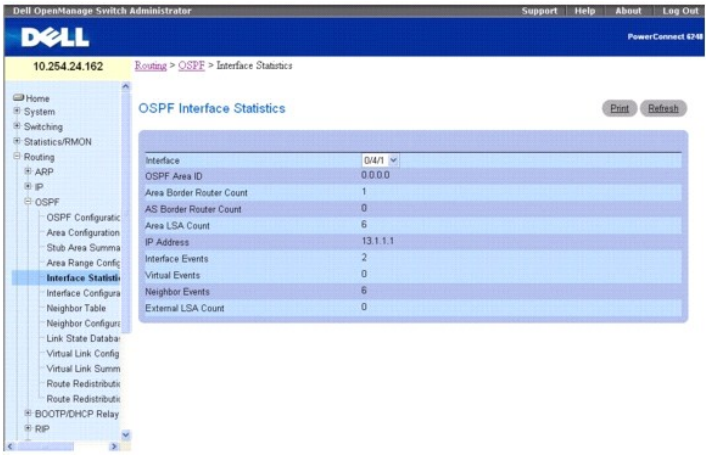
- OSPF Commands (OSPF-Befehle)

Schnittstellenstatistiken

Auf der Seite **OSPF Interface Statistics** (OSPF-Schnittstellenstatistik) werden die Statistikdaten für die ausgewählte Schnittstelle angezeigt. Die Informationen werden nur angezeigt, wenn OSPF aktiviert ist.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ OSPF→ Interface Statistics (Schnittstellenstatistik)**.

Abbildung 10-10. OSPF-Schnittstellenstatistik



Die Seite **OSPF Interface Statistics** (OSPF-Schnittstellenstatistik) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie aus dem Dropdown-Menü die Schnittstelle aus, für die Daten angezeigt werden sollen.

OSPF Area ID (OSPF-Bereichs-ID) – Der OSPF-Bereich, zu dem die ausgewählte Routerschnittstelle gehört. Bei der OSPF-Bereichs-ID handelt es sich um ein 32-Bit-Integer in der Schreibweise mit Trennzeichen, das den Bereich, mit dem die Schnittstelle verbunden ist, eindeutig kennzeichnet.

Area Border Router Count (Anzahl ABRs) – Die Gesamtzahl der ABRs, die innerhalb dieses Bereichs erreicht werden können. Dieses Feld ist ursprünglich auf Null gesetzt und wird bei jedem SPF-Durchlauf neu berechnet.

AS Border Router Count (Anzahl ASRBs) – Die Gesamtzahl der ASBRs (Autonomous System Border Router), die innerhalb dieses Bereichs erreicht werden können. Dieses Feld ist ursprünglich auf Null gesetzt und wird bei jedem SPF-Durchlauf neu berechnet.

Area LSA Count (Anzahl Area-LSAs) – Die Gesamtzahl der LSAs in der Verbindungsstatusdatenbank des Bereichs; AS-external-LSAs werden nicht berücksichtigt.

IP Address (IP-Adresse) – Die IP-Adresse der Schnittstelle.

Interface Events (Schnittstellenereignisse) – Gibt an, wie oft Statusänderungen oder Fehler für die angegebene OSPF-Schnittstelle aufgetreten sind.

Virtual Events (Virtuelle Ereignisse) – Gibt an, wie oft Statusänderungen oder Fehler für diese virtuelle Verbindung aufgetreten sind.

Neighbor Events (Nachbarereignisse) – Gibt an, wie oft Statusänderungen oder Fehler für diese Nachbarschaftsbeziehung aufgetreten sind.

External LSA Count (Anzahl externer LSAs) – Die Anzahl externer Mitteilungen des Verbindungsstatus (LSA) (LS-Typ 5) in der Verbindungsstatusdatenbank.

Anzeigen der OSPF-Schnittstellenstatistikdaten

1. Öffnen Sie die Seite **OSPF Interface Statistics** (OSPF-Schnittstellenstatistik).
2. Wählen Sie aus dem Dropdown-Menü die Schnittstelle aus, für die Daten angezeigt werden sollen.

   Die Statistikdaten dieser Schnittstelle werden angezeigt.

Anzeigen der OSPF-Schnittstellenstatistik mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide (CLI-Referenzhandbuch) in folgendem Kapitel:*

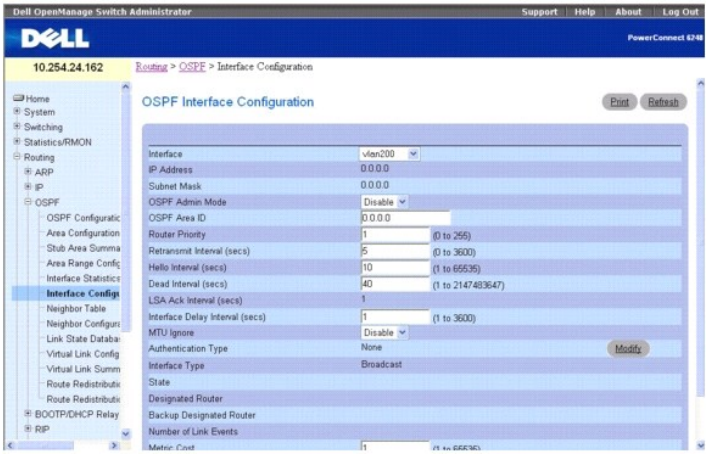
- OSPF Commands (OSPF-Befehle)

Schnittstellenkonfiguration

Auf der Seite **OSPF Interface Configuration** (OSPF-Schnittstellenkonfiguration) können Sie OSPF-Schnittstellen konfigurieren.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ OSPF→ Interface Configuration (Schnittstellenkonfiguration)**.

Abbildung 10-11. OSPF-Schnittstellenkonfiguration



Die Seite **OSPF Interface Configuration** (OSPF-Schnittstellenkonfiguration) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie aus dem Dropdown-Menü die Schnittstelle aus, für die Daten angezeigt oder konfiguriert werden sollen.

IP Address (IP-Adresse) – Zeigt die IP-Adresse der VLAN-Schnittstelle an.

Subnet Mask (Subnetzmaske) – Zeigt die Subnetzmaske der VLAN-Schnittstelle an.

OSPF Admin Mode (OSPF-Verwaltungsmodus) – Wählen Sie "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus dem Dropdown-Menü. Der Standardwert ist **Disable** (Deaktivieren). Sie können OSPF-Parameter auch ohne Aktivierung des OSPF-Verwaltungsmodus konfigurieren; die Änderungen werden allerdings erst wirksam, wenn dieser Modus aktiviert wird. Folgende Informationen werden nur bei Aktivierung des Verwaltungsmodus angezeigt: Status, designierter Router, designierter Backup-Router, Anzahl der Verbindungsereignisse, LSA-Bestätigungsintervall und Aufwandsmetrik. Damit OSPF uneingeschränkt funktioniert, müssen Sie über die Seite "IP Interface Configuration" eine gültige IP-Adresse (IP Address) und Subnetzmaske (Subnet Mask) eingeben.

ANMERKUNG: OSPF bleibt nach der Initialisierung auf dem Router so lange aktiv, bis der Router zurückgesetzt wird.

OSPF Area ID (OSPF-Bereichs-ID) – Geben Sie ein 32-Bit-Integer in der Schreibweise mit Trennzeichen ein, das den OSPF-Bereich, mit dem die ausgewählte Routerschnittstelle verbunden ist, eindeutig kennzeichnet. Bei Zuordnung einer nicht vorhandenen Bereichs-ID wird der Bereich unter Verwendung der Standardwerte erstellt.

Router Priority (Routerpriorität) – Geben Sie die OSPF-Priorität für die ausgewählte Schnittstelle ein. Die Schnittstellenpriorität wird als eine ganze Zahl zwischen 0 und 255 angegeben. Der Standardwert ist 1 (höchste Routerpriorität). Der Wert 0 gibt an, dass der Router nicht als designierter Router in diesem Netzwerk zur Verfügung steht.

Retransmit Interval (secs) (Rückübertragungsintervall) – Geben Sie das OSPF-Rückübertragungsintervall für die angegebene Schnittstelle an. Dies ist die Zeit in Sekunden zwischen LSAs für Nachbarschaftsbeziehungen (Adjacencies), die zu dieser Routerschnittstelle gehören. Dieser Wert wird auch bei der Rückübertragung von Datenbankbeschreibungen und LS-Anforderungspaketen verwendet. Zulässig sind Werte zwischen 0 und 3600 Sekunden (1 Stunde). Der Standardwert ist 5 Sekunden.

Hello Interval (secs) (Hello-Intervall) – Geben Sie das OSPF-Hello-Intervall (in Sekunden) für die angegebene Schnittstelle an. Dieser Parameter muss für alle Router, die mit einem Netzwerk verbunden sind, derselbe sein. Zulässig sind Werte zwischen 1 und 65535 Sekunden; der Standardwert ist 10 Sekunden.

Dead Interval (secs) (Totintervall) – Geben Sie das OSPF-Totintervall (in Sekunden) für die angegebene Schnittstelle an. Gibt an, wie lange ein Router auf das Eintreffen von Hello-Paketen eines benachbarten Routers wartet, bevor dieser als ausgefallen bezeichnet wird. Dieser Parameter muss für alle Router, die mit einem Netzwerk verbunden sind, derselbe sein. Er sollte ein Vielfaches des Hello-Intervalls sein (z. B 4). Zulässig sind Werte zwischen 1 und 2147483647; der Standardwert ist 40.

LSA Ack Interval (LSA-Bestätigungsintervall) – Die Zeit in Sekunden zwischen der Übertragung von LSA-Bestätigungspaketen; dieses Intervall muss kürzer als das Rückübertragungsintervall sein.

Interface Delay Interval (secs) (Verzögerungsintervall der Schnittstelle) – Geben Sie die OSPF-Verzögerung bei Statusübergängen für die angegebene Schnittstelle an. Gibt die geschätzte Zeit in Sekunden an, die die Übertragung eines LSU-Pakets über die ausgewählte Schnittstelle dauert. Zulässig sind Werte zwischen 1 und 3600 Sekunden (1 Stunde). Der Standardwert ist 1 Sekunde.

MTU Ignore (MTU ignorieren) – Deaktiviert die Erkennung nicht übereinstimmender OSPF-MTUs bei empfangenen Paketen. Der Standardwert ist **Disable** (Deaktivieren).

Authentication Type (Authentifizierungstyp) – Sie können auch einen anderen Authentifizierungstyp als "None" (Keiner) angeben, indem Sie auf **Modify** (Ändern) klicken. Daraufhin wird eine neue Webseite angezeigt, auf der Sie im Dropdown-Menü den gewünschten Authentifizierungstyp auswählen können. Mögliche Werte:

- **None** (Keiner) – Der ursprüngliche Status der Schnittstelle. Wenn Sie diese Option im Dropdown-Menü der zweiten Anzeige auswählen und auf **Apply Changes** (Änderungen übernehmen) klicken, kehren Sie in die erste Anzeige zurück, und es werden keine Authentifizierungsprotokolle ausgeführt.
- **Simple** (Einfach) – Bei Auswahl dieser Option werden Sie zur Eingabe eines Authentifizierungsschlüssels aufgefordert. Dieser Schlüssel wird im Klartext in den OSPF-Header aller Pakete übernommen, die über das Netzwerk gesendet werden. Für alle Router im Netzwerk muss derselbe Schlüssel konfiguriert werden.
- **Encrypt** (Verschlüsseln) – Bei Auswahl dieser Option werden Sie zur Eingabe eines Authentifizierungsschlüssels und einer Authentifizierungs-ID aufgefordert. Die Verschlüsselung erfolgt mit dem MD5-Message-Digest-Algorithmus. Für alle Router im Netzwerk muss derselbe Schlüssel konfiguriert werden.

Interface Type (Schnittstellentyp) – Der OSPF-Schnittstellentyp, der immer übertragen wird.

State (Status) – Der aktuelle Status der ausgewählten Routerschnittstelle. Mögliche Werte:

- **Down** (Nicht in Betrieb) – Der ursprüngliche Status der Schnittstelle. In diesem Status haben die Lower-Level-Protokolle angegeben, dass die Schnittstelle nicht verwendet werden kann. Die Schnittstellenparameter werden in diesem Status auf ihre ursprünglichen Werte zurückgesetzt. Alle Schnittstellenzeitgeber sind deaktiviert, und der Schnittstelle sind keine Nachbarschaftsbeziehungen zugeordnet.
- **Loopback** (Schleifentest) – In diesem Status wird die Schnittstelle des Routers zum Netzwerk per Hardware oder Software rückgeschleift. Die Schnittstelle steht daher für den normalen Datenverkehr nicht zur Verfügung. Trotzdem kann es wünschenswert sein, Angaben zur Qualität dieser Schnittstelle zu erhalten; dies geschieht entweder über ICMP-Ping-Signale zur Schnittstelle oder z. B. über einen Bitfehlertest. Daher können auch an eine Schnittstelle im Loopback-Status noch IP-Pakete gesendet werden. Um dies zu ermöglichen, werden diese Schnittstellen in Router-LSAs als einzelne Hostrouten mitgeteilt, bei deren Ziel es sich um die IP-Schnittstellenadresse handelt.
- **Waiting** (Wartestatus) – Der Router versucht, den designierten (Backup-)Router für das Netzwerk durch Überwachung der empfangenen Hello-Pakete zu ermitteln. Dabei darf der Router keinen designierten Backup-Router oder designierten Router bestimmen, bevor der Wartestatus nicht wieder verlassen wird. Dadurch werden unnötige Änderungen des designierten (Backup-)Routers verhindert.
- **Designated Router** (Designierter Router) – Dieser Router ist selbst der designierte Router im verbundenen Netzwerk. Zu allen anderen Routern, die mit dem Netzwerk verbunden sind, werden Nachbarschaftsbeziehungen aufgebaut. Der Router muss außerdem eine Network-LSA für den Netzwerkknoten senden. Diese Network-LSA enthält Verbindungen zu allen Routern (einschließlich des designierten Routers), die mit dem Netzwerk verbunden sind.
- **Backup Designated Router** (Designierter Backup-Router) – Dieser Router ist selbst der designierte Backup-Router im verbundenen Netzwerk. Fällt der aktive designierte Router aus, wird dieser Router zum designierten Router. Er baut Nachbarschaftsbeziehungen zu allen anderen Routern auf, die mit dem Netzwerk verbunden sind. Die Aufgaben des designierten Backup-Routers beim Flooding (Fluten) unterscheiden sich geringfügig von denen des designierten Routers.
- **Other Designated Router** (Anderer designierter Router) – Die Schnittstelle ist mit einem Broadcast- oder NBMA-Netzwerk verbunden, in dem andere Router als designierter Router und Backup-Router festgelegt wurden. Der Router versucht, Nachbarschaftsbeziehungen zum designierten Router und zum designierten Backup-Router aufzubauen.

Der Status wird nur angezeigt, wenn der OSPF-Verwaltungsmodus aktiviert ist.

Designated Router (Designierter Router) – Die Kennung des designierten Routers für dieses Netzwerk, wie sie sich für den mitteilenden Router darstellt. Hier wird der designierte Router über seine Router-ID identifiziert; der Wert 0.0.0.0 gibt an, dass kein designierter Router vorhanden ist. Dieses Feld wird nur angezeigt, wenn der OSPF-Verwaltungsmodus aktiviert ist.

Backup Designated Router (Designierter Backup-Router) – Die Kennung des designierten Backup-Routers für dieses Netzwerk, wie sie sich für den mitteilenden Router darstellt. Hier wird der designierte Backup-Router über seine Router-ID identifiziert; das Feld wird auf 0.0.0.0 gesetzt, wenn kein designierter Backup-Router vorhanden ist. Dieses Feld wird nur angezeigt, wenn der OSPF-Verwaltungsmodus aktiviert ist.

Number of Link Events (Anzahl der Verbindungsereignisse) – Gibt an, wie oft sich der OSPF-Schnittstellenstatus geändert hat. Dieses Feld wird nur angezeigt, wenn der OSPF-Verwaltungsmodus aktiviert ist.

Metric Cost (Aufwandsmetrik) – Geben Sie den Wert dieser Schnittstelle für die Dienstart "Aufwand" (TOS = cost) ein. Für die Aufwandsmetrik kann ein Wert zwischen 1 und 65535 eingegeben werden. Dieser Parameter kann nur konfiguriert/angezeigt werden, wenn OSPF für die Schnittstelle aktiviert ist.

Konfigurieren einer OSPF-Schnittstellenkonfiguration

1. Öffnen Sie die Seite **OSPF Interface Configuration** (OSPF-Schnittstellenkonfiguration).
2. Geben Sie die Schnittstelle an, die konfiguriert werden soll.
3. Geben Sie in den Feldern je nach Bedarf die entsprechenden Werte an.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die OSPF-Schnittstelle wird konfiguriert.

Anzeigen einer OSPF-Schnittstellenkonfiguration

1. Öffnen Sie die Seite **OSPF Interface Configuration** (OSPF-Schnittstellenkonfiguration).
2. Wählen Sie aus dem Dropdown-Menü die VLAN-Schnittstelle aus, für die Daten angezeigt werden sollen.

   Die Konfigurationsdaten dieser Schnittstelle werden angezeigt.

Konfigurieren einer OSPF-Schnittstelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) im folgenden Kapitel:

- OSPF Commands (OSPF-Befehle)

Nachbarschaftstabelle

Auf der Seite **OSPF Neighbor Table** (OSPF-Nachbarschaftstabelle) können Sie die OSPF-Nachbarschaftstabelle anzeigen. Bei Angabe einer bestimmten Nachbar-ID werden ausführliche Informationen zu einem benachbarten Router angezeigt. Die nachstehenden Informationen werden nur angezeigt, wenn OSPF aktiviert ist.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ OSPF→ Neighbor Table (Nachbarschaftstabelle)**.

Abbildung 10-12. OSPF-Nachbarschaftstabelle

Die Seite **OSPF Neighbor Table** (OSPF-Nachbarschaftstabelle) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie aus einem Dropdown-Menü die Schnittstelle aus, für die Daten angezeigt werden sollen.

Router ID (Router-ID) – Ein 32-Bit-Integer in Schreibweise mit Trennzeichen, das die benachbarte Schnittstelle darstellt.

IP Address (IP-Adresse) – Die IP-Adresse der benachbarten Routerschnittstelle zu dem Netzwerk, mit dem der Router verbunden ist. Diese Adresse wird als Ziel-IP-Adresse verwendet, wenn Protokollpakete in Form von Unicast-Paketen über diese Nachbarschaftsverbindung gesendet werden. Außerdem wird diese Adresse in Router-LSAs als Verbindungs-ID für das Netzwerk, zu dem eine Verbindung besteht, verwendet, wenn der benachbarte Router als designierter Router festgelegt ist. Die Nachbar-IP-Adresse wird anhand der Hello-Pakete ermittelt, die vom benachbarten Router gesendet werden. Für virtuelle Verbindungen wird die Nachbar-IP-Adresse bei der Erstellung der Routingtabelle ermittelt.

Neighbor Interface Index (Nachbarschnittstellenindex) – Eine Schnittstelle, die den Nachbarschnittstellenindex kennzeichnet.

Anzeigen der OSPF-Nachbarschaftstabelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- OSPF Commands (OSPF-Befehle)

Nachbarschaftskonfiguration

Auf der Seite **OSPF Neighbor Configuration** (OSPF-Nachbarkonfiguration) können Sie die OSPF-Nachbarkonfiguration für eine ausgewählte Nachbar-ID anzeigen. Bei Angabe einer bestimmten Nachbar-ID werden ausführliche Informationen zu dem betreffenden benachbarten Router angezeigt. Die nachstehenden Informationen werden nur angezeigt, wenn OSPF aktiviert ist und die Schnittstelle einen Nachbarn hat. Bei der IP-Adresse handelt es sich um die IP-Adresse des Nachbarn.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ OSPF→ Neighbor Configuration (Nachbarkonfiguration)**.

Abbildung 10-13. OSPF-Nachbarkonfiguration

Die Seite **OSPF Neighbor Configuration** (OSPF-Nachbarkonfiguration) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie im Dropdown-Menü die VLAN-Schnittstelle aus, für die die Routingfunktion aktiviert werden soll.

Neighbor IP Address (IP-Adresse des Nachbars) – Wählen Sie die IP-Adresse des Nachbarn aus, für den Daten angezeigt werden sollen.

Router ID (Router-ID) – Ein 32-Bit-Integer in Schreibweise mit Trennzeichen, das den benachbarten Router angibt.

Options (Optionen) – Die vom benachbarten Router unterstützten optionalen OSPF-Funktionen. Das Feld mit den OSPF-Optionen ist in OSPF-Hello-Paketen, Datenbankbeschreibungspaketen sowie in allen LSAs enthalten. Über das Feld **Options** (Optionen) kann festgelegt werden, ob OSPF-Router optionale Funktionen unterstützen (oder nicht unterstützen) und ob sie anderen OSPF-Routern ihre Funktionsstufe mitteilen können. Auf diese Weise können in einer OSPF-Routingdomäne Router mit unterschiedlichen Funktionen eingesetzt werden. Der Wert in diesem Feld ist eine Bitmap, die die Funktionen des benachbarten Routers angibt.

Router Priority (Routerpriorität) – Zeigt die OSPF-Priorität für den angegebenen benachbarten Router an. Die Priorität eines benachbarten Routers wird als ganze Zahl zwischen 0 und 255 angegeben. Der Wert 0 gibt an, dass der Router nicht als designierter Router für dieses Netzwerk ausgewählt werden kann.

State (Status) – Für einen benachbarten Router können folgende Statusangaben gemacht werden:

- **Down** (Nicht in Betrieb) – Der ursprüngliche Kommunikationsstatus des benachbarten Routers. Er gibt an, dass keine neuen Daten vom benachbarten Router empfangen wurden. In NBMA-Netzwerken können auch an Router, die nicht in Betrieb sind, noch Hello-Pakete gesendet werden, allerdings weniger häufig.
- **Attempt** (Versuch) – Dieser Status ist nur für Nachbarn zulässig, die mit NBMA-Netzwerken verbunden sind. Er gibt an, dass keine neuen Daten vom Nachbarn empfangen wurden, aber unbedingt versucht werden sollte, den Nachbarn zu kontaktieren. Dazu werden in regelmäßigen Abständen (die über das Hello-Intervall festgelegt werden) Hello-Pakete an den benachbarten Router gesendet.
- **Init** (Initialisierung) – In diesem Status wurde vor kurzem ein Hello-Paket vom Nachbarn empfangen. Allerdings wurde noch keine bidirektionale Kommunikation mit dem Nachbarn eingerichtet (d. h. der Router selbst war noch nicht im Hello-Paket des Nachbarn enthalten). Alle Nachbarn in diesem Status (oder höher) sind in den von der zugeordneten Schnittstelle gesendeten Hello-Paketen aufgeführt.
- **2-Way** (Bidirektional) – In diesem Status ist die bidirektionale Kommunikation zwischen den beiden Routern eingerichtet. Dies kann über das Hello-Protokoll überprüft werden. Dies ist der Status kurz vor Einrichtung einer Nachbarschaftsbeziehung. Der designierte Backup-Router wird aus Nachbarpaaren ausgewählt, die mindestens den Status **2-Way** (Bidirektional) haben.
- **Exchange Start** (Start des Austausches) – Der erste Schritt bei der Herstellung einer Beziehung zwischen zwei benachbarten Routern. Hier wird festgelegt, bei welchem Router es sich um den Master handeln soll; außerdem wird die anfängliche DD-Sequenznummer festgelegt. Die Kommunikation zwischen benachbarten Routern in diesem Status oder höher wird als "Beziehung" (Adjacency) bezeichnet.
- **Exchange** (Austausch) – In diesem Status beschreibt der Router die gesamte Verbindungsstatusdatenbank, indem er Pakete mit der Datenbankbeschreibung an den benachbarten Router sendet. In diesem Status können auch Pakete mit Verbindungsstatusanforderungen gesendet werden, die die aktuellen LSAs des benachbarten Routers anfordern. Beziehungen in diesem Status oder höher werden von der Flooding-Prozedur verwendet. Über diese Verbindungen können sämtliche OSPF-Routingprotokollpakete gesendet und empfangen werden.
- **Loading** (Ladestatus) – In diesem Status werden Pakete mit Verbindungsstatusanforderungen an den benachbarten Router gesendet, die die aktuelleren LSAs anfordern, die im Status "Exchange" (Austausch) zwar erkannt, aber noch nicht empfangen wurden.
- **Full** (Vollständig) – In diesem Status besteht zwischen den benachbarten Routern eine vollständige Nachbarschaftsbeziehung. Diese Beziehungen sind in Router- und in Network-LSAs enthalten.

Events (Ereignisse) – Gibt an, wie oft Statusänderungen oder Fehler für diese Nachbarschaftsbeziehung aufgetreten sind.

Permanence (Persistenz) – Diese Variable gibt den Status des Eintrags an. "Dynamisch" und "persistent" beziehen sich auf die Art und Weise, in der der Nachbar mitgeteilt wurde.

Hellos Suppressed (Hello-Pakete unterdrückt) – Gibt an, ob Hello-Pakete an den benachbarten Router unterdrückt werden.

Retransmission Queue Length (Länge der Warteschlange für Übertragungswiederholungen) – Die aktuelle Länge der Warteschlange für Übertragungswiederholungen.

Anzeigen der OSPF-Nachbarkonfiguration

1. Öffnen Sie die Seite **OSPF Neighbor Configuration** (OSPF-Nachbarkonfiguration).
2. Wählen Sie die Schnittstelle und die IP-Adresse aus, die angezeigt werden sollen.

   Die Nachbarkonfiguration wird angezeigt.

Anzeigen der OSPF-Nachbarkonfiguration mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

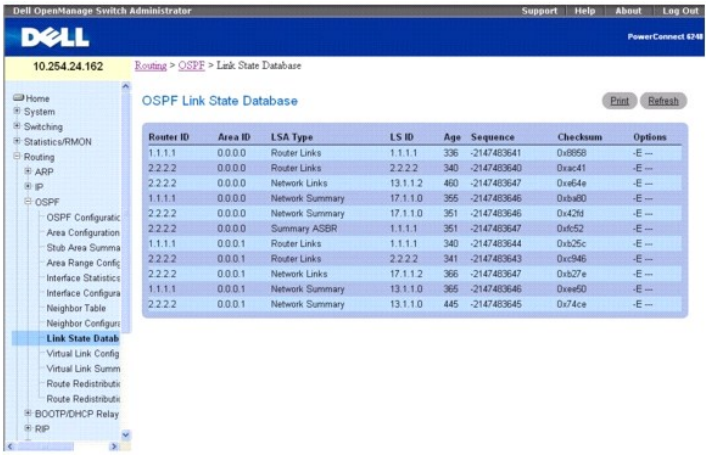
- OSPF Commands (OSPF-Befehle)

Verbindungsstatusdatenbank

Über die Seite **OSPF Link State Database** (OSPF-Verbindungsstatusdatenbank) können Sie OSPF-Verbindungsstatusinformationen anzeigen.

Um diese Seite anzuzeigen, klicken Sie auf **Routing→ OSPF→ Link State Database (Verbindungsstatusdatenbank)**.

Abbildung 10-14. OSPF-Verbindungsstatusdatenbank



Die Seite **OSPF Link State Database** (OSPF-Verbindungsstatusdatenbank) enthält folgende Felder:

Router ID (Router-ID) – Ein 32-Bit-Integer in der Schreibweise mit Trennzeichen, das den Router im autonomen System (AS) eindeutig kennzeichnet. Die Router-ID wird auf der Seite **IP Configuration** (IP-Konfiguration) gesetzt. Soll die Router-ID geändert werden, müssen Sie zunächst OSPF deaktivieren. Nachdem die neue Router-ID gesetzt wurde, müssen Sie OSPF wieder aktivieren, damit die Änderung wirksam wird. Standardwert ist 0.0.0.0, obwohl es sich hier nicht um eine gültige Router-ID handelt.

Area ID (Bereichs-ID) – Die ID eines OSPF-Bereichs, mit dem eine der Routerschnittstellen verbunden ist. Bei der Bereichs-ID handelt es sich um ein 32-Bit-Integer in der Schreibweise mit Trennzeichen, das den Bereich, mit dem eine Schnittstelle verbunden ist, eindeutig kennzeichnet.

LSA Type (LSA-Typ) – Format und Funktion einer LSA (Link-State Advertisement). Mögliche Werte:

- Router Links (Routerverbindungen)
- Network Links (Netzwerkverbindungen)
- Network Summary (Zusammenfassende Daten zum Netzwerk)
- ASBR Summary (Zusammenfassende Daten zum ASBR)
- **AS-external** (AS-extern)

LS ID (LS-ID) – Die Link-State-ID gibt den Teil der Routingdomäne an, der in der Mitteilung (Advertisement) beschrieben ist. Der Wert der LS-ID hängt vom LS-Typ der Mitteilung ab.

Age (Alter) – Die Zeit (in Sekunden), die seit dem ersten Senden der LSA vergangen ist.

Sequence (Sequenznummer) – In diesem Feld wird die Sequenznummer als ein 32-Bit-Integer mit Vorzeichen angegeben. Über dieses Feld werden alte und mehrfach vorhandene LSAs ermittelt. Je höher die Sequenznummer, desto aktueller die LSA.

Checksum (Prüfsumme) – Über die Prüfsumme können fehlerhafte Daten in einer LSA ermittelt werden. Solche Fehler können beim Flooding (Fluten) einer LSA auftreten oder während sich eine LSA im Routerspeicher befindet. Dieses Feld enthält die Prüfsumme des gesamten LSA-Inhalts mit Ausnahme des Feldes, das das LS-Alter enthält.

Options (Optionen) – In diesem Feld des LSA-Headers werden die optionalen Funktionen angegeben, über die die LSA verfügt. Mögliche Werte:

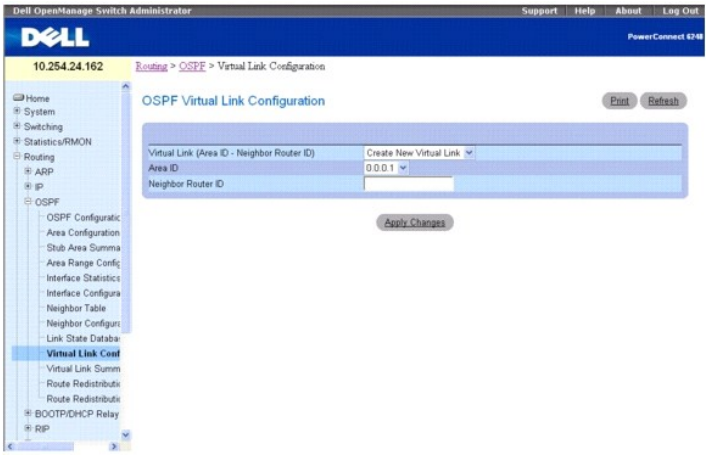
- **Q** – Aktiviert die Unterstützung für "QoS Traffic Engineering".
- **E** – Gibt an, wie AS-external-LSAs geflutet werden.
- **MC** – Gibt an, wie IP-Multicast-Datagramme entsprechend der Standardspezifikation weitergeleitet werden.
- **O** – Gibt an, ob Opaque-LSAs unterstützt werden.
- **V** – Gibt an, ob OSPF++-Erweiterungen für VPN/COS unterstützt werden.

Konfiguration virtueller Verbindungen

Über die Seite **Virtual Link Configuration** (Konfiguration virtueller OSPF-Verbindungen) können Sie Informationen zu einer virtuellen Schnittstelle für einen bestimmten Bereich und einen bestimmten Nachbarn erstellen und konfigurieren. Diese Seite kann erst angezeigt werden, nachdem ein gültiger OSPF-Bereich konfiguriert wurde.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ OSPF→ Virtual Link Configuration (Konfiguration einer virtuellen Verbindung)**.

Abbildung 10-15. Konfiguration einer virtuellen OSPF-Verbindung erstellen



Die Seite **OSPF Virtual Link Configuration** (Konfiguration virtueller OSPF-Verbindungen) enthält folgende Felder:

Virtual Link (Area ID - Neighbor Router ID) (Virtuelle Verbindung (Bereichs-ID - ID des benachbarten Routers)) – Wählen Sie die virtuelle Verbindung aus, für die Daten angezeigt oder konfiguriert werden sollen. Sie besteht aus der Bereichs-ID und der ID des benachbarten Routers. Um eine neue virtuelle Verbindung zu erstellen, wählen Sie über das Dropdown-Menü die Option **Create New Virtual Link** (Neue virtuelle Verbindung erstellen) aus. Wenn **Create New Virtual Link** (Neue virtuelle Verbindung erstellen) ausgewählt ist, werden folgende Felder angezeigt:

Area ID (Bereichs-ID) – Das 32-Bit-Integer in der Schreibweise mit Trennzeichen, das den Bereich, mit dem eine Routerschnittstelle verbunden ist, eindeutig kennzeichnet.

Neighbor Router ID (ID des benachbarten Routers) – Das 32-Bit-Integer in der Schreibweise mit Trennzeichen, das den benachbarten Router, der Teil der virtuellen Verbindung ist, eindeutig kennzeichnet.

Hello Interval (Hello-Intervall) – Geben Sie das OSPF-Hello-Intervall (in Sekunden) für die angegebene Schnittstelle an. Dieser Parameter muss für alle Router, die mit einem Netzwerk verbunden sind, derselbe sein. Zulässig sind Werte zwischen 1 und 65535 Sekunden; der Standardwert ist 10 Sekunden.

Dead Interval) (Totintervall) – Geben Sie das OSPF-Totintervall (in Sekunden) für die angegebene Schnittstelle an. Gibt an, wie lange ein Router auf das Eintreffen von Hello-Paketen eines benachbarten Routers wartet, bevor dieser als ausgefallen bezeichnet wird. Dieser Parameter muss für alle Router, die mit einem Netzwerk verbunden sind, derselbe sein. Er sollte ein Vielfaches des Hello-Intervalls sein (z. B 4). Zulässig sind Werte zwischen 1 und 65535 Sekunden; der Standardwert ist 40 Sekunden.

Interface Delay Interval (secs) (Verzögerungsintervall der Schnittstelle) – Die OSPF-Verzögerung bei Statusübergängen (in Sekunden) für die virtuelle Verbindung. Gibt die geschätzte Zeit in Sekunden an, die die Übertragung eines LSU-Pakets über diese Schnittstelle dauert.

State (Status) – Der aktuelle Status der ausgewählten virtuellen Verbindung. Dabei kann es sich um eine der folgenden Statusangaben handeln:

- **Down** (Nicht in Betrieb) – Der ursprüngliche Status der Schnittstelle. In diesem Status haben die Lower-Level-Protokolle angegeben, dass die Schnittstelle nicht verwendet werden kann. Die Schnittstellenparameter werden in diesem Status auf ihre ursprünglichen Werte zurückgesetzt. Alle Schnittstellenzeitgeber sind deaktiviert, und der Schnittstelle sind keine Nachbarschaftsbeziehungen zugeordnet.
- **Waiting** (Wartestatus) – Der Router versucht, den designierten (Backup-)Router durch Überwachung der empfangenen Hello-Pakete zu ermitteln. Dabei darf der Router keinen designierten Backup-Router oder designierten Router bestimmen, bevor der Wartestatus nicht wieder verlassen wird. Dadurch werden unnötige Änderungen des designierten (Backup-)Routers verhindert.
- **Poin-to-Point** (Punkt-zu-Punkt) – Die Schnittstelle ist funktionsfähig und mit der virtuellen Verbindung verbunden. Wenn der Router in diesen Status wechselt, versucht er, eine Beziehung zu dem benachbarten Router herzustellen. Dazu werden an den Nachbarn Hello-Pakete in Sekundenintervallen gesendet, deren Anzahl über das Feld **Hello Interval** (Hello-Intervall) vorgegeben ist.
- **Designated Router** (Designierter Router) – Dieser Router ist selbst der designierte Router im verbundenen Netzwerk. Zu allen anderen Routern, die mit dem Netzwerk verbunden sind, werden Nachbarschaftsbeziehungen aufgebaut. Der Router muss außerdem eine Network-LSA für den Netzwerkknoten senden. Diese Network-LSA enthält Verbindungen zu allen Routern (einschließlich des designierten Routers), die mit dem Netzwerk verbunden sind.
- **Backup Designated Router** (Designierter Backup-Router) – Dieser Router ist selbst der designierte Backup-Router im verbundenen Netzwerk. Fällt der aktive designierte Router aus, wird dieser Router zum designierten Router. Er baut Nachbarschaftsbeziehungen zu allen anderen Routern auf, die mit dem Netzwerk verbunden sind. Die Aufgaben des designierten Backup-Routers beim Flooding (Fluten) unterscheiden sich geringfügig von denen des designierten Routers.
- **Other Designated Router** (Anderer designierter Router) – Die Schnittstelle ist mit einem Broadcast- oder NBMA-Netzwerk verbunden, in dem andere Router als designierter Router und Backup-Router festgelegt wurden. Der Router versucht, Nachbarschaftsbeziehungen zum designierten Router und zum designierten Backup-Router aufzubauen.

Neighbor State (Nachbarschaftsstatus) – Der Status der virtuellen Beziehung zum benachbarten Router.

Retransmit Interval (Rückübertragungsintervall) – Geben Sie das OSPF-Rückübertragungsintervall für die angegebene Schnittstelle an. Dies ist die Zeit in Sekunden zwischen LSAs für Nachbarschaftsbeziehungen (Adjacencies), die zu dieser Routerschnittstelle gehören. Dieser Wert wird auch bei der Rückübertragung von Datenbankbeschreibungen und LS-Anforderungspaketen verwendet. Zulässig sind Werte zwischen 0 und 3600 Sekunden (1 Stunde). Der Standardwert ist 5 Sekunden.

Authentication Type (Authentifizierungstyp) – Sie können auch einen anderen Authentifizierungstyp als "None" (Keiner) angeben, indem Sie auf **Configure Authentication** (Authentifizierung konfigurieren) klicken. Daraufhin wird ein neue Bildschirm angezeigt, auf dem Sie im Dropdown-Menü den gewünschten Authentifizierungstyp auswählen können. Sie haben folgende Möglichkeiten:

- **None** (Keiner) – Der ursprüngliche Status der Schnittstelle. Wenn Sie diese Option im Dropdown-Menü der zweiten Anzeige auswählen und auf **Apply Changes** (Änderungen übernehmen) klicken, kehren Sie in die erste Anzeige zurück.
- **Simple** (Einfach) – Bei Auswahl dieser Option werden Sie zur Eingabe eines Authentifizierungsschlüssels aufgefordert. Dieser Schlüssel wird im Klartext in den OSPF-Header aller Pakete übernommen, die über das Netzwerk gesendet werden. Für alle Router im Netzwerk muss derselbe Schlüssel konfiguriert werden.

- **Encrypt** (Verschlüsseln) – Bei Auswahl dieser Option werden Sie zur Eingabe eines Authentifizierungsschlüssels und einer Authentifizierungs-ID aufgefordert. Die Verschlüsselung erfolgt mit dem MD5-Message-Digest-Algorithmus. Für alle Router im Netzwerk muss derselbe Schlüssel konfiguriert werden.

Authentication Key (Authentifizierungsschlüssel) – Geben Sie den OSPF-Authentifizierungsschlüssel für die angegebene Schnittstelle an. Wenn keine Authentifizierung verwendet werden soll (Auswahl **None**), werden Sie auch nicht zur Eingabe eines Schlüssels aufgefordert. Bei Auswahl von "Simple" (Einfach) kann kein Schlüssel mit mehr als 8 Zeichen verwendet werden. Bei Auswahl von "Encrypt" (Verschlüsseln) kann der Schlüssel bis zu 16 Zeichen lang sein. Der Schlüsselwert wird nur angezeigt, wenn Sie mit Lese- und Schreibberechtigung angemeldet sind; andernfalls wird er in Form von Sternchen angezeigt.

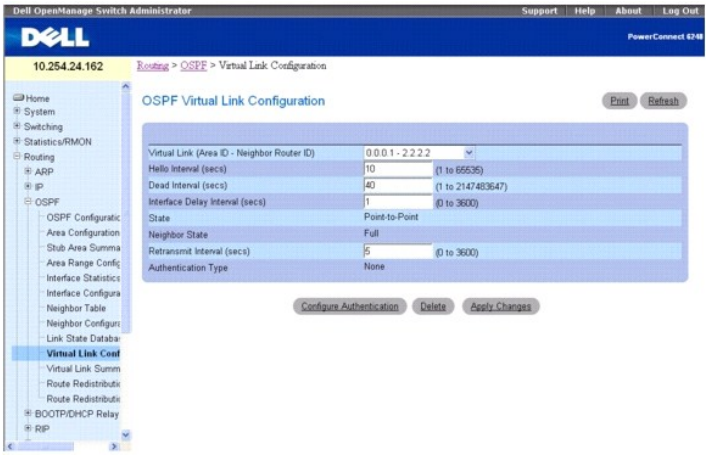
Authentication ID (Authentifizierungs-ID) – Geben Sie die ID ein, die für die Authentifizierung verwendet werden soll. Nur bei Auswahl von **Encrypt** (Verschlüsseln) als Authentifizierungstyp werden Sie zur Eingabe einer ID aufgefordert. Die ID ist eine Zahl zwischen 0 und 255 (einschließlich).

Definieren einer neuen virtuellen Verbindung

1. Öffnen Sie die Seite **OSPF Virtual Link Configuration** (Konfiguration virtueller OSPF-Verbindungen).
2. Wählen Sie im Dropdown-Menü **Virtual Link (Area ID - Neighbor Router ID)** (Virtuelle Verbindung [Bereichs-ID - ID des benachbarten Routers]) die Option **Create New Virtual Link** (Neue virtuelle Verbindung erstellen).
3. Geben Sie für die neue virtuelle Verbindung die ID des benachbarten Routers an.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Nach der Erstellung der virtuellen Verbindung werden die übrigen Felder angezeigt.

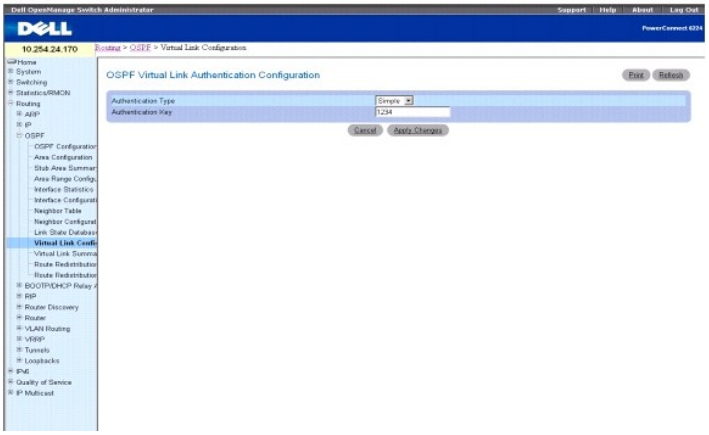
Abbildung 10-16. Konfiguration einer virtuellen OSPF-Verbindung



5. Klicken Sie auf **Configure Authentication** (Authentifizierung konfigurieren), um die Authentifizierung zu ändern.

   Die folgende Seite wird geöffnet:

Abbildung 10-17. Konfiguration der Authentifizierung für eine virtuelle OSPF-Verbindung



6. Wählen Sie Werte für **Authentication Type** (Authentifizierungstyp) und **Authentication Key** (Authentifizierungsschlüssel) aus.
7. Klicken Sie anschließend auf **Apply Changes** (Änderungen übernehmen).

Konfigurieren der Daten einer virtuellen Verbindung

1. Öffnen Sie die Seite **OSPF Virtual Link Configuration** (Konfiguration virtueller OSPF-Verbindungen).
2. Geben Sie die Bereichs-ID (Area ID) und die ID des benachbarten Routers (Neighbor Router ID) für die Konfiguration an.
3. Geben Sie in die Felder die entsprechenden Werte ein.
4. Klicken Sie auf **Configure Authentication** (Authentifizierung konfigurieren), um die Authentifizierung zu ändern.
5. Klicken Sie anschließend auf **Apply Changes** (Änderungen übernehmen).

   Die virtuellen Verbindungsdaten für die angegebenen IDs werden konfiguriert, und das Gerät wird entsprechend aktualisiert.

Anzeigen der Daten einer virtuellen Verbindung

1. Öffnen Sie die Seite **OSPF Virtual Link Configuration** (Konfiguration virtueller OSPF-Verbindungen).
2. Geben Sie die Bereichs-ID und die ID des benachbarten Routers an, die angezeigt werden sollen.

   Die Daten der virtuellen Verbindung für diese IDs werden angezeigt.

Entfernen einer virtuellen Verbindung

1. Öffnen Sie die Seite **OSPF Virtual Link Configuration** (Konfiguration virtueller OSPF-Verbindungen).
2. Geben Sie die Bereichs-ID und die ID des benachbarten Routers an, die der virtuellen Verbindung zugeordnet sind, die entfernt werden soll.

   Die Daten der virtuellen Verbindung werden angezeigt.
3. Klicken Sie auf **Delete** (Löschen).

   Die virtuelle Verbindung wird entfernt und das Gerät aktualisiert.

Konfigurieren der Daten einer virtuellen Verbindung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

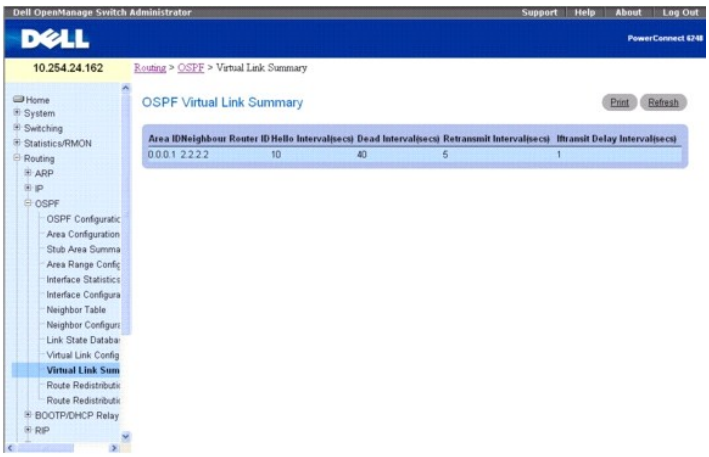
- OSPF Commands (OSPF-Befehle)

Zusammenfassende Daten zu virtuellen Verbindungen

Über die Seite **OSPF Virtual Link Summary** (Zusammenfassende Daten zu virtuellen OSPF-Verbindungen) können alle konfigurierten virtuellen Verbindungen angezeigt werden.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ OSPF→ Virtual Link Summary (Zusammenfassende Daten zu virtuellen Verbindungen)**.

Abbildung 10-18. Zusammenfassende Daten zu virtuellen OSPF-Verbindungen



Seite **OSPF Virtual Link Summary** (Zusammenfassende Daten zu virtuellen OSPF-Verbindungen) enthält folgende Felder:

Area ID (Bereichs-ID) – Die Bereichs-ID, Teil der Kennung der virtuellen Verbindung, zu der Daten angezeigt werden sollen. Die Bereichs-ID und die ID des benachbarten Routers zusammen kennzeichnen eine virtuelle Verbindung.

Neighbor Router ID (ID des benachbarten Routers) – Die ID des benachbarten Routers, Teil der Kennung der virtuellen Verbindung. Virtuelle Verbindungen können zwischen jeweils zwei ABR-Routern konfiguriert werden, die über Schnittstellen zu einem gemeinsamen Bereich (bei dem es sich nicht um eine Backbone Area handelt) verfügen.

Hello Interval (secs) (Hello-Intervall) – Das OSPF-Hello-Intervall (in Sekunden) für eine virtuelle Verbindung. Dieser Wert muss für alle Router, die mit einem Netzwerk verbunden sind, derselbe sein.

Dead Interval (secs) (Totintervall) – Das OSPF-Totintervall (in Sekunden) für eine virtuelle Verbindung. Gibt an, wie lange ein Router auf das Eintreffen von Hello-Paketen eines benachbarten Routers wartet, bevor dieser als ausgefallen bezeichnet wird. Dieser Parameter muss für alle Router, die mit einem gemeinsamen Netzwerk verbunden sind, derselbe sein und ein Vielfaches des Hello-Intervalls darstellen (z. B. 4).

Retransmit Interval (secs) (Rückübertragungsintervall) – Das OSPF-Rückübertragungsintervall (in Sekunden) für eine virtuelle Verbindung. Gibt die Zeit in Sekunden zwischen LSAs für Nachbarschaftsbeziehungen (Adjacencies) an, die zu dieser Routerschnittstelle gehören. Dieser Wert wird auch bei der Rückübertragung von Datenbankbeschreibungen und LS-Anforderungspaketen verwendet.

Iftransit Delay Interval (secs) (Verzögerungsintervall bei Schnittstellenstatusübergängen) – Die OSPF-Verzögerung (in Sekunden) bei Statusübergängen für die virtuelle Verbindung. Gibt die geschätzte Zeit in Sekunden an, die die Übertragung eines LSU-Pakets über diese Schnittstelle dauert.

Anzeigen der zusammenfassenden Daten zu einer virtuellen Verbindung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- OSPF Commands (OSPF-Befehle)

Konfiguration der Routenumverteilung

Über die Seite **OSPF Route Redistribution Configuration** (Konfiguration der OSPF-Routenumverteilung) können Sie die Umverteilung in OSPF für Routen konfigurieren, die über **Static** (Statisch), **Connected** (Verbunden) und **RIP** ermittelt wurden. Dabei kann die Umverteilung von Routen festgelegt werden, die entweder über alle diese Angaben oder nur über bestimmte Angaben ermittelt wurden.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ OSPF→ Route Redistribution Configuration (Konfiguration der Routenumverteilung)**.

Abbildung 10-19. Konfiguration der OSPF-Routenumverteilung

Die Seite **OSPF Route Redistribution Configuration** (Konfiguration der OSPF-Routenumverteilung) enthält folgende Felder:

Configured Source (Konfigurierte Quelle) – Ein für OSPF konfiguriertes Protokoll für die Umverteilung von Routen, die über dieses Protokoll ermittelt wurden. Es stehen nur Quellrouten zur Verfügung, die durch OSPF für eine Umverteilung konfiguriert wurden. Über **Create** (Erstellen) können Sie eine neue Quellroute konfigurieren.

Available Source (Verfügbare Quelle) – Ein Protokoll, mit dem OSPF für die Umverteilung der Routen konfiguriert werden kann. Dieses Feld ist nur verfügbar, wenn **Create** (Erstellen) für **Configured Source** (Konfigurierte Quelle) ausgewählt wurde. Mögliche Werte sind "Static" (Statisch), "Connected" (Verbunden) und "RIP".

Metric (Metrik) – Setzt den Metrikwert für umverteilte Routen. Für vorab konfigurierte Quellen wird in diesem Feld ein Metrikwert angezeigt. Mögliche Werte sind 0 bis 16777214.

Metric Type (Metriktyp) – Wählen Sie im Dropdown-Menü den OSPF-Metriktyp für umverteilte Routen aus.

Tag – Setzt das Tag-Feld in umverteilten Routen. Wurde die Quelle vorab konfiguriert, wird in diesem Feld ein Tag-Wert angezeigt; andernfalls enthält das Feld den Wert 0. Mögliche Werte sind 0 bis 4294967295.

Subnets (Subnetze) – Wählen Sie im Dropdown-Menü aus, ob Subnetzrouten umverteilt werden sollen.

Distribute List (Verteilungsliste) – Legt die Zugriffsliste fest, über die Routen nach Zielprotokoll umverteilt werden. Es werden nur zugelassene Routen umverteilt. Bezieht sich dieser Befehl auf eine nicht vorhandene Zugriffsliste, können alle Routen umverteilt werden. Im Dropdown-Menü werden die über die Seiten **Switching→ Network Security (Netzwerksicherheit)→ Access Control Lists (Zugriffssteuerungslisten)→ IP Access Control Lists (IP-Zugriffssteuerungslisten)** konfigurierten Zugriffssteuerungslisten (ACL) aufgeführt. Bei Verwendung als Routenfilter werden nur die folgenden Felder einer Zugriffsliste verwendet:

- Source IP Address and netmask (Quell-IP-Adresse und Netzwerkmaske)
- Destination IP Address and netmask (Ziel-IP-Adresse und Netzwerkmaske)
- Action (Aktion) (zulassen oder ablehnen)

Alle anderen Felder (**Source and Destination Port** (Quell- und Ziel-Port), **Precedence** (Bevorzugung), **tos** (TOS) usw.) werden ignoriert.

Die Quell-IP-Adresse wird mit der Ziel-IP-Adresse der Route verglichen. Die Quell-IP-Netzwerkmaske in der Zugriffslistenregel wird wie eine Wildcard-Maske gehandhabt, die angibt, welche Bits der Quell-IP-Adresse mit der Zieladdresse der Route übereinstimmen müssen. (Eine 1 in der Maske entspricht einem "Don't Care" (Beliebig) im entsprechenden Adressbit.)

Enthält eine Zugriffslistenregel eine Ziel-IP-Adresse und Netzwerkmaske (d. h. es handelt sich um eine erweiterte Zugriffsliste), wird die Ziel-IP-Adresse mit der Netzwerkmaske des Routenziels verglichen. Die Zielnetzwerkmaske in der Zugriffsliste dient als Wildcard-Maske, die angibt, welche Bits in der Zielmaske der Route für den Filtervorgang relevant sind.

Erstellen einer Quelle für die OSPF-Routenumverteilung

Wird keine Umverteilung konfiguriert, wird vom System im Feld **Configured Source** (Konfigurierte Quelle) nur die Option **Create** (Erstellen) angezeigt, im Feld **Available Source** (Verfügbare Quelle) werden die möglichen Quellen angezeigt. Bei Auswahl einer verfügbaren Quelle müssen Sie die Konfigurationsdaten eingeben und anschließend auf **Apply Changes** (Änderungen übernehmen) klicken; die Quelle wird daraufhin in der Dropdown-Liste **Configured Source** (Konfigurierte Quelle) angezeigt und aus der Dropdown-Liste **Available Source** (Verfügbare Quelle) entfernt.

1. Öffnen Sie die Seite **OSPF Route Redistribution Configuration** (Konfiguration der OSPF-Routenumverteilung).
2. Geben Sie **Create** (Erstellen) im Feld **Configured Source** (Konfigurierte Quelle) an.
3. Wählen Sie im Feld "Available Source" (Verfügbare Quelle) die Option "Static" (Statisch), "Connected" (Verbunden) oder "RIP" aus.
4. Klicken Sie anschließend auf **Apply Changes** (Änderungen übernehmen).

   Die Daten für die Routenumverteilung werden konfiguriert, und das Gerät wird entsprechend aktualisiert.

Ändern der Daten für die OSPF-Routenumverteilung

1. Öffnen Sie die Seite **OSPF Route Redistribution Configuration** (Konfiguration der OSPF-Routenumverteilung).
2. Wählen Sie in der Dropdown-Liste **Configured Source** (Konfigurierte Quelle) eine Quelle aus.
3. Geben Sie in die Felder die entsprechenden Werte ein.
4. Klicken Sie anschließend auf **Apply Changes** (Änderungen übernehmen).

   Die Daten für die Routenumverteilung werden konfiguriert und das Gerät entsprechend aktualisiert.

Konfigurieren der Daten für die OSPF-Routenumverteilung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

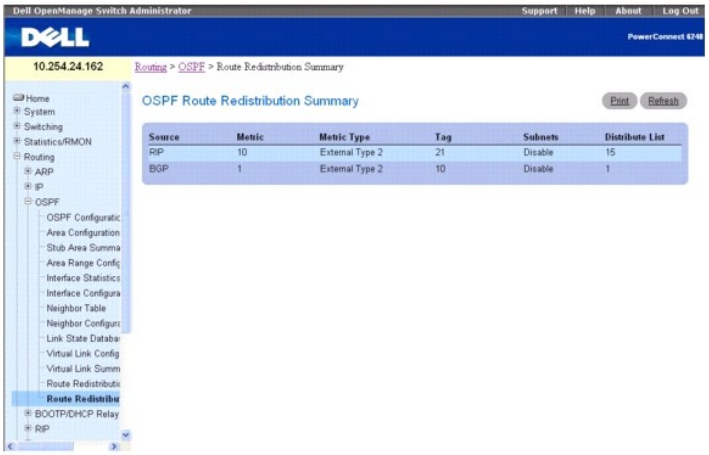
- OSPF Commands (OSPF-Befehle)

Zusammenfassende Daten zur Routenumverteilung

Über die Seite **OSPF Route Redistribution Summary** (Zusammenfassende Daten zur OSPF-Routenumverteilung) können Sie OSPF-Routenumverteilungskonfigurationen anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ OSPF→ Route Redistribution Summary (Zusammenfassende Daten zur Routenumverteilung)**.

Abbildung 10-20. Zusammenfassende Daten zur OSPF-Routenumverteilung



Die Seite **OSPF Route Redistribution Summary** (Zusammenfassende Daten zur OSPF-Routenumverteilung) enthält folgende Felder:

Source (Quelle) – Die Quellroute, die von OSPF umverteilt werden soll.

Metric (Metrik) – Der Metrikwert der umverteilten Routen für die Quellroute. Wird kein Wert konfiguriert, wird in diesem Feld **Unconfigured** (Nicht konfiguriert) angezeigt.

Metric Type (Metriktyp) – Der OSPF-Metriktyp der umverteilten Routen.

Tag – Das Tag-Feld in umverteilten Routen. Wurde die Quelle vorab konfiguriert, wird in diesem Feld der Tag-Wert angezeigt; andernfalls enthält das Feld den Wert 0.

Subnets (Subnetze) – Gibt an ob Subnetzrouten umverteilt werden sollen.

Distribute List (Verteilungsliste) – Die Zugriffsliste, über die Routen nach Zielprotokoll umverteilt werden.

Anzeigen der zusammenfassenden Daten zur Routenumverteilung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- OSPF Commands (OSPF-Befehle)

BOOTP / DHCP Relay Agent

Mit Hilfe des BootP/DHCP Relay Agent können BootP/DHCP-Clients und -Server BootP/DHCP-Meldungen über verschiedene Subnetze austauschen. Der Relay Agent empfängt Anforderungen von den Clients und überprüft die gültigen Hops und 'giaddr'-Felder. Ist die Anzahl der Hops größer als die der konfigurierten Hops, geht der Agent davon aus, dass das Paket durch die Agenten durchgeschleift wurde, und lehnt das Paket ab. Enthält das Feld 'giaddr' einen Nullwert, muss der Agent in diesem Feld die IP-Adresse der Schnittstelle eingeben, von der die Anforderung empfangen wurde. Die gültigen Pakete werden vom Agenten per Unicasting an das nächste konfigurierte Ziel gesendet. Der Server reagiert mit einer Unicast-BOOTREPL an den Relay Agent, der dem im Feld 'giaddr' angegebenen Client am nächsten ist. Nach Empfang des BOOTREPLY vom Server leitet der Agent diese Antwort per Broadcasting oder Unicasting an die Schnittstelle weiter, an der die BOOTREQUEST eingegangen ist. Diese Schnittstelle kann über das Feld 'giaddr' ermittelt werden.

Die DHCP-Komponente der 6200-Reihe unterstützt auch DHCP Relay Agent-Optionen, über die die Quellschaltung ermittelt werden kann, wenn Benutzer über ein Hochgeschwindigkeitsmodem mit dem Internet verbunden sind. Der Relay Agent fügt diese Optionen beim Weiterleiten der Anforderung an den Server ein und entfernt sie wieder, wenn er eine Antwort an die Clients sendet.

Hat eine Schnittstelle mehrere IP-Adressen, sollte der Relay Agent die primäre IP-Adresse verwenden, die für ihn als Relay Agent-IP-Adresse konfiguriert wurde.

Die Seite **BOOTP / DHCP Relay Agent** enthält Links zu Webseiten, auf denen der BOOTP/DHCP Relay Agent konfiguriert und angezeigt wird kann. Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ BOOTP / DHCP Relay Agent**. Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

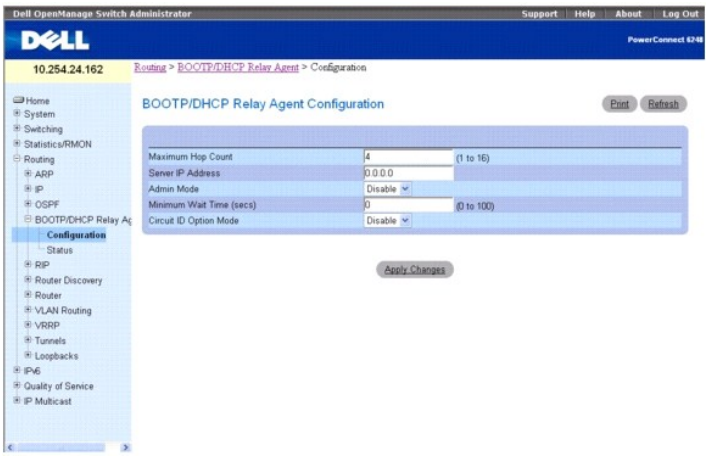
- BOOTP/DHCP Relay Agent-Konfiguration
- BOOTP/DHCP Relay Agent-Status

BOOTP / DHCP Relay Agent-Konfiguration

Über die Seite **BOOTP / DHCP Relay Agent Configuration** (BOOTP/DHCP Relay Agent-Konfiguration) können Sie einen BOOTP/DHCP Relay Agent konfigurieren und anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ BOOTP / DHCP Relay Agent→ Configuration (Konfiguration)**.

Abbildung 10-21. BOOTP / DHCP Relay Agent-Konfiguration



Die Seite **BOOTP / DHCP Relay Agent Configuration** (BOOTP/DHCP Relay Agent-Konfiguration) enthält folgende Felder:

Maximum Hop Count (Max. Anzahl Hops) – Geben Sie die Anzahl der Hops an, über die eine Clientanforderung maximal geleitet werden kann, bevor sie abgelehnt wird.

Server IP Address (Server-IP-Adresse) – Geben Sie die IP-Adresse des BOOTP/DHCP-Servers oder des nächsten BOOTP/DHCP Relay Agent ein.

Admin Mode (Verwaltungsmodus) – Wählen Sie **Enable** (Aktivieren) oder **Disable** (Deaktivieren) aus dem Dropdown-Menü. Bei Auswahl von **Enable** (Aktivieren) werden BOOTP/DHCP-Anforderungen an die im Feld **Server IP Address** (Server-IP-Adresse) angegebene IP-Adresse weitergeleitet.

Minimum Wait Time(secs) (Mindestwartezeit) – Geben Sie einen Zeitraum (in Sekunden) ein. Diese Angabe wird mit der Zeitmarke in den Anforderungspaketen des Clients verglichen, die den Zeitraum seit dem Start des Clients angeben sollte. Es werden nur Pakete weitergeleitet, deren Zeitmarkenwert die Mindestwartezeit überschreitet.

Circuit ID Option Mode (Schaltungs-ID-Option) – Wählen Sie im Dropdown-Menü "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus. Bei Auswahl von **Enable** (Aktivieren) fügt der Relay Agent Option-82-Headerpakete in die DHCP-Anforderungspakete ein, bevor sie an den Server weitergeleitet werden, und entfernt sie wieder, wenn die Antworten an den Client gesendet werden.

Konfigurieren von BOOTP / DHCP

1. Öffnen Sie die Seite **BOOTP / DHCP Configuration** (BOOTP/DHCP-Konfiguration).
2. Geben Sie in die Felder die entsprechenden Werte ein.

3. Klicken Sie anschließend auf **Apply Changes** (Änderungen übernehmen).

   Die BOOTP/DHCP-Daten werden konfiguriert und das Gerät entsprechend aktualisiert.

Konfigurieren von BOOTP/DHCP mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

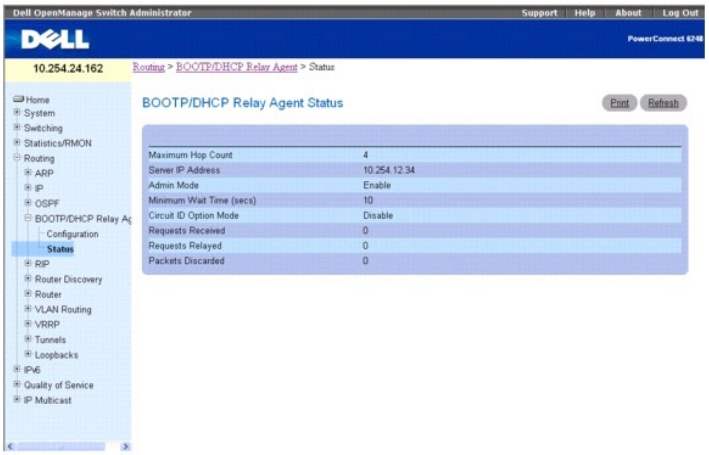
- DHCP and BOOTP Relay Commands (DHCP- und BOOTP Relay-Befehle)

BOOTP/DHCP Relay Agent-Status

Über die Seite **BOOTP/DHCP Relay Agent Status** (BOOTP/DHCP Relay Agent-Status) können Sie Konfigurations- und Statusdaten zum BOOTP/DHCP Relay Agent anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing**→ **BOOTP/DHCP Relay Agent**→ **Status**.

Abbildung 10-22. BOOTP/DHCP Relay Agent-Status



Die Seite **BOOTP/DHCP Status** (BOOTP/DHCP-Status) enthält folgende Felder:

Maximum Hop Count (Max. Anzahl Hops) – Die Anzahl der Hops, über die eine Clientanforderung maximal geleitet werden kann, ohne abgelehnt zu werden.

Server IP Address (Server-IP-Adresse) – Die IP-Adresse des BOOTP/DHCP-Servers oder des nächsten BOOTP/DHCP Relay Agent.

Admin Mode (Verwaltungsmodus) – Der Relay-Verwaltungsmodus. Bei Auswahl von **Enable** (Aktivieren) auf der Konfigurationsseite werden BOOTP/DHCP-Anforderungen an die im Feld **Server IP Address** (Server-IP-Adresse) angegebene IP-Adresse weitergeleitet.

Minimum Wait Time(secs) (Mindestwartezeit) – Der Mindestzeitraum in Sekunden. Diese Angabe wird mit der Zeitmarke in den Anforderungspaketen des Clients verglichen, die den Zeitraum seit dem Start des Clients angeben sollte. Es werden nur Pakete weitergeleitet, deren Zeitmarkenwert die Mindestwartezeit überschreitet.

Circuit ID Option Mode (Schaltungs-ID-Option) – Die Relay Agent-Option, die aktiviert oder deaktiviert werden kann. Bei Auswahl von **Enable** (Aktivieren) fügt der Relay Agent Option-82-Headerpakete in die DHCP-Anforderungspakete ein, bevor sie an den Server weitergeleitet werden, und entfernt sie wieder, wenn die Antworten an den Client gesendet werden.

Requests Received (Empfangene Anforderungen) – Die Gesamtzahl der BOOTP/DHCP-Anforderungen, die seit dem letzten Reset des Switch von allen Clients empfangen wurden.

Requests Relayed (Weitergeleitete Anforderungen) – Die Gesamtzahl der BOOTP/DHCP-Anforderungen, die seit dem letzten Reset des Switch an den Server weitergeleitet wurden.

Packets Discarded (Abgelehnte Pakete) – Die Gesamtzahl der BOOTP/DHCP-Anforderungen, die seit dem letzten Reset des Switch von diesem Relay Agent abgelehnt wurden.

Anzeigen von BOOTP/DHCP mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- DHCP and BOOTP Relay Commands (DHCP- und BOOTP Relay-Befehle)

RIP

RIP ist ein internes Gateway-Protokoll (IGP), das auf dem Bellman-Ford-Algorithmus basiert und für kleinere Netzwerke (mit einem Netzwerkdurchmesser von max. 15 Hops) gedacht ist. Die Routinginformationen werden in RIP-Aktualisierungspaketen weitergeleitet, die sowohl in regelmäßigen Abständen und bei Änderungen an der Netzwerktopologie gesendet werden. Bei Empfang einer RIP-Aktualisierung kann der Router die Route – je nachdem, ob sie in der Routentabelle vorhanden ist oder nicht – ändern, löschen oder der Routentabelle hinzufügen. Routenprioritäten werden über eine konfigurierbare Metrik übergeben, die die Entfernung für die einzelnen Ziele angibt.

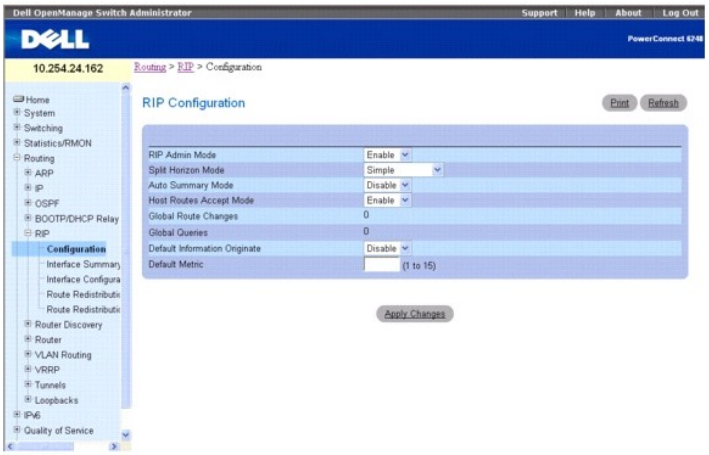
Die Menüseite **RIP** enthält Links zu Webseiten, auf denen RIP-Parameter und -Daten konfiguriert und angezeigt werden können. Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ RIP**. Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

- RIP-Konfiguration
- Zusammenfassende Daten zu RIP-Schnittstellen
- RIP-Schnittstellenkonfiguration
- Konfiguration der RIP-Routenumverteilung
- Zusammenfassende Daten zur RIP-Routenumverteilung

RIP-Konfiguration

Über die Seite **RIP Configuration** (RIP-Konfiguration) können Sie RIP im globalen Modus aktivieren und konfigurieren oder deaktivieren. Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ RIP→ Configuration (Konfiguration)**.

Abbildung 10-23. RIP-Konfiguration



Die Seite **RIP Configuration** (IP-Konfiguration) enthält folgende Felder:

RIP Admin Mode (RIP-Verwaltungsmodus) – Wählen Sie "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus dem Dropdown-Menü. Bei Auswahl von **Enable** (Aktivieren)

wird RIP für den Switch aktiviert. Die Standardeinstellung ist **Disable** (Deaktivieren).

Split Horizon Mode (Split Horizon) – Wählen Sie im Dropdown-Menü "None" (Keines), "Simple" (Einfach) oder "Poison Reverse" aus. Der Standardwert **Simple** (Einfach). Bei "Split Horizon" handelt es sich um ein Verfahren, mit dem Probleme vermieden werden können, die dadurch entstehen, dass Routen in Aktualisierungspaketen auch an den Router gesendet werden, von dem diese Route ursprünglich mitgeteilt wurde. Dies sind die möglichen Optionen:

- **None** (Keines) – Es gibt keine besonderen Maßnahmen für diesen Fall.
- **Simple** (Einfach) – Eine Route wird nicht in Aktualisierungspakete an den Router eingefügt, von dem sie ursprünglich mitgeteilt wurde.
- **Poison Reverse** – Eine Route wird zwar auch in Aktualisierungspakete an den Router eingefügt, von dem sie ursprünglich mitgeteilt wurde, die Metrik wird jedoch auf "unendlich" gesetzt".

Auto Summary Mode (Automatische Zusammenfassung) – Wählen Sie "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus dem Dropdown-Menü. Bei Auswahl von **Enable** (Aktivieren) werden benachbarte Routen zu je einem Eintrag zusammengefasst, um so die Gesamtzahl der Einträge zu verringern. Der Standardwert ist **Enable** (Aktivieren).

Host Routes Accept Mode (Hostrouten akzeptieren) – Wählen Sie im Dropdown-Menü "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus. Bei Auswahl von **Enable** (Aktivieren), werden vom Router Hostrouten akzeptiert. Der Standardwert ist **Enable** (Aktivieren).

Global Route Changes (Globale Routenänderungen) – Zeigt die Anzahl der Routenänderungen an, die von RIP in der IP-Routendatenbank vorgenommen wurden. Die Aktualisierung des Alters einer Route fällt nicht darunter.

Global Queries (Globale Abfragen) – Zeigt die Anzahl der Antworten an, die von anderen Systemen auf RIP-Abfragen hin gesendet wurden.

Default Information Originate (Standardinformationen senden) – Aktivieren oder deaktivieren Sie "Default Route Advertise" (Standardroute mitteilen).

Default Metric (Standardmetrik) – Gibt die Standardmetrik für umverteilte Routen an. Die Standardmetrik wird in diesem Feld nur angezeigt, wenn bereits ein Wert gesetzt wurde; wurde kein Wert konfiguriert, ist dieses Feld leer. Zulässige Werte sind 1 bis 15.

Konfigurieren von RIP

1. Öffnen Sie die Seite **RIP Configuration**(RIP-Konfiguration).
2. Geben Sie in die Felder die entsprechenden Werte ein.
3. Klicken Sie anschließend auf **Apply Changes** (Änderungen übernehmen).

   RIP wird konfiguriert und das Gerät entsprechend aktualisiert.

Konfigurieren von RIP mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

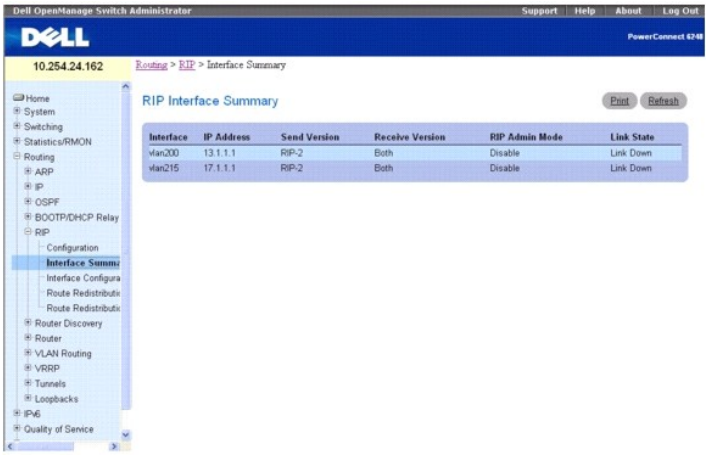
- Routing Information Protocol (RIP) Commands (RIP-Befehle)

Zusammenfassende Daten zu RIP-Schnittstellen

Über die Seite **RIP Interface Summary** (Zusammenfassende Daten zu RIP-Schnittstellen) kann der RIP-Konfigurationsstatus einer Schnittstelle angezeigt werden.

Um die Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ RIP→ Interface Summary (Schnittstellenzusammenfassung)**.

Abbildung 10-24. Zusammenfassende Daten zu RIP-Schnittstellen



Die Seite **RIP Interface Summary** (Zusammenfassende Daten zu RIP-Schnittstellen) enthält folgende Felder:

Interface (Schnittstelle) – Die Schnittstelle, wie beispielsweise das routingfähige VLAN, auf dem RIP aktiviert ist.

IP Address (IP-Adresse) – Die IP-Adresse der Routerschnittstelle.

Send Version (Gesendete Version) – Gibt die RIP-Version an, der RIP-Steuerungspakete entsprechen, die von der Schnittstelle gesendet werden. Der Standardwert ist RIP-2. Mögliche Werte sind:

- **RIP-1** – RIP-Version-1-Pakete werden per Broadcasting gesendet.
- **RIP-1c** – RIP-Version-1-Kompatibilitätsmodus. Pakete, die gemäß RIP-Version 2 formatiert sind, werden per Broadcasting übertragen.
- **RIP-2** – RIP-Version-2-Pakete werden per Multicasting gesendet.
- **None** (Keine) – Es werden keine RIP-Steuerungspakete übertragen.

Receive Version (Empfangene Version) – Gibt die RIP-Versionssteuerungspakete an, die von der Schnittstelle akzeptiert werden. Der Standardwert ist **Both** (Beide). Mögliche Werte:

- **RIP-1** – Es werden nur Pakete der RIP-Version 1 empfangen.
- **RIP-2** – Es werden nur Pakete der RIP-Version 2 empfangen.
- **Both** (Beide) – Pakete beider Versionen werden empfangen.
- **None** (Keine) – Es werden keine RIP-Steuerungspakete empfangen.

RIP Admin Mode (RIP-Verwaltungsmodus) – Gibt an, ob RIP für die Schnittstelle aktiviert oder deaktiviert ist.

Link State (Verbindungsstatus) – Gibt an, ob die RIP-Schnittstelle aktiv oder ausgefallen ist.

Anzeigen der zusammenfassenden Daten zu RIP-Schnittstellen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

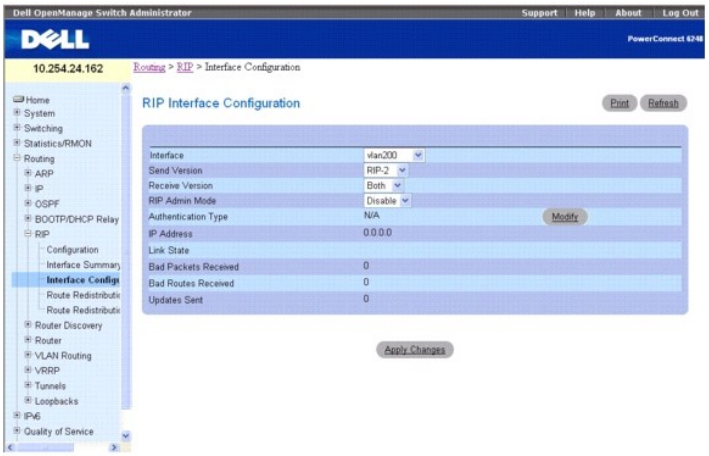
- Routing Information Protocol (RIP) Commands (RIP-Befehle)

RIP-Schnittstellenkonfiguration

Über die Seite **RIP Interface Configuration** (RIP-Schnittstellenkonfiguration) können Sie RIP für eine bestimmte Schnittstelle aktivieren und konfigurieren oder deaktivieren.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ RIP→ Interface Configuration (Schnittstellenkonfiguration)**.

Abbildung 10-25. RIP-Schnittstellenkonfiguration



Die Seite **RIP Interface Configuration** (RIP-Schnittstellenkonfiguration) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie aus dem Dropdown-Menü die Schnittstelle aus, für die Daten konfiguriert werden sollen.

Send Version (Gesendete Version) – Die RIP-Version, die der Router mit der Routeraktualisierung sendet. Der Standardwert ist RIP-2. Mögliche Werte sind:

- **RIP-1** – Pakete der RIP-Version 1 werden per Broadcasting gesendet.
- **RIP-1c** – RIP-Version-1-Kompatibilitätsmodus. Pakete, die gemäß RIP-Version 2 formatiert sind, werden per Broadcasting gesendet.
- **RIP-2** – RIP-Version-2-Pakete werden per Multicasting gesendet.
- **None** (Keine) – Es werden keine RIP-Steuerungspakete gesendet.

Receive Version (Empfangene Version) – Die RIP-Version der Routingaktualisierungen, die der Router akzeptieren muss. Der Standardwert ist **Both** (Beide). Mögliche Werte:

- **RIP-1** – Es werden nur Pakete der RIP-Version 1 akzeptiert.
- **RIP-2** – Es werden nur Pakete der RIP-Version 2 akzeptiert.
- **Both** (Beide) – Pakete beider Versionen werden akzeptiert.
- **None** (Keine) – Es werden keine RIP-Steuerungspakete akzeptiert.

RIP Admin Mode (RIP-Verwaltungsmodus) – Wählen Sie "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus dem Dropdown-Menü. Vor der Aktivierung von RIP-1 oder RIP-1c für eine Schnittstelle müssen Sie für diese zunächst den Modus "Broadcasting über Netzwerk" aktivieren. Der Standardwert ist **Disable** (Deaktivieren).

Authentication Type (Authentifizierungstyp) – Sie können auch einen anderen Authentifizierungstyp als "None" (Keiner) angeben, indem Sie auf **Modify** (Ändern) klicken. Daraufhin wird ein neue Bildschirm angezeigt, auf dem Sie im Dropdown-Menü den gewünschten Authentifizierungstyp auswählen können. Mögliche Werte:

- **None** (Keiner) – Der ursprüngliche Status der Schnittstelle. Wenn Sie diese Option im Dropdown-Menü der zweiten Anzeige auswählen und auf **Apply Changes** (Änderungen übernehmen) klicken, kehren Sie in die erste Anzeige zurück, und es werden keine Authentifizierungsprotokolle ausgeführt.
- **Simple** (Einfach) – Bei Auswahl dieser Option werden Sie zur Eingabe eines Authentifizierungsschlüssels aufgefordert. Dieser Schlüssel wird im Klartext in den RIP-Header aller Pakete übernommen, die über das Netzwerk gesendet werden. Für alle Router im Netzwerk muss derselbe Schlüssel konfiguriert werden.
- **Encrypt** (Verschlüsseln) – Bei Auswahl dieser Option werden Sie zur Eingabe eines Authentifizierungsschlüssels und einer Authentifizierungs-ID aufgefordert. Die Verschlüsselung erfolgt mit dem MD5-Message-Digest-Algorithmus. Für alle Router im Netzwerk muss derselbe Schlüssel konfiguriert werden.

IP Address (IP-Adresse) – Zeigt die IP-Adresse der Routerschnittstelle an.

Link State (Verbindungsstatus) – Gibt an, ob die RIP-Schnittstelle aktiv oder ausgefallen ist.

Bad Packets Received (Empfangene fehlerhafte Pakete) – Zeigt die Anzahl der ungültigen oder fehlerhaften RIP-Pakete an. Dies gilt NICHT für gesendete vollständige Aktualisierungspakete, die neue Informationen enthalten.

Bad Routes Received (Empfangene fehlerhafte Routen) – Zeigt die Anzahl der Routen in gültigen RIP-Paketen an, die aus irgendeinem Grund ignoriert wurden, z. B. die Anzahl der ausgelösten RIP-Aktualisierungen, die tatsächlich über diese Schnittstelle gesendet wurden. Dies gilt NICHT für gesendete vollständige Aktualisierungspakete, die neue Informationen enthalten.

Updates Sent (Gesendete Aktualisierungen) – Zeigt die Anzahl der gesendeten Routenaktualisierungen an.

Konfigurieren der RIP-Schnittstelle

1. Öffnen Sie die Seite **RIP Interface Configuration** (RIP-Schnittstellenkonfiguration).
2. Geben Sie die Schnittstelle an, für die Daten konfiguriert werden sollen.
3. Geben Sie in die Felder die entsprechenden Werte ein:

   Send Version (Gesendete Version) – Wählen Sie im Dropdown-Feld **None** (Keine), **RIP-1**, **RIP-1c** oder **RIP2** aus.

   Receive Version (Empfangene Version) – Wählen Sie im Dropdown-Feld **None** (Keine), **RIP-1**, **RIP-2** oder **Both** (Beide) aus.

   RIP Admin Mode (RIP-Verwaltungsmodus) – Wählen Sie **Enable** (Aktivieren) oder **Disable** (Deaktivieren) aus.

   Authentication Type (Authentifizierungstyp) – Klicken Sie auf **Modify** (Ändern), wenn andere Authentifizierungstypen konfiguriert werden sollen.
4. Klicken Sie anschließend auf **Apply Changes** (Änderungen übernehmen).

Die neue RIP-Schnittstelle wird konfiguriert und das Gerät aktualisiert.

Auswählen einer Authentifizierungsmethode

1. Öffnen Sie die Seite **RIP Interface Configuration** (RIP-Schnittstellenkonfiguration).
2. Geben Sie die Schnittstelle an, für die die Authentifizierungsmethode konfiguriert werden soll.
3. Klicken Sie auf **Modify** (Ändern).

   Die Seite **Authentication Method** (Authentifizierungsmethode) wird angezeigt.
4. Geben Sie im Dropdown-Menü den Authentifizierungstyp an ("None" (Keiner), "Simple" (Einfach) oder "Encrypt" (Verschlüsseln)).
5. Bei Angabe von **Simple** (Einfach) oder **Encrypt** (Verschlüsseln) werden weitere Felder angezeigt. Geben Sie den Authentifizierungsschlüssel (**Simple** (Einfach) oder **Encrypt** (Verschlüsseln)) und die ID für diesen Schlüssel (**Encrypt** (Verschlüsseln)) an.
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).
7. Die Authentifizierungsmethode und das Gerät werden aktualisiert.

Konfigurieren der RIP-Schnittstelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

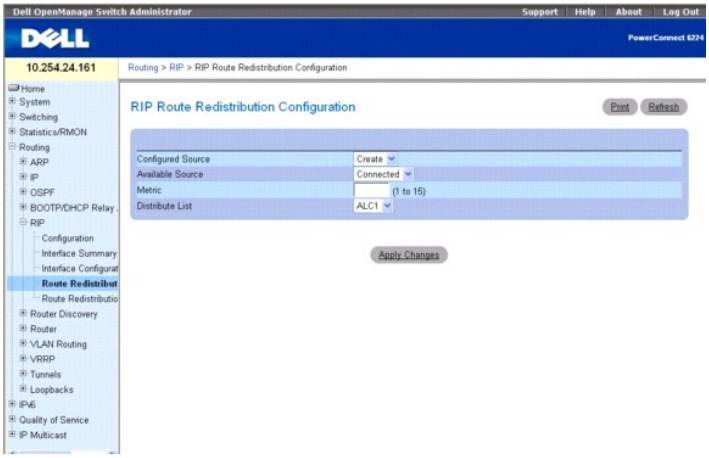
- Routing Information Protocol (RIP) Commands (RIP-Befehle)

Konfiguration der RIP-Routenumverteilung

Über die Seite **RIP Route Redistribution Configuration** (Konfiguration der RIP-Routenumverteilung) können Sie die Parameter für die RIP-Routenumverteilung konfigurieren. Die zulässigen Werte für die einzelnen Felder werden jeweils neben dem betreffenden Feld angezeigt. Bei Eingabe ungültiger Werte wird eine Alarmmeldung mit einer Liste aller zulässigen Werte ausgegeben.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ RIP→ Route Redistribution Configuration (Konfiguration der Routenumverteilung)**.

Abbildung 10-26. Konfiguration der RIP-Routenumverteilung



Die Seite **RIP Route Redistribution Configuration** (Konfiguration der RIP-Routenumverteilung) enthält folgende Felder:

Configured Source (Konfigurierte Quelle) – Dieses Auswahlfeld ist dynamisch und wird nur mit den Quellrouten gefüllt, die bereits für die Umverteilung durch RIP konfiguriert wurden. Über **Create** (Erstellen) können Sie eine verfügbare Quellroute konfigurieren.

Available Source (Verfügbare Quelle) – Dieses Auswahlfeld ist dynamisch und wird nur mit den Quellrouten gefüllt, die noch nicht für die Umverteilung durch RIP konfiguriert wurden. Dieses Feld ist nur verfügbar, wenn **Create** (Erstellen) für **Configured Source** (Konfigurierte Quelle) ausgewählt wurde. Mögliche Werte:

- **Static** (Statisch)
- **Connected** (Verbunden)
- **OSPF**

Metric (Metrik) – Legt den Wert fest, der als Metrik für umverteilte Routen verwendet werden soll. In diesem Feld wird die Metrik angezeigt, wenn die Quelle vorab konfiguriert wurde und geändert werden kann. Mögliche Werte sind 1 bis 15.

Distribute List (Verteilungsliste) – Dieses Auswahlfeld legt die Zugriffsliste fest, über die Routen nach Zielprotokoll umverteilt werden. Es werden nur zugelassene Routen umverteilt.

Im Dropdown-Menü werden die über die Seiten unter **Switching→ Network Security (Netzwerksicherheit)→ Access Control Lists (Zugriffssteuerungslisten)→ IP Access Control Lists (IP-Zugriffssteuerungslisten)** konfigurierten Zugriffssteuerungslisten (ACL) aufgeführt. Bei Verwendung als Routenfilter werden nur die folgenden Felder einer Zugriffsliste verwendet:

- Source IP Address and netmask (Quell-IP-Adresse und Netzwerkmaske)
- Destination IP Address and netmask (Ziel-IP-Adresse und Netzwerkmaske)
- Action (Aktion) (zulassen oder ablehnen)

Alle anderen Felder (**Source and Destination Port** (Quell- und Ziel-Port), **Precedence** (Bevorzugung), **tos** (TOS) usw.) werden ignoriert.

Die Quell-IP-Adresse wird mit der Ziel-IP-Adresse der Route verglichen. Die Quell-IP-Netzwerkmaske in der Zugriffslistenregel wird wie eine Wildcard-Maske gehandhabt, die angibt, welche Bits der Quell-IP-Adresse mit der Zieladdresse der Route übereinstimmen müssen. (Eine 1 in der Maske entspricht einem "Don't Care" (Beliebig) im entsprechenden Adressbit.)

Enthält eine Zugriffslistenregel eine Ziel-IP-Adresse und Netzwerkmaske (d. h. es handelt sich um eine erweiterte Zugriffsliste), wird die Ziel-IP-Adresse mit der Netzwerkmaske des Routenziels verglichen. Die Zielnetzwerkmaske in der Zugriffsliste dient als Wildcard-Maske, die angibt, welche Bits in der Zielmaske der Route für den Filtervorgang relevant sind.

Erstellen einer konfigurierten Quelle

1. Öffnen Sie die Seite **RIP Route Redistribution Configuration** (Konfiguration der RIP-Routenumverteilung).
2. Wählen Sie eine verfügbare Quelle aus, die konfiguriert werden soll.
3. Geben Sie in den restlichen Feldern die entsprechenden Werte ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die angegebene Quelle wird konfiguriert und das Gerät entsprechend aktualisiert.

Ändern einer konfigurierten Quelle

1. Öffnen Sie die Seite **RIP Route Redistribution Configuration** (Konfiguration der RIP-Routenumverteilung).

2. Wählen Sie die konfigurierte Quelle aus, die geändert werden soll.
3. Ändern Sie in der Anzeige die Werte nach Bedarf.
4. Klicken Sie auf **Apply Changes**

   Die Änderungen werden gespeichert, und das Gerät wird aktualisiert.

Konfigurieren der RIP-Routenumverteilung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

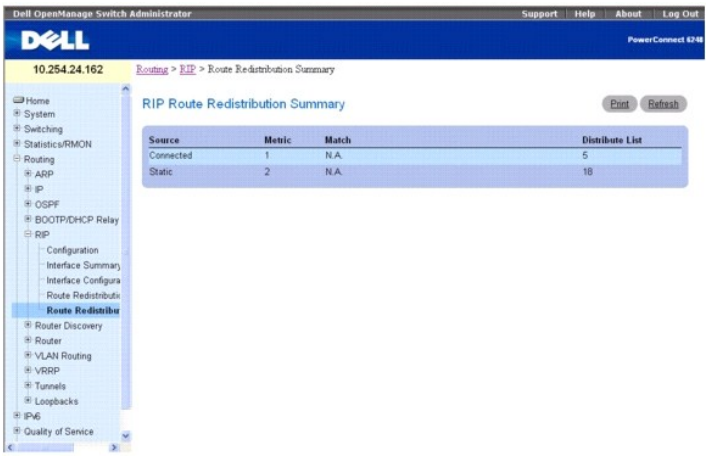
- Routing Information Protocol (RIP) Commands (RIP-Befehle)

Zusammenfassende Daten zur RIP-Routenumverteilung

Über die Seite **RIP Route Redistribution Summary** (Zusammenfassende Daten zur RIP-Routenumverteilung) können Sie Routenumverteilungskonfigurationen anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ RIP→ Route Redistribution Summary (Zusammenfassende Daten zur Routenumverteilung)**.

Abbildung 10-27. Zusammenfassende Daten zur RIP-Routenumverteilung



Die Seite **RIP Route Redistribution Summary** (Zusammenfassende Daten zur RIP-Routenumverteilung) enthält folgende Felder:

Source (Quelle) – Die Quellroute, die von RIP umverteilt werden soll.

Metric (Metrik) – Der Metrikwert der umverteilten Routen für die Quellroute. Wird kein Wert konfiguriert, wird in diesem Feld **Unconfigured** (Nicht konfiguriert) angezeigt.

Match (Treffer) – Liste der Routen, die bei Auswahl von OSPF als Quelle umverteilt werden. Diese Liste kann eine oder mehrere der folgenden Routen enthalten:

- Internal
- External 1
- External 2
- NSSA-External 1
- NSSA-External 2
- entfällt (wenn nicht OPSF)

Distribute List (Verteilungsliste) – Legt die Zugriffsliste fest, über die Routen nach Zielprotokoll umverteilt werden. Wird die Verteilungsliste nicht konfiguriert, bleibt dieses Feld leer.

Anzeigen der zusammenfassenden Daten zur RIP-Routenumverteilung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- Routing Information Protocol (RIP) Commands (RIP-Befehle)

Routersuche

Hosts verwenden das Routersuchprotokoll (Router Discovery Protocol), um betriebsfähige Router im Subnetz zu ermitteln. Es gibt zwei Meldungstypen für die Routersuche: "Router Advertisements" (Routermitteilungen) und "Router Solicitations" (Routeranfragen). Das Protokoll gibt vor, dass jeder Router in regelmäßigen Abständen die ihm zugeordneten IP-Adressen mitteilen muss. Hosts überwachen den Eingang dieser Mitteilungen und ermitteln so die IP-Adressen benachbarter Router.

Die Menüseite **Router Discovery** (Routersuche) enthält Links zu Webseiten, auf denen Daten für die Routersuche konfiguriert und angezeigt werden können. Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ Router Discovery** (Routersuche). Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

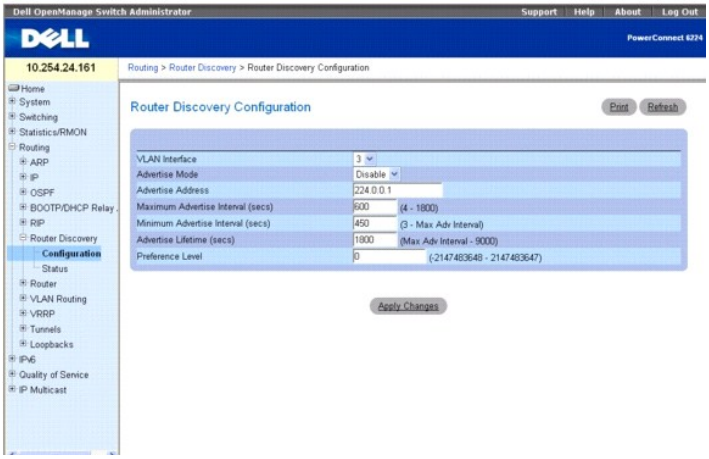
- Routersuchkonfiguration
- Routersuchstatus

Routersuchkonfiguration

Über die Seite **Router Discovery Configuration** (Routersuchkonfiguration) können Sie Routersuchparameter eingeben oder ändern.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ Router Discovery (Routersuche)→ Configuration (Konfiguration)**.

Abbildung 10-28. Routersuchkonfiguration



Die Seite **Router Discovery Configuration** (Routersuchkonfiguration) enthält folgende Felder:

VLAN Interface (VLAN-Schnittstelle) – Wählen Sie die Routerschnittstelle aus, für die Daten konfiguriert werden sollen.

Advertise Mode (Mitteilungsmodus) – Wählen Sie "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus dem Dropdown-Menü. Bei Auswahl von **Enable** (Aktivieren) werden Routermitteilungen von der ausgewählten Schnittstelle aus übertragen.

Advertise Address (Mitteilungsadresse) – Geben Sie die IP-Adresse an, über die der Router mitgeteilt werden soll.

Maximum Advertise Interval (secs) (Max. Mitteilungsintervall) – Geben Sie den maximalen Zeitabstand (in Sekunden) an, in dem Routermitteilungen von der Schnittstelle aus gesendet werden dürfen.

Minimum Advertise Interval (secs) (Mindestmitteilungsintervall) – Geben Sie den Mindestzeitabstand (in Sekunden) an, in dem Routermitteilungen von der Schnittstelle aus gesendet werden dürfen.

Advertise Lifetime (secs) (Mitteilungslebenszeit) – Geben Sie den Wert (in Sekunden) an, der im Lebenszeitfeld der Routermitteilungen verwendet werden soll, die von der Schnittstelle aus gesendet werden. Dieser Wert gibt an, wie lange die mitgeteilten Adressen vom Host maximal als gültige Routeradressen betrachtet werden.

Preference Level (Bevorzugung) – Geben Sie an, inwieweit der Router anderen Routern in demselben Subnetz als Standardrouter vorgezogen wird. Je höher die Nummer einer Adresse, desto eher wird der betreffende Router bevorzugt. Hier muss eine ganze Zahl eingegeben werden.

Konfigurieren der Routersuche

1. Öffnen Sie die Seite **Router Discovery Configuration** (Routersuchkonfiguration).
2. Wählen Sie die Routerschnittstelle aus, die konfiguriert werden soll.
3. Konfigurieren Sie in den restlichen Feldern die Daten nach Bedarf.

4. Klicken Sie auf **Apply Changes**

   Die Konfigurationsänderungen werden gespeichert, und das Gerät wird aktualisiert.

Konfigurieren der Routersuche mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

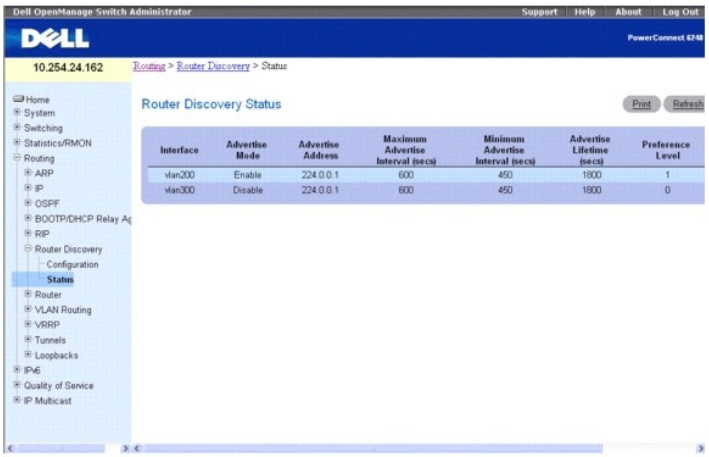
- Router Discovery Protocol Commands (Router Discovery Protocol-Befehle)

Routersuchstatus

Über die Seite **Router Discovery Status** (Routersuchstatus) können Sie die Routersuchdaten für jeden Port anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ Router Discovery (Routersuche)→ Status**.

Abbildung 10-29. Routersuchstatus



Die Seite **Router Discovery Status** (Routersuchstatus) enthält folgende Felder:

Interface (Schnittstelle) – Die Routerschnittstelle, für die Daten angezeigt werden.

Advertise Mode (Mitteilungsmodus) – Dieser Modus kann auf "Enable" (Aktivieren) oder "Disable" (Deaktivieren) gesetzt werden. **Enable** (Aktivieren) gibt an, dass die Routersuche (Routersuche) für diese Schnittstelle aktiviert ist.

Advertise Address (Mitteilungsadresse) – Die IP-Adresse an, über die der Router mitgeteilt wird.

Maximum Advertise Interval (secs) (Max. Mitteilungsintervall) – Der maximale Zeitabstand (in Sekunden), in dem Routermitteilungen von der Schnittstelle aus gesendet werden dürfen.

Minimum Advertise Interval (secs) (Mindestmitteilungsintervall) – Der Mindestzeitabstand (in Sekunden), in dem Routermitteilungen von der Schnittstelle aus gesendet werden dürfen.

Advertise Lifetime (secs) (Mitteilungslebenszeit) – Der Wert (in Sekunden), der im Lebenszeitfeld der Routermitteilungen verwendet werden soll, die von der Schnittstelle aus gesendet werden. Dieser Wert gibt an, wie lange die mitgeteilten Adressen vom Host maximal als gültige Routeradressen betrachtet werden.

Preference Level (Bevorzugung) – Gibt an, inwieweit der Router anderen Routern in demselben Subnetz als Standardrouter vorgezogen wird. Je höher die Nummer einer Adresse, desto eher wird der betreffende Router bevorzugt.

Anzeigen des Routersuchstatus mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- Router Discovery Protocol Commands (Router Discovery Protocol-Befehle)

Router

Die Menüseite **Router** enthält Links zu Webseiten, auf denen Routentabellen konfiguriert und angezeigt werden können. Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ Router**. Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

- Routentabelle

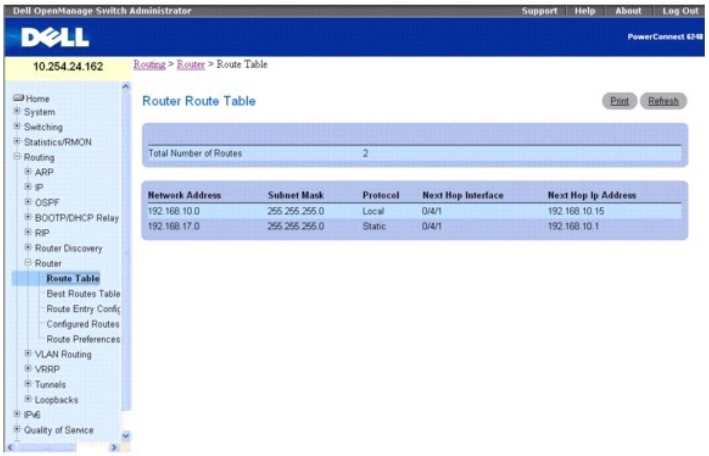
- Tabelle mit den vorteilhaftesten Routen
- Konfiguration von Routeneinträgen
- Konfigurierte Routen
- Konfiguration der Routenbevorzugung

Routentabelle

Über die Seite **Route Table** (Routentabelle) können Sie die Konfiguration der Routentabelle anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ Router→ Route Table (Routentabelle)**.

Abbildung 10-30. Router-Routentabelle



Die Seite **Router Route Table** (Router-Routentabelle) enthält folgende Felder:

Total Number of Routes (Gesamtzahl der Routen) – Die Gesamtzahl der in der Routentabelle enthaltenen Routen.

Network Address (Netzwerkadresse) – Das IP-Routenpräfix für das Ziel.

Subnet Mask (Subnetzmaske) – Wird auch als Subnetz-/Netzwerkmaske bezeichnet und stellt den Teil der IP-Schnittstellenadresse dar, der das verbundene Netzwerk identifiziert.

Protocol (Protokoll) – Dieses Feld gibt das Protokoll an, von dem die angegebene Route erstellt wurde. Möglich ist einer der folgenden Werte:

- Local (Lokal)
- Static (Statisch)
- Default (Standardwert)
- OSPF Intra
- OSPF Inter
- OSPF Type-1
- OSPF Type-2
- RIP

Next Hop Interface (Nächste Hopschnittstelle) – Routerschnittstelle für den Datenausgang, die für die Weiterleitung von Daten an das Ziel verwendet wird.

Next Hop IP Address (IP-Adresse des nächsten Hops) – IP-Adresse des Routers für den Datenausgang, die bei der Weiterleitung von Daten an den nächsten Router (sofern vorhanden) im Pfad zum Ziel verwendet werden soll. Der nächste Router ist immer einer der benachbarten Router oder die IP-Adresse der lokalen Schnittstelle für ein direkt verbundenes Netzwerk.

Anzeigen der Router-Routentabelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

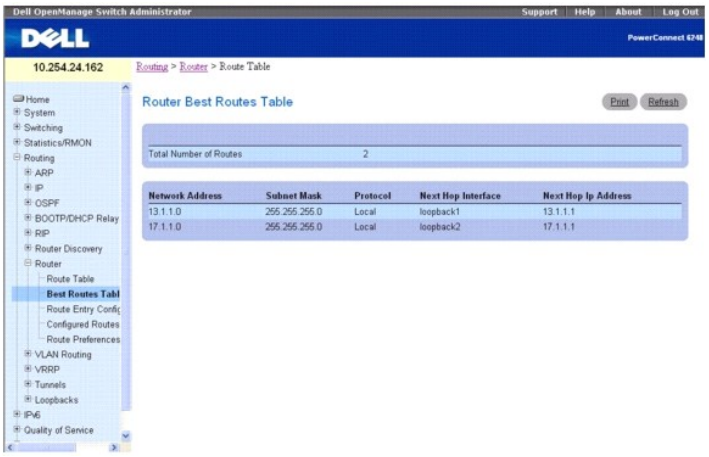
- IP Routing Commands (IP-Routingbefehle)

Tabelle mit den vorteilhaftesten Routen

Über die Seite **Router Best Routes Table** (Routertabelle mit den vorteilhaftesten Routen) können die vorteilhaftesten Routen der Routingtabelle angezeigt werden.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ Router→ Best Routes Table (Tabelle mit den vorteilhaftesten Routen)**.

Abbildung 10-31. Routertabelle mit den vorteilhaftesten Routen



Die Seite **Router Best Route Table** (Routertabelle mit den vorteilhaftesten Routen) enthält folgende Felder:

Total Number of Routes (Gesamtzahl der Routen) – Die Gesamtzahl der in der Routentabelle enthaltenen Routen.

Network Address (Netzwerkadresse) – Das IP-Routenpräfix für das Ziel.

Subnet Mask (Subnetzmaske) – Wird auch als Subnetz-/Netzwerkmaske bezeichnet und stellt den Teil der IP-Schnittstellenadresse dar, der das verbundene Netzwerk identifiziert.

Protocol (Protokoll) – Dieses Feld gibt das Protokoll an, von dem die angegebene Route erstellt wurde. Möglich ist einer der folgenden Werte:

- Local (Lokal)
- Static (Statisch)
- Default (Standardwert)
- OSPF Intra
- OSPF Inter
- OSPF Type-1
- OSPF Type-2
- RIP

Next Hop Interface (Nächste Hopschnittstelle) – Routerschnittstelle für den Datenausgang, die für die Weiterleitung von Daten an das Ziel verwendet wird.

Next Hop IP Address (IP-Adresse des nächsten Hops) – IP-Adresse des Routers für den Datenausgang, die bei der Weiterleitung von Daten an den nächsten Router (sofern vorhanden) im Pfad zum Ziel verwendet werden soll. Der nächste Router ist immer einer der benachbarten Router oder die IP-Adresse der lokalen Schnittstelle für ein direkt verbundenes Netzwerk.

Anzeigen der Tabelle mit den vorteilhaftesten Routen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

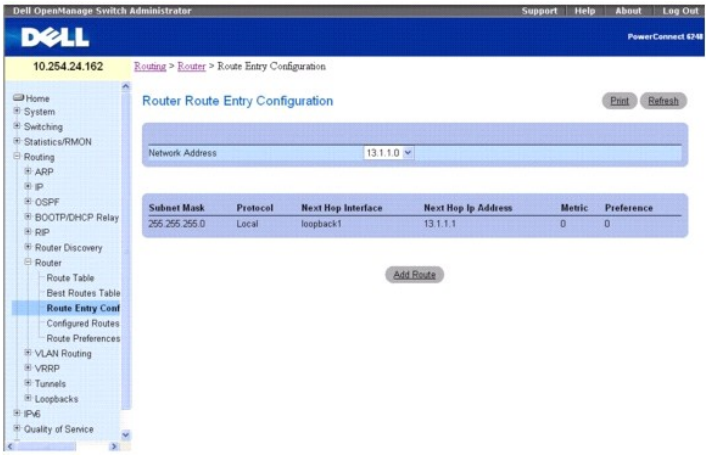
- IP Routing Commands (IP-Routingbefehle)

Konfiguration von Routeneinträgen

Über die Seite **Router Route Entry Configuration** (Konfiguration von Routerrouteneinträgen) können Sie Routerrouten konfigurieren und hinzufügen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht **Routing→ Router→ Route Entry Configuration (Konfiguration von Routeneinträgen)**.

Abbildung 10-32. Konfiguration von Routerrouteneinträgen



Die Seite **Router Route Entry Configuration** (Konfiguration von Routerrouteneinträgen) enthält folgende Felder:

Network Address (Netzwerkadresse) – Geben Sie über das Dropdown-Menü das IP-Routenpräfix für das Ziel an. Eine Route kann nur erstellt werden, wenn eine gültige Routingschnittstelle vorhanden ist und sich die IP-Adresse des nächsten Hops in demselben Netzwerk befindet wie diese Routingschnittstelle. Routingschnittstellen werden über die Seite **IP Interface Configuration** (IP-Schnittstellenkonfiguration) erstellt. Gültige IP-Adressen für den nächsten Hop können auf der Seite **Route Table** (Routentabelle) angezeigt werden.

Subnet Mask (Subnetzmaske) – Wird auch als Subnetz-/Netzwerkmaske bezeichnet und stellt den Teil der IP-Schnittstellenadresse dar, der das verbundene Netzwerk identifiziert.

Protocol (Protokoll) – Dieses Feld gibt das Protokoll an, von dem die angegebene Route erstellt wurde. Mögliche Werte:

- Local (Lokal)
- Static (Statisch)
- Default (Standardwert)
- OSPF Intra
- OSPF Inter
- OSPF Type-1
- OSPF Type-2
- RIP

Next Hop Interface (Nächste Hopschnittstelle) – Routerschnittstelle für den Datenausgang, die für die Weiterleitung von Daten an das Ziel verwendet wird.

Next Hop IP Address (IP-Adresse des nächsten Hops) – IP-Adresse des Routers für den Datenausgang, die bei der Weiterleitung von Daten an den nächsten Router (sofern vorhanden) im Pfad zum Ziel verwendet werden soll. Der nächste Router ist immer einer der benachbarten Router oder die IP-Adresse der lokalen Schnittstelle für ein direkt verbundenes Netzwerk. Bei der Erstellung einer Route muss sich die IP-Adresse des nächsten Hops in demselben Netzwerk befinden wie die Routingschnittstelle. Gültige IP-Adressen für den nächsten Hop können auf der Seite **Route Table** (Routentabelle) angezeigt werden.

Metric (Metrik) – Verwaltungsaufwand für den Pfad zum Ziel. Erfolgt keine Angabe, wird 1 als Standardwert übernommen; es sind Angaben zwischen 0 und 255 möglich. Dieses Feld ist nur bei der Erstellung einer statischen Route verfügbar.

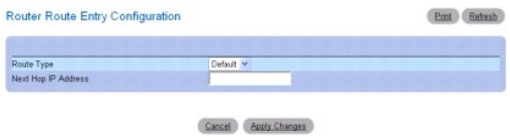
Preference (Bevorzugung) – Gibt die Bevorzugung für den nächsten konfigurierten Hop an.

Hinzufügen einer Routerroute

1. Öffnen Sie die Seite **Router Route Entry Configuration** (Konfiguration von Routerrouteneinträgen).
2. Klicken Sie auf **Add Route** (Route hinzufügen).

   Der Bildschirm wird aktualisiert, und die Seite **Router Route Entry Configuration** (Konfiguration von Routerrouteneinträgen) zeigt neue Felder an (siehe Abbildung 10-33).

Abbildung 10-33. Route hinzufügen - Standardroutentyp



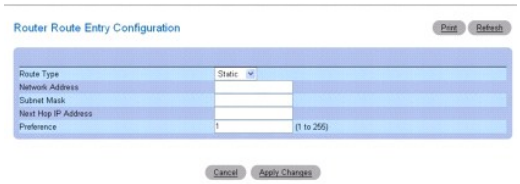
3. Fügen Sie über das Dropdown-Feld neben **Route Type** (Routentyp) eine Standardroute (**Default**) oder eine Statische Route (**Static**) hinzu.

Wenn Sie "Static" (Statisch) wählen, wird die Seite aktualisiert, und es werden neue Felder angezeigt, wie in Abbildung 10-34 zu sehen.

Default (Standard) – Geben Sie im Feld **Next Hop IP Address** (IP-Adresse des nächsten Hops) die Adresse des Standard-Gateways ein.

Static (Statisch) – Geben Sie Werte für **Network Address** (Netzwerkadresse), **Subnet Mask** (Subnetzmaske), **Next Hop IP Address** (IP-Adresse des nächsten Hops) und **Preference** (Bevorzugung) ein.

Abbildung 10-34. Konfiguration von Routeneinträgen - Statischen Routentyp hinzufügen



4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die neue Route wird hinzugefügt, und die Seite **Configured Routes** (Konfigurierte Routen) wird wieder geöffnet.

Hinzufügen einer Routerroute über den entspechenden CLI-Befehl

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

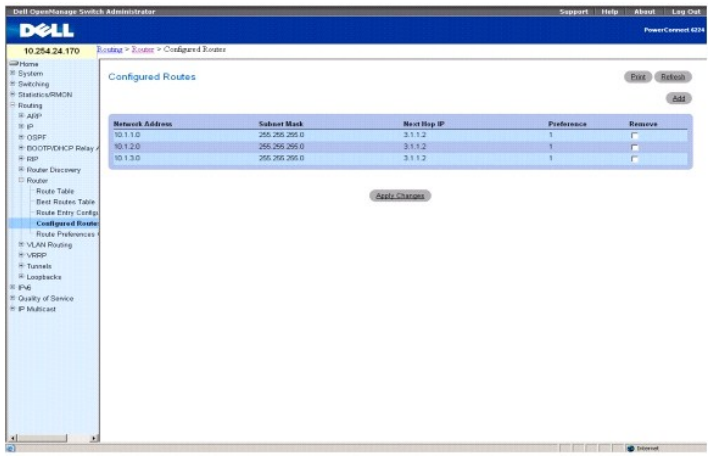
- IP Routing Commands (IP-Routingbefehle)

Konfigurierte Routen

Über die Seite **Configured Routes** (Konfigurierte Routen) können die konfigurierten Routen angezeigt werden.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ Router→ Configured Routes (Konfigurierte Routen)**.

Abbildung 10-35. Konfigurierte Routen



Die Seite **Configured Routes** (Konfigurierte Routen) enthält folgende Felder:

Network Address (Netzwerkadresse) – Das IP-Routenpräfix für das Ziel.

Subnet Mask (Subnetzmaske) – Wird auch als Subnetz-/Netzwerkmaske bezeichnet und stellt den Teil der IP-Schnittstellenadresse dar, der das verbundene Netzwerk identifiziert.

Next Hop IP (IP-Adresse des nächsten Hops) – Routerschnittstelle für den Datenausgang, die bei der Weiterleitung von Daten an das Ziel verwendet wird.

Preference (Bevorzugung) – Zeigt die für die hinzugefügten Routen konfigurierte Bevorzugung an.

Remove (Entfernen) – Über dieses Kontrollkästchen kann eine konfigurierte Route entfernt werden.

Hinzufügen einer Routerroute

1. Öffnen Sie die Seite **Configured Routes** (Konfigurierte Routen).

2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Router Route Entry Configuration** (Konfiguration von Routerrouteneinträgen) wird angezeigt, wie in Abbildung 10-33 zu sehen.

3. Fügen Sie über das Dropdown-Feld neben **Route Type** (Routentyp) eine **Standardroute** oder eine **Statische Route** hinzu.

   Default (Standard) – Geben Sie im Feld **Next Hop IP Address** (IP-Adresse des nächsten Hops) die Adresse des Standard-Gateways ein. Abbildung 10-33 zeigt die Felder, die angezeigt werden, wenn die Option **Route Type** den Standardwert aufweist.

   Static (Statisch) – Geben Sie Werte für **Network Address** (Netzwerkadresse), **Subnet Mask** (Subnetzmaske), **Next Hop IP Address** (IP-Adresse des nächsten Hops) und **Preference** (Bevorzugung) ein. Abbildung 10-34 zeigt die Felder, die angezeigt werden, wenn die Option **Route Type** den Wert "Static" (Statisch) aufweist.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die neue Route wird hinzugefügt, und die Seite **Configured Routes** (Konfigurierte Routen) wird wieder geöffnet.

Anzeigen von konfigurierten Routen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- IP Routing Commands (IP-Routingbefehle)

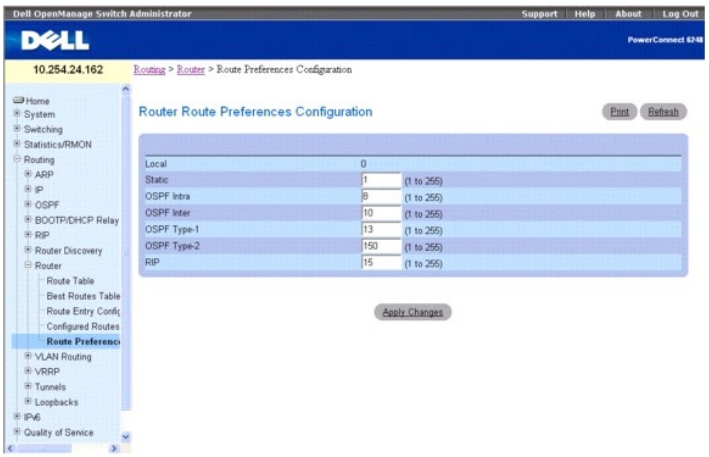
Konfiguration der Routenbevorzugung

Über die Seite **Router Route Preferences Configuration** (Konfiguration der Routerroutenbevorzugung) können Sie die Standardbevorzugung für die einzelnen Protokolle konfigurieren (z. B. 60 für statische Routen). Hier handelt es sich um wahlfreie Werte zwischen 1 und 255, die unabhängig von der Routenmetrik sind. Die meisten Protokolle ermitteln den kürzesten bekannten Pfad unabhängig von allen anderen Protokollen über eine Routenmetrik.

Die vorteilhafteste Route zu einem Ziel wird über die Auswahl der Route mit dem niedrigsten Bevorzugungswert ausgewählt. Gibt es mehrere Routen zu einem Ziel, wird die bevorzugte Route anhand des Bevorzugungswertes ausgewählt. Gibt es auch dann noch die Wahl zwischen mehreren Routen, wird die Route mit dem vorteilhaftesten Metrikwert ausgewählt. Um Probleme im Fall von nicht vergleichbaren Metriken zu verhindern (so entsprechen sich beispielsweise RIP- und OSPF-Metriken nicht direkt), müssen Sie für die einzelnen Protokolle andere Bevorzugungswerte konfigurieren.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ Router→ Route Preferences Configuration (Konfiguration der Routenbevorzugung)**.

Abbildung 10-36. Konfiguration von Routerroutenbevorzugungen



Die Seite **Router Route Preferences Configuration** (Konfiguration von Routerroutenbevorzugungen) enthält folgende Felder:

Local (Lokal) – Dieses Feld zeigt den Bevorzugungswert für lokale Routen an.

Static (Statisch) – Der Bevorzugungswert im Router für statische Routen. Der Standardwert ist 1, mögliche Werte sind 1 bis 255.

OSPF Intra – Der routenübergreifende OSPF-Bevorzugungswert im Router. Der Standardwert ist 8, mögliche Werte sind 1 bis 255. Die OSPF-Spezifikation (RFC 2328) gibt vor, dass über OSPF mitgeteilte Routen in der folgenden Reihenfolge bevorzugt werden müssen: intra < inter < Type-1 < Type-2.

OSPF Inter – Der routenübergreifende OSPF-Bevorzugungswert im Router. Der Standardwert ist 10, mögliche Werte sind 1 bis 255. Die OSPF-Spezifikation (RFC 2328) gibt vor, dass über OSPF mitgeteilte Routen in der folgenden Reihenfolge bevorzugt werden müssen: intra < inter < Type-1 < Type-2.

OSPF Type-1 – Der OSPF-Bevorzugungswert Type-1 für Routen im Router. Der Standardwert ist 13, mögliche Werte sind 1 bis 255. Die OSPF-Spezifikation (RFC 2328) gibt vor, dass über OSPF mitgeteilte Routen in der folgenden Reihenfolge bevorzugt werden müssen: intra < inter < Type-1 < Type-2.

OSPF Type-2 – Der OSPF-Bevorzugungswert Type-2 für Routen im Router. Der Standardwert ist 150, mögliche Werte sind 1 bis 255. Die OSPF-Spezifikation (RFC 2328) gibt vor, dass über OSPF mitgeteilte Routen in der folgenden Reihenfolge bevorzugt werden müssen: intra < inter < Type-1 < Type-2.

RIP – Der Bevorzugungswert im Router für RIP-Routen. Der Standardwert ist 15, mögliche Werte sind 1 bis 255.

Konfigurieren der Routenbevorzugung

1. Öffnen Sie die Seite **Route Preferences Configuration** (Konfiguration der Routenbevorzugung).
2. Definieren Sie auf dieser Seite die entsprechenden Felder
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Routenbevorzugung wird konfiguriert und das Gerät entsprechend aktualisiert.

Konfiguration der Routenbevorzugung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- OSPF Commands (OSPF-Befehle)

VLAN-Routing

Sie können die Software der Serie 6200 mit einigen VLANS konfigurieren, die Routing unterstützen. Außerdem können Sie die Software so konfigurieren, dass Daten an ein VLAN so gehandhabt werden, als würde es sich bei dem VLAN um einen Routerport handeln.

Ist ein Port nicht für Routing, sondern für Bridging aktiviert (Standardeinstellung), erfolgt für eingehende Pakete die normale Bridge-Verarbeitung, die dann einem VLAN zugeordnet werden. Die MAC-Adresstabelle wird anhand der MAC-DA (MAC-Zieladresse) und der VLAN-ID durchsucht. Ist "Routing"für das VLAN aktiviert und ist die MAC-DA eines eingehenden Unicast-Pakets mit der der internen Bridge-Routerschnittstelle identisch, wird das Paket weitergeleitet. Eingehende Multicast-Pakete werden an alle Ports im VLAN und an die interne Bridge-Routerschnittstelle weitergeleitet, wenn sie in einem VLAN, das für Routing aktiviert ist, empfangen wurden.

Ein Port kann für mehrere VLANs konfiguriert werden, daher kann VLAN-Routing für alle VLANs am Port oder nur für einen Teil der VLANs aktiviert werden. Über VLAN-Routing ist es möglich, dass sich in ein und demselben Subnetz mehrere physikalische Ports befinden können. VLAN-Routing kann auch verwendet werden, wenn sich ein VLAN über mehrere physikalische Netzwerke erstreckt oder wenn eine zusätzliche Segmentierung oder Sicherheitsfunktionen erforderlich sind. In diesem Abschnitt wird die Konfiguration der Software der 6200-Reihe für die Unterstützung von VLAN-Routing erläutert. Ein Port kann als VLAN-Port oder als Routerport konfiguriert werden, nicht aber für beides. Dagegen kann ein VLAN-Port Teil eines VLAN sein, dass selbst als Routerport agiert.

Die Menüseite **VLAN-Routing** enthält einen Link zu einer Webseite, auf der Parameter und Daten zum VLAN-Routing angezeigt werden. Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ VLAN Routing** (VLAN-Routing). Folgende Webseite ist über diese Menüseite zugänglich:

- Zusammenfassende Daten zu VLAN-Routing

Zusammenfassende Daten zu VLAN-Routing

Über die Seite **VLAN Routing Summary** (Zusammenfassende Daten zu VLAN-Routing) können Sie Informationen zu den im System konfigurierten VLAN-Routingschnittstellen anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ VLAN Routing→ Summary (Übersicht)**.

Abbildung 10-37. Zusammenfassende Daten zum VLAN-Routing

Die Seite **VLAN Routing Summary** (Zusammenfassende Daten zum VLAN-Routing) enthält folgende Felder:

VLAN ID (VLAN-ID) – Die ID des VLAN, dessen Daten in der aktuellen Tabellenzeile angezeigt werden.

MAC Address (MAC-Adresse) – Die der VLAN-Routingschnittstelle zugeordnete MAC-Adresse.

IP Address (IP-Adresse) – Die für die VLAN-Routingschnittstelle konfigurierte IP-Adresse. Wird bei der Erstellung eines VLAN keine IP-Adresse konfiguriert, wird auf dieser Seite die Standard-IP-Adresse 0.0.0.0 angezeigt. Sie können die IP-Adresse unter **IP→ Interface Configuration (Schnittstellenkonfiguration)** konfigurieren.

Subnet Mask (Subnetzmaske) – Die für die VLAN-Routingschnittstelle konfigurierte Subnetzmaske. Wird die VLAN-Routingschnittstelle zum ersten Mal konfiguriert, ist dieser Wert "0.0.0.0"; er muss auf der Seite **IP Interface Configuration** (IP-Schnittstellenkonfiguration) angegeben werden.

Anzeigen der zusammenfassenden Daten zum VLAN-Routing mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in den folgendem Kapiteln:

- IP Addressing Commands (IP-Adressierungsbefehle)
- Virtual LAN Routing Commands (VLAN-Routingbefehle)

VRRP

Das virtuelle Routerredundanzprotokoll (VRRP) ist für den Einsatz bei Ausfällen des Standardrouters gedacht, indem es ein Schema für die dynamische Auswahl eines Backup-Routers bereitstellt. Ziel war es, so genannte "schwarze Löcher" zu verhindern, die bei Ausfall des Standard-Gateway-Routers auftreten; sämtliche an diesen Router geleiteten Daten gehen verloren, bis der Ausfall erkannt wird. Für Standardrouten ist zwar die statische Konfiguration gängig, doch werden diese damit zu Komponenten, deren Ausfall das gesamte System zum Erliegen bringen kann. VRRP unterstützt das Konzept eines "virtuellen Routers", dem eine oder mehrere IP-Adressen zugeordnet sind, die als Standard-Gateways dienen. Bei Ausfall des VRRP-Routers, der diese IP-Adressen steuert (der so genannte Master), übernimmt ein Backup-VRRP-Router diese IP-Adressen und die Weiterleitung.

Die Menüseite **VRRP** enthält Links zu Webseiten, auf denen Parameter und Daten konfiguriert und angezeigt werden können. Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ VRRP**. Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

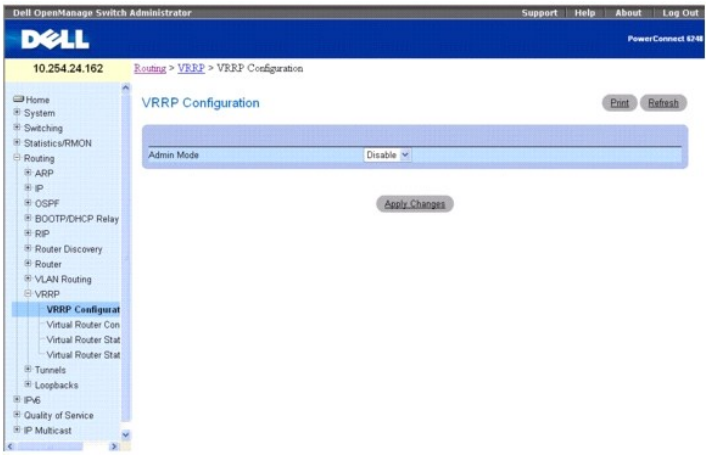
- VRRP-Konfiguration
- Konfiguration eines virtuellen Routers
- Status eines virtuellen Routers
- Statistische Daten eines virtuellen Routers

VRRP-Konfiguration

Über die Seite **VRRP Configuration** (VRRP-Konfiguration) können Sie den Verwaltungsstatus eines virtuellen Routers aktivieren oder deaktivieren.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ VRRP→ VRRP Configuration (VRRP-Konfiguration)**.

Abbildung 10-38. VRRP-Konfiguration



Die Seite **VRRP Configuration** (VRRP-Konfiguration) enthält folgende Felder:

Admin Mode (Verwaltungsmodus) – Setzt den Verwaltungsstatus von VRRP im Router auf "aktiv" oder "inaktiv". Wählen Sie "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus dem Dropdown-Menü. Die Standardeinstellung ist **Disable** (Deaktivieren).

Ändern des VRRP-Status mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

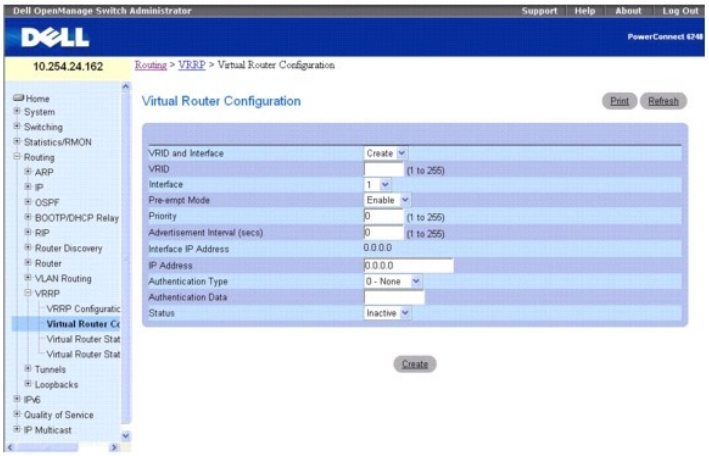
- Virtual Router Redundancy Protocol Commands (VRRP-Befehle)

Konfiguration eines virtuellen Routers

Über die Seite **Virtual Router Configuration** (Konfiguration eines virtuellen Routers) können Sie einen neuen virtuellen Router erstellen bzw. einen vorhandenen konfigurieren.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ VRRP→ Virtual Router Configuration (Konfiguration eines virtuellen Routers)**.

Abbildung 10-39. Konfiguration eines virtuellen Routers



Die Seite **Virtual Router Configuration** (Konfiguration eines virtuellen Routers) enthält folgende Felder:

VRID and Interface (VRID und Schnittstelle) – Wählen Sie im Dropdown-Menü "Create" (Erstellen) aus, um einen neuen virtuellen Router zu konfigurieren, oder wählen Sie einen der bereits vorhandenen Router aus, die nach Schnittstellennummer und VRID aufgeführt sind.

VRID – Dieses Feld kann nur bei der Erstellung eines neuen virtuellen Routers konfiguriert werden; in diesem Fall müssen Sie hier eine VRID zwischen 1 und 255 eingeben.

Interface (Schnittstelle) – Dieses Feld kann nur bei der Erstellung eines neuen virtuellen Routers konfiguriert werden; in diesem Fall müssen Sie im Dropdown-Menü die Schnittstelle für den neuen virtuellen Router auswählen.

Pre-empt Mode (Verdrängungsmodus) – Wählen Sie "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus dem Dropdown-Menü. Bei Auswahl von **Enable** (Aktivieren) wird der Master-Router von einem Backup-Router verdrängt, wenn dessen Priorität höher ist als die des virtuellen Master-Routers und der Master nicht Besitzer der IP-Adresse des virtuellen Routers ist. Der Standardwert ist **Enable** (Aktivieren).

Priority (Priorität) – Geben Sie die Priorität an, über die der VRRP-Router den virtuellen Master-Router auswählen soll. Ist die virtuelle IP-Adresse dieselbe wie die IP-Adresse der Schnittstelle, wird die Priorität unabhängig von Ihrer Eingabe auf 255 gesetzt. Wird eine Priorität von 255 eingegeben und virtuelle IP-Adresse und IP-Adresse der Schnittstelle sind nicht identisch, wird automatisch der Standardwert 100 gesetzt.

Advertisement Interval (secs) (Mitteilungsintervall) – Geben Sie den Zeitraum (in Sekunden) zwischen der Übertragung der Mitteilungspakete durch diesen virtuellen Router ein. Hier muss eine Zahl zwischen 1 und 255 eingegeben werden; der Standardwert ist 1 Sekunde.

Interface IP Address (IP-Adresse der Schnittstelle) – Gibt die IP-Adresse der ausgewählten Schnittstelle an.

IP Address (IP-Adresse) – Geben Sie die IP-Adresse des virtuellen Routers ein. Die Standardeinstellung ist 0.0.0.0; dieser Wert muss geändert werden, bevor Sie auf **Create** (Erstellen) klicken.

Authentication Type (Authentifizierungstyp) – Wählen Sie im Dropdown-Menü den Authentifizierungstyp für den virtuellen Router aus. Der Standardwert ist **None** (Keiner). Sie haben folgende Möglichkeiten:

- **0-None** (0-Keiner) – Es erfolgt keine Authentifizierung.
- **1-Simple** (1-Einfach) – Die Authentifizierung erfolgt über ein Textkennwort.

Authentication Data (Authentifizierungsdaten) – Bei Auswahl der einfachen Authentifizierung müssen Sie hier das Kennwort eingeben.

Status – Wählen Sie im Dropdown-Menü "aktiv" oder "inaktiv" aus, um den Betrieb des virtuellen Routers zu starten oder zu stoppen. Der Standardwert ist "aktiv".

Soll eine sekundäre VRRP-Adresse konfiguriert werden, müssen Sie für den virtuellen Router zunächst eine, nämlich die primäre IP-Adresse konfigurieren. Anschließend können Sie der Schnittstelle mehrere sekundäre Adressen hinzufügen.

Erstellen eines neuen virtuellen Routers

1. Öffnen Sie die Seite **Virtual Router Configuration** (Konfiguration eines virtuellen Routers).
2. Wählen Sie im Dropdown-Menü "VRID and Interface" (VRID und Schnittstelle) die Option **Create** (Erstellen) aus.
3. Geben Sie die VRID und die Schnittstelle für den neuen virtuellen Router an.
4. Definieren Sie die übrigen Felder je nach Bedarf.
5. Klicken Sie auf **Create** (Erstellen).

   Der neue virtuelle Router wird gespeichert und das Gerät aktualisiert.

Konfigurieren eines virtuellen Routers

1. Öffnen Sie die Seite **Virtual Router Configuration** (Konfiguration eines virtuellen Routers).
2. Wählen Sie die VRID und die Schnittstelle des virtuellen Routers aus, der konfiguriert werden soll.
3. Ändern Sie die Felder nach Bedarf.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Konfiguration wird gespeichert und das Gerät aktualisiert.

Konfigurieren eines virtuellen Routers mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

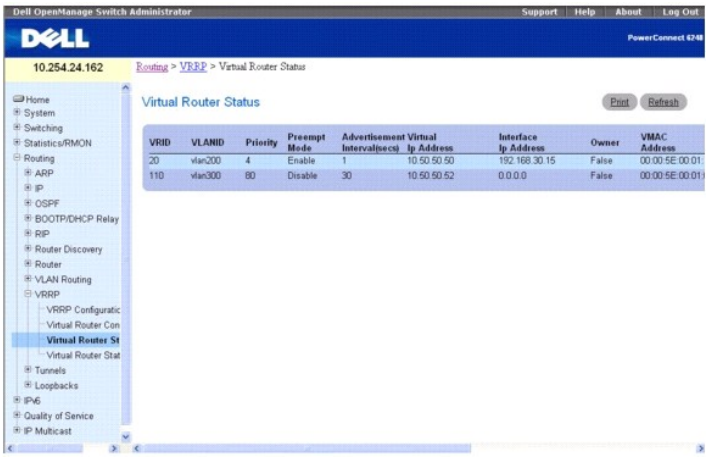
- Virtual Router Redundancy Protocol Commands (VRRP-Befehle)

Status eines virtuellen Routers

Auf der Seite Virtual Router Status (Status eines virtuellen Routers) können Sie den Status eines virtuellen Routers anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ VRRP→Virtual Router Status** (Status eines virtuellen Routers).

Abbildung 10-40. Status eines virtuellen Routers



Die Seite **Router Router Status** (Status eines virtuellen Routers) enthält folgende Felder:

VRID – Die ID des virtuellen Routers.

VLANID (VLAN-ID) - Die der VRID zugeordnete Schnittstelle.

Priority (Priorität) – Die Priorität, über die der VRRP-Router den virtuellen Master-Router auswählt.

Pre-empt Mode (Verdrängungsmodus)

- **Enable** (Aktivieren) – Ist der virtuelle Router ein Backup-Router, verdrängt er den Master-Router, wenn seine Priorität höher ist als die des virtuellen

Master-Routers und der Master nicht Besitzer der IP-Adresse des virtuellen Routers ist.

- **Disable** (Deaktivieren) – Ist der virtuelle Router ein Backup-Router, verdrängt er den Master-Router auch dann nicht, wenn er eine höhere Priorität hat als dieser.

Advertisement Interval (secs) (Mitteilungsintervall) – Der Zeitraum (in Sekunden) zwischen der Übertragung der Mitteilungspakete durch diesen virtuellen Router.

Virtual IP Address (Virtuelle IP-Adresse) – Die dem virtuellen Router zugeordnete IP-Adresse.

Interface IP Address (IP-Adresse der Schnittstelle) – Die tatsächliche IP-Adresse der vom virtuellen Router verwendeten Schnittstelle.

Owner (Besitzer) – Wird auf "True" gesetzt, wenn virtuelle IP-Adresse und Schnittstellen-IP-Adresse identisch sind; andernfalls wird hier "False" gesetzt. Wird für diesen Parameter **True** angegeben, ist der virtuelle Router Besitzer der virtuellen IP-Adresse und wird immer als Master-Router gewählt, sofern er aktiv ist.

VMAC Address (VMAC-Adresse) – Die virtuelle MAC-Adresse des virtuellen Routers; hier handelt es sich um eine organisationsweit eindeutige 24-Bit-Kennung; dabei bezeichnet die 16-Bit-Konstante den VRRP-Adressblock und die 8-Bit-VRID. Die virtuelle MAC-Adresse ist 00:00:5e:00:01:XX; dabei steht XX für die VRID.

Auth Type (Authentifizierungstyp) – Der Authentifizierungstyp, der für den virtuellen Router verwendet wird.

- None (Keiner) – Gibt an, dass kein Authentifizierungstyp verwendet wird.
- Simple (Einfach) – Gibt an, dass es sich bei dem Authentifizierungstyp um ein einfaches Textkennwort handelt.

State (Status) – Der aktuelle Status des virtuellen Routers:

- Initialize (Initialisieren)
- Master
- Backup

State (Status) – Der aktuelle Status des virtuellen Routers:

- Inactive (Inaktiv)
- Active (Aktiv)

Secondary IP Address (Sekundäre IP-Adresse) – Eine für den primären VRRP konfigurierte sekundäre VRRP-Adresse.

Anzeigen des Status eines virtuellen Routers mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

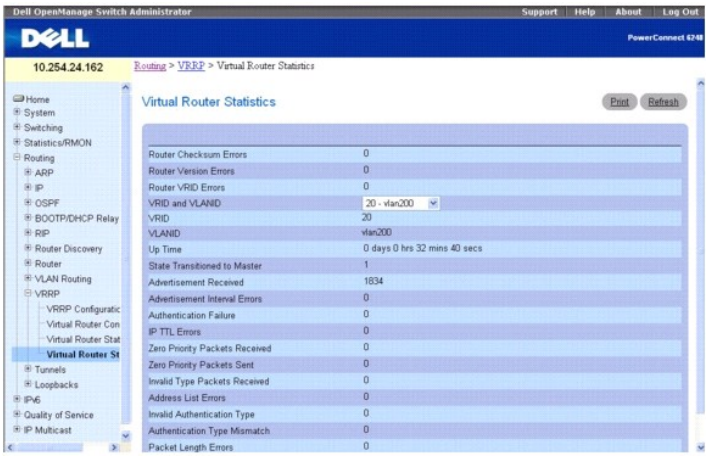
- Virtual Router Redundancy Protocol Commands (VRRP-Befehle)

Statistische Daten eines virtuellen Routers

Über die Seite **Virtual Router Statistics** (Statistische Daten eines virtuellen Routers) können Sie die Statistikdaten für einen bestimmten virtuellen Router anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ VRRP→ Virtual Router Statistics (Statistische Daten eines virtuellen Routers)**.

Abbildung 10-41. Statistische Daten eines virtuellen Routers



Die Seite **Virtual Router Statistics** (Statistische Daten eines virtuellen Routers) enthält folgende Felder. Viele davon werden nur angezeigt, wenn eine gültige VRRP-Konfiguration vorhanden ist:

Router Checksum Errors (Prüfsummenfehler des Routers) – Die Anzahl aller VRRP-Pakete, die mit einem ungültigen VRRP-Prüfsummenwert empfangen

wurden.

Router Version Errors (Versionsfehler des Routers) – Die Anzahl aller VRRP-Pakete, die mit einer unbekannten oder nicht unterstützten Versionsnummer empfangen wurden.

Router VRID Errors (VRID-Fehler des Routers) – Die Anzahl aller VRRP-Pakete, die mit einer ungültigen VRID für diesen virtuellen Router empfangen wurden.

VRID and VLAN ID (VRID und VLAN-ID) – Wählen Sie den vorhandenen virtuellen Router aus (wird nach Schnittstellen und VRID aufgeführt), zu dem statische Daten angezeigt werden sollen.

VRID – Die VRID des ausgewählten virtuellen Routers.

VLAN ID (VLAN-ID) – Die Schnittstelle des ausgewählten virtuellen Routers.

Up Time (Betriebszeit) – Die Zeit (in Tagen, Stunden, Minuten und Sekunden), die seit der Initialisierung des virtuellen Routers vergangen ist.

State Transitioned to Master (Statusübergang zu Master) – Gibt an, wie oft der Status des virtuellen Routers zu 'Master' gewechselt ist.

Advertisement Received (Empfangene Mitteilungen) – Gibt die Gesamtzahl der VRRP-Mitteilungen an, die von diesem virtuellen Router empfangen wurden.

Advertisement Interval Errors (Falsche Mitteilungsintervalle) – Gibt die Gesamtzahl der empfangenen VRRP-Mitteilungspakete an, deren Mitteilungsintervall sich von dem unterschied, das für den lokalen virtuellen Router konfiguriert wurde.

Authentication Failure (Authentifizierungsfehler) – Die Gesamtzahl der empfangenen VRRP-Pakete, für die die Authentifizierung nicht erfolgreich war.

IP TTL Errors (IP-TTL-Fehler) – Die Gesamtzahl der vom virtuellen Router empfangenen VRRP-Pakete, deren IP-TTL (IP-Lebenszeit) nicht dem Wert 255 entsprach.

Zero Priority Packets Received (Empfangene Pakete mit Priorität Null) – Die Gesamtzahl der vom virtuellen Router empfangenen VRRP-Pakete, deren Priorität 0 war.

Zero Priority Packets Sent (Gesendete Pakete mit Priorität Null) – Die Gesamtzahl der vom virtuellen Router gesendeten VRRP-Pakete, deren Priorität 0 war.

Invalid Type Packets Received (Empfangene Pakete mit ungültigem Typ) – Die Anzahl der vom virtuellen Router empfangenen VRRP-Pakete, bei denen das Feld "Typ" einen ungültigen Wert enthielt.

Address List Errors (Adresslistenfehler) – Die Gesamtzahl der empfangenen Pakete, für die die Adressliste nicht der lokal konfigurierten Liste für den virtuellen Router entspricht.

Invalid Authentication Type (Ungültiger Authentifizierungstyp) – Die Gesamtzahl der empfangenen Pakete mit einem unbekannten Authentifizierungstyp.

Authentication Type Mismatch (Unterschiedliche Authentifizierungstypen) – Die Gesamtzahl der empfangenen Pakete mit einem Authentifizierungstyp, der sich von der lokal konfigurierten Authentifizierungsmethode unterscheidet.

Packet Length Errors (Paketlängenfehler) – Die Gesamtzahl der empfangenen Pakete, deren Länge unter der des VRRP-Headers lag.

Anzeigen der statistischen Daten eines virtuellen Routers

1. Öffnen Sie die Seite **Virtual Router Statistics** (Statistische Daten eines virtuellen Routers).
2. Wählen Sie über das Feld **VRID** und **VLANID** den virtuellen Router aus, für den statistische Daten angezeigt werden sollen. Diese Informationen werden nur angezeigt, wenn eine gültige VRRP-Konfiguration vorliegt.

Anzeigen der statistischen Daten eines virtuellen Routers mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- Virtual Router Redundancy Protocol Commands (VRRP-Befehle)

Tunnel

Die 6200-Reihe unterstützt das Erstellen, Löschen und Verwalten von Tunnelschnittstellen. Dabei handelt es sich um dynamische Schnittstellen, die über die Benutzerkonfiguration erstellt und gelöscht werden.

Es gibt zwei Tunnelkategorien, die den Übergang von IPv4- zu IPv6-Netzwerken ermöglichen: konfigurierte und automatische Tunnel. Konfigurierte Tunnel werden explizit mit einem Ziel- oder Endpunkttunnel konfiguriert. Automatische Tunnel dagegen ermitteln den Tunnelendpunkt über die Zieladresse der Pakete, die über den Tunnel geleitet werden.

Die 6200-Reihe unterstützt Punkt-zu-Punkt-Tunnel. Punkt-zu-Punkt-Schnittstellen ermöglichen rein schnittstellenbasiertes Routing (es muss keine explizite Adresse für den nächsten Hop angegeben werden) und die Definition nicht nummerierter Schnittstellen.

Die Menüseite **Tunnels** (Tunnel) enthält Links zu Webseiten, auf denen Tunnelparameter und -daten konfiguriert und angezeigt werden können. Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ Tunnels** (Tunnel). Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

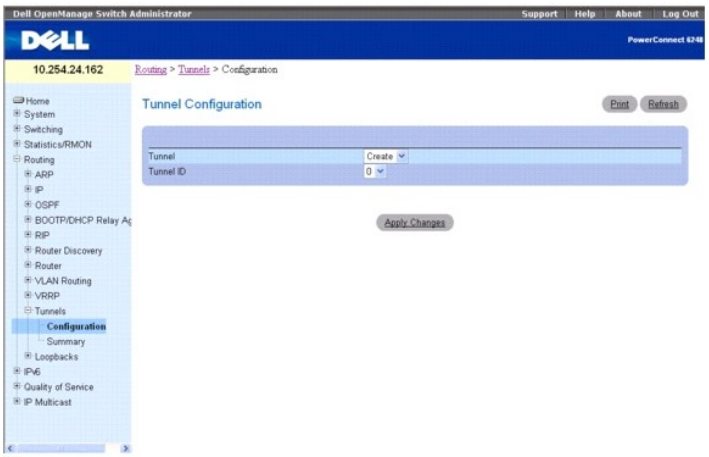
- Tunnelkonfiguration
- Zusammenfassende Daten zu Tunneln

Tunnelkonfiguration

Über die Seite **Tunnels Configuration** (Tunnelkonfiguration) kann ein Tunnel erstellt, konfiguriert oder gelöscht werden.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing**→ **Tunnels (Tunnel)**→ **Configuration (Konfiguration)**.

Abbildung 10-42. Tunnelkonfiguration



Die Seite **Tunnels Configuration** (Tunnelkonfiguration) enthält folgende Felder:

Tunnel – Wählen Sie im Dropdown-Menü aus der Liste der aktuell konfigurierten Tunnel-IDs den gewünschten Tunnel aus. Wenn die maximal mögliche Anzahl an Tunnelschnittstellen noch nicht erstellt wurde, können Sie auch **Create** (Erstellen) auswählen.

Tunnel ID (Tunnel-ID) – Bei Auswahl von "Create" (Erstellen) im Dropdown-Menü "Tunnel" wird hier die Liste der verfügbaren Tunnel-IDs angezeigt. Sie müssen eine Tunnel-ID für den neuen Tunnel auswählen und auf **Apply Changes** (Änderungen übernehmen) klicken, damit die restlichen Felder auf der Seite angezeigt werden.

Mode (Modus) – Wählen Sie den Tunnelmodus aus. Nur der Modus **IPV6-in-IPV4** wird unterstützt.

Link Local Only Mode (Nur Link-Local) – Aktivieren Sie IPv6 für diese Schnittstelle unter Verwendung der Link-Local-Adresse. Diese Option kann nur vor Angabe einer expliziten IPv6-Adresse konfiguriert werden.

IPv6 Address (IPv6-Adresse) – Wählen Sie eine IPv6-Adresse für die ausgewählte Tunnelschnittstelle aus. Wenn die maximal mögliche Anzahl an Adressen noch nicht konfiguriert wurde, können Sie auch **Add** (Hinzufügen) auswählen.

IPv6 Address (IPv6-Adresse) – Bei Auswahl von "Add" (Hinzufügen) im Feld "IPv6 Address" (IPv6-Adresse) wird dieses Eingabefeld für die IPv6-Adresse angezeigt. Die Adresse muss im Format Präfix/Länge eingegeben werden.

Sie können auch eine EUI-64 (erweiterte eindeutige 64-Bit-Kennung) angeben.

Source (Quelle) – Wählen Sie die gewünschte Quelle, IPv4-Addresse oder Schnittstelle, aus. Bei Auswahl von **Address** (Adresse) muss die Quelladresse für diesen Tunnel in der Schreibweise mit Trennzeichen eingegeben werden. Bei Auswahl von **Interface** (Schnittstelle) muss die Quellschnittstelle für diesen Tunnel ausgewählt werden. Die Adresse, die der ausgewählten Schnittstelle zugeordnet ist, wird als Quelladresse verwendet.

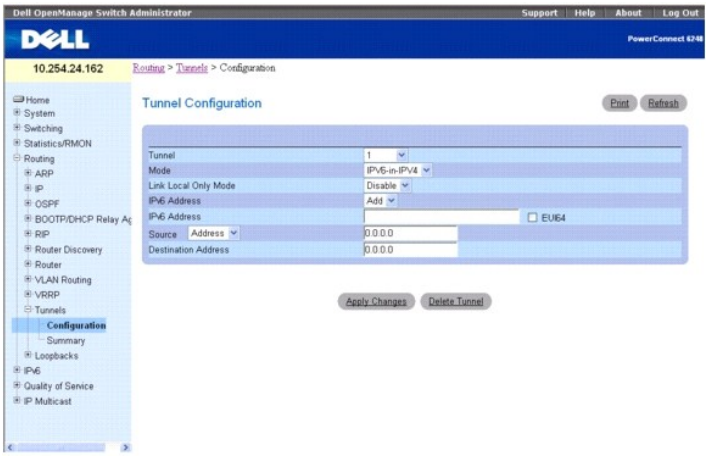
Destination Address (Zieladresse) – Die IPv4-Zieladresse für diesen Tunnel; sie wird in der Schreibweise mit Trennzeichen angegeben.

Erstellen eines neuen Tunnels

1. Öffnen Sie die Seite **Tunnels Configuration** (Tunnelkonfiguration).
2. Wählen Sie im Dropdown-Menü **Tunnel** die Option **Create** (Erstellen).
3. Geben Sie im Feld **Tunnel ID** (Tunnel-ID) eine ID an.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Das Feld **Tunnel ID** (Tunnel-ID) wird entfernt, und die restlichen Tunnelfelder werden angezeigt.

Abbildung 10-43. Tunnelkonfiguration - Eintrag



5. Konfigurieren Sie die Felder nach Bedarf.
6. Geben Sie in den restlichen Feldern die gewünschten Werte ein.
7. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der neue Tunnel wird gespeichert und das Gerät aktualisiert.

Ändern eines vorhandenen Tunnels

1. Öffnen Sie die Seite **Tunnels Configuration** (Tunnelkonfiguration).
2. Geben Sie im Dropdown-Menü **Tunnel** den Tunnel an, der geändert werden soll.
3. Ändern Sie nach Bedarf die Werte in den restlichen Feldern.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die neue Konfiguration wird gespeichert und das Gerät aktualisiert.

Entfernen eines Tunnels

1. Öffnen Sie die Seite **Tunnels Configuration** (Tunnelkonfiguration).
2. Geben Sie im Dropdown-Menü **Tunnel** den Tunnel an, der gelöscht werden soll.
3. Klicken Sie auf **Delete Tunnel** (Tunnel löschen).

   Der Tunnel wird gelöscht und das Gerät aktualisiert.

Konfigurieren eines Tunnels mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

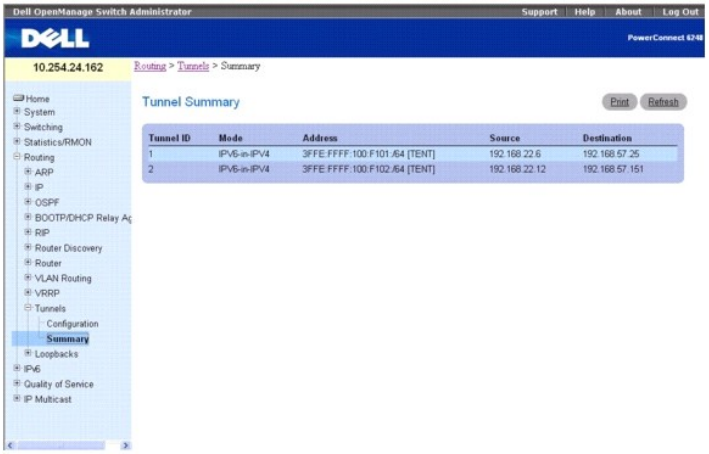
- Tunnel Interface Commands (Tunnelschnittstellenbefehle)

Zusammenfassende Daten zu Tunneln

Über die Seite **Tunnels Summary** (Zusammenfassende Daten zu Tunneln) können zusammenfassende Informationen zu konfigurierten Tunneln angezeigt werden.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ Tunnels→ Summary (Zusammenfassende Daten)**.

Abbildung 10-44. Zusammenfassende Daten zu Tunneln



Die Seite **Tunnels Summary** (Zusammenfassende Daten zu Tunneln) enthält folgende Felder:

Tunnel ID – Die Tunnel-ID.

Mode (Modus) – Der Tunnelmodus.

Address (Adresse) – Die IPv6-Adresse(n) des Tunnels.

Source (Quelle) – Die Quelladresse des Tunnels. Wurde eine Schnittstelle konfiguriert, werden sowohl die Schnittstelle als auch die Adresse angezeigt. Wurde für die Quellschnittstelle keine Adresse konfiguriert, wird **unconfigured** (nicht konfiguriert) anstelle der Adresse angezeigt.

Destination (Ziel) – Die Zieladresse des Tunnels.

Anzeigen der zusammenfassenden Daten zu Tunneln mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- Tunnel Interface Commands (Tunnelschnittstellenbefehle)

Loopback-Schnittstellen

Die 6200-Reihe unterstützt das Erstellen, Löschen und Verwalten von Loopback-Schnittstellen. Dabei handelt es sich um dynamische Schnittstellen, die über die Benutzerkonfiguration erstellt und gelöscht werden. Die 6200-Reihe unterstützt mehrere Loopback-Schnittstellen

Eine Loopback-Schnittstelle muss immer betriebsfähig sein. So ermöglicht sie die Konfiguration stabiler IP-Adressen auf dem Gerät, auf das andere Switches verweisen. Diese Schnittstelle stellt die Quelladresse für gesendete Pakete bereit und kann lokale Pakete und Remote-Pakete empfangen. Sie wird typischerweise von Routingprotokollen verwendet.

Das Verhalten von Loopback-Schnittstellen unterscheidet sich von dem des Netzwerkports des Switching-Systems. Insbesondere gibt es in einer Loopback-Schnittstelle keine Nachbarn. Es handelt sich vielmehr um ein Pseudogerät für die Zuordnung lokaler Adressen, so dass eine Kommunikation mit dem Router über diese Adresse möglich ist, die immer erreichbar ist und Daten von sämtlichen vorhandenen aktiven Schnittstellen empfangen kann. Da die Loopback-Schnittstelle auch von einem Remote-Client aus erreicht werden kann, ist über ihre Adresse die Kommunikation mit dem Router über eine Reihe von Diensten möglich, wie beispielsweise Telnet und ssh. In Bezug auf die Verarbeitung eingehender Pakete verhält sich die Adresse einer Loopback-Schnittstelle daher genauso wie die lokalen Adressen des Routers.

Die Menüseite **Loopbacks** (Loopback-Schnittstellen) enthält Links zu Webseiten, auf denen Loopback-Parameter und -Daten konfiguriert und angezeigt werden können. Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ Loopbacks (Loopback-Schnittstellen)**. Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

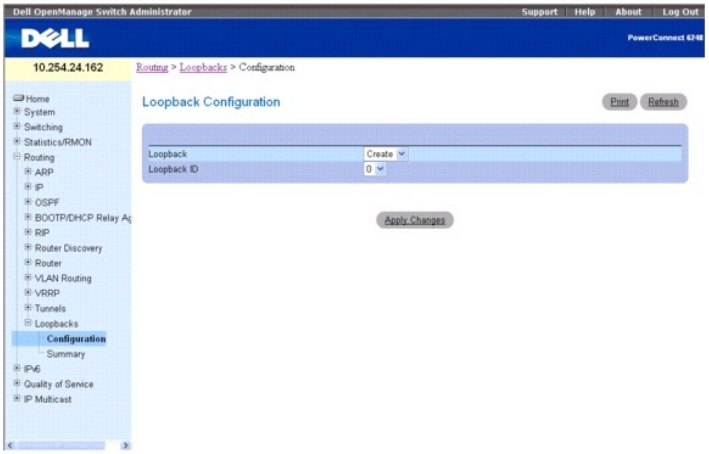
- Konfiguration von Loopback-Schnittstellen
- Zusammenfassende Daten zu Loopback-Schnittstellen

Konfiguration von Loopback-Schnittstellen

Über die Seite **Loopbacks Configuration** (Konfiguration von Loopback-Schnittstellen) können Loopback-Schnittstellen erstellt, konfiguriert oder entfernt werden. Sie können für eine Loopback-Schnittstelle außerdem eine sekundäre Adresse einrichten oder löschen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ Loopbacks (Loopback-Schnittstellen)→ Configuration (Konfiguration)**.

Abbildung 10-45. Konfiguration von Loopback-Schnittstellen



Die Seite **Loopbacks Configuration** (Konfiguration von Loopback-Schnittstellen) enthält folgende Felder:

Loopback (Loopback-Schnittstelle) – Wählen Sie im Dropdown-Menü aus der Liste der aktuell konfigurierten Loopback-Schnittstellen die gewünschten Schnittstelle aus. Wenn die maximal mögliche Anzahl an Loopback-Schnittstellen noch nicht erstellt wurde, können Sie auch **Create** (Erstellen) auswählen.

Loopback ID (Loopback-ID) – Bei Auswahl von "Create" im Feld "Loopback" (Loopback-Schnittstelle) wird eine Liste der verfügbaren Loopback-IDs angezeigt.

Protocol (Protokoll) – Wählen Sie IPv4 oder IPv6 aus, um die entsprechenden Attribute für die Loopback-Schnittstelle zu konfigurieren. Welche Felder auf der Seite angezeigt werden, hängt von dem ausgewählten Protokoll ab.

Link Local Only Mode (Nur Link-Local) – Aktivieren Sie IPv6 für diese Schnittstelle unter Verwendung der Link-Local-Adresse. Diese Option wird nur angezeigt, wenn IPv6 als Protokoll ausgewählt wurde, und kann nur vor der Angabe einer expliziten IPv6-Adresse konfiguriert werden.

IPv6 Address (IPv6-Adresse) – Liste mit den für die ausgewählte Loopback-Schnittstelle konfigurierten IPv6-Adressen. Wenn die maximal mögliche Anzahl an Adressen noch nicht konfiguriert wurde, können Sie auch **Add** (Hinzufügen) auswählen. Diese Option wird nur angezeigt, wenn IPv6 als Protokoll ausgewählt wurde.

IPv6 Address (IPv6-Adresse) – Bei Auswahl von "Add" (Hinzufügen) im Feld "IPv6 Adresse" (IPv6-Adresse) wird dieses Eingabefeld für die IPv6-Adresse angezeigt. Geben Sie die Adresse im Format Präfix/Länge ein. Diese Option wird nur angezeigt, wenn IPv6 als Protokoll ausgewählt wurde.

EU164 – Sie können auch eine EUI-64 (erweiterte eindeutige 64-Bit-Kennung) angeben. Diese Option wird nur angezeigt, wenn IPv6 als Protokoll ausgewählt wurde.

IPv4 Address (IPv4-Adresse) – Die primäre IPv4-Zieladresse für diese Schnittstelle; sie wird in der Schreibweise mit Trennzeichen angegeben. Diese Option wird nur angezeigt, wenn IPv4 als Protokoll ausgewählt wurde.

IPv4 Subnet Mask (IPv4-Subnetzmaske) – Die primäre IPv4-Subnetzmaske für diese Schnittstelle; sie wird in der Schreibweise mit Trennzeichen angegeben. Diese Option wird nur angezeigt, wenn IPv4 als Protokoll ausgewählt wurde.

Die folgenden Felder werden bei der Konfiguration einer primären Adresse angezeigt. Sie können mehrere sekundäre Adressen konfigurieren.

Secondary Address (Sekundäre Adresse) – Wählen Sie im Dropdown-Menü eine konfigurierte IPv4-Adresse als sekundäre Adresse für die ausgewählte Loopback-Schnittstelle aus. Im Feld **Secondary IP Address** (Sekundäre IP-Adresse) kann eine neue Adresse eingegeben werden, indem Sie hier **Add Secondary IP Address** (Sekundäre IP-Adresse hinzufügen) auswählen (sofern noch nicht die maximal mögliche Anzahl an sekundären Adressen konfiguriert wurde). Sekundäre Adressen können erst nach der Konfiguration einer primären Adresse hinzugefügt werden.

Secondary IP Address (Sekundäre IP-Adresse) – Die sekundäre IP-Adresse für diese Schnittstelle; sie wird in der Schreibweise mit Trennzeichen angegeben. Dieses Eingabefeld wird nur bei Auswahl von **Add Secondary** (Sekundäre Adresse hinzufügen) angezeigt.

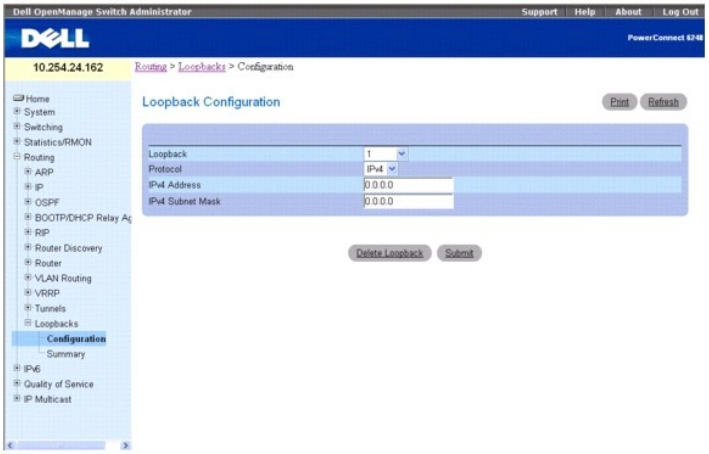
Secondary Subnet Mask (Sekundäre Subnetzmaske) – Die sekundäre Subnetzmaske für diese Schnittstelle; sie wird in der Schreibweise mit Trennzeichen angegeben. Dieses Eingabefeld wird nur bei Auswahl von **Add Secondary** (Sekundäre Adresse hinzufügen) angezeigt.

Erstellen einer neuen Loopback-Schnittstelle (IPv4)

1. Öffnen Sie die Seite **Loopbacks Configuration** (Konfiguration von Loopback-Schnittstellen).
2. Wählen Sie im Dropdown-Menü **Loopback** die Option **Create** (Erstellen).
3. Geben Sie im Feld **Loopback ID** (Loopback-ID) eine ID an.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Das Feld **Loopback ID** (Loopback-ID) wird entfernt, und die restlichen Loopback-Felder werden angezeigt.

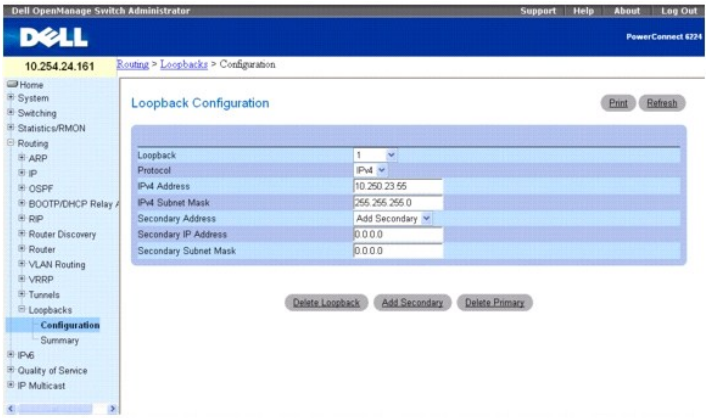
Abbildung 10-46. Konfiguration von Loopback-Schnittstellen - IPv4-Eintrag



5. Geben Sie **IPv4** im Feld **Protocol** (Protokoll) an.
6. Geben Sie in den restlichen Feldern die gewünschten Werte ein.
7. Klicken Sie auf **Submit** (Übergeben).

   Die neue Loopback-Schnittstelle wird gespeichert, und die Webseite wird wieder angezeigt; sie enthält nun die Felder für die Konfiguration einer sekundären Adresse.

Abbildung 10-47. Konfiguration von Loopback-Schnittstellen - Sekundäre Adresse hinzufügen



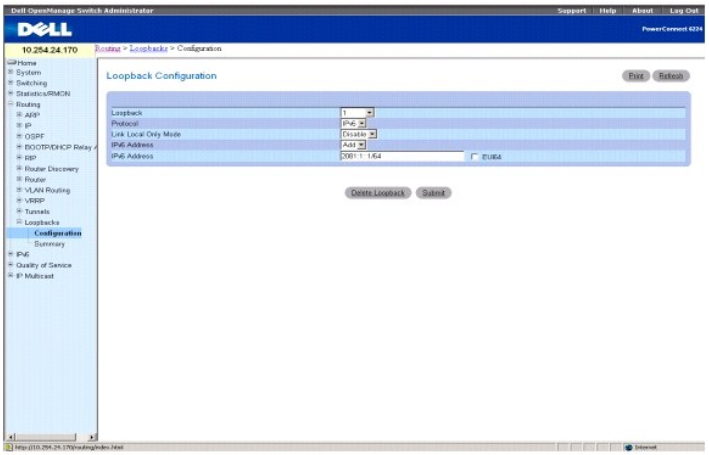
8. Füllen Sie die Felder **Secondary Address** (Sekundäre Adresse), **Secondary IP Address** (Sekundäre IP-Adresse) und **Secondary Subnet Mask** (Sekundäre Subnetzmaske) aus.
9. Klicken Sie auf **Add Secondary** (Sekundäre Adresse hinzufügen). Die sekundäre Adresse wird gespeichert, und die Webseite wird wieder angezeigt; sie enthält nun die primären und sekundären Loopback-Adressen.

Erstellen einer neuen Loopback-Schnittstelle (IPv6)

1. Öffnen Sie die Seite **Loopbacks Configuration** (Konfiguration von Loopback-Schnittstellen).
2. Wählen Sie im Dropdown-Menü **Loopback** die Option **Create** (Erstellen).
3. Geben Sie im Feld **Loopback ID** (Loopback-ID) eine ID an.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das Feld **Loopback ID** (Loopback-ID) wird entfernt, und die restlichen Loopback-Felder werden angezeigt.

Abbildung 10-48. Konfiguration von Loopback-Schnittstellen - IPv6-Eintrag



5. Wählen Sie im Dropdown-Menü unter **Protocol** (Protokoll) die Option **IPv6** aus.
6. Fügen Sie die **IPv6 Address** (IPv6-Adresse) hinzu.
7. Geben Sie in den restlichen Feldern die gewünschten Werte ein.
8. Klicken Sie auf **Submit** (Übergeben).

   Die neue Loopback-Schnittstelle wird gespeichert und das Gerät aktualisiert.

Konfigurieren einer vorhandenen Looooback-Schnittstelle

1. Öffnen Sie die Seite **Loopbacks Configuration** (Konfiguration von Loopback-Schnittstellen).
2. Geben Sie im Dropdown-Menü **Loopback** die Loopback-Schnittstelle an, die konfiguriert werden soll.
3. Ändern Sie nach Bedarf die Werte in den restlichen Feldern.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die neue Konfiguration wird gespeichert und das Gerät aktualisiert.

Entfernen einer Loopback-Schnittstelle

1. Öffnen Sie die Seite **Loopbacks Configuration** (Konfiguration von Loopback-Schnittstellen).
2. Geben Sie im Dropdown-Menü **Loopback** die Loopback-Schnittstelle an, die gelöscht werden soll.
3. Klicken Sie auf **Delete Loopback** (Loopback-Schnittstelle löschen).

   Die Loopback-Schnittstelle wird gelöscht und das Gerät aktualisiert.

Entfernen einer sekundären Adresse

1. Öffnen Sie die Seite **Loopbacks Configuration** (Konfiguration von Loopback-Schnittstellen).
2. Geben Sie die betreffende Loopback-Schnittstelle an.
3. Geben Sie die sekundäre Adresse an, die entfernt werden soll.
4. Klicken Sie auf **Delete Selected Secondary** (Ausgewählte sekundäre Adresse löschen).

   Die sekundäre Adresse wird gelöscht und das Gerät aktualisiert.

Konfigurieren eine Loopback-Schnittstelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in den folgendem Kapiteln:

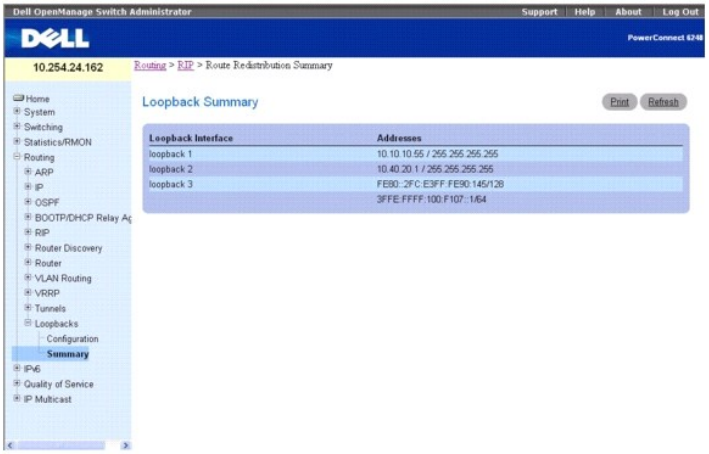
- Loopback Interface Commands (Befehle für Loopback-Schnittstellen)
- IP Addressing Commands (IP-Adressierungsbefehle)
- IPv6 Routing Commands (IPv6-Routingbefehle)

Zusammenfassende Daten zu Loopback-Schnittstellen

Über die Seite **Loopbacks Summary** (Zusammenfassende Daten zu Loopback-Schnittstellen) können zusammenfassende Informationen zu konfigurierten Loopback-Schnittstellen angezeigt werden.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Routing→ Loopbacks (Loopback-Schnittstellen)→ Summary (Zusammenfassende Daten)**.

Abbildung 10-49. Zusammenfassende Daten zu Loopback-Schnittstellen



Die Seite **Loopbacks Summary** (Zusammenfassende Daten zu Loopback-Schnittstellen) enthält folgende Felder:

Loopback Interface (Loopback-Schnittstelle) – Die ID der konfigurierten Loopback-Schnittstelle.

Addresses (Adressen) – Eine Liste der für die Loopback-Schnittstelle konfigurierten Adressen.

Anzeigen der zusammenfassenden Daten zu Loopback-Schnittstellen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- Loopback Interface Commands (Befehle für Loopback-Schnittstellen)

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

IPv6-Konfiguration

Benutzerhandbuch für die Dell™ PowerConnect™ 6200-Reihe

- Globale Konfiguration
- Schnittstellenkonfiguration
- Zusammenfassende Daten zu Schnittstellen
- IPv6-Statistik
- IPv6-Nachbarschaftstabelle
- DHCPv6
- OSPFv3
- IPv6-Routen

IPv6 ist die nächste Generation des Internetprotokolls. Mit 128-Bit-Adressen bietet IPv6 einen ungleich größeren Adressraum als IPv4 mit einer Adresslänge von 32 Bit; dadurch ist keine Netzwerkadressumsetzung (NAT) mehr erforderlich, mit der in IPv4-Netzwerken die Zahl der global eindeutigen IP-Adressen reduziert werden kann, die in einem Netzwerk erforderlich sind. Durch die Zusammenfassung von Adressen kann mit IPv6 die globale Routingtabelle erheblich verkleinert werden. Außerdem ist eine mehr integrierte Sicherheit möglich, und die Netzwerkkonfiguration wird vereinfacht, gestaltet sich aber gleichzeitig wesentlich flexibler.

In der 6200-Reihe können IPv6 und IPv4 zusammen eingesetzt werden. Wie bei IPv4 kann auch IPv6-Routing für Loopback- und VLAN-Schnittstellen aktiviert werden. Dabei kann jede Layer 3-Routingschnittstelle für IPv4 und/oder IPv6 verwendet werden. Für IP-Protokolle in Layer 3 (z. B. UDP und TCP) ergibt sich bei Verwendung von IPv6 keine Änderung. Daher wird für die Übertragung von IPv4 und IPv6 ein einziger CPU-Stack verwendet; eine einzige Sockelschnittstelle ermöglicht den Zugriff auf beide Protokolle. Routingprotokolle können Routen für eine IP-Version oder beide IP-Versionen berechnen.

Die Menüseite **IPv6** enthält Links zu den folgenden Merkmalen:

- Globale Konfiguration
- Schnittstellenkonfiguration
- Zusammenfassende Daten zu Schnittstellen
- **IPv6-Statistics** (IPv6-Statistik)
- IPv6-Nachbarschaftstabelle
- DHCPv6
- OSPFv3
- IPv6-Routen

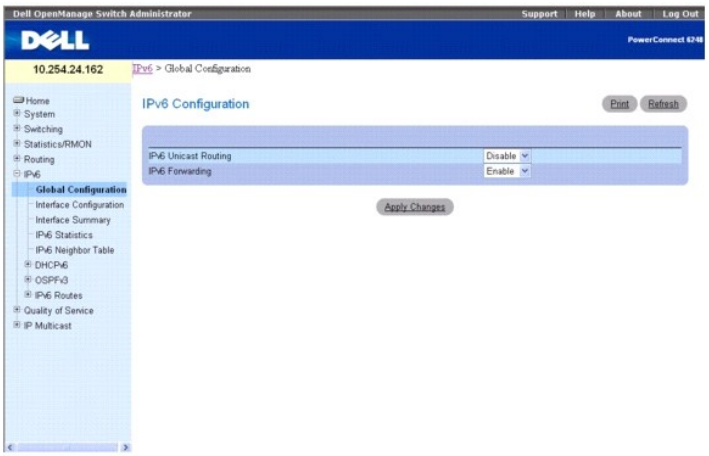
ANMERKUNG: CLI-Befehle sind nicht für alle IPv6-Seiten verfügbar.

Globale Konfiguration

Über die Seite **Global Configuration** (Globale Konfiguration) kann die IPv6-Weiterleitung für den Router und die Weiterleitung von IPv6-Unicast-Datagrammen aktiviert werden.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ Global Configuration (Globale Konfiguration)**.

Abbildung 11-1. Globale IPv6-Konfiguration



Die Seite **IPv6 Global Configuration** (IPv6 - Globale Konfiguration) enthält folgende Felder:

IPv6 Unicast Routing (IPv6-Unicast-Routing) – Sie können IPv6-Unicast-Routing für den Router global aktivieren oder deaktivieren. Die Standardeinstellung ist **Disable** (Deaktivieren).

IPv6 Forwarding (IPv6-Weiterleitung) – Sie können die Weiterleitung von IPv6-Frame im Router aktivieren oder deaktivieren. Der Standardwert ist **Enable** (Aktivieren).

Konfigurieren von IPv6-Parametern

1. Öffnen Sie die Seite **IPv6 Global Configuration** (IPv6 - Globale Konfiguration).
2. Aktivieren bzw. deaktivieren Sie Unicast-Routing über das Dropdown-Menü .
3. Aktivieren bzw. deaktivieren Sie über das Dropdown-Menü die Weiterleitung von IPv6-Frames.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Einstellungen werden gespeichert, und das Gerät wird aktualisiert.

Konfigurieren von IPv6 mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

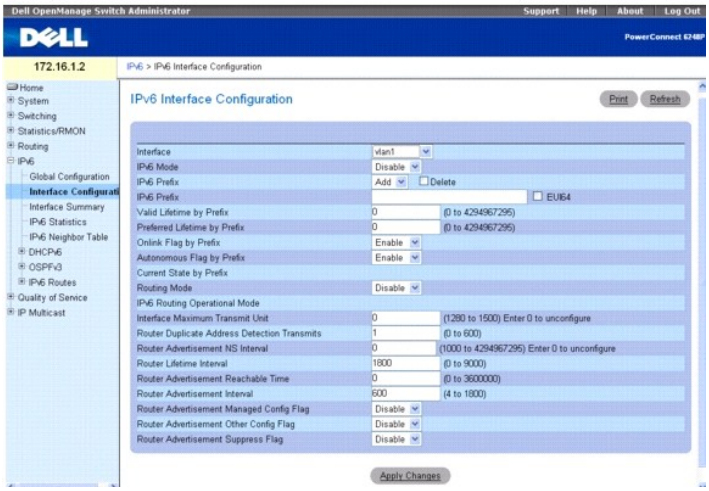
- IPV6 Routing Commands (IPv6-Routingbefehle)

Schnittstellenkonfiguration

Über die Seite **Interface Configuration** (Schnittstellenkonfiguration) können Sie die IPv6-Schnittstellenparameter konfigurieren.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ Interface Configuration (Schnittstellenkonfiguration)**.

Abbildung 11-2. IPv6-Schnittstellenkonfiguration



Die Seite **IPv6 Interface Configuration** (IPv6-Schnittstellenkonfiguration) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie die Schnittstelle aus, die konfiguriert werden soll. Bei einer Änderung der Auswahl wird der Bildschirm aktualisiert, und alle Felder werden mit den Werten für den neu ausgewählten Port gefüllt. Nur die routingfähigen Schnittstellen und Tunnel werden angezeigt.

IPv6 Mode (IPv6-Modus) – Ist der IPv6-Modus aktiviert, ist für die Schnittstelle ein IPv6-Betrieb ohne globale Adresse möglich. In diesem Fall wird eine EUI-64-basierte Link-Local-Adresse verwendet. Für den IPv6-Modus stehen die folgenden beiden Optionen zur Auswahl: **Enable** (Aktivieren) und **Disable** (Deaktivieren). Der Standardwert ist **Disable** (Deaktivieren).

IPv6 Prefix (IPv6-Präfix) – Wählen Sie "Add" oder "Delete" aus, um ein IPv6-Präfix für diese Schnittstelle hinzuzufügen bzw. zu löschen. Wird ein Präfix hinzugefügt, müssen Sie dieses Präfix im Feld **IPv6 Prefix** (IPv6-Präfix) angeben. Über **Delete** (Löschen) wird ein angezeigtes IPv6-Präfix gelöscht.

IPv6 Prefix (IPv6-Präfix) – Gibt das IPv6-Präfix mit Präfixlänge für eine Schnittstelle an. Bei Änderung der Auswahl wird der Bildschirm aktualisiert, und die gültige Lebensdauer, das On-Link-Flag und das Autonomous-Flag werden für die ausgewählte IPv6-Adresse aktualisiert.

EUI-64 – Bei Auswahl dieser Option wird das 64-Bit-Unicast-Präfix angegeben.

Valid Lifetime by Prefix (Gültige Lebenszeit nach Präfix) – Der Wert (in Sekunden), der im Feld **Valid Lifetime** (Gültige Lebenszeit) der Option **Prefix Information** (Präfix-Informationen) in einer Routermitteilung eingegeben wird. Das Präfix gilt zur Ermittlung der On-Link-Ziele für die festgelegte Zeitdauer. Hosts, die mittels nicht statusbezogener Adress-Autokonfiguration eine Adresse aus diesem Präfix generieren, können sie für die hier angegebene Zeitdauer benutzen. Eine autokonfigurierte Adresse, die die bevorzugte Lebenszeit überschritten, aber die gültige Lebenszeit noch nicht erreicht hat, erhält den Status "deprecated address"(Nicht erwünschte Adresse). Gemäß RFC 2462 ist eine Adresse mit dem Status "deprecated" einer Schnittstelle zugewiesen, deren Nutzung möglichst vermieden werden soll, jedoch nicht verboten ist. Adressen mit dem Status "deprecated" sollten nicht mehr als Quelladresse bei neuen Kommunikationsvorgängen verwendet werden. Pakete, von oder an diese(n) Adressen werden jedoch wie vorgesehen zugestellt. Eine Adresse mit dem Status "deprecated" kann als Quelladresse bei der Kommunikation verwendet werden, wenn der Umstieg auf eine bevorzugte Adresse zu Problemen mit einer bestimmten Aktivität des oberen Layers (z. B. einer vorhandenen TCP-Verbindung) führt." Der gültige Wertebereich reicht von 0 bis 4.294.967.295 Sekunden.

Preferred Lifetime by Prefix (Bevorzugte Lebenszeit nach Präfix) – Der Wert (in Sekunden), der im Feld **Preferred Lifetime** (Bevorzugte Lebenszeit) der Option **Prefix Information** (Präfix-Informationen) in einer Routermitteilung eingegeben wird. Adressen, die mittels nicht statusbezogener Adress-Autokonfiguration aus einem Präfix generiert wurden, haben für die hier angegebene Zeitdauer den Status "preferred" (bevorzugt). Gemäß RFC 2462 ist eine Adresse mit dem Status "preferred" (bevorzugt) "eine Adresse, die einer Schnittstelle zugewiesen ist, deren Verwendung durch Protokolle der oberen Layer nicht eingeschränkt ist. Bevorzugte Adressen können als Quell- (oder Ziel-)adressen für Pakete dienen, die von der bzw. an die Schnittstelle gesendet werden." Der Wertebereich reicht von 0 bis 4.294.967.295 Sekunden.

Onlink Flag by Prefix (On-Link-Flag nach Präfix) – Gibt das ausgewählte Präfix an, über das On-Link-Ziele ermittelt werden. Der Standardwert ist **Enable** (Aktivieren). Für dieses Flag stehen die folgenden beiden Optionen zur Auswahl: **Enable** (Aktivieren) und **Disable** (Deaktivieren).

Autonomous Flag by Prefix (Autonomous-Flag nach Präfix) – Gibt das ausgewählte Präfix an, das für eine autonome Adresskonfiguration verwendet werden kann. Der Standardwert ist **Disable** (Deaktivieren). Für dieses Flag stehen die folgenden beiden Optionen zur Auswahl: **Enable** (Aktivieren) und **Disable** (Deaktivieren).

Current State by Prefix (Aktueller Status nach Präfix) – Der Betriebsstatus der Schnittstelle für das ausgewählte IPv6-Präfix.

Routing Mode (Routingmodus) – Gibt den Routingmodus einer Schnittstelle an. Für diesen Modus stehen die folgenden beiden Optionen zur Auswahl: **Enable** (Aktivieren) und **Disable** (Deaktivieren). Der Standardwert ist **Disable** (Deaktivieren).

IPv6 Routing Operational Mode (Betriebsmodus für IPv6-Routing) – Gibt den Betriebsmodus einer Schnittstelle an. Der Standardwert ist **Disable** (Deaktivieren).

Interface Maximum Transmit Unit (MTU für Schnittstelle) – Gibt die maximale Größe der Übertragungseinheiten für eine Schnittstelle an. Bei Angabe von 0 ist diese Schnittstelle nicht für Routing aktiviert. Wenn Routing aktiviert ist, darf der Wert 0 nicht gesetzt werden. Die zulässigen Werte für MTU liegen zwischen 1280 und 1500.

Router Duplicate Address Detection Transmits (Anzahl Router-DAD-Übertragungen) – Gibt die Anzahl von DAD-Übertragungen für eine Schnittstelle an. Der Wert für DAD-Übertragungen muss zwischen 0 und 600 liegen.

Router Advertisement NS Interval (NS-Intervall in Routermitteilung) – Gibt den Wert im Feld für das Intervall zwischen Nachbaranfragen (Neighbor Solicitation) in der von der Schnittstelle gesendeten Routermitteilung (Router Advertisement) an. Der Wert 0 weist darauf hin, dass für diesen Router kein Intervall angegeben ist. Für dieses Intervall kann ein Wert zwischen 1000 und 4294967295 angegeben werden.

Router Lifetime Interval (Routerlebenszeit) – Gibt den Wert im Feld für die Routerlebenszeit in der von der Schnittstelle gesendeten Routermitteilung an. Dieser Wert muss größer oder gleich dem maximalen Mitteilungsintervall sein. Der Wert 0 gibt an, dass der Router nicht als Standardrouter verwendet wird. Die Routerlebenszeit liegt zwischen 0 und 9000.

Router Advertisement Reachable Time (Verfügbarkeit in Routermitteilung) – Gibt an, wie lange ein Nachbar nach Bestätigung seiner Verfügbarkeit durch die Nachbarsuche in der Routermitteilung als verfügbar gilt. Der Verfügbarkeitszeitraum liegt zwischen 0 und 3600000.

Router Advertisement Interval (Routermitteilungs-Intervall) – Gibt die maximale Zeitspanne an, die zwischen zwei von der Schnittstelle gesendeten Routermitteilungen liegen kann. Der Standardwert ist 600, mögliche Werte sind 4 bis 1800.

Router Advertisement Managed Config Flag (Flag für verwaltete Konfiguration in Routermitteilung) – Gibt das Flag für die verwaltete Adresskonfiguration in der Routermitteilung an. Wird das Bit auf **True** gesetzt, verwendet der Endknoten DHCPv6. Wird es auf **False** gesetzt, verwenden die Endknoten die automatische Adresskonfiguration. Der Standardwert für dieses Flag ist **Disable** (Deaktivieren).

Router Advertisement Other Config Flag (Flag für weitere Konfiguration in Routermitteilung) – Gibt das Flag für die weitere statusbezogene Adresskonfiguration in der Routermitteilung an. Der Standardwert für dieses Flag ist **Disable** (Deaktivieren).

Router Advertisement Suppress Flag (Flag für Unterdrückung von Routermitteilungen) – Gibt an, dass Routermitteilungen für die Schnittstelle unterdrückt werden. Der Standardwert für dieses Flag ist **Disable** (Deaktivieren).

Konfigurieren der IPv6-Schnittstelle

1. Öffnen Sie die Seite **IPv6 Interface Configuration** (IPv6-Schnittstellenkonfiguration).
2. Ändern Sie die Felder je nach Bedarf.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Änderungen an der IPv6-Schnittstelle werden gespeichert, und das Gerät wird aktualisiert.

Konfigurieren der IPv6-Schnittstelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- IPV6 Routing Commands (IPv6-Routingbefehle)

Zusammenfassende Daten zu Schnittstellen

Über die Seite **Interface Summary** (Zusammenfassende Daten zu Schnittstellen) können Sie die Einstellungen für alle IPv6-Schnittstellen anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ Interface Summary (Zusammenfassende Daten zu Schnittstellen)**.

Abbildung 11-3. Zusammenfassende Daten zu IPv6-Schnittstellen

Die Seite **IPv6 Interface Summary** (Zusammenfassende Daten zu IPv6-Schnittstellen) enthält folgende Felder:

Interface (Schnittstelle) – Gibt die Schnittstelle an, deren Einstellungen in der aktuellen Tabellenzeile angezeigt werden.

Routing Mode (Routingmodus) – Gibt den Routingmodus der Schnittstelle an.

Admin Mode (Verwaltungsmodus) – Gibt den Verwaltungsmodus der Schnittstelle an.

Operational Mode (Betriebsmodus) – Gibt den Betriebsmodus der Schnittstelle an.

IPv6 Prefix/PrefixLength (IPv6-Präfix/Präfixlänge) – Gibt die konfigurierten IPv6-Adressen der Schnittstelle an.

State (Status) – Gibt an, ob die Schnittstelle aktiv ist oder nicht.

Anzeigen der zusammenfassenden Daten zu IPv6-Schnittstellen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

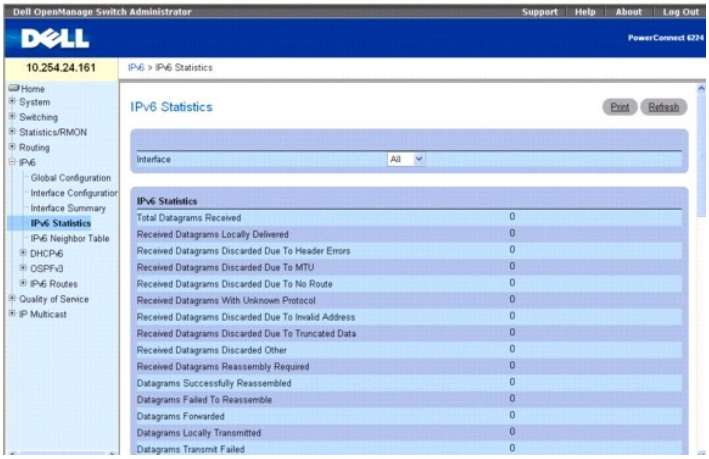
- IPV6 Routing Commands (IPv6-Routingbefehle)

IPv6-Statistik

Über die Seite **IPv6 Statistics** (IPv6-Statistik) können Sie die IPv6-Verkehrsstatistik für eine bestimmte oder alle Schnittstellen anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ IPv6 Statistics (IPv6-Statistik)**.

Abbildung 11-4. IPv6-Statistik



Die Seite **IPv6 Statistics** (IPv6-Statistik) enthält folgende Felder:

Interface (Schnittstelle) – Dient zur Auswahl der Schnittstelle, für die die Statistiken angezeigt werden. Bei einer Änderung der Auswahl wird der Bildschirm aktualisiert, und alle Felder werden mit den Werten für die neu ausgewählte Schnittstelle gefüllt.

IPv6-Statistics (IPv6-Statistik)

Total Datagrams Received (Gesamtzahl der empfangenen Datagramme) – Die Gesamtzahl der von der Schnittstelle empfangenen Eingabedatagramme, einschließlich der fehlerhaft empfangenen Datagramme.

Received Datagrams Locally Delivered (Anzahl der empfangenen lokal zugestellten Datagramme) – Die Gesamtzahl der erfolgreich an IPv6-Benutzerprotokolle (einschließlich ICMP) gesendeten Datagramme. Dieser Zähler wird an der Schnittstelle erhöht, an die diese Datagramme adressiert sind; für einige Datagramme muss es sich hier nicht unbedingt um die Eingabeschnittstelle handeln.

Received Datagrams Discarded Due To Header Errors (Empfangene Datagramme - Abgelehnt auf Grund von Headerfehlern) – Die Anzahl der Eingabedatagramme, die auf Grund von Fehlern in den IPv6-Headern abgelehnt wurden; dazu gehören nicht übereinstimmende Versionen, andere Formatfehler, Überschreitung der maximalen Anzahl an Hops, Fehler bei der Verarbeitung der IPv6-Optionen usw.

Received Datagrams Discarded Due To MTU (Empfangene Datagramme - Abgelehnt auf Grund von MTU) – Die Anzahl der Eingabedatagramme, die nicht weitergeleitet werden konnten, da ihre Länge die der Verbindungs-MTUs der Schnittstelle für den Datenausgang überschritt.

Received Datagrams Discarded Due To No Route (Empfangene Datagramme - Abgelehnt, da keine Route vorhanden) – Die Anzahl der Eingabedatagramme, die abgelehnt wurden, weil keine Route für die Weiterleitung an ihr Ziel gefunden werden konnte.

Received Datagrams With Unknown Protocol (Empfangene Datagramme mit unbekanntem Protokoll) – Die Anzahl der lokal adressierten Datagramme, die zwar erfolgreich empfangen, aber auf Grund eines unbekannten oder nicht unterstützten Protokolls abgelehnt wurden. Dieser Zähler wird an der Schnittstelle erhöht, an die diese Datagramme adressiert sind; für einige Datagramme muss es sich hier nicht unbedingt um die Eingabeschnittstelle handeln.

Received Datagrams Discarded Due To Invalid Address (Empfangene Datagramme - Abgelehnt auf Grund einer ungültigen Adresse) – Die Anzahl der Eingabedatagramme, die abgelehnt wurden, weil das Zielfeld im IPv6-Header keine gültige Adresse für den Empfang in dieser Einheit enthielt. Dazu gehören ungültige Adressen (z. B. ::0) sowie Adressen nicht unterstützter Klassen (z. B. Adressen mit nicht zugeordneten Präfixen). Bei Einheiten, bei denen es sich nicht um IPv6-Router handelt, die also keine Datagramme weiterleiten, zählen hierzu auch Datagramme, die abgelehnt wurden, weil die Zieladresse keine lokale Adresse war.

Received Datagrams Discarded Due To Truncated Data (Empfangene Datagramme - Abgelehnt auf Grund abgeschnittener Daten) – Die Anzahl der Eingabedatagramme, die abgelehnt wurden, da der Datagramm-Frame nicht genug Daten enthielt.

Received Datagrams Discarded Other (Empfangene Datagramme - Abgelehnt aus anderen Gründen) – Die Anzahl der IPv6-Eingabedatagramme, die zwar problemlos weiterverarbeitet werden konnten, jedoch abgelehnt wurden (weil beispielsweise nicht genügend Pufferspeicher vorhanden war). Datagramme, die beim Warten auf ihre Zusammensetzung abgelehnt wurden, werden hier nicht berücksichtigt.

Received Datagrams Reassembly Required (Empfangene Datagramme, für die eine Zusammensetzung erforderlich war) – Die Anzahl der IPv6-Fragmente, die an dieser Schnittstelle wieder zusammengesetzt werden mussten. Dieser Zähler wird an der Schnittstelle erhöht, an die diese Fragmente adressiert sind; für einige Fragmente muss es sich hier nicht unbedingt um die Eingabeschnittstelle handeln.

Datagrams Successfully Reassembled (Erfolgreich zusammengesetzte Datagramme) – Die Anzahl der IPv6-Datagramme, die erfolgreich wieder zusammengesetzt wurden. Dieser Zähler wird an der Schnittstelle erhöht, an die diese Datagramme adressiert sind; für einige Fragmente muss es sich hier nicht unbedingt um die Eingabeschnittstelle handeln.

Datagrams Failed To Reassemble (Datagramme, die nicht zusammengesetzt werden konnten) – Die Anzahl der Datengramme, bei denen der IPv6-Algorithmus für die Wiederzusammensetzung Fehler bei ihrer Zusammensetzung festgestellt hat, z. B. auf Grund von Zeitüberschreitung, Fehlern usw. Einige Algorithmen (vor allem der RFC-815-Algorithmus) verlieren die Übersicht über die Anzahl der IPv6-Fragmente , da diese gleich beim Empfang zusammengesetzt werden; daher entspricht der Wert hier nicht unbedingt der Anzahl der abgelehnten IP-Fragmente. Dieser Zähler wird an der Schnittstelle erhöht, an die diese Fragmente adressiert sind; für einige Fragmente muss es sich hier nicht unbedingt um die Eingabeschnittstelle handeln.

Datagrams Forwarded (Weitergeleitete Datagramme) – Die Anzahl der Ausgabedatagramme, die von dieser Einheit empfangen und an ihr eigentliches Ziel weitergeleitet wurden. Für Geräte, bei denen es sich nicht um IPv6-Router handelt, zählen hierzu nur die Pakete, die per Quellrouting (Routenbestimmung durch den Sender) an dieses Gerät gesendet wurden und bei denen die Quellroutingverarbeitung erfolgreich war. Bei erfolgreich weitergeleiteten Datagrammen wird der Zähler der Schnittstelle für den Datenausgang erhöht.

Datagrams Locally Transmitted (Lokal übertragene Datagramme) – Die Anzahl der Datagramme, die von dieser Einheit erfolgreich über diese Schnittstelle für den Datenausgang übertragen wurden.

Datagrams Transmit Failed (Nicht erfolgreich übertragene Datagramme) – Die Anzahl der Datagramme, die von dieser Einheit nicht erfolgreich übertragen werden konnten.

Datagrams Successfully Fragmented (Erfolgreich fragmentierte Datagramme) – Die Anzahl der IPv6-Datagramme, die an dieser Schnittstelle für den Datenausgang erfolgreich fragmentiert werden konnten.

Datagrams Failed To Fragment (Nicht erfolgreich fragmentierte Datagramme) – Die Anzahl der abgehenden Datagramme, die an dieser Schnittstelle nicht fragmentiert werden konnten.

Datagrams Fragments Created – Die Anzahl der abgehenden Datagrammfragmente, die bei der Fragmentierung an dieser Schnittstelle für den Datenausgang generiert wurden.

Multicast Datagrams Received (Empfangene Multicast-Datagramme) – Die Anzahl der von dieser Schnittstelle empfangenen Multicast-Pakete.

Multicast Datagrams Transmitted (Übertragene Multicast-Datagramme) – Die Anzahl der von dieser Schnittstelle übertragenen Multicast-Pakete.

ICMPv6 Statistics (ICMPv6-Statistik)

Total ICMPv6 Messages Received (Gesamtzahl der empfangenen ICMPv6-Meldungen) – Die Gesamtzahl der von dieser Schnittstelle empfangenen ICMP-Meldungen; dazu gehören auch die über "ipv6IfIcmpInErrors" ermittelten Meldungen. Dies ist die Schnittstelle, an die ICMP-Meldungen gerichtet sind; es muss sich dabei nicht unbedingt um die Eingabeschnittstelle für die Meldungen handeln.

ICMPv6 Messages With Errors Received (Fehlerhaft empfangene ICMPv6-Meldungen) – Die Anzahl der von der Schnittstelle empfangenen ICMP-Meldungen, bei denen ICMP-spezifische Fehler (fehlerhafte Prüfsumme, falsche Länge usw.) festgestellt wurden.

ICMPv6 Destination Unreachable Messages Received (Empfangene ICMPv6-Meldungen über nicht erreichbares Ziel) – Die Anzahl der von der Schnittstelle empfangenen ICMP-Meldungen, die darauf hinweisen, dass ein Ziel nicht erreicht werden kann.

ICMPv6 Messages Prohibited Administratively Received (Empfangene ICMPv6-Meldungen über administrativ verhinderte Kommunikation) – Die Anzahl der von der Schnittstelle empfangenen ICMP-Meldungen, die darauf hinweisen, dass ein Ziel nicht erreicht werden kann bzw. die Kommunikation administrativ verhindert wurde.

ICMPv6 Time Exceeded Messages Received (Empfangene ICMPv6-Meldungen über Zeitüberschreitung) – Die Anzahl der von der Schnittstelle empfangenen

ICMP-Meldungen, die auf eine Zeitüberschreitung hinweisen.

ICMPv6 Parameter Problem Messages Received (Empfangene ICMPv6-Meldungen über Parameterfehler) – Die Anzahl der von der Schnittstelle empfangenen ICMP-Meldungen, die auf Parameterfehler hinweisen.

ICMPv6 Packet Too Big Messages Received (Empfangene ICMPv6-Meldungen über zu große Pakete) – Die Anzahl der von der Schnittstelle empfangenen ICMP-Meldungen, die auf zu große Pakete hinweisen.

ICMPv6 Echo Request Messages Received (Empfangene ICMPv6-Meldungen mit Echoanforderung) – Die Anzahl der von der Schnittstelle empfangenen ICMP-Meldungen, die eine Echoanforderung darstellen.

ICMPv6 Echo Reply Messages Received (Empfangene ICMPv6-Meldungen mit Echoantwort) – Die Anzahl der von der Schnittstelle empfangenen ICMP-Meldungen, die eine Echoantwort darstellen.

ICMPv6 Router Solicit Messages Received (Empfangene ICMPv6-Meldungen mit Routeranfrage) – Die Anzahl der von der Schnittstelle empfangenen ICMP-Meldungen, die eine Routeranfrage (Router Solicitation) darstellen.

ICMPv6 Router Advertisement Messages Received (Empfangene ICMPv6-Meldungen mit Routermitteilung) – Die Anzahl der von der Schnittstelle empfangenen ICMP-Meldungen, die eine Routermitteilung (Router Advertisement) darstellen.

ICMPv6 Neighbor Solicit Messages Received (Empfangene ICMPv6-Meldungen mit Nachbaranfrage) – Die Anzahl der von der Schnittstelle empfangenen ICMP-Meldungen, die eine Nachbaranfrage (Neighbor Solicitation) darstellen.

ICMPv6 Neighbor Advertisement Messages Received (Empfangene ICMPv6-Meldungen mit Nachbarmitteilung) – Die Anzahl der von der Schnittstelle empfangenen ICMP-Meldungen, die eine Nachbarmitteilung (Neighbor Advertisement) darstellen.

ICMPv6 Redirect Messages Received (Empfangene ICMPv6-Meldungen über Umleitung) – Die Anzahl der empfangenen ICMPv6-Meldungen, die auf eine Umleitung hinweisen.

ICMPv6 Group Membership Query Messages Received (Empfangene ICMPv6-Meldungen mit Gruppenzugehörigkeitsabfrage) – Die Anzahl der empfangenen ICMPv6-Meldungen, die Gruppenzugehörigkeiten abfragen.

ICMPv6 Group Membership Response Messages Received (Empfangene ICMPv6-Meldungen mit Antwort auf Gruppenzugehörigkeitsabfrage) – Die Anzahl der empfangenen ICMPv6-Meldungen, die in Antwort auf eine Gruppenzugehörigkeitsabfrage gesendet wurden.

ICMPv6 Group Membership Reduction Messages Received (Empfangene ICMPv6-Meldungen über Reduzierung der Gruppenzugehörigkeiten) – Die Anzahl der empfangenen ICMPv6-Meldungen, die auf eine Reduzierung der Gruppenzugehörigkeiten hinweisen.

Total ICMPv6 Messages Transmitted (Gesamtzahl der übertragenen ICMPv6-Meldungen) – Die Gesamtzahl der ICMP-Meldungen, die diese Schnittstelle versucht hat zu übertragen. Dazu gehören auch alle über **icmpOutErrors** ermittelten ICMP-Meldungen.

ICMPv6 Messages Not Transmitted Due To Error ICMPv6-Meldungen, die auf Grund von Fehlern nicht übertragen wurden) – Die Anzahl der ICMP-Meldungen, die von dieser Schnittstelle auf Grund von ICMP-spezifischen Problemen nicht gesendet wurden (beispielsweise weil nicht genügend Pufferspeicher vorhanden war). Fehler, die außerhalb der ICMP-Schicht festgestellt wurden (wenn beispielsweise das Datagramm von IPv6 nicht weitergeleitet werden kann), sollten in diesem Wert nicht berücksichtigt werden. In einigen Implementierungen gibt es unter Umständen keine Fehlertypen für diesen Zähler.

ICMPv6 Destination Unreachable Messages Transmitted (Gesendete ICMPv6-Meldungen über nicht erreichbares Ziel) – Die Anzahl der von der Schnittstelle gesendeten ICMP-Meldungen, die darauf hinweisen, dass ein Ziel nicht erreicht werden kann.

ICMPv6 Messages Prohibited Administratively Transmitted (Übertragene ICMPv6-Meldungen über administrativ verhinderte Kommunikation) – Die Anzahl der von der Schnittstelle gesendeten ICMP-Meldungen, die darauf hinweisen, dass ein Ziel nicht erreicht werden kann bzw. die Kommunikation administrativ verhindert wurde.

ICMPv6 Time Exceeded Messages Transmitted (Übertragene ICMPv6-Meldungen über Zeitüberschreitung) – Die Anzahl der von der Schnittstelle gesendeten ICMP-Meldungen, die auf eine Zeitüberschreitung hinweisen.

ICMPv6 Parameter Problem Messages Transmitted (Übertragene ICMPv6-Meldungen über Parameterfehler) – Die Anzahl der von der Schnittstelle gesendeten ICMP-Meldungen, die auf Parameterfehler hinweisen.

ICMPv6 Packet Too Big Messages Transmitted (Übertragene ICMPv6-Meldungen über zu große Pakete) – Die Anzahl der von der Schnittstelle gesendeten ICMP-Meldungen, die auf zu große Pakete hinweisen.

ICMPv6 Echo Request Messages Transmitted (Übertragene ICMPv6-Meldungen mit Echoanforderung) – Die Anzahl der von der Schnittstelle gesendeten ICMP-Meldungen, die eine Echoanforderung darstellen.

ICMPv6 Echo Reply Messages Transmitted (Übertragene ICMPv6-Meldungen mit Echoantwort) – Die Anzahl der von der Schnittstelle gesendeten ICMP-Meldungen, die eine Echoantwort darstellen.

ICMPv6 Router Solicit Messages Transmitted (Übertragene ICMPv6-Meldungen mit Routeranfrage) – Die Anzahl der von der Schnittstelle gesendeten ICMP-Meldungen, die eine Routeranfrage (Router Solicitation) darstellen.

ICMPv6 Router Advertisement Messages Transmitted (Übertragene ICMPv6-Meldungen mit Routermitteilung) – Die Anzahl der von der Schnittstelle gesendeten ICMP-Meldungen, die eine Routermitteilung (Router Advertisement) darstellen.

ICMPv6 Neighbor Solicit Messages Transmitted (Übertragene ICMPv6-Meldungen mit Nachbaranfrage) – Die Anzahl der von der Schnittstelle gesendeten ICMP-Meldungen, die eine Nachbaranfrage (Router Solicitation) darstellen.

ICMPv6 Neighbor Advertisement Messages Transmitted (Übertragene ICMPv6-Meldungen mit Nachbarmitteilung) – Die Anzahl der von der Schnittstelle gesendeten ICMP-Meldungen, die eine Nachbarmitteilung (Neighbor Advertisement) darstellen.

ICMPv6 Redirect Messages Transmitted (Übertragene ICMPv6-Meldungen über Umleitung) – Die Anzahl der gesendeten Umleitungsmeldungen.

ICMPv6 Group Membership Query Messages Transmitted (Übertragene ICMPv6-Meldungen mit Gruppenzugehörigkeitsabfrage) – Die Anzahl der gesendeten ICMPv6-Meldungen, die Gruppenzugehörigkeiten abfragen.

ICMPv6 Group Membership Response Messages Transmitted (Übertragene ICMPv6-Meldungen mit Antwort auf Gruppenzugehörigkeitsabfrage) – Die Anzahl der gesendeten ICMPv6-Meldungen, die in Antwort auf eine Gruppenzugehörigkeitsabfrage gesendet wurden.

ICMPv6 Group Membership Reduction Messages Transmitted (Übertragene ICMPv6-Meldungen über Reduzierung der Gruppenzugehörigkeiten) – Die Anzahl der gesendeten ICMPv6-Meldungen, die auf eine Reduzierung der Gruppenzugehörigkeiten hinweisen.

ICMPv6 Duplicate Address Detects (Anzahl der doppelten ICMPv6-Adressen) – Die Anzahl der von der Schnittstelle festgestellten doppelten Adressen.

Anzeige von IPv6-Statistikdaten

1. Öffnen Sie die Seite **IPv6 Statistics** (IPv6-Statistik).
2. Wählen Sie über das Dropdown-Menü **Interface** (Schnittstelle) die Schnittstelle aus, die angezeigt werden soll.

   Die Statistiken für die gewählte Schnittstelle werden angezeigt.

Anzeigen von IPv6- und ICMPv6-Statistikdaten mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

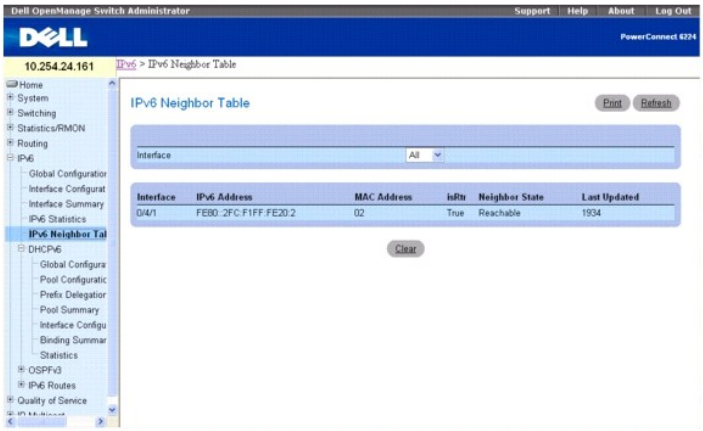
- IPv6 Routing Commands (IPv6-Routingbefehle)

IPv6-Nachbarschaftstabelle

Über die **IPv6 Neighbor Table** (IPv6-Nachbarschaftstabelle) können Sie Angaben zu IPv6-Nachbarn für eine bestimmte Schnittstelle anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ IPv6 Neighbor Table (IPv6-Nachbarschaftstabelle)**.

Abbildung 11-5. IPv6-Nachbarschaftstabelle



Die Seite **IPv6 Neighbor Table** (IPv6-Nachbarschaftstabelle) enthält folgende Felder:

Interface (Schnittstelle) – Hier wird die Schnittstelle ausgewählt, für die Informationen zum Status des Nachbarn angezeigt werden.

Interface (Schnittstelle) – Gibt die Schnittstelle an, deren Einstellungen in der aktuellen Tabellenzeile angezeigt werden.

IPv6 Address (IPv6-Adresse) – Gibt die IPv6-Adresse des Nachbarn oder der Schnittstelle an.

MAC Address (MAC-Adresse) – Gibt die einer Schnittstelle zugeordnete MAC-Adresse an.

IsRtr – Gibt an, ob es sich bei dem Nachbarn um einen Router handelt. Ist dies der Fall, ist der Wert **True** . Ist dies nicht der Fall, ist der Wert **False** .

Neighbor State (Status des Nachbarn) – Gibt den Status des Eintrags im Cache für Nachbarn an. Für dynamische Einträge im Cache für die IPv6-Nachbarsuche (Neighbor Discovery) sind folgende Statusangaben möglich:

- **Incmp** – Für den Eintrag wird eine Adressauflösung durchgeführt. An die Solicited-Node-Multicast-Adresse des Ziel wurde eine Nachbarabfrage geschickt, auf die hin jedoch noch keine Nachbarmitteilung (Neighbor Advertisement) empfangen wurde.
- **Reachable** (Erreichbar) – Innerhalb der letzten (über "Reachable Time" in Millisekunden festgelegten) Zeit wurde eine Bestätigung empfangen, dass der Weiterleitungspfad an den Nachbarn verfügbar ist. Solange der Status REACH ist, werden vom Gerät beim Senden der Pakete keine besonderen Maßnahmen ergriffen.
- **Stale** (Veraltet) – Es ist mehr Zeit vergangen, als über "Reachable Time" (in Millisekunden) festgelegt wurde, seit die letzte Bestätigung empfangen wurde, dass der Weiterleitungspfad verfügbar ist. Solange der Status STALE ist, werden vom Gerät keine besonderen Maßnahmen ergriffen, bis ein Paket gesendet wird.
- **Delay** (Verzögerung) – Es ist mehr Zeit vergangen, als über "Reachable Time" (in Millisekunden) festgelegt wurde, seit die letzte Bestätigung empfangen wurde, dass der Weiterleitungspfad verfügbar ist. Es wurde ein Paket innerhalb der letzten, über DELAY_FIRST_PROBE_TIME in Sekunden festgelegten Zeit gesendet. Wird innerhalb der über DELAY_FIRST_PROBE_TIME festgelegten Zeit, die seit dem Übergang in den Status DELAY vergangen ist, kein Meldung empfangen, die die Verfügbarkeit bestätigt, wird eine Nachbaranfrage (Neighbor Solicitation) gesendet und der Status auf

PROBE gesetzt.

- **Probe** (Abfrage) – Die Bestätigung der Verfügbarkeit wird gezielt angefordert, indem in bestimmen, über "RetransTimer" in Millisekunden festgelegten Abständen Nachbaranfragen (Neighbor Solicitation) gesendet werden, bis eine Bestätigung der Verfügbarkeit empfangen wird.

Last Updated (Letzte Aktualisierung) – Die Zeit, die seit der letzten Bestätigung über die Verfügbarkeit der Adresse vergangen ist.

Anzeigen der IPv6-Nachbarschaftstabelle

1. Öffnen Sie die Seite **IPv6 Neighbor Table** (IPv6-Nachbarschaftstabelle).
2. Wählen Sie über das Dropdown-Menü **Interface** (Schnittstelle) die Schnittstelle aus, die angezeigt werden soll.

   Für die ausgewählte Schnittstelle werden Informationen zu den Nachbarn angezeigt.

Anzeigen der Pv6-Nachbarschaftstabelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- IPv6 Routing Commands (IPv6-Routingbefehle)

DHCPv6

DHCP wird generell zwischen Clients (z. B. Hosts) und Servern (z. B. Routern) für die Zuordnung von IP-Adressen, Gateways und anderen Netzwerkdefinitionen (z. B. DNS-, NTP- und/oder Sitzungsinitiierungsprotokoll (SIP)-Parametern) verwendet. Über das IPv6-Nachbarsuchprotokoll (NDP) und die Verwendung von Routermitteilungen (Router Advertisement) ermöglicht IPv6 jedoch selbst die automatische Konfiguration von IP-Adressen. DHCPv6 hat daher eine andere Rolle in einem Netzwerk als DHCPv4, da DHCPv6 weniger für die Zuordnung von IP-Adressen verwendet wird.

Es gibt eine Reihe von DHCP-Optionen, die allgemein von DHCPv4 unterstützt werden und auch von DHCPv6 unterstützt und daher konfiguriert werden müssen.

ANMERKUNG: Die wichtigste ist die DNS-Serveroption, die über die Webseite **IPv6→ DHCPv6→ Pool Configuration (Poolkonfiguration)** konfiguriert wird.

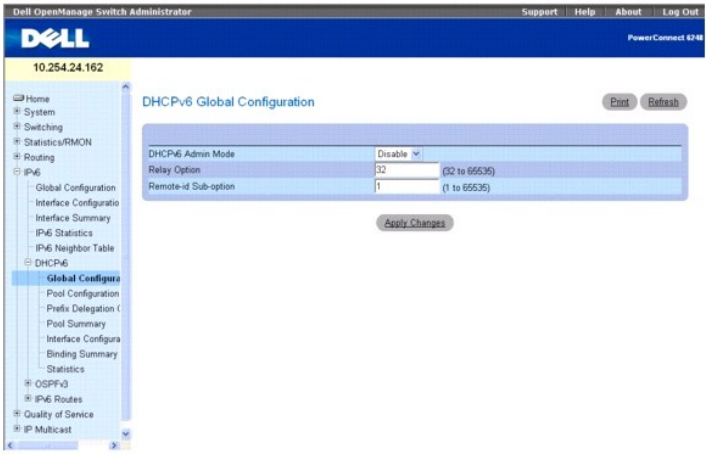
Die Menüseite **DHCPv6** enthält Links zu Webseiten, auf denen DHCPv6-Parameter und -Daten definiert und angezeigt werden können. Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ DHCPv6**. Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

- DHCPv6 - Globale Konfiguration
- DHCPv6-Poolkonfiguration
- Konfiguration einer Präfixdelegierung
- Zusammenfassende Daten zu DHCPv6-Pools
- DHCPv6-Schnittstellenkonfiguration
- Zusammenfassende Daten zu DHCPv6-Serverbindungen
- DHCPv6-Statistik

DHCPv6 - Globale Konfiguration

Über die Seite **DHCPv6 Global Configuration** (DHCPv6 - Globale Konfiguration) können Sie die globalen DHCPv6-Parameter konfigurieren. Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ DHCPv6→ Global Configuration (Globale Konfiguration)**.

Abbildung 11-6. Globale DHCPv6-Konfiguration



Die Seite **DHCPv6 Global Configuration** (DHCPv6 - Globale Konfiguration) enthält folgende Felder:

DHCPv6 Admin Mode (DHCPv6-Verwaltungsmodus) – Gibt den DHCPv6-Betrieb im Switch an. Mögliche Werte sind **Enable** (Aktivieren) und **Disable** (Deaktivieren); der Standardwert ist **Disable** (Deaktivieren).

Relay Option (Relay-Option) – Gibt den Wert der Relay Agent-Informationsoption an. Zulässig sind Werte zwischen 32 und 65535; dies ist der Wert, der zwischen dem Relay Agent und dem Server ausgetauscht wird. Jeder Wert hat eine eigene Bedeutung, die Werte 1 bis 39 sind vordefiniert. Der Standardwert ist 32 (OPTION_INFORMATION_REFRESH_TIME = Wartezeit für Informationsaktualisierung).

Remote-id Sub-option (Suboption Remote-ID) – Hier können Sie den Typ der Suboption "Remote-ID" der Relay Agent-Informationsoption angeben. Zulässig sind Werte zwischen 1 und 65535; der Standardwert ist 1.

Konfigurieren der globalen DHCPv6-Parameter

1. Öffnen Sie die Seite **DHCPv6 Global Configuration** (DHCPv6 - Globale Konfiguration).
2. Ändern Sie die Felder je nach Bedarf.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Änderungen an der DHCPv6-Schnittstelle werden gespeichert, und das Gerät wird aktualisiert.

Konfigurieren der globalen DHCPv6-Parameter mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- DHCPv6 Commands (DHCPv6-Befehle)

DHCPv6-Poolkonfiguration

DHCP for IPv6-Clients werden mit einem Server verbunden, der für die Verwendung von Parametern aus einem Pool konfiguriert wird, der von Ihnen eingerichtet wurde. Dieser Pool wird über einen Poolnamen gekennzeichnet und enthält IPv6-Addressen und Domänennamen von DNS-Servern.

Über die Seite **Pool Configuration** (Poolkonfiguration) können Sie einen Pool erstellen und/oder Poolparameter konfigurieren.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ DHCPv6→ Pool Configuration (Poolkonfiguration)**.

Abbildung 11-7. Poolkonfiguration - Erstellen

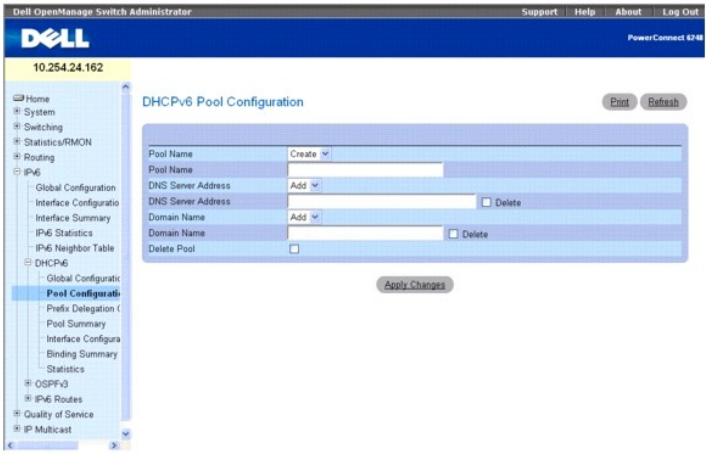
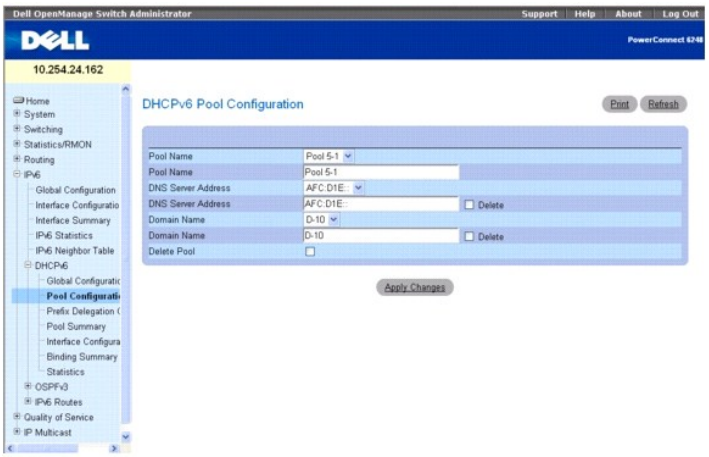


Abbildung 11-8. Poolkonfiguration - Anzeigen



Die Seite **Pool Configuration** (Poolkonfiguration) enthält folgende Felder:

Pool Name (Poolname) – Ein Dropdown-Menü mit den Namen aller konfigurierten Pools. Bei Auswahl von **Create** (Erstellen) werden die Angaben in den Feldern auf dieser Seite gelöscht, so dass neue Poolwerte eingegeben werden können.

Pool Name (Poolname) – Zeigt den Pool an, der im vorigen Feld ausgewählt wurde, oder ermöglicht die Eingabe eines eindeutigen Namens für einen DHCPv6-Pool (wenn "Create" (Erstellen) ausgewählt wurde). Hier können bis zu 31 alphanumerische Zeichen eingegeben werden.

DNS Server Address (DNS-Serveradresse) – Ein Dropdown-Menü, das die IPv6-Adresse eines DNS-Servers in einem bestimmten DHCPv6-Pool angibt. Bei Auswahl von **Add** (Hinzufügen) im Menü wird der Inhalt des folgenden Felds gelöscht, so dass eine neue Adresse eingegeben werden kann.

DNS Server Address (DNS-Serveradresse) – Zeigt die im vorigen Feld ausgewählte DNS-Serveradresse an. Wurde im vorigen Feld **Add** (Hinzufügen) ausgewählt, geben Sie hier eine neue DNS-Serveradresse ein. Klicken Sie auf **Delete** (Löschen), um eine Adresse aus diesem Pool zu entfernen. Bei Klicken auf **Apply Changes** (Änderungen übernehmen) wird die Adresse entfernt.

Domain Name (Domänenname) – Ein Dropdown-Menü, das die Liste der Domänennamen enthält, die in einem bestimmten DHCPv6-Pool konfiguriert sind. Bei Auswahl von **Add** (Hinzufügen) im Menü wird der Inhalt des folgenden Felds gelöscht, so dass ein neuer Name eingegeben werden kann.

Domain Name (Domänenname) – Zeigt den im vorigen Feld ausgewählten DNS-Domänennamen an. Wurde im vorigen Feld **Add** (Hinzufügen) ausgewählt, geben Sie hier einen neuen DNS-Domänennamen ein. Hier können bis zu 255 alphanumerische Zeichen eingegeben werden. Klicken Sie auf **Delete** (Löschen), um einen Domänennamen aus diesem Pool zu entfernen. Bei Klicken auf **Apply Changes** (Änderungen übernehmen) wird der Name entfernt.

Delete Pool (Pool löschen) – Aktivieren Sie dieses Kontrollkästchen, um den angezeigten Pool zu löschen. Bei Klicken auf **Apply Changes** (Änderungen übernehmen) wird der Pool entfernt.

Erstellen eines DHCPv6-Pools

1. Öffnen Sie die Seite **Pool Configuration** (Poolkonfiguration).
2. Wählen Sie im Dropdown-Menü **Pool Name** (Poolname) die Option **Create** (Erstellen) aus.
3. Geben Sie im Feld **Pool Name** (Poolname) einen neuen Namen ein.

4. Geben Sie eine bereit vorhandene DNS-Serveradresse ein, die dem Pool zugeordnet werden soll, oder erstellen Sie eine neue DNS-Serveradresse.
5. Geben Sie einen bereits vorhandenen Domänennamen ein, der dem Pool zugeordnet werden soll, oder erstellen Sie einen neuen Domänennamen.
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der neue Pool wird gespeichert und das Gerät aktualisiert. Wurde eine neue DNS-Serveradresse oder ein neuer Domänenname angegeben, werden auch diese Angaben gespeichert.

Ändern von DHCPv6-Poolparametern

1. Öffnen Sie die Seite **Pool Configuration** (Poolkonfiguration).
2. Wählen Sie über das Dropdown-Menü **Pool Name** (Poolname) den Pool aus, dessen Parameter geändert werden sollen.
3. Ändern Sie die DNS-Serveradresse für den angegebenen Pool, oder richten Sie eine neue DNS-Serveradresse ein.
4. Ändern Sie den Domänennamen für den angegebenen Pool, oder richten Sie einen neuen Domänennamen ein.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Änderungen an den DHCPv6-Parametern werden gespeichert, und das Gerät wird aktualisiert.

Löschen eines DHCPv6-Pools oder -Parameters

1. Öffnen Sie die Seite **Pool Configuration** (Poolkonfiguration).
2. Wählen Sie über das Dropdown-Menü **Pool Name** (Poolname) den Pool aus, der gelöscht werden soll.
3. Soll die DNS-Serveradresse für diesen Pool gelöscht werden, klicken Sie auf **Delete** (Löschen).
4. Soll der Domänenname für diesen Pool gelöscht werden, klicken Sie auf **Delete** (Löschen).
5. Soll der gesamte Pool gelöscht werden, klicken Sie auf **Delete Pool** (Pool löschen).
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Pool bzw. die Parametereinstellung wird gelöscht und das Gerät aktualisiert.

Konfigurieren der DHCPv6-Poolparameter mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

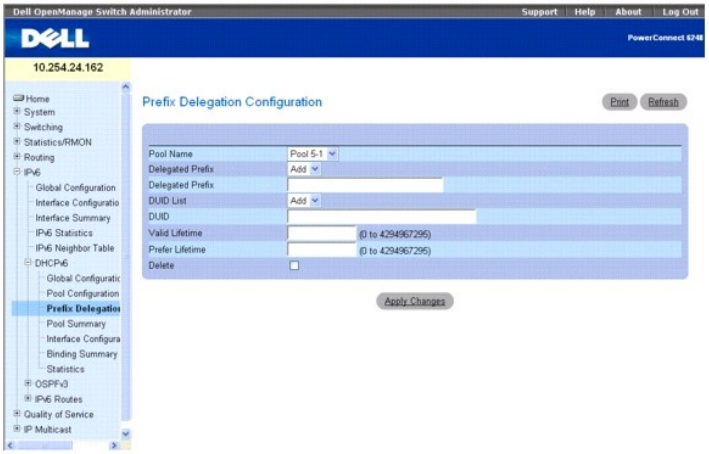
- DHCPv6 Commands (DHCPv6-Befehle)

Konfiguration einer Präfixdelegierung

Über die Seite **Prefix Delegation Configuration** (Konfiguration einer Präfixdelegierung) können Sie ein delegiertes Präfix für einen Pool konfigurieren. Damit ein delegiertes Präfix konfiguriert werden kann, muss mindestens ein Pool über DHCPv6 Pool Configuration (DHCPv6-Poolkonfiguration) erstellt werden.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ DHCPv6→ Pool Configuration (Poolkonfiguration)**.

Abbildung 11-9. Konfiguration einer Präfixdelegierung



Die Seite **Prefix Delegation Configuration** (Konfiguration einer Präfixdelegierung) enthält folgende Felder:

Pool Name (Poolname) – Gibt alle konfigurierte Poolnamen an. Wählen Sie den Pool aus, der konfiguriert werden soll.

Delegated Prefix (Delegiertes Präfix) – Ein Dropdown-Menü, das das delegierte IPv6-Präfix angibt, das dem angegebenen Pool zugeordnet werden soll. Wählen Sie **Add** (Hinzufügen) aus, um ein neues delegiertes Präfix für diesen Pool zu definieren.

Delegated Prefix (Delegiertes Präfix) – Zeigt das ausgewählte delegierte Präfix an oder erlaubt die Eingabe eines neuen Präfixes.

DUID List (DUID-Liste) – Ein Dropdown-Menü, über das die eindeutige DUID des Clients ausgewählt werden kann. Wählen Sie **Add** (Hinzufügen) aus, um eine neue DUID für diesen Pool zu definieren.

DUID – Zeigt die ausgewählte DUID an oder erlaubt die Eingabe einer neuen DUID.

Valid Lifetime (Gültige Lebenszeit) – Gibt die gültige Lebenszeit eines delegierten Präfixes in Sekunden an.

Prefer Lifetime (Bevorzugte Lebenszeit) – Gibt die bevorzugte Lebenszeit eines delegierten Präfixes in Sekunden an.

Delete (Löschen) – Bei Klicken auf **Apply Changes** (Änderungen übernehmen) wird die Konfiguration des angezeigten delegierten Poolpräfixes gelöscht.

Konfigurieren eines neuen Präfixes für einen Pool

1. Öffnen Sie die Seite **Prefix Delegation Configuration** (Konfiguration einer Präfixdelegierung).
2. Wählen Sie den Pool aus, der konfiguriert werden soll.
3. Geben Sie das delegierte Präfix an.
4. Ändern Sie die übrigen Felder je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Das delegierte Präfix und die Parameter werden gespeichert, und das Gerät wird aktualisiert.

Konfigurieren eines delegierten Präfixes mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

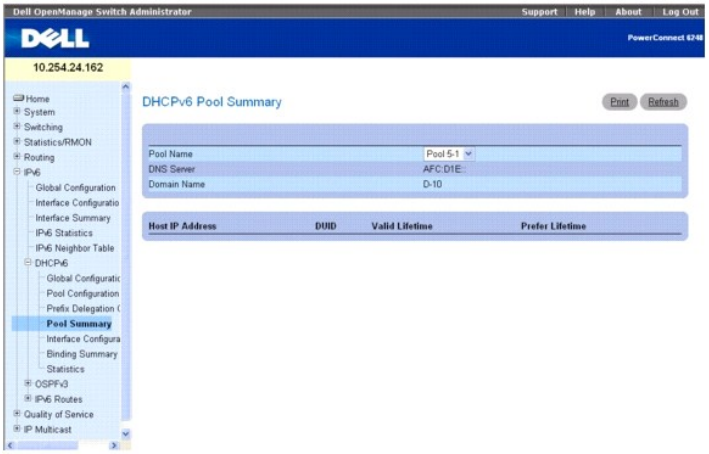
- DHCPv6 Commands (DHCPv6-Befehle)

Zusammenfassende Daten zu DHCPv6-Pools

Über die Seite **Pool Summary** (Zusammenfassende Daten zu Pools) können Sie die Einstellungen für alle DHCPv6-Pools anzeigen. Diese Seite wird nur angezeigt, wenn mindestens ein Pool über DHCPv6 Pool Configuration (DHCPv6-Poolkonfiguration) konfiguriert wurde.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ DHCPv6→ Pool Summary (Zusammenfassende Daten zu Pools)**.

Abbildung 11-10. Zusammenfassende Daten zu Pools



Die Seite **Pool Summary** (Zusammenfassende Daten zu Pools) enthält folgende Felder:

Pool Name (Poolname) – Hier wird der Pool ausgewählt, der angezeigt werden soll.

DNS Server (DNS-Server) – Zeigt die IPv6-Adresse des zugeordneten DNS-Servers an.

Domain Name (Domänenname) – Zeigt den Domänennamen an.

Host IP Address (Host-IP-Adresse) – Zeigt die IPv6-Adresse und die Maskenlänge des delegierten Präfixes an.

DUID – Eine Kennung, die die eindeutige DUID eines Clients angibt.

Valid Lifetime (Gültige Lebenszeit) – Zeigt die gültige Lebenszeit eines delegierten Präfixes in Sekunden an.

Prefer Lifetime (Bevorzugte Lebenszeit) – Zeigt die bevorzugte Lebenszeit eines delegierten Präfixes in Sekunden an.

Anzeigen der zusammenfassenden Daten zu Pools mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

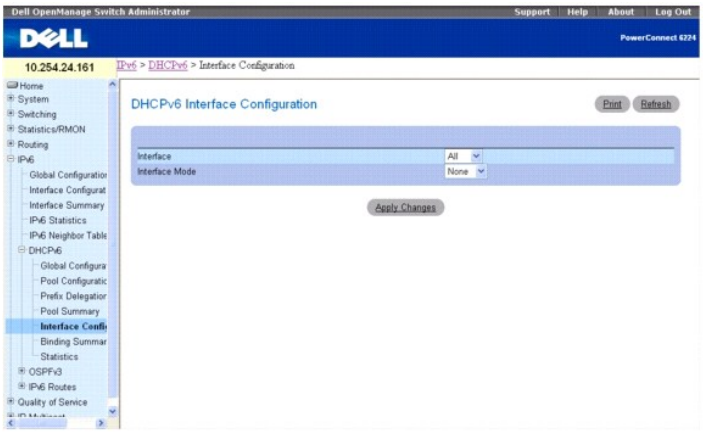
- DHCPv6 Commands (DHCPv6-Befehle)

DHCPv6-Schnittstellenkonfiguration

Über die Seite **IDHCPv6 Interface Configuration** (DHCPv6-Schnittstellenkonfiguration) können Sie eine DHCPv6-Schnittstelle konfigurieren.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ DHCPv6→ Pool Configuration (Poolkonfiguration)**.

Abbildung 11-11. DHCPv6-Schnittstellenkonfiguration



Die Seite **DHCPv6 Interface Configuration** (DHCPv6-Schnittstellenkonfiguration) enthält folgende Felder:

Interface (Schnittstelle) – Hier wird die Schnittstelle ausgewählt, für die die DHCPv6-Serverfunktion konfiguriert werden soll.

Interface Mode (Schnittstellenmodus) – Sie können für den DHCPv6-Modus "Server" oder "Relay" definieren. DHCPv6-Server- und DHCPv6-Relay-Funktionen schließen sich gegenseitig aus.

Pool Name (Poolname) – Hier wird der DHCPv6-Pool ausgewählt, der Parameter für die nicht statusbezogene Präfixdelegierung und/oder die Präfixdelegierung enthält. Dieses Feld wird angezeigt, wenn als Schnittstellenmodus **Server** definiert wurde.

Rapid Commit (Rasche Festlegung) – Dies ist ein optionaler Parameter. Über ihn kann der Austausch zwischen dem Client und dem Server beschleunigt werden. Dieses Feld wird angezeigt, wenn als Schnittstellenmodus **Server** definiert wurde.

Preference (Bevorzugung) – Hier wird ein Wert angegeben, über den Clients festlegen, in welcher Reihenfolge die Auswahl unter mehreren DHCPv6-Servern erfolgt. Zulässig sind Werte zwischen 0 und 4294967295. Dieses Feld wird angezeigt, wenn als Schnittstellenmodus **Server** definiert wurde.

Delete (Löschen) – Aktivieren Sie dieses Kontrollkästchen, und klicken Sie auf **Apply Changes** (Änderungen übernehmen), um die Konfiguration zu löschen. Dieses Feld wird angezeigt, wenn als Schnittstellenmodus "Server" oder "Relay" definiert wurde.

Relay Interface (Relay-Schnittstelle) – Hier wird die Schnittstelle ausgewählt, über die ein Relay-Server erreicht wird. Dieses Feld wird angezeigt, wenn als Schnittstellenmodus **Relay** definiert wurde.

Destination IP Address (Ziel-IP-Adresse) – Hier wird die IPv6-Adresse des DHCPv6-Relay-Servers ausgewählt. Dieses Feld wird angezeigt, wenn als Schnittstellenmodus **Relay** definiert wurde.

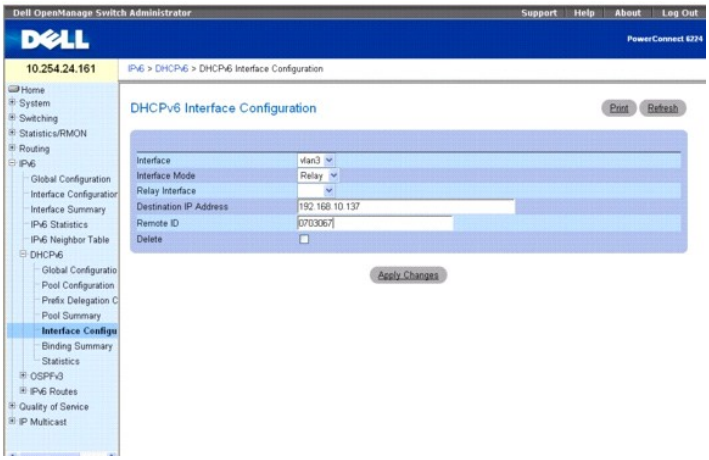
Remote ID (Remote-ID) – Hier wird die Relay Agent-Informationsoption ausgewählt. Die Remote-ID muss aus der DHCPv6-Server-DUID und der Relay-Schnittstellennummer abgeleitet werden, Sie können aber auch eine benutzerdefinierte Zeichenkette angeben. Dieses Feld wird angezeigt, wenn als Schnittstellenmodus **Relay** definiert wurde.

Konfigurieren einer DHCPv6-Schnittstelle für den Relay-Schnittstellenmodus

1. Öffnen Sie die Seite **DHCPv6 Interface Configuration** (DHCPv6-Schnittstellenkonfiguration).
2. Geben Sie die gewünschte Schnittstelle an, und wählen Sie über das Dropdown-Menü **Interface Mode** (Schnittstellenmodus) die Option **Relay** aus.

   Der folgende Bildschirm wird angezeigt:

Abbildung 11-12. DHCPv6-Schnittstellenkonfiguration – Relay



3. Ändern Sie die Felder je nach Bedarf.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Änderungen an der DHCPv6-Schnittstellenkonfiguration werden gespeichert, und das Gerät wird aktualisiert.

Konfigurieren einer DHCPv6-Schnittstelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- DHCPv6 Commands (DHCPv6-Befehle)

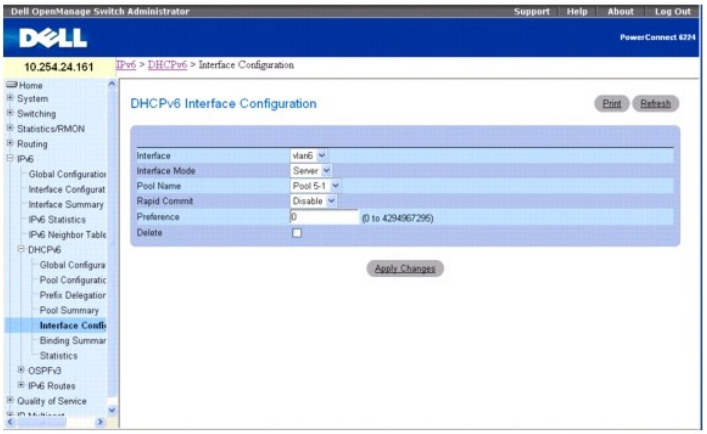
Konfigurieren einer DHCPv6-Schnittstelle für den Serverschnittstellenmodus

1. Öffnen Sie die Seite **DHCPv6 Interface Configuration** (DHCPv6-Schnittstellenkonfiguration).

2. Geben Sie die gewünschte Schnittstelle an, und wählen Sie über das Dropdown-Menü **Interface Mode** (Schnittstellenmodus) die Option **Server** aus.

   Der folgende Bildschirm wird angezeigt:

Abbildung 11-13. DHCPv6-Schnittstellenkonfiguration – Server



3. Ändern Sie die Felder je nach Bedarf.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Änderungen an der DHCPv6-Schnittstellenkonfiguration werden gespeichert, und das Gerät wird aktualisiert.

Konfigurieren einer DHCPv6-Schnittstelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

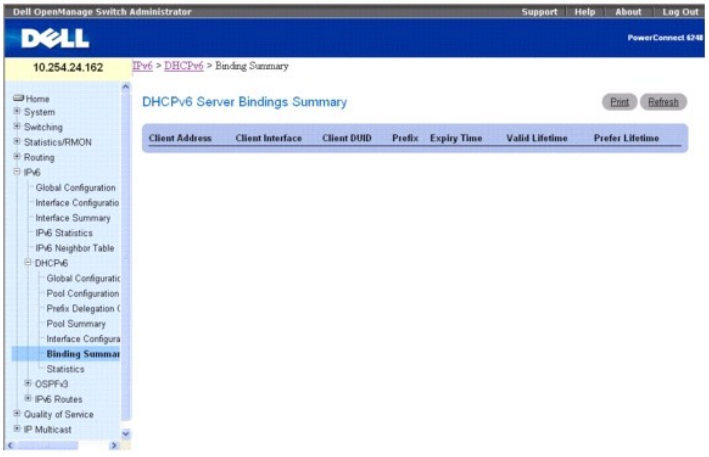
- DHCPv6 Commands (DHCPv6-Befehle)

Zusammenfassende Daten zu DHCPv6-Serverbindungen

Über die Seite **Server Bindings Summary** (Zusammenfassende Daten zu Serverbindungen) können Sie alle DHCPv6-Serverbindungen anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ DHCPv6→ Bindings Summary (Zusammenfassende Daten zu Bindungen)**.

Abbildung 11-14. Zusammenfassende Daten zu Serverbindungen



Die Seite **Server Bindings Summary** (Zusammenfassende Daten zu Serverbindungen) enthält folgende Felder:

Client Address (Clientadresse) – Gibt die IPv6-Adresse des Clients an, der dieser Bindung zugeordnet ist.

Client Interface (Clientschnittstelle) – Gibt die Schnittstellennummer an, an der die Clientbindung erfolgt ist.

Client DUID (Client-DUID) – Gibt die eindeutige DHCPv6-Kennung des Clients an.

Prefix (Präfix) – Gibt den Präfixtyp an, der dieser Bindung zugeordnet ist.

Expiry Time (Ablaufzeit) – Gibt die Zeit (in Sekunden) an, nach der das einer Bindung zugeordnete Präfix abläuft.

Valid Lifetime (Gültige Lebensdauer) – Gibt die Gültigkeitsdauer (in Sekunden) für das einer Bindung zugeordnete Präfix an.

Prefer Lifetime (Bevorzugte Lebensdauer) – Gibt die Bevorzugungsdauer (in Sekunden) für das einer Bindung zugeordnete Präfix an.

Anzeigen von Serverbindungen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- DHCPv6 Commands (DHCPv6-Befehle)

DHCPv6-Statistik

Über die Seite **DHCPv6 Statistics** (DHCPv6-Statistik) können Sie die DHCPv6-Statistik für eine bestimmte oder alle Schnittstellen anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ DHCPv6→ Statistics (Statistik)**.

Abbildung 11-15. DHCPv6-Statistik

Die Seite **DHCPv6 Statistics** (DHCPv6-Statistik) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie hier die Schnittstelle aus, für die Daten angezeigt oder konfiguriert werden sollen. Bei Auswahl von **All** (Alle) werden Daten für alle Schnittstellen angezeigt.

Empfangene Meldungen

Dieser Abschnitt enthält eine Zusammenfassung aller Statistikdaten auf Schnittstellenebene für empfangene Meldungen.

DHCPv6 Solicit Packets Received – Gibt die Anzahl der Anfragen an.

DHCPv6 Request Packets Received – Gibt die Anzahl der Anforderungen an.

DHCPv6 Confirm Packets Received – Gibt die Anzahl der Bestätigungen an.

DHCPv6 Renew Packets Received – Gibt die Anzahl der Erneuerungen an.

DHCPv6 Rebind Packets Received – Gibt die Anzahl der Neubindungen an.

DHCPv6 Release Packets Received – Gibt die Anzahl der Freigaben an.

DHCPv6 Decline Packets Received – Gibt die Anzahl der Ablehnungen an.

DHCPv6 Inform Packets Received – Gibt die Anzahl der Informationspakete an.

DHCPv6 Relay-forward Packets Received – Gibt die Anzahl der Relay-Weiterleitungen an.

DHCPv6 Relay-reply Packets Received – Gibt die Anzahl der Relay-Antworten an.

DHCPv6 Malformed Packets Received – Gibt die Anzahl der fehlerhaften Pakete an.

Received DHCPv6 Packets Discarded – Gibt die Anzahl der abgelehnten Pakete an.

Total DHCPv6 Packets Received – Gibt die Gesamtzahl der empfangenen Pakete an.

Gesendete Nachrichten

Dieser Abschnitt enthält eine Zusammenfassung aller Statistikdaten auf Schnittstellenebene für gesendete Meldungen.

DHCPv6 Advertisement Packets Transmitted – Gibt die Anzahl der Mitteilungen an.

DHCPv6 Reply Packets Transmitted – Gibt die Anzahl der Antworten an.

DHCPv6 Reconfig Packets Transmitted – Gibt die Anzahl der Neukonfigurationen an.

DHCPv6 Relay-forward Packets Transmitted – Gibt die Anzahl der Relay-Weiterleitungen an.

DHCPv6 Relay-reply Packets Transmitted – Gibt die Anzahl der Relay-Antworten an.

Total DHCPv6 Packets Sent – Gibt die Gesamtzahl der übertragenen Pakete an.

Clear (Löschen) – Setzt die Zähler für Schnittstellenpakete zurück.

Anzeigen von DHCPv6-Statistiken

1. Öffnen Sie die Seite **DHCPv6 Statistics** (DHCPv6-Statistik).
2. Wählen Sie über das Dropdown-Menü **Interface** (Schnittstelle) die Schnittstelle aus, die angezeigt werden soll.

   Die HDCPv6-Statistikdaten für die ausgewählte Schnittstelle werden angezeigt.

Anzeigen von DHCPv6-Statistikdaten mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- DHCPv6 Commands (DHCPv6-Befehle)

OSPFv3

OSPFv3 ist das OSPF-Routingprotokoll (Open Shortest Path First) für IPv6. Mit OSPFv2 hat dieses Protokoll die Verbindungsstatusbank (Link-State Database), das bereichsinterne/bereichsübergreifende Konzept sowie AS-externen Routen und virtuellen Verbindungen gemeinsam. Es unterscheidet sich allerdings in einer Reihe von Punkten von dem Routingprotokoll für IPv4; hier einige der Unterschiede: die Peer-Bildung erfolgt über Link-Local-Adressen, das Protokoll ist eher verbindungs- als netzwerkspezifisch und die Adressierungssemantik wurde in Leaf-LSAs verlagert, so dass OSPFv3 schließlich für IPv4 und IPv6 verwendet werden kann. Außerdem werden Punkt-zu-Punkt-Verbindungen unterstützt, um den Tunnelbetrieb zu ermöglichen.

OSPF und OSPFv3 können gleichzeitig aktiviert werden. OSPF wird für IPv4, OSPFv3 für IPv6 eingesetzt.

Die Menüseite **OSPFv3** enthält Links zu Webseiten, auf denen OSPFv3-Parameter und -Daten definiert und angezeigt werden können. Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ OSPFv3**.

Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

- OSPFv3-Konfiguration
- OSPFv3-Bereichskonfiguration
- Zusammenfassende Daten zu OSPFv3-Stub Areas
- Konfiguration des Adressbereichs eines OSPFv3-Bereichs
- OSPFv3-Schnittstellenkonfiguration
- OSPFv3-Schnittstellenstatistik
- OSPFv3-Nachbarschaften
- OSPFv3-Nachbarschaftstabelle
- OSPFv3-Verbindungsstatusdatenbank
- Konfiguration virtueller OSPFv3-Verbindungen
- Zusammenfassende Daten zu virtuellen OSPFv3-Verbindungen
- Konfiguration der OSPFv3-Routenumverteilung
- Zusammenfassende Daten zur OSPFv3-Routenumverteilung

OSPFv3-Konfiguration

Über die Seite **OSPFv3 Configuration** (OSPFv3-Konfiguration) können Sie OSPFv3 für einen Switch aktivieren und konfigurieren.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ OSPFv3→ Configuration (Konfiguration)**.

Abbildung 11-16. OSPFv3-Konfiguration

Die Seite **OSPFv3 Configuration** (OSPFv3-Konfiguration) enthält folgende Felder:

Router ID (Router-ID) – Ein 32-Bit-Integer in der Schreibweise mit Trennzeichen, das den Router im autonomen System (AS) eindeutig kennzeichnet. Soll die Router-ID geändert werden, müssen Sie zunächst OSPFv3 deaktivieren. Nachdem die neue Router-ID gesetzt wurde, müssen Sie OSPFv3 wieder aktivieren, damit die Änderung wirksam wird. Der Standardwert ist 0.0.0.0, allerdings ist dies keine gültige Routen-ID; sie muss geändert werden, bevor Sie auf **Apply Changes** (Änderungen übernehmen) klicken.

OSPFv3 Admin Mode (OSPFv3-Verwaltungsmodus) – Wählen Sie im Dropdown-Menü "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus. Bei Auswahl von **Enable** (Aktivieren) wird OSPFv3 für den Switch aktiviert. Der Standardwert ist **Enable** (Aktivieren). Damit OSPFv3 verwendet wird, müssen Sie zunächst eine Router-ID konfigurieren. Dies kann bei einem IPv6-Router im OSPF-Modus über den CLI-Befehl `router-id` erfolgen.

ANMERKUNG: OSPFv3 bleibt nach der Initialisierung auf dem Router so lange aktiv, bis der Router zurückgesetzt wird.

ASBR Mode (ASBR-Modus) – Gibt an, ob der ASBR-Modus aktiviert oder deaktiviert ist. Eine Aktivierung bedeutet, dass es sich um einen Router handelt, der Routen aus fremden Netzen über AS importiert (ASBR). Ein Router wird automatisch zu einem ASBR-Router, wenn er für die Umverteilung von Routen konfiguriert wird, die er von anderen Protokollen erhält.

ABR Status (ABR-Status) – Hier kann "Enabled" (Aktiviert) oder "Disabled" (Deaktiviert) angegeben werden. Dieses Feld wird nur angezeigt, wenn eine gültige Konfiguration vorhanden ist. Eine Aktivierung bedeutet, dass es sich um einen ABR (Area Border Router) handelt. Eine Deaktivierung bedeutet, dass es sich nicht um einen ABR handelt.

Exit Overflow Interval (secs) (Überlaufstatus beenden) – Geben Sie die Zeit in Sekunden ein, die der Router bei Auftreten eines Überlaufs warten soll, bevor er versucht, den Überlaufstatus zu beenden. Der Router erhält dadurch die Möglichkeit, fehlerfreie AS-external-LSAs erneut zu senden. Bei Angabe von 0 verlässt der Router den Überlaufstatus erst bei einem Neustart. Der Wertebereich liegt zwischen 0 und 2147483647 Sekunden.

External LSA Count (Anzahl externer LSAs) – Die Anzahl externer LSAs (LS-Typ 5) in der Verbindungsstatusdatenbank (Link-State Database).

External LSA Checksum (Prüfsumme externer LSAs) – Die Summe der LS-Prüfsummen externer LSAs in der Verbindungsstatusdatenbank. Anhand dieser Summe kann festgestellt werden, ob es in der Verbindungsstatusdatenbank Änderungen gab; außerdem kann sie für den Vergleich der Verbindungsstatusdatenbanken zweier Router herangezogen werden.

New LSAs Originated (Neue gesendete LSAs) – In einem OSPFv3-Bereich sendet ein Router mehrere LSAs. Jeder Router sendet eine Router-LSA. Handelt es sich bei dem Router außerdem um den designierten Router für eines der Bereichsnetzwerke, sendet er Network-LSAs für die betreffenden Netzwerke. Dieser Wert entspricht der Anzahl der von diesem Router gesendeten LSAs.

LSAs Received (Empfangene LSAs) – Die Anzahl der empfangenen LSAs, die als neue Instanziierungen festgelegt wurden. Dieser Wert umfasst keine neueren Instanziierungen selbst gesendeter LSAs.

External LSDB Limit (Grenzwert für DB für AS-external-LSAs) – Die Anzahl an AS-external-LSAs, die maximal in der Datenbank gespeichert werden können. Der Wert 1 gibt an, dass eine umbegrenzte Anzahl solcher LSAs gespeichert werden kann. Die zulässigen Werte liegen zwischen 1 und 2147483647.

Default Metric (Standardmetrik) – Setzt eine Standardmetrik für umverteilte Routen. Wurde bereits eine Standardmetrik konfiguriert, wird sie in diesem Feld angezeigt. Wurde noch keine Metrik konfiguriert, ist dieses Feld leer. Zulässige Werte sind 1 bis 16777214.

Maximum Paths (Max. Anzahl Pfade) – Gibt die maximale Anzahl an Pfaden an, über die OSPFv3 Meldungen an ein gegebenes Ziel senden kann. Zulässige Werte sind 1 bis 2.

Default Information Originate (Standardinformationen senden) – Aktivieren oder deaktivieren Sie "Default Route Advertise" (Standardroute mitteilen). Die Werte für **Always** (Immer), **Metric** (Metrik) und **Metric Type** (Metriktyp) können erst konfiguriert werden, nachdem **Default Information Originate** (Standardinformationen senden) auf Enable (Aktivieren) gesetzt wurde. Ist dieses Feld auf **Enable** (Aktivieren) gesetzt und wurden bereits Werte in den Feldern **Always** (Immer), **Metric** (Metrik) und **Metric Type** (Metriktyp) konfiguriert, dann werden diese drei Felder wieder auf ihre Standardwerte zurückgesetzt, wenn **Default Information Originate** (Standardinformationen senden) auf **Disable** (Deaktivieren) gesetzt wird.

Always (Immer) – Setzt bei Angabe von "True" die Routermitteilung auf ::/0.

Metric (Metrik) – Gibt die Metrik der Standardroute an. Zulässige Werte sind 0 bis 16777214.

Metric Type (Metriktyp) – Gibt den Metriktyp der Standardroute an. Zulässige Werte sind **External Type 1** (Externer Typ 1) und **External Type 2** (Externer Typ 2).

Konfigurieren von OSPFv3

1. Öffnen Sie die Seite **OSPFv3 Configuration** (OSPFv3-Konfiguration).
2. Ändern Sie die Felder je nach Bedarf.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die OSPFv3-Konfiguration wird gespeichert und das Gerät aktualisiert.

Konfigurieren von OSPFv3 mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- OSPFv3 Commands (OSPFv3-Befehle)

OSPFv3-Bereichskonfiguration

Über die Seite **OSPFv3 Area Configuration** (OSPFv3-Bereichskonfiguration) können Sie einen OSPFv3-Bereich erstellen und konfigurieren.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ OSPFv3→ Area Configuration (Bereichskonfiguration)**.

Abbildung 11-17. OSPFv3-Bereichskonfiguration

Die Seite **OSPFv3 Area Configuration** (OSPFv3-Bereichskonfiguration) enthält folgende Felder:

Area ID (Bereichs-ID) – Der OSPFv3-Bereich. Bei der Bereichs-ID handelt es sich um ein 32-Bit-Integer in der Schreibweise mit Trennzeichen, das den Bereich, mit dem eine Routerschnittstelle verbunden ist, eindeutig kennzeichnet.

External Routing (Externes Routing) – Eine Definition des Routerleistungsspektrums für den Bereich, unter anderem ob AS-external-LSAs in den Bereich/in den gesamten Bereich geflutet werden. Handelt es sich um eine Stub Area, sind dies die möglichen Optionen für die Konfiguration der externen Routingfunktionen; andernfalls steht nur die Option **Import External LSAs** (Externe LSAs importieren) zur Verfügung.

SPF Runs (SPF-Läufe) – Gibt an, wie oft die Tabelle mit Routen innerhalb eines Bereichs unter Verwendung der Verbindungsstatusdatenbank des betreffenden Bereichs berechnet wurde. Die Berechnung erfolgt in der Regel mit Hilfe des Dijkstra-Algorithmus.

Area Border Router Count (Anzahl ABRs) – Die Gesamtzahl der ABRs, die innerhalb dieses Bereichs erreicht werden können. Dieses Feld ist ursprünglich auf Null gesetzt und wird bei jedem SPF-Durchlauf neu berechnet.

Area LSA Count (Anzahl Area-LSAs) – Die Gesamtzahl der LSAs in der Verbindungsstatusdatenbank des Bereichs; AS-external-LSAs werden nicht berücksichtigt.

Area LSA Checksum (Prüfsumme der Area-LSAs) – Die 32-Bit-Summe (ohne Vorzeichen) der LS-Prüfsummen der LSAs, die in der Verbindungsstatusdatenbank des Bereichs enthalten sind. Externe LSAs des LS-Typs 5 sind nicht in diesem Wert berücksichtigt. Anhand dieser Summe kann festgestellt werden, ob es in der Verbindungsstatusdatenbank Änderungen gab; außerdem kann sie für den Vergleich der Verbindungsstatusdatenbanken zweier Router herangezogen werden. Hier wird ein hexadezimaler Wert angegeben.

Konfigurieren eines OSPFv3-Bereichs

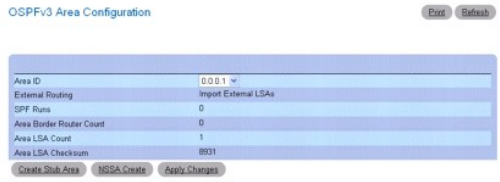
1. Öffnen Sie die Seite **OSPFv3 Area Configuration** (OSPFv3-Bereichskonfiguration).

2. Ändern Sie die Felder je nach Bedarf.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Konfiguration wird gespeichert und das Gerät aktualisiert.

   Die Webseite wird wieder angezeigt und enthält nun die Schaltflächen **Create Stub Area** (Stub Area erstellen) und **NSSA Create** (NSSA erstellen).

Abbildung 11-18. OSPFv3-Bereichskonfiguration - Stub Area und NSSA erstellen



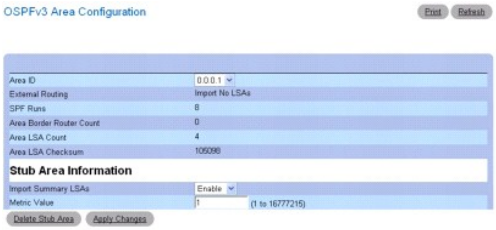
Konfigurieren einer OSPFv3-Stub Area

1. Öffnen Sie die Seite **OSPFv3 Area Configuration** (OSPFv3-Bereichskonfiguration).
2. Ändern Sie die Felder je nach Bedarf.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Webseite wird wieder angezeigt und enthält nun die Schaltflächen **Create Stub Area** (Stub Area erstellen) und **NSSA Create** (NSSA erstellen). Siehe Abbildung 11-18.
4. Klicken Sie auf **Create Stub Area** (Stub Area erstellen).

   Die Felder unter **Stub Area Information** (Stub Area-Angaben) werden angezeigt.

Abbildung 11-19. OSPFv3- Stub Area-Konfiguration



5. Füllen Sie die übrigen Felder aus.
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Stub Area-Angaben werden gespeichert, und das Gerät wird aktualisiert.

Konfigurieren eines OSPFv3-NSSA-Bereichs

1. Öffnen Sie die Seite **OSPFv3 Area Configuration** (OSPFv3-Bereichskonfiguration).
2. Ändern Sie die Felder je nach Bedarf.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Webseite wird wieder angezeigt und enthält nun die Schaltflächen **Create Stub Area** (Stub Area erstellen) und **NSSA Create** (NSSA erstellen). Siehe Abbildung 11-18.
4. Klicken Sie auf der Webseite **OSPFv3 Area Configuration** (OSPFv3-Bereichskonfiguration) auf die **NSSA Create** (NSSA erstellen).

   Die Webseite wird wieder angezeigt und enthält jetzt die Optionen für die NSSA-Konfiguration.

Abbildung 11-20. OSPFv3-Bereichskonfiguration – NSSA

5. Füllen Sie die übrigen Felder aus.
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die NSSA-Einstellungen werden gespeichert, und das Gerät wird aktualisiert.

Löschen der Informationen zu OSPFv3-Stub Areas

1. Öffnen Sie die Seite **OSPFv3 Area Configuration** (OSPFv3-Bereichskonfiguration) mit konfigurierten Stub Area-Informationen.
2. Klicken Sie auf **Delete Stub Area** (Stub Area löschen).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Löschen von OSPFv3-NSSA-Informationen

1. Öffnen Sie die Seite **OSPFv3 Area Configuration** (OSPFv3-Bereichskonfiguration) mit konfigurierten NSSA-Informationen.
2. Klicken Sie auf **NSSA Delete** (NSSA löschen).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Konfigurieren eines OSPFv3-Bereichs mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

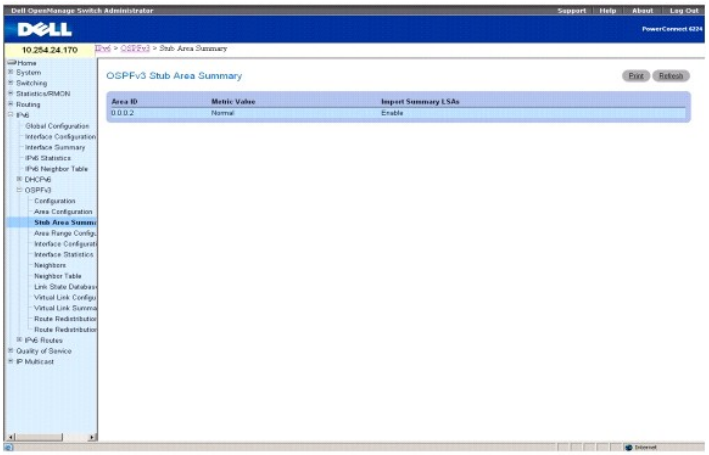
- OSPFv3 Commands (OSPFv3-Befehle)

Zusammenfassende Daten zu OSPFv3-Stub Areas

Über die Seite **OSPFv3 Stub Area Summary** (Zusammenfassende Daten zu OSPFv3-Stub Areas) können Sie die Informationen zu OSPFv3-Stub Areas anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ OSPFv3→ Stub Area Summary (Zusammenfassende Daten zu Stub Areas)**.

Abbildung 11-21. Zusammenfassende Daten zu OSPFv3-Stub Areas



Die Seite **OSPFv3 Stub Area Summary** (Zusammenfassende Daten zu OSPFv3-Stub Areas) enthält folgende Felder:

Area ID (Bereichs-ID) – Die Bereichs-ID der Stub Area.

Metric Value (Metrikwert) – Legt den Wert fest, der als Metrik für die Standardroute verwendet werden soll, die in dem Bereich mitgeteilt wird.

Import Summary LSAs (Summary-LSAs importieren) – Gibt an, ob der Import von Summary-LSAs aktiviert oder deaktiviert ist.

Anzeigen der zusammenfassenden Daten zu OSPFv3-Stub Areas mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

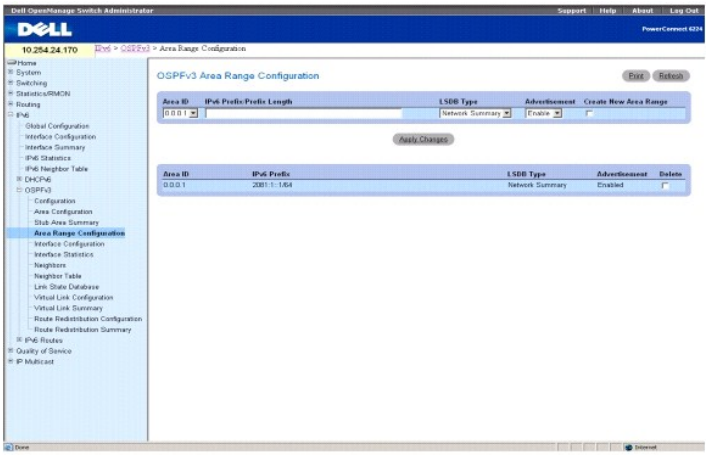
- OSPFv3 Commands (OSPFv3-Befehle)

Konfiguration des Adressbereichs eines OSPFv3-Bereichs

Über die Seite **OSPFv3 Area Range Configuration** (Konfiguration des Adressbereichs eines OSPFv3-Bereichs) können Sie Adressbereiche für einen OSPFv3-Bereich konfigurieren.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ OSPFv3→ Area Range Configuration (Konfiguration des Adressbereichs eines Bereichs)**.

Abbildung 11-22. Konfiguration des Adressbereichs eines OSPFv3-Bereichs



Die Seite **OSPFv3 Area Range Configuration** (Konfiguration des Adressbereichs eines OSPFv3-Bereichs) enthält folgende Felder:

Area ID (Bereichs-ID) – Hier wird der Bereich ausgewählt, dessen Einstellungen konfiguriert werden sollen.

IPv6 Prefix/Prefix Length (IPv6-Präfix/Präfixlänge) – Geben Sie IPv6-Präfix/Präfixlänge für den Adressbereich des ausgewählten Bereichs ein.

LSDB Type (LSDB-Typ) – Wählen Sie den Typ der Verbindungsmitteilung aus, der dem angegebenen Bereich und dem Adressbereich zugeordnet ist. Standardtyp ist **Network Summary** (Zusammenfassende Daten zum Netzwerk).

Advertisement (Mitteilung) – Wählen Sie "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus dem Dropdown-Menü. Bei Auswahl von "Enable" (Aktivieren) wird der Adressbereich außerhalb des Bereichs über eine Network-Summary-LSA mitgeteilt. Der Standardwert ist **Enable** (Aktivieren).

Create New Area Range (Neuen Adressbereich für Bereich erstellen) – Aktivieren Sie dieses Kontrollkästchen, um einen neuen Adressbereich für einen OSPFv3-Bereich mit den von Ihnen angegebenen Werten zu erstellen.

Area ID (Bereichs-ID) – Der OSPFv3-Bereich.

IPv6 Prefix (IPv6-Präfix) - Das IPv6-Präfix eines Adressbereichs für den Bereich.

LSDB Type (LSDB-Typ) – Der Typ der Verbindungsmitteilung für den Adressbereich und den Bereich.

Advertisement (Mitteilung) – Der Mitteilungsmodus für den Adressbereich und den Bereich.

Delete (Löschen) – Aktivieren Sie dieses Kontrollkästchen, um den angegebenen Adressbereich des OSPFv3-Bereichs zu löschen.

Konfigurieren des Adressbereichs eines OSPFv3-Bereichs

1. Öffnen Sie die Seite **OSPFv3 Area Range Configuration** (Konfiguration des Adressbereichs eines OSPFv3-Bereichs).
2. Ändern Sie die Felder je nach Bedarf.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die OSPFv3-Bereichskonfiguration wird gespeichert und das Gerät aktualisiert.

Konfigurieren des Adressbereichs eines OSPFv3-Bereichs mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

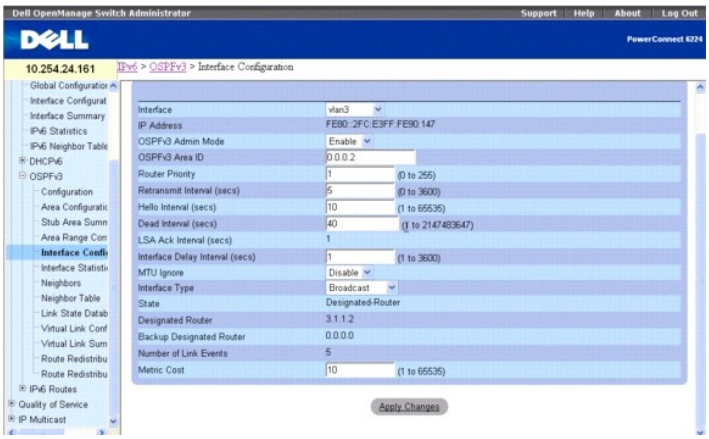
- OSPFv3 Commands (OSPFv3-Befehle)

OSPFv3-Schnittstellenkonfiguration

Über die Seite **OSPFv3 Interface Configuration** (OSPFv3-Schnittstellenkonfiguration) können Sie OSPFv3-Schnittstellen erstellen und konfigurieren.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ OSPFv3→ Interface Configuration (Schnittstellenkonfiguration)**.

Abbildung 11-23. OSPFv3-Schnittstellenkonfiguration



Die Seite **OSPFv3 Interface Configuration** (OSPFv3-Schnittstellenkonfiguration) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie hier die Schnittstelle aus, für die Daten angezeigt oder konfiguriert werden sollen.

IP Address (IP-Adresse) – Die IPv6-Adresse der Schnittstelle.

OSPFv3 Admin Mode (OSPFv3-Verwaltungsmodus) – Wählen Sie "Enable" (Aktivieren) oder "Disable" (Deaktivieren) aus dem Dropdown-Menü. Der Standardwert ist **Disable** (Deaktivieren). Sie können OSPFv3-Parameter auch ohne Aktivierung des OSPFv3-Verwaltungsmodus konfigurieren; die Änderungen werden allerdings erst wirksam, wenn dieser Modus aktiviert wird. Folgende Informationen werden nur bei Aktivierung des Verwaltungsmodus angezeigt: Status, designierter Router, designierter Backup-Router, Anzahl der Verbindungsereignisse, LSA-Bestätigungsintervall und Aufwandsmetrik. Damit OSPFv3 vollständig betriebsfähig ist, muss der Schnittstelle ein gültiger Wert für IPv6-Präfix/Präfixlänge zugeordnet sein. Dies kann im Schnittstellenkonfigurationsmodus über den CLI-Befehl `ipv6 address` erfolgen.

OSPFv3 bleibt nach der Initialisierung auf dem Router so lange aktiv, bis der Router zurückgesetzt wird.

OSPFv3 Area ID (OSPFv3-Bereichs-ID) – Geben Sie ein 32-Bit-Integer in der Schreibweise mit Trennzeichen ein, das den OSPFv3-Bereich, mit dem die ausgewählte Routerschnittstelle verbunden ist, eindeutig kennzeichnet. Bei Zuordnung einer nicht vorhandenen Bereichs-ID wird der Bereich unter Verwendung der Standardwerte erstellt.

Router Priority (Routerpriorität) – Geben Sie die OSPFv3-Priorität für die ausgewählte Schnittstelle ein. Die Schnittstellenpriorität wird als eine ganze Zahl zwischen 0 und 255 angegeben. Der Standardwert ist 1 (höchste Routerpriorität). Der Wert 0 gibt an, dass der Router nicht als designierter Router in diesem Netzwerk zur Verfügung steht.

Retransmit Interval (secs) (Rückübertragungsintervall) – Geben Sie das OSPFv3-Rückübertragungsintervall für die angegebene Schnittstelle an. Dies ist die Zeit in Sekunden zwischen LSAs für Nachbarschaftsbeziehungen (Adjacencies), die zu dieser Routerschnittstelle gehören. Dieser Wert wird auch bei der Rückübertragung von Datenbankbeschreibungen und LS-Anforderungspaketen verwendet. Zulässig sind Werte zwischen 0 und 3600 Sekunden (1 Stunde). Der Standardwert ist 5 Sekunden.

Hello Interval (secs) (Hello-Intervall) – Geben Sie das OSPFv3-Hello-Intervall (in Sekunden) für die angegebene Schnittstelle an. Dieser Parameter muss für alle Router, die mit einem Netzwerk verbunden sind, derselbe sein. Zulässig sind Werte zwischen 1 und 65535 Sekunden; der Standardwert ist 10 Sekunden.

Dead Interval (secs) (Totintervall) – Geben Sie das OSPFv3-Totintervall (in Sekunden) für die angegebene Schnittstelle an. Gibt an, wie lange ein Router auf das Eintreffen von Hello-Paketen eines benachbarten Routers wartet, bevor dieser als ausgefallen bezeichnet wird. Dieser Parameter muss für alle Router, die mit einem Netzwerk verbunden sind, derselbe sein. Er sollte ein Vielfaches des Hello-Intervalls sein (z. B 4). Zulässig sind Werte zwischen 1 und 2147483647; der Standardwert ist 40.

LSA Ack Interval (secs) (LSA-Bestätigungsintervall) – Zeigt die Zeit in Sekunden zwischen der Übertragung von LSA-Bestätigungspaketen an; dieses Intervall muss kürzer als das Rückübertragungsintervall sein.

Interface Delay Interval (secs) (Verzögerungsintervall der Schnittstelle) – Geben Sie die OSPFv3-Verzögerung bei Statusübergängen für die angegebene Schnittstelle an. Gibt die geschätzte Zeit in Sekunden an, die die Übertragung eines LSU-Pakets über die ausgewählte Schnittstelle dauert. Zulässig sind Werte zwischen 1 und 3600 Sekunden (1 Stunde). Der Standardwert ist 1 Sekunde.

MTU Ignore (MTU ignorieren) – Deaktiviert die Erkennung nicht übereinstimmender OSPFv3-MTUs bei empfangenen Paketen. Der Standardwert ist **Disable** (Deaktivieren).

Interface Type (Schnittstellentyp) – Geben Sie den Schnittstellentyp an; dieser kann auf Broadcast- oder Punkt-zu-Punkt-Modus gesetzt werden. Der Standardtyp ist "Broadcast".

State (Status) – Der aktuelle Status der ausgewählten Routerschnittstelle. Dabei kann es sich um eine der folgenden Statusangaben handeln:

- **Down** (Nicht in Betrieb) – Der ursprüngliche Status der Schnittstelle. In diesem Status haben die Lower-Level-Protokolle angegeben, dass die Schnittstelle nicht verwendet werden kann. Die Schnittstellenparameter werden in diesem Status auf ihre ursprünglichen Werte zurückgesetzt. Alle Schnittstellenzeitgeber sind deaktiviert, und der Schnittstelle sind keine Nachbarschaftsbeziehungen zugeordnet.
- **Loopback** (Schleifentest) – In diesem Status wird die Schnittstelle des Routers zum Netzwerk per Hardware oder Software rückgeschleift. Die Schnittstelle steht daher für den normalen Datenverkehr nicht zur Verfügung. Trotzdem kann es wünschenswert sein, Angaben zur Qualität dieser Schnittstelle zu erhalten; dies geschieht entweder über ICMP-Ping-Signale zur Schnittstelle oder z. B. über einen Bitfehlertest. Daher können auch an eine Schnittstelle im Loopback-Status noch IP-Pakete gesendet werden. Um dies zu ermöglichen, werden diese Schnittstellen in Router-LSAs als einzelne Hostrouten mitgeteilt, bei deren Ziel es sich um die IP-Schnittstellenadresse handelt.
- **Waiting** (Wartestatus) – Der Router versucht, den designierten (Backup-)Router für das Netzwerk durch Überwachung der empfangenen Hello-Pakete zu ermitteln. Dabei darf der Router keinen designierten Backup-Router oder designierten Router bestimmen, bevor der Wartestatus nicht wieder verlassen wird. Dadurch werden unnötige Änderungen des designierten (Backup-)Routers verhindert.
- **Designated Router** (Designierter Router) – Dieser Router ist selbst der designierte Router im verbundenen Netzwerk. Zu allen anderen Routern, die mit dem Netzwerk verbunden sind, werden Nachbarschaftsbeziehungen aufgebaut. Der Router muss außerdem eine Network-LSA für den Netzwerkknoten senden. Diese Network-LSA enthält Verbindungen zu allen Routern (einschließlich des designierten Routers), die mit dem Netzwerk verbunden sind.
- **Backup Designated Router** (Designierter Backup-Router) – Dieser Router ist selbst der designierte Backup-Router im verbundenen Netzwerk. Fällt der aktive designierte Router aus, wird dieser Router zum designierten Router. Er baut Nachbarschaftsbeziehungen zu allen anderen Routern auf, die mit dem Netzwerk verbunden sind. Die Aufgaben des designierten Backup-Routers beim Flooding (Fluten) unterscheiden sich geringfügig von denen des designierten Routers.
- **Other Designated Router** (Anderer designierter Router) – Die Schnittstelle ist mit einem Broadcast- oder NBMA-Netzwerk verbunden, in dem andere Router als designierter Router und Backup-Router festgelegt wurden. Der Router versucht, Nachbarschaftsbeziehungen zum designierten Router und zum designierten Backup-Router aufzubauen.

Dieser Status wird nur angezeigt, wenn der OSPFv3-Verwaltungsmodus aktiviert ist.

Designated Router (Designierter Router) – Die Kennung des designierten Routers für dieses Netzwerk, wie sie sich für den mitteilenden Router darstellt. Hier wird der designierte Router über seine Router-ID identifiziert; der Wert 0.0.0.0 gibt an, dass kein designierter Router vorhanden ist. Dieses Feld wird nur angezeigt, wenn der OSPFv3-Verwaltungsmodus aktiviert ist.

Backup Designated Router (Designierter Backup-Router) – Die Kennung des designierten Backup-Routers für dieses Netzwerk, wie sie sich für den mitteilenden Router darstellt. Hier wird der designierte Backup-Router über seine Router-ID identifiziert; das Feld wird auf 0.0.0.0 gesetzt, wenn kein designierter Backup-Router vorhanden ist. Dieses Feld wird nur angezeigt, wenn der OSPFv3-Verwaltungsmodus aktiviert ist.

Number of Link Events (Anzahl der Verbindungsereignisse) – Gibt an, wie oft sich der OSPFv3-Schnittstellenstatus geändert hat. Dieses Feld wird nur angezeigt, wenn der OSPFv3-Verwaltungsmodus aktiviert ist.

Metric Cost (Aufwandsmetrik) – Geben Sie den Wert dieser Schnittstelle für die Dienstart "Aufwand" (TOS = cost) ein. Für die Aufwandsmetrik kann ein Wert zwischen 1 und 65535 eingegeben werden. Dieser Parameter kann nur konfiguriert werden, wenn OSPFv3 für die Schnittstelle aktiviert ist.

Konfigurieren einer OSPFv3-Schnittstelle

1. Öffnen Sie die Seite **OSPFv3 Interface Configuration** (OSPFv3-Schnittstellenkonfiguration).
2. Wählen Sie die Schnittstelle aus, für die OSPFv3 konfiguriert werden soll.
3. Ändern Sie die übrigen Felder je nach Bedarf.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Schnittstelle wird für OSPFv3 konfiguriert und das Gerät aktualisiert.

Konfigurieren einer OSPFv3-Schnittstelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

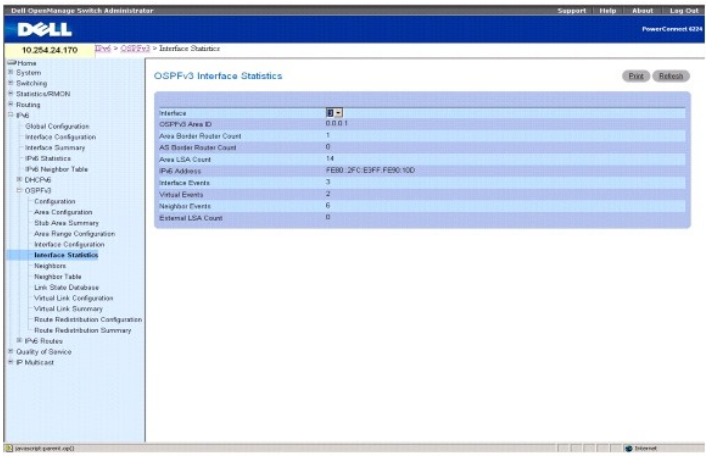
- OSPFv3 Commands (OSPFv3-Befehle)

OSPFv3-Schnittstellenstatistik

Über die Seite **OSPFv3 Interface Statistics** (OSPFv3-Schnittstellenstatistik können Sie OSPFv3-Schnittstellenstatistkdaten anzeigen. Die Informationen werden nur angezeigt, wenn OSPF aktiviert ist.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ OSPFv3→ Interface Statistics (Schnittstellenkonfiguration)**.

Abbildung 11-24. OSPFv3-Schnittstellenstatistik



Die Seite **OSPFv3 Interface Statistics** (OSPFv3-Schnittstellenstatistik) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie hier die Schnittstelle aus, für die Daten angezeigt werden sollen.

OSPF Area ID (OSPF-Bereichs-ID) – Der OSPF-Bereich, zu dem die ausgewählte Routerschnittstelle gehört. Bei der OSPF-Bereichs-ID handelt es sich um ein 32-Bit-Integer in der Schreibweise mit Trennzeichen, das den Bereich, mit dem die Schnittstelle verbunden ist, eindeutig kennzeichnet.

Area Border Router Count (Anzahl ABRs) – Die Gesamtzahl der ABRs, die innerhalb dieses Bereichs erreicht werden können. Dieses Feld ist ursprünglich auf Null gesetzt und wird bei jedem SPF-Durchlauf neu berechnet.

AS Border Router Count (Anzahl ASRBs) – Die Gesamtzahl der ASBRs (Autonomous System Border Router), die innerhalb dieses Bereichs erreicht werden können. Dieses Feld ist ursprünglich auf Null gesetzt und wird bei jedem SPF-Durchlauf neu berechnet.

Area LSA Count (Anzahl Area-LSAs) – Die Gesamtzahl der LSAs in der Verbindungsstatusdatenbank des Bereichs; AS-external-LSAs werden nicht berücksichtigt.

IPv6 Address (IPv6-Adresse) – Die IP-Adresse der Schnittstelle.

Interface Events (Schnittstellenereignisse) – Gibt an, wie oft Statusänderungen oder Fehler für die angegebene OSPF-Schnittstelle aufgetreten sind.

Virtual Events (Virtuelle Ereignisse) – Gibt an, wie oft Statusänderungen oder Fehler für diese virtuelle Verbindung aufgetreten sind.

Neighbor Events (Nachbarereignisse) – Gibt an, wie oft Statusänderungen oder Fehler für diese Nachbarschaftsbeziehung aufgetreten sind.

External LSA Count (Anzahl externer LSAs) – Die Anzahl externer Mitteilungen des Verbindungsstatus (LSA) (LS-Typ 5) in der Verbindungsstatusdatenbank.

Anzeigen der OSPFv3-Schnittstellenstatistik

1. Öffnen Sie die Seite **OSPFv3 Interface Statistics** (OSPFv3-Schnittstellenstatistik).

2. Wählen Sie die Schnittstelle, die Sie anzeigen wollen, im Dropdown-Menü **Interface** (Schnittstelle).

   Die Statistikdaten dieser Schnittstelle werden angezeigt.

Anzeigen der OSPFv3-Schnittstellenstatistik mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

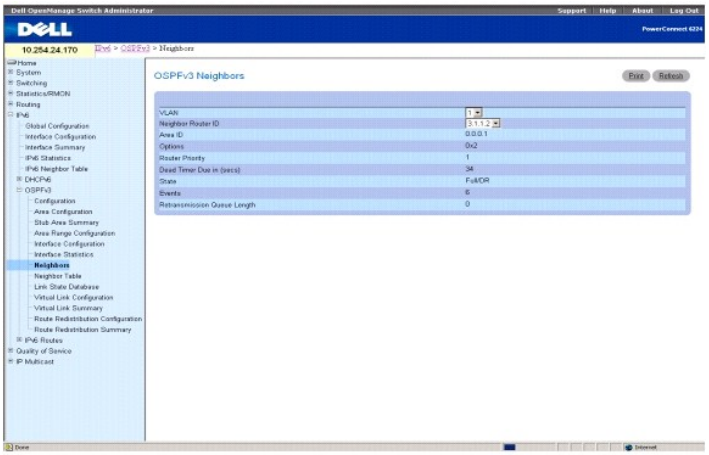
- OSPFv3 Commands (OSPFv3-Befehle)

OSPFv3-Nachbarschaften

Auf der Seite **OSPFv3-Neighbors** (OSPFv3-Nachbarschaften) können Sie die OSPF-Nachbarkonfiguration für eine ausgewählte Nachbar-ID anzeigen. Bei Angabe einer bestimmten Nachbar-ID werden ausführliche Informationen zu dem betreffenden benachbarten Router angezeigt. Die Informationen zu Nachbarn werden nur angezeigt, wenn OSPF aktiviert ist und die Schnittstelle einen Nachbarn hat. Bei der IP-Adresse handelt es sich um die IP-Adresse des Nachbarn.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ OSPFv3→ Configuration (Konfiguration)**.

Abbildung 11-25. OSPFv3-Nachbarschaften



Die Seite **OSPF Neighbors** (OSPF-Nachbarn) enthält folgende Felder:

Interface (Schnittstelle) – Wählt die Schnittstelle aus, für die Daten angezeigt oder konfiguriert werden sollen.

Neighbor Router ID (ID des benachbarten Routers) – Hier wird die IP-Adresse des Nachbarn ausgewählt, für den Daten angezeigt werden sollen.

Area ID (Bereichs-ID) – Ein 32-Bit-Integer in Schreibweise mit Trennzeichen, das den benachbarten Router angibt.

Options (Optionen) – Die vom benachbarten Router unterstützten optionalen OSPF-Funktionen. Die optionale OSPF-Funktionalität des Nachbarn wird ebenfalls in dessen Hello-Paketen angegeben. Dadurch können Hello-Pakete abgelehnt werden (d. h. es werden erst gar keine Nachbarschaftsbeziehungen aufgebaut), wenn sich eine Differenz in wichtigen OSPF-Funktionen ergibt.

Router Priority (Routerpriorität) – Zeigt die OSPF-Priorität für den angegebenen benachbarten Router an. Die Priorität eines benachbarten Routers wird als ganze Zahl zwischen 0 und 255 angegeben. Der Wert 0 gibt an, dass der Router nicht als designierter Router für dieses Netzwerk ausgewählt werden kann.

Dead Timer Due in (secs) (Zeitgeber für nicht erreichbare Nachbarn läuft ab in (Sek.)) – Wenn keine Hello-Pakete empfangen werden, gibt dieses Feld die Zeit an, nach der ein Nachbar als nicht erreichbar erklärt wird.

State (Status) – Für einen benachbarten Router können folgende Statusangaben gemacht werden:

- **Down** (Nicht in Betrieb) – Der ursprüngliche Kommunikationsstatus des benachbarten Routers. Er gibt an, dass keine neuen Daten vom benachbarten Router empfangen wurden. In NBMA-Netzwerken können auch an Router, die nicht in Betrieb sind, noch Hello-Pakete gesendet werden, allerdings weniger häufig.
- **Attempt** (Versuch) – Dieser Status ist nur für Nachbarn zulässig, die mit NBMA-Netzwerken verbunden sind. Er gibt an, dass keine neuen Daten vom Nachbarn empfangen wurden, aber unbedingt versucht werden sollte, den Nachbarn zu kontaktieren. Dazu werden in regelmäßigen Abständen (die über das Hello-Intervall festgelegt werden) Hello-Pakete an den benachbarten Router gesendet.
- **Init** (Initialisierung) – In diesem Status wurde vor kurzem ein Hello-Paket vom Nachbarn empfangen. Allerdings wurde noch keine bidirektionale Kommunikation mit dem Nachbarn eingerichtet (d. h. der Router selbst war noch nicht im Hello-Paket des Nachbarn enthalten). Alle Nachbarn in diesem Status (oder höher) sind in den von der zugeordneten Schnittstelle gesendeten Hello-Paketen aufgeführt.
- **2-Way** (Bidirektional) – In diesem Status ist die bidirektionale Kommunikation zwischen den beiden Routern eingerichtet. Dies kann über das Hello-Protokoll überprüft werden. Dies ist der Status kurz vor Einrichtung einer Nachbarschaftsbeziehung. Der designierte Backup-Router wird aus Nachbarpaaren ausgewählt, die mindestens den Status **2-Way** (Bidirektional) haben.
- **Exchange Start** (Start des Austausches) – Der erste Schritt bei der Herstellung einer Beziehung zwischen zwei benachbarten Routern. Hier wird festgelegt, bei welchem Router es sich um den Master handeln soll; außerdem wird die anfängliche DD-Sequenznummer festgelegt. Die Kommunikation zwischen benachbarten Routern in diesem Status oder höher wird als "Beziehung" (Adjacency) bezeichnet.
- **Exchange** (Austausch) – In diesem Status beschreibt der Router die gesamte Verbindungsstatusdatenbank, indem er Pakete mit der Datenbankbeschreibung an den benachbarten Router sendet. In diesem Status können auch Pakete mit Verbindungsstatusanforderungen gesendet werden, die die aktuellen LSAs des benachbarten Routers anfordern. Beziehungen in diesem Status oder höher werden von der Flooding-Prozedur verwendet. Über diese Verbindungen können sämtliche OSPF-Routingprotokollpakete gesendet und empfangen werden.

- **Loading** (Ladestatus) – In diesem Status werden Pakete mit Verbindungsstatusanforderungen an den benachbarten Router gesendet, die die aktuelleren LSAs anfordern, die im Status "Exchange" (Austausch) zwar erkannt, aber noch nicht empfangen wurden.
- **Full** (Vollständig) – In diesem Status besteht zwischen den benachbarten Routern eine vollständige Nachbarschaftsbeziehung. Diese Beziehungen sind nun in Router- und in Network-LSAs enthalten.

Events (Ereignisse) – Gibt an, wie oft Statusänderungen oder Fehler für diese Nachbarschaftsbeziehung aufgetreten sind.

Retransmission Queue Length (Länge der Warteschlange für Übertragungswiederholungen) – Die aktuelle Länge der Warteschlange für Übertragungswiederholungen.

Anzeigen von OSPFv3-Nachbarn

1. Öffnen Sie die Seite **OSPFv3 Neighbors** (OSPFv3-Nachbarn).
2. Wählen Sie die Schnittstelle, die Sie anzeigen wollen, im Dropdown-Menü **Interface** (Schnittstelle).
3. Wählen Sie die **Neighbor Router ID** (ID des benachbarten Routers) aus, die angezeigt werden soll.

   Die Statistikdaten für die ausgewählte Schnittstelle mit der **Neighbor ID** (Nachbar-ID) werden angezeigt.

Anzeigen der OSPFv3-Nachbarschaften mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

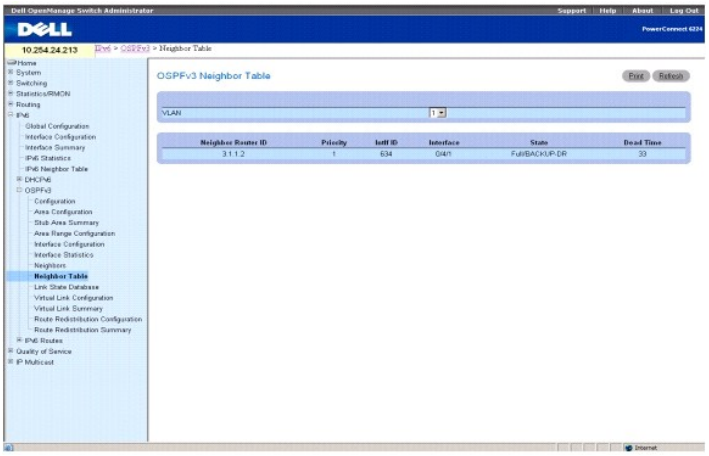
- OSPFv3 Commands (OSPFv3-Befehle)

OSPFv3-Nachbarschaftstabelle

Auf der Seite **OSPFv3 Neighbor Table** (OSPFv3-Nachbarschaftstabelle) können Sie die OSPF-Nachbarschaftstabelle anzeigen. Bei Angabe einer bestimmten Nachbar-ID werden ausführliche Informationen zu einem benachbarten Router angezeigt. Diese Tabelle wird nur angezeigt, wenn OSPF aktiviert ist.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ OSPFv3→ Neighbor Table (Nachbarschaftstabelle)**.

Abbildung 11-26. OSPFv3-Nachbarschaftstabelle



Die Seite **OSPFv3 Neighbor Table** (OSPFv3-Nachbarschaftstabelle) enthält folgende Felder:

Interface (Schnittstelle) – Wählt die Schnittstelle aus, für die Daten angezeigt oder konfiguriert werden sollen.

Neighbor Router ID (ID des benachbarten Routers) – Ein 32-Bit-Integer in Schreibweise mit Trennzeichen, das die benachbarte Schnittstelle darstellt.

Priority (Priorität) – Die Priorität, die dieser Nachbar im Algorithmus für die Auswahl des designierten Routers erhält. Der Wert 0 gibt an, dass der Nachbar nicht als designierter Router in diesem Netzwerk zur Verfügung steht.

IntIfID – Die Schnittstellen-ID, die der Nachbar über diese Verbindung in Hello-Paketen mitteilt.

Interface (Schnittstelle) – Der Steckplatz/Port, der den Nachbarschnittstellenindex angibt.

State (Status) – Der Status der Beziehung mit diesem Nachbarn.

Dead Time (Totzeit) – Die Zeit in Sekunden, seit das letzte Hello-Paket von Nachbarn empfangen wurde. Für Nachbarn mit einem Status kleiner oder gleich **Init** wird dieser Wert auf 0 gesetzt.

Anzeigen der OSPFv3-Nachbarschaftstabelle

1. Öffnen Sie die Seite **OSPFv3 Neighbor Table** (OSPFv3-Nachbarschaftstabelle).
2. Wählen Sie die Schnittstelle, die Sie anzeigen wollen, im Dropdown-Menü **Interface** (Schnittstelle).

   Die OSPF-Nachbarschaftstabelle für die ausgewählte Schnittstelle wird angezeigt.

Anzeigen der OSPFv3-Nachbarschaftstabelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

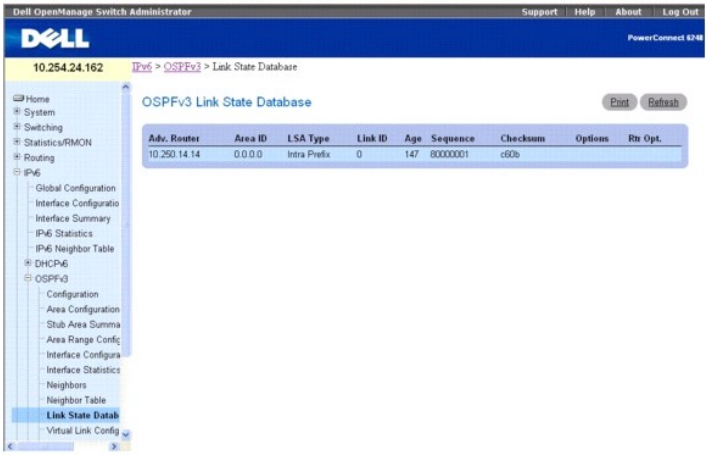
- OSPFv3 Commands (OSPFv3-Befehle)

OSPFv3-Verbindungsstatusdatenbank

Über die Seite **OSPFv3 Link State Database** (OSPFv3-Verbindungsstatusdatenbank) können Sie die Verbindungsstatusdatenbank anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ OSPFv3→ Link State Database (Verbindungsstatusdatenbank)**.

Abbildung 11-27. OSPFv3-Verbindungsstatusdatenbank



Die Seite **OSPFv3 Link State Database** (OSPFv3-Verbindungsstatusdatenbank) enthält folgende Felder:

Adv. Router – Ein 32-Bit-Integer in der Schreibweise mit Trennzeichen, das den Router im autonomen System (AS) eindeutig kennzeichnet. Die Router-ID wird auf der Seite "OSPFv3 Configuration" (OSPFv3-Konfiguration) gesetzt.

Area ID (Bereichs-ID) – Die ID eines OSPF-Bereichs, mit dem eine der Routerschnittstellen verbunden ist. Bei der Bereichs-ID handelt es sich um ein 32-Bit-Integer in der Schreibweise mit Trennzeichen, das den Bereich, mit dem eine Schnittstelle verbunden ist, eindeutig kennzeichnet.

LSA Type (LSA-Typ) – Format und Funktion einer LSA (Link-State Advertisement). Die Typen sind in RFC 2740, Abschnitt A.4 definiert. Es wird zwischen folgenden Typen unterschieden:

- Router-LSA
- Network-LSA
- Inter-Area-Prefix-LSA
- Inter-Area-Router-LSA
- AS-External-LSA
- Type-7-LSA
- Link-LSA
- Intra-Area-Prefix-LSA

Link ID (Link-ID) – Die Link-State-ID gibt den Teil der Routingdomäne an, der in der Mitteilung (Advertisement) beschrieben ist. Der Wert der LS-ID hängt vom LS-Typ der Mitteilung ab.

Age (Alter) – Die Zeit (in Sekunden), die seit dem ersten Senden der LSA vergangen ist.

Sequence (Sequenznummer) – In diesem Feld wird die Sequenznummer als ein 32-Bit-Integer mit Vorzeichen angegeben. Über dieses Feld werden alte und

mehrfach vorhandene LSAs ermittelt. Je höher die Sequenznummer, desto aktueller die LSA.

Checksum (Prüfsumme) – Über die Prüfsumme können fehlerhafte Daten in einer LSA ermittelt werden. Solche Fehler können beim Flooding (Fluten) einer LSA auftreten oder während sich eine LSA im Routerspeicher befindet. Dieses Feld enthält die Prüfsumme des gesamten LSA-Inhalts mit Ausnahme des Feldes, das das LS-Alter enthält.

Options (Optionen) – In diesem Feld des LSA-Headers werden die optionalen Funktionen angegeben, über die die LSA verfügt. Dies sind die möglichen Optionen:

- V6 – Wenn diese Option nicht markiert ist, wird die Verbindung von den IPv6-Weiterleitungsberechnungen ausgeschlossen.
- E – Gibt an, wie AS-external-LSAs geflutet werden
- MC – Gibt an, ob IP-Multicast-Datagramme entsprechend der Standardspezifikation weitergeleitet werden
- N – Gibt an, wie Typ-7-LSAs gehandhabt werden
- R – Zeigt an, ob der Urheber ein aktiver Router ist. Die Option R ist das Router-Bit. Wenn sie nicht markiert ist, können Routen, die den mitteilenden Knoten passieren, nicht berechnet werden.
- DC – Gibt an, wie das System angeforderte Verbindungen handhabt.

Rtr Opt. – Zeigt die routerspezifischen Optionen an.

Anzeigen der OSPFv3-Verbindungsstatusdatenbank mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

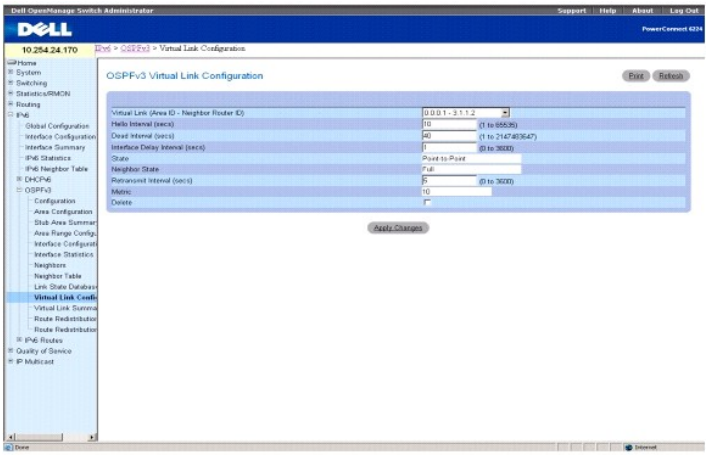
- OSPFv3 Commands (OSPFv3-Befehle)

Konfiguration virtueller OSPFv3-Verbindungen

Über die Seite **OSPFv3 Virtual Link Configuration** (Konfiguration virtueller OSPFv3-Verbindungen) können Sie eine neue virtuelle Verbindung definieren bzw. eine bereits vorhandene Verbindung konfigurieren. Damit diese Seite angezeigt wird, muss zunächst über die Seite "OSPFv3 Area Configuration" (OSPFv3-Bereichskonfiguration) ein gültiger OSPFv3-Bereich definiert werden.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ OSPFv3→ Virtual Link Configuration (Konfiguration einer virtuellen Verbindung)**.

Abbildung 11-28. Konfiguration einer virtuellen OSPFv3-Verbindung



Die Seite **OSPFv3 Virtual Link Configuration** (Konfiguration virtueller OSPFv3-Verbindungen) enthält folgende Felder:

Create New Virtual Link (Neue virtuelle Verbindung erstellen) – Wählen Sie im Dropdown-Menü diese Option aus, um eine neue virtuelle Verbindung zu definieren. Der Bereichsteil der ID der virtuellen Verbindung ist fest vorgegeben: Sie werden aufgefordert, die ID des benachbarten Routers in einer neuen Anzeige einzugeben.

Virtual Link (Area ID - Neighbor Router ID) (Virtuelle Verbindung (Bereichs-ID - ID des benachbarten Routers)) – Wählen Sie die virtuelle Verbindung aus, für die Daten angezeigt oder konfiguriert werden sollen. Sie besteht aus der Bereichs-ID und der ID des benachbarten Routers.

Hello Interval (secs) (Hello-Intervall) – Geben Sie das OSPF-Hello-Intervall (in Sekunden) für die angegebene Schnittstelle an. Dieser Parameter muss für alle Router, die mit einem Netzwerk verbunden sind, derselbe sein. Zulässig sind Werte zwischen 1 und 65535 Sekunden; der Standardwert ist 10 Sekunden.

Dead Interval (secs) (Totintervall) – Geben Sie das OSPF-Totintervall (in Sekunden) für die angegebene Schnittstelle an. Gibt an, wie lange ein Router auf das Eintreffen von Hello-Paketen eines benachbarten Routers wartet, bevor dieser als ausgefallen bezeichnet wird. Dieser Parameter muss für alle Router, die mit einem Netzwerk verbunden sind, derselbe sein. Er sollte ein Vielfaches des Hello-Intervalls sein (z. B 4). Zulässig sind Werte zwischen 1 und 2147483647; der Standardwert ist 40.

Interface Delay Interval (secs) (Verzögerungsintervall der Schnittstelle) – Geben Sie die OSPF-Verzögerung bei Statusübergängen für die angegebene Schnittstelle an. Gibt die geschätzte Zeit in Sekunden an, die die Übertragung eines LSU-Pakets über die ausgewählte Schnittstelle dauert. Zulässig sind Werte zwischen 1 und 3600 Sekunden (1 Stunde). Der Standardwert ist 1 Sekunde.

State (Status) – Der aktuelle Status der ausgewählten virtuellen Verbindung. Dabei kann es sich um eine der folgenden Statusangaben handeln:

- **Down** (Nicht in Betrieb) – Der ursprüngliche Status der Schnittstelle. In diesem Status haben die Lower-Level-Protokolle angegeben, dass die Schnittstelle nicht verwendet werden kann. Die Schnittstellenparameter werden in diesem Status auf ihre ursprünglichen Werte zurückgesetzt. Alle Schnittstellenzeitgeber sind deaktiviert, und der Schnittstelle sind keine Nachbarschaftsbeziehungen zugeordnet.
- **Waiting** (Wartestatus) – Der Router versucht, den designierten (Backup-)Router durch Überwachung der empfangenen Hello-Pakete zu ermitteln. Dabei darf der Router keinen designierten Backup-Router oder designierten Router bestimmen, bevor der Wartestatus nicht wieder verlassen wird. Dadurch werden unnötige Änderungen des designierten (Backup-)Routers verhindert.
- **Poin-to-Point** (Punkt-zu-Punkt) – Die Schnittstelle ist funktionsfähig und mit der virtuellen Verbindung verbunden. Wenn der Router in diesen Status wechselt, versucht er, eine Beziehung zu dem benachbarten Router herzustellen. Dazu werden an den Nachbarn Hello-Pakete in Sekundenintervallen gesendet, deren Anzahl über das Feld **Hello Interval** (Hello-Intervall) vorgegeben ist.
- **Designated Router** (Designierter Router) – Dieser Router ist selbst der designierte Router im verbundenen Netzwerk. Zu allen anderen Routern, die mit dem Netzwerk verbunden sind, werden Nachbarschaftsbeziehungen aufgebaut. Der Router muss außerdem eine Network-LSA für den Netzwerkknoten senden. Diese Network-LSA enthält Verbindungen zu allen Routern (einschließlich des designierten Routers), die mit dem Netzwerk verbunden sind.
- **Backup Designated Router** (Designierter Backup-Router) – Dieser Router ist selbst der designierte Backup-Router im verbundenen Netzwerk. Fällt der aktive designierte Router aus, wird dieser Router zum designierten Router. Er baut Nachbarschaftsbeziehungen zu allen anderen Routern auf, die mit dem Netzwerk verbunden sind. Die Aufgaben des designierten Backup-Routers beim Flooding (Fluten) unterscheiden sich geringfügig von denen des designierten Routers.
- **Other Designated Router** (Anderer designierter Router) – Die Schnittstelle ist mit einem Broadcast- oder NBMA-Netzwerk verbunden, in dem andere Router als designierter Router und Backup-Router festgelegt wurden. Der Router versucht, Nachbarschaftsbeziehungen zum designierten Router und zum designierten Backup-Router aufzubauen.

Neighbor State (Nachbarschaftsstatus) – Der Status der virtuellen Beziehung zum benachbarten Router.

Retransmit Interval (Rückübertragungsintervall) – Geben Sie das OSPF-Rückübertragungsintervall für die angegebene Schnittstelle an. Dies ist die Zeit in Sekunden zwischen LSAs für Nachbarschaftsbeziehungen (Adjacencies), die zu dieser Routerschnittstelle gehören. Dieser Wert wird auch bei der Rückübertragung von Datenbankbeschreibungen und LS-Anforderungspaketen verwendet. Zulässig sind Werte zwischen 1 und 3600 Sekunden (1 Stunde). Der Standardwert ist 5 Sekunden.

Metric (Metrik) – Die für die virtuelle Verbindung verwendete Metrik.

Delete (Löschen) – Löscht die angegebene virtuelle Verbindung aus der Routerkonfiguration.

Erstellen einer neuen virtuellen Verbindung

1. Öffnen Sie die Seite **OSPFv3 Virtual Link Configuration** (Konfiguration virtueller OSPFv3-Verbindungen).
2. Wählen Sie über das Dropdown-Menü **Create New Virtual Link** (Neue virtuelle Verbindung erstellen) diese Option aus, um eine neue virtuelle Verbindung zu definieren.
3. Geben Sie die **Neighbor Router ID** (ID des benachbarten Routers) ein.
4. Klicken Sie auf **Create** (Erstellen).

   Die neue Verbindung wird erstellt, und Sie kehren wieder zur Seite **Virtual Link Configuration** (Konfiguration einer virtuellen Verbindung) zurück.

Konfigurieren einer virtuellen Verbindung

1. Öffnen Sie die Seite **OSPFv3 Virtual Link Configuration** (Konfiguration virtueller OSPFv3-Verbindungen).
2. Wählen Sie die virtuelle Verbindung aus, die konfiguriert werden soll.
3. Ändern Sie die übrigen Felder je nach Bedarf.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).
5. Die virtuelle Verbindung wird für OSPFv3 konfiguriert und das Gerät aktualisiert.

Konfigurieren einer virtuellen OSPFv3-Verbindung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

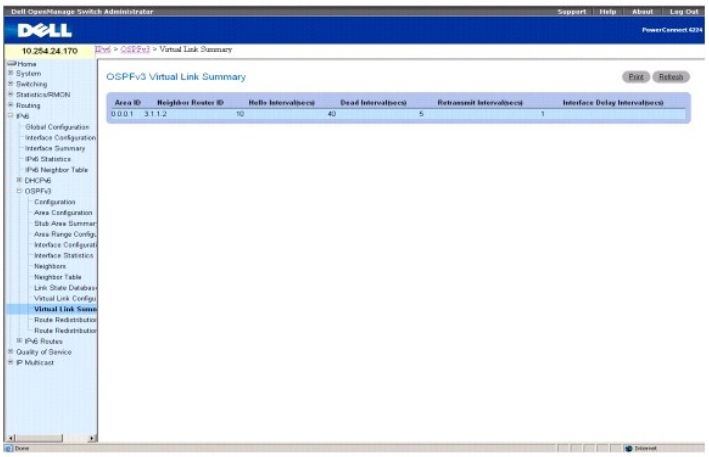
- OSPFv3 Commands (OSPFv3-Befehle)

Zusammenfassende Daten zu virtuellen OSPFv3-Verbindungen

Über die Seite **OSPFv3 Virtual Link Summary** (Zusammenfassende Daten zu virtuellen OSPFv3-Verbindungen) können Sie Daten zu virtuellen Verbindungen nach Bereichs-ID und der ID des benachbarten Routers anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ OSPFv3→ Virtual Link Summary (Zusammenfassende Daten zu virtuellen Verbindungen)**.

Abbildung 11-29. Zusammenfassende Daten zu virtuellen OSPFv3-Verbindungen



Die Seite **OSPFv3 Virtual Link Summary** (Zusammenfassende Daten zu virtuellen OSPFv3-Verbindungen) enthält folgende Felder:

Area ID (Bereichs-ID) – Die Bereichs-ID, Teil der Kennung der virtuellen Verbindung, zu der Daten angezeigt werden sollen. Die Bereichs-ID und die ID des benachbarten Routers zusammen kennzeichnen eine virtuelle Verbindung.

Neighbor Router ID (ID des benachbarten Routers) – Die ID des benachbarten Routers, Teil der Kennung der virtuellen Verbindung. Virtuelle Verbindungen können zwischen jeweils zwei ABR-Routern konfiguriert werden, die über Schnittstellen zu einem gemeinsamen Bereich (bei dem es sich nicht um eine Backbone Area handelt) verfügen.

Hello Interval (secs) (Hello-Intervall) – Das OSPF-Hello-Intervall (in Sekunden) für eine virtuelle Verbindung. Dieser Wert muss für alle Router, die mit einem Netzwerk verbunden sind, derselbe sein.

Dead Interval (secs) (Totintervall) – Das OSPF-Totintervall (in Sekunden) für eine virtuelle Verbindung. Gibt an, wie lange ein Router auf das Eintreffen von Hello-Paketen eines benachbarten Routers wartet, bevor dieser als ausgefallen bezeichnet wird. Dieser Parameter muss für alle Router, die mit einem gemeinsamen Netzwerk verbunden sind, derselbe sein und ein Vielfaches des Hello-Intervalls darstellen (z. B. 4).

Retransmit Interval (secs) (Rückübertragungsintervall) – Das OSPF-Rückübertragungsintervall (in Sekunden) für eine virtuelle Verbindung. Gibt die Zeit in Sekunden zwischen LSAs für Nachbarschaftsbeziehungen (Adjacencies) an, die zu dieser Routerschnittstelle gehören. Dieser Wert wird auch bei der Rückübertragung von Datenbankbeschreibungen und LS-Anforderungspaketen verwendet.

Interface Delay Interval (secs) (Verzögerungsintervall der Schnittstelle) – Die OSPF-Verzögerung bei Statusübergängen (in Sekunden) für die virtuelle Verbindung. Gibt die geschätzte Zeit in Sekunden an, die die Übertragung eines LSU-Pakets über diese Schnittstelle dauert.

Anzeigen der zusammenfassenden Daten zu virtuellen OSPFv3-Verbindungen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

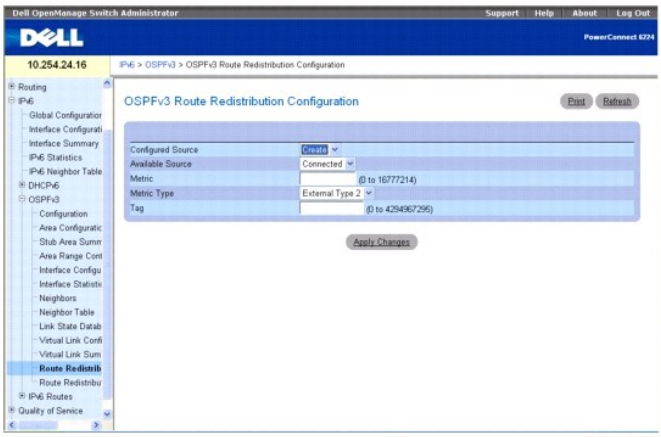
- OSPFv3 Commands (OSPFv3-Befehle)

Konfiguration der OSPFv3-Routenumverteilung

Über die Seite **OSPFv3 Route Redistribution Configuration** (Konfiguration der OSPFv3-Routenumverteilung) können Sie die Routenumverteilung konfigurieren.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ OSPFv3→ Route Redistribution Configuration (Konfiguration der Routerumverteilung)**.

Abbildung 11-30. Konfiguration der OSPFv3-Routenumverteilung



Die Seite **OSPFv3 Route Redistribution Configuration** (Konfiguration der OSPFv3-Routenumverteilung) enthält folgende Felder:

Configured Source (Konfigurierte Quelle) – Dieses Dropdown-Menü ist ein dynamisches Auswahlfeld, das immer nur die Quellrouten enthält, die für die OSPF-Umverteilung konfiguriert wurden. Die erste Option ist **Create** (Erstellen), über die Sie unter den verfügbaren Routen eine weitere Quellroute konfigurieren können. Mögliche Werte sind "Static" (Statisch), "Connected" (Verbunden) und "Create" (Erstellen).

Available Source (Verfügbare Quelle) – Dieses Dropdown-Menü ist ein dynamisches Auswahlfeld, das immer nur die Quellrouten enthält, die noch nicht für die OSPF-Umverteilung konfiguriert wurden. Dieses Menü ist nur verfügbar, wenn **Create** (Erstellen) für **Configured Source** (Konfigurierte Quelle) ausgewählt wurde. Mögliche Werte sind "Static" (Statisch) und "Connected" (Verbunden).

Metric (Metrik) – Legt den Wert fest, der als Metrik für umverteilte Routen verwendet werden soll. In diesem Feld wird die Metrik angezeigt, wenn die Quelle vorab konfiguriert wurde und geändert werden kann. Zulässige Werte sind 0 bis 16777214.

Metric Type (Metriktyp) – Legt den OSPF-Metriktyp der umverteilten Routen fest.

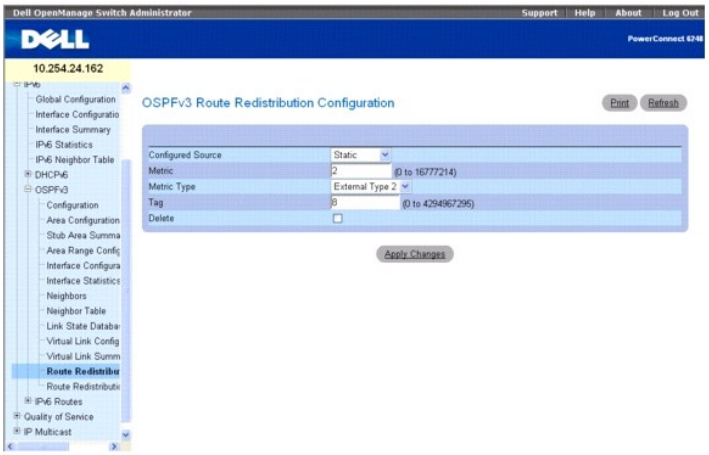
Tag – Setzt das Tag-Feld in umverteilten Routen. Wurde die Quelle vorab konfiguriert, wird in diesem Feld der Tag-Wert angezeigt; andernfalls enthält das Feld den Wert 0. Zulässige Werte sind 0 bis 4294967295.

Konfigurieren der OSPFv3-Routenumverteilung

1. Öffnen Sie die Seite **OSPFv3 Route Redistribution Configuration** (Konfiguration der OSPFv3-Routenumverteilung).

2. Soll eine neue konfigurierte Quelle eingerichtet werden, geben Sie **Create** (Erstellen) an, soll eine vorhandene konfigurierte Quelle geändert werden, geben Sie "Connected" (Verbunden) oder "Static" (Statisch) ein.

Abbildung 11-31. Konfiguration der OSPFv3-Routenumverteilung – Konfigurierte Quelle



3. Konfigurieren bzw. ändern Sie die restlichen Felder nach Bedarf.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die ausgewählte Routenumverteilung wird für OSPFv3 konfiguriert und das Gerät aktualisiert.

Konfigurieren der OSPFv3-Routenumverteilung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

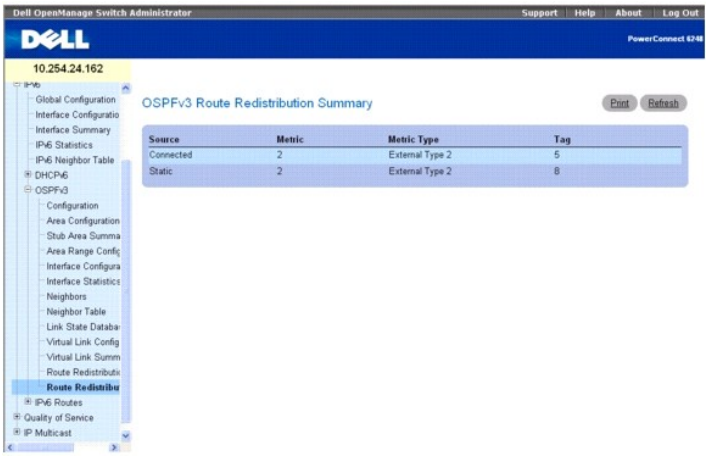
- OSPFv3 Commands (OSPFv3-Befehle)

Zusammenfassende Daten zur OSPFv3-Routenumverteilung

Über die Seite **OSPFv3 Route Redistribution Summary** (Zusammenfassende Daten zur OSPFv3-Routenumverteilung) können Sie die Routenumverteilung nach Quelle anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ OSPFv3→ Route Redistribution Summary (Zusammenfassende Daten zur Routenumverteilung)**.

Abbildung 11-32. Zusammenfassende Daten zur OSPFv3-Routenumverteilung



Die Seite **OSPFv3 Route Redistribution Summary** (Zusammenfassende Daten zur OSPFv3-Routenumverteilung) enthält folgende Felder:

Source (Quelle) – Die Quellroute, die von OSPF umverteilt werden soll.

Metric (Metrik) – Der Metrikwert der umverteilten Routen für die Quellroute. Wird kein Wert konfiguriert, wird in diesem Feld **Unconfigured** (Nicht konfiguriert) angezeigt.

Metric Type (Metriktyp) – Der OSPF-Metriktyp der umverteilten Routen.

Tag – Das Tag-Feld in umverteilten Routen. Wurde die Quelle vorab konfiguriert, wird in diesem Feld der Tag-Wert angezeigt; andernfalls enthält das Feld den Wert 0.

Anzeigen der zusammenfassenden Daten zur OSPFv3-Routenumverteilung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- OSPFv3 Commands (OSPFv3-Befehle)

IPv6-Routen

Die Menüseite **IPv6 Routes** enthält Links zu Webseiten, auf denen IPv6-Routenparameter und -daten definiert und angezeigt werden können. Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ IPv6 Routes (IPv6-Routen)**. Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

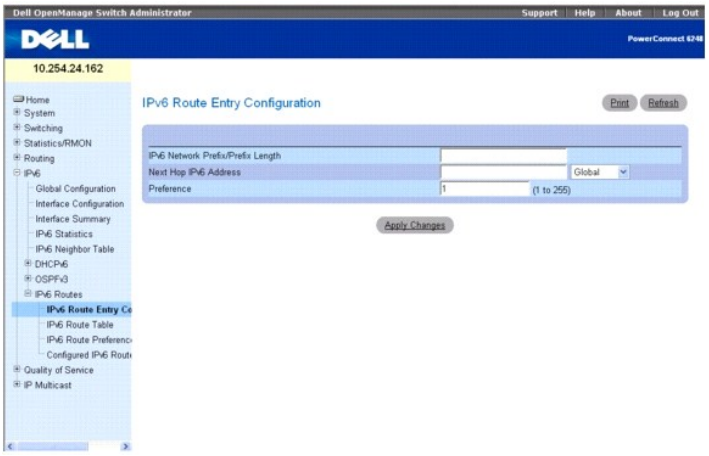
- Konfiguration von IPv6-Routeneinträgen
- IPv6-Routentabelle
- IPv6-Routenbevorzugung
- Konfigurierte IPv6-Routen

Konfiguration von IPv6-Routeneinträgen

Über die Seite **IPv6 Route Entry Configuration** (Konfiguration von IPv6-Routeneinträgen) können Sie die Angaben für IPv6-Routen konfigurieren.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ IPv6 Routes→ IPv6 Route Entry Configuration (Konfiguration von IPv6-Routeneinträgen)**.

Abbildung 11-33. Konfiguration von IPv6-Routeneinträgen



Die Seite **IPv6 Route Entry Configuration** (Konfiguration von IPv6-Routeneinträgen) enthält folgende Felder:

IPv6 Network Prefix/PrefixLength (IPv6-Netzwerk - Präfix/Präfixlänge) – Geben Sie eine gültige IPv6-Netzwerkadresse und ein gültiges Präfix ein.

Next Hop IPv6 Address (IPv6-Adresse des nächsten Hops) – Geben Sie eine IPv6-Adresse für den nächsten Hop ein. Wird hier eine Link-Local-IPv6-Adresse angegeben, müssen Sie auch die Schnittstelle für die Link-Local-IPv6-Adresse des nächsten Hops angeben. Wählen Sie für diese Adresse im Dropdown-Menü **Global** oder **Link-Local** aus.

Preference (Bevorzugung) – Geben Sie für die Route einen Bevorzugungswert ein. Zulässige Werte sind 1 bis 255; der Standardwert ist 1.

Konfigurieren eines IPv6-Routeneintrags

1. Öffnen Sie die Seite **IPv6 Route Entry Configuration** (Konfiguration von IPv6-Routeneinträgen).
2. Ändern Sie die Felder je nach Bedarf.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Routeneintrag wird für IPv6 konfiguriert und das Gerät entsprechend aktualisiert.

Konfigurieren von Routeneinträge mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

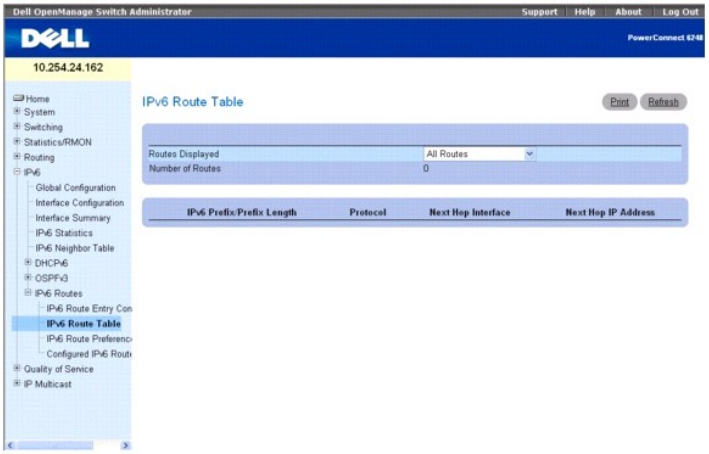
- IPv6 Routing Commands (IPv6-Routingbefehle)

IPv6-Routentabelle

Über die Seite **IPv6 Route Table** (IPv6-Routentabelle) können Sie alle aktiven IPv6-Routen und deren Einstellungen anzeigen.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ IPv6 Routes→ IPv6 Route Table (IPv6-Routentabelle)**.

Abbildung 11-34. IPv6-Routentabelle



Die Seite **IPv6 Route Table** (IPv6-Routentabelle) enthält folgende Felder:

Routes Displayed (Angezeigte Routen) – In diesem Dropdown-Menü können Sie angeben, ob die konfigurierten Routen, die vorteilhaftesten Routen oder alle Routen angezeigt werden sollen.

Number of Routes (Anzahl Routen) – Zeigt in der Routentabelle die Gesamtzahl der aktiven/vorteilhaftesten Routen für den ausgewählten Routentyp an.

IPv6 Prefix/Prefix Length (IPv6-Präfix/Präfixlänge) – Zeigt das Netzwerkpräfix und die Präfixlänge für die aktive Route an.

Protocol (Protokoll) – Zeigt den Protokolltyp der aktiven Route an.

Next Hop Interface (Nächste Hopschnittstelle) – Zeigt die Schnittstelle an, über die die Route aktiv ist.

Next Hop IP Address (IP-Adresse des nächsten Hops) – Zeigt die IPv6-Adresse des nächsten Hops für die aktive Route an.

Anzeigen der IPv6-Routentabelle

1. Öffnen Sie die Seite **IPv6 Router Table** (IPv6-Routentabelle).
2. Wählen Sie im Feld **Routes Displayed** (Angezeigte Routen) den Routentyp aus, der angezeigt werden soll.

   Die ausgewählten Routen werden angezeigt.

Anzeigen der IPv6-Routentabelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

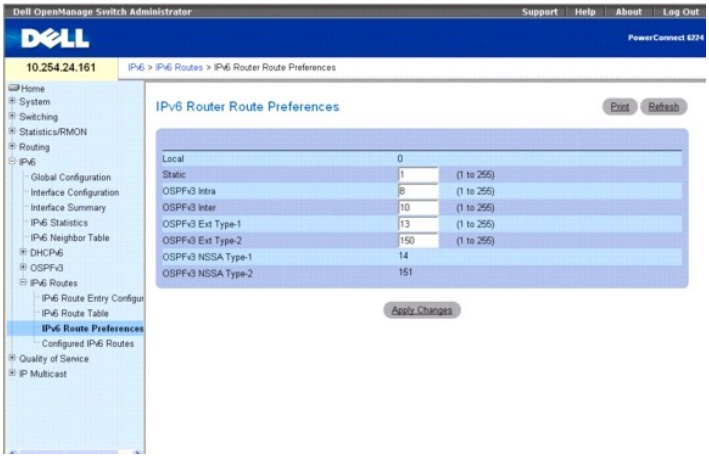
- IPv6 Routing Commands (IPv6-Routingbefehle)

IPv6-Routenbevorzugung

Über die Seite **IPv6 Route Preferences** (IPv6-Routenbevorzugung) können Sie für jedes Protokoll eine Standardbevorzugung konfigurieren. Hier handelt es sich um wahlfreie Werte zwischen 1 und 255, die unabhängig von der Routenmetrik sind. Die meisten Protokolle ermitteln den kürzesten bekannten Pfad unabhängig von allen anderen Protokollen über eine Routenmetrik. Die vorteilhafteste Route zu einem Ziel wird über die Auswahl der Route mit dem niedrigsten Bevorzugungswert ausgewählt. Gibt es mehrere Routen zu einem Ziel, wird die bevorzugte Route anhand des Bevorzugungswertes ausgewählt. Gibt es auch dann noch die Wahl zwischen mehreren Routen, wird die Route mit dem vorteilhaftesten Metrikwert ausgewählt. Um Probleme mit nicht übereinstimmenden Metrikwerten zu verhindern, müsse Sie für jedes Protokoll einen eigenen Bevorzugungswert angeben.

Um diese Seite anzuzeigen, klicken Sie in der Strukturansicht auf **IPv6→ IPv6 Routes→ IPv6 Route Preferences (IPv6-Routenbevorzugungen)**.

Abbildung 11-35. IPv6-Routenbevorzugungen



Die Seite **IPv6 Route Preferences** (IPv6-Routenbevorzugungen) enthält die nachstehend aufgeführten Felder. In allen Fällen gibt der niedrigste Wert die höchste Bevorzugung an.

Local (Lokal) – Zeigt die lokale Bevorzugung an, die nicht geändert werden kann. Der Wert ist 0, der höchste Wert für die Bevorzugung.

Static (Statisch) – Der Bevorzugungswert im Router für statische Routen. Der Standardwert ist 1, mögliche Werte sind 1 bis 255.

OSPFv3 Intra – Der routeninterne OSPFv3-Bevorzugungswert im Router. Der Standardwert ist 8, mögliche Werte sind 1 bis 255. Die OSPFv3-Spezifikation gibt vor, dass über OSPFv3 mitgeteilte Routen in der folgenden Reihenfolge bevorzugt werden müssen: intra < inter < Type-1 < Type-2.

OSPFv3 Inter – Der routenübergreifende OSPFv3-Bevorzugungswert im Router. Der Standardwert ist 10, mögliche Werte sind 1 bis 255. Die OSPFv3-Spezifikation gibt vor, dass über OSPFv3 mitgeteilte Routen in der folgenden Reihenfolge bevorzugt werden müssen: intra < inter < Type-1 < Type-2.

OSPFv3 Type-1 – Der OSPFv3-Bevorzugungswert im Router für Type-1-Routen. Der Standardwert ist 13, mögliche Werte sind 1 bis 255. Die OSPFv3-Spezifikation gibt vor, dass über OSPFv3 mitgeteilte Routen in der folgenden Reihenfolge bevorzugt werden müssen: intra < inter < Type-1 < Type-2.

OSPFv3 Type-2 – Der OSPFv3-Bevorzugungswert im Router für Type-2-Routen. Der Standardwert ist 150, mögliche Werte sind 1 bis 255. Die OSPFv3-Spezifikation gibt vor, dass über OSPFv3 mitgeteilte Routen in der folgenden Reihenfolge bevorzugt werden müssen: intra < inter < Type-1 < Type-2.

OSPFv3 NSSA Type-1 – Der OSPFv3-Bevorzugungswert im Router für NSSA-Type-1-Routen.

OSPFv3 NSSA Type-2 – Der OSPFv3-Bevorzugungswert im Router für NSSA-Type-2-Routen.

Konfigurieren von IPv6-Routenbevorzugungn

1. Öffnen Sie die Seite **IPv6 Router Preferences** (IPv6-Routenbevorzugungen).
2. Konfigurieren Sie für jedes Protokoll die Standardbevorzugung.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Routenbevorzugung wird für IPv6 konfiguriert und das Gerät entsprechend aktualisiert.

Konfigurieren der IPv6-Routenbevorzugung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

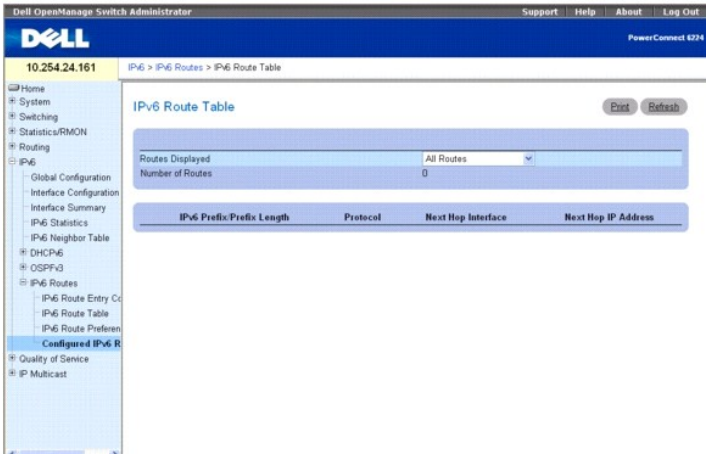
- IPv6 Routing Commands (IPv6-Routingbefehle)

Konfigurierte IPv6-Routen

Über die Seite **Configured IPv6 Routes** (Konfigurierte IPv6-Routen) können Sie ausgewählte IPv6-Routen anzeigen.

Um diese Seite anzuzeigen, klicken Sie auf **IPv6→ IPv6 Routes→ Configured IPv6 Routes (Konfigurierte IPv6-Routen)**.

Abbildung 11-36. Konfigurierte IPv6-Routen



Die Seite **Configured IPv6 Routes** (Konfigurierte IPv6-Routen) enthält folgende Felder:

Routes Displayed (Angezeigte Routen) – Geben Sie an, ob die konfigurierten Routen, die vorteilhaftesten Routen oder alle Routen angezeigt werden sollen.

Wenn die Option Configured Routes (Konfigurierte Routen) ausgewählt ist, werden folgende Felder angezeigt:

IPv6 Prefix/Prefix Length (IPv6-Präfix/Präfixlänge) – Zeigt das Netzwerkpräfix und die Präfixlänge für die konfigurierte Route an.

Next Hop IP (IP-Adresse des nächsten Hops) – Zeigt die IPv6-Adresse des nächsten Hops für die konfigurierte Route an.

Next Hop Interface (Nächste Hopschnittstelle) – Zeigt die nächste Hopschnittstelle für die konfigurierte Route an.

Preference (Bevorzugung) – Zeigt den für die konfigurierte Route definierten Bevorzugungswert an.

Delete (Löschen) – Markieren Sie dieses Kontrollkästchen und klicken Sie anschließend auf "Refresh" (Aktualisieren), um die angezeigte Route zu löschen.

Wenn die Optionen "Best Routes" (Beste Routen) oder "All Routes" (Alle Routen) ausgewählt sind, werden folgende Felder angezeigt:

Number of Routes (Anzahl der Routen) – Zeigt die Anzahl der "Best Routes" (besten Routen bzw. "All Routes" (aller Routen) an.

IPv6 Prefix/Prefix Length (IPv6-Präfix/Präfixlänge) – Zeigt das Netzwerkpräfix und die Präfixlänge für die konfigurierte Route an.

Protocol (Protokoll) – Zeigt das für die konfigurierten Routen verwendete Protokoll an.

Next Hop Interface (Nächste Hopschnittstelle) – Zeigt die nächste Hopschnittstelle für die konfigurierte Route an.

Next Hop IP Address (IP-Adresse des nächsten Hops) – Zeigt die IPv6-Adresse des nächsten Hops für die konfigurierte Route an.

Anzeigen von IPv6-Routen

1. Öffnen Sie die Seite **Configured IPv6-Routes** (Konfigurierte IPv6-Routen).
2. Wählen Sie über das Dropdown-Menü **Routes Displayed** (Angezeigte Routen) die Routen aus, die angezeigt werden sollen.

   Die ausgewählten Routen und ihre Konfigurationsdaten werden angezeigt.

Anzeigen der IPv6-Routen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- IPv6 Routing Commands (IPv6-Routingbefehle)

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Konfigurieren von Quality of Service (QoS)

Benutzerhandbuch für die Dell™ PowerConnect™ 6200-Reihe

- Quality of Service-Überblick
- Konfigurieren von Differentiated Services
- Class of Service

In diesem Abschnitt finden Sie einen Überblick über Quality of Service (QoS) und Erläuterungen der QoS-Funktionen, die auf der Menüseite "Quality of Service" unter "Differentiated Services" und "Class of Service" zur Verfügung stehen.

Quality of Service-Überblick

In einem typischen Switch arbeitet jeder physikalische Port eine oder mehrere Warteschlangen für die Übertragung von Paketen im angeschlossenen Netzwerk ab. Mehrere Warteschlangen pro Port werden häufig vorgesehen, um Paketen Prioritäten auf der Basis von benutzerdefinierten Kriterien zuzuweisen. Wenn ein Paket in der Warteschlange eines Ports auf die Übertragung wartet, hängt die Geschwindigkeit der Abarbeitung von der Konfiguration der Warteschlange und möglicherweise vom Verkehrsaufkommen in den anderen Warteschlangen des Ports ab. Falls eine Verzögerung unabdingbar ist, verbleiben die Pakete so lange in der Warteschlange, bis der Scheduler die Warteschlange für die Übertragung freigibt. Wenn die Warteschlangen voll werden, können keine Pakete mehr vorgehalten werden und werden vom Switch verworfen.

QoS ist ein Mittel zur konsistenten, vorhersehbaren Datenübertragung, indem zwischen Paketen unterschieden wird, für die strikte zeitliche Anforderungen gelten, und solchen, die verzögerungstoleranter sind. In einem QoS-fähigen Netzwerk erhalten Pakete mit strengen zeitlichen Vorgaben eine "Sonderbehandlung". Dafür müssen jedoch alle Elemente des Netzwerks QoS-fähig sein. Schon ein einziger Knoten ohne QoS-Kapazität führt im Netzwerkpfad zu Beeinträchtigungen und kompromitiert den gesamten Paketfluss.

Klicken Sie in der Strukturansicht auf **Quality of Service,** um die Quality of Service-Menüseite anzuzeigen. Die beiden QoS-Typen stehen auf dieser Menüseite als Links zur Verfügung. Es handelt sich dabei um folgende Links:

- Konfigurieren von Differentiated Services
- Class of Service

Konfigurieren von Differentiated Services

DiffServ-Überblick

Das QoS-Funktionsmerkmal enthält Unterstützung für Differentiated Services (DiffServ), die es ermöglicht, den Datenverkehr in Datenströme einzuteilen und eine bestimmte QoS-Behandlung gemäß eines festgelegten Verhaltens auf Hop-Basis zuzuweisen.

IP-basierte Standardnetzwerke sind für einen Best Effort-Datentransport ausgelegt. Best Effort bedeutet, dass das Netzwerk die Daten zeitgerecht überträgt, aber dass die Übertragung nicht garantiert wird. In Überlastungszeiten können Pakete verzögert oder nur sporadisch gesendet bzw. verworfen werden. Bei typischen Internetanwendungen wie E-Mail und Dateiübertragungen ist eine geringfügige Leistungseinbuße akzeptabel und wird in vielen Fällen nicht bemerkt. Im Gegensatz dazu wirken sich solche Leistungseinbußen negativ auf Anwendungen mit hohen zeitlichen Anforderungen wie Sprache oder Multimedia aus.

Definieren von DiffServ

Zur Verwendung von DiffServ für QoS muss zunächst auf die Webseiten zugegriffen werden, die auf der Menüseite **Differentiated Services** verfügbar sind, um die folgenden Kategorien und deren Kriterien zu definieren:

1. Class: Erstellen von Klassen und Definieren von Klassenkriterien
2. Policy: Erstellen von Richtlinien, Verknüpfen von Klassen mit Richtlinien und Definieren von Richtlinienparametern
3. Service: Hinzufügen einer Richtlinie zu einer Schnittstelle für eingehenden Datenverkehr

Pakete werden gemäß vorgegebener Kriterien klassifiziert und verarbeitet. Das Klassifizierungskriterium wird über eine Klasse definiert. Die Verarbeitung wird über die Attribute einer Richtlinie festgelegt. Richtlinienattribute können auf Instanzbasis für die einzelnen Klassen definiert werden. Diese Attribute werden dann angewendet, wenn eine Übereinstimmung auftritt. Eine Richtlinie kann mehrere Klassen umfassen. Wenn die Richtlinie aktiv ist, hängen die durchgeführten Vorgänge davon ab, welche Klasse dem jeweiligen Paket entspricht.

Die Paketverarbeitung beginnt mit der Prüfung, ob passende Klassenkriterien für ein Paket vorhanden sind. Eine Richtlinie wird dann auf ein Paket angewendet, wenn eine passende Klasse innerhalb dieser Richtlinie gefunden wird.

Die Menüseite **Differentiated Services** enthält Links zu den diversen Diffserv-Konfigurations- und -Anzeigefunktionen.

Um die Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Quality of Service**→ **Differentiated Services**. Die Differentiated Services-Menüseite enthält Links zu den folgenden Funktionen:

- Diffserv-Konfiguration
- Klassenkonfiguration

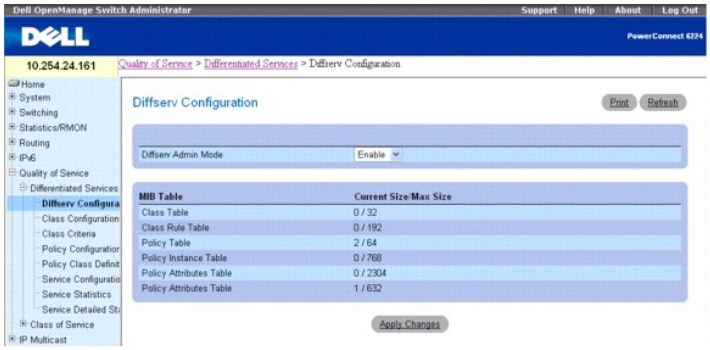
- Klassenkriterien
- Richtlinienkonfiguration
- Definition von Richtlinienklassen
- Dienstekonfiguration
- Detaillierte Dienststatistiken

Diffserv-Konfiguration

Verwenden Sie die Seite **Diffserv Configuration** (Diffserv-Konfiguration) zur Anzeige der allgemeinen Statusinformationen der Diffserv-Gruppen. Diese enthalten die aktuelle Einstellung für den Verwaltungsmodus und die maximale Anzahl der Zeilen in jeder der zugriffsbeschränkten DiffServ-MIB-Haupttabellen.

Zur Anzeige der Seite klicken Sie in der Strukturansicht auf **Quality of Service→ Differentiated Services→ Diffserv Configuration (Diffserv-Konfiguration)**.

Abbildung 12-1. Diffserv-Konfiguration



Die Seite **Diffserv Configuration** (Diffserv-Konfiguration) enthält folgende Felder:

Diffserv Admin Mode - Zum Ein- und Ausschalten des Verwaltungsmodus. Wenn er deaktiviert ist, wird die Diffserv-Konfiguration beibehalten und kann geändert werden, ist aber nicht aktiv. Ist er aktiviert, sind die Differentiated Services aktiv.

MIB-Tabelle

Class Table (Klassentabelle) – Zeigt die aktuelle und maximale Anzahl der Zeilen in der Klassentabelle an.

Class Rule Table (Klassenregeltabelle) – Zeigt die aktuelle und maximale Anzahl der Zeilen in der Klassenregeltabelle an.

Policy Table (Richtlinientabelle) – Zeigt die aktuelle und maximale Anzahl der Zeilen in der Richtlinientabelle an.

Policy Instance Table (Richtlinieninstanztabelle) – Zeigt die aktuelle und maximale Anzahl der Zeilen in der Richtlinieninstanztabelle an.

Policy Attributes Table (Richtlinienattributtabelle) – Zeigt die aktuelle und maximale Anzahl der Zeilen in der Richtlinienattributtabelle an.

Service Table (Dienstetabelle) – Zeigt die aktuelle und maximale Anzahl der Zeilen in der Dienstetabelle an.

Ändern des Diffserv-Verwaltungsmodus

1. Öffnen Sie die Seite **Diffserv Configuration** (Diffserv-Konfiguration).
2. Schalten Sie den **Diffserv Admin Mode** (Diffserv-Verwaltungsmodus) ein oder aus, indem Sie "Enable" (Aktivieren) bzw. "Disable" (Deaktivieren) aus dem Dropdown-Menü wählen.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Diffser-Verwaltungsmodus wird geändert und das Gerät aktualisiert.

Anzeigen von MIB-Tabellen mithilfe der CLI-Befehle

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

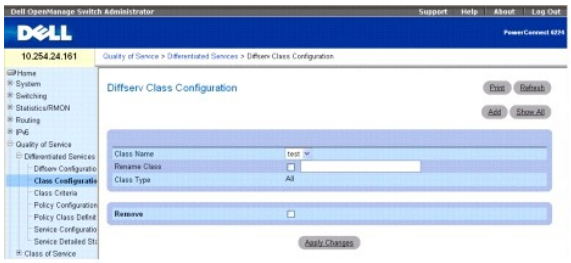
- QoS Commands (QoS-Befehle)

Klassenkonfiguration

Verwenden Sie die Seite **Diffserv Class Configuration** (Diffserv-Klassenkonfiguration), um einen neuen Diffserv-Klassennamen hinzuzufügen, oder eine vorhandene Klasse umzubenennen oder zu löschen.

Zur Anzeige der Seite klicken Sie in der Strukturansicht auf **Quality of Service**→ **Differentiated Services**→ **Class Configuration (Klassenkonfiguration)**.

Abbildung 12-2. Diffserv-Klassenkonfiguration



Die Seite **Diffserv Class Configuration** (Diffserv-Klassenkonfiguration) enthält folgende Felder:

Class Name (Klassennamen) – Zur Auswahl eines Klassennamens, der umbenannt oder gelöscht werden soll. Klicken Sie auf **Add** (Hinzufügen), um einen neuen Klassennamen anzulegen.

Rename Class (Klasse umbenennen) – Benennt die angezeigte Klasse um, wenn das Kontrollkästchen aktiviert ist und ein neuer Name eingegeben wird.

Class Type (Klassentyp) – Listet alle Klassentypen auf. Die Hardware unterstützt aktuell nur den **Class Type**-Wert **All** (Alle).

All (Alle) – Für eine Paketentsprechung müssen alle verschiedenen, für die Klasse definierten Vergleichskriterien übereinstimmen. **All** (Alle) entspricht der logischen **UND**-Verknüpfung aller Vergleichskriterien.

Remove (Löschen) – Löscht den angezeigten Klassennamen, wenn es aktiviert und **Apply Changes** (Änderungen übernehmen) angeklickt ist.

Umbenennen einer Klassenkonfiguration

1. Öffnen Sie die Seite **Class Configuration** (Klassenkonfiguration).
2. Wählen Sie den zu ändernden Klassennamen aus dem Dropdown-Menü **Class Name** (Klassenname).
3. Aktivieren Sie das Kontrollkästchen **Rename Class** (Klasse umbenennen), und geben Sie den neuen Namen in das Feld daneben ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

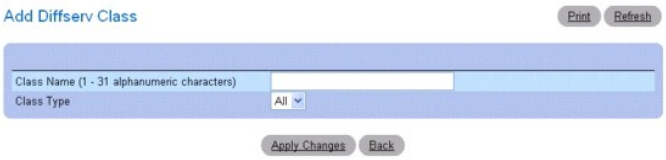
   Die Klassenkonfiguration wird umbenannt und das Gerät aktualisiert.

Hinzufügen einer Diffserv-Klassenkonfiguration

1. Öffnen Sie die Seite **Class Configuration** (Klassenkonfiguration).
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add Diffserv Class** (Diffserv-Klasse hinzufügen) wird angezeigt.

Abbildung 12-3. Diffserv-Klasse hinzufügen



3. Geben Sie den neuen Namen in das Feld **Class Name** (Klassenname) ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der **Class Name** (Klassenname) wird hinzugefügt und das Gerät aktualisiert.

Entfernen einer Klassenkonfiguration

1. Öffnen Sie die Seite **Class Configuration** (Klassenkonfiguration).
2. Wählen Sie den zu löschenden Klassennamen aus dem Dropdown-Menü **Class Name** (Klassenname).
3. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

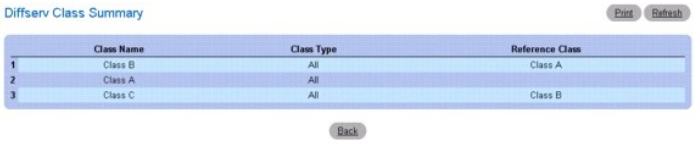
   Die zugehörige Klassenkonfiguration wird entfernt und das Gerät aktualisiert.

Anzeigen von Klassenkonfigurationen

1. Öffnen Sie die Seite **Class Configuration** (Klassenkonfiguration).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Sämtliche Klassenkonfigurationen werden auf der Seite **Diffserv Class Summary** (Zusammenfassung der Diffserv-Klassen) angezeigt.

Abbildung 12-4. Zusammenfassung der Diffserv-Klassen



Hinzufügen einer Klassenkonfiguration mithilfe der CLI-Befehle

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

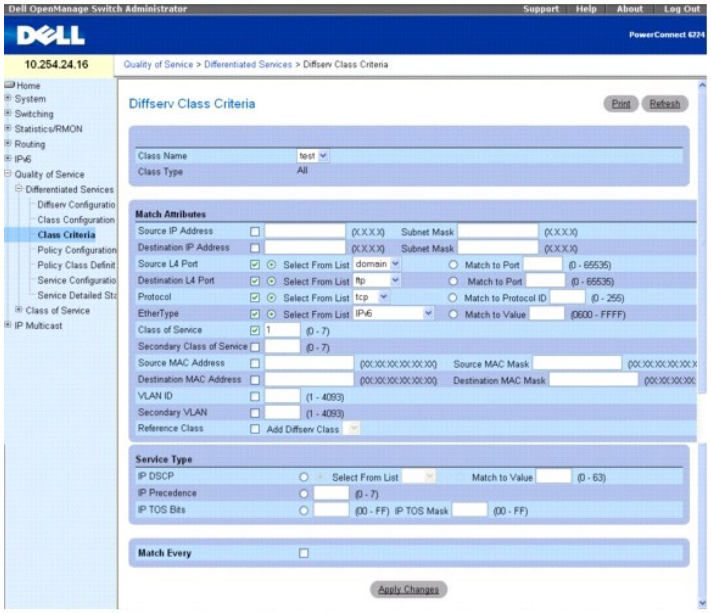
- QoS Commands (QoS-Befehle)

Klassenkriterien

Verwenden Sie die Seite **Diffserv Class Criteria** (Diffserv-Klassenkriterien), um die Kriterien zu definieren, die einer DiffServ-Klasse zugeordnet werden sollen. Wenn Pakete empfangen werden, werden diese DiffServ-Klassen zur Priorisierung der Pakete verwendet.

Zur Anzeige der Seite klicken Sie in der Strukturansicht auf **Quality of Service→ Differentiated Services→ Class Criteria (Klassenkriterien)**.

Abbildung 12-5. Kriterien von Diffserv-Klassen



Die Seite **Diffserv Class Criteria** (Diffserv-Klassenkriterien) enthält folgende Felder:

Class Name (Klassenname) – Zur Wahl des Klassennamens, für den Kriterien festgelegt werden.

Class Type (Klassentyp) – Zeigt den Klassentyp an. Der einzige unterstützte konfigurierbare Klassentyp ist **All** (Alle).

Attribute zuordnen

Verwenden Sie die folgenden Felder, um Pakete einer Klasse zuzuordnen. Aktivieren Sie die Kontrollkästchen für die einzelnen Felder, die als Kriterium für eine Klasse verwendet werden sollen, und geben Sie Daten in das jeweilige Feld ein. Sie können einer Klasse mehrere Vergleichskriterien zuordnen. Für dieses Kriterium gilt die Boolesche logische UND-Verknüpfung.

Source IP Address (Quelle IP-Adresse) – Die IP-Adresse des Quell-Ports eines Pakets muss mit der hier angegebenen Adresse übereinstimmen.

Subnet Mask (Subnetzmaske) – Die Subnetzmaske der Quell-IP-Adresse. Dieses Feld ist erforderlich, wenn **Source IP Address** (IP-Quelladresse) aktiviert ist.

Destination IP Address (Ziel IP-Adresse) – Die IP-Adresse des Ziel-Ports eines Pakets muss mit der hier angegebenen Adresse übereinstimmen.

Subnet Mask (Subnetzmaske) – Die Subnetzmaske der Ziel-IP-Adresse. Dieses Feld ist erforderlich, wenn **Destination IP Address** (IP-Zieladresse) aktiviert ist.

Source L4 Port (Quelle L4-Port) – Der TCP/UDP-Quell-Port eines Pakets muss mit dem hier angegebenen Port übereinstimmen. Wählen Sie eine der folgenden Optionen:

Select From List (Aus Liste wählen) – Klicken Sie hier, um den Port, mit dem die Pakete übereinstimmen müssen, aus einer Liste bekannter Quell-Ports zu wählen.

Match to Port (Portübereinstimmung) – Klicken Sie hier, um eine benutzerdefinierte Port-ID hinzuzufügen, mit der die Pakete übereinstimmen müssen.

Destination L4 Port (Ziel L4-Port) – Der TCP/UDP-Ziel-Port eines Pakets muss mit dem hier angegebenen Port übereinstimmen. Wählen Sie eine der folgenden Optionen:

Select From List (Aus Liste wählen) – Klicken Sie hier, um den Port, mit dem die Pakete übereinstimmen müssen, aus einer Liste bekannter Ziel-Ports zu wählen.

Match to Port (Portübereinstimmung) – Klicken Sie hier, um eine benutzerdefinierte Port-ID hinzuzufügen, mit der die Pakete übereinstimmen müssen.

Protocol (Protokoll) – Das Protokoll eines Pakets muss mit dem hier angegebenen Protokoll übereinstimmen. Wählen Sie eine der folgenden Optionen:

Select from List (Aus Liste wählen) – Ein Protokoll aus der Dropdown-Liste wählen.

Match to Protocol ID (Protokoll-ID-Übereinstimmung) – Eine Protokoll-ID eingeben, mit der die Pakete übereinstimmen müssen.

EtherType – Der Ethertype eines Frame muss mit dem hier angegebenen Ethertype übereinstimmen. Wählen Sie eine der folgenden Optionen:

Select from List (Aus Liste wählen) – Einen Ethertype aus der Dropdown-Liste wählen.

Match to Port (Portübereinstimmung) – Eine Ethertype-ID eingeben, mit der die Pakete übereinstimmen müssen.

Class of Service CoS – Die CoS eingehender Pakete muss mit der hier eingegebenen CoS übereinstimmen.

Source MAC Address (MAC-Quelladresse) – Die MAC-Quelladresse eingehender Pakete muss mit der hier eingegebenen Adresse übereinstimmen.

Source MAC Mask (MAC-Quelladress-Maske) – Gibt die Platzhaltermaske der MAC-Quelladresse an. Durch Platzhaltermasken wird festgelegt, welche Bits verwendet und welche ignoriert werden. Die Platzhaltermaske 255.255.255.255 gibt an, dass kein Bit von Bedeutung ist. Die Platzhaltermaske 0.0.0.0 gibt an, dass alle Bits berücksichtigt werden. Dieses Feld ist erforderlich, wenn **Source MAC Address** (MAC-Quelladresse) aktiviert ist.

Destination MAC Address (MAC-Zieladresse) – Die MAC-Zieladresse eingehender Pakete muss mit der hier eingegebenen Adresse übereinstimmen.

Destination MAC Mask (MAC-Zieladress-Maske) – Gibt die Platzhaltermaske der MAC-Zieladresse an. Durch Platzhaltermasken wird festgelegt, welche Bits verwendet und welche ignoriert werden. Die Platzhaltermaske 255.255.255.255 gibt an, dass kein Bit von Bedeutung ist. Die Platzhaltermaske 0.0.0.0 gibt an, dass alle Bits berücksichtigt werden. Dieses Feld ist erforderlich, wenn **Destination MAC Address** (MAC-Zieladresse) aktiviert ist.

VLAN ID (VLAN-ID) – Die VLAN ID eingehender Pakete muss mit der hier eingegebenen VLAN-ID übereinstimmen.

Secondary VLAN ID (Sekundäre VLAN-ID) – Die sekundäre VLAN ID eingehender Pakete muss mit der hier eingegebenen VLAN-ID übereinstimmen.

Reference Class (Referenzklasse) – Zur Wahl bzw. Abwahl einer Klasse für den Kriterienbezug. Markieren Sie das Kontrollkästchen **Add Diffserv Class** (Diffserv-Klasse hinzufügen), und wählen Sie anschließend eine zuvor konfigurierte Diffserv-Klasse aus dem zugehörigen Dropdown-Menü aus:

Kriterien für Diensttypen

Aktivieren Sie eines der folgenden drei Kontrollkästchen für den Diensttyp, der für den Abgleich von Paketen mit Klassenkriterien verwendet werden soll:

IP DSCP (IP-DSCP) – Der DSCP-Typ des Paket muss mit den Klassenkriterien übereinstimmen. Wählen Sie den DSCP-Typ entweder aus dem Dropdown-Menü, oder geben Sie einen DSCP-Wert ein, der übereinstimmen muss.

IP Precedence (IP-Precedence) – Der IP-Precedence-Wert des Pakets muss mit den Klassenkriterien übereinstimmen, wenn diese Auswahl getroffen und ein Wert eingegeben wird.

IP TOS Bits (IP-TOS-Bits) – Die Type of Service-Bits im IP-Header des Pakets müssen mit den Klassenkriterien übereinstimmen, wenn diese Auswahl getroffen und ein Wert eingegeben wird.

Match Every (Vollständige Übereinstimmung) – Wenn diese Option gewählt wird, müssen alle Kriterien übereinstimmen.

Definieren von Klassenkriterien

1. Öffnen Sie die Seite **Class Criteria** (Klassenkriterien).
2. Wählen Sie aus dem Dropdown-Menü den **Class Name** (Klassennamen), für den Sie Vergleichsattribute eingeben möchten.
3. Wählen Sie die Attribute, die mit dieser Klasse übereinstimmen sollen, und legen Sie deren Kriterien fest.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Kriterien werden zu dieser Klasse hinzugefügt und das Gerät aktualisiert.

Konfigurieren von Klassenkriterien über CLI-Befehle

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

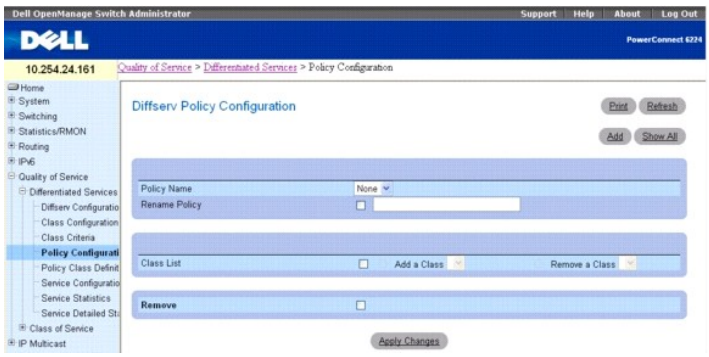
- QoS Commands (QoS-Befehle)

Richtlinienkonfiguration

Verwenden Sie die Seite **Diffserv Policy Configuration** (Diffserv-Richtlinienkonfiguration), um eine Sammlung von Klassen mit einem oder mehreren Richtlinienparametern zu verknüpfen.

Zur Anzeige der Seite klicken Sie in der Strukturansicht auf **Quality of Service→ Differentiated Services→ Policy Configuration (Richtlinienkonfiguration)**.

Abbildung 12-6. Diffserv-Richtlinienkonfiguration



Die Seite **Diffserv Policy Configuration** (Diffserv-Richtlinienkonfiguration) enthält folgende Felder:

Policy Name (Richtliniennamen) – Zur Wahl des Richtliniennamens, die der oder den Klassen zugeordnet werden soll.

Rename Policy (Richtlinie umbenennen) – Wenn dieses Kontrollkästchen aktiviert, ein neuer Namen eingegeben und auf **Apply Changes** (Änderungen übernehmen) geklickt wird, wird die Richtlinie umbenannt.

Class List (Klassenliste) – Konfiguriert die Klassenverknüpfung für die Richtlinie.

Add a Class (Klasse hinzufügen) – Zur Verknüpfung der im Dropdown-Menü gewählten Klasse mit einer Richtlinie.

Remove a Class (Klasse entfernen) – Zum Aufheben der Verknüpfung der gewählten Klasse mit der Richtlinie.

Remove – Zum Löschen des gewählten Richtliniennamens vom Gerät.

Verknüpfen einer Klasse mit einer Richtlinie oder Aufheben der Verknüpfung

1. Öffnen Sie die Seite **Diffserv Policy Configuration** (Diffserv-Richtlinienkonfiguration).
2. Wählen Sie den **Policy Name** (Richtlinienname), der mit der Klasse verknüpft werden soll.
3. Markieren Sie das Kontrollkästchen im Feld **Class List** (Klassenliste),. Klicken Sie anschließend auf das Optionsfeld **Add a Class** (Klasse hinzufügen) bzw. **Remove a Class** (Klasse entfernen), und wählen Sie die **Class** (Klasse) im zugehörigen Dropdown-Menü aus

   Verwenden Sie den Befehl **Add a Class** (Klasse hinzufügen), um eine Klasse mit einer Richtlinie zu verknüpfen. Verwenden Sie den Befehl **Remove a Class** (Klasse entfernen), um die Verknüpfung einer Klasse mit einer Richtlinie aufzuheben.
4. Wählen Sie die betreffende Klasse aus dem zugehörigen Dropdown-Menü aus.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die geänderte Richtlinie wird gespeichert und das Gerät aktualisiert.

Umbenennen einer Richtlinie

1. Öffnen Sie die Seite **Diffserv Policy Configuration** (Diffserv-Richtlinienkonfiguration).
2. Wählen Sie den **Policy Name** (Richtliniennamen), der umbenannt werden soll.
3. Nennen Sie die Richtlinie um, indem Sie das Kontrollkästchen **Rename Policy** (Richtlinie umbenennen) aktivieren und den neuen Namen in das Feld daneben eingeben.

   Der geänderte Richtlinienname wird gespeichert und das Gerät aktualisiert.

Hinzufügen eines neuen Richtliniennamens

1. Öffnen Sie die Seite **Diffserv Policy Configuration** (Diffserv-Richtlinienkonfiguration).
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add Diffserv Policy** (Diffserv-Richtlinie hinzufügen) wird angezeigt.

Abbildung 12-7. Diffserv-Richtlinie hinzufügen

3. Geben Sie den neuen **Policy Name** (Richtliniennamen) ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die neue Richtlinie wird gespeichert und das Gerät aktualisiert.

Anzeigen der Richtlinienzusammenfassung

1. Öffnen Sie die Seite **Policy Configuration** (Richtlinienkonfiguration.
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Auf der Seite **Diffserv Policy Summary** (Diffserv-Richtlinienzusammenfassung) werden alle Richtlinienname, -typen und die zugehörigen Klassen angezeigt.

Abbildung 12-8. Zusammenfassung der Diffserv-Richtlinien

Entfernen einer Richtlinienkonfiguration

1. Öffnen Sie die Seite **Diffserv Policy Configuration** (Diffserv-Richtlinienkonfiguration).
2. Wählen Sie den zu löschenden Richtliniennamen aus dem Dropdown-Menü **Policy Name** (Richtlinienname).
3. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die zugehörige Richtlinienkonfiguration wird entfernt und das Gerät aktualisiert.

Definieren von Richtlinienkonfigurationen mithilfe der CLI-Befehle

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

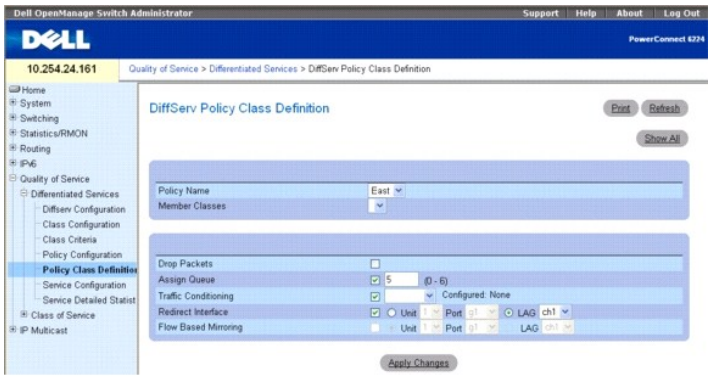
- QoS Commands (QoS-Befehle)

Definition von Richtlinienklassen

Verwenden Sie die Seite **Diffserv Policy Class Definition** (Definition von Richtlinienklassen), um eine Klasse einer Richtlinie zuzuordnen und Attribute für diese Richtlinienklasseninstanz festzulegen.

Zur Anzeige der Seite klicken Sie in der Strukturansicht auf **Quality of Service→ Differentiated Services→ Policy Class Definition(Definition von Richtlinienklassen)**.

Abbildung 12-9. Definition von Diffserv-Richtlinienklassen



Die Seite **Diffserv Policy Class Definition** (Definition von Diffserv-Richtlinienklassen) enthält folgende Felder:

Policy Name (Richtlinienname) – Zur Auswahl der Richtlinie, die einer Klasse zugeordnet werden soll, aus einem Dropdown-Menü.

Member Classes (Verbundene Klassen) – Zur Auswahl der Klasse, die mit diesem Richtliniennamen verknüpft werden soll, aus einem Dropdown-Menü.

Drop Packets (Pakete verwerfen) – Wählen Sie dieses Feld, um Pakete für diese Richtlinienklasse zu verwerfen.

Assign Queue (Warteschlange zuweisen) – Weist die Pakete dieser Richtlinienklasse einer Warteschlange zu. Der gültige Wertebereich liegt zwischen 0 und 6.

Traffic Conditioning (Verkehrskonditionierung) – Wenn dieses Kontrollkästchen aktiviert und eine Bedingung aus dem Dropdown-Menü gewählt wird, wird ein Verkehrskonditionierungstyp zugewiesen. Diese Option wirkt sich darauf aus, wie Datenverkehr, der dieser Richtlinienklasse entspricht, behandelt wird. Wählen Sie aus den Optionen **None** (Keine), **Marking** (Markierung) und **Policing** (Richtlinienkontrolle). Wenn **Marking** (Markierung) oder **Policing** (Richtlinienkontrolle) gewählt wird, werden entsprechende Felder auf dem Bildschirm angezeigt.

- **None** (Keine): Damit wird festgelegt, dass während der Paketverarbeitung keine Verkehrskonditionierung durchgeführt wird. Dies ist die Standardeinstellung.
- **Marking** (Markierung): Ermöglicht es, eines der folgenden Felder im Paket zu markieren: IP-DSCP, IP-Precedence oder Class of Service. Informationen über die Felder, die bei der Wahl von **Marking** (Markierung) angezeigt werden, finden Sie unter "Verkehrsbedingung Paketmarkierung".
- **Policing** (Richtlinienkontrolle): Ermöglicht die Konfiguration der Richtlinienkontrolle sowie der Handhabung von konformen und nicht-konformen Paketen. Informationen über die Felder, die bei der Wahl von **Policing** (Richtlinienkontrolle) angezeigt werden, finden Sie unter "Verkehrsbedingung Richtlinienkontrolle".

Redirect Interface (Schnittstelle umleiten) – Zeigt an, ob der Befehl "Schnittstelle umleiten" auf diese Richtlinienklasse angewandt wird, und gibt die verwendete Schnittstelle oder LAG an.

Flow Based Mirroring (Flussbasierte Datenspiegelung) – Zeigt an, ob flussbasierte Datenspiegelung auf diese Richtlinienklasse angewandt wird, und gibt die verwendete Schnittstelle oder LAG an.

Definieren einer Richtlinienklasseninstanz

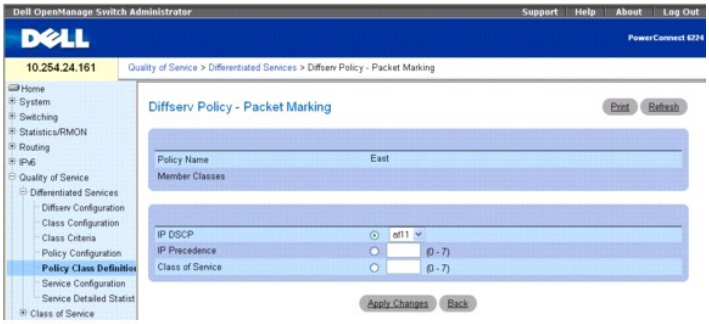
1. Öffne Sie die Seite **Diffserv Policy Class Definition** (Definition von Diffserv-Richtlinienklassen).
2. Wählen Sie eine Richtlinie und eine zuzuordnende Klasse.
3. Legen Sie mithilfe der verbleibenden Felder auf der Seite Attribute fest, die für diese Richtlinienklasseninstanz gelten sollen.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Richtlinienklasse wird definiert und das Gerät aktualisiert.

Verkehrsbedingung Paketmarkierung

Wenn **Marking** (Markierung) als **Traffic Condition** (Verkehrsbedingung) gewählt wird, wird die folgende Seite zur Paketmarkierung angezeigt.

Abbildung 12-10. Definition von Richtlinienklassen - Paketmarkierung



Die Seite **Diffserv Policy - Packet Marking** (Diffserv-Richtlinienklassen - Paketmarkierung) enthält folgende Felder:

Policy Name (Richtlinienname) – Zeigt die Richtlinie an, die einer Klasse zugeordnet ist.

Member Classes (Verbundene Klassen) – Zeigt die Klasse an, der dieser Richtlinienname zugeordnet wurde.

Sie haben die Möglichkeit, eines der folgenden Felder im Paket zu markieren:

IP DSCP – Zur Wahl des zu markierenden IP-DSCP-Wertes. Wählen Sie diesen aus dem Dropdown-Menü, oder geben Sie ihn direkt in das Feld für den Benutzerwert ein.

IP Precedence – Zur Wahl der zu markierenden Warteschlangennummer für die vorgegebene IP-Precedence.

Class of Service – Markiert die angegebene Class of Service-Warteschlangennummer.

Konfigurieren der Paketmarkierung für eine Richtlinienklasseninstanz

1. Wählen Sie aus dem Dropdown-Menü **Traffic Conditioning** (Verkehrskonditionierung) auf der Seite **Diffserv Policy Class Definition** (Definition von Diffserv-Richtlinienklassen) den Eintrag **Marking** (Markierung).

   Die Seite **Packet Marking** (Paketmarkierung) wird angezeigt, wie in Abbildung 12-10 dargestellt.

2. Wählen Sie den IP-DSCP-Wert, die IP-Precedence oder die Class of Service, die für diese Richtlinienklasse markiert werden sollen.

3. Wählen Sie einen Wert für dieses Feld aus, oder geben Sie ihn ein.

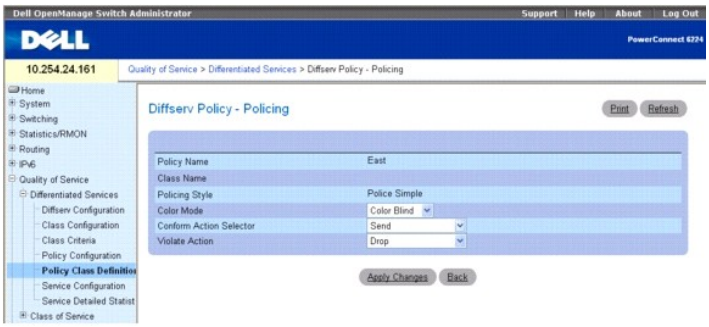
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Richtlinienklasse wird definiert und das Gerät aktualisiert.

Verkehrsbedingung Richtlinienkontrolle

Wenn **Policing** (Richtlinienkontrolle) als **Traffic Condition** (Verkehrsbedingung) gewählt wird, wird die nachstehende Seite **Diffserv Policy - Policing** (Diffserv-Richtlinienkontrolle) angezeigt.

Abbildung 12-11. Definition von Richtlinienklassen - Richtlinienkontrolle



Die Seite **Diffserv Policy - Policing** (Diffserv-Richtlinie - Kontrolle) enthält folgende Felder:

Policy Name (Richtlinienname) – Zeigt die Richtlinie an, für die die Richtlinienkontrolle konfiguriert wird.

Class Name (Klassenname) – Zeigt die Klasse an, der dieser Richtlinienname zugeordnet wurde.

Policing Style (Richtlinienkontrollstil) – Zeigt den verwendeten Richtlinienkontrollstil an.

Color Mode (Farbkontrolltyp) – Zur Wahl des verwendeten Farbkontrolltyps. Wählen Sie aus dem Dropdown-Menü Color Blind (Farbe irrelevant) oder Color Aware (Farbe relevant).

Conform Action Selector (Aktion bei Konformität) – Zur Vorgabe, was mit Paketen geschieht, die als konform eingestuft werden (unterhalb der Kontrollrate). Es stehen die Optionen Send (Senden), Drop (Verwerfen), Mark CoS (CoS markieren), Mark IP DSCP (IP-DSCP markieren) und Mark IP Precedence (IP-Precedence markieren) zur Verfügung.

Violate Action (Aktion bei Nicht-Konformität) – Zur Vorgabe, was mit Paketen geschieht, die als nicht-konform eingestuft werden (oberhalb der Kontrollrate). Es stehen die Optionen Send (Senden), Drop (Verwerfen), Mark CoS (CoS markieren), Mark IP DSCP (IP-DSCP markieren) und Mark IP Precedence (IP-Precedence markieren) zur Verfügung.

Konfigurieren der Richtlinienkontrolle für eine Richtlinienklasseninstanz

1. Wählen Sie aus dem Dropdown-Menü **Traffic Conditioning** (Verkehrskonditionierung) auf der Seite **Diffserv Policy Class Definition** (Definition von Diffserv-Richtlinienklassen) den Eintrag **Policing** (Richtlinienkontrolle).

   Die Seite **Diffserv Policy - Policing** (Diffserv-Richtlinie – Richtlinienkontrolle) wird angezeigt (siehe Abbildung 12-11).

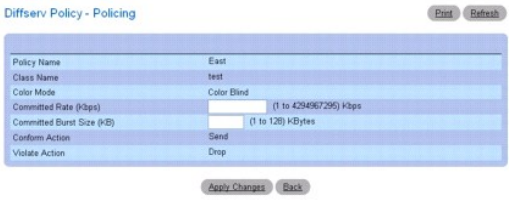
2. Aktivieren, um ein oder mehrere Richtlinienkontrollkriterien zur Verwendung für diese Richtlinienklasse zu wählen.

3. Wählen Sie einen Wert für jedes aktivierte Feld aus, oder geben Sie einen ein.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die folgende Seite **Policy Rate Configuration** (Konfiguration der Richtlinienrate) wird angezeigt.

Abbildung 12-12. Konfiguration der Richtlinienrate



5. Geben Sie die gewünschten Kriterienwerte für "Committed Rate" (Garantierte Rate) und/oder "Committed Burst Size" (Garantierte Burstgröße) ein.

6. Klicken Sie auf **Apply Changes**

   (Änderungen übernehmen).

   Die Richtlinienkontrolle wird für die angegebene Richtlinienklasseninstanz konfiguriert und das Gerät aktualisiert.

Definieren von Richtlinienklassen mithilfe der CLI-Befehle

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

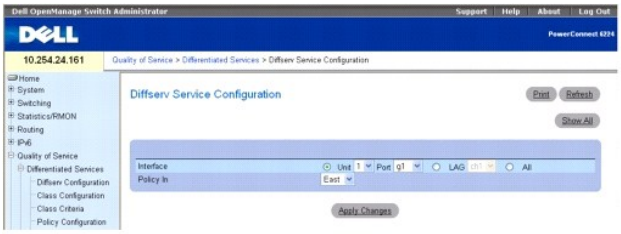
- QoS Commands (QoS-Befehle)

Dienstekonfiguration

Verwenden Sie die Seite **Diffserv Service Configuration** (Diffserv-Dienstekonfiguration) zur Aktivierung einer Richtlinie auf einem Port.

Zur Anzeige der Seite klicken Sie in der Strukturansicht auf **Quality of Service**→ **Differentiated Services**→ **Service Configuration (Dienstekonfiguration)**.

Abbildung 12-13. Diffserv-Dienstekonfiguration



Die Seite **Diffserv Service Configuration** (Diffserv-Dienstekonfiguration) enthält folgende Felder:

Interface (Schnittstelle) – Dient zur Auswahl der Schnittstelle (Einheit/Port, LAG oder Alle), auf die die Optionen der Dropdown-Menüs angewandt werden.

Policy In (Richtlinie) – Zur Wahl der dem Port zuzuordnenden Richtlinie aus einem Dropdown-Menü.

Aktivieren einer Richtlinie auf einem Port

1. Öffnen Sie die Seite **Diffserv Service Configuration** (Diffserv-Dienstekonfiguration).
2. Wählen Sie die Schnittstelle aus den Dropdown-Menüs.
3. Wählen Sie die Richtlinie aus dem Dropdown-Menü.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Richtlinie wird auf der Schnittstelle aktiviert und das Gerät aktualisiert.

Anzeigen der Zusammenfassung der Diffserv-Dienste

1. Öffnen Sie die Seite **Diffserv Service Configuration** (Diffserv-Dienstekonfiguration).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite zur Zusammenfassung der Diffserv-Dienste wird angezeigt.

Abbildung 12-14. Zusammenfassung der Diffserv-Dienste

Zuweisen einer Richtlinie zu einem Port mithilfe der CLI-Befehle

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- QoS Commands (QoS-Befehle)

Detaillierte Dienstestatistiken

Verwenden Sie die Seite **Diffserv-Service Detailed Statistics** (Detaillierte Diffserv-Dienstestatistiken), um detaillierte Paketinformationen für einen bestimmten Port und eine bestimmte Klasse anzuzeigen.

Zur Anzeige der Seite klicken Sie in der Strukturansicht auf **Quality of Service→ Differentiated Services→ Service Detailed Statistics (Detaillierte Dienstestatistiken)**.

Abbildung 12-15. Detaillierte Diffserv-Dienstestatistiken

Die Seite **Service Detailed Statistics** (Detaillierte Diffserv-Dienststatistiken) enthält folgende Felder:

Counter Mode Selector (Zählermodusauswahl) – Der anzuzeigende Statistiktyp Der einzige verfügbare Typ sind Pakete.

Interface (Schnittstelle) – Zur Wahl der Einheit und des Ports oder der LAG, für die Dienststatistiken angezeigt werden sollen.

Direction (Richtung) – Zur Wahl der Richtung der Pakete, für die Dienststatistiken angezeigt werden sollen.

Policy Name (Richtlinienname) – Zeigt die Richtlinie an, die der gewählten Schnittstelle zugeordnet ist.

Operational Status (Betriebsstatus) – Zeigt an, ob die Richtlinie auf dieser Schnittstelle aktiv ist oder nicht.

Member Classes (Verbundene Klassen) – Zur Wahl der zugeordneten Klasse, für die Oktettstatistiken angezeigt werden sollen.

Offered Packets (Angebotene Pakete) – Zeigt an, wie viele Pakete der Richtlinie entsprechen.

Discarded Packets (Verworfene Pakete) – Zeigt an, wie viele Pakete von der Richtlinie verworfen werden.

Anzeigen von Dienststatistiken

1. Öffnen Sie die Seite **Diffserv Service Detailed Statistics** (Detaillierte Diffserv-Dienststatistiken).
2. Füllen Sie die Felder je nach Bedarf aus.

   Paketstatistiken werden für die angegebene Schnittstelle, Richtung und Klasse angezeigt.

Konfigurieren von Dienststatistiken mithilfe des CLI-Befehls

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- QoS Commands (QoS-Befehle)

Class of Service

Mit der Warteschlangenfunktion Class of Service (CoS) können bestimmte Aspekte von Switch-Warteschlangen direkt konfiguriert werden. Damit wird das gewünschte QoS-Verhalten für unterschiedliche Typen von Netzwerkverkehr ermöglicht, wenn die Komplexitäten von DiffServ nicht benötigt werden. Anhand der Priorität eines Pakets, das an einer Schnittstelle eintrifft, kann das Paket über eine Zuweisungstabelle zur entsprechenden abgehenden CoS-Warteschlange gelenkt werden. CoS-Warteschlangenmerkmale, die sich auf die Warteschlangenzuordnung auswirken, wie beispielsweise garantierte Mindestbandbreite, Formung der Übertragungsrate etc., können auf Warteschlange- (oder Port-) ebene vom Benutzer konfiguriert werden.

Pro Port werden sieben Warteschlangen unterstützt. Obwohl die Hardware acht Warteschlangen unterstützt, wird eine Warteschlange immer für die interne Verwendung durch das Stack-Subsystem reserviert.

Um die Seite anzuzeigen, klicken Sie in der Strukturansicht auf **Quality of Service**→ **Class of Service**. Die Menüseite **Class of Service** enthält Links zu den folgenden Funktionen:

- Konfiguration der Zuweisungstabelle
- Schnittstellenkonfiguration
- Konfiguration der Schnittstellenwarteschlangen

Konfiguration der Zuweisungstabelle

Jeder Port im Switch kann für den Trust-Modus mit einem der Paketfelder (802.1p, IP-Precedence oder IP-DSCP) konfiguriert werden, oder für den Untrust-Modus mit einem beliebigen Prioritätsziel von Paketen. Wenn der Port für einen Trust-Modus konfiguriert ist, nutzt er eine Zuweisungstabelle, die dem verwendeten Trust-Feld entspricht. Die Zuweisungstabelle gibt die CoS-Warteschlange an, an die das Paket auf dem oder den entsprechenden Egress-Ports weitergeleitet werden soll. Selbstverständlich muss das vertrauenswürdige Feld im Paket vorliegen, damit die Zuweisungstabelle von Nutzen ist. Falls dies

nicht der Fall ist, werden Standardvorgänge durchgeführt. Zu diesen Vorgängen gehört die Weiterleitung des Pakets zu einer bestimmten CoS-Ebene, die insgesamt für den Ingress-Port konfiguriert wurde und auf der vorhandenen Standardpriorität des Ports basiert, so wie diese einer Verkehrsklasse durch die aktuelle 802.1p-Zuweisungstabelle zugeordnet ist.

Wenn ein Port als nicht vertrauenswürdig konfiguriert ist, stuft er alternativ jegliches Prioritätsziel eingehender Pakete als nicht vertrauenswürdig ein und verwendet stattdessen seinen Standardprioritätswert. Alle Pakete, die beim Ingress eines nicht vertrauenswürdigen Ports eintreffen, werden gemäß der konfigurierten Standardpriorität des Ingress-Ports an eine bestimmte CoS-Warteschlange auf dem oder den entsprechenden Egress-Ports weitergeleitet. Dieser Vorgang wird auch in Fällen durchgeführt wird, wo einer Trust-Port-Zuordnung nicht entsprochen werden kann, zum Beispiel, wenn ein Nicht-IP-Paket bei einem Port eintrifft, der für den Trust-Modus mit dem IP-DSCP-Wert konfiguriert ist.

Verwenden Sie die Seite **Mapping Table Configuration** (Konfiguration der Zuweisungstabelle), um festzulegen, wie Class of Service einem Paket zugewiesen wird.

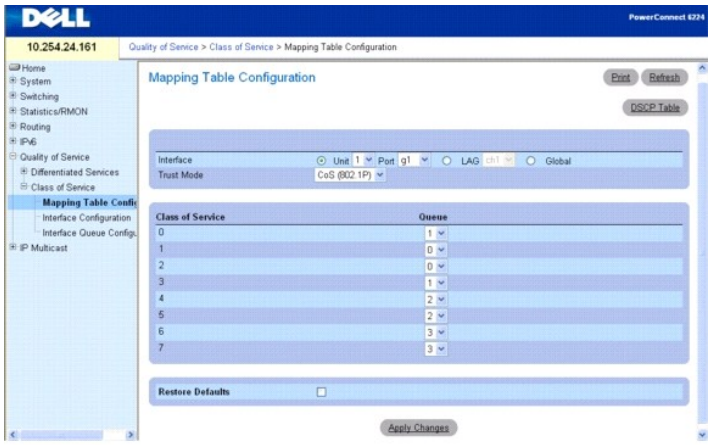
Zur Anzeige der Seite klicken Sie in der Strukturansicht auf **Quality of Service→ Class of Service→ Mapping Table Configuration (Konfiguration der Zuweisungstabelle)**.

Der auf der Seite **Mapping Table Configuration** (Konfiguration der Zuweisungstabelle) gewählte Trust-Modus wirkt sich darauf aus, wie die Seite und die von dort zugänglichen Felder angezeigt werden. Hier stehen drei Trust-Modi zur Verfügung:

- Untrusted (None) (Untrust-Modus (keiner))
- CoS(802.1P)
- IP DSCP

CoS(802.1P) ist der Standardmodus, deshalb wird diese Seite angezeigt, wenn **Mapping Table Configuration** (Konfiguration der Zuweisungstabelle) aus der Menüseite **Class of Service** gewählt wird.

Abbildung 12-16. Konfiguration der Zuweisungstabelle – CoS (802.1P)



Trust-Modus CoS(802.1P)

Die Seite **CoS (802.1P) Mapping Table Configuration** (Konfiguration der Zuweisungstabelle – CoS (802.1P)) enthält die folgenden Felder:

Interface (Schnittstelle) – Zur Wahl der Schnittstelle(n), auf die die Class of Service-Konfiguration angewendet wird. Wählen Sie eine Einheit und einen Port oder eine LAG, oder wählen Sie "Global", um die Konfigurationsklasse auf alle Schnittstellen anzuwenden.

Trust Mode (Trust-Modus) – Zur Auswahl des anzuwendenden Trust-Modus. **CoS (802.1P)** ist die Standardeinstellung.

Class of Service – Listet jede Class of Service in einer separaten Zeile auf, so dass diesen jeweils eine separate Warteschlange zugewiesen werden kann.

Queue (Warteschlange) – Zur Wahl einer Warteschlange für jede **Class of Service** aus dem Dropdown-Menü. Anfangs werden die Standardwarteschlangen angezeigt.

Restore Defaults (Standard wiederherstellen) – Wenn dieses Kontrollkästchen aktiviert und **Apply Changes** (Änderungen übernehmen) gewählt wird, werden die Standardwarteschlangenwerte wiederhergestellt.

Konfigurieren des Trust-Modus CoS(802.1P)

1. Öffnen Sie die Seite **Mapping Table Configuration** (Konfiguration der Zuweisungstabelle).
2. Wählen Sie die betreffende Einheit und den Port oder die LAG aus, oder wählen Sie "Global", um die Einstellungen auf alle Schnittstellen anzuwenden.
3. Wählen Sie einen **Trust Mode** (Trust-Modus).
4. Wählen Sie für jede **Class of Service** eine **Queue** (Warteschlange) aus, die dieser zugeordnet werden soll.

5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Änderungen werden auf die gewählten Schnittstellen angewendet und das Gerät aktualisiert.

Wiederherstellen der Standardeinstellungen für Warteschlangen

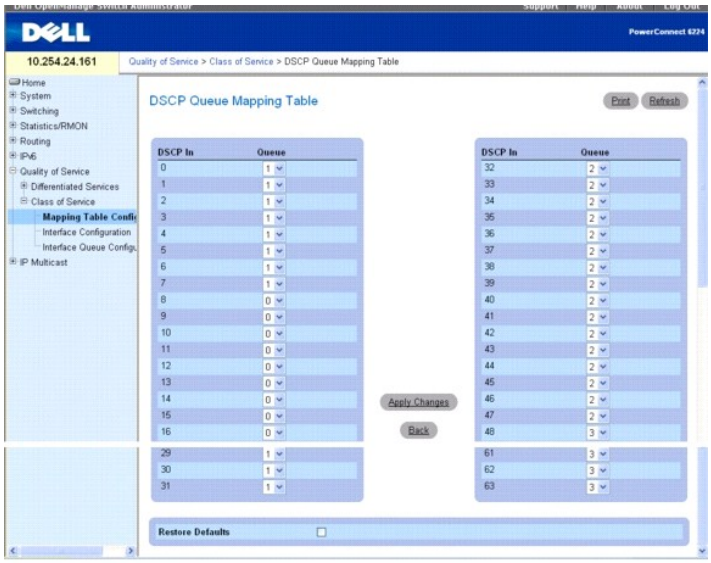
1. Öffnen Sie die Seite **Mapping Table Configuration** (Konfiguration der Zuweisungstabelle).
2. Aktivieren Sie das Kontrollkästchen **Restore Defaults** (Standardeinstellungen wiederherstellen).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Für jede Class of Service werden die Warteschlangen auf die Standardeinstellungen zurückgesetzt und das Gerät aktualisiert.

Konfigurieren der IP-DSCP-Tabelle

Um auf die **DSCP Queue Mapping Table**(DSCP-Warteschlangen-Zuweisungstabelle) zuzugreifen, klicken Sie in der Strukturansicht auf **Quality of Service→ Class of Service→ Mapping Table Configuration (Konfiguration der Zuweisungstabelle)** und anschließend auf die Verknüpfung "DSCP Table" (DSCP-Tabelle).

Abbildung 12-17. DSCP-Warteschlangen-Zuweisungstabelle



Die Seite **DSCP Queue Mapping Table** (DSCP-Warteschlangen-Zuweisungstabelle) enthält folgende Felder:

DSCP In – Zur Auswahl als Kriterium aktivieren und eingeben, welcher DiffServ Code Point im Paket zu verwenden ist. Mit diesem Feld wird bestimmt, an welche Warteschlange das Paket gesendet wird.

Queue ID (Warteschlangen-ID) – Zur Wahl der Warteschlange, an die das Paket gesendet wird.

Wiederherstellen der Standardeinstellungen für Warteschlangen

1. Öffnen Sie die Seite **DSCP Queue Mapping Table** (DSCP-Warteschlangen-Zuweisungstabelle).
2. Aktivieren Sie das Kontrollkästchen **Restore Defaults** (Standardeinstellungen wiederherstellen).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Warteschlangen werden auf ihre Standardwerte zurückgesetzt und das Gerät aktualisiert.

Konfiguration der Zuweisungstabelle mithilfe der CLI-Befehle

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

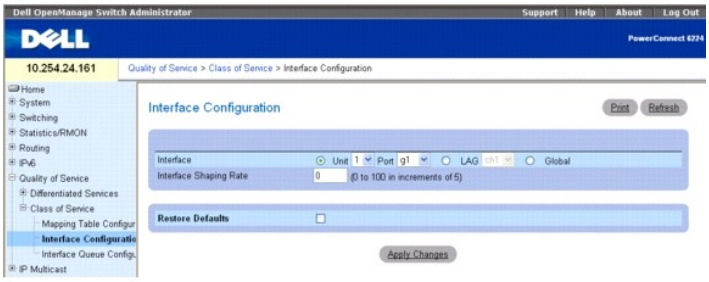
- QoS Commands (QoS-Befehle)

Schnittstellenkonfiguration

Verwenden Sie die Seite **Interface Configuration** (Schnittstellenkonfiguration) zur individuellen Festlegung von Ports für die CoS-Konfiguration und zur Anwendung einer Schnittstellenformungsrate auf die gewählten Ports.

Klicken Sie zur Anzeige der Seite **Interface Configuration** (Schnittstellenkonfiguration) in der Strukturansicht auf **Quality of Service→ Class of Service→ Interface Configuration (Schnittstellenkonfiguration)**.

Abbildung 12-18. Schnittstellenkonfiguration



Die Seite **Interface Configuration** (Schnittstellenkonfiguration) enthält folgende Felder:

Interface (Schnittstelle) – Zur Auswahl der Schnittstelle(n), auf die sich die **Interface Shaping Rate** (Schnittstellenformungsrate) auswirken soll.

Interface Shaping Rate (Schnittstellenformungsrate) – Zum Setzen eines Grenzwerts für die Menge des Datenverkehrs, der von einem Port abgehen darf. Bei dem Wert handelt es sich um einen Prozentsatz der maximalen ausgehandelten Bandbreite. Werte von 0-100, in Fünfer-Schritten, sind zulässig.

Restore Defaults (Standard wiederherstellen) – Wenn dieses Kontrollkästchen aktiviert ist, wird die Standard-Schnittstellenformungsrate für die gewählten Schnittstellen wiederhergestellt.

Festlegen der Schnittstellenkonfiguration

1. Öffnen Sie die Seite **Interface Configuration** (Schnittstellenkonfiguration).
2. Wählen Sie die betreffende Einheit und den Port oder die LAG aus, oder wählen Sie "Global", um die Einstellungen auf alle Schnittstellen anzuwenden.
3. Geben Sie die **Interface Shaping Rate** (Schnittstellenformungsrate) ein, die auf diese Ports angewendet werden soll.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die neue **Interface Shaping Rate** (Schnittstellenformungsrate) wird auf die ausgewählte(n) Schnittstelle(n) angewandt, und das Gerät wird aktualisiert.

Wiederherstellen der Standardformungsrate

1. Öffnen Sie die Seite **Interface Configuration** (Schnittstellenkonfiguration).
2. Aktivieren Sie das Kontrollkästchen **Restore Defaults** (Standardeinstellungen wiederherstellen).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Alle Ports werden auf die Standardformungsrate zurückgesetzt und das Gerät aktualisiert.

Definieren der Schnittstellenkonfiguration mithilfe der CLI-Befehle

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- QoS Commands (QoS-Befehle)

Konfiguration der Schnittstellenwarteschlangen

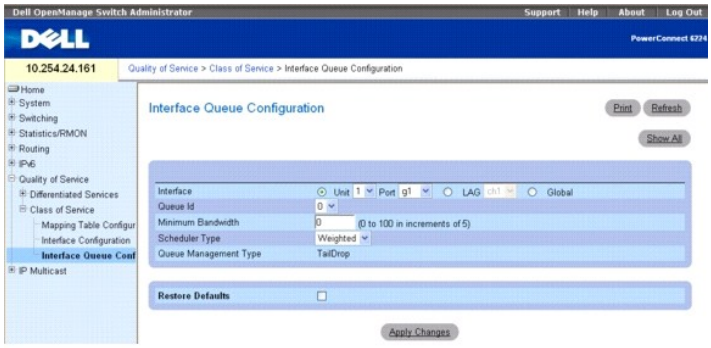
Verwenden Sie die Seite **Interface Queue Configuration** (Konfiguration der Schnittstellenwarteschlangen), um das Verhalten einer bestimmten Warteschlange über die Konfiguration der Egress-Warteschlangen des Switch festzulegen. Über benutzerkonfigurierbare Parameter wird die von der Warteschlange genutzte Bandbreite, die Warteschlangentiefe während Überlastungszeiten und die Planung der Paketübertragung von allen Warteschlangen auf einem Port gesteuert.

Jeder Port weist seine eigene Konfiguration in Bezug auf die CoS-Warteschlangen auf.

Der Konfigurationsvorgang wird dadurch vereinfacht, dass jeder CoS-Warteschlangenparameter global oder per Port konfiguriert werden kann. Eine globale Konfigurationsänderung wird automatisch für alle Ports im System übernommen.

Klicken Sie zur Anzeige der Seite **Interface Queue Configuration** (Konfiguration der Schnittstellenwarteschlangen) in der Strukturansicht auf **Quality of Service→ Class of Service→ Interface Queue Configuration (Konfiguration der Schnittstellenwarteschlangen)**.

Abbildung 12-19. Konfiguration der Schnittstellenwarteschlangen



Die Seite **Interface Queue Configuration** (Konfiguration der Schnittstellenwarteschlangen) enthält folgende Felder:

Interface (Schnittstelle) – Gibt die zu konfigurierende **Schnittstelle** an(Einheit/Port, LAG oder Global).

Queue ID (Warteschlangen-ID) – Zur Auswahl der zu konfigurierenden Warteschlange aus dem Dropdown-Menü.

Minimum Bandwidth (Minimale Bandbreite) – Zur Wahl eines Prozentsatzes der maximal ausgehandelten Bandbreite für den Port. Geben Sie einen Prozentwert von 0 bis 100, in Fünfer-Schritten, an.

Scheduler Type (Scheduler-Typ) – Zur Auswahl des Typs der Warteschlangenverarbeitung aus dem Dropdown-Menü. Die Optionen **Weighted** (Gewichtung) und **Strict** (Strikt) stehen zur Verfügung. Über die Festlegung auf Warteschlangenbasis kann der Benutzer die gewünschten Dienstemerkmale für unterschiedliche Verkehrstypen vorgeben.

Weighted (Gewichtung) – Weighted Round Robin weist jeder Warteschlange eine Gewichtung zu. Dies ist die Standardeinstellung.

Strict (Strikt) – Bei strikter Priorität wird der Datenverkehr mit der höchsten Priorität in einer Warteschlange zuerst abgearbeitet.

Queue Management Type (Warteschlangenverwaltung) – Zeigt den Paketverwaltungstyp für alle Pakete an: Taildrop. Alle Pakete in einer Warteschlange sind sicher, bis eine Überlastung eintritt. Dann werden weitere Pakete für die Warteschlange verworfen.

Konfigurieren einer Schnittstellenwarteschlange

1. Öffnen Sie die Seite **Interface Queue Configuration** (Konfiguration der Schnittstellenwarteschlangen).
2. Wählen Sie den betreffenden Port aus den Dropdown-Menüs **Interface** (Schnittstelle), **Unit** (Einheit) und **Port**.
3. Konfigurieren Sie die Schnittstelle und deren Einstellungen für diesen Port mithilfe der übrigen Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

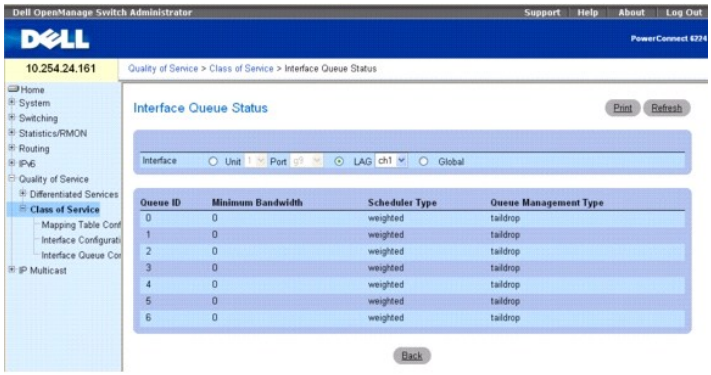
   Die Warteschlange wird konfiguriert und das Gerät aktualisiert.

Anzeigen von Einstellungen der Schnittstellenwarteschlangen

1. Öffnen Sie die Seite **Interface Queue Configuration** (Konfiguration der Schnittstellenwarteschlangen).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **Interface Queue Status** (Status der Schnittstellenwarteschlangen) wird angezeigt.
3. Wählen Sie **Unit / Port** (Einheit / Port), **LAG** oder **Global**.

Abbildung 12-20. Status der Schnittstellenwarteschlangen



Konfigurieren einer Schnittstellenwarteschlange mithilfe der CLI-Befehle

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- QoS Command (QoS-Befehle)

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Konfigurieren von IP-Multicast

Benutzerhandbuch für die Dell™ PowerConnect™ 6200-Reihe

- DVMRP
- IGMP
- Multicast
- PIM-DM
- PIM-SM

Multicast-Protokolle werden dazu verwendet, Multicast-Pakete von einer einzelnen Quelle an mehrere Empfänger zuzustellen. Sie sorgen für eine bessere Nutzung der Bandbreite sowie eine geringere Verarbeitungslast auf Host und Router, so dass sie sich ideal für Anwendungen wie Video-/Audio-Konferenzen, Whiteboard-Tools, Aktienkurs-Ticker etc. eignen.

Multicast-Anwendungen senden eine Kopie eines Pakets und adressieren diese für eine Gruppe von Empfängern (Multicast-Gruppenadresse), die dieses Paket empfangen wollen, statt nur für einen einzelnen Empfänger (Unicast-Adresse). Die Multicast-Funktion ist abhängig von dem Netzwerk, das die Pakete ausschließlich an diejenigen Netzwerke und Hosts weiterleitet, die sie auch empfangen sollen/müssen.

Multicast-fähige Router leiten Multicast-Pakete auf Basis der Routen weiter, die in der Multicast Routing Information Base (MRIB, Multicast-Routing-Informationsbasis) aufgelistet sind. Diese Routen werden im Rahmen der Einrichtung von Multicast-Verteilerbäumen von den Multicast-Protokollen erstellt, die auf dem Router laufen. Dabei verwenden die verschiedenen IP-Multicast-Routingprotokolle für den Aufbau dieser Multicast-Verteilerbäume unterschiedliche Techniken.

Wenn Multicast-Datenverkehr durch einen Teil des Netzwerks geroutet werden muss, der Multicasting nicht unterstützt (d. h. über Router, die nicht Multicast-fähig sind), werden die Multicast-Pakete in ein IP-Datagramm verkapselt und als Unicast-Paket verschickt. Sobald dann der Multicast-Router am fernen Ende des Tunnels das Paket empfängt, entfernt er die IP-Verkapselung und leitet das Paket wieder als IP-Multicast-Paket weiter. Dieser Vorgang des Verkapselns von Multicast-Paketen in IP wird als Tunnelung bezeichnet.

Klicken Sie zum Öffnen der Menüseite **IP Multicast** in der Strukturansicht auf **IP Multicast**. Die Seite **IP Multicast** enthält Links zu folgenden Prozeduren:

- DVMRP
- IGMP
- Multicast
- PIM-DM
- PIM-SM

DVMRP

Das DVMRP tauscht Probe-Pakete mit allen DVMRP-fähigen Routern aus, richtet Zwei-Wege-Nachbarschaftsverhältnisse ein und stellt eine Tabelle der Nachbarn zusammen. Es tauscht Berichtpakete aus und erstellt eine Unicast-Topologietabelle, mit deren Hilfe es die Multicast-Routing-Tabelle zusammenstellt. Diese Tabelle wird dann für das Routing der Multicast-Pakete zugrunde gelegt. Da jeder DVMRP-Router dasselbe Unicast-Routing-Protokoll verwendet, werden Routing-Schleifen vermieden.

Die Menüseite **DVMRP** enthält Links auf Webseiten, die DVMRP-Parameter und -Daten definieren und anzeigen. Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ DVMRP**.

Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

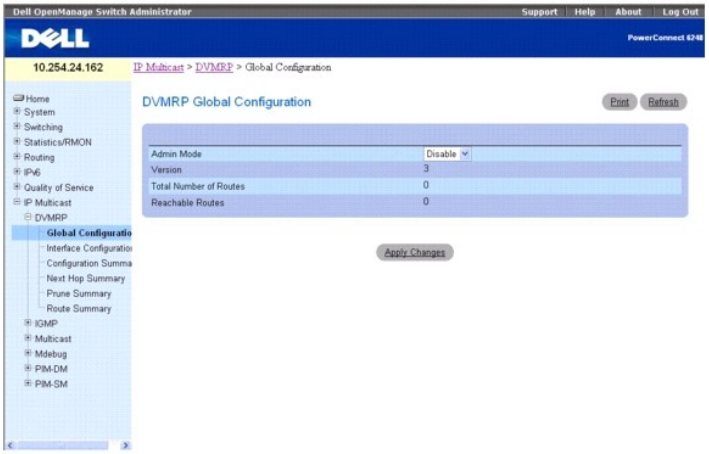
- Globale DVMRP-Konfiguration
- DVMRP-Schnittstellen-Konfiguration
- DVMRP-Konfigurationsübersicht
- Next-Hop-Übersicht
- Prune-Übersicht
- Routen-Übersicht

Globale DVMRP-Konfiguration

Verwenden Sie die Seite **DVMRP Global Configuration** (Globale DVMRP-Konfiguration), um die globalen DVMRP-Einstellungen zu konfigurieren.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ DVMRP→ Global Configuration** (Globale Konfiguration).

Abbildung 13-1. Globale DVMRP-Konfiguration



Die Seite **DVMRP Global Configuration** (Globale DVMRP-Konfiguration) enthält folgende Felder:

Admin Mode (Verwaltungsmodus) – Wählen Sie **Enable** (Aktivieren) oder **Disable** (Deaktivieren) aus dem Dropdown-Menü. Damit setzen Sie den Verwaltungsstatus des DVMRP auf aktiv bzw. inaktiv. Die Standardeinstellung ist **Disable** (Deaktivieren).

Version – Die aktuelle DVMRP-Version.

Total Number of Routes (Gesamtzahl Routen) – Die Anzahl der Routen in der DVMRP-Routing-Tabelle.

Reachable Routes (Erreichbare Routen) – Die Anzahl der Routen in der DVMRP-Routing-Tabelle, die eine nicht unendliche Metrik haben.

Einstellen des DVMRP-Verwaltungsmodus

1. Öffnen Sie die Seite **DVMRP Global Configuration** (Globale DVMRP-Konfiguration).
2. Setzen Sie den **Admin Mode** (Verwaltungsmodus) auf **Enable** (Aktivieren) oder **Disable** (Deaktivieren), um DVMRP ein- bzw. auszuschalten.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Daraufhin wird die DVMRP-Konfiguration gespeichert und das Gerät aktualisiert.

Konfigurieren des DVMRP mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

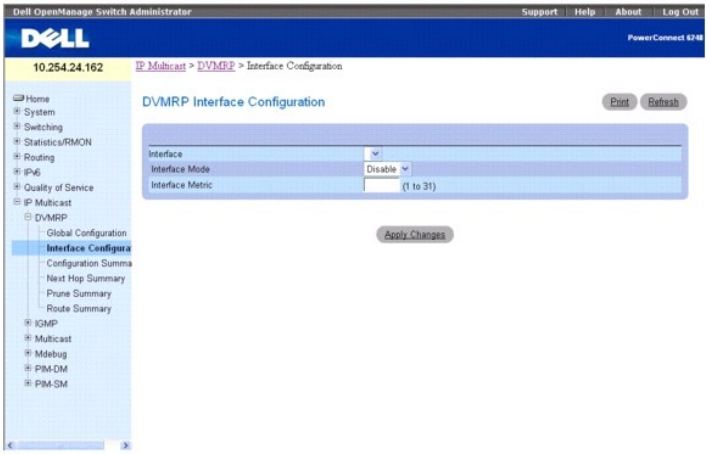
- DVMRP Commands (DVMRP-Befehle)

DVMRP-Schnittstellen-Konfiguration

Verwenden Sie die Seite **DVMRP Interface Configuration** (DVMRP-Schnittstellen-Konfiguration), um eine DVMRP-Schnittstelle zu konfigurieren. Sie müssen mindestens eine Router-Schnittstelle konfigurieren, bevor Sie eine DVMRP-Schnittstelle konfigurieren können. Andernfalls wird eine Meldung angezeigt, dass keine Router-Schnittstellen verfügbar sind, und öffnet sich das Konfigurationsfenster nicht.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast**→ **DVMRP**→ **Interface Configuration** (Schnittstellen-Konfiguration).

Abbildung 13-2. DVMRP-Schnittstellen-Konfiguration



Die Seite **DVMRP Interface Configuration** (DVMRP-Schnittstellen-Konfiguration) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie hier die Schnittstelle aus, für die Daten konfiguriert werden sollen. Sie müssen mindestens eine Router-Schnittstelle konfigurieren, bevor Sie eine DVMRP-Schnittstelle konfigurieren können.

Interface Mode (Schnittstellenmodus) – Wählen Sie **Enable** (Aktivieren) oder **Disable** (Deaktivieren) aus dem Dropdown-Menü, um den Verwaltungsmodus der ausgewählten DVMRP-Routing-Schnittstelle einzustellen.

Interface Metric (Schnittstellen-Metrik) – Geben Sie die DVMRP-Metrik für die ausgewählte Schnittstelle ein. Dieser Wert wird in DVMRP-Nachrichten gesendet als die Kosten für das Erreichen dieses Netzwerks. Zulässige Werte sind 1 bis 31.

Konfigurieren einer DVMRP-Schnittstelle

1. Öffnen Sie die Seite **DVMRP Interface Configuration** (Schnittstellen-Konfiguration).
2. Wählen Sie die Schnittstelle, die Sie konfigurieren wollen, im Feld **Interface** (Schnittstelle).
3. Ändern Sie die übrigen Felder je nach Bedarf.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Daraufhin wird die Schnittstellen-Konfiguration gespeichert und das Gerät aktualisiert.

Konfigurieren einer DVMRP-Schnittstelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

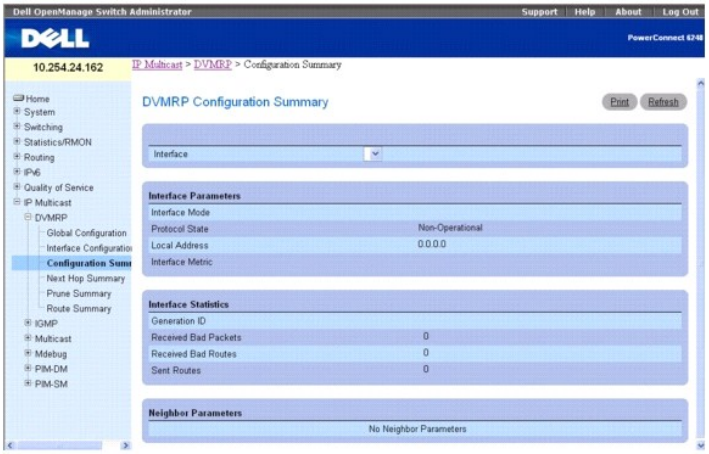
- DVMRP Commands (DVMRP-Befehle)

DVMRP-Konfigurationsübersicht

Verwenden Sie die Seite **DVMRP Configuration Summary** (DVMRP-Konfigurationsübersicht), um die DVMRP-Konfiguration und die Daten für die ausgewählte Schnittstelle anzuzeigen oder auszudrucken. Sie müssen mindestens eine Router-Schnittstelle konfigurieren, bevor Sie die Daten für eine DVMRP-Schnittstelle anzeigen lassen können. Andernfalls wird eine Meldung angezeigt, dass keine Router-Schnittstellen verfügbar sind, und öffnet sich das Konfigurationsübersichts-Fenster nicht.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast**→ **DVMRP**→ **Configuration Summary** (Konfigurationsübersicht).

Abbildung 13-3. DVMRP-Konfigurationsübersicht



Die Seite **DVMRP Configuration Summary** (DVMRP-Konfigurationsübersicht) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie hier die Schnittstelle aus, für die Daten angezeigt werden sollen. Sie müssen mindestens eine Router-Schnittstelle konfigurieren, bevor Sie die Daten für eine DVMRP-Schnittstelle anzeigen lassen können.

Interface Parameters (Schnittstellenparameter)

Interface Mode (Schnittstellenmodus) – Zeigt den Verwaltungsmodus der ausgewählten DVMRP-Routing-Schnittstelle an: **Enable** (Aktivieren) oder **Disable** (Deaktivieren).

Protocol State (Protokollstatus) – Zeigt den Betriebszustand des DVMRP-Protokolls an der ausgewählten Schnittstelle an: **Operational** (betriebsbereit) oder **Non-operational** (nicht betriebsbereit).

Local Address (Lokale Adresse) – Zeigt die IP-Adresse an, die in den über die ausgewählte Schnittstelle übertragenen Paketen als Quelladresse verwendet wird.

Interface Metric (Schnittstellen-Metrik) – Zeigt die Metrik, die für die Berechnung der Distanzvektoren für die ausgewählte Schnittstelle benutzt wird.

Schnittstellenstatistiken

Generation ID (Generations-ID) – Zeigt die DVMRP-Generations-ID an, die von dem Router für die ausgewählte Schnittstelle benutzt wird. Dieser Wert wird jedes Mal zurückgesetzt, wenn eine Schnittstelle (neu) gestartet wird, und in Prune-Nachrichten eingetragen. Eine Änderung der Generations-ID informiert die Nachbar-Router, dass alle bisherigen Informationen über diesen Router verworfen werden müssen.

Received Bad Packets (Empfangene ungültige Pakete) – Die Anzahl der über die ausgewählte Schnittstelle empfangenen ungültigen Pakete.

Received Bad Routes (Empfangene ungültige Routen) – Die Anzahl der über die ausgewählte Schnittstelle empfangenen ungültigen Routen.

Sent Routes (Gesendete Routen) – Die Anzahl der über die ausgewählte Schnittstelle gesendeten Routen.

Neighbor Parameters (Nachbar-Parameter)

Neighbor IP (Nachbar-IP-Adresse) – Die IP-Adresse des Nachbarn, dessen Informationen angezeigt werden.

State (Status) – Der Status des angegebenen Nachbar-Routers an der ausgewählten Schnittstelle: **active** (aktiv) oder **down** (inaktiv).

Neighbor Uptime (Nachbar-Betriebszeit) – Die DVMRP-Betriebszeit für den angegebenen Nachbarn an der ausgewählten Schnittstelle. Dies ist die Zeit, seit der Nachbar-Eintrag erkannt wurde.

Neighbor Expiry Time (Nachbar-Ablaufzeit) – Die DVMRP-Ablaufzeit für den angegebenen Nachbarn an der ausgewählten Schnittstelle. Dies ist die Zeit, die noch verbleibt, bevor dieser Nachbar-Eintrag abläuft; sie gilt nicht, wenn der Nachbar-Router inaktiv ist.

Generation ID (Generations-ID) – Die DVMRP-Generations-ID für den angegebenen Nachbarn an der ausgewählten Schnittstelle.

Major Version (Hauptversion) – Die DVMRP-Major-Version für den angegebenen Nachbarn an der ausgewählten Schnittstelle.

Minor Version (Nebenversion) – Die DVMRP-Minor-Version für den angegebenen Nachbarn an der ausgewählten Schnittstelle.

Capabilities(Fähigkeiten) – Die DVMRP-Fähigkeiten des angegebenen Nachbarn an der ausgewählten Schnittstelle.

Received Routes (Empfangene Routen) – Die Anzahl der für den angegebenen Nachbarn an der ausgewählten Schnittstelle empfangenen Routen.

Received Bad Packets (Empfangene ungültige Pakete) – Die Anzahl der für den angegebenen Nachbarn an der ausgewählten Schnittstelle empfangenen ungültigen Pakete.

Received Bad Routes (Empfangene ungültige Routen) – Die Anzahl der für den angegebenen Nachbarn an der ausgewählten Schnittstelle empfangenen ungültigen Routen.

Anzeigen der DVMRP-Konfigurationsübersicht mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

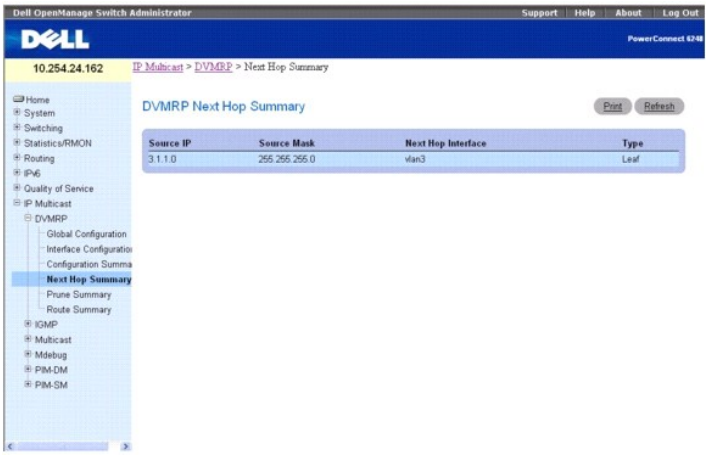
- DVMRP Commands (DVMRP-Befehle)

Next-Hop-Übersicht

Verwenden Sie die Seite **Next Hop Summary** (Next-Hop-Übersicht), um die Next-Hop-Übersicht nach Quell-IP anzuzeigen oder auszudrucken.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast**→ **DVMRP**→ **Next Hop Summary** (Next-Hop-Übersicht).

Abbildung 13-4. Next-Hop-Übersicht



Die Seite **Next Hop Summary** (Next-Hop-Übersicht) enthält folgende Felder:

Source IP (Quell-IP-Adresse) – Zeigt die IP-Adresse an, die mit der Quellmaske verwendet wird, um das Quellnetzwerk für diesen Tabelleneintrag zu identifizieren.

Source Mask (Quellmaske) – Zeigt die Netzwerkmaske an, die zusammen mit der Quell-IP-Adresse verwendet wird.

Next Hop Interface (Next-Hop-Schnittstelle) – Zeigt die Ausgangsschnittstelle für diesen nächsten Hop.

Type (Typ) – Zeigt den Typ des nächsten Hops. **Leaf** (Blatt) bedeutet, dass an der Ausgangsschnittstelle keine abhängigen Downstream-Nachbarn mehr vorhanden sind. Andernfalls lautet die Typangabe **Branch** (Zweig).

Anzeigen der Next-Hop-Übersicht mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

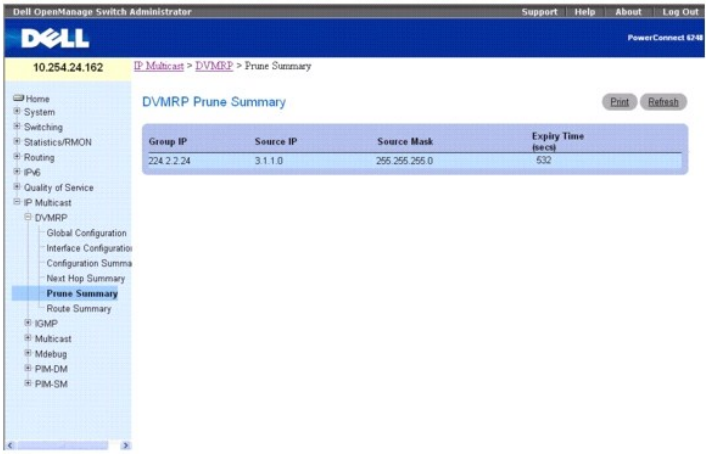
- DVMRP Commands (DVMRP-Befehle)

Prune-Übersicht

Verwenden Sie die Seite **Prune Summary** (Prune-Übersicht), um die Prune-Übersicht nach der IP-Adresse der Gruppe (Group IP) anzuzeigen oder auszudrucken.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast**→ **DVMRP**→ **Prune Summary** (Prune-Übersicht).

Abbildung 13-5. Prune-Übersicht



Die Seite **Prune Summary** (Prune-Übersicht) enthält folgende Felder:

Group IP (Gruppen-IP-Adresse) – Die Gruppenadresse, die gekürzt wurde.

Source IP (Quell-IP-Adresse) – Die Adresse der Quelle oder des Quellnetzwerks, die gekürzt wurde.

Source Mask (Quellmaske) – Die Subnetzmaske, die mit der Quell-IP-Adresse kombiniert wird, um die Quelle oder das Quellnetzwerk zu identifizieren, die gekürzt wurde.

Expiry Time (secs) (Ablaufzeit) – Die verbleibende Zeit bis zum Verfall dieses Prune am Upstream-Nachbarn. Wenn von den Downstream-Nachbarn keine Prune-Nachrichten empfangen wurden, wird hier der Standardwert für den Prune-Gültigkeits-Timer eingesetzt, andernfalls wird er auf den kleinsten empfangenen Wert oder auf den Standard-Timer eingestellt, je nachdem, welcher Wert kleiner ist.

Anzeigen der Prune-Übersicht mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

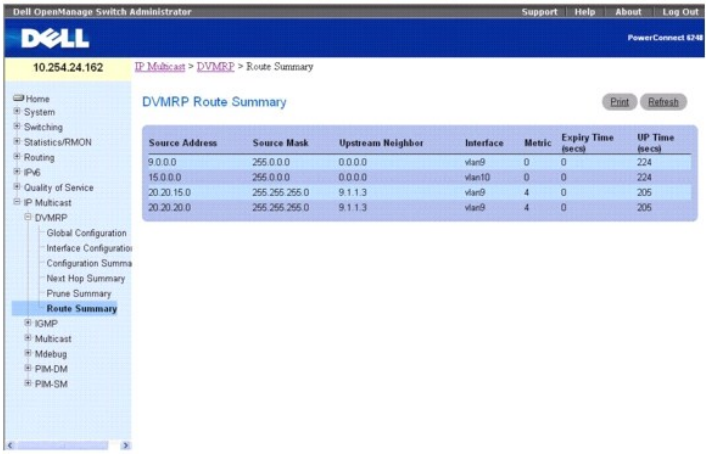
- DVMRP Commands (DVMRP-Befehle)

Routen-Übersicht

Verwenden Sie die Seite **Route Summary** (Routen-Übersicht), um die Übersicht über die DVMRP-Routen anzuzeigen oder auszudrucken.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ DVMRP→ Route Summary** (Routen-Übersicht).

Abbildung 13-6. Routen-Übersicht



Die Seite **Route Summary** (Routen-Übersicht) enthält folgende Felder:

Source Address (Quelladresse) – Zeigt die Netzwerkadresse an, die mit der Quellmaske verwendet wird, um die Quellen für diesen Eintrag zu identifizieren.

Source Mask (Quellmaske) – Die Subnetzmaske, die mit der Quelladresse kombiniert wird, um die Quellen für diesen Eintrag zu identifizieren.

Upstream Neighbor (Upstream-Nachbar) – Die Adresse des Upstream-Nachbarn (z. B. RPF-Nachbar), von dem IP-Datagramme aus diesen Quellen empfangen werden.

Interface (Schnittstelle) – Die Schnittstelle, an der die von diesen Quellen gesendeten Datagramme empfangen werden. Ein Wert "0" bedeutet üblicherweise, dass die Route eine Aggregatroute ist, für die keine Next-Hop-Schnittstelle vorhanden ist.

Metric (Metrik) – Die Entfernung zum Quell-Subnetz in Hops.

Expiry Time (Ablaufzeit) – Die minimale verbleibende Zeit bis zum Verfall dieses Eintrags.

Up Time (Betriebszeit) – Die Zeit, seit die von diesem Eintrag repräsentierte Route von dem Router erkannt wurde.

Anzeigen der DVMRP-Routen-Übersicht mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- DVMRP Commands (DVMRP-Befehle)

IGMP

Das Internet Group Management Protocol (IGMP) wird von IPv4-Systemen (Hosts und Routern) verwendet, um deren IP-Multicast-Gruppenmitgliedschaften an benachbarte Multicast-Router zu melden. Die Systeme der 6200-Reihe führen die Rolle des Multicast-Routers des IGMP-Protokolls aus, das heißt, sie erfassen die Mitgliedschaftsinformationen, die für aktives Multicast-Routing benötigt werden. Derzeit unterstützt die 6200-Reihe die Multicast-Routing-Protokolle DVMRP, PIM-DM und PIM-SM.

Die 6200-Reihe unterstützt die IGMP-Version 3. Neu in Version 3 ist die Unterstützung des Source Filtering, also der Fähigkeit eines Systems, sein Interesse anzumelden, ausschließlich von bestimmten Quelladressen, wie für die Unterstützung des Source-Specific Multicast [SSM, quellenspezifisches Multicast] erforderlich, oder von allen Quellen außer bestimmten Quelladressen Pakete zu empfangen, die an eine bestimmte Multicast-Adresse gesendet werden. Die Version 3 ist für Zusammenarbeit mit den Versionen 1 und 2 ausgelegt.

Die Menüseite **IGMP** enthält Links auf Webseiten, die IGMP-Parameter und -Daten definieren und anzeigen. Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ IGMP**.

Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

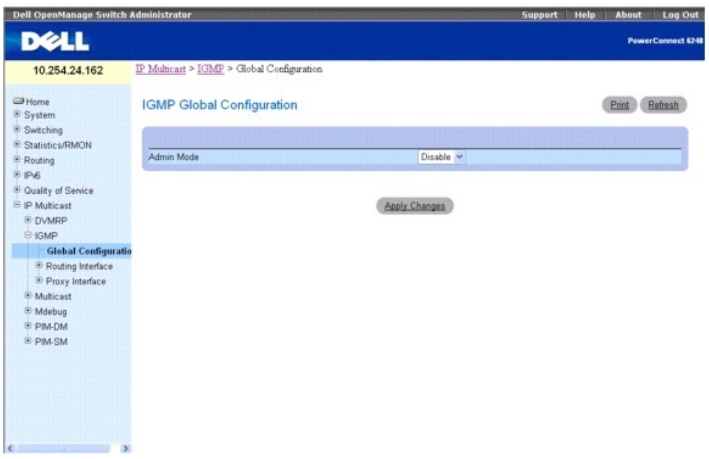
- Globale IGMP-Konfiguration
- Routing-Schnittstelle
- Proxy-Schnittstelle

Globale IGMP-Konfiguration

Verwenden Sie die Seite **IGMP Global Configuration** (Globale IGMP-Konfiguration), um das IGMP im System zu aktivieren bzw. zu deaktivieren.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ IGMP→ Global Configuration** (Globale Konfiguration).

Abbildung 13-7. Globale IGMP-Konfiguration



Die Seite **IGMP Global Configuration** (Globale IGMP-Konfiguration) enthält folgendes Feld:

Admin Mode (Verwaltungsmodus) - Wählen Sie **Enable** (Aktivieren) oder **Disable** (Deaktivieren) aus dem Dropdown-Menü, um den Verwaltungsstatus des IGMP im Router auf Aktiv oder Inaktiv zu setzen. Die Standardeinstellung ist **Disable** (Deaktivieren).

Einstellen des IGMP-Modus

1. Öffnen Sie die Seite **IGMP Global Configuration** (Globale IGMP-Konfiguration).
2. Setzen Sie den **Admin Mode** (Verwaltungsmodus) auf Enable (Aktivieren) oder Disable (Deaktivieren), um IGMP ein- bzw. auszuschalten.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Daraufhin wird die IGMP-Konfiguration gespeichert und das Gerät aktualisiert.

Einstellen des IGMP-Modus mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- IGMP Commands (IGMP-Befehle)

Routing-Schnittstelle

Die Menüseite **Routing Interface** (Routing-Schnittstelle) enthält Links auf Webseiten, die IGMP-Routing-Parameter und -Daten konfigurieren und anzeigen. Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ IGMP→ Routing Interface** (Routing-Schnittstelle). Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

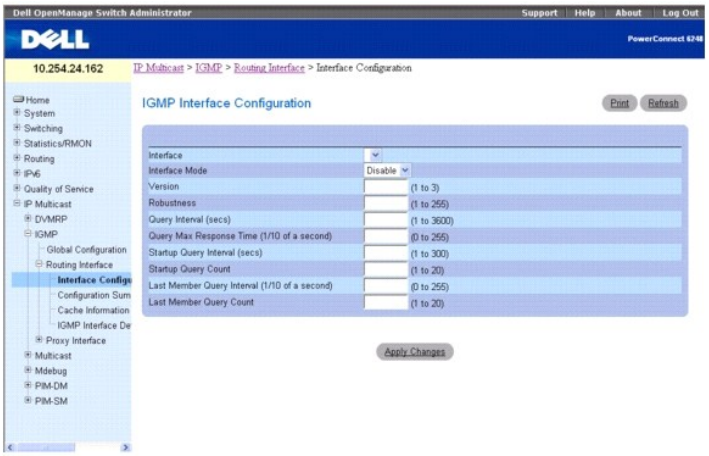
- IGMP-Schnittstellenkonfiguration
- IGMP-Konfigurationsübersicht
- IGMP-Cache-Informationen
- Detaillierte Mitgliedschaftsinformationen zur IGMP-Schnittstelle

IGMP-Schnittstellenkonfiguration

Verwenden Sie die Seite **IGMP Interface Configuration** (IGMP-Schnittstellenkonfiguration), um Schnittstellenparameter für den Router zu konfigurieren und/oder anzuzeigen. Sie müssen mindestens eine gültige Routing-Schnittstelle konfigurieren, bevor Sie auf diese Seite zugreifen und IP Multicast IGMP konfigurieren können.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ IGMP→ Routing Interface (Routing-Schnittstelle)→ Interface Configuration (Schnittstellenkonfiguration)**.

Abbildung 13-8. IGMP-Schnittstellenkonfiguration



Die Seite **IGMP Interface Configuration** (IGMP-Schnittstellenkonfiguration) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie aus dem Dropdown-Menü die Schnittstelle aus, für die Daten angezeigt oder konfiguriert werden sollen.

Interface Mode (Schnittstellenmodus) – Wählen Sie **Enable** (Aktivieren) oder **Disable** (Deaktivieren) aus dem Dropdown-Menü, um den Verwaltungsstatus des IGMP an der ausgewählten Schnittstelle einzustellen. Die Standardeinstellung ist **Disable** (Deaktivieren).

Version – Geben Sie die Version des IGMP ein, die Sie an der ausgewählten Schnittstelle konfigurieren wollen. Gültig sind die Werte 1 bis 3, Standardwert ist 3. Dieses Feld können Sie nur dann konfigurieren, wenn der IGMP-Schnittstellenmodus aktiviert ist.

Robustness (Robustheit) – Geben Sie den Robustheitswert ein. Diese Variable erlaubt die Abstimmung entsprechend dem erwarteten Paketverlust in einem Subnetz. Wenn Sie in einem Subnetz Datenverluste erwarten, sollten Sie für diesen Parameter einen höheren Wert eingeben. Das IGMP ist robust (Robustheits-Variable-1) gegen Paketverluste. Zulässige Werte sind 1 bis 255. Der Standardwert ist 2.

Query Interval (secs) (Abfrageintervall) – Geben Sie den Abstand in Sekunden ein, in dem IGMP-Host-Abfragepakete auf dieser Schnittstelle übertragen werden sollen. Zulässige Werte sind 1 bis 3600. Der Standardwert ist 125.

Query Max Response Time (1/10 of a second) (Max. Reaktionszeit auf Abfrage) – Geben Sie die maximale Zeit für die Reaktion auf Abfragen, die in IGMPv2-Abfragen auf dieser Schnittstelle angegeben werden soll, in Zehntelsekunden an. Der Standardwert ist 100. Zulässige Werte sind 0 bis 255.

Startup Query Interval (secs) (Start-Abfrageintervall) – Geben Sie die Anzahl Sekunden zwischen der Übertragung von Start-Abfragen auf der ausgewählten Schnittstelle an. Zulässige Werte sind 1 bis 300. Der Standardwert ist 31.

Startup Query Count (Anzahl Start-Abfragen) – Geben Sie die Anzahl der Abfragen ein, die bei Systemstart gesendet werden sollen. Zulässige Werte sind 1 bis 20. Der Standardwert ist 2.

Last Member Query Interval (1/10 of a second) (Abfrageintervall letztes Mitglied) – Geben Sie das Abfrageintervall für das letzte Mitglied in Zehntelsekunden an. Dies ist die maximale Reaktionszeit, die in gruppenspezifische Abfragen einzutragen ist, welche als Reaktion auf Leave Group-Nachrichten gesendet werden, und gleichzeitig die Zeit zwischen gruppenspezifischen Abfragenachrichten. Zulässige Werte sind 0 bis 255. Der Standardwert ist 10. Dieser Wert wird für die IGMP-Version 1 nicht verwendet.

Last Member Query Count (Anzahl Abfragen letztes Mitglied) – Geben Sie die Anzahl der Abfragen ein, die bei Eingang eines Leave Group-Berichts gesendet werden sollen. Zulässige Werte sind 1 bis 20. Der Standardwert ist 2.

Konfigurieren einer IGMP-Routing-Schnittstelle

1. Öffnen Sie die Seite **IGMP Interface Configuration** (IGMP-Schnittstellenkonfiguration).
2. Wählen Sie die Schnittstelle, die Sie konfigurieren wollen, im Feld **Interface** (Schnittstelle).
3. Ändern Sie die übrigen Felder je nach Bedarf.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Daraufhin wird die Schnittstellen-Konfiguration gespeichert und das Gerät aktualisiert.

Konfigurieren einer IGMP-Routing-Schnittstelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

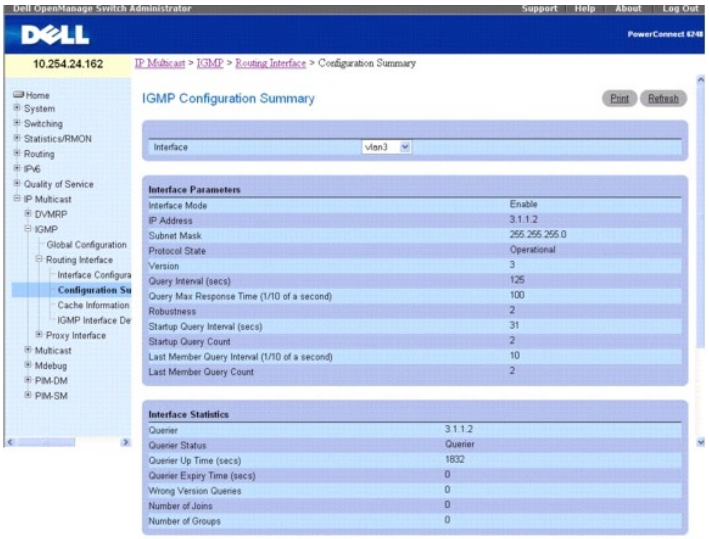
- IGMP Commands (IGMP-Befehle)

IGMP-Konfigurationsübersicht

Verwenden Sie die Seite **IGMP Configuration Summary** (IGMP-Konfigurationsübersicht), um IGMP-Routing-Parameter und -Daten anzuzeigen. Sie müssen mindestens eine gültige IGMP-Router-Schnittstelle konfigurieren, bevor Sie auf diese Seite zugreifen können.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ IGMP→ Routing Interface (Routing-Schnittstelle)→ Configuration Summary (Konfigurationsübersicht)**.

Abbildung 13-9. IGMP-Konfigurationsübersicht



Die Seite **IGMP Configuration Summary** (IGMP-Konfigurationsübersicht) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie hier die Schnittstelle aus, für die Daten angezeigt werden sollen.

Interface Parameters (Schnittstellenparameter)

Interface Mode (Schnittstellenmodus) – Der Verwaltungsstatus des IGMP an der ausgewählten Schnittstelle.

IP Address (IP-Adresse) – Die IP-Adresse der ausgewählten Schnittstelle.

Subnet Mask (Subnetzmaske) – Die Subnetzmaske für die IP-Adresse der ausgewählten Schnittstelle.

Protocol State (Protokollstatus) – Zeigt den Betriebszustand des IGMP-Protokolls an der ausgewählten Schnittstelle an.

Version – Die an der ausgewählten Schnittstelle konfigurierte IGMP-Version.

Query Interval (secs) (Abfrageintervall) – Der Abstand in Sekunden, in dem IGMP-Host-Abfragepakete auf der ausgewählten Schnittstelle übertragen werden.

Query Max Response Time (1/10 of a second) (Max. Reaktionszeit auf Abfragen) – Die maximale Zeit (in Zehntelsekunden) für die Reaktion auf Abfragen, die in den von der ausgewählten Schnittstelle gesendeten IGMPv2-Abfragen angegeben werden soll.

Robustness (Robustheit) – Der Robustheits-Parameter für die ausgewählte Schnittstelle. Diese Variable erlaubt die Abstimmung entsprechend dem erwarteten Paketverlust in einem Subnetz. Wenn in einem Subnetz Paketverluste erwartet werden, sollte die Robustheits-Variable erhöht werden. Das IGMP ist robust (Robustheits-Variable-1) gegen Paketverluste.

Startup Query Interval (secs) (Start-Abfrageintervall) – Das Intervall (in Sekunden), in dem Start-Abfragen auf der ausgewählten Schnittstelle gesendet werden.

Startup Query Count (Anzahl Start-Abfragen) – Die Anzahl der Abfragen, die bei Systemstart gesendet werden sollen.

Last Member Query Interval (1/10 of a second) (Abfrageintervall für das letzte Mitglied, 1/10-Sekunde) – Das Abfrageintervall für das letzte Mitglied ist die maximale Reaktionszeit, die in gruppenspezifische Abfragen eingetragen wird, welche als Reaktion auf Leave Group-Nachrichten gesendet werden, und gleichzeitig die Zeit zwischen gruppenspezifischen Abfragenachrichten. Dieser Wert kann abgestimmt werden, um die Leave-Latenzzeit des Netzwerks zu verändern. Ein geringerer Wert verkürzt die Zeit für das Erkennen, dass das letzte Mitglied einer Gruppe verloren gegangen ist. Dieser Wert wird für die IGMP-Version 1 nicht verwendet.

Last Member Query Count (Anzahl Abfragen letztes Mitglied) – Die Anzahl der Abfragen, die bei Eingang eines Leave Group-Berichts gesendet werden sollen.

Schnittstellenstatistiken

Querier – Die Adresse des IGMP-Queriers in dem IP-Subnetzk, mit dem die ausgewählte Schnittstelle verbunden ist.

Querier Status (Querier-Status) – Zeigt an, ob sich die ausgewählte Schnittstelle im Querier-Modus oder im Non-Querier-Modus befindet.

Querier Up Time (secs) (Querier-Betriebszeit) – Zeit in Sekunden seit dem letzten Wechsel des IGMP-Schnittstellen-Queriers.

Querier Expiry Time (secs) (Querier-Ablaufzeit) – Die verbleibende Zeit in Sekunden, bevor der Other-Querier-Present-Timer abläuft. Wenn das lokale System der Querier ist, ist dieser Wert 0.

Wrong Version Queries (Abfragen in falscher Version) – Die Anzahl von an der ausgewählten Schnittstelle empfangenen Abfragen, deren IGMP-Version nicht derjenigen entspricht, die für diese Schnittstelle konfiguriert wurde, während der Lebensdauer des Eintrags. Bei IGMP müssen alle Router in einem LAN mit derselben IGMP-Version arbeiten. Daher wird ein Konfigurationsfehler angezeigt, wenn Abfragen mit einer falschen Versionsnummer eingehen.

Number of Joins (Anzahl Beitritte) – Gibt an, wie häufig an der ausgewählten Schnittstelle eine Gruppenmitgliedschaft hinzugefügt wurde, d. h. wie häufig ein Eintrag für diese Schnittstelle in die Cache-Tabelle eingefügt wurde. Dies gibt einen Hinweis auf den Grad der IGMP-Aktivität an dieser Schnittstelle.

Number of Groups (Anzahl Gruppen) – Die aktuelle Anzahl von Einträgen für die ausgewählte Schnittstelle in der Cache-Tabelle.

Anzeigen der IGMP-Routing-Konfiguration mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

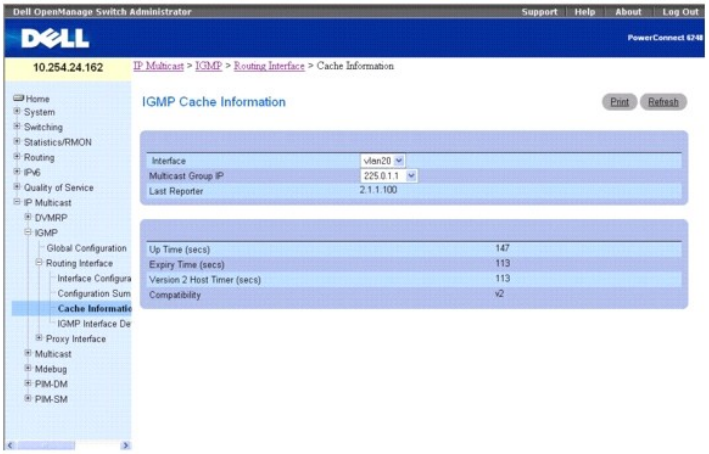
- IGMP Commands (IGMP-Befehle)

IGMP-Cache-Informationen

Verwenden Sie die Seite **IGMP Cache Information** (IGMP-Cache-Informationen), um Cache-Parameter und -Daten für eine IP-Multicast-Gruppenadresse anzuzeigen. Sie müssen mindestens eine gültige IGMP-Router-Schnittstelle konfigurieren, bevor Sie auf diese Seite zugreifen können. Außerdem müssen Berichte zur Gruppenmitgliedschaft an der ausgewählten Schnittstelle eingegangen sein, damit hier Daten angezeigt werden.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ IGMP→ Routing Interface (Routing-Schnittstelle)→ Cache Information (Cache-Informationen)**.

Abbildung 13-10. IGMP-Cache-Informationen



Die Seite **IGMP Cache Information (IGMP-Cache-Informationen) enthält folgende Felder:**

Interface (Schnittstelle) – Wählen Sie hier die Schnittstelle aus, für die Daten angezeigt werden sollen.

Multicast Group IP (Multicast-Gruppen-IP-Adresse) – Wählen Sie hier die IP-Multicast-Gruppenadresse aus, für die Daten angezeigt werden sollen. Wenn an der ausgewählten Schnittstelle keine Gruppen-Mitgliedschaftsberichte empfangen wurden, steht diese Option nicht zur Verfügung und werden die Daten dieser Seite nicht angezeigt.

Last Reporter (Letzter Berichtender) – Die IP-Adresse der Quelle des letzten eingegangenen Mitgliedschaftsberichts, der für die IP-Multicast-Gruppenadresse an der ausgewählten Schnittstelle empfangen wurde.

Up Time (Betriebszeit) – Die Zeit seit Erstellung dieses Eintrags.

Expiry Time (Ablaufzeit) – Die minimale verbleibende Zeit bis zum Verfall dieses Eintrags.

Version 1 Host Timer – Die Zeit, die verbleibt, bis der lokale Router annimmt, dass in dem mit dieser Schnittstelle verbundenen IP-Subnetz keine Mitglieder mit der IGMP-Version 1 mehr vorhanden sind. Wenn ein IGMPv1-Mitgliedschaftsbericht empfangen wird, wird dieser Timer auf den Gruppenmitgliedschafts-Timer zurückgesetzt. Solange dieser Timer einen anderen Wert als 0 hat, ignoriert der lokale Router alle IGMPv2-Leave-Nachrichten für diese Gruppe, die er über die ausgewählte Schnittstelle empfängt. Dieses Feld wird nur angezeigt, wenn die Schnittstelle für die IGMP-Version 1 konfiguriert ist.

Version 2 Host Timer – Die Zeit, die verbleibt, bis der lokale Router annimmt, dass in dem mit dieser Schnittstelle verbundenen IP-Subnetz keine Mitglieder mit der IGMP-Version 2 mehr vorhanden sind. Wenn ein IGMPv2-Mitgliedschaftsbericht empfangen wird, wird dieser Timer auf den Gruppenmitgliedschafts-Timer zurückgesetzt. Solange dieser Timer einen anderen Wert als 0 hat, ignoriert der lokale Router alle IGMPv1- und IGMPv3-Leave-Nachrichten für diese Gruppe, die er über die ausgewählte Schnittstelle empfängt. Dieses Feld wird nur angezeigt, wenn die Schnittstelle für die IGMP-Version 2 konfiguriert ist.

Compatibility (Kompatibilität) – Dieser Parameter zeigt den Gruppenkompatibilitätsmodus (v1, v2 und v3) für diese Gruppe an der angegebenen Schnittstelle.

Filter Mode (Filtermodus) – Der Source-Filter-Modus (Include/Exclude/NA - Einschließen/Ausschließen/Nicht verfügbar) für die angegebene Gruppe an dieser Schnittstelle. Wenn der NA-Modus aktiv ist, ist dieses Feld leer.

Anzeigen der Cache-Informationen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

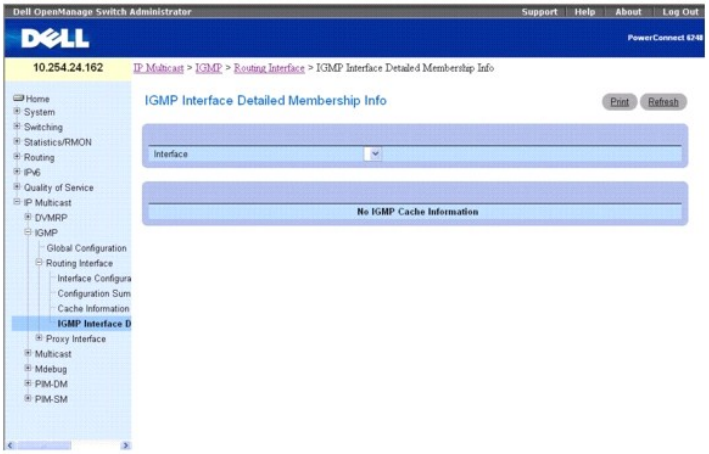
- IGMP Commands (IGMP-Befehle)

Detaillierte Mitgliedschaftsinformationen zur IGMP-Schnittstelle

Verwenden Sie die Seite **IGMP Interface Detailed Membership Info** (Detaillierte Mitgliedschaftsinformationen zur IGMP-Schnittstelle), um ausführliche Informationen zur Mitgliedschaft einer Schnittstelle anzuzeigen. Sie müssen mindestens eine gültige IGMP-Router-Schnittstelle konfigurieren, bevor Sie auf diese Seite zugreifen können. Außerdem müssen Berichte zur Gruppenmitgliedschaft an der ausgewählten Schnittstelle eingegangen sein, damit hier Daten angezeigt werden.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ IGMP→ Routing Interface (Routing-Schnittstelle)→ IGMP Interface (IGMP-Schnittstelle)Detailed Membership Info (Detaillierte Mitgliedschaftsinformationen)** .

Abbildung 13-11. Detaillierte Mitgliedschaftsinformationen zur IGMP-Schnittstelle



Die Seite **IGMP Interface Detailed Membership Info** (Detaillierte Mitgliedschaftsinformationen zur IGMP-Schnittstelle) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie hier die Schnittstelle aus, für die Daten angezeigt werden sollen.

Multicast Group IP (Multicast-Gruppen-IP-Adresse) – Wählen Sie hier die IP-Multicast-Gruppenadresse aus, für die Daten angezeigt werden sollen. Wenn an der ausgewählten Schnittstelle keine Gruppen-Mitgliedschaftsberichte empfangen wurden, steht diese Option nicht zur Verfügung und werden die übrigen Felder nicht angezeigt.

Interface (Schnittstelle) – Die Schnittstelle, an der Multicast-Pakete weitergeleitet werden.

Group Compatibility Mode (Gruppenkompatibilitätsmodus) – Der Gruppenkompatibilitätsmodus (v1, v2 und v3) für diese Gruppe an der angegebenen Schnittstelle.

Source Filter Mode (Source-Filter-Modus) – Der Source-Filter-Modus (Include/Exclude/NA - Einschließen/Ausschließen/Nicht verfügbar) für die angegebene Gruppe an dieser Schnittstelle.

Source Hosts (Quell-Hosts) – Die Quelladressen, die Mitglieder dieser Multicast-Adresse sind.

Expiry Time (Ablaufzeit) – Das Ablaufzeitintervall für alle Quelladressen, die Mitglieder dieser Multicast-Adresse sind. Dies ist die Zeit, nach der der angegebene Quelleintrag verfällt.

Anzeigen von detaillierten Mitgliedschaftsinformationen zur IGMP-Schnittstelle

1. Öffnen Sie die Seite **IGMP Interface Detailed Membership Info** (Detaillierte Mitgliedschaftsinformationen zur IGMP-Schnittstelle).
2. Wählen Sie die Schnittstelle, die Sie anzeigen wollen, im Dropdown-Menü **Interface** (Schnittstelle).
3. Wählen Sie die gewünschte **Multicast Group IP** (Multicast-Gruppen-IP-Adresse) aus.

   Daraufhin werden ausführliche Mitgliedschaftsinformationen für diese Schnittstelle und diese Multicast-Gruppen-IP-Adresse angezeigt.

Anzeigen von detaillierten Mitgliedschaftsinformationen zur IGMP-Schnittstelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- IGMP Commands (IGMP-Befehle)

Proxy-Schnittstelle

Mit dem IGMP-Proxy soll ein Multicast-Router befähigt werden, Informationen zur Mitgliedschaft in Multicast-Gruppen zu erfassen und auf der Grundlage dieser Gruppen-Mitgliedschaftsinformationen Multicast-Pakete weiterzuleiten. Der IGMP-Proxy kann nur in bestimmten Topologien arbeiten, für die kein Multicast-Routing-Protokoll (d. h. DVMRP, PIM-DM und PIM-SM) erforderlich ist und die eine baumartige Struktur aufweisen, da er Funktionen wie etwa Spanning Tree zum Korrigieren von Schleifen in Paketrouten nicht unterstützt.

Die Menüseite **Proxy Interface** (Proxy-Schnittstelle) enthält Links auf Webseiten, die Proxy-Schnittstellenparameter und -Daten definieren und anzeigen. Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ IGMP→ Proxy Interface** (Proxy-Schnittstelle). Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

- IGMP-Proxy-Schnittstellenkonfiguration
- IGMP-Proxy-Konfigurationsübersicht
- IGMP-Proxy-Schnittstellen-Mitgliedschaftsinformationen
- Detaillierte IGMP-Proxy-Schnittstellen-Mitgliedschaftsinformationen

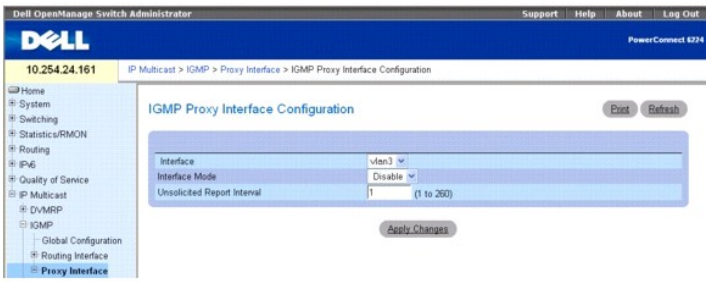
IGMP-Proxy-Schnittstellenkonfiguration

Der IGMP-Proxy wird von dem IGMP-Router (IPv4-System) dafür benutzt, dass das System IGMP-Host-Nachrichten im Namen der Hosts ausgeben kann, die das System über standardmäßige IGMP-Router-Schnittstellen erkannt hat. Auf diese Weise fungiert diese Funktion als Proxy für alle Hosts, die auf ihren Router-Schnittstellen angesiedelt sind.

Verwenden Sie die Seite **IGMP Proxy Interface Configuration** (IGMP-Proxy-Schnittstellen-Konfiguration), um eine Proxy-Schnittstelle zu konfigurieren. Sie müssen mindestens eine Router-Schnittstelle konfiguriert haben, bevor Sie Daten für eine IGMP-Proxy-Schnittstelle konfigurieren und anzeigen können, und diese sollte keine IGMP-Routing-Schnittstelle sein.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast**→ **IGMP**→ **Proxy Interface (Proxy-Schnittstelle)**→ **Interface Configuration** (Schnittstellen-Konfiguration).

Abbildung 13-12. IGMP-Proxy-Schnittstellenkonfiguration



Die Seite **IGMP Proxy Interface Configuration** (IGMP-Proxy-Schnittstellenkonfiguration) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie aus dem Dropdown-Menü den Port aus, für den Daten angezeigt oder konfiguriert werden sollen. Sie müssen mindestens eine Router-Schnittstelle konfiguriert haben, bevor Sie Daten für eine IGMP-Proxy-Schnittstelle konfigurieren und anzeigen können, und diese sollte keine IGMP-Routing-Schnittstelle sein. Dieses Feld können Sie nur dann konfigurieren, wenn der Schnittstellenmodus deaktiviert ist.

Interface Mode (Schnittstellenmodus) – Wählen Sie **Enable** (Aktivieren) oder **Disable** (Deaktivieren) aus dem Dropdown-Menü, um den Verwaltungsstatus des IGMP-Proxy an der ausgewählten Schnittstelle einzustellen. Die Standardeinstellung ist **Disable** (Deaktivieren). Die globalen Verwaltungsmodi für Routing, IGMP und Multicast sollten aktiviert sein, um den IGMP-Proxy-Schnittstellenmodus zu aktivieren.

Unsolicited Report Interval (Intervall nicht angeforderte Berichte) – Geben Sie hier das Zeitintervall für nicht angeforderte Berichte in Sekunden ein. Das Unsolicited Report Interval gibt die Zeit zwischen Wiederholungen des ersten Berichts eines Hosts über die Mitgliedschaft in einer Gruppe an. Zulässige Werte sind 1 bis 260. Der Standardwert ist 1.

Konfigurieren einer Proxy-Schnittstelle

1. Öffnen Sie die Seite **IGMP Proxy Interface Configuration** (IGMP-Proxy-Schnittstellenkonfiguration).
2. Wählen Sie die Schnittstelle, die Sie anzeigen wollen, im Dropdown-Menü **Interface** (Schnittstelle).
3. Ändern Sie die übrigen Felder je nach Bedarf.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Daraufhin wird die Proxy-Schnittstellen-Konfiguration gespeichert und das Gerät aktualisiert.

Konfigurieren einer IGMP-Proxy-Schnittstelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

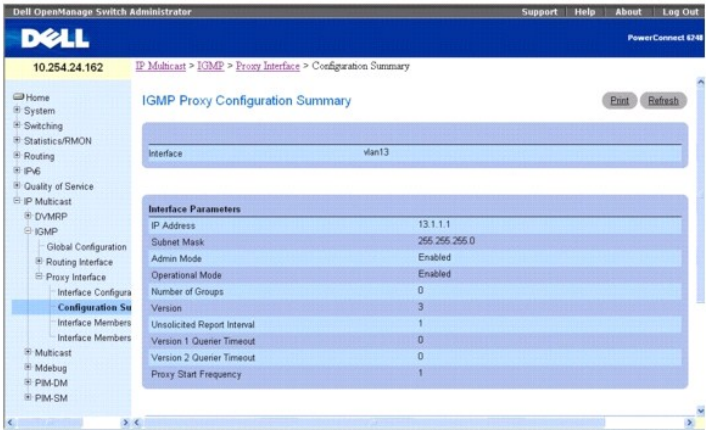
- IGMP-Proxy Commands (IGMP-Proxy-Befehle)

IGMP-Proxy-Konfigurationsübersicht

Verwenden Sie die Seite **IGMP Proxy Interface Configuration Summary** (IGMP-Proxy-Schnittstellen-Konfigurationsübersicht), um die Konfigurationen der Proxy-Schnittstellen nach Schnittstelle anzuzeigen. Sie müssen mindestens eine Router-Schnittstelle konfiguriert haben, bevor auf dieser Seite Daten angezeigt werden.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast**→ **IGMP**→ **Proxy Interface (Proxy-Schnittstelle)**→ **Configuration Summary (Konfigurationsübersicht)**.

Abbildung 13-13. IGMP-Proxy-Konfigurationsübersicht



Die Seite **IGMP Proxy Configuration Summary** (IGMP-Proxy-Konfigurationsübersicht) enthält folgende Felder:

Interface (Schnittstelle) – Gibt die Schnittstelle an, an der IGMP-Proxy aktiviert ist. Es kann immer nur eine IGMP-Proxy-Schnittstelle vorhanden sein.

IP Address (IP-Adresse) – Die IP-Adresse der IGMP-Proxy-Schnittstelle.

Subnet Mask (Subnetzmaske) – Die Subnetzmaske für die IP-Adresse der IGMP-Proxy-Schnittstelle.

Admin Mode (Verwaltungsmodus) – Der Verwaltungsstatus des IGMP-Proxy an der ausgewählten Schnittstelle.

Operational Mode (Betriebsmodus) – Der Betriebszustand der IGMP-Proxy-Schnittstelle.

Number of Groups (Anzahl Gruppen) – Die aktuelle Anzahl von Multicast-Gruppen-Einträgen für die IGMP-Proxy-Schnittstelle in der Cache-Tabelle.

Version – Die an der ausgewählten IGMP-Proxy-Schnittstelle konfigurierte IGMP-Version.

Unsolicited Report Interval (Intervall nicht angeforderte Berichte) – Gibt die Zeit zwischen Wiederholungen des ersten Berichts eines Hosts über die Mitgliedschaft in einer Gruppe an. Standard: 1 Sekunde.

Version 1 Querier Timeout (Zeitüberschreitung für Version-1-Querier) – Der Zeitüberschreitungswert für Querier der älteren IGMP-Version 1 in Sekunden. Das Older Version Querier Interval (Intervall Querier ältere Version) ist der Zeitüberschreitungswert für die Wiederumstellung eines Hosts auf den IGMPv3-Modus, nachdem eine Abfrage einer älteren Version erkannt wurde. Wenn eine Abfrage einer älteren Version empfangen wird, setzen Hosts ihren Older Version Querier Present-Timer auf das Older Version Querier Interval.

Version 2 Querier Timeout (Zeitüberschreitung für Version-2-Querier) – Der Zeitüberschreitungswert für Querier der älteren IGMP-Version 2 in Sekunden.

Proxy Start Frequency (Häufigkeit Proxy-Start) – Gibt an, wie oft der Proxy hochgefahren wurde.

Proxy Interface Statistics (Proxy-Schnittstellen-Statistik) – Angaben zu empfangenen Abfragen, empfangenen/gesendeten Berichten, empfangenen/gesendeten Leave-Nachrichten

Anzeigen der IGMP-Proxy-Schnittstellen-Konfigurationen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

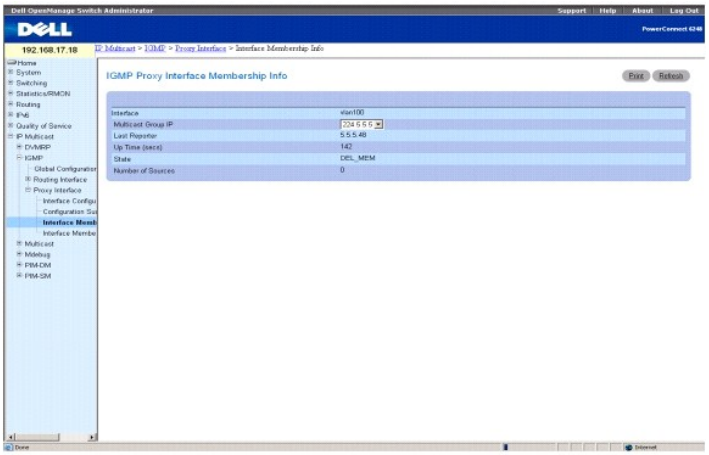
- IGMP-Proxy Commands (IGMP-Proxy-Befehle)

IGMP-Proxy-Schnittstellen-Mitgliedschaftsinformationen

Verwenden Sie die Seite **IGMP Proxy Interface Membership Info** (IGMP-Proxy-Schnittstellen-Mitgliedschaftsinformationen), um die Schnittstellen-Mitgliedschaftsdaten für eine bestimmte IP-Multicast-Gruppenadresse anzuzeigen. Sie müssen mindestens eine Router-Schnittstelle konfiguriert haben, bevor Sie Schnittstellen-Mitgliedschaftsinformationen anzeigen können, und diese sollte keine IGMP-Routing-Schnittstelle sein. Ebenso werden auf dieser Seite keinerlei Daten angezeigt, wenn an der ausgewählten Schnittstelle keine Gruppen-Mitgliedschaftsberichte empfangen wurden.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ IGMP→ Proxy Interface (Proxy-Schnittstelle)→ Interface Membership Info (Schnittstellen-Mitgliedschaftsinformationen)**.

Abbildung 13-14. IGMP-Proxy-Schnittstellen-Mitgliedschaftsinformationen



Die Seite **IGMP Proxy Interface Detailed Membership Info (Detaillierte Mitgliedschaftsinformationen zur IGMP-Proxy-Schnittstelle) enthält folgende Felder:**

Interface (Schnittstelle) – Gibt die Schnittstelle an, an der IGMP-Proxy aktiviert ist.

Multicast Group IP (Multicast-Gruppen-IP-Adresse) – Wählen Sie hier die IP-Multicast-Gruppenadresse aus, für die Daten angezeigt werden sollen. Wenn an der ausgewählten Schnittstelle keine Gruppen-Mitgliedschaftsberichte empfangen wurden, steht diese Option nicht zur Verfügung und werden die folgenden Daten nicht angezeigt.

Last Reporter (Letzter Berichtender) – Die IP-Adresse der Quelle des letzten eingegangenen Mitgliedschaftsberichts, der für die IP-Multicast-Gruppenadresse an der IGMP-Proxy-Schnittstelle empfangen wurde.

Up Time (secs) (Betriebszeit) – Die Zeit seit Erstellung dieses Eintrags in Sekunden.

State (Status) – Der Status des Host-Eintrags. Ein Host kann sich in einem der folgenden Zustände befinden: Non-Member-Status – Der Host gehört der Gruppe an der Schnittstelle nicht an. Delaying Member-Status – Der Host gehört der Gruppe an der Schnittstelle an und der Bericht-Timer läuft. Der Bericht-Timer wird zum Senden der Berichte verwendet. Idle Member-Status – Der Host gehört der Gruppe an der Schnittstelle an, und es läuft kein Bericht-Timer.

Number of Sources (Anzahl Quellen) – Die Anzahl der Quell-Hosts, die in der ausgewählten Multicast-Gruppe enthalten sind.

Anzeigen der IGMP-Proxy-Schnittstellen-Mitgliedschaftsinformationen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

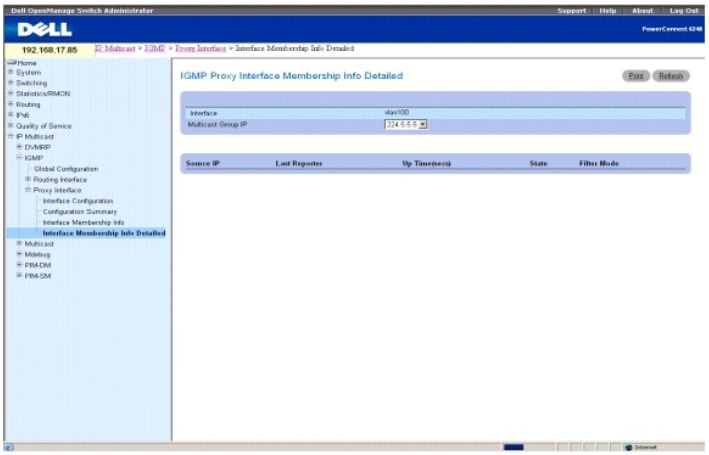
- IGMP-Proxy Commands (IGMP-Proxy-Befehle)

Detaillierte IGMP-Proxy-Schnittstellen-Mitgliedschaftsinformationen

Verwenden Sie die Seite **IGMP Proxy Interface Membership Info Detailed** (Detaillierte IGMP-Proxy-Schnittstellen-Mitgliedschaftsinformationen), um ausführliche Schnittstellen-Mitgliedschaftsdaten anzuzeigen. Sie müssen mindestens eine Router-Schnittstelle konfiguriert haben, bevor Sie detaillierte Schnittstellen-Mitgliedschaftsinformationen anzeigen können, und diese sollte keine IGMP-Routing-Schnittstelle sein. Ebenso können Sie keinerlei Daten anzeigen, wenn an der ausgewählten Schnittstelle keine Gruppen-Mitgliedschaftsberichte empfangen wurden.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast**→ **IGMP**→ **Proxy Interface (Proxy-Schnittstelle)**→ **Interface Membership Info Detailed (Detaillierte Schnittstellen-Mitgliedschaftsinformationen)**.

Abbildung 13-15. Detaillierte IGMP-Proxy-Schnittstellen-Mitgliedschaftsinformationen



Die Seite **IGMP Proxy Interface Membership Info Detailed** (Detaillierte Mitgliedschaftsinformationen zur IGMP-Proxy-Schnittstelle) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie hier die Schnittstelle aus, für die Daten angezeigt werden sollen.

Multicast Group IP (Multicast-Gruppen-IP-Adresse) – Wählen Sie hier die IP-Multicast-Gruppenadresse aus, für die Daten angezeigt werden sollen. Wenn an der ausgewählten Schnittstelle keine Gruppen-Mitgliedschaftsberichte empfangen wurden, können Sie diese Option nicht wählen und werden die nicht-konfigurierbaren Daten nicht angezeigt.

Source IP (Quell-IP-Adresse) – Dieser Parameter zeigt Quelladressen, die Mitglieder dieser Multicast-Adresse sind.

Last Reporter (Letzter Berichtender) – Die IP-Adresse der Quelle des letzten eingegangenen Mitgliedschaftsberichts für die IP-Multicast-Gruppenadresse der ausgewählten Schnittstelle.

UpTime (secs) (Betriebszeit) – Zeigt die Betriebszeit (in Sekunden) seit Erstellung des Eintrags in der Cache-Tabelle an.

State (Status) – Der Status des Host-Eintrags. Ein Host kann sich in einem der folgenden Zustände befinden:

Non-Member State (Non-Member-Status) – Der Host gehört der Gruppe an der Schnittstelle nicht an.

Delaying Member State (Delaying Member-Status) – Der Host gehört der Gruppe an der Schnittstelle an und der Bericht-Timer läuft. Der Bericht-Timer wird zum Senden der Berichte verwendet.

Idle Member State (Idle Member-Status) – Der Host gehört der Gruppe an der Schnittstelle an, und es läuft kein Bericht-Timer.

Filter Mode (Filtermodus) – Der Gruppen-Filter-Modus (Include/Exclude/None - Einschließen/Ausschließen/Keine) für die angegebene Gruppe an der IGMP-Proxy-Schnittstelle.

Anzeigen detaillierter IGMP-Proxy-Schnittstellen-Mitgliedschaftsinformationen

1. Öffnen Sie die Seite **Interface Membership Info Detailed** (Detaillierte Schnittstellen-Mitgliedschaftsinformationen).
2. Wählen Sie die Schnittstelle, die Sie anzeigen wollen, im Dropdown-Menü **Interface** (Schnittstelle).
3. Wählen Sie die gewünschte **Multicast Group IP** (Multicast-Gruppen-IP-Adresse) aus.

   Daraufhin werden ausführliche Mitgliedschaftsdaten für diese Schnittstelle und diese Multicast-Gruppen-IP-Adresse angezeigt.

Anzeigen detaillierter IGMP-Proxy-Schnittstellen-Mitgliedschaftsinformationen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- IGMP-Proxy Commands (IGMP-Proxy-Befehle)

Multicast

Die Menüseite **Multicast** enthält Links auf Webseiten, die **Multicast-**Parameter und -Daten definieren und anzeigen. Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ Multicast**. Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

- Globale Multicast-Konfiguration
- Multicast-Schnittstellen-Konfiguration
- Multicast-MRoute-Übersicht

- Konfigurieren statischer Multicast-Routen
- Übersicht über statische Multicast-Routen
- Konfigurieren einer administrativen Multicast-Adressbereichsbeschränkung
- Übersicht über administrativ beschränkte Multicast-Adressbereiche

Globale Multicast-Konfiguration

Verwenden Sie die Seite **Multicast Global Configuration** (Globale Multicast-Konfiguration), um den Verwaltungsstatus der Multicast-Weiterleitung im Router zu konfigurieren und die globalen Multicast-Parameter anzuzeigen.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast**→ **Multicast**→ **Global Configuration** (Globale Konfiguration).

Abbildung 13-16. Globale Multicast-Konfiguration

Die Seite **Multicast Global Configuration** (Globale Multicast-Konfiguration) enthält folgende Felder:

Admin Mode (Verwaltungsmodus) – Wählen Sie **Enable** (Aktivieren) oder **Disable** (Deaktivieren), um den Verwaltungsstatus der Multicast-Weiterleitung im Router einzustellen. Die Standardeinstellung ist **Disable** (Deaktivieren).

Protocol State (Protokollstatus) – Zeigt den Betriebszustand des Multicast-Weiterleitungs-Moduls an.

Table Maximum Entry Count (Maximale Anzahl Einträge in Tabelle) – Die maximale Anzahl der Einträge in der IP-Multicast-Routing-Tabelle.

Number Of Packets For Which Source Not Found (Pakete, für die keine Quelle gefunden wurde) – Die Anzahl von Multicast-Paketen, die geroutet werden sollten, die aber die RPF-Prüfung nicht bestanden haben.

Number Of Packets For Which Group Not Found (Pakete, für die keine Gruppe gefunden wurde) – Die Anzahl von Multicast-Paketen, die geroutet werden sollten, für die aber keine Multicast-Route gefunden wurde.

Protocol (Protokoll) – Das aktuell am Router aktivierte Multicast-Routing-Protokoll, sofern zutreffend.

Table Entry Count (Anzahl Tabelleneinträge) – Die Anzahl der aktuell in der Multicast-Routen-Tabelle enthaltenen Multicast-Routen-Einträge.

Table Highest Entry Count (Höchstzahl Einträge in Tabelle) – Die höchste Anzahl von Multicast-Routen-Einträgen, die in der Multicast-Routen-Tabelle enthalten waren.

Konfigurieren des Verwaltungsstatus für Multicast-Weiterleitung

1. Öffnen Sie die Seite **Multicast Global Configuration** (Globale Multicast-Konfiguration.
2. Wählen Sie Enable (Aktivieren) oder Disable (Deaktivieren) für den **Admin Mode** (Verwaltungsmodus).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Daraufhin wird die globale Multicast-Konfiguration gespeichert und das Gerät aktualisiert.

Konfigurieren/Anzeigen der Parameter für Multicast-Weiterleitung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

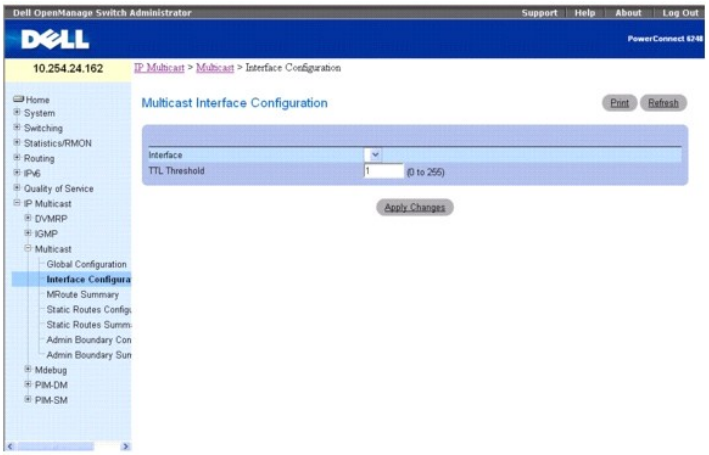
- Multicast Commands (Multicast-Befehle)

Multicast-Schnittstellen-Konfiguration

Verwenden Sie die Seite **Multicast Interface Configuration** (Multicast-Schnittstellen-Konfiguration), um den TTL-Schwellenwert einer Multicast-Schnittstelle zu konfigurieren. Sie müssen mindestens eine Router-Schnittstelle konfigurieren, bevor auf dieser Seite Felder angezeigt werden.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast**→ **Multicast**→ **Interface Configuration** (Schnittstellen-Konfiguration).

Abbildung 13-17. Multicast-Schnittstellen-Konfiguration



Die Seite **Multicast Interface Configuration** (Multicast-Schnittstellen-Konfiguration) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie aus dem Dropdown-Menü die Routing-Schnittstelle, die Sie konfigurieren wollen.

TTL Threshold (TTL-Schwellenwert) – Geben Sie den TTL-Schwellenwert ein, bei dessen Unterschreitung ein Multicast-Datenpaket von der ausgewählten Schnittstelle nicht weitergeleitet wird. Geben Sie einen Wert zwischen 0 und 255 ein. Wenn Sie 0 eingeben, werden alle Multicast-Pakete für die ausgewählte Schnittstelle weitergeleitet. Sie müssen mindestens eine Router-Schnittstelle konfigurieren, bevor Sie dieses Feld sehen.

Konfigurieren einer Multicast-Schnittstelle

1. Öffnen Sie die Seite **Multicast Interface Configuration** (Multicast-Schnittstellen-Konfiguration).
2. Wählen Sie die Schnittstelle, die Sie konfigurieren wollen, im Dropdown-Menü **Interface** (Schnittstelle).
3. Geben Sie den gewünschten Wert für **TTL Threshold** (TTL-Schwellenwert) ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Daraufhin wird die Multicast-Schnittstellen-Konfiguration gespeichert und das Gerät aktualisiert.

Konfigurieren einer Multicast-Schnittstelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

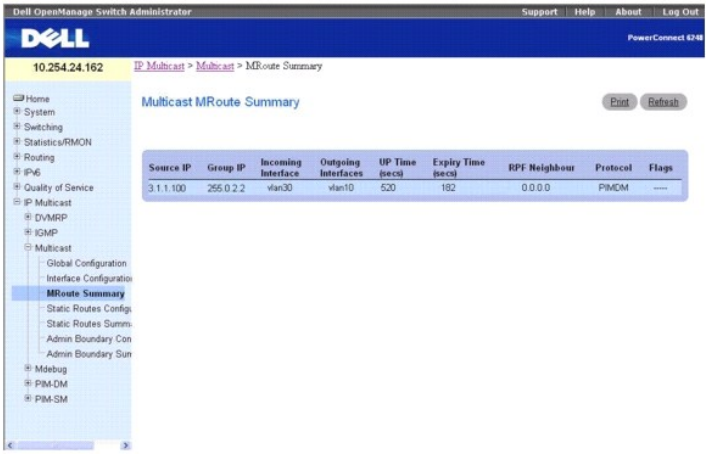
- Multicast Commands (Multicast-Befehle)

Multicast-MRoute-Übersicht

Verwenden Sie die Seite **Multicast MRoute Summary** (Multicast-MRoute-Übersicht), um MRoute-Daten anzuzeigen.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast**→ **Multicast**→ **MRoute Summary** (MRoute-Übersicht).

Abbildung 13-18. Multicast-MRoute-Übersicht



Die Seite **Multicast MRoute Summary** (Multicast-MRoute-Übersicht) enthält folgende Felder:

Source IP (Quell-IP-Adresse) – Die IP-Adresse der Multicast-Paket-Quelle, die zusammen mit der Gruppen-IP-Adresse einen Mroute-Tabelleneintrag identifiziert.

Group IP (Gruppen-IP-Adresse) – Die Zielgruppen-IP-Adresse.

Incoming Interface (Eingangsschnittstelle) – Die Eingangsschnittstelle, an der die Multicast-Pakete für diese Quelle/Gruppe ankommen.

Outgoing Interfaces (Ausgangsschnittstellen) – Die Liste der Ausgangsschnittstellen, auf denen Multicast-Pakete für diese Quelle/Gruppe weitergeleitet werden.

Up Time (secs) (Betriebszeit) – Die Zeit seit Erstellung des Eintrags (in Sekunden).

Expiry Time (secs) (Ablaufzeit) – Die Zeit in Sekunden, bis der Eintrag verfällt und aus der Tabelle gelöscht wird.

RPF Neighbor (RPF-Nachbar) – Die IP-Adresse des Reverse Path Forwarding-Nachbarn.

Protocol (Protokoll) – Das Multicast-Routing-Protokoll, das diesen Eintrag erstellt hat. Mögliche Alternativen:

- **PIM-DM**
- **PIM-SM**
- **DVMRP**

Flags (Merker) – Der in diesem Feld angegebene Wert gilt, wenn das aktive Multicast-Routing-Protokoll PIM-SM ist. Die möglichen Werte sind RPT oder SPT. Für alle anderen Protokolle erscheint hier "------".

Anzeigen der MRoute-Übersicht mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

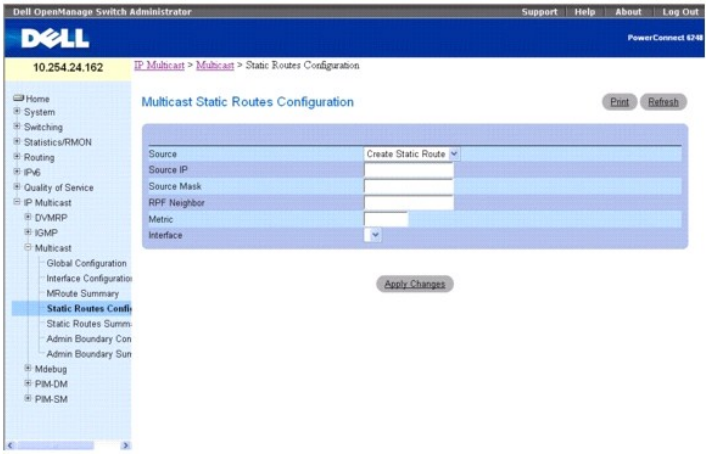
- Multicast Commands (Multicast-Befehle)

Konfigurieren statischer Multicast-Routen

Verwenden Sie die Seite **Multicast Static Routes Configuration** (Konfigurieren statischer Multicast-Routen), um einen neuen statischen Eintrag in der MRoute-Tabelle zu erstellen oder einen vorhandenen Eintrag zu bearbeiten.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ Multicast→ Static Routes Configuration (Konfigurieren statischer Routen)**.

Abbildung 13-19. Konfigurieren statischer Multicast-Routen



Die Seite **Static Routes Configuration** (Konfigurieren statischer Multicast-Routen) enthält folgende Felder:

Source (Quelle) – Wählen Sie **Create Static Route** (Statische Route einrichten), um einen neuen statischen Eintrag in der MRoute-Tabelle zu erstellen, oder wählen Sie aus dem Dropdown-Menü einen der vorhandenen Einträge aus.

Source IP (Quell-IP-Adresse) – Geben Sie die IP-Adresse ein, die die Quelle der Multicast-Pakete für den zu erstellenden Eintrag identifiziert.

Source Mask (Quellmaske) – Geben Sie die Subnetzmaske ein, die für die Quell-IP-Adresse verwendet werden soll.

RPF Neighbor (RPF-Nachbar) – Geben Sie die IP-Adresse des Nachbar-Routers auf dem Pfad zur Quelle an.

Metric (Metrik) – Geben Sie die Link-State-Kosten des Pfades zur Multicast-Quelle an. Der Wert liegt im Bereich 0 - 255, Standardwert ist 1. Sie können die Metrik für eine konfigurierte Route ändern, indem Sie die statische Route auswählen und dieses Feld bearbeiten.

Interface (Schnittstelle) – Wählen Sie aus dem Dropdown-Menü die Schnittstellennummer. Dies ist die Schnittstelle, über die die Verbindung zum Nachbar-Router hergestellt wird, für die angegebene Quell-IP-Adresse.

Konfigurieren einer statischen Route

1. Öffnen Sie die Seite **Static Routes** (Statische Routen).
2. Wählen Sie **Create Static Route** (Statische Route einrichten) im Feld **Source** (Quelle), um einen neuen statischen Eintrag zu erstellen, oder wählen Sie einen der vorhandenen Einträge aus.
3. Ändern Sie die übrigen Felder je nach Bedarf.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die neue bzw. geänderte statische Route wird gespeichert und das Gerät aktualisiert.

Konfigurieren einer statischen Route mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

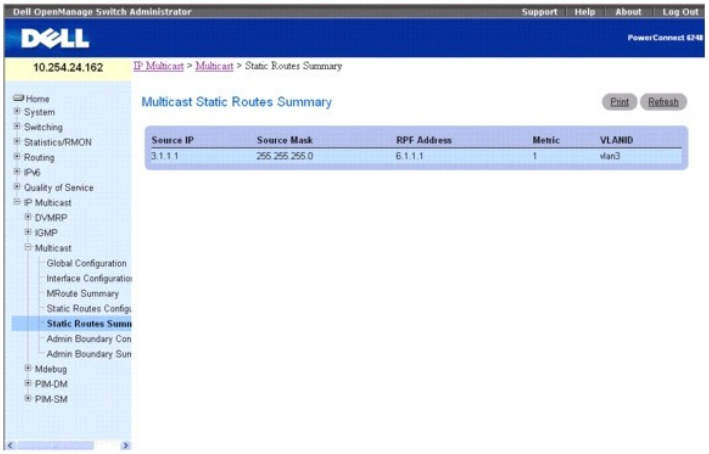
- Multicast Commands (Multicast-Befehle)

Übersicht über statische Multicast-Routen

Verwenden Sie die Seite **Multicast Static Routes Summary** (Übersicht über statische Multicast-Routen), um die statischen Routen mit der zugehörigen Konfiguration anzuzeigen.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast**→ **Multicast**→ **Static Routes Summary** (Übersicht statische Routen).

Abbildung 13-20. Übersicht über statische Multicast-Routen



Die Seite **Multicast Static Routes Summary** (Übersicht über statische Multicast-Routen) enthält folgende Felder:

Source IP (Quell-IP-Adresse) – Die IP-Adresse, die die Quelle der Multicast-Pakete für diese Route identifiziert.

Source Mask (Quellmaske) – Die Subnetzmaske, die für die Quell-IP-Adresse verwendet wird.

RPF Address (RPF-Adresse) – Die IP-Adresse des RPF-Nachbarn.

Metric (Metrik) – Die Link-State-Kosten des Pfades zur Multicast-Quelle. Bereich 0–255.

VLANID – Die Nummer des Eingangs-VLAN, dessen IP-Adresse als RPF für die angegebene Quell-IP-Adresse verwendet wird.

Anzeigen der Übersicht über die statischen Routen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

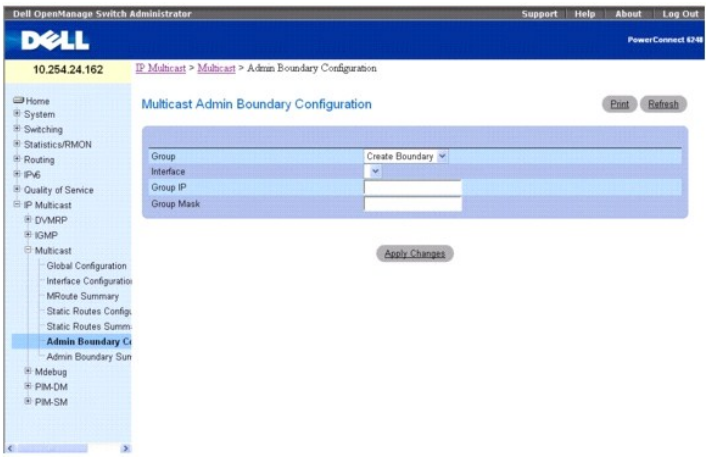
- Multicast Commands (Multicast-Befehle)

Konfigurieren einer administrativen Multicast-Adressbereichsbeschränkung

Die Definition eines administrativ beschränkten Adressbereichs ist eine Möglichkeit, den Eingang und Ausgang von Multicast-Datenverkehr auf einen bestimmten Bereich von Multicast-Adressen an einer bestimmten Routing-Schnittstelle zu begrenzen. Verwenden Sie die Seite **Multicast Admin Boundary Configuration** (Konfigurieren einer administrativen Multicast-Adressbereichsbeschränkung), um eine neue oder vorhandene administrative Adressbereichsdefinition zu konfigurieren. Um diese Seite anzeigen zu können, müssen Sie bereits eine gültige Routing-Schnittstelle und Multicast konfiguriert haben.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast**→ **Multicast**→ **Admin Boundary Configuration** (Konfigurieren einer administrativen Adressbereichsbeschränkung).

Abbildung 13-21. Konfigurieren einer administrativen Multicast-Adressbereichsbeschränkung



Die Seite **Multicast Admin Boundary Configuration** (Konfigurieren einer administrativen Multicast-Adressbereichsbeschränkung) enthält folgende Felder:

Group (Gruppe) – Wählen Sie **Create Boundary** (Adressbereich einrichten) aus dem Dropdown-Menü, um einen neuen administrativen Adressbereich zu

definieren, oder wählen Sie eine der vorhandenen Adressbereich-Spezifikationen, um die zugehörige Konfiguration anzuzeigen bzw. zu aktualisieren.

Interface (Schnittstelle) – Wählen Sie die Router-Schnittstelle aus, für die der administrativ beschränkte Adressbereich konfiguriert werden soll.

Group IP (Gruppen-IP-Adresse) – Geben Sie die erste Multicast-Gruppenadresse des auszuschließenden Adressbereichs ein. Diese Adresse muss im Bereich 239.0.0.0 bis 239.255.255.255 liegen.

Group Mask (Gruppenmaske) – Geben Sie die Maske ein, die für die Multicast-Gruppenadresse verwendet werden soll. Die Kombination aus Maske und Gruppen-IP-Adresse gibt den Bereich der administrativ beschränkten Adressen für die ausgewählte Schnittstelle an.

Konfigurieren einer administrativen Adressbereichsbeschränkung

1. Öffnen Sie die Seite **Multicast Admin Boundary Configuration** (Konfigurieren einer administrativen Multicast-Adressbereichsbeschränkung).
2. Wählen Sie **Create Boundary** (Adressbereich einrichten) im Feld **Group IP** (Gruppen-IP-Adresse), um einen neuen administrativ beschränkten Adressbereich zu konfigurieren, oder wählen Sie einen der vorhandenen Einträge aus.
3. Ändern Sie die übrigen Felder je nach Bedarf.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der neue bzw. geänderte administrativ eingeschränkte Adressbereich wird gespeichert und das Gerät aktualisiert.

Konfigurieren einer administrativen Adressbereichsbeschränkung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

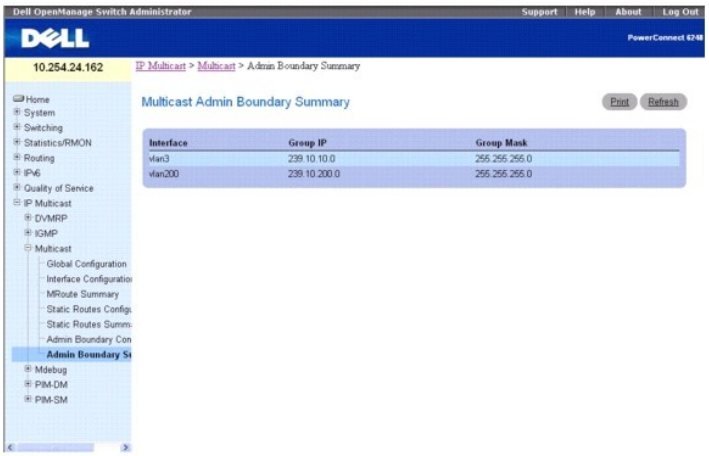
- Multicast Commands (Multicast-Befehle)

Übersicht über administrativ beschränkte Multicast-Adressbereiche

Verwenden Sie die Seite **Multicast Admin Boundary Summary** (Übersicht über administrativ beschränkte Multicast-Adressbereiche), um vorhandene administrativ beschränkte Adressbereiche anzuzeigen.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ Multicast→ Admin Boundary Summary** (Übersicht administrativ beschränkte Adressbereiche).

Abbildung 13-22. Übersicht über administrativ beschränkte Multicast-Adressbereiche



Die Seite **Multicast Admin Boundary Summary** (Übersicht über administrativ beschränkte Multicast-Adressbereiche) enthält folgende Felder:

Interface (Schnittstelle) – Die Router-Schnittstelle, für die der administrativ eingeschränkte Adressbereich verwendet werden soll.

Group IP (Gruppen-IP-Adresse) – Die erste Multicast-Gruppenadresse des auszuschließenden Adressbereichs.

Group Mask (Gruppenmaske) – Die Maske, die für die Multicast-Gruppenadresse verwendet werden soll. Die Kombination aus Maske und Gruppen-IP-Adresse gibt den Bereich der administrativ beschränkten Adressen für die ausgewählte Schnittstelle an.

Anzeigen der Übersicht über die administrativ beschränkten Multicast-Adressbereiche mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- Multicast Commands (Multicast-Befehle)

PIM-DM

Das PIM-DM-Protokoll ist ein einfaches, protokollunabhängiges Multicast-Routing-Protokoll. Es nutzt eine vorhandene Unicast-Routing-Tabelle und einen Join/Prune/Graft-Mechanismus, um eine Baumstruktur aufzubauen. Das PIM-DM erstellt, basierend auf der Quelle, Shortest-Path-Verteilerbäume, die RPF nutzen. Es kann nicht dafür genutzt werden, einen Shared-Tree-Verteilerbaum zu bauen, wie dies bei PIM-SM der Fall ist. Das PIM-DM geht davon aus, dass alle Downstream-Router und -Hosts ein von einem Sender übertragenes Multicast-Datagramm erhalten wollen. Daher flutet PIM-DM zunächst das gesamte Netzwerk mit dem Multicast-Datenverkehr. Router, die keine Downstream-Nachbarn haben, prunen den unerwünschten Datenverkehr. Neben den PRUNE-Nachrichten werden bei PIM-DM Graft- und Assert-Nachrichten verwendet. Graft-Nachrichten werden benutzt, wenn ein neuer Host der Gruppe beitreten will. Assert-Nachrichten dienen dazu, duplizierte Datenflüsse in demselben Mehrfachzugriffsnetzwerk auszuschließen.

Es gibt zwei PIM-DM-Versionen. Version 2 verwendet die IGMP-Nachricht nicht; stattdessen wird hier eine Nachricht benutzt, die in ein IP-Paket eingekapselt ist, mit Protokoll Nummer 103. In Version 2 wird an Stelle der Abfragenachricht die Hello-Nachricht eingeführt.

PIM-DM eignet sich für:

- Umgebungen mit hoher Teilnehmerdichte
- Wenige Sender - viele Empfänger (bedingt durch das häufige Fluten)
- Hohes Multicast-Datenverkehrsaufkommen
- Konstanter Datenverkehrsstrom

Die Menüseite **PIM-DM** enthält Links auf Webseiten, die **PIM-DM-**Parameter und -Daten definieren und anzeigen. Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→PIM-DM**.

Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

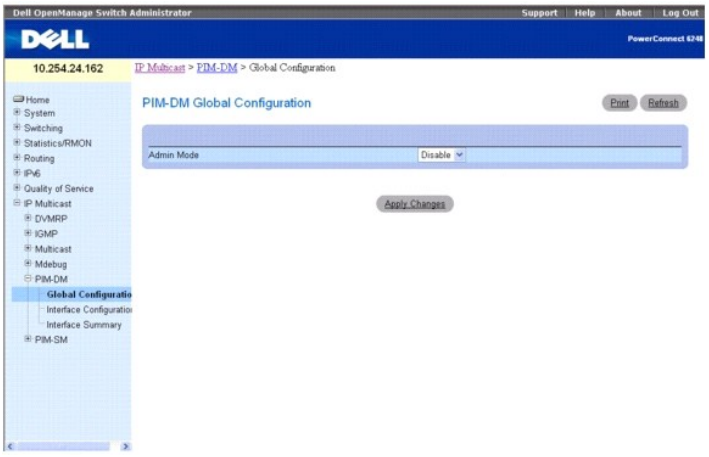
- Globale PIM-DM-Konfiguration
- PIM-DM-Schnittstellen-Konfiguration
- PIM-DM-Schnittstellen-Übersicht

Globale PIM-DM-Konfiguration

Verwenden Sie die Seite **PIM-DM Global Configuration** (Globale PIM-DM-Konfiguration), um den Verwaltungsstatus des PIM-DM für dieses System zu konfigurieren.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ PIM-DM→ Global Configuration** (Globale Konfiguration).

Abbildung 13-23. Globale PIM-DM-Konfiguration



Die Seite **PIM-DM Global Configuration** (Globale PIM-DM-Konfiguration) enthält folgendes Feld:

Admin Mode (Verwaltungsmodus) – Wählen Sie **Enable** (Aktivieren) oder **Disable** (Deaktivieren) aus dem Dropdown-Menü, um den Verwaltungsstatus des PIM-DM für das System einzustellen. Die Standardeinstellung ist **Disable** (Deaktivieren).

Konfigurieren des PIM-DM

1. Öffnen Sie die Seite **PIM-DM Global Configuration** (Globale PIM-DM-Konfiguration).

2. Setzen Sie den **Admin Mode** (Verwaltungsmodus) auf **Enable** (Aktivieren) oder **Disable** (Deaktivieren), um PIM-DM ein- bzw. auszuschalten.

3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Daraufhin wird die PIM-DM-Konfiguration gespeichert und das Gerät aktualisiert.

Konfigurieren des PIM-DM mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

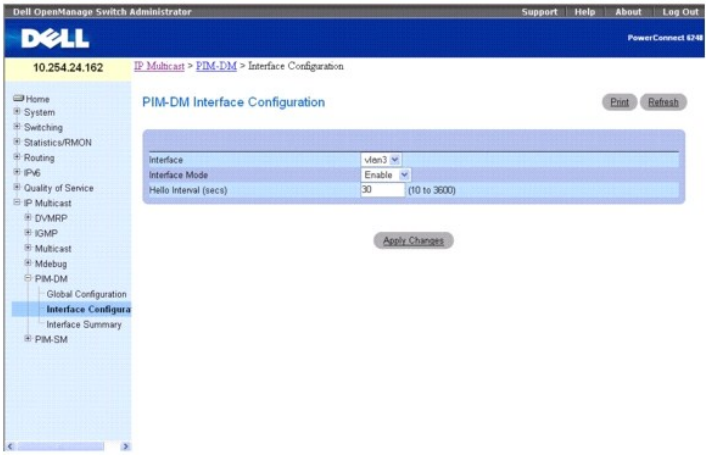
- PIM-DM Commands (PIM-DM-Befehle)

PIM-DM-Schnittstellen-Konfiguration

Verwenden Sie die Seite **PIM-DM Interface Configuration** (PIM-DM-Schnittstellen-Konfiguration), um bestimmte Schnittstellen mit PIM-DM zu konfigurieren. PIM-DM muss auf der Seite **PIM-DM Global Configuration** (Globale PIM-DM-Konfiguration) aktiviert worden sein, damit die Seite zum Konfigurieren der Schnittstellen angezeigt werden kann.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ PIM-DM→ Interface Configuration (Schnittstellen-Konfiguration)**.

Abbildung 13-24. PIM-DM-Schnittstellen-Konfiguration



Die Seite **PIM-DM Interface Configuration** (PIM-DM-Schnittstellen-Konfiguration) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie hier die Schnittstelle aus, für die Daten angezeigt oder konfiguriert werden sollen. Sie müssen mindestens eine Router-Schnittstelle konfiguriert haben, bevor Sie Daten für eine PIM-DM-Schnittstelle konfigurieren oder anzeigen können, andernfalls wird eine Fehlermeldung ausgegeben.

Interface Mode (Schnittstellenmodus) – Wählen Sie **Enable** (Aktivieren) oder **Disable** (Deaktivieren) aus dem Dropdown-Menü, um den Verwaltungsstatus des PIM-DM an der ausgewählten Schnittstelle einzustellen. Die Standardeinstellung ist **Disable** (Deaktivieren).

Hello Interval (secs) (Hello-Intervall) – Geben Sie die Anzahl Sekunden zwischen PIM-Hello-Nachrichten ein, die von der ausgewählten Schnittstelle übertragen werden. Der Standardwert ist 30. Zulässige Werte sind 10 bis 3600.

Konfigurieren des PIM-DM für eine Schnittstelle

1. Öffnen Sie die Seite **PIM-DM Interface Configuration** (PIM-DM-Schnittstellen-Konfiguration.

2. Wählen Sie die Schnittstelle, die Sie konfigurieren wollen, im Feld **Interface** (Schnittstelle).

3. Ändern Sie die übrigen Felder je nach Bedarf.

4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Daraufhin wird die Schnittstellen-Konfiguration gespeichert und das Gerät aktualisiert.

Konfigurieren des PIM-DM für eine Schnittstelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

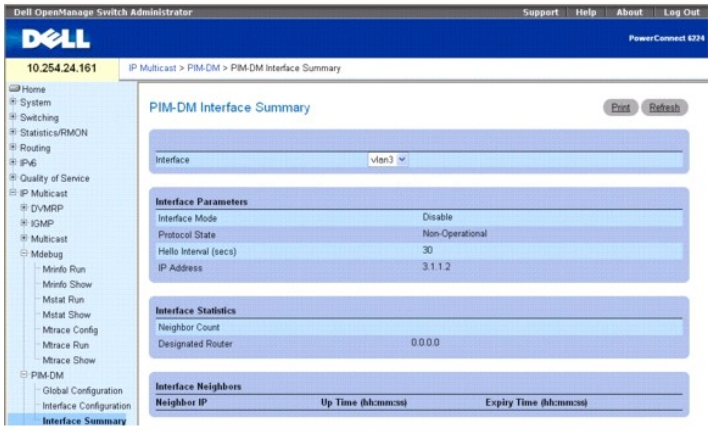
- PIM-DM Commands (PIM-DM-Befehle)

PIM-DM-Schnittstellen-Übersicht

Verwenden Sie die Seite **PIM-DM Interface Summary** (PIM-DM-Schnittstellen-Übersicht), um eine PIM-DM-Schnittstelle und die zugehörigen Einstellungen anzuzeigen. Mindestens eine Schnittstelle dieses Routers muss für PIM-DM eingerichtet sein, damit diese Seite angezeigt werden kann.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ PIM-DM→ Interface Summary (Schnittstellen-Übersicht)**.

Abbildung 13-25. PIM-DM-Schnittstellen-Übersicht



Die Seite **PIM-DM Interface Summary** (PIM-DM-Schnittstellen-Übersicht) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie hier die Schnittstelle aus, für die Daten angezeigt werden sollen. Es muss mindestens eine Router-Schnittstelle konfiguriert sein, bevor Daten für eine PIM-DM-Schnittstelle angezeigt werden können, andernfalls wird eine Fehlermeldung ausgegeben.

Interface Parameters (Schnittstellenparameter)

Interface Mode (Schnittstellenmodus) – Zeigt den Verwaltungsstatus des PIM-DM für die ausgewählte Schnittstelle an. Die Standardeinstellung ist **Disable** (Deaktivieren).

Protocol State (Protokollstatus) – Der Betriebszustand des PIM-DM-Protokolls an dieser Schnittstelle.

Hello Interval (secs) (Hello-Nachrichtenabstand in Sekunden) – Der Abstand, mit dem PIM-Hello-Nachrichten an der ausgewählten Schnittstelle übertragen werden.

IP Address (IP-Adresse) – Die IP-Adresse der ausgewählten Schnittstelle.

Schnittstellenstatistiken

Neighbor Count (Anzahl Nachbarn) – Die Anzahl der PIM-Nachbarn an der ausgewählten Schnittstelle.

Designated Router – Der Designated Router an der ausgewählten PIM-Schnittstelle. Für Punkt-zu-Punkt-Schnittstellen ist dies 0.0.0.0.

Interface Neighbors (Schnittstellen-Nachbarn)

Neighbor IP (Nachbar-IP-Adresse) – Die IP-Adresse des PIM-Nachbarn, zu dem dieser Eintrag Informationen enthält.

Up Time (Betriebszeit) (hh:mm:ss) – Die Zeit, seit dieser PIM-Nachbar (zuletzt) ein Nachbar des lokalen Routers geworden ist.

Expiry Time (Ablaufzeit) (hh:mm:ss) – Die minimale verbleibende Zeit bis zum Verfall dieses PIM-Nachbarn.

Anzeigen der PIM-DM-Schnittstellen-Übersicht mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- PIM-DM Commands (PIM-DM-Befehle)

PIM-SM

Das PIM-SM wird benutzt, um Multicast-Datenverkehr effizient an Multicast-Gruppen weiterzuleiten, die sich über Weitverkehrsnetzwerke verteilen, in denen nur begrenzt Bandbreite zur Verfügung steht. PIM-SM verwendet standardmäßig gemeinsam verwendete Bäume und implementiert aus Effizienzgründen quellbasierte Bäume. Anhand eines Grenzwerts für die Datenrate wird zwischen den Bäumen umgeschaltet. Bei PIM-SM wird davon ausgegangen, dass keiner der Hosts Multicast-Datenverkehr empfangen will, solange er ihn nicht ausdrücklich anfordert. Dieses Protokoll erstellt einen Shared-Tree-Verteilerbaum,

dessen Wurzel ein definierter Rendezvous-Punkt (RP) ist, von dem aus der von der Quelle kommende Datenverkehr an die Empfänger weitergeleitet wird. Die Sender übermitteln ihre Multicast-Daten zunächst an den RP, der sie wiederum entlang dem Shared-Tree-Verteilerbaum abwärts an die Empfänger verteilt. Allerdings bilden Shared-Tree-Verteilerbäume, die von einem RP ausgehen, nicht unbedingt den kürzesten/optimalen Pfad. In solchen Fällen sieht das PIM-SM eine Möglichkeit vor, auf effizientere quellenspezifische Bäume umzuschalten.

Die Menüseite **PIM-SM** enthält Links auf Webseiten, die PIM-SM-Parameter und -Daten definieren und anzeigen. Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **IP Multicast→ PIM-SM**.

Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

- Globale PIM-SM-Konfiguration
- Globaler PIM-SM-Status
- PIM-SM-Schnittstellen-Konfiguration
- PIM-SM-Schnittstellen-Übersicht
- Komponentenübersicht
- RP-Set-Übersicht
- RP-Kandidaten-Übersicht
- Konfigurieren statischer RP

Globale PIM-SM-Konfiguration

Verwenden Sie die Seite **PIM-SM Global Configuration** (Globale PIM-DM-Konfiguration), um globale PIM-DM-Einstellungen für dieses System zu konfigurieren.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **Multicast→ PIM-SM→ Global Configuration (Globale Konfiguration)**.

Abbildung 13-26. Globale PIM-SM-Konfiguration

Die Seite **PIM-SM Global Configuration** (Globale PIM-SM-Konfiguration) enthält folgende Felder:

Admin Mode (Verwaltungsmodus) – Wählen Sie **Enable** (Aktivieren) oder **Disable** (Deaktivieren) aus dem Dropdown-Menü, um den Verwaltungsstatus des PIM-SM für das System einzustellen. Sie müssen IGMP aktivieren, bevor Sie PIM-SM aktivieren können. Die Standardeinstellung ist **Disable** (Deaktivieren).

Join/Prune Interval (secs) (Join/Prune-Intervall) – Geben Sie das Intervall (in Sekunden) zwischen den einzelnen Übertragungen von PIM-SM-Join/Prune-Nachrichten ein. Zulässige Werte sind 10 bis 3600 Sekunden. Der Standardwert ist 60.

Data Threshold Rate (Kbps) (Datenraten-Schwellenwert) — Geben Sie hier die minimale Quell-Datenrate in Kbit/s an, oberhalb deren der Last-Hop-Router auf einen quellenspezifischen Shortest-Path-Verteilerbaum umschaltet. Zulässige Werte sind 0 bis 2000 Kbit/s. Der Standardwert ist 50.

Register Threshold Rate (Kbps) (Schwellenwert) – Geben Sie hier die minimale Quell-Datenrate in Kbit/s an, oberhalb deren der Router des Rendezvous-Punkts auf einen quellenspezifischen Shortest-Path-Verteilerbaum umschaltet. Zulässige Werte sind 0 bis 2000 Kbit/s. Der Standardwert ist 50.

Konfigurieren des PIM-SM

1. Öffnen Sie die Seite **PIM-SM Global Configuration** (Globale PIM-SM-Konfiguration).
2. Setzen Sie den **Admin Mode** (Verwaltungsmodus) auf **Enable** (Aktivieren) oder **Disable** (Deaktivieren), um PIM-SM ein- bzw. auszuschalten.
3. Ändern Sie die übrigen Felder je nach Bedarf.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Daraufhin wird die Schnittstellen-Konfiguration gespeichert und das Gerät aktualisiert.

Konfigurieren des PIM-SM mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

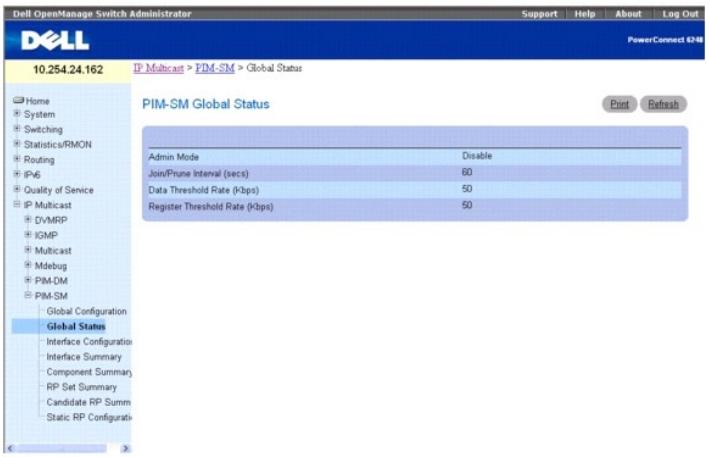
- PIM-SM Commands (PIM-SM-Befehle)

Globaler PIM-SM-Status

Verwenden Sie die Seite **PIM-SM Global Status** (Globaler PIM-SM-Status), um die globalen Einstellungen anzuzeigen, die Sie auf der Seite **PIM-SM Global Configuration** (Globale PIM-SM-Konfiguration) ausgewählt haben.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **Multicast→ PIM-SM→ Global Status (Globaler Status)**.

Abbildung 13-27. Globaler PIM-SM-Status



Die Seite **PIM-SM Global Status** (Globaler PIM-SM-Status) enthält folgende Felder:

Admin Mode (Verwaltungsmodus) – Der Verwaltungsstatus des PIM-SM im Router: **Enable** (Aktivieren) oder **Disable** (Deaktivieren).

Join/Prune Interval (secs) (Join/Prune-Intervall) – Das Intervall (in Sekunden) zwischen den einzelnen Übertragungen von PIM-SM-Join/Prune-Nachrichten.

Data Threshold Rate (Kbps) (Datenraten-Schwellenwert) – Die minimale Quell-Datenrate in Kbit/s, oberhalb deren der Last-Hop-Router auf einen quellenspezifischen Shortest-Path-Verteilerbaum umschaltet.

Register Threshold Rate (Kbps) (Schwellenwert) – Die minimale Quell-Datenrate in Kbit/s, oberhalb deren der Router des Rendezvous-Punkts auf einen quellenspezifischen Shortest-Path-Verteilerbaum umschaltet.

Anzeigen des globalen PIM-SM-Status mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

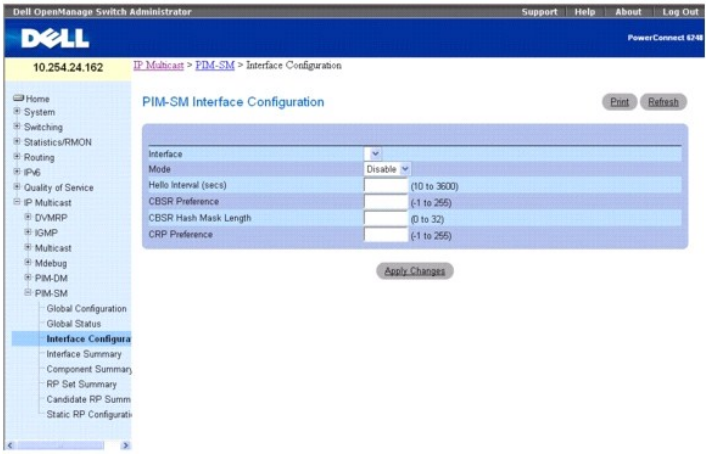
- PIM-SM Commands (PIM-SM-Befehle)

PIM-SM-Schnittstellen-Konfiguration

Verwenden Sie die Seite **PIM-SM Interface Configuration** (PIM-SM-Schnittstellen-Konfiguration), um PIM-SM für eine Schnittstelle zu konfigurieren. PIM-SM muss auf der Seite **PIM-SM Global Configuration** (Globale PIM-DM-Konfiguration) aktiviert worden sein, damit die Seite zum Konfigurieren der Schnittstellen angezeigt werden kann.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **Multicast→ PIM-SM→ Interface Configuration (Schnittstellen-Konfiguration)**.

Abbildung 13-28. PIM-SM-Schnittstellen-Konfiguration



Die Seite **PIM-SM Interface Configuration** (PIM-SM-Schnittstellen-Konfiguration) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie hier die Schnittstelle aus, für die Daten angezeigt oder konfiguriert werden sollen. Es muss mindestens eine Routing-Schnittstelle vorhanden sein, damit Daten angezeigt oder konfiguriert werden können.

Mode (Modus) – Wählen Sie **Enable** (Aktivieren) oder **Disable** (Deaktivieren) aus dem Dropdown-Menü, um den Verwaltungsstatus des PIM-SM an dieser Schnittstelle einzustellen. Die Standardeinstellung ist **Disable** (Deaktivieren).

Hello Interval (secs) (Hello-Intervall) – Geben Sie die Zeit in Sekunden zwischen der Übertragung der einzelnen PIM-Hello-Nachrichten an dieser Schnittstelle ein. Zulässige Werte sind 10 bis 3600 Sekunden. Der Standardwert ist 30.

CBSR Preference (CBSR-Voreinstellung) – Geben Sie den Voreinstellungswert für die lokale Schnittstelle als Bootstrap-Router-Kandidat ein. Mit dem Wert -1 wird dabei angegeben, dass die lokale Schnittstelle nicht als BSR-Schnittstelle in Frage kommt. Zulässige Werte sind -1 bis 255. Der Standardwert ist 0.

CBSR Hash Mask Length (Länge der CBSR-Hash-Maske) – Geben Sie die Länge der CBSR-Hash-Maske ein, die in Bootstrap-Nachrichten angegeben werden soll, wenn diese Schnittstelle als Bootstrap-Router ausgewählt wird. Diese Hash-Masken-Länge wird in dem Hash-Algorithmus zum Auswählen des RP für eine bestimmte Gruppe verwendet. Zulässige Werte sind 0 bis 32. Der Standardwert ist 30.

CRP Preference (CRP-Voreinstellung) – Geben Sie den Voreinstellungswert für die lokale Schnittstelle als Bootstrap-Router-Kandidat ein. Mit dem Wert -1 wird dabei angegeben, dass die lokale Schnittstelle nicht als BSR-Schnittstelle in Frage kommt. Zulässige Werte sind -1 bis 255. Der Standardwert ist 0.

Konfigurieren des PIM-SM für eine Schnittstelle

1. Öffnen Sie die Seite **PIM-SM Interface Configuration** (PIM-SM-Schnittstellen-Konfiguration).
2. Wählen Sie die Schnittstelle, die Sie konfigurieren wollen, im Feld **Interface** (Schnittstelle).
3. Wählen Sie **Enable** (Aktivieren) im Feld **Mode** (Modus).
4. Ändern Sie die übrigen Felder je nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Daraufhin wird die Schnittstellen-Konfiguration gespeichert und das Gerät aktualisiert.

Konfigurieren des PIM-SM für eine Schnittstelle mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

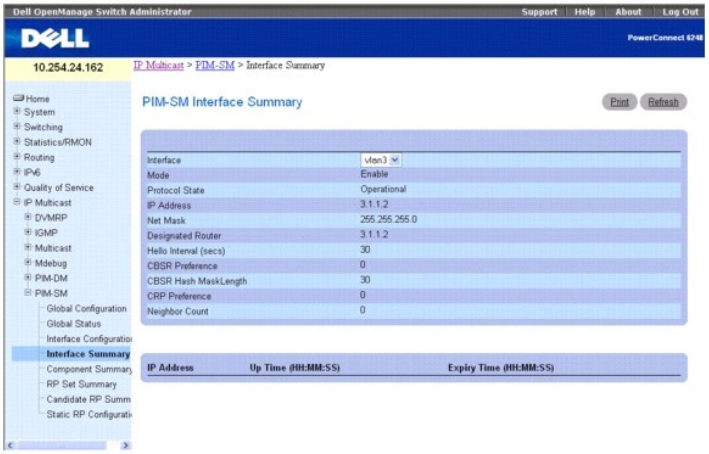
- PIM-SM Commands (PIM-SM-Befehle)

PIM-SM-Schnittstellen-Übersicht

Verwenden Sie die Seite **PIM-SM Interface Summary** (PIM-SM-Schnittstellen-Übersicht), um eine PIM-SM-Schnittstelle und die zugehörigen Einstellungen anzuzeigen. Mindestens eine Schnittstelle dieses Routers muss für PIM-SM eingerichtet sein, damit diese Seite angezeigt werden kann.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **Multicast→ PIM-SM→ Interface Summary (Schnittstellen-Übersicht)**.

Abbildung 13-29. PIM-SM-Schnittstellen-Übersicht



Die Seite **PIM-SM Interface Summary** (PIM-SM-Schnittstellen-Übersicht) enthält folgende Felder:

Interface (Schnittstelle) – Wählen Sie hier die Schnittstelle aus, für die Daten angezeigt werden sollen.

Mode (Modus) – Der Verwaltungsstatus des PIM-SM im Router: **Enable** (Aktivieren) oder **Disable** (Deaktivieren).

Protocol State (Protokollstatus) – Der Betriebszustand des PIM-SM-Protokolls an der ausgewählten Schnittstelle: **Operational** (betriebsbereit) oder **Non-operational** (nicht betriebsbereit).

IP Address (IP-Adresse) – Die IP-Adresse der ausgewählten PIM-Schnittstelle.

Net Mask (Netzwerkmaske) – Die Netzwerkmaske für die IP-Adresse der ausgewählten PIM-Schnittstelle.

Designated Router – Der Designated Router an der ausgewählten PIM-Schnittstelle. Für Punkt-zu-Punkt-Schnittstellen hat dieses Objekt den Wert 0.0.0.0.

Hello Interval (secs) (Hello-Intervall) – Der Abstand in Sekunden, mit dem PIM-Hello-Nachrichten an der ausgewählten Schnittstelle übertragen werden.

CBSR Preference (CBSR-Voreinstellung) – Der Voreinstellungswert für die lokale Schnittstelle als Bootstrap-Router-Kandidat. Mit dem Wert -1 wird dabei angegeben, dass die lokale Schnittstelle nicht als BSR-Schnittstelle in Frage kommt.

CBSR Hash Mask Length (Länge der CBSR-Hash-Maske) – Die Länge der CBSR-Hash-Maske, die in Bootstrap-Nachrichten angegeben werden soll, wenn diese Schnittstelle als Bootstrap-Router ausgewählt wird. Diese Hash-Masken-Länge wird in dem Hash-Algorithmus zum Auswählen des RP für eine bestimmte Gruppe verwendet.

CRP Preference (CRP-Voreinstellung) – Der Voreinstellungswert für die lokale Schnittstelle als Bootstrap-Router-Kandidat. Mit dem Wert -1 wird dabei angegeben, dass die lokale Schnittstelle nicht als BSR-Schnittstelle in Frage kommt.

Neighbor Count (Anzahl Nachbarn) – Die Anzahl der PIM-Nachbarn an der ausgewählten Schnittstelle.

IP Address (IP-Adresse) – Die IP-Adresse des PIM-Nachbarn für diesen Eintrag.

Up Time (Betriebszeit) – Die Zeit (hh:mm:ss), seit dieser PIM-Nachbar (zuletzt) ein Nachbar des lokalen Routers geworden ist.

Expiry Time (Ablaufzeit) – Die minimale verbleibende Zeit (hh:mm:ss) bis zum Verfall dieses PIM-Nachbarn.

Anzeigen der PIM-SM-Schnittstellen-Übersicht

1. Öffnen Sie die Seite **PIM-SM Interface Summary** (PIM-SM-Schnittstellen-Übersicht).
2. Wählen Sie die Schnittstelle, die Sie anzeigen wollen, im Dropdown-Menü **Interface** (Schnittstelle).

   Daraufhin werden die PIM-SM-Konfigurationsdaten für diese Schnittstelle angezeigt.

Anzeigen der PIM-SM-Schnittstellen-Übersicht mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- PIM-SM Commands (PIM-SM-Befehle)

Komponentenübersicht

Verwenden Sie die Seite **Component Summary** (Komponentenübersicht), um Daten zu den PIM-SM-Komponenten anzuzeigen.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **Multicast→ PIM-SM→ Component Summary (Komponentenübersicht)**.

Abbildung 13-30. Komponentenübersicht

Die Seite **Component Summary** (Komponentenübersicht) enthält folgende Felder:

Component Index (Komponentenindex) – Eine eindeutige Nummer, die die Komponente identifiziert.

Component BSR Address (BSR-Adresse der Komponente) – Die IP-Adresse des Bootstrap-Routers (BSR) für den lokalen PIM-Bereich.

Component BSR Expiry Time (hh:mm:ss) (Ablaufzeit BSR-Komponente) – Die minimale verbleibende Zeit, bevor der Bootstrap-Router in der lokalen Domäne deklariert wird.

Component CRP Hold Time (hh:mm:ss) (Haltezeit der BSR-Komponente) – Diie Haltezeit der Komponente, wenn sie ein Kandidat für den Rendezvous-Punkt in der lokalen Domäne ist.

Anzeigen der PIM-SM-Komponentenübersicht mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

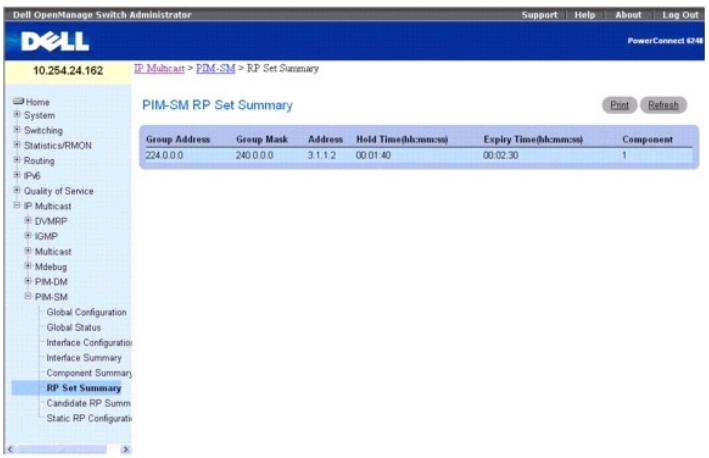
- PIM-SM Commands (PIM-SM-Befehle)

RP-Set-Übersicht

Verwenden Sie die Seite **PIM-SM RP Set Summary** (PIM-SM-RP-Set-Übersicht), um die statischen RP-Informationen für den PIM-SM-Router anzuzeigen.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **Multicast→ PIM-SM→ RP Set Summary (RP-Set-Übersicht)**.

Abbildung 13-31. PIM-SM-RP-Set-Übersicht



Die Seite **PIM-SM RP Set Summary** (PIM-SM RP-Set-Übersicht) enthält folgende Felder in einer Tabelle:

Group Address (Gruppenadresse) – Zeigt die IP-Multicast-Gruppenadresse an.

Group Mask (Gruppenmaske) – Zeigt die Multicast-Gruppenadressmaske an.

Address (Adresse) – Zeigt die IP-Adresse des RP-Kandidaten an.

Hold Time (hh:mm:ss) (Haltezeit) – Die Haltezeit eines RP-Kandidaten. Wenn der lokale Router nicht der BSR ist, erscheint hier der Wert 0.

Expiry Time (hh:mm:ss) (Ablaufzeit) – Die minimal verbleibende Zeit, bevor der RP-Kandidat als inaktiv deklariert wird.

Component (Komponente) – Eine Nummer, die die Komponente eindeutig identifiziert. Jede Protokollinstanz, die mit einer separaten Domäne verbunden ist, sollte einen anderen Indexwert haben.

Anzeigen der RP-Set-Übersicht mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

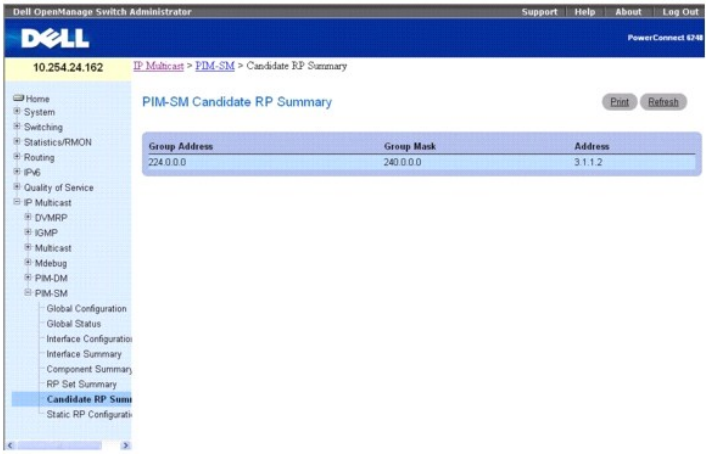
- PIM-SM Commands (PIM-SM-Befehle)

RP-Kandidaten-Übersicht

Verwenden Sie die Seite **PIM-SM Candidate RP Summary** (PIM-SM-RP-Kandidaten-Übersicht), um PIM-Informationen zu Rendezvous-Punkt (RP) -Kandidaten für jede IP-Multicast-Gruppe anzuzeigen.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **Multicast→ PIM-SM→ Candidate RP Summary (RP-Kandidaten-Übersicht)**.

Abbildung 13-32. PIM-SM-RP-Kandidaten-Übersicht



Die Seite **PIM-SM RP Candidate RP Summary** (PIM-SM RP-Set-Übersicht) enthält folgende Felder in einer Tabelle:

Group Address (Gruppenadresse) – Die Gruppenadresse, die in RP-Kandidaten-Ankündigungen übertragen wird.

Group Mask (Gruppenmaske) – Die Maske der Gruppenadresse, die in RP-Kandidaten-Ankündigungen übertragen wird, um den Umfang der Gruppe eindeutig zu identifizieren, die der Router unterstützt, wenn er als Rendezvous-Punkt ausgewählt wird.

Address (Adresse) – Zeigt die Unicast-Adresse der Schnittstelle an, die als RP-Kandidat angekündigt wird.

Anzeigen der PIM-SM-RP-Kandidaten-Übersicht mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

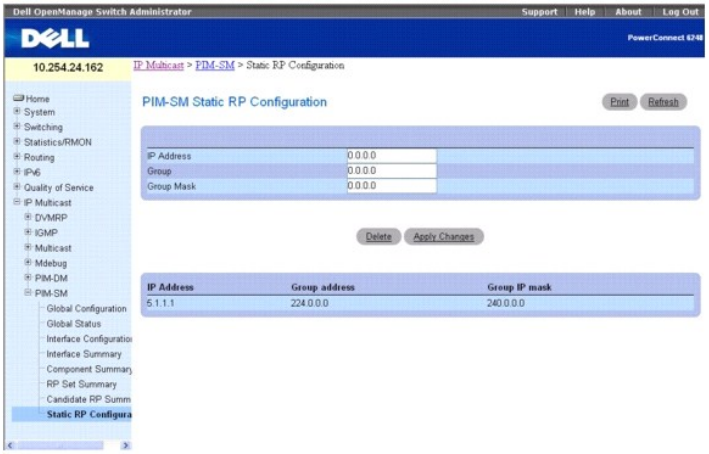
- PIM-SM Commands (PIM-SM-Befehle)

Konfigurieren statischer RP

Verwenden Sie die Seite **Static RP Configuration** (Konfigurieren statischer RP), um die spezifizierte statische RP-IP-Adresse für den PIM-SM-Router zu erstellen.

Klicken Sie zum Öffnen dieser Seite in der Strukturansicht auf **Multicast→ PIM-SM→ Static RP Configuration (Konfigurieren statischer RP)**.

Abbildung 13-33. Konfigurieren statischer RP



Die Seite **Static RP Configuration** (Konfigurieren statischer RP) enthält folgende Felder:

IP Address (IP-Adresse) – Die IP Adresse des einzurichtenden RP.

Group Address (Gruppenadresse) – Die Gruppenadresse des einzurichtenden RP.

Group Mask (Gruppenmaske) – Die Gruppen-IP-Maske des einzurichtenden RP.

Vorhandene Konfigurationen werden in der Tabelle im unteren Bereich der Seite angezeigt.

Konfigurieren von statischen RP

1. Öffnen Sie die Seite **Static RP Configuration** (Konfigurieren statischer RP).
2. Geben Sie in **IP Address** die IP-Adresse, in **Group** die IP-Adresse der Gruppe und in **Group Mask** die Gruppenmaske für die Konfiguration des statischen RP ein.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die angegebene IP-Adresse des statischen RP für den PIM-SM-Router wird eingerichtet und das Gerät wird aktualisiert.

Konfigurieren eines statischen RP mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch) in folgendem Kapitel:

- PIM-SM Commands (PIM-SM-Befehle)

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Konfigurieren von Dell™ PowerConnect™

Benutzerhandbuch für die Dell™ PowerConnect™ 6200-Reihe

- Starten von CLI
- Allgemeine Konfigurationsinformationen
- Starten des Switch
- Konfigurationsübersicht
- Fortgeschrittene Konfiguration
- Software-Download und Neustart
- Boot-Menü (Systemstart)
- Beispiel eines Konfigurationsverfahrens

In diesem Kapitel wird die erste Switch-Konfiguration beschrieben. Folgende Themen werden abgedeckt:

- Starten von CLI
- Allgemeine Konfigurationsinformationen
- Starten des Switch
- Konfigurationsübersicht
- Fortgeschrittene Konfiguration
- Software-Download und Neustart
- Menü "Boot" (Systemstart)
- Beispiel eines Konfigurationsverfahrens

Nachdem Sie alle externen Verbindungen vorgenommen haben, schließen Sie den Switch an ein Terminal an, um den Startvorgang und andere Vorgänge zu überwachen.

ANMERKUNG: Wenn Sie einen Switch-*Stack* installieren , verbinden Sie das Terminal mit dem Master-Switch. Beim ersten Einschalten eines Stacks wird der Master-Switch bestimmt, der sich an beliebiger Position im Stack befinden kann. Bei diesem Switch leuchtet die Master-Switch-LED. Wenn Sie das Terminal an einem untergeordneten Switch anschließen, können Sie CLI nicht verwenden.

Führen Sie anschließend die Installations- und Konfigurationsverfahren in der Reihenfolge durch, die in Abbildung 5-1 dargestellt ist. Nehmen Sie bei der erstmaligen Konfiguration die Standard-Switch-Konfiguration vor. Die Ausführung weiterer Funktionen wird weiter unten in diesem Abschnitt beschrieben.

HINWEIS: Lesen Sie die Versionshinweise für dieses Produkt, bevor Sie fortfahren. Sie können die Versionshinweise von der Dell Support-Website unter **support.dell.com** herunterladen.

Starten von CLI

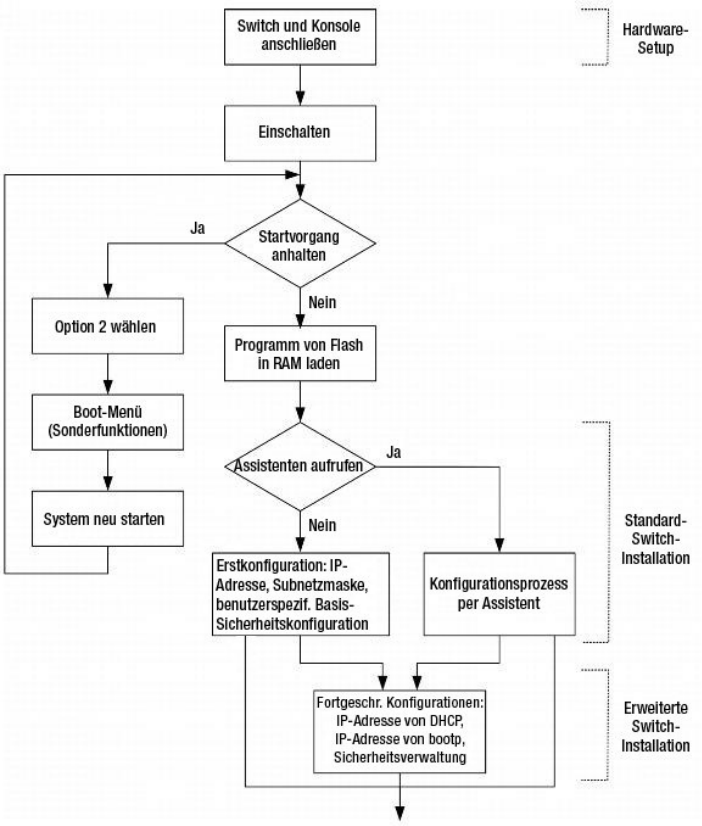
Führen Sie die folgenden Schritte durch, um mit der Ausführung von CLI zu beginnen:

ANMERKUNG: Die folgenden Schritte sind nur für die Ausführung auf der Konsolenbefehlszeile bestimmt.

1. Starten Sie den Switch, und warten Sie, bis der Startvorgang abgeschlossen ist. Die Begrüßungsmeldung des **Easy-Setup-Assistenten** wird nun angezeigt.
2. Konfigurieren Sie den Switch mithilfe des **Easy-Setup-Assistenten**, und geben Sie die nötigen Befehle zu Durchführung der erforderlichen Aufgaben ein.
3. Wenn Sie fertig sind, beenden Sie die Sitzung mit dem Befehl **quit** oder **exit**.

Der Switch (oder Stack) kann über eine direkte Verbindung zum Switch-Konsolenanschluss oder über eine Telnet-Verbindung verwaltet werden. Sie können ohne Benutzerkonto auf den Switch zugreifen, wenn Sie direkt mit dem Switch verbunden sind. Für den Zugriff auf den Switch über Telnet muss jedoch mindestens ein Benutzerkonto eingerichtet sein. Beim Zugriff über eine Telnet-Verbindung muss der Switch zudem eine festgelegte IP-Adresse aufweisen, der entsprechende Verwaltungszugriff eingeräumt und eine Workstation mit dem Switch verbunden sein, bevor CLI-Befehle verwendet werden können.

Abbildung 5-1.



Flussdiagramm zu Installation und Konfiguration

Allgemeine Konfigurationsinformationen

Die Switches der Reihe 6200 werden mit Binärdateien ausgeliefert, die das Switch-Betriebssystem enthalten, und mit ASCII-Konfigurationsdateien, die die Beziehung des Switch zur Netzwerkumgebung definieren. Der Konfigurationsvorgang besteht darin, die ASCII-Konfigurationsdateien so anzupassen, dass sich jeder Switch in seine einzigartige Netzwerktopologie einfügt.

Auto-Verhandlung

Über die automatische Verbindungsaushandlung hat ein Switch (oder Stack, der als eine einzige Einheit operiert) die Möglichkeit, Betriebsarten mitzuteilen und andere Informationen mit einem anderen Switch auszutauschen, mit dem er ein Punkt-zu-Punkt-Verbindungssegment gemeinsam nutzt. Damit werden beide Switches automatisch so konfiguriert, dass sie ihre Fähigkeiten maximal ausnutzen.

Die automatische Verbindungsaushandlung wird während des Verbindungsaufbaus komplett innerhalb der physikalischen Schichten durchgeführt, ohne zusätzlichen Datenverkehr in den MAC-Schichten oder höheren Protokollschichten. Aufgrund der Auto-Verhandlung haben die Ports folgende Optionen:

- Bekanntgeben der Funktionsmerkmale
- Quittieren des Empfangs und Ermitteln gemeinsamer Betriebsarten, die beide Switches nutzen
- Ablehnen von Betriebsarten, die nicht von beiden Switches gemeinsam genutzt werden
- Konfigurieren der einzelnen Ports für die hochrangigste Betriebsart, die beide Ports unterstützen

ANMERKUNG: Achten Sie darauf, stets wenn irgend möglich die automatische Verbindungsaushandlung auf beiden Seiten der Verbindung zu verwenden, um potenzielle Probleme zu vermeiden.

Wenn Sie einen Port des Switch mit dem Netzwerkadapter (NIC) einer Workstation oder eines Servers verbinden, die Auto-Verhandlung nicht unterstützen oder nicht auf Auto-Verhandlung eingestellt sind, werden mehrere zusätzliche Schritte benötigt. Sowohl Switching-Port als auch NIC müssen manuell auf die gleiche Geschwindigkeit und den gleichen Duplex-Modus eingestellt werden. Das kann entweder über die Web-Browser-Schnittstelle oder CLI-Befehle erfolgen.

HINWEIS: Falls die Station am anderen Ende der Verbindung versucht, eine Auto-Verhandlung mit einem Port durchzuführen, der manuell für den Vollduplex-Modus konfiguriert ist, bewirkt die Auto-Verhandlung, dass die Station versucht, im Halbduplex-Modus zu arbeiten. Die daraus resultierende Fehlanpassung kann einen signifikanten Frame-Verlust verursachen. Dieser Umstand ist charakteristisch für die automatische Verbindungsaushandlung.

Konfiguration der Terminalverbindung

Ihr Switch benötigt die folgenden Terminalverbindungsparameter für die Konfiguration:

- keine Parität
- 1 Stoppbit
- 8 Datenbits
- keine Flusskontrolle

Baudrate

Die Baudraten können manuell auf beliebige folgende Werte geändert werden:

- 2400
- 4800
- 9600 (Standard-Baudrate)
- 19200
- 38400
- 57600
- 115200

Im Folgenden sehen Sie eine Beispielkonfiguration zum Ändern der Standard-Baudrate mithilfe von CLI-Befehlen:

```
console#configure

console(config)#line console

console(config-line)#speed 115200
```

ANMERKUNG: Vergessen Sie nicht, die Baudrate in der Terminalemulations-Software auf der Workstation so einzustellen, dass sie der Geschwindigkeit des Switch entspricht.

Weitere Konfigurationsanforderungen

Zum Herunterladen der integrierten Software und zur Konfiguration des Switch müssen folgende Voraussetzungen erfüllt sein:

- Das ASCII-Terminal (bzw. dessen Emulation) muss am seriellen Port (Kreuzkabel) hinten an der Einheit angeschlossen sein.
- Dem Switch muss eine IP-Adresse für die Switch-Fernsteuerung mit Telnet, SSH etc. zugewiesen sein.

Starten des Switch

Wenn das Gerät mit dem lokalen Terminal verbunden ist und der Strom eingeschaltet wird, durchläuft der Switch den Einschalt-Selbsttest (POST, Power On Self Test). Der Einschalt-Selbsttest wird bei jeder Initialisierung des Switch durchlaufen; dabei werden Hardwarekomponenten überprüft, um vor dem eigentlichen Startvorgang festzustellen, ob das Gerät vollständig betriebsbereit ist.

Wenn ein kritischer Fehler festgestellt wird, wird der Programmablauf unterbrochen. Bei erfolgreicher Ausführung des Einschalt-Selbsttests wird ein gültiges, ausführbares Image in das RAM geladen.

Die Fehler- bzw. Erfolgsmeldungen des Einschalt-Selbsttests werden auf dem Terminal angezeigt.

Führen Sie die folgenden Schritte aus, um den Switch zu starten:

1. Stellen Sie sicher, dass das serielle Kabel am Terminal angeschlossen ist.
2. Verbinden Sie das Netzteil mit dem Switch.
3. Schalten Sie den Switch ein.

   Beim Starten des Switch prüft der Starttest zunächst den verfügbaren Speicher und setzt dann den Startvorgang fort.
4. Während des Startvorgangs können Sie ggf. über das Menü **Boot** (Systemstart) spezielle Verfahren durchführen. Um das Menü **Boot** (Systemstart) aufzurufen, drücken Sie innerhalb der ersten zehn Sekunden nach Erscheinen der folgenden Meldung die Taste **2**.

   ```
   Select an option. (Wählen Sie eine Option.) If no selection in 10 seconds then

   operational code will start. (Wenn Sie innerhalb von 10 Sekunden keine Auswahl treffen, wird ausführbarer Code gestartet.)
   ```

```
1 - Start operational code. (Ausführbaren Code starten.)

2 - Start Boot Menu. (Boot-Menü starten).

Select (1, 2):2 (Auswahl)
```

Informationen über das Menü **Boot** (Systemstart) finden Sie unter "Boot-Menü (Systemstart)." Folgender Text ist ein Beispiel für die gesamte POST-Anzeige:

```
CPU Card ID: (Prozessorkarten-ID) 0x508541

volume descriptor ptr (pVolDesc): (Volume-Deskriptor-Pointer:) 0xffefd00

cache block I/O descriptor ptr (cbio): (Cacheblock-Deskriptor-Pointer:) 0xffefde0

auto disk check on mount: NOT ENABLED (Automatische Datenträgerprüfung beim Mounten: NICHT AKTIVIERT)

max # of simultaneously open files: (Maximale Anzahl gleichzeitig geöffneter Dateien): 22

file descriptors in use: (Verwendete Dateideskriptoren:) 0

# of different files in use: (Anzahl verschiedener verwendeter Dateien:) 0

# of descriptors for deleted files: (Anzahl Deskriptoren gelöschter Dateien:) 0

# of obsolete descriptors: (Anzahl veralteter Deskriptoren:) 0

current volume configuration: (Konfiguration des aktuellen Datenträgers:)

- volume label: NO LABEL ; (in boot sector: ((Volume-Bezeichnung: KEINE BEZEICHNUNG; (in Boot-Sektor)) )

- volume Id: (Volume-ID:) 0x0

- total number of sectors: (Gesamtanzahl Sektoren:) 60,716

- bytes per sector: (Bytes pro Sektor:) 512

- # of sectors per cluster: (Anzahl Sektoren pro Cluster:) 4

- # of reserved sectors: (Anzahl reservierter Sektoren:) 1

- FAT entry size: FAT16 (FAT-Eintragsgröße: FAT16)

- # of sectors per FAT copy: (Anzahl Sektoren pro FAT-Kopie:) 60

- # of FAT table copies: (Anzahl FAT-Tabellenkopien:) 2

- # of hidden sectors: (Anzahl versteckter Sektoren:) 4

- first cluster is in sector # 136 (Erster Cluster befindet sich in Sektor Nr. 136)

- Update last access date for open-read-close = FALSE (Letztes Zugriffsdatum für Öffnen-Lesen-Schließen aktualisieren = FALSCH)

- directory structure: VFAT (Verzeichnisstruktur: VFAT)

- root dir start sector: Startsektor im Root-Verzeichnis:) 121

- # of sectors per root: (Anzahl Sektoren pro Root:) 15

- max # of entries in root: (Max. Anzahl Einträge im Root:) 240

FAT handler information: (FAT-Handler-Information:)

------------------------

- allocation group size: Zuordnungs-Gruppengröße:) 2 clusters (2 Cluster)

- free space on volume: (Freier Speicherplatz auf Volume:) 15,335,424 bytes (15.335.424 Bytes)

Boot Menu Version: 22 Dec 2006 (Version des Bootmenüs: 22. Dez. 2006)

Select an option. (Wählen Sie eine Option.) If no selection in 10 seconds then

operational code will start. (Wenn Sie innerhalb von 10 Sekunden keine Auswahl treffen, wird ausführbarer Code gestartet.)

1 - Start operational code. (Ausführbaren Code starten.)

2 - Start Boot Menu. (Boot-Menü starten).

Select (1, 2):2 (Auswahl)

Boot Menu Version: 22 Dec 2006 (Version des Bootmenüs: 22. Dez 2006

Options available (Verfügbare Optionen)
```

```
1 - Start operational code (Ausführbaren Code starten)

2 - Change baud rate (Baudrate ändern)

3 - Retrieve event log using XMODEM (Ereignisprotokoll über XMODEM abrufen)

4 - Load new operational code using XMODEM (Neuen ausführbaren Code über XMODEM laden)

5 - Display operational code vital product data (Kritische Produktdaten für ausführbaren Code anzeigen)

6 - Run flash diagnostics (Flash-Diagnose ausführen)

7 - Update boot code (Startcode aktualisieren)

8 - Delete backup image (Sicherungs-Image löschen)

9 - Reset the system (System zurücksetzen)

10 - Restore configuration to factory defaults (delete config files) (Konfiguration mit werksseitigen Standardeinstellungen
wiederherstellen (Konfigurationsdateien löschen))

11 - Activate Backup Image (Sicherungs-Image aktivieren)

12 - Password Recovery Procedure (Verfahren zur Kennwort-Wiederherstellung)

[Boot Menu]
```

Der Startvorgang dauert ungefähr 60 Sekunden.

Die Meldung für den automatischen Systemstart, die am Ende des Einschalt-Selbsttests erscheint (siehe die letzten Zeilen) zeigt an, dass während des Startvorgangs keine Probleme auftraten. Um von der Eingabeaufforderung [Boot Menu] zum ausführbaren Code zurückzukehren, drücken Sie die Taste **1**.

ANMERKUNG: Die folgende Ausgabe entspricht einer Beispielkonfiguration. Adressen, Versionen und Datumsangaben können je nach Switch variieren.

```
Operational Code Date: Fri May 4 07:44:08 2007 (Datum des ausführbaren Codes: Fr 4 Mai 07:44:08 2007)

Uncompressing..... (Dekomprimieren läuft)

50% 100%

||||||||||||||||||||||||||||||||||||||||||||||||||

Attaching interface lo0...done (Schnittstelle lo0 wird verbunden...fertig)

Adding 36263 symbols for standalone. (36263 Symbole für eigenst. Betrieb werden hinzugefügt).

volume descriptor ptr (pVolDesc): (Volume-Deskriptor-Pointer:) 0xffc0650

cache block I/O descriptor ptr (cbio): (Cacheblock-Deskriptor-Pointer:) 0xffc0730

auto disk check on mount: (Automatische Datenträgerprüfung beim Mounten:) NOT ENABLED (Automatische Datenträgerprüfung beim Mounten: NICHT
AKTIVIERT

max # of simultaneously open files: (Maximale Anzahl gleichzeitig geöffneter Dateien): 22

file descriptors in use: (Verwendete Dateideskriptoren:) 0

# of different files in use: (Anzahl verschiedener verwendeter Dateien:) 0

# of descriptors for deleted files: (Anzahl Deskriptoren gelöschter Dateien:) 0

# of obsolete descriptors: (Anzahl veralteter Deskriptoren:) 0

current volume configuration: (Konfiguration des aktuellen Datenträgers:)

- volume label: NO LABEL ; (in boot sector: ((Volume-Bezeichnung: KEINE BEZEICHNUNG; (in Boot-Sektor)) )

- volume Id: (Volume-ID:) 0x0

- total number of sectors: (Gesamtanzahl Sektoren:) 60,716

- bytes per sector: (Bytes pro Sektor:) 512

- # of sectors per cluster: (Anzahl Sektoren pro Cluster:) 4

- # of reserved sectors: (Anzahl reservierter Sektoren:) 1

- FAT entry size: FAT16 (FAT-Eintragsgröße: FAT16

- # of sectors per FAT copy: (Anzahl Sektoren pro FAT-Kopie:) 60

- # of FAT table copies: (Anzahl FAT-Tabellenkopien:) 2
```

```
- # of hidden sectors: (Anzahl versteckter Sektoren:) 4

- first cluster is in sector # 136 (Erster Cluster befindet sich in Sektor Nr. 136)

- Update last access date for open-read-close = FALSE (Letztes Zugriffsdatum für Öffnen-Lesen-Schließen aktualisieren = FALSCH)

- directory structure: VFAT (Verzeichnisstruktur: VFAT)

- root dir start sector: Startsektor im Root-Verzeichnis:) 121

- # of sectors per root: (Anzahl Sektoren pro Root:) 15

- max # of entries in root: (Max. Anzahl Einträge im Root:) 240

FAT handler information: (FAT-Handler-Information:)

------------------------

- allocation group size: Zuordnungs-Gruppengröße:) 2 clusters (2 Cluster)

- free space on volume: (Freier Speicherplatz auf Volume:) 15.337.472 bytes (15.337.472 Bytes)

Timebase: (Zeitbasis) 66,666666 MHz, MEM: 266,666664 MHz, PCI: 66,666666 MHz, CPU: 533.33332

8 MHz

SOC unit 0 attached to PCI device BCM56314_A0 (SOC-Einheit 0 verbunden mit PCI-Gerät BCM56314_A0)

SOC unit 1 attached to PCI device BCM56314_A0 (SOC-Einheit 1 verbunden mit PCI-Gerät BCM56314_A0)

Adding BCM transport pointers (BCM-Transportzeiger werden hinzugefügt)

Configuring CPUTRANS TX (CPUTRANS TX wird konfiguriert)

Configuring CPUTRANS RX (CPUTRANS RX wird konfiguriert)

hpc - No stack ports. (Keine Stack-Ports.) Starting in stand-alone mode. (Start im Standalone-Modus.

(Unit 1 - Waiting to select management unit)> ((Einheit 1 - Warten auf Auswahl der Verwaltungseinheit)>)

<188> JAN 01 00:00:08 0.0.0.0-1 POE[254746256]: broad_poe.c(286) 4 % Unable to set POE Power bank 73 (broad_poe.c(286) 4 % POE Power Bank 73
kann nicht eingestellt werden)

Applying configuration, please wait ... (Konfiguration wird übernommen, bitte warten...)

No Potential unit to configure as Standby when unit 1 joined (Keine potenzielle Einheit kann für Standby konfiguriert werden, wenn Einheit 1
verbunden ist)

<187> JAN 01 00:00:13 192.168.2.1-1 UNITMGR[244207968]: unitmgr.c(4490) 15 % No

Potential unit to configure as Standby when unit 1 joined (Potenzielle Einheit für Standby-Konfiguration, wenn Einheit 1 verbunden ist)

....

console>
```

Nachdem der Switch erfolgreich gestartet wurde, erscheint eine Eingabeaufforderung, und Sie können unter Verwendung des lokalen Terminals mit der Konfiguration des Switch beginnen. Stellen Sie vor der Konfiguration jedoch sicher, dass es sich bei der installierten Softwareversion auf dem Switch um die neueste Version handelt. Wenn nicht die neueste Version installiert ist, laden Sie diese herunter und installieren sie. Siehe "Software-Download und Neustart".

Konfigurationsübersicht

Bevor Sie den Switch konfigurieren, erfragen Sie die folgenden Angaben vom Netzwerkadministrator:

- IP-Subnetzmaske für das Netzwerk
- IP-Adresse des Standard-Gateway (nächster Hop-Router) zur Konfiguration des Standardpfads

Es gibt zwei Konfigurationstypen:

- Die *Erstkonfiguration* umfasst Konfigurationsfunktionen mit Berücksichtigung grundlegender Sicherheitsaspekte.
- Die *fortgeschrittene* Konfiguration umfasst die dynamische IP-Konfiguration und berücksichtigt erweiterte Sicherheitsaspekte.

HINWEIS: Nach der Änderung von Konfigurationseinstellungen muss die neue Konfiguration vor dem Neustart gespeichert werden. Geben Sie zum Speichern der Konfiguration Folgendes ein:

```
console#copy running-config startup-config
```

Easy-Setup-Assistent

Der **Easy-Setup-Assistent** wird aufgerufen, wenn das System ohne Konfiguration oder nur mit der werksseitigen Standardkonfiguration gestartet wird. Der **Easy-Setup-Assistent** ist dazu bestimmt, Sie durch einige Anfangsschritte bei der Einrichtung der grundlegenden System- und Sicherheitskonfiguration zu führen und den Switch verwaltbar zu machen. Für den **Easy-Setup-Assistenten** ist es erforderlich, dass das ursprüngliche Administratorkonto beim Einschalten des Switch eingerichtet wird. Dieses administrative Konto, das vom Assistenten eingerichtet wird, weist die höchste Berechtigungsstufe (Stufe 15) auf.

Der **Easy-Setup-Assistent** führt Sie durch die anfängliche Basiskonfiguration eines neu installierten Switch, damit er unverzüglich implementiert, in Betrieb genommen und komplett über das Web, CLI und den Dell Network Manager per Fernzugang verwaltet werden kann. Nach der ersten Einrichtung können Sie im System eine erweiterte Konfiguration vornehmen.

Der Switch wird werksseitig mit der IP-Adresse 192.168.2.1 und der Netzmaske 255.255.255.0 ausgeliefert. Das System ist mit VLAN ID=1 als Standardverwaltungskennung eingerichtet. Die erste Konfiguration muss über die serielle Schnittstelle erfolgen, da ohne eine IP-Adresse nicht auf die anderen Verwaltungsschnittstellen zugegriffen werden kann.

Der Assistent konfiguriert den Switch wie folgt:

- Einrichtung des anfänglichen uneingeschränkten Benutzerkontos mit gültigem Kennwort. Der Assistent konfiguriert beim Setup ein uneingeschränktes Benutzerkonto. Diesem Konto wird die höchste Berechtigungsstufe zugewiesen (Stufe 15).
- Möglichkeit für CLI-Login und HTTP/HTTPS-Zugriff zur Verwendung der lokalen Authentifizierungseinstellungen. Sie können hier später Radius oder TACACS+ konfigurieren.
- Einrichtung der IP-Adresse für das Management-VLAN.
- Einrichtung des SNMP-Community-Strings für den SNMP-Manager an einer bestimmten IP-Adresse. Sie können diesen Schritt auslassen, wenn für den Switch kein SNMP-Management verwendet wird. Falls konfiguriert, ist die Standard-Zugriffsebene für die SNMP-Verwaltungsschnittstelle auf den höchstmöglichen Wert gesetzt. Anfänglich ist nur SNMPv1/2c aktiviert. SNMPv3 ist deaktiviert, bis Sie zurückkehren und den Sicherheitszugriff für SNMPv3 konfigurieren (z. B. engine ID, view etc.). Der SNMP-Community-String kann Leerzeichen enthalten. Im Assistenten ist die Verwendung von Anführungszeichen erforderlich, um Leerzeichen in den Community-String einzugeben. Obwohl Leerzeichen im Community-String zulässig sind, wird von deren Verwendung abgeraten. Der Standard-Community-String enthält keine Leerzeichen.
- Möglichkeit zum Festlegen der Management-Server-IP oder zum SNMP-Zugriff von allen IP-Adressen.
- Einrichtung der IP-Adresse des Standard-Gateway.

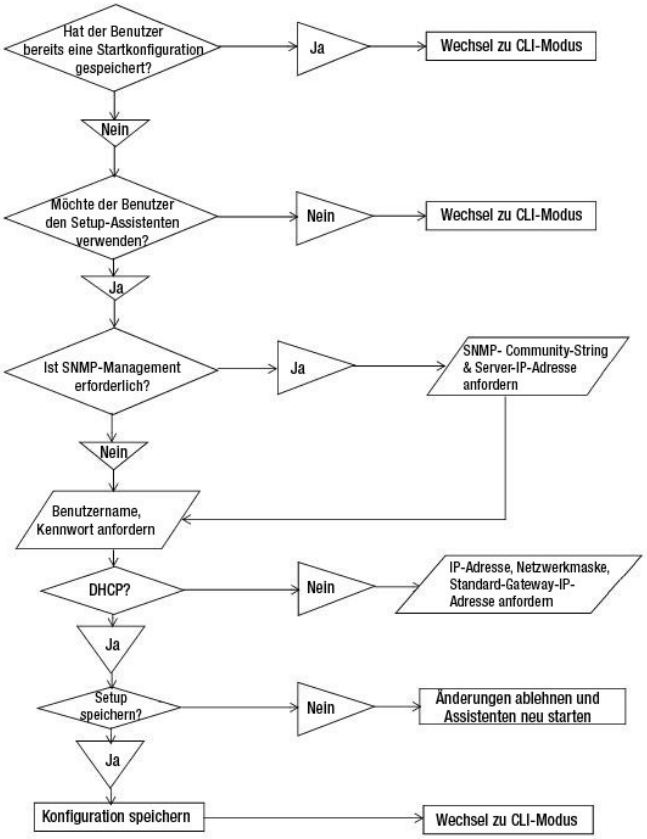
Wenn Sie den Assistenten nicht erstmalig verwenden, wird die Sitzung standardmäßig im CLI-Modus ausgeführt. Der Einrichtungsassistent wird weiter bei jeder Anmeldung aufgerufen, bis eine Konfiguration gespeichert wird. Nach dem Speichern wird die Assistentenoption nur dann wieder angeboten, wenn der Switch auf die werksseitigen Standardeinstellungen zurückgesetzt wird.

Da der Switch vor Ort ohne eine serielle Verbindung eingeschaltet werden kann, wartet er 60 Sekunden auf eine Einrichtungseingabe, falls er noch nicht konfiguriert wurde. Erfolgt keine Eingabe, fährt der Switch unter Verwendung der werksseitigen Standardkonfiguration mit dem Normalbetrieb fort. Beim nächsten Systemstart wird erneut die Ausführung des Einrichtungsassistenten angeboten.

Funktionsablauf

Im nachfolgenden Diagramm wird der Funktionsablauf für den **Easy-Setup-Assistenten** dargestellt.

Abbildung 5-2. Flussdiagramm für den Setup-Assistenten



Beispielsitzung des Easy-Setup-Assistenten

In diesem Abschnitt ist eine Sitzung mit dem **Easy-Setup-Assistenten** beschrieben. Im Ablaufdiagramm im vorherigen Abschnitt ist der allgemeine Arbeitsablauf dargestellt. Die in der folgenden Sitzung verwendeten Werte sind nur Beispiele. Bitte fordern Sie die tatsächlichen Werte von Ihrem oder Ihren Netzwerkadministratoren an:

- Die IP-Adresse für das Management-VLAN lautet 192.168.1.1:255.255.255.0.
- Der Benutzername lautet *admin*, und das Kennwort ist *admin123*.
- Die IP-Adresse des Netzwerk-Management-Systems lautet 192.168.1.10.
- Das Standard-Gateway ist 192.168.1.100.
- Der zu verwendende SNMP-Community-String lautet *Dell_Network_Manager*.

Der Setup-Assistent konfiguriert die Anfangswerte wie oben definiert. Nach dem Abschließen des Assistenten ist das System wie folgt konfiguriert:

- SNMPv1/2c ist aktiviert, und der Community-String ist eingerichtet wie oben definiert. SNMPv3 ist deaktiviert.
- Das admin-Benutzerkonto ist eingerichtet wie definiert.
- Ein Netzwerk-Management-System ist konfiguriert. Von dieser Management-Station können Sie auf die SNMP-, HTTP- und CLI-Schnittstelle zugreifen. Sie können auch festlegen, dass diese Management-Schnittstellen von allen IP-Adressen zugänglich sein sollen, indem Sie die IP-Adresse (0.0.0.0) wählen.
- Eine IP-Adresse ist für das Standard-Management-VLAN (1) konfiguriert.
- Eine Standard-Gateway-Adresse ist konfiguriert.

ANMERKUNG: Im folgenden Beispiel stehen die für den Benutzer möglichen Optionen in eckigen Klammern [ ]. Der Standardwert ist gegebenenfalls in geschweiften Klammern { } angegeben. Wenn Sie die <Eingabetaste> drücken, ohne eine Option gewählt zu haben, akzeptieren Sie damit den Standardwert. Hilfetexte sind in Klammern gesetzt.

Das folgende Beispiel enthält eine Abfolge von Eingabeaufforderungen und Reaktionen im Rahmen einer beispielhaften Sitzung mit dem Dell **Easy-Setup-Assistenten**, wobei die oben genannten Eingabewerte verwendet werden.

```
Welcome to Dell Easy Setup Wizard

The setup wizard guides you through the initial switch configuration, and gets you up and running as quickly as possible. (Der
Einrichtungsassistent führt Sie durch die anfängliche Switch-Konfiguration, damit Sie so schnell wie möglich mit dem Switch arbeiten können.)
You can skip the setup wizard, and enter CLI mode to manually configure the switch. You must respond to the next question to run the setup
```

wizard within 60 seconds, otherwise the system will continue with normal operation using the default system configuration. (Sie müssen auf die nächste Frage zur Ausführung des Einrichtungsassistenten innerhalb von 60 Sekunden antworten, andernfalls setzt das System den Normalbetrieb unter Verwendung der Standardsystemkonfiguration fort.) Note: (Anmerkung:) You can exit the setup wizard at any point by entering [ctrl+z].

Would you like to run the set up wizard (you must answer this question within 60 seconds)? (Möchten Sie den Einrichtungsassistenten ausführen (Sie müssen innerhalb von 60 Sekunden antworten)?) [Y/N] ***y***

Step 1:

The system is not set up for SNMP management by default. (Das System ist standardmäßig nicht für SNMP-Management eingerichtet.) To manage the switch using SNMP (required for Dell Network Manager) you can:

o Set up the initial SNMP version 2 account now.

o Return later and set up other SNMP accounts. (Später hierher zurückkehren und weitere SNMP-Konten einrichten.) (For more information on setting up an SNMP version 3 account, see the user documentation).

Would you like to set up the SNMP management interface now? (Möchten Sie die SNMP-Management-Schnittstelle jetzt einrichten?) [Y/N] ***y***

To set up the SNMP management account you must specify the management system IP address and the "community string" or password that the particular management system uses to access the switch. (Zum Einrichten des SNMP-Management-Kontos müssen Sie die IP-Adresse des Management-Systems und den "Community-String" oder das Kennwort eingeben, die ein bestimmtes Management-System für den Zugriff auf den Switch verwendet.) The wizard automatically assigns the highest access level [Privilege Level 15] to this account. You can use Dell Network Manager or other management interfaces to change this setting and to add additional management system later. (Sie können diese Einstellung mithilfe von Dell Network Manager oder anderen Management-Schnittstellen später ändern oder zusätzliche Management-Systeme hinzufügen.) For more information on adding management systems, see the user documentation.

To add a management station:

Please enter the SNMP community string to be used {public}: (Bitte geben Sie den zu verwendenden SNMP-Community-String ein {public}:)

>> ***Dell_Network_Manager***<Return>

Please enter the IP address of the Management System (A.B.C.D) or wildcard (0.0.0.0) to manage from any Management Station {0.0.0.0}: (Bitte geben Sie die IP-Adresse des Management-Systems (A.B.C.D) ein, oder einen Platzhalter (0.0.0.0), um eine Management-Station zu verwenden {0.0.0.0}:)

>> ***192.168.1.10***<Return>

Step 2:

Now we need to set up your initial privilege (Level 15) user account. (In diesem Schritt wird Ihr Benutzerkonto mit der anfänglichen Berechtigungsstufe (Stufe 15) eingerichtet.) This account is used to login to the CLI and Web interface. You may set up other accounts and change privilege levels later. (Sie können zu einem späteren Zeitpunkt weitere Konten einrichten und die Berechtigungsstufen ändern.) For more information on setting up user accounts and changing privilege levels, see the user documentation.

To set up a user account: (So richten Sie ein Benutzerkonto ein:)

Please enter the user name {admin}: (Bitte geben Sie den Benutzernamen ein {admin}:) ***admin***<Return>

Please enter the user password: ********<Return>

Please reenter the user password: ********<Return>

ANMERKUNG: Wenn der erste Eintrag für das Kennwort nicht mit dem zweiten Eintrag übereinstimmt, wird der Benutzer jeweils erneut zur Eingabe aufgefordert.

Step 3:

Next, an IP address is set up. (Als Nächstes wird eine IP-Adresse eingerichtet.) The IP address is defined on the default VLAN (VLAN #1), of which all ports are members. This is the IP address you use to access the CLI, Web interface, or SNMP interface for the switch. Optionally you may request that the system automatically retrieve an IP address from the network via DHCP (this require that you have a DHCP server running on the network). (Optional können Sie vorgeben, dass das System automatisch eine IP-Adresse vom Netzwerk per DHCP abruft (dafür muss ein DHCP-Server im Netzwerk betrieben werden).)

To set up an IP address: (So richten Sie eine IP-Adresse ein:)

Please enter the IP address of the device (A.B.C.D) or enter "DHCP" (without the quotes) to automatically request an IP address from the network DHCP server: (Bitte geben Sie die IP-Adresse des Geräts (A.B.C.D) ein bzw. "DHCP" (ohne Anführungszeichen), um eine IP-Adresse vom DHCP-Netzwerkserver zu beziehen (192.168.2.1):

>> ***192.168.2.1***<Return>

Please enter the IP subnet mask (A.B.C.D or /nn){255.255.255.0}: (Bitte geben Sie die IP-Subnetzmaske ein (A.B.C.D oder /nn){255.255.255.0}:)

>> ***255.255.255.0***<Return>

ANMERKUNG: Wenn Sie oben DHCP gewählt haben, fragt das System nicht nach der IP-Subnetzmaske, da diese Information vom DHCP-Server geliefert wird.

Step 4:

Finally, set up the default gateway. (Richten Sie schließlich das Standard-Gateway ein.) Please enter the IP address of the gateway from which this network is reachable (e.g. 0.0.0.0): (Bitte geben Sie die IP-Adresse des Gateway ein, von dem aus dieses Netzwerk erreicht werden kann (z. B 0.0.0.0). >> ***192.168.2.100***<Return>

ANMERKUNG: Wenn Sie oben DHCP gewählt haben, fragt das System nicht nach dem Standard-Gateway, da diese Information vom DHCP-Server geliefert wird.

```
This is the configuration information that has been collected:

SNMP Interface = "Dell_Network_Manager"@192.168.1.10

User Account set up = admin

Password = **********

Management IP address = 192.168.2.1 255.255.255.0

Default Gateway = 192.168.2.100
```

Step 5:

```
If the information is correct, please select (Y) to save the configuration, and copy to the start-up configuration file. If the information is
incorrect, select (N) to discard configuration and restart the wizard: [Y/N] y

Thank you for using Dell Easy Set up Wizard. (Danke für die Verwendung des Dell-Easy-Setup-Assistenten.) You will now enter CLI mode.
```

Fortgeschrittene Konfiguration

CLI-Grundlagen

Mit dem Befehl help (Hilfe) im Benutzer-EXEC-Modus und im privilegierten EXEC-Modus werden die Tastaturkürzel angezeigt. Im Folgenden finden Sie ein Beispiel für eine durch den Hilfebefehl ausgelöste Anzeige:

```
Console>help

HELP:

Special keys: (Sondertasten:)

DEL, BS .... delete previous character (Entf, Zurücktaste .... Vorheriges Zeichen löschen)

Ctrl-A .... go to beginning of line (Strg-A .... Zum Anfang der Zeile)

Ctrl-E .... go to end of line (Strg-E .... Zum Ende der Zeile)

Ctrl-F .... go forward one character (Strg-F .... Ein Zeichen vorwärts)

Ctrl-B .... go backward one character (Strg-B .... Ein Zeichen zurück)

Ctrl-D .... delete current character (Strg-D .... Aktuelles Zeichen löschen)

Ctrl-U, X .. delete to beginning of line (Strg-U, X .... Bis zum Anfang der Zeile löschen)

Ctrl-K .... delete to end of line (Strg-K .... Bis zum Ende der Zeile löschen)

Ctrl-W .... delete previous word (Strg-W .... Vorheriges Wort löschen)

Ctrl-T .... transpose previous character (Strg-T .... Vorheriges Zeichen umstellen)

Ctrl-P .... go to previous line in history buffer (Strg-P .... Zur vorherigen Zeile im Verlaufspuffer)

Ctrl-R .... rewrites or pastes the line (Strg-R .... Zeile neu schreiben oder einfügen)

Ctrl-N .... go to next line in history buffer (Strg-N .... Zur nächsten Zeile im Verlaufspuffer)

Ctrl-Y .... print last deleted character (Strg-Y .... Zuletzt gelöschtes Zeichen drucken)

Ctrl-Z .... return to root command prompt (Strg-Z .... Zurück zur Eingabeaufforderung für root-Befehle)

Ctrl-Q  .... enables serial flow (Strg-Q ... aktiviert den seriellen Datenfluss)

Ctrl-S  .... disables serial flow (Strg-S ... deaktiviert den seriellen Datenfluss)

Tab, <SPACE> command-line completion (Tabulator, <LEERTASTE>: Befehlszeilenabschluss)

Exit .... go to next lower command prompt (Exit .... Zur darunterliegenden Befehlseingabeaufforderung)

? .... list choices (Wahlmöglichkeiten auflisten)
```

Kontextsensitive Hilfe

Verwenden Sie den Befehl **?**, um kontextsensitive Hilfe in CLI zu erhalten. Er kann verwendet werden, um die Liste mit möglichen Unterbefehlen abzurufen oder um mögliche Befehle aufzulisten, die mit teilweise eingegebenen Befehlen beginnen. Wenn der Befehl **?** in einer leeren Zeile eingegeben wird, wird die Liste der Befehle aufgerufen, die für die entsprechende Ebene im Befehlsbaum zur Verfügung stehen. **?** kann auch innerhalb einer Befehlseingabe verwendet werden, um die Liste der Parameter abzurufen, die für die Vervollständigung des Befehls benötigt werden. Parameter, die bereits vom Benutzer spezifiziert wurden, werden nicht in die Befehlsliste aufgenommen, d. h., nur die fehlenden Parameter werden aufgelistet.

Vereinbarte Schnittstellenbezeichnung

In einer CLI-Implementierung nach Industriestandard gibt es eine allgemein anerkannte Konvention für die Bezeichnung von Schnittstellen in CLI. Für die Schnittstellenbezeichnung auf Dell-Geräten gilt folgende Konvention:

- **Unit#/Interface ID** – Jede Schnittstelle wird über die *Unit#* (Einheitennummer) gekennzeichnet, gefolgt vom Zeichen / und der *Interface ID* (Schnittstellen-ID) (siehe unten). Der Wert **2/g10** steht beispielsweise für Gigabit-Port 10 in der zweiten Einheit eines Stack.
- **Unit#** — Die Einheitennummer wird nur in einer Stack-Lösung verwendet, bei der eine Anzahl von Switches für die Bildung eines virtuellen Geräts zusammengefasst sind. In diesem Fall bezeichnet die *Einheitennummer* die physikalische Gerätekennzeichnung innerhalb des Stack.
- **Interface ID** — besteht aus dem Schnittstellentyp gefolgt von der Schnittstellennummer. Es gibt aktuell eine vordefinierte Liste von *Schnittstellentypen* (siehe unten). Falls zusätzliche Schnittstellentypen definiert werden sollen, müssen diese bei Dell registriert werden. Der Wert **2/g10** steht beispielsweise für Gigabit-Port 10 auf der zweiten Einheit.
- **Interface Types** — Die folgenden Schnittstellentypeen sind in den Switches der Reihe 6200 definiert:
  - **g** — Gigabit-Ethernet-Port (1/**g2** ist zum Beispiel Gigabit-Ethernet-Port 2).
  - **xg** — 10-Gigabit-Ethernet-Port (1/**xg2** ist zum Beispiel 10-Gigabit-Ethernet-Port 2).

CLI-Referenzhandbuch für PowerConnect 6200 Systeme

Detaillierte Informationen über alle CLI-Befehle, die für Switches der Reihe 6200 zur Verfügung stehen, finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch).

Dieser Abschnitt enthält zusammenfassende Informationen über häufige Aufgaben, wie zum Beispiel:

- Ändern der Standardeinstellungen von Switch-Ports
- Abrufen einer IP-Adresse von einem DHCP-Server
- Konfigurieren eines ersten Konsolenkennworts
- Konfigurieren eines ersten Telnet-Kennworts
- Konfigurieren eines ersten HTTP-Kennworts
- Konfigurieren eines ersten HTTPS-Kennworts

Ändern der Standardeinstellungen von Switch-Ports

Werden IP-Adressen über DHCP und BOOTP konfiguriert bzw. empfangen, umfasst die von diesen Servern eingehende Konfiguration neben den IP-Adressen gegebenenfalls auch eine Subnetzmaske sowie ein Standard-Gateway.

Bei der ersten Anmeldung wird CLI im Stammverzeichnis der Befehlshierarchie aufgerufen. Um zu einer anderen Ebene der Befehlshierarchie zu springen, geben Sie Befehle wie z. B. **configure** (Konfigurieren) ein, die dazu führen, dass CLI in das Unterverzeichnis *config* wechselt. Um zur vorherigen Ebene in der Befehlshierarchie zurückzukehren, verwenden Sie den exit-Befehl.

```
SwitchA#configure
SwitchA(config)#exit
SwitchA#
```

In den folgenden Beispielen sind die Eingabeaufforderungen des Systems dargestellt, die von den Switches der Reihe 6200 verwendet werden:

- **SwitchA>** — Zeigt an, dass der Gerätename *SwitchA* ist und sich CLI aktuell auf der oberen Ebene der Befehlshierarchie befindet. CLI wird zudem im *Benutzer-EXEC-Modus* ausgeführt.
- **SwitchA#** — Diese Eingabeaufforderung ähnelt der obigen mit der Ausnahme, dass durch # angezeigt wird, dass CLI in einem privilegierten EXEC-Modus ausgeführt wird (nicht im Benutzer-EXEC-Modus).
- **SwitchA(config)#** – Zeigt an, dass CLI aktuell im *globalen Konfigurationsmodus* der Befehlshierarchie ausgeführt wird. Diesen Modus aktivieren Sie, indem Sie auf der oberen Ebene **configure** (Konfigurieren) eingeben.
- **SwitchA(config-if)#** – Diese Eingabaufforderung zeigt an, dass CLI aktuell im *Schnittstellenkonfigurationsmodus* ausgeführt wird. Sie aktivieren diesen Modus, indem Sie im Konfigurationsmodus **interface range ethernet** (Schnittstellenbereich Ethernet), **interface range port-channel** (Schnittstellenbereich Port-Kanal) oder **interface range vlan** (Schnittstellenbereich VLAN) eingeben. In diesen Fällen ist kein spezifischer Verweis auf eine Schnittstelle vorhanden, d. h., das System wird mit einem allgemeinen Schnittstellensatz betrieben.
- **SwitchA(config-if-1/g1)#** – Zeigt an, dass CLI aktuell auf der Gigabit-Ethernet-Schnittstelle 1 ausgeführt wird.

Standardeinstellungen von Switch-Ports

In der folgenden Tabelle werden die Standardeinstellungen von Switch-Ports beschrieben.

Tabelle 5-1. Standardeinstellungen von Ports

Funktion	Standardeinstellung
Geschwindigkeit und Betriebsart	1000M-Auto-Verhandlung
Weiterleitungsstatus der Ports	Aktiviert
Schutz vor Head-of-Line-Blocking	Ein (aktiviert)
Flusskontrolle	Aus
Backpressure	Aus

Im Folgenden finden Sie ein Beispiel für die Änderung der Geschwindigkeit auf Port 1/ g1 mithilfe von CLI-Befehlen:

```
console(config)#interface ethernet 1/g1

console(config-if-1/g1)#speed 100
```

Abrufen einer IP-Adresse von einem DHCP-Server

Wenn eine IP-Adresse über das DHCP-Protokoll abgerufen wird, fungiert der Switch als DHCP-Client.

Gehen Sie wie folgt vor, um eine IP-Adresse von einem DHCP-Server abzurufen:

Wählen Sie einen beliebigen Port, und verbinden Sie diesen mit einem DHCP-Server oder einem Subnetz, das über einen DHCP-Server verfügt, um die IP-Adresse abzurufen.

ANMERKUNG: Die Switch-Konfiguration muss nicht gelöscht werden, um eine IP-Adresse für den DHCP-Server abrufen zu können.

1. Geben Sie die nachfolgenden Befehle ein, um den gewählten Port für den Empfang der IP-Adressen zu nutzen.
   - Zuweisen von dynamischen IP-Adressen:

   ```
   console#config

   console(config)#ip address dhcp
   ```

   Die IP-Adresse wird über die Schnittstelle automatisch empfangen.

2. Geben Sie an der Systemeingabeaufforderung den Befehl **show ip interface** wie im nachfolgenden Beispiel gezeigt ein, um die IP-Adresse zu überprüfen.

   ```
   console#show ip interface

   Management Interface: (Management-Schnittstelle:)

   IP Address (IP-Adresse)..................... 10.240.4.125

   Subnet Mask (Subnetzmaske)..................... 255.255.255.0

   Default Gateway (Standard-Gateway).............. 10.240.4.1

   Burned In MAC Address (Übertragene MAC-Adresse)................. 00:10:18:82:04:35

   Network Configuration Protocol Current Aktuelles Netzwerkkonfigurationsprotokoll)......... DHCP

   Management VLAN ID (Management-VLAN-ID)............................ 1

   Routing Interfaces: (Routing-Schnittstellen:)

                                              Netdir Multi
   Interface IP Address IP Mask Bcast CastFwd

   ---------- --------------- --------------- -------- --------

   vlan1        192.168.10.10 255.255.255.0 Disable Disable

   vlan2        0.0.0.0 0.0.0.0 Enable Disable

   loopback2 0.0.0.0 0.0.0.0 Disable Disable
   ```

Sicherheitsverwaltung und Kennwortkonfiguration

Die Systemsicherheit wird über den so genannten AAA-Mechanismus (Authentifizierung, Autorisierung und Accounting) realisiert, der eine Verwaltung der

benutzerspezifischen Zugriffsrechte, Privilegien und Management-Verfahren ermöglicht. AAA greift hierbei auf lokale und dezentral installierte Benutzerdatenbanken zurück. Die Datenverschlüsselung erfolgt über den SSH-Mechanismus.

Das System wird ohne vorkonfiguriertes Standardkennwort ausgeliefert; sämtliche Kennwörter werden benutzerseitig definiert. Falls ein benutzerdefiniertes Kennwort verloren geht, kann über das Menü **Boot (Systemstart) eine Prozedur zur Kennwortwiederherstellung aufgerufen werden.** Diese Prozedur, die am lokalen Terminal verfügbar ist, bietet die Möglichkeit, von diesem Terminal aus einmalig ohne Kennworteingabe auf den Switch zuzugreifen.

Konfigurieren von Sicherheitskennwörtern

Für folgende Dienste können Sicherheitskennwörter konfiguriert werden:

- Konsole
- Telnet
- SSH
- HTTP
- HTTPS

ANMERKUNG: Bei der Einrichtung eines Benutzernamens wird standardmäßig die Priorität 1 gesetzt (d. h. einfacher Zugang ohne Konfigurationsrechte). Um Switch-Zugriffe mit Konfigurationsrechten zu ermöglichen, muss ausdrücklich die Priorität 15 festgelegt werden.

Konfigurieren eines ersten Konsolenkennworts

Zum Konfigurieren eines ersten Konsolenkennworts geben Sie die folgenden Befehle ein:

```
console(config)#aaa authentication login default line

console(config)#aaa authentication enable default line

console(config)#line console

console(config-line)#login authentication default

console(config-line)#enable authentication default

console(config-line)#password secret123
```

- Wenn Sie sich erstmalig über eine Konsolensitzung bei einem Switch anmelden, geben Sie an der Kennwort-Eingabeaufforderung **secret123** ein.
- Wenn Sie einen Switch-Modus erstmalig von deaktiviert in aktiviert ändern, geben Sie an der Kennwort-Eingabeaufforderung **secret123** ein.

Konfigurieren eines ersten Telnet-Kennworts

Zum Konfigurieren eines ersten Telnet-Kennworts geben Sie die folgenden Befehle ein:

```
console(config)#aaa authentication login default line

console(config)#aaa authentication enable default line

console(config)#line telnet

console(config-line)#login authentication default

console(config-line)#enable authentication default

console(config-line)#password pass1234
```

- Wenn Sie sich erstmalig über eine Telnet-Sitzung bei einem Switch anmelden, geben Sie an der Kennwort-Eingabeaufforderung **pass1234** ein.
- Wenn Sie einen Switch-Modus erstmalig von deaktiviert in aktiviert ändern, geben Sie **pass1234** ein.

Konfigurieren eines ersten HTTP-Kennworts

Geben Sie die folgenden Befehle ein, um ein erstes HTTP-Kennwort zu konfigurieren:

```
console(config)#ip http authentication local

console(config)#username admin password user1234 level 15
```

Konfigurieren eines ersten HTTPS-Kennworts

Zum Konfigurieren eines ersten HTTPS-Kennworts geben Sie die folgenden Befehle ein:

```
console(config)#ip https authentication local
```

ANMERKUNG: Sie sollten bei jedem Upgrade (Installieren einer neuen Version) der Steuersoftware-Anwendung auf dem Switch ein neues "crypto certificate" (Schlüsselzertifikat) erzeugen.

Geben Sie die folgenden Befehle einmal ein, wenn Sie die Verwendung einer HTTPS-Sitzung über eine Konsolen-, Telnet- oder SSH-Sitzung konfigurieren.

ANMERKUNG: Aktivieren Sie im Webbrowser SSL 2.0 (oder höher) für den anzuzeigenden Seiteninhalt.

```
console(config)#crypto certificate 1 generate

console(config)#ip https server
```

ANMERKUNG: Eine Nutzung der Dienste HTTP und HTTPS ist nur auf Zugriffsebene 15 sowie bei direkter Anbindung an den Konfigurationszugang möglich.

Software-Download und Neustart

Software-Download über XModem

Dieser Abschnitt enthält Anleitungen zum Herunterladen von Switch-Software (System- und Boot-Images) über XModem, einem Datenübertragungsprotokoll für die Aktualisierung von Sicherungs-Konfigurationsdateien.

ANMERKUNG: Sie müssen während dieser Vorgänge mit der seriellen Konsolenschnittstelle verbunden sein, weil der XModem-Download bei einer anderen Verbindung nicht funktioniert.

So laden Sie eine Software-Image-Datei mithilfe von XModem herunter:

Geben Sie den Pfad der Quelldatei an, um mit der Übertragung zu beginnen.

Es werden beispielsweise folgende Informationen angezeigt:

```
console#copy xmodem image

Mode (Modus)..................................... XMODEM

Data Type (Datentyp)............................... Code

Destination Filename (Zieldateiname)..................... image2

Management access will be blocked for the duration of the transfer (Der Management-Zugriff ist während der Übertragungsdauer blockiert.)

Are you sure you want to start? (Möchten Sie den Vorgang starten?) (y/n) y

console#boot system image2
```

Software-Download über einen TFTP-Server

Dieser Abschnitt enthält Anleitungen zum Herunterladen der Switch-Software (System- und Boot-Images) über einen TFTP-Server. Vor dem Herunterladen der Software muss der TFTP-Server im Netzwerk verfügbar sein.

Beim Start des Switch wird das System-Image aus dem Flash-Speicherbereich, wo eine Kopie des System-Image gespeichert ist, dekomprimiert.

HINWEIS: Sie müssen den Befehl **boot system** (System starten) ausführen, um das neu heruntergeladene Image zu aktivieren.

Beim nächsten Startvorgang dekomprimiert und führt der Switch das derzeit aktive System-Image aus, falls nicht anders festgelegt.

So laden Sie ein Image vom TFTP-Server herunter:

1. Stellen Sie sicher, dass an einem der Switch-Ports eine IP-Adresse konfiguriert ist und Ping-Befehle an einen TFTP-Server gesendet werden können.
2. Die herunterzuladende Datei (die STK-Datei) muss auf dem TFTP-Server gespeichert sein.
3. Geben Sie den Befehl **show version** ein, um die derzeitige Versionsnummer der Software auf dem Switch zu überprüfen.

   Es werden beispielsweise folgende Informationen angezeigt:

   ```
   console>show version

   Image Descriptions (Image-Beschreibungen)
   ```

```
image1 : default image (Standard-Image)

image2 :

Images currently available on Flash (Derzeit auf Flash verfügbare Images)

--------------------------------------------------------------

unit image1     image2   current-active next-active

--------------------------------------------------------------

1   0.15.0.0   0.15.0.0    image1          image1
```

4. Geben Sie den Befehl **show bootvar** ein, um festzustellen, welches System-Image derzeit aktiv ist. Es werden beispielsweise folgende Informationen angezeigt:

```
console>show bootvar

Image Descriptions (Image-Beschreibungen)

image1 : default image (Standard-Image

image2 :

Images currently available on Flash (Derzeit auf Flash verfügbare Images)

--------------------------------------------------------------

unit image1    image2   current-active  next-active

--------------------------------------------------------------

1   0.15.0.0   0.15.0.0   image1          image1
```

5. Geben Sie den Befehl **copy tftp://{*TFTP-Adresse*}/{*Dateiname*} image2** ein, um ein neues System-Image zum Switch zu kopieren.

   Nach dem Herunterladen des neuen Image wird es in dem Bereich gespeichert, der für die andere Kopie des System-Image vorgesehen ist (im Beispiel image2). Es werden beispielsweise folgende Informationen angezeigt:

```
console#copy tftp://10.254.24.64/pc62xxr0v34.stk image2

Mode (Modus)..................................... TFTP

Set TFTP Server IP (TFTP-Server-IP-Adresse festlegen)..... 10.254.24.64

TFTP Path (TFTP-Pfad)..... ./

TFTP Filename TFTP-Dateiname)..... pc62xxr0v34.stk

Data Type (Datentyp)..... Code

Destination Filename (Zieldateiname)..... image2

Management access will be blocked for the duration of the transfer (Der Management-Zugriff ist während der Übertragungsdauer blockiert.)

Are you sure you want to start? (Möchten Sie den Vorgang starten?) (y/n) y
```

   Ausrufezeichen zeigen den Fortschritt des Kopiervorgangs an. Ein Punkt zeigt an, dass das Zeitlimit für den Kopiervorgang überschritten wurde. Viele Punkte in einer Reihe zeigen an, dass der Kopiervorgang fehlgeschlagen ist.

6. Wählen Sie das Image für den nächsten Start aus, indem Sie den Systembefehl **boot** (Starten) eingeben. Geben Sie danach den Befehl **show bootvar** ein, um zu überprüfen, dass die im Start-Systembefehl **boot system** als Parameter eingegebene Kopie für den nächsten Start ausgewählt ist.

   Es werden beispielsweise folgende Informationen angezeigt:

```
console#boot system image2

Activating image image2 .. (Image image2 wird aktiviert ..)

console>show bootvar

Image Descriptions (Image-Beschreibungen)

image1 : default image (Standard-Image

image2 :

Images currently available on Flash (Derzeit auf Flash verfügbare Images)

--------------------------------------------------------------
```

```
unit   image1    image2    current-active   next-active

-------------------------------------------------------------

1    0.15.0.0   0.15.0.0      image1          image2
```

Wenn das Image für den nächsten Start durch Eingabe des Start-Systembefehls **boot system** nicht ausgewählt wird, startet das System vom derzeit aktiven Image (im Beispiel image1).

7. Geben Sie den Befehl **reload** (Neu laden) ein. Die folgende Meldung wird angezeigt:

```
console#reload

Management switch has unsaved changes. (Nicht gespeicherte Änderungen im Management-Switch.)

Are you sure you want to continue? (Möchten Sie den Vorgang fortsetzen?) (y/n)
```

8. Geben Sie **y** für "ja" ein. Daraufhin wird die folgende Meldung wird angezeigt:

```
Configuration Not Saved! (Konfiguration nicht gespeichert!)

Are you sure you want to start? (Möchten Sie den Stack neu laden?) (y/n)
```

9. Geben Sie **y** ein, um den Switch neu zu starten.

Aktualisieren des Startcode

Verwenden Sie den Befehl **update bootcode**, um den Startcode auf alle Switches zu aktualisieren. Für jeden Switch wird der Startcode aus dem aktiven Image extrahiert und in den Flash-Speicher gelesen. Um den Startcode für einen einzelnen Switch zu aktualisieren, geben Sie die Einheit im Befehl an (wie im folgenden Beispiel gezeigt).

Um den Startcode auf einem Switch anzuzeigen, starten Sie diesen Switch neu. Die Build-Daten werden während des Startvorgangs angezeigt.

1. Geben Sie den folgenden Befehl ein, wobei 2 die Einheitennummer ist:

```
console# update bootcode 2

Updating boot code ... (Startcode wird aktualisiert ...)

Boot code update completed successfully. (Startcode-Aktualisierung erfolgreich abgeschlossen)
```

2. Geben Sie den Befehl **reload** (Neu laden) ein.

```
console#reload

Are you sure you want to start? (Möchten Sie den Stack neu laden?) (y/n)
```

3. Geben Sie **y** ein, um den Switch neu zu starten.

Menü Boot (Systemstart)

Sie können im Menü **Boot** (Systemstart) viele Konfigurationsaufgaben durchführen. Das Menü kann nach dem Durchlauf des ersten Teils des POST aufgerufen werden.

So zeigen Sie das Menü **Boot** (Systemstart) an:

1. Drücken Sie während des Startvorgangs innerhalb von zehn Sekunden nach dem Erscheinen der folgenden Meldung die Taste **2**:

```
Boot Menu Version: Oct 20 2004 (Bootmenü-Version: 20. Okt. 2004)

Select an option. (Wählen Sie eine Option.) If no selection in 10 seconds then

operational code will start. (Wenn Sie innerhalb von 10 Sekunden keine Auswahl treffen, wird ausführbarer Code gestartet.)

1 - Start operational code. (Ausführbaren Code starten.)

2 - Start Boot Menu. (Boot-Menü starten).

Select (1, 2): (Auswahl)
```

Das Menü **Boot** (Systemstart) wird angezeigt und enthält die folgenden Konfigurationsfunktionen:

```
1 - Start operational code (Ausführbaren Code starten)
```

```
2 - Change baud rate (Baudrate ändern)

3 - Retrieve event log using XMODEM (Ereignisprotokoll über XMODEM abrufen)

4 - Load new operational code using XMODEM (Neuen ausführbaren Code über XMODEM laden)

5 - Display operational code vital product data (Kritische Produktdaten für ausführbaren Code anzeigen)

6 - Run flash diagnostics (Flash-Diagnose ausführen)

7 - Update boot code (Startcode aktualisieren)

8 - Delete backup image (Sicherungs-Image löschen)

9 - Reset the system (System zurücksetzen)

10 - Restore configuration to factory defaults (delete config files) (Konfiguration mit werksseitigen Standardeinstellungen
wiederherstellen (Konfigurationsdateien löschen))

11 - Activate Backup Image (Sicherungs-Image aktivieren)

12 - Password Recovery Procedure (Verfahren zur Kennwort-Wiederherstellung)
```

In den folgenden Abschnitten werden die Optionen im Menü **Boot** (Systemstart) beschrieben.

Ausführbaren Code starten

Verwenden Sie Option 1, um mit dem Laden des ausführbaren Codes fortzufahren.

So starten Sie den Vorgang zum Systemstart aus dem Menü **Boot (Systemstart)**:

1. Wählen Sie im Menü **Boot (Systemstart)** die Option **1** , und drücken Sie die <Eingabetaste>.

   Die folgende Eingabeaufforderung wird angezeigt:

```
Operational Code Date: Thu Jun 8 12:51:44 2006 (Datum des ausführbaren Codes: Do 8 Jun 12:51:44 2006)

Uncompressing..... (Dekomprimieren läuft)

50% 100%

||||||||||||||||||||||||||||||||||||||||||||||||||

1 File: (1 Datei:) bootos.c Line: (Zeile:) 462 Task: (Aufgabe:) ffffe00 EC: 2863311530 (0xaaaaaaaa)

(0 d 0 hrs 0 min 13 sec)

Timebase: (Zeitbasis) 24,750275 MHz, MEM: 99,001100 MHz, PCI: 33,000366 MHz, CPU: 198,002200 MHz

PCI device BCM5675_A0 attached as unit 0. (PCI-Gerät BCM5675_A0 verbunden als Einheit 0.)

PCI device BCM5695_B0 attached as unit 1. (PCI-Gerät BCM5695_B0 verbunden als Einheit 2.)

PCI device BCM5695_B0 attached as unit 2. (PCI-Gerät BCM5695_B0 verbunden als Einheit 2.)

PCI device BCM5673_A1 attached as unit 3. (PCI-Gerät BCM5673_A1 verbunden als Einheit 4.)

PCI device BCM5673_A1 attached as unit 4. (PCI-Gerät BCM5673_A1 verbunden als Einheit 4.)

Adding BCM transport pointers (BCM-Transportzeiger werden hinzugefügt)

Configuring CPUTRANS TX (CPUTRANS TX wird konfiguriert)

Configuring CPUTRANS RX (CPUTRANS RX wird konfiguriert)

st_state(0) = 0x0

st_state(1) = 0x3

st_state(2) = 0x2
```

Baudrate ändern

Verwenden Sie Option **2**, um die Baudrate der seriellen Schnittstelle zu ändern.

So ändern Sie die Baudrate aus dem Menü **Boot (Systemstart)**:

1. Wählen Sie im Menü **Boot (Systemstart)** die Option **2,** und drücken Sie die <Eingabetaste>.

   Die folgende Eingabeaufforderung wird angezeigt:

   ```
   [Boot Menu]2

   Select baud rate: (Baudrate wählen:)

   1 - 1200

   2 - 2400

   3 - 4800

   4 - 9600

   5 - 19200

   6 - 38400

   7 - 57600

   8 - 115200

   0 - no change (keine Änderung)
   ```

ANMERKUNG: Die gewählte Baudrate wird sofort aktiviert.

2. Der Startvorgang wird fortgesetzt.

Ereignisprotokoll über XMODEM abrufen

Verwenden Sie Option 3, um das Ereignisprotokoll abzurufen und es in Ihr ASCII-Terminal herunterzuladen.

So rufen Sie das Ereignisprotokoll aus dem Menü **Boot (Systemstart) ab**:

1. Wählen Sie im Menü **Boot (Systemstart)** die Option **3**, und drücken Sie die <Eingabetaste>.

   Die folgende Eingabeaufforderung wird angezeigt:

   ```
   [Boot Menu] 3

   Sending event log, start XMODEM receive..... (Ereignisprotokoll wird gesendet, XMODEM-Empfang wird gestartet ...)

   File asciilog.bin Ready to SEND in binary mode (Datei asciilog.bin zum Senden im Binärmodus bereit)

   Estimated File Size 169K, 1345 Sectors, 172032 Bytes (Geschätzte Dateigröße 169 K, 1345 Sektoren, 172032 Bytes)

   Estimated transmission time 3 minutes 20 seconds (Geschätzte Übertragungsdauer 3 Minuten 20 Sekunden)

   Send several Control-X characters to cancel before transfer starts. (Senden Sie mehrere Control-X-Zeichen zum Abbrechen vor dem Start der Übertragung.)
   ```

2. Der Startvorgang wird fortgesetzt.

Neuen ausführbaren Code über XMODEM laden

Verwenden Sie Option 4, wenn eine neue Softwareversion heruntergeladen muss, um defekte Dateien zu ersetzen oder die Systemsoftware zu aktualisieren bzw. zu erweitern.

So laden Sie Software über das Menü **Boot (Systemstart) herunter**:

1. Wählen Sie im Menü **Boot (Systemstart)** die Option **4**, und drücken Sie die <Eingabetaste>.

   Die folgende Eingabeaufforderung wird angezeigt:

   ```
   [Boot Menu] 4

   Ready to receive the file with XMODEM/CRC.... (Bereit für den Empfang der Datei über XMODEM/CRC ...)

   Ready to RECEIVE File xcode.bin in binary mode (Bereit zum Empfang der Datei xcode.bin im Binärmodus)

   Send several Control-X characters to cancel before transfer starts. (Senden Sie mehrere Control-X-Zeichen zum Abbrechen vor dem Start der Übertragung.)
   ```

2. Klicken Sie bei Einsatz von HyperTerminal in der **HyperTerminal**-Menüleiste auf **Übertragung**.

3. Klicken Sie im Menü **Übertragung** auf **Datei senden**.

   Das Fenster **Datei senden** wird angezeigt.

4. Geben Sie den Dateipfad für die herunterzuladende Datei ein.

5. Achten Sie darauf, dass das Protokoll Xmodem angegeben ist.

6. Klicken Sie auf **Senden**.

   Die Software wird heruntergeladen. Der Software-Download dauert mehrere Minuten. Die Terminalemulationsanwendung, z. B. HyperTerminal, zeigt möglicherweise den Fortschritt des Ladevorgangs an.

Kritische Produktdaten für ausführbaren Code anzeigen

Verwenden Sie Option 5, um Informationen zum Boot-Image anzuzeigen.

So zeigen Sie Boot-Image-Informationen aus dem Menü **Boot (Systemstart) an**:

1. Wählen Sie im Menü **Boot (Systemstart)** die Option **5**, und drücken Sie die <Eingabetaste>.

   Die folgende Eingabeaufforderung wird angezeigt:

   ```
   [Boot Menu]5

   The following image is in the Flash File System: (Das folgende Image befindet sich im Flash-Dateisystem:)

   File Name (Dateiname).....image1

   CRC.....0xb017 (45079)

   Target Device (Ziellaufwerk).....0x00508541

   Size (Größe).....0x8ec50c (9356556)

   Number of Components (Anzahl Komponenten).....2

   Operational Code Size (Größe des ausführbaren Codes).....0x7ec048 (8306760)

   Operational Code Offset (Offset für ausführbaren Code).....0x74 (116)

   Operational Code FLASH flag (FLASH-Flag für ausführbaren Code).....1

   Operational Code CRC (CRC für ausführbaren Code).....0x9B4D

   Boot Code Version (Startcode-Version).....1

   Boot Code Size (Startcodegröße).....0x100000 (1048576)

   Boot Code Offset (Startcode-Offset).....0x7ec0bc (8306876)

   Boot Code FLASH flag (FLASH-Flag für Startcode.....0

   Boot Code CRC (Startcode-CRC).....0x1CB8

   VPD - rel 0 ver 31 maint_lvl 0

   Timestamp - Thu Jun 8 12:51:44 2006 (Zeitmarke - Do 8 Jun 8 12:51:44 2006)

   File (Datei) - pc62xxr0v31.stk
   ```

2. Der Startvorgang wird fortgesetzt.

Flash-Diagnose ausführen

Verwenden Sie Option **6**, um die FLASH-Diagnose auszuführen. Die Benutzeraktion muss durch Beantworten einer Ja/Nein- (Y/N) Frage bestätigt werden, bevor der Befehl ausgeführt wird.

So führen Sie einen kompletten Test des FLASH-Speichers aus dem Menü **Boot (Systemstart) durch**:

1. Wählen Sie im Menü **Boot (Systemstart)** die Option **6**, und drücken Sie die <Eingabetaste>.

Die folgende Eingabeaufforderung wird angezeigt:

```
[Boot Menu]6

Do you wish to run flash diagnostics? (Möchten Sie die Flash-Diagnose ausführen?) (Boot code region will not be tested.) (Der Startcode-
Bereich wird nicht geprüft.) (y/n): y

Input number of diagnostic iterations (Input-Nummer diagnostischer Wiederholungen) -> 1

Testing 2 x 28F128J3 base (Test für 2 x 28F128J3-Basis): 0xfe000000

Iterations remaining (Verbleibende Wiederholungen) = 1

Erasing sector 0 (Sektor 6 wird gelöscht)

Verify sector 0 erased (Löschen von Sektor 6 bestätigt)

Writing sector 0 (Sektor 6 wird beschrieben)

Erasing sector 1 (Sektor 6 wird gelöscht)

Verify sector 1 erased (Löschen von Sektor 6 bestätigt)

Writing sector 1 (Sektor 6 wird beschrieben)

Erasing sector 2 (Sektor 6 wird gelöscht)

Verify sector 2 erased (Löschen von Sektor 6 bestätigt)

Writing sector 2 (Sektor 6 wird beschrieben)

Erasing sector 3 (Sektor 6 wird gelöscht)

Verify sector 3 erased (Löschen von Sektor 6 bestätigt)

Writing sector 3 (Sektor 6 wird beschrieben)

Erasing sector 4 (Sektor 6 wird gelöscht)

Verify sector 4 erased (Löschen von Sektor 6 bestätigt)

Writing sector 4 (Sektor 6 wird beschrieben)

Erasing sector 5 (Sektor 6 wird gelöscht)

Verify sector 5 erased (Löschen von Sektor 6 bestätigt)

Writing sector 5 (Sektor 6 wird beschrieben)

Erasing sector 6 (Sektor 6 wird gelöscht)

Verify sector 6 erased (Löschen von Sektor 6 bestätigt)

Writing sector 6 (Sektor 6 wird beschrieben)
```

ANMERKUNG: Dieser Vorgang wird so lange durchgeführt, bis alle Sektoren gelöscht, als gelöscht bestätigt und beschrieben wurden.

```
Flash Diagnostics passed (Flash-Diagnose bestanden)

[Boot Menu]
```

2. Der Startvorgang wird fortgesetzt.

Startcode aktualisieren

Verwenden Sie Option **7**, um den Startcode im FLASH-Speicher zu aktualisieren. Diese Option ist nur verfügbar, nachdem der neue Startcode mithilfe der Boot-Menü-Option 4 geladen wurde. Die Benutzeraktion muss durch Beantworten einer Ja/Nein- (Y/N) Frage bestätigt werden, bevor der Befehl ausgeführt wird.

So laden Sie Software über das Menü **Boot (Systemstart) herunter**:

1. Wählen Sie im Menü **Boot (Systemstart)** die Option **7**, und drücken Sie die <Eingabetaste>.

   Die folgende Eingabeaufforderung wird angezeigt:

```
Do you wish to update Boot Code? (Möchten Sie den Startcode aktualisieren?) (y/n) y

Erasing Boot Flash.....Done. (Start-Flash wird gelöscht ... fertig.)
```

```
Wrote 0x10000 bytes. (0x10000 Bytes geschrieben.)

Wrote 0x20000 bytes. (0x20000 Bytes geschrieben.)

Wrote 0x30000 bytes. (0x30000 Bytes geschrieben.)

Wrote 0x40000 bytes. (0x40000 Bytes geschrieben.)

Wrote 0x50000 bytes. (0x50000 Bytes geschrieben.)

Wrote 0x60000 bytes. (0x60000 Bytes geschrieben.)

Boot code updated (Der Startcode wurde aktualisiert.)
```

2. Der Startvorgang wird fortgesetzt.

Sicherungs-Image löschen

Verwenden Sie Option 8, um das Sicherungs-Image aus dem FLASH-Speicher zu löschen. Die Benutzeraktion muss durch Beantworten einer Ja/Nein- (Y/N) Frage bestätigt werden, bevor der Befehl ausgeführt wird.

So löschen Sie das Sicherungs-Image über das Menü **Boot (Systemstart)**:

1. Wählen Sie im Menü **Boot (Systemstart)** die Option **8**, und drücken Sie die <Eingabetaste>.

   Die folgende Eingabeaufforderung wird angezeigt:

   ```
   Are you SURE you want to delete backup image : (Sind Sie SICHER, dass Sie das folgende Sicherungs-Image löschen möchten?) image2 ? (y/n)
   y

   Backup image deleted... (Das Sicherungs-Image wird gelöscht ...)

   [Boot Menu]
   ```

2. Der Startvorgang wird fortgesetzt.

Das System zurücksetzen

Verwenden Sie Option 9, um sämtlichen FLASH-Speicher zu löschen und das System auf die Standardeinstellungen zurückzusetzen. Die Benutzeraktion muss durch Beantworten einer Ja/Nein- (Y/N) Frage bestätigt werden, bevor der Befehl ausgeführt wird.

So setzen Sie das System über das Menü **Boot (Systemstart) zurück**:

1. Wählen Sie im Menü **Boot (Systemstart)** die Option **9**, und drücken Sie die <Eingabetaste>.

   Die folgende Eingabeaufforderung wird angezeigt:

   ```
   [Boot Menu] 9

   Are you SURE you want to reset the system? (Sind Sie SICHER, dass Sie das System zurücksetzen möchten?) (y/n) y
   ```

2. Das Hochfahren des Systems beginnt von neuem.

Konfiguration mit werksseitigen Standardeinstellungen wiederherstellen (Konfigurationsdateien löschen)

Verwenden Sie Option **10**, um die Standardkonfiguration des Systems zu laden und das System zu starten, ohne die aktuelle Startkonfiguration zu nutzen. Über die Wahl von Option **10** aus dem Boot-Menü werden die Standardeinstellungen des Systems wiederhergestellt. Die Startsequenz kann dann durch Wählen von Option **1** aus dem Boot-Menü angestoßen werden.

So laden Sie Software über das Menü **Boot (Systemstart) herunter**:

1. Wählen Sie im Menü **Boot (Systemstart)** die Option **10**, und drücken Sie die <Eingabetaste>.

   Die folgende Eingabeaufforderung wird angezeigt:

   ```
   Are you SURE you want to delete the configuration? (Sind Sie SICHER, dass Sie die Konfiguration löschen möchten?) (y/n) y
   ```

2. Der Startvorgang wird fortgesetzt.

Sicherungs-Image aktivieren

Verwenden Sie Option 11, um das Sicherungs-Image zu aktivieren. Das aktive Image wird zum Sicherungs-Image, wenn diese Option gewählt wird.

So aktivieren Sie das Sicherungs-Image:

1. Wählen Sie im Menü **Boot** (Systemstart) die Option **11**, und drücken Sie die <Eingabetaste>.

   Die folgende Meldung wird angezeigt:

   ```
   Backup image - image2 activated. (Sicherungs-Image - image2 aktiviert.)
   ```

2. Der Startvorgang wird fortgesetzt.

Verfahren zur Kennwort-Wiederherstellung

Verwenden Sie Option 12, wenn ein Kennwort verloren gegangen ist. Damit kann der Switch einmal gestartet werden, ohne dass nach einem Konsolenkennwort gefragt wird. Beachten Sie, dass das Kennwort zum *Aktivieren* in diesem Modus ebenfalls nicht abgefragt wird.

So stellen Sie ein verloren gegangenes Kennwort wieder her (nur bei Zugriff auf das lokale Terminal):

1. Wählen Sie im Menü **Boot** (Systemstart) die Option **12**, und drücken Sie die <Eingabetaste>.

   Das Kennwort wird gelöscht.

2. Der Startvorgang wird fortgesetzt.

3. Um die Sicherheit des Switch sicherzustellen, müssen die Kennwörter für alle relevanten Management-Verfahren neu konfiguriert werden.

Beispiel eines Konfigurationsverfahrens

Dieser Abschnitt enthält die grundlegenden Schritte, die für den Aufbau einer Verbindung für das Remote-Netzwerk-Management mit dem Switch erforderlich sind. Die diversen verfügbaren Konfigurationen des Switch oder die entsprechenden Befehle werden hingegen nicht erläutert.

In diesem Abschnitt wird auch der erstmalige Zugriff auf einen Switch mit der Standardkonfiguration und den Standardeinstellungen beschrieben. Falls eine zuvor eingegebene Konfiguration Probleme verursacht, sollte die Start-Konfigurationsdatei – d. h. die Konfiguration des Switch beim Einschalten – gelöscht und der Switch neu gestartet werden. Siehe "Standardeinstellungen von Geräten".

Voraussetzungen für das Switch-Setup

Die folgenden Komponenten sind für die Zwecke dieses Beispiels erforderlich:

- Switch der PowerConnect 6200-Reihe
- Eine Workstation mit den folgenden installierten Komponenten:
  - Netzwerkadapterkarte
  - ASCII-Terminalanwendung (zum Beispiel Microsoft® Windows® HyperTerminal oder Procomm Plus™ Terminal)
  - Browser-Anwendung
- Nullmodem-F2F-Kabel
- Durchgehende(s) oder gekreuzte(s) UTP-Kabel (Kategorie 5)

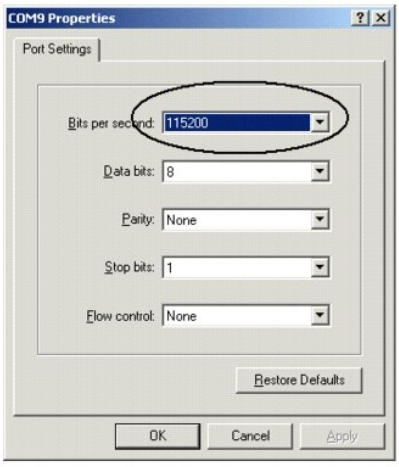
Erste Verbindung

1. Verbinden Sie den Switch über den RS-232-Anschluss mit der Workstation.

2. Konfigurieren Sie das ASCII-Terminal mit den folgenden Einstellungen, und wählen Sie den entsprechenden COM-Port.

   Im Beispiel-Bildschirm wird HyperTerminal verwendet.

Abbildung 5-3. Eigenschaften-Fenster von HyperTerminal



ANMERKUNG: 9600 ist die Standard-Baudrate für einen neuen Switch. Der Switch kann eine andere Baudrate aufweisen. Wenn bei Verwendung der Standard-Baudrate nicht das Switch-Terminal angezeigt wird, versuchen Sie es mit einer anderen Baudrate.

3. Verwenden Sie ein F2F-Nullmodemkabel zur Verbindung der Workstation mit dem Switch.

ANMERKUNG: Wenn Sie einen *Stack* konfigurieren, verbinden Sie die Workstation mit dem Master-Switch.

4. Schließen Sie das Netzkabel des Switch an, und schalten Sie den Switch ein. Das System beginnt mit dem Startvorgang. Bei folgender Anzeige können Sie das Menü **Boot (Systemstart) aufrufen, indem Sie ggf. Option 2** wählen, um spezielle Verfahren durchzuführen.

```
Select an option. (Wählen Sie eine Option.) If no selection in 10 seconds then operational code will start. (Wenn Sie innerhalb von 10 Sekunden keine Auswahl treffen, wird ausführbarer Code gestartet.)

1 - Start operational code. (Ausführbaren Code starten.)

2 - Start Boot Menu. (Boot-Menü starten).

Select (1, 2):2 (Auswahl)
```

Wenn Sie nicht das Menü **Boot** (Systemstart) aufrufen, setzt das System den Betrieb fort, indem es den Code in das RAM dekomprimiert. Der Code wird aus dem RAM ausgeführt und die Liste der verfügbaren Port-Nummern und deren Status (in Betrieb/außer Betrieb) wird angezeigt.

ANMERKUNG: Der folgende Bildschirm entspricht einer Beispielkonfiguration. Adressen, Versionen und Datumsangaben können je nach Switch variieren.

```
current volume configuration: (Konfiguration des aktuellen Datenträgers:)

- volume label: NO LABEL ; (in boot sector: ((Volume-Bezeichnung: KEINE BEZEICHNUNG; (in Boot-Sektor)) )

- volume Id: (Volume-ID:) 0x

- total number of sectors: (Gesamtanzahl Sektoren:) 60,716

- bytes per sector: (Bytes pro Sektor:) 512

- # of sectors per cluster: (Anzahl Sektoren pro Cluster:) 4

- # of reserved sectors: (Anzahl reservierter Sektoren:) 1

- FAT entry size: FAT16 (FAT-Eintragsgröße: FAT16)

- # of sectors per FAT copy: (Anzahl Sektoren pro FAT-Kopie:) 60

- # of FAT table copies: (Anzahl FAT-Tabellenkopien:) 2

- # of hidden sectors: (Anzahl versteckter Sektoren:) 4

- first cluster is in sector # 136 (Erster Cluster befindet sich in Sektor Nr. 136)

- Update last access date for open-read-close = FALSE (Letztes Zugriffsdatum für Öffnen-Lesen-Schließen aktualisieren = FALSCH)

- directory structure: VFAT (Verzeichnisstruktur: VFAT

- root dir start sector: Startsektor im Root-Verzeichnis:) 121

- # of sectors per root: (Anzahl Sektoren pro Root:) 15
```

- max # of entries in root: (Max. Anzahl Einträge im Root:) 240

FAT handler information: (FAT-Handler-Information:)

- allocation group size: Zuordnungs-Gruppengröße:) 2 clusters (2 Cluster)

- free space on volume: (Freier Speicherplatz auf Volume:) 21.348.352 bytes (21.348.352 Bytes)

Boot Menu Version: 27 Apr 2006

Select an option. (Wählen Sie eine Option.) If no selection in 10 seconds then

operational code will start. (Wenn Sie innerhalb von 10 Sekunden keine Auswahl treffen, wird ausführbarer Code gestartet.)

1 - Start operational code. (Ausführbaren Code starten.)

2 - Start Boot Menu. (Boot-Menü starten).

Select (1, 2):1 (Auswahl)

Operational Code Date: Wed May 17 10:54:19 2006 (Datum des ausführbaren Codes: Mi 17 Mai 10:54:19 2006

Uncompressing..... (Dekomprimieren läuft)

50% 100%

||||||||||||||||||||||||||||||||||||||||||||||||||

volume descriptor ptr (pVolDesc): (Volume-Deskriptor-Pointer:) 0xfd7e6c0

cache block I/O descriptor ptr (cbio): (Cacheblock-Deskriptor-Pointer:) 0xfd7fe40

auto disk check on mount: (Automatische Datenträgerprüfung beim Mounten:) NOT ENABLED (Automatische Datenträgerprüfung beim Mounten: NICHT AKTIVIERT

max # of simultaneously open files: (Maximale Anzahl gleichzeitig geöffneter Dateien): 22

file descriptors in use: (Verwendete Dateideskriptoren:) 0

# of different files in use: (Anzahl verschiedener verwendeter Dateien:) 0

# of descriptors for deleted files: (Anzahl Deskriptoren gelöschter Dateien:) 0

# of obsolete descriptors: (Anzahl veralteter Deskriptoren:) 0

current volume configuration: (Konfiguration des aktuellen Datenträgers:)

- volume label: NO LABEL ; (in boot sector: ((Volume-Bezeichnung: KEINE BEZEICHNUNG; (in Boot-Sektor)))

- volume Id: (Volume-ID:) 0x

- total number of sectors: (Gesamtanzahl Sektoren:) 60,716

- bytes per sector: (Bytes pro Sektor:) 512

- # of sectors per cluster: (Anzahl Sektoren pro Cluster:) 4

- # of reserved sectors: (Anzahl reservierter Sektoren:) 1

- FAT entry size: FAT16 (FAT-Eintragsgröße: FAT16

- # of sectors per FAT copy: (Anzahl Sektoren pro FAT-Kopie:) 60

- # of FAT table copies: (Anzahl FAT-Tabellenkopien:) 2

- # of hidden sectors: (Anzahl versteckter Sektoren:) 4

- first cluster is in sector # 136 (Erster Cluster befindet sich in Sektor Nr. 136)

- Update last access date for open-read-close = FALSE (Letztes Zugriffsdatum für Öffnen-Lesen-Schließen aktualisieren = FALSCH)

- directory structure: VFAT (Verzeichnisstruktur: VFAT)

- root dir start sector: Startsektor im Root-Verzeichnis:) 121

- # of sectors per root: (Anzahl Sektoren pro Root:) 15

- max # of entries in root: (Max. Anzahl Einträge im Root:) 240

FAT handler information: (FAT-Handler-Information:)

```
------------------------

- allocation group size: Zuordnungs-Gruppengröße:) 2 clusters (2 Cluster)

- free space on volume: (Freier Speicherplatz auf Volume:) 21.350.400 bytes (21.348.352 Bytes)

File (Datei:): unitmgr.c, Line: 3419, Error 0 (0x0) (unitmgr.c, Zeile: 3419, Fehler 0 (0x0))

Timebase: (Zeitbasis) 66,666666 MHz, MEM: 266,666664 MHz, PCI: 66,666666 MHz, CPU: 533,333328 MHz

SOC unit 0 attached to PCI device BCM56304_B0 (SOC-Einheit 1 verbunden mit PCI-Gerät BCM56304_B0)

SOC unit 1 attached to PCI device BCM56304_B0 (SOC-Einheit 1 verbunden mit PCI-Gerät BCM56304_B0)

Adding BCM transport pointers (BCM-Transportzeiger werden hinzugefügt)

Configuring CPUTRANS TX (CPUTRANS TX wird konfiguriert)

Configuring CPUTRANS RX (CPUTRANS RX wird konfiguriert)

hpc - No stack ports. (Keine Stack-Ports.) Starting in stand-alone mode. (Start im Standalone-Modus.)

(Unit 1 - Waiting to select management unit)> ((Einheit 1 - Warten auf Auswahl der Verwaltungseinheit)>)
```

Standardeinstellungen von Geräten

Um zu den Standardeinstellungen eines Geräts zurückzukehren, verwenden Sie den Befehl `delete startup-config` an der Eingabeaufforderung des privilegierten Modus (#), und starten Sie das Gerät neu. Wenn das Gerät neu geladen wird, wird es mit den Standardeinstellungen konfiguriert.

```
console>

console>enable

console#delete startup-config

Startup file was deleted (Start-Datei wurde gelöscht)

console#reload

Management switch has unsaved changes. (Nicht gespeicherte Änderungen im Management-Switch.)

Are you sure you want to continue? (Möchten Sie den Vorgang fortsetzen?) (y/n) y

Configuration Not Saved! (Konfiguration nicht gespeichert!)

Are you sure you want to start? (Möchten Sie den Stack neu laden?) (y/n) y

Reloading all switches.. (Alle Switches werden neu geladen)
```

Aktivieren der Remote-Verwaltung

1. Geben Sie den Befehl **enable** (Aktivieren) an der Konsole ein, um wie folgt in den privilegierten EXEC-Bildschirm-Modus zu wechseln:

   ```
   console>enable

   console#
   ```

2. Verbinden Sie die Management-Station (PC) über einen der Ethernet-Ports mit dem Switch oder mithilfe eines CAT5-Kabels über ein Netzwerk, das mit dem Switch verbunden ist.

   Bei diesem Beispiel wird Port **1/g1** verwendet.

3. Achten Sie darauf (auf dem ASCII-Terminal), dass sich der Schnittstellenstatus auf "In Betrieb" geändert hat und dass der STP-Status auf "Forwarding" (Weiterleiten) (nach 30 Sekunden) gesetzt ist, wie unten dargestellt:

   ```
   console#

   01-Jan-2000 01:43:03 %LINK-I-Up: Vlan 1

   01-Jan-2000 01:43:03 %LINK-I-Up: 1/g1

   01-Jan-2000 01:43:34 %STP-I-PORTSTATUS: Port 1/g1: STP status Forwarding
   ```

4. Geben Sie den Befehl **config** (Konfigurieren) an der Konsole ein, um wie folgt in den privilegierten EXEC-Bildschirm-Modus zu wechseln:

```
console#config
```

5. Verwenden Sie den folgenden Befehl, um die IP-Adresse auf DHCP zu setzen:

```
console(config)#ip address dhcp
```

6. Verwenden Sie den folgenden Befehl, um das Standard-Gateway einzustellen:

```
console(config)#ip default-gateway 10.254.24.162
```

7. Wenn die Management-Station zu einem Remote-Netzwerk gehört und nicht direkt mit der Schnittstelle verbunden ist, konfigurieren Sie eine statische Route.

   Die konfigurierte IP-Adresse muss demselben Subnetz wie eine der IP-Schnittstellen des Switch angehören. In diesem Beispiel ist die statische Adresse 192.168.20.100.

```
console(config)#ip route 192.168.10.10 255.255.255.0 192.168.20.1 200
```

8. Senden Sie einen Ping-Befehl vom Switch an die Management-Station, um sicherzugehen, dass eine Verbindung besteht.

   Warten Sie 30 Sekunden, bis der Port im STP-Weiterleitungsmodus ist, bevor Sie den Ping-Befehl an die Management-Station senden. In diesem Beispiel ist die IP der Management-Station 50.1.1.2.

```
console>ping 50.1.1.2

64 bytes from 50.1.1.2: icmp_seq=1. time=0 ms

64 bytes from 50.1.1.2: icmp_seq=2. time=0 ms

64 bytes from 50.1.1.2: icmp_seq=3. time=0 ms

64 bytes from 50.1.1.2: icmp_seq=4. time=0 ms

----50.1.1.2 PING Statistics----

4 packets transmitted, 4 packets received, 0% packet loss (4 Pakete übertragen, 4 Pakete empfangen, 0 % Paketverluste)

round-trip (ms) min/avg/max = 0/0/0
```

9. Legen Sie einen Benutzernamen und ein Kennwort fest, um den Zugriff auf den Switch mit Berechtigungsstufe 15 für einen Remote-Benutzer einzuräumen (HTTP und HTTPS).

   In diesem Beispiel ist der Benutzername **Dell**, das Kennwort lautet **Dell1234** und die Berechtigungsstufe ist 15. Die Berechtigungsstufen reichen von 1–15, wobei 15 die höchste Stufe ist. Berechtigungsstufe 15 ist die einzige Stufe, die Zugriff über die Webschnittstelle ermöglicht.

```
console#config

console(config)#username Dell password Dell1234 level 15

console(config)#ip http authentication local

console(config)#ip https authentication local

console(config)#crypto certificate generate key_generate

Generating RSA private key, 1024 bit long modulus

console(config)#ip https server
```

10. Legen Sie einen Benutzernamen und ein Kennwort für die Zugriffsberechtigung eines lokalen Benutzers – zum Beispiel Konsole, Telnet oder Webserver – fest.

    In diesem Beispiel ist der Benutzername **Dell, das Kennwort Dell1234** und die Berechtigungsstufe 15.

```
console(config)#username Dell password Dell1234 level 15

console(config)#aaa authentication login default line

console(config)#aaa authentication enable default line

console(config)#line console

console(config-line)#login authentication default

console(config-line)#enable authentication default

console(config-line)#password tommy123

console(config-line)#exit
```

```
console(config)#line telnet

console(config-line)#login authentication default

console(config-line)#enable authentication default

console(config-line)#password bobby123

console(config-line)#exit

console(config)#line ssh

console(config-line)#login authentication default

console(config-line)#enable authentication default

console(config-line)#password jones123

console(config-line)#exit
```

11. Speichern Sie die Datei **running-config** in die Datei **startup-config**.

    Damit wird sichergestellt, dass die soeben abgeschlossene Konfiguration mit derjenigen identisch ist, die beim Neustart des Switch greift.

    ```
    console(config)#exit

    console#copy running-config startup-config
    ```

Der Switch ist nun konfiguriert und kann über die verschiedenen Optionen wie Telnet, Web-Browser-Schnittstelle und andere verwaltet werden.

Konfigurieren des sicheren Management-Zugriffs (HTTPS)

Wenn der Switch sicher über den Standard-Web-Browser verwaltet wird, wird das Sicherheitsprotokoll SSL (Secure Socket Layer) verwendet.

Führen Sie folgende Schritte durch, um den Switch sicher über den Standard-Web-Browser zu verwalten:

1. Um dem Switch die Verbindungsaufnahme mit einem HTTPS-Server zu gestatten und einen Sicherheitsschlüssel zu erstellen, verwenden Sie die Befehle **ip https server** und **crypto certificate 1 generate** (Schlüsselzertifikat 1 erzeugen):

   ```
   console#configure

   console(config)#crypto certificate 1 generate

   Generating RSA private key, 1024 bit long modulus

   console(config)#ip https server

   console(config)#
   ```

2. Konfigurieren Sie die Management-Station auf die gleiche Weise wie für eine reguläre HTTP-Verbindung.

3. Verbinden Sie den Switch per HTTPS, indem Sie die Adresse `https:// IP-Adresse des Geräts` im Browser-Fenster eingeben (*https* muss eingegeben werden).

   Das Fenster **Security Alert** (Sicherheitswarnung) wird angezeigt.

4. Klicken Sie auf **Yes** (Ja), um die Sicherheitszertifizierung zu akzeptieren (falls sie nicht von einer dritten Partei authentifiziert wird).

   Der **Login Screen** (Anmeldebildschirm) wird angezeigt.

5. Geben Sie den zugewiesenen Benutzernamen und das Kennwort ein.

   Dell OpenManage™ Switch Administrator wird angezeigt.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Wie Sie Hilfe bekommen

Benutzerhandbuch für die Dell™ PowerConnect™ 6200-Reihe

- Anfordern von Unterstützung
- Dell Unternehmensschulungen und Zertifizierungen
- Probleme mit der Bestellung
- Produktinformationen
- Einsenden von Teilen zur Reparatur auf Garantie oder zur Gutschrift
- Bevor Sie anrufen
- Kontaktaufnahme mit Dell

Anfordern von Unterstützung

Wenn ein Problem mit Ihrem Computer auftritt, können Sie die folgenden Schritte durchführen, um es zu diagnostizieren und zu beheben:

1. Füllen Sie die Diagnose-Checkliste aus.
2. Nutzen Sie das umfassende Online-Serviceangebot auf der Dell Support-Website (**support.dell.com**) zur Unterstützung bei der Installation und Fehlerbehebung. Eine ausführliche Liste des Online-Supportangebots von Dell finden Sie unter Online-Dienste.
3. Falls das Problem mithilfe der oben genannten Schritte nicht gelöst werden konnten, sehen Sie unter Kontaktaufnahme mit Dell nach.

ANMERKUNG: Achten Sie darauf, den Dell Support von einem Telefon aus anzurufen, das sich in der Nähe des Computers befindet, damit die Support-Mitarbeiter Sie bei den erforderlichen Schritten unterstützen können.

ANMERKUNG: Der Express-Service von Dell ist möglicherweise nicht in allen Ländern verfügbar.

Geben Sie nach Aufforderung des automatischen Telefonsystems den Express-Service-Code ein, damit Sie direkt mit dem zuständigen Support-Mitarbeiter verbunden werden können. Wenn Sie über keinen Express-Service-Code verfügen, öffnen Sie den Ordner **Dell Accessories** (Dell-Zubehör), doppelklicken Sie auf das Symbol **Express Service Code** und befolgen Sie die weiteren Anweisungen.

Anweisungen zur Inanspruchnahme des Dell Supports finden Sie unter Support-Service.

ANMERKUNG: Einige der nachstehend aufgeführten Dienstleistungen sind nicht in allen Ländern durchgängig verfügbar. Informationen hierzu erhalten Sie von Ihrem Dell-Vertriebsbeauftragten.

Online-Dienste

Informationen zum Produkt- und Serviceangebot von Dell finden Sie auf den folgenden Websites:

www.dell.com

www.dell.com/ap (nur Asien/Pazifik)

www.dell.com/jp (nur Japan)

www.euro.dell.com/ (nur für Europa)

www.dell.com/la (Lateinamerika und Karibik)

www.dell.ca (nur Kanada)

Sie erreichen den Support von Dell über folgende Websites und E-Mail-Adressen:

- Websites des Dell Supports

  support.dell.com

  support.jp.dell.com (nur Japan)

  support.euro.dell.com (nur Europa)

- E-Mail-Adressen des Dell Supports

  mobile_support@us.dell.com

  support@us.dell.com

  la-techsupport@dell.com (nur für Lateinamerika und die Karibik)

  apsupport@dell.com (nur für Asien und den Pazifikraum)

- E-Mail-Adressen des Marketing- und Vertriebsteams von Dell

apmarketing@dell.com (nur für Asien und den Pazifikraum)

sales_canada@dell.com (nur Kanada)

- Anonymes Dateiübertragungsprotokoll (File Transfer Protocol, FTP)

  ftp.dell.com

  Melden Sie sich als Benutzer anonymous (anonym) an, und verwenden Sie Ihre E-Mail-Adresse als Kennwort.

Automatisches Auftragsauskunftsystem

Um den Status eines bestellten Dell-Produktes zu überprüfen, können Sie die Website **support.dell.com** besuchen oder das Automatische Auftragsauskunftssystem anrufen. Eine elektronische Ansage fordert Sie zur Eingabe der Bestelldaten auf; die Bestellung wird aufgerufen und der Stand der Bearbeitung angesagt. Die entsprechende Rufnummer für Ihre Region finden Sie unter So erreichen Sie Dell.

Support-Service

Der Support-Service von Dell steht an sieben Tagen der Woche rund um die Uhr zur Verfügung, um Ihre Fragen zu Dell-Hardware zu beantworten. Unsere Support-Mitarbeiter verwenden computergestützte Diagnoseprogramme, um Fragen schnell und präzise zu beantworten.

Zur Kontaktaufnahme mit dem technischen Support von Dell lesen Sie die Informationen unter Vor dem Anruf und informieren sich dann anhand der Kontaktinformationen für Ihre Region.

Dell Unternehmensschulungen und Zertifizierungen (Dell Enterprise Training and Certification)

Dell bietet Schulungen und Zertifizierungen für Unternehmen an. Weitere Informationen finden Sie unter **www.dell.com/training**. Diese Dienstleistungen stehen unter Umständen nicht an allen Standorten zur Verfügung.

Probleme mit der Bestellung

Sollten sich Probleme mit der Bestellung ergeben (fehlende oder falsche Teile, fehlerhafte Rechnung), so setzen Sie sich mit dem Kundendienst von Dell in Verbindung. Halten Sie beim Anruf Lieferschein oder Packzettel bereit. Die entsprechende Rufnummer für Ihre Region finden Sie unter So erreichen Sie Dell.

Produktinformationen

Wenn Sie Informationen über weitere Produkte von Dell wünschen oder etwas bestellen möchten, besuchen Sie uns im Internet unter **www.dell.com/**. Die Telefonnummer für Ihre Region oder Ihren Verkaufsberater finden Sie unter So erreichen Sie Dell.

Einsenden von Teilen zur Reparatur auf Garantie oder zur Gutschrift

Möchten Sie Artikel zur Reparatur oder Gutschrift zurücksenden, so gehen Sie wie folgt vor:

1. Auf telefonische Anfrage erhalten Sie von Dell eine Rücksendegenehmigungsnummer (Return Material Authorization Number); schreiben Sie diese gut lesbar auf den Versandkarton.

   Die entsprechende Rufnummer für Ihre Region finden Sie unter So erreichen Sie Dell.

2. Legen Sie eine Kopie des Lieferscheins und ein Begleitschreiben bei, in dem Sie den Grund für die Rücksendung erläutern.

3. Legen Sie eine Kopie der Diagnose-Checkliste bei (siehe Diagnose-Checkliste). Diese sollte die durchgeführten Tests und alle Fehlermeldungen der Dell Diagnose aufführen.

4. Für eine Gutschrift müssen die betreffenden Artikel komplett mit Zubehör (wie z. B. Netzstromkabel, Datenträger wie CDs und Disketten sowie Handbücher) eingesandt werden.

5. Schicken Sie die Geräte in der Originalverpackung (oder einer ebenso geeigneten Verpackung) zurück.

Die Versandkosten gehen zu Ihren Lasten. Außerdem sind Sie verantwortlich für die Transportversicherung aller zurückgeschickten Produkte, und Sie tragen das Verlustrisiko für den Versand an Dell. Nachnahmesendungen werden verweigert.

Rücksendungen, die nicht diesen Voraussetzungen entsprechen, werden an Dells Annahmestelle verweigert und an den Absender zurückgeschickt.

Bevor Sie anrufen

ANMERKUNG: Halten Sie den Express-Service-Code bereit. Mit diesem Code werden Sie innerhalb des automatischen Support-Telefonsystems schneller verbunden.

Vergessen Sie nicht, vor dem Anruf bei Dell die Diagnose-Checkliste auszufüllen (siehe Diagnose-Checkliste). Schalten Sie vor dem Anruf bei Dell nach Möglichkeit das System ein, und benutzen Sie ein Telefon in der Nähe des Computers. Während des Anrufs sollten Sie in der Lage sein, einige Befehle einzugeben, detaillierte Informationen während des Betriebs zu nennen oder andere Fehlerbehebungsverfahren auszuprobieren, die nur am Computer durchgeführt werden können. Die Computerdokumentation sollte immer griffbereit sein.

VORSICHT: Bevor Sie Arbeiten im Inneren des Computers ausführen, lesen Sie die Sicherheitshinweise im *Systeminformationshandbuch*.

Diagnose-Checkliste
Name:
Datum:
Adresse:
Telefonnummer:
Service-Kennnummer (Strichcode auf der Rückseite oder Unterseite des Computers):
Express-Servicecode:
Rücksendegenehmigungsnummer (falls von einem Service-Mitarbeiter ausgegeben):
Betriebssystem und Version:
Geräte:
Erweiterungskarten:
Sind Sie an ein Netzwerk angeschlossen? Ja Nein
Netzwerk, Version und Netzwerkadapter:
Programme und Versionen:
Ermitteln Sie mit Hilfe der Dokumentation zum Betriebssystem den Inhalt der Startdateien Ihres Systems. Falls am Computer ein Drucker angeschlossen ist, drucken Sie jede Datei aus. Halten Sie andernfalls den Inhalt aller Dateien schriftlich fest, bevor Sie bei Dell anrufen.
Fehlermeldung, Signaltoncode oder Diagnosecode:
Beschreibung des Problems und der bereits durchgeführten Maßnahmen zur Fehlerbeseitigung:

Kontaktaufnahme mit Dell

Als Kunde in den USA wählen Sie bitte die Telefonnummer 800-WWW.DELL (800.999.3355).

ANMERKUNG: Wenn Sie nicht über eine aktive Internetverbindung verfügen, finden Sie Kontaktinformationen auf Ihrem Kaufbeleg, dem Packzettel, der Rechnung oder im Dell Produktkatalog.

Dell bietet eine Reihe verschiedener Support- und Serviceoptionen online oder über Telefon an. Das Serviceangebot ist abhängig von Land und Produkt. Einige Services sind in Ihrer Region möglicherweise nicht verfügbar. So nehmen Sie Verbindung mit Dell auf, um Fragen des Vertriebs, des technischen Supports oder des Kundendienstes zu erörtern:

1. Besuchen Sie die Website **support.dell.com**.
2. Überprüfen Sie im Dropdown-Menü zur **Regions- und Landesauswahl** am unteren Seitenrand Ihr Land bzw. Ihre Region.
3. Klicken Sie am linken Seitenrand auf **Kontakt**.
4. Klicken Sie auf den Link für den benötigten Service- oder Supporttyp.
5. Wählen Sie das gewünschte Verfahren der Kontaktaufnahme mit Dell.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Verwenden von Dell™ OpenManage™ Switch Administrator

Benutzerhandbuch für die Dell™ PowerConnect™ 6200-Reihe

- Einrichten der IP-Adresse des Switch
- Starten der Anwendung
- Aufbau der Benutzeroberfläche
- Verwenden der Schaltflächen in Switch Administrator
- Definieren von Feldern
- Zugreifen auf den Switch über CLI
- Verwenden von CLI

Einrichten der IP-Adresse des Switch

Die IP-Adresse kann mit zwei Verfahren eingestellt werden: über DHCP oder die statische Zuweisung der Adresse. Informationen zum Starten von CLI finden Sie im Abschnitt Zugreifen auf den Switch über CLI.

Einstellen der IP-Adresse mit DHCP

1. Geben Sie `enable` an der Eingabeaufforderung console> ein, und drücken Sie die <Eingabetaste>.
2. Geben Sie an der Eingabeaufforderung `console# config` ein, und drücken Sie die <Eingabetaste>.
3. Geben Sie `ip address dhcp` ein, und drücken Sie die <Eingabetaste>.
4. Geben Sie `exit` ein.
5. Geben Sie an der Eingabeaufforderung `console#` den Befehl `show ip interface management` ein.

Einrichten einer statischen Adresse

1. Geben Sie `enable` an der Eingabeaufforderung console> ein, und drücken Sie die <Eingabetaste>.
2. Geben Sie an der Eingabeaufforderung `console# config` ein, und drücken Sie die <Eingabetaste>.
3. Geben Sie `ip address none` ein.
4. Geben Sie Folgendes ein, um zum Beispiel die IP-Adresse 10.256.24.64 mit der Netzmaske 255.255.248.0 und dem Gateway 10.256.24.1 zu konfigurieren:
   ```
   ip address 10.256.24.64 255.255.248.0
   ip default-gateway 10.256.24.1
   ```
5. Geben Sie `exit` ein.
6. Geben Sie `show ip interface management` ein.

Starten der Anwendung

1. Öffnen Sie einen Webbrowser.
2. Geben Sie die IP-Adresse des Switch (gemäß Definition in CLI) in die Adresszeile ein, und drücken Sie die <Eingabetaste>.

   Informationen über die Zuweisung einer IP-Adresse zu einem Switch finden Sie unter "Konfigurationsübersicht."
3. Wenn das Fenster **Login** (Anmeldung) erscheint, geben Sie einen Benutzernamen und das Kennwort ein.

   ANMERKUNG: Der Switch ist nicht mit einem Standardkennwort konfiguriert. Sie können den Switch ohne Kennworteingabe konfigurieren, wenn Sie über die Konsolenschnittstelle auf die CLI zugreifen. Kennwörter sind alphanumerisch, und es wird zwischen Groß- und Kleinschreibung unterschieden. Informationen zum Wiederherstellen eines verloren gegangenen Kennworts finden Sie unter "Verfahren zur Kennwort-Wiederherstellung".

4. Klicken Sie auf **OK**.

5. Die Startseite von **Dell OpenManage Switch Administrator** wird angezeigt.

Aufbau der Benutzeroberfläche

Die Startseite (siehe Abbildung 3-1) enthält die folgenden Ansichten:

- **Strukturansicht** – Sie befindet sich links auf der Startseite und bietet eine erweiterbare Ansicht der Merkmale und ihrer Komponenten.
- **Geräteansicht** – Sie befindet sich rechts auf der Startseite und wird u. a. für die Anzeige einer Geräteansicht, eines Informations- oder Tabellenbereichs und/oder von Konfigurationsanleitungen verwendet.

Abbildung 3-1. Komponenten von Switch Administrator

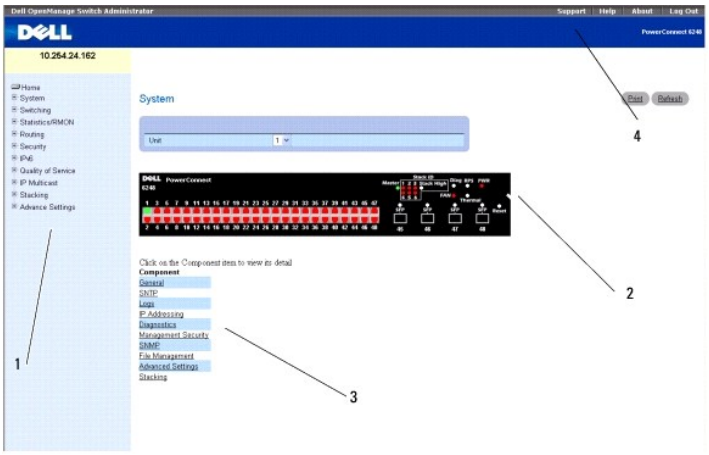


Tabelle 3-1 enthält die Schnittstellenkomponenten mit den entsprechenden Nummern.

Tabelle 3-1. Schnittstellenkomponenten

Komponente	Name
1	Die Strukturansicht enthält eine Liste der diversen Gerätefunktionen. Die Verzweigungen der Strukturansicht können eingeblendet werden, um alle Komponenten unterhalb einer bestimmten Funktion anzuzeigen, bzw. ausgeblendet werden, um die Funktionskomponenten zu verbergen. Indem Sie die vertikale Leiste nach rechts ziehen, können Sie den Strukturbereich so erweitern, dass der volle Name einer Komponente angezeigt wird.
2	Die Geräteansicht enthält Informationen zu den Geräte-Ports, die aktuelle Konfiguration und den Status sowie Tabelleninformationen und Funktionskomponenten. An der Farbgebung der Ports ist erkennbar, ob ein Port derzeit aktiv ist. Grün zeigt an, dass der Port aktiviert ist, Rot, dass auf dem Port ein Fehler aufgetreten ist, und Blau, dass die Verbindung deaktiviert wurde. **ANMERKUNG:** Der Status der LEDs wird in der Geräteansicht nicht angezeigt. Sie können den LED-Status nur durch Blick auf den realen Switch feststellen. Informationen zu den LEDs finden Sie unter "LED-Definitionen". Je nach ausgewählter Option erscheinen im unteren Bereich der Geräteansicht andere Geräteinformationen und/oder Dialogfelder zum Konfigurieren von Parametern.
3	Die Komponentenliste enthält eine Liste mit Funktionskomponenten. Komponenten können auch durch Erweiterung einer Funktion in der Strukturansicht eingesehen werden.
4	Über die Informationsschaltflächen kann man Informationen zum Switch abrufen und auf den Dell-Support zugreifen. Weitere Informationen finden Sie unter "Informationsschaltflächen."

Verwenden der Schaltflächen in Switch Administrator

Informationsschaltflächen

Tabelle 3-2. Informationsschaltflächen

Schaltfläche	Beschreibung
Support	Öffnet die Dell-Support-Website **support.dell.com**.
Help (Hilfe)	Onlinehilfe mit Informationen zum Konfigurieren und Verwalten des Switch. Die Seiten der Onlinehilfe sind kontextsensitiv. Ist beispielsweise die Seite **IP Addressing** (IP-Adressierung) geöffnet, wird das entsprechende Hilfethema angezeigt, sobald man auf **Help** (Hilfe) klickt.
About (Info)	**Enthält die Versions- und Build-Nummer sowie Informationen zum Dell C**opyright.
Log Out (Abmelden)	Führt die Abmeldung von der Anwendung durch.

Schaltflächen für die Geräteverwaltung

Tabelle 3-3. Schaltflächen für die Geräteverwaltung

Schaltfläche	Beschreibung
Apply Changes (Änderungen übernehmen)	Übernimmt die vorgenommenen Änderungen für das Gerät.
Add (Hinzufügen)	Ermöglicht die Eingabe von Information in Tabellen oder Dialogen.
Telnet	Startet eine Telnet-Sitzung.
Query (Abfrage)	Führt Tabellenabfragen durch.
Show All (Alle anzeigen)	Zeigt die Gerätetabellen an.
Linkspfeil/Rechtspfeil	Verschiebt Informationen zwischen Listen.
Refresh (Aktualisieren)	Aktualisiert Geräteinformationen.
Reset All Counters (Alle Zähler zurücksetzen)	Setzt die Statistikzähler zurück.
Print (Drucken)	Druckt die Seite **Network Management System** (Netzwerk-Management-System) und/oder Tabelleninformationen.
Draw (Zeichnen)	Erstellt Ad-hoc-Statistiken in Diagrammform.

Kontrollkästchen

Tabelle 3-4. Kontrollkästchen

Typ des Kontrollkästchens	Beschreibung
Add (Hinzufügen)	Hyperlink, der Sie zu einer Konfigurationsseite bringt.
Remove (Entfernen)	Entfernt das gewählte Element.
Allgemeine Auswahl	Zur Aktivierung eines Konfigurationselements, d. h., zum Anpassen der Sensitivität von Protokolldateien, Auswählen von Vergleichskriterien für Diffserv, Auswählen von ACL-Regelparametern.

Definieren von Feldern

Benutzerdefinierte Felder können 1–159 Zeichen enthalten, es sei denn, auf der Webseite Dell OpenManage Switch Administrator ist etwas anderes angegeben.

Alle Zeichen mit Ausnahme der folgenden dürfen verwendet werden:

- \
- /
- :
- *
- ?
- <
- >
- |

Zugreifen auf den Switch über CLI

Der Switch kann über eine direkte Verbindung zum Konsolen-Port oder über eine Telnet-Verbindung verwaltet werden.

ANMERKUNG: Achten Sie beim Verwalten eines Stack darauf, dass das serielle Schnittstellenkabel am Master-Switch des Stack angeschlossen wird.

Die Verwendung von CLI ist mit der Eingabe von Befehlen in einem Linux-System vergleichbar. Beim Zugriff über eine Telnet-Verbindung sollten Sie sicherstellen, dass eine IP-Adresse für das Gerät definiert wurde und dass die für den Gerätezugriff verwendete Workstation bereits vor Verwendung der CLI-Befehle mit dem Gerät verbunden ist.

Informationen zum Konfigurieren einer ersten IP-Adresse finden Sie unter "Konfigurationsübersicht".

Konsolenverbindung

1. Schalten Sie den Switch (oder Stack) ein, und warten Sie, bis der Startvorgang abgeschlossen ist.

   ANMERKUNG: Wenn Sie einen Switch-*Stack* installieren , verbinden Sie das Terminal mit dem Master-Switch. Bei diesem Switch leuchtet die Master-Switch-LED. Beim ersten Einschalten eines Stacks wird der Master-Switch bestimmt, der sich an beliebiger Position im Stack befinden kann. Wenn Sie das Terminal mit einem untergeordneten Switch verbinden, können Sie CLI über die serielle Schnittstelle dieses Switch nicht verwenden.

2. Wenn der Administrator kein Verfahren zur Anmeldeauthentifizierung konfiguriert hat, wird die Eingabeaufforderung `console>` beim Starten des Switch angezeigt. Andernfalls wird dem Benutzer die Eingabeaufforderung `User:` login (Benutzeranmeldung) angezeigt.

   ANMERKUNG: Die nachstehend beschriebenen Schritte setzen voraus, dass der Benutzer "Admin" mit zugehörigem Kennwort auf dem System konfiguriert ist.

3. Geben Sie an der Eingabeaufforderung `admin` ein, und drücken Sie die <Eingabetaste>.

   Jetzt wird die Eingabeaufforderung `Password:` (Kennwort:) angezeigt.

4. Geben Sie das Kennwort ein. Es wird auf dem Bildschirm durch Sternchen (*) repräsentiert.

   Jetzt wird die Eingabeaufforderung `console#` angezeigt.

5. Konfigurieren Sie das Gerät, und geben Sie die erforderlichen Befehle ein, um die gewünschten Vorgänge auszuführen.

6. Wenn Sie fertig sind, beenden Sie die Sitzung mit dem Befehl **`quit`** oder **`exit`**.

Telnet-Verbindung

Telnet ist ein TCP/IP-Protokoll für die Terminalemulation. ASCII-Terminals können über ein Netzwerk mit TCP/IP-Protokoll virtuell mit dem lokalen Gerät verbunden werden. Telnet stellt eine Alternative zur Anmeldung am lokalen Terminal dar, wenn eine Remote-Anmeldung erforderlich ist.

Ihr Switch unterstützt bis zu vier Telnet-Sitzungen gleichzeitig. In einer Telnet-Sitzung können sämtliche CLI-Befehle verwendet werden.

Verwenden von CLI

Befehlsmodus (Übersicht)

CLI ist in verschiedene Befehlsmodi unterteilt. Jeder Befehlsmodus verfügt über einen spezifischen Befehlssatz. Durch Eingabe eines Fragezeichens (?) an der Konsolen-Eingabeaufforderung wird eine Liste der für diesen spezifischen Befehlsmodus verfügbaren Befehle angezeigt.

In jedem Modus wird ein spezifischer Befehl verwendet, um von einem Befehlsmodus zum anderen zu wechseln.

Während der Initialisierung der CLI-Sitzung wird der Benutzer-EXEC-Modus als CLI-Modus verwendet. Im User EXEC-Modus ist nur eine Teilmenge der Befehle verfügbar. Diese Ebene ist für Vorgänge reserviert, die keinen Einfluss auf die Switch-Konfiguration haben; sie wird zum Zugriff auf Konfigurationsteilsysteme genutzt. Für den privilegierten EXEC-Modus kann ein Kennwort erforderlich sein, wenn das Aktivierungskennwort konfiguriert ist. Weitere Informationen zum Einrichten des Aktivierungskennworts finden Sie unter Sicherheitsverwaltung und Kennwortkonfiguration.

Der Privileged EXEC-Modus bietet Zugriff auf die globale Gerätekonfiguration. Für bestimmte globale Konfigurationen innerhalb des Gerätes wechseln Sie zur nächsten Ebene, dem globalen Konfigurationsmodus. Es ist kein Passwort erforderlich.

Im Global Configuration-Modus wird die Gerätekonfiguration auf globaler Ebene verwaltet.

Im Schnittstellen-Konfigurationsmodus wird das Gerät auf der physikalischen Schnittstellenebene konfiguriert. Schnittstellenbefehle, die Unterbefehle erfordern, sind einer anderen Ebene zugeordnet, dem so genannten Subinterface Configuration-Modus.

Benutzer-EXEC-Modus

Die Eingabeaufforderung auf Benutzer-EXEC-Ebene besteht aus dem Hostnamen gefolgt von einer spitzen Klammer (>). Beispiel:

```
console>
```

ANMERKUNG: Sofern er bei der Erstkonfiguration nicht geändert wurde, lautet der Standardhostname console.

Mithilfe der Benutzer-EXEC-Befehle werden Verbindungen zu Remote-Geräten hergestellt, Terminaleinstellungen temporär geändert, grundlegende Tests durchgeführt und Systeminformationen aufgelistet.

Um die Benutzer-EXEC-Befehle aufzulisten, geben Sie ein Fragezeichen in der Befehlszeile ein.

Privilegierter EXEC-Modus

Der privilegierte Zugang kann durch ein Kennwort geschützt werden, um unbefugte Zugriffe zu verhindern und sicherzustellen, dass alle Betriebsparameter funktionstüchtig sind. Bei den Kennwörtern ist die Groß- und Kleinschreibung relevant, und die einzelnen Zeichen des Kennworts werden auf dem Bildschirm als Sternchen angezeigt.

So können Sie auf die Befehle im privilegierten EXEC-Modus zugreifen und diese auflisten:

1. Geben Sie an der Eingabeaufforderung enable ein, und drücken Sie die <Eingabetaste>.
2. Falls eine Kennwort-Eingabeaufforderung erscheint, geben Sie das Kennwort ein und drücken die <Eingabetaste>.

   Die Eingabeaufforderung für den privilegierten EXEC-Modus besteht aus dem Hostnamen des Gerätes, gefolgt von einem Rautenzeichen (#). Beispiel:

   ```
   console#
   ```
3. Um die Privileged EXEC-Befehle aufzulisten, geben Sie ein Fragezeichen in der Befehlszeile ein.
4. Um vom privilegierten EXEC-Modus zum Benutzer-EXEC-Modus zurückzukehren, geben Sie den Befehl exit ein oder drücken die Tastenkombination <Strg><Z>.

Das folgende Beispiel veranschaulicht, wie Sie den privilegierten EXEC-Modus aufrufen und zum Benutzer-EXEC-Modus zurückkehren:

```
console>enable

Enter Password: ******

console#

console#exit

console>
```

Mit dem Befehl exit können Sie zu einem vorherigen Modus zurückkehren. So ist beispielsweise ein Wechsel vom Schnittstellen-Konfigurationsmodus zum globalen Konfigurationsmodus und vom globalen Konfigurationsmodus zum privilegierten EXEC-Modus möglich.

Globaler Konfigurationsmodus

Die globalen Konfigurationsbefehle werden auf Systemfunktionen und nicht auf ein bestimmtes Protokoll bzw. eine Schnittstelle angewendet.

So greifen Sie auf den globalen Konfigurationsmodus zu:

1. Geben Sie an der Eingabeaufforderung für den privilegierten EXEC-Modus configure ein und drücken die <Eingabetaste>. Die Eingabeaufforderung für den globalen Konfigurationsmodus erscheint als Hostname des Gerätes gefolgt von (config) und einem Rautenzeichen (#).

   ```
   console(config)#
   ```
2. Um die globalen Konfigurationsbefehle aufzulisten, geben Sie ein Fragezeichen in der Befehlszeile ein.
3. Um vom globalen Konfigurationsmodus zum privilegierten EXEC-Modus zurückzukehren, geben Sie den Befehl exit ein oder drücken die Tastenkombination <Strg><Z>.

Das folgende Beispiel veranschaulicht, wie Sie den *globalen Konfigurationsmodus* aufrufen und zum *privilegierten EXEC-Modus* zurückkehren:

```
console#

console#configure

console(config)#exit
```

```
console#
```

Schnittstellen-Konfigurationsmodus

Mit Hilfe der Schnittstellen-Konfigurationsbefehle werden die Einstellungen für eine bestimmte IP-Schnittstelle, einschließlich Bridge-Gruppe, Beschreibung usw., geändert. Die Interface Configuration Modes lauten:

- **VLAN** – Umfasst Befehle zum Erstellen und Konfigurieren eines vollständigen VLAN, beispielsweise um ein VLAN zu erstellen und eine IP-Adresse darauf anzuwenden.
- **Port Channel** – Enthält Befehle zur Konfiguration von Link Aggregation Groups (LAGs).
- **Ethernet** – Enthält Befehle zur Verwaltung von Ethernet-Ports.
- **Loopback** (Schleifentest) – Enthält Befehle zur Konfiguration der Loopback-Schnittstelle.
- **Tunnel** – Enthält Befehle zur Konfiguration der Tunnelschnittstelle.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Hardwarebeschreibung

Benutzerhandbuch für die Dell™ PowerConnect™ 6200-Reihe

- Port-Beschreibung
- Weitere Merkmale
- LED-Definitionen

Dieser Abschnitt enthält Informationen über Gerätemerkmale und die Hardwarekonfiguration von Modulen. Folgende Themen werden abgedeckt:

- Vorderseite der Dell™ PowerConnect™ 6200-Reihe
- Rückseite der PowerConnect 6200-Reihe
- Konsolen-Port (RS-232)
- Abmessungen
- Netzteile
- Belüftungssystem
- Stacking
- LED-Definitionen

Port-Beschreibung

Vorderseite der Dell™ PowerConnect™ 6200-Reihe

An der Vorderseite des PowerConnect 6224-Switch befinden sich 24 10/100/1000 Base-T-RJ-45-Ports mit vier SFP-Kombinations-Ports, die einen Auto-Sensormodus für Geschwindigkeit, Flusskontrole und Duplex-Modus aufweisen. SFP-Transceiver sind separat zu erwerben. An der Vorderseite des PowerConnect 6248 befinden sich 48 10/100/1000 Base-T-RJ-45-Ports mit vier SFP-Kombinations-Ports.

Abbildung 2-1. PowerConnect 6224 mit 24 10/100/1000-Base-T-Ports

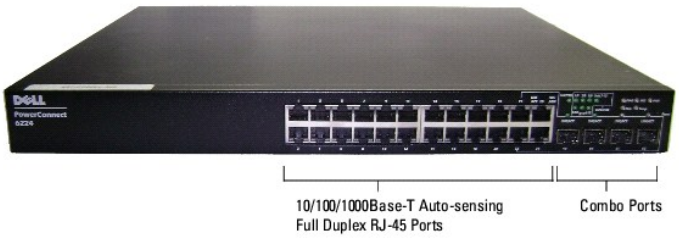


Abbildung 2-2. PowerConnect 6248 mit 48 10/100/1000-Base-T-Ports

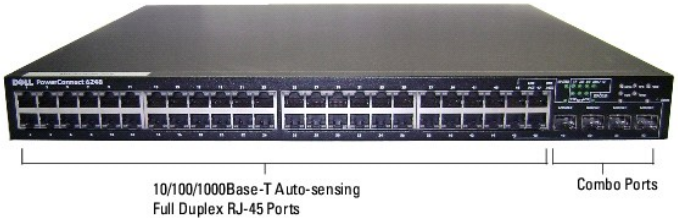


Abbildung 2-3. PowerConnect 6224F mit 24 SFP-Ports

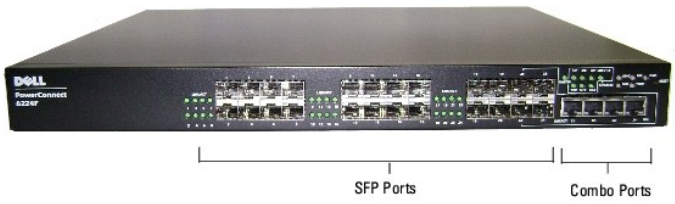


Abbildung 2-4. PowerConnect 6224P mit 24 10/100/1000-Base-T-Ports

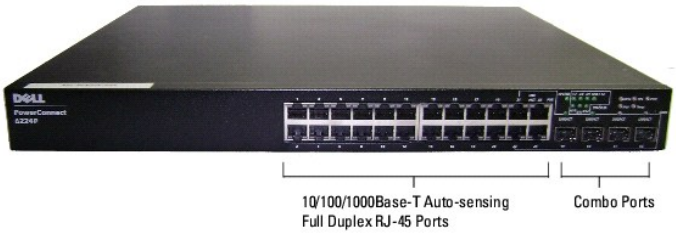
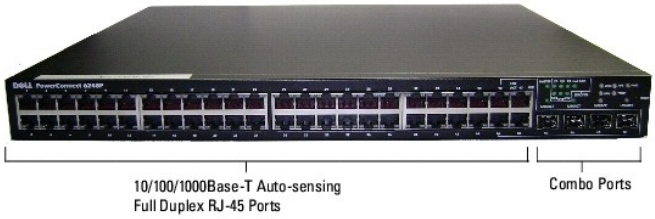


Abbildung 2-5. PowerConnect 6248P mit 48 10/100/1000-Base-T-Ports



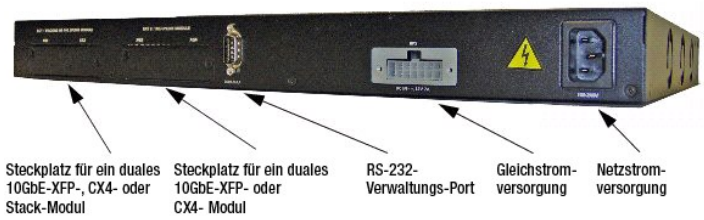
- Der Switch erkennt automatisch den Unterschied zwischen gekreuzten und durchgehenden Kabeln an RJ-45-Ports.
- SFP-Ports unterstützen sowohl SX- als auch LX-Module.
- RJ-45-Ports unterstützen den Halbduplex- und Vollduplex-Betrieb mit 10/100/1000 Mbit/s.
- Das Nadelloch zum Zurücksetzen befindet sich an der Vorderseite.

Rückseite der PowerConnect 6200-Reihe

Jeder PowerConnect Switch der Reihe 6200 besitzt einen RS-232-Wartungs-Port auf der Rückseite. Dieser serielle Anschluss kann zur Verwaltung eines ganzen Stack verwendet werden.

Zwei 10-Gbit/s-Erweiterungssteckplätze sind ebenfalls auf der Rückseite des Switch angebracht. Der rechte Steckplatz unterstützt ein duales 10GbE-XFP-Modul oder ein CX4-Modul. Der linke Steckplatz unterstützt ein duales 10GbE-XFP-Modul, ein CX4-Modul oder ein Stack-Modul.

Abbildung 2-6. PowerConnect 6200-Reihe, Rückseite



Konsolen-Port (RS-232)

Der Konsolen-Port (RS-232) wird nur für die Verwaltung über eine serielle Schnittstelle verwendet. Dieser Port sieht eine direkte Verbindung zum Switch vor und wird für den Zugriff auf CLI von einem Konsolenterminal verwendet, das an einen EIA/TIA-232-Port angeschlossen ist.

Der Konsolen-Port unterstützt die asynchrone Datenübertragung mit folgenden Eigenschaften: acht Datenbits, ein Stoppbit, kein Paritätsbit und keine Flusskontrolle. Die Standardbaudrate beträgt 9600 Bit/s.

ANMERKUNG: Wenn Sie einen Switch-*Stack* installieren, müssen Sie den Stack vor dem Einschalten und Konfigurieren zusammenfügen und verkabeln. Beim ersten Einschalten eines Stack wird der Master-Switch bestimmt, der sich an beliebiger Position im Stack befinden kann. Bei diesem Switch leuchtet die Master-Switch-LED auf der Vorderseite links oben. Verbinden Sie das Terminal mit dem Master-Switch. Wenn Sie das Terminal an einem untergeordneten Switch anschließen, können Sie CLI nicht verwenden.

Weitere Merkmale

Abmessungen

Die Abmessungen der Switches der Reihe 6200 sind wie folgt:

- 440 mm x 460 mm x 44 mm (B x T x H)
- 17,32 x 18,11 x 1,73 Zoll (B x T x H)

Netzteile

Die Switches der Reihe 6200 besitzen ein internes Netzteil, das Standard-Wechselstrom benötigt. Bei Switches ohne PoE-Unterstützung können Sie auch ein redundantes Gleichstromnetzteil anschließen, etwa das PowerConnect RPS-600. Bei Switches mit PoE-Unterstützung können Sie ein PowerConnect EPS-470 anschließen. Der Betrieb kann durch Beobachtung der LEDs überprüft werden. Nähere Informationen finden Sie unter "System-LEDs".

Belüftungssystem

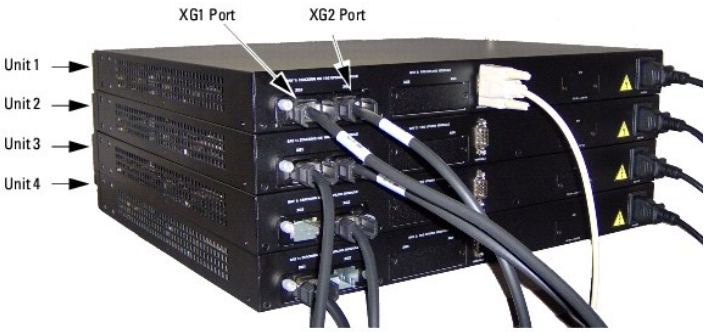
Der PowerConnect 6224 wird von drei Lüftern gekühlt. Der PowerConnect 6248 besitzt vier Lüfter. Der Betrieb kann durch Beobachtung der LEDs überprüft werden. Informationen zu den LEDs finden Sie unter "System-LEDs".

Stacking

PowerConnect 6224- und/oder 6248-Switches lassen sich zu einem Stack mit bis zu 12 Switches zusammenfügen, wodurch bis zu 576 Ports auf der Vorderseite verfügbar werden. Sie erstellen einen Stack, indem Sie benachbarte Geräte über die Stack-Anschlüsse im linken Bereich der Switch-Rückseiten miteinander verbinden. Siehe Abbildung 2-7.

1. Installieren Sie eines der kurzen Stack-Kabel zwischen einem der Stack-Ports des obersten Switch und des Switch direkt darunter. Installieren Sie ein separat erworbenes Stack-Modul im rückseitigen "Schacht 1" der einzelnen Switches im Stack.
2. Falls erforderlich, verwenden Sie ein separat erworbenes langes Stack-Kabel (3 Meter) zum Verbinden der Switches. Wiederholen Sie diesen Vorgang, bis alle Geräte verbunden sind.
3. Verbinden Sie mit dem verbleibenden Stacking-Kabel die noch freien Ports miteinander, den einen am obersten und den anderen am untersten Gerät.

Abbildung 2-7. Anschließen eines Switch-Stack



In Abbildung 2-7 weist der Stack die folgenden physikalischen Verbindungen zwischen den Switches auf:

- Einheit 1 und Einheit 2 sind über die XG1-Ports an den einzelnen Switches verbunden.
- Einheit 2 und Einheit 3 sind über die XG2-Ports an den einzelnen Switches verbunden.
- Einheit 1 und Einheit 4 sind über den XG2-Port an Einheit 1 und den XG1-Port an Einheit 4 verbunden.

Stacking-Standby

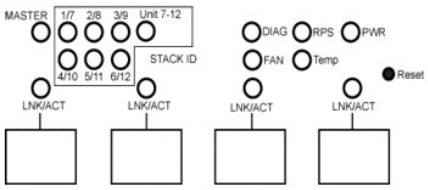
Die Stacking-Funktion unterstützt eine "Standby"- bzw. Reserveeinheit, die bei einem Ausfall des Stacks die Rolle der Master-Einheit übernimmt. Sobald im Stack ein Ausfall der Master-Einheit festgestellt wird, initialisiert die Standby-Einheit die Steuerungsplatine und aktiviert alle anderen Einheiten des Stacks mit der aktuellen Konfiguration. Auf der Standby-Einheit wird eine synchronisierte Kopie der aktiven Stack-Konfiguration verwaltet. Während der Umschaltung werden alle Ports herunter- und wieder hochgefahren, um Schleifen zu vermeiden und neue Master-Softwareanwendungen in einen konsistenten Zustand zu bringen.

Die Standby-Einheit ist im Stack vorkonfiguriert. Sie können jedoch über die CLI ein anderes Stack-Mitglied als Standby-Einheit definieren. Weitere Informationen finden Sie im *CLI Reference Guide* (CLI-Referenzhandbuch).

LED-Definitionen

An der Vorderseite befinden sich mehrere Leuchtdioden (LEDs), die den aktuellen Status der Verbindung, Netzteile, Lüfter, Systemdiagnose und des Stack signalisieren.

Abbildung 2-8. LEDs auf der Vorderseite



SFP-Port-LEDs

In Abbildung 2-9 sind die SFP-Port-LEDs dargestellt, die sich über jedem SFP-Port befinden.

Abbildung 2-9. SFP-Port-LEDs

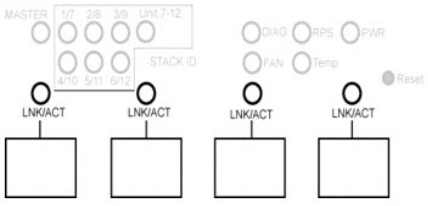


Tabelle 2-1 enthält die LED-Definitionen für SFP-Ports.

Tabelle 2-1. Definitionen der SFP-Port-LEDs

LED	Farbe	Definition
LNK/ACT	Leuchtet stetig grün	Der Port ist derzeit verbunden.
	Blinkt grün	Der Port sendet oder empfängt derzeit Netzwerkverkehr.
	Aus	Der Port ist derzeit nicht verbunden.

LEDs an den XFP-Modul-Ports

Die XFP-Anschlüsse befinden sich am XFP-Modul, das an der Rückseite eingesetzt wird. Tabelle 2-2 enthält die LED-Definitionen für XFP-Ports.

Tabelle 2-2. Definitionen der XFP-Port-LEDs

LED	Farbe	Definition
XFP	Grün	Der Port ist derzeit verbunden.
	Blinkt grün	Der Port sendet oder empfängt derzeit Netzwerkverkehr.
	Aus	Der Port ist derzeit nicht verbunden.

LEDs des 10/100/1000 Base-T-Ports

An jedem 10/100/1000 Base-T-Port befinden sich zwei LEDs. Die folgende Abbildung zeigt die LEDs des 10/100/100 Base-T-Ports.

Abbildung 2-10. LEDs des 10/100/1000 Base-T-Ports

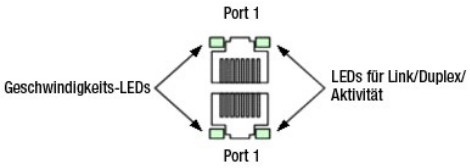


Tabelle 2-3 enthält LED-Definitionen des 10/100/1000 Base-T-Ports für die Modelle PowerConnect 6224, 6248, and 6224F.

Tabelle 2-3. LED-Definitionen des 10/100/1000 Base-T-Ports (6224, 6248 und 6224F)

LED	Farbe	Definition
Speed	Grün	Der Port wird mit 1000 Mbit/s betrieben.
	Gelb	Der Port wird mit 10/100 Mbit/s betrieben.
	Dauerlicht	Verbindung ohne Aktivität.
	Blinkend	Verbindung und Aktivität.
	Aus	Keine Verbindung.
Verbindung	Grün	Vollduplex-Modus.
	Aus	Halbduplex-Modus.

Tabelle 2-4 enthält LED-Definitionen des 10/100/1000 Base-T-Ports für die Modelle PowerConnect 6224P und 6248P.

Tabelle 2-4. LED-Definitionen des 10/100/1000 Base-T-Ports (6224P und 6248P)

LED	Farbe	Definition
Geschwindigkeit/LNK/ACT	Stetig grün	Der Port wird mit 1000 Mbit/s betrieben.
	Grün blinkend	Der Port wird mit 10/100 Mbit/s betrieben.
	Aus	Keine Verbindung.
FDX	Stetig grün	Das PoE-Gerät wurde erkannt und arbeitet bei normaler Last.
	Grün blinkend	Der Port arbeitet im Übergangsmodus. Das PoE-Gerät wird ermittelt oder ist defekt.
	Stetig gelb	Am PD ist eine Überlastung bzw. ein Kurzschluss aufgetreten.
	Gelb blinkend	Das PD-Stromversorgungskonzept überschreitet die vorgegebene Stromzuweisung.
	Aus	Es wurde kein PD erkannt.

System-LEDs

Die System-LEDs, die sich auf der Vorderseite rechts befinden, liefern Informationen über die Netzteile, Lüfter und Temperaturbedingungen sowie den aktuellen Diagnosestatus. In Abbildung 2-11 sind die System-LEDs dargestellt.

Abbildung 2-11. System-LEDs

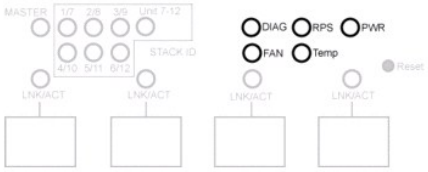


Tabelle 2-5 enthält die Definitionen für die System-LEDs.

Tabelle 2-5. Definitionen für System-LEDs

LED	Farbe	Definition
DIAG	Blinkt grün	Eine Diagnoseprüfung wird derzeit durchgeführt.
	Grün	Die Diagnoseprüfung wurde erfolgreich abgeschlossen.
	Rot	Die Diagnoseprüfung ist fehlgeschlagen.
RPS	Grün	Ein redundantes Netzteil (Redundant Power Supply, RPS) ist vorhanden und funktioniert ordnungsgemäß.
	Rot	Ein redundantes Netzteil ist vorhanden, ist jedoch ausgefallen.
	Aus	Ein redundantes Netzteil ist nicht vorhanden.
PWR	Grün	Das Netzteil funktioniert ordnungsgemäß.
	Rot	Das Netzteil ist ausgefallen.
FAN	Grün	Die Lüfter funktionieren ordnungsgemäß.
	Rot	Ein oder mehrere Lüfter sind ausgefallen.
Temp	Grün	Die Systemtemperatur liegt unterhalb des Grenzwerts.
	Rot	Die Systemtemperatur liegt oberhalb des Grenzwerts.

Stack-LEDs

Die Stack-LEDs, die sich auf der Vorderseite rechts befinden, liefern Informationen über den Ort und den Status des Switch im Stack. In Abbildung 2-12 sind die Stack-LEDs dargestellt. Tabelle 2-6 enthält die Definitionen für die Stack-LEDs.

Abbildung 2-12. Stack-LEDs

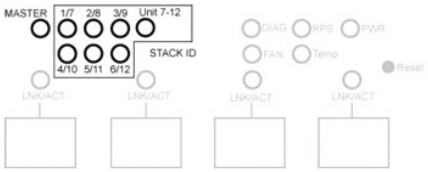


Tabelle 2-6. Definitionen für Stack-LEDs

LED	Farbe	Definition
Alle LEDs aus		Die Einheit wird als Standalone-Switch betrieben.
MASTER	Grün	Die Einheit ist derzeit der Master-Switch im Stack.
	Aus	Die Einheit ist nicht der Master-Switch im Stack.
Einheit 7-12	Grün	Die Stack-ID liegt im Bereich von 7 bis 12.
	Aus	Die Stack-ID liegt im Bereich von 1 bis 6.
1/7	Grün	Die Einheit ist der erste oder siebte Switch im Stack.
	Aus	Die Einheit ist nicht der erste oder siebte Switch im Stack.
2/8	Grün	Die Einheit ist der zweite oder achte Switch im Stack.

	Aus	Die Einheit ist nicht der zweite oder achte Switch im Stack.
3/9	Grün	Die Einheit ist der dritte oder neunte Switch im Stack.
	Aus	Die Einheit ist nicht der dritte oder neunte Switch im Stack.
4/10	Grün	Die Einheit ist der vierte oder zehnte Switch im Stack.
	Aus	Die Einheit ist nicht der vierte oder zehnte Switch im Stack.
5/11	Grün	Die Einheit ist der fünfte oder elfte Switch im Stack.
	Aus	Die Einheit ist nicht der fünfte oder elfte Switch im Stack.
6/12	Grün	Die Einheit ist der sechste oder zwölfte Switch im Stack.
	Aus	Die Einheit ist nicht der sechste oder zwölfte Switch im Stack.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Einführung

Benutzerhandbuch für die Dell™ PowerConnect™ 6200-Reihe

- Funktionen
- CLI-Dokumentation

HINWEIS: Lesen Sie die Versionshinweise für dieses Produkt, bevor Sie fortfahren. Sie können die Versionshinweise von der Dell Support-Website unter **support.dell.com** herunterladen.

Die Dell™ PowerConnect™ 6200-Reihe umfasst Layer 2- and Layer 3-Switches in Standalone- oder Stack-Konfiguration, die das Dell PowerConnect LAN-Switch-Produktspektrum erweitern. Diese Switches weisen folgende Merkmale und Funktionen auf:

- 1U-Formfaktor, rack-montierbares Gehäuse.
- Unterstützung aller Anforderungen an die Datenkommunikation eines Multi-Layer-Switch einschließlich Layer 2-Switching, IPv4-Routing, IPv6-Routing, IP-Multicast, Quality of Service sowie Funktionsmerkmale für Sicherheit und System-Management.
- Hohe Verfügbarkeit aufgrund untergeordneter Hot-Swap-Switches.

Funktionsmerkmale

In diesem Abschnitt werden die benutzerkonfigurierbaren Funktionen des Switch beschrieben. Eine Liste aller Funktionen finden Sie in den Versionshinweisen der Software.

Port-basierte Funktionen

Jumbo-Frames-Unterstützung

Jumbo-Frames ermöglichen den Transport identischer Daten in weniger Frames für geringeren Overhead, kürzere Verarbeitungszeiten und weniger Unterbrechungen.

Auto-MDI/MDIX-Unterstützung

Ihr Switch unterstützt die automatische Erkennung von gekreuzten und durchgehenden Kabeln.

Die Standardverkabelung für Endstationen ist Media-Dependent Interface (MDI), und die Standardverkabelung für Hubs und Switches wird als Media-Dependent Interface with Crossover (MDIX) bezeichnet.

Informationen zur MDI/MDIX-Konfiguration für Ports oder LAGs finden Sie unter "Port-Konfiguration" bzw. "LAG-Konfiguration".

Auto-Verhandlung

Die Auto-Verhandlung ermöglicht dem Switch, Betriebsarten bekannt zu geben und "auszuhandeln". Diese Funktion ist ein Mittel zum Informationsaustausch zwischen zwei Switches mit gemeinsamem Punkt-zu-Punkt-Verbindungssegment und ermöglicht die automatische Konfiguration beider Switches, um deren Übertragungsfähigkeiten optimal zu nutzen.

Bei den Geräten der PowerConnect 6200-Reihe wird diese automatische Abstimmung durch Port-Anzeige optimiert. Anhand der Port-Anzeige kann der Systemadministrator die angezeigten Port-Geschwindigkeiten konfigurieren.

Informationen über die Auto-Verhandlung finden Sie unter "Port-Konfiguration" bzw. "LAG-Konfiguration".

Unterstützung von Flusskontrolle (IEEE 802.3x)

Durch Flusskontrolle kann ein langsamerer Switch mit einem schnelleren Switch kommunizieren, indem er den schnelleren Switch dazu auffordert, keine Pakete zu senden. Die Übertragung wird zeitweise angehalten, um einen Pufferüberlauf zu verhindern.

Informationen zur Flusskontrolle für Ports oder LAGs finden Sie unter "Port-Konfiguration" bzw. "LAG-Konfiguration".

Schutz vor Head-of-Line-Blocking

Der Schutz vor Head-of-Line- (HOL) Blocking verhindert Verzögerungen und Frame-Verluste durch Datenströme, die um die gleichen Egress-Port-Ressourcen konkurrieren. Beim HOL-Blocking befinden sich die Pakete in einer Warteschlange, wobei die Pakete am Anfang der Warteschlange vor den weiter hinten liegenden Paketen weitergeleitet werden.

Backpressure-Unterstützung

Bei Halbduplex-Verbindungen kann der Empfänger Pufferüberläufe verhindern, indem er die Verbindung belegt, so dass diese für weitere Daten nicht verfügbar ist.

Alternate Store and Forward (ASF)

Das Merkmal ASF (Alternate Store and Forward) reduziert die Latenzzeiten großer Pakete. Wenn ASF aktiviert ist, kann die Speicherverwaltungseinheit ein Paket an den Egress-Port weiterleiten, bevor es vollständig im (Cell Buffer Pool)-Speicher eingetroffen ist. AFS – auch als Durchschaltmodus bezeichnet – ist über die Befehlszeilenschnittstelle konfigurierbar. Hinweise zum Konfigurieren von AFS finden Sie im "CLI Reference Guide" (CLI-Referenzhandbuch).

Unterstützte MAC-Adressen-Funktionen

Unterstützung von MAC-Adressen

Der Switch unterstützt bis zu 8000 MAC-Adressen und reserviert zwei MAC-Adressen für die Verwendung durch das System.

Selbsterlernung von MAC-Adressen

Der Switch kann MAC-Adressen aus eingehenden Paketen automatisch lernen.

Automatisches Altern von MAC-Adressen

MAC-Adressen, an die während eines bestimmten Zeitraums kein Datenverkehr geflossen ist, werden aussortiert, um einen Überlauf der Bridging-Tabelle zu verhindern.

Informationen über die Konfiguration des Überalterungszeitraums von MAC-Adressen finden Sie unter "Dynamische Adressentabelle".

Statische MAC-Einträge

Benutzerdefinierte MAC-Einträge werden in der Bridging-Tabelle mit den selbsterlernten Adressen gespeichert.

Informationen über die Konfiguration der statischen MAC-Adressen finden Sie unter "Statische Adressentabelle".

VLAN-fähiges MAC-basiertes Switching

Pakete, die von einer unbekannten Quelladresse eingehen, werden an die CPU gesendet und zur Hardwaretabelle hinzugefügt. Zukünftige Pakete, die an diese Adresse gehen oder von ihr kommen, werden effizienter weitergeleitet.

MAC-Multicast-Unterstützung

Der Multicast-Dienst ist ein eingeschränkter Broadcast-Dienst, über den sich "Eins-zu-Viele"- und "Viele-zu-Viele"-Verbindungen für die Informationsverteilung einrichten lassen. Bei Layer 2-Multicast-Diensten wird ein einzelner Frame, der an eine bestimmte Multicast-Adresse gerichtet ist, empfangen, und Kopien des zu übertragenden Frame werden auf jedem relevanten Port erstellt.

Informationen über die Konfiguration der MAC-Multicast-Unterstützung finden Sie unter "Verwalten der Multicast-Unterstützung".

Layer 2-Funktionen

IGMP-Snooping

Beim IGMP-Snooping wird der Inhalt von IGMP-Frames geprüft, bevor diese durch den Switch von Stationen an einen Upstream-Multicast-Router weitergeleitet werden. Snooping ermöglicht es dem Switch, Stationen zu ermitteln, die an Multicast-Sitzungen interessiert sind, und welche Multicast-Router Multicast-Frames senden.

Port-Spiegelung

Durch die Port-Spiegelung wird der Netzwerkdatenverkehr überwacht und gespiegelt, indem Kopien eingehender und ausgehender Pakete von bis zu vier Quell-Ports an einen Überwachungs-Port weitergeleitet werden.

Broadcast-Sturmkontrolle

Beim Weiterleiten von Layer 2-Frames werden Broadcast-, unbekannte Unicast- und Multicast-Frames an alle Ports des relevanten virtuellen lokalen Datennetzes (VLAN =Virtual Local Area Network) gesendet). Dieser immense Datenverkehr belegt Bandbreite und bewirkt, dass sämtliche Knoten an allen Ports geladen werden. Die Sturmkontrollfunktion begrenzt die Menge der vom Switch angenommenen und weitergeleiteten Broadcast-, unbekannten Unicast- und Multicast-Frames.

Merkmale mit VLAN-Unterstützung

VLAN-Unterstützung

VLANs sind Gruppen von Switch-Ports mit gemeinsamer Broadcast-Domäne. Pakete werden VLANs entweder aufgrund der VLAN-Kennung oder einer Kombination von Ingress-Port und Paketinhalt zugeordnet. Pakete mit gemeinsamen Attributen können Gruppen im gleichen VLAN sein.

Informationen zum Konfigurieren von VLANs finden Sie unter "Konfigurieren von VLANs".

Port-basierte VLANs

Port-basierte VLANs ordnen eingehende Pakete VLANs aufgrund des Ingress-Ports zu.

Informationen zum Konfigurieren von VLANs finden Sie unter "Konfigurieren von VLANs".

Auf dem IEEE 802.1v-Protokoll basierte VLANs

Die Regeln zur VLAN-Klassifizierung sind in der Protokollidentifikation auf der Sicherungsschicht (Layer 2) festgelegt. Protokollbasierte VLANs werden für die Trennung des Layer 2-Verkehrs von abweichenden Layer 3-Protokollen verwendet.

Informationen zum Definieren von protokollbasierten VLANs finden Sie unter "Protokollgruppe."

Umfassende VLAN-Tagging-Konformität gemäß IEEE 802.1Q

IEEE 802.1Q definiert eine Architektur für virtuelle Bridge-LANs, die in VLANs bereitgestellten Dienste sowie die Protokolle und Algorithmen für die Dienstebereitstellung.

GVRP-Unterstützung

Das GARP-VLAN-Registrierungsprotokoll (GVRP) ermöglicht ein IEEE 802.1Q-konformes VLAN-Pruning sowie eine dynamische VLAN-Generierung an 802.1Q Trunk-Ports. Ist GVRP aktiviert, registriert und propagiert der Switch die VLAN-Mitgliedschaft an allen Ports, die zur aktiven zugrundeliegenden Spanning Tree Protocol-Topologie gehören.

Informationen zum Konfigurieren von GVRP finden Sie unter "GVRP-Parameter".

Geschützte Anschlüsse (PVE = Private VLAN Edge)

PVE- (Private VLAN Edge) Ports sind ein Layer 2-Sicherheitsmerkmal, das port-basierte Sicherheit zwischen Ports vorsieht, die zum selben VLAN gehören. Es ist eine Erweiterung des gewöhnlichen VLANs. Der Datenverkehr von geschützten Ports wird nur an die Uplink-Ports gesendet und kann nicht an andere Ports innerhalb des VLAN gesendet werden.

Subnetzbasiertes VLAN

Dieses Merkmal ermöglicht die Zuweisung eingehender Pakete ohne Kennung zu einem VLAN und einer Verkehrsklasse auf der Grundlage der Quell-IP-Adresse des Pakets.

Informationen zum Konfigurieren subnetzbasierter VLANs finden Sie unter "IP-Subnetz an VLAN binden."

MAC-basiertes VLAN

Dieses Merkmal ermöglicht die Zuweisung eingehender Pakete ohne Kennung zu einem VLAN und einer Verkehrsklasse auf der Grundlage der Quell-MAC-Adresse des Pakets.

Informationen zum Konfigurieren MAC-basierter VLANs finden Sie unter "MAC an VLAN binden".

Funktionen des Spanning Tree-Protokolls

Spanning Tree Protocol (STP) per Switch

802.1d STP ist eine Standardanforderung an Layer 2-Switches, die es Bridges ermöglicht, L2-Weiterleitungsschleifen automatisch zu vermeiden bzw. aufzuheben. Switches tauschen Konfigurationsinformationen untereinander aus, indem sie speziell formatierte Frames verwenden und eine selektive Weiterleitung auf Ports durchführen.

Hinweise zum Konfigurieren des Spanning Tree-Protokolls finden Sie unter "Konfigurieren des Spanning Tree-Protokolls".

IEEE 802.1w Rapid Spanning Tree

Das Rapid Spanning Tree Protocol (RSTP) erkennt und nutzt Netzwerktopologien, um eine schnellere Konvergenz zu ermöglichen, ohne Weiterleitungsschleifen zu erzeugen.

Hinweise zum Konfigurieren des Rapid Spanning Tree-Protokolls finden Sie unter "Rapid Spanning Tree."

Multiple Spanning Tree Protocol

Im Multiple Spanning Tree Protocol- (MSTP) Betrieb werden VLANs bestimmten Spanning Tree-Instanzen zugeordnet. MSTP unterstützt verschiedene Lastausgleichskonfigurationen. Pakete, die verschiedenen VLANs zugewiesen sind, werden auf unterschiedlichen Pfaden der MSTP-Regionen (MST-Regionen) übermittelt. Bei Regionen handelt es sich um eine oder mehrere miteinander verbundene MSTP-Bridges mit identischen MSTP-Einstellungen. Standardmäßig können Administratoren den VLAN-Verkehr über bestimmte Pfade leiten.

Hinweise zum Konfigurieren des Multiple Spanning Tree-Protokolls finden Sie unter "MSTP-Einstellungen."

Spanning Tree Root Guard

Spanning Tree Root Guard wird verwendet, um den Root einer Spanning Tree-Instanz vor unerwarteten Änderungen zu schützen. Die Priorität einer Bridge-ID kann auf null gesetzt werden, aber bei einer anderen Bridge-ID mit einer niedrigeren MAC-Adresse könnte die Priorität auch auf null gesetzt werden, und sie könnte den Root übernehmen.

Bridge Protocol Data Unit Guard (BPDU Guard)

Spanning Tree BPDU Guard wird verwendet, um den Port zu deaktivieren, falls ein neues Gerät versucht, in eine bereits vorhandene STP-Topologie einzudringen. Solchen Geräten, die ursprünglich nicht Teil des STP waren, wird die Einflussnahme auf die STP-Topologie verweigert.

Link-Aggregation-Merkmale

Link-Aggregation

Bis zu acht Ports können für die Bildung einer Link Aggregated Group (LAG) zusammengefasst werden. Das ermöglicht einen Fehlertoleranzschutz vor physikalischen Verbindungsunterbrechungen und zudem Verbindungen mit höherer Bandbreite und verbesserter Bandbreitengranularität.

Eine LAG besteht aus Ports der gleichen Geschwindigkeit im Vollduplex-Betrieb.

Informationen zum Konfigurieren von LAGs finden Sie unter "LAG-Konfiguration".

Link-Aggregation und LACP

Durch verbindungsübergreifenden Peer-Austausch überwacht das Link Aggregate Control Protocol (LACP) permanent die Aggregationsfähigkeit der verschiedenen Verbindungen und gewährleistet auf diese Weise eine maximale Aggregationsfähigkeit zwischen den einzelnen Systempaaren. LACP bestimmt, konfiguriert, bindet und überwacht automatisch die Port-Anbindung an Aggregatoren innerhalb des Systems.

Informationen über LACP finden Sie unter "LACP-Parameter".

Funktionsmerkmale IP-Telefon und Access Point-Support

Konfigurieren von PoE (Power Over Ethernet)

Der PowerConnect 6200 unterstützt PoE-Konfiguration für die System-Verbrauchsgrenze, SNMP-Traps und die Unterstützung älterer PoE-Geräte.

Hinweise zum Konfigurieren von PoE finden Sie unter "Konfigurieren der Stromversorgung über Ethernet (PoE)".

LLDP (Link Layer Discovery Protocol) für Medien-Endpoint-Geräte

Das LLPD-MED-Protokoll (Link Layer Discovery Protocol for Media Endpoint Devices) erweitert den LLDP-Standard um Funktionen für Netzwerkkonfiguration und -richtlinien, Geräteaufstellung, Verwaltung der Stromversorgung über Ethernet und Inventarmanagement.

Hinweise zum Konfigurieren von LLDP-MED finden Sie unter "Konfigurieren von LLDP (Link Layer Discovery Protocol) für Medien-Endpoint-Geräte".

Voice-VLAN

Die Voice-VLAN-Funktion ermöglicht Switch-Ports, Telefoniedaten mit einer festgelegten Prioritätsstufe zu übermitteln. Über die Prioritätsstufe kann der am Port eingehende Telefonverkehr separat vom übrigen Datenverkehr behandelt werden.

Hinweise zum Konfigurieren von Voice-VLAN finden Sie unter "Konfigurieren von Ports für Voice-VLAN".

IPv4-Routing-Funktionen

Address Resolution Protocol (ARP)

Der PowerConnect 6200 nutzt das ARP-Protokoll zur Verknüpfung einer Layer 2-MAC-Adresse mit einer Layer 3-IPv4-Adresse. Außerdem kann der Administrator statisch Einträge in die ARP-Tabelle aufnehmen.

OSPF (Open Shortest Path First)

Im OSPF-Routing-Protokoll sind zwei Bereichstypen definiert: der reguläre OSPF-Bereich und der OSPF-Stub-Bereich. OSPF-interne und -externe Routing-Informationen können überall im regulären OSPF-Bereich propagiert werden. Das Protokoll unterstützt Transit-Verkehr und virtuelle Verbindungen. OSPF-Stub-Bereiche empfangen keine externen Routing-Informationen. Stub-Bereiche werden zu dem Zweck eingerichtet, die Größe der Bereichsdatenbank für diejenigen Router zu begrenzen, die über begrenzte Ressourcen verfügen.

BOOTP/DHCP Relay Agent

Das BootP-Protokoll ermöglicht einem Gerät, Konfigurationsdaten und Parameter von einem geeigneten Server anzufordern und zu empfangen. Mit DHCP als einer Erweiterung von BootP können beim Systemstart zusätzliche Setup-Parameter von einem Netzwerkserver empfangen werden. Während die Ausführung von BootP nach dem Bezug einer IP-Adresse jedoch stoppt, wird der DCHP-Dienst fortlaufend ausgeführt. Die dem System zugewiesene IP-Adresse weist zum Beispiel eine "Mietdauer" auf, die auslaufen und ad-hoc erneuert werden kann.

RIP (Routing Information Protocol)

Das Routing-Protokoll, das innerhalb eines autonomen Internetsystems verwendet wird, wird als Interior Gateway Protocol (IGP) bezeichnet. RIP ist ein IGP, das für die Funktion in Netzwerken moderater Größe ausgelegt ist.

VRRP (Virtual Routing Redundancy Protocol)

VRRP (Virtual Routing Redundancy Protocol) wird verwendet, um Hosts redundante Router in der Netzwerktopologie bereitzustellen, ohne dass die Hosts neu konfiguriert werden oder wissen müssen, dass mehrere Router vorhanden sind.

IPv6-Routing-Funktionen

DHCPv6

DHCPv6 setzt die Vorstellung eines "zustandslosen" Servers um, wobei DHCPv6 nicht für die IP-Adressenzuordnung zu einem Client verwendet wird, sondern nur andere Netzwerkinformationen wie DNS-, NTP (Network Time Protocol)- und/oder SIP (Session Initiation Protocol)-Informationen liefert.

OSPFv3

OSPFv3 stellt ein Routing-Protokoll für den IPv6-Netzwerkbetrieb bereit. OSPFv3 ist eine neue Routing-Komponente, die auf der OSPF-Komponente in Version 2 basiert. Bei Dual-Stack-IPv6 können sowohl OSPF- als auch OSPFv3-Komponenten konfiguriert werden.

IPv6-Routen

Da IP4 und IPV6 gemeinsam in einem Netzwerk verwendet werden können, muss der Router in solch einem Netzwerk beide Verkehrstypen weiterleiten. Wegen dieser Koexistenz hält der PowerConnect 6200 zwei Routing-Tabellen vor, rto und rto6, die beide in der Lage sind, Daten über den gleichen Schnittstellensatz weiterzuleiten. IPV6-Schnittstellen werden auf ähnliche Weise verwaltet wie IPV4-Schnittstellen.

QoS- (Quality of Service) Funktionen

QoS- (Quality of Service) Unterstützung

Um unvorhersehbaren Netzwerkverkehr zu vermeiden und die Leistung zu optimieren, können Sie Quality of Service (QoS) im gesamten Netzwerk einsetzen. So wird sichergestellt, dass der Netzwerkverkehr gemäß spezifischer Kriterien priorisiert wird. Ihr Switch unterstützt zwei QoS-Typen: Differentiated Services und Class of Service.

Differentiated Services

Das QoS-Funktionsmerkmal enthält Unterstützung für Differentiated Services (DiffServ), die es ermöglicht, den Datenverkehr in Datenströme einzuteilen und eine bestimmte QoS-Behandlung gemäß eines festgelegten Verhaltens auf Hop-Basis zuzuweisen.

Class of Service

Mit der Warteschlangenfunktion Class of Service (CoS) können bestimmte Aspekte von Switch-Warteschlangen direkt konfiguriert werden. Damit wird das gewünschte QoS-Verhalten für unterschiedliche Typen von Netzwerkverkehr ermöglicht, wenn die Komplexitäten von DiffServ nicht benötigt werden.

IPv4-Multicast-Funktionen

DVMRP (Distance Vector Multicast Routing Protocol)

DVMRP tauscht Testpakete mit allen DVMRP-fähigen Routern aus und baut damit Zwei-Wege-Übertragungsstrecken mit benachbarten Geräten und eine Nachbartabelle auf. Es tauscht Berichtspakete aus und erstellt eine Unicast-Topologietabelle, die für den Aufbau der Multicast-Routing-Tabelle verwendet wird. Diese Multicast-Routing-Tabelle wird dann für die Weiterleitung der Multicast-Pakete verwendet.

IGMP (Internet Group Management Protocol)

Das Internet Group Management Protocol (IGMP) wird von IPv4-Systemen (Hosts und Routern) verwendet, um deren IP-Multicast-Gruppenmitgliedschaften an benachbarte Multicast-Router zu melden. Der PowerConnect 6200 übernimmt die Multicast-Router-Funktion des IGMP-Protokolls, d. h., er erfasst die Mitgliedschaftsinformationen, die für das aktive Multicast-Routing benötigt werden.

PIM-DM (Protocol Independent Multicast-Dense Mode)

Protocol Independent Multicast (PIM) ist ein Standard-Multicast-Routing-Protokoll, das skalierbares, domänenübergreifendes Multicast-Routing im Internet bereitstellt, und zwar unabhängig von den Mechanismen, die von bestimmten Unicast-Routing-Protokollen vorgesehen werden. Das PIM-DM-Protokoll verwendet eine vorhandene Unicast-Routing-Tabelle und einen Join/Prune/Graft-Mechanismus für den Aufbau eines Baumes. PIM-DM erstellt quellbasierte Verteilungsbäume mit den kürzesten Pfaden und nutzt dabei RPF (Reverse Path Forwarding).

PIM-SM (Protocol Independent Multicast-Sparse Mode)

PIM-SM wird für das effiziente Routing von Multicast-Verkehr an Multicast-Gruppen verwendet, die sich über WANs erstrecken können; außerdem wird das Protokoll dort eingesetzt, wo Bandbreite knapp ist. PIM-SM verwendet standardmäßig gemeinsam verwendete Bäume und implementiert aus Effizienzgründen quellbasierte Bäume. Anhand eines Grenzwerts für die Datenrate wird zwischen den Bäumen umgeschaltet.

Switch-Management-Funktionen

SNMP-Alarme und Trap-Protokolle

Das System protokolliert alle Ereignisse mit Schweregrad und Zeitangabe. Die Ereignisse werden als SNMP-Traps an eine Trap-Empfängerliste übermittelt.

Informationen über SNMP-Alarme und -Traps finden Sie unter "Definieren von globalen SNTP-Parametern".

Webbasiertes Management

Sie können das System von einem beliebigen Webbrowser verwalten. Der Switch enthält einen integrierten Webserver, der HTML-Seiten beliefert, anhand derer Sie das System überwachen und konfigurieren können.

Download der Konfigurationsdatei

Die Konfigurationsdatei des Switch enthält sowohl systemweite als auch port-spezifische Gerätekonfigurationsdaten. Konfigurationsdateien können durch Eingabe von Befehlen an der Befehlszeilenschnittstelle (CLI) angezeigt werden.

Informationen zum Herunterladen von Konfigurationsdateien finden Sie unter "Herunterladen von Dateien".

Software-Download

Über einen Software-Download können Sicherungs-Firmware-Images gespeichert werden. Informationen zum Herunterladen der Software finden Sie unter "Software-Download und Neustart."

Trivial File Transfer Protocol (TFTP)

Der PowerConnect der Reihe 6200 unterstützt den Upload/Download des Boot-Image, der Firmware und von Konfigurationsdateien über TFTP.

Fernüberwachung (RMON)

RMON ist eine Standard-MIB, die aktuelle und frühere MAC-Layer-Statistiken und -Kontrollobjekte definiert, wodurch sich im gesamten Netzwerk Echtzeitinformationen erfassen lassen.

Simple Network Management Protocol (SNMP), Versionen 1, 2 und 3

Das System ist über eine Kombination der MIB- (Management Information Base) Variablen und des SNMP-Protokolls komplett verwaltbar. Die verknüpften MIB-Werte stellen sämtliche Facetten des Systemzustands dar, und das SNMP-Protokoll wird zur Analyse und ggf. zur Modifizierung dieser Werte verwendet. SNMP v1/v2c/v3 über das UDP/IP-Transportprotokoll wird unterstützt.

Befehlszeilenschnittstelle (CLI)

Die Befehlszeilenschnittstelle (Command Line Interface, CLI) entspricht unter syntaktischen und semantischen Gesichtspunkten weitestgehend der gängigen Branchenpraxis. CLI setzt sich aus obligatorischen und optionalen Elementen zusammen. Die kontextsensitive Hilfe gibt Format- und Wertebereiche an, die für die aktuellen Befehle zulässig sind, und der CLI-Interpreter sieht die Vervollständigung von Befehlen und Schlüsselwörtern vor.

Syslog

Das Syslog-Protokoll ermöglicht die Übermittlung von Ereignisbenachrichtigungen an mehrere Remote-Server, wo sich diese speichern und prüfen lassen, damit entsprechend reagiert werden kann.

Informationen über Syslog finden Sie unter "Verwalten von Protokollen".

SNTP

Das Simple Network Time Protocol (SNTP) gewährleistet eine präzise, bis auf die Millisekunde genaue Zeitsynchronisierung der Switch-Uhr im Netzwerk. Die Zeitsynchronisierung erfolgt über einen SNTP-Server des Netzwerks.

Weitere Informationen über SNTP finden Sie unter "Konfigurieren von SNTP-Einstellungen".

Sicherheitsfunktionen

Access Control Lists (ACLs)

Access Control Lists (ACLs) stellen sicher, dass nur autorisierte Benutzer Zugriff auf bestimmte Ressourcen haben, während jegliche unberechtigte Zugriffsversuche auf Netzwerkressourcen abgeblockt werden. ACLs werden für die Verkehrsflusskontrolle, Inhaltsbeschränkungen von Routing-Aktualisierungen und zur Entscheidung darüber eingesetzt, welche Verkehrstypen weitergeleitet oder blockiert werden. In erster Linie sorgen sie damit für Netzwerksicherheit.

Informationen zum Definieren von ACLs finden Sie unter "IP-ACL-Konfiguration" und "MAC-ACL-Konfiguration".

Port-basierte Authentifizierung (802.1x)

Bei Systemen mit port-basierter Authentifizierung erfolgt die Identitätsprüfung der Systembenutzer für jeden einzelnen Port über einen externen Server. Nur überprüfte und zugelassene Systembenutzer dürfen Daten senden und empfangen. Die Port-Authentifizierung erfolgt über einen RADIUS (Remote Authentication Dial In User Service)-Server unter Verwendung des EAP-Protokolls (Extensible Authentication Protocol). PEAP, EAP-TTL, EAP-TTLS und EAP-TLS werden ebenfalls unterstützt.

Port-Sperre

Mit der Funktion zur Port-Sperre wird der Zugriff auf einen Port auf Benutzer mit bestimmten MAC-Adressen beschränkt. Diese Adressen werden manuell definiert oder vom jeweiligen Port automatisch gelernt. Liegt ein Frame an einem gesperrten Port an und ist die MAC-Quelladresse dieses Frame nicht an diesen Port gekoppelt, wird der Schutzmechanismus automatisch aktiviert.

Informationen zum Aktivieren des Sicherheitsmerkmals Port-Sperre finden Sie unter "Port-Sicherheit".

Kennwortverwaltung

Die Kennwortverwaltung sorgt für mehr Netzwerksicherheit sowie eine verbesserte Kennwortkontrolle. Bei den Kennwörtern für den SSH-, Telnet-, HTTP-, HTTPS- und SNMP-Zugang handelt es sich um zugewiesene Sicherheitsfunktionen.

Weitere Informationen über die Kennwortverwaltung finden Sie unter "Kennwortverwaltung".

TACACS+

TACACS+ bietet eine zentrale Sicherheitsfunktionalität für die Validierung von Benutzerzugriffen auf den Switch. TACACS+ stellt ein zentrales Benutzerverwaltungssystem bereit, das jedoch die Konsistenz zu RADIUS und anderen Authentifizierungsprozessen wahrt.

RADIUS-Client

RADIUS ist ein Protokoll auf Client-/Server-Basis, bei dem der Server eine Benutzerdatenbank mit benutzerbezogenen Authentifizierungsinformationen wie Benutzername, Kennwort und Kontendaten vorhält.

SSH/SSL

Secure Shell (SSH) ist ein Protokoll, über das eine geschützte Remote-Verbindung zu einem anderen Gerät hergestellt werden kann. Über diese Verbindung wird eine Funktionalität bereitgestellt, die mit einer eingehenden Telnet-Verbindung vergleichbar ist.

Das SSL- (Secure Sockets Layer) Protokoll stellt ein Mittel dar, um die Verbindungsverschlüsselung zwischen zwei Stationen separat abzuwickeln. Wenn die Verbindung einmal aufgebaut ist, kann sie praktisch wie eine ungesicherte Verbindung verwendet werden.

CLI-Dokumentation

Eine weitere Informationsquelle für die Dell™ PowerConnect™ 6200-Reihe ist der *CLI Reference Guide* (CLI-Referenzhandbuch). Dieses Handbuch liefert Informationen über die CLI-Befehle, die für die Konfiguration und Verwaltung von Switch und Stack verwendet werden. Das Dokument enthält detaillierte CLI-Beschreibungen, einschließlich Syntax, Standardwerte und Beispiele.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Benutzerhandbuch für die Dell™ PowerConnect™ 6200-Reihe

Modelle PC6224, PC6248, PC6224P, PC6248P und PC6224F

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie das System besser einsetzen können.

HINWEIS: Ein HINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und informiert darüber, wie dies zu vermeiden ist.

VORSICHT: Hiermit werden Sie auf eine potentiell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen könnte.

Irrtümer und technische Änderungen vorbehalten.
© 2007 Dell Inc. Alle Rechte vorbehalten.

Die Vervielfältigung oder Wiedergabe in jeglicher Weise ohne vorherige schriftliche Genehmigung von Dell Inc. sind strengstens untersagt.

In diesem Text verwendete Marken: *Dell*, *Dell OpenManage*, das *DELL* Logo, *Inspiron*, *Dell Precision*, *Dimension*, *OptiPlex*, *PowerConnect*, *PowerApp*, *PowerVault*, *Axim*, *DellNet* und *Latitude* sind Marken von Dell Inc.; *Microsoft*, *Windows* und *Windows Vista* sind Marken oder eingetragene Marken von Microsoft Corporation in den USA und/oder anderen Ländern. *Procomm Plus* ist eine eingetragene Marke von Symantec Corporation oder ihren Tochtergesellschaften in den USA und anderen Ländern.

Alle anderen in dieser Dokumentation genannten Marken und Handelsbezeichnungen sind Eigentum der jeweiligen Hersteller und Firmen. Dell Inc. erhebt keinen Anspruch auf Besitzrechte an Marken und Handelsbezeichnungen mit Ausnahme der eigenen.

Modelle PC6224, PC6248, PC6224P, PC6248P und PC6224F

September 2007 Rev. A00

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Anzeigen von Statistiken / RMON

Benutzerhandbuch für die Dell™ PowerConnect™ 6200-Reihe

- Tabellenansichten
- RMON
- Diagramme

Remote Monitoring (RMON) vermittelt dem Netzwerkadministrator eine Vorstellung von der Leistung und dem Zustand des Netzwerks über einen Remote-Zugang. Im Rahmen des RMON-Standards werden vier Überwachungsgruppen unterstützt: Statistik, Verlauf, Alarme und Ereignisse.

In diesem Abschnitt werden die RMON-Optionen erläutert, auf die von der Menüseite **Statistics / RMON** (Statistiken/RMON)) zugegriffen werden kann. Die Optionen umfassen unter anderem die Anzeige von Statistiken in Tabellenform, die Bearbeitung und Anzeige von RMON-Statistiken und die Diagrammerstellung zu Port- und LAG-Statistiken. Von der Menüseite **Statistics / RMON** (Statistiken/RMON) kann auf diese Optionen über die folgenden Menüseiten zugegriffen werden:

- Tabellenansichten
- RMON
- Diagramme

ANMERKUNG: Für die Statistik-/RMON-Seiten sind keine CLI-Befehle verfügbar.

Tabellenansichten

Die Menüseite **Table Views** (Tabellenansichten) enthält Links auf Webseiten, die Statistiken in Tabellenform anzeigen. Klicken Sie zur Anzeige dieser Seite in der Strukturansicht auf **Statistics / RMON (Statistiken / RMON)→ Table Views (Tabellenansichten)**. Von dieser Menüseite können Webseiten für Folgendes aufgerufen werden:

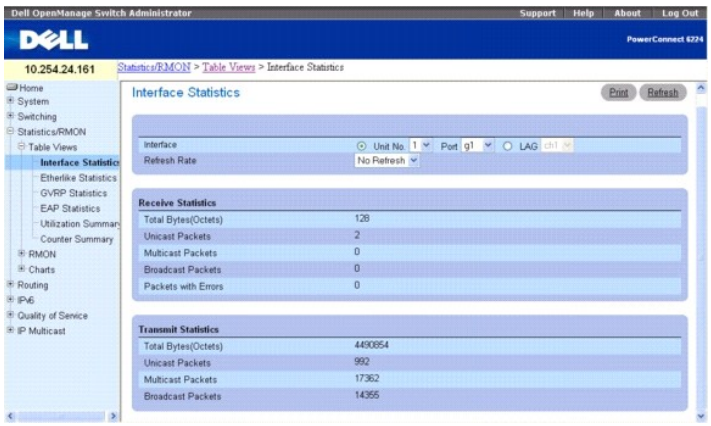
- Schnittstellenstatistiken
- Etherlike-Statistiken
- GVRP-Statistiken
- EAP-Statistiken
- Nutzungsübersicht
- Zählerübersicht

Schnittstellenstatistiken

Verwenden Sie die Seite **Interface Statistics** (Schnittstellenstatistiken), um Statistiken sowohl für empfangene als auch gesendete Pakete anzuzeigen. Die Felder für empfangene und gesendete Datenpakete sind identisch.

Klicken Sie zur Anzeige der Seite in der Strukturansicht auf **Statistics / RMON (Statistiken / RMON)→ Table Views (Tabellenansichten)→ Interface Statistics (Schnittstellenstatistiken)**.

Abbildung 9-1. Schnittstellenstatistiken



Die Seite **Interface Statistics** (Schnittstellenstatistiken) enthält folgende Felder:

Interface (Schnittstelle) – Zur Auswahl der physikalischen Schnittstelle (Einheit, Port) oder der LAG-Schnittstelle, für die Statistiken angezeigt werden sollen.

Refresh Rate (Aktualisierungsrate) – Zur Vorgabe des Zeitraums bis zur Aktualisierung der Statistiken. Die Feldwerte No Refresh (Keine Aktualisierung) sowie 15, 30 und 60 Sekunden sind möglich. Die Standardeinstellung ist No Refresh (Keine Aktualisierung).

Received Statistics (Empfangsstatistiken)

Total Bytes (Octets) (Gesamt Bytes (Oktette)) – Zeigt die Gesamtzahl der über die ausgewählte Schnittstelle empfangenen Oktette an.

Unicast Packets (Unicast-Pakete) – Zeigt die Gesamtzahl der über die ausgewählte Schnittstelle empfangenen Unicast-Pakete an.

Multicast Packets (Multicast-Pakete) – Zeigt die Gesamtzahl der über die ausgewählte Schnittstelle empfangenen Multicast-Pakete an.

Broadcast Packets (Broadcast-Pakete) – Zeigt die Gesamtzahl der über die ausgewählte Schnittstelle empfangenen Broadcast-Pakete an.

Packets with Errors (Fehlerhafte Pakete) – Zeigt die Gesamtzahl der über die ausgewählte Schnittstelle empfangenen fehlerhaften Pakete an.

Transmit Statistics (Sendestatistiken)

Total Bytes (Octets) (Gesamt Bytes (Oktette)) – Zeigt die Gesamtzahl der über die ausgewählte Schnittstelle gesendeten Oktette an.

Unicast Packets (Unicast-Pakete) – Zeigt die Gesamtzahl der über die ausgewählte Schnittstelle gesendeten Unicast-Pakete an.

Multicast Packets (Multicast-Pakete) – Zeigt die Gesamtzahl der über die ausgewählte Schnittstelle gesendeten Multicast-Pakete an.

Broadcast Packets (Broadcast-Pakete) – Zeigt die Gesamtzahl der über die ausgewählte Schnittstelle gesendeten Broadcast-Pakete an.

Anzeigen von Schnittstellenstatistiken

1. Öffnen Sie die Seite **Interface Statistics** (Schnittstellenstatistiken).
2. Geben Sie eine Schnittstelle an.

   Die Statistiken für die angegebene Schnittstelle werden angezeigt.

Anzeigen von Schnittstellenstatistiken mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- Ethernet Configuration Commands (Befehle zur Ethernet-Konfiguration)

Etherlike-Statistiken

Verwenden Sie die Seite **Etherlike Statistics** (Etherlike-Statistiken) zur Anzeige von Etherlike-Statistiken.

Klicken Sie zur Anzeige der Seite in der Strukturansicht auf **Statistics/RMON (Statistiken/RMON)→ Table Views (Tabellenansichten)→ Etherlike Statistics (Etherlike-Statistiken)**.

Abbildung 9-2. Etherlike-Statistiken

Die Seite **Etherlike Statistics** (Etherlike-Statistiken) enthält folgende Felder:

Interface (Schnittstelle) – Zur Auswahl der physikalischen Schnittstelle (Einheit, Port) oder der LAG-Schnittstelle, für die Statistiken angezeigt werden sollen.

Refresh Rate (Aktualisierungsrate) – Zur Vorgabe des Zeitraums bis zur Aktualisierung der Statistiken. Die Feldwerte No Refresh (Keine Aktualisierung) sowie 15, 30 und 60 Sekunden sind möglich. Die Standardeinstellung ist No Refresh (Keine Aktualisierung).

Frame Check Sequence (FCS) Errors (Frame Check Sequence-(FCS-)Fehler) – Zeigt die Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen FCS-Fehler an.

Signal Collision Frames (Frame-Signal-Kollisionen) – Zeigt die Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen Frame-Signal-Kollisionen an.

Late Collisions (Verspätete Kollisionen) – Zeigt die Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen verspäteten Kollisionen an.

Excessive Collisions (Übermäßige Kollisionen) – Zeigt die Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen übermäßigen Kollisionen an.

Internal MAC Transmit Errors (Interne MAC-Übertragungsfehler) – Zeigt die Anzahl interner MAC-Übertragungsfehler an der ausgewählten Schnittstelle an.

Oversize Packets (Zu große Pakete) – Zeigt die Gesamtzahl der empfangenen Pakete an, die länger als 1518 Oktette waren (ausschließlich Synchronisierbits, aber einschließlich FCS-Oktette), andererseits jedoch in Ordnung.

Internal MAC Receive Errors (Interne MAC-Empfangsfehler) – Zeigt die Anzahl interner MAC-Empfangsfehler an der ausgewählten Schnittstelle an.

Received Pause Frames (Angehaltene Frames beim Empfang) – Zeigt die Anzahl der beim Empfang über die ausgewählte Schnittstelle angehaltenen Frames an.

Transmitted Pause Frames (Angehaltene Frames beim Senden) – Zeigt die Anzahl der beim Senden über die ausgewählte Schnittstelle angehaltenen Frames an.

Anzeigen von Etherlike-Statistiken für eine Schnittstelle

1. Öffnen Sie die Seite **Etherlike Statistics** (Etherlike-Statistiken).
2. Geben Sie eine Schnittstelle an.

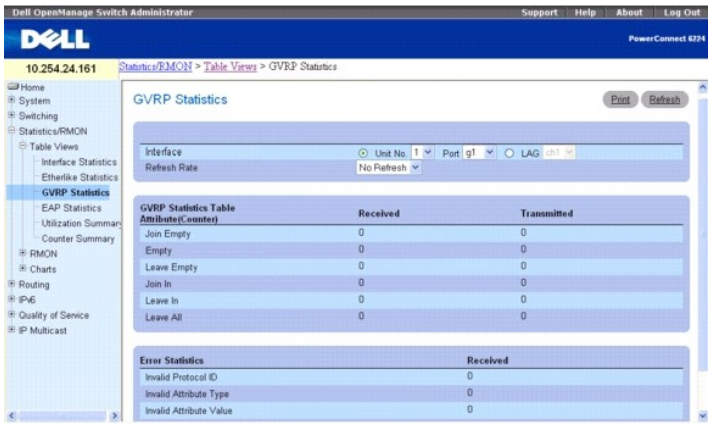
   Die Statistiken für die angegebene Schnittstelle werden angezeigt.

GVRP-Statistiken

Verwenden Sie die Seite **GVRP Statistics** zur Anzeige von Switch-Statistiken für GVRP.

Klicken Sie zur Anzeige der Seite in der Strukturansicht auf **Statistics/RMON (Statistiken/RMON)**→ **Table Views (Tabellenansichten)**→ **GVRP Statistics (GVRP-Statistiken)**.

Abbildung 9-3. GVRP-Statistiken



Die Seite **GVRP Statistics** (GVRP-Statistiken) enthält folgende Felder:

Interface (Schnittstelle) – Zur Auswahl der physikalischen Schnittstelle (Einheit, Port) oder der LAG-Schnittstelle, für die Statistiken angezeigt werden sollen.

Refresh Rate (Aktualisierungsrate) – Zur Vorgabe des Zeitraums bis zur Aktualisierung der Statistiken. Die Feldwerte No Refresh (Keine Aktualisierung) sowie 15, 30 und 60 Sekunden sind möglich. Die Standardeinstellung ist No Refresh (Keine Aktualisierung).

GVRP Statistics Table (GVRP-Statistiktabelle) Attribute (Counters) (Attribut (Zähler)) - Received (Empfangen) und Transmitted (Gesendet)

Join Empty – Zeigt switch-spezifische GVRP Join Empty-Statistik an.

Empty – Zeigt switch-spezifische GVRP Empty-Statistik an.

Leave Empty – Zeigt switch-spezifische GVRP Leave Empty-Statistik an.

Join In – Zeigt switch-spezifische GVRP Join In-Statistik an.

Leave In – Zeigt switch-spezifische GVRP Leave In-Statistik an.

Leave All – Zeigt switch-spezifische GVRP Leave All-Statistik an.

Error Statistics (Fehlerstatistiken) – **Received (Empfangen)**

Invalid Protocol ID (Ungültige Protokoll-ID) – Zeigt GVRP-Switch-Statistik zu ungültigen Protokoll-IDs an.

Invalid Attribute Type (Ungültiger Attributtyp) – Zeigt GVRP-Switch-Statistik zu ungültigen Attributtypen an.

Invalid Attribute Value (Ungültiger Attributwert) – Zeigt GVRP-Switch-Statistik zu ungültigen Attributwerten an.

Invalid Attribute Length (Ungültige Attributlänge) – Zeigt GVRP-Switch-Statistik zu ungültigen Attributlängen an.

Invalid Event (Ungültige Ereignisse) – Zeigt GVRP-Switch-Statistik zu ungültigen Ereignissen an.

Anzeigen von GVRP-Statistiken für eine Schnittstelle

1. Öffnen Sie die Seite **GVRP Statistics** (GVRP-Statistiken).
2. Wählen Sie im Feld Interface (Schnittstelle) eine Schnittstelle aus.

   Die GVRP-Statistiken für die angegebene Schnittstelle werden angezeigt.

Anzeigen von GVRP-Statistiken mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

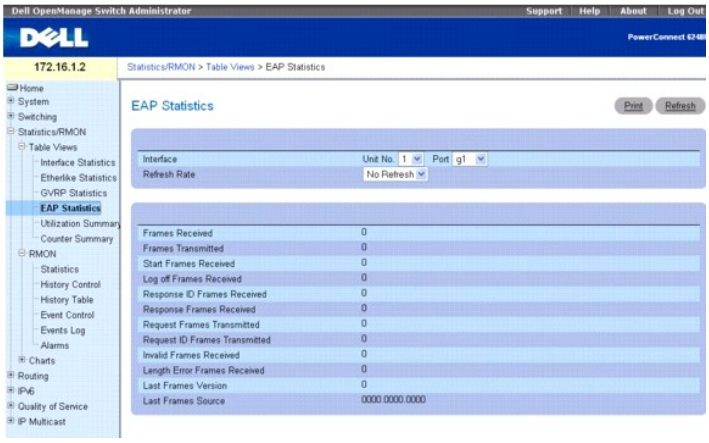
- GVRP Commands (GVRP-Befehle)

EAP-Statistiken

Verwenden Sie die Seite **EAP Statistics** (EAP-Statistiken), um Informationen über EAP-Pakete anzuzeigen, die an einem bestimmten Port empfangen wurden. Weitere Informationen über EAP finden Sie unter "Port-basierte Authentifizierung".

Zur Anzeige der Seite **EAP Statistics (EAP-Statistiken)** klicken Sie in der Strukturansicht auf **Statistics/RMON (Statistiken/RMON)**→ **Table Views (Tabellenansichten)**→ **EAP Statistics (EAP-Statistiken)**.

Abbildung 9-4. EAP-Statistiken



Interface (Schnittstelle) – Gibt an, von welcher Schnittstelle Statistikdaten abgerufen werden.

Refresh Rate (Aktualisierungsrate) – Zur Vorgabe des Zeitraums bis zur Aktualisierung der Statistiken. Die Feldwerte No Refresh (Keine Aktualisierung) sowie 15, 30 und 60 Sekunden sind möglich. Die Standardeinstellung ist No Refresh (Keine Aktualisierung).

Frames Received (Empfangene Frames) – Zeigt die Anzahl der port-seitig empfangenen gültigen EAPOL-Frames an.

Frames Transmitted (Gesendete Frames) – Zeigt die Anzahl der über den Port übertragenen EAPOL-Frames an.

Start Frames Received (Empfangene Start-Frames) – Zeigt die Anzahl der port-seitig empfangenen EAPOL-Start-Frames an.

Log off Frames Received (Empfangene Abmelde-Frames) – Zeigt die Anzahl der port-seitig empfangenen EAPOL-Abmelde-Frames an.

Respond ID Frames Received (Empfangene Antwort-ID-Frames) – Zeigt die Anzahl der port-seitig empfangenen EAP-Antwort-ID-Frames an.

Respond Frames Received (Empfangene Antwort-Frames) – Zeigt die Anzahl der port-seitig empfangenen gültigen EAP-Antwort-Frames an.

Request ID Frames Received (Empfangene Anforderungs-Frames) – Zeigt die Anzahl der port-seitig empfangenen EAP-Anforderungs-ID-Frames an.

Request Frames Transmitted (Gesendete Anforderungs-Frames) – Zeigt die Anzahl der über den Port übertragenen EAP-Anforderungs-Frames an.

Request ID Frames Transmitted (Gesendete Anforderungs-ID-Frames) – Zeigt die Anzahl der über den Port übertragenen EAP-Anforderungs-ID-Frames an.

Invalid Frames Received (Empfangene ungültige Frames) – Zeigt die Anzahl der port-seitig empfangenen nicht erkannten Frames an.

Length Error Frames Received (Empfangene Frames ungültiger Länge) – Zeigt die Anzahl der port-seitig empfangenen EAPOL-Frames mit einer ungültigen Paketkörperlänge an.

Last Frames Version (Version letzter Frame) – Zeigt die Protokollversionsnummer für den zuletzt empfangenen EAPOL-Frame an.

Last Frames Source (Quelle letzter Frame) – Zeigt die MAC-Quelladresse für den zuletzt empfangenen EAPOL-Frame an.

Anzeigen der EAP-Statistiken für eine Schnittstelle

1. Öffnen Sie die Seite **EAP Statistics** (EAP-Statistiken).
2. Wählen Sie im Feld **Interface** (Schnittstelle) eine Schnittstelle aus.

   Die EAP-Statistiken für die ausgewählte Schnittstelle werden angezeigt.

Anzeigen von EAP-Statistiken mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

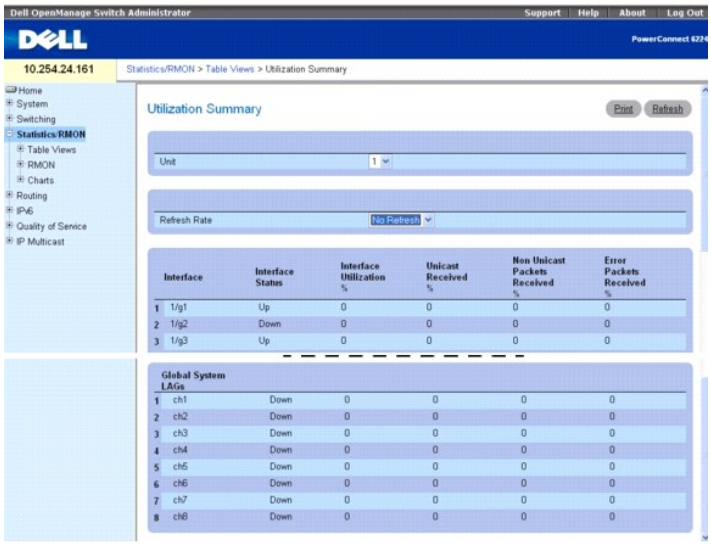
- 802.1X Commands (802.1X-Befehle)

Nutzungsübersicht

Verwenden Sie die Seite **Utilization Summary** (Nutzungsübersicht), um Statistiken zur Schnittstellennutzung anzuzeigen.

Klicken Sie zur Anzeige dieser Seite in der Strukturansicht auf **Statistics/RMON (Statistiken/RMON)** → **Table Views (Tabellenansichten)**→ **Utilization Summary** (Nutzungsübersicht).

Abbildung 9-5. Nutzungsübersicht



Die Seite **Utilization Summary** (Nutzungsübersicht) enthält folgende Felder:

Unit (Einheit) – Gibt die Einheit an, für die die Statistiken angezeigt werden.

Refresh Rate (Aktualisierungsrate) – Zur Vorgabe des Zeitraums bis zur Aktualisierung der Statistiken. Die Feldwerte No Refresh (Keine Aktualisierung) sowie 15, 30 und 60 Sekunden sind möglich. Die Standardeinstellung ist No Refresh (Keine Aktualisierung).

Interface (Schnittstelle) – Gibt die Schnittstelle an, für die die Statistiken angezeigt werden.

Interface Status (Schnittstellenstatus) – Zeigt den Status der Schnittstelle an.

Interface Utilization % (Schnittstellennutzung %) – Zeigt die prozentuale Auslastung der Netzwerkschnittstelle im Duplex-Modus an. Der hier angezeigte Wert kann zwischen 0 und 200 % liegen. Der maximale Anzeigewert für eine Vollduplex-Verbindung (200 %) signalisiert, dass die gesamte Bandbreite der ein- und ausgehenden Verbindungen für den Datenverkehr über diese Schnittstelle belegt ist. Der maximale Anzeigewert für eine Halbduplex-Verbindung ist 100 %.

Unicast Received % (Unicast empfangen %) – Zeigt den prozentualen Anteil der schnittstellenseitig empfangenen Unicast-Pakete an.

Non Unicast Packets Received % (Sonstige empfangen %) – Zeigt den prozentualen Anteil der schnittstellenseitig empfangenen sonstigen Datenpakete (nicht Unicast) an.

Error Packets Received % (Fehlerhafte Pakete empfangen %) – Zeigt den prozentualen Anteil der schnittstellenseitig empfangenen fehlerhaften Datenpakete an.

Anzeigen von Statistiken zur Schnittstellenauslastung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

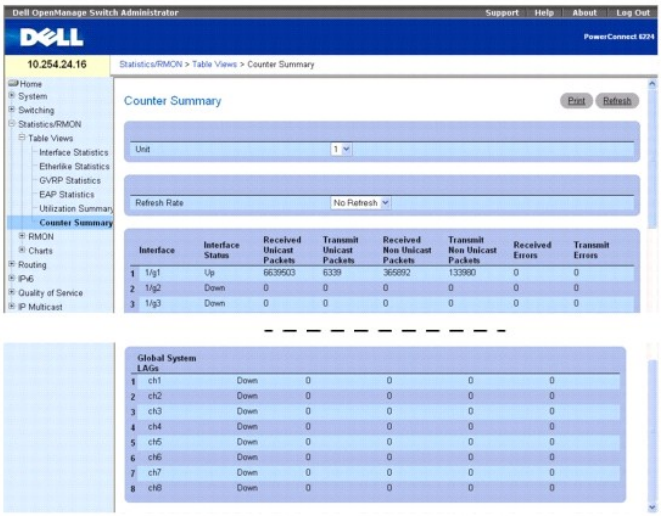
- RMON Commands (RMON-Befehle)

Zählerübersicht

Verwenden Sie die Seite **Counter Summary (Zählerübersicht)** zur Anzeige von Statistiken zur Schnittstellenauslastung in numerischen Summen statt in Prozentwerten.

Klicken Sie zur Anzeige der Seite in der Strukturansicht auf **Statistics/RMON (Statistiken/RMON)**→ **Table Views (Tabellenansichten)**→ **Counter Summary (Zählerübersicht)**.

Abbildung 9-6. Zählerübersicht



Die Seite **Counter Summary** (Zählerübersicht) enthält folgende Felder:

Unit (Einheit) – Gibt die Einheit an, für die die Statistiken angezeigt werden.

Refresh Rate (Aktualisierungsrate) – Zur Vorgabe des Zeitraums bis zur Aktualisierung der Statistiken. Die Feldwerte No Refresh (Keine Aktualisierung) sowie 15, 30 und 60 Sekunden sind möglich. Die Standardeinstellung ist No Refresh (Keine Aktualisierung).

Interface (Schnittstelle) – Gibt die Schnittstelle an, für die die Statistiken angezeigt werden.

Interface Status (Schnittstellenstatus) – Zeigt den Status der Schnittstelle an.

Received Unicast Packets (Empfangene Unicast-Pakete) – Zeigt die Anzahl der schnittstellenseitig empfangenen Unicast-Pakete an.

Transmit Unicast Packets (Gesendete Unicast-Pakete) – Zeigt die Anzahl der über die Schnittstelle gesendeten Unicast-Pakete an.

Received Non Unicast Packets (Empfangene Nicht-Unicast-Pakete) – Zeigt die Anzahl der schnittstellenseitig empfangenen Nicht-Unicast-Pakete an.

Transmit Non Unicast Packets (Gesendete Nicht-Unicast-Pakete) – Zeigt die Anzahl der über die Schnittstelle gesendeten Nicht-Unicast-Pakete an.

Received Errors (Empfangene fehlerhafte Pakete) – Zeigt die Anzahl der schnittstellenseitig empfangenen fehlerhaften Datenpakete an.

Transmit Errors (Gesendete fehlerhafte Pakete) – Zeigt die Anzahl der über die Schnittstelle gesendeten fehlerhaften Datenpakete an.

Einstellen der Aktualisierungsrate

1. Öffnen Sie die Seite **Counter Summary** (Zählerübersicht).
2. Wählen Sie die **Refresh Rate** (Aktualisierungsrate) aus dem Dropdown-Menü.

   Die Statistiken für die angezeigte Schnittstelle werden mit der gewählten Frequenz aktualisiert.

Anzeigen von numerischen Statistiken zur Schnittstellenauslastung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- RMON Commands (RMON-Befehle)

RMON

Remote Monitoring (RMON) vermittelt dem Netzwerkadministrator eine Vorstellung von der Leistung und dem Zustand des Netzwerks über einen Remote-Zugang.

Klicken Sie zur Anzeige der Menüseite **RMON** in der Strukturansicht auf **Statistics/RMON (Statistiken/RMON)→ RMON**. Die Menüseite **RMON** enthält Links zu den folgenden Funktionen:

- RMON-Statistiken
- Statistiken der RMON-Verlaufssteuerung

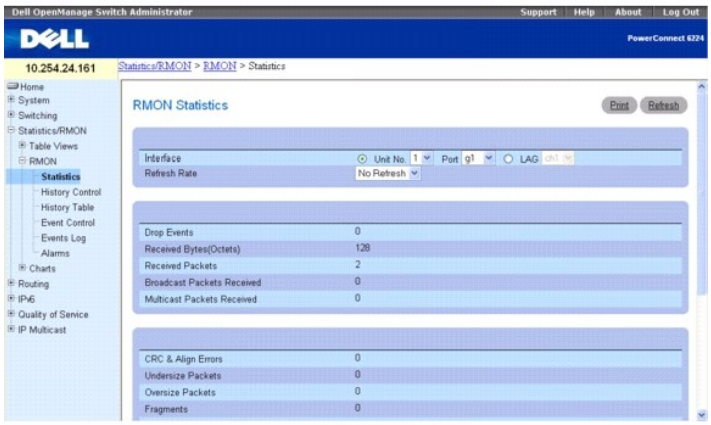
- RMON-Verlaufstabelle
- RMON-Ereignissteuerung
- RMON-Ereignisprotokoll
- RMON-Alarme

RMON-Statistiken

Verwenden Sie die Seite **RMON Statistics** (RMON-Statistiken), um Details zur Switch-Nutzung, z. B. Statistiken zur Paketverarbeitung und am Switch aufgetretene Fehler, anzuzeigen.

Klicken Sie zur Anzeige der Seite in der Strukturansicht auf **Statistics/RMON (Statistiken/RMON)**→ **RMON**→ **Statistics (Statistiken)**.

Abbildung 9-7. RMON-Statistiken



Die Seite **RMON Statistics** (RMON-Statistiken) enthält folgende Felder:

Interface (Schnittstelle) – Gibt an, ob Statistiken für eine Einheit oder eine LAG angezeigt werden und welche Einheit/LAG angezeigt wird.

Refresh Rate (Aktualisierungsrate) – Zur Vorgabe des Zeitraums bis zur Aktualisierung der Statistiken. Die Feldwerte No Refresh (Keine Aktualisierung) sowie 15, 30 und 60 Sekunden sind möglich. Die Standardeinstellung ist No Refresh (Keine Aktualisierung).

Drop Events (Ablehnungsereignisse) – Zeigt die Anzahl der Ereignisse an, die seit der letzten Aktualisierung des Switch an der Schnittstelle abgewiesen wurden.

Received Bytes (Octets) (Empfangene Bytes (Oktetts)) – Zeigt die Anzahl der Oktette an, die seit der letzten Aktualisierung des Switch an der Schnittstelle empfangen wurden. Diese Zahl schließt ungültige Pakete und FCS-Oktetts ein, nicht aber Synchronisierbits.

Received Packets (Empfangene Pakete) – Zeigt die Anzahl der an der Schnittstelle empfangenen Pakete seit der letzten Aktualisierung des Switch an, einschließlich ungültiger Pakete sowie Multicast- und Broadcast-Pakete.

Broadcast Packets Received (Empfangene Broadcast-Pakete) – Zeigt die Anzahl der schnittstellenseitig empfangenen gültigen Broadcast-Pakete seit der letzten Aktualisierung des Switch an. Diese Zahl beinhaltet keine Multicast-Pakete.

Multicast Packets Received (Empfangene Multicast-Pakete) – Zeigt die Anzahl der schnittstellenseitig empfangenen gültigen Multicast-Pakete seit der letzten Aktualisierung des Switch an.

CRC & Align Errors (CRC- und Align-Fehler) – Zeigt die Anzahl der CRC- und Align-Fehler an, die seit der letzten Aktualisierung des Switch an der Schnittstelle aufgetreten sind.

Undersize Packets (Kleine Pakete) – Zeigt die Anzahl der Pakete unter Normalgröße (weniger als 64 Oktette) an, die seit der letzten Aktualisierung des Switch an der Schnittstelle eingegangen sind.

Oversize Packets (Große Pakete) – Zeigt die Anzahl der Pakete über Normalgröße (mehr als 1518 Oktette) an, die seit der letzten Aktualisierung des Switch an der Schnittstelle eingegangen sind.

Fragments (Fragmente) – Zeigt die Anzahl der Fragmente (Pakete mit weniger als 64 Oktetten, ohne Synchronisierbits, aber einschließlich FCS-Oktetten) an, die seit der letzten Aktualisierung des Switch an der Schnittstelle eingegangen sind.

Jabbers – Zeigt die Anzahl der empfangenen Pakete mit einer Länge über 1.518 Oktette an, für die während der Stichprobensitzung eine Frame-Prüfsequenz generiert wurde.

Collisions (Kollisionen) – Zeigt die Anzahl der Kollisionen an, die seit der letzten Aktualisierung des Switch an der Schnittstelle registriert wurden.

Frames of 64 Bytes (Frames mit 64 Bytes) – Zeigt die Anzahl der *64*-Byte-Frames an, die seit der letzten Aktualisierung des Switch an der Schnittstelle eingegangen sind.

Frames of 65 to 127 Bytes (Frames mit 65 bis 127 Bytes) – Zeigt die Anzahl der Frames mit 65 bis 127 Bytes an, die seit der letzten Aktualisierung des Switch an der Schnittstelle eingegangen sind.

Frames of 128 to 255 Bytes (Frames mit 128 bis 255 Bytes) – Zeigt die Anzahl der Frames mit *128 bis 255* Bytes an, die seit der letzten Aktualisierung des Switch an der Schnittstelle eingegangen sind.

Frames of 256 to 511 Bytes (Frames mit 256 bis 511 Bytes) – Zeigt die Anzahl der Frames mit *256 bis 511* Bytes an, die seit der letzten Aktualisierung des Switch an der Schnittstelle eingegangen sind.

Frames of 512 to 1023 Bytes (Frames mit 512 bis 1023 Bytes) – Zeigt die Anzahl der Frames mit *512 bis 1023* Bytes an, die seit der letzten Aktualisierung des Switch an der Schnittstelle eingegangen sind.

Frames of 1024 to 1518 Bytes (Frames mit 1024 bis 1518 Bytes) – Zeigt die Anzahl der Frames mit *1024 bis 1518* Bytes an, die seit der letzten Aktualisierung des Switch an der Schnittstelle eingegangen sind.

Anzeigen von Schnittstellenstatistiken

1. Öffnen Sie die Seite **RMON Statistics Group** (RMON-Statistikgruppe).
2. Wählen Sie im Feld **Interface** (Schnittstelle) eine Schnittstelle aus.

   Die Statistiken für die gewählte Schnittstelle werden angezeigt.

Anzeigen von RMON-Statistiken mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

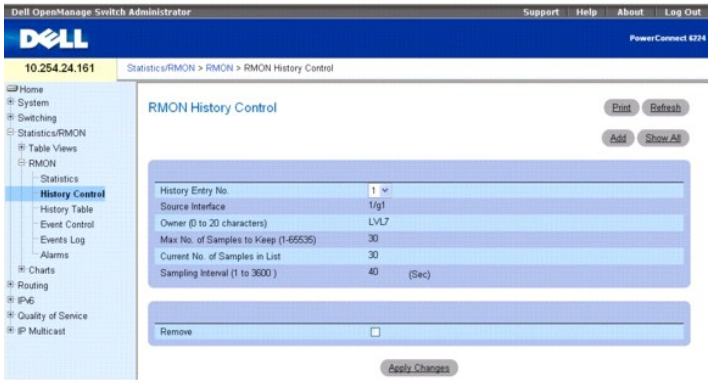
- RMON Commands (RMON-Befehle)

Statistiken der RMON-Verlaufssteuerung

Verwenden Sie die Seite **RMON History Control** (RMON-Verlaufssteuerung), um Statistikverlaufsdaten für jeden Port vorzuhalten. Sie können für jede Schnittstelle (einem physikalischen Port oder einem Port-Kanal) festlegen, wie viele Buckets vorliegen, und das Zeitintervall zwischen den einzelnen Bucket-Snapshots definieren.

Klicken Sie zur Anzeige der Seite in der Strukturansicht auf **Statistics/RMON (Statistiken/RMON)**→ **RMON**→ **History Control (Verlaufssteuerung)**.

Abbildung 9-8. RMON-Verlaufssteuerung



Die Seite **RMON History Control enthält folgende Felder:**

New History Entry (Neuer Verlaufseintrag) – Zur Auswahl der Eintragsnummer in der **RMON-Verlaufssteuerungstabelle**.

Source Interface (Quellschnittstelle) – Gibt die Schnittstelle an, von der die Verlaufsstichproben erfasst werden.

Owner (0-20 characters) (Besitzer, 0-20 Zeichen) – Gibt die RMON-Station bzw. den Benutzer an, die/der die RMON-Informationen angefordert hat.

Max No. of Samples to Keep (1-65535) (Max. Anzahl Einträge, 1-65535) – Zur Einstellung der Anzahl von Verlaufs-Buckets für diese Schnittstelle.

Current No. of Samples in List (Aktuelle Anzahl Stichproben) – Zeigt die Anzahl der derzeit erfassten Stichproben an.

Sampling Interval (1-3600) (Stichprobenintervall, 1-3600) – Zur Einstellung der Frequenz, mit der Stichproben von den Ports erfasst werden. Die möglichen Werte liegen zwischen 1 und 3.600 Sekunden. Der Standardwert ist 1.800 Sekunden (30 Minuten).

Remove (Entfernen) – Wenn diese Option aktiviert ist, wird der angezeigte Eintrag aus der **RMON-Verlaufssteuerungstabelle** entfernt.

Hinzufügen eines Verlaufssteuerungseintrags

1. Öffnen Sie die Seite **RMON History Control** (RMON-Verlaufssteuerung).
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add History Entry** (Verlaufseintrag hinzufügen) wird angezeigt.

Abbildung 9-9. Verlaufseintrag hinzufügen

3. Konfigurieren Sie die Felder auf dieser Seite, und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

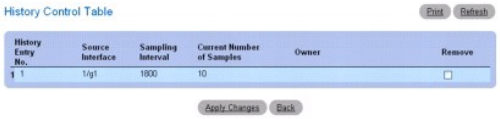
   Der Eintrag wird in die **RMON-Verlaufssteuerungstabelle** aufgenommen.

Anzeigen der RMON-Verlaufssteuerungstabelle

1. Öffnen Sie die Seite **RMON History Control** (RMON-Verlaufssteuerung).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **RMON-Verlaufssteuerungstabelle** wird angezeigt.

Abbildung 9-10. RMON-Verlaufssteuerungstabelle



Entfernen eines Eintrags aus der Verlaufssteuerungstabelle

1. Öffnen Sie die Seite **RMON History Control** (RMON-Verlaufssteuerung).
2. Aktivieren Sie in der Zeile des Verlaufseintrags, der entfernt werden soll, das Kontrollkästchen **Remove** (Entfernen).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Tabelleneintrag wird entfernt und das Gerät aktualisiert.

Anzeigen der RMON-Verlaufssteuerung mit Hilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

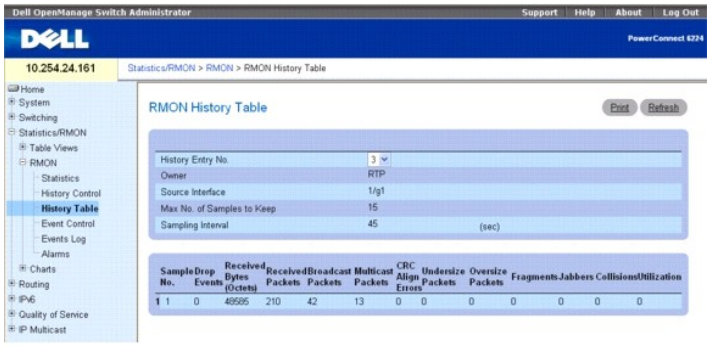
- RMON Commands (RMON-Befehle)

RMON-Verlaufstabelle

Verwenden Sie die Seite mit der RMON-Verlaufstabelle zur Anzeige statistischer schnittstellenspezifischer Netzwerkmesswerte. Jeder Tabelleneintrag repräsentiert alle während einer einzelnen Stichprobe erfassten Zählerwerte.

Klicken Sie zur Anzeige der Seite **RMON History Table** (RMON-Verlaufstabelle) in der Strukturansicht auf **Statistics/RMON (Statistiken/RMON)→ RMON→ History Table (Verlaufstabelle)**.

Abbildung 9-11. RMON-Verlaufstabelle



Die Seite **RMON History Table (RMON-Verlaufstabelle) enthält folgende Felder:**

History Entry No. (Nummer Verlaufseintrag) – Zur Auswahl der Nummer des Verlaufseintrags, der in der RMON **History Table** (RMON-Verlaufstabelle) angezeigt werden soll.

Owner (Besitzer) – Zeigt den Namen des Verantwortlichen für die RMON-Statistikgruppe an, falls zutreffend.

Source Interface (Quell-Schnittstelle) – Zeigt die Schnittstelle oder LAG an, an der die Statistiken erfasst werden.

Max No. of Samples to Keep (Max. Anzahl Stichproben) – Legt die Länge der Verlaufsliste für jede Verlaufseintragsnummer fest.

Sampling Interval (Stichprobenintervall) – Legt den Zeitabstand zwischen aufeinanderfolgenden Stichproben (in Sekunden) fest.

Sample No. (Stichprobennummer) – Gibt die jeweilige Stichprobe an, die die Informationen in der Tabelle darstellen.

Drop Events (Ablehnungsereignisse) – Zeigt die Gesamtzahl der Ereignisse an, bei denen Pakete aufgrund fehlender Ressourcen vom Port verworfen wurden. Beachten Sie, dass diese Zahl nicht unbedingt die Anzahl der verworfenen Pakete wiedergibt. Es handelt sich dabei lediglich um die Häufigkeit, mit der dieser Zustand entdeckt wurde.

Received Bytes (Octets) (Empfangene Bytes (Oktetts)) – Zeigt die Gesamtzahl der Daten-Oktette (einschließlich jener in fehlerhaften Paketen) an, die im Netzwerk empfangen wurden, einschließlich Synchronisierbits aber ohne FCS- (Frame Check Sequence) Oktette.

Received Packets (Empfangene Pakete) – Zeigt die Gesamtzahl der während des Erfassungsintervalls empfangenen Pakete an (einschließlich fehlerhafter Pakete, Broadcast-Pakete und Multicast-Pakete).

Broadcast Packets (Broadcast-Pakete) – Zeigt die Gesamtzahl fehlerfreier empfangener Pakete an, die an die Broadcast-Adresse übermittelt wurden. Beachten Sie, dass diese Zahl keine Multicast-Pakete beinhaltet.

Multicast Packets (Multicast-Pakete) – Zeigt die Gesamtzahl fehlerfreier empfangener Pakete an, die an eine Multicast-Adresse übermittelt wurden. Beachten Sie, dass diese Zahl keine Pakete beinhaltet, die an die Broadcast-Adresse übermittelt wurden.

CRC Align Errors (CRC-/Align-Fehler) – Zeigt die Gesamtzahl der empfangenen Pakete mit einer Länge zwischen 64 und 1518 Oktetten (ausschließlich Synchronisierbits, aber mit FCS-Oktetten) an, die entweder eine ungültige FCS mit einer Ganzzahl von Oktetten (FCS-Fehler) oder eine ungültige FCS mit einer nicht-ganzzahligen Anzahl von Oktetten (Ausrichtungsfehler) aufwiesen.

Undersize Packets (Zu kleine Pakete) – Zeigt die Gesamtzahl der empfangenen Pakete an, die kürzer als 64 Oktette waren (ausschließlich Synchronisierbits, aber einschließlich FCS-Oktette), andererseits jedoch in Ordnung.

Oversize Packets (Zu große Pakete) – Zeigt die Gesamtzahl der empfangenen Pakete an, die länger als 1518 Oktette waren (ausschließlich Synchronisierbits, aber einschließlich FCS-Oktette), andererseits jedoch in Ordnung.

Fragments (Fragmente) – Zeigt die Gesamtzahl der empfangenen Pakete an, die kürzer als 64 Oktette waren (ohne Synchronisierbits aber mit FCS) und eine Ganzzahl von Oktetten aufwiesen (FCS-Fehler) bzw. eine ungültige FCS mit einer nicht-ganzzahligen Anzahl von Oktetten (Ausrichtungsfehler).

Jabbers – Zeigt die Gesamtzahl der empfangenen Pakete an, die länger als 1518 Oktette waren (ohne Synchronisierbits, aber einschließlich FCS-Oktette) und entweder eine ungültige Frame Check Sequence (FCS) mit einer ganzzahligen Oktettanzahl (FCS-Fehler) oder eine ungültige FCS mit einer nicht-ganzzahligen Oktettanzahl (Ausrichtungsfehler) aufwiesen.

Collisions (Kollisionen) – Zeigt die bestmögliche Schätzung der Gesamtzahl an Kollisionen in diesem Ethernet-Segment an.

Utilization – Ein Schätzwert, der die Nutzung der primären Bitübertragungsschicht des Netzwerks an einer Schnittstelle während der Stichprobensitzung angibt. Der Wert wird in x-hundert Prozent angegeben.

Anzeigen von Statistiken für einen bestimmten Verlaufseintrag

1. Öffnen Sie die Seite **RMON History Table** (RMON-Verlaufstabelle).
2. Wählen Sie einen Eintrag im Feld **History Entry No.** aus.

   Die Statistiken für den Eintrag werden auf dem Bildschirm angezeigt.

Anzeigen der RMON-Verlaufssteuerung mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

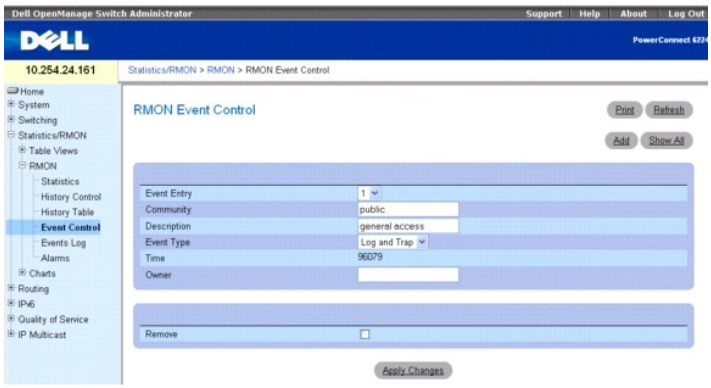
- RMON Commands (RMON-Befehle)

RMON-Ereignissteuerung

Auf der Seite **R MON Events Control** (RMON-Ereignissteuerung) können Sie RMON-Ereignisse definieren. Die Ereignisse werden von RMON-Alarmen verwendet, um bestimmte Vorgänge bei Überschreiten eines Grenzwerts für einen bestimmten RMON-Zähler auszulösen. Die Ereignisinformationen können in einem Protokoll gespeichert und/oder als Trap an einen Trap-Empfänger gesendet werden.

Klicken Sie zur Anzeige der Seite in der Strukturansicht auf **Statistics / RMON (Statistiken / RMON)→ RMON→ Event Control (Ereignissteuerung)**.

Abbildung 9-12. RMON-Ereignissteuerung



Die Seite **RMON Event Control (RMON-Ereignissteuerung) enthält folgende Felder:**

Event Entry (Ereigniseintrag) – Zur Auswahl des Ereignisses.

Community – Gibt die Community an, der das Ereignis angehört.

Description (Beschreibung) – Eine Beschreibung des benutzerdefinierten Ereignisses.

Event Type (Ereignistyp) – Dient zur Auswahl des Ereignistyps. Mögliche Werte:

Log (Protokolleintrag) – Der Ereignistyp ist ein Protokolleintrag.

Trap – Der Ereignistyp ist ein Trap.

Log and Trap (Protokolleintrag und Trap) – Der Ereignistyp ist sowohl ein Protokolleintrag als auch ein Trap.

None (Kein) – Es liegt kein Ereignis vor.

Time (Zeit) – Zeigt die Uhrzeit an, zu der das Ereignis aufgetreten ist.

Owner (Besitzer) – Listet den Switch oder Benutzer auf, von dem das Ereignis definiert wurde.

Remove (Entfernen) – Entfernt das Ereignis aus der Ereignistabelle, wenn die Option aktiviert ist.

Hinzufügen eines RMON-Ereignisses

1. Öffnen Sie die Seite **RMON Events Control** (RMON-Ereignissteuerung).
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add an Event Entry** (Ereigniseintrag hinzufügen) wird angezeigt.

Abbildung 9-13. Ereigniseintrag hinzufügen

3. Konfigurieren Sie die Felder auf dieser Seite.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Das **Ereignis wird in die RMON Event Table** (RMON-Ereignistabelle) aufgenommen und das Gerät aktualisiert.

Ändern eines RMON-Ereignisses

1. Öffnen Sie die Seite **RMON Events Control** (RMON-Ereignissteuerung).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **Event Control Table** (Tabelle der Profilregeln) anzuzeigen.
3. Markieren Sie für den Ereigniseintrag, der geändert werden soll, das Kontrollkästchen **Edit** (Bearbeiten).
4. Modifizieren Sie die Felder auf der Seite nach Bedarf.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Eintrag in der **RMON Events Table** (RMON-Ereignistabelle) wird geändert und das Gerät aktualisiert.

Anzeigen der RMON-Ereignissteuerungstabelle

1. Öffnen Sie die Seite **RMON Events Control** (RMON-Ereignissteuerung).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die **Event Control Table** (Ereignissteuerungstabelle) wird angezeigt.

Abbildung 9-14. Ereignissteuerungstabelle

Entfernen von RMON-Ereigniseinträgen

1. Öffnen Sie die Seite **RMON Events Control** (RMON-Ereignissteuerung).
2. Wählen Sie das zu entfernende Ereignis aus dem Dropdown-Menü im Feld **Event Entry** (Ereigniseintrag), und aktivieren Sie die Option **Remove** (Entfernen).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Tabelleneintrag wird entfernt und das Gerät aktualisiert.

Definieren von Switch-Ereignissen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

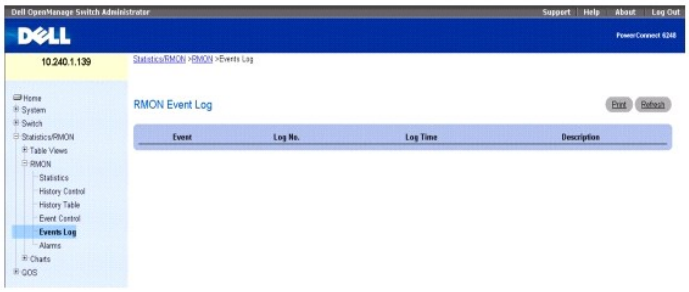
- RMON Commands (RMON-Befehle)

RMON-Ereignisprotokoll

Verwenden Sie die Seite **RMON Event Log** (RMON-Ereignisprotokoll), um eine Liste der RMON-Ereignisse anzuzeigen.

Klicken Sie zur Anzeige der Seite in der Strukturansicht auf **Statistics/RMON (Statistiken/RMON)→ RMON→ Event Log (Ereignisprotokoll)**.

Abbildung 9-15. RMON-Ereignisprotokoll



Die Seite **RMON Event Log (RMON-Ereignisprotokoll) enthält folgende Felder:**

Event (Ereignis) – Zeigt die Nummer des Eintrags im RMON-Ereignisprotokoll an.

Log No. (Protokollnummer) – Zeigt die Protokollnummer an.

Log Time (Protokollierzeit) – Zeigt die Uhrzeit an, zu der der Protokolleintrag erfasst wurde.

Description (Beschreibung) – Eine Beschreibung des Protokolleintrags.

Definieren von Switch-Ereignissen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

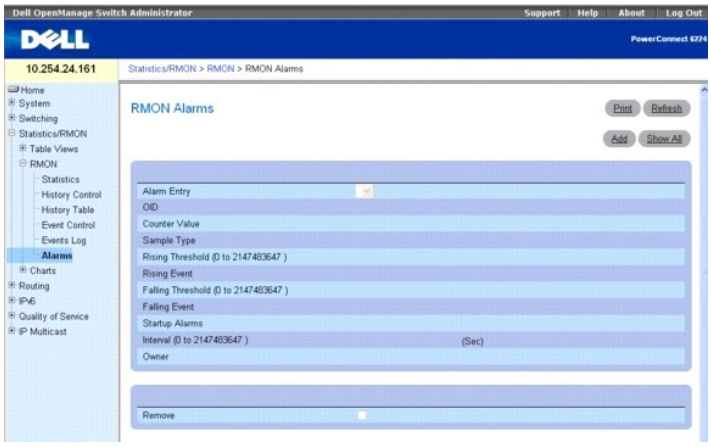
- RMON Commands (RMON-Befehle)

RMON-Alarme

Auf der Seite **RMON Alarms** (RMON-Alarme) können Sie Netzwerkalarme einrichten. Alarme werden ausgelöst, wenn bestimmte Grenzwerte für die konfigurierten RMON-Zähler überschritten werden. Der Alarm wiederum löst ein Ereignis aus. Die Ereignisse können als Teil der RMON-Ereignisgruppe konfiguriert werden. Weitere Informationen über Ereignisse finden Sie unter "RMON Event Log" (RMON-Ereignisprotokoll).

Klicken Sie zur Anzeige der Seite in der Strukturansicht auf **Statistics/RMON (Statistiken/RMON)→ RMON→ Alarms (Alarme)**.

Abbildung 9-16. RMON-Alarme



Die Seite **RMON Alarms (RMON-Alarme) enthält folgende Felder:**

Alarm Entry (Alarmeintrag) – Zur Auswahl eines bestimmten Alarms aus dem Dropdown-Menü.

OID – Zur Vorgabe des Object Identifier.

Counter Value (Zählerwert) – Zeigt die Anzahl der gewählten Ereignisse an, die erfasst wurden.

Sample Type (Stichprobentyp) – Zeigt das Stichprobenverfahren für die ausgewählte Variable an und vergleicht den Wert mit den Schwellenwerten. Die für dieses Feld möglichen Werte sind:

Delta – Subtrahiert den letzten Stichprobenwert vom aktuellen Wert. Die Differenz zwischen den Werten wird mit dem Schwellenwert verglichen.

Absolute (Absolut) – Vergleicht die Werte am Ende des Stichprobenintervalls direkt mit den Schwellenwerten. Dies ist die Standardeinstellung.

Rising Threshold (0-2147483647) (Oberer Zählerwert, 0-2147483647) – Zeigt den oberen Zählerwert an, durch den der Alarm für die Überschreitung des

oberen Schwellenwertes ausgelöst wird. Der obere Schwellenwert ist oben auf den Diagrammbalken dargestellt. Jeder überwachten Variablen ist eine eigene Farbe zugewiesen. Der Standardwert ist 100.

Rising Event (Ereignis bei Auslösung) – Zeigt den Mechanismus für die Ausgabe der Alarme an: Protokoll, Trap oder beides. Bei Auswahl eines Protokolls verfügen weder der Switch noch das Management-System über einen Speichermechanismus. Wird der Switch jedoch nicht zurückgesetzt, verbleibt das Ereignis in der switch-spezifischen Protokolltabelle. Bei Auswahl eines Traps wird ein SNMP-Trap generiert und über einen entsprechenden Trap-Mechanismus gemeldet. Der Trap kann mit demselben Mechanismus gespeichert werden.

Falling Threshold (0-2147483647) (Unterer Zählerwert, 0-2147483647) – Zeigt den unteren Zählerwert an, durch den der Alarm für die Unterschreitung des unteren Schwellenwertes ausgelöst wird. Der untere Schwellenwert ist oben auf den Diagrammbalken grafisch dargestellt. Jeder überwachten Variablen ist eine eigene Farbe zugewiesen. Der Standardwert ist 20.

Falling Event (Ereignis bei Auslösung) – Zeigt den Mechanismus für die Ausgabe der Alarme an: Protokoll, Trap oder beides. Bei Auswahl eines Protokolls verfügen weder der Switch noch das Management-System über einen Speichermechanismus. Wird der Switch jedoch nicht zurückgesetzt, verbleibt das Ereignis in der switch-spezifischen Protokolltabelle. Bei Auswahl eines Traps wird ein SNMP-Trap generiert und über einen entsprechenden Trap-Mechanismus gemeldet. Der Trap kann mit demselben Mechanismus gespeichert werden.

Startup Alarms (Alarme) – Zeigt den Ereignistyp an. Die Optionen sind Rising (oberer Schwellenwert), Rising-falling (oberer/unterer Schwellenwert) und Falling (unterer Schwellenwert).

Interval (0-2147483647) (Intervall, 0-2147483647) – Zeigt die Intervalldauer für den Alarm an. Der Standardwert ist 100.

Owner (Besitzer) – Zeigt den Switch oder Benutzer an, von dem der Alarm definiert wurde.

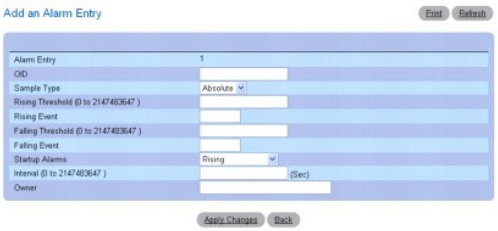
Remove (Entfernen) – Entfernt einen RMON-Alarm, wenn die Option aktiviert ist.

Hinzufügen eines Eintrags in die Alarmtabelle

1. Öffnen Sie die Seite **RMON Alarms**.
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add an Alarm Entry** (Alarmeintrag hinzufügen) wird angezeigt.

Abbildung 9-17. Alarmeintrag hinzufügen



3. Konfigurieren Sie die Felder auf dieser Seite nach Bedarf.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der RMON-Alarm wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der Alarmtabelle

1. Öffnen Sie die Seite **RMON Alarms**.
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die linke Seite der **RMON Alarms Table (RMON-Alarmtabelle) wird angezeigt**.

Abbildung 9-18. RMON-Alarmtabelle

3. Klicken Sie auf den Nach-rechts-Pfeil unten im Bildschirm, um die rechte Seite der Tabelle anzuzeigen.

Entfernen eines Eintrags aus der Alarmtabelle

1. Öffnen Sie die Seite **RMON Alarms**.
2. Wählen Sie einen Eintrag im Dropdown-Menü **Alarm Entry** (Alarmeintrag) aus.
3. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen), und klicken Sie auf **Apply Changes** (Änderungen übernehmen.

   Der Eintrag wird entfernt und das Gerät aktualisiert.

Entfernen mehrerer Einträge aus der Alarmtabelle

1. Öffnen Sie die Seite **RMON Alarms**.
2. Klicken Sie auf **Show All**

   (Alle anzeigen).

   Die **RMON Alarms Table (RMON-Alarmtabelle) wird angezeigt**.
3. Aktivieren Sie für jeden Alarmeintrag, der entfernt werden soll, das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Einträge werden entfernt und das Gerät aktualisiert.

Definieren von Switch-Alarmen mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) im folgenden Kapitel:

- RMON Commands (RMON-Befehle)

Diagramme

Die Menüseite **Chart** (Diagramm) enthält Links auf Webseiten, die die Darstellung von Statistiken in Diagrammen ermöglichen. Klicken Sie zur Anzeige der Menüseite **Charts** (Diagramme) in der Strukturansicht auf **Statistics/RMON (Statistiken/RMON)**→ **Charts (Diagramme)**. Die Menüseite **Charts** (Diagramme) enthält Links zu den folgenden Funktionen:

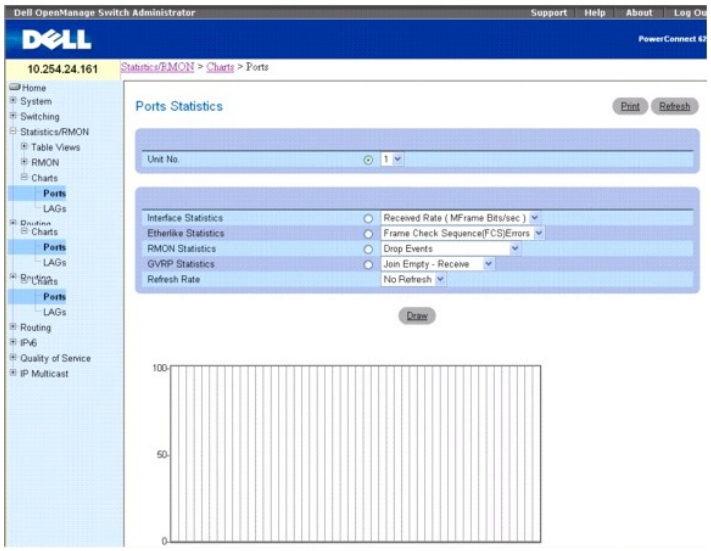
- Port-Statistiken
- LAG-Statistiken

Port-Statistiken

Verwenden Sie die Seite **Ports Statistics** (Port-Statistiken), um portbezogene Statistiken in einem Diagramm darzustellen.

Klicken Sie zur Anzeige der Seite in der Strukturansicht auf **Statistics/RMON (Statistiken/RMON)**→ **Chart (Diagramme)**→ **Ports**.

Abbildung 9-19. Port-Statistiken



Die Seite **Ports Statistics (Port-Statistiken) enthält folgende Felder:**

Unit No. (Einheit-Nr.) – Zur Auswahl des anzuzeigenden Ports.

Interface Statistics (Schnittstellenstatistik) – Mit dieser Option wird die Schnittstellenstatistik gewählt, und der Typ der Statistik, die grafisch dargestellt werden soll, kann aus dem Dropdown-Menü gewählt werden. Die Standardeinstellung ist hierbei Received Rate (MFrame Bits/sec) (Empfangsrate (MFrame Bits/s)).

Etherlike Statistics (Etherlike-Statistik) – Mit dieser Option wird die Etherlike-Statistik gewählt, und der Typ der Statistik, die grafisch dargestellt werden soll, kann aus dem Dropdown-Menü gewählt werden. Die Standardeinstellung ist Frame Check Sequence (FCS) Errors (FCS-Fehler).

RMON Statistics (RMON-Statistik) – Mit dieser Option wird die RMON-Statistik gewählt, und der Typ der Statistik, die grafisch dargestellt werden soll, kann aus dem Dropdown-Menü gewählt werden. Die Standardeinstellung ist Drop Events (Ablehnungsereignisse).

GVRP Statistics (GVRP-Statistik) – Mit dieser Option wird die GVRP-Statistiken gewählt, und der Typ der Statistik, die grafisch dargestellt werden soll, kann aus dem Dropdown-Menü gewählt werden. Die Standardeinstellung ist Join Empty - Receive (Join Empty - Empfangen).

Refresh Rate (Aktualisierungsrate) – Zur Auswahl des Zeitraums bis zur Aktualisierung der Statistiken. Die Feldwerte No Refresh (Keine Aktualisierung) sowie 15, 30 und 60 Sekunden sind möglich. Standardwert ist "No Refresh" (Keine Aktualisierung).

Anzeigen von Port-Statistiken

1. Öffnen Sie die Seite **Port Statistics** (Port-Statistiken).
2. Wählen Sie den Port, für den Statistiken grafisch dargestellt werden sollen.
3. Klicken Sie auf das Optionsfeld, das der Statistik zugeordnet ist, die grafisch dargestellt werden soll.
4. Wählen Sie den Statistiktyp aus dem entsprechenden Dropdown-Menü aus.
5. Wählen Sie im Dropdown-Menü **Refresh Rate** (Aktualisierungsrate) die gewünschte Aktualisierungsrate aus.
6. Klicken Sie auf **Draw** (Zeichnen).

   Die gewählten Statistiken werden im Diagramm dargestellt.

Anzeigen von Port-Statistiken mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) in den folgendem Kapiteln:

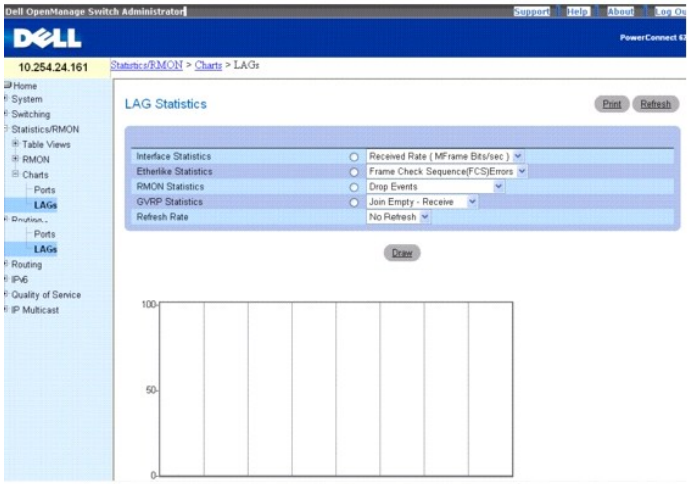
- System Management Commands (System-Management-Befehle)
- RMON Commands (RMON-Befehle)
- GVRP Commands (GVRP-Befehle)

LAG-Statistiken

Verwenden Sie die Seite **LAG Statistics** (LAG-Statistiken), um LAG-bezogene Statistiken in einem Diagramm darzustellen.

Klicken Sie zur Anzeige der Seite in der Strukturansicht auf **Statistics/RMON (Statistiken/RMON)**→ **Charts (Diagramme)**→ **LAGs**.

Abbildung 9-20. LAG-Statistiken



Die Seite **LAG Statistics (LAG-Statistiken) enthält folgende Felder:**

Interface Statistics (Schnittstellenstatistik) – Mit dieser Option wird die Schnittstellenstatistik gewählt, und der Typ der Statistik, die grafisch dargestellt werden soll, kann aus dem Dropdown-Menü gewählt werden. Die Standardeinstellung ist Received Rate (Empfangsrate).

Etherlike Statistics (Etherlike-Statistik) – Mit dieser Option wird die Etherlike-Statistik gewählt, und der Typ der Statistik, die grafisch dargestellt werden soll, kann aus dem Dropdown-Menü gewählt werden. Die Standardeinstellung ist Frame Check Sequence Errors (FCS-Fehler).

RMON Statistics (RMON-Statistik) – Mit dieser Option wird die RMON-Statistik gewählt, und der Typ der Statistik, die grafisch dargestellt werden soll, kann aus dem Dropdown-Menü gewählt werden. Die Standardeinstellung ist Drop Events (Ablehnungsereignisse).

GVRP Statistics (GVRP-Statistik) – Mit dieser Option wird die GVRP-Statistiken gewählt, und der Typ der Statistik, die grafisch dargestellt werden soll, kann aus dem Dropdown-Menü gewählt werden. Die Standardeinstellung ist Join Empty - Receive (Join Empty - Empfangen).

Refresh Rate (Aktualisierungsrate) – Zur Auswahl des Zeitraums bis zur Aktualisierung der Statistiken. Die Feldwerte No Refresh (Keine Aktualisierung) sowie 15, 30 und 60 Sekunden sind möglich. Die Standardrate beträgt 15 Sekunden.

Anzeigen von LAG-Statistiken

1. Öffnen Sie die Seite **LAG Statistics** (LAG-Statistiken).
2. Klicken Sie auf das Optionsfeld, das der Statistik zugeordnet ist, die grafisch dargestellt werden soll.
3. Wählen Sie den Statistiktyp aus dem entsprechenden Dropdown-Menü aus.
4. Wählen Sie im Dropdown-Menü **Refresh Rate** (Aktualisierungsrate) die gewünschte Aktualisierungsrate aus.
5. Klicken Sie auf **Draw** (Zeichnen).

   Die gewählten Statistiken werden im Diagramm dargestellt.

Anzeigen von LAG-Statistiken mithilfe von CLI-Befehlen

Informationen über die CLI-Befehle, die diese Funktion ausführen, finden Sie im CLI Reference Guide (CLI-Referenzhandbuch) in den folgendem Kapiteln:

- System Management Commands (System-Management-Befehle)
- RMON Commands (RMON-Befehle)
- GVRP Commands (GVRP-Befehle)

Zurück zum Inhaltsverzeichnis