Dell™ PowerConnect™ 6024/6024F Systeme

Anmerkungen, Hinweise und Vorsichtshinweise

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

HINWEIS: Ein HINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und zeigt, wie diese vermieden werden können.

VORSICHT: Ein VORSICHTSHINWEIS weist auf Gefahrenquellen hin, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

Januar 2005

Zurück zum Inhaltsverzeichnis

Kabel, Portverbindungen und Pinbelegung

Dell™ PowerConnect™ 6024/6024F-Systeme

Dieser Abschnitt beschreibt die physikalische Schnittstelle des Switch und liefert Informationen über Kabelverbindungen.

Stationen werden durch die physikalischen Schnittstellenports an der Frontblende mit den Switchports verbunden. Für jede Station ist der entsprechende Modus (Halb- oder Vollduplex, automatisch) eingestellt.

Pinverbindungen für die Ethernet-Schnittstelle 10/100/1000

Der Switchport kann an Stationen angeschlossen werden, die im standardmäßigen RJ-45-Ethernet-Stationsmodus mithilfe von 1:1 Kabeln verkabelt sind. Miteinander verbundene Übertragungsgeräte verwenden gekreuzte Kabel.

Abbildung 3-1 zeigt die RJ-45-Pins, und Tabelle 3-1 enthält die RJ-45-Pinbelegungen.

Abbildung 3-1. RJ-45-Steckverbinder

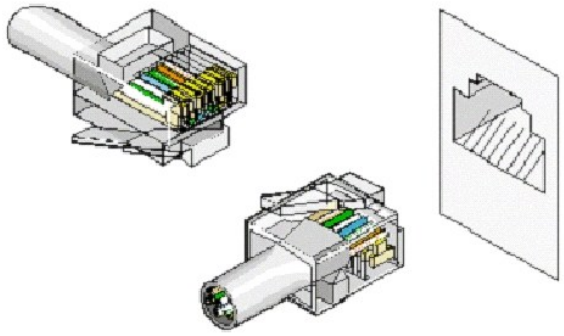


Tabelle 3-1. RJ-45-Pinverbindungen für 10/100/1000 Base-T

Pin	Verwendung
1	TxRx 1+
2	TxRx 1-
3	TxRx 2+
4	TxRx 2-
5	TxRx3+
6	TxRx 3-
7	TxRx 4+
8	TxRx 4-

Pinverbindungen für SFP-Schnittstellen

Abbildung 3-2 zeigt einen SFP-Anschluss, und Tabelle 3-2 zeigt die Pinbelegung für einen optionalen SFP-Anschluss.

Abbildung 3-2. SFP-Anschluss

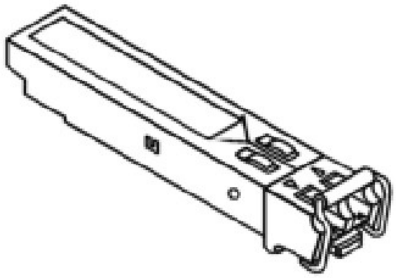


Tabelle 3-2. SFP-Pinverbindungen

Pin	Verwendung
1	Masse (gemeinsam für Sender und Empfänger).
2	Senderfehler.
3	Sendersperre; Laser abgeschaltet bei high oder offen.
4	Moduldefinition 2; Datenleitung für serielle ID.
5	Moduldefinition 1; Taktleitung für serielle ID.
6	Moduldefinition 0; geerdet innerhalb des Moduls.
7	Ratenauswahl; keine Verbindung erforderlich.
8	Verlust der Signalindikation; logic 0 zeigt normalen Betrieb an.
9	Masse (gemeinsam für Sender und Empfänger).
10	Masse (gemeinsam für Sender und Empfänger).
11	Masse (gemeinsam für Sender und Empfänger).
12	Empfangsdaten-Ausgang invertiert; Wechselstrom gekoppelt.
13	Empfangsdaten-Ausgang nicht invertiert; Wechselstrom gekoppelt.
14	Masse (gemeinsam für Sender und Empfänger).
15	Stromversorgung Empfänger.
16	Stromversorgung Sender.
17	Masse (gemeinsam für Sender und Empfänger).
18	Sendedaten-Eingang nicht invertiert.
19	Sendedaten-Eingang invertiert.
20	Masse (gemeinsam für Sender und Empfänger).

Serielle Kabelverbindung

Sie können serielle Kabel (Nullmodem) verwenden, um den Switch mit einem Terminal zum ersten Einrichten und Konfigurieren zu verbinden (Sie können auch eine auf dem PC laufende Terminal-Emulation-Software verwenden). Das serielle Kabel des Switch ist ein gekreuztes Buchse-an-Buchse DB-9-Kabel (siehe Abbildung 3-3).

Abbildung 3-3 zeigt das serielle Kabel, und Tabelle 3-3 zeigt die Pinbelegung des seriellen Anschlusses.

Abbildung 3-3. Serieller Anschluss

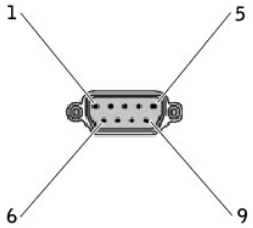


Tabelle 3-3 enthält die Pinbelegungen des seriellen Kabels.

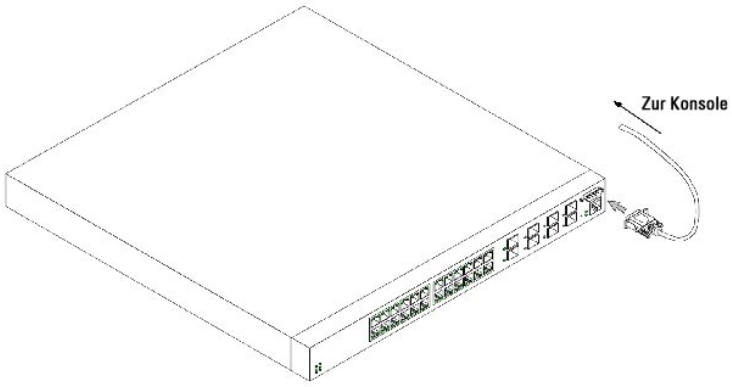
Tabelle 3-3. Pinbelegung für den seriellen Port

Signal	Pin	Signal Verwaltungskonsolenport
Unbenutzt	1	Unbenutzt
TXD	2	TXD
RXD	3	RXD
Unbenutzt	4	RXD
GND	5	GND
Unbenutzt	6	Unbenutzt
CTS	7	CTS
RTS	8	RTS
Unbenutzt	9	Unbenutzt

Verbinden des Switch mit einem Terminal

1. Schließen Sie das (serielle) Nullmodemkabel an die ASCII DTE RS-232-Verbindung des Terminals (Konsole) an.
2. Verbinden Sie das Schnittstellenkabel mit dem seriellen Port (siehe Abbildung 3-4).

Abbildung 3-4. Serieller Anschluss an Switch



Netzstromanschluss

1. Schließen Sie das Netzkabel mithilfe eines 1,5 m langen Standardnetzkabels mit Sicherheitserdung an den Hauptstromsockel auf der rückseitigen Abdeckung (siehe Abbildung 3-5) an.
2. Schließen Sie das Netzkabel an einer geerdeten Wechselstromsteckdose an.

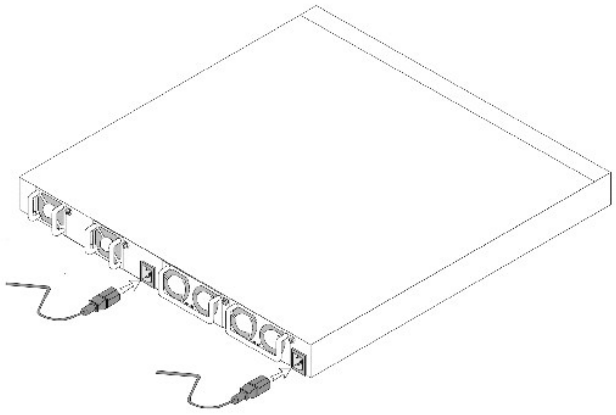
ANMERKUNG: Es wird empfohlen, die zweite Stromversorgung an eine andere Stromquelle anzuschließen.

3. Stellen Sie sicher, dass das Gerät angeschlossen ist und ordnungsgemäß funktioniert, indem Sie die Leuchtdioden auf der vorderen und rückseitigen Abdeckung überprüfen.

   Eine vollständige Beschreibung der Leuchtdioden finden Sie unter „Beschreibung der Hardware".

4. Wiederholen Sie den Vorgang für die zweite Stromversorgung.

Abbildung 3-5. Netzstromanschluss an Switch



Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

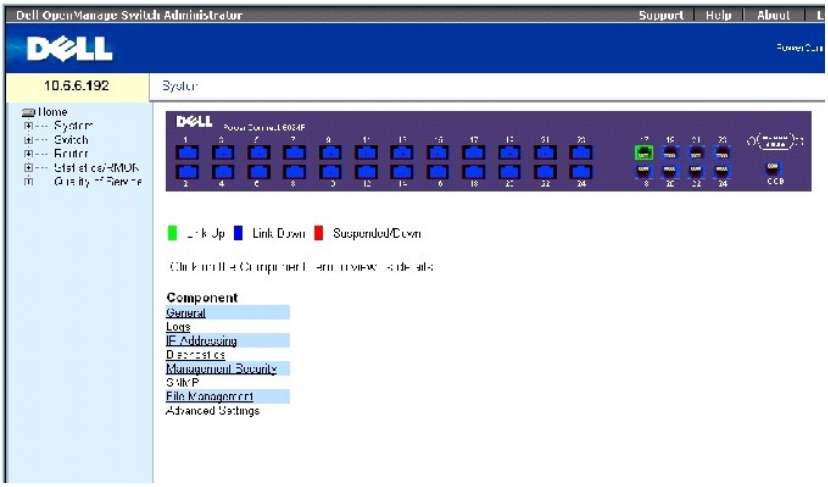
Konfigurieren von Systeminformationen:

Dell PowerConnect 6024/6024F-Systeme

Öffnen der Systemseite

Um die Seite **System** zu öffnen, klicken Sie in der Strukturansicht auf **System** (siehe Abbildung 6-1).

Abbildung 6-1. System



Definieren allgemeiner Geräteinformationen

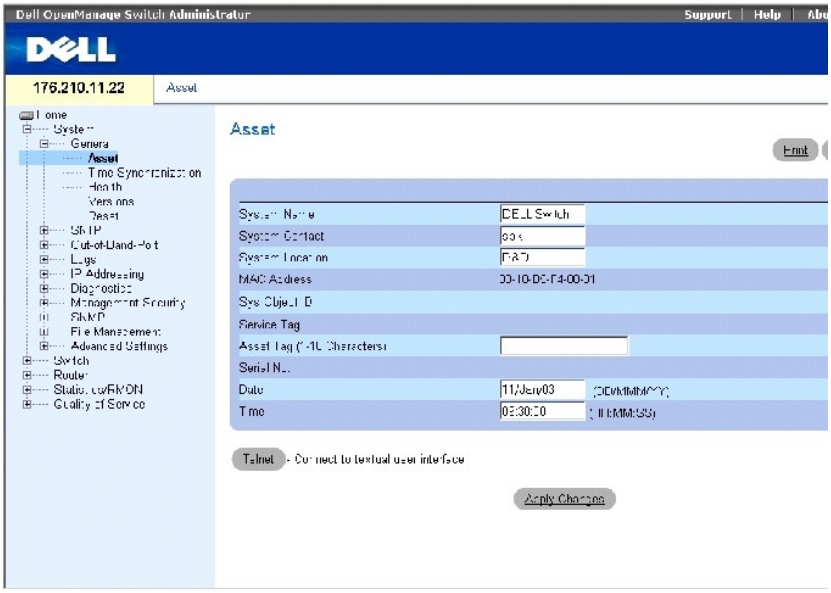
Die Seite **Allgemein** enthält Verknüpfungen zu Seiten, die es Netzwerkmanagern ermöglichen, Geräteparameter zu konfigurieren.

Konfigurieren von Geräteinformationen

Die Seite **Asset** (Anlage) enthält Parameter zur Konfiguration und Ansicht allgemeiner Geräteinformationen, einschließlich Systemname, Standort und Kontakt, die System-MAC-Adresse sowohl für den Switch als auch für den Out of Band-Management-Port, Systemobjekt-ID, Datum, Uhrzeit und Systembetriebszeit.

Um die Seite **Anlage** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **General**→ **Asset**.

Abbildung 6-2. Anlage



Die Seite **Anlage** enthält die folgenden Felder:

System Name (Systemname) Der vom Benutzer zugewiesene Systemname des Geräts.

System Contact (Systemkontakt) Der Name der Kontaktperson.

System Location (Systemstandort) Der Standort des laufenden Systems.

MAC Address (MAC-Adresse) Die MAC-Adresse des Switch.

Sys Object ID (Systemobjekt-ID) die MIB-Objekt-ID.

Service Tag (Service-Tag-Nummer) Die Wartungsreferenznummer, die zur Wartung des Geräts verwendet wird.

Asset Tag (Systemkennnummer) Die vom Benutzer definierte Gerätereferenznummer. Die möglichen Parameterwerte sind 1-16.

Serial No. (Seriennummer) Die Seriennummer des Geräts.

Date (DD/MMM/YY) (Datum (TT/MMM/JJ)) Das aktuelle Systemdatum. Das Format lautet Tag, Monat, Jahr, z. B. steht 11/Jan/02 für 11. Januar 2002.

Time (HH/MM/SS) (Uhrzeit (HH/MM/SS) Die aktuelle Uhrzeit im System. Das Format lautet Stunde, Minute, Sekunde, z. B. steht 20:12:03 für 8:12:03 abends.

Definieren von Systeminformationen

1. Öffnen sie die Seite **Asset** (Anlage).
2. Definieren Sie die folgenden Felder: **System Name** (Systemname), **System Contact** (Systemkontakt), **System Location** (Systemstandort) und **Asset Tag** (Systemkennnummer).
3. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

Die Systemparameter werden angewendet, und das wird Gerät aktualisiert.

Initiieren einer Telnet-Sitzung

1. Öffnen sie die Seite **Asset** (Anlage).

ANMERKUNG: Die entsprechenden Telnet-Parameter werden vor dem Initiieren der Telnet-Sitzung eingestellt. Weitere Informationen zum Konfigurieren eines anfänglichen Telnet-Kennworts finden Sie unter Konfigurieren eines anfänglichen Telnet-Kennworts".

2. Klicken Sie auf **Telnet**.

Konfigurieren von Geräteinformationen mithilfe von CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für die Ansicht von Feldern auf der Seite **Asset** (Anlage) zusammen.

Tabelle 6-1. CLI-Befehle für Asset (Bestand)

CLI-Befehl	Beschreibung
`hostname name`	Legt den Hostnamen des Gerätes fest oder ändert ihn.
`snmp-server contact` `text`	Richtet eine Kontaktperson für das System ein.
`snmp-server location` `text`	Spezifiziert Informationen über den Standort des Geräts.
`show clock`	Zeigt Systemuhrzeit und -datum an.
`asset-tag` `tag`	Spezifiziert die Systemkennnummer für das Gerät.
`show system-id`	Zeigt die Systemkennungsinformationen an, einschließlich Service-Tag-Nummer, Systemkennnummer und Seriennummer.
`show system`	Zeigt Systeminformationen an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# hostname dell

Console (config)# snmp-server contact Dell_Tech_Supp

Console (config)# snmp-server location New_Yorks

Console (config)# exit
```

```
Console# clock set 13:32:00 7 Mar 2002

Console# show clock

15:29:03 Jun 17 2002
```

Definieren von Systemzeiteinstellungen

Die Seite **Zeitsynchronisation** enthält Felder zum Synchronisieren der Systemzeit mit der lokalen Hardware-Uhr oder mit der externen SNTP-Uhr.

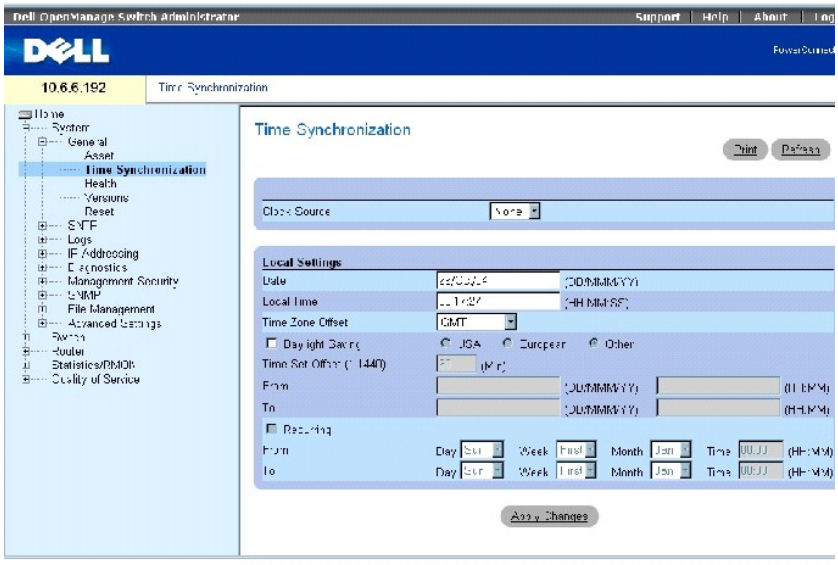
Wenn die Systemuhr mit einer externen SNTP-Uhr synchronisiert wird und die Uhr nicht die richtige Zeit anzeigt, schaltet der Zeitgeber der Systemuhr automatisch auf die lokale Hardware-Uhrzeit um.

Die Systemuhr kann so konfiguriert werden, dass sie automatisch auf Sommerzeit umgestellt wird.

Weitere Informationen zu SNTP finden Sie unter **Konfigurieren der SNTP-Einstellungen**.

Öffnen Sie die Seite **Time Synchronization** (Zeitsynchronisation), indem Sie auf **System**→ **General**→ **Time Synchronization** in der *Strukturansicht*.

Abbildung 6-3. Zeitsynchronisation



Die Seite **Zeitsynchronisation** enthält die folgenden Felder:

Clock Source (Zeitquelle) Die Zeitquelle, die zum Verwalten der Systemuhr verwendet wird. Die möglichen Feldwerte sind:

None (Kein) Definiert, dass die Systemzeit mit der lokalen Hardware-Uhr synchronisiert wird.

SNTP (SNTP) Definiert, dass die Systemzeit mit einer SNTP-Serveruhr synchronisiert wird. Weitere Informationen finden Sie unter **Konfigurieren von SNTP-Einstellungen**.

Date (Datum) Legt das Systemdatum fest. Das Feldformat lautet: TT:MMM:JJ.

Local Time (Ortszeit) Legt die Systemuhrzeit fest. Das Feldformat lautet: HH:MM:SS.

Time Zone Offset (Zeitzonenausgleich) Definiert die Differenz in Stunden zwischen der Greenwich Mean Time (GMT, koordinierte Weltzeit) und der aktuellen Ortszeit.

Die Systemuhr kann so eingestellt werden, dass sie zu einem festgelegten Zeitpunkt eines Jahres oder zu ständig wiederkehrenden Zeitpunkten automatisch auf Sommerzeit umschaltet. Verwenden Sie die Parameter im Bereich Sommerzeit", um den Zeitpunkt in einem bestimmten Jahr festzulegen und die Parameter im Bereich Wiederkehrend", um wiederkehrende Zeitpunkte festzulegen.

Daylight Savings (Sommerzeit) Markieren Sie dieses Kontrollkästchen, um auf Basis des Gerätestandorts auf dem Gerät die Sommerzeit zu aktivieren. Die möglichen Feldwerte sind:

USA Die Geräteuhr wird um 2 Uhr am ersten Sonntag im April auf Sommerzeit umgestellt und kehrt am letzten Sonntag im Oktober um 2 Uhr zur Standardzeit zurück.

European (Europäisch) Die Geräteuhr schaltet am letzten Sonntag im März um 1 Uhr auf Sommerzeit um und kehrt am letzten Sonntag im Oktober um 1 Uhr zur Standardzeit zurück. Diese Option gilt für EU-Mitglieder und andere europäische Länder, die dem EU-Standard folgen.

Other (Andere) Die Uhrzeit im Gerät schaltet entsprechend der benutzerdefinierten Zeitspanne auf Sommerzeit um.

Time Set Offset (1-1440) (Zeitausgleich (1- 1440)) In Staaten außerhalb der USA und Europa kann die Differenz zwischen Standardzeit und Sommerzeit in Minuten angegeben werden. Die Standardzeit ist 60 Minuten.

From/To (Von/bis) Legt das Datum und den Zeitpunkt fest, zu dem die Sommerzeit in Staaten außerhalb der USA und Europa beginnt und endet. Das Datumsformat lautet TT/MMM/YY, und das Zeitformat lautet HH:MM.

Recurring (Wiederkehrend) Markieren Sie dieses Kontrollkästchen, um die Sommerzeit auf der Basis eines wiederkehrenden Zeitrahmens zu aktivieren. Die möglichen Feldwerte sind:

From/To (Von/bis) Legt Tag, Woche, Monat und Zeitpunkt fest, zu dem die Sommerzeit beginnt und endet. Das Zeitformat lautet: HH:MM.

Auswählen einer Zeitquelle

1. Öffnen Sie die Seite **Time Synchronization** (Zeitsynchronisation).
2. Definieren Sie das Feld **Clock Source** (Zeitquelle).
3. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

Die ausgewählte Zeitquelle wird ausgewählt und das Gerät wird aktualisiert.

Festlegen von Ortszeiteinstellungen

1. Öffnen Sie die Seite **Time Synchronization** (Zeitsynchronisation).
2. Definieren Sie die Felder im Bereich **Local Settings**" (Lokale Einstellungen).
3. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

Die Einstellungen für die Ortszeit werden übernommen und das Gerät aktualisiert.

Definieren der Sommerzeit

1. Öffnen Sie die Seite **Time Synchronization** (Zeitsynchronisation).
2. Definieren Sie die Felder in den Bereichen **Daylight Saving**" (Sommerzeit) oder **Reccuring**" (Wiederkehrend).
3. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

Die Einstellungen für die Sommerzeit werden übernommen und das Gerät aktualisiert.

Definieren der Zeiteinstellungen mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Einstellung der Felder, die auf der Seite **Time Synchronization** (Zeitsynchronisation) angezeigt werden.

Tabelle 6-2. CLI-Befehle für Zeitsynchronisation

CLI-Befehl	Beschreibung
`clock source {sntp}`	Synchronisiert die Systemzeit mit einer SNTP-Serveruhr.
`no clock source`	Synchronisiert die Systemzeit mit der Geräteuhr.
`clock timezone hours- offset [minutes minutes- offset] [zone acronym]`	Stellt die Zeitzone für Anzeigezwecke ein.
`no clock timezone`	Stellt die Uhrzeit auf Coordinated Universal Time (UTC, koordinierte Weltzeit) ein.
`clock summer-time recurring {usa | eu | {`*`week day month hh:mm week day month hh:mm`*`}} [offset `*`offset`*`] [zone `*`acronym`*`]`	Konfiguriert das System so, dass es auf der Basis des USA- oder Europastandards oder eines benutzerdefinierten Zeitrahmens auf Sommerzeit umschaltet.
`clock summer-time date date month year hh:mm date month year hh:mm [offset offset] [zone acronym]`	Konfiguriert das System so, dass es während eines benutzerdefinierten Zeitrahmens auf Sommerzeit umschaltet.
`no clock summer-time`	Konfiguriert das System so, dass es nicht auf Sommerzeit umschaltet.
`show clock`	Zeigt die Zeit und das Datum der Systemuhr an.
`show clock [detail]`	Zeigt die Zeit, das Datum, die Zeitzone und die Sommerzeitkonfiguration der Systemuhr an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# clock timezone -6 zone CST
```

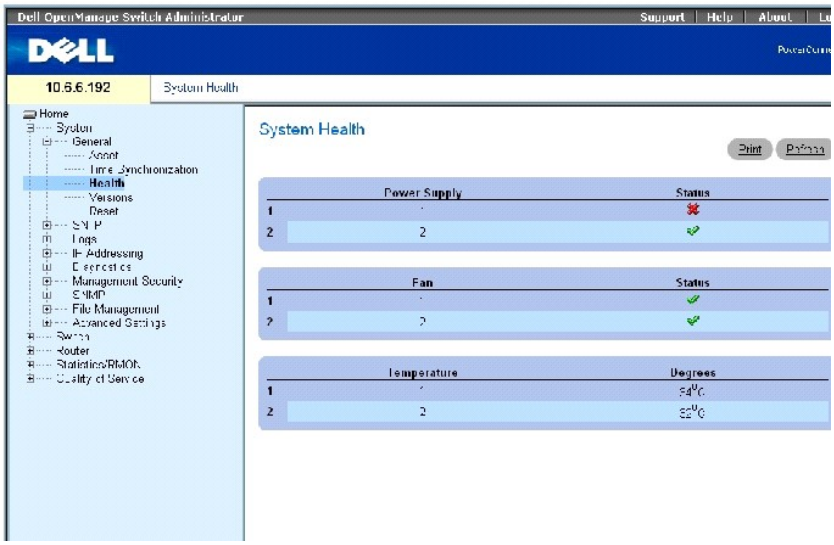
```
Console (config)# clock summer-time recurring first sun apr 2:00 last sun oct 2:00
```

Konfigurieren von Systemzustandsdaten

Die Seite **Systemzustand** zeigt physische Gerätedaten an, darunter Daten zur Stromversorgung und den Belüftungsquellen des Swichtes. Um die Seite

Systemzustand anzuzeigen, klicken Sie in der Strukturansicht auf **System**→ **General**→ **Health**.

Abb. 6-4. Systemzustand (System Health)



Die Seite **Systemzustand** enthält die folgenden Felder:

Power Supply (Stromversorgung) Der Status der Stromversorgung.

Die Stromversorgung arbeitet normal.

Die Stromversorgung arbeitet nicht normal.

Not Present (Nicht vorhanden) Es ist derzeit keine Stromversorgung vorhanden.

Fan (Lüfter) Zeigt den Lüfterstatus an. Der PowerConnect 6024/6024F hat zwei Lüfter.

Der Lüfter arbeitet normal.

Der Lüfter arbeitet nicht normal.

Not Present (Nicht vorhanden) Es ist derzeit kein Lüfter vorhanden.

Temperature (Temperatur) Die Temperatur, bei der das Gerät derzeit betrieben wird.

Anzeigen der Systemzustandsinformationen mithilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Anzeige der Felder zusammengefasst, die auf der Seite **Systemzustand** angezeigt werden.

Tabelle 6-3. CLI-Befehle für Systemzustand

CLI-Befehl	Beschreibung
show system	Zeigt Systeminformationen an.

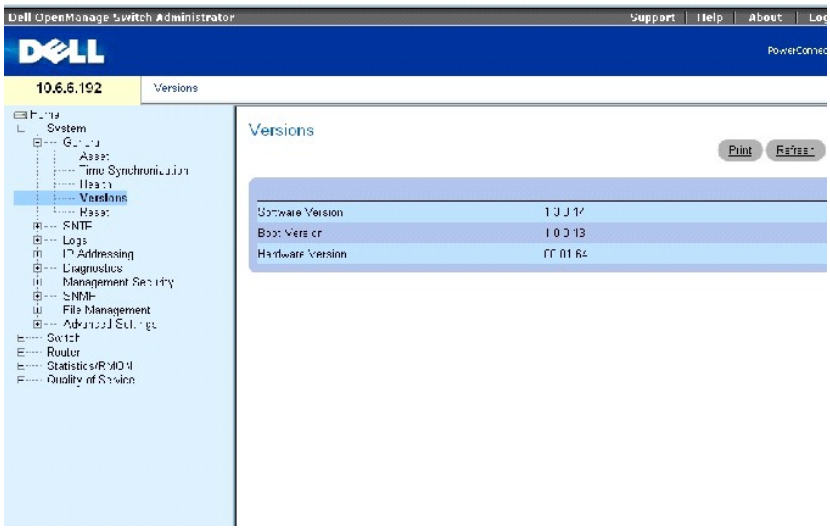
Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console# show system

System Description:                 Ethernet Routing Switch
System Up Time (days,hour:min:sec): 0,00:32:04
System Contact:
System Name:
System Location:
System MAC Address:                 00:0d:56:2f:45:30
OOB MAC Address:                    00:00:00:00:00:18
System Object ID:                   1.3.6.1.4.1.674.10895.3000
Type:                               PowerConnect 6024

Main Power Supply Status:           OK
Redundant Power Supply Status:      OK
Fan 1 Status:                       OK
Fan 2 Status:                       OK
Temperature (Celsius):              45
Temperature Sensor Status:          OK
```

Versionsinformationen

Die Seite **Versions** (Versionen) enthält Informationen zu den Versionen der derzeit ausgeführten Hardware und Software. Um die Seite **Versionen** anzuzeigen, klicken Sie in der Strukturansicht auf **System**→ **General**→ **Versions** (siehe Abbildung 6-5).

Abbildung 6-5. Versionen



Die Seite **Versionen** enthält die folgenden Felder:

Software Version Die Version der derzeit auf dem Gerät ausgeführten Software.

Boot Version (Startversion) Die auf dem Gerät derzeit ausgeführte Startversion.

Hardware Version (Hardwareversion) Die Version der derzeit auf dem Gerät betriebenen Hardware.

Anzeigen der Geräteversionen mithilfe von CLI-Befehlen

In der folgenden Tabelle wird der entsprechende CLI-Befehl für die Anzeige der Felder zusammengefasst, die auf der Seite **Versionen** angezeigt werden.

Tabelle 6-4. CLI-Befehle für Versionen

CLI-Befehl	Beschreibung
show version	Zeigt Informationen zu den Systemversionen an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

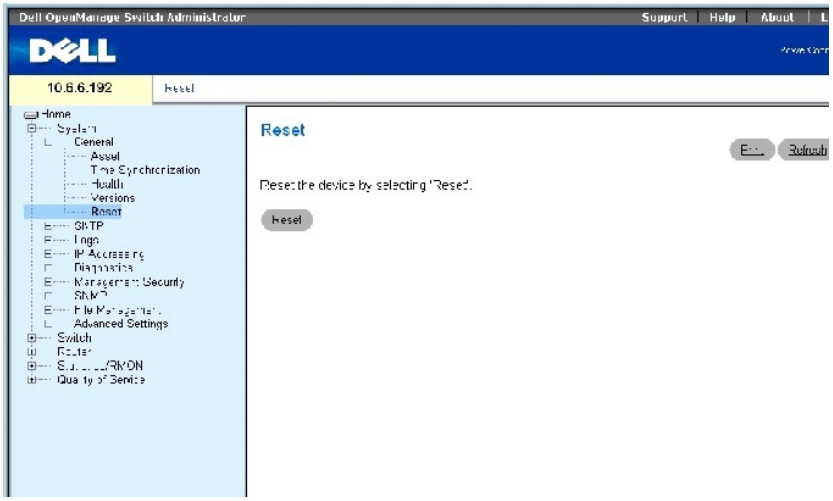
```
Console# show version

SW version 1.0.0.67 ( date 26-Jun-2003 time 18:15:42 )
```

```
Boot version 1.0.0.11 ( date 12-Jun-2003 time 15:55:01 )


HW version 00.01.64
```

Zurücksetzen des Gerätes

Sie können die Seite **Reset** (Zurücksetzen) verwenden, um das Gerät zurückzusetzen. Um die Seite **Zurücksetzen** zu öffnen, klicken Sie in der Strukturansicht auf **System→ General→ Reset** (siehe Abbildung 6-6).

Abbildung 6-6. Zurücksetzen



ANMERKUNG: Speichern Sie alle Änderungen in der aktiven Konfigurationsdatei, bevor Sie das Gerät zurücksetzen, um zu vermeiden, dass die aktuelle Gerätekonfiguration verloren geht. Weitere Informationen über das Speichern von Konfigurationsdateien finden Sie unter Verwalten von Dateien.

Zurücksetzen des Gerätes

1. Öffnen Sie die Seite **Reset** (Zurücksetzen).
2. Klicken Sie auf **Reset** (Zurücksetzen).
3. Wenn die Bestätigungsmeldung erscheint, klicken Sie auf **OK**.

Das Gerät wird zurückgesetzt. Nach dem Zurücksetzen des Geräts geben Sie einen Benutzernamen und ein Kennwort ein.

Zurücksetzen des Geräts mithilfe der CLI

1. Wenn Sie nicht bereits im Privileged User EXEC-Modus der CLI sind, geben Sie `enable` (Aktivieren) ein.
2. Wenn Sie eventuelle Änderungen an der aktiven Konfiguration des Geräts speichern wollen, geben Sie `copy running-config startup-config` (aktive Konfiguration Startkonfiguration kopieren) ein.
3. Geben Sie `reload` (Erneut laden) ein.
4. Drücken Sie `y` (Ja), wenn Sie gefragt werden, ob Sie fortfahren möchten.

Konfigurieren von SNTP-Einstellungen

Das Gerät unterstützt das Simple Network Time Protocol (SNTP). SNTP stellt die genaue Netzwerkschalter-Zeitsynchronisation bis auf die Millisekunde sicher. Die zeitliche Synchronisierung wird von einem Netzwerk-SNTP-Server ausgeführt. Der Gerät wird nur als SNTP-Client betrieben. Es kann keine Zeitdienste für andere Systeme liefern.

Zeitquellen werden durch Strata ermittelt. Strata definieren die Präzision der Referenzuhr. Je höher das Stratum (Null ist am höchsten), desto genauer die Uhr. Das Gerät erhält die Uhrzeit von Stratum 1 und höher.

Nachstehend ein Beispiel für Strata:

- **Stratum 0** Eine Echtzeituhr wird als Zeitquelle verwendet, z. B. ein GPS-System.
- **Stratum 1** Ein Server, der direkt mit einer Stratum-0-Zeitquelle verbunden ist, wird verwendet. Server mit Stratum-1-Zeit stellen primäre Netzwerk-Zeitstandards bereit.
- **Stratum 2** Die Zeitquelle ist über einen Netzwerkpfad vom Stratum-1-Server entfernt. Zum Beispiel empfängt ein Stratum-2-Server die Zeit über eine Netzwerkverbindung, über NTP, von einem Stratum-1 Server.

Die von SNTP-Servern eingehenden Informationen werden auf der Grundlage des Zeitlevels und Servertyps beurteilt.

SNTP-Zeitdefinitionen werden anhand der folgenden Zeitlevels beurteilt und bestimmt:

- **T1** Zeitpunkt, zu dem die ursprüngliche Anfrage vom Client gesendet wurde.
- **T2** Zeitpunkt, zu dem die ursprüngliche Anfrage vom Client durch den Server erhalten wurde.
- **T3** Zeitpunkt, zu dem der Server eine Antwort gesendet hat.
- **T4** Zeitpunkt, zu dem der Client die Antwort des Clients erhalten hat.

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

Die Abfrage von Unicast-Informationen wird zur Abfrage bei einem Server verwendet, dessen IP-Adresse bekannt ist. SNTP-Server, die auf dem Gerät konfiguriert wurden, sind die einzigen, die auf Synchronisationsdaten abgefragt werden. T1-T4 werden zur Ermittlung der Serverzeit verwendet. Dies ist das bevorzugte Verfahren für die Synchronisierung der Gerätezeit, da es das sicherste Verfahren darstellt. Wenn dieses Verfahren ausgewählt wird, werden die SNTP-Daten nur von den SNTP-Servern akzeptiert, die über die Seite **SNTP-Server** für das Gerät definiert wurden.

Die Abfrage von Anycast-Informationen wird verwendet, wenn die IP-Adresse des Servers nicht bekannt ist. Wenn dieses Verfahren ausgewählt wird, können sämtliche sich im Netzwerk befindliche SNTP-Server Synchronisationsdaten senden. Das Gerät wird synchronisiert, wenn es aktiv Synchronisationsdaten anfordert. Die beste Antwort (niedrigstes Stratum), die von den ersten drei SNTP-Servern auf eine Anfrage nach Synchronisationsdaten eingeht, wird verwendet, um den Zeitwert einzustellen. Die Zeitlevels T3 and T4 werden zur Ermittlung der Serverzeit verwendet.

Bei der Abfrage von Zeitdaten für die Synchronisierung der Gerätezeit wird die Anycast-Abfrage gebenüber der Broadcast-Abfrage bevorzugt gewählt. Dieses Verfahren ist jedoch weniger sicher als die Unicast-Abfrage, da SNTP-Pakete von SNTP-Servern akzeptiert werden, die nicht für das Gerät konfiguriert wurden.

Broadcast-Informationen werden verwendet, wenn die IP-Adresse des Servers nicht bekannt ist. Wenn eine Broadcast-Meldung von einem SNTP-Server aus gesendet wird, wartet der SNTP-Client auf die Meldung. Wenn die Broadcast-Abfrage aktiviert wurde, werden sämtliche Synchronisationdaten akzeptiert, auch wenn sie nicht durch das Gerät angefragt wurden. Dies ist das am wenigsten sichere Verfahren.

Das Gerät empfängt die Synchronisationdaten entweder über das aktive Anfragen von Daten oder bei jedem Poll-Intervall. Wenn Unicast-, Anycast- und Broadcast-Abfrage aktiviert sind, werden die Daten in der folgenden Reihenfolge empfangen:

- Daten von im Gerät definierten Servern werden bevorzugt behandelt. Wenn die Unicast-Abfrage nicht aktiviert ist oder keine Server für das Geräte definiert wurden, akzeptiert das Gerät Zeitdaten von jedem antwortenden SNTP-Server.
- Wenn mehr als ein Unicast-Gerät antwortet, werden die Synchronisationdaten bevorzugt, die vom Gerät mit dem niedrigsten Stratum eingehen.
- Wenn sämtliche Server über das gleiche Stratum verfügen, werden die Synchronisationdaten des Servers akzeptiert, der als erster antwortet.

MD5 (Message Digest 5)-Authentifizierung schützt die Geräte-Synchronisierungspfade zu den SNTP-Servern. MD5 ist ein Algorithmus, der einen 128-Bit-Hash produziert. MD5 ist eine Variante von MD4 und bietet höhere Sicherheit als MD4. MD5 verifiziert die Integrität der Kommunikation und authentifiziert den Ursprung der Kommunikation.

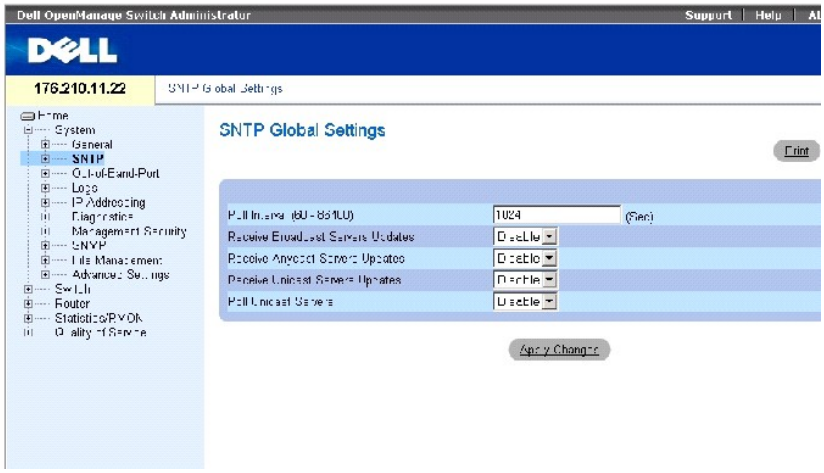
Die SNTP-Seite enthält Verknüpfungen zu Seiten, die es Netzwerkmanagern ermöglichen, SNTP-Parameter zu konfigurieren. Um die Seite **SNTP** zu öffnen, klicken Sie in der Strukturansicht auf **System→ SNTP**.

Definieren globaler SNTP-Parameter

Die Seite **Globale SNTP-Einstellungen** enthält Informationen zum Definieren von SNTP-Parametern.

Um die Seite **SNTP Global Settings** (Globale SNTP-Einstellungen) zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **SNTP**→ **Global Settings** (Globale Einstellungen).

Abbildung 6-7. Globale SNTP-Einstellungen



Die Seite **Globale SNTP-Einstellungen** enthält die folgenden Felder:

Poll Interval (Abfragungsintervall, 60-86400) Legt das Intervall (in Sekunden) fest, in dem Unicast-Informationen vom SNTP-Server abgefragt werden.

Receive Broadcast Servers Updates (Empfangen von Broadcast-Server-Aktualisierungen) Wartet, wenn aktiviert, auf den ausgewählten Schnittstellen auf Broadcast-Server-Zeitinformationen von den SNTP-Servern. Das Geräte wird immer dann synchronisiert, wenn ein SNTP-Paket empfangen wird, auch wenn keine Synchronisation angefordert wurde.

Receive Anycast Servers Updates (Empfangen von Anycast-Servers-Aktualisierungen) Fragt, wenn aktiviert, Anycast-Server-Zeitinformationen vom SNTP-Server ab. Das Gerät wird nur dann synchronisiert, wenn eine Synchronisationsanfrage durch das Gerät gesendet wurde.

Receive Unicast Servers Updates (Empfangen von Unicast-Server-Aktualisierungen) Fragt, wenn aktiviert, die SNTP-Server, die für das Gerät definiert wurden, nach Unicast-Serverzeitinformationen ab. Wenn die Felder **Receive Broadcast Servers Updates** (Empfangen von Broadcast-Server-Aktualisierungen), **Receive Anycast Servers Updates** (Empfangen von Anycast-Server-Aktualisierungen) und **Receive Unicast Servers Updates** (Empfangen von Unicast-Server-Aktualisierungen) alle aktiviert sind, wird die Serverzeit nach den Unicast-Server-Zeitinformationen eingestellt.

Poll Unicast Servers (Abfragen von Unicast-Servern) Sendet, wenn aktiviert, Anfragen zu SNTP-Unicast-Server-Zeitinformationen an den SNTP-Server.

Definieren globaler SNTP-Parameter mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Anzeige der Felder zusammengefasst, die auf der Seite **SNTP Global Settings** (Globale SNTP-Einstellungen) angezeigt werden.

Tabelle 6-5. CLI-Befehle für globale SNTP-Parameter

CLI-Befehl	Beschreibung

`sntp client poll timer seconds`	Definiert die Abfragezeit für den SNTP-Client.
`sntp broadcast client enable`	Aktiviert SNTP-Broadcast-Clients.
`sntp unicast client enable`	Aktiviert vordefinierte SNTP-Unicast-Clients.
`sntp unicast client poll`	Aktiviert abfragende vordefinierte Unicast-SNTP-Server.
`show sntp configuration`	Zeigt die SNTP-Konfiguration an.
`show sntp status`	Zeigt den SNTP-Status an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

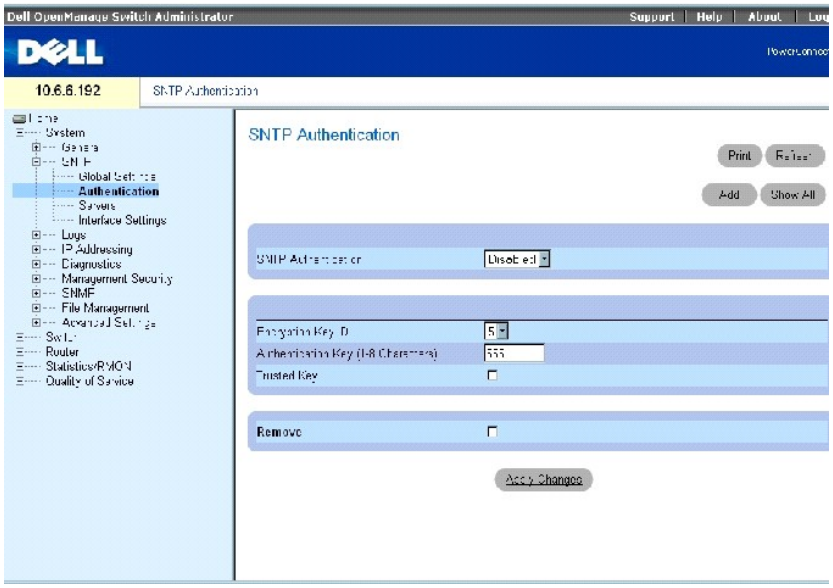
```
Console (config)# sntp anycast client enable
```

Definieren von SNTP-Authentifizierungsmethoden

Die Seite **SNTP-Authentifizierung** ermöglicht die SNTP-Authentifizierung zwischen dem Gerät und einem SNTP-Server. Der SNTP-Server wird auch auf der Seite **SNTP-Authentifizierung** ausgewählt.

Klicken Sie auf **System**→ **SNTP**→ **Authentication** in der Strukturansicht, um die Seite **SNTP Authentication** zu öffnen.

Abbildung 6-8. SNTP-Authentifizierung



Die Seite **SNTP-Authentifizierung** enthält die folgenden Felder:

SNTP Authentication (SNTP-Authentifizierung) Fordert, wenn aktiviert, die Authentifizierung einer SNTP-Sitzung zwischen dem Gerät und einem SNTP-Server.

Encryption Key ID (Verschlüsselungscode-ID) Enthält eine Liste mit benutzerdefinierten Schlüssel-IDs zur Authentifizierung des SNTP-Servers und des Geräts. Mögliche Werte sind 1-4294967295.

Authentication Key (**1-8** Zeichen) Schlüssel, der für die Authentifizierung verwendet wird.

Trusted Key (Verschlüsselung) Markieren Sie dieses Kontrollkästchen, um den Verschlüsselungscode (Unicast/Anycast, verwendet) oder (Broadcast, gewählt) zu definieren, um den SNTP-Server zu authentifizieren.

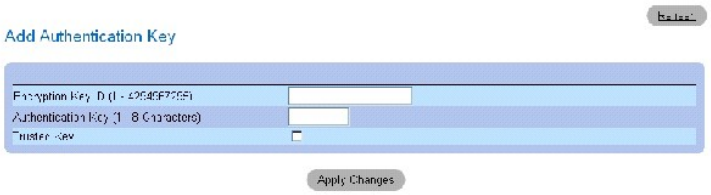
Remove (Entfernen) Markieren Sie dieses Kontrollkästchen, um den ausgewählten Authentifizierungsschlüssel zu entfernen.

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 geöffnet:

Abbildung 6-9. Hinzufügen eines Authentifizierungsschlüssels



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

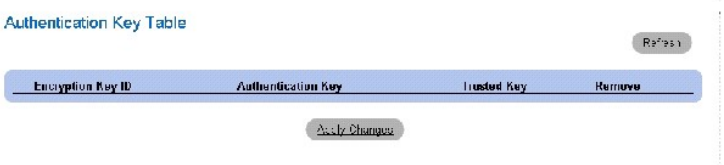
Der SNTP-Authentifizierungsschlüssel wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der Authentifizierungsschlüssel-Tabelle

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

Die Seite **Authentifizierungsschlüssel-Tabelle** wird geöffnet:

Abbildung 6-10. Authentifizierungsschlüssel-Tabelle



Löschen eines Authentifizierungsschlüssels

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

   Die Seite **Authentifizierungsschlüssel-Tabelle** wird geöffnet.
3. Wählen Sie einen Eintrag in der **Authentication Key Table** (Authentifizierungsschlüssel-Tabelle).
4. Wählen Sie das Kontrollkästchen **Remove**" (Entfernen).
5. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

   Der Eintrag wird entfernt und das Gerät wird aktualisiert.

Definieren der SNTP-Authentifizierungseinstellungen mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite **SNTP Authentication** angezeigt werden.

Tabelle 6-6. CLI-Befehle für SNTP-Authentifizierung

CLI-Befehl	Beschreibung
sntp authenticate	Definiert, um Authentifizierung für empfangenen Datenverkehr über das Network Time Protocol (NTP) von den Servern anzufordern.
sntp authentication-key *number* **md5** *value*	Legt einen Authentifizierungsschlüssel für SNTP fest.
sntp trusted-key key-number	Definiert den verwendeten Authentifizierungsschlüssel, um den SNTP-Server zu authentifizieren.
show sntp configuration	Zeigt die SNTP-Konfiguration an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

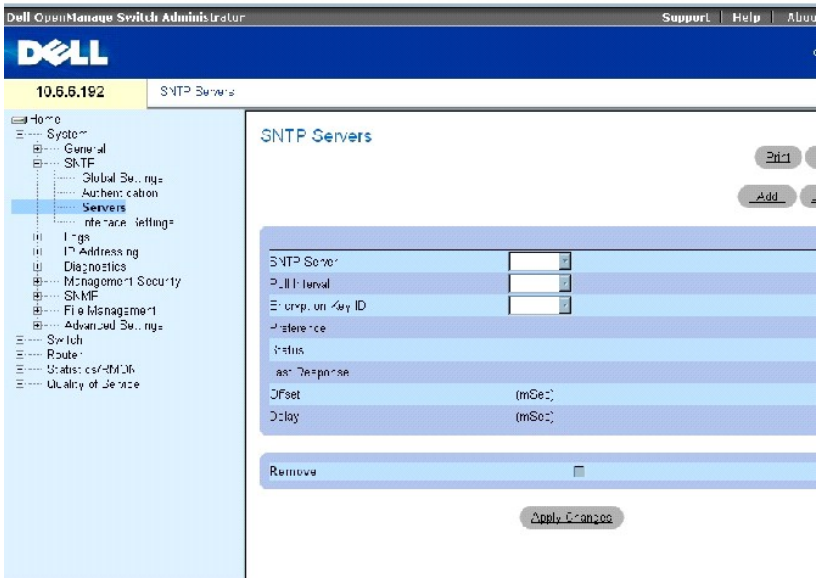
```
Console (config)# sntp authentication-key 8 md5 ClkKey

Console (config)# sntp trusted-key 8

Console (config)# sntp authenticate
```

Definieren von SNTP-Servern

Die Seite **SNTP Servers** enthält Informationen zur Aktivierung von SNTP-Servern sowie zum Hinzufügen von neuen SNTP-Servern.

Um die Seite **SNTP Servers** (SNTP-Server) zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **SNTP**→ **Servers** (SNTP-Server).

Abbildung 6-11. SNTP-Server



Die Seite **SNTP-Server** enthält die folgenden Felder:

SNTP Server (SNTP-Server) Enthält eine Liste von benutzerdefinierten IP-Adressen eines SNTP-Servers. Bis zu acht SNTP-Server können definiert werden.

Poll Interval (Abfrageintervall) Ermöglicht, wenn aktiviert, die Abfrage von Systemzeitinformationen vom ausgewählten SNTP-Server.

Encryption Key ID (Verschlüsselungscode-ID) Enthält eine Liste mit benutzerdefinierten Schlüssel-IDs für die Kommunikation zwischen SNTP-Server und Gerät. Die Verschlüsselungscode-ID wird auf der Seite **SNTP-Authentifizierung** definiert.

Preference (Vorrang) Gibt den SNTP-Server an, der die SNTP-Systemzeitinformation bereitstellt. Die möglichen Feldwerte sind:

Primary (Primär) Der primäre Server liefert SNTP-Informationen.

Secondary (Sekundär) Der Backup-Server liefert SNTP-Informationen.

Status Status des operativen SNTP-Servers. Die möglichen Feldwerte sind:

Up (In Betrieb) Der SNTP-Server funktioniert gegenwärtig normal.

Down Zeigt an, dass derzeit kein SNTP-Server verfügbar ist. Zum SNTP-Server besteht z. B. derzeit keine Verbindung oder er ist ausgeschaltet.

In progress Der SNTP-Server sendet oder empfängt gerade SNTP-Daten.

Unknown Der Fortschritt der gerade gesendeten SNTP-Daten ist unbekannt. So sucht das Geräte beispielsweise gerade nach einer Schnittstelle.

Last Response (Letzte Antwort) Gibt den letzte Zeitpunkt an, an dem vom SNTP-Server eine Antwort erhalten wurde.

Offset (Differenz) Die Zeitstempel-Differenz zwischen der lokalen Uhr des Geräts und der vom SNTP-Server bezogenen Zeit.

Delay (Verzögerung) Die Zeit, die es dauert, den SNTP-Server zu erreichen.

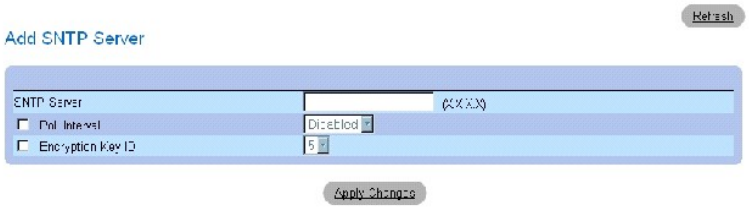
Remove (Entfernen) Markieren Sie dieses Kontrollkästchen, um einen bestimmten SNTP-Server aus der Liste **SNTP Servers** (SNTP-Server) zu entfernen.

Hinzufügen eines SNTP-Servers

1. Öffnen Sie die Seite **SNTP Servers**.
2. Klicken Sie auf **Add**" (Hinzufügen).

Die Seite **Add SNTP Server** (SNTP-Server hinzufügen) wird geöffnet:

Abbildung 6-12. Hinzufügen eines SNTP-Servers



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

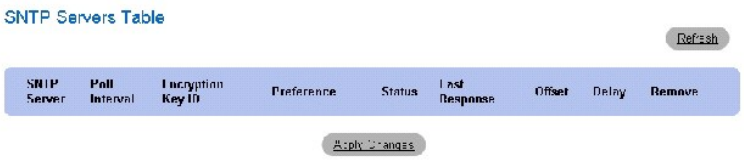
Der SNTP-Server wird hinzugefügt, und das wird Gerät aktualisiert.

Anzeigen der SNTP-Server-Tabelle

1. Öffnen Sie die Seite **SNTP Servers**.
2. Klicken Sie auf **Show All"** (Alle anzeigen).

Die Seite **SNTP-Server-Tabelle** wird geöffnet:

Abbildung 6-13. SNTP-Server-Tabelle



Ändern eines SNTP-Servers

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

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

3. Wählen Sie einen SNTP-Server-Eintrag.
4. Ändern Sie die betreffenden Felder.
5. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

Die SNTP-Serverinformationen werden aktualisiert.

Löschen des SNTP-Servers

1. Öffnen Sie die Seite **SNTP Servers**.
2. Klicken Sie auf **Show All**" (Alles anzeigen).

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

3. Wählen Sie einen **SNTP Server**-Eintrag.
4. Wählen Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

Der Eintrag wird entfernt und das Gerät wird aktualisiert.

Definieren von SNTP-Servern mithilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite **SNTP Servers** angezeigt werden.

Tabelle 6-7. CLI-Befehle für SNTP-Authentifizierung

CLI-Befehl	Beschreibung
sntp server {ip- address | hostname} [**poll**] [**key keyid**]	Definiert einen SNTP-Server, der für die Synchronisation von Zeitinformationen verwendet werden kann.
no sntp server ip- address	Entfernt einen Server aus der Liste der SNTP-Server.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

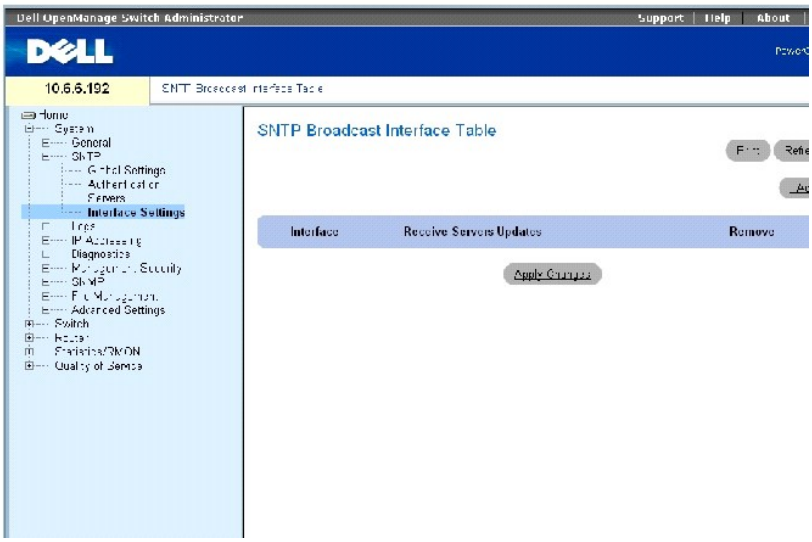
```
Console (config)# sntp server 100.1.1.1 poll key 10
```

Definieren von SNTP-Schnittstellen

Die **SNTP Broadcast Interface Table** (SNTP-Broadcast-Schnittstellentabelle) enthält Felder zur Einstellung von SNTP auf verschiedenen Schnittstellen.

Öffnen Sie die Seite **SNTP Broadcast Interface Table** (SNTP-Broadcast-Schnittstellentabelle), indem Sie auf **System→ SNTP→ Interfaces Settings** klicken.

Abbildung 6-14. SNTP-Broadcast-Schnittstellentabelle



Die **SNTP-Broadcast-Schnittstellentabelle** enthält die folgenden Felder:

Interface (Schnittstelle) Zeigt eine Liste von Schnittstellen an, auf denen SNTP aktiviert werden kann.

Receive Servers Updates (Empfangen von Server-Aktualisierungen) Aktiviert oder deaktiviert eingehende SNTP-Aktualisierungen auf einer bestimmten Schnittstelle.

Remove (Entfernen) Markieren Sie dieses Kontrollkästchen, um SNTP auf dieser Schnittstelle zu deaktivieren.

Aktivieren von SNTP auf einer Schnittstelle

1. Öffnen Sie die **SNTP-Broadcast-Schnittstellentabelle**.
2. Klicken Sie auf **Add**" (Hinzufügen).

   Die Seite **SNTP-Schnittstelle hinzufügen** wird geöffnet.
3. Definieren Sie die entsprechenden Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   SNTP wird auf der Schnittstelle aktiviert, und das Gerät wird aktualisiert.

Definieren der SNTP-Schnittstelleneinstellungen mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite **SNTP Broadcast Interface Table** angezeigt werden.

ANMERKUNG: Wenn Anycast- oder Broadcast-Schnittstellen definiert werden, muss mindestens eine IP-Adresse definiert sein.

Tabelle 6-8. CLI-Befehle zu SNTP-Schnittstellen-Einstellungen

CLI-Befehl	Beschreibung
	Aktiviert den SNTP-Broadcast- und Anycast-Client auf einer Schnittstelle.

sntp client enable	
show sntp configuration	Zeigt die SNTP-Konfiguration an.

Im folgenden Beispiel sind CLI-Befehle zum Konfigurieren von SNTP-Schnittstellen dargestellt:

```
Console (config)# interface ethernet g1
Console (config-if)# sntp client enable
Console (config-if)# end
Console# show sntp configuration
Polling interval: 7200 seconds.

MD5 Authentication keys: 8, 9
Authentication is required for synchronization.
Trusted Keys: 8,9

Unicast Clients Polling: Enabled.

Server          Polling          Encryption Key
-----------     --------         -----------------
176.1.1.8       Enabled (Aktiviert)   9
176.1.8.179     Disabled         Disabled

Broadcast Clients: Enabled (Aktiviert)
Broadcast Clients Poll: Enabled (Aktiviert)
Broadcast Interfaces: g1
```

Konfigurieren von bandexternen (OOB) Management-Ports

Dieser Abschnitt beschreibt die Verwaltung der folgenden Gerätefunktionen über den bandexternen Management-Port. Es beinhaltet auch Informationen über den bandexternen Remote-Protokollserver, das bandexterne Standard-Gateway, die bandexternen IP-Schnittstellenparameter, den bandexternen TACACS+-Server und den bandexternen RADIUS-Server.

Bei der Verwaltung dieser Funktionen mithilfe des bandexternen Management-Ports ist die bandinterne Verwaltung dieser Funktionen deaktiviert. Verwenden Sie die SNMP-Schnittstelle, um diese Funktionen über den bandexternen Port zu konfigurieren.

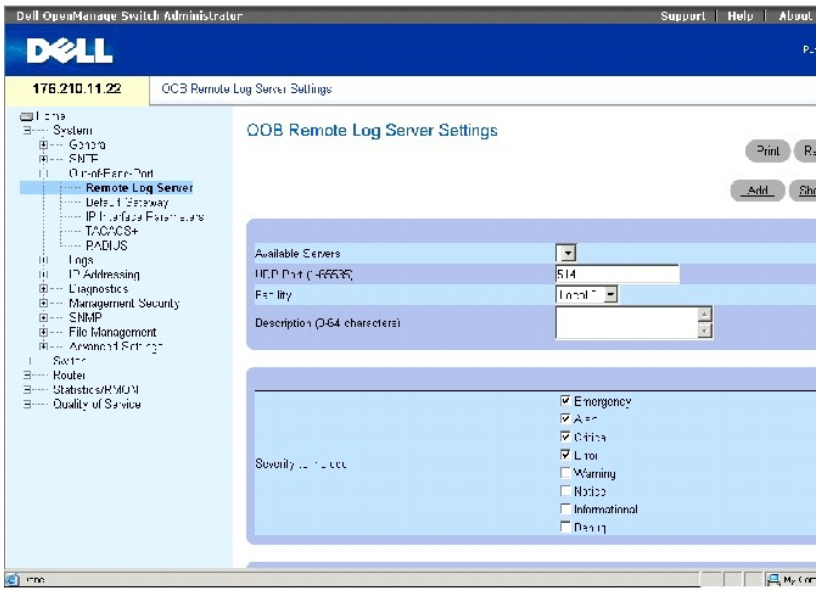
Um die Seite „OOB-Konfiguration" zu öffnen, klicken Sie in der Strukturansicht auf **System→ Out of Band**.

Konfigurieren der OBB-Remote-Protokollserver

Die Seite **OOB Remote Log Server Settings** (Einstellungen des OOB-Remote-Protokollservers) enthält Felder zur Ansicht der verfügbaren Protokollserver des bandexternen Ports. Zusätzlich können neue OBB-Protokollserver und der Schweregrad der an den Server geschickten Protokolle definiert werden.

Um die Seite **OOB-Remote-Protokollserver-Einstellungen** zu öffnen, klicken Sie in der Strukturansicht auf **System→ Out-of-Band Port→ Remote Log Server**.

Abbildung 6-15. OOB-Remote-Protokollserver-Einstellungen



Die Seite **OOB-Remote-Protokollserver-Einstellungen** enthält die folgenden Felder:

Available Servers (Verfügbare Server) Server, an die Protokolle gesendet werden können.

UDP Port (1-65535) (UDP-Port) Der UDP-Port, von dem die Protokolle verschickt werden. Der Standardwert ist 514.

Facility (Einrichtung) Eine benutzerdefinierte Anwendung, von der Systemprotokolle an den Remote-Server gesendet werden. Nur eine Einrichtungsebene kann einem einzelnen Server zugeordnet werden. Wenn eine zweite Einrichtungsebene zugeordnet wird, wird die erste Einrichtungsebene außer Kraft gesetzt. Alle Anwendungen, die für ein Gerät definiert sind, verwenden dieselbe Einrichtung auf einem Server. Folgende Feldwerte sind möglich: local 0, local 1, local 2, local 3, local 4, local 5, local 6 und local 7.

Description (0-64 characters) (Beschreibung (0-64 Zeichen)) Zeigt die benutzerdefinierte Server-Beschreibung an.

Severity to Include (Einzuschließender Schweregrad) Der Protokollschweregrad. Die Auswahl eines Schweregrads wählt automatisch alle höheren Schweregrade.

Delete Server (Server löschen) Wenn diese Option markiert ist, wird ein Server aus der Liste **Available Servers** (Verfügbare Server) gelöscht.

Die Seite OOB Remote Log Server Settings (Einstellungen des OOB-Remote-Protokollservers) enthält ebenfalls eine Schweregradliste. Die Schweregraddefinitionen sind dieselben wie die Schweregraddefinitionen in der RAM-Protokolltabelle.

Senden von Protokollen an einen bandexternen Protokollserver

1. Öffnen Sie die Seite **OOB Remote Log Server Settings** (Einstellungen des OOB-Remote-Protokollservers).
2. Definieren Sie die Felder **UDP Port** (UDP-Port), **Facility** (Einrichtung) und **Description** (Beschreibung).
3. Wählen Sie den Protokolltyp und den Protokollschweregrad.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Protokolleinstellungen werden gespeichert und das Gerät aktualisiert.

ANMERKUNG: Vor dem Hinzufügen eines neuen Servers müssen Sie die IP-Adresse des OBB-Remote-Protokollservers bestimmen.

Definieren eines neuen bandexternen Protokollservers

1. Öffnen Sie die Seite **OOB Remote Log Server Settings** (Einstellungen des OOB-Remote-Protokollservers).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add an OOB Log Server** (Einen OOB-Protokollserver hinzufügen) anzuzeigen.
3. Füllen Sie die Felder im Dialogfeld aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Server wird definiert und der Liste **Available Servers** (Verfügbare Server) hinzugefügt.

Löschen eines bandexternen Protokollservers

1. Öffnen Sie die Seite **OOB Remote Log Server Settings** (OOB-Remote-Protokollserver-Einstellungen).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **OOB Remote Log Servers Table** (OOB-Remote-Protokollservertabelle) anzuzeigen.
3. Wählen Sie einen Server, und markieren Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Server wird gelöscht und das Gerät aktualisiert.

Konfigurieren von OBB-Remote-Server-Protokollen unter Verwendung von CLI-Befehlen

Die folgende Tabelle fasst die CLI-Befehle für das Arbeiten mit Feldern auf der Seite OOB-Remote-Protokollserver-Einstellungen zusammen.

Tabelle 6-9. CLI-Befehle für Remote-Protokollserver-Einstellungen

CLI-Befehl	Beschreibung
logging *oob/ip- address* [**port** *port*][**severity** *level*] [**facility** *facility*][**description** *text*]	Definiert einen neuen Remote-Protokollserver.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)#logging oob/10.2.2.2 severity critical facility local0 description syslog_server_1
```

Definieren von OBB-Standard-Gateways

Verwenden Sie die Seite **OOB Default Gateway** (OOB-Standard-Gateways) für die Zuordnung von Gateway-Geräten. Pakete werden zur standardmäßigen IP weitergeleitet, wenn Frames an ein Fernnetzwerk geschickt werden. Die konfigurierte IP-Adresse muss zu demselben IP-Adressen-Teilnetz einer der IP-Schnittstellen gehören. Entfernen der IP-Schnittstelle, mit der ein Standard-Gateway verbunden ist, entfernt auch das Standard-Gateway.

Um die Seite **OBB-Standard-Gateway** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **Out-of-Band Port**→ **Default Gateway**.

Abbildung 6-16. OOB-Standard-Gateway

Die Seite **OOB-Standard-Gateway** enthält die folgenden Parameter:

Default Gateway (Standard-Gateway) Zeigt die IP-Adresse des Gateways an.

Auswählen eines OBB-Gateway-Geräts

1. Öffnen Sie die Seite **OOB Default Gateway** (OOB-Standard-Gateway).
2. Definieren Sie eine IP-Adresse in dem Feld **Default Gateway** (Standard-Gateway).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das OBB-Gateway-Gerät wurde definiert, und das Gerät wurde aktualisiert.

Tabelle 6-10. CLI-Befehle für OBB-Standard-Gateways

CLI-Befehl	Beschreibung
`ip default gateway` *ip- address*	Definiert das OBB-IP-Gateway.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface out-of-band-eth
```

```
Console (config-oob)# ip address 10.0.0.1 /8
```

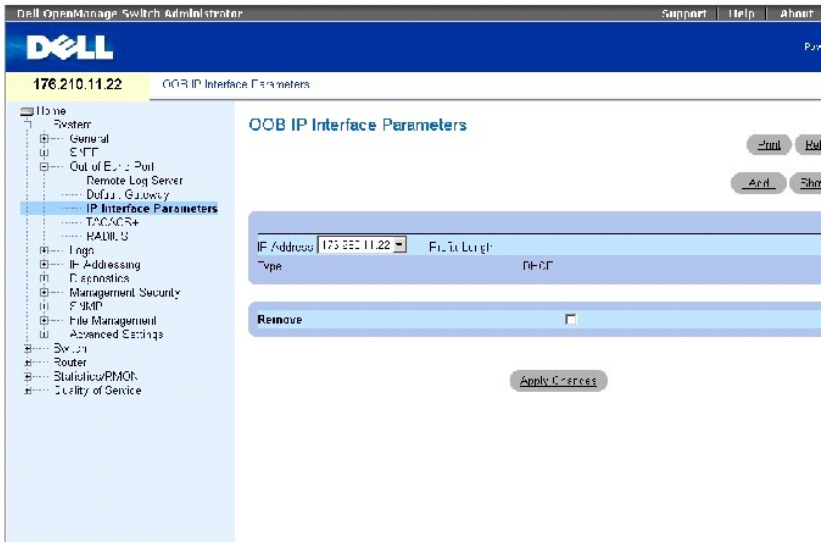
```
Console (config-oob)# ip default-gateway 10.1.1.1
```

Definieren von OBB-IP-Schnittstellenparametern

Die Seite **OBB-IP-Schnittstellenparameter** enthält Parameter für die Zuordnung von bandexternen IP-Adressen zu Schnittstellen.

Um die Seite **OBB-IP-Schnittstellenparameter** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **Out-of-Band Port**→ **IP Interface Parameters**.

Abbildung 6-17. OBB-IP-Schnittstellenparameter



Die Seite **OBB-IP-Schnittstellenparameter** enthält die folgenden Parameter:

IP Address (IP-Adresse) Die bandexterne IP-Adresse der Schnittstellen.

Prefix Length (Präfixlänge) Gibt die Anzahl der Bits an, die das Präfix der Quell-IP-Adresse enthält, oder die Netzwerkmaske der Quell-IP-Adresse.

Type (Typ) Die Methode, mit der die OBB-IP-Schnittstelle erstellt wurde; DHCP oder statisch.

Remove (Entfernen) Wenn diese Option markiert ist, wird die Schnittstelle aus der Liste der Drop-Down-Liste **IP Address** (IP-Adresse) entfernt.

ANMERKUNG: Sie können DHCP-IP-Adressen für Out of Band-Management auf der Seite DHCP-IP-Schnittstelle (**System**→ **IP Address**→ **DHCP IP Interface**) konfigurieren.

Hinzufügen einer IP-Schnittstelle

1. Öffnen Sie die Seite **OOB IP Interface Parameters** (Bandexterne IP-Schnittstellenparameter).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add a Static OOB IP Interface** (Eine statische bandexterne IP-Schnittstelle hinzufügen) zu öffnen.
3. Das Feld **Network Mask** (Netzwerkmaske) spezifiziert die Teilnetzwerkmaske der Quellen-IP-Adresse.
4. Geben Sie die Daten in die Felder auf der Seite ein.

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

Die neue Schnittstelle wird hinzugefügt und das Gerät aktualisiert.

Löschen von IP-Adressen

1. Öffnen Sie die Seite **OOB IP Interface Parameters** (Bandexterne IP-Schnittstellenparameter).
2. Klicken Sie auf **Show All** (Alle anzeigen).
3. Die Seite **Schnittstellenparametertabelle** wird geöffnet.
4. Wählen Sie eine IP-Adresse aus der Drop-Down-Liste **IP Address** (IP-Adresse).
5. Wählen Sie einen Eintrag in der **Interface Parameters Table** (Schnittstellenparametertabelle).
6. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
7. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die IP-Adresse wird gelöscht und das Gerät aktualisiert.

Definieren der IP-Schnittstellen mithilfe der CLI-Befehle

Die folgende Tabelle fasst die CLI-Befehle für das Arbeiten mit den Feldern auf der Seite **OBB-IP-Schnittstellenparameter** zusammen.

Tabelle 6-11. CLI-Befehle für OBB-IP-Schnittstellenparameter

CLI-Befehl	Beschreibung
`interface out-of- band-eth`	Konfiguriert den bandexternen Ethernet-Port und stellt den Konfigurationsmodus für Schnittstellen ein.
`ip address ip- address {mask | prefix-length}`	Stellt eine IP-Adresse ein.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip address 192.168.0.1 /8
```

Konfigurieren von OBB-TACACS+-Servern

Die Geräte stellen Terminal Access Controller Access Control System (TACACS+)-Client-Support bereit. TACACS+ stellt eine zentralisierte Sicherheit zur Validierung von Benutzern, die auf das Gerät zugreifen, dar.

TACACS+ stellt ein zentralisiertes Benutzerverwaltungssystem dar, das jedoch mit RADIUS und anderen Authentifizierungsprozessen übereinstimmt. TACACS+ stellt die folgenden Dienste bereit:

- **Authentication** (Authentifizierung) Stellt Authentifizierung bei der Anmeldung und über Benutzernamen und benutzerdefinierte Kennwörter bereit.
- **Authorization** (Berechtigung) Wird bei der Anmeldung ausgeführt. Nach Abschluss der Authentifizierungssitzung beginnt eine Authentifizierungssitzung mit dem authentifizierten Benutzernamen. Der TACACS+-Server überprüft die Benutzerrechte.

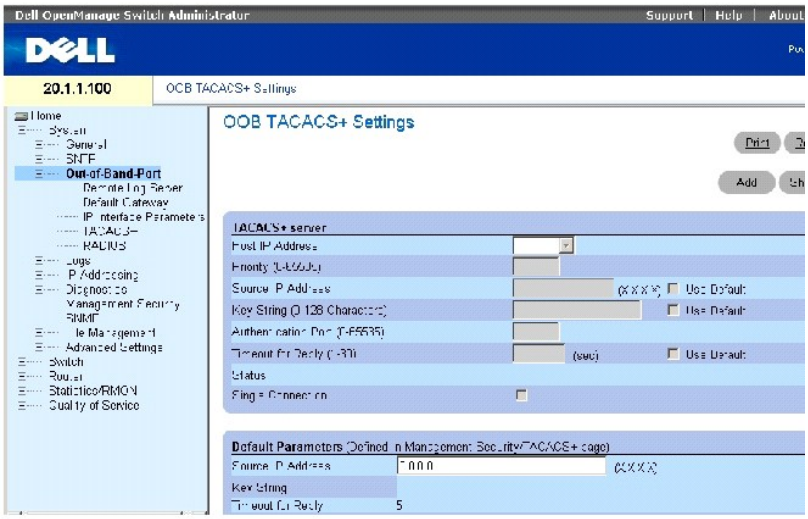
TACACS+ Server können auf bandinternen Ports auf der Seite **TACACS+-Einstellungen** oder auf dem bandexternen Port konfiguriert werden.

Das TACACS+-Protokoll stellt die Netzwerkintegrität mittels verschlüsselter Protokollaustausche zwischen dem Gerät und dem TACACS+-Server sicher.

Die Seite **OBB-TACACS+-Einstellungen** enthält sowohl benutzerdefinierte als auch standardmäßige TACACS+-Einstellungen für den Out of Band-Management-Port.

Öffnen Sie die Seite **Bandexterne TACACS+-Einstellungen**, und klicken Sie in der Strukturansicht auf **System→ Out-of-Band-Port→ TACACS+**.

Abbildung 6-18. OBB-TACACS+-Einstellungen



Die Seite **OBB-TACACS+-Einstellungen** enthält die folgenden Felder:

Host IP Address Gibt die IP-Adresse des TACACS+-Servers an.

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

Source IP Address (Quell-IP-Adresse) Die Quell-IP-Adresse des Geräts, die für die TACACS+-Sitzung zwischen dem Gerät und dem TACACS+-Server verwendet wird.

Key String (Schlüssel-Zeichenkette, 0-128 Zeichen) Legt den Authentifizierungs- und Verschlüsselungscode für die TACACS+-Kommunikation zwischen dem Gerät und dem TACACS+-Server fest. Dieser Schlüssel muss mit der auf dem TACACS+-Server verwendeten Verschlüsselung übereinstimmen.

Authentication Port (0-65535) Die Portnummer, über die die TACACS+-Sitzung erfolgt. Port 49 ist der Standardport.

Reply Timeout (Antwort-Zeitlimit, 1-30) Die Zeit, die vergeht, bis das Zeitlimit der Verbindung zwischen dem Gerät und dem TACACS+-Server erreicht wird. Es sind Werte im Feldbereich von 1-30 möglich.

Status Der Verbindungsstatus zwischen dem Gerät und dem TACACS+-Server. Die möglichen Feldwerte sind:

Connected (Verbunden) Zwischen dem Gerät und dem TACACS+-Server ist gegenwärtig eine Verbindung aufgebaut.

Not Connected (Nicht verbunden) Zwischen dem Gerät und dem TACACS+-Server ist gegenwärtig keine Verbindung aufgebaut.

Single Connection (Einzige Verbindung) Erhält, wenn ausgewählt, eine einzige offene Verbindung zwischen dem Gerät und dem TACACS+-Server aufrecht

Die TACACS+-Standardparameter sind benutzerdefinierte Standards. Die Standardeinstellungen werden auf neu definierte TACACS+-Server angewendet. Wenn keine Standardwerte definiert sind, werden die Systemstandardwerte auf die neuen TACACS+-Server angewendet. Die TACACS+-Standardwerte lauten:

Source IP Address (Quell-IP-Adresse) Die Quell-IP-Adresse des Geräts, die für die TACACS+-Sitzung zwischen dem Gerät und dem TACACS+-Server verwendet wird.

Key String (Schlüssel-Zeichenkette, 0-128 Zeichen) Legt den Authentifizierungs- und Verschlüsselungscode für die TACACS+-Kommunikation zwischen dem Gerät und dem TACACS+-Server fest.

Timeout for Reply (Antwort-Zeitlimit, 1-30) Die Standardzeit, die vergeht, bis das Timelimit der Verbindung zwischen dem Gerät und dem TACACS+Server erreicht wird.

ANMERKUNG: Sie können die Werte für oben genannte Standardeinstellungen auf der Seite **TACACS+-Einstellungen** (**System**→ **Management Security**→ **TACACS+**) definieren.

Definieren von TACACS+-Parametern

1. Öffnen Sie die Seite **OBB-TACACS+-Einstellungen**.
2. Definieren Sie die Felder.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die TACACS+-Einstellungen werden in dem Gerät aktualisiert.

Hinzufügen eines TACACS+-Servers

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

Die Seite **OOB-TACACS+-Host hinzufügen** wird geöffnet.

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

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

Löschen eines TACACS+-Servers von der Liste der TACACS+-Server

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

Die Seite **TACACS+-Tabelle** wird geöffnet.

3. Wählen Sie einen Eintrag in der **TACACS+-Tabelle**.
4. Wählen Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

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

Definieren der TACACS+-Server mithilfe von CLI-Befehlen

Die folgende Tabelle fasst die CLI-Befehle für das Arbeiten mit Feldern auf der Seite **OBB-TACACS+-Einstellungen** zusammen.

Tabelle 6-12. CLI-Befehle für OBB-TACACS+-Einstellungen

CLI-Befehl	Beschreibung
`tacacs-server host {oob/ip-address | hostname} [single-connection] [port port-number] [timeout timeout] [key key-string] [source source] [priority priority]`	Definiert einen TACACS+-Server-Host.
`no tacacs-server host {ip-address | hostname}`	Löscht einen bestimmten TACACS+-Server-Host.
`tacacs-server key [key-string]`	Definiert den Authentifizierungs- und Verschlüsselungscode, der für die gesamte TACAS-Kommunikation zwischen dem Gerät und dem TACACS+-Server verwendet wird. Dieser Schlüssel muss mit der auf dem TACACS-Daemon verwendeten Verschlüsselung übereinstimmen. (Bereich: 0-128 Zeichen)
`no tacacs-server key`	Standardeinstellung wird wiederhergestellt.
`tacacs-server timeout` *timeout*	Gibt den Zeitlimit-Wert in Sekunden an. (Bereich: 1-30)
`no tacacs-server timeout`	Standardeinstellung wird wiederhergestellt.
`tacacs-server source-ip` *oob/ip-address*	Gibt eine Quell-IP-Adresse an. (Bereich: Gültige IP-Adresse)
`no tacacs-server source-ip` *oob/ip-address*	Standardeinstellung wird wiederhergestellt.
`show tacacs [oob/ip-address]`	Zeigt die Konfiguration und Statistiken für einen TACACS+-Server an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# tacacs-server host oob/172.16.8.1 key abc

Console (config)# end

Console# show tacacs

                                                                    

Gerätekonfiguration

--------------------                                                

IP address:  Status     Port  Single Connection  TimeOut  Source IP  Priority
-----------  ---------  ----  -----------------  -------  ---------  --------

Es wurde kein TACACS-Server konfiguriert.

                                                                    

OOB-Host-Konfiguration

IP address:  Status     Port  Single Connection  TimeOut  Source IP  Priority
```

----------	---------	----	----------	--------	------	--------
172.16.8.1	Not Connected	49	Nein	globalem	globalem	0
Globale Werte						

TimeOut: 5						
Gerätekonfiguration						

Source IP: 0.0.0.0 (Versant-Produktversion: 6.0.0.1)						
OOB-Host-Konfiguration						

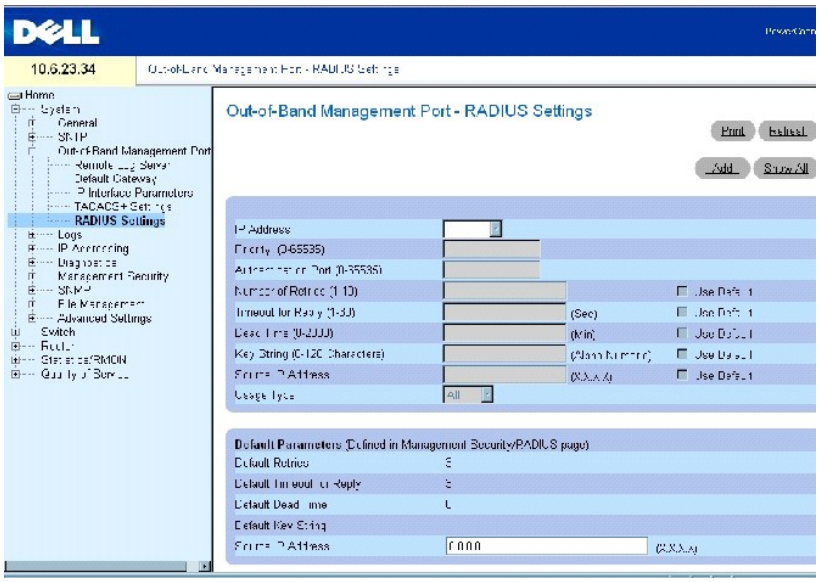
Source IP : 0.0.0.0						

Konfigurieren von OBB-RADIUS-Servern

Die Seite **OOB-RADIUS-Einstellungen** enthält sowohl benutzerdefinierte als auch standardmäßige RADIUS-Einstellungen für den Out of Band-Management-Port. Weitere Informationen zu RADIUS-Servern finden Sie unter Konfigurieren von TACACS+-Einstellungen.

Um die Seite **OOB-RADIUS-Einstellungen** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **Out-of-Band Port**→ RADIUS (siehe OOB-RADIUS-Einstellungen, Abbildung 6-19).

Abbildung 6-19. OOB-RADIUS-Einstellungen



Die Seite **OOB-RADIUS-Einstellungen** enthält die folgenden Felder:

IP Address (IP-Adresse) Die IP-Adresse für die Authentifizierung des bandexternen Ports.

Priority (0-65535) (Priorität) Die Priorität des bandexternen Ports. Die möglichen Werte sind 0-65535.

Authentication Port (Authentifizierungsport) Der Authentifizierungsport, der zum Überprüfen der RADIUS-Server-Authentifizierung verwendet wird.

Number of Retries (1-10) (Anzahl der Versuche) Anzahl der übermittelten Anfragen, die an den RADIUS-Server gesendet werden, bevor ein Fehler auftritt. Die möglichen Feldwerte sind 1-10. Der Standardwert ist 3. Wenn kein hostspezifischer Wert festgelegt ist, gilt der globale Wert für alle Hosts.

Timeout for Reply (1-30) (Zeitüberschreitung bei Antwort) Zeitdauer (in Sekunden), die das Gerät auf eine Antwort vom RADIUS-Server wartet, bevor die Zeit überschritten ist. Die möglichen Feldwerte sind 1-30. Der Standardwert ist 3. Wenn kein hostspezifischer Wert festgelegt ist, gilt der globale Wert für alle Hosts.

Dead Time (0-2000) (Totzeit) Zeitdauer (in Minuten), die ein RADIUS-Server für Serviceanfragen deaktiviert wird. Der Bereich ist 0-2000. Wenn kein hostspezifischer Wert festgelegt ist, gilt der globale Wert für alle Hosts.

Key String (0-128 Characters) (Schlüsselzeichenkette (0-128 Zeichen) Schlüsselzeichenkette, die für die Authentifizierung und Verschlüsselung der gesamten RADIUS-Kommunikation zwischen dem Gerät und dem RADIUS-Server verwendet wird. Der Schlüssel muss der RADIUS-Verschlüsselung entsprechen. Wenn kein hostspezifischer Wert festgelegt ist, gilt der globale Wert für alle Hosts.

Source IP Address (Quellen-IP-Adresse) IP-Adresse des Geräts, das auf den RADIUS-Server zugreift.

Die RADIUS-Standardparameter sind benutzerdefinierte Standards. Die Standardeinstellungen werden auf neu definierte RADIUS-Server angewendet. Wenn keine Standardwerte definiert sind, werden die Systemstandardwerte auf die neuen RADIUS-Server angewendet. Die RADIUS-Standardwerte lauten:

Default Timeout for Reply (Standardmäßiges Zeitlimit für Antwort) Standardmäßige Zeitdauer, die das Gerät auf eine Antwort vom RADIUS-Server wartet, bevor das Zeitlimit erreicht ist.

Default Retries (sec) (Standardmäßige Versuche (in Sekunden)) Standardmäßige Anzahl der übermittelten Anfragen, die an RADIUS-Server gesendet werden, bevor ein Fehler auftritt.

Default Dead Time (sec) (Standardmäßige Totzeit (in Sekunden) Standardmäßige Zeitdauer (in Minuten), die ein RADIUS-Server für Serviceanfragen deaktiviert wird. Der Bereich ist 0-2000.

Default Key String (Standardmäßige Schlüsselzeichenkette) Standardmäßige Schlüsselzeichenkette, die für die Authentifizierung und Verschlüsselung der gesamten RADIUS-Kommunikation zwischen dem Gerät und dem RADIUS-Server verwendet wird. Der Schlüssel muss der RADIUS-Verschlüsselung entsprechen.

ANMERKUNG: Sie können die Werte für die oben genannten Standardeinstellungen auf der Seite RADIUS-Einstellungen (**System→ Management Security→ RADIUS**) definieren.

Source IP Address (Quellen-IP-Adresse) Standardmäßige IP-Adresse eines Geräts, das auf den RADIUS-Server zugreift.

Definieren von OBB-RADIUS-Parametern

1. Öffnen Sie die Seite **OOB RADIUS Settings** (OOB-RADIUS-Einstellungen).
2. Definieren Sie die folgenden Felder: **Default Timeout for Reply** (Standardmäßiges Zeitlimit für Antwort), **Default Retries** (Standardmäßige Anzahl der Versuche), **Default Dead Time** (Standardmäßige Totzeit) und **Default Key** (Standardmäßiger Schlüssel).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die RADIUS-Einstellungen werden in dem Gerät aktualisiert.

Hinzufügen eines OBB-RADIUS-Servers

1. Öffnen Sie die Seite **OOB RADIUS Settings** (OOB-RADIUS-Einstellungen).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add OOB RADIUS Server** (OOB-RADIUS-Server hinzufügen) anzuzeigen.
3. Füllen Sie die Felder im Dialogfeld aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

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

Löschen eines OBB-RADIUS-Servers aus der Liste der RADIUS-Server

1. Öffnen Sie die Seite **OOB RADIUS Settings** (OOB-RADIUS-Einstellungen).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Liste **OOB RADIUS Servers** (OOB-RADIUS-Server) anzuzeigen.
3. Wählen Sie einen RADIUS-Server, und markieren Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der RADIUS-Server wird von der Liste der RADIUS-Server entfernt.

Definieren der RADIUS-Server mithilfe der CLI-Befehle

Die folgende Tabelle fasst die CLI-Befehle zum Arbeiten mit Feldern auf der Seite **OOB-RADIUS-Einstellungen** zusammen.

Tabelle 6-13. CLI-Befehle für OBB-RADIUS-Einstellungen

CLI-Befehl	Beschreibung
`radius-server host` *`ip- address`* `[auth-port` *`auth- port-number`*`] [timeout` *`timeout`*`] [retransmit retries] [deadtime` *`deadtime`*`] [key` *`key- string`*`] [source` *`source`*`] [priority` *`priority`*`]`	Spezifiziert einen RADIUS-Serverhost.
	Löscht einen spezifizierten RADIUS-Serverhost.

`no radius-server host ip-address`	
`radius-server source-ip source`	Spezifiziert die Quellen-IP-Adresse, die für die Kommunikation mit RADIUS-Servern verwendet wird.
`no radius-server-ip`	Stellt Standardeinstellung wieder her.
`radius-server timeout timeout`	Stellt die Zeitdauer ein, die ein Router auf die Antwort des Serverhosts wartet.
`no radius-server deadtime`	Stellt die Totzeit auf 0.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface out-of-band eth 1
```

```
Console radius-server host oob/10.2.2.2 key 123
```

Verwalten von Protokollen

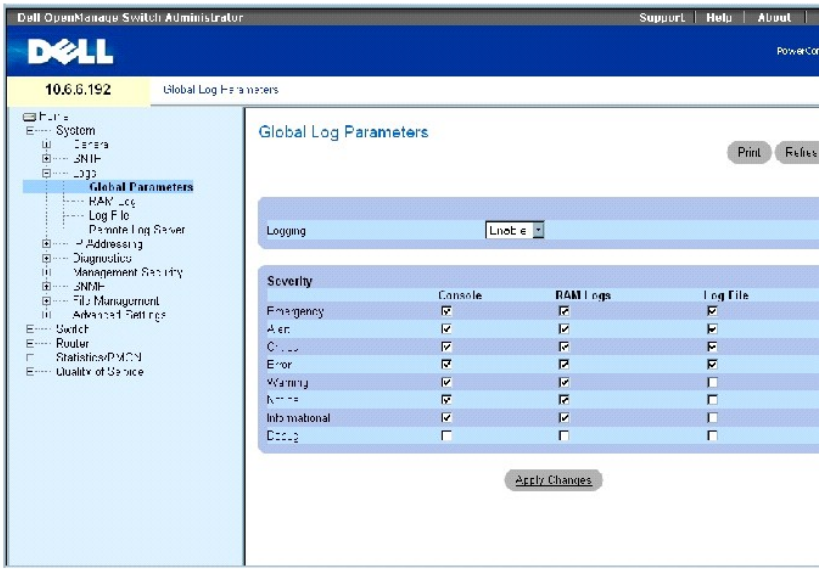
Die Seite **Logs** (Protokolle) enthält Links zu verschiedenen Protokollseiten. Um die Seite **Protokolle** anzuzeigen, klicken Sie in der Strukturansicht auf **System**→ **Logs**.

Globale Protokollparameter

Die Seite **Globale Protokollparameter** enthält Felder zum globalen Aktivieren von Protokollen und Felder zum Definieren von Protokollparametern. Die Protokollmeldungen **Severity** (Schweregrad) werden vom höchsten Schweregrad zum niedrigsten aufgelistet.

Öffnen Sie die Seite **Globale Protokollparameter**, indem Sie auf **System**→ **Logs**→ **Global Parameters** in der *Strukturansicht* klicken.

Abbildung 6-20. Globale Protokollparameter



Die Seite **Globale Protokollparameter** enthält die folgenden Felder:

Logging (Protokollführung) Ermöglicht die Erstellung globaler Geräteprotokolle in Form von Cache-, Datei- und Serverprotokollen. Alle Protokolle, die auf der Konsole gedruckt werden, werden in den Protokolldateien gespeichert. Die möglichen Feldwerte sind:

Enable (Aktivieren) Aktiviert das Speichern von Protokollen in Cache (RAM), Datei (FLASH) und einem externen Server.

Disable (Deaktivieren) Deaktiviert das Speichern von Protokollen. Es ist nicht möglich, die Aufzeichnung von Protokollen zu deaktivieren, die auf der Konsole gedruckt werden.

Emergency (Notfall) Stellt die höchste Warnstufe dar. Wenn das Gerät ausgefallen ist oder nicht ordnungsgemäß funktioniert, wird ein Notprotokoll auf dem Gerät gespeichert.

Alert (Alarm) Stellt die zweithöchste Warnstufe dar. Ein Meldungsprotokoll wird gespeichert, wenn eine schwere Gerätefehlfunktion aufgetreten ist, wie z. B. alle Gerätefunktionen sind ausgefallen.

Critical (Kritisch) Stellt die dritthöchste Warnstufe dar. Ein kritisches Protokoll wird gespeichert, wenn eine kritische Gerätefehlfunktion auftritt, z. B. zwei Geräteports funktionieren nicht, während der Rest der Geräteports funktioniert.

Error (Fehler) Ein Gerätefehler ist aufgetreten, z.B. wenn ein Port offline ist.

Warning (Warnung) Entspricht der niedrigsten Gerätewarnstufe.

Notice (Hinweis) Stellt dem Netzwerkadministrator Gerätedaten zur Verfügung.

Informational (Zur Information) Liefert Geräteinformationen.

Debug (Debug) Stellt ausführliche Informationen über das Protokoll zur Verfügung. Debuggen sollte nur von qualifiziertem Support-Personal vorgenommen werden.

Die Kontrollkästchen erscheinen unter den folgenden drei Spalten:

Console (Konsole) Protokolle, die an die Konsole gesendet wurden.

RAM Logs (RAM-Protokolle) Protokolle, die an den (Cache) RAM gesendet wurden.

Log File (Protokolldatei) Protokolle, die an die Datei (FLASH) gesendet wurden.

Aktivieren von Protokollen

1. Öffnen Sie die Seite **Global Log Parameters** (Globale Protokollparameter).
2. Wählen Sie **Enable** (Aktivieren) in dem Drop-Down-Menü **Logging** (Protokollierung).
3. Verwenden Sie die Kontrollkästchen, um den Protokolltyp und den Schweregrad auszuwählen.

ANMERKUNG: Wenn Sie einen Schweregrad auswählen, werden alle höheren Schweregrade automatisch ausgewählt.

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

Die Protokolleinstellungen werden gespeichert und das Gerät aktualisiert.

Aktivieren der globalen Protokolle mithilfe der CLI

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für die Arbeit mit Feldern zusammen, die auf der Seite **Globale Protokollparameter** angezeigt werden.

Tabelle 6-14. CLI-Befehle für globale Protokollparameter

CLI-Befehl	Beschreibung
`logging on (Protokollführung läuft)`	Aktiviert die Protokollierung von Fehlermeldungen.
`logging ip-address[port port] [severity level] [facility facility] [description text]`	Protokolliert Meldungen auf einem Syslog-Server.
`logging console level`	Beschränkt die Protokollierung auf der Konsole auf Fehlermeldungen des angegebenen Schweregrads.
`logging buffered level (Protokollzwischenspeicherebene)`	Beschränkt die Anzeige von Syslog-Meldungen aus einem internen Pufferspeicher (RAM) auf Meldungen des angegebenen Schweregrads.
`logging file [level]`	Beschränkt das Senden von Syslog-Meldungen an die Protokolldatei auf Meldungen des angegebenen Schweregrads.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# logging on

Console (config)# logging 10.1.1.1 severity critical

Console (config)# logging Console errors
```

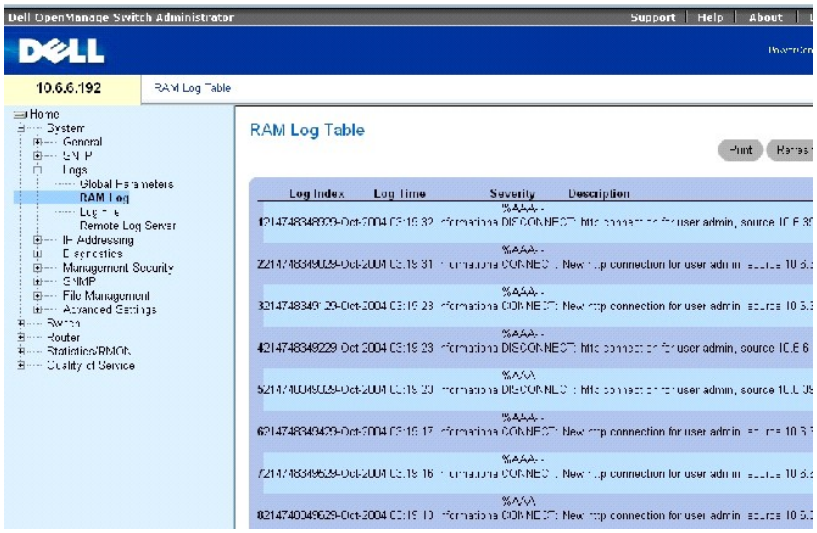
```
Console (config)# logging buffered debugging


Console (config)# logging file alerts



Console # clear logging


Clear Logging Buffer [y/n]? y
```

RAM-Protokolltabelle

Die **RAM-Protokolltabelle** enthält Informationen zu bestimmten Protokolleinträgen im RAM (Cache), einschließlich der Uhrzeit, zu der das Protokoll aufgezeichnet wurde, des Protokollschweregrads und einer Beschreibung des Protokolls.

Um die **RAM-Protokolltabelle** anzuzeigen, klicken Sie in der Strukturansicht auf **System**→ **Logs**→ **RAM Log** (siehe Abbildung 6-21).

Abbildung 6-21. RAM-Protokolltabelle



Die **RAM-Protokolltabelle** enthält die folgenden Felder:

Log Index (Protokollverzeichnis) Gibt die Protokollnummer innerhalb der Protokoll-RAM-Tabelle an.

Log Time (Protokollzeitpunkt) Der Zeitpunkt, zu dem das Protokoll in die Protokoll-RAM-Tabelle eingegeben wurde.

Severity (Schweregrad) Der Schweregrad des Protokolls.

Description (Beschreibung) Die Beschreibung des Protokolls.

Entfernen von Protokollinformationen

1. Öffnen Sie die Seite **RAM Log Table** (RAM-Protokolltabelle).
2. Klicken Sie auf **Clear Logs** (Protokolle löschen).

Die Protokollinformationen werden aus der Protokolldateitabelle entfernt und das Gerät aktualisiert.

Anzeigen der RAM-Protokolltabelle mithilfe der CLI

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für die Ansicht von Feldern in der RAM-Protokolltabelle zusammen.

Tabelle 6-15. CLI-Befehle für die RAM-Protokolltabelle

CLI-Befehl	Beschreibung
show logging	Zeigt den Protokollierungsstatus und die im internen Pufferspeicher enthaltenen Syslog-Meldungen an.
clear logging (Protokollierung löschen)	Löscht Meldungen vom Protokollzwischenspeicher.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console # show logging

Console Logging: Level info. Console Messages: 0 Dropped.

Buffer Logging: Level info. Buffer Messages: 30 Logged, 30 Displayed, 200 Max.

File Logging: Level error. File Messages: 1 Logged, 30 Dropped.

1 messages were not logged

10-Jan-2003 16:53:44 :%MSCM-I-NEWTERM: New TELNET connection from 143.166.155.18


10-Jan-2003 16:53:14 :%MSCM-I-TERMTERMINATED: TELNET connection from 143.166.155.18 terminated


10-Jan-2003 16:41:26 :%MSCM-I-NEWTERM: New TELNET connection from 143.166.155.18

10-Jan-2003 09:24:59 :%INIT-I-Startup: Cold Startup
```

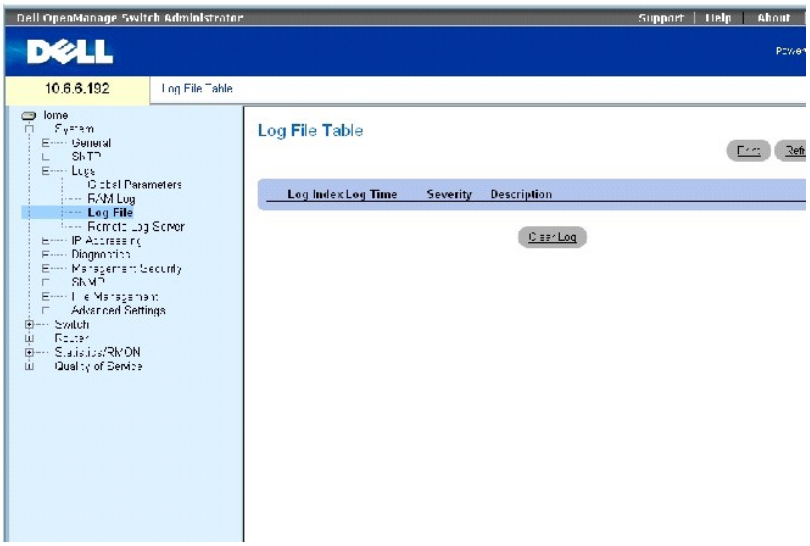
Protokolldateitabelle

Die Seite **Protokolldateitabelle** enthält Informationen zu bestimmten Protokolleinträgen, einschließlich der Uhrzeit, zu der das Protokoll eingegeben wurde,

des Schweregrads des Protokolls und einer Beschreibung des Protokolls.

Um die Seite **Protokolldateitabelle** anzuzeigen, klicken Sie in der Strukturansicht auf **System**→ **Logs**→ **Log File** (siehe Tabelle 6-22).

Abbildung 6-22. Protokolldateitabelle (Log File Table)



Die Seite Protokolldateitabelle enthält die folgenden Felder:

- **Log Index** (Protokollverzeichnis) Die Protokollnummer innerhalb der **Log File Table** (Protokolldateitabelle).
- **Log Time** (Protokollzeitpunkt) Der Zeitpunkt, zu dem das Protokoll in die **Log File Table** (Protokolldateitabelle) eingegeben wurde.
- **Severity** (Schweregrad) Der Schweregrad des Protokolls.
- **Description** (Beschreibung) Die Beschreibung des Protokolls.

Anzeigen der Protokolldateitabelle mithilfe der CLI

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für die Ansicht von Feldern auf der Seite **Log File Table** (Protokolldateitabelle) zusammen.

Tabelle 6-16. CLI-Befehle für die Protokolldateitabelle (Log File Table)

CLI-Befehl	Beschreibung
`show logging file`	Zeigt den Zustand der Protokollierung und die in der Protokolldatei gespeicherten Syslog-Meldungen an.
`clear logging (Protokollierung löschen)`	Löscht Meldungen vom Protokollzwischenspeicher.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console # show logging file

Console Logging: Level info. Console Messages: 0 Dropped.
```

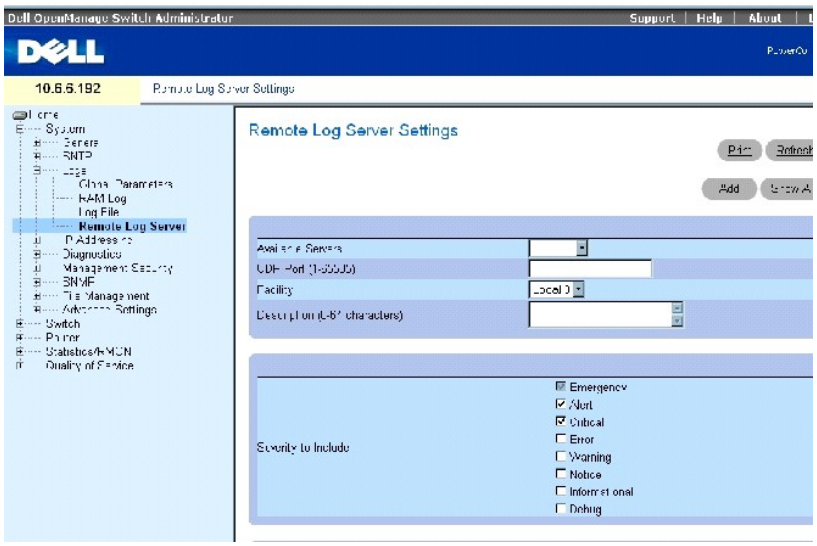
```
Buffer Logging: Level info. Buffer Messages: 30 Logged, 30 Displayed, 200 Max.

File Logging: Level error. File Messages: 1 Logged, 30 Dropped.

1 messages were not logged

10-Jan-2003 16:53:44 :%MSCM-I-NEWTERM: New TELNET connection from 143.166.155.18

10-Jan-2003 16:53:14 :%MSCM-I-TERMTERMINATED: TELNET connection from 143.166.155.18 terminated

10-Jan-2003 16:41:26 :%MSCM-I-NEWTERM: New TELNET connection from 143.166.155.18

10-Jan-2003 09:24:59 :%INIT-I-Startup: Cold Startup

10-Jan-2003 09:22:51 :%LINK-I-Up: Oob-eth 1

10-Jan-2003 09:22:51 :%LINK-W-Down: g24

10-Jan-2003 09:22:51 :%LINK-W-Down: g23

10-Jan-2003 09:22:51 :%LINK-W-Down: g22

10-Jan-2003 09:22:51 :%LINK-W-Down: g21
```

Remote Log Server (Remote-Protokollserver)

Die Seite **Remote-Protokollserver-Einstellungen** enthält Felder zur Anzeige der verfügbaren Protokollserver. Zusätzlich können neue Protokollserver und der Schweregrad der an den Server geschickten Protokolle definiert werden.

Um die Seite **Remote-Protokollserver-Einstellungen** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **Logs**→ **Remote Log Server**.

Abbildung 6-23. Einstellungen des Remote-Protokollservers



Die Seite **Remote-Protokollserver-Einstellungen** enthält die folgenden Felder:

Available Servers (Verfügbare Server) Server, an die Protokolle gesendet werden können.

UDP Port (1-65535) (UDP-Port) Der UDP-Port, von dem die Protokolle gesendet werden. Der Standardwert ist 514.

Facility (Einrichtung) Eine benutzerdefinierte Anwendung, von der Systemprotokolle an den Remote-Server gesendet werden. Nur eine Einrichtungsebene kann einem einzelnen Server zugeordnet werden. Wenn eine zweite Einrichtungsebene zugeordnet wird, wird die erste Einrichtungsebene außer Kraft gesetzt. Alle Anwendungen, die für ein Gerät definiert sind, verwenden dieselbe Einrichtung auf einem Server. Die möglichen Feldwerte lauten **Local 0** - **Local 7**.

Description (Beschreibung) Die Beschreibung des Servers. Die maximale Länge beträgt 64 Zeichen.

Severity (Schweregrad) Der Schweregrad des Protokolls. Die Auswahl eines Schweregrads wählt automatisch alle höheren Schweregrade.

Delete Server (Server löschen) Löscht einen Server aus der Liste **Available Server** (Verfügbare Server). Durch Markieren des Kontrollkästchens wird der Server von der Liste gelöscht. Indem das Kontrollkästchen nicht markiert wird, verbleibt der Server auf der Liste.

Die Seite **Remote Log Server Settings** (Remote-Protokollserver-Einstellungen) enthält ferner eine Liste der Schweregrade. Die Schweregraddefinitionen sind dieselben wie die Schweregraddefinitionen auf der Seite **RAM Log Table** (RAM-Protokolltabelle).

Verschicken von Protokollen an einen Server:

1. Öffnen Sie die Seite **Remote Log Server Settings**.
2. Definieren Sie die Felder **UDP Port** (UDP-Port), **Facility** (Einrichtung) und **Description** (Beschreibung).
3. Wählen Sie den Protokolltyp und den Schweregrad des Protokolls, indem Sie die Kontrollkästchen **Log Parameters** (Protokollparameter) verwenden.

ANMERKUNG: Wenn Sie einen Schweregrad auswählen, werden alle höheren Schweregrade automatisch ausgewählt.

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

Die Protokolleinstellungen werden gespeichert und das Gerät aktualisiert.

Definieren eines neuen Servers

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

ANMERKUNG: Vor Hinzufügen eines neuen Servers bestimmen Sie die IP-Adresse des Remote-Protokollservers.

3. Füllen Sie die Felder in dem Dialogfeld aus und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Seite **Remote-Protokollserver-Einstellungen** zeigt den Server in der Liste **Available Server** (Verfügbare Server) erst dann an, wenn Sie die Seite manuell aktualisiert haben.

Löschen eines Protokollservers

1. Öffnen Sie die Seite **Remote Log Server Settings**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **Protokollservertabelle** anzuzeigen.
3. Wählen Sie einen Server, und markieren Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Server wird gelöscht und das Gerät aktualisiert.

Arbeiten mit Remote-Serverprotokollen mithilfe der CLI-Befehle

Die folgende Tabelle führt die CLI-Befehle für die Arbeit mit Protokollen von Remote-Servern auf.

Tabelle 6-17. CLI-Befehle für Remote-Serverprotokolle

CLI-Befehl	Beschreibung
`logging ip-address [port port] [severity level] [facility facility] [description text]`	Protokolliert Meldungen auf einem Remote-Server.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config) # logging 10.1.1.1 severity critical
```

Definieren der IP-Adressierung

Auf der Seite **IP-Adressierung** können Sie Schnittstellen- und Standard-Gateways-IP-Adressen zuordnen und ARP- und DHCP-Parameter für die Schnittstellen definieren.

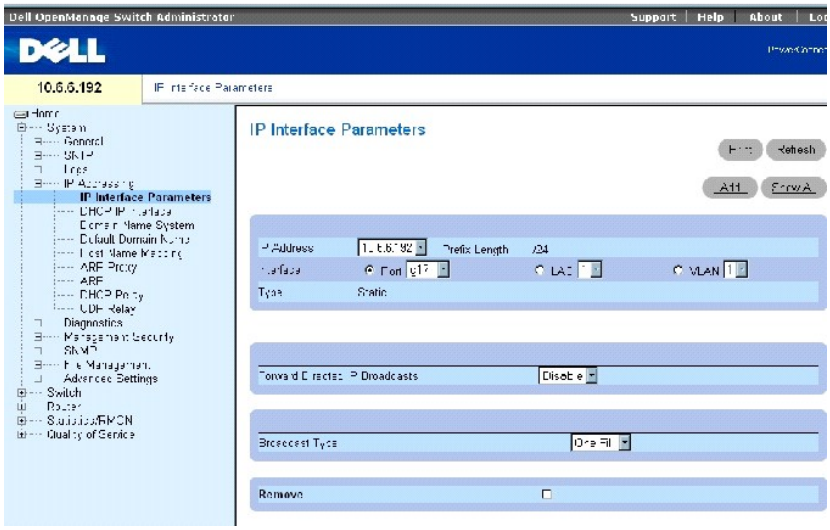
Öffnen Sie die Seite **IP Addressing"**, indem Sie auf **System→ IP Addressing** in der *Strukturansicht* klicken.

Definieren von IP-Schnittstellen

Die Seite **IP-Schnittstellenparameter** enthält Parameter für die Zuordnung von IP-Adressen zu Schnittstellen.

Öffnen Sie die Seite **IP Interface Parameters**, indem Sie auf **System**→ **IP Addressing**→ **Interface Parameters** in der *Strukturansicht* klicken.

Abbildung 6-24. IP-Schnittstellenparameter



Die Seite **IP-Schnittstellenparameter** enthält die folgenden Felder:

IP Address Gibt die IP-Adresse der Schnittstelle an.

Prefix Length (Präfixlänge) Gibt die Anzahl der Bits an, die das Präfix der Quell-IP-Adresse enthält, oder die Netzwerkmaske der Quell-IP-Adresse.

Interface Legt den Schnittstellentyp fest, für den die ausgewählte IP-Adresse definiert ist. Mögliche Werte sind: **Port**, **LAG** oder **VLAN**.

Weitere Informationen über das Konfigurieren von Link Aggregated Groups (LAGs) finden Sie unter Aggregieren von Ports. Informationen über das Konfigurieren von VLANs finden Sie unter Konfigurieren von VLANs.

Type (Typ) Gibt an, ob die IP-Adresse als statische IP-Adresse konfiguriert wurde.

Forward Directed IP Broadcasts (Vorwärtsgerichtete IP-Broadcasts) Ermöglicht die Umsetzung einer adressierten Broadcast in physische Broadcasts. Deaktiveren lässt IP-Directed Broadcasts fallen und leitet sie nicht weiter.

Broadcast Type (Broadcast-Typ) Definiert eine Broadcast-Adresse für die Schnittstelle.

One Fill gibt an, dass die Schnittstellen-Broadcast-Adresse One Fill (255.255.255.255) ist.

Zero Fill gibt an, dass die Schnittstellen-Broadcast-Adresse Zero Fill (0.0.0.0) ist.

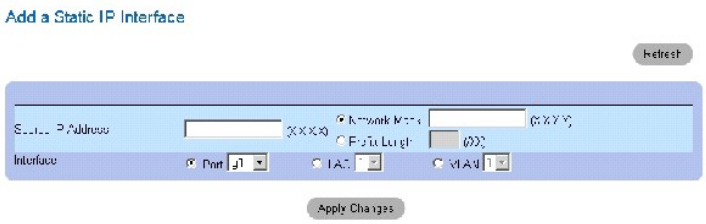
Remove (Entfernen) Wenn diese Option markiert ist, wird die Schnittstelle aus dem Drop-Down-Menü **IP Address** (IP-Adresse) entfernt.

Hinzufügen einer IP-Schnittstelle

1. Öffnen Sie die Seite **IP Interface Parameters** (IP-Schnittstellenparameter).

2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Statische IP-Adresse hinzufügen** zu öffnen.

Abbildung 6-25. Hinzufügen einer statischen IP-Schnittstelle



3. Geben Sie die Informationen in die Felder auf der Seite ein.

   Network Mask (Netzwerkmaske) gibt die Subnetzmaske der Quell-IP-Adresse an.

   Jeder Teil der IP-Adresse muss mit einer Zahl beginnen, die ungleich 0 (Null) ist. So sind z. B. die IP-Adressen 001.100.192.6 und 192.001.10.3 unzulässig.

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

   Die neue Schnittstelle wird hinzugefügt und das Gerät aktualisiert.

Modifizieren der IP-Adressenparameter

1. Öffnen Sie die Seite **IP Interface Parameters** (IP-Schnittstellenparameter).
2. Wählen Sie eine IP-Adresse im Drop-Down-Menü **IP Address** (IP-Adresse) aus.
3. Ändern Sie die entsprechenden Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Parameter werden geändert und das Gerät aktualisiert.

Löschen von IP-Adressen

1. Öffnen Sie die Seite **IP Interface Parameters** (IP-Schnittstellenparameter).
2. Klicken Sie auf **Show All** (Alle anzeigen) um die **Seite Interface Parameters Table** (Schnittstellenparametertabelle) anzuzeigen.
3. Wählen Sie eine IP-Adresse und aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die IP-Adresse wird gelöscht und das Gerät aktualisiert.

Definieren von IP-Schnittstellenparametern mithilfe von CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für das Arbeiten mit Feldern auf der Seite IP-Schnittstellenparameter zusammen.

Tabelle 6-18. CLI-Befehle für IP-Schnittstellen

CLI-Befehl	Beschreibung
`ip address` *`ip-address`* `{mask | prefix-length}`	Stellt eine IP-Adresse ein.

`no ip address [ip- address]`	Entfernt eine IP-Adresse.
`show ip interface [ethernet s | vlan vlan- id | port-channel number]`	Zeigt den Nutzbarkeitsstatus von Schnittstellen an, die für IP konfiguriert wurden.
`directed-broadcast`	Aktiviert die Übersetzung eines Directed Broadcasts in physische Broadcasts.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

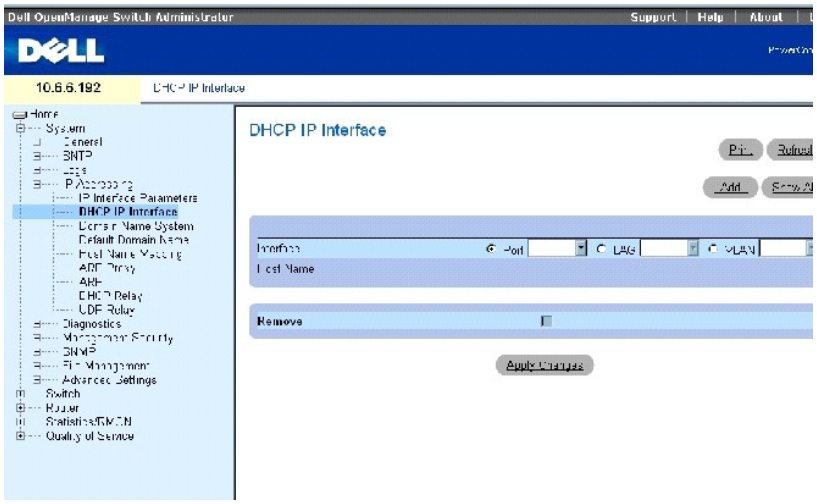
```
Console (config)# interface vlan 1

Console (config-if)# ip address 192.168.1.1 255.255.255.0

Console (config-if)# no ip address 192.168.1.1
```

Definieren von DHCP IP-Schnittstellenparametern

Die Seite **DHCP-IP-Schnittstelle** bestimmt die DHCP-Clients, die mit dem Gerät verbunden sind.

Um die Seite **DHCP-IP-Schnittstelle** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **IP Addressing**→ **DHCP IP Interface**.

Abbildung 6-26. DHCP IP-Schnittstelle



Die Seite **DHCP-IP-Schnittstelle** enthält die folgenden Felder:

Interface (Schnittstelle) Gibt die spezielle am Gerät angeschlossene Schnittstelle an. Klicken Sie auf die Optionsschaltfläche neben **Port**, **LAG** oder **VLAN** und wählen Sie die am Gerät angeschlossene Schnittstelle aus.

Host Name Gibt den Systemnamen an.

Remove (Entfernen) Wenn diese Option aktiviert ist, werden DHCP-Clients entfernt.

Hinzufügen von DHCP-Clients

1. Öffnen Sie die Seite **DHCP IP Interface** (DHCP IP-Schnittstelle).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add DHCP IP Interface** (DHCP-IP-Schnittstelle hinzufügen) zu öffnen.
3. Vervollständigen Sie die Informationen auf der Seite und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die DHCP-Schnittstelle wird hinzugefügt und das Gerät aktualisiert.

Ändern einer DHCP-IP-Schnittstelle

1. Öffnen Sie die Seite **DHCP IP Interface** (DHCP IP-Schnittstelle).
2. Ändern Sie die entsprechenden Felder.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag wird geändert und das Gerät aktualisiert.

Löschen einer DHCP-IP-Schnittstelle

1. Öffnen Sie die Seite **DHCP IP Interface** (DHCP IP-Schnittstelle).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **DHCP-IP-Schnittstellentabelle anzuzeigen**.
3. Wählen Sie einen DHCP-Client-Eintrag aus.
4. Klicken Sie das Kontrollkästchen **Remove** (Entfernen) an.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag wird entfernt und das Gerät aktualisiert.

Definieren der DHCP-IP-Schnittstellen mithilfe der CLI-Befehle

Die folgende Tabelle enthält den CLI-Befehl für das Definieren von DHCP-Clients.

Tabelle 6-19. CLI-Befehle für DHCP-IP-Schnittstellen

CLI-Befehl	Beschreibung
`ip address dhcp [hostname` *`hostname`*`]`	Zum Erhalten einer IP-Adresse oder Ethernet-Schnittstelle vom Dynamic Host Configuration Protocol (DHCP)

Im Folgenden werden CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config-if)# ip address dhcp hostname LA01
```

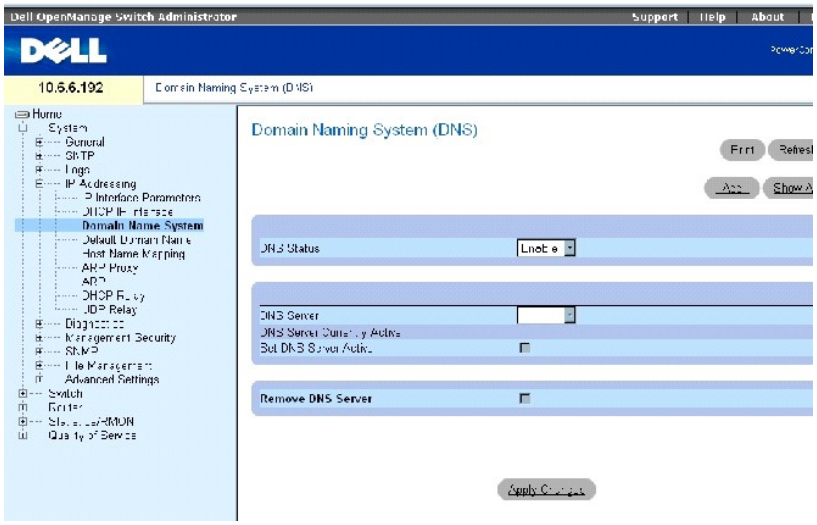
Konfigurieren von Domänennamensystemen (DNS)

DNS (Domain Name System) konvertiert benutzerdefinierte Domänennamen in IP-Adressen. Bei jeder Zuweisung eines Domänennamens wandelt der DNS-Service den Namen in eine numerische IP-Adresse um. Beispielsweise wird www.ipexample.com konvertiert in 192.87.56.2. DNS-Server führen Datenbanken mit Domänennamen und ihren entsprechenden IP-Adressen.

Die Seite **Domain Naming System (DNS)** enthält Felder zur Aktivierung von speziellen DNS-Servern.

Öffnen Sie die Seite **Domain Naming System (DNS)**, indem Sie auf **System→ IP Addressing→ Domain Name System** in der *Strukturansicht* klicken.

Abbildung 6-27. Domain Naming System (DNS)



Die Seite **DNS-Server** enthält die folgenden Felder:

DNS Status Aktiviert/deaktiviert die Konversion von DNS-Namen in IP-Adressen.

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

DNS Server Currently Active Der derzeit aktive DNS-Server.

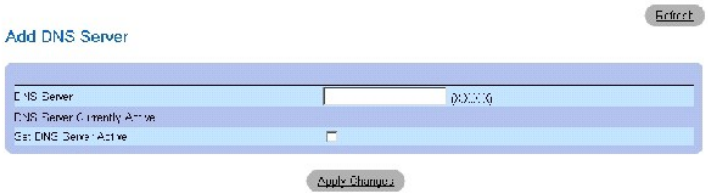
Remove DNS Server (DNS-Server entfernen) Entfernt, wenn ausgewählt, den ausgewählten DNS-Server.

Hinzufügen eines DNS-Servers

1. Öffnen Sie die Seite **Domain Naming System (DNS)**.
2. Klicken Sie auf **Add** (Hinzufügen).

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

Abbildung 6-28. Hinzufügen eines DNS-Servers



Die Seite **DNS-Server hinzufügen** enthält die folgenden Felder:

DNS Server (DNS-Server) Bestimmt die IP-Adresse des DNS-Servers.

DNS Server Currently Active (Derzeit aktiver DNS-Server) Zeigt den derzeit aktiven DNS-Server an.

Set DNS Server Active (DNS-Server aktivieren) Markieren Sie dieses Kontrollkästchen, um den DNS-Server als aktiven DNS-Server zu bestimmen.

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

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

Anzeigen der DNS-Server-Tabelle

1. Öffnen Sie die Seite **Domain Naming System (DNS)**.
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die Seite **DNS-Servertabelle** wird geöffnet:

Abbildung 6-29. DNS-Server-Tabelle

Entfernen von DNS-Servern

1. Öffnen Sie die Seite **Domain Naming System (DNS)**.
2. Klicken Sie auf **Show All** (Alle anzeigen).
3. Die Seite **DNS-Servertabelle** wird geöffnet.
4. Wählen Sie einen Eintrag in der **DNS Server Table**.
5. Wählen Sie das Kontrollkästchen **Remove** (Entfernen).
6. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

Der ausgewählte DNS-Server wird gelöscht und das Gerät wird aktualisiert.

Konfigurieren von DNS-Servern mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle für die Konfiguration der DNS-Server.

Tabelle 6-20. CLI-Befehle für DNS-Server

CLI-Befehl	Beschreibung
ip name-server *server-address*	Stellt die verfügbaren DNS-Namensserver ein. Bis zu acht DNS-Namensserver können eingestellt werden.
no ip name-server *server-address*	Entfernt einen DNS-Namensserver.
ip domain-name *name*	Definiert einen Standarddomänennamen, mit dem die Software nicht-qualifizierte Hostnamen vervollständigt. (Bereich: 1-58 Zeichen)
no ip domain-name	Löscht den standardmäßigen Domänennamen (DNS).
clear host {name | *}	Löscht Einträge aus dem host name-to-address"-Cache.
show hosts [*name*]	Zeigt den Standarddomänennamen, eine Liste der DNS-Namensserver-Hosts, die statische und die gecachte Liste der Hostnamen und Adressen an.
ip domain-lookup	Aktiviert das DNS-System für die Übertragung von Hostnamen in IP-Adressen.
no ip domain-lookup	Deaktiviert das DNS-System für die Übertragung von Hostnamen zu IP-Adressen.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

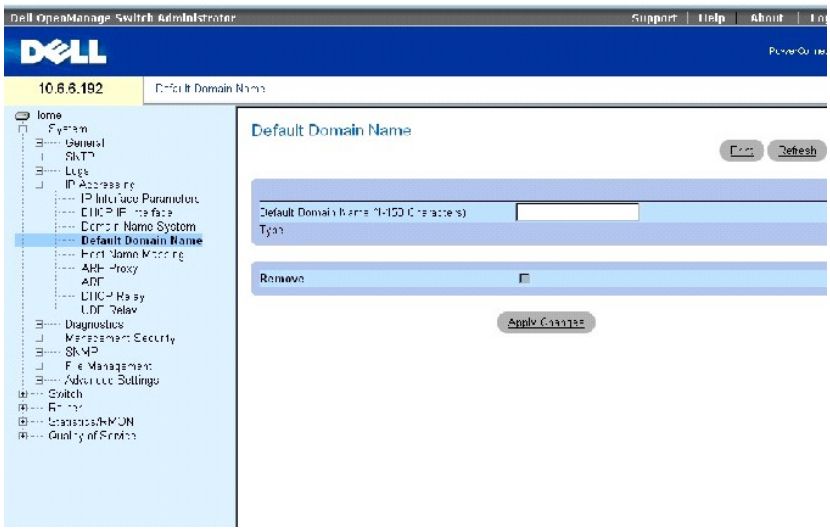
```
Console (config)# ip name-server 176.16.1.18
```

Definieren von Standarddomänen

Die Seite **Default Domain Name** (Standard-Domänenname) enthält Informationen zur Definition der Standard-DNS-Domänennamen.

Zum Öffnen der Seite **Default Domain Name** (Standard-Domänenname) klicken Sie in der Strukturansicht auf **System** (System)→ **IP Addressing** (IP-Adressierung)→ **Default Domain Name** (Standard-Domänenname).

Abbildung 6-30. Standard-Domänenname



Die Seite **Standard-Domänenname** enthält die folgenden Felder:

Default Domain Name (1-158 Zeichen) Enthält einen benutzerdefinierten DNS-Server. Der Standard-Domänenname wird, wenn entsprechend konfiguriert, auf alle unqualifizierten Hostnamen angewendet.

Type (Typ) Zeigt an, dass der Standard-Domänenname dynamisch oder statisch erstellt wurde.

Remove (Entfernen) Entfernt, wenn ausgewählt, den Standard-Domänennamen.

Definieren von DNS-Domänennamen mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Konfiguration der DNS-Domänennamen.

Tabelle 6-21. CLI-Befehle für DNS-Domänennamen

CLI-Befehl	Beschreibung
ip domain-name name	Definiert einen Standarddomänennamen, mit dem die Software nicht-qualifizierte Hostnamen vervollständigt.
no ip domain-name	Löscht den Standard-Domänennamen (DNS).
show hosts [*name***]**	Zeigt den Standarddomänennamen, eine Liste der DNS-Namensserver-Hosts, die statische und die gecachte Liste der Hostnamen und Adressen an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

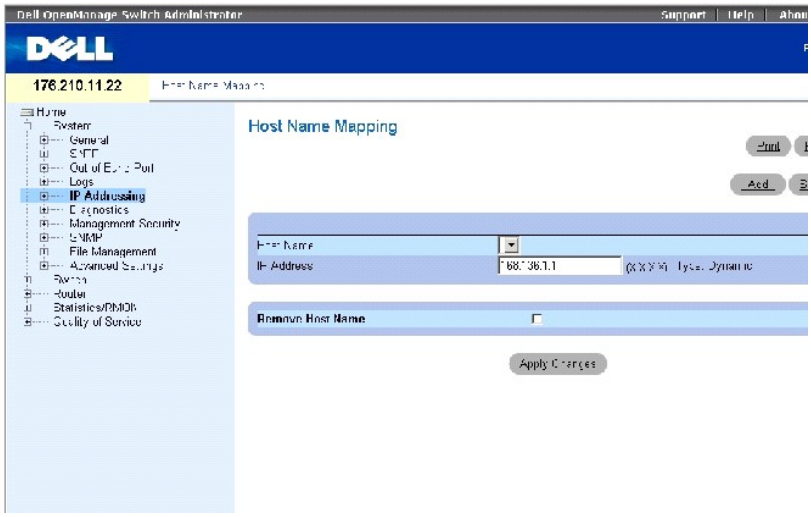
Console (config)# **ip domain-name** dell.com

Zuweisen von Domänenhosts

Die Seite **Zuweisen von Hostnamen** enthält Parameter für die Zuordnung einer IP-Adresse zu einem statischen Hostnamen. Die Seite **Host Name Mapping** (Zuweisung von Hostnamen) liefert eine IP-Adresse pro Host.

Öffnen Sie die Seite **Host Name Mapping**, indem Sie auf **System→ IP Addressing→ Host Name Mapping klicken**.

Abbildung 6-31. Zuweisung von Hostnamen



Die Seite **Zuweisen von Hostnamen** enthält die folgenden Felder:

Host Name (Hostname) Enthält eine Liste der Hostnamen. Hostnamen werden auf der Seite **Hostnamen-Zuweisung hinzufügen** definiert. Jeder Host liefert eine IP-Adresse.

IP Address (X.X.X.X) Liefert eine IP-Adresse, die dem spezifizierten Hostnamen zugewiesen wird.

Type Der IP-Adressentyp. Die möglichen Feldwerte sind:

Dynamic Die IP-Adresse wurde dynamisch erstellt.

Static Die IP-Adresse ist statisch.

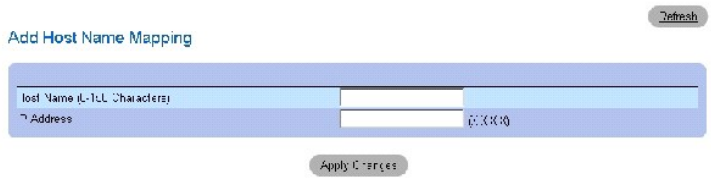
Remove Host Name (Hostnamen entfernen) Entfernt, wenn aktiviert, die DNS-Hostzuweisung.

Hinzufügen von Host-Domänennamen

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

Die Seite **Add Host Name Mapping** (Zuweisen von Hostnamen) wird geöffnet:

Abbildung 6-32. Zuweisen von Hostnamen



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

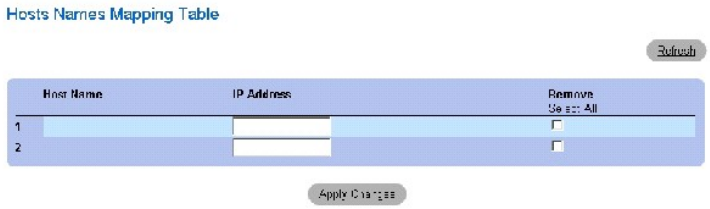
Die IP-Adresse wird dem Hostnamen zugewiesen, und das Gerät wird aktualisiert.

Anzeigen der Zuweisungstabelle für Hostnamen

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

Die Seite Hostnamenzuweisungstabelle wird geöffnet:

Abbildung 6-33. Hostnamenzuweisungstabelle



Entfernen eines Hostnamen aus der IP-Adresszuweisung

1. Öffnen Sie die Seite **Host Name Mapping** (Zuweisen von Hostnamen).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die Seite Hostnamenzuweisungstabelle wird geöffnet.

3. Wählen Sie einen Eintrag aus der Tabelle **Host Name Mapping Table**" (Hostnamenzuweisungstabelle) aus.
4. Klicken Sie das Kontrollkästchen **Remove** (Entfernen) an.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag auf der Seite Hostnamenzuweisungstabelle wurde gelöscht, und das Gerät wurde aktualisiert.

Zuweisung einer IP-Adressen zu Domänenhostnamen mithilfe von CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für die Zuweisung von Domänenhostnamen zu IP-Adressen zusammen.

Tabelle 6-22. CLI-Befehle für für Domänenhostnamen

CLI-Befehl	Beschreibung
	Definiert die statische Zuweisung von Hostname zu Adresse im Hostcache.

ip host name address	
no ip host name	Entfernt die Name-Adresse-Zuweisung.
clear host {name | *}	Löscht Einträge aus dem host name-to-address"-Cache.
clear host dhcp {name | *}	Löscht die Einträge aus dem Hostname-zu-Adresse-Cache, die vom Dynamic Host Configuration-Protokollserver (DHCP) empfangen wurden.
show hosts [*name*]	Zeigt den Standarddomänennamen, eine Liste der DNS-Namensserver-Hosts, die statische und die gecachte Liste der Hostnamen und Adressen an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

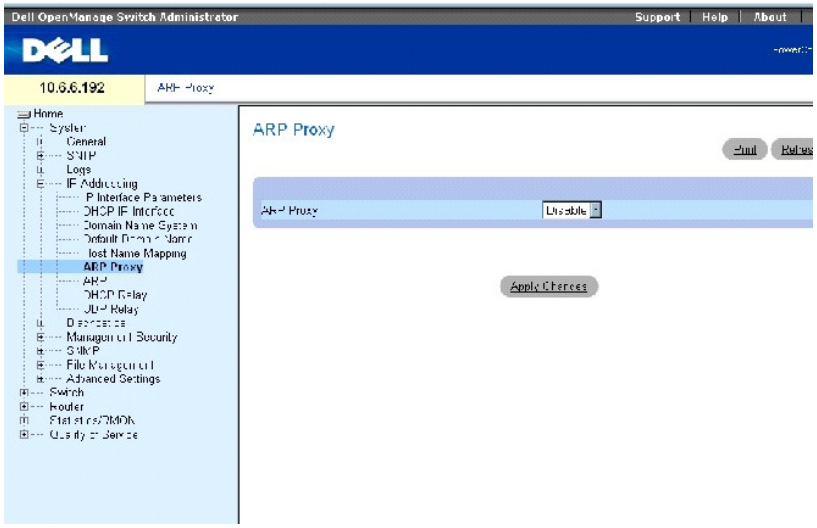
Console (config)# **ip host** accounting.abc.com 176.10.23.1

Aktivieren von ARP-Proxy

Das Address Resolution Protocol (ARP) ist ein TCP/IP-Protokoll, das IP-Adressen in physische Adressen umwandelt. Die Seite **ARP Proxy** ermöglicht es Netzwerkverwaltern, ARP-Proxy auf dem Switch zu aktivieren.

Um die Seite **ARP-Proxy** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **IP Addressing**→ **ARP Proxy**.

Abbildung 6-34. ARP-Proxy



Das Feld **ARP Proxy** aktiviert das Gerät dahingehend, dass es auf ARP-Anforderungen für Knoten antwortet, deren Speicherstelle festgelegt ist. Wenn es deaktiviert ist, reagiert das Gerät mit seiner eigenen MAC-Adresse.

Aktivieren von ARP

1. Öffnen Sie die Seite **ARP Proxy**.
2. Wählen Sie **Enabled** (Aktiviert) im Feld **ARP Proxy**.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der ARP-Proxy wird auf dem Gerät aktiviert.

Aktivieren von ARP-Proxy mithilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für das Aktivieren des ARP-Proxy.

Tabelle 6-23. CLI-Befehle für ARP-Proxy

CLI-Befehl	Beschreibung
`ip proxy-arp`	Aktiviert ARP-Proxy
`no ip proxy-arp`	Deaktiviert ARP-Proxy

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

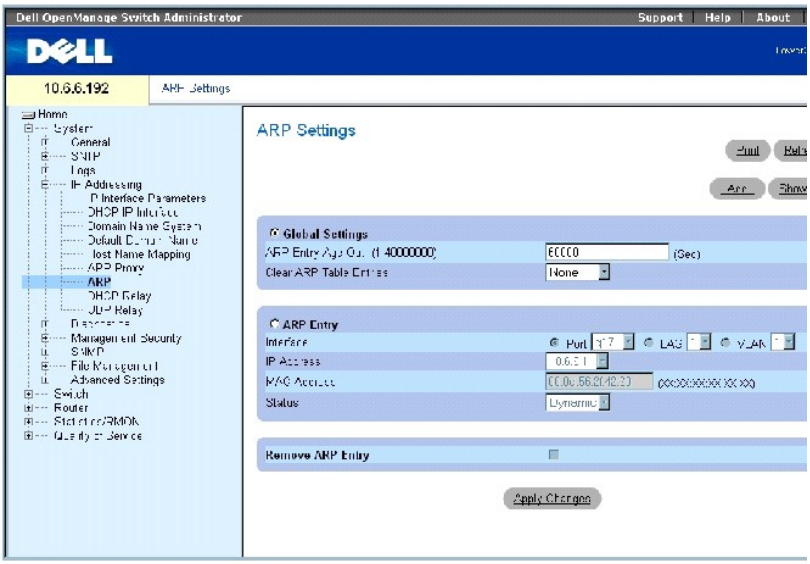
```
Console (config)# ip proxy-arp
```

Definieren von ARP-Einstellungen

Verwenden Sie die Seite **ARP-Einstellungen**, um ARP-Parameter für eine IP-Schnittstelle zu definieren. Die ARP-Tabelle wird verwendet, um die Beziehung der jeweiligen MAC-Adresse und ihrer entsprechenden IP-Adresse zu verwalten. Die ARP-Tabelle kann statisch vom Benutzer ausgefüllt werden. Wenn ein statischer ARP-Eintrag definiert wird, wird ein dauerhafter Eintrag in der Tabelle vorgenommen, den das System verwendet, um IP-Adressen in MAC-Adressen zu übersetzen.

Öffnen Sie die Seite **ARP-Einstellungen**, indem Sie auf **System**→ **IP Addressing**→ **ARP** in der *Strukturansicht* klicken.

Abbildung 6-35. ARP-Einstellungen



Die Seite **ARP-Einstellungen** enthält die folgenden Felder:

Global Settings (Globale Einstellungen) Mit dieser Option können Sie die Felder für globale ARP-Einstellungen aktivieren.

ARP Entry Age Out (0- 40000000) (Laufzeit des ARP-Eintrags) Für alle Geräte die Zeit (in Sekunden), die zwischen ARP-Abfragen über einen Eintrag in der ARP-Tabelle liegt. Nach diesem Zeitraum wird der Eintrag aus der Tabelle gelöscht. Der Bereich ist 0 - 4000000, wobei Null angibt, dass die Einträge nie aus dem Cache gelöscht werden.

Clear ARP Table Entries (ARP-Tabelleneinträge löschen) Gibt die Art der auf allen Geräten zu löschenden ARP-Einträge an. Die möglichen Werte sind:

None (Keine) Gibt an, dass keine ARP-Einträge gelöscht werden.

All (Alle) Gibt an, dass alle ARP-Einträge gelöscht werden.

Dynamic Gibt an, dass lediglich dynamische ARP-Einträge gelöscht werden.

Static Gibt an, dass lediglich statische ARP-Einträge gelöscht werden.

ARP Entry (ARP-Eintrag) Diese Option wird gewählt, um die Felder für ARP-Einstellungen auf einem einzelnen Gerät zu aktivieren.

Interface (Schnittstelle) Die Schnittstellennummer des am Gerät angeschlossenen Ports, LAG oder VLAN.

IP Address Die IP-Adresse der Station, die mit der nachstehend angegebenen MAC-Adresse verknüpft ist.

MAC Address Die MAC-Adresse der Station, die in der ARP-Tabelle mit der IP-Adresse verknüpft ist.

Status Gibt den Status des Eintrags in der ARP-Tabelle an. Mögliche Feldwerte sind:

Other (Andere) Der ARP-Eintrag wurde nicht dynamisch erlernt und ist kein statischer Eintrag.

Invalid (Ungültig) Der ARP-Eintrag ist ungültig.

Dynamic (Dynamisch) Der ARP-Eintrag wurde dynamisch erlernt.

Static Der ARP-Eintrag ist statisch.

Remove ARP Entry (ARP-Eintrag entfernen) Wenn diese Option markiert ist, wird ein ARP-Eintrag entfernt.

Hinzufügen eines ARP-Tabelleneintrags

1. Öffnen Sie die Seite **ARP Settings** (ARP-Einstellungen).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add ARP Entry** (ARP-Eintrag hinzufügen) anzuzeigen.

Abb. 6-36. Hinzufügen eines ARP-Eintrags

3. Wählen Sie eine Schnittstelle aus und füllen Sie die Felder auf dieser Seite mit Daten.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der statische ARP-Tabelleneintrag wird hinzugefügt und das Gerät aktualisiert.

Ändern eines ARP-Tabelleneintrags

1. Öffnen Sie die Seite **ARP Settings** (ARP-Einstellungen).
2. Wählen Sie einen Tabelleneintrag.
3. Ändern Sie die erforderlichen Felder für die jeweilige Schnittstelle.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der statische **ARP-Tabelleneintrag** wird hinzugefügt und das Gerät aktualisiert.

Löschen eines ARP-Tabelleneintrags

1. Öffnen Sie die Seite **ARP Settings** (ARP-Einstellungen).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **ARP Table** (ARP-Tabelle) anzuzeigen.
3. Wählen Sie einen Tabelleneintrag.
4. Markieren Sie **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Tabelleneintrag wird entfernt und das Gerät aktualisiert.

Konfigurieren des ARPs mithilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle zum Konfigurieren von ARP.

Tabelle 6-24. CLI-Befehle für ARP-Einstellungen

CLI-Befehl	Beschreibung
`arp ip_addr hw_addr {ethernet interface- number | vlan vlan-id | port-channel number | out-of-band-eth oob- interface}`	Zum Hinzufügen eines permanenten Eintrags in das Address Resolution Protocol (ARP)-Cache.
`arp timeout`	Zum Konfigurieren der Dauer, die ein Eintrag im ARP-Cache bleibt.
`show arp`	Zum Anzeigen der Einträge in der ARP-Tabelle.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

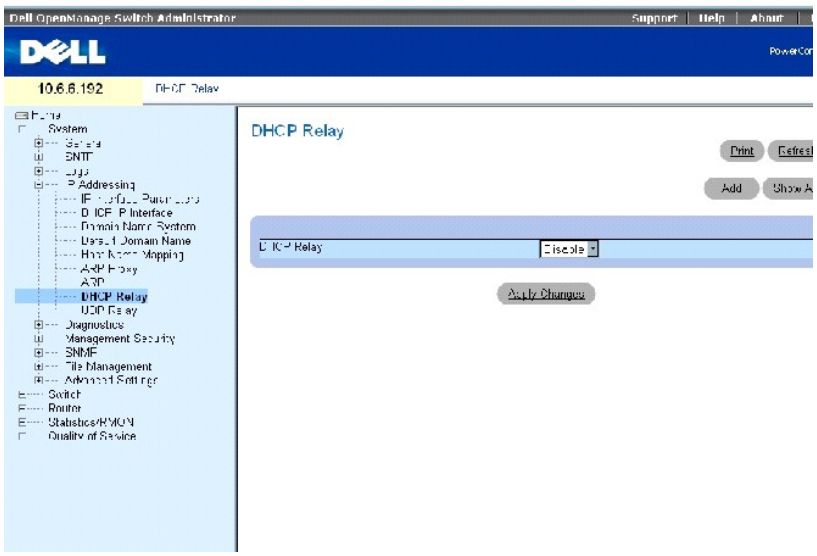
```
Console (config)# arp timeout 5

Console (config)# arp 10.1.1.1 0060.704C.73FF ethernet g5

Console# show arp

Interface  IP Address  HW Address      Status

---------  ----------  -------------   -------

g20        10.1.1.1    0060.704c.73ff  dynamic
```

Definieren von DHCP-Relais-Parametern

Verwenden Sie die Seite **DHCP-Relais**, um Informationen für das Erstellen einer DHCP-Konfiguration mit mehreren DHCP-Servern zur Sicherstellung von Redundanz anzugeben. IP-Adressen werden einzeln kontrolliert und verteilt, um ein Überladen des Geräts zu vermeiden.

Um die Seite **DHCP-Relais** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **IP Addressing**→ **DHCP Relay**.

Abbildung 6-37. DHCP-Relais



Aktivieren des DHCP-Relais

1. Öffnen Sie die Seite **DHCP Relay** (DHCP-Relais).
2. Wählen Sie **Enable** (Aktivieren) im Drop-Down-Menü **DHCP Relay** (DHCP-Relais).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der **DHCP-Relais**-Eintrag wird zur DHCP-Relaistabelle hinzugefügt.

Hinzufügen eines DHCP-Relais-Eintrags

1. Öffnen Sie die Seite **DHCP Relay** (DHCP-Relais).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **DHCP-Server hinzufügen** zu öffnen.
3. Geben Sie einen **Wert** für **New DHCP Server** (Neuer DHCP-Server) ein.

   DHCP-Server dienen als ein DHCP-Relais, wenn dieser Parameter nicht gleich 0.0.0.0. ist. DHCP-Anfragen werden nur weitergeleitet, wenn ihr SEC-Feld größer oder gleich dem Schwellenwert ist. Dies ermöglicht es lokalen DHCP-Servern, als erstes zu antworten.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der DHCP-Server wird der DHCP-Relaistabelle hinzugefügt.

Löschen eines Eintrags in der DHCP-Relaistabelle

1. Öffnen Sie die Seite **DHCP Relay** (DHCP-Relais).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **DHCP-Server-Tabelle** zu öffnen.
3. Wählen Sie einen **DHCP Server** (DHCP-Server) und markieren Sie **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Eintrag wird entfernt und das Gerät aktualisiert.

Definieren der DHCP-Relais-Server mithilfe der CLI-Befehle

Die folgende Tabelle enthält CLI-Befehle für das Definieren von DHCP-Relais-Server.

Tabelle 6-25. CLI-Befehle für DHCP-Relais-Server

CLI-Befehl	Beschreibung
`ip dhcp relay enable`	Aktiviert die Relais-Funktionen des Dynamic Host Configuration Protocol (DHCP) auf dem Router.
`ip dhcp relay address` *`ip_address`*	Stellt die Verfügbarkeit der DHCP-Server für das DHCP-Relais ein.

Im Folgenden wird der CLI-Befehl zur Aktivierung des DHCP-Relais-Services anhand eines Beispiels dargestellt:

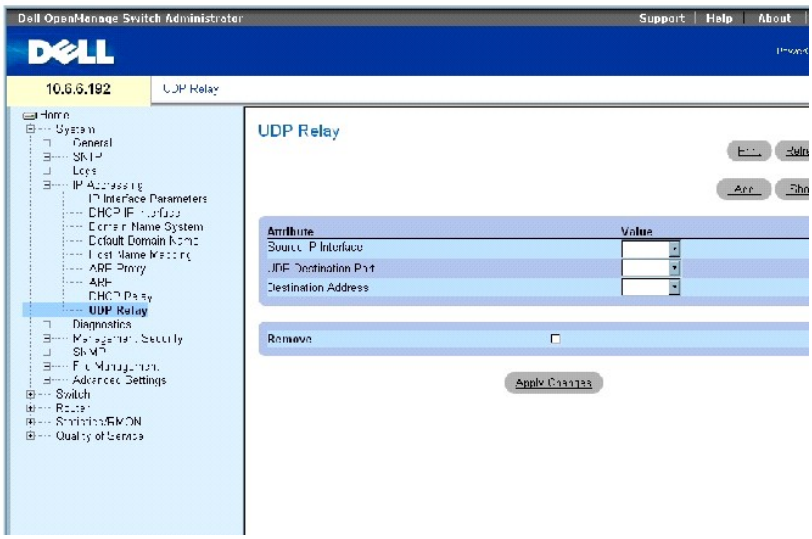
```
Console (config)# ip dhcp relay enable
```

Konfigurieren eines UDP-Relais

Das UDP-Relais ermöglicht es UDP-Paketen, andere Netzwerke zu erreichen. Diese Funktion ermöglicht das Browsen von Workstations zu Servern in anderen Netzwerken.

Um die Seite **UDP-Relais** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **IP Addressing**→ **UDP Relay**.

Abbildung 6-38. UDP-Relais



Die Seite **UDP-Relais** enthält die folgenden Felder:

Source IP Interface (Quellen-IP-Schnittstelle) Die IP-Eingabeschnittstelle, die UDP-Pakete weiterleitet. Wenn dieses Feld 255.255.255.255 ist, werden UDP-Pakete von allen Schnittstellen weitergeleitet. Die folgenden Adressenbereiche 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) Die Kennnummer des UDP-Zielports von weiterzuleitenden UDP-Paketen. Die folgende Tabelle enthält eine Liste mit UDP-Portbelegungen.

Tabelle 6-26. UDP-Portbelegungen

UDP-Portnummer	Akronym	Anwendung
7	Echo	Echo
11	SysStat	Aktiver Benutzer
15	NetStat	Netzstatistik
17	Quote	Zitat des Tages
19	CHARGEN	Zeichengenerator
20	FTP-data	FTP-Daten
21	FTP	FTP
37	Time	Time
42	NAMESERVER	Hostnamen-Server
43	NICNAME	Wer ist
53	DOMAIN	Domain Name Server
69	TFTP	Trivial File Transfer
111	SUNRPC	Sun Microsystems Rpc
123	NTP	Netzwerkzeit
137	NetBiosNameService	Verbindungen NT-Server mit Endstelle
138	NetBiosDatagramService	Verbindungen NT-Server mit Endstelle
139	NetBIOS	Verbindungen SessionServiceNT-Server mit Endstelle
161	SNMP	Simple Network Management
162	SNMP-trap	Simple Network Management Traps
513	who (wer)	Unix Rwho Daemon
514	syslog	Systemprotokoll

525	timed	Time Daemon

Destination Address (Zieladresse) Die IP-Schnittstelle, die UDP-Paketrelais empfängt. Wenn dieses Feld 0.0.0.0 ist, werden UDP-Pakete verworfen. Wenn dieses Feld 255.255.255.255 ist, werden UDP-Pakete an alle IP-Schnittstellen geleitet.

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.
3. Geben Sie die IP-Adresse des UDP-Servers in das Feld **UDP Destination Port** (UDP-Zielport) ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der DHCP-Server wird der DHCP-Relaistabelle hinzugefügt.

Ändern eines Eintrags in der UDP-Relaistabelle

ANMERKUNG: Wenn UDP-Relais aktiviert ist, aber keine UDP-Portnummer definiert wurde, leitet das Gerät standardmäßig UDP-Broadcast-Pakete für die folgenden Services 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)

1. Öffnen Sie die Seite **UDP Relay** (UDP-Relais).
2. Definieren Sie die Felder.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der neue UDP-Eintrag wird der **UDP-Relaistabelle** hinzugefügt, und das wird Gerät aktualisiert.

Löschen eines Eintrags in der UDP-Relaistabelle

1. Öffnen Sie die Seite **UDP Relay** (UDP-Relais).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **UDP Relay Table** (UDP-Relaistabelle) anzuzeigen.
3. Wählen Sie einen UDP-Relais-Server, und markieren Sie **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag wird entfernt und das Gerät aktualisiert.

Konfigurieren der UDP-Relaistabelle mithilfe der CLI-Befehle

Die folgende Tabelle enthält den CLI-Befehl zum Konfigurieren des UDP-Relais.

Tabelle 6-27. CLI-Befehle für UDP-Relais

CLI-Befehl	Beschreibung
`helper-address` *`address`* `[`*`udp-port-list`*`]`	Ermöglicht das Weiterleiten von User Datagram Protocol (UDP)-Broadcasts, die auf einer Schnittstelle empfangen wurden. Dieser Befehl ermöglicht nicht das Weiterleiten von Paketen über BOOTP/DHCP. Um Pakete über BOOTP/DHCP weiterleiten zu können, müssen Sie die Befehle **ip dhcp relay enable** (IP-DHCP-Relais aktivieren), **ip dhcp relay address** (IP-DHCP-Relais-Adresse) und **show ip dhcp** (IP-DHCP anzeigen) verwenden. Weitere Informationen über diese Befehle erhalten Sie unter **Definieren von DHCP-Relais-Parametern**.

Im Folgenden werden CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config-ip)# helper-address 172.16.9.9 49 53
```

Ausführen der Kabeldiagnose

Verwenden Sie die Seite **Diagnostics** (Diagnose), um virtuelle Kabelprüfungen an Kupfer- und Glasfaserkabeln durchzuführen.

Öffnen Sie die Seite **Diagnostics**, indem Sie auf **System**→ **Diagnostics** in der *Strukturansicht* klicken.

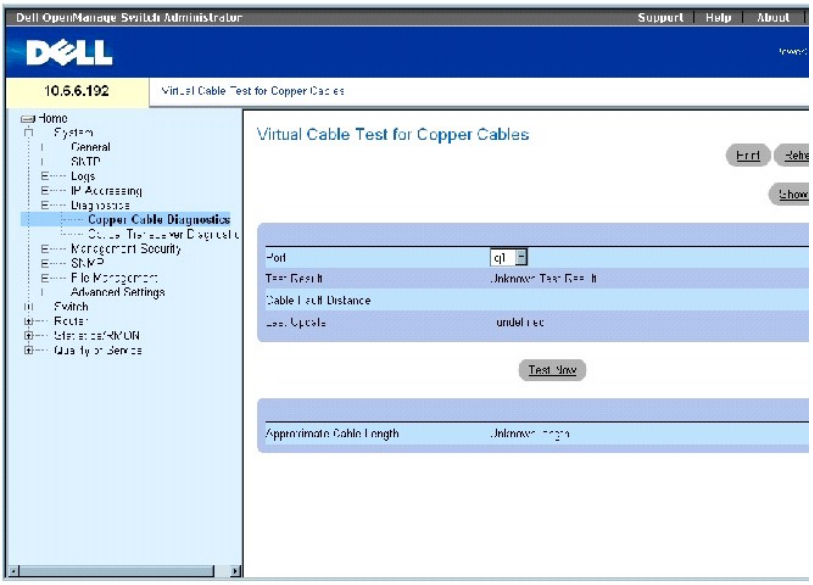
Die Seite **Diagnose** enthält Verknüpfungen zu Diagnoseseiten für Kupferkabel und optische Transceiver.

Anzeigen der Kupferkabel-Diagnose

Verwenden Sie die Seite **Virtual Cable Test for Copper Cables** (Virtuelle Kabelprüfung für Kupferkabel), um Prüfungen an Kupferkabeln durchzuführen. Das Prüfen von Kabeln bietet Informationen darüber, wo Fehler im Kabel aufgetreten sind, über den Zeitpunkt der letzten Kabelprüfung und die Art des aufgetretenen Kabelfehlers. Die Tests bedienen sich der Time Domain Reflectometry (TDR)-Technologie, um die Qualität und Eigenschaften eines an einem Port angeschlossenen Kupferkabels zu testen. Kabel bis zu einer Länge von 120 Metern können geprüft werden. Kabel werden geprüft, wenn die Ports im ausgeschalteten Zustand sind, mit Ausnahme des Tests Approximate Cable Length (Ungefähre Kabellänge).

Um die Seite **Virtueller Kabeltest für Kupferkabel** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **Diagnose**→ **Copper Cable Diagnostics** (Kupferkabeldiagnose).

Abbildung 6-39. Virtueller Kabeltest für Kupferkabel



Die Seite **Virtueller Kabeltest für Kupferkabel** enthält die folgenden Felder:

Port Der Port, an dem das Kabel angeschlossen ist.

Test Result (Testergebnis) Die Ergebnisse des Kabeltests. Die möglichen Werte sind:

No Cable (Kein Kabel) Es ist kein Kabel an den Port angeschlossen.

Open Cable (Offenes Kabel) Das Kabel ist offen.

Short Cable (Kurzes Kabel) Im Kabel ist ein Kurzschluss aufgetreten.

OK Das Kabel hat den Test bestanden.

Fiber Cable (Glasfaserkabel) Am Port ist ein Glasfaserkabel angeschlossen.

Cable Fault Distance (Entfernung zum Kabelfehler) Die Entfernung der Stelle, wo der Kabelfehler aufgetreten ist, vom Port.

Last Update (Letzte Aktualisierung) Der Zeitpunkt, an dem der Port das letzte Mal getestet wurde.

Approximate Cable Length (Ungefähre Kabellänge) Die ungefähre Kabellänge. Diese Prüfung kann nur durchgeführt werden, wenn der Port aktiv ist und mit 1 gbps arbeitet.

Durchführen einer Kabelprüfung

1. Stellen Sie sicher, dass beide Enden des Kupferkabels an einem Gerät angeschlossen sind.
2. Öffnen Sie die Seite **Virtueller Kabeltest für Kupferkabel**.
3. Klicken Sie auf **Test Now** (Jetzt testen).

Es wird nun ein Kupferkabeltest durchgeführt, und die Ergebnisse werden auf der Seite **Virtueller Kabeltest für Kupferkabel** angezeigt.

Anzeigen von Virtual Cable Test Results Table (Ergebnistabelle der virtuellen Kabelprüfung)

1. Öffnen Sie die Seite **Virtueller Kabeltest für Kupferkabel**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Prüfungen auszuführen und die Seite **Virtual Cable Test Results Table** (Ergebnistabelle für virtuelle Kabelprüfungen) anzuzeigen.

Durchführen von Kupferkabelprüfungen mithilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für das Durchführen von Kupferkabelprüfungen.

Tabelle 6-28. CLI-Befehle für Kupferkabeltests

CLI-Befehl	Beschreibung
`test copper-port tdr` *`interface`*	Führt VCT-Tests (virtuelle Kupferkabeltests) aus.
`show copper-port tdr` *`interface`*	Zeigt die Ergebnisse der letzten VCT-Tests an Ports an.
`show copper-port cable-length` *`interface`*	Zeigt einen Schätzwert der Länge eines an einem Port angeschlossenen Kupferkabels an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console# show copper-ports cable-length

Port  Length [meters]

----  ---------------

g1    < 50

g2    Copper not active

g3    110-140

g4    Fiber
```

ANMERKUNG: Die von VCT zurückgemeldete Kabellänge ist ein Annäherungswert im Bereich von bis zu 50 Metern, 50 m bis 80 m, 80 m bis 110 m, 110 m bis 120 m oder mehr als 120 m. Die Abweichung kann bis zu 20 Meter betragen, und Kabellängenmessungen können nicht für Verbindungen mit 10 Mbps durchgeführt werden.

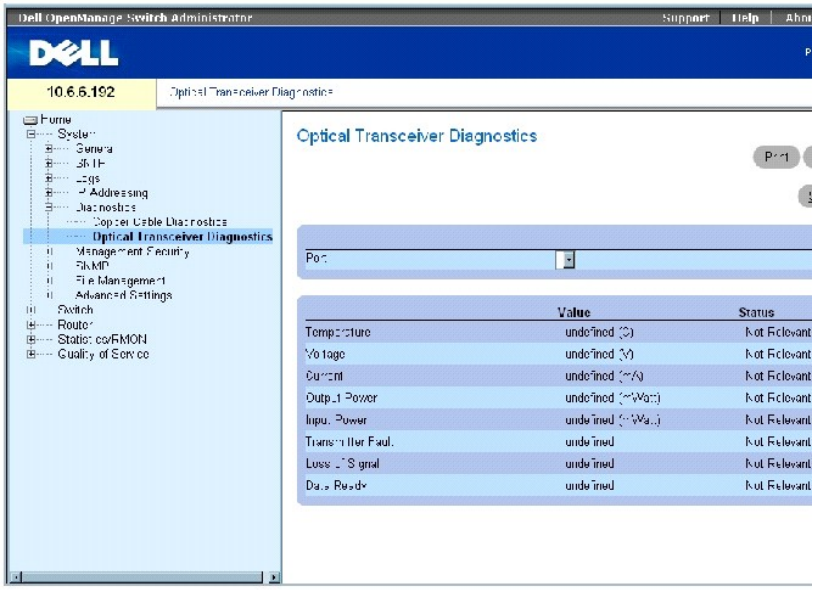
Anzeigen der Diagnose für optische Transceiver

Auf der Seite **Diagnose der optischen Transceiver** können Sie Tests an Glasfaserkabeln durchführen.

Öffnen Sie die Seite **Optical Transceiver Diagnostics**, indem Sie auf **System**→ **Diagnostics**→ **Optical Transceiver Diagnostics** in der *Strukturansicht* klicken.

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

Abb. 6-40. Diagnose für optische Transceiver



Die Seite **Diagnose der optischen Transceiver** enthält die folgenden Felder:

Port Die IP-Portadresse, an der das Kabel getestet wird.

Temperature (Temperatur) Die Temperatur (°C), bei der das Kabel arbeitet.

Voltage (Spannung) Die Betriebsspannung des Kabels.

Current (Strom) Der Betriebsstrom des Kabels.

Output Power (Ausgangsstrom) Die Übertragungsrate des Ausgangsstroms.

Input Power (Eingangsstrom) Die Übertragungsrate des Eingangsstroms.

Transmitter Fault (Senderfehler) Zeigt an, ob während der Übertragung ein Fehler aufgetreten ist.

Loss of Signal (Signalverlust) Zeigt an, ob im Kabel ein Signalverlust aufgetreten ist.

Data Ready (Daten bereit) Gibt an, dass der Transceiver eingeschaltet ist und die Daten bereit sind.

Anzeigen der Tabelle Optical Transceiver Diagnostics Test Results (Diagnosetestergebnisse für optische Sender-Empfänger)

1. Öffnen Sie die Seite **Optical Transceiver Diagnostics** (Diagnose für optische Transceiver).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Prüfung durchzuführen und die Seite **Ergebnistabelle der virtuellen Kabelprüfung** zu öffnen.

Durchführen von Glasfaserkabelprüfungen mithilfe der CLI-Befehle

Die folgende Tabelle enthält den CLI-Befehl für das Durchführen von Glasfaserkabelprüfungen.

Tabelle 6-29. CLI-Befehle für Glasfaserkabel-Tests

CLI-Befehl	Beschreibung
`show fiber-ports optical- transceiver [interface] [detailed]`	Zeigt die Diagnose der optischen Transceive an.

Im Folgenden werden CLI-Befehle anhand eines Beispiels dargestellt:

```
Console# show fiber-ports optical-transceiver
```

Die folgenden Spalten werden auf dem Bildschirm angezeigt:

- **Temp** (Temperatur) Intern gemessene Transceiver-Temperatur.
- **Voltage** (Spannung) Intern gemessene Versorgungsspannung.
- **Current** (Strom) Gemessener TX-Ruhestrom.
- **Output Power** (Ausgangsleistung) Gemessene TX-Ausgangsleistung in Milliwatt.
- **Input Power** (Eingangsleistung) Gemessene RX-Eingangsleistung in Milliwatt.
- **TX Fault** (TX-Fehler) Senderfehler.

ANMERKUNG: Finisar-Sender-Empfänger unterstützen die Diagnoseprüfung für Senderfehler nicht.

- **LOS** Signalverlust.
- **Data Ready** (Daten bereit) Zeigt an, dass der Transceiver eingeschaltet ist und die Daten bereit sind.
- **N/A** Nicht verfügbar, N/S Nicht unterstützt, W Warnung, E Fehler.

ANMERKUNG: Die Faseroptik-Analysefunktion funktioniert nur bei SFPs, die den digitalen Diagnosestandard SFF- unterstützen 4872.

Verwalten der Gerätesicherheit

Verwenden Sie die Seite **Management Security** (Managementsicherheit), um die Managementsicherheitsparameter für Port-, Benutzer- und Serversicherheit einzustellen.

Öffnen Sie die Seite **Management Security**, indem Sie auf **System→ Management Security** in der *Strukturansicht* klicken.

Definieren von Zugangsprofilen

Verwenden Sie die Seite Zugangsprofile, um Profile und Regeln für den Zugang zum Gerät zu definieren. Sie können den Zugriff auf Verwaltungsmethoden durch Ingress-Schnittstellen, Quell-IP-Adressen und/oder Quell-IP-Subnetze auf spezifische Benutzergruppen beschränken.

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

Zugang zu verschiedenen Managementmethoden kann je nach Benutzergruppe unterschiedlich sein. Benutzergruppe 1 kann z. B. auf das Gerät nur über eine HTTPs-Sitzung zugreifen, während Benutzergruppe 2 auf das Gerät sowohl über HTTPs- als auch über Telnet-Sitzungen zugreifen kann.

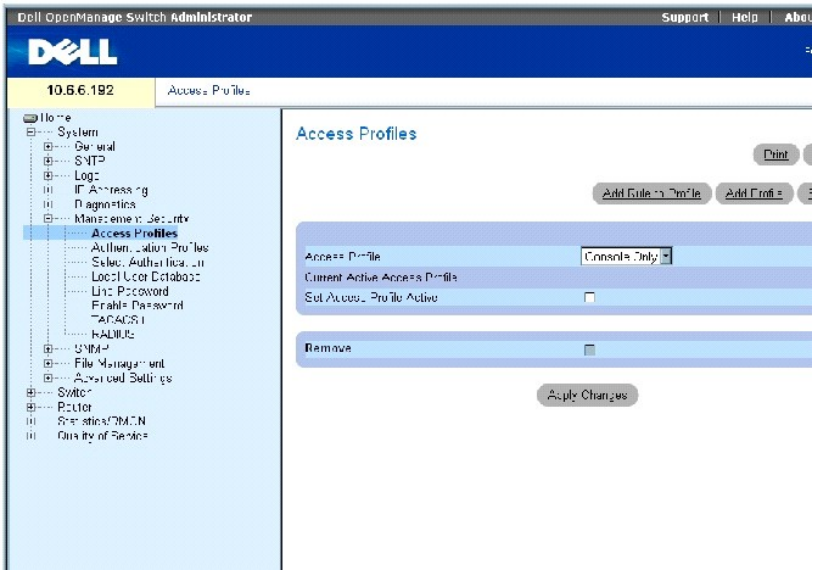
Die Verwaltungszugriffslisten umfassen Regeln, die festlegen, auf welche Weise Geräte von welchem Benutzer verwaltet werden. Benutzer können auch vom

Zugang zu dem Gerät gesperrt werden.

Verwenden Sie die Seite **Access Profiles** (Zugangsprofile), um Managementlisten zu konfigurieren und sie auf bestimmte Schnittstellen anzuwenden.

Öffnen Sie die Seite **Access Profiles**, indem Sie auf **System**→ **Management Security**→ **Access Profiles** in der *Strukturansicht* klicken.

Abbildung 6-41. Zugangsprofile



Access Profile (Zugangsprofil) Enthält eine Liste aller Zugangsprofile. Der Standardwert, zu dem benutzerdefinierte Zugangsprofile hinzugefügt werden, ist **Console Only** (Nur Konsole). Bei Auswahl von **Console Only** (nur Konsole) als **Access Profile**-Name wird die Verbindung der Session getrennt und ausschließlicher Zugriff auf das Gerät von der Konsole aktiviert.

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

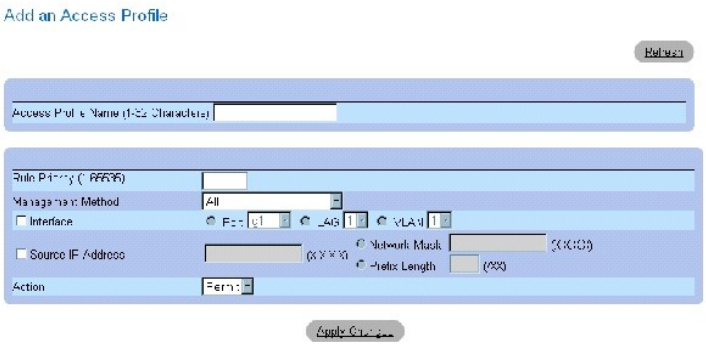
Set Access Profile Active (Zugangsprofil auf Aktiv einstellen) Aktiviert das ausgewählte Zugangsprofil.

Remove (Entfernen) Wenn diese Option markiert ist, wird ein Zugangsprofil von der Liste **Access Profile Name** (Zugangsprofilnamen) entfernt.

Hinzufügen eines Zugangsprofils

1. Öffnen Sie die Seite **Access Profiles** (Zugangsprofile).
2. Klicken Sie auf **Add Profile** (Profil hinzufügen), um die Seite **Zugangsprofil hinzufügen** zu öffnen.

Abbildung 6-42. Hinzufügen eines Zugangsprofils



Die Seite **Zugangsprofil hinzufügen** enthält die folgenden Felder:

Access Profile Name Benutzerdefinierter Name für das Zugangsprofil.

Rule Priority (Regelpriorität) Gibt die Priorität der Regel an. Wenn das Paket einer Regel entspricht, wird den Benutzergruppen Zugang zur Geräteverwaltung gewährt oder verweigert. Die Regelreihenfolge wird eingestellt, indem eine Regelnummer in der Tabelle **Profile Rules** (Profilregeln) definiert wird. Die Regelnummer ist wesentlich beim Zuordnen von Paketen zu Regeln, da die Pakete auf Basis der ersten Entsprechung zugeordnet werden. Die Regelprioritäten werden in der Profilregeltabelle zugeordnet.

Management Method (Verwaltungsmethode) Gibt die Verwaltungsmethode an, für die das Zugangsprofil definiert wurde. Benutzer mit diesem Zugangsprofil können auf das Gerät zugreifen, indem Sie die gewählte Managementmethode verwenden.

Interface (Schnittstelle) Gibt den Schnittstellentyp an, auf den die Regel angewendet wird. Dies ist ein optionales Feld. Sie können diese Regel auf einen ausgewählten Port, LAG oder VLAN anwenden, indem Sie das Kontrollkästchen markieren und die entsprechende Optionstaste und Schnittstelle wählen.

ANMERKUNG: Die Zuordnung eines Zugangsprofils zu einer Schnittstelle bringt mit sich, dass der Zugang über andere Schnittstellen verweigert wird. Wenn ein Zugangsprofil keiner Schnittstelle zugeordnet ist, kann von allen auf das Gerät zugegriffen werden.

Source IP Address (Quell-IP-Adresse) Gibt die Quell-IP-Adresse der Schnittstelle an, für die die Regel gilt. Dies ist ein optionales Feld und gibt an, dass die Regel für ein Teilnetzwerk gilt.

Network Mask (Netzwerkmaske) Gibt die IP-Subnetzmaske an.

Prefix Length (Präfixlänge) Gibt die Anzahl der Bits an, die das Präfix der Quell-IP-Adresse enthält, oder die Netzwerkmaske der Quell-IP-Adresse.

Action Legt fest, ob der angegebene Verwaltungszugriff auf die Schnittstelle gewährt oder verwehrt werden soll.

3. Geben Sie den Profilnamen in das Textfeld **Access Profile Name** (Name des Zugangsprofils) ein.
4. Füllen Sie die Felder mit Daten und 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 Profiles** (Zugangsprofile).
2. Wählen Sie ein **Zugangsprofil** von der Liste.
3. Markieren Sie das Kontrollkästchen **Set Access Profile Active** (Zugangsprofil auf aktiv setzen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

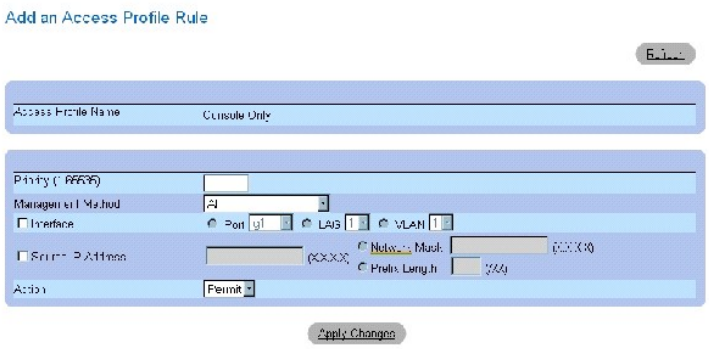
Das Zugangsprofil wird für den Benutzer aktiviert.

Hinzufügen von Regeln zu einem Zugangsprofil

1. Öffnen Sie die Seite **Access Profiles** (Zugangsprofile).
2. Wählen Sie ein **Zugangsprofil** aus dem Drop-Down-Menü.

   Dies ist das Profil, dem Regeln hinzugefügt werden, wenn die Seite Zugangsprofilregel hinzufügen geöffnet wird.
3. Klicken Sie auf **Add Rule to Profile**, um die Seite Zugangsprofilregel hinzufügen zu öffnen.

Abb. 6-43. Hinzufügen einer Regel zum Zugriffsprofil



4. Füllen Sie die Felder in dem Dialogfeld aus und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Regel wird dem Zugangsprofil hinzugefügt und das Gerät aktualisiert.

Entfernen einer Regel

1. Öffnen Sie die Seite **Access Profiles** (Zugangsprofile).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **Profile Rules Table** (Profilregeltabelle) anzuzeigen.
3. Wählen Sie eine Regel.
4. Markieren Sie das Kontrollkästchen **Remove** (Entfernen) und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Regel wird gelöscht und das Gerät aktualisiert.

Definieren der Zugangsprofile mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Konfiguration von Zugangsprofilen zusammen.

Tabelle 6-30. CLI-Befehle für Zugangsprofile

CLI-Befehl	Beschreibung
`management access-list` *name* **ANMERKUNG:** Umgeben Sie *n a m e* mit Anführungszeichen, falls dieser Leerstellen enthält. Zum Beispiel workgroup 1"	Definiert eine Verwaltungszugriffsliste und erfasst den Zugriffslistenkontext zu Konfigurationszwecken.
`permit [ethernet` *interface- number* `| vlan` *vlan-id* `| port- channel` *number*`]`	Legt Port-Zugriffsbedingungen für die Verwaltungszugriffsliste fest.

[service *service*]	
permit ip-source ip-address [mask mask | *prefix-length*] [ethernet *interface-number* | vlan *vlan-id* | port-channel *number*] [service *service*]	Legt Port-Zugriffsbedingungen für die Verwaltungszugriffsliste sowie die ausgewählte Verwaltungsmethode fest.
deny [ethernet interface-number | vlan vlan-id | port-channel number] [service service]	Legt Port-Sperrbedingungen für die Verwaltungszugriffsliste sowie die ausgewählte Verwaltungsmethode fest.
deny ip-source ip-address [mask mask | *prefix-length*] [ethernet *interface-number* | vlan *vlan-id* | port-channel *number*] [service *service*]	Legt Port-Sperrbedingungen für die Verwaltungszugriffsliste sowie die ausgewählte Verwaltungsmethode fest.
management access-class {console-only | *name*}	Definiert, welche Zugriffsliste für aktive Verwaltungsverbindungen verwendet wird.
show management access-list [*name*]	Zeigt die aktiven Verwaltungszugriffslisten an.
show management access-class	Zeigt Informationen über die Verwaltungszugriffsklasse an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

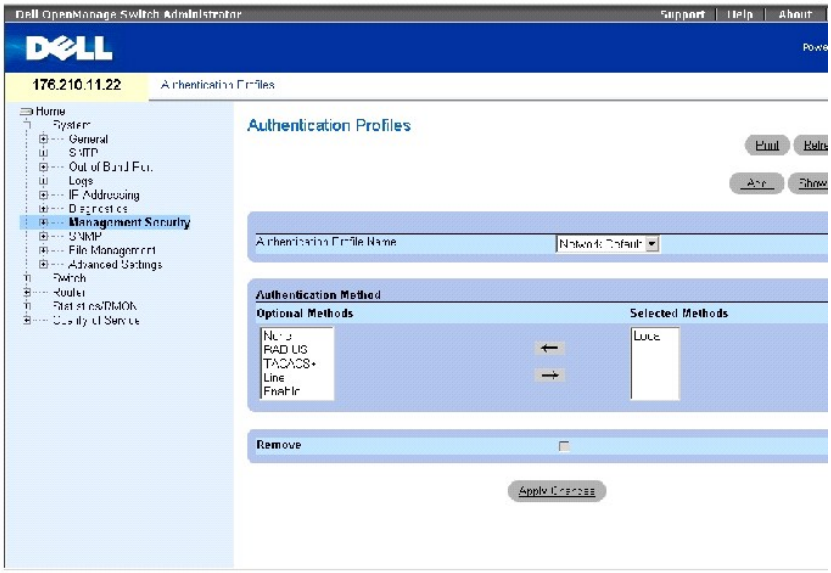
```
Console (config)# management access-list mlist

Console (config-macl)# permit ethernet g1

Console (config-macl)# permit ethernet g9

Console (config-macl)# exit

Console# show management access-class

Management access-class is enabled, using access list mlist
```

Definieren von Authentifizierungsprofilen

Die Benutzerauthentifizierung findet lokal und auf einem externen Server statt. Verwenden Sie die Seite **Authentication Profiles** (Authentifizierungsprofile), um die Benutzerauthentifizierungsmethode auf dem Gerät zu wählen.

Um die Seite **Authentifizierungsprofile** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **Management Security**→ **Authentication Profiles**.

Abbildung 6-44. Authentifizierungprofile



Die Seite **Authentifizierungsprofile** enthält die folgenden Felder:

Authentication Profile Name (Authentifizierungsprofilname) Zeigt die Listen benutzerdefinierter Authentifizierungsmethoden an, zu denen benutzerdefinierte Authentifizierungsprofile hinzugefügt werden. Die Standardeinstellungen sind **Network Default** (Netzwerkstandard) und **Console Default** (Konsolenstandard).

Optional Methods (Optionale Methoden) Listet die Benutzer-Authentifizierungsmethoden auf. Mögliche Optionen sind:

None (Keine) Gibt an, dass keine Benutzer-Authentifizierung erfolgt.

Local (Lokal) Die Benutzerauthentifizierung findet auf Geräteebene statt; das Gerät prüft den Benutzernamen und das Kennwort zur Authentifizierung.

RADIUS Gibt an, dass die Benutzer-Authentifizierung auf dem RADIUS-Server erfolgt. Weitere Informationen über RADIUS-Server erhalten Sie unter Konfigurieren von RADIUS-Einstellungen.

TACACS+ Gibt an, dass die Benutzerauthentifizierung auf dem TACACS+-Server erfolgt. Weitere Informationen zu TACACS+-Servern finden Sie unter Konfigurieren von TACACS+-Einstellungen.

Line (Leitung) Gibt an, dass das Leitungskennwort für die Authentifizierung verwendet wird.

Enable (Aktivieren) Gibt an, dass das Aktivierungskennwort für die Authentifizierung verwendet wird.

ANMERKUNG: Die Benutzerauthentifizierung findet in der Reihenfolge statt, in der die Methoden ausgewählt werden. Wenn während der Authentifizierung ein Fehler auftritt, wird die nächste gewählte Methode verwendet. Wenn zum Beispiel die Optionen **Local** (Lokal) und **RADIUS** gewählt sind, wird der Benutzer erst lokal und dann über einen externen Server authentifiziert.

Selected Methods (Gewählte Methoden) Die gewählte Authentifizierungsmethode.

Hinzufügen eines Authentifizierungsprofils

1. Öffnen Sie die Seite **Authentication Profiles** (Authentifizierungsprofile).

2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Authentifizierungsprofil hinzufügen** anzuzeigen.
3. Geben Sie den 1-12 Zeichen langen Profilnamen in das Feld **Profile Name** (Profilname) ein.

ANMERKUNG: Der Profilname darf keine Leerzeichen enthalten.

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

Sitzungen werden ein Authentifizierungsprofil zugeordnet.

Wählen einer Authentifizierungsmethode

1. Öffnen Sie die Seite **Authentication Profiles** (Authentifizierungsprofile).
2. Wählen Sie ein Element aus der Liste in dem Feld **Authentication Profile Name** (Authentifizierungsprofilname).
3. Wählen Sie einen Wert **Optional Methods** (Optionale Methoden) unter Verwendung der Pfeile.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das Benutzerauthentifizierungsprofil wird auf dem Gerät aktualisiert.

Entfernen eines Authentifizierungsprofileintrags

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

Die Tabelle **Authentifizierungsprofile** wird geöffnet.

3. Markieren Sie das Kontrollkästchen **Remove** (Entfernen) neben dem Profil, das entfernt werden soll.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag wird entfernt.

Konfigurieren eines Authentifizierungsprofils mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zum Definieren von Authentifizierungsprofilen zusammen.

Tabelle 6-31. CLI-Befehle für Authentifizierungsprofile

CLI-Befehl	Beschreibung
`aaa authentication login {default | list-name} method1 [method2...]`	Konfiguriert die Anmeldungs-Authentifizierung.
`no aaa authentication login {default | list-name}`	Entfernt ein Anmeldungs-Authentifizierungsprofil.
`show authentication methods`	Zeigt Informationen zu den Authentifizierungsmethoden an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

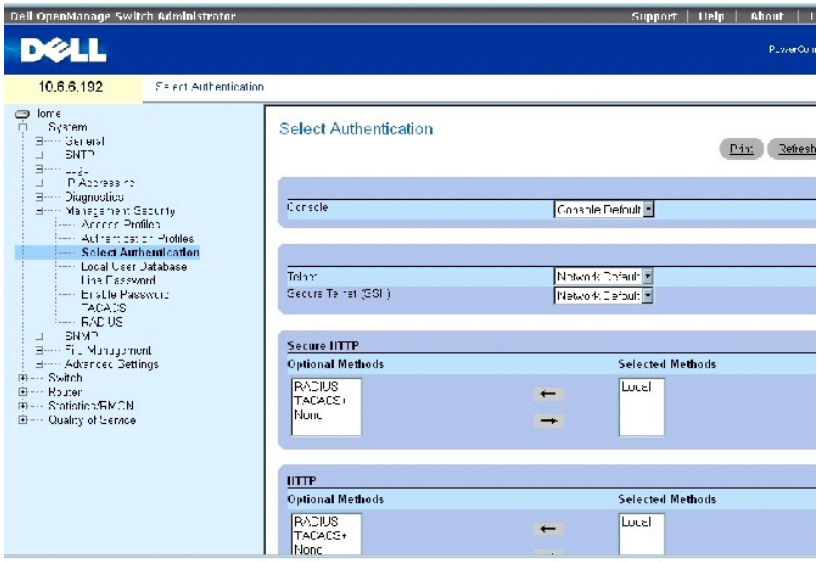
```
Console (config)# aaa authentication login default radius local enable none

Console (config)# no aaa authentication login default
```

Auswählen von Authentifizierungsprofilen

Nach der Definition der Authentifizierungsprofile können diese auf Verwaltungszugriffsmethoden angewendet werden. Konsolenbenutzer können zum Beispiel mit Authentifizierungsprofilliste 1 authentifiziert werden, während Telnet-Benutzer mit Authentifizierungsmethodenliste 2 authentifiziert werden.

Um die Seite Authentifizierung auswählen zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **Management Security**→ **Select Authentication**.

Abbildung 6-45. Auswählen einer Authentifizierung



Die Seite **Authentifizierung auswählen** enthält die folgenden Felder:

Console Zeigt die zur Authentifizierung von Konsolenbenutzern verwendeten Authentifizierungsprofile an.

Telnet Zeigt die zur Authentifizierung von Telnet-Benutzern verwendeten Authentifizierungsprofile an.

Secure Telnet (SSH) Zeigt die zur Authentifizierung von Secure Shell (SSH)-Benutzern verwendeten Authentifizierungsprofile an. SSH ermöglicht es SSH-Clients, eine sichere, verschlüsselte Verbindung mit einem Gerät herzustellen.

HTTP and **Secure HTTP** Zeigt die jeweils für den HTTP-Zugriff und sicheren HTTP-Zugriff verwendeten Authentifizierungsmethoden an. Mögliche Feldwerte sind:

None (Keine) Gibt an, dass keine Authentifizierungsmethode für Zugriffe verwendet wird.

Local (Lokal) Gibt an, dass die Authentifizierung lokal erfolgt.

RADIUS Gibt an, dass die Authentifizierung auf dem RADIUS-Server erfolgt.

TACACS+ Gibt an, dass die Authentifizierung auf dem TACACS+-Server erfolgt.

Local, None (Lokal, keine) Die Authentifizierung findet zunächst lokal statt. Wenn die Authentifizierung nicht verifiziert werden kann, wird keine Authentifizierungsmethode verwendet.

RADIUS, None (RADIUS, Keine) Die Authentifizierung findet zunächst am RADIUS-Server statt. Wenn die Authentifizierung nicht verifiziert werden kann, wird keine Authentifizierungsmethode verwendet.

TACACS+, None (TACACS+, Keine) Die Authentifizierung findest zunächst am TACACS+-Server statt. Wenn die Authentifizierung nicht verifiziert werden kann, wird keine Authentifizierungsmethode verwendet.

Local, RADIUS (Lokal, RADIUS) Die Authentifizierung findet zunächst lokal statt. Wenn die Authentifizierung nicht lokal verifiziert werden kann, authentifiziert der RADIUS-Server die Verwaltungsmethode. Wenn der RADIUS-Server die Verwaltungsmethode nicht authentifizieren kann, wird die Sitzung gesperrt.

Local, TACACS+ (Lokal, TACACS+) Die Authentifizierung findet zunächst lokal statt. Wenn die Authentifizierung nicht lokal verifiziert werden kann, authentifiziert der TACACS+-Server die Verwaltungsmethode. Wenn der TACACS+-Server die Verwaltungsmethode nicht authentifizieren kann, wird die Sitzung gesperrt.

RADIUS, Local (RADIUS, lokal) Die Authentifizierung findet zunächst am RADIUS-Server statt. Wenn die Authentifizierung nicht am RADIUS-Server verifiziert werden kann, wird die Sitzung lokal authentifiziert. Wenn die Sitzung nicht lokal authentifiziert werden kann, wird die Sitzung gesperrt.

TACACS+, None (TACACS+, lokal) Die Authentifizierung findest zunächst am TACACS+-Server statt. Wenn die Authentifizierung nicht am TACACS+-Server verifiziert werden kann, wird die Sitzung lokal authentifiziert. Wenn die Sitzung nicht lokal authentifiziert werden kann, wird die Sitzung gesperrt.

Local, RADIUS, None (Lokal, RADIUS, keine) Die Authentifizierung findet zunächst lokal statt. Wenn die Authentifizierung nicht lokal verifiziert werden kann, authentifiziert der RADIUS-Server die Verwaltungsmethode. Wenn der RADIUS-Server die Verwaltungsmethode nicht authentifizieren kann, wird die Sitzung erlaubt.

RADIUS, Local, None (RADIUS, lokal, keine) Die Authentifizierung findet zunächst am RADIUS-Server statt. Wenn die Authentifizierung nicht am RADIUS-Server verifiziert werden kann, wird die Sitzung lokal authentifiziert. Wenn die Sitzung nicht lokal authentifiziert werden kann, wird die Sitzung erlaubt.

Local, TACACS+, None (Lokal, TACACS+, keine) Die Authentifizierung findet zunächst lokal statt. Wenn die Authentifizierung nicht lokal verifiziert werden kann, authentifiziert der TACACS+-Server die Verwaltungsmethode. Wenn der TACACS+-Server die Verwaltungsmethode nicht authentifizieren kann, wird die Sitzung erlaubt.

TACACS+, Local, None (TACACS+, Lokal, keine) Die Authentifizierung findet zunächst am TACACS+-Server statt. Wenn die Authentifizierung nicht am TACACS+-Server verifiziert werden kann, wird die Sitzung lokal authentifiziert. Wenn die Sitzung nicht lokal authentifiziert werden kann, wird die Sitzung erlaubt.

Anwenden einer Authentifizierungsmethodenliste auf Konsolensitzungen

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

Konsolensitzungen ist eine Authentifizierungsmethodenliste zugeordnet.

Anwenden eines Authentifizierungsprofils auf Telnet-Sitzungen

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

Konsolensitzungen werden Authentifizierungsprofile zugeordnet.

Anwenden eines Authentifizierungsprofils auf Secure Telnet (SSH)-Sitzungen

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

Secure Telnet (SSH)-Sitzungen sind Authentifizierungsprofile zugeordnet.

Zuordnen einer Authentifizierungssequenz zu HTTP-Sitzungen

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

Die ausgewählte Authentifizierungsmethode geht über in das Feld Selected Methods" (Ausgewählte Methoden).

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 ist eine Authentifizierungsreihenfolge zugeordnet.

Zuordnen einer Authentifizierungssequenz zu Secure HTTP-Sitzungen

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

Die ausgewählte Authentifizierungsmethode geht über in das Feld Selected Methods" (Ausgewählte Methoden).

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 ist eine Authentifizierungsreihenfolge zugeordnet.

Zuordnen von Zugangsmethoden-Authentifizierungsprofilen oder -sequenzen

Die folgende Tabelle enthält CLI-Befehle für das Zuordnen von Zugangsmethoden, Authentifizierungsmethodenlisten oder -reihenfolgen.

Tabelle 6-32. CLI-Befehle für Zugangsmethoden

CLI-Befehl	Beschreibung
`enable authentication {default | list-name}`	Spezifiziert die Authentifizierungsmethodenliste, wenn der Benutzer auf höhere Privilegienebenen in Remote-Telnet oder Konsole zugreift.
`login authentication {default | list-name}`	Spezifiziert Authentifizierungsmethodenlisten für die Anmeldung für Remote-Telnet oder Konsole.
	Spezifiziert Authentifizierungsmethoden für HTTP-Serverbenutzer.

ip http authentication method1 [*method2...*]	
ip https authentication method1 [*method2...*]	Spezifiziert Authentifizierungsmethoden für HTTPs-Serverbenutzer.
show authentication methods	Zeigt Informationen zu den Authentifizierungsmethoden an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console# show authentication methods

Login Authentication Method Lists

---------------------------------

Default : Local



Enable Authentication Method Lists

---------------------------------

Console_Default : Enable None

Network_Default : Enable



Line Login Method List Enable Method List

------- ----------------- -------------------

Console Default Default

Telnet Default Default

SSH Default Default



http : Local

https : Local
```

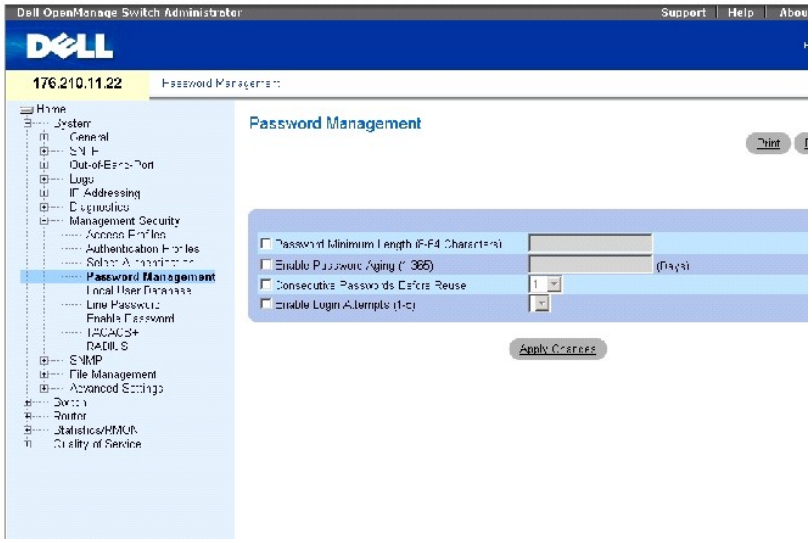
Verwalten von Kennwörtern

Die Kennwortverwaltung bietet verbesserte Netzwerksicherheit und Kennwortkontrolle. Kennwörter für den Zugang zu SSH, Telnet, HTTP, HTTPS und SNMP unterliegen z.B. den folgenden Sicherheitsfunktionen:

- Definieren von maximalen Kennwortlängen
- Kennwortablauf
- Schutz vor häufiger Kennwortwiederverwendung
- Sperren von Benutzern mit fehlgeschlagenen Anmeldeversuchen

Um die Seite **Kennwortverwaltung** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **Management Security**→ **Password Management**.

Abbildung 6-46. Kennwortverwaltung



Die Seite **Kennwortverwaltung** enthält die folgenden Felder:

Password Minimum Length (8-64 Characters) (Maximale Kennwortlänge (8-64 Zeichen) Zeigt, wenn ausgewählt, die maximale Kennwortlänge an. So kann der Administrator beispielsweise festlegen, dass alle Verbindungskennwörter über mindestens 10 Zeichen verfügen müssen.

Enable Password Aging (1-365) (Kennwortablauf aktivieren 1-365) Zeigt, wenn ausgewählt, die Zeitdauer an, die vergehen darf, bis ein Kennwort abläuft. Die Feldwerte liegen zwischen 1 und 365 Tagen.

Consecutive Passwords Before Reuse (Regelmäßige Kennwortänderung vor Wiederverwendung) Zeigt an, wie oft ein Kennwort geändert werden muss, bevor es erneut verwendet werden kann. Die möglichen Feldwerte liegen zwischen 1 und 10.

ANMERKUNG: Der Anwender wird vor dem Ablauf des Kennworts über eine Benachrichtigung zum Ändern des Kennworts aufgefordert. Der Internetbenutzer kann diese Benachrichtigung nicht sehen.

Enable Login Attempts (1-5) (Anmeldeversuche aktivieren (1-5) Wenn ausgewählt, kann einem Benutzer die Anmeldung an ein Gerät verweigert werden, wenn der Benutzer bei dem Versuch, sich anzumelden, eine vordefinierte Anzahl an Fehlversuchen überschritten hat. Wenn beispielsweise die maximale Zahl für Anmeldefehlversuche auf 5 festgelegt wurde und der Benutzer versucht, sich fünf Mal mal mit einem falschen Kennwort anzumelden, wird dem Benutzer beim sechsten Versuch der Zugang zum Gerät verweigert. Es sind Feldwerte von 1-5 vorgesehen.

Definieren von Kennwortbeschränkungen

1. Öffnen Sie die Seite **Kennwortverwaltung**.
2. Definieren Sie die entsprechenden Felder.

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

Die Kennwortbeschränkungen werden definiert, und das Gerät wird aktualisiert.

Definieren von Kennwortbeschränkung mithilfe von CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für das Konfigurieren von Kennwörtern auf der Seite **Kennwortverwaltung** zusammen.

Tabelle 6-33. CLI-Befehle für die Kennwortverwaltung

CLI-Befehl	Beschreibung
`password min-length length`	Legt die Mindestlänge für ein Kennwort fest.
`passwords aging days`	Legt das Ablaufdatum von Kennwörtern in der lokalen Datenbank fest.
`passwords history number`	Legt die Anzahl an erforderlichen Kennwortänderungen fest, bevor ein Kennwort in der lokalen Datenbank wiederverwendet werden kann.
`passwords lock-out number`	Sperrt ein Benutzerkonto nach einer festgelegten Anzahl von fehlgeschlagenen Anmeldeversuchen.
`show password configuration`	Zeigt Informationen über die Kennwortverwaltung an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

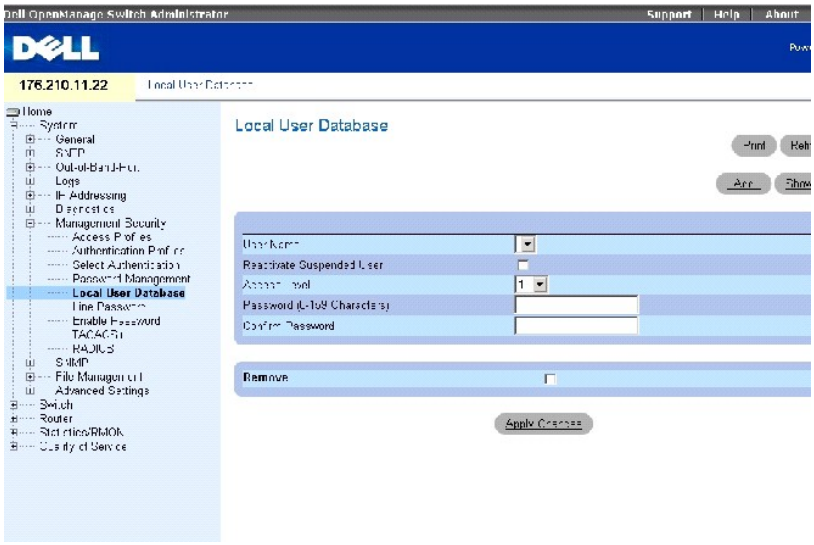
```
Console (config)# password min-length 8

Console (config)# password aging 120

Console (config)# passwords history 2

Console (config)# passwords lock-out 3

Console (config)# exit

Console# show passwords configuration

Minimal length: 8

Aging: 120 days

History: 2

Lock-out: Disabled
```

Definieren der lokalen Benutzerdatenbanken

Auf der Seite **Lokale Benutzerdatenbank** können Sie Kennwörter festlegen, Zugangsberechtigungen für Benutzer vergeben und Benutzer reaktivieren, deren Konten gesperrt wurden.

Um die Seite **Lokale Benutzerdatenbank** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **Management Security**→ **Local User Database**.

Abbildung 6-47. Lokale Benutzerdatenbank



Die Seite **Lokale Benutzerdatenbank** enthält die folgenden Felder:

User Name (Benutzername) Enthält eine Benutzerliste.

Reactivated Suspended User (Gesperrte Benutzer reaktivieren) Wählen Sie diese Option aus, um die festgelegten Zugangsberechtigungen des Benutzer zu reaktivieren. Zugangsberechtigung können nach nicht erfolgreichen Anmeldeversuchen gesperrt werden.

Access Level (1-15) (Zugangsebene) Benutzerzugangsebene. Die niedrigste Benutzerzugangsebene ist **1**, und **15** ist die höchste Benutzerzugangsebene.

Password (Kennwort) Benutzerdefiniertes Kennwort.

Confirm Password (Kennwort bestätigen) Bestätigt das benutzerdefinierte Kennwort.

Remove (Entfernen) Entfernt, wenn ausgewählt, Benutzer aus der Liste **User Name** (Benutzername).

Zuweisen von Zugangsberechtigungen an einen Benutzer

1. Öffnen Sie die Seite **Local User Database** (Lokale Benutzerdatenbank).
2. Wählen Sie einen Benutzer im Feld **User Name** (Benutzename).
3. Definieren Sie die Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Benutzerzugangsberechtigungen und Kennwörter wurden definiert, und das wurde Gerät aktualisiert.

Hinzufügen eines Benutzers zu der lokalen Benutzerdatenbank

1. Öffnen Sie die Seite **Local User Database** (Lokale Benutzerdatenbank).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add User** (Benutzer hinzufügen) anzuzeigen.
3. Geben Sie die Informationen in den Feldern ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der neue Benutzer wird definiert und das Gerät aktualisiert.

ANMERKUNG: Sie können bis zu 30 Benutzer auf dem Gerät definieren.

Reaktivieren eines gesperrten Benutzerkontos

1. Öffnen Sie die Seite **Local User Database** (Lokale Benutzerdatenbank).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **Lokale Benutzertabelle zu öffnen**.
3. Wählen Sie einen **User Name** (Benutzernamen) aus.
4. Markieren Sie das Kontrollkästchen Reactivate Suspended User" (Gesperrten Benutzer reaktivieren).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Benutzerzugangsberechtigungen wurden reaktiviert, und das wurde Gerät aktualisiert.

Löschen von Benutzern von einer lokalen Benutzerdatenbank

1. Öffnen Sie die Seite **Local User Database** (Lokale Benutzerdatenbank).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **Lokale Benutzertabelle** zu öffnen.
3. Wählen Sie einen **User Name** (Benutzernamen).
4. Klicken Sie das Kontrollkästchen **Remove** (Entfernen) an.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Benutzer wird gelöscht und das Gerät aktualisiert.

Zuordnen von Benutzern mithilfe der CLI-Befehle

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für die Ansicht von Feldern auf der Seite **Local User Database** (Lokale Benutzerdatenbank) zusammen.

Tabelle 6-34. CLI-Befehle für Datenbank der lokalen Benutzer

CLI-Befehl	Beschreibung
`username name [password password] [privilege level] [encrypted]`	Richtet ein auf Benutzernamen basierendes Authentifizierungssystem ein.
`set username name active`	Reaktiviert ein gesperrtes Benutzerkonto.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

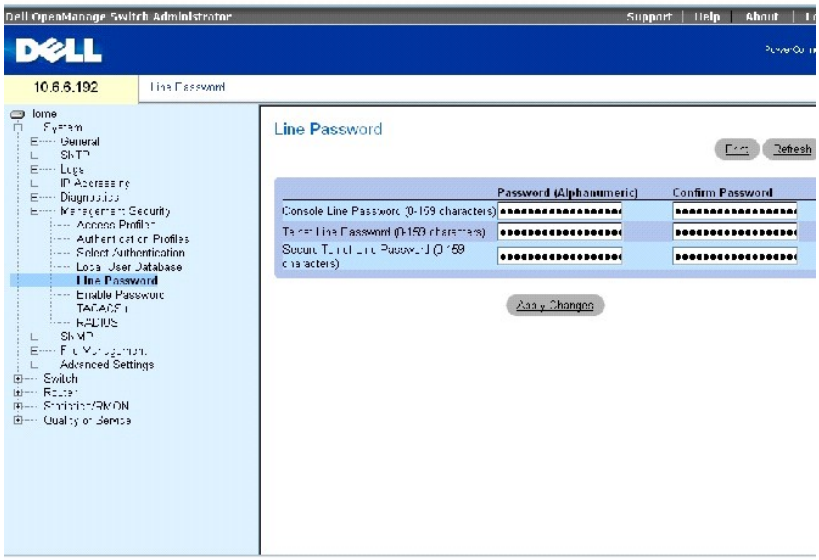
```
Console (config)#username bob password lee privilege 15


Console# set username bob active
```

Definieren von Leitungskennwörtern

Verwenden Sie die Seite **Line Password** (Leitungskennwort), um Leitungskennwörter für Verwaltungsmethoden zu definieren.

Um die Seite **Verbindungskennwort** zu öffnen, klicken Sie in der Strukturansicht auf **System→ Management Security→ Line Password**.

Abbildung 6-48. Leitungskennwort



Die Seite **Verbindungskennwort** enthält die folgenden Felder:

Line Password for Console/Telnet/Secure Telnet (Verbindungskennwort für Konsole/Telnet/Secure Telnet) Das Verbindungskennwort für den Zugang zu dem Gerät über eine Konsolen-, Telnet- oder Secure Telnet-Sitzung.

Confirm Password (Kennwort bestätigen) Bestätigt das neue Leitungskennwort. Das Kennwort erscheint im Format *****.

Definieren von Leitungskennwörtern

1. Öffnen Sie die Seite **Line Password** (Leitungskennwort).
2. Definieren Sie das Feld **Line Password** (Leitungskennwort) für den Sitzungstyp, den Sie verwenden, um mit dem Gerät eine Verbindung einzugehen.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das Leitungskennwort für den Sitzungstyp wird definiert und das Gerät aktualisiert.

Zuordnen von Leitungskennwörtern mithilfe der CLI-Befehle

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zum Definieren von Verbindungskennwörtern zusammen.

Tabelle 6-35. CLI-Befehle für Leitungskennwort

CLI-Befehl	Beschreibung
`password password [encrypted]`	Legt ein Kennwort für eine Leitung fest.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

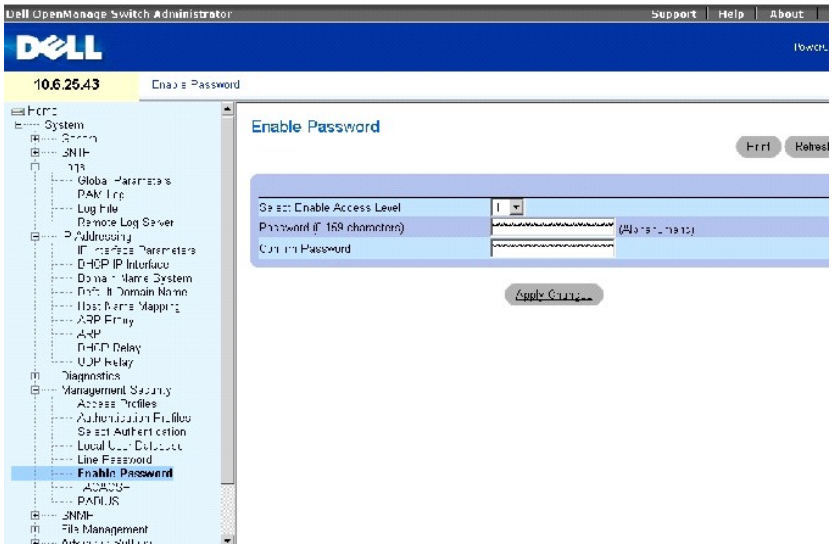
```
Console (config-line)# password ****
```

Definieren von Aktivierungskennwörtern

Auf der Seite **Kennwortaktivierung ändern** können Sie ein lokales Kennwort vergeben, um den Zugang zu verschiedenen Berechtigungsebenen (1-15) zu steuern.

Um die Seite **Kennwortaktivierung ändern** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **Management Security**→ **Enable Password**.

Abb. 6-49. Ändern eines Aktivierungskennworts:



Die Seite **Kennwortaktivierung ändern** enthält die folgenden Felder:

Select Enable Access Level (Aktivierung einer Zugriffsebene auswählen) Legt die mit dem Aktivierungskennwort verknüpfte Zugriffsebene fest. Mögliche Feldwerte sind 1-15.

Password (Kennwort) Das aktuelle Aktivierungskennwort.

Confirm Password (Kennwort bestätigen) Bestätigt das neue Aktivierungskennwort. Das Kennwort erscheint im Format *****.

Definieren eines neuen Aktivierungskennworts

1. Öffnen Sie die Seite **Modify Enable Password** (Ändern des Aktivierungskennworts).
2. Füllen Sie die Felder im Dialogfeld aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das neue Kennwort wird definiert und das Gerät aktualisiert.

Zuordnen von Aktivierungskennwörtern mithilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für das Konfigurieren von Feldern zusammengefasst, die auf der Seite Kennwortaktivierung ändern angezeigt werden.

Tabelle 6-36. CLI-Befehle für das Aktivierungskennwort

CLI-Befehl	Beschreibung
`enable password [level` *`level`*`] password [encrypted]`	Richtet ein lokales Kennwort ein, um den Zugriff auf die Benutzer- und Berechtigungsebenen zu steuern.
`show users accounts`	Zeigt Informationen über die lokale Benutzerdatenbank an.

Im Folgenden werden CLI-Befehle anhand eines Beispiels dargestellt:

```
Console# show users accounts

Username   Privilege

---------  ---------

Bob        15

Jim        15

Dell       1515
```

Konfigurieren von TACACS+-Einstellungen

Das Gerät stellt Terminal Access Controller Access Control System (TACACS+)-Client-Support bereit. TACACS+ stellt eine zentralisierte Sicherheit zur Validierung von Benutzern, die auf das Gerät zugreifen, dar.

TACACS+ stellt ein zentralisiertes Benutzerverwaltungssystem dar, das jedoch mit RADIUS und anderen Authentifizierungsprozessen übereinstimmt. TACACS+ stellt die folgenden Dienste bereit:

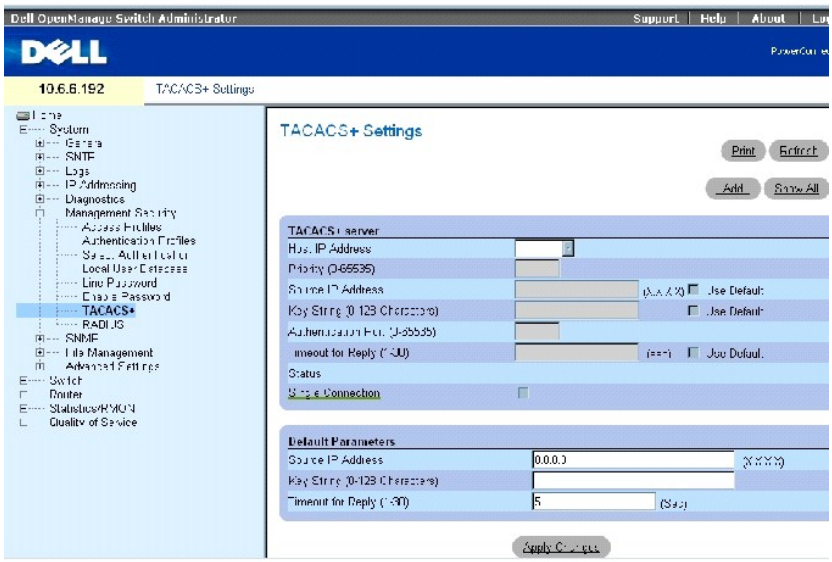
- **Authentication** (Authentifizierung) Stellt Authentifizierung bei der Anmeldung und über Benutzernamen und benutzerdefinierte Kennwörter bereit.
- **Authorization** (Berechtigung) Wird bei der Anmeldung ausgeführt. Nach Abschluss der Authentifizierungssitzung beginnt eine Authentifizierungssitzung mit dem authentifizierten Benutzernamen. Der TACACS+-Server überprüft die Benutzerrechte.

Das TACACS+-Protokoll stellt die Netzwerkintegrität mittels verschlüsselter Protokollaustausche zwischen dem Gerät und dem TACACS+-Server sicher.

Die Seite **TACACS+-Einstellungen** enthält sowohl benutzerdefinierte als auch standardmäßige TACACS+-Einstellungen für den bandinternen Management-Port.

Öffnen Sie die Seite **TACACS+-Einstellungen**, indem Sie auf **System→ Management Security→ TACACS+** in der *Strukturansicht* klicken.

Abbildung 6-50. TACACS+-Einstellungen



Die Seite TACACS+-Einstellungen enthält die folgenden Felder:

Host IP Address Gibt die IP-Adresse des TACACS+-Servers an.

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

Source IP Address (Quell-IP-Adresse) Die Quell-IP-Adresse des Geräts, die für die TACACS+-Sitzung zwischen dem Gerät und dem TACACS+-Server verwendet wird.

Key String (Schlüssel-Zeichenkette, 0-128 Zeichen) Legt den Authentifizierungs- und Verschlüsselungscode für die TACACS+-Kommunikation zwischen dem Gerät und dem TACACS+-Server fest. Dieser Schlüssel muss mit der auf dem TACACS+-Server verwendeten Verschlüsselung übereinstimmen.

Authentication Port (0-65535) Die Portnummer, über die die TACACS+-Sitzung erfolgt. Port 49 ist der Standardport.

Reply Timeout (Antwort-Zeitlimit, 1-30) Die Zeit, die vergeht, bis das Zeitlimit der Verbindung zwischen dem Gerät und dem TACACS+Server erreicht wird. Es sind Werte im Feldbereich von 1-30 möglich.

Status Der Verbindungsstatus zwischen dem Gerät und dem TACACS+-Server. Die möglichen Feldwerte sind:

Connected (Verbunden) Zwischen dem Gerät und dem TACACS+-Server ist gegenwärtig eine Verbindung aufgebaut.

Not Connected (Nicht verbunden) Zwischen dem Gerät und dem TACACS+-Server ist gegenwärtig keine Verbindung aufgebaut.

Single Connection (Einzige Verbindung) Erhält, wenn ausgewählt, eine einzige offene Verbindung zwischen dem Gerät und dem TACACS+-Server aufrecht

Die TACACS+-Standardparameter sind benutzerdefinierte Standards. Die Standardeinstellungen werden auf neu definierte TACACS+-Server angewendet. Wenn keine Standardwerte definiert sind, werden die Systemstandardwerte auf die neuen TACACS+-Server angewendet. Die TACACS+-Standardwerte lauten:

Source IP Address (Quell-IP-Adresse) Die Quell-IP-Adresse des Geräts, die für die TACACS+-Sitzung zwischen dem Gerät und dem TACACS+-Server verwendet wird.

Key String (Schlüssel-Zeichenkette, 0-128 Zeichen) Legt den Authentifizierungs- und Verschlüsselungscode für die TACACS+-Kommunikation zwischen dem Gerät und dem TACACS+-Server fest.

Timeout for Reply (Antwort-Zeitlimit, 1-30) Die Standardzeit, die vergeht, bis das Timelimit der Verbindung zwischen dem Gerät und dem TACACS+Server erreicht wird.

ANMERKUNG: Die oben genannten Standardeinstellungen treffen auch auf die Seite **OBB-TACACS+-Einstellungen** (**System→ Out-of-Band-Port→ TACACS+**) zu.

Definieren von TACACS+-Parametern

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

Die TACACS+-Einstellungen werden in dem Gerät aktualisiert.

Hinzufügen eines TACACS+-Servers

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

Die Seite TACACS+**-Host hinzufügen** wird geöffnet.

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

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

Löschen eines TACACS+-Servers von der Liste der TACACS+-Server

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

Die Seite TACACS+ **Table** (TACACS+-Tabelle) **wird geöffnet**.

3. Wählen Sie einen Eintrag in der **TACACS+-Tabelle**.
4. Wählen Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

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

Definieren der TACACS+-Server mithilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für das Konfigurieren der Felder zusammengefasst, die auf der Seite TACACS+-Einstellungen angezeigt werden.

Tabelle 6-37. CLI-Befehle für TACACS+-Einstellungen

CLI-Befehl	Beschreibung
`tacacs-server host {ip- address | hostname} [single-connection] [port port-number] [timeout timeout] [key key-string] [source source] [priority priority]`	Definiert einen TACACS+-Server-Host.
`no tacacs-server host {ip-address | hostname}`	Löscht einen ausgewählten TACACS+-Server-Host.
`tacacs-server key [key- string]`	Definiert den Authentifizierungs- und Verschlüsselungscode, der für die gesamte TACAS-Kommunikation zwischen dem Router und dem TACACS+-Server verwendet wird. Dieser Schlüssel muss mit der auf dem TACACS-Daemon verwendeten Verschlüsselung übereinstimmen. (Bereich: 0-128 Zeichen)
`no tacacs-server key`	Standardeinstellung wird wiederhergestellt.
`tacacs-server timeout` *`timeout`*	Gibt den Zeitlimit-Wert in Sekunden an. (Bereich: 1-30)
`no tacacs-server timeout`	Standardeinstellung wird wiederhergestellt.
`tacacs-server source-ip ip-address`	Gibt eine Quell-IP-Adresse an. (Bereich: Gültige IP-Adresse)
`no tacacs-server source- ip ip-address`	Standardeinstellung wird wiederhergestellt.
`show tacacs+` [*`ip-address`*]	Zeigt die Konfiguration und Statistiken für einen TACACS+-Server an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# tacacs-server host 171.16.8.1 port 49 key abc

Console (config)# end

Console# show tacacs

                                                                    

Gerätekonfiguration

--------------------

IP address:  Status     Port  Single Connection  TimeOut  Source IP  Priority
-----------  ---------  ----  -----------------  -------  ---------  --------
171.16.8.1   Not        49    Nein               globalem globalem   0
```

	Connected					
OOB-Host-Konfiguration						
IP address:	Status	Port	Single Connection	TimeOut	Source IP	Priority
----------	---------	----	----------	-------	------	--------
Es wurde kein TACACS-Server konfiguriert.						
Gerätekonfiguration						

Source IP: 0.0.0.0 (Versant-Produktversion: 6.0.0.1)						
OOB-Host-Konfiguration						

Source IP : 0.0.0.0						

Konfigurieren von RADIUS-Einstellungen

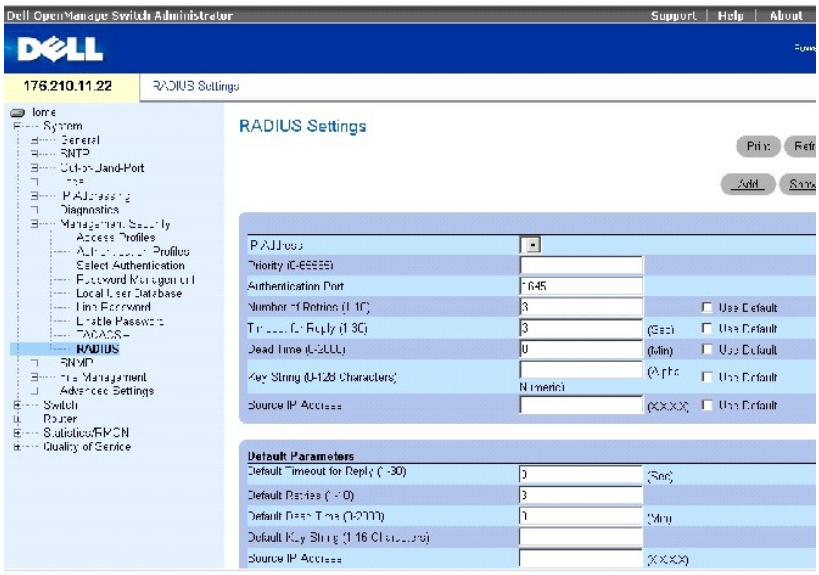
RADIUS-Server (Remote Authorization Dial-In User Service) bieten zusätzliche Sicherheit für Netzwerke. Der RADIUS-Server unterhält eine Benutzerdatenbank, die Authentifizierungsinformationen pro Benutzer enthält. RADIUS-Server bieten eine zentralisierte Authentifizierungsmethode für:

- Telnet-Zugriff
- Webzugriff
- Konsole-zu-Switch-Zugang

Die Seite **RADIUS Settings** (RADIUS-Einstellungen) enthält sowohl vom Benutzer definierte als auch standardmäßige RADIUS-Einstellungen.

Öffnen Sie die Seite **RADIUS Settings**" (RADIUS-Einstellungen), indem Sie auf **System**→ **Management Security**→ **RADIUS** in der *Strukturansicht* klicken.

Abbildung 6-51. RADIUS-Einstellungen



Die Seite **RADIUS-Einstellungen** enthält die folgenden Felder:

IP Address (IP-Adresse) IP-Adresse des Authentifizierungsports.

Priority (0-65535) (Priorität (0-065534) Gibt die Portpriorität an. Die möglichen Werte sind 0-65535.

Authentication Port (Authentifizierungsport) Identifiziert den Authentifizierungsport, der verwendet wird, um die RADIUS-Serverauthentifizierung zu überprüfen.

Number of Retries (1-10) (Anzahl der Versuche) Anzahl der übermittelten Anfragen, die an RADIUS-Server gesendet werden, bevor ein Fehler auftritt. Mögliche Feldwerte sind 1 - 10. Drei ist der Standardwert. Wenn kein hostspezifischer Wert festgelegt ist, gilt der globale Wert für alle Hosts. Klicken Sie auf **Use Default** (Standardeinstellung verwenden), um den Standardwert zu verwenden.

Timeout for Reply (1-30) (Zeitlimit für Antwort) Zeitdauer (in Sekunden), die das Gerät auf eine Antwort vom RADIUS-Server wartet, bevor das Zeitlimit erreicht ist. Mögliche Feldwerte sind 1 - 30. Drei ist der Standardwert. Wenn kein hostspezifischer Wert festgelegt ist, gilt der globale Wert für alle Hosts. Klicken Sie auf **Use Default** (Standardeinstellung verwenden), um den Standardwert zu verwenden.

Dead Time (0-2000) (Totzeit) Zeitdauer (in Minuten), die ein RADIUS-Server für Serviceanfragen deaktiviert wird. Der Bereich ist 0-2000. Wenn kein hostspezifischer Wert festgelegt ist, gilt der globale Wert für alle Hosts. Klicken Sie auf **Use Default** (Standardeinstellung verwenden), um den Standardwert zu verwenden.

Key String (0-128 Characters) (Schlüsselzeichenkette (0-128 Zeichen) Schlüsselzeichenkette, die für die Authentifizierung und Verschlüsselung der gesamten RADIUS-Kommunikation zwischen dem Gerät und dem RADIUS-Server verwendet wird. Der Schlüssel muss der RADIUS-Verschlüsselung entsprechen. Wenn kein hostspezifischer Wert festgelegt ist, gilt der globale Wert für alle Hosts.

Source IP Address (Quellen-IP-Adresse) IP-Adresse des Geräts, das auf den RADIUS-Server zugreift.

ANMERKUNG: Die standardmäßigen Parameter auf dieser Seite werden vom Benutzer definiert.

Default Retries (1-10) (Standardmäßige Anzahl der Versuche) Standardmäßige Anzahl der übermittelten Anfragen, die an RADIUS-Server gesendet werden, bevor ein Fehler auftritt.

Default Timeout for Reply (1-30) (Standardmäßiges Zeitlimit für Antwort) Standardmäßige Anzahl der übermittelten Anfragen, die an RADIUS-Server

gesendet werden, bevor ein Fehler auftritt. Mögliche Feldwerte sind 1 - 30.

Default Dead Time (0-2000) Legt die Standardzeit in Minuten fest, in der der RADIUS-Server für Dienstanfragen umgangen wird. Der Bereich ist 0-2000.

Default Key String (0-128 Characters) (Standardmäßige Schlüsselzeichenkette (0-128 Zeichen)) Standardmäßige Schlüsselzeichenkette, die für die Authentifizierung und Verschlüsselung der gesamten RADIUS-Kommunikation zwischen dem Gerät und dem RADIUS-Server verwendet wird. Der Schlüssel muss der RADIUS-Verschlüsselung entsprechen.

Source IP Address (Quellen-IP-Adresse) Standardmäßige IP-Adresse 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), um die Seite **RADIUS Server hinzufügen** anzuzeigen.
3. Definieren Sie die Felder im Dialogfeld.
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. Definieren Sie die Felder im Dialogfeld.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die RADIUS-Einstellungen werden in dem Gerät aktualisiert.

Ändern der RADIUS-Servereinstellungen

1. Öffnen Sie die Seite **RADIUS Settings** (RADIUS-Einstellungen).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Liste **RADIUS Servers** (RADIUS-Server) anzuzeigen.
3. Ändern Sie die Dialogfelder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die RADIUS-Servereinstellungen werden geändert und das Gerät aktualisiert.

Löschen eines RADIUS-Servers von der Liste der RADIUS-Server

1. Öffnen Sie die Seite **RADIUS Settings** (RADIUS-Einstellungen).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Liste **RADIUS Servers** (RADIUS-Server) anzuzeigen.
3. Wählen Sie einen RADIUS-Server, und markieren Sie das Kontrollkästchen **Remove** (Entfernen).

Der RADIUS-Server wird von der Liste *entfernt*.

Definieren der RADIUS-Server mithilfe der CLI-Befehle

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für das Definieren von Feldern zusammen, die auf der Seite **RADIUS-Einstellungen** angezeigt werden.

Tabelle 6-38. CLI-Befehle für RADIUS-Server

CLI-Befehl	Beschreibung
`radius-server timeout timeout`	Stellt die Zeitdauer ein, die ein Router auf die Antwort des Serverhosts wartet.
`radius-server retransmit retries`	Spezifiziert die Anzahl der Durchläufe, die die Software die Liste der RADIUS-Serverhosts durchsucht.
`radius-server deadtime deadtime`	Konfiguriert, dass nicht verfügbare Server übersprungen werden.
`radius-server key key-string`	Stellt die Authentifizierung und den Verschlüsselungscode für die gesamte RADIUS-Kommunikation zwischen dem Router und der RADIUS-Umgebung ein.
`radius-server host ip- address [auth-port auth-port-number] [timeout timeout] [retransmit retries] [deadtime deadtime] [key key-string] [source source] [priority priority]`	Spezifiziert einen RADIUS-Serverhost.
`show radius-servers`	Zeigt die RADIUS-Servereinstellungen an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# radius-server timeout 5

Console (config)# radius-server retransmit 5

Console (config)# radius-server deadtime 10

Console (config)# radius-server key dell-server

Console (config)# radius-server host 196.210.100.1 auth-port 127 timeout 20

Console# show radius-servers

IP address  Auth   Acct   TimeOut  Retransmit  Deadtime   Source IP  Priority

----------  ----   ----   -------  ----------  --------   ---------  --------


172.16.1.1  164    51646  3        3           0                     01
172.16.1.2  164    51646  3        3           0                     02
```

Definieren von SNMP-Parametern

Das **Simple Network Management Protocol** (SNMP - Einfaches Netzwerkverwaltungsprotokoll) bietet eine Methode zur Verwaltung von Netzwerkgeräten. Das Gerät unterstützt SNMP Version 1, SNMP Version 2 und SNMP Version 3.

ANMERKUNG: Standardmäßig ist SNMPv2 automatisch auf dem Gerät aktiviert. Um SNMPv3 zu aktivieren, muss eine lokale Engine-ID für das Gerät definiert werden. Die lokale Engine-ID kann eine durch den Benutzer erstellte Zeichenkette sein oder eine generierte Standardzeichenkette auf der Basis der MAC-Adresse des Geräts. Weitere Informationen über das Konfigurieren der lokalen Engine-ID finden Sie unter **Definieren von globalen SNMP-Parametern**.

SNMP v1 und v2

Der SNMP-Agent verwaltet eine Liste von Variablen, die der Verwaltung des Geräts dienen. Diese Variablen sind in der **Management Information Base** (MIB) definiert. Die MIB präsentiert die vom Agenten gesteuerten Variablen. Die SNMP-Software definiert das Format der MIB-Spezifikation sowie das Format, das für den Informationszugriff über das Netzwerk verwendet wird. Die Zugangsberechtigung für den SNMP-Agenten werden über Zugangszeichenketten gesteuert.

SNMP v3

SNMP v3 wendet auch Zugangssteuerung und ein neues Trapverfahren auf PDUs der Versionen SNMPv1 und SNMPv2. Außerdem wurde für SNMPv3 das User Security Model (Benutzersicherheitsmodell, USM) entwickelt und beinhaltet Folgendes:

- **Authentication** (Authentifizierung) Bietet Datenintegritäts- und Datenursprungsauthentifizierung.
- **Privacy** (Datenschutz) Schützt vor Veröffentlichung von Meldungsinhalten. Cipher-Bock-Chaining (CBC) wird für die Verschlüsselung verwendet. Entweder ist nur die Authentifizierung für eine SNMP-Meldung aktiviert, oder Authentifizierung als auch Datenschutz sind für eine SNMP-Meldung aktiviert. Datenschutz kann jedoch nicht ohne gleichzeitiges Aktivieren der Authentifizierung aktiviert werden.
- **Timeliness** (Ohne Zeitlimit) Schützt vor verspätetem Eingang von Meldungen oder vor Meldungsredundanz. Der SNMP-Agent vergleicht eingehende Meldungen mit der Zeitinformation der Meldung.
- **Key Management** (Schlüsselverwaltung) Definiert die Verwaltung der Schlüsselerstellung, von Schlüsselaktualisierungen und der Schlüsselverwendung.

Das Gerät unterstützt SNMP-Benachrichtigungsfilter auf der Basis von Objekt-IDs (OID). Objekt-IDs werden vom System zum Verwalten von Gerätefunktionen verwendet. SNMP v3 unterstützt die folgenden Funktionen:

- Sicherheit
- Zugangskontrolle
- Traps

Authentifizierungs- oder Datenschutzschlüssel werden im SNMPv3-Benutzersicherheitsmodell, USM geändert.

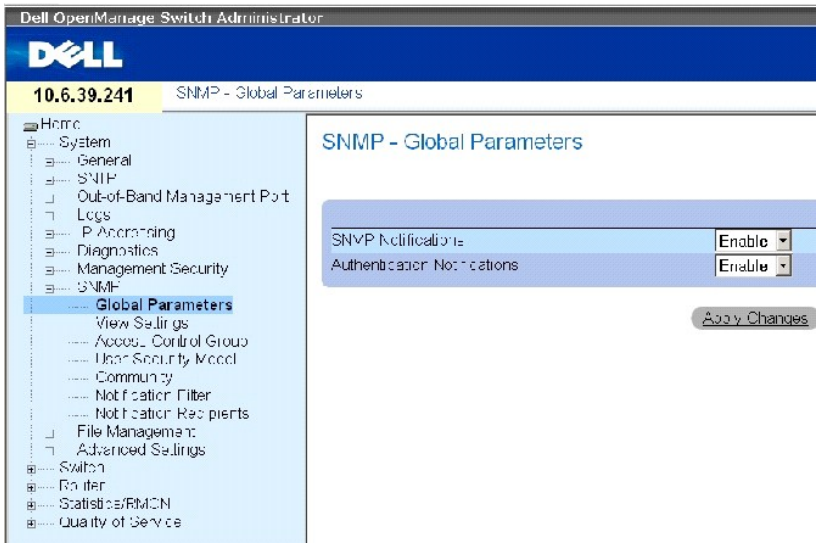
Verwenden Sie die SNMP-Seite, um SNMP-Parameter zu definieren. Öffnen Sie die Seite SNMP, indem Sie auf **System→ SNMP** in der *Strukturansicht* klicken.

Definieren von globalen SNMP-Parametern

Auf der Seite **Globale Parameter** können Sie SNMP- und Authentifizierungsbenachrichtigungen aktivieren.

Um die Seite **Globale Parameter** zu öffnen, klicken Sie in der *Strukturansicht* auf **System→ SNMP→ Global Parameters**.

Abbildung 6-52. Globale Parameter



Die Seite **Globale Parameter** enthält die folgenden Parameter:

SNMP Notifications (SNMP-Benachrichtigungen) Aktiviert oder deaktiviert das Versenden von SNMP-Benachrichtigungen durch das Gerät.

Authentication Notifications (Authentifizierungsbenachrichtigungen) Aktiviert oder deaktiviert den Versand von SNMP-Traps durch das Gerät, wenn die Authentifizierung fehlgeschlagen ist.

Aktivieren von SNMP-Benachrichtigungen

1. Öffnen Sie die Seite **Global Parameter**.
2. Wählen Sie **Enable** (Aktivieren) aus dem Feld **SNMP Notifications** (SNMP-Benachrichtigungen) aus.
3. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

SNMP-Benachrichtigungen wurden aktiviert, und das Gerät wurde aktualisiert.

Aktivieren von Authentifizierungsbenachrichtigungen

1. Öffnen Sie die Seite **Global Parameter**.
2. Wählen Sie **Enable** (Aktivieren) aus dem Feld **Authentication Notifications** (Authentifizierungsbenachrichtigungen) aus.
3. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

Authentifizierungsbenachrichtigungen wurden aktiviert, und das Gerät wurde aktualisiert.

Aktivieren von SNMP-Benachrichtigungen mithilfe von CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite **Globale Parameter** angezeigt werden.

Tabelle 6-39. CLI-Befehle für SNMP-Benachrichtigungen

CLI-Befehl	Beschreibung
snmp-server engineID local {*engineid-string* | default}	Definiert die SNMP-Engine-ID auf dem lokalen Gerät.
show snmp	Zeigt die aktuelle SNMP-Gerätekonfiguration an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# snmp-server enable traps

Console (config)# snmp-server trap authentication

Console (config)# end

Console# show snmp

                                                                    

Community-String                Community-Access        IP address:
------------                    ----------------        ----------------
public.                         read only               All
private                         read write              172.16.1.1
private                         read write              172.17.1.1
                                                        

OBB-Management-Stations
Community-String                Community-Access        IP address:
------------                    ----------------        ----------------
private                         read write              176.16.8.9
                                                        

Traps are enabled.

Authentication trap is enabled.
                                                        

Trap-Rec-Address                Trap-Rec-Community      Version
192.122.173.42                  public.                 2
                                                        
```

OOB trap receivers		
Trap-Rec-Address	Trap-Rec-Community	Version
176.16.8.9	public.	2
System Contact: Robert		
System Location: Marketing		

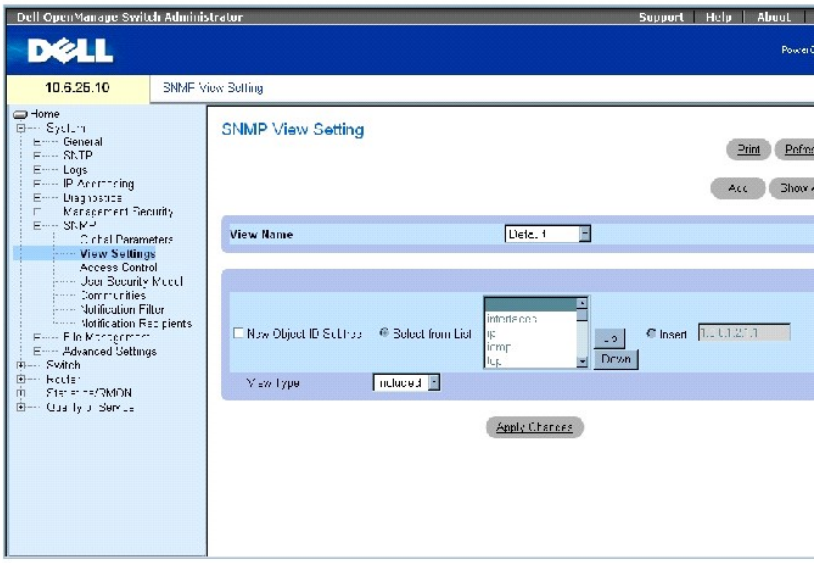
Definieren von SNMP-Ansichten

SNMP-Ansichten gewähren Zugang zu Gerätefunktionen oder Funktionsaspekten oder sperren den Zugang. So kann eine Ansicht beispielsweise so definiert sein, dass SNMP-Gruppe A nur Leserechte auf Routing eingeräumt wird, SNMP-Gruppe B jedoch über Lese- und Schreibrechte auf Routing verfügt. Zugang zu den Funktionen wird über den MIB-Namen oder die MIB-Objekt-ID gewährt.

Sie können die Seite **SNMP-Ansichtseinstellungen** verwenden, um SNMP-Ansichten zu definieren.

Um die Seite **SNMP-Ansichtseinstellungen** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **SNMP**→ **View Settings**.

Abbildung 6-53. SNMP-Ansichtseinstellungen



Die Seite **SNMP-Ansichtseinstellungen** enthält die folgenden Felder:

View Name (Ansichtsname) Enthält eine Liste von benutzerdefinierten Ansichten. Ein Ansichtsname kann aus bis zu 30 alphanumerischen Zeichen bestehen.

New Object ID Subtree (Neue Objekt-ID-Unterstruktur) Legt die Gerätefunktion OID" fest, die in der SNMP-Ansicht ein- oder ausgeschlossen ist.

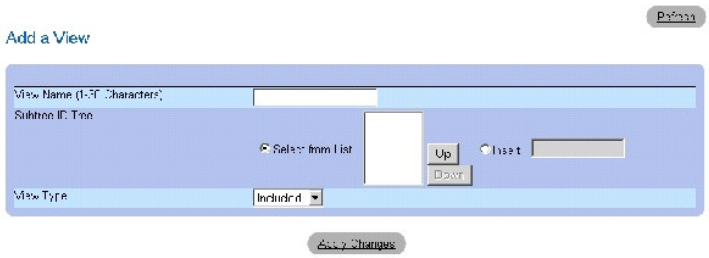
View Type (Ansichtstyp) Aktiviert, wenn ausgewählt, den Zugang zu einer bestimmen Funktion oder einem bestimmen Funktionsaspekt in der SNMP-Ansicht.

Hinzufügen einer Ansicht

1. Öffnen Sie die Seite **SNMP-Ansichtseinstellungen**.
2. Klicken Sie auf **Add**" (Hinzufügen).

Die Seite **Ansicht hinzufügen** wird geöffnet:

Abbildung 6-54. Ansicht hinzufügen



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

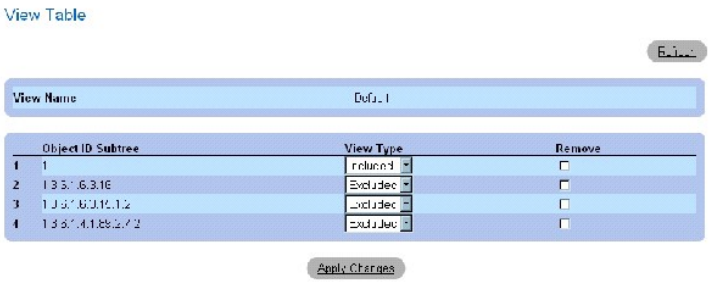
Die SNMP-Ansicht wurde hinzugefügt, und das Gerät wurde aktualisiert.

Anzeigen der Ansichtstabelle

1. Öffnen Sie die Seite **SNMP-Ansichtseinstellungen**.
2. Klicken Sie auf **Show All**" (Alles anzeigen).

Die Seite **Ansichtstabelle** wird geöffnet:

Abbildung 6-55. Ansichtstabelle



Entfernen von SNMP-Ansichten

1. Öffnen Sie die Seite **SNMP-Ansichtseinstellungen**.
2. Klicken Sie auf **Show All**" (Alles anzeigen).

Die Seite **Ansichtstabelle** wird geöffnet.

3. Wählen Sie eine SNMP-Ansicht aus.
4. Klicken Sie das Kontrollkästchen **Remove** (Entfernen) an.
5. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

Die SNMP-Ansicht wurde gelöscht, und das Gerät wurde aktualisiert.

Definieren von SNMP-Ansichten mithilfe von CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für das Definieren der Felder zusammengefasst, die auf der Seite **SNMP-Ansichtseinstellungen** angezeigt werden.

Tabelle 6-40. CLI-Befehle für SNMP-Ansichten

CLI-Befehl	Beschreibung
show snmp views [*viewname*]	Zeigt die Konfiguration der Ansichten an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# snmp-server view user1 1 included

Console (config)# end

Console # show snmp views
```

Name	OID Tree	Typ
----------	----------	----------
user1	iso	included
Standard	iso	included
Standard	snmpVacmMIB	excluded
Standard	usmUser	excluded
Standard	rndCommunityTable	excluded
DefaultSuper	iso	included

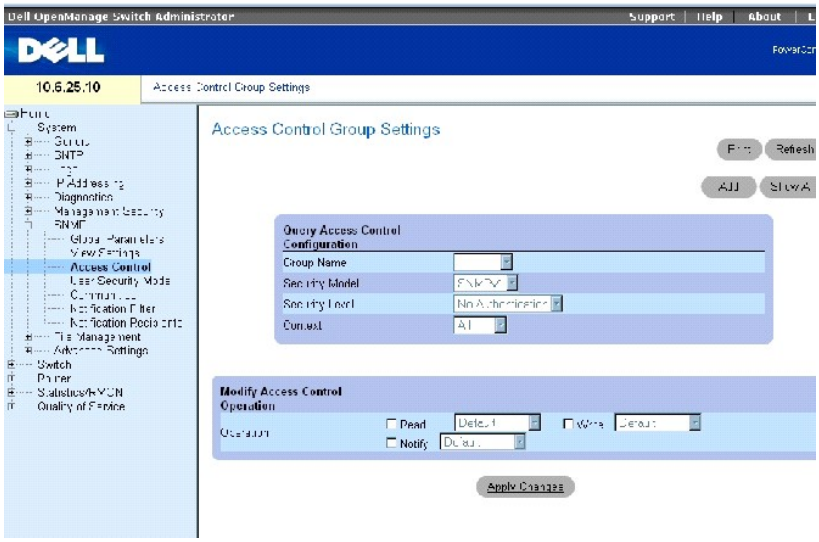
Definieren der SNMP-Zugangskontrolle

Die Seite **Zugangskontrollgruppe** bietet Informationen über das Erstellen von SNMP-Gruppen und die Vergabe von SNMP-Zugangsberechtigungen. Über Gruppen können Netzwerk-Manager Zugangsberechtigungen auf bestimmte Gerätefunktionen oder Funktionsaspekte vergeben.

Der bandexterne Port wird als separates Gerät behandelt, wenn SNMP-Funktionen verwendet werden. Ansichten können auf bandexterne MIBs, Geräte-MIBs oder alle MIBs eingeschränkt werden.

Um die Seite **Zugangskontrollgruppe** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **SNMP**→ **Access Control**.

Abbildung 6-56. Zugangskontrollgruppe



Die Seite **Zugangskontrollgruppe** enthält die folgenden Felder:

Group Name (Gruppenname) Enthält eine Liste von benutzerdefinierten Gruppen, auf die die Zugangskontrollregeln angewendet werden. Eine Gruppe kann aus bis zu 30 alphanumerischen Zeichen bestehen.

Security Model (Sicherheitsmodell) Definiert die SNMP-Version, die mit der Gruppe zusammenhängt. Die möglichen Feldwerte sind:

SNMPv1 SNMPv1 wird für die Gruppe definiert.

SNMPv2 SNMPv2 wird für die Gruppe definiert.

SNMPv3 SNMPv3 wird für die Gruppe definiert.

Security Level (Sicherheitsstufe) Die Sicherheitsstufe, die mit der Gruppe zusammenhängt. Sicherheitsstufen können nur auf SNMPv3-Gruppen angewendet werden. Die möglichen Feldwerte sind:

No Authentication (Keine Authentifizierung) Es können weder Sicherheitsstufen der Art Authentifizierung noch der Art Datenschutz auf die Gruppe angewendet werden.

Authentication (Authentifizierung) Authentifiziert SNMP-Meldungen, ohne diese zu verschlüsseln.

Privacy (Datenschutz) Authentifiziert SNMP-Meldung und verschlüsselt diese.

Operation (Arbeitsgang) Definiert Zugangsberechtigungen für Gruppen. Die möglichen Feldwerte sind:

Read (Lesen) Wählen Sie eine Ansicht aus, die den Verwaltungszugang auf das Anzeigen von Inhalten für den Agenten 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 Management Schreibrechte für die Inhalte des Agenten, nicht jedoch für die Community gewährt.

Notify (Benachrichtigen) Wählen Sie eine Ansicht aus, die das Versenden von SNMP-Traps oder Informs gewährt.

Context (Kontext) Kontext, für den die Zugangsgruppe konfiguriert wurde. Die möglichen Feldwerte sind:

Router (Router) Die Zugangsgruppe wurde für bandinternes Management konfiguriert.

OOB (Bandextern) Die Zugangsgruppe wurde für bandexternes Management konfiguriert.

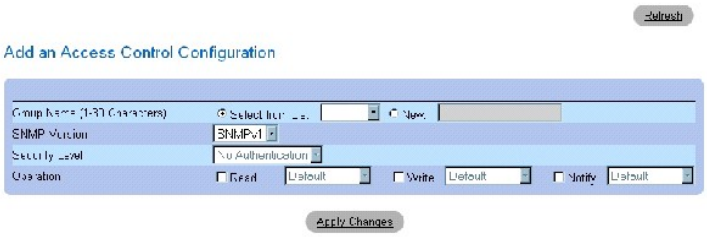
All (Alle) Die Zugangsgruppe wurde sowohl für bandinternes als auch für bandexternes Management konfiguriert.

Definieren von SNMP-Gruppen

1. Öffnen Sie die Seite **Zugangskontrollgruppe**.
2. Klicken Sie auf **Add**" (Hinzufügen).

Die Seite **Zugangskontrollgruppe hinzufügen** wird geöffnet:

Abbildung 6-57. Zugangskontrollgruppe hinzufügen



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

Die Gruppe wurde hinzugefügt und das Gerät aktualisiert.

Anzeigen der Zugangstabelle

1. Öffnen Sie die Seite **Zugangskontrollgruppe**.
2. Klicken Sie auf **Show All**" (Alles anzeigen).

Die Seite **Zugangstabelle** wird geöffnet:

Abbildung 6-58. Zugangstabelle

Löschen einer Gruppe

1. Öffnen Sie die Seite **Zugangskontrollgruppe**.
2. Klicken Sie auf **Show All**" (Alles anzeigen).

Die **Zugangstabelle** wird geöffnet.

3. Wählen Sie eine Gruppe aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

Die Gruppe wurde gelöscht und das Gerät aktualisiert.

Definieren der SNMP-Zugangskontrolle mithilfe von CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für das Definieren von Feldern zusammen, die auf der Seite Zugangskontrollgruppe angezeigt werden.

Tabelle 6-41. CLI-Befehle für die SNMP-Zugangskontrolle

CLI-Befehl	Beschreibung
snmp-server group *groupname* {**v1** | **v2** | **v3** {**noauth** | **auth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*]	Konfigurieren Sie eine neue einfache Netzwerkverwaltungsprotokollgruppe oder eine Tabelle, die SNMP-Benutzer zu SNMP-Ansichten hinzufügt.
show snmp groups [*groupname*]	Zeigt die Konfiguration der Gruppen an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

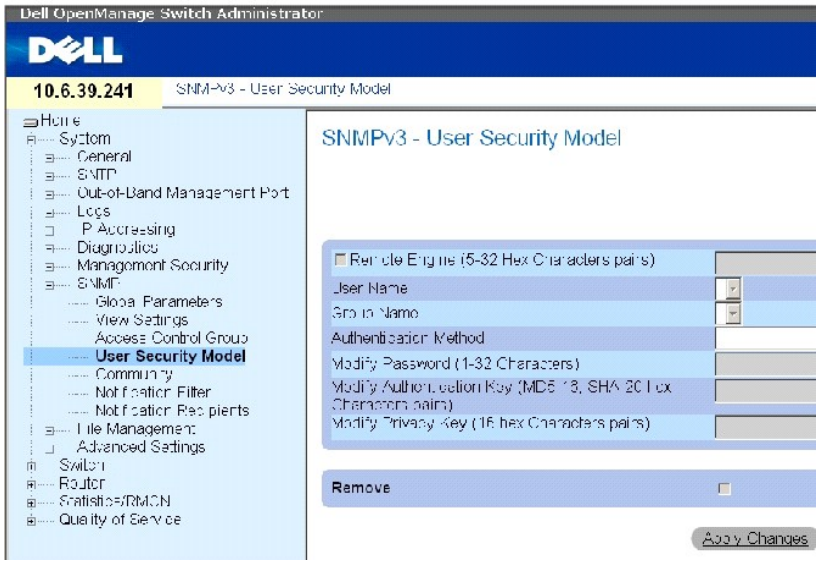
```
Console (config)# snmp-server group user-group v3 priv read user- view
```

Zuordnen von SNMP-Benutzersicherheit

Die Seite **SNMPv3-Benutzersicherheitsmodell, USM** ermöglicht das Zuordnen von Systembenutzern zu SNMP-Gruppen sowie das Definieren des Benutzerauthentifizierungsverfahrens.

Um die Seite **SNMPv3-Benutzersicherheitsmodell, USM** zu öffnen, klicken Sie in der Strukturansicht auf **System→ SNMP→ User Security Model**.

Abbildung 6-59. SNMPv3-Benutzersicherheitsmodell, USM



Die Seite **SNMPv3-Benutzersicherheitsmodell, USM** enthält die folgenden Felder:

Engine ID (Engine-ID) Identifiziert das über Remote-SNMPv3 aktivierte Gerät, mit dem der ausgewählte Benutzer verbunden ist.

Remote Engine ID (Remote-Engine-ID) Gibt an, dass der Benutzer auf einem über Remote-SNMPv3 aktivierten Gerät konfiguriert ist. Wenn die Engine-ID definiert ist, können Remote-Geräte Informationsmeldungen erhalten.

User Name (Benutzername) Enthält eine Liste mit benutzerdefinierten Benutzernamen.

Group Name (Gruppenname) Enthält eine Liste mit benutzerdefinierten SNMP-Gruppen. SNMP-Gruppen werden auf der Seite **Zugangskontrollgruppe** definiert.

Authentication Method (Authentifizierungsmethode) Legt die Authentifizierungsmethode fest, die zur Authentifizierung der Benutzers verwendet werden soll. Die möglichen Feldwerte sind:

None (Kein) Es wird keine Benutzerauthentifizierung angewendet.

MD5 Password (MD5-Kennwort) Benutzer werden über das HMAC-MD5-96-Authentifizierungslevel authentifiziert. Der Benutzer muss ein Kennwort festlegen.

SHA Password (SHA-Kennwort) Benutzer werden über das HMAC-SHA-96-Authentifizierungslevel authentifiziert. Der Benutzer muss ein Kennwort eingeben.

MD5 Key (MD5-Schlüssel) Die Benutzer werden über das HMAC-MD5-96-Authentifizierungslevel authentifiziert. Der Benutzer muss entweder einen Authentifizierungsschlüssel oder einen Datenschutzschlüssel eingeben.

SHA Key (SHA-Schlüssel) Benutzer werden über das HMAC-SHA-96-Authentifizierungslevel authentifiziert. Der Benutzer muss entweder einen Authentifizierungsschlüssel oder einen Datenschutzschlüssel eingeben.

Password (0-32 Characters) (Kennwort (0-32 Zeichen)) Ändert das benutzerdefinierte Kennwort für die Gruppe. Das Kennwort kann maximal 32 Zeichen enthalten. Kennwörter werden nur dann definiert, wenn Authentifizierungsmethode MD5- oder SHA-Kennwort ist.

Authentication Key (MD5-16; SHA-20 hexa chars) (Authentifizierungsschlüssel (MD5-16; SHA-20 hexa chars)) Legt den Authentifizierungsschlüssel fest. Ein Authentifizierungsschlüssel wird nur dann definiert, wenn die Authentifizierungsmethode MD5-Schlüssel oder SHA-Schlüssel lautet.

Privacy Key (16 hexa chars) (Datenschutzschlüssel (16 hexa chars)) Legt ein Kennwort für die Authentifizierung und das Erstellen eines DES-Schlüssels für Datenschutz fest. Ein Datenschutzschlüssel wird nur dann definiert, wenn die Authentifizierungsmethode MD5-Schlüssel oder SHA-Schlüssel lautet.

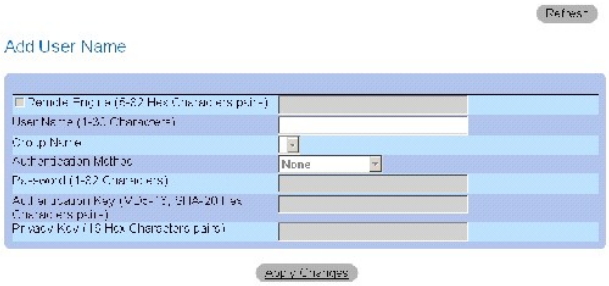
Remove (Entfernen) Wenn diese Option markiert wurde, wird der ausgewählte Benutzer aus der markierten Gruppe entfernt.

Hinzufügen von SNMPv3-Benutzern zu einer Gruppe

1. Öffnen Sie die Seite **SNMPv3-Benutzersicherheitsmodell, USM**.
2. Klicken Sie auf **Add**" (Hinzufügen).

Die Seite **SNMPv3-Benutzername hinzufügen** wird geöffnet:

Abbildung 6-60. SNMPv3-Benutzername hinzufügen



3. Definieren Sie die entsprechenden Felder.
4. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).
5. Der Benutzer wird zu der Gruppe hinzugefügt, und das Gerät wird aktualisiert.

Anzeigen der Benutzersicherheitsmodelltabelle

1. Öffnen Sie die Seite **SNMPv3-Benutzersicherheitsmodell, USM.**
2. Klicken Sie auf **Show All**" (Alles anzeigen).

Die **Benutzersicherheitsmodelltabelle** wird geöffnet:

Abbildung 6-61. SNMPv3-Benutzersicherheitsmodelltabelle

Löschen eines Eintrags aus der Benutzersicherheitsmodelltabelle

1. Öffnen Sie die Seite **SNMPv3-Benutzersicherheitsmodell, USM**.
2. Klicken Sie auf **Show All**" (Alles anzeigen).

   Die Seite **Benutzersicherheitsmodelltabelle** wird geöffnet.
3. Wählen Sie einen Eintrag aus.
4. Klicken Sie das Kontrollkästchen **Remove** (Entfernen) an.
5. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

   Der Eintrag wird entfernt und das Gerät aktualisiert.

Definieren von SNMP-Benutzern mithilfe von CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für das Definieren der Felder zusammengefasst, die auf der Seite **SNMPv3-Benutzersicherheitsmodell, USM** angezeigt werden.

Tabelle 6-42. CLI-Befehle für SNMP-Benutzer

CLI-Befehl	Beschreibung
show snmp users [*username*]	Zeigt die Konfiguration des Benutzers an.

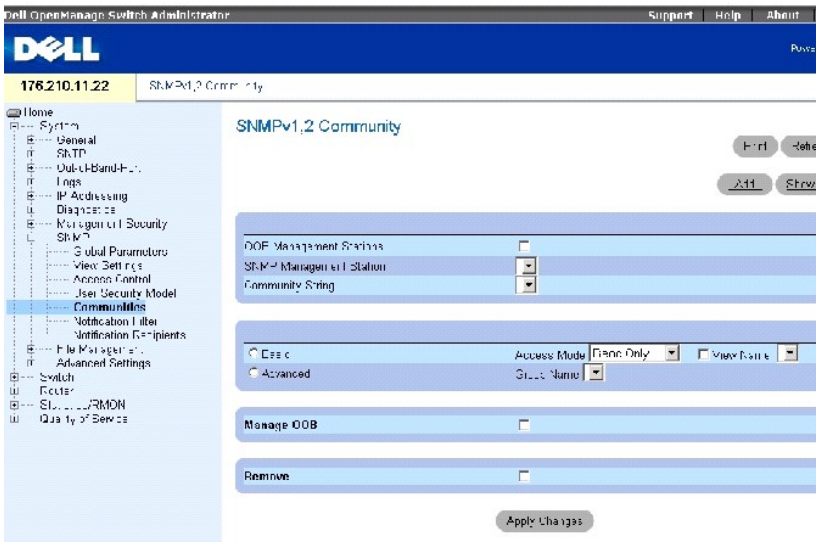
```
Console (config)# snmp-server user John auth-md5 1234

Console (config)# end

Console (config)# show snmp users

Name        Group Name      Auth Method     Fern
-------     ----------      -----------     ------
John        user-group      md5
```

Definieren von Communities

Zugangsberechtigungen werden über das Definieren von Communitys auf der Seite **SNMPv1, 2-Community** verwaltet. Wenn die Communitynamen geändert werden, werden die Zugangsberechtigungen ebenfalls geändert. SNMP-Communitys werden nur für SNMP v1 und SNMP v2 definiert.

Um die Seite **SNMPv1, 2-Community** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **SNMP**→ **Communities**.

Abbildung 6-62. SNMPv1, 2-Community



Die Seite **SNMPv1, 2-Community** enthält die folgenden Felder:

OOB Management Station (OBB-Management-Station) Markieren Sie dieses Kontrollkästchen, um eine separate SNMP-Community für den bandexternen Port zu erstellen. Wenn dieses Kontrollkästchen nicht markiert ist, greift die Management-Station über bandinterne Ports auf das Gerät zu.

SNMP Management Station (SNMP-Management-Station) Enthält eine Liste mit IP-Adressen von Management-Stationen, für die Communityzeichenfolgen definiert wurden.

ANMERKUNG: Nur Superuser verwenden dieselbe Community, um bandexterne und bandinterne Ports zu konfigurieren.

Community String (Communityzeichenfolge) Enthält eine Liste mit benutzerdefinierten Communityzeichenfolgen, die als Kennwort dienen und zum Authentifizieren der SNMP-Management-Station gegenüber dem Gerät verwendet werden. Eine Communityzeichenfolge darf höchstens 20 Zeichen enthalten.

Basic (Basis) Aktiviert den SNMP-Basismodus für die ausgewählte Community. Die möglichen Feldwerte sind:

Access Mode (Zugriffsmodus) Definiert die Zugriffsrechte der Community. . Die möglichen Feldwerte sind:

Read-Only (Schreibgeschützt) Der Managementzugang ist schreibgeschützt. Es können daher keine Änderungen an der Community vorgenommen werden.

Read-Write (Schreib-Lese-Zugriff) Der Managementzugang verfügt über Schreib- und Leserechte. Daher können Änderungen an der Gerätekonfiguration, nicht aber an der Community vorgenommen werden.

SNMP-Admin (SNMP-Verwaltung) Der Benutzer kann auf alle Konfigurationsoptionen des Geräts zugreifen und besitzt Rechte, die Community zu verändern.

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

Advanced (Erweitert) Enthält eine Liste mit benutzerdefinierten Gruppen. Wenn der erweiterte SNMP-Modus ausgewählt ist, werden die Zugangskontrollregeln einschließlich der Gruppe für die ausgewählte Community aktiviert. Durch den erweiterten Modus werden auch die SNMP-Gruppen für bestimmte SNMP-Communitys aktiviert. Der erweiterte SNMP-Modus wird nur für SNMPv3 definiert.

Manage OOB (OBB-Verwaltung) Wenn dieses Kontrollkästchen markiert ist, wird SNMP-Management für die OBB-Management-Stations ermöglicht, die mit

dem Gerät lediglich über einen bandexternen Port verbunden sind.

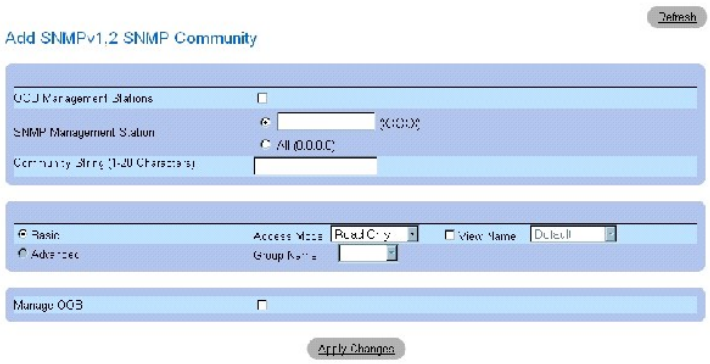
Remove (Entfernen) Wenn dieses Kontrollkästchen markiert ist, wird eine Community entfernt.

Definieren einer neuen Community

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

   Die Seite **SNMPv1, 2-Community hinzufügen** wird geöffnet:

Abbildung 6-63. SNMPv1, 2-Community hinzufügen



3. Füllen Sie die entsprechenden Felder aus.

   Zusätzlich zu den Feldern auf der Seite **SNMPv1, 2-Community** enthält die Seite **SNMPv1, 2-Community hinzufügen** das Feld **All (0.0.0.0)** (Alle (0.0.0.0)), das angibt, ob für eine bestimmte oder für sämtliche Management-Stationen überhaupt eine SNMP-Community definiert wurde.

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

   Die neue Community wird gespeichert und das Gerät aktualisiert.

Löschen von Communities

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

   Die Seite **SNMPv1, 2-Community-Tabellen** wird geöffnet.

3. Wählen Sie eine Community, und markieren Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Community-Eintrag wird entfernt und das Gerät aktualisiert.

Konfigurieren der Communities mithilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für das Definieren der Felder zusammengefasst, die auf der Seite **SNMPv1, 2-Community** angezeigt werden.

Tabelle 6-43. CLI-Befehle für SNMP-Community

CLI-Befehl	Beschreibung
`snmp-server community community [ro | rw | su] [ip-address][view view-name][type {router | oob}]`	Konfiguriert die Community-Zugriffszeichenkette so, dass SNMP-Protokollzugriffe zulässig sind.
`snmp-server community-group community group-name [ip-address] [type {router | oob}]`	Konfiguriert die Community-Zugriffszeichenkette so, dass eingeschränkter Zugriff auf SNMP-Protokolle auf der Basis von Gruppenzugangsberechtigungen zulässig ist.
`show snmp`	Zeigt die aktuelle SNMP-Gerätekonfiguration an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

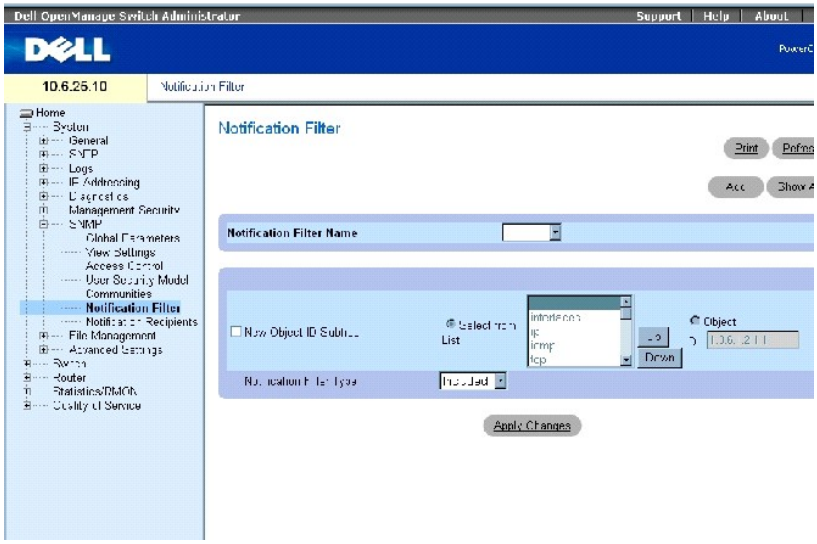
```
Console (config)# snmp-server community dell ro 10.1.1.1
```

Definieren von SNMP-Benachrichtigungsfiltern

Auf der Seite **Benachrichtigungsfilter** können Sie Rechte zum Filtern von Traps auf der Basis von Objekt-IDs einräumen. Jede Objekt-ID ist mit einer Gerätefunktion oder einem Funktionsaspekt verknüpft. Die Seite **Benachrichtigungsfilter** ermöglicht Netzwerkmanagern, Benachrichtigungen zu filtern.

Um die Seite **Benachrichtigungsfilter** zu öffnen, klicken Sie in der Strukturansicht auf **System→ SNMP→ Notification Filters**.

Abbildung 6-64. Benachrichtigungsfilter



Die Seite **Benachrichtigungsfilter** enthält die folgenden Felder:

Notification Filter Name (Name Benachrichtigungsfilter) Enthält eine Liste mit benutzerdefinierten Benachrichtigungsfiltern. Der Name eines Benachrichtigungsfilters kann aus maximal 30 Zeichen bestehen.

New Object Identifier Subtree (Neue Objekt-ID-Unterstruktur) Die Objekt-ID, für die Benachrichtigungen gesendet oder geblockt werden. Wenn ein Filter auf eine Objekt-ID angewendet wird, werden Traps oder Informs generiert und an die Trap-Empfänger gesendet. Objekt-IDs werden entweder aus dem

Listenfeld *Select from List* (Auswählen aus) ausgewählt oder im Feld **Object ID** (Objekt-ID) angegeben.

Notification Filter Type (Typ Benachrichtigungsfilter) Gibt an, ob Informs oder Traps in Bezug auf die Objekt-ID an die Trap-Empfänger gesendet werden.

Excluded (Ausgeschlossen) Schränkt die Objekt-ID ein, Traps oder Informs zu senden.

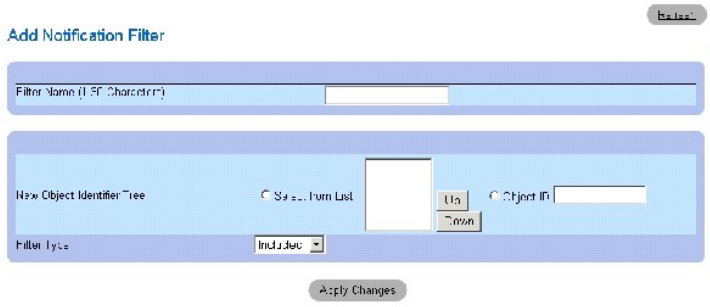
Included (Eingeschlossen) Sendet Objekt-ID-bezogene Traps oder Informs.

Hinzufügen von SNMP-Filtern

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

Die Seite **Filter hinzufügen** wird geöffnet:

Abbildung 6-65. Filter hinzufügen



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

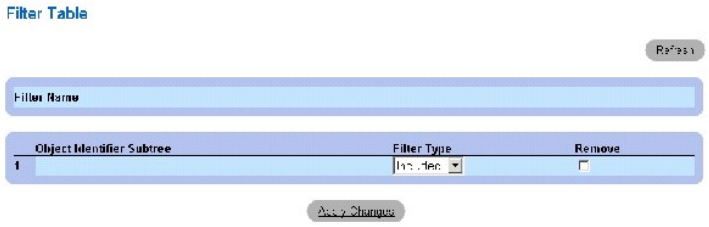
Der neue Filter wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der Filtertabelle

1. Öffnen Sie die Seite **Benachrichtigungsfilter**.
2. Klicken Sie auf **Show All**" (Alles anzeigen).

Die Seite **Filtertabelle** wird geöffnet:

Abbildung 6-66. Filtertabelle



Entfernen des Filters

1. Öffnen Sie die Seite **Benachrichtigungsfilter**.
2. Klicken Sie auf **Show All**" (Alles anzeigen).

   Die Seite **Filtertabelle** wird geöffnet.
3. Wählen Sie einen Eintrag aus der **Filtertabelle** aus.
4. Markieren Sie das Kontrollkästchen **Remove** (Entfernen).

   Der Filtereintrag wurde gelöscht und das Gerät aktualisiert.

Konfigurieren von Benachrichtigungsfiltern mithilfe von CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für das Definieren von Feldern zusammen, die auf der Seite **Benachrichtigungsfilter** angezeigt werden.

Tabelle 6-44. CLI-Befehle für SNMP-Benachrichtigungsfilter

CLI-Befehl	Beschreibung
`snmp-server filter filter-name oid-tree {included | excluded}`	Erstellt oder aktualisiert einen SNMP-Benachrichtigungsfilter.
`show snmp filters [filtername]`	Zeigt die Konfiguration eines SNMP-Benachrichtigungsfilters an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# snmp-server filter user1 1 included

Console (config)# end

Console # show snmp filters

Name          OID Tree      Typ
----------    ------------  --------
user1         iso           Included
```

Definieren von SNMP-Benachrichtigungsempfängern

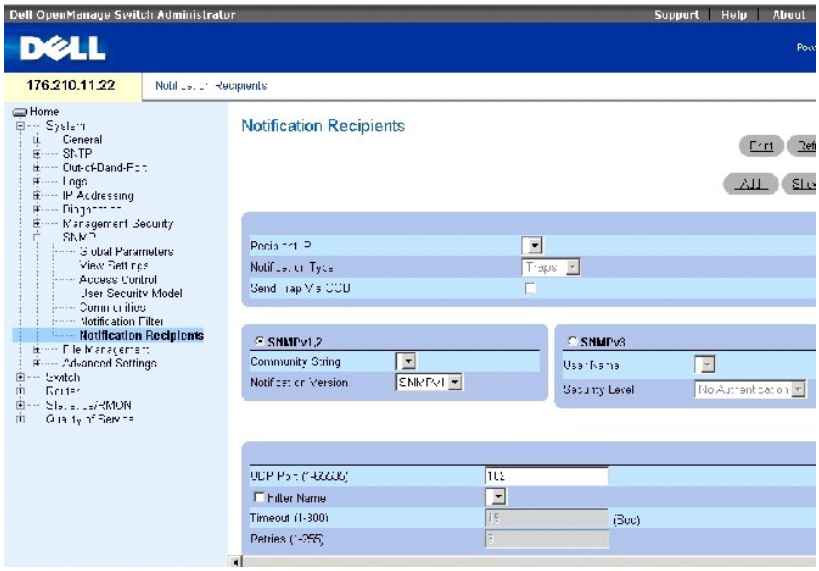
Die Seite **Benachrichtigungsempfänger** enthält Informationen über das Definieren von Filtern, die bestimmen, ob und welche Art von Traps an einen bestimmten Benutzer gesendet werden. SNMP-Benachrichtigungsfilter ermöglichen die folgenden Dienste:

- Identifizieren von Management-Trapzielen
- Filtern von Traps
- Auswählen von Trap-Erstellungsparametern

- Überprüfen von Zugangskontrollen

Um die Seite **Benachrichtigungsempfänger** zu öffnen, klicken Sie in der Strukturansicht auf **System→ SNMP→ Notification Recipient**.

Abbildung 6-67. Benachrichtigungsempfänger



Die Seite **Benachrichtigungsempfänger** enthält die folgenden Felder:

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

Notification Type (Benachrichtigungsart) Die Art der gesendeten Benachrichtigung. Die möglichen Feldwerte sind:

Trap Traps werden gesendet.

Inform Informs werden gesendet.

SNMPv1, 2 Die SNMP-Versionen 1 oder 2 werden für den ausgewählten Empfänger aktiviert. Die möglichen Feldwerte sind:

Community String (Communityzeichenfolge) Enthält eine Liste mit Communityzeichenfolgen. Wählen Sie eine Communityzeichenfolge aus, die mit der Benachrichtigung gesendet werden soll.

Notification Version (Benachrichtigungsversion) Bestimmt die Version der Benachrichtigung. Die möglichen Feldwerte sind:

SNMP V1 Traps der SNMP-Version 1 werden gesendet.

SNMP V2 Traps oder Informs der SNMP-Version 2 werden gesendet.

SNMPv3 SNMP-Version 3 ist für den ausgewählten Empfänger aktiviert. Die möglichen Feldwerte sind:

User Name (Benutzername) Enthält eine Liste mit Benutzern. Wählen Sie einen Benutzer aus, für den Benachrichtigungen erstellt werden sollen.

Security Level (Sicherheitsstufe) Die Sicherheitsstufe, die auf Benachrichtigungen angewendet wird. Die möglichen Feldwerte sind:

No Authentication (Keine Authentifizierung) Das Paket ist weder authentifiziert noch verschlüsselt.

Authentication (Authentifizierung) Das Paket ist authentifiziert.

Privacy (Datenschutz) Das Paket ist authentifiziert und verschlüsselt.

UDP Port (1-65535) (UDP-Port (1-65535)) Der zum Versenden von Benachrichtigungen verwendete UDP-Port. Die Standardeinstellung ist 162.

Filter Name (Filtername) Markieren Sie dieses Kontrollkästchen, um einen benutzerdefinierten SNMP-Filter auf Benachrichtigungen anzuwenden. Wählen Sie dazu einen SNMP-Filter aus der Liste aus.

Timeout (1-300) (Zeitüberschreitung (1-30) Zeit (in Sekunden), die das Gerät wartet, bevor Informs erneut gesendet werden. Der Standardwert beträgt 15 Sekunden.

Retries (1-255) (Wiederholung (1-255) Maximale Anzahl an neuen Versuchen, eine Inform-Anfrage durch das Gerät zu versenden. Die Standardeinstellung ist 3.

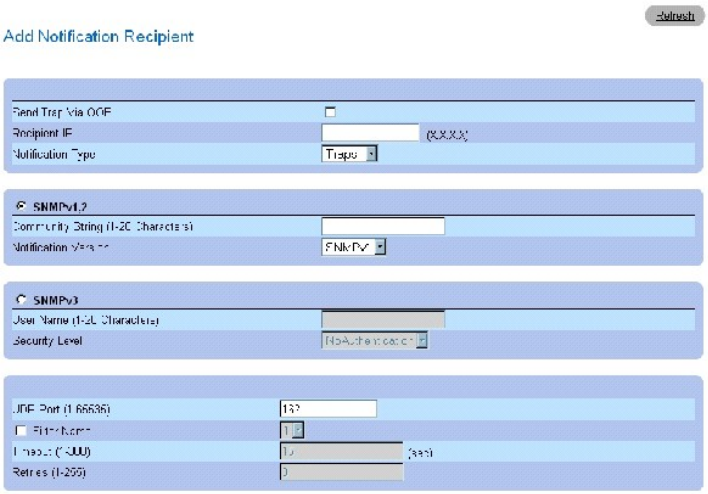
Remove Notification Recipient (Benachrichtigungsempfänger entfernen) Wenn diese Option markiert ist, wird der ausgewählte Benachrichtigungsempfänger entfernt.

Hinzufügen eines neuen Benachrichtigungsempfängers

1. Öffnen Sie die Seite **Benachrichtigungsempfänger**.
2. Klicken Sie auf **Add**" (Hinzufügen).

Die Seite **Benachrichtigungsempfänger hinzufügen** wird geöffnet:

Abbildung 6-68. Benachrichtigungsempfänger hinzufügen



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

Der Benachrichtigungsempfänger wird hinzugefügt, und das Gerät wird aktualisiert.

Anzeigen der Benachrichtigungsempfängertabelle

1. Öffnen Sie die Seite **Benachrichtigungsempfänger**.
2. Klicken Sie auf **Show All**" (Alles anzeigen).

Die Seite **Benachrichtigungsempfängertabelle** wird geöffnet:

Abbildung 6-69. Benachrichtigungsempfängertabelle

Löschen von Benachrichtigungsempfängern

1. Öffnen Sie die Seite **Benachrichtigungsempfänger**.
2. Klicken Sie auf **Show All**" (Alles anzeigen).

Die Seite Benachrichtigungsempfängertabelle" wird geöffnet.

3. Wählen Sie einen oder mehrere Benachrichtigungsempfänger aus den folgenden Tabellen aus: **SNMPv1, 2 Notification Recipient** (SNMPv1, 2-Benachrichtigungsempfängertabelle) und/oder **SNMPv3 Notification Recipient Tables** (SNMPv3-Benachrichtigungsempfängertabelle).
4. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

Die Empfänger werden gelöscht, und das Gerät wird aktualisiert.

Definieren von SNMP-Benachrichtigungsempfängern mithilfe von CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für das Definieren von Feldern zusammen, die auf der Seite **Benachrichtigungsempfänger** angezeigt werden.

Tabelle 6-45. CLI-Befehle für SNMP-Benachrichtigungsempfänger

CLI-Befehl	Beschreibung
snmp-server host {ip- address | hostname} community-string [traps | informs] [1 | 2] [udp-port port] [filter filtername] [timeout seconds] [retries retries]	Erstellt oder aktualisiert einen Benachrichtigungsempfänger, der Benachrichtigungen der Versionen SNMP 1 oder 2 empfängt.
snmp-server v3-host {ip-address | hostname} username [traps | informs] {noauth | auth | priv} [udp-port port] [filter filtername] [timeout seconds] [retries retries]	Erstellt oder aktualisiert einen Benachrichtigungsempfänger, der Benachrichtigungen der Version SNMP 3 empfängt.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# snmp-server host 12.1.1.1 Dell-community

Console (config)# end

Console# show snmp

Community-String    Community-Access    View name    IP address:    Typ
------------------  ------------------  -----------  -------------  ----

Community-String    Group name          IP address:                 Typ
------------------  ------------------  -----------                 ----

Bandexterne Management-Stations

Community-String    Community-Access    View name    IP address:    Typ
------------------  ------------------  -----------  -------------  ----

Community-String    Group Name          IP address:                 Typ
```

----------		---------		---------		----	
Traps are enabled.							
Authentication-failure trap is enabled.							

Version 1, 2 notifications							
Target Address	Typ	Community	Version	Udp Port	Filter name	To Sec	Retries
--------	----	---------	-------	----	------	---	-------
12.1.1.1	Trap	Dell_community	2	162		1500	3
OOB Notification Receivers (OOB-Benachrichtigungs-Receivers							
Target Address	Typ	Community	Version	Udp Port	Filter name	To Sec	Retries
--------	----	---------	----	----	------	---	-------
Version 3 notifications							
Target Address	Typ	Benutzername	Sicherheitsstufe	Udp Port	Filter name	To Sec	Retries
--------	----	--------	-------	----	------	---	-------
OOB Notification Receivers (OOB-Benachrichtigungs-Receivers)							
Target Address	Typ	Benutzername	Sicherheitsstufe	Udp Port	Filter name	To Sec	Retries
--------	----	--------	-------	----	------	---	-------

Verwalten von Dateien

Auf der Seite **Dateiverwaltung** können Sie die Gerätesoftware, die Abbilddatei und die Konfigurationsdateien verwalten. Dateien können über einen TFTP-Server herunter- oder hochgeladen werden.

Übersicht über die Dateiverwaltung

Die Managementdateistruktur besteht aus den folgenden Dateien:

- **Startup configuration file** (Startup-Konfigurationsdatei) Bewahrt die genaue Gerätekonfiguration, wenn das Gerät heruntergefahren oder neu gestartet wird. Die Startdatei bewahrt Konfigurationsbefehle, und Konfigurationsbefehle von der aktiven Konfigurationsdatei können in der Startdatei gespeichert werden.
- **Running configuration file** (Aktive Konfigurationsdatei) Enthält sämtliche Startup-Dateibefehle und auch die Befehle, die während der aktuellen Sitzung eingegeben wurden. Nachdem das Gerät heruntergefahren oder erneut gestartet wurde, sind alle in der aktiven Konfigurationsdatei gespeicherten Befehle verloren. Während des Startvorgangs werden alle Befehle in der Startdatei in die aktive Konfigurationsdatei kopiert und auf das Gerät angewandt. Während der Sitzung werden alle neu eingegebenen Befehle zu den Befehlen in der aktiven Konfigurationsdatei hinzugefügt. Befehle werden nicht überschrieben. Um die Startdatei zu aktualisieren, bevor das Gerät heruntergefahren wird, muss die aktive Konfigurationsdatei in die Startkonfigurationsdatei kopiert werden. Wenn das Gerät das nächste Mal gestartet wird, werden die Befehle wieder von der Startkonfigurationsdatei in die aktive Konfigurationsdatei kopiert.
- **Backup Configuration File** (Backup-Konfigurationsdatei) Enthält eine Sicherungskopie der Gerätekonfiguration. Die Sicherungsdatei ändert sich, wenn die aktive Konfigurationsdatei oder die Startdatei in die Sicherungsdatei kopiert wird. Die in die Datei kopierten Befehle ersetzen die vorhandenen Befehle, die in der Sicherungsdatei gespeichert wurden. Die Inhalte der Sicherungsdatei können entweder in die aktive Konfigurations- oder Startkonfigurationsdatei kopiert werden.
- **Image Files** (Abbilddateien) Systemabbildungen werden in zwei Flash-Sektoren gespeichert, die als Images (Image 1 und Image 2) bezeichnet werden. Das aktive Image speichert die aktive Kopie, und das andere Image speichert eine zweite Kopie. Das Gerät startet und arbeitet von dem aktiven Abbild. Wenn das aktive Abbild korrupt ist, startet das System automatisch von dem nicht-aktiven Abbild. Dies ist eine Sicherheitsfunktion für Fehler, die beim Startaktualisierungsverfahren auftreten.

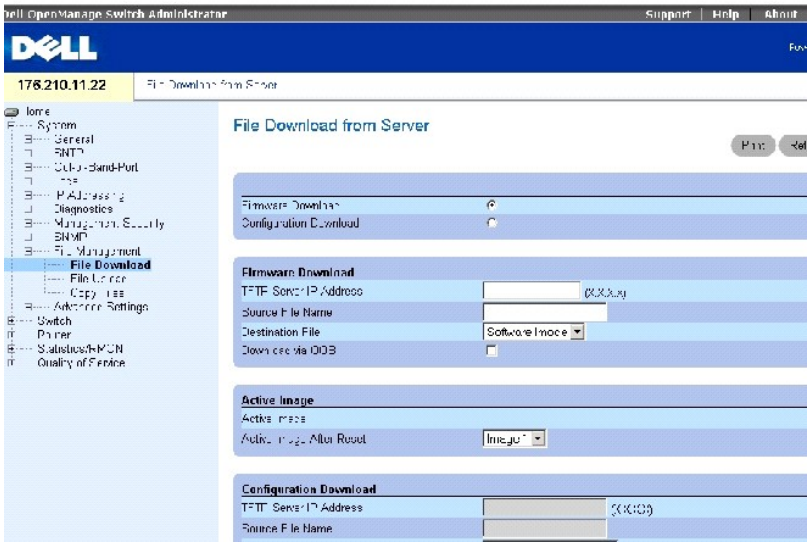
Öffnen Sie die Seite **File Management**", indem Sie auf **System**→ **File Management** in der *Strukturansicht* klicken.

Herunterladen von Dateien

Die Seite **Herunterladen der Datei vom Server** enthält Felder zum Herunterladen der Software vom TFTP-Server zu dem Gerät. Die Abbilddatei kann auch von der Seite **File Download from Server** (Herunterladen von Dateien vom Server) heruntergeladen werden.

Öffnen Sie die Seite **File Download From Server** (Herunterladen von Dateien vom Server), indem Sie auf **System**→ **File Management**→ **File Download** in der *Strukturansicht* klicken.

Abbildung 6-70. Herunterladen von Dateien vom Server



Die Seite **Herunterladen der Datei vom Server** enthält die folgenden Felder:

Firmware Download (Herunterladen von Firmware) Wenn diese Option gewählt ist, wird angezeigt, dass die Firmware-Datei heruntergeladen wird. Wenn diese Option gewählt ist, sind die Felder **Configuration Download** (Herunterladen der Konfiguration) grau unterlegt.

Configuration Download (Herunterladen der Konfiguration) Wenn diese Option ausgewählt ist, wird angezeigt, dass die Konfigurationsdatei heruntergeladen wird. Wenn **Configuration Download** (Herunterladen der Konfiguration) gewählt ist, sind die Felder **Firmware Download** (Herunterladen der Firmware) grau unterlegt.

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

Firmware Source File Name (Name der Firmwarequelldatei) Firmware-Datei, die heruntergeladen werden soll.

Firmware Destination File (Firmwarezieldatei) Bestimmt, ob die Datei in eine Abbilddatei oder eine Startdatei heruntergeladen wird.

Firmware Download via OOB (Herunterladen der Firmware über OOB) Lädt die Firmware-Datei über den Out of Band-Management-Port herunter.

Active Image (Aktives Abbild) Abbilddatei, die derzeit aktiv ist.

Active Image After Reset (Aktives Abbild nach Rückstellung) Die Abbilddatei, die nach Zurücksetzen des Geräts aktiv ist. Mögliche Werte sind wie folgt:

Image 1 (Abbild 1) Die Datei Abbild 1 ist aktiv, nachdem das Gerät zurückgesetzt wurde.

Image 2 (Abbild 2) Die Datei Abbild 2 ist aktiv, nachdem das Gerät zurückgesetzt wurde.

Configuration File TFTP Server IP Address (TFTP-Server-IP-Adresse der Konfigurationsdatei) Die IP-Adresse des TFTP-Servers, über den die Konfigurationsdateien heruntergeladen werden.

Configuration File Source File Name (Quelldateiname der Konfigurationsdatei) Die Konfigurationsdatei, die heruntergeladen werden soll.

Configuration File Destination (Ziel der Konfigurationsdatei) Die Zieldatei, zu der die Konfigurationsdateien heruntergeladen werden sollen. Die möglichen Werte sind:

Running Configuration (Aktive Konfiguration) Lädt die aktiven Konfigurationsdateien herunter.

Startup Configuration (Startkonfiguration) Lädt die Startkonfigurationsdateien herunter.

Backup Configuration (Konfigurationssicherung) Lädt die Konfigurationssicherungsdateien herunter.

Configuration Download via OOB (Herunterladen der Konfiguration über OOB) Lädt die Konfigurationsdatei über den Out of Band-Management-Port herunter.

Herunterladen von Dateien

1. Öffnen Sie die Seite **File Download From Server** (Herunterladen von Datei vom Server).
2. Verifizieren Sie die IP-Adresse des TFTP-Servers und stellen Sie sicher, dass die Softwareabbild- oder Startdatei, die heruntergeladen werden soll, auf dem TFTP-Server zur Verfügung steht.
3. Füllen Sie die Felder **TFTP Server IP Address** (IP-Adresse des TFTP-Servers), **Source File Name** (Name der Quelldatei) (vollständiger Pfad ohne IP-

Adresse des TFTP-Servers) und **Destination File** (Zieldatei) (Softwareabbild oder Boot) aus.

ANMERKUNG: Das Abbild der Abbilddatei überschreibt das nicht-aktive Abbild. Es wird empfohlen zu bestimmen, dass das nicht-aktive Abbild nach der Rückstellung das aktive Abbild wird, und dann das Gerät nach dem Herunterladen zurückzusetzen.

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

Die Software wird auf das Gerät heruntergeladen.

Aktivieren von Abbilddateien

1. Öffnen Sie die Seite **File Download From Server** (Herunterladen von Datei vom Server).
2. Wählen Sie das zu aktivierende Abbild aus dem Drop-Down-Menü **Active Image After Reset** (Aktives Abbild nach Rückstellung).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Abbilddatei wird ausgewählt.

ANMERKUNG: Um die ausgewählte Image-Datei zu aktivieren, setzen Sie das Gerät zurück. Informationen zur Rückstellung des Geräts finden Sie unter Resetting the Device" (Zurücksetzen des Gerätes).

Herunterladen von Dateien mithilfe der CLI-Befehle

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für das Definieren von Feldern zusammen, die auf der Seite **Herunterladen der Datei vom Server** angezeigt wird.

Tabelle 6-46. CLI-Befehle für das Herunterladen

CLI-Befehl	Beschreibung
copy *source-url destination-url*	Kopiert eine beliebige Datei von einem Quellort an einen Zielort.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console # copy tftp://172.16.101.101/file1 image

Accessing file 'file1' on 172.16.101.101...

Loading file1 from 172.16.101.101:

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!

[OK]

Copy took 0:01:11 [hh:mm:ss]
```

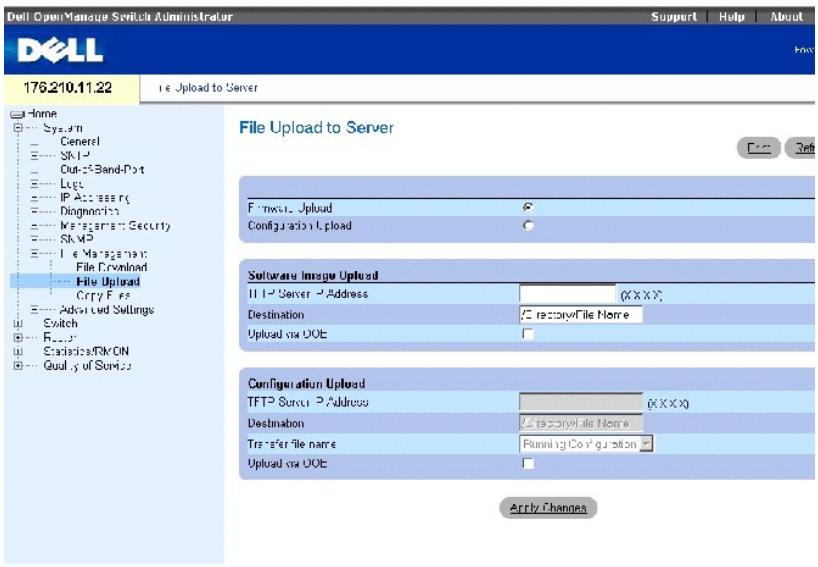
ANMERKUNG: Jedes „!" gibt an, dass das Herunterladen der Datei erfolgreich vonstatten geht.

Hochladen von Dateien

Die Seite **File Upload to Server** (Hochladen von Dateien auf den Server) enthält Felder für das Hochladen von Dateien vom TFTP-Server zu dem Gerät. Die Image-Datei kann außerdem von der Seite **File Upload to Server** (Hochladen von Dateien auf den Server) hochgeladen werden.

Öffnen Sie die Seite **File Upload to Server** (Hochladen von Dateien auf den Server), indem Sie auf **System→ File Management→ File Upload** in der *Strukturansicht* klicken.

Abbildung 6-71. Hochladen von Dateien auf den Server



Die Seite **Hochladen der Datei auf den Server** enthält die folgenden Felder:

Firmware Upload (Hochladen von Firmware) Zeigt an, dass die Firmware-Datei hochgeladen wird. Wenn **Firmware Upload** (Hochladen der Firmware) gewählt ist, sind die Felder **Configuration Upload** (Hochladen der Konfiguration) grau unterlegt.

Configuration Upload (Hochladen der Konfiguration) Zeigt an, dass die Konfigurationsdatei hochgeladen wird. Wenn **Configuration Upload** (Hochladen der Konfiguration) gewählt ist, sind die Felder **Firmware Upload** (Hochladen der Firmware) grau unterlegt.

Software Image Upload TFTP Server IP Address (IP-Adresse des TFTP-Servers zum Hochladen des Softwareabbilds) IP-Adresse des TFTP-Servers, auf den das Softwareabbild hochgeladen wird.

Software Image Upload Destination (Bestimmungsort für Hochladung des Softwareabbilds) Dateipfad, auf den das Softwareabbild hochgeladen wird.

Software Image Upload via OOB (Hochladen des Softwareabbilds über OOB) Gibt an, dass das Softwareabbild über den Out of Band-Management-Port hochgeladen wird.

Configuration Upload TFTP Server IP Address (TFTP-Server-IP-Adresse für das Hochladen der Konfiguration) Die IP-Adresse des TFTP-Servers, zu der die Konfigurationsdatei hochgeladen wird.

Configuration Upload Destination (Ziel für das Hochladen der Konfiguration) Der Pfad der Konfigurationsdatei, von der die Datei hochgeladen wird.

Configuration Upload Transfer File Name (Transferdateiname für das Hochladen der Konfiguration) Die Softwaredatei, die hochgeladen wird. Mögliche Feldwerte sind:

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

Startup Configuration (Startkonfiguration) Lädt die Startkonfigurationsdateien hoch.

Backup Configuration (Konfigurationssicherung) Lädt die Konfigurationssicherungsdateien hoch.

Configuration Upload via OOB (Hochladen der Konfiguration über OOB) Gibt an, dass die Konfigurationsdatei über den Out of Band-Management-Port hochgeladen wird.

Hochladen von Dateien

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

Die Software wird auf den Server hochgeladen.

Hochladen von Dateien mithilfe der CLI-Befehle

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für das Definieren von Feldern zusammen, die auf der Seite **Hochladen der Datei auf den Server** angezeigt wird.

Tabelle 6-47. CLI-Befehle für das Hochladen

CLI-Befehl	Beschreibung
`copy source-url destination-url`	Kopiert eine beliebige Datei von einem Quellort an einen Zielort.

Im Folgenden werden CLI-Befehle anhand eines Beispiels dargestellt:

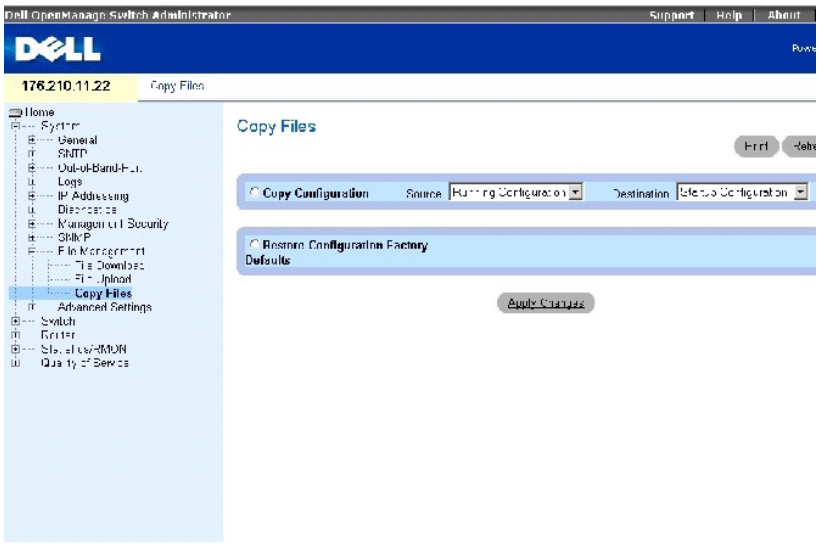
```
-----------------------------------------------------

Console#copy image tftp:16.1.1.200/file1
```

Kopieren von Dateien

Verwenden Sie die Seite **Dateien kopieren**, um Konfigurationsstandardeinstellungen zu kopieren und wiederherzustellen.

Um die Seite **Dateien kopieren** zu öffnen, klicken Sie in der Strukturansicht auf **System**→ **File Management**→ **Copy**.

Abbildung 6-72. Kopieren von Dateien



Die Seite **Dateien kopieren** enthält die folgenden Felder:

Copy Configuration (Konfiguration kopieren) Legt fest, dass eine Konfigurationsdatei kopiert werden soll.

Source (Quelle) Die Quelldatei der Konfiguration (aktiv, Start, Sicherung), von der die Datei kopiert wird.

Destination (Zielort) Die Zieldatei der Konfiguration (aktiv, Start, Sicherung), in die die Datei kopiert werden soll.

Restore Configuration Factory Defaults (Werkseitige Konfigurationsstandardeinstellungen wiederherstellen) Wenn diese Option markiert ist, wird festgelegt, dass die Standarddateien der werkseitigen Konfiguration zurückgesetzt werden sollen. Wenn sie nicht markiert ist, werden die derzeitigen Konfigurationseinstellungen beibehalten.

ANMERKUNG: Das Kopieren von Dateien in eine aktive Konfigurationsdatei fügt lediglich Konfigurationsdaten hinzu; die Konfigurationsdatei wird dabei nicht ersetzt.

Kopieren von Dateien

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

Die Datei wird kopiert.

Kopieren von Dateien mithilfe von CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für das Definieren der Felder zusammengefasst, die auf der Seite **Dateien kopieren** angezeigt werden.

Tabelle 6-48. CLI-Befehle für das Kopieren von Dateien

CLI-Befehl	Beschreibung
copy *source-url destination-url*	Kopiert eine beliebige Datei von einem Quellort an einen Zielort.

`delete startup-config`	Löscht die Startkonfigurationsdatei.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console# delete startup-config
```

Definieren erweiterter Einstellungen

Verwenden Sie erweiterte Einstellungen, um verschiedene globale Attribute des Geräts einzustellen. Die Änderungen an diesen Attributen werden erst übernommen, nachdem das Gerät zurückgesetzt wurde. Öffnen Sie die Seite **Erweiterte Einstellungen**, indem Sie auf **System**→ **Advanced Settings** in der *Strukturansicht* klicken.

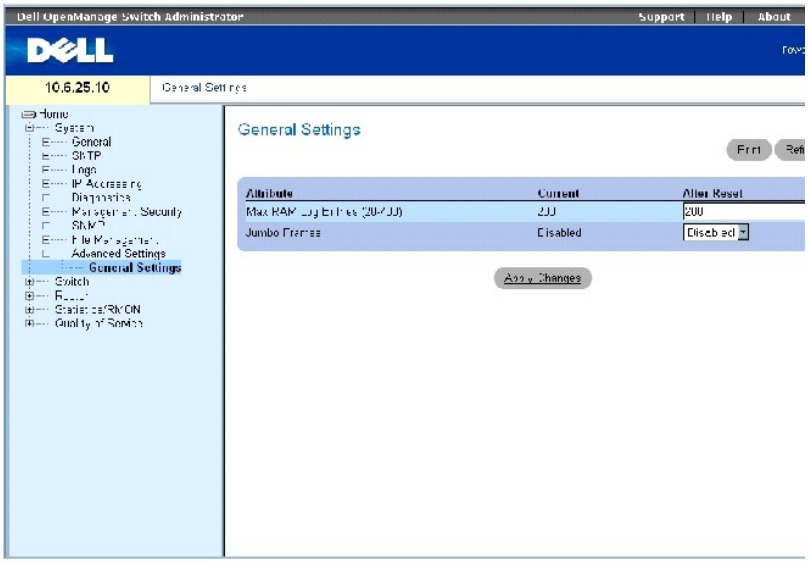
Die Seite **Advanced Settings** (Erweiterte Einstellungen) enthält einen Link zur Konfiguration allgemeiner Einstellungen.

Konfigurieren von allgemeinen Einstellungen

Verwenden Sie die Seite **General Settings** (Allgemeine Einstellungen), um die allgemeinen Geräteparameter zu definieren.

Öffnen Sie die Seite **General Settings** (Allgemeine Einstellungen), indem Sie auf **System**→ **Advanced Settings**→ **General** in der *Strukturansicht* klicken.

Abbildung 6-73. Allgemeine Einstellungen



Die Seite **Allgemeine Einstelllungen** enthält die folgenden Felder:

Current (Aktuell) Maximale Anzahl an Einträgen.

After Reset (Nach dem Zurücksetzen) Maximale Anzahl an Einträgen, nachdem das Gerät zurückgesetzt wurde. Durch Eingeben eines Werts in dieser Spalte

wird der Feldtabelle Speicherplatz zugewiesen.

Max RAM Log Entries (20-400) (Maximale RAM-Protokolleinträge) Maximale Anzahl an Einträgen in der RAM-Protokolltabelle. Der Standardwert ist 200 Einträge.

Jumbo Frames Ermöglicht die Übertragung von identischen Daten in weniger Frames. Damit fallen weniger Restkapazität, geringere Verarbeitungszeit und weniger Interrupts an. Interne Frames werden möglicherweise durch das Aktivieren der Jumbo-Frames-Funktion beeinträchtigt.

Aktivieren von Jumbopaketen

1. Öffnen Sie die Seite **Allgemeine Einstelllungen**.
2. Wählen Sie **Enabled** (Aktiviert) in dem Feld **Jumbo packets** (Jumbopakete).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Jumbopakete werden auf dem Gerät aktiviert.

Ansicht allgemeiner Einstellungen mithilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für das Definieren der Felder zusammengefasst, die auf der Seite Allgemeine Einstelllungen angezeigt werden.

Tabelle 6-49. CLI-Befehle für allgemeine Einstellungen

CLI-Befehl	Beschreibung
`logging buffered size number`	Legt die Anzahl der im internen Pufferspeicher (RAM) gespeicherten Syslog-Meldungen fest.
`port jumbo-frame`	Aktiviert Jumbopakete für das Gerät.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# logging buffered size 300
```

```
Console (config)#port jumbo-frame
```

Zurück zum Inhaltsverzeichnis

Konfigurieren von Switch-Informationen

Dell PowerConnect 6024/6024F Systeme

Dieser Abschnitt enthält alle Systemvorgänge und allgemeinen Informationen für das Konfigurieren von Netzwerksicherheit, Ports, Adressentabellen, GARP, VLANs, Spanning Tree, Port Aggregation und Multicast-Unterstützung.

Konfigurieren der Netzwerksicherheit

Auf der Seite **Network Security** (Netzwerksicherheit) stellen Sie die Netzwerksicherheit sowohl über Access Control -Listen als auch über gesperrte Ports ein. Um die Seite **Netzwerksicherheit** zu öffnen, klicken Sie auf **Switch→ Network Security**.

Die Seite **Netzwerksicherheit** enthält Links, über die Sie Port-bezogene Authentifizierung, Portsicherheit, IP-basierte ACLs, MAC-basierte ACLs und ACL-Bindungen konfigurieren können.

Portbasierte Authentifizierung (802.1x)

Portbasierte Authentifizierung ermöglicht die Authentifizierung von Systembenutzern auf Portbasis über einen externen Server. Nur authentifizierte und genehmigte Systembenutzer können Daten übertragen und empfangen. Ports werden über den RADIUS (Remote Authentication Dial In User Service)-Server unter Einsatz des Extensible Authentication-Protokolls (EAP) authentifiziert.

Das 802.1x-Netzwerk verfügt über drei Komponenten:

- **Authenticators** Gibt den Port an, der authentifiziert wird, bevor ein Systemzugriff gewährt wird.
- **Supplicants** Gibt den Host an, der mit dem authentifizierten Port verbunden ist, der Zugriff auf Systemdienste anfordert.
- **Authentication Server** (Authentifizierungs-Server) Gibt den externen Server an, z. B. den RADIUS-Server, der die Authentifizierung für den Authenticator durchführt, und gibt an, ob der Benutzer zum Zugriff auf Systemdienste autorisiert ist.

Die portbasierte Authentifizierung erzeugt zwei Zugriffszustände:

- **Controlled Access** Ermöglicht die Kommunikation zwischen dem Benutzer und dem System, wenn der Benutzer autorisiert ist.
- **Uncontrolled Access** Ermöglicht freie Kommunikation, unabhängig vom Portzustand.

Das Gerät unterstützt zurzeit die portbasierte Authentifizierung über den RADIUS-Server.

Erweiterte portbasierte Authentifizierung

Die erweiterte portbasierte Authentifizierung ermöglicht die Verbindung mehrerer Hosts an einem Port. Die erweiterte portbasierte Authentifizierung erfordert lediglich, dass ein Host autorisiert ist, damit alle Hosts Systemzugriff haben. Wenn der Port nicht autorisiert ist, wird allen angeschlossenen Hosts der Zugriff auf das Netzwerk verweigert.

Die erweiterte portbasierte Authentifizierung aktiviert außerdem die Authentifizierung auf VLAN-Basis. Spezifische VLANs im Switch sind immer verfügbar, selbst wenn spezifische, mit dem VLAN verbundene Ports nicht freigegeben sind. Zum Beispiel ist für Voice über IP keine Authentifizierung erforderlich, während diese jedoch für Datenverkehr erforderlich ist. VLANs, für die keine Authentifizierung erforderlich ist, können definiert werden. Den Benutzern stehen nicht authentifizierte VLANs zur Verfügung, selbst wenn die am VLAN angeschlossenen Ports als autorisiert definiert sind.

Die erweiterte portbasierte Authentifizierung wird in den folgenden Modi implementiert:

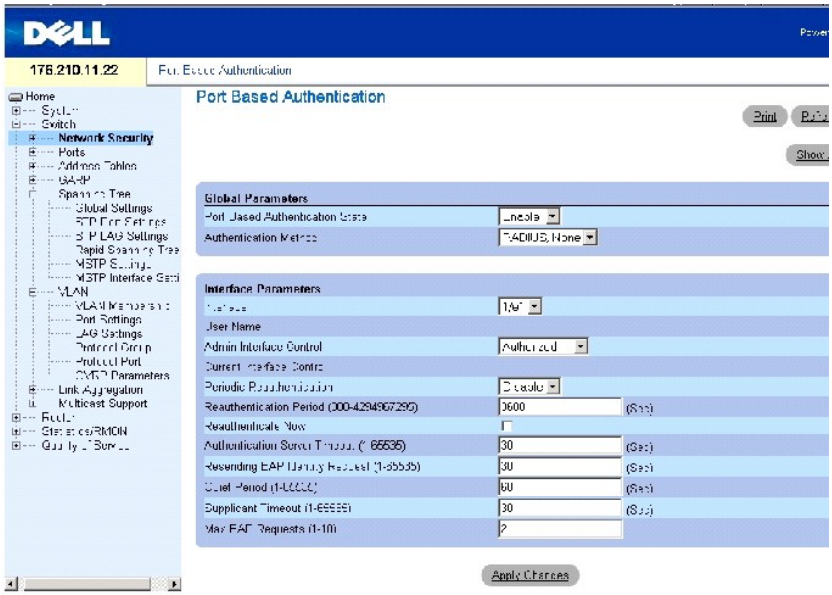
- **Single Host Mode** Ermöglicht nur dem autorisierten Host Zugriff auf den Port.
- **Multiple Host Mode** Ermöglicht die Verbindung mehrerer Hosts an einem Port. Nur ein Host muss autorisiert sein, um allen Hosts Netzwerkzugriff zu geben. Wenn die Host-Authentifizierung fehlschlägt oder eine EAPOL-Logoff-Meldung erhalten wird, wird allen angeschlossenen Clients der Netzwerkzugriff verwehrt.

Konfigurieren der portbasierten Authentifizierung

Die Seite **Portbasierte Authentifizierung** enthält Felder zur Konfiguration der portbasierten Authentifizierung.

Öffnen Sie die Seite **Portbasierte Authentifizierung**, indem Sie auf **Switch→ Network Security→ Port Based Authentication** klicken.

Abbildung 7-1. Portbasierte Authentifizierung



Die Seite **Portbasierte Authentifizierung** enthält die folgenden Felder:

Port Based Authentication State Ermöglicht die portbasierte Authentifizierung für das Gerät. Die möglichen Feldwerte sind:

Enable Aktiviert die portbasierte Authentifizierung für das Gerät.

Disable Deaktiviert die portbasierte Authentifizierung für das Gerät.

Authentication Method Gibt die verwendete Authentifizierungsmethode an. Die möglichen Feldwerte sind:

RADIUS, None Zeigt an, dass die Portauthentifizierung zunächst über den RADIUS-Server vorgenommen wird. Wenn der RADIUS-Server nicht erreicht

werden kann, wird keine Authentifizierungsmethode verwendet. Wenn jedoch ein Fehler auftritt, verbleibt der Port als nicht freigegeben und Zugang wird nicht erlaubt.

RADIUS Zeigt an, dass die Authentifizierung am RADIUS-Server stattfindet.

None Zeigt an, dass keine Authentifzierungsmethode verwendet wird.

Interface (Schnittstelle) Enthält eine Liste von zu authentifizierenden Schnittstellen.

User Name Gibt den Benutzernamen, wie er im RADIUS-Server konfiguriert ist, an.

Admin Interface Control Definiert den Port-Authorisierungsstatus. Die möglichen Feldwerte sind:

Auto Aktiviert die portbasierte Authentifizierung pro Port. Die Schnittstelle wechselt zwischen einem freigegebenen und einem nicht freigegebenen Status, entsprechend dem Authentifizierungsaustausch zwischen Gerät und Client.

Authorized (Freigegeben) Setzt die Schnittstelle in einen freigegebenen Status ohne Authentifizierung. Die Schnittstelle sendet und erhält normalen Datenverkehr ohne Authentifizierung auf Client-Port-Basis.

Unauthorized (Nicht freigegeben) Verweigert der ausgewählten Schnittstelle den Zugang zum System, indem die Schnittstelle auf den nicht freigegebenen Status gesetzt wird. Das Gerät kann dem Client keine Authentifizierungsdienste über die Schnittstelle bieten.

Current Interface Control Der aktuelle Port-Authorisierungsstatus. Wenn der Port nicht aktiv ist, wird ein Sternchen angezeigt.

Periodic Reauthentication Führt, wenn aktiviert, periodisch eine erneute Authentifizierung des Ports durch.

Reauthentication Period (300-4294967295) (Reauthentifizierungsperiode) Zeigt die Zeitspanne an, nach der der ausgewählte Port erneut authentifiziert wird. Der Feldwert wird in Sekunden angegeben. Der Standardwert des Feldes ist 3600 Sekunden.

Reauthenticate Now (Jetzt reauthentifizieren) Erzwingt, wenn ausgewählt, die sofortige Reauthentifizierung des Ports.

Authentication Server Timeout (1-65535) Legt die Zeit fest, die vergeht, bevor das Gerät eine Anforderung an den Authentifizierungsserver erneut sendet. Der Feldwert wird in Sekunden angegeben. Der Standardwert des Feldes ist 30 Sekunden.

Resending EAP Identity Request (1-65535) (EAP-Identitätsanforderung erneut senden) Legt die Zeit fest, die vergeht, bevor EAP-Anforderungen erneut gesendet werden. Der Feldwert wird in Sekunden angegeben. Der Standardwert des Feldes ist 30 Sekunden.

Quiet Period (1-65535) (Untätigkeit) Legt die Zeit fest, die das Gerät in Untätigkeitszustand verbleibt, nachdem eine Authentifizierungskommunikation fehlgeschlagen ist. Der mögliche Feldwert ist 0-65535. Der Feldwert wird in Sekunden angegeben. Der Standardwert des Feldes ist 60 Sekunden.

Supplicant Timeout (1-65535) (Zeitüberschreitung) Legt die Zeit fest, die vergeht, bis EAP-Anfragen an den Benutzer zurückgeschickt werden. Der Feldwert wird in Sekunden angegeben. Der Standardwert des Feldes ist 30 Sekunden.

Max EAP Requests (1-10) (Maximale Anzahl an EAP-Anfragen) Die maximale Anzahl, die das Geräte Anfragen an EAP senden kann, bevor der Authentifizierungsprozess neu gestartet wird, wenn keine Antwort erhalten wird. Der Bereich der möglichen Feldwerte ist 1-10. Der Standardfeldwert für Wiederholungen ist 2.

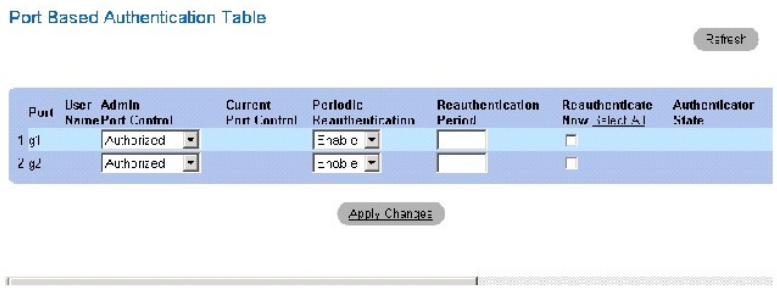
Anzeigen der portbasierten Authentifizierungstabelle

1. Öffnen Sie die Seite **Portbasierte Authentifizierung**.

2. Klicken Sie auf **Show All**" (Alles anzeigen).

Die Seite **Portbasierte Authentifizierungstabelle** wird geöffnet:

Abbildung 7-2. Portbasierte Authentifizierungstabelle



Die Tabelle **Portbasierte Authentifizierungstabelle** enthält die folgenden Felder:

Copy Parameters From Port No. (Parameter von Portnummer kopieren) Der Port, von dem die Parameter kopiert werden sollen.

Termination Cause Zeigt den Grund für den Abbruch der Port-Authentifizierung an.

Copy To Kopiert Portparameter von einem Port zu den ausgewählten Ports.

Select All Dient zur Auswahl aller Ports in der **Port Based Authentication Table**.

Kopieren von Parametern in die Portbasierte Authentifizierungstabelle

1. Öffnen Sie die Seite **Portbasierte Authentifizierung**.
2. Klicken Sie auf **Show All**" (Alles anzeigen).

Die **Port Based Authentication Table** wird geöffnet.

3. Wählen Sie die Schnittstelle im Feld **Copy Parameters from** (Kopieren der Parameter von).
4. Aktivieren Sie das Kontrollkästchen **Copy to** (Kopieren von), um die Schnittstellen zu definieren, auf die die portbasierten Authentifizierungparameter kopiert werden.
5. Klicken Sie auf **Apply Changes**" (Änderungen übernehmen).

Die Parameter werden auf den ausgewählten Port in der **Port Based Authentication Table** kopiert und das Gerät wird aktualisiert.

Aktivieren der portbasierten Authentifizierung mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zum Aktivieren der portbasierten Authentifizierung zusammen, wie Sie auf der Seite **Portbasierte Authentifizierung** angezeigt werden.

Tabelle 7-1. CLI-Befehle zur Port-Authentifizierung

CLI-Befehl	Beschreibung
	Gibt eine oder mehrere AAA (Authentifizierung, Autorisierung und Abrechnung)-Methoden zur Verwendung

aaa authentication dot1x default *method1* [*method2*.]	auf Schnittstellen, die IEEE 802.1X entsprechen, an.
dot1x system-auth- control	Führt eine globale Aktivierung von 802.1X aus.
dot1x port-control {auto | force-authorized | force- unauthorized}	Steuert den Portauthorisierungsstatus manuell.
dot1x max-req *count*	Stellt die maximale Anzahl der EAP-Sendeversuche des Geräts an den Client ein, bevor der Authentifizierungsprozess neu gestartet wird.
dot1x re-authenticate [**ethernet** *interface*]	Iniitiert eine manuelle Reauthentifizierung aller 802.1X-aktivierten Ports oder des angegebenen 802.1X-aktivierten Ports.
dot1x re-authentication	Aktiviert die periodische Reauthentifizierung eines Clients.
dot1x timeout quiet-period seconds	Stellt die Anzahl der Sekunden ein, die das Gerät im Untätigkeitszustand verbleibt, nachdem ein Authentifizierungsaustausch fehlgeschlagen ist.
dot1x timeout re-authperiod *seconds*	Stellt die Anzahl der Sekunden zwischen Reauthentifizierungsversuchen ein.
dot1x timeout server-timeout *seconds*	Stellt die Zeit für die erneute Übertragung von Paketen an den Authentifizierungsserver ein.
dot1x timeout supp-timeout *seconds*	Stellt die Zeit für die erneute Übertragung eines EAP-Anforderungs-Frame an den Client ein.
dot1x timeout tx-period *seconds*	Stellt die Anzahl der Sekunden ein, die das Gerät auf eine Antwort auf einen EAP-Anforderungs-/Identitäts-Frame vom Client wartet, bevor die Anforderung erneut gesendet wird.
show dot1x [**ethernet** *interface*]	Zeigt den 802.1X-Status für das Gerät oder für die angegebene Schnittstelle ein.
show dot1x users [username username]	Zeigt 802.1X-Benutzer für das Gerät an.
show dot1x statistics ethernet interface	Zeigt die 802.1X-Statistiken für die angegebene Schnittstelle an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

Console# **show dot1x**

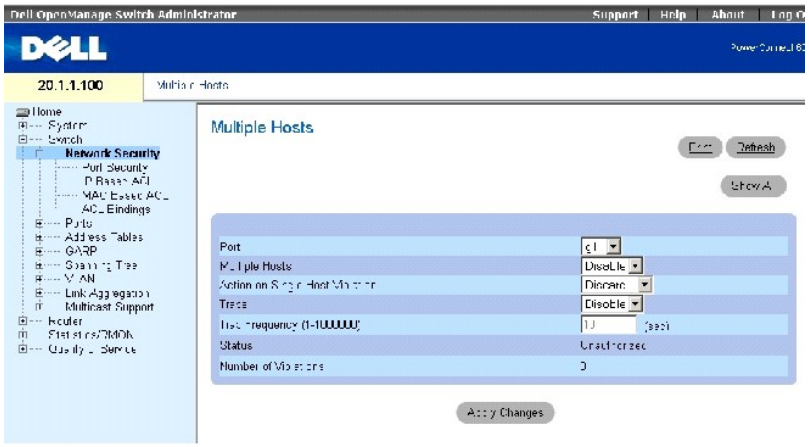
Port	Admin Mode	Oper Mode	Reauth Control	Reauth Period	Benutzername
----	----------	----------	-------	------	--------
g11	Auto	Authorized	Ena	3600	Bob
g12	Auto	Authorized	Ena	3600	John
g13	Auto	Unauthorized	Ena	3600	Clark
g14	Force-auth	Authorized	Dis	3600	Nicht verfügbar

Konfigurieren der erweiterten portbasierten Authentifizierung

Die Seite **Multiple Hosts** (Mehrere Hosts) enthält Informationen zur Definition der Einstellungen für die erweiterte portbasierte Authentifizierung für bestimmte Ports.

Um die Seite **Mehrere Hosts** zu öffnen, klicken Sie auf **Switch→ Network Security→ Multiple Hosts**.

Abbildung 7-3. Mehrere Hosts



Die Seite **Mehrere Hosts** enthält die folgenden Felder:

Port Gibt die Portnummer, für die die erweiterte portbasierte Authentifizierung aktiviert wird, an.

Multiple Hosts Aktiviert/deaktiviert einen Host zur Authorisierung des Systemzugriffs mehrerer Hosts. Diese Einstellung muss aktiviert werden, um entweder den Eingangsfilter zu aktivieren oder die Port-Lock-Sicherheitsfunktion am ausgewählten Port zu verwenden.

Action on Single Host Violation Definiert die Aktion, die auf im Single-Host-Modus eingehende Pakete angewendet wird, die von einem Host kommen, dessen MAC-Adresse nicht der Client (Supplicant)-MAC-Adresse entspricht. Die möglichen Feldwerte sind:

Forward Leitet die Pakete unbekannten Ursprungs weiter, ohne dass jedoch die MAC-Adresse erfasst wird.

Discard Lehnt die Pakete von einer nicht erfassten Quelle ab. Dies ist die Standardeinstellung.

Discard Shutdown Lehnt das Paket von einer nicht erfassten Quelle ab und schließt den Port. Ports bleiben geschlossen, bis sie aktiviert werden oder das Gerät zurückgesetzt wird.

Traps Aktiviert/deaktiviert das Senden von Traps an den Host bei Auftreten eines Verstoßes.

Trap Frequency (1-1000000) Legt das Intervall fest, in dem Traps an den Host gesandt werden. Der Standardwert des Feldes ist 10 Sekunden.

Status Gibt den Hoststatus an. Die möglichen Feldwerte sind:

Unauthorized Zeigt an, dass die Portsteuerung *Force Unauthorized* ist, die Portverbindung nicht aktiv ist oder die Portsteuerung auf Automatik steht, ein Client jedoch nicht über den Port authentifiziert wurde.

Not in auto mode Zeigt an, dass die Portsteuerung *Forced Authorized* ist und die Clients vollständigen Portzugang haben.

Single-host Lock Zeigt an, dass die Portsteuerung *Auto* ist und dass ein einziger Client über den Port authentifiziert wurde.

No Single Host Zeigt an, dass Multiple Host aktiviert ist.

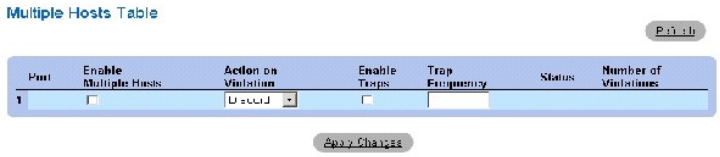
Number of Violations Gibt die Anzahl der im Single-Host-Modus an der Schnittstelle eingegangenen Pakete an, die von einem Host kommen, dessen MAC-Adresse nicht der Client (Supplicant)-MAC-Adresse entspricht.

Anzeigen der Multiple Hosts Table (Mehrere Hosts-Tabelle)

1. Öffnen Sie die Seite **Multiple Hosts**.
2. Klicken Sie auf **Show All"** (Alles anzeigen).

Die **Multiple Hosts Table** (Mehrere Hosts-Tabelle) wird geöffnet.

Abbildung 7-4. Mehrere Hosts-Tabelle



Aktivieren mehrerer Hosts mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Aktivierung der erweiterten portbasierten Authentifizierung, wie auf der Seite **Multiple Hosts** angezeigt, zusammen.

Tabelle 7-2. CLI-Befehle für mehrere Hosts

CLI-Befehl	Beschreibung
dot1x multiple-hosts	Ermöglicht mehrere Hosts (Clients) für einen 802.1X-autorisierten Port, bei dem der Schnittstellenkonfigurationsbefehl dot1x port-control auf auto gesetzt ist.
dot1x single-host- violation {forward |discard |discard- shutdown}[trap seconds]	Legt die Aktion fest, die erfolgt, wenn eine Station, deren MAC-Adresse nicht die Client (Supplicant)-MAC-Adresse ist, einen Zugriff auf die Schnittstelle versucht.

Das folgende Beispiel illustriert die CLI-Befehle:

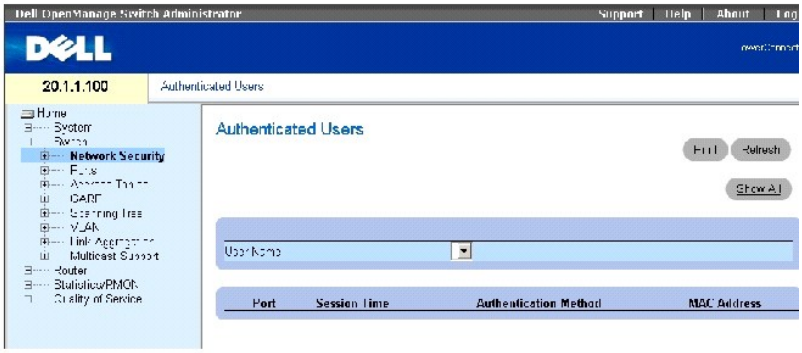
```
Console (config)# interface ethernet g11

Console (config-if)# dot1x multiple-hosts
```

Authentifizieren von Benutzern

Die Seite **Authenticated Users** (Authentifizierte Benutzer) zeigt Benutzer-Portzugriffslisten an.

Öffnen Sie die Seite **Authenticated Users**, indem Sie auf Switch→ Network Security→ Authenticated Users klicken.

Abbildung 7-5. Authentifizierte Benutzer



Die Seite **Authentifizierte Benutzer** enthält die folgenden Felder:

User Name Zeigt die Liste der Benutzer an, die über den RADIUS-Server autorisiert wurden.

Port Listet die für die Authentifizierung verwendeten Portnummern auf. Die Ports werden sortiert nach Benutzername aufgelistet.

Session Time Die Zeitdauer, die der Benutzer am Gerät angemeldet war. Das Feldformat lautet **Tage:Stunden:Minuten:Sekunden**, z. B. 3 Tage: 2 Stunden: 4 Minuten: 39 Sekunden.

Authentication Method Die Methode, mit der die letzte Sitzung authentifiziert wurde. Die möglichen Feldwerte sind:

Remote Der Benutzer wurde von einem Remote-Server authentifiziert.

None Der Benutzer wurde nicht authentifiziert.

MAC Address Die anfordernde MAC Adresse.

Anzeigen der Tabelle authentifizierter Benutzer

1. Öffnen Sie die Seite **Authenticated Users** (Authentifizierte Benutzer).
2. Klicken Sie auf **Show All"** (Alles anzeigen).

Die **Authenticated Users Table** (Tabelle authentifizierter Benutzer) wird geöffnet:

Abbildung 7-6. Tabelle authentifizierter Benutzer

Anzeigen der Benutzerauthentifizierung mithilfe der CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Authentifizierung von Nutzern zusammen, wie auf der Seite **Authenticated Users** (Authentifizierte Benutzer) angezeigt.

Tabelle 7-3. CLI-Befehle zum Hinzufügen von Benutzernamen

CLI-Befehl	Beschreibung
show dot1x users [username username]	Zeigt 802.1X-Benutzer für das Gerät an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console# show dot1x users

Port   Benutzername   Session Time   Auth Method   MAC-Adress
----   --------       ------------   -----------   -----------------
g12    bob            00:09:27       Fern          00:80:c8:b9:dc:1d
```

Konfigurieren der Portsicherheit

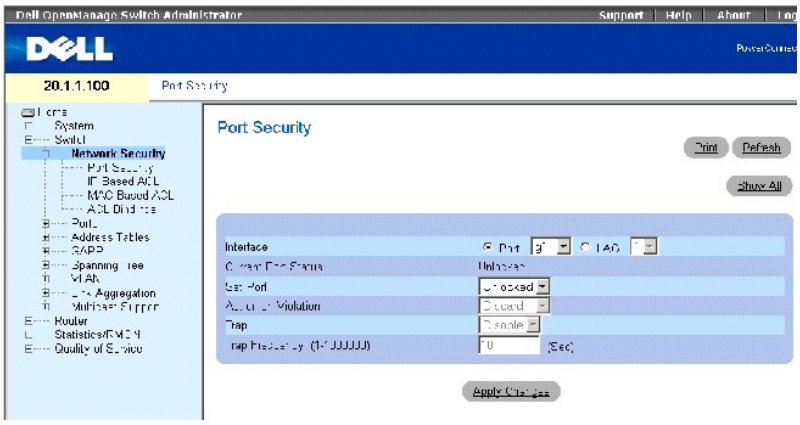
Die Netzwerksicherheit kann erhöht werden, indem der Zugriff auf bestimmte Ports auf Benutzer mit bestimmten MAC-Adressen beschränkt wird. Die MAC-Adressen können bis zu dem Punkt dynamisch gelernt werden oder sie können statisch konfiguriert werden. Bei Verwendung der Locked-Port-Sicherheitsfunktion werden sowohl eingegangene als auch erfasste Pakete, die an bestimmten Ports eingehen, überwacht. Der Zugriff auf die gesperrten Ports ist auf Benutzer mit bestimmten MAC-Adressen beschränkt. Diese Adressen werden entweder manuell für den Port definiert oder sie werden an dem Port bis zu dem Zeitpunkt, an dem der Port gesperrt wird, erfasst. Wenn ein Paket an einem gesperrten Port eingeht und die MAC-Quelladresse des Pakets nicht mit dem Port verknüpft ist (d. h. sie wurde entweder an einem anderen Port erfasst oder ist dem System nicht bekannt), wird der Schutzmechanismus ausgelöst, der verschiedene Optionen bietet. Nicht freigegebene Pakete, die an einem gesperrten Port ankommen, werden entweder weitergeleitet, ohne Trap abgelehnt, mit Trap abgelehnt, oder der Eingangsport wird deaktiviert.

Die Locked-Port-Sicherheitsfunktion ermöglicht auch das Speichern einer Liste von MAC-Adressen in der Konfigurationsdatei. Die MAC-Adressliste kann nach einem Zurücksetzen des Geräts wiederhergestellt werden.

Deaktivierte Ports können nur über die Seite **Portkonfiguration** aktiviert werden.

Um die Seite **Portsicherheit** zu öffnen, klicken Sie auf **Switch→ Network Security→ Port Security**.

Abbildung 7-7. Portsicherheit



Interface (Schnittstelle) Zeigt an, ob die gesperrte Portsicherheit auf einem Port oder einer LAG aktiviert ist.

Current Port Status (Aktueller Portzustand) Zeigt an, ob der Port derzeit gesperrt oder deaktiviert ist, oder ob er entsperrt ist.

Set Port (Port festlegen) Aktiviert die Portsperre. Ist ein Port gesperrt, werden alle aktuellen Adressen, die vom Switch dynamisch ermittelt wurden, in statische MAC-Adressen umgewandelt. Beim Entsperren des Ports werden diese aus der statischen Liste entfernt.

Action on Violation (Aktion bei Verletzung) Aktion, die auf Pakete angewendet wird, die am Port ankommen. Das Feld ist grau hinterlegt, falls der Port entsperrt ist. Die möglichen Werte sind:

Discard Lehnt die Pakete von einer nicht erfassten Quelle ab. Dies ist die Standardeinstellung.

Forward (Weiterleiten) Leitet die Pakete aus einer unbekannten Quelle weiter. Die MAC-Adresse wird nicht ermittelt.

Shutdown (Herunterfahren) Verwirft das Paket aus nicht ermittelten Quellen und sendet eine Trap. Darüber hinaus wird der eingehende Port deaktiviert.

Trap Aktiviert oder deaktiviert das Senden einer Trap, wenn ein Paket an einem gesperrten Port empfangen wird.

Trap Frequency (Trap-Frequenz) Zeit (in Sekunden) zwischen zwei Traps.

Definieren eines gesperrten Ports

1. Öffnen Sie die Seite **Port Security**.
2. Wählen Sie einen Schnittstellentyp und -nummer.
3. Wählen Sie im Drop-Down-Menü **Set Port** (Port einstellen) die Option **Locked** (Gesperrt) aus.
4. Füllen Sie die verbleibenden Felder aus.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der gesperrte Port wird der Portsicherheitstabelle hinzugefügt und das Gerät aktualisiert.

Kopieren von Parametern in die Tabelle mit gesperrten Ports.

1. Öffnen Sie die Seite **Port Security**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **Port Security Table** (Portsicherheitstabelle) anzuzeigen.

   Die Felder in der Portsicherheitstabelle entsprechen den Feldern auf der Seite **Port Security** (Portsicherheit).
3. Wählen Sie im Feld **Copy Parameters from** (Parameter kopieren aus) eine Schnittstelle entweder aus dem Drop-Down-Menü **Port** oder **LAG**.

   Die Portsicherheitsdefinitionen für diese Schnittstelle werden auf die ausgewählten Schnittstellen kopiert (siehe Schritt 5).
4. Aktivieren Sie das Kontrollkästchen **Copy to** (Kopieren nach), um die Schnittstellen auszuwählen, auf die die Portsicherheitsdefinitionen kopiert werden.

   Oder

   Klicken Sie auf **Select All** (Alle auswählen), um die Definitionen auf alle Ports oder LAGs zu kopieren.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Parameter werden an die ausgewählten Ports oder LAGs in der **Port Security Table** (Portsicherheitstabelle) kopiert und das Gerät aktualisiert.

Konfigurieren der Locked Port Security mit CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Konfiguration der gesperrten Portsicherheit, wie auf der Seite **Portsicherheit** angezeigt, zusammen.

Tabelle 7-4. CLI-Befehle für gesperrte Portsicherheit

CLI-Befehl	Beschreibung
`port security [forward | discard | discard-shutdown] [trap seconds]`	Deaktiviert das Erlernen neuer Adressen auf der Schnittstelle.
`show ports security [ethernet interface | port-channel port- channel-number]`	Zeigt den Sperrstatus des Ports an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface ethernet g1

Console (config-if)# port security forward trap 100

Console (config-if)# exit

Console (config)# exit

Console # show ports security
```

Port	status	Action	Trap	Frequency	Counter

----	------	------	----	---------	-------
g1	Locked	Forward	Enabled (Aktiviert)	100	0
g2	Unlocked	-	-	-	-
...					
g24	Unlocked	-	-	-	-
ch1	Unlocked	-	-	-	-
...					
ch7	Unlocked	-	-	-	-

Definieren von IP-basierten ACLs

Zugriffssteuerungslisten (ACL) ermöglichen Netzwerkverwaltern die Definition von Klassifizierungsaktionen für bestimmte eingehende Port. Ihr Switch unterstützt bis zu 1024 ACLs. Pakete, die bei eines eingehenden Ports mit einer aktiven ACL ankommen, werden entweder eingelassen oder zurückgewiesen und der eingehende Port wird deaktiviert. Falls diese nicht eingelassen werden, können Benutzer den Port deaktivieren.

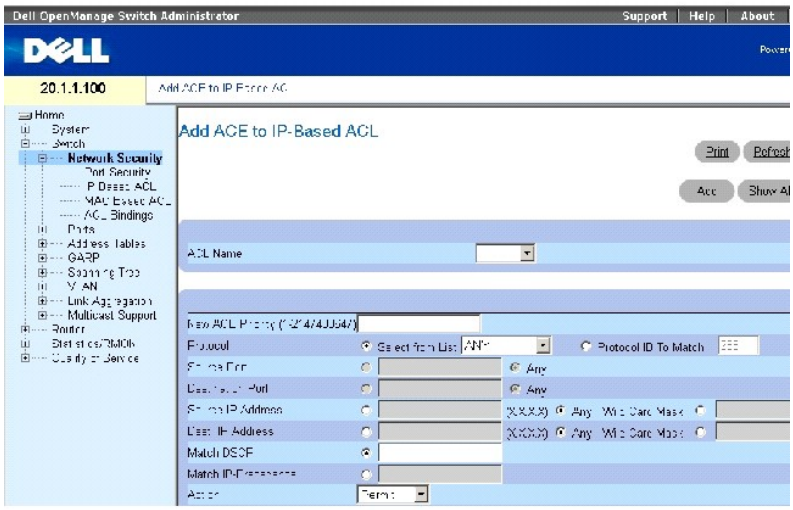
Ein Netzwerkadministrator kann beispielweise eine ACL-Regel definieren, die besagt, dass Portnummer 20 zwar TCP-Pakete empfangen kann, bei Empfang eines UDP-Pakets wird dieses jedoch zurückgewiesen.

ACLs setzen sich aus Zugriffssteuerungseinträgen (ACEs) zusammen, die wiederum aus Filtern bestehen, welche die Datenverkehrklassifizierungen bestimmen. Die Gesamtzahl der ACEs, die in allen ACLs definiert werden können, beträgt 1024.

Auf der Seite **Add ACE to IP Based ACL** (ACE zur IP-basierten ACL hinzufügen) können Sie IP-basierte ACEs definieren.

Um die Seite **ACE zu IP-basierter hinzufügen** zu öffnen, klicken Sie auf **Switch→ Network Security→ IP Based ACL**.

Abbildung 7-8. ACE zu IP-basierter ACL hinzufügen



Die Seite **ACE zu IP-basierter ACL hinzufügen** enthält die folgenden Felder:

ACL Name Benutzerdefinierte ACLs.

New ACE Priority (Neue ACE-Priorität) ACE-Priorität, die bestimmt, welche ACE auf ein Paket nach dem Prinzip der ersten Übereinstimmung zutrifft.

Protocol (Protokoll) Ermöglicht die Erstellung einer ACE auf der Basis eines bestimmten Protokolls.

Select from List (Aus Liste auswählen) Klicken Sie hierauf, um aus einer Liste mit Protokollen auszuwählen, auf denen eine ACE basiert werden kann.

Protocol ID To Match (Abzugleichende Protokoll-ID) Klicken Sie hierauf, um ein benutzerdefiniertes Protokoll hinzuzufügen, anhand dessen Pakete mit der ACE verglichen werden.

ANMERKUNG: Die Option any" (beliebige) gibt an, dass alle IP-Protokolle ausgewählt werden.

Source Port (Quellport) Der TCP/UDP-Quellport. Dieses Feld ist nur aktiv, falls die Optionen **800/6-TCP** oder **800/17-UDP** im Drop-Down-Menü **Select from List** (Aus Liste auswählen) markiert sind.

Destination Port (Zielport) Der TCP/UDP -Zielport. Dieses Feld ist nur aktiv, falls die Optionen **800/6-TCP** oder **800/17-UDP** im Drop-Down-Menü **Select from List** (Aus Liste auswählen) markiert sind.

Source IP Address (Quell-IP-Adresse) Vergleicht die IP-Adresse des Quellports, an den Pakete adressiert sind, mit der ACE.

Wild Card Mask (Wildcard-Maske) Wildcard-Maske der Quell-IP-Adresse. Wildcard-Masken geben an, welche Bits verwendet und welche ignoriert werden. Die Wildcard-Maske 255.255.255.255 zeigt an, dass kein Bit wichtig ist. Die Wildcard 0.0.0.0 zeigt an, dass alle Bits wichtig sind.

Dest. IP Address (Ziel-IP-Adresse) Vergleicht die IP-Adresse des Zielports, an den Pakete adressiert sind, mit der ACE.

Wild Card Mask (Wildcard-Mask) Die Wildcard-Maske der Ziel-IP-Adresse. Wählen Sie entweder **Match DSCP** (DSCP vergleichen) oder **Match IP Precedence** (IP-Priorität vergleichen):

Match DSCP (DSCP vergleichen) Vergleicht den DSCP-Wert des Pakets mit der ACE. Entweder der DSCP-Wert oder der IP-Prioritätswert wird für den

Vergleich von Paketen mit ACLs verwendet.

Match IP Precedence (IP-Priorität vergleichen) Vergleicht den IP-Prioritätswert mit der ACE. Entweder der DSCP-Wert oder der IP-Prioritätswert wird für den Vergleich von Paketen mit ACLs verwendet.

Action (Aktion) Die ACL-Weiterleitungsaktion. Die möglichen Werte sind:

Permit (Zulassen) Leitet Pakete weiter, welche die ACL-Kriterien erfüllen.

Deny (Verweigern) Weist Pakete zurück, welche die ACL-Kriterien erfüllen.

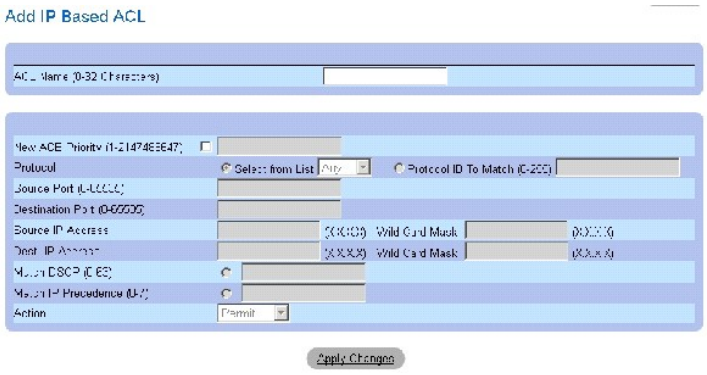
Shutdown (Herunterfahren) Weist Pakete zurück, welche die ACL-Kriterien erfüllen und deaktiviert den Port, an den das Paket adressiert war. Ports werden auf der Seite **Portkonfiguration** reaktiviert. Weitere Informationen finden Sie unter "Definieren der Portkonfiguration".

Um alle ACEs anzuzeigen, die an die ACE angehängt sind, klicken Sie auf **Show All** (Alle anzeigen).

Hinzufügen einer IP-basierten ACL

1. Öffnen Sie die Seite **ACE zu IP-basierter ACL hinzufügen**.
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add IP Based ACL** (Eine IP-basierte ACL hinzufügen) anzuzeigen.

Abbildung 7-9. IP-basierte ACL hinzufügen



3. Geben Sie unter **ACL Name** einen ACL-Namen ein.
4. Markieren Sie das Kontrollkästchen **New ACE Priority** (Neue ACE-Priorität) und definieren Sie alle Felder auf der Seite.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die IP-basierte ACL wird definiert und das Gerät aktualisiert.

Ändern einer IP-basierten ACL

ANMERKUNG: ACEs können nur geändert werden, wenn die ACL, der sie angehören, nicht an eine Schnittstelle gebunden ist.

1. Öffnen Sie die Seite **ACE zu IP-basierter ACL hinzufügen**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um alle ACEs in der ACL anzuzeigen.
3. Wählen Sie eine ACL im Feld **ACL Name** aus.
4. Ändern Sie die Felder wie gewünscht.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die IP-basierte ACE wird geändert und das Gerät aktualisiert.

Hinzufügen von neuen ACEs zu einer IP-basierten ACL

1. Öffnen Sie die Seite **ACE zu IP-basierter ACL hinzufügen**.
2. Wählen Sie eine ACL im Feld **ACL Name** aus.
3. Definieren Sie die Felder im Dialogfeld.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die ACE wird der IP-basierten ACL zugewiesen.

5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen), um die Parameter der neuen ACEs einzugeben und weitere ACEs zu einer vorhandenen ACL hinzuzufügen.

Neu anordnen von ACEs in einer ACL

1. Öffnen Sie die Seite **ACE zu IP-basierter ACL hinzufügen**, und wählen Sie den zu verarbeitenden ACL aus dem Dropdown-Menü **ACL Name** aus.
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die Seite **ACEs Associated with IP-ACL** (mit IP-ACL verknüpfte ACEs) wird angezeigt.

3. Geben Sie eine Prioritätsnummer ein, die die ACE wie gewünscht anordnet.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die ACE wird neu angeordnet und das Gerät aktualisiert.

Entfernen von ACLs

1. Öffnen Sie die Seite **ACE zu IP-basierter ACL hinzufügen**, und wählen Sie den zu verarbeitenden ACL aus dem Dropdown-Menü **ACL Name** aus.
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die Seite **ACEs Associated with IP-ACL** (mit IP-ACL verknüpfte ACEs) wird angezeigt.

3. Markieren Sie das Kontrollkästchen **Remove ACL** (ACL entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die IP-basierte ACL wird entfernt und das Gerät aktualisiert.

Zuweisen von IP-basierten ACEs zu ACLs mithilfe von CLI-Befehlen

Die folgende Tabelle fast die entsprechenden CLI-Befehle für die Zuweisung IP-basierter ACEs zu ACLs, wie auf der Seite **ACE zu IP-basierter ACL hinzufügen** angezeigt, zusammen.

Tabelle 7-5. CLI-Befehle zu IP-basierten ACEs zu ACLs

CLI-Befehl	Beschreibung
`ip access-list` *`name`*	Erstellt IP-ACLs und startet den IP Access-list-Konfigurationsmodus.
`permit {any |` *`protocol`*`} {any | source` *`source-wildcard`*`} {any | destination` *`destination-wildcard`*`} [dscp` *`dscp number`* `| ip-precedence` *`ip-precedence`*`]`	Lässt Datenverkehr zu, falls die im permit-Befehl definierten Bedingungen erfüllt werden.
	Weist Datenverkehr zurück, falls die im deny-Befehl

deny [disable-port] {any | *protocol*} {any | source *source-wildcard*} {any | destination *destination- wildcard*} [dscp *dscp number* | ip-precedence *ip-precedence*]	definierten Bedingungen erfüllt werden.
show access-lists [*name*]	Zeigt die im Switch definierten Access Control-Listen an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

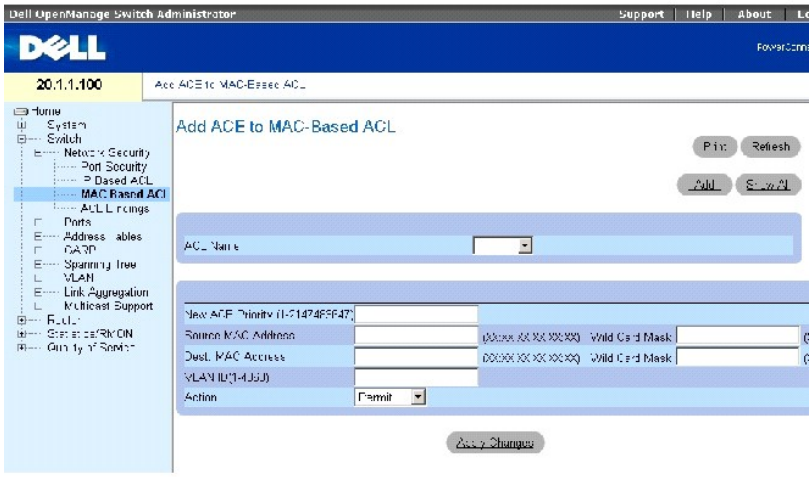
```
Console (config)# ip access-list Dell

Console (config-ip-al)# permit rsvp 12.1.1.1 0.0.0.0 any dscp 56

Console (config-ip-al)# deny any 192.1.1.10 0.0.0.255 any

Console# show access-lists

IP access list one

permit ip host 12.1.1.1 any

permit rsvp host 176.30.40.1 any

Console# show access-lists

IP access list Dell

permit rsvp 12.1.1.1 0.0.0.0 any dscp 56

deny any 192.1.1.10 0.0.0.255 any
```

Definieren von MAC-basierten ACLs

Die Seite **Add ACE to MAC Based ACL** (ACE zu MAC-basierter ACL hinzufügen) ermöglicht Netzwerkadministratoren die Definition einer MAC-basierten ACL. Eine Erläuterung von ACLs finden Sie unter **Definieren von IP-basierten ACLs**".

Um die Seite **ACE zu MAC-basierter ACL hinzufügen** zu öffnen, klicken Sie auf **Switch→ Network Security→ MAC based ACL**.

Abbildung 7-10. ACE zu MAC-basierter ACL hinzufügen



Die Seite **ACE zu MAC-basierter ACL hinzufügen** enthält die folgenden Felder:

ACL Name Benutzerdefinierter ACL.

New ACE Priority (Neue ACE-Priorität) ACE-Priorität, die bestimmt, welche ACE auf ein Paket nach dem Prinzip der ersten Übereinstimmung zutrifft.

Source MAC Address (Quell-MAC-Adresse) Vergleicht die MAC-Adresse des Quellports, vom dem Pakete adressiert sind, mit der ACE.

Wild Card Mask (Wildcard-Maske) Die Wildcard-Maske der Quell-MAC-Adresse. Mithilfe von Wildcards werden Quell-MAC-Adressen vollständig oder teilweise maskiert. Wildcard-Masks geben an, welche Bits verwendet und welche ignoriert werden. Eine Wildcard-Maske mit der Adresse FF:FF:FF:FF:FF:FF gibt an, dass keine Bits von Bedeutung sind. Eine Wildcard mit der Adresse 00.00.00.00.00.00 gibt an, dass alle Bits wichtig sind.
Wenn beispielsweise die Quell-MAC-Adresse E0:3B:4A:C2:CA:E2 lautet und die Wildcard-Maske 00:3B:4A:C2:CA:FF, werden die ersten zwei Bits der MAC-Adresse verwendet und die zwei letzten Bits ignoriert.

Destination MAC Address (Ziel-MAC-Adresse) Vergleicht die Ziel-MAC-Adresse, an die Paketen adressiert sind, mit der ACE.

Wild Card Mask (Wildcard-Mask) Die Wildcard-Maske der MAC-Zieladresse. Mithilfe von Wildcards werden Ziel-MAC-Adressen vollständig oder teilweise maskiert.

VLAN ID Vergleicht die VLAN-ID des Pakets mit der ACE. Die möglichen Feldwerte sind 1-4094.

Action Zeigt die ACL-Weiterleitungsaktion an. Mögliche Feldwerte sind:

Permit (Zulassen) Leitet Pakete weiter, welche die ACL-Kriterien erfüllen.

Deny (Verweigern) Weist Pakete zurück, welche die ACL-Kriterien erfüllen.

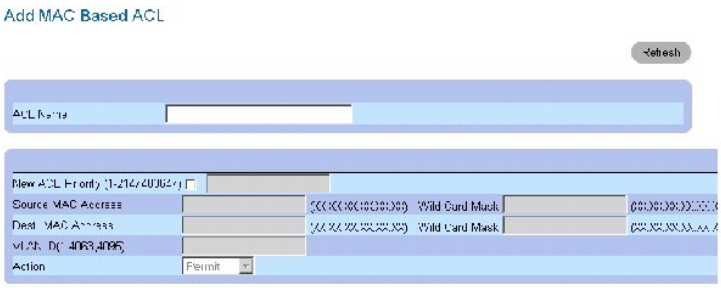
Shutdown (Herunterfahren) Weist Pakete zurück, welche die ACL-Kriterien erfüllen und deaktiviert den Port, an den das Paket adressiert war. Ports werden auf der Seite **Portkonfiguration** reaktiviert. Weitere Informationen finden Sie unter Definieren der Portkonfiguration".

Hinzufügen einer MAC-basierten ACL

1. Öffnen Sie die Seite **Add ACE to MAC Based ACL** (ACE zur MAC-basierten ACL hinzufügen).

2. Klicken Sie auf **Add** (Hinzufügen), um die Seite MAC-basierte ACL hinzufügen zu öffnen.

Abbildung 7-11. MAC-basierte ACL hinzufügen



3. Geben Sie unter **ACL Name** einen ACL-Namen ein.
4. Um eine neue ACE zu einer neu erstellten ACL hinzuzufügen, aktivieren Sie das Kontrollkästchen **New ACE Priority** (Neue ACE-Priorität), und definieren Sie die Felder **Source**- und **Destination** MAC Address (Quell- und Ziel-MAC-Adresse), **VLAN ID** und **Action**.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die MAC-basierte ACL wird definiert und das Gerät aktualisiert.

Ändern einer MAC-basierten ACL

1. Öffnen Sie die Seite **Add ACE to MAC Based ACL** (ACE zur MAC-basierten ACL hinzufügen).
2. Wählen Sie eine ACL im Feld **ACL Name** aus.
3. Ändern Sie die entsprechenden Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Felder werden geändert und das Gerät aktualisiert.

Hinzufügen von ACEs zu einer MAC-basierten ACL

ANMERKUNG: ACEs können nur hinzugefügt werden, wenn die ACL nicht an eine Schnittstelle gebunden ist.

1. Öffnen Sie die Seite **Add ACE to MAC Based ACL** (ACE zur MAC-basierten ACL hinzufügen).
2. Wählen Sie eine ACL im Feld **ACL Name** aus.
3. Definieren Sie die Felder **New ACE Priority** (Neue ACE-Priorität), **Source**- und **Destination** MAC Address (Quell- und Ziel-MAC-Adresse), **VLAN ID** und **Action**.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die ACE wird der MAC-basierten ACL zugewiesen.

ANMERKUNG: Um mehr als eine ACE zu einer bestehenden ACL hinzuzufügen, klicken Sie auf **Apply Changes** (Änderungen übernehmen) und füllen die neuen ACE-Parameter aus.

Anzeigen von ACL-spezifischen ACEs

1. Öffnen Sie die Seite **Add ACE to MAC Based ACL** (ACE zur MAC-basierten ACL hinzufügen).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **ACEs Associated with MAC ACL** (Mit der MAC-ACL verknüpfte ACEs) anzuzeigen.

Entfernen von ACLs

ANMERKUNG: ACLs können nur hinzugefügt werden, wenn diese nicht an eine Schnittstelle gebunden ist.

1. Wählen Sie eine ACL aus.
2. Öffnen Sie die Seite **Add ACE to MAC Based ACL** (ACE zur MAC-basierten ACL hinzufügen).
3. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **ACEs Associated with MAC ACL** (Mit der MAC-ACL verknüpfte ACEs) anzuzeigen.
4. Aktivieren Sie das Kontrollkästchen **Remove ACL** (ACL entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die MAC-basierte ACL wird entfernt und das Gerät aktualisiert.

Entfernen von ACEs aus einer ACL

1. Wählen Sie eine ACL aus.
2. Öffnen Sie die Seite **Add ACE to MAC Based ACL** (ACE zur MAC-basierten ACL hinzufügen).
3. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **ACEs Associated with MAC ACL** (Mit der MAC-ACL verknüpfte ACEs) anzuzeigen.
4. Aktivieren Sie das Kontrollkästchen **Remove ACE** (ACE entfernen) in der Zeile der zu entfernenden ACE.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die MAC-basierte ACL wird entfernt und das Gerät aktualisiert.

Zuweisen von MAC-basierten ACEs zu ACLs mithilfe von CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für die Zuweisung MAC-basierter ACEs zu ACLs auf der Seite Add ACE to MAC Based ACL (ACE zur MAC-basierter ACL hinzufügen) zusammen.

Tabelle 7-6. CLI-Befehle für MAC-basierte ACE

CLI-Befehl	Beschreibung
`mac access-list name`	Erstellt Schicht-2-MAC-ACLs und startet den MAC Access-list-Konfigurationsmodus.
`permit {any | host source source-wildcard} {any | destination destination-wildcard}[vlan vlan-id]`	Lässt Datenverkehr zu, falls die im permit-Befehl definierten Bedingungen erfüllt werden.
`deny [disable-port] {any | source source- wildcard} {any | destination destination- wildcard}[vlan vlan-id]`	Weist Datenverkehr zurück, falls die im deny-Befehl definierten Bedingungen erfüllt werden.
`show access-lists [name]`	Zeigt die im Switch konfigurierten Access Control-Listen an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

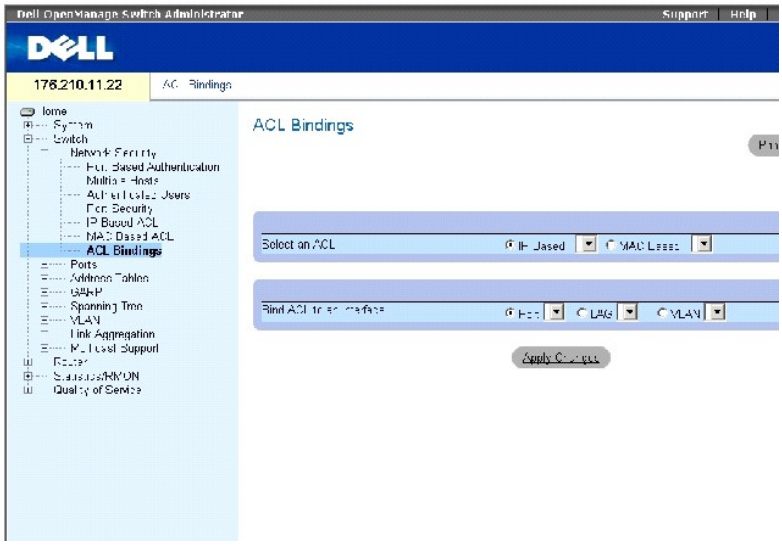
```
Console (config)# mac access-list dell

Console (config-mac-al)# permit 6:6:6:6:6:6 0:0:0:0:0:0 any vlan 4

Console (config-mac-al)# deny 6:6:6:6:6:6 0:0:255:255:255:255
```

Konfigurieren von ACL-Bindung

Ist eine ACL an eine Schnittstelle gebunden, werden alle definierten ACE-Regeln auf die ausgewählte Schnittstelle angewendet. Auf der Seite **ACL-Bindungen** können Sie ACL-Listen zu Klassifizierungsmethoden und Schnittstellen zuweisen.

Um die Seite **ACL-Bindungen** zu öffnen, klicken Sie auf **Switch→ Network Security→ ACL Binding**.

Abbildung 7-12. ACL-Bindungen



Die Seite **ACL-Bindungen** enthält die folgenden Felder:

Select an ACL (ACL auswählen) Der ACL-Typ, mit dem eingehende Pakete verglichen werden. Pakete lassen sich entweder mit IP-basierten ACLs vergleichen oder ACLs, die auf der MAC-Adresse basieren.

Bind ACL to Interface (ACL mit Schnittstelle verbinden) Die Schnittstelle und der Schnittstellentyp, mit dem ACL verbunden ist. Sie können die ACL an einen Port, eine LAG oder ein VLAN anbinden.

Zuweisen einer ACL zu einer Schnittstelle

1. Öffnen Sie die Seite **ACL-Bindungen**.
2. Wählen Sie im Feld **Select ACL** (ACL auswählen) den ACL-Typ aus.
3. Wählen Sie im Feld **Bind ACL to Interface** (ACL an Schnittstelle binden) die Schnittstelle aus, an die die ACL gebunden wird.

ANMERKUNG: Bei der Zuordnung einer ACL zu einem Port, einer LAG oder einem VLAN werden Flüsse aus dieser eingehenden Schnittstelle, die nicht der ACL entsprechen, mit der Standardregel Nicht übereinstimmende Pakete zurückweisen" abgeglichen.

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

Die ACL wird an die Schnittstelle gebunden.

Entfernen eines Eintrags aus der Tabelle mit ACL-Bindungen.

1. Öffnen Sie die Seite **ACL-Bindungen**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Tabelle **ACL-Bindungen** anzuzeigen.

3. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen) für den zu entfernenden Eintrag.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der ausgewählte Eintrag wird aus der Tabelle entfernt und das Gerät aktualisiert.

Anzeigen der Tabelle mit ACL-Bindungen

1. Öffnen Sie die Seite **ACL-Bindungen**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Tabelle **ACL-Bindungen** anzuzeigen.

Die Felder unter **ACL Bindings Table** (Tabelle mit ACL-Bindungen) entsprechen den Feldern auf der Seite **ACL Bindings** (ACL-Bindungen).

Kopieren von Parametern in die Tabelle mit ACL-Bindungen

1. Öffnen Sie die Seite **ACL-Bindungen**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Tabelle **ACL-Bindungen** anzuzeigen.
3. Wählen Sie im Feld **Copy Parameters from** (Kopieren von Parametern aus) eine Schnittstelle aus.
4. Wählen Sie im Drop-Down-Menü **Port/LAG** oder **VLAN** einen Port oder eine Anschlussstelle aus.

Die Definitionen für diese Schnittstelle werden an die ausgewählten Zielports/-anschlussstellen kopiert.

5. Aktivieren Sie für jeden zu bearbeitenden Eintrag das Kontrollkästchen **Copy to** (Kopieren nach), oder klicken Sie auf **Select All** (Alle auswählen), um die Definitionen auf alle verfügbaren Ports/Anschlussstellen zu kopieren.
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Parameter werden auf die Zielports/-anschlussstellen in der **ACL Bindings Table** (Tabelle mit ACL-Bindungen) kopiert und das Gerät aktualisiert.

Zuweisen von ACL-Mitgliedschaft mithilfe von CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für die Zuweisung von ACL Mitgliedschaft auf der Seite **ACL Bindings** zusammen.

Tabelle 7-7. CLI-Befehle für ACL-Bindungen

CLI-Befehl	Beschreibung
`class-map class-map-name [match-all | match-any]`	Erstellt Klassenmap und startet den class-map-Konfigurationsmodus.
`match access-group acl-name`	Definiert das Vergleichskriterium, nach dem der Datenverkehr klassifiziert wird.
`show class-map [class-map-name]`	Zeigt alle auf dem Gerät konfigurierten Klassenmaps an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# class-map class1 match-all

Console (config-cmap)# match access-group dell

Console (config-cmap)# exit
```

```
Console (config)# exit


Console> exit


Console> show class-map class1


Class Map match-all class1 (id4)
```

Konfigurieren von Ports

Die Seite **Ports** enthält Verknüpfungen für die Konfiguration von Portfunktionalität, einschließlich erweiterter Funktionen wie Sturmkontrolle und Portspiegelung sowie für die Durchführung virtueller Porttests.

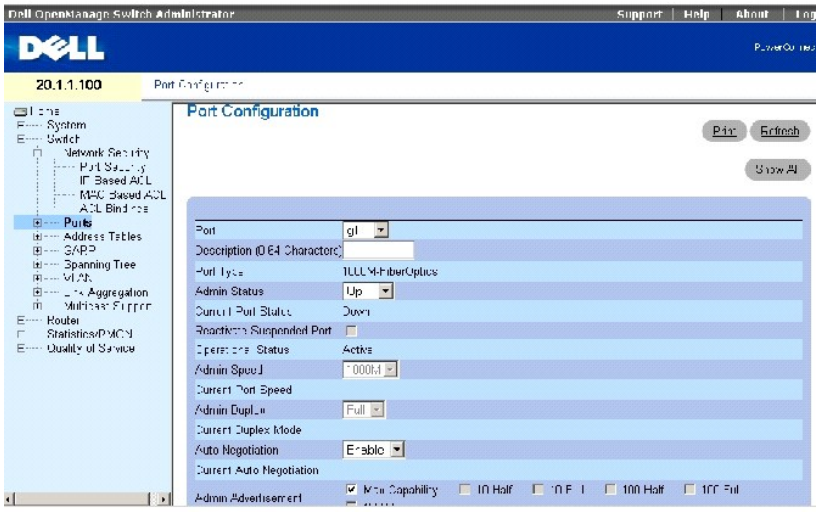
Um die Seite **Ports**zu öffnen, wählen Sie **Switch**→ **Ports** aus.

Definieren der Portkonfiguration

Auf der Seite **Port Configuration** (Portkonfiguration) definieren Sie die Portparameter.

Öffnen Sie die Seite **Port Configuration**, indem Sie auf **Switch**→ **Ports**→ **Port Configuration** in der *Strukturansicht* klicken.

Abbildung 7-13. Portkonfiguration



Die Seite **Portkonfiguration** enthält die folgenden Felder:

Port Gibt die Anschlussnummer an, für die Portparameter definiert werden.

Description (0-64 Characters) Enthält eine kurze Schnittstellenbeschreibung, z. B. Ethernet.

Port Type Gibt den Porttyp an.

Admin Status Aktiviert/deaktiviert den über den Port geleiteten Datenverkehr.

Current Port Status (Aktueller Portzustand) Gibt den Betriebszustand des Ports an.

Reactivate Suspended Port (Reaktivierter inaktiver Port) Reaktiviert einen Port, wenn der Port über die Sicherheitsfunktion Gesperrter Port" deaktiviert wurde.

Operational Status (Betriebsmodus) Zeigt den aktuellen Betriebsmodus des Ports an. Mögliche Feldwerte sind:

Suspended Der Port ist gegenwärtig aktiv und empfängt oder überträgt gegenwärtig keinen Verkehr.

Active Der Port ist gegenwärtig aktiv und empfängt und überträgt gegenwärtig Verkehr.

Disable Der Port ist gegenwärtig deaktiviert und empfängt oder überträgt gegenwärtig keinen Verkehr.

Admin Speed Gibt die konfigurierte Geschwindigkeit an, mit der der Port arbeitet. Der Porttyp bestimmt, welche Geschwindigkeitseinstellungen verfügbar sind. Sie können die Verwaltungseinstellung nur festlegen, wenn der Port deaktiviert ist.

Current Port Speed (Derzeitige Portgeschwindigkeit) Die derzeitige synchronisierte Portgeschwindigkeit (bps).

Admin Duplex Der Port-Duplexmodus in bps. **Full** (Voll) gibt an, dass die Schnittstelle die Übertragung zwischen dem Gerät und dem Client in beide Richtungen gleichzeitig unterstützt. **Half** zeigt an, dass die Schnittstelle ein Übertragung zwischen dem Gerät und dem Client nur in jeweils eine Richtung unterstützt.

Current Duplex Mode (Derzeitiger Duplexmodus) Der synchronisierte Duplexmodus des Ports.

Auto Negotiation Aktiviert Auto-Negotiation für den Port.
Die automatische Verbindungseinstellung ist ein Protokoll zwischen zwei Verbindungsteilnehmern, das es einem Port ermöglicht, seine Funktionen bezüglich Übertragungsrate, Duplexmodus und Datenflusssteuerung der Gegenstelle bekannt zu geben.

Current Auto Negotiation (Derzeitige Auto-Verhandlung) Die derzeitige Einstellung zu Auto-Verhandlung.

Admin Advertisement (Admin-Meldung) Legt die Kapazitäten fest, die durch den Port gemeldet werden sollen. Die möglichen Feldwerte sind:

Max Capability (Maximale Kapazität) Zeigt an, dass alle Portgeschwindigkeiten und Duplexmoduseinstellungen akzeptiert werden können.

10 Half (Halb) Zeigt an, dass der Port eine Geschwindigkeit von 10 mbps und die Einstellung Halbduplexmodus meldet.

10 Half (Voll) Zeigt an, dass der Port eine Geschwindigkeit von 10 mbps und die Einstellung Vollduplexmodus meldet.

100 Half (Halb) Zeigt an, dass der Port eine Geschwindigkeit von 100 mbps und die Einstellung Halbduplexmodus meldet.

100 Half (Voll) Zeigt an, dass der Port eine Geschwindigkeit von 100 mbps und die Einstellung Vollduplexmodus meldet.

1000 Half (Voll) Zeigt an, dass der Port eine Geschwindigkeit von 1000 mbps und die Einstellung Vollduplexmodus meldet.

Current Advertisement (Derzeitige Meldung) Der Port meldet seine Geschwindigkeit an den benachbarten Port, um den Verhandlungsprozess zu starten. Die möglichen Feldwerte entsprechen denen des Felds Admin Advertisement" (Admin-Meldung).

Neighbor Advertisement (Nachbarnmeldung) Der Nachbarnport (der Port, mit dem die ausgewählte Schnittstelle verbunden ist), meldet ihre Kapazität an den Port, um den Verhandlungsprozess zu starten. Die möglichen Werte entsprechen denen des Felds Admin Advertisement" (Admin-Meldung).

Back Pressure Aktiviert den Backpressure-Modus (Zurückweisung) am Port. Der Backpressure-Modus wird im Halbduplexmodus verwendet, um den Eingang von Meldungen am Port zu verhindern. Back Pressure wird bei bandexternen Ports nicht unterstützt.

Current Back Pressure (Derzeitiger Back Pressure) Die aktuellen Back Pressure-Einstellungen.

Flow Control Aktiviert oder deaktiviert Datenflusssteuerung oder aktiviert Auto-Negotiation der Datenflusssteuerung für den Port.

Current Flow Control (Derzeitige Datenflusssteuerung) Die aktuelle Datenflusssteuerungseinstellung.

MDI/MDIX Ermöglicht dem Gerät die Erkennung gekreuzter und nicht gekreuzter Kabel.

Hubs und Schalter sind entgegengesetzt zu Endstationen verkabelt, so dass, wenn ein Hub oder Schalter mit einer Endstation verbunden ist, ein ungekreuztes Ethernetkabel verwendet werden kann und sichergestellt wird, dass die Paare richtig angeschlossen sind. Wenn zwei Hubs/Schalter bzw. zwei Endstationen miteinander verbunden werden, wird mithilfe eines gekreuzten Kabels sichergestellt, dass die Paare richtig angeschlossen sind. Auto-MDIX funktioniert nicht bei FE-Ports, falls die automatische Verbindungseinstellung deaktiviert ist. MDIX wird bei bandexternen Ports nicht unterstützt.

Die möglichen Werte sind:

Media Dependent Interface with Crossover (MDIX) Wird für Hubs und Switches verwendet.

Media Dependent Interface (MDI) Wird für Endstellen verwendet.

Current MDI/MDIX (Derzeitiger MDI/MDIX) Gibt die aktuellen MDIX-Einstellungen des Gerätes an. Mögliche Feldwerte sind:

MDI Die aktuelle MDI-Einstellung ist MDI.

MDIX Die aktuelle MDI-Einstellung ist MDIX.

Auto Der Wert wird automatisch festgelegt.

LAG Gibt an, ob der Port Teil einer LAG ist.

PVE Definiert einen Port als Private VLAN Edge-Port (PVE). Wenn ein Port als PVE definiert ist, deaktiviert es die Forwarding Database (FDB) und leitet den gesamten Unicast-, Multicast- und Broadcast-Datenverkehr an einen Uplink (außer MAC-to-me-Pakete) weiter. Uplinks können ein Port oder ein LAG sein. Datenverkehr vom Uplink wird auf alle Ports verteilt.

Definieren von Portparametern

1. Öffnen Sie die Seite **Port Configuration**.
2. Wählen Sie einen Port im Feld **Port**.
3. Definieren Sie die verfügbaren Felder im Dialogfeld.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Portparameter werden im Gerät gespeichert.

Anzeigen der Porttabelle

1. Öffnen Sie die Seite **Port Configuration**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **Port Configuration Table** (Portkonfigurationstabelle) anzuzeigen.

Konfigurieren von Ports mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Konfiguration von Ports, wie auf der Seite Portkonfiguration angezeigt, zusammen.

Tabelle 7-8. CLI-Befehle zur Portkonfiguration

CLI-Befehl	Beschreibung
`interface ethernet interface`	Aktiviert den Schnittstellenkonfigurationsmodus, um eine Ethernet-Schnittstelle zu konfigurieren.
`description string`	Fügt einer Schnittstellenkonfiguration eine Beschreibung hinzu.
`Shutdown`	Deaktiviert Schnittstellen innerhalb des derzeit festgelegten Kontexts.
`set interface active { ethernet interface | port-channel port-channel-number }`	Reaktiviert eine Schnittstelle, die aus Sicherheitsgründen deaktiviert wurde.
`speed {10 | 100 | 1000}`	Konfiguriert die Geschwindigkeit einer bestimmten Ethernet-Schnittstelle, wenn keine Auto-Negotiation verwendet wird.
`duplex {half | full}`	Konfiguriert den Voll-/Halbduplexbetrieb einer bestimmten Ethernet-Schnittstelle, wenn keine Auto-Negotiation verwendet wird.
`negotiation`	Aktiviert die Auto-Negotiation für Geschwindigkeit und Duplexparameter einer bestimmten Schnittstelle.
`back-pressure`	Aktiviert Backpressure für eine bestimmte Schnittstelle.
`flowcontrol {auto | on | off}`	Konfiguriert die Flusskontrolle für eine bestimmte Schnittstelle.
`mdix {on | auto}`	Aktiviert die automatische Kreuzkabel-Erkennung für eine bestimmte Schnittstelle bzw. einen bestimmten Portkanal.
`show interfaces configuration [ethernet interface | port-channel port-channel-number oob- eth interface]`	Zeigt die Konfiguration aller konfigurierten Schnittstellen an.
`show interfaces status [ethernet interface | port- channel port-channel- number oob-eth interface]`	Zeigt den Status aller konfigurierten Schnittstellen an.
`show interfaces description [ethernet interface | port-channel port-channel-number oob- eth interface]`	Zeigt die Beschreibung aller konfigurierten Schnittstellen an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface ethernet g18

Console (config-if)# description RD_SW#3

Console (config-if)# speed 100

Console (config-if)# shutdown

Console (config-if)# no shutdown

Console (config-if)# duplex full

Console (config-if)# negotiation

Console (config-if)# back-pressure

Console (config-if)# flowcontrol on

Console (config-if)# mdix auto

Console (config-if)# exit

Console (config)# exit

Console> set interface active ethernet g9
```

```
Console> show interfaces status
```

					Flow	Link	Back	Mdix
Port	Typ	Duplex	Speed	Neg	ctrl	Status	Pressure	Mode
---	------	----	---	---	-----	-----	-----	-----
g1	1G-Copper	Full	1000	Enabled (Aktiviert)	Off	Up	Disabled	Off
g2	1G-Copper	Full	1000	Enabled (Aktiviert)	Off	Up	Disabled	Off
g3	1G-Copper	Full	1000	Enabled (Aktiviert)	Off	Up	Disabled	Off

					Flow	Link	Back
Ch	Typ	Duplex	Speed	Neg	control	Status	Pressure
---	--------	-----	----	----	------	------	-------
ch1	Unknown	Unknown		Unknown	Off	Not Present	Unknown
ch2	Unknown	Unknown		Unknown	Off	Not Present	Unknown
ch3	Unknown	Unknown		Unknown	Off	Not Present	Unknown
ch4	Unknown	Unknown		Unknown	Off	Not Present	Unknown

```
Console# show interfaces configuration
```

					Flow	Admin	Back
Ch	Typ	Duplex	Speed	Neg	control	Status	Pressure
---	-------	---	---	----	-------	-----	--------
ch1	Unknown			Enable d	Off	Up	Disabled
ch2	Unknown			Enable d	Off	Up	Disabled
ch3	Unknown			Enable d	Off	Up	Disabled

```
Console# show interfaces description ethernet 1
```

Port	Beschreibung
-----	----------
g1	connect_to_server

Definieren der LAG-Konfiguration

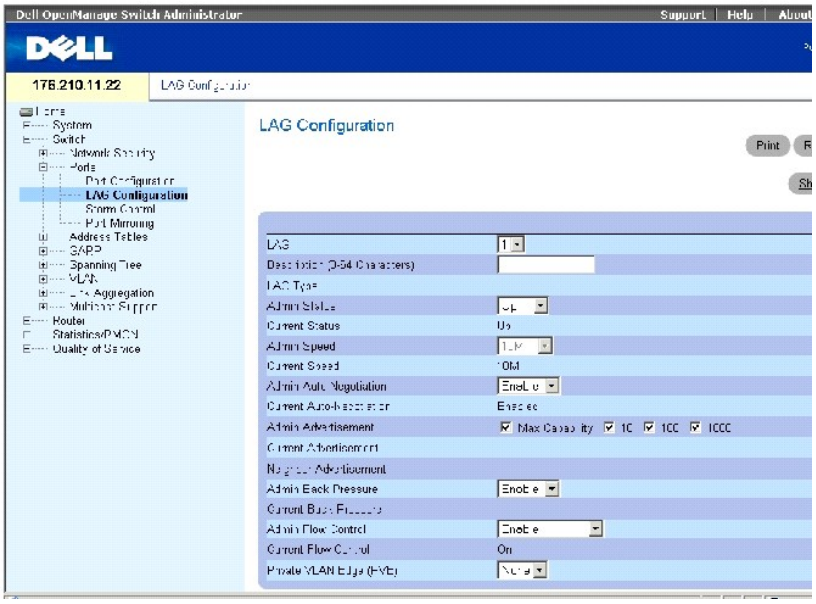
Multilayer-Switche unterstützen die Bündelung mehrerer Links zu einem logischen Link mit zusammengefasster Kapazität, einer sogenannten Link Aggregrated Group (LAG). LAGs werden häufig auch Trunks oder aggregierte Verbindung bezeichnet.

Auf der Seite **LAG Configuration** (LAG-Konfiguration) konfigurieren Sie die LAG-Parameter. Ihr Switch unterstützt bis zu sieben Schnittstellen pro LAG und sieben LAGs pro System. Wird die Portkonfiguration geändert, während ein Port ein LAG-Mitglied ist, tritt die Konfigurationsänderung erst in Kraft, nachdem der Port aus der LAG entfernt wird.

Informationen über das Aggregieren von Ports finden Sie unter Aggregieren von Ports”.

Öffnen Sie die Seite **LAG Configuration**, indem Sie auf **Switch→ Ports→ LAG Configuration** in der *Strukturansicht* klicken.

Abbildung 7-14. LAG-Konfiguration



Die Seite **LAG-Konfiguration** enthält die folgenden Felder:

LAG Enthält eine Liste von LAG-Nummern.

Description (0-64 Zeichen) Beschreibung des Ports.

LAG Type Gibt die Porttypen an, die in der LAG enthalten sind.

Admin Status Aktiviert/deaktiviert den über die ausgewählte LAG geleiteten Datenverkehr.

Current Status Gibt den LAG-Status an.

Admin Speed Gibt die Betriebsgeschwindigkeit der LAG an.

Current Speed Gibt die aktuelle Geschwindigkeit der LAG an.

Admin Auto Negotiation Aktiviert/deaktiviert die Auto-Negotiation für die LAG. Auto-Negotiation bezeichnet ein Protokoll zwischen zwei Verbindungspartnern, mit dessen Hilfe der jeweils anderen LAG Übertragungsrate, Duplexmodus und Flusskontrollverhalten (standardmäßig deaktiviert) mitgeteilt werden.

Current Auto Negotiation (Aktuelle Auto-Verhandlung) Die derzeitige Einstellung zu Auto-Verhandlung.

Admin Advertisement (Admin-Meldung) Legt die Kapazitäten fest, die durch die LAG gemeldet werden sollen. Die möglichen Feldwerte sind:

Max Capability (Maximale Kapazität) Zeigt an, dass alle LAG-Geschwindigkeiten und Duplexmoduseinstellungen akzeptiert werden können.

10 Zeigt an, dass die LAG eine Geschwindigkeit von 10 mbps und die Einstellung Vollduplexmodus meldet.

100 Zeigt an, dass die LAG eine Geschwindigkeit von 100 mbps und die Einstellung Vollduplexmodus meldet.

1000 Zeigt an, dass die LAG eine Geschwindigkeit von 1000 mbps und die Einstellung Vollduplexmodus meldet.

Current Advertisement (Derzeitige Meldung) Die LAG meldet ihre Kapazitäten an die benachbarte LAG, um den Verhandlungsprozess zu starten. Die möglichen Feldwerte entsprechen denen des Felds Admin Advertisement" (Admin-Meldung).

Neighbor Advertisement (Nachbarnmeldung) Die benachbarte LAG (die LAG, mit der die ausgewählte Schnittstelle verbunden ist), meldet ihre Kapazität an die LAG, um den Verhandlungsprozess zu starten. Die möglichen Werte entsprechen denen des Felds Admin Advertisement" (Admin-Meldung).

Admin Back Pressure Aktiviert oder deaktiviert den Back Pressure-Modus auf dem Gerät. Der Backpressure-Modus wird im Halbduplexmodus verwendet, um den Eingang von Meldungen am Port zu verhindern.

Admin Flow Control (Admin-Datenflusssteuerung) Aktiviert bzw. deaktiviert die Datenflusssteuerung oder aktiviert die automatische Einstellung der Datenflusssteuerung auf der LAG.

Admin Flow Control Aktiviert oder deaktiviert Datenflusssteuerung oder aktiviert Auto-Negotiation der Datenflusssteuerung in der LAG.

Current Flow Control Die benutzerdefinierte Datenflusssteuerungseinstellung.

Definieren von LAG-Parametern

1. Öffnen Sie die Seite **LAG Configuration**.
2. Wählen Sie eine LAG im Feld **LAG**.
3. Definieren Sie die verfügbaren Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die LAG-Parameter werden im Gerät gespeichert.

Anzeigen der LAG-Konfigurationstabelle

1. Öffnen Sie die Seite **LAG Configuration**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **LAG Configuration Table** (LAG-Konfigurationstabelle) anzuzeigen.

Konfigurieren von LAGs mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Konfiguration von LAGs, wie auf der Seite **LAG Configuration** angezeigt, zusammen.

Tabelle 7-9. CLI-Befehle zur LAG-Konfiguration

CLI-Befehl	Beschreibung
`interface port-channel` *`port-channel-number`*	Aktiviert den Schnittstellenkonfigurationsmodus eines spezifischen Portkanals.

channel-group *port-channel-number* mode {on | auto}	Verknüpft einen Port mit einem Portkanal.
show interfaces port-channel [*port-channel-number*]	Zeigt Portkanalinformationen an (welche Ports einem Portkanal angehören und ob sie derzeit aktiv sind oder nicht).

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface ethernet g5

Console (config-if)# channel-group 1 mode on

Console (config-if)# exit

Console# show interfaces port-channel

Channel     Port

-------     --------------------------------

Ch 1        Active   g1, g2, g5   Inactive g3

Ch 2        Active   g2

Ch 3        Inactive g8
```

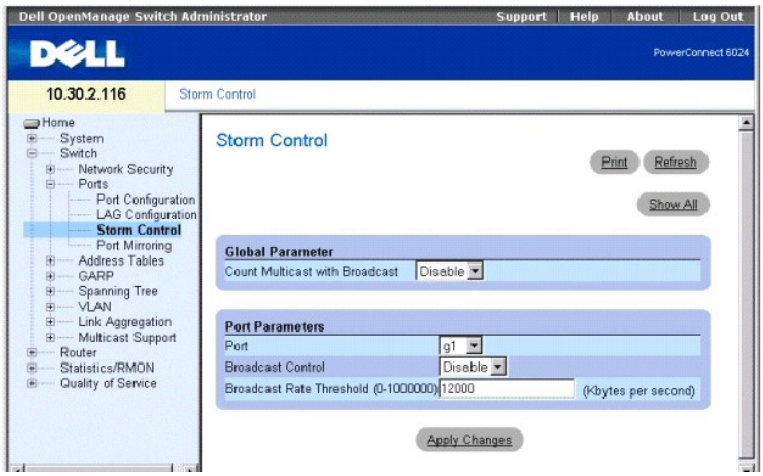
Aktivieren der Sturmkontrolle

Ein Broadcast-Sturm ist das Ergebnis einer übermäßig hohen Anzahl von Broadcast-Meldungen, die gleichzeitig über das Netzwerk von einem einzelnen Port übertragen werden. Weitergeleitete Antworten auf Meldungen können Netzwerkressourcen überlasten und/oder eine Zeitüberschreitung des Netzwerks bewirken.

Ihr Switch misst die eingehende Broadcast-/Multicast-Paketrate pro Port und verwirft Pakete, wenn die Rate den definierten Wert überschreitet. Die Sturmkontrolle wird pro Gerät aktiviert, indem der Pakettyp und die Rate definiert wird, mit der die Pakete übertragen werden. Portgruppen bieten Sturmschutz für eine gesamte Portgruppe.

Auf der Seite **Storm Control** (Sturmkontrolle) können Sie die Sturmkontrolle aktivieren und konfigurieren. Öffnen Sie die Seite **Storm Control**, indem Sie auf **Switch→ Ports→ Storm Control** in der *Strukturansicht* klicken.

Abbildung 7-15. Sturmkontrolle



Count Multicast with Broadcast (Multicast mit Broadcast zählen) **Aktiviert** Multicast mit Broadcast zählen; **deaktiviert** Nur Broadcast-Datenverkehr zählen.

Port Der Port, von welchem die Sturmkontrolle aktiviert wird.

Broadcast Control (Broadcast-Steuerung) Aktiviert oder deaktiviert die Weiterleitung von unbekannten Pakettypen auf dem Gerät.

Broadcast Rate Threshold (Schwellenwert der Broadcast-Rate) Die maximale Rate (Kilobyte pro Sekunde), mit der unbekannte Pakete weitergeleitet werden. Der Bereich liegt zwischen 0 und 148,800. Der Standardwert ist 12.000. Alle Werte werden auf die nächsten 64 KBit/s gerundet. Liegt der Feldwert unter 64 Bit/s, wird der Wert auf 64 Bit/s aufgerundet.

Ändern der Portparameter für die Sturmkontrolle

1. Öffnen Sie die Seite **Storm Control**.
2. Geben Sie die Informationen in die Felder auf der Seite ein.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Portparameter für die Sturmkontrolle werden auf dem Gerät gespeichert.

Kopieren von Parametern in die Tabelle mit Sturmkontrolleinstellungen

1. Öffnen Sie die Seite **Storm Control**.
2. Klicken Sie auf **Show All** (Alles anzeigen), um die Seite **Storm Control Settings Table** (Tabelle mit Sturmkontrolleinstellungen) anzuzeigen.
3. Wählen Sie im Feld **Copy Parameters from Port** (Parameter kopieren aus Port) den Port aus, von dem Sie die Einstellungen kopieren möchten.
4. Aktivieren Sie das Kontrollkästchen **Copy to** (Kopieren nach), um die Schnittstellen zu definieren, auf die die Sturmkontrolleinstellungen kopiert werden, oder klicken Sie auf **Select All** (Alle auswählen), um die Definitionen auf alle Ports zu kopieren.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Parameter werden auf die ausgewählten Ports in der **Storm Control Settings Table** (Tabelle mit Sturmkontrolleinstellungen) kopiert und das Gerät aktualisiert.

Konfigurieren der Sturmkontrolle mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für die Konfiguration der Sturmkontrolle auf der Seite **Storm Control** (Sturmkontrolle) zusammen.

Tabelle 7-10. CLI-Befehle für Sturmkontrolle

CLI-Befehl	Beschreibung
`port storm-control include-multicast`	Ermöglicht dem Gerät das Zählen von Multicast- zusammen mit Broadcast-Paketen.
`port storm-control broadcast enable`	Aktiviert die Broadcast Sturmkontrolle.
`port storm-control broadcast rate` *rate*	Konfiguriert die maximale Broadcast-Rate.
`show ports storm-control` *port*	Zeigt die Konfiguration der Sturmkontrolle an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# port storm-control include-multicast

Console (config)# interface ethernet g1

Console (config-if)# port storm-control broadcast enable

Console (config-if)# port storm-control broadcast rate 100000

Console (config-if)# exit
```

Port	Broadcast and Multicast Storm Control (Broadcast- und Multicast-Sturmkontrolle) [KBytes/Sek.]	
----	----------	
g1		100000
g2		Disabled
...		
g24		Disabled

Definieren von Portspiegelungssitzungen

Port-Mirroring (Portspiegelung) überwacht und spiegelt Netzwerk-Datenverkehr durch Weiterleitung von Kopien der eingehenden und ausgehenden Pakete von einem überwachten Port zu einem Überwachungsport. Die Portspiegelung kann als Diagnosetool und/oder Funktion zur Fehlerbehebung verwendet werden. Sie ermöglicht außerdem die Leistungsüberwachung des Switch.

Netzwerkadministratoren konfigurieren die Portspiegelung, indem Sie einen bestimmten Port zum Kopieren aller Pakete auswählen, sowie anderen Ports, von denen die Pakete kopiert werden. Vor dem Konfigurieren der Portspiegelung sollten folgende Punkte beachtet werden:

- Überwachte Ports können nicht schneller als die überwachende Ports betrieben werden.
- Die maximale Anzahl der Quellports beträgt acht.

- Es kann jeweils nur eine Spiegelungssitzung gleichzeitig konfiguriert werden.

Die folgenden Beschränkungen gelten für Ports, die als Zielports konfiguriert sind:

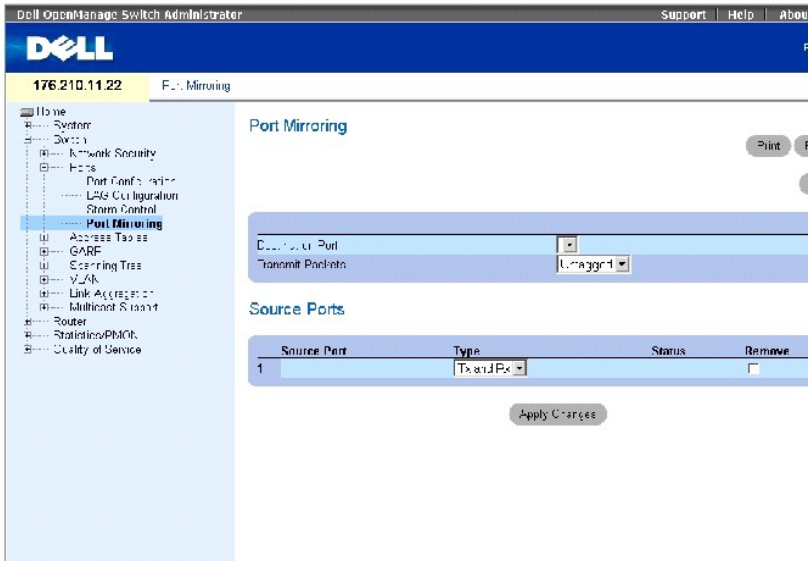
- Ports dürfen nicht als Quellport konfiguriert werden.
- Ports dürfen keine LAG-Komponente sein.
- IP-Schnittstellen dürfen nicht auf dem Port konfiguriert werden.
- GVRP darf nicht für den Port aktiviert werden.
- Der Port darf keine VLAN-Komponente sein.
- Es darf nur ein Zielport definiert sein.

Die folgenden Beschränkungen gelten für Ports, die als Quellports konfiguriert sind:

- Quellports dürfen keine LAG-Komponente sein.
- Ports dürfen nicht als Zielport konfiguriert werden.
- Alle Pakete werden mit Kennung (Tagging) vom Zielport aus übertragen.
- Alle TX-Pakete sollten von demselben Port aus überwacht werden.

Öffnen Sie die Seite **Port Mirroring** (Portspiegelung), indem Sie auf **Switch**→ **Ports**→ **Port Mirroring** in der *Strukturansicht* klicken.

Abbildung 7-16. Portspiegelung



Die Seite **Portspiegelung** enthält die folgenden Felder:

Destination Port (Zielport) Enthält eine Liste von Portnummern, von denen Portdatenverkehr kopiert werden kann.

Transmit Packets (Pakete übertragen) Legt fest, ob Pakete getagged oder ungetagged vom Zielport übertragen werden.

Source Port (Quellport) Portnummer, auf den der Portdatenverkehr gespiegelt wird.

Type Legt den Typ des gespiegelten Datenverkehrs fest. Mögliche Feldwerte sind:

TX Nur übertragene Pakete werden überwacht.

RX Nur empfangene Pakete werden überwacht.

TX and RX Sowohl übertragene als auch empfangene Pakete werden überwacht.

Status Gibt an, ob der Port gegenwärtig überwacht (**Active**) oder nicht überwacht (**Not Ready**) wird.

Remove (Entfernen) Wenn diese Option markiert ist, wird die Portspiegelungssitzung entfernt.

Hinzufügen einer Portspiegelungssitzung

1. Öffnen Sie die Seite **Port Mirroring** (Portspiegelung).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add Source Port** (Quellport hinzufügen) anzuzeigen.
3. Wählen Sie den Quellport aus dem Drop-Down-Menü **Source Port**.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die neue Portspiegelungssitzung wird für den Port aktiviert und das Gerät aktualisiert.

Bearbeiten einer Portspiegelungssitzung

1. Öffnen Sie die Seite **Port Mirroring** (Portspiegelung).
2. Ändern Sie die entsprechenden Felder.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Felder für die Portspiegelungssitzung werden geändert und das Gerät aktualisiert.

Löschen einer Portspiegelungssitzung

1. Öffnen Sie die Seite **Port Mirroring** (Portspiegelung).
2. Klicken Sie das Kontrollkästchen **Remove** (Entfernen) an.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Portspiegelungssitzung wird gelöscht und das Gerät aktualisiert.

Konfigurieren einer Portspiegelungssitzung mit den CLI-Befehlen

Die folgende Tabelle fast die entsprechenden CLI-Befehle für das Konfigurieren einer Portspiegelungssitzung, wie auf der Seite **Portspiegelung** angezeigt, zusammen.

Tabelle 7-11. CLI-Befehle zur Portspiegelung

CLI-Befehl	Beschreibung
`port monitor src-interface [rx | tx]`	Startet eine Portspiegelungssitzung.
`show ports monitor`	Zeigt den Status der Portüberwachung an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config-if)# port monitor g2
```

Konfigurieren von Adresstabellen

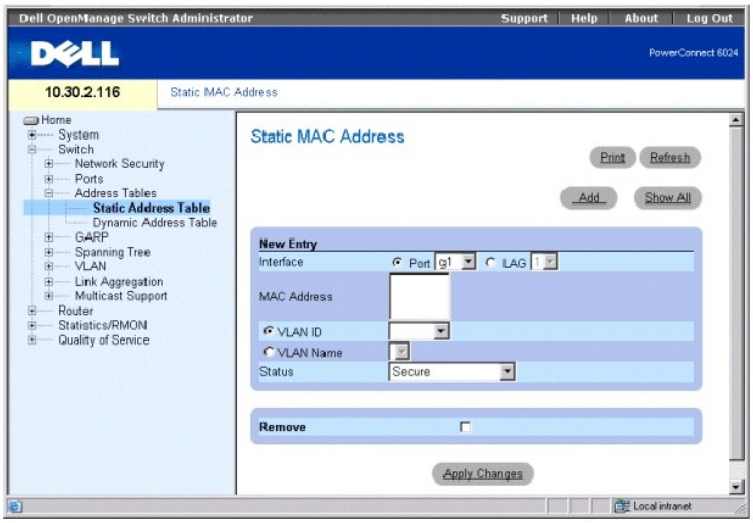
MAC-Adressen werden entweder in Datenbanken mit statischen oder mit dynamischen Adressen gespeichert. Statische werden durch den Benutzer festgelegt. Dynamische Adressen werden vom System ermittelt und dann nach einer Zeitüberschreitung gelöscht. Ein Paket mit einer in einer der Datenbanken gespeicherten Zieladresse wird sofort an den Port weitergeleitet. Die statischen und dynamischen Adresstabellen können nach Schnittstelle, VLAN und Schnittstellentyp sortiert werden. Darüber hinaus lassen sich Adressen zu den statischen und dynamischen Adresstabellen hinzufügen.

Öffnen Sie die Seite **Address Tables**, indem Sie auf **Switch→ Address Table** in der *Strukturansicht* klicken.

Definieren statischer Adressen

Die Seite **Static Address** (Statische Adresse) enthält eine Liste der MAC-Adressen. Eine statische Adresse kann in die Tabelle für statische MAC-Adressen eingefügt oder daraus entfernt werden. Um die Seite **Statische Adresse** zu öffnen, klicken Sie in der Strukturansicht auf **Switch→ Address Table→ Static Address**.

Abbildung 7-17. Statische MAC-Adresse



Interface Gibt den spezifischen Port bzw. LAG an, für die eine statische MAC-Adresse hinzugefügt wird.

MAC Address Die MAC-Adresse, die in der aktuellen Liste statischer Adressen aufgeführt ist.

ANMERKUNG: Nur MAC-Adressen, die der angegebenen Schnittstelle und dem VLAN zugeordnet sind, werden angezeigt. Um MAC-Adressen anzuzeigen, die einem unterschiedlichen VLAN zugeordnet sind, wählen Sie das VLAN aus der VLAN-Auswahlliste.

VLAN ID Gibt den Wert der mit der MAC-Adresse verknüpften VLAN-ID an.

VLAN Name Gibt den benutzerdefinierten VLAN-Namen an.

Status Der Status der MAC-Adresse. Die möglichen Werte sind:

Secure Stellt sicher, dass eine mit der Locked-Port-Sicherheitsoption konfigurierte MAC-Adresse nicht gelöscht wird.

Permanent Gibt an, dass es sich um eine dauerhafte MAC-Adresse handelt.

Delete on Reset Gibt an, dass die MAC-Adresse beim Zurücksetzen des Gerätes gelöscht wird.

Delete on Timeout Gibt an, dass die MAC-Adresse gelöscht wird, nachdem das Zeitlimit des Gerätes erreicht wurde.

Hinzufügen einer statischen MAC-Adresse

1. Öffnen Sie die Seite **Static MAC Address**.
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add Static MAC Address** (Statische MAC-Adresse hinzufügen) anzuzeigen.
3. Geben Sie die Informationen in den Feldern ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die neue statische Adresse wird der **Static MAC Address Table** hinzugefügt und das Gerät aktualisiert.

Ändern einer statischen Adresse in der Static MAC Address Table

1. Öffnen Sie die Seite **Static MAC Address**.
2. Ändern Sie die entsprechenden Felder.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die statische MAC-Adresse wird geändert und das Gerät aktualisiert.

Entfernen einer statischen Adresse aus der Static Address Table

1. Öffnen Sie die Seite **Static MAC Address**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **Static MAC Address Table** (Tabelle für statische MAC-Adressen) anzuzeigen.
3. Wählen Sie einen Tabelleneintrag.
4. Klicken Sie das Kontrollkästchen **Remove** (Entfernen) an.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die statische Adresse wird gelöscht und das Gerät aktualisiert.

Konfigurieren der Parameter statischer Adressen mit den CLI-Befehlen

Die folgende Tabelle fast die entsprechenden CLI-Befehle für das Konfigurieren der Parameter für die statische Adresse, wie auf der Seite **Statische MAC-Adresse** angezeigt, zusammen.

Tabelle 7-12. CLI-Befehle für statische Adressen

CLI-Befehl	Beschreibung
`bridge address mac-address {ethernet` *`interface`* `| port-channel` *`port-channel-number`*`}`	Fügt der Bridge-Tabelle die statische Quelladresse einer Station auf MAC-Layer hinzu.

[permanent | delete-on-reset | delete-on-timeout | secure]	
show bridge address-table static [vlan *vlan*] [ethernet *interface* | port-channel *port-channel-number*]	Zeigt statisch erstellte Einträge in der Datenbank für die Brückenweiterleitung an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface vlan 1 console

(config-vlan)# bridge address 3aa2.64b3.a245 ethernet g8 permanent....



Console (config-vlan)# exit

Console (config)#exit

Console> show bridge address-table static



Aging time is 300 sec



Vlan  Mac Address           Port   Type

----  --------------------  -----  ----------------------

1     3a:a2:64:b3:a2:45     g8     permanent
```

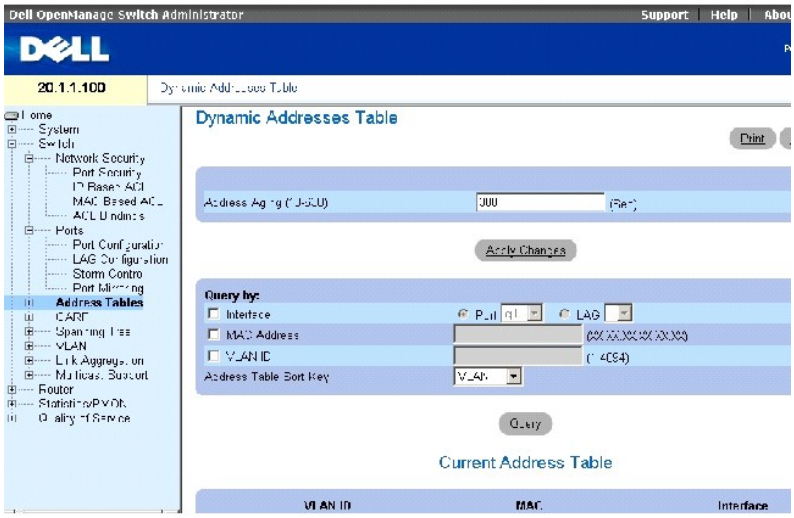
Anzeigen dynamischer Adressen

Die Tabelle **Dynamische Adressen** enthält Felder für die Abfrage von Informationen in derTabelle Dynamische Adressen", einschließlich des Schnittstellentyps, der MAC-Adresse, VLAN und des Schlüssels für die Tabellensortierung. Pakete, die an eine in der Adresstabelle gespeicherte Adresse weitergeleitet werden, werden direkt an diese Ports weitergeleitet.

Die Tabelle **Dynamische Adresse** enthält auch Informationen über den Zeitpunkt, zu dem eine dynamische MAC-Adresse aus der Tabelle entfernt wird.

Um die Tabelle **Dynamische Adresse** zu öffnen, klicken Sie in der Strukturansicht auf **Switch→ Address Tables→ Dynamic Addresses Table**.

Abb. 7-18. Tabelle dynamischer Adressen



Die Tabelle **Dynamische Adresse** enthält die folgenden Felder:

Address Aging (10-630) (Gültigkeitsdauer der Adresse) Legt den Zeitpunkt fest, zu dem eine dynamische MAC-Adresse gelöscht wird. Der Standardwert lautet 300 Sekunden.

Die Tabelle **Dynamische Adresse** kann auf folgende Arten angefragt werden:

Port Schnittstelle, von der eine Adresse abgefragt wird.

MAC Address Die MAC-Adresse, von der eine Adresse abgefragt wird.

VLAN ID Die VLAN-Nummer (zu der die MAC-Adresse gehört), von der eine Adresse abgefragt wird.

Address Table Sort Key (Sortierschlüssel der Adresstabelle) Legt fest, ob die Tabelle Dynamische Adresse" nach Adresse, VLAN oder Schnittstelle sortiert wird.

Definieren der Gültigkeitsdauer

1. Öffnen Sie die Seite **Dynamic Address Table** (Tabelle mit dynamischen Adressen).
2. Definieren Sie das Feld **Address Aging** (Adressgültigkeit).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Speicherdauer wird geändert und das Gerät aktualisiert.

Abfragen der Tabelle mit dynamischen Adressen.

1. Öffnen Sie die Seite **Dynamic Address Table** (Tabelle mit dynamischen Adressen).
2. Definieren Sie die Parameter, nach denen die **Dynamic Address Table** abgefragt wird.

Einträge können nach **Port**, **MAC-Adresse** oder **VLAN-ID** abgefragt werden.

3. Klicken Sie auf **Query** (Abfragen).

Die Tabelle mit dynamischen Adressen wird abgefragt.

Sortieren der Tabelle mit dynamischen Adressen

1. Öffnen Sie die Seite **Dynamic Address Table** (Tabelle mit dynamischen Adressen).
2. Wählen Sie im Drop-Down-Menü **Address Table Sort Key** aus, ob die Adressen nach Adresse, VLAN ID oder Schnittstelle geordnet werden sollen.
3. Klicken Sie auf **Query** (Abfragen).

Die Tabelle mit dynamischen Adressen wird sortiert.

Aktuelle Adresstabelle

DieCurrent Address Table (aktuelle Adresstabelle) enthält dynamische Adressparameter, gemäß denen Pakete direkt an die Ports weitergeleitet werden. Die aktuelle Adresstabelle enthält die folgenden Felder:

- **VLAN ID** Gibt den Wert des VLAN-Tags an.
- **MAC** Gibt die MAC-Adresse an.
- **Port** Gibt die Portnummer an.

Abfragen und Sortieren von dynamischen Adressen mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zum Abfragen und Sortieren dynamischer Adressen, wie auf der Seite **Dynamic Address Table** (Tabelle mit dynamischen Adressen) gezeigt, zusammen.

Tabelle 7-13. CLI-Befehle für Abfragen und Sortieren

CLI-Befehl	Beschreibung
`bridge aging-time` *seconds*	Stellt die Speicherdauer der Adresstabelle ein.
`show bridge address-table [vlan vlan] [ethernet` *interface* `| port-channel` *port-channel-number*`]`	Zeigt Klassen dynamisch erstellter Einträge in der Datenbank für die Bridge-Weiterleitung an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# bridge aging-time 300

Console (config)# exit

Console# show bridge address-table

Aging time is 300 sec

vlan   mac address      port    type

----   --------------   -----   -----
```

```
1       0060.704C.73FF   g8       dynamic

1       0060.708C.73FF   g8       dynamic

200     0010.0D48.37FF   g9       static
```

Konfigurieren von GARP

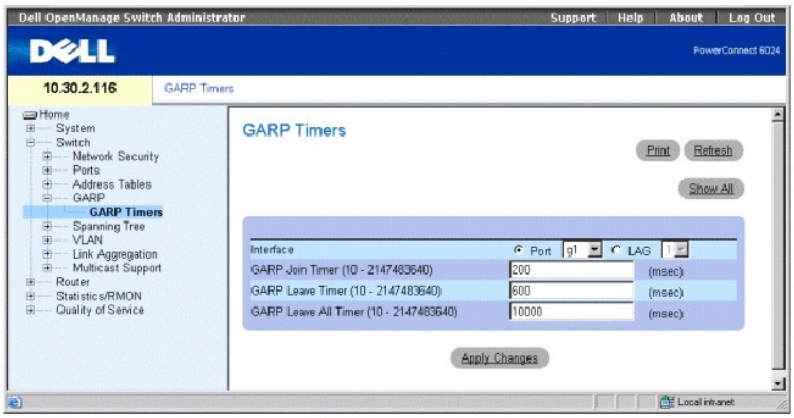
Das Generic Attribute Registration Protocol (GARP) ist ein Universalprotokoll, durch das beliebige Informationen zur Netzwerkkonnektivität und zum Mitgliedschaftstyp registriert werden. GARP definiert eine Reihe von Geräten, die an einem bestimmten Netzwerkattribut interessiert sind, wie etwa VLAN oder Multicast-Adresse.

Öffnen Sie die Seite **GARP**, indem Sie auf **Switch→ GARP** in der *Strukturansicht* klicken.

Definieren von GARP-Timern

Die Seite **GARP Timers** (GARP-Zeitgeber) enthält die Parameter für die Aktivierung von GARP auf dem Gerät. Öffnen Sie die Seite **GARP Timers**, indem Sie auf **Switch→ GARP→ GARP Timers** in der *Strukturansicht* klicken.

Abbildung 7-19. GARP-Timer



Die Seite **GARP-Zeitgeber** enthält die folgenden Felder:

Interface Legt fest, ob die Aktivierung für einen Port oder eine LAG gilt.

GARP Join Timer (10 - 2147483640) Gibt die Zeit für die Übertragung von PDUs in Millisekunden an. Der Wertebereich ist 10-2147483640. Der Standardwert ist 200 Millisekunden.

GARP Leave Timer (10 - 2147483640) Gibt die Zeit in Millisekunden an, die ein Gerät vor Beenden seines GARP-Status wartet. Die Leave-Time wird durch eine gesendete/empfangene Leave All Time-Nachricht aktiviert und durch die empfangene Join-Nachricht beendet. Die Leave-Zeit muss größer oder gleich der dreifachen Join-Zeit sein. Der Wertebereich ist 0-2147483640. Der Standardwert ist 600 Millisekunden.

GARP Leave All Timer (10 - 2147483640) Gibt die Zeit in Millisekunden an, die ein Gerät vor Beenden seines GARP-Status wartet. Die Leave-all-Zeit muss größer als die Leave-Zeit sein. Der Wertebereich ist 0-2147483640. Der Standardwert ist 10,000 Millisekunden.

Definieren von GARP-Timern

1. Öffnen Sie die Seite **GARP Timers**.
2. Geben Sie die Informationen in den Feldern ein.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die GARP-Parameter werden im Gerät gespeichert.

Kopieren von Parametern in die GARP Timers-Tabelle

1. Öffnen Sie die Seite **GARP Timers**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **GARP Timers Table** (GARP-Zeitgebertabelle) anzuzeigen.
3. Wählen Sie den Schnittstellentyp im Feld **Copy Parameters from** (Kopieren der Parameter von)
4. Wählen Sie eine Schnittstelle im Drop-Down-Menü **Port** oder **LAG**.
5. Die Definitionen für diese Schnittstelle werden auf die ausgewählten Schnittstellen kopiert. Siehe Schnitt 6.
6. Aktivieren Sie das Kontrollkästchen **Copy to** (Kopieren nach), um die Schnittstellen zu definieren, auf die die GARP-Zeitgebereinstellungen kopiert werden, oder klicken Sie auf **Select All** (Alle auswählen), um die Definitionen auf alle Ports oder LAGs zu kopieren.
7. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Parameter werden auf den ausgewählten Port oder LAGs in der GARP-Zeitgebertabelle kopiert und das Gerät aktualisiert.

Definieren von GARP-Zeitgebern mit den CLI-Befehlen

Die Tabelle 7-14 fast die entsprechenden CLI-Befehle für das Definieren von GARP-Zeitgebern, wie auf der Seite **GARP-Zeitgeber** angezeigt, zusammen.

Tabelle 7-14. CLI-Befehle für GARP-Timer

CLI-Befehl	Beschreibung
`garp timer {join | leave | leaveall} timer_value`	Legt die Join-, Leave- und Leaveall-GARP-Timer-Werte der GARP-Anwendung fest.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface ethernet g8

Console (config-if)# garp timer leave 900
```

Konfigurieren des Spanning Tree-Protokolls

Das Spanning Tree-Protokoll (STP) stellt eine Baumstruktur-Topologie für jede Brückenanordnung bereit. STP stellt auch einen einzelnen Pfad zwischen Endstationen in einem Netzwerk bereit und vermeidet so Netzwerkschleifen.

Schleifen treten immer dann auf, wenn alternative Routen zwischen Hosts existieren. Schleifen in einem erweiterten Netzwerk können dazu führen, dass Datenverkehr über Brücken auf unbegrenzte Zeit weitergeleitet wird, was zu erhöhtem Datenaufkommen und einer Minderung der Netzwerkleistung führt.

Das Gerät unterstützt die folgenden Spanning Tree-Versionen: Classic STP, Rapid STP und Multiple STP.

Classic STP bietet einen einzelnen Leitweg zwischen Endstationen und vermeidet so Netzwerkschleifen. Weitere Informationen über das Konfigurieren von Classic STP finden Sie unter **Definieren von globalen STP-Einstellungen**.

Rapid STP (RSTP) erfasst und verwendet Netzwerktopologien, die eine schnellere Konvergierung des Spanning-Tree ermöglichen, ohne dass Weiterleitungsschleifen geschaffen werden Weitere Informationen über das Konfigurieren von RSTP finden Sie unter **Definieren des Rapid Spanning Tree**.

Multiple STP (MSTP) ermöglicht volle Konnektivität für Pakete, die einem beliebigen VLAN zugeordnet sind. MSTP basiert auf RSTP. Darüber hinaus überträgt MSTP Pakete, die unterschiedlichen VLANs über unterschiedliche MST-Regionen zugeordnet sind. MST-Regionen fungieren als einzelne Brücke. MSTP erhöht die Fehltertoleranz des Systems und ermöglicht Lastenausgleich. Weitere Informationen über das Konfigurieren von MSTP finden Sie unter **Definieren des Multiple Spanning Tree**.

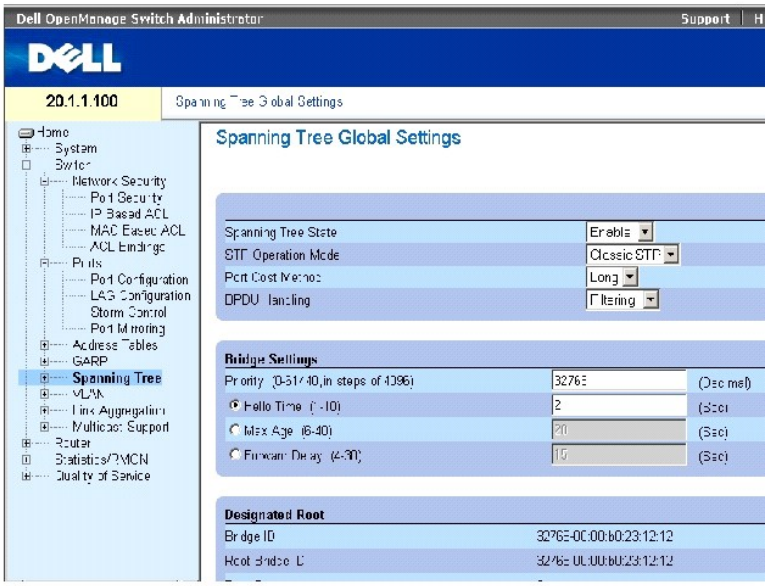
Öffnen Sie die Seite **Spanning Tree**, indem Sie auf **Switch→ Spanning Tree** in der *Strukturansicht* klicken.

Definieren globaler STP-Einstellungen

Die Seite **Spanning Tree Global Settings** (Globale Spanning Tree-Einstellungen) enthält Parameter für die Aktivierung von STP auf dem Gerät.

Um die Seite **Globale Spanning Tree-Einstellungen** zu öffnen, klicken Sie in der Strukturansicht auf **Switch→ Spanning Tree→ Global Settings**.

Abbildung 7-20. Globale Spanning Tree-Einstellungen



Die Seite **Globale Spanning Tree-Einstellungen** enthält die folgenden Felder:

Spanning Tree State (Status des Spanning Tree) Aktiviert oder deaktiviert STP, RSTP oder MSTP auf dem Gerät.

STP Operation Mode Gibt den STP-Modus an, nach dem STP für das Gerät aktiviert wird. Mögliche Feldwerte sind: **Classic STP**, **Rapid STP und Multiple STP**.

Path Cost Method (Pfadkostenmethode) Legt die Methode fest, die verwendet wird, um standardmäßige Pfadkosten STP-Ports zuzuweisen. Die möglichen Feldwerte sind:

Long (Lang) Pfadkostenmethode mit einen Bereich von 1-200.000.000.

Short (Kurz) Pfadkostenmethode mit einem Bereich von 1-65.535. Dies ist die Standardmethode.

Die standardmäßigen Pfadkosten, die auf eine Schnittstelle angewendet werden, können in Abhängigkeit von der ausgewählten Methode schwanken:

Schnittstelle	Long	Short
LAG	20.000	4
1.000 Mbps	20.000	4
100 Mbps	200.000	19
10 Mbps	2.000.000	100

BPDU Handling (BPDU-Bearbeitung) Legt die Bearbeitungsweise für BPDU-Pakete fest, wenn Spanning Tree auf einer Schnittstelle deaktiviert ist. Mögliche Feldwerte sind Filtering (Filtern) und Flooding (Überlaufen). Der Standardwert ist Flooding (Überlaufen).

Priority (0-65535) (Priorität (0-65535) Der Wert der Brückenpriorität. Wenn Switches oder Brücken STP ausführen, wird jedem Gerät eine Priorität zugewiesen. Nach dem Austausch von BPDUs wird der Switch mit der niedrigsten Priorität zur Stammbrücke. Der Standardwert lautet 32768.

Hello Time (1-10) (Hello-Zeit (1-10)) Die Hello-Zeit des Switch zeigt die Zeit (in Sekunden) an, die eine Root-Brücke zwischen zwei Konfigurationmeldungen wartet. Der Standardwert ist 2.

Max Age (6-40) (Maximales Speicherdauer (4-40) Die maximale Speicherdauer des Switch zeigt die Zeit (in Sekunden) an, die eine Brücke wartet, bevor eine topologische Änderung vorgenommen wird. Der Standardwert ist 20.

Forward Delay (4-30) (Weiterleitungsverzögerung 4-30) Die Weiterleitungsverzögerungszeit des Switch zeigt die Zeit (in Sekunden) an, die eine Brücke im Hör- und Lesestatus verbleibt, bevor Pakete weitergeleitet werden. Der Standardwert ist 15.

Bridge ID Die ID der Brücke.

Root Bridge ID Die ID des Root.

Root Port Portnummer, die den Pfad mit den geringsten Kosten von der Brücke zur Root-Brücke anbietet. Dies ist von Bedeutung, wenn die Brücke nicht die Stammbrücke ist. Der Standardwert lautet 0.

Root Path Cost (Root-Pfadkosten) Kosten des Pfads von der Brücke zum Root.

Topology Changes Counts (Letzte Topologieänderung) Gesamtzahl der Änderungen am STP-Status.

Last Topology Change (Letzte Topologieänderung) Zeit, die seit der letzten Topologieänderung vergangen ist. Die Zeit wird im Format Stunde/Minute/Sekunde angezeigt, z. B. 5 Stunden, 10 Minuten und 4 Sekunden.

Definieren der globalen STP-Parameter

1. Öffnen Sie die Seite **Globale Spanning Tree-Einstellungen**.
2. Wählen Sie aus dem Drop-Down-Menü **Select a Port** (Port auswählen) den zu aktivierenden Port aus.
3. Wählen Sie **Enable** im Feld **Spanning Tree State** aus.
4. Wählen Sie den Modus **STP** im Feld **STP Operation Mode** aus und definieren Sie die Bridge-Einstellungen.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

STP wird für das Gerät aktiviert.

Ändern von globalen STP-Parametern

1. Öffnen Sie die Seite **Globale Spanning Tree-Einstellungen**.
2. Definieren Sie die Felder im Dialogfeld.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die STP-Parameter werden geändert und das Gerät aktualisiert.

Definieren globaler STP-Parameter mit den CLI-Befehlen

Die folgende Tabelle fast die entsprechenden CLI-Befehle zum Definieren von globalen STP-Parametern, wie auf der Seite **Globale Spanning Tree-Einstellungen** angezeigt, zusammen.

Tabelle 7-15. CLI-Befehle für globale STP-Einstellungen

CLI-Befehl	Beschreibung
`spanning-tree`	Aktiviert die Spanning Tree-Funktion.
`spanning-tree mode {stp | rstp}`	Konfiguriert den Spanning Tree-Protokollmodus.
`spanning-tree pathcost method {long | short}`	Konfiguriert die Pfadkostenmethode des Spanning Tree.
`spanning-tree bpdu {filtering | flooding}`	Konfiguriert die Bearbeitung von BPDU-Paketen, wenn Spanning Tree auf einer Schnittstelle deaktiviert ist.
`spanning-tree priority` *`priority`*	Konfiguriert die Spanning Tree-Priorität.
`spanning-tree hello-time` *`seconds`*	Konfiguriert die Hello-Zeit der Spanning-Tree-Brücke. Diese gibt an, wie oft der Switch einen Broadcast von Hello-Meldungen an andere Switches durchführt.
`spanning-tree max-age` *`seconds`*	Konfiguriert die maximale Speicherdauer für die Spanning Tree-Bridge.
`spanning-tree forward-time` *`seconds`*	Konfiguriert die Weiterleitungszeit für die Spanning Tree-Bridge. Diese entspricht der Dauer, die ein Port vor Aktivierung des Weiterleitungsstatus im Überwachungs- und Erfassungsstatus verbleibt.
`show spanning-tree [ethernet` *`interface`* `| port-channel` *`port-channel-number`* `]`	Zeigt die Spanning Tree-Konfiguration an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# spanning-tree

Console (config)# spanning-tree mode rstp

Console (config)# spanning-tree priority 12288
```

```
Console (config)# spanning-tree hello-time 5

Console (config)# spanning-tree max-age 10

Console (config)# spanning-tree forward-time 25

Console (config)# exit

Console# show spanning-tree

Spanning tree enabled mode RSTP

Root ID Priority 32768

Address 0001.4297.e000

Cost 57

Port g1

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769

Address 0002.4b29.7a00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Number of topology changes 8 last change occurred 00:37:24 ago

Times: hold 1, topology change 35, notification 2

hello 2, max age 20, forward delay 15
```

Interface	Port ID				Designated		Port ID	
Name	Prio	Sts	Enb	Cost	Cost	Bridge Id	Prio.Nbr	
----	----	----	---	----	----	---- ---------	---	---

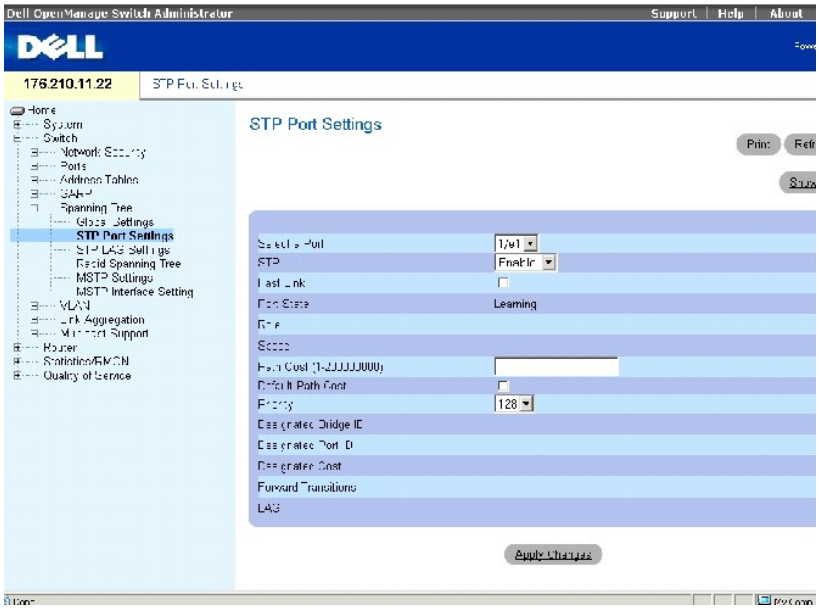
g1	128	DSBL	FALSE	100	0	8000	00:00:b0:70:09:00	80	001
g2	128	DSBL	FALSE	100	0	8000	00:00:b0:70:09:00	80	002
g3	128	DSBL	FALSE	100	0	8000	00:00:b0:70:09:00	80	003
ch1	128	DSBL	TRUE	4	0	8000	00:00:b0:70:09:00	80	019
ch2	128	DSBL	TRUE	4	0	8000	00:00:b0:70:09:00	80	01a
ch3	128	DSBL	TRUE	4	0	8000	00:00:b0:70:09:00	80	01b

Definieren von STP-Einstellungen für Ports

Auf der Seite **STP Port Settings** (STP-Schnittstelleneinstellungen) können Sie einzelnen Ports STP-Eigenschaften zuweisen.

Öffnen Sie die Seite **STP Port Settings** (STP-Porteinstellungen), indem Sie auf **Switch**→ **Spanning Tree**→ **Port Settings** (Porteinstellungen) in der *Strukturansicht* klicken.

Abbildung 7-21. STP-Porteinstellungen



Die Seite **STP-Porteinstellungen** enthält die folgenden Felder:

Select a Port Der Port, für den STP aktiviert wird.

STP Aktiviert/deaktiviert STP für den Port.

Fast Link Aktiviert, wenn ausgewählt, den Fast Link-Modus für den Port. Falls der Fast Link-Modus für einen Port aktiviert ist, wird der **Port** automatisch in den Weiterleitungsstatus versetzt, sobald die Portverbindung aktiv ist. Der Fast Link-Modus optimiert die Zeit, die zur Konvergierung des STP-Protokolls

erforderlich ist. Die STP-Konvergierung kann in großen Netzwerken 30 bis 60 Sekunden dauern.

Port State Zeigt den aktuellen STP-Status eines Ports an. Falls aktiviert, wird durch den Portzustand die Weiterleitungsaktion für den Datenverkehr bestimmt. Folgende Portzustände sind möglich:

Disabled (Deaktiviert) STP ist derzeit auf dem Port deaktiviert. Der Port leitet während des Erlernens von MAC-Adressen den Datenverkehr weiter.

Blocking Der Port ist derzeit blockiert und kann nicht für die Weiterleitung von Datenverkehr oder die Erfassung von MAC-Adressen verwendet werden.

Listening Der Port befindet sich derzeit im Überwachungsmodus. Der Port kann weder Datenverkehr weiterleiten noch MAC-Adressen erfassen.

Learning Der Port befindet sich derzeit im Erfassungsmodus. Der Port kann zwar keinen Datenverkehr weiterleiten, jedoch neue MAC-Adressen erfassen.

Forwarding Der Port befindet sich derzeit im Weiterleitungsmodus. Der Port kann Datenverkehr weiterleiten und neue MAC-Adressen erfassen.

Speed Gibt die Portgeschwindigkeit an.

Path Cost (1-200,000,000) (Pfadkosten (1-200.000.000) Die Beteiligung des Ports an den Root-Pfadkosten. Die Pfadkosten können an einen höheren oder niedrigeren Wert angepasst werden, und außerdem werden sie zur Weiterleitung des Datenverkehrs bei einem Pfad-Rerouting verwendet.

Default Path Cost (Standardpfadkosten) Zeigt an, dass die Standardpfadkosten entsprechend der auf der Seite Globale Spanning Tree-Einstellungen ausgewählten Methode zugeordnet werden.

Priority (0-240) (Priorität) Der Prioritätswert des Ports. Durch den Prioritätswert kann Einfluss auf die Portauswahl genommen werden, wenn eine Bridge über zwei Ports verfügt, die sich in einer Schleifenkonfiguration befinden.

Designated Bridge ID Die ID der festgelegten Brücke.

Designated Port ID Die ID des ausgewählten Ports.

Designated Cost Kosten der Teilnahme des Ports an der STP-Topologie. Bei Ports mit niedrigeren Kosten ist die Wahrscheinlichkeit einer Blockierung geringer, wenn STP Schleifen erfasst.

Forward Transitions (Transitions weiterleiten) Anzahl der Wechsel des Ports vom Status **Forwarding** (Weiterleiten) zum Status **Disabled** (Deaktiviert).

LAG Gibt die LAG an, mit der der Port verknüpft ist.

Aktivieren von STP für einen Port

1. Öffnen Sie die Seite **STP Port Settings** (STP-Porteinstellungen).
2. Wählen Sie **Enabled** im Feld **STP Port Status** (STP-Portstatus).
3. Definieren Sie die Felder **Fast Link**, **Path Cost** und **Priority**.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

STP wird für den Port aktiviert.

Ändern der STP-Eigenschaften für Ports

1. Öffnen Sie die Seite **STP Port Settings** (STP-Porteinstellungen).
2. Ändern Sie die Felder **Priority**, **Fast Link**, **Path Cost** und **Fast Link**.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die STP-Portparameter werden geändert und das Gerät aktualisiert.

Anzeigen der 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 geöffnet.

Definieren von STP-Portparametern mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Definition von STP-Portparametern, wie auf der Seite **STP Port Settings** (STP-Porteinstellungen) angezeigt, zusammen.

Tabelle 7-16. CLI-Befehle für STP-Porteinstellungen

CLI-Befehl	Beschreibung
`spanning-tree disable`	Deaktiviert Spanning Tree für einen spezifischen Port.
`spanning-tree cost` *`cost`*	Konfiguriert die Spanning Tree-Pfadkosten für einen Port.
`spanning-tree port-priority` *`priority`*	Konfiguriert die Portpriorität.
`show spanning-tree [ethernet interface | port-channel` *`port-channel-number`*`]`	Zeigt die Spanning Tree-Konfiguration an.
`spanning-tree portfast`	Aktiviert den PortFast-Modus.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface ethernet g5

Console (config-if)# spanning-tree disable

Console (config-if)# spanning-tree cost 35000

Console (config-if)# spanning-tree port-priority 96

Console (config-if)# spanning-tree portfast

Console (config-if)# exit
```

```
Console (config)# exit
```

```
Console# show spanning-tree ethernet g1
```

Schnittstelle	Port ID	Designated			Port ID
Name	Prio.Nbr	Cost	Sts	Kosten-Brücken-ID	Prio.Nbr
--------	-------	---	--	-------------------	------
g1	128.1	19	FWD	38 32768 0030.9441.62c1	128.25

```
Spanning tree enabled
```

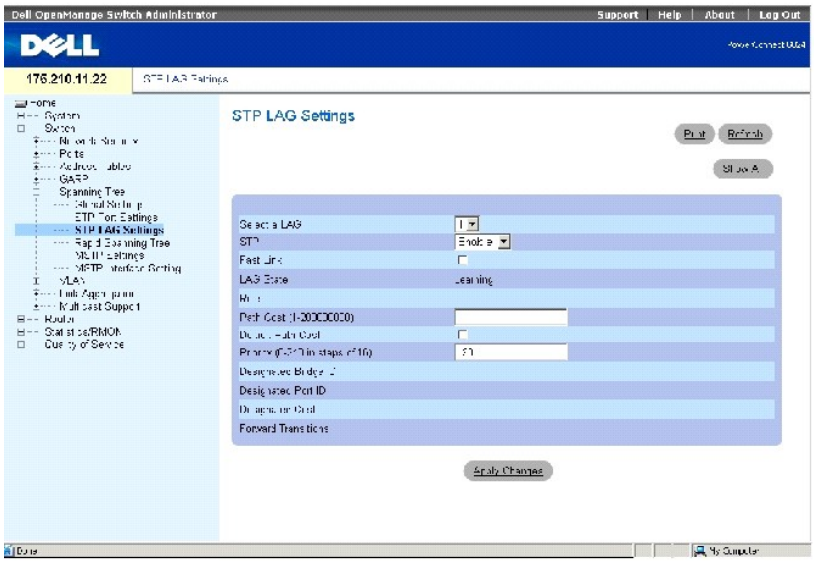
```
Type: point-to-point (configured: auto)
```

```
Port Fast: no (configured: no)
```

Definieren von STP-Einstellungen für LAGs

Auf der Seite **STP LAG Settings** (STP-LAG-Einstellungen) können Sie gebündelten Ports STP-Parameter zuweisen. Öffnen Sie die Seite **STP LAG Settings**, indem Sie auf **Switch→ Spanning Tree→ LAG Settings** in der *Strukturansicht* klicken.

Abbildung 7-22. STP-Einstellungen für LAGs



Die Seite **STP-Einstellungen für LAGs** enthält die folgenden Felder:

Select a LAG (Eine LAG auswählen) Die LAG-Nummer, für die STP-Einstellungen geändert werden sollen.

STP Aktiviert/deaktiviert STP für die LAG.

Fast Link Aktiviert den Fast Link-Modus für die LAG. Falls der Fast Link-Modus für eine LAG aktiviert ist, wird der **Port** automatisch in den Weiterleitungsstatus versetzt, sobald die LAG-Verbindung aktiv ist. Der Fast Link-Modus optimiert die Zeit, die zur Konvergierung des STP-Protokolls erforderlich ist. Die STP-Konvergierung kann in großen Netzwerken 30 bis 60 Sekunden dauern.

LAG State Gibt den aktuellen STP-Status für eine LAG an. Falls aktiviert, wird durch den LAG-Status die Weiterleitungsaktion für den Datenverkehr bestimmt. Wenn die Bridge eine fehlerhaft arbeitende LAG identifiziert, wird die LAG in den Status **Broken** versetzt. Folgende LAG-Zustände sind möglich:

Disabled (Deaktiviert) STP ist derzeit auf dem LAG nicht aktiviert. Die LAG leitet während des Erlernens von MAC-Adressen Datenverkehr weiter.

Blocking Die LAG ist derzeit blockiert und kann nicht für die Weiterleitung von Datenverkehr oder die Erfassung von MAC-Adressen verwendet werden.

Listening Die LAG befindet sich derzeit im Überwachungsmodus und ist nicht in der Lage, Datenverkehr weiterzuleiten oder MAC-Adressen zu erfassen.

Learning Die LAG befindet sich derzeit im Erfassungsmodus und kann zwar keinen Datenverkehr weiterleiten, jedoch neue MAC-Adressen erfassen.

Forwarding Die LAG befindet sich derzeit im Weiterleitungsmodus und kann Datenverkehr weiterleiten und neue MAC-Adressen erfassen.

Broken Die LAG ist derzeit defekt und kann nicht für die Weiterleitung von Datenverkehr verwendet werden.

Path Cost (1-200000000) Gibt an, welchen Anteil diese LAG an den Root-Pfadkosten hat. Die Pfadkosten können an einen höheren oder niedrigeren Wert angepasst werden, und außerdem werden sie zur Weiterleitung des Datenverkehrs bei einem Pfad-Rerouting verwendet.

Default Path Cost (Standardpfadkosten) Zeigt an, dass die Standardpfadkosten entsprechend der auf der Seite Globale Spanning Tree-Einstellungen ausgewählten Methode zugeordnet werden.

Priority (0-240) (Priorität) Der Prioritätswert der LAG. Durch den Prioritätswert kann Einfluss auf die LAG-Auswahl genommen werden, wenn eine Bridge über zwei Ports verfügt, die sich in einer Schleifenkonfiguration befinden. Der Prioritätswert liegt zwischen 0 und 240, in Schritten von 16.

Designated Bridge ID Die ID der festgelegten Brücke.

Designated Port ID Die ID des ausgewählten Ports.

Designated Cost Kosten der Teilnahme des Ports an der STP-Topologie. Bei Ports mit niedrigeren Kosten ist die Wahrscheinlichkeit einer Blockierung geringer, wenn STP Schleifen erfasst.

Forward Transitions (Transitions weiterleiten) Anzahl der Wechsel des **LAG-Status** von **Forwarding** (Weiterleiten) zum Status **Disabled** (Deaktiviert).

Ändern der STP-Parameter für LAGs:

1. Öffnen Sie die Seite **STP LAG Settings**.
2. Wählen Sie eine LAG aus dem Drop-Down-Menü **Select a LAG** aus.
3. Ändern Sie die Felder wie gewünscht.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die STP-Parameter der LAG werden geändert und das Gerät aktualisiert.

Definieren von STP-Einstellungen für LAGs mit den CLI-Befehlen

Die folgende Tabelle enthält CLI-Befehle für das Definieren von STP-LAG-Einstellungen.

Tabelle 7-17. CLI-Befehle für STP-Einstellungen für LAGs

CLI-Befehl	Beschreibung
`spanning-tree`	Aktiviert die Spanning Tree-Funktion.
`spanning-tree cost` *`cost`*	Konfiguriert die Spanning Tree-Pfadkosten für einen Port.
`spanning-tree port-priority` *`priority`*	Konfiguriert die Portpriorität.
`show spanning-tree [ethernet interface | port-channel` *`port-channel-number`*`]`	Zeigt die Spanning Tree-Konfiguration an.
`spanning-tree portfast`	Aktiviert den PortFast-Modus.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface port-channel 1

Console (config-if)# spanning-tree disable

Console (config-if)# spanning-tree cost 35000

Console (config-if)# spanning-tree port-priority 96

Console (config-if)# spanning-tree portfast

Console (config-if)# exit

Console (config)# exit

Console# show spanning-tree port-channel 1

Interface Port ID Designated Port ID

Name   Prio  Sts    Enb    Cost   Cost   Bridge Id               Prio.Nbr

------ ----  ------ -----  ------ ------ ----------------------  ----------------
ch1    96    DSBL   FALSE  35000  0      32768 00:00:b0:11:00:00  96
```

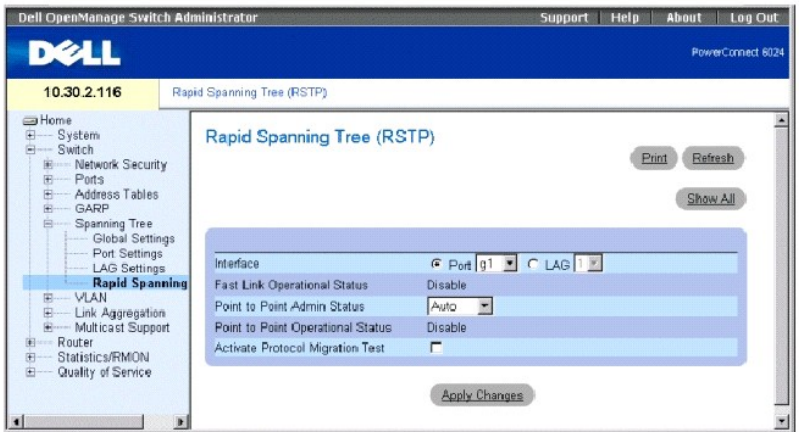
```
Spanning tree disabled


Port Fast: yes (configured: yes)


Type: point-to-point (configured: auto)


Number of transitions to forwarding state: 0
```

Definieren des Rapid Spanning Tree (RSTP)

Obwohl die klassischen Spanning Tree Schicht-2-Weiterleitungsschleifen in einer allgemeinen Netzwerktopologie verhindern, kann die Konvergenz 30 bis 60 Sekunden dauern. Die Verzögerung gibt auch Gelegenheit zur Erkennung möglicher Schleifen und zur Verbreitung von Statusänderungen.

Das Rapid Spanning Tree Protocol (RSTP) erkennt und verwendet Netzwerktopologien, die eine schnellere Konvergenz des Spanning Tree ermöglichen, ohne dass Weiterleitungsschleifen erstellt werden müssen. Öffnen Sie die Seite Rapid Spanning Tree (RSTP)", indem Sie auf **Switch→ Spanning Tree→ Rapid Spanning Tree** in der *Strukturansicht* klicken.

Abbildung 7-23. Rapid Spanning Tree (RSTP)



Interface Gibt die Nummer des Ports oder der LAG an, für die RSTP aktiviert wird.

Fast Link Operational Status Gibt an, ob Fast Link für den Port oder die LAG aktiviert oder deaktiviert ist. Wenn Fast Link für einen Port aktiviert ist, wird der Port automatisch in den Weiterleitungszustand versetzt.

Point-to-Point Admin Status Aktiviert/deaktiviert die Fähigkeit des Geräts zur Herstellung einer Punkt-zu-Punkt-Verbindung oder legt die automatische Herstellung einer Punkt-zu-Punkt-Verbindung für das Gerät fest.

Zur Herstellung von Kommunikation über eine Punkt-zu-Punkt-Verbindung sendet die Quell-PPP zuerst Link Control Protocol (LCP)-Pakete zur Konfiguration und Testen der Datenverbindung. Nachdem eine Verbindung hergestellt wurde und optionale Einrichtungen gemäß den Erfordernissen des LCP ausgehandelt wurden, sendet das Quell-PPPNetwork Control Protocols (NCP)-Pakete zur Auswahl und Konfiguration eines oder mehrer Netzwerk-Layer-Protokolle aus. Wenn jedes der gewählten Netzwerk-Layer-Protokolle konfiguriert wurde, können Pakete von jedem Netzwerk-Layer-Protokoll über die Verbindung übertragen werden. Die Verbindung bleibt solange für die Kommunikation konfiguriert, bis explizite LCP- oder NCP-Pakete die Verbindung schließen oder irgendein externes Ereignis auftritt. Dies ist der tatsächliche Verbindungsporttyp des Switch Sie kann vom Verwaltungszustand abweichen.

Point-to-Point Operational Status Gibt den Punkt-zu-Punkt-Betriebsstatus an.

Activate Protocol Migration Test (Protokollmigrationstest aktivieren) Wenn diese Option ausgewählt ist, wird PPP zum Senden von Link Control Protocoll-Paketen (LPC) aktiviert, um den Data-Link konfigurieren und testen zu können.

Aktivieren von Rapid STP

1. Öffnen Sie die Seite Rapid Spanning Tree (RSTP).
2. Definieren Sie die Felder **Point-to-Point Admin**, **Point-to-Point Oper** und **Activate Protocol Migration**.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das Rapid STP wird geändert und das Gerät aktualisiert.

Anzeigen der Rapid Spanning Tree (RSTP)-Tabelle

1. Öffnen Sie die Seite Rapid Spanning Tree (RSTP).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die Seite **Rapid Spanning Tree (RSTP) Table** wird geöffnet.

Definieren von Rapid STP-Parametern mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für die Definition der Rapid STP-Parameter auf der Seite **RSTP** zusammen.

Tabelle 7-18. CLI-Befehle für RSTP-Einstellungen

CLI-Befehl	Beschreibung
`spanning-tree link-type {point-to-point | shared}`	Setzt die Einstellung für den Standardverbindungstyp außer Kraft.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface ethernet g5

Console (config-if)# spanning-tree link-type shared
```

Definieren des Multiple Spanning Tree

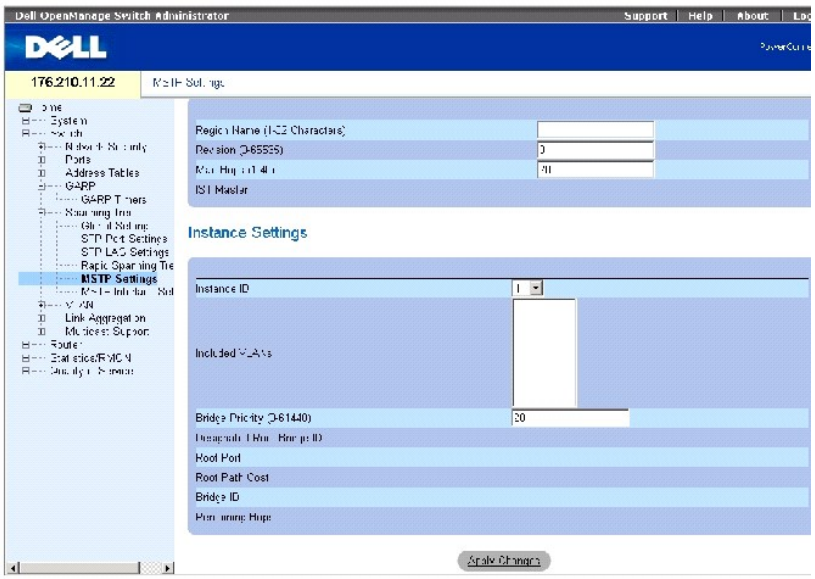
Der Betrieb über das Multiple Spanning Tree-Protokoll (MSTP) verknüpft VLANs mit STP-Instanzen.

MSTP ermöglicht ein anderes Ladeausgleichsszenario. Wenn beispielsweise Port A in einer STP-Instanz blockiert ist, wird der gleiche Port in den Weiterleitungsstatus einer anderen STP-Instanz überführt. Die Seite **MSTP-Einstellungen** ermöglicht Ihnen, bis zu 16 MSTP-Instanzen für das Gerät zu definieren.

Darüber hinaus werden Pakete, die verschiedenen VLANs zugeordnet sind, auf verschiedenen Pfaden innerhalb von Multiple Spanning Tree-Regionen (MST-Regionen) übertragen. Unter Regionen versteht man eine oder mehrere miteinander verbundene Multiple Spanning Tree-Brücken mit identischer MSTP-Konfiguration. Durch das Konfigurieren einer MST wird die MST-Region, zu der Ihr Gerät gehört, definiert. Eine Konfiguration besteht aus Name, Version und der Region, zu der Ihr Gerät gehört.

Um die Seite **MSTP-Einstellungen** zu öffnen, klicken Sie in der Strukturansicht auf **Switch**→ **Spanning Tree**→ **MSTP Region Configuration**.

Abbildung 7-24. MSTP-Einstellungen



Die Seite **MSTP-Einstellungen** enthält die folgenden Felder, die in zwei Abschnitte unterteilt sind:

Region Name (1-32) Zeigt einen benutzerdefinierten MST-Regionsnamen an.

Revision (0-65535) (Version) Zeigt eine unsignierte 16-Bit-Nummer an, die die Version der aktuellen MST-Konfiguration anzeigt. Die Versionsnummer wird als Teil der MST-Konfiguration benötigt.

Max Hops (1-40) (Maximale Anzahl an Hops) Gibt die maximale Anzahl an Hops an, die in einer bestimmten Region auftreten, bevor die BPDU abgelehnt wird. Sobald die BPDU abgelehnt wurde, werden die Portdaten gelöscht. Der Standardwert des Feldes ist 20.

IST Master Zeigt die interne Master ID des Spanning Tree an. Der IST Master ist der Root der ausgewählten Instanz, und seine Instanz ist 0.

Instance ID Legt die ID der Spanning Tree-Instanz fest. Mögliche Feldwerte sind 1-15.

Included VLANs (Eingeschlossene VLANs) Verknüpft die ausgewählten VLANs mit der ausgewählten Instanz. Jeder VLAN gehört zu nur einer Instanz.

Bridge Priority (0-61440) (Brückenpriorität) Legt die Priorität des Geräts für die ausgewählte Spanning Tree-Instanz fest.

Designated Root Bridge ID (Festgelegte ID der Root-Brücke) Zeigt die ID der Brücke mit den niedrigsten Pfadkosten zum Instanz-Root an.

Root Port Zeigt den Root-Port der ausgewählten Instanz an.

Root Path Cost (Root-Pfadkosten) Zeigt die Pfadkosten der ausgewählten Instanz zum Regions-Root an.

Bridge ID (Brücken-ID) Zeigt die Brücken-ID der ausgewählten Instanz an.

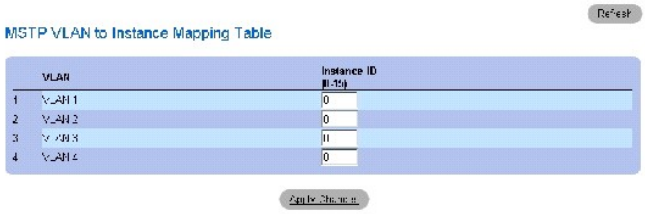
Remaining Hops (Verbleibende Hops) Zeigt die Anzahl der Hops an, die bis zum nächsten Ziel verbleiben.

Anzeigen der MSTP-VLAN-an-Instanz-Zuweisungstabelle

1. Öffnen Sie die Seite **MSTP-Einstellungen**.
2. Klicken Sie auf **Show All"** (Alles anzeigen).

Die Seite **MSTP-VLAN-an-Instanz-Zuweisungstabelle** wird geöffnet:

Abbildung 7-25. MSTP-VLAN-an-Instanz-Zuweisungstabelle



Definieren von MST-Instanzen mithilfe von CLI-Befehlen

Die folgende Tabelle fast die entsprechenden CLI-Befehle zum Definieren von MST-Instanz-Gruppen, wie auf der Seite **MSTP-Einstellungen** angezeigt, zusammen.

Tabelle 7-19. CLI-Befehle für MSTP-Instanzen

CLI-Befehl	Beschreibung
`spanning-tree mst configuration`	Startet den MST-Konfigurationsmodus.
`instance instance-id {add | remove} vlan vlan-range`	Verknüpft VLANs mit der MST-Instanz.
`name string`	Legt den Konfigurationsnamen fest.
`revision value`	Legt die Versionsnummer der Konfiguration fest.
`spanning-tree mst instance-id port- priority priority`	Legt die Portpriorität fest.
`spanning-tree mst instance-id priority priority`	Legt die Gerätepriorität für die ausgewählte Spanning Tree-Instanz fest.
`spanning-tree mst max- hops hop-count`	Legt die Anzahl an Hops in einer MST-Region fest, bevor BPDU abgelehnt wird und die für den Port bereitgehaltenen Informationen gelöscht werden.
`spanning-tree mst instance-id cost cost`	Legt die Pfadkosten des Port für die MST-Berechnung fest.
`exit`	Beendet den MST-Konfigurationsmodus und wendet die Konfigurationsänderungen an.
`abort`	Beendet den MST-Konfigurationsmodus, ohne die Konfigurationsänderungen anzuwenden.

show {current | pending}	Zeigt die aktuelle oder in der Schwebe befindliche Konfiguration der MST-Region an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# spanning-tree mst configuration

Console (config-mst)# instance 1 add vlan 10-20

Console (config-mst)# name region1

Console (config-mst)# revision 1

Console (config)# spanning-tree mst configuration

Console (config-mst)# instance 2 add vlan 21-30

Console (config-mst)# name region1

Console (config-mst)# revision 1

Console (config-mst)# show pending
```

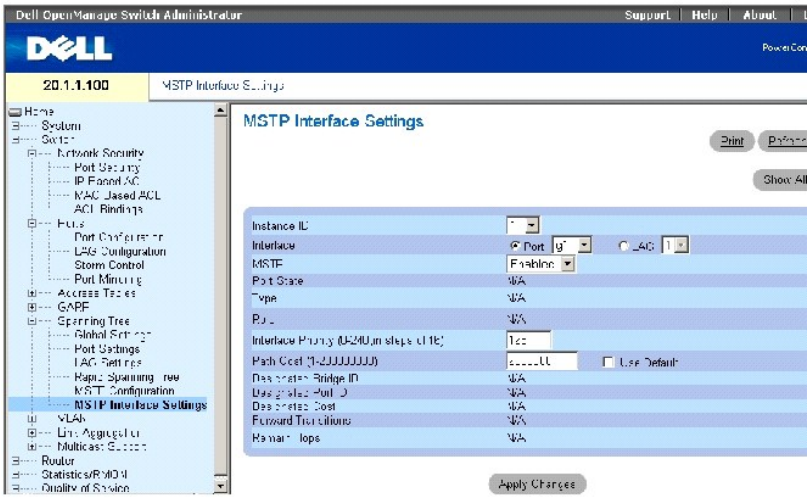
In der Schwebe befindliche MST-Konfiguration	
Name: Region1	
Revision: 1	
Instance	Vlans Mapped
--------	----------
0	1-9,31-4094
1	10-20
2	21-30

Definieren von MSTP-Schnittstellen-Einstellungen

Auf der Seite **MSTP-Schnittstellen-Einstellungen** können Sie MSTP-Einstellungen auf bestimmte Schnittstelle anwenden.

Um die Seite **MSTP-Schnittstellen-Einstellungen** zu öffnen, klicken Sie in der Strukturansicht auf **Switch→ Spanning Tree→ MSTP Interface Setting**.

Abbildung 7-26. MSTP-Schnittstellen-Einstellungen



Die Seite **MSTP-Schnittstellen-Einstellungen** enthält die folgenden Parameter:

Instance ID Listet die MSTP-Instanzen auf, die auf dem Gerät konfiguriert sind. Mögliche Feldwerte sind 0-15.

Interface Vergibt entweder einen Port oder eine LAG auf die ausgewählte MSTP-Instanz.

Port State Zeigt an, ob der Port in der ausgewählten Instanz aktiviert oder deaktiviert ist.

Type Zeigt an, ob MSTP den Port als Punkt-zu-Punkt-Port betrachtet oder als Port, der mit einem Hub verbunden ist. Außerdem wird angezeigt, ob es sich bei diesem Port um einen internen Port der MST-Region handelt oder um einen angrenzenden Port Wenn es dich um einen angrenzenden Port handelt, wird außerdem angezeigt, ob das Gerät auf der anderen Seite des Links im RSTP- oder im STP-Modus arbeitet.

Role Gibt die Rolle des Ports an, die vom STP-Algorithmus zur Bereitstellung von STP-Pfaden zugewiesen wird. Die möglichen Feldwerte sind:

Root Stellt den Pfad mit den niedrigsten Kosten zur Weiterleitung von Paketen an das Root-Gerät bereit.

Designated Zeigt den Port oder die LAG an, über die das designierte Gerät mit dem LAN verbunden ist.

Alternate Stellt einen alternativen Pfad zum Root-Gerät von der Schnittstelle bereit.

Backup Ermöglicht einen Backup-Pfad zum ausgewählten LAN. Backup-Ports gibt es nur dann, wenn zwei Ports in einer Schleife über einen Punkt-zu-Punkt-Link verbunden sind. Backup-Ports treten auch dann auf, wenn in einem LAN mindestens zwei Verbindungen zu einem gemeinsamen Segment anliegen.

Disabled Gibt an, dass der Port kein Bestandteil des Spanning Tree ist.

Interface Priority (Schnittstellenpriorität) Legt die Schnittstellenpriorität für die ausgewählte Instanz fest. Der Prioritätsbereich liegt bei 0-240, aufgeteilt in 16er-Schritten. Der Standardwert ist 128.

Path Cost (Pfadkosten) Zeigt die Beteiligung des Ports an der Spanning Tree-Instanz an. Der Bereich sollte immer von 1-200.000.000 gehen.

Default Path Cost (Standardpfadkosten) Zeigt an, dass die Standardpfadkosten entsprechend der auf der Seite Globale Spanning Tree-Einstellungen ausgewählten Methode zugeordnet werden.

Designated Bridge ID (Designierte Brücken-ID) Die Nummer der Brücken-ID, die den Link oder das freigegebene LAN mit dem Root verbindet.

Designated Port ID (Designierte Port-ID) Die Nummer der Port-ID auf der designierten Brücke, die den Link oder das freigegebene LAN mit dem Root verbindet.

Designated Cost (Designierte Kosten) Kosten des Pfads vom Link oder dem freigegebenen LAN zum Root.

Forward Transitions (Transitions weiterleitet) Anzahl der Wechsel des Ports in den **Weiterleitungsstatus**.

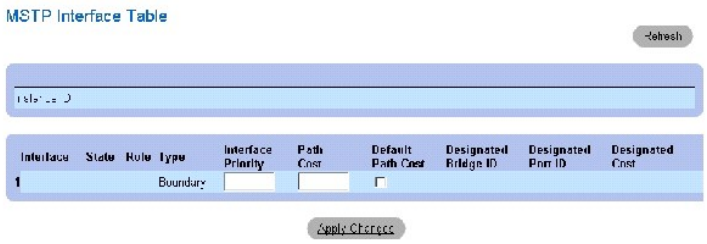
Remain Hops (Verbleibende Hops) Zeigt die Anzahl an Hops an, die bis zum nächsten Ziel verbleiben.

Anzeigen der MSTP-Schnittstellentabelle

1. Öffnen Sie die Seite **MSTP-Schnittstellen-Einstellungen**.
2. Klicken Sie auf **Show All"** (Alles anzeigen).

Die Seite **MSTP-Schnittstellentabelle** wird geöffnet:

Abbildung 7-27. MSTP-Schnittstellentabelle



Definieren von MSTP-Schnittstellen mithilfe von CLI-Befehlen

Die folgende Tabelle fast die entsprechenden CLI-Befehle zum Definieren von MSTP-Schnittstellen, wie auf der Seite **MSTP-Schnittstellen-Einstellungen** angezeigt, zusammen.

Tabelle 7-20. CLI-Befehle für die MSTP-Schnittstelle

CLI-Befehl	Beschreibung
`spanning-tree mst instance-id cost cost`	Legt die Pfadkosten des Ports für MST-Berechnungen fest.
`spanning-tree mst instance-id priority priority`	Legt die Geräteprioriät für die ausgewählte ST-Instanz fest.
`show spanning-tree mst- configuration`	Zeigt die MST-Konfiguration an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface ethernet g9

Console (config-if) # spanning-tree mst 1 cost 4

Console (config-if)# spanning-tree mst 1 port-priority 142

Console (config-if)# end

Console# show spanning-tree

Spanning tree enabled mode MSTP

Default port cost method: long

###### MST 0 Vlans Mapped: 1-9, 21-4094

CST Root ID Priority 32768

Address 00:01:42:97:e0:00

Path Cost 20000

Root Port 1 (ig)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

IST Master ID Priority 32768

Address 00:02:4b:19:7a:00

Path Cost 10000

Rem hops 19

Bridge ID Priority 32768

Address 00:02:4b:29:7a:00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

Max hops 20

Konfigurieren von VLANs

Bei VLANs handelt es sich um logische Untergruppen innerhalb eines LAN, die mit Software erstellt wurden, anstatt eine Hardwarelösung zu definieren. VLANs verbinden Benutzerstationen und Netzwerkgeräte zu einer einzelnen Einheit, unabhängig vom physischen LAN-Segment, mit dem sie verbunden sind. VLANs schaffen die Voraussetzung für einen effizienteren Netzdatenverkehrsfluss durch Untergruppen. Per Software verwaltete VLAN verkürzen den Zeitraum, der für die Implementierung von Änderungen, Erweiterungen und Verschiebungen benötigt wird.

VLANs besitzen keine minimale Anzahl von Ports und können pro Einheit, Gerät, Stack oder einer anderen logischen Verbindungskombination erstellt werden, da VLANs softwarebasiert sind und nicht von physischen Attributen definiert werden.

VLANs funktionieren auf der Schicht 2. Da VLANs den Datenverkehr innerhalb des VLAN isolieren, wird ein Schicht-3-Router, der auf Protokollebene arbeitet, benötigt, um den Fluss von Datenverkehr zwischen VLANs zu ermöglichen. Layer 3-Router dienen zur Identifikation von Segmenten und kooperieren mit VLANs. VLANs sind Broadcast- und Multicast-Domäne. Broadcast- und Multicast-Datenverkehr wird nur in dem VLAN übertragen, in dem der Datenverkehr generiert wird.

VLAN-Kennungen bieten eine Methode, um VLAN-Informationen zwischen VLAN-Gruppen zu übertragen. Beim VLAN-Tagging wird ein 4-Byte-Tag an den Paketheader angehängt. Die VLAN-Kennung gibt das VLAN an, dem das Paket angehört. Das Anhängen von VLAN-Tags an das VLAN erfolgt entweder durch die Datenendstelle oder durch ein Netzwerkgerät. VLAN-Kennungen enthalten darüber hinaus Informationen zur Priorität von VLAN-Netzwerken.

Die Kombination von VLANs und GVRP ermöglicht Netzwerkmanagern die Definition von Netzwerkknoten innerhalb Broadcast-Domänen. Broadcast- und Multicast-Datenverkehr ist auf die Ursprungsgruppe beschränkt.

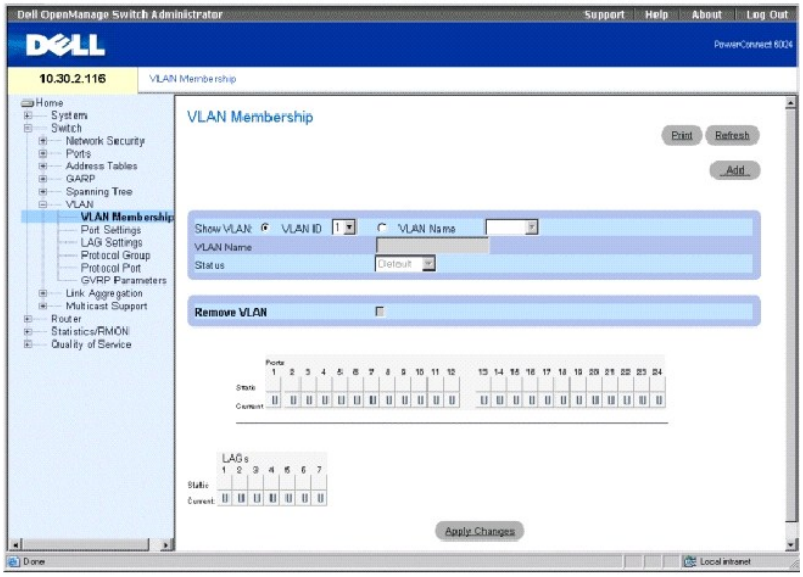
Um die Seite **VLAN** anzuzeigen, klicken Sie in der Strukturansicht auf **Switch**→ **VLAN**.

Definieren von VLAN-Mitgliedschaften

Auf der Seite **VLAN Membership** (VLAN-Mitgliedschaft) können Sie VLAN-Gruppen definieren.

Öffnen Sie die Seite **VLAN Membership**, indem Sie auf **Switch**→ **VLAN**→ **VLAN Membership** in der *Strukturansicht* klicken.

Abb. 7-28. VLAN-Komponenten



Die Seite **VLAN-Mitgliedschaft** ist in die VLAN-Mitgliedschaftstabelle und die VLAN-Port-Mitgliedschaftstabelle unterteilt.

VLAN-Mitgliedschaftstabelle

Der Bereich **VLAN Membership Table** enthält Parameter für die Zuweisung der VLAN-Mitgliedschaft zu Ports. Ihr Switch unterstützt bis zu 4095 VLANs. Tatsächlich können Sie jedoch aus folgenden Gründen nur 4062 VLANs erstellen:

- VLANs 4064 bis 4094 werden vom Gerät für den internen Betrieb reserviert.
- VLAN 1 ist das Standard-LAN, bei dem alle Ports standardmäßig Mitglieder sind.
- VLAN 4095 ist als Discard VLAN" bestimmt.

Show VLAN Listet spezifische VLAN-Informationen nach VLAN-ID oder VLAN-Name auf und zeigt sie an.

VLAN Name Zeigt den benutzerdefinierten VLAN-Namen an.

Status Zeigt den VLAN-Typ an. Die möglichen Werte sind:

Dynamic Zeigt an, dass VLAN dynamisch über GVRP erstellt wurde.

Static Zeigt an, dass das VLAN benutzerdefiniert ist.

Remove VLAN (VLAN entfernen) Wenn diese Option ausgewählt ist, wird das VLAN aus der VLAN-Mitgliedschaftstabelle entfernt.

Hinzufügen neuer VLANs

1. Öffnen Sie die Seite **VLAN Membership**.
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Create New VLAN** (Neues virtuelles LAN) zu erstellen.
3. Geben Sie die VLAN ID und den VLAN-Namen ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das neue VLAN wird hinzugefügt und das Gerät aktualisiert.

Ändern von VLAN-Mitgliedschaftsgruppen

1. Öffnen Sie die Seite **VLAN Membership**.
2. Wählen Sie ein VLAN im Drop-Down-Menü **Show VLAN** aus.
3. Ändern Sie die Felder wie gewünscht.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die VLAN-Membership-Informationen werden geändert und das Gerät aktualisiert.

Löschen von VLAN-Mitgliedschaftsgruppen

1. Öffnen Sie die Seite **VLAN Membership**.
2. Wählen Sie ein VLAN im Feld **Show VLAN** aus.
3. Aktivieren Sie das Kontrollkästchen **Remove VLAN** (VLAN entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das VLAN wird entfernt und das Gerät aktualisiert.

Definieren von VLAN-Mitgliedschaftsgruppen mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für die Definition der VLAN-Mitgliedschaftsgruppen auf der Seite **VLAN Membership** (VLAN-Mitgliedschaft) zusammen.

Tabelle 7-21. CLI-Befehle für VLAN-Mitgliedschaftsgruppen

CLI-Befehl	Beschreibung
`vlan database`	Ruft den Schnittstellenkonfigurationsmodus (VLAN) auf.
`vlan {`*`vlan-range`*`}`	Erstellt ein VLAN.
`name` *`string`*	Fügt einem VLAN einen Namen hinzu.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface vlan 1972
```

```
Console (config-if)#name Marketing
```

VLAN-Port-Mitgliedschaftstabelle

Der Bereich **VLAN Port Membership Table** enthält eine **Porttabelle** für die Zuweisung von Ports zu VLANs. Ports wird eine VLAN-Mitgliedschaft zugewiesen, indem die Einstellungen unter **Port Control** (Portsteuerung) geändert werden. Ports können über die folgenden Werte verfügen:

Tabelle 7-22. VLAN-Port-Mitgliedschaftstabelle

Port-Kontrolle	Definition
T	Die Schnittstelle ist ein Mitglied eines VLANs. Alle über die Schnittstelle weitergeleiteten Pakete verfügen über eine Kennung. Die Pakete enthalten VLAN-Informationen.
U	Die Schnittstelle gehört dem VLAN an. Über die Schnittstelle weitergeleitete Pakete besitzen keine Kennung.
F	Der Schnittstelle wird die Mitgliedschaft in einem VLAN verweigert.
Keine	Die Schnittstelle gehört diesem VLAN nicht an. Mit der Schnittstelle verknüpfte Pakete werden nicht weitergeleitet.

Im Bereich **VLAN Port Membership Table** werden die Ports, ihr Status sowie die LAGs angezeigt.

Zuweisen von Ports zu einer VLAN-Gruppe

1. Öffnen Sie die Seite **VLAN Membership** (VLAN-Mitgliedschaft).
2. Klicken Sie auf die Optionsschaltfläche **VLAN ID** oder **VLAN Name** und wählen Sie ein VLAN aus dem Drop-Down-Menü aus.
3. Wählen Sie einen Port in der **Port Membership Table** und weisen Sie dem Port einen Wert zu.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Port wird der VLAN-Gruppe zugewiesen und das Gerät wird aktualisiert.

Löschen von VLANs

1. Öffnen Sie die Seite **VLAN Membership.**
2. Klicken Sie auf die Optionsschaltfläche **VLAN ID** oder **VLAN Name** und wählen Sie ein VLAN aus dem Drop-Down-Menü aus.
3. Aktivieren Sie das Kontrollkästchen **Remove VLAN** (VLAN entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das VLAN wird entfernt und das Gerät aktualisiert.

Zuweisen von Ports zu VLAN-Gruppen mit den CLI-Befehlen

Die folgende Tabelle beinhaltet die CLI-Befehle für die Zuweisung von Ports zu VLAN-Gruppen.

Tabelle 7-23. CLI-Befehle für die Zuweisung von Ports zu VLAN-Gruppen

CLI-Befehl	Beschreibung
`switchport general acceptable-frame-types tagged-only`	Aktiviert die Eingangsfilterung für Frames ohne Kennung.
`switchport forbidden vlan {add`*`vlan-list`* `| remove `*`vlan-list`*`}`	Verhindert das Hinzufügen spezifischer VLANs zum Port.

Im Folgenden werden CLI-Befehle an Hand eines Beispiels dargestellt:

```
Console (config)# interface ethernet g1
```

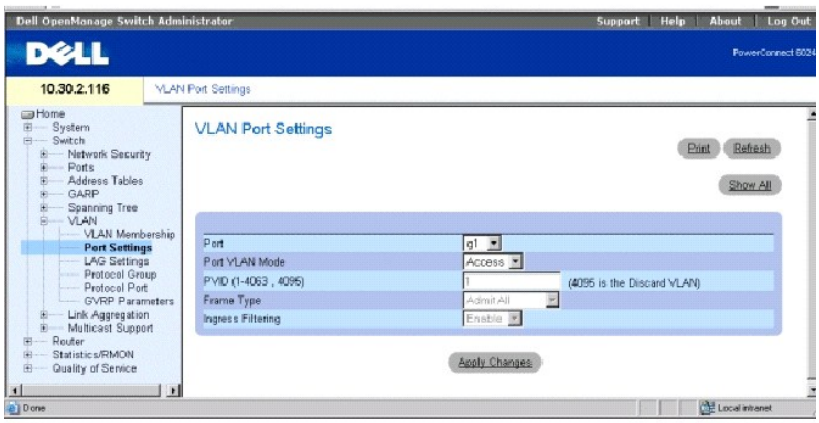
```
Console (config-if)#switchport general acceptable-frame-types tagged-only


Console (config-if)#switchport forbidden vlan add 234-256
```

Definieren von VLAN-Einstellungen für Ports

Auf der Seite **VLAN Port Settings** (VLAN-Porteinstellungen) geben Sie Parameter für die Verwaltung von Ports ein, die Teil eines VLANs sind. Die Standard-VLAN-ID (PVID) wird auf der Seite **VLAN Port Settings** konfiguriert. Alle über das Gerät eingehenden Pakete ohne Kennung werden mit der PVID des Ports versehen.

Öffnen Sie die Seite **VLAN Port Settings**, indem Sie auf **Switch→ VLAN→ Port Settings** in der *Strukturansicht* klicken.

Abbildung 7-29. VLAN-Einstellungen für Ports



Port Die Nummer des Ports, der Teil des VLAN ist.

Port VLAN Mode Gibt den Portmodus an. Die möglichen Werte sind:

General Gibt an, dass der Port VLANs angehört und dass jedes VLAN vom Benutzer als VLAN mit oder ohne Kennung definiert wurde (voller 802.1Q-Modus).

Access Gibt an, dass der Port zu einem einzelnen VLAN ohne Kennung gehört. Wenn sich eine Schnittstelle im Zugangsmodus befindet, können die Pakettypen, die auf dem Port (Pakettyp) akzeptiert werden, nicht festgelegt werden. Es ist weiterhin nicht möglich, die Eingangsfilterung auf einem Zugangsport zu aktivieren/deaktivieren.

Trunk Gibt an, dass der Port VLANs angehört, in der alle Ports über eine Kennung verfügen (mit Ausnahme von einem optionalen nativen VLAN).

PVID (1-4063, 4095) Vergibt eine VLAN-ID für nicht gekennzeichnete Pakete. Die möglichen Werte sind 1 bis 4063 und 4095. VLAN 4095 wird standardmäßig und branchenüblich als Discard VLAN" definiert. In diesem VLAN klassifizierte Pakete werden verworfen.

Frame Type Der am Port akzeptierte Frametyp. Die möglichen Werte sind:

Admit Tag Only (Nur Tag zulassen) Zeigt an, dass nur gekennzeichnete Frames auf dem Port akzeptiert werden.

Admit All (Alle akzeptieren) Zeigt an, dass sowohl gekennzeichnete als auch nicht gekennzeichnete Frames auf dem Port akzeptiert werden.

Ingress Filtering Aktiviert/deaktiviert die Eingangsfilterung für den Port. Durch Eintrittsfilterung (Ingress filtering) werden Frames abgelehnt, bei denen der VLAN-Tag mit keinem Port-VLAN übereinstimmt.

Zuweisen von Porteinstellungen

1. Öffnen Sie die Seite **VLAN Port Settings** (VLAN-Einstellungen für Ports).
2. Wählen Sie aus dem Drop-Down-Menü **Port** den Port aus, dem Sie Einstellungen zuweisen möchten.
3. Vervollständigen Sie die verbleibenden Felder auf der Seite und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die VLAN-Portparameter werden definiert und das Gerät aktualisiert.

Anzeigen der VLAN Porttabelle

1. Öffnen Sie die Seite **VLAN Port Settings**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **VLAN Port Table** (VLAN-Porttabelle) anzuzeigen.

ANMERKUNG: Falls ein **Zugangs** port ausgewählt wird, lassen sich die Pakettypen, die auf dem Port (Pakettyp) akzeptiert werden, nicht festlegen. Es ist weiterhin nicht möglich, die Eingangsfilterung auf einer Zugangsport zu aktivieren bzw. zu deaktivieren.

Zuweisen von Ports zu VLAN-Gruppen mit den CLI-Befehlen

Die folgende Tabelle beinhaltet die CLI-Befehle für die Zuweisung von Ports zu VLAN-Gruppen.

Tabelle 7-24. CLI-Befehle für VLAN-Ports

CLI-Befehl	Beschreibung
`switchport mode {access | trunk | general}`	Konfiguriert den VLAN-Mitgliedschaftsmodus für einen Port.
`switchport trunk native vlan vlan-id`	Definiert den Port als Mitglied des angegebenen VLAN und die VLAN ID als die port default VLAN ID (PVID)".
`switchport general pvid vlan-id`	Konfiguriert die PVID (Port VLAN ID), während sich die Schnittstelle im allgemeinen Modus befindet.
`switchport general allowed vlan add vlan- list [tagged | untagged]`	Entfernt oder fügt VLANs zu einem allgemeinen Port hinzu.
`switchport general acceptable-packet-types tagged-only`	Aktiviert die Eingangsfilterung für Frames ohne Kennung.
`switchport general ingress-filtering disable`	Deaktiviert die Eingangsfilterung für einen Port.
`Shutdown`	Deaktiviert Schnittstellen.
`set interface active {ethernet interface | port-channel port-channel-number }`	Reaktiviert eine Schnittstelle, die aus Sicherheitsgründen deaktiviert wurde.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

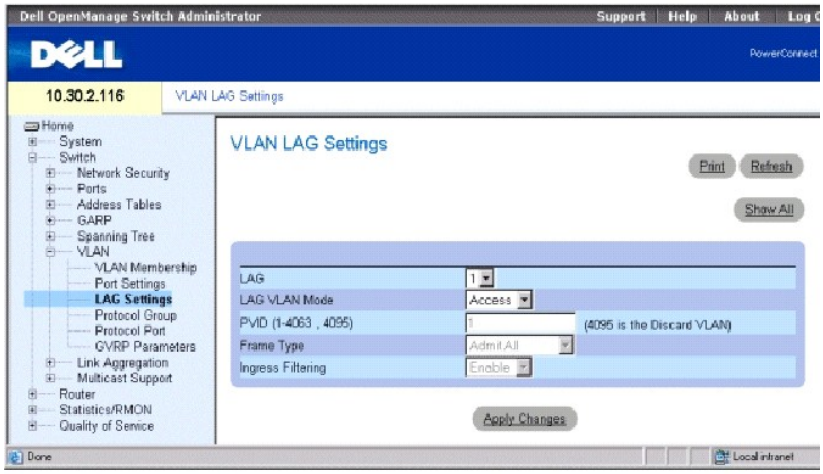
```
Console (config)# interface ethernet g8
```

```
Console (config-if)# switchport mode access


Console (config-if)# switchport trunk native vlan 123


Console (config-if)# switchport general pvid 234


Console (config-if)# switchport general allowed vlan add 1,2,5,6 tagged


Console (config-if)# switchport general acceptable-packet-types tagged-only
```

Definieren von VLAN-Einstellungen für LAGs

Die Seite **VLAN LAG Settings** (VLAN-LAG-Einstellungen) enthält Parameter für die Verwaltung von LAGs, die Teil eines VLANs sind. VLANs setzen sich entweder aus einzelnen Ports oder LAGs zusammen. Pakete ohne Tags, die das Switch erreichen, werden mit LAG-Kennungen versehen, die vom PVID festgelegt sind. Um die Seite **VLAN-Einstellungen für LAGs** zu öffnen, klicken Sie in der Strukturansicht auf **Switch→ VLAN→ LAG Settings**.

Abbildung 7-30. VLAN-Einstellungen für LAGs



LAG Gibt die Nummer der im VLAN enthaltenen LAG an.

LAG VLAN Mode Gibt den VLAN-LAG-Modus an. Die möglichen Werte sind:

General Gibt an, dass die LAG VLANs angehört und dass jedes VLAN vom Benutzer als VLAN mit oder ohne Kennung definiert wird (voller 802.1Q-Modus).

Access Gibt an, dass die LAG zu einem einzelnen VLAN ohne Kennung gehört.

Trunk Gibt an, dass die LAG VLANs angehört, in der alle Ports über eine Kennung verfügen (mit Ausnahme von einem einzigen optionalen nativen VLAN).

PVID (1-4063, 4095) Vergibt eine VLAN-ID für nicht gekennzeichnete Pakete. Die möglichen Feldwerte sind 1 bis 4063 und 4095. VLAN 4095 wird

standardmäßig und branchenüblich als „Discard VLAN" definiert. In diesem VLAN klassifizierte Pakete werden verworfen.

Frame Type Gibt den von der LAG akzeptierten Pakettyp an. Die möglichen Werte sind:

Admit Tag Only Gibt an, dass nur Pakete mit Kennung von der LAG akzeptiert werden.

Admit All Gibt an, dass Pakete sowohl mit als auch ohne Kennung von der LAG akzeptiert werden.

Ingress Filtering Aktiviert/deaktiviert die Eingangsfilterung für die LAG. Durch Eintrittsfilterung (Ingress filtering) werden Pakete abgelehnt, bei denen der VLAN-Tag mit keinem LAG-VLAN übereinstimmt.

Zuweisen von VLAG-Einstellungen

1. Öffnen Sie die Seite **VLAN LAG Settings** (VLAN-LAG-Einstellungen).
2. Wählen Sie eine LAG aus dem Drop-Down-Menü **LAG** und geben Sie die Informationen in den Feldern auf der Seite ein.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die VLAN-Parameter der LAG werden geändert 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), um die **VLAN LAG Table** (VLAN-LAG-Tabelle) anzuzeigen.

Zuweisen von LAGs zu VLAN-Gruppen mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für die Zuweisung von LAGs zu VLAN-Gruppen auf der Seite **VLAN LAG Settings** (VLAN-LAG-Einstellungen) zusammen.

Tabelle 7-25. CLI-Befehle für die Zuweisung von LAGs zu VLAN-Gruppen

CLI-Befehl	Beschreibung
`switchport mode {access | trunk | general}`	Konfiguriert den VLAN-Mitgliedschaftsmodus für einen Port.
`switchport trunk native vlan vlan-id`	Definiert den Port als Mitglied des angegebenen VLAN und die VLAN ID als die „port default VLAN ID (PVID)".
`switchport general pvid vlan-id`	Konfiguriert die PVID (Port VLAN ID), während sich die Schnittstelle im allgemeinen Modus befindet.
`switchport general allowed vlan add vlan-list [tagged | untagged]`	Entfernt oder fügt VLANs zu einem allgemeinen Port hinzu.
`switchport general acceptable-frame-type tagged-only`	Aktiviert die Eingangsfilterung für Frames ohne Kennung.
`switchport general ingress-filtering disable`	Deaktiviert die Eingangsfilterung für einen Port.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

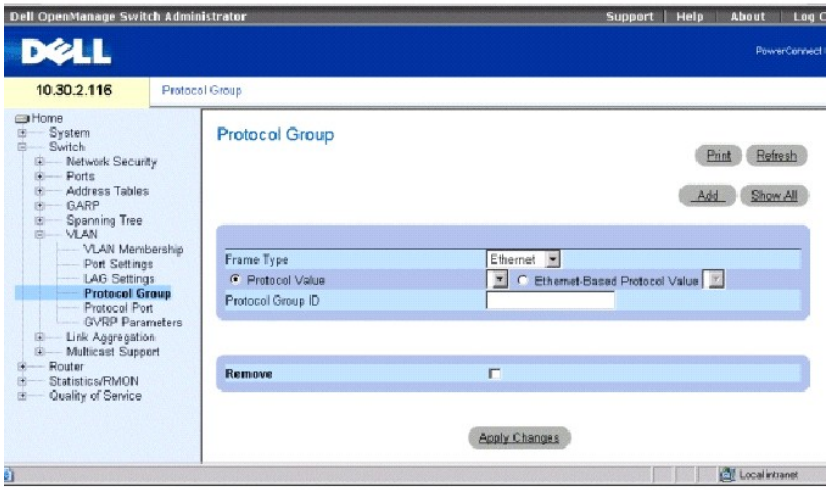
```
Console (config-if)# switchport mode access
```

```
Console (config-if)# switchport trunk native vlan 123


Console (config-if)# switchport general pvid 234


Console (config-if)# switchport general allowed vlan add 1,2,5,6 tagged


Console (config-if)# switchport general acceptable-frame-type tagged-only
```

Definieren von VLAN-Protokollgruppen

Die Seite **Protokollgruppe** enthält Informationen über Protokollnamen und den VLAN-Ethernet-Typ. Schnittstellen lassen sich als eine spezifische protokollbasierte Schnittstelle klassifizieren. Durch die Klassifizierung wird die Schnittstelle in eine Protokollgruppe gesetzt. Um die Seite **Protokollgruppe** zu öffnen, klicken Sie in der Strukturansicht auf **Switch**→ **VLAN**→ **Protocol Group**.

Abbildung 7-31. Protokollgruppentabelle



Frame Type Gibt den Pakettyp an. Mögliche Feldwerte sind **Ethernet**, **RFC1042** und **LLC Other**.

Protocol Value Gibt den benutzerdefinierten Protokollnamen an.

Ethernet-Based Protocol Value Gibt den Typ der Ethernet-Protokollgruppe an.

Protocol Group ID Gibt die ID-Nummer der VLAN-Gruppe an.

Hinzufügen einer Protokollgruppe

1. Öffnen Sie die Seite **Protocol Group**.
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Protokoll zur Gruppe zuordnen** anzuzeigen.
3. Vervollständigen Sie die Felder auf der Seite und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Protokollgruppe wird zugewiesen und das Gerät wird aktualisiert.

Zuweisung von VLAN-Protokollgruppeneinstellungen

1. Öffnen Sie die Seite **Protocol Group**.
2. Vervollständigen Sie die Felder auf der Seite und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die VLAN-Protokollgruppen-Parameter werden definiert und das Gerät aktualisiert.

Entfernen von Protokollen aus der Protokollgruppentabelle

1. Öffnen Sie die Seite **Protocol Group**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **Protocol Group Table** (Protokollgruppentabelle) anzuzeigen.
3. Aktivieren Sie für die zu entfernenden Protokollgruppen das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das Protokoll wird entfernt und das Gerät wird aktualisiert.

Definieren von VLAN-Protokollgruppen mit den CLI-Befehlen

Die folgende Tabelle enthält die entsprechenden CLI-Befehle zur Konfiguration von Protokollgruppen.

Tabelle 7-26. CLI-Befehle für VLAN-Protokollgruppen

CLI-Befehl	Beschreibung
`map protocol protocol [encapsulation] protocols -group group`	Fügt einer benannten Protokollgruppe ein spezielles Protokoll hinzu, das für die protokollbasierte VLAN-Zuweisung verwendet werden kann.

Im folgenden Beispiel wird das ip-arp-Protokoll der Gruppe „213" zugeordnet:

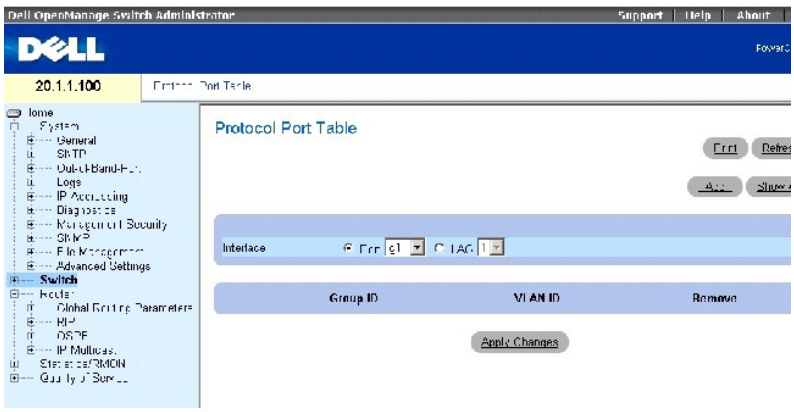
```
Console (config)# vlan database

Console (config-vlan)# map protocol ip-arp protocols-group 213
```

Hinzufügen von Protokollports

Auf der Seite **Protokollport** können Sie Schnittstellen zu Protokollgruppen hinzufügen.

Öffnen Sie die Seite **Protocol Port** (Protokollport), indem Sie auf **Switch→ VLAN→ Protocol Port** in der *Strukturansicht* klicken.

Abbildung 7-32. Protokollport



Interface Gibt die einer Protokollgruppe hinzugefügte Port- oder LAG-Nummer an.

Protocol Group ID (Protokollgruppen-ID) Gibt die Protokollgruppen-ID an, der die Schnittstelle hinzugefügt wird. Protokollgruppen-IDs werden in der Protokollgruppentabelle definiert.

VLAN ID Verbindet die Schnittstelle mit einer benutzerdefinierten VLAN-ID an. Die VLAN ID wird auf der Seite **Create a New VLAN** definiert. Protokollports können entweder einerVLAN ID oder einem VLAN-Namen angefügt werden.

VLAN Name Verbindet die Schnittstelle mit einem benutzerdefinierten VLAN-Namen. Der VLAN-Name wird auf der Seite **Create a New VLAN** (Neues VLAN erstellen) definiert. Dieses Feld ist nur auf der Seite **Add Protocol Port** (Protokollport hinzufügen) verfügbar.

Remove (Entfernen) Wenn diese Option ausgewählt ist, wird die Portzuordnung vom VLAN oder der Protokollgruppe entfernt.

Hinzufügen eines neuen Protokollports

1. Öffnen Sie die Seite **Protocol Port Table** (Protokollporttabelle).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add Protocol Port** (Protokollport hinzufügen) anzuzeigen.
3. Füllen Sie die Felder in dem Dialogfeld aus und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die neue VLAN-Protokollgruppe wird der **Protocol Port Table** (Protokollporttabelle) hinzugefügt und das Gerät wird aktualisiert.

Definieren von Protokollports mit den CLI-Befehlen

Die folgende Tabelle enthält CLI-Befehle für das Definieren von Protokollports.

Tabelle 7-27. CLI-Befehle für Protokollports

CLI-Befehl	Beschreibung
`switchport general map protocols-group group vlan vlan- id`	Richtet eine protokollbasierte Klassifizierungsregel ein.

Das folgende Beispiel stellt eine protokollbasierte Klassifizierungsregel von Protokollgruppe 1 auf VLAN 8 ein:

```
Console (config-if)# switchport general map protocols-group 1 vlan 8
```

Konfigurieren von GVRP

Das GARP VLAN Registration Protocol (GVRP) ist speziell für die automatische Verteilung von VLAN-Mitgliedschaftsinformationen an VLAN-orientierte Bridges konzipiert. Mittels GVRP können VLAN-orientierte Bridges VLANs automatisch erfassen und Portzuweisungen ohne Konfiguration einzelner Bridges überbrücken sowie die VLAN-Mitgliedschaft registrieren.

Zur Minimierung der Speicheranforderung bei der Ausführung des GVRP-Protokolls wurden die Standardvariablen um zwei proprietäre Optimierungstabellen erweitert:

- **Maximum number of GVRP VLANs** (Maximale Anzahl der GVRP-VLANs) Maximale Anzahl der GVRP-VLANs wird für die Optimierung verwendet.
- **Maximum number of GVRP VLANs after Reset** (Maximale Anzahl von GVRP-LANs nach dem Zurücksetzen) Maximale Anzahl von GVRP-VLANs nach dem Zurücksetzen wird für die Optimierung verwendet. Dieser Wert wird nur nach dem Zurücksetzen gültig.

Die maximale Anzahl von GVRP-VLANs beinhaltet alle VLANs, die bei der GVRP-Optimierung beteiligt sind, unabhängig davon, ob sie statisch oder dynamisch sind.

Folgendes sollte bei der Angabe der maximalen Anzahl der VLAN, die am GVRP teilnehmen, berücksichtigt werden (indem ein Wert für Maximale Anzahl der GVRP-VLANs nach dem Zurücksetzen" eingestellt wird):

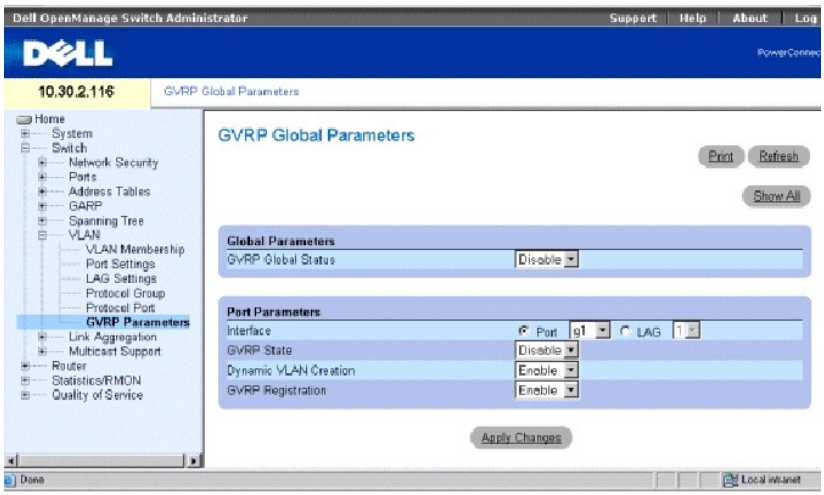
- Die maximale Anzahl der GVRP VLANs entspricht standardmäßig 255.
- Die maximale Anzahl der VLANs (verwaltet durch die Variable Max VLANs MIB") beschränkt die maximale Anzahl der GVRP-VLANs.

Um eine korrekte Operation des GVRP-Protokolls sicherzustellen, stellen Sie die maximale Anzahl der GVRP-VLANs auf einen Wert ein, der die Summe folgender Elemente wesentlich überschreitet:

- Die Anzahl aller statischen VLANs, die bereits ordnungsgemäß konfiguriert sind oder demnächst konfiguriert werden.
- Die Anzahl aller dynamischen VLANs, die am GVRP teilnehmen, die sowohl aktuell konfiguriert sind (Ausgangszahl der dynamischen GVRP-VLANs beträgt 255) und noch konfiguriert werden sollen.

Auf der Seite **GVRP Global Parameters** kann GVRP global aktiviert werden. GVRP kann auch für einzelne Schnittstellen aktiviert werden. Öffnen Sie die Seite **GVRP Global Parameters** (globale GVRP-Parameter), indem Sie auf **Switch→ VLAN→ GVRP Parameters** in der *Strukturansicht* klicken.

Abbildung 7-33. Globale GVRP-Parameter



GVRP Global Status Aktiviert/deaktiviert GVRP für das Gerät. GVRP ist standardgemäß deaktiviert.

Interface Gibt die Nummer des Ports oder der LAG an, für die GVRP aktiviert wird.

GVRP State Aktiviert/deaktiviert GVRP für eine Schnittstelle.

Dynamic VLAN Creation Aktiviert/deaktiviert die VLAN-Erstellung über GVRP.

GVRP Registration Zeigt den Status der GVRP-Registrierung.

Aktivieren von GVRP für das Gerät

1. Öffnen Sie die Seite **GVRP Global Parameters**.
2. Wählen Sie **Enable** im Feld **GVRP Global Status**.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

GVRP wird für das Gerät aktiviert.

Aktivieren der VLAN-Registration über GVRP

1. Öffnen Sie die Seite **GVRP Global Parameters**.
2. Wählen Sie **Enable** im Feld **GVRP Global Status** für die gewünschte Schnittstelle aus.
3. Wählen Sie **Enable** im Feld **GVRP Registration** aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die VLAN-Registrierung über GVRP wird für den Port aktiviert und das Gerät wird aktualisiert.

Konfigurieren von GVRP mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für die Konfiguration von GVRP auf der Seite **GVRP Global Parameters** (Globale GVRP-Einstellungen) zusammen.

Tabelle 7-28. CLI-Befehle für globale GVRP-Parameter

CLI-Befehl	Beschreibung
`gvrp enable (global)`	Aktiviert GVRP global.
`gvrp enable (interface)`	Aktiviert GVRP für eine Schnittstelle.
`gvrp vlan-creation-forbid`	Aktiviert/deaktiviert dynamische VLAN-Erstellung.
`gvrp registration-forbid`	Deregistriert alle dynamischen VLANs und verhindert die dynamische VLAN-Registrierung für den Port.
`show gvrp configuration [ethernet` *`interface`*`| port-channel`*`port-channel-number`* `]`	Zeigt GVRP-Konfigurationsinformationen an, einschließlich Timer-Werte, Aktivierungsstatus von GVRP und dynamischer VLAN-Erstellung und Angabe der Ports, die GVRP ausführen.
`show gvrp error-statistics [ethernet`*`interface`* `| port- channel` *`port-channel- number`* `]`	Zeigt die GVRP-Fehlerstatistiken an.
	Zeigt die GVRP-Statistiken an.

show gvrp statistics [ethernet*interface* | port-channel *port-channel- number*]	
clear gvrp statistics [ethernet interface | port-channel *port-channel-number*]	Löscht alle GVRP-Statistikinformationen.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# gvrp enable

Console (config)# interface ethernet g8

Console (config-if)# gvrp enable

Console (config-if)# gvrp vlan-creation-forbid

Console (config-if)# gvrp registration-forbid

Console> show gvrp configuration

GVRP Feature is currently Enabled on the device.

Maximum VLANs: 4063, Maximum VLANs after reset: 4063.


Port(s)  GVRP-Status Registration Dynamic VLAN Timers(milliseconds)

                                 Creation      Join      Leave      Leave All

-------- ----------- ------------ ------------  ----      -----      ---------

g1       Disabled    Normal       Enabled       200       600        10000

...

g7       Disabled    Normal       Enabled       200       600        10000

g8       Enabled     Forbidden    Disabled      200       600        10000

g9       Disabled    Normal       Enabled       200       600        10000

...
```

```
g24       Disabled    Normal       Enabled       200       600       10000

ch1       Disabled    Normal       Enabled       200       600       10000

...

ch7       Disabled    Normal       Enabled       200       600       10000

...

Console> show gvrp statistics



GVRP statistics:

----------------

Legend:

rJE : Join Empty Received rJIn : Join In Received

rEmp : Empty Received rLIn : Leave In Received

rLE : Leave Empty Received rLA : Leave All Received

sJE : Join Empty Sent sJIn : Join In Sent

sEmp : Empty Sent sLIn : Leave In Sent

sLE : Leave Empty Sent sLA : Leave All Sent
```

Port	rJE	rJIn	rEmp	rLIn	rLE	rLA	sJE	sJIn	sEmp	sLIn	sLE	sLA
g1	0	0	0	0	0	0	0	0	0	0	0	0
g2	0	0	0	0	0	0	0	0	0	0	0	0
g3	0	0	0	0	0	0	0	0	0	0	0	0
g4	0	0	0	0	0	0	0	0	0	0	0	0

g5	0	0	0	0	0	0	0	0	0	0	0	0
g6	0	0	0	0	0	0	0	0	0	0	0	0
g7	0	0	0	0	0	0	0	0	0	0	0	0
g8	0	0	0	0	0	0	0	0	0	0	0	0

```
Console# clear gvrp statistics ethernet g8
```

Aggregieren von Ports

Durch Link-Aggregation wird die Portnutzung optimiert, indem eine Gruppe von Ports zu einer Link Aggregated Group (LAG) zusammengefasst werden. Durch die Aggregierung von Ports wird die Bandbreite zwischen Geräten um ein Vielfaches erhöht, die Portflexibilität gesteigert und Verbindungsredundanz gewährleistet.

Ihr Switch unterstützt sowohl statische LAGs als auch Link Aggregation Control Protocol (LACP)-LAGs. LACP-LAGs handeln mit anderen LACP-Ports, die sich an einem anderen Gerät befinden, Verbindungen mit aggregierten Ports aus. Wenn es sich bei den Ports des anderen Gerätes ebenfalls um LACP-Ports handelt, richten die Geräte eine LAG für diese Ports ein.

Bei der Konfiguration von gebündelten Ports sollten die folgenden Richtlinien beachtet werden.

- Alle Ports innerhalb einer LAG müssen denselben Medientyp haben.
- Ein VLAN ist nicht auf dem Port konfiguriert.
- Der Port ist keiner anderen LAG zugewiesen.
- Es ist eine verfügbare MAC-Adresse vorhanden, die dem Port zugewiesen werden kann.
- Die automatische Verbindungsaushandlung ist auf dem Port nicht konfiguriert.
- Der Port befindet sich im Vollduplexmodus.
- Alle Ports in der LAG verfügen über dieselben Eingangsfilterungs- und Tagmodi.
- Alle Ports in der LAG verfügen über dieselben Rückstau- und Datenflusssteuerungs-Modi.
- Alle Ports in der LAG verfügen über dieselbe Priorität.
- Alle Ports in der LAG verfügen über denselben Sender-Empfängertyp.
- PowerConnect 6024/6024F unterstützt bis zu sieben LAGs.
- Ports dürfen nur als LACP-Ports konfiguriert werden, wenn sie keiner zuvor konfigurierten LAG angehören.

Ports, die einer LAG hinzugefügt wurden, verlieren ihre einzelne Portkonfiguration. Beim Entfernen von Ports aus der LAG wird die ursprüngliche Portkonfiguration auf die Ports angewendet.

Ihr Switch verfügt über eine Hash-Funktion, um zu ermitteln, welche Pakete auf welchem Mitglied der gebündelten Verbindung transportiert werden. Die Hash-Funktion berechnet den statistischen Lastenausgleich für aggregierte Verbindungskomponenten. Der Switch behandelt eine gebündelte Verbindung als einen logischen Port.

Öffnen Sie die Seite **Link Aggregation**, indem Sie auf **Switch→ Link Aggregation** in der *Strukturansicht* klicken.

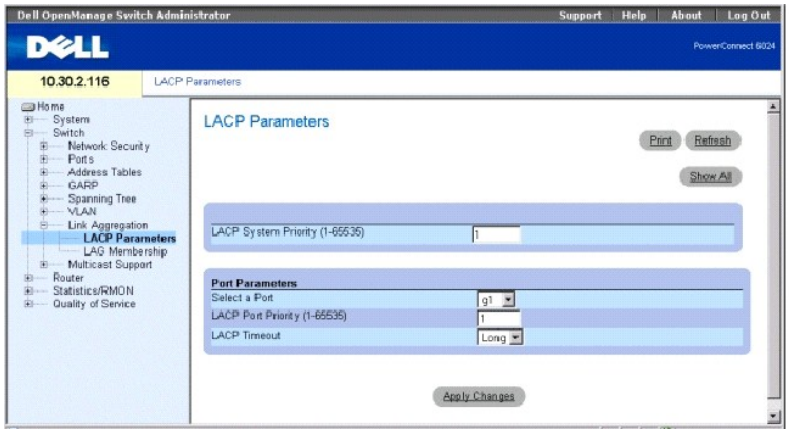
Definieren von LACP-Parametern

Aggregierte Ports können in Gruppen für die Link-Aggregation zusammengefasst werden. Jede Gruppe besteht aus Ports mit gleicher Geschwindigkeit, die auf Vollduplexbetrieb eingestellt sind.

Ports in einer Link Aggregated Group (LAG) können verschiedene Medientypen enthalten, wenn die Ports mit gleicher Geschwindigkeit betrieben werden. Aggregierte Links können sowohl manuell als auch automatisch konfiguriert werden, indem Link Aggregation Control Protocol (LACP) auf den entsprechenden Links aktiviert wird.

Auf der Seite **LACP Parameters** können Sie LACP-LAGs konfigurieren. Öffnen Sie die Seite **LACP Parameters**, indem Sie auf **Switch→ Link Aggregation→ LACP Parameters** in der *Strukturansicht* klicken.

Abbildung 7-34. LACP-Parameter



Die Seite **LACP-Parameter** enthält Abschnitte für das Definieren von globalen Parametern und Portparametern.

LACP System Priority (1-65535) (LACP-Systempriorität) Zeigt den LACP-Prioritätswert für globale Einstellungen an. Der Standardwert ist 1.

Select a Port Gibt die Portnummer an, der Timeout- und Prioritätswerte zugewiesen werden.

LACP Port Priority (1-65535) (LACP-Portpriorität) Gibt den LACP-Prioritätswert für den Port an.

LACP Timeout Weist ein administratives LACP-Zeitlimit zu. Die möglichen Werte sind:

Short Legt ein kurzes Zeitlimit fest.

Long Legt ein langes Zeitlimit fest.

Definieren globaler Verbindungsaggregations-Parameter

1. Öffnen Sie die Seite **LACP Parameters**.
2. Vervollständigen Sie die Felder **LACP System Priority** (LACP-Systempriorität) und **LACP Timeout** (LACP-Zeitüberschreitung).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Parameter werden definiert und das Gerät aktualisiert.

Definieren von Verbindungsaggregations-Parametern für Ports

1. Öffnen Sie die Seite **LACP Parameters**.
2. Führen Sie einen Bildlauf zur Tabelle**Port Parameters** table (Portparametertabelle) durch.

3. Wählen Sie den Port aus, für die Sie Parameter definieren möchten.
4. Definieren Sie die Felder **LACP System Priority** (LACP-Systempriorität) und **LACP Timeout** (LACP-Zeitüberschreitung).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Parameter werden definiert und das Gerät aktualisiert.

Anzeigen der LACP-Parameter-Tabelle

1. Öffnen Sie die Seite **LACP Parameters**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **LACP Parameters Table** anzuzeigen.

Konfigurieren von LACP-Parametern mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für die Konfiguration von LACP-Parametern auf der Seite **Link Aggregation** (Verbindungsaggregation) zusammen.

Tabelle 7-29. CLI-Befehle für LACP-Parameter

CLI-Befehl	Beschreibung
`lacp system-priority` *value*	Konfiguriert die Systempriorität.
`lacp port-priority` *value*	Konfiguriert den Prioritätswert für physische Ports.
`lacp timeout {long | short}`	Weist ein administratives LACP-Zeitlimit zu.
`show lacp ethernet` *interface* `[parameters | statistics | protocol- state]`	Zeigt LACP-Informationen für Ethernet-Ports an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

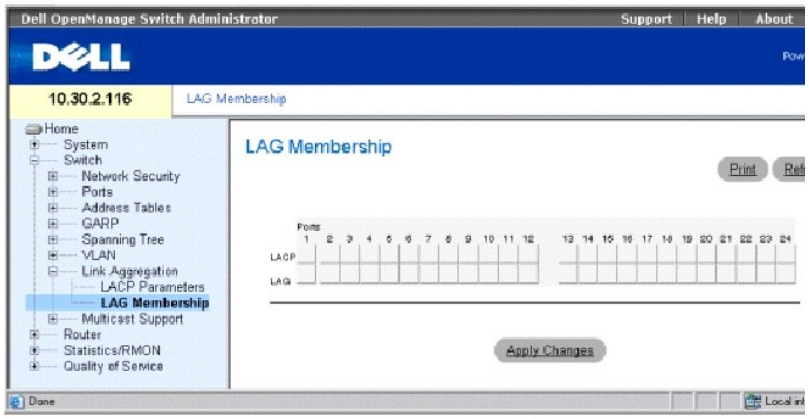
```
Console (config)# lacp system-priority 120

Console (config)# interface ethernet g8

Console (config-if)# lacp port-priority 247

Console (config-if)# lacp timeout long

Console (config-if)# exit

Console# show lacp ethernet g1 statistics

Port 1 LACP Statistics:

LACP PDUs sent:2
```

```
LACP PDUs received:2
```

Definieren von LAG-Mitgliedschaften

Ihr Switch unterstützt sieben LAGs pro System und sieben Ports pro LAG. Auf der Seite **LAG-Mitgliedschaft** können Sie Ports zu LAGs zuordnen. Öffnen Sie die Seite **LAG Membership**, indem Sie auf **Switch→ Link Aggregation→ LAG Membership** in der *Strukturansicht* klicken.

Abbildung 7-35. LAG-Mitgliedschaft



LACP Fügt den Port über LACP einer LAG hinzu.

LAG Fügt einer LAG einen Port hinzu und gibt die spezifische LAG an, welcher der Port angehört.

Hinzufügen eines Ports zu einer LAG

1. Öffnen Sie die Seite **LAG Membership**.
2. Betätigen Sie die Schaltfläche unter der Portnummer, um die statische Einstellung und die LAG-Nummer zuzuweisen.
3. Ändern Sie die Schaltfläche in der LACP-Zeile in **L**, um den Port in eine LAG mit LACP zu bündeln.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Port wird der LAG hinzugefügt und das Gerät aktualisiert.

Zuweisen von Ports zu LAGs mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Zuweisung von Ports zu LAGs, wie auf der Seite **LAG Membership** angezeigt, zusammen.

Tabelle 7-30. CLI-Befehle für LAG-Mitgliedschaft

CLI-Befehl	Beschreibung
`interface port-channel` *`port-channel-number`*	Aktiviert den Schnittstellenkonfigurationsmodus eines spezifischen Portkanals.
`channel-group` *`port-channel-number`* `mode {on | auto}`	Weist einen Port einem Portkanal zu. Verwenden Sie die Neinform (`no`") dieses Befehls, um die Kanalgruppenkonfiguration aus der Schnittstelle zu entfernen.

show interfaces port- channel [*port-channel- number*]	Zeigt Portkanal-Informationen an.

```
Console (config)# interface port-channel 1

Console (config-if)# channel-group 1 mode on

Console# show interfaces port-channel

Channel       Port

------------  --------------------------------

Ch 1          Active    g1, g2    Inactive g3

Ch 2          Active    g2

Ch 3          Inactive  g8
```

Unterstützung von Multicast-Weiterleitung

Bei der Multicast-Weiterleitung können einzelne Pakete an mehrere Ziele weitergeleitet werden. Der L2-Multicast-Service basiert auf einem L2-Switch, der ein an eine spezifische Multicast-Adresse adressiertes Einzelpaket empfängt. Bei der Multicast-Weiterleitung werden Kopien der Pakete erstellt und die Pakete an die relevanten Ports übertragen.

Das Gerät unterstützt die beiden folgenden Einstellungen:

- **Forwarding L2 Multicast Packets** (Weiterleiten von L2-Multicast-Paketen) Leitet Multicast-Pakete der Schicht 2 weiter. Multicast-Filtern auf Schicht 2 ist standardmäßig aktiviert und kann nicht durch den Benutzer konfiguriert werden.

ANMERKUNG: Das System unterstützt Multicast-Filtern für 256 Multicastgruppen.

- **Filtering L2 Multicast Packets** (Filtern von L2 Multicast-Paketen) Leitet Schicht 2-Pakete an Schnittstellen weiter. Wenn Multicast-Filtern deaktiviert ist, werden Multicast-Pakete an alle relevanten VLAN-Ports weitergeleitet.

Öffnen Sie die Seite **Multicast Support**, indem Sie auf **Switch→ Multicast Support** in der *Strukturansicht* klicken.

Definieren von globalen Multicast-Parametern

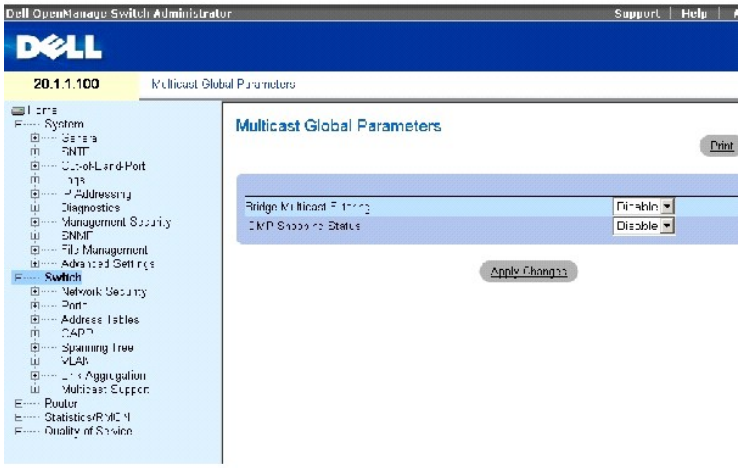
Beim Layer 2-Switching werden Multicast-Pakete standardmäßig an alle relevanten VLAN-Ports weitergeleitet, wobei die Pakete als Multicast-Pakete behandelt werden. Das Weiterleiten über Multicast-Datenverkehr ist zwar effektiv, es stellt jedoch nicht die optimale Lösung dar, da irrelevante Ports ebenfalls Multicast-Pakete empfangen. Die überflüssigen Pakete erhöhen unnötigerweise das Netzwerkdatenaufkommen. Multicast-Weiterleitungsfilter ermöglichen das Weiterleiten von Layer 2-Paketen an Port-Teilmengen.

Wenn IGMP-Snooping global aktiviert ist, werden sämtliche IGMP-Pakete an die CPU weitergeleitet. Die CPU analysiert in eingehenden Pakete und bestimmt, welcher Port welcher Multicast-Gruppe beitreten soll, welche Ports über Multicast-Router verfügen, die IGMP-Anfragen generieren und welche Routing-Protokolle Pakete und Multicast-Datenverkehr weiterleiten.

Ports, die einer bestimmten Multicast-Gruppe beitreten möchten, erstellen einen IGMP-Bericht, der festlegt, dass die Multicast-Gruppe Mitglieder akzeptiert. So wird die Multicast-Filter-Datenbank erstellt.

Die Seite **Multicast Global Parameters** (Globale Multicast-Parameter) ermöglicht die Aktivierung von IGMP-Snooping auf dem Gerät. Öffnen Sie die Seite **Multicast Global Parameters**, indem Sie auf **Switch**→ **Multicast Support**→ **Global Parameters** in der *Strukturansicht* klicken.

Abbildung 7-36. Globale Multicast-Parameter



Die Seite **Globale Multicast-Parameter** enthält die folgenden Felder:

Bridge Multicast Filtering Aktiviert/deaktiviert die Bridge-Multicast-Filterung. Die Standardeinstellung ist Disabled (Deaktiviert).

IGMP Snooping Status Aktiviert/deaktiviert IGMP-Snooping auf dem Gerät. Die Standardeinstellung ist Disabled (Deaktiviert).

Aktivieren der Bridge-Multicast-Filterung für das Gerät

1. Öffnen Sie die Seite **Multicast Global Parameters**.
2. Wählen Sie **Enable**(Entfernen) im Feld **Bridge Multicast Filtering**.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Bridge Multicastwird für das Gerät aktiviert.

Aktivieren von IGMP-Snooping für das Gerät

1. Öffnen Sie die Seite **Multicast Global Parameters**.
2. Wählen Sie **Enable**(Entfernen) im Feld **IGMP Snooping Status**.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

IGMP-Snooping wird für das Gerät aktiviert.

Aktivieren von Multicast-Weiterleitung und IGMP-Snooping mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für Multicast-Weiterleitung und IGMP-Snooping auf der Seite **Multicast Support** (Multicast-Unterstützung) zusammen.

Tabelle 7-31. CLI-Befehle für Multicast-Weiterleitung und Snooping

CLI-Befehl	Beschreibung
`bridge multicast filtering`	Aktiviert die Filterung von Multicastadressen.
`ip igmp snooping`	Aktiviert das IGMP-(Internet Group Management Protocol-)Snooping.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# bridge multicast filtering
```

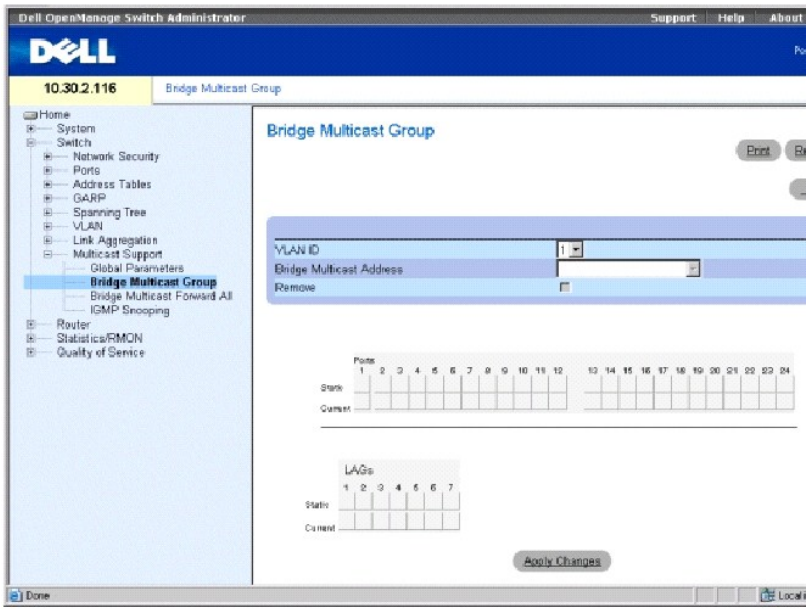
```
Console (config)# ip igmp snooping
```

Hinzufügen von Komponenten zu einer Bridge-Multicast-Adresse

Auf der Seite **Bridge Multicast Group** (Brücken-Multicast-Gruppe) werden die Schnittstellen und LAGs, die mit der Multicast-Servicegruppe verbunden sind, in den Tabellen **Ports** und **LAGs** angezeigt. In den Port- und LAG-Tabellen wird auch angegeben, wie der Port oder die LAG der Multicast-Gruppe hinzugefügt wird. Ports können entweder vorhandenen Gruppen oder einer neuen Multicast-Dienstgruppe hinzugefügt werden. Auf der Seite **Brücken-Multicast-Gruppe** können neue Multicast-Dienstgruppen erstellt werden. Auf der Seite **Brücken-Multicast-Gruppe** werden einer bestimmten Multicast-Dienst-Adressgruppe darüber hinaus Ports zugewiesen.

Öffnen Sie die Seite **Bridge Multicast Group**, indem Sie auf **Switch→ Multicast Support→ Bridge Multicast Address** in der *Strukturansicht* klicken.

Abbildung 7-37. Brücken-Multicast-Gruppe



VLAN ID Identifiziert ein VLAN und enthält Informationen über die Multicast-Gruppenadresse.

Bridge Multicast Address Identifiziert die MAC-Adresse/IP-Adresse der Multicast-Gruppe.

Remove (Entfernen) Wenn diese Option markiert ist, wird eine Brücken-Multicast-Adresse entfernt.

Ports Listet den Port auf, der einem Multicast-Dienst hinzugefügt werden kann.

LAGs Listet die LAGs auf, die einem Multicast-Dienst hinzugefügt werden können.

Die folgende Tabelle enthält die Einstellungen für die Verwaltung von IGMP-Port- und LAG-Mitgliedern.

Tabelle 7-32. Tabelle der Kontrolleinstellungen für IGMP-Port/LAG-Mitglieder

Port-Kontrolle	Definition
D	Gibt in der Zeile **Current** (Aktuell) an, dass der Port/die LAG der Multicast-Gruppe dynamisch beigetreten ist.
S	Verknüpft den Port in der Zeile *Static*als statische Komponente mit der Multicast-Gruppe. Gibt in der Zeile **Current** (Aktuell) an, dass der Port/die LAG der Multicast-Gruppe statisch beigetreten ist.
F	Zeigt an, dass der Port/die LAG einen unzulässigen Eintrag in der Multicast-Gruppe darstellt.
Keine	Gibt an, dass der Port nicht mit einer Multicast-Gruppe verknüpft ist.

Hinzufügen von Bridge-Multicastadressen

1. Öffnen Sie die Seite **Bridge Multicast Group**.
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Brücken-Multicast-Gruppe hinzufügen** anzuzeigen.

Abbildung 7-38. Brücken-Multicast-Gruppe hinzufügen

3. Definieren Sie die Felder **VLAN ID** und **New Bridge Multicast Address**.
4. Ändern Sie die Einstellung eines Ports in **S**, um den Port in die ausgewählte Multicast-Gruppe aufzunehmen.
5. Ändern Sie die Einstellung eines Ports in **F**, um das Hinzufügen spezifischer Multicast-Adressen zu eines bestimmten Ports zu verbieten.
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Brücken-Multicast-Adresse wird der Multicast-Gruppe zugeordnet und das Gerät aktualisiert.

Definieren von Ports für den Empfang eines Multicast-Dienstes:

1. Öffnen Sie die Seite **Bridge Multicast Group**.
2. Definieren Sie die Felder **VLAN ID** und **Bridge Multicast Address**.

3. Ändern Sie die Einstellung eines Ports in **S**, um den Port in die ausgewählte Multicast-Gruppe aufzunehmen.
4. Ändern Sie die Einstellung eines Ports in **F**, um das Hinzufügen spezifischer Multicast-Adressen zu einem bestimmten Port zu verbieten.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Port wird der Multicast-Gruppe zugewiesen und das Gerät aktualisiert.

Definieren von LAGs für den Empfang eines Multicast-Dienstes:

1. Öffnen Sie die Seite **Bridge Multicast Group**.
2. Definieren Sie die Felder **VLAN ID** und **Bridge Multicast Address**.
3. Ändern Sie die Einstellung der LAG in **S**, um die LAG in die ausgewählte Multicast-Gruppe aufzunehmen.
4. Ändern Sie die Einstellung der LAG in **F**, um das Hinzufügen spezifischer Multicast-Adressen zu einer bestimmten LAG zu verbieten.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die LAG wird der Multicast-Gruppe zugewiesen und das Gerät aktualisiert.

Verwalten von Multicast-Dienstkomponenten mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für die Verwaltung von Multicast-Service-Mitgliedern auf der Seite **Bridge Multicast Group** (Brücken-Multicast-Gruppe) zusammen.

Tabelle 7-33. CLI-Befehle für Multicast-Dienstmitgliedschaft

CLI-Befehl	Beschreibung
`bridge multicast address {`*`mac-multicast-address`*` | `*`ip-multicast-address`*`} [add | remove] {ethernet `*`interface-list`*` | port- channel `*`port-channel- number-list`*` }`	Registriert Multicast-Adressen der MAC-Schicht bei der Brückentabelle, und fügt der Gruppe statische Ports hinzu.
`bridge multicast forbidden address {`*`mac-multicast- address`*` | `*`ip-multicast- address`*`} [add | remove] {ethernet interface-list | port-channel port-channel-number-list}`	Verbietet das Hinzufügen spezifischer Multicast-Adressen zu bestimmten Ports. Verwenden Sie die no-Form dieses Befehls, um zur Standardeinstellung zurückzukehren.
`show bridge multicast address-table [vlan vlan-id ] [address mac-multicast- address | `*`ip-multicast- address`*`] [format ip | mac]`	Zeigt Informationen der Multicast-MAC-Adresstabelle an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console# config


Console (config)# vlan database


Console (config-if)# vlan 8


Console (config-if)# exit


Console (config)# interface range ethernet g1-9


Console (config-if)# switchport mode general
```

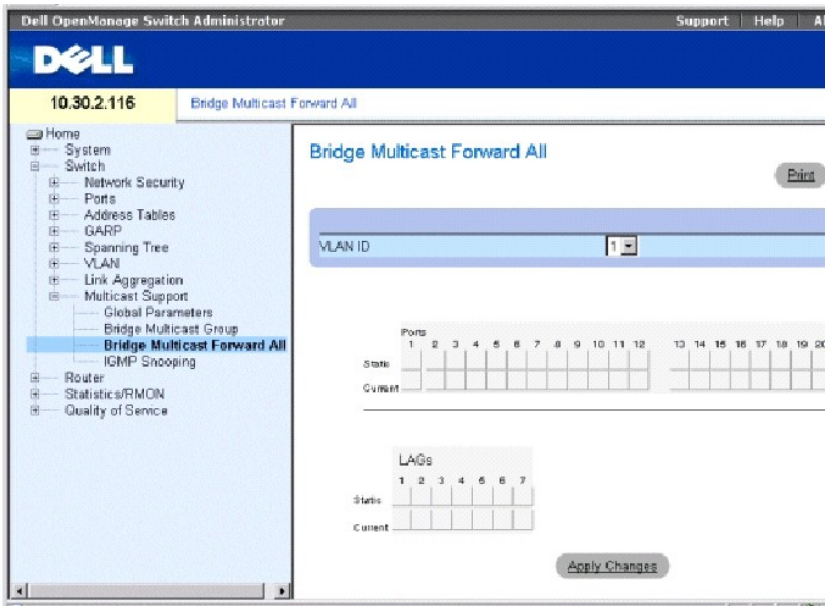
```
Console (config-if)# switchport general allow vlan add 8

Console (config)# interface vlan 8

Console (config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1-9

Console (config-if)# exit

Console (config)# exit

Console# show bridge multicast address-table

Vlan   MAC Address      type      Ports

----   --------------   ----      -----------

1      0100.5e02.0203   static    g1, g2

19     0100.5e02.0208   static    g1-8

19     0100.5e02.0208   dynamic   g9-11

Forbidden ports for multicast addresses:

Vlan   MAC Address      Ports

----   --------------   -------------------

1      0100.5e02.0203   g8

19     0100.5e02.0208   g8

Console# configuration

Console (config)# interface vlan 8

Console (config-if)# bridge multicast address 0100.5e02.0203

Console (config-if)# bridge multicast forbidden address 0100.5e02.0203 add ethernet g9
```

Zuweisen von Parametern für die globale Multicast-Weiterleitung

Auf der Seite **Bridge Multicast Forward All** (Brücken-Multicast Alles weiterleiten") können Sie Ports oder LAGs mit einem Switch verknüpfen, der mit einem benachbarten Router-/Switch verbunden ist. Sobald IGMP-Snooping aktiviert ist, werden Multicast-Pakete an entsprechende Ports oder VLANs weitergeleitet.

Um die Seite **Bridge Multicast Forward All** zu öffnen, klicken Sie in der Strukturansicht auf **Switch→ Multicast Support→ Bridge Multicast→ Bridge Multicast Forward All**.

Abbildung 7-39. Brücken-Multicast Alles weiterleiten"



VLAN ID Identifiziert ein Paket-VLAN und enthält Informationen über die Adresse der Multicast-Gruppe.

Ports Listet Ports auf, die einem Multicast-Service hinzugefügt werden können.

LAGs Listet die LAGs auf, die einem Multicast-Service hinzugefügt werden können.

Die folgende Tabelle enthält die Einstellungen für die Verwaltung von Router- und Porteinstellungen.

Tabelle 7-34. Brücken-Multicast Alles weiterleiten"-Router/Port-Kontrolle

Port-Kontrolle	Definition
D	Fügt den Port dem Multicast-Router oder Schalter als dynamischen Port hinzu.
S	Fügt den Port dem Multicast-Router oder Schalter als statischen Port hinzu.
F	Forbidden (Verboten).
Keine	Gibt an, dass der Port nicht mit einem Multicast-Router oder -Switch verknüpft ist.

Anfügen eines Ports an einen Multicast-Router oder Schalter

1. Öffnen Sie die Seite **Bridge Multicast Forward All**.
2. Definieren Sie das Feld **VLAN ID**.
3. Wählen Sie einen Port in der **Ports**-Tabelle und weisen Sie dem Port einen Wert zu.

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

Der Port wird mit dem Multicast-Router oder Switch verbunden.

Anfügen einer LAG an einen Multicast-Router oder Schalter

1. Öffnen Sie die Seite **Bridge Multicast Forward All**.
2. Definieren Sie das Feld **VLAN ID**.
3. Wählen Sie einen Port in der **LAG**-Tabelle und weisen Sie der LAG einen Wert zu.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die LAG wird mit dem Multicast-Router oder Switch verbunden.

Verwaltung von an Multicast-Router angeschlossene LAGs und Ports mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle für die Verwaltung von an Multicast-Router angeschlossenen LAGs und Ports auf der Seite **Bridge Multicast Forward All** (Brücken-Multicast Alles weiterleiten") zusammen.

Tabelle 7-35. CLI-Befehle zur Verwaltung von LAGs und Ports, die an Multicast- Router angeschlossen sind

CLI-Befehl	Beschreibung
`show bridge multicast filtering` *`vlan-id`*	Zeigt die Multicast-Filterkonfiguration an.
`bridge multicast forward-all {add | remove} {ethernet` *`interface-list`* `| port-channel` *`port-channel-number-list`*`}`	Ermöglicht die Weiterleitung aller Multicast-Pakete an einen Port. Verwenden Sie die no-Form dieses Befehls, um zur Standardeinstellung zurückzukehren.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

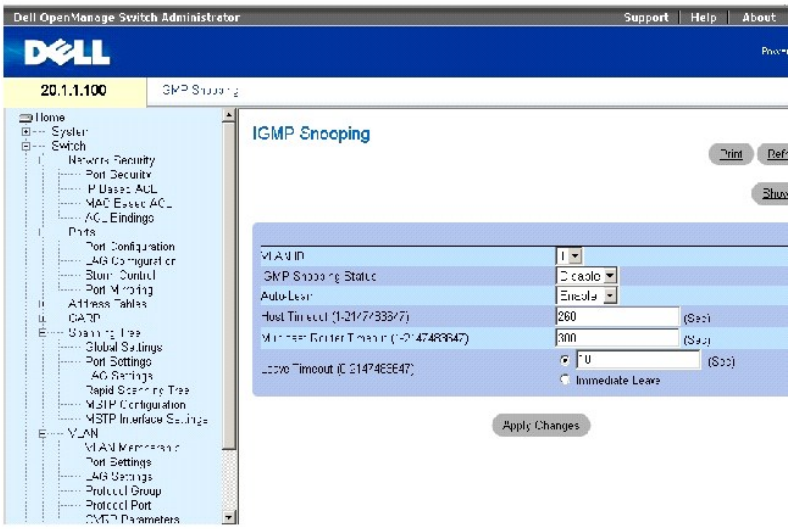
```
Console# show bridge multicast filtering 1

Filtering: Disabled

VLAN: 1

Forward-All

Port Static Status

------ --------- ---------

g1 - Filter

g2 - Filter

...
```

```
Console# config

Console (config)#vlan database

Console (config-if)#vlan 8

Console (config-vlan)#exit

Console (config)#interface range ethernet g1-9

Console (config-if)# switchport mode general

Console (config-if)# switchport general allow vlan add 8

Console (config)# interface vlan 8

Console (config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1-9

Console (config-if)# exit

Console (config)# exit

Console# configuration

Console (config)# interface vlan 1

Console (config-if)# bridge multicast forward-all add ethernet g8
```

IGMP-Snooping

Auf der Seite **IGMP-Snooping** können Sie IGMP-Mitglieder hinzufügen. Öffnen Sie die Seite **IGMP Snooping**, indem Sie auf **Switch→ Multicast Support→ IGMP Snooping** in der *Strukturansicht* klicken.

Abbildung 7-40. IGMP-Snooping



VLAN ID Gibt die VLAN ID an.

IGMP Snooping Status Aktiviert/deaktiviert IGMP-Snooping auf dem VLAN.

Auto Learn Aktiviert/deaktiviert Auto Learn auf dem Gerät.

Host Timeout (1-2147483647) Speicherdauer, bevor ein IGMP-Snooping-Eintrag gelöscht wird. Die Standardzeit ist 260 Sekunden.

Multicast Router Timeout (1-2147483647) Speicherdauer, bevor ein Multicast-Router-Eintrag gelöscht wird. Der Standardwert lautet 300 Sekunden.

Leave Timeout (0-2147483647) Speicherdauer (in Sekunden) nach Eingang einer Port-Leave-Meldung, bevor der Eintrag gelöscht wird. **User-defined** (Benutzerdefiniert) ermöglicht die Einstellung des Zeitüberschreitungszeitraums, und **Immediate Leave** gibt einen sofortigen Zeitüberschreitungszeitraum an. Das Standard-Zeitlimit ist 10 Sekunden.

Aktivieren von IGMP-Snooping für das Gerät

1. Öffnen Sie die Seite **IGMP Snooping**.
2. Wählen Sie die VLAN-ID für das Gerät, auf dem Sie IGMP-Snooping aktivieren möchten.
3. Wählen Sie **Enable** (Aktivieren) im Feld **IGMP Snooping Status**.
4. Geben Sie die Informationen in die Felder auf der Seite ein.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

IGMP-Snooping wird auf dem Gerät aktiviert.

Anzeigen der IGMP-Snooping-Tabelle

1. Öffnen Sie die Seite **IGMP Snooping**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **IGMP Snooping Table** anzuzeigen.

Konfigurieren von IGMP-Snooping mit den CLI-Befehlen

Die folgende Tabelle fast die entsprechenden CLI-Befehle zum Konfigurieren der gesperrten Portsicherheit, wie auf der Seite **IGMP-Snooping** angezeigt, zusammen.

Tabelle 7-36. CLI-Befehle für IGMP-Snooping

CLI-Befehl	Beschreibung
`ip igmp snooping`	Aktiviert das IGMP-(Internet Group Management Protocol-)Snooping.
`ip igmp snooping mrouter learn-pim-dvmrp`	Aktiviert die automatische Erkennung von Multicast-Router-Ports im Kontext eines spezifischen VLAN.
`ip igmp snooping host-time-out` *`time-out`*	Konfiguriert das Host-Zeitlimit.
`ip igmp snooping mrouter- time-out` *`time-out`*	Konfiguriert das Multicast-Router-Zeitlimit.
`ip igmp snooping leave-time -out {`*`time-out`* `| immediate-leave}`	Konfiguriert das Leave-Zeitlimit.
`show ip igmp snooping interface` *`vlan-id`*	Zeigt die IGMP-Snooping-Konfiguration an.
`show ip igmp snooping mrouter [interface`*`vlan-id`*`]`	Zeigt Informationen zu dynamisch erfassten Multicast-Router-Schnittstellen an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# ip igmp snooping

Console (config)# interface vlan 1

Console (config-if)# ip igmp snooping mrouter learn-pim-dvmrp

Console (config-if)# ip igmp snooping host-time-out 300

Console (config-if)# ip igmp snooping mrouter-time-out 200

Console (config-if)# exit

Console (config)# interface vlan 1

Console (config-if)# ip igmp snooping leave-time-out 60

Console (config-if)# exit

Console (config)# exit

Console # show ip igmp snooping interface 1000
```

```
IGMP Snooping is globally enabled

IGMP Snooping is enabled on VLAN 1000

IGMP host timeout is 300 sec

IGMP Immediate leave is disabled. IGMP leave timeout is 10 sec

IGMP mrouter timeout is 200 sec

Automatic learning of multicast router ports is enabled

Console> show igmp-snooping mrouter

VLAN      Ports

-------   ---------------------------------------

2         g9
```

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Konfigurieren von Routing

Dell PowerConnect 6024/6024F Systeme

Übersicht über Routing

Geräte in unterschiedlichen Teilnetzmasken kommunizieren miteinander über einen Layer 3-Router zwischen den VLANs. Routing ist standardmäßig auf Ihrem Switch aktiviert. Dennoch muss mindestens eine IP-Schnittstelle für den Switch konfiguriert werden, damit mit dem Routen von Netzwerkdatenverkehr begonnen werden kann. Routen sind entweder statisch oder mithilfe von RIP (RIP - Routing Information Protocol) oder OSPF (OSPF - Shortest Path First) konfiguriert.

Weitere Informationen über RIP finden Sie unter Konfigurieren von RIP.

Weitere Informationen über OSPF finden Sie unter Konfigurieren von Parametern und Filtern für OSPF".

Konfigurieren von globalem IP-Routing

Die Seite **Globale Routing-Parameter** enthält Verknüpfungen für das Konfigurieren von Routing. Routing ist zwar grundsätzlich eingeschaltet, wird aber nur aktiviert, wenn das System über mindestens eine IP-Adresse verfügt. Um die Seite **Globale Routing-Parameter** zu öffnen, klicken Sie in der Strukturansicht auf **Router→ Global Routing Parameters**.

Die Seite **Globale Routing-Parameter** enthält Verknüpfungen, die es ermöglichen, die folgenden Schritte auszuführen:

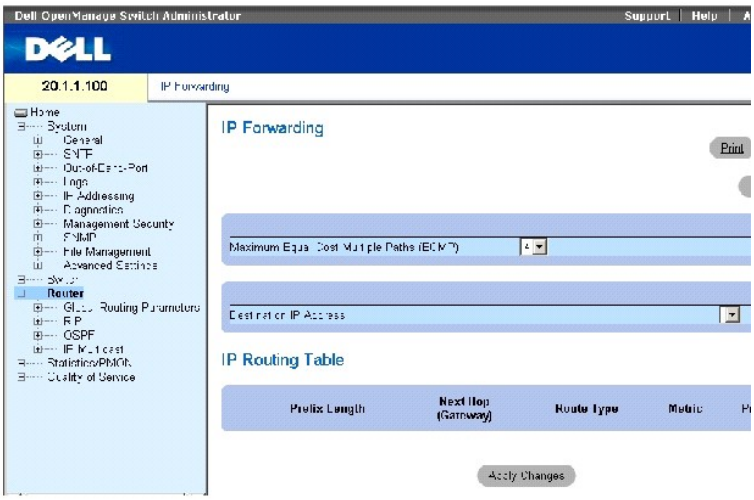
- Konfigurieren der IP-Übermittlungstabelle
- Konfigurieren von statischen IP-Routen
- Konfigurieren von VRRP
- Konfigurieren der MD5-Routing-Authentifizierung
- Konfigurieren von MD5-Schlüsselketteneinstellungen

Konfigurieren der IP-Übermittlungstabelle

Auf der Seite **IP-Übermittlung** können Sie sich die Routing-Parameter anzeigen lassen, mit denen der IP-Datenverkehr übermittelt wird. Die Seite liefert eine Liste mit IP-Routen für ausgewählte Ziel-IP-Adressen, einschließlich statisch oder dynamisch definierter IP-Routen. IP-Routen basieren auf Netzwerkmasken, Next Hops, Metriken und Übermittlungsprotokollen. Diese Parameter bestimmen, wie spezifisch Pakete übermittelt oder verworfen werden. Wenn eine IP-Adresse auf einer Schnittstelle konfiguriert ist, ist sie in der IP-Übermittlungstabelle enthalten.

Um die Seite **IP-Übermittlung** zu öffnen, klicken Sie in der Strukturansicht auf **Router→ Global Routing Parameters→ IP Forwarding**.

Abbildung 8-1. IP-Übermittlung



Maximum Equal Cost Multipaths (ECMP) ECMP-Wert, der bei der Übermittlung von IP-Paketen definiert sein muss. Der ECMP-Wert gibt an, wie viele Pfade zwischen dem Router und einem Netzwerk verfügbar sind. Die möglichen Werte reichen von 1-4. So gibt beispielsweise der Wert 1 an, dass nur ein Pfad zum Netzwerk zur Verfügung steht. Je höher der Wert ist, desto mehr Speicherressourcen sind erforderlich. Änderungen in diesem Feld werden erst übernommen, wenn das Gerät zurückgesetzt wird.

Destination IP Address (Ziel-IP-Adresse) Das Ziel-IP-Netzwerk.

Prefix Length (Präfixlänge) Die Anzahl der Bits, die im Präfix der Ziel-IP-Adresse enthalten sind. Die Länge liegt zwischen 1-32 Bits.

Next Hop (**Gateway**) (Nächster Hop) Die nächste Routeradresse auf dem Weg zum Zielnetzwerk.

Route Type (Route-Typ) Legt fest, wie das Remote-Routing ausgeführt wird. Die möglichen Werte sind:

Remote Paket wird gesendet.

Reject (Verweigert) Paket wird verworfen.

Local (Lokal) Paket wird zu einem lokalen Netzwerk gesendet.

Metric (Metrisch) Die Anzahl der Hops bis zum Zielnetzwerk.

Protocol (Protokoll) Routing-Protokoll, über das diese Route hinzugefügt wurde.

Anzeigen der IP Forwarding Table (IP-Übermittlungstabelle)

Die **IP Forwarding Table** (IP-Übermittlungstabelle) liefert eine Liste aller IP-Routen des Systems.

1. Öffnen Sie die Seite **IP Forwarding** (IP-Übermittlung).
2. Klicken Sie auf **Show All** (Alle anzeigen) um die **Tabelle IP Forwarding** (IP-Übermittlung) anzuzeigen.

Anzeigen von IP Fowarding (IP-Übermittlung) mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Anzeigen von IP Forwarding (IP-Übermittlung).

Tabelle 8-1. CLI-Befehle für die IP-Übermittlung

CLI-Befehl	Beschreibung
show ip route [address]<*ip- address*>	Zeigt den aktuellen Status der Routingtabelle an.
ip maximum-paths number-paths	Steuert die maximale Anzahl paralleler Routen in einer Routingtabelle.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface ip 10.10.10.2

Console (config-ip)# ip maximum-paths 2

Console (config-ip)# exit

Console (config)# exit

Console# exit

Console> show ip route

Codes: C - connected, S - static, R - RIP, O - OSPF, E - OSPF extern

R 10.0.0.0/8 is rejected

C 10.0.1.1/32 is directly connected, Loopback0

C 10.0.1.0/24 is directly connected, Ethernet g1

C 10.0.2.0/24 is directly connected, Ethernet g2

R 10.8.2.0/24 [230/50] via 10.0.2.2, 00:17:19, Ethernet g2

S 10.9.1.0/24 [5/2] via 10.0.1.2, 17:19:18, Ethernet g1

S 10.9.1.0/24 [5/3] via 10.0.2.2, Backup Not Active

O 10.8.1.0/24 [30/2000] via 10.0.1.2, 00:39:08, Ethernet g1

S 172.1.0.0/16 [5/3] via 10.0.1.1, 18:21:58, Ethernet g1
```

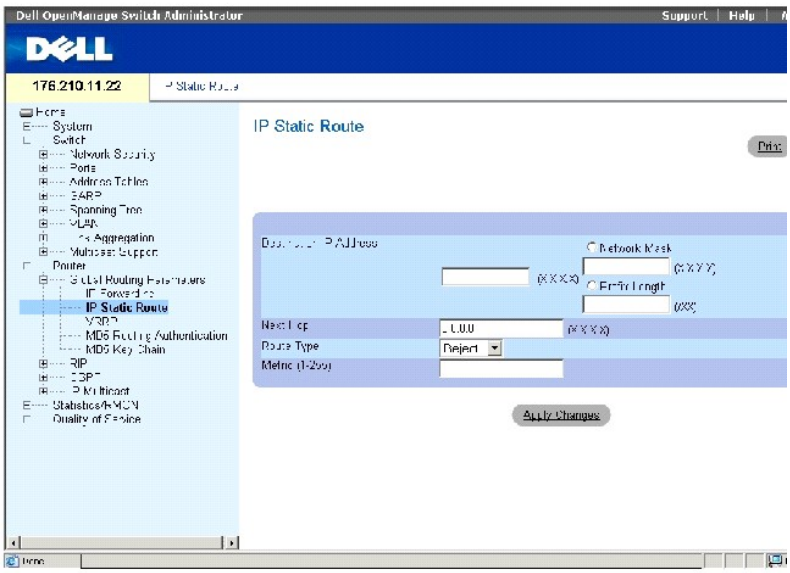
```
S 172.1.1.0/24 [5/3] via 10.0.2.1, 17:12:19, Ethernet g1

S 172.1.1.1/32 [5/3] via 10.0.3.1, 19:51:18, Ethernet g1

Maximale Parallelpfade: 2
```

Konfigurieren von statischen IP-Routen

Verwenden Sie die Seite **IP Static Route** (Statische IP-Route) um statische Routen zu definieren.

Um die Seite **Statische IP-Routes** zu öffnen, klicken Sie in der Strukturansicht auf **Router**→ **Global Routing Parameters**→ **IP Static Route**.

Abbildung 8-2. Statische IP-Routes



Destination IP Address (Ziel-IP-Adresse) Ziel-IP-Netzwerk der statischen Route.

Network Mask (Netzwerkmaske) Die Zielnetzwerkmaske dieser Route.

Prefix Length (Präfixlänge) Die Anzahl der Bits, die im Präfix der Ziel-IP-Adresse enthalten sind. Die Länge liegt zwischen 1-32 Bits.

Next Hop (Nächster Hop) Gibt die nächste Systemadresse auf der Route an.

Route Type (Route-Typ) Legt fest, wie das Remote-Routing ausgeführt wird. Die möglichen Feldwerte sind:

Remote Paket wird gesendet.

Reject (Verweigert) Paket wird verworfen.

Local (Lokal) Paket wird zu einem lokalen Netzwerk gesendet.

Metric (1-255) (Metrisch (1-255) Die Anzahl der Hops bis zum Zielnetzwerk.

Hinzufügen von statischen IP-Routen

ANMERKUNG: Als Gateway kann nur ein direkt angeschlossener Router definiert werden.

1. Öffnen Sie die Seite **IP Static Route** (Statische IP-Route).
2. Definieren Sie die Felder der Seite.

ANMERKUNG: Wird bei **Route Type** (Routentyp) **Reject** (Verweigert) ausgewählt, wird sichergestellt, dass die Routen zum Zielnetzwerk nicht benutzt werden können.

Um einem Host auf einem Remote-Netzwerk eine statische Route zuzuordnen, wählen Sie **Remote** als **Route Type** (Routentyp).

Um einem Host auf einem lokalen Netzwerk eine statische Route zuzuordnen, wählen Sie **Local** (Lokal) als **Route Type** (Routentyp).

Die **Destination IP Address** (Ziel-IP-Adresse) und **Network Mask** (Netzwerkmaske) bezeichnen die Remote-Netzwerkadresse. **Next Hop** (Nächster Hop) bezeichnet die Adresse eines direkt mit Ihrem Switch verbundenen Routers.

Die **Destination IP Address** (Ziel-IP-Adresse) ist die Hostadresse. Das Feld **Next Hop** (Nächster Hop) sollte mit 0.0.0.0. ausgefüllt werden.

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

Die neue statische Route wird hinzugefügt und das Gerät aktualisiert.

Entfernen einer statischen IP-Route

1. Öffnen Sie die Seite **IP Static Route** (Statische IP-Route).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Tabelle **IP Static Route Table** (Statische IP-Routentabelle) anzuzeigen.
3. Wählen Sie **Remove for the Destination IP Address** (Als Ziel-IP-Adresse entfernen) bei der statischen Route, die Sie entfernen möchten.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die statische Route wird entfernt und das Gerät aktualisiert.

Konfigurieren der statischen IP-Tabelle mithilfe von CLI-Befehlen

Die folgende Tabelle beinhaltet die CLI-Befehle zum Konfigurieren der statischen IP-Tabelle.

Tabelle 8-2. CLI-Befehle für die statische IP-Routentabelle

CLI-Befehl	Beschreibung
`ip route prefix {mask | *prefix-length*} *gateway* [metric *distance*] [reject-route]`	Erzeugt statische IP-Routen.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# ip route 172.16.0.0 255.255.0.0 131.16.1.1
```

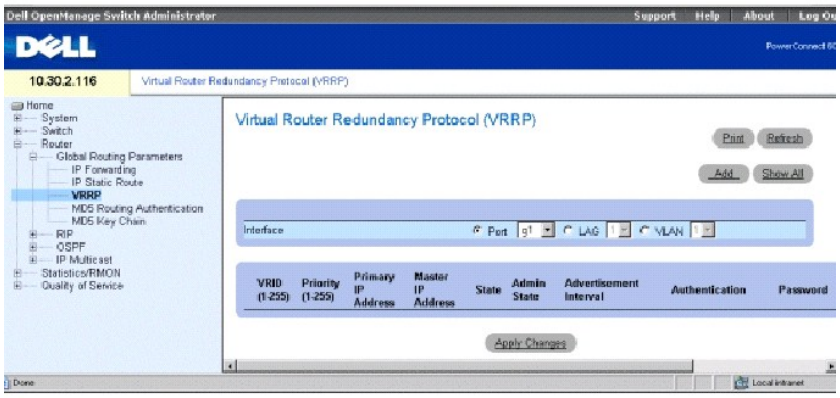
Konfigurieren von VRRP

Das Protokoll **Virtual Router Redundancy Protocol**" (VRRP) legt ein auswählendes Protokoll fest, das einem der VRRP-Router auf dem lokalen Netzwerk (LAN) dynamisch die Routing-Zuständigkeit zuweist (Master-Router). Dieser Auswahlprozess ermöglicht das dynamische Failover der Routing-Zuständigkeit, für den Fall, dass der Masterrouter ausfällt.

Der Vorteil von VRRP ist, dass das innerhalb der Routing-Umgebung auftretende Problem der Ausfallsicherheit an einem einzelnen Punkt durch eine größere Verfügbarkeit von Standardpfaden eliminiert wird und gleichzeitig das Konfigurieren von dynamischem Routing oder Router Discovery Protokollen an jedem einzelnen End-Host nicht notwendig sind.

Die Seite **Virtuelles Router-Redundanzprotokoll (VRRR)** legt die VRRP-Routingparameter des Switch fest. Um die Seite **Virtuelles Router-Redundanzprotokoll (VRRR)** zu öffnen, klicken Sie in der Strukturansicht auf **Router→ Global Routing Parameters→ VRRP**.

Abbildung 8-3. Virtuelles Routerredundanzprotokoll (VRRR)



Interface (Schnittstelle) Art und Anzahl der am VRRP-Router angeschlossenen Schnittstellen.

VRID (1-255) Virtuelle Router-ID.

Priority (1-255) (Priorität, 1-255) Routerpriorität, die für den virtuellen Router-Auswahlprozess verwendet wird. Der Wert kann anzeigen, ob ein VRRP-Router mit einer höheren Priorität den mit einer niedrigeren Priorität außer Kraft setzt.

Primary IP Address Primäre IP-Adresse) Virtuelle IP-Adresse, die durch den virtuellen Router identifiziert wird. Die primäre IP-Adresse wird aus tatsächlichen Schnittstellenadressen ausgewählt, die auf einem VRRP-Router konfiguriert sind.

Master IP Address (Master-IP-Adresse) Der VRRP-Router, der derzeit als Master für diesen virtuellen Router aktiv ist.

State (Status) Der aktuelle Status des Routers. Die möglichen Werte sind:

Master (Master) Der Router fungiert als Übermittlungsrouter für die mit dem virtuellen Router assoziierten IP-Adresse. Der Master-Router antwortet auf ARP-Anforderungen mit assoziierten IP-Adressen im ARP-Ziel, befördert Pakete mit virtuellen MAC-Adressen (VMAC) als Ziel-MAC und nimmt Pakete an, die mit den virtuellen IP-Adressen assoziiert sind (nur wenn der Router die assoziierte IP-Adresse besitzt).

Initialize (Initialisieren) Der Router warten auf das Startereignis. Wenn das Startereignis empfangen wird, geht der Router zum entsprechenden Status über.

Backup (Sicherung) Der Router sichert sich beim Master-Router ab. Der Router prüft kontinuierlich die Verfügbarkeit des Master-Routers mittels regelmäßiger Meldungen, die der Master sendet, oder durch besondere Bekanntgaben, die der Master sendet, um anzukündigen, dass er nicht mehr zur Verfügung stehen wird.

Admin State (Verwaltungsstatus) Gibt an, ob der Router zur Verfügung steht.

Advertisement Interval (Meldungsintervall) Gibt den Abstand an, in dem Meldungen versendet werden, wenn der Router als Master fungiert.

Authentication (Authentifizierung) Legt fest, ob kein Authentifizierungsprozess stattfindet oder ob Kennwörter für die Authentifizierung des VRRP-Protokoll-Austauschs verwendet werden.

Password (Kennwort) Das Kennwort, das für die Authentifizierung des VRRP-Protokollaustauschs verwendet wird.

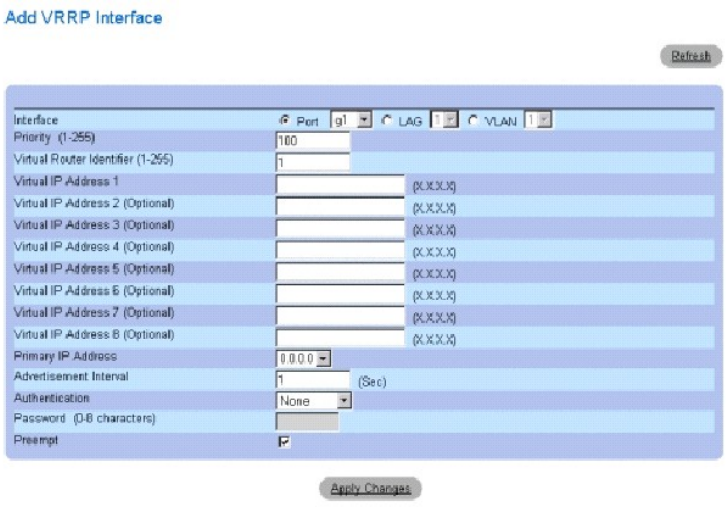
Preempt (Vorbelegen) Wenn diese Funktion ausgewählt ist, können VRRP-Router mit einer höheren Priorität Router mit niedrigerer Priorität außer Kraft setzen.

Remove (Entfernen) Wenn diese Funktion ausgewählt ist, werden VRRP-Einträge aus der VRRP-Tabelle entfernt.

Hinzufügen von Routern zu einer VRRP-Gruppe

1. Öffnen Sie die Seite **Virtuelles Router-Redundanzprotokoll (VRRR)**.
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add VRRP Interface** (VRRP-Schnittstelle hinzufügen) anzuzeigen.

Abbildung 8-4. VRRP-Schnittstelle hinzufügen



3. Definieren Sie die Felder.

Weitere Informationen über die Felder erhalten Sie unter Konfigurieren von VRRP".

ANMERKUNG: VRRP-Schnittstellen müssen definiert werden, bevor der **Admin State** (Verwaltungsstatus) auf **Enabled** (Aktiviert) gesetzt werden kann.

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

Die neue VRRP-Schnittstelle wird hinzugefügt und das Gerät aktualisiert.

ANMERKUNG: Wird eine unzulässige virtuelle IP-Adresse eingegeben, erscheint zwar eine Warnung, jedoch wird der virtuelle Router trotzdem hinzugefügt. Es wird empfohlen, diesen Eintrag aus der virtuellen Routertabelle zu löschen.

Ändern von VRRP-Routern

1. Öffnen Sie die Seite **Virtuelles Router-Redundanzprotokoll (VRRR)**.
2. Wählen Sie eine Schnittstelle im Feld **Interface.**
3. Definieren Sie die Felder nach Wunsch.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Entfernen eines VRRP-Eintrags

1. Öffnen Sie die Seite **Virtuelles Router-Redundanzprotokoll (VRRR)**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **VRRP Table** (VRRP-Tabelle) anzuzeigen.
3. Wählen Sie einen Tabelleneintrag.
4. Klicken Sie das Kontrollkästchen **Remove** (Entfernen) an.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der VRRP-Eintrag wird entfernt und das Gerät aktualisiert.

Konfigurieren von VRRP mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Konfigurieren von VRRP.

Tabelle 8-3. CLI-Befehle zu VRRR

CLI-Befehl	Beschreibung
vrrp *virtual-router* ip *ip-address* [*ip- address2...ip-address8*]	Definiert das virtuelle Routerredundanzprotokoll (VRRR) für eine Schnittstelle.
vrrp *virtual-router* up	Aktiviert VRRP auf einer Schnittstelle.
vrrp *virtual-router* timer *seconds*	Konfiguriert das Zeitintervall zwischen dem Senden von Bekanntgabemeldungen.
vrrp *virtual-router* priority *priority*	Konfiguriert die VRRP-Priorität auf einer Schnittstelle.
vrrp *virtual-router* source-ip *ip-address*	Definiert die Quell-IP-Adresse (primäre IP-Adresse), die für VRRP-Meldungen auf einer Schnittst
vrrp *virtual-router* authentication *text*	Ermöglicht die Authentifizierung von VRRP auf einer Schnittstelle.
vrrp *virtual-router* preempt	Ermöglicht die Vorbelegung von VRRP auf einer Schnittstelle.
show vrrp configuration [ethernet *interface*-number | *vlan vlan-id* | *port-channel number*]	Zeigt die VRRP-Konfiguration an.
	Zeigt den VRRP-Status an.

show vrrp status [ethernet *interface-number* | *vlan vlan-id* | *port-channel number*]

Konfigurieren von VRRP mithilfe der CLI-Befehle

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

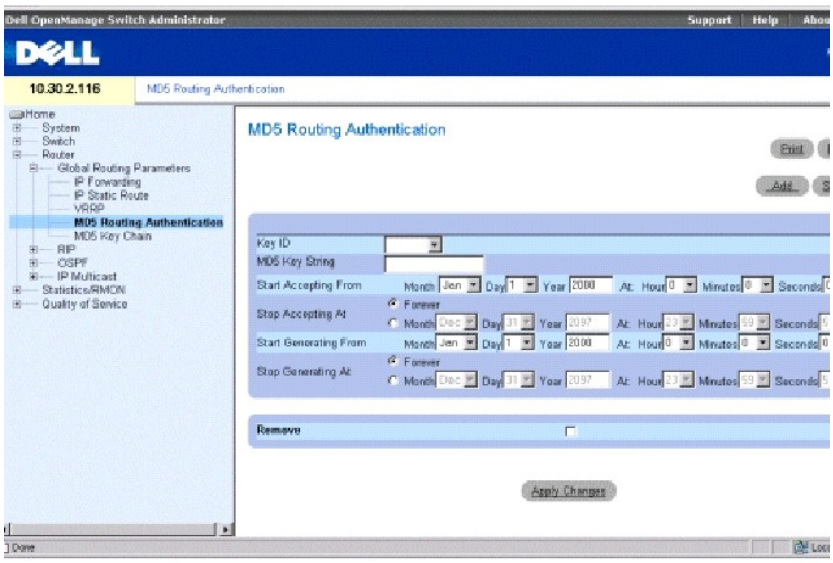
```
Console (config)# interface ethernet g8

Console (config-if)# vrrp 45 ip 172.16.1.1 172.16.2.1

Console (config-if)# vrrp 45 up

Console (config-if)# vrrp 45 timer 100

Console (config-if)# vrrp 45 priority 150

Console (config-if)# vrrp 45 source-ip 168.192.1.1

Console (config-if)# vrrp 45 authentication Dell

Console (config-if)# vrrp 45 preempt

Console (config-if)# exit

Console (config)# exit
```

Konfigurieren der MD5-Routing-Authentifizierung

MD5-Tasten werden durch den Message Digest-5 Authentifizierungsalgorithmus verwendet. Die Start- und Endzeiten sowohl für Senden als auch Empfangen können für jeden Schlüssel definiert werden. Aktive Schlüssel, die zur Rücksetzzeit ihre Gültigkeit verlieren, können konfiguriert werden. Schnittstellen, die untereinander kommunizieren, müssen die gleiche Schlüssel-ID haben. Wenn sich die Schlüsselzeiten auf Senderseite überlappen, verwendet das Gerät den Schlüssel mit der spätesten Startzeit. Beim Empfangen von Paketen verwendet die Schnittstelle den Schlüssel, der als **Schlüssel-ID** auf dem Paket angegeben ist.

Verwenden Sie die Seite **MD5 Routing Authentication** (MD5-Routing-Authentifizierung), um Schlüssel zu definieren und zu verwalten. Um die Seite **MD-Routing-Authentifizierung** zu öffnen, klicken Sie in der Strukturansicht auf **Router**→ **Global Routing Parameters**→ **MD5 Routing Authentication**.

Abbildung 8-5. MD5-Routing-Authentifizierung



Key ID (Schlüssel-ID) Legt die Schlüssel-ID fest.

MD5 Key String (MD5-Schlüsselzeichenkette) Gibt das für die Routing-Authentifizierung verwendete Kennwort an.

Start Accepting From (Annahme beginnen ab) Datum und Uhrzeit, zu der der MD5-Schlüssel beginnt, Datenverkehr mit dem spezifischen MD5-Schlüssel anzunehmen. Das Feld **Start Accept** (Annahme starten) hat das Format **Monat Tag Jahr: Stunde Minute Sekunde**.

Stop Accepting At (Annahme stoppen ab) Datum und Uhrzeit, zu der der MD5-Schlüssel aufhört, Datenverkehr mit dem spezifischen MD5-Schlüssel anzunehmen. Das Feld **Start Accept** (Annahme stoppen) hat das Format **Monat Tag Jahr: Stunde Minute Sekunde**. Wenn **Forever** (Immer) ausgewählt wurde, ist die Annahme von Datenverkehr mit MD5-Schlüsseln unbegrenzt.

Start Generating From (Senden beginnen ab) Datum und Uhrzeit, zu der Protokollpakete mit MD5-Schlüsseln gesendet werden. Das Feldformat für **Start Generate** (Senden beginnen) ist **Monat Tag Jahr: Stunde Minute Sekunde**.

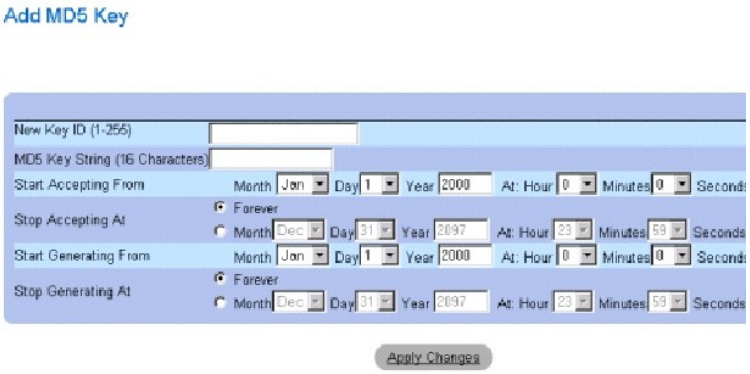
Stop Generating At (Senden stoppen ab) Datum und Uhrzeit, zu der die Protokollpakete nicht mehr mit MD5-Schlüsseln gesendet werden. Das Feldformat für **Stop Generate** (Senden stoppen) ist **Monat Tag Jahr: Stunde Minute Sekunde**. Wenn **Forever** (Immer) ausgewählt wurde, ist die Annahme von Datenverkehr mit MD5-Schlüsseln unbegrenzt.

Remove (Entfernen) Wenn diese Option markiert ist, wird der MD5-Schlüssel entfernt.

Hinzufügen eines MD5-Schlüssels

1. Öffnen Sie die Seite **MD5-Routing-Authentifizierung**.
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add MD5 Key** (Hinzufügen eines MD5-Schlüssels) anzuzeigen.

Abbildung 8-6. MD5-Schlüssel hinzufügen



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

Der neue MD5-Schlüssel wird der **MD5 Key Table** (MD5-Schlüsseltabelle) hinzugefügt und das Gerät aktualisiert.

Ändern eines MD5-Schlüssels

1. Öffnen Sie die Seite **MD5-Routing-Authentifizierung**.
2. Wählen Sie aus dem Drop-Down-Menü **Entry No.** (Eintragsnr.) den MD5-Schlüssel, den Sie ändern möchten.
3. Ändern Sie die Dialogfelder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der neue MD5-Schlüssel wird geändert und das Gerät aktualisiert.

Entfernen eines MD5-Schlüssels

1. Öffnen Sie die Seite **MD5-Routing-Authentifizierung**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **MD5 Key Table** (MD5-Schlüsseltabelle) anzuzeigen.
3. Wählen Sie einen Eintrag aus dem Feld **Key ID** (Schlüssel-ID).
4. Klicken Sie das Kontrollkästchen **Remove** (Entfernen) an.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der MD5-Schlüssel wird entfernt und das Gerät aktualisiert.

Konfigurieren der MD5-Authentifizierung mithilfe von CLI-Befehlen

Die folgende Tabelle beinhaltet die CLI-Befehle zum Konfigurieren der MP5-Authentifizierung.

Tabelle 8-4. CLI-Befehle für MD5-Authentifizierung

CLI-Befehl	Beschreibung
key *key-id*	Erstellt einen Authentifizierungsschlüssel.
	Stellt die Zeitspanne ein, in der der Authentifizierungsschlüssel auf einer

`accept-lifetime { duration time-to-start day-of-the-month` *`day-of-the-month`* `year-to-start key-lifetime-duration-in-seconds } | { infinite time-to-start day-of-the-month` *`day-of-the-month`* `year-to-start } | { time-to-start day-of-the-month` *`day-of-the-month`* `year-to-start time-to-stop day-of-the-month` *`day-of-the-month`* `year-to-stop }`	Schlüsselkette empfangen werden kann.
`send-lifetime { duration time-to-start day-of-the-month` *`day-of-the-month`* `year-to-start key-lifetime-duration-in-seconds } | { infinite time-to-start day-of-the-month` *`day-of-the-month`* `year-to-start } | { time-to-start day-of-the-month` *`day-of-the-month`* `year-to-start time-to-stop day-of-the-month` *`day-of-the-month`* `year-to-stop }`	Stellt die Zeitspanne ein, in der ein Authentifizierungsschlüssel auf einer Schlüsselkette gesendet werden kann.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# key 3
```

```
Console (config-key)# accept-lifetime duration 13:30:00 Jan 25 2002 7200
```

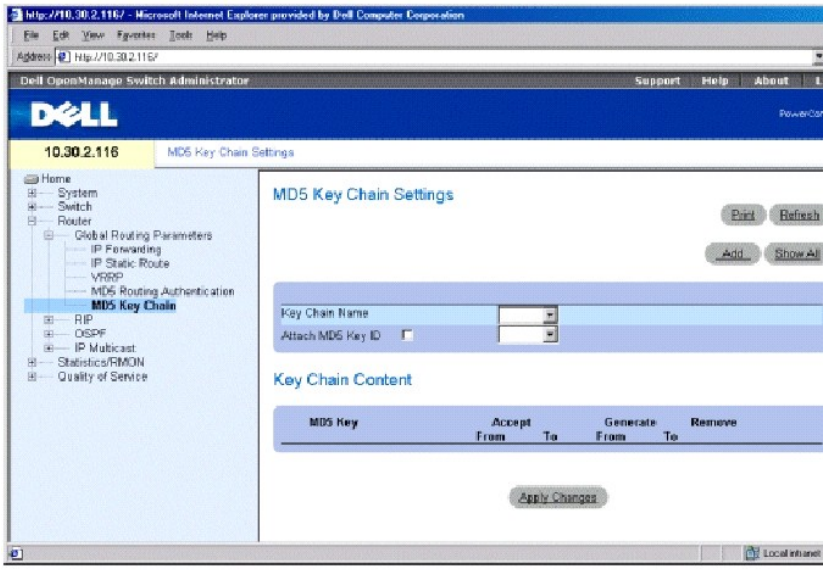
```
Console (config-key)# send-lifetime duration 14:00:00 Jan 25 2002 3600
```

Konfigurieren von MD5-Schlüsselketteneinstellungen

Nachdem die Schlüssel definiert wurden, werden Sie in einer so genannten Schlüsselkette" angeordnet. Jeder Router-Schnittstelle können mehrere Schlüssel auf einmal zugewiesen werden. Schlüssel können zur einfacheren Schnittstellenzuweisung in Schlüsselketten angeordnet werden. Jeder Schlüssel kann in mehreren Schlüsselketten enthalten sein. Schlüsselketten werden den Schnittstellen über RIP- oder OSPF-Schnittstellenparameter zugewiesen. MD5-Schlüssel werden einer MD5-Schlüsselkette hinzugefügt, um die Schlüsselkette zu generieren.

Verwenden Sie die Seite **MD5 Key Chain Settings** (MD5-Schlüsselketteneinstellungen), um Schlüsselketten zu definieren und ihnen Schlüssel zuzuweisen. Um die Seite **MD5-Schlüsselketteneinstellungen** zu öffnen, klicken Sie in der Strukturansicht auf **Router→ Global Routing Parameters→ MD5 Key Chain**.

Abbildung 8-7. MD5-Schlüsselketteneinstellungen



Key Chain Name (Schlüsselkettenname) Benutzerdefinierte Namen der Schlüsselzeichenkette.

Attach MD5 Key ID (Zuweisen der MD5-Schlüssel-ID) Gibt die ID der Schlüsselzeichenkette an, die der Schlüsselkette zugewiesen wurde.

MD5 Key (MD5-Schlüssel) Der Schlüssel, der Teil der Schlüsselkette ist.

Accept From (Annahme ab) Datum und Uhrzeit, zu der der ausgewählte MD5-Schlüssel beginnt, Datenverkehr mit dem festgelegten MD5-Schlüssel anzunehmen. Das Format für Feld **Accept From** (Annahme ab) ist **Monat Tag Jahr: Stunde Minute Sekunde**. Das Feld **Accept From** (Annahme ab) stellt den Schlüssel dar, der auf der Seite **MD5-Routing-Authentifizierung** definiert wurde.

Accept To (Annahme bis) Datum und Uhrzeit, zu der der MD5-Schlüssel aufhört, Datenverkehr mit dem festgelegten MD5-Schlüssel zuzulassen. Das Format des Feldes ist **Monat Tag Jahr: Stunde Minute Sekunde**. Das Feld **Accept To** (Annahme bis) stellt den Schlüssel dar, der auf der Seite **MD5-Routing-Authentifizierung** definiert wurde.

Generate From (Senden ab) Datum und Uhrzeit, zu der der ausgewählte MD5-Schlüssel beginnt, Datenverkehr zu senden. Das Feldformat für **Generate From** (Senden ab) ist **Monat Tag Jahr: Stunde Minute Sekunde**. Das Feld **Generate From** (Senden ab) stellt den Schlüssel dar, der auf der Seite **MD5-Routing-Authentifizierung** definiert wurde.

Generate To (Senden bis) Datum und Uhrzeit, zu der der ausgewählte MD5-Schlüssel aufhört, Datenverkehr zu senden. Das Feldformat für **Generate To** (Senden bis) ist **Monat Tag Jahr: Stunde Minute Sekunde**. Das Feld **Generate To** (Senden bis) stellt den Schlüssel dar, der auf der Seite **MD5-Routing-Authentifizierung** definiert wurde.

Remove (Entfernen) Wenn diese Funktion ausgewählt ist, wird der MD5-Schlüssel von der MD5-Schlüsselkettentabelle entfernt.

Hinzufügen einer MD5-Schlüsselkette

1. Öffnen Sie die Seite **MD5-Schlüsselketteneinstellungen**.
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add MD5 Key Chain** (MD5-Schlüsselkette hinzufügen) anzuzeigen.
3. Füllen Sie die Felder **New Key Chain Name** (Neuer Schlüsselkettenname) und **Attach MD5 Key No.** (MD5-Schlüsselnummer zuweisen) aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die neue MD5-Schlüsselkette wird der Tabelle **MD5 Key Chain Table** (MD5-Schlüsselkettentabelle) hinzugefügt und das Gerät aktualisiert.

Ändern einer MD5-Schlüsselkette

1. Öffnen Sie die Seite **MD5-Schlüsselketteneinstellungen**.
2. Ändern Sie die Felder **Name** und/ oder **Key Chain ID** (Schlüsselketten-ID).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die neue MD5-Schlüsselkette wird geändert und das Gerät aktualisiert.

Entfernen einer MD5-Schlüsselkette

1. Öffnen Sie die Seite **MD5-Schlüsselketteneinstellungen**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Tabelle **MD5 Key ChainTable** (MD5-Schlüsseltabelle) anzuzeigen.
3. Wählen Sie einen Eintrag im Feld **Key Chain Name** (Schlüsselkettenname).
4. Klicken Sie das Kontrollkästchen **Remove** (Entfernen) an.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die MD5-Schlüsselkette wird entfernt und das Gerät aktualisiert.

Konfigurieren der Schlüsselketten mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Konfigurieren der Schlüsselketten.

Tabelle 8-5. CLI-Befehle für Schlüsselketten

CLI-Befehl	Beschreibung
`key-chain name-of-chain`	Identifiziert eine Authentifizierungsschlüsselgruppe.
`key key-id`	Identifiziert einen Authentifizierungsschlüssel auf einer Schlüsselkette.
`key-string text`	Legt eine Authentifizierungszeichenkette für einen Schlüssel fest.
`accept-lifetime start-time end- time | {infinite | start-time | duration start- time seconds} no accept-lifetime`	Stellt die Zeitspanne ein, in der der Authentifizierungsschlüssel gültig ist, um ankommende Pakete zu authentifizieren.
`send-lifetime start-time end- time | {infinite | start-time | duration start- time seconds}no send-lifetime`	Stellt die Zeitspanne ein, in der ein Authentifizierungsschlüssel gültig ist, um einen MD5-Digest (Auszug) für ausgehende Pakete zu generieren.
`show key-chains [name-of-chain]`	Zeigt Informationen über die Schlüsselkette an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# key chain M

Console (config-key-chain)# key 1

Console (config-key)# key-string mountain

Console (config-key)# accept-lifetime duration 13:30:00 Jan 25 2002 7200

Console (config-key)# send-lifetime duration 14:00:00 Jan 25 2002 3600

Console (config-key)# exit

Console (config)# exit

Console# show key-chains

key chain internal

key 1

accept: 13:30:00 Jan 25 2002 duration 7200

send: 14:00:00 Jan 25 2002 duration 3600
```

```
key 2

accept: 14:30:00 Jan 25 2002 duration 7200

send: 15:00:00 Jan 25 2002 duration 3600

key chain external

key 1

accept: 13:30:00 Jan 25 2002 until 15:30:00 Jan 25 2002

send: 14:00:00 Jan 25 2002 until 15:00:00 Jan 25 2002

key 2

accept: 14:30:00 Jan 25 2002 until 16:30:00 Jan 25 2002

send: 15:00:00 Jan 25 2002 until 16:00:00 Jan 25 2002

25 2002
```

Konfigurieren von RIP

Das **Routing Information Protocol** (Routing-Informationsprotokoll) ist der am häufigsten verwendete Internetstandard für Interior Gateway Protocols. Das Protokoll übermittelt Routinginformationen, um die schnellste Route zum nächsten Zielort zu bestimmen. RIP ist ein Routingprotokoll auf Basis von Distanzvektoren, das idealerweise in kleinen Netzwerken verwendet wird. Die Routen werden anhand des niedrigsten Hopcounts (Anzahl von Hops) bestimmt. Routing-Aktualisierungen beinhalten Wertepaare, die aus einer IP-Adresse und der Entfernung zum Knoten bestehen.

RIP-Version 2 zeichnet sich wie folgt aus:

- Es unterstützt Subnetzmasken.
- Es liefert Authentifizierungsmethoden.
- Es unterstützt Routingprotokolle.
- Es liefert eine breitere Verteilung bei niedrigeren Anforderungen an die Restkapazitäten der Bandbreiten.

RIP wird auf der Seite **RIP** konfiguriert. Um die Seite **RIP** zu öffnen, klicken Sie in der Strukturansicht auf **Router→ RIP**.

Definieren von globalen RIP-Parametern

Die Seite **RIP Global Parameters** (Globale RIP-Parameter) bietet Felder für die Aktivierung von RIP auf dem Gerät an sowie für die Umverteilung von OSPF und die Umverteilung statischer Routen.

Klicken Sie in der Strukturansicht auf **Router→ RIP→ Global Parameters**, um die Seite **Globale RIP-Parameter** zu öffnen.

Abbildung 8-8. Globale RIP-Parameter

RIP Status (RIP-Status) Aktivieren oder deaktiviert RIP auf dem Gerät.

Redistribute OSPF Routes (OSFP-Routen umverteilen) Wenn diese Funktion ausgewählt ist, werden Routen von OSPF zu RIP umverteilt. Die Umverteilung von Routen beinhaltet das Importieren fremder Routing-Schnittstellen in RIP.

Redistribute Static Routes (Statische Routen umverteilen) Wenn diese Funktion ausgewählt ist, werden Routen von statischen Route zu RIP umverteilt.

Aktivieren von RIP, Umverteilen von OSPF-Routen, Umverteilen von statischen Routen

1. Öffnen Sie die Seite **RIP Global Parameters** (Globale RIP-Parameter).
2. Wählen Sie **Enabled** (Aktiviert) in dem Feld globaler RIP-Parameter, das Sie aktivieren möchten.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

RIP ist auf dem Gerät aktiviert.

Konfigurieren globaler RIP-Parameter mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Konfigurieren der globalen RIP-Parameter.

Tabelle 8-6. CLI-Befehle zu globalen RIP-Parametern

CLI-Befehl	Beschreibung
`router rip enable`	Aktiviert RIP auf dem Gerät.
`no router rip enable`	Deaktiviert RIP auf dem Gerät.
`router rip redistribute ospf`	Gibt Routen bekannt, die OSPF während des RIP-Vorgangs gelernt hat.
`no router rip redistribute ospf`	Unterbindet die Bekanntgabe von Routen, die OSPF während des RIP-Vorgangs gelernt hat.
	Gibt Routen bekannt, die während des RIP-Vorgangs statisch konfiguriert wurden.

`router rip redistribute static`	
`no router rip redistribute static`	Unterbindet die Bekanntgabe von Routen, die während des RIP-Vorgangs statisch konfiguriert wurden.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# router rip enable

Console (config)# router rip redistribute ospf

Console (config)# router rip redistribute static

Console (config)# no router rip enable

Console (config)# no router rip redistribute ospf

Console (config)# no router rip redistribute static
```

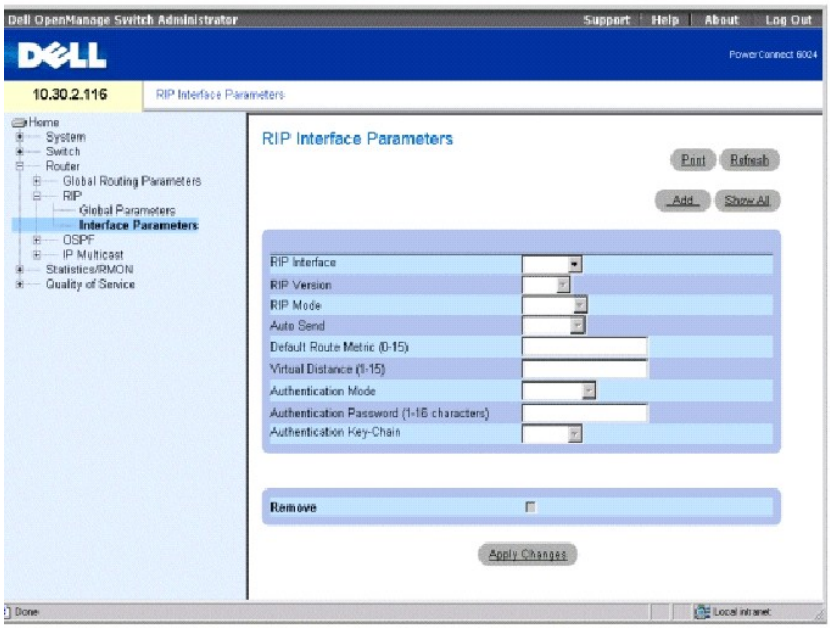
Definieren von RIP-Schnittstellenparametern

Verwenden Sie die Seite **RIP-Schnittstellenparameter**, um die IP-Adressen zu definieren, auf denen RIP aktiviert ist, um Routingmetriken zu definieren, **Auto Send** (Automatisches Senden) zu aktivieren, die virtuelle Entfernung zu definieren und den IP-Status zu definieren.

ANMERKUNG: Um eine RIP-Schnittstelle zu definieren, muss RIP aktiviert sein. Weitere Informationen finden Sie unter Aktivieren von RIP, Umverteilen von OSPF-Routen, Umverteilen von statischen Routen".

Um die Seite **RIP-Schnittstellenparameter** zu öffnen, klicken Sie in der Strukturansicht auf **Router→ RIP→ RIP Interface Parameters**.

Abbildung 8-9. RIP-Schnittstellenparameter



RIP Interface (RIP-Schnittstelle) Die aktuelle IP-Adresse der Schnittstelle.

RIP Version Der Typ des zu übertragenden RIP. Die möglichen Werte sind:

Ver. 1 Überträgt RFC 1058-konforme RIP-Aktualisierungen.

Ver. 2 Gibt an, dass das Gerät Aktualisierungen der RIP-Version 2 überträgt.

RIP Mode (RIP-Modus) Der Typ der RIP-Operation. Die möglichen Werte sind:

RX RIP-Empfangsbroadcasts werden auf dem Gerät empfangen.

RX & TX RIP-Empfangs- und Sendebroadcasts werden auf dem Gerät empfangen.

Auto Send (Automatisches Senden) Ermöglicht es dem Gerät, RIP-Meldungen nur in der Standardmetrik bekanntzugeben, so dass Stationen die standardmäßige Routeradresse erlernen können. Dadurch wird vermieden, dass der Router zu viele RIP-Aktualisierungen auf Links sendet, die über keinen Empfangsrouter verfügen. Solange **Auto Send** (Automatisches Senden) aktiv ist, wird ein verkürztes RIP-Update gesendet, damit Stationen, die RIP abfangen, u.a. Router Discovery betreiben und ein RIP-Update an die Router senden können, die möglicherweise erst zu einem späteren Zeitpunkt an das Netzwerk angeschlossen werden.

Wird ein RIP-Update auf einer Schnittstelle empfangen, wird **Auto Send** (Automatisches Senden) auf dieser Schnittstelle deaktiviert und vollständige RIP-Aktualisierungen werden gesendet. Erkennt das Gerät eine weitere RIP-Meldung, wird **Auto Send** (Automatisches Senden) deaktiviert.

Default Route Metric (1-16) (Standardrouten-Metrik, (1-16)) Die Eingabemetrik der Standardroute in RIP-Aktualisierungen, die aus dieser Schnittstelle stammen. Null gibt an, dass keine Standardroute entstanden ist.

Virtual Distance (1-16) (Virtuelle Entfernung) Anzahl von virtuellen Hops, die der Schnittstelle zugewiesen werden. Dies ermöglicht die Feinabstimmung des RIP-Routingalgorithmus.

Authentication Mode (Authentifizierungsmodus) Der Authentifizierungstyp der Schnittstellen, Kennwort oder MD5, die verwendet werden, um RIP-Meldungen der Version 2 zu authentifizieren.

Authentication Password (Authentifizierungskennwort) Das Kennwort für die Authentifizierung.

Authentication Key-Chain (Authentifizierungsschlüsselkette) Die Authentifizierungsschlüsselkette.

Remove (Entfernen) Wenn diese Funktion ausgewählt ist, wird die RIP-Schnittstelle entfernt.

Hinzufügen einer RIP-Schnittstelle

1. Öffnen Sie die Seite **RIP Interface Parameters** (RIP-Schnittstellenparameter).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **New RIP Interface** (Neue RIP-Schnittstelle) anzuzeigen.
3. Geben Sie die Informationen in die Felder auf der Seite ein.

   Die Felder auf dieser Seite sind mit den Feldern auf der Seite **RIP-Schnittstellenparameter** identisch.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Ändern von RIP-Schnittstellenparametern

1. Öffnen Sie die Seite **RIP Interface Parameters** (RIP-Schnittstellenparameter).
2. Ändern Sie die Felder wie gewünscht.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die RIP-Schnittstellenparameter werden geändert und das Gerät aktualisiert.

Löschen einer RIP-Schnittstelle

1. Öffnen Sie die Seite **RIP Interface Parameters** (RIP-Schnittstellenparameter).
2. Verwenden Sie das Drop-Down-Menü **RIP Interface** (RIP-Schnittstelle), um eine RIP-Schnittstelle auszuwählen.
3. Klicken Sie das Kontrollkästchen **Remove** (Entfernen) an.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die RIP-Schnittstelle wird entfernt und das Gerät aktualisiert.

Konfigurieren von RIP-Schnittstellen mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Konfigurieren der globalen RIP-Parameter.

Tabelle 8-7. CLI-Befehle für die RIP-Konfiguration

CLI-Befehl	Beschreibung
`rip`	Aktiviert RIP auf einer Schnittstelle.
`rip version {1 | 2}`	Legt eine RIP-Version fest.
`rip passive-interface`	Deaktiviert das Senden von Routing-Aktualisierungen auf einer Schnittstelle.
	Erkennt automatisch, ob auf der Schnittstelle RIP-Informationen gesendet werden müssen.

`rip auto-send`	
`rip offset offset`	Fügt der Metrik einen durch RIP gelernten Offset hinzu, bevor sie der Schnittstellentabelle hinzugefügt wird.
`rip default-route offset *offset*`	Generiert durch Anwendung eines Offset-Wertes eine Standardroute in RIP.
`rip authentication {text *text* | *md5 name-of-chain*}`	Ermöglicht die Authentifizierung von Paketen der RIP-Version 2 und legt den Authentifizierungstypen fest.
`show ip rip`	Zeigt IP-RIP-Informationen an.
`show ip rip md5`	Zeigt IP-RIP-MD5-Informationen an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# router rip enable

Console (config)# interface ip 100.1.1.1

Console (config-ip)# rip

Console (config-ip)# rip version 1

Console (config-ip)# rip passive interface

Console (config-ip)# rip auto-send

Console (config-ip)# rip offset 5

Console (config-ip)# rip default-route offset 5

Console (config-ip)# rip authorization text dell

Console (config-ip)# exit

Console (config)# exit

Console# show ip rip

RIP is enabled.

OSPF leaking is enabled.

Static leaking is enabled.
```

```
Interface State Ver Offset Default Route Passive Auto Send Auth


176.16.0.0/16 Enabled 2 1 Disabled No Yes MD5


192.168.0.0/16 Enabled 2 1 Disabled No No Text
```

Konfigurieren von Parametern und Filtern für OSPF

Das interne Gateway-Protokoll OSPF (OSPF - Open Shortest Path First) ermöglicht es Routern, über die Erfassung von Netzwerkinformationen sogenanten Link State Advertisements auszutauschen und den besten Routingpfad zu bestimmen, der auf Basis der Knotenentfernung ermittelt wird.

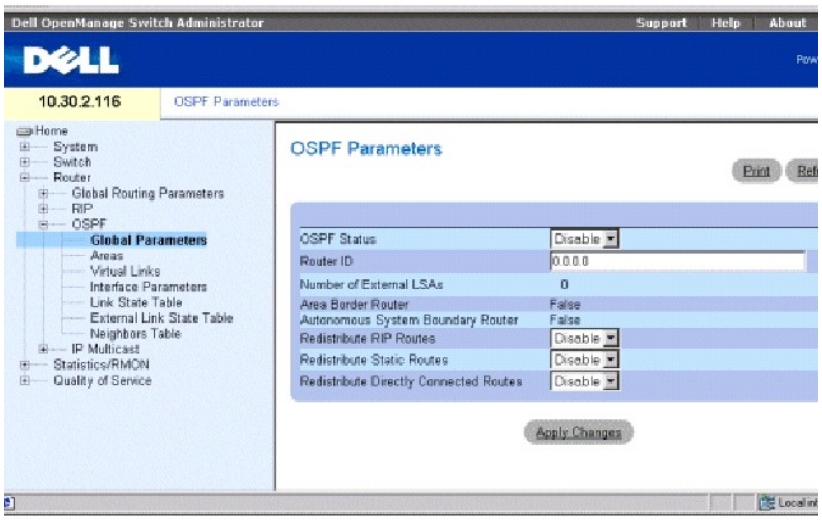
OSPF ist eher ein Link-Status-Protokoll als ein Protokoll auf Basis von Distanzvektoren und benötigt daher eine geringere Bandbreite als RIP. Die Aktivierung und Definition von OSPF geschieht über:

- Konfigurieren von OSPF-Parametern
- Konfigurieren von OSPF-Areas
- Konfigurieren von virtuellen OSPF-Links
- Anzeigen der Link-Status-Tabelle
- Anzeigen der externen Link-Status-Tabelle
- Anzeigen der OSPF-Nachbarntabelle

Konfigurieren von OSPF-Parametern

OSPF ermittelt den besten Routenpfad unter Zugrundelegung der Knotenentfernung. Die Aktivierung von OSPF erfolgt über die Seite **OSPF-Parameter**. Um die Seite **OSPF-Parameter** zu öffnen, klicken Sie in der Strukturansicht auf **Router**→ **OSPF**→ **Global Parameters**.

Abbildung 8-10. Globale OSPF-Parameter



OSPF Status Aktiviert OSPF auf mindestens einer Schnittstelle oder deaktiviert OSPF auf allen Schnittstellen.

Router ID Die Nummer der Router-ID. Standardmäßig ist die Router-ID eine IP-Adresse auf dem Gerät. Das Feld **Router ID** ist optional und beinhaltet einen Standardwert für die kleinste IP-Schnittstelle des Geräts.

Number of External LSAs (Anzahl externer LSAs) Die Anzahl externer Link-Status-Advertisements (LSA) in der Link-Status-Datenbank.

Area Border Router (ABR) Gibt an, ob das Gerät ein Area Border Router ist. Wenn das Gerät als ABR konfiguiert ist, ist das Gerät mit zwei oder mehreren Areas verbunden. Eine Area ist dabei die Backbone Area.

Autonomous System Boundary Router (ASBR) Gibt an, ob das Gerät als ASBR konfigurierbar ist. Wenn das Gerät als ASBR konfiguriert ist, importiert das Gerät Routing-Daten aus Routingprotokollen, die keine OSPF-Protokolle sind.

Redistribute RIP Routes (RIP-Routen umverteilen) Aktiviert oder deaktiviert die Umverteilung von Routen, die der IP-Routingtabelle durch RIP hinzugefügt wurden, um sich in OSPF als externe Routen bekanntzugeben.

Redistribute Static Routes (Statische Routen umverteilen) Ermöglicht es allen statisch konfigurierten Routen, als OSPF-externe Routen bekanntgegeben zu werden oder deaktiviert die Umverteilung von statischen Routen.

Redistribute Directly Connected Routes (Direkt verbundene Routen umverteilen) Ermöglicht es allen externen Routen, sich in OSPF als externe Routen bekanntzugeben, oder deaktiviert die Umverteilung von externen direkten Routen.

Aktivieren von OSPF

1. Öffnen Sie die Seite **OSPF Parameters**.
2. Definieren Sie die Felder **OSPF Status**, **Router ID**, **Redistribute RIP Routes** (RIP-Routen umverteilen), **Redistribute Static Routes** (Statische Routen umverteilen) und **Redistribute Directly Connected Routes** (Direkt verbundene Routen umverteilen).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

OSPF ist auf dem Gerät aktiviert.

ANMERKUNG: OSPF-Prozesse können nur über den CLI-Befehl **clear ip ospf process** gelöscht werden.

Aktivieren von OSPF mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Aktivieren von OSPF.

Tabelle 8-8. CLI-Befehle für OSPF

CLI-Befehl	Beschreibung
`router ospf enable`	Aktiviert den OSPF-Routing-Vorgang.
`router ospf router-id` *`ip-address`*	Konfiguriert eine OSPF-Router-ID.
`router ospf redistribute rip`	Aktiviert durch den RIP-Vorgang gelernte, propagierende Routen im OSPF-Routing-Vorgang.
`router ospf redistribute static`	Propagierende, statisch konfigurierte Routen im OSPF-Routing-Vorgang.
`outer ospf redistribute connected`	Propagierende, direkt verbundene Routen.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# router ospf enable
```

```
Console (config)# router ospf router-id 196.127.2.1
```

```
Console (config)# router ospf redistribute rip
```

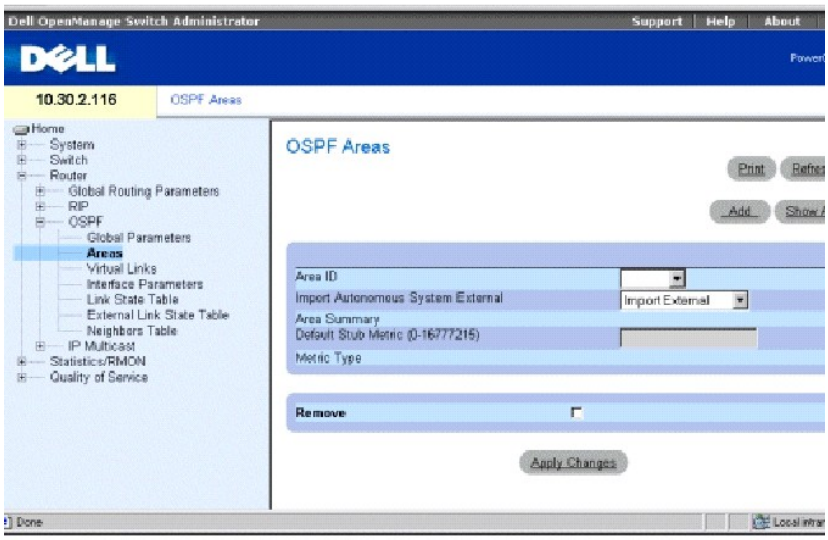
```
Console (config)# router ospf redistribute static
```

Konfigurieren von OSPF-Areas

Die Seite **OSPF Areas** liefert Informationen über Definition und Aufrechterhaltung von OSPF-Areas innerhalb derer Schnittstellen und virtuelle Links definiert sind. Sobald eine OSPF-Area erzeugt wurde, ist OSPF automatisch auf allen IP-Schnittstellen aktiviert.

Um die Seite **OSPF-Areas** zu öffnen, klicken Sie in der Strukturansicht auf **Router**→ **OSPF**→ **Areas**.

Abbildung 8-11. OSPF-Areas



Area ID Die Area-ID. Das Format ist eine IP-Adresse.

Import Autonamous System External (Autonomes System extern importieren) Zeigt an, ob es sich um eine Stub Area handelt. Die möglichen Werte sind:

Import External (Extern importieren) Externe Link-Status-Meldungen (LSA) eines autonomen Systems (AS) können in die Area importiert werden.

Import No External (Nicht extern importieren) Externe LSAs können nicht in die Area importiert werden, da es sich um eine Stub Area handelt.

Area Summary (Area-Zusammenfassung) Steuert den Import von LSA-Zusammenfassungen in die Stub Areas. Diese Variable hat auf andere Areas keine Auswirkung. Die möglichen Werte sind:

No Area Summary (Keine Area-Zusammenfassung) Legt fest, dass es sich um eine Totally Stubby Area handelt.

Send Area Summary (Area-Zusammenfassung senden) Legt fest, dass es sich nicht um eine Totally Stubby Area handelt.

Eine Stub Area ist eine Area, in die externe LSAs autonomer Systeme nicht hineinimportiert werden. Totally Stubby Areas verwenden eine Standardroute nicht nur, um zu Zielen außerhalb des autonomen Systems zu gelangen, sondern auch zu sämtlichen anderen Zielen außerhalb der Area. Um die Vorzüge der OSPF-Stub Area Unterstützung nutzen zu können, muss Default Routing in der Stub Area angewendet werden.

Default Stub Metric (0-16777216) (Standard-Stub-Metrik) Metrik der Standardroute, die für die Stub Area erzeugt wurde. Stub Areas importieren keine externen AS. Deshalb wird eine Standardroute für die Stub Area vom Area Border Router erzeugt.

Metric Type Metriktyp des Protokolls.

Remove (Entfernen) Wenn diese Funktion gewählt wurde, wird die IP-Adresse aus der OSPF-Areatabelle entfernt.

Definieren einer neuen OSPF Area

1. Öffnen Sie die Seite **OSPF Areas**.
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add an OSPF Area** (OSPF-Area hinzufügen) anzuzeigen.
3. Füllen Sie die Felder im Dialogfeld aus.

ANMERKUNG: Das Feld **Stub Metric** ist für Area Border Router definiert.

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

Die neue Area wird der OSPF-Areatabelle hinzugefügt.

Ändern von OSPF-Area-Parametern

1. Öffnen Sie die Seite **OSPF Areas**.
2. Wählen Sie eine **Area ID**.

Die Parameter für die OSPF-Area werden angezeigt.

3. Ändern Sie die Felder wie gewünscht.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Area-Parameter werden geändert und das Gerät aktualisiert.

Entfernen einer OSPF Area

1. Öffnen Sie die Seite **OSPF Areas**.
2. Klicken Sie auf **Show All** (Alle anzeigen) um die OSPF Areatabelle anzuzeigen.
3. Wählen Sie eine OSPF Area und aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die OSPF-Area wird aus der Tabelle entfernt und das Gerät aktualisiert.

Definieren von OSPF-Areas mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Definieren von OSPF-Areas.

Tabelle 8-9. CLI-Befehle für die OSPF-Area

CLI-Befehl	Beschreibung
`router ospf area area-id stub`	Definiert eine Area als Stub Area. Um diese Funktion zu deaktivieren, verwenden Sie bei diesem Befehl die Verneinungsformno.
`router ospf area area-id default-cost cost`	Legt Kosten für die in eine Stub Area gesendete Standardrouten-Zusammenfassung fest.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# router ospf enable
```

```
Console (config)# router ospf area 7.7.7.7 stub
```

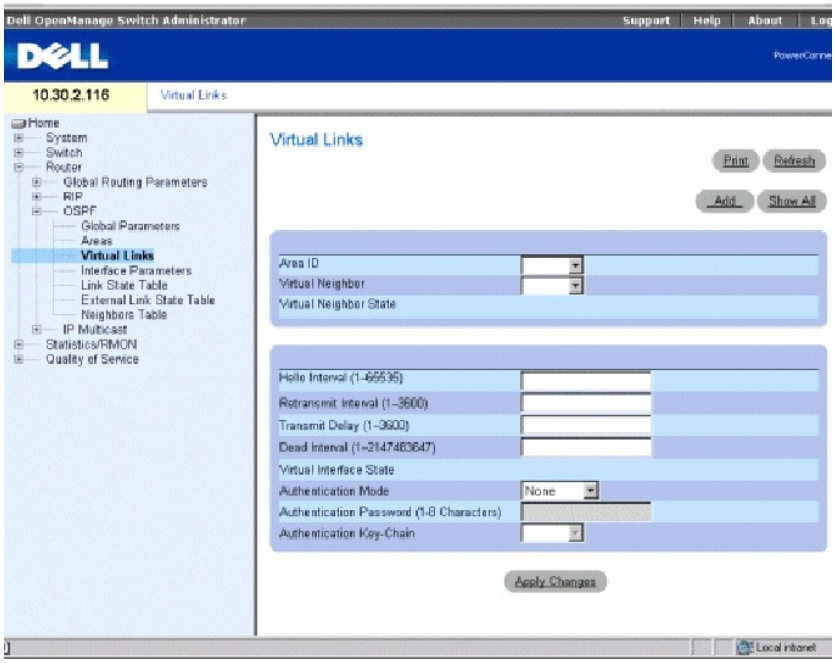
```
Console (config)# router ospf area 192.168.3.1 default-cost 10000
```

Konfigurieren von virtuellen OSPF-Links

OSPF erfordert die Verknüpfung aller Areas über eine Backbone Area. Ist jedoch eine Area nicht mit einem Backbone verbunden, können Sie zwei Area Border Routers mithilfe eines virtuellen Links verbinden. Virtuelle Links werden über die Konfiguration eines virtuellen Nachbarn definiert. Virtuelle Links können nicht durch eine Stub Area konfiguriert werden.

Sie können virtuelle Links auf der Seite **Virtual Links** (Virtuelle Links) definieren. Um die Seite **Virtuelle Links** anzuzeigen, klicken Sie in der Strukturansicht auf **Router→ OSPF→ Virtual Links**.

Abbildung 8-12. Virtuelle Links



Area ID Die OSPF-Schnittstellen-Area-ID der Transit-Area.

Virtual Neighbor (Virtueller Nachbar) Router-ID des virtuellen Nachbarn.

Virtual Neighbor State Status des virtuellen Nachbarn.

Hello Interval (1-65535) (Hello-Intervall) Zeit (in Sekunden) zwischen den Hello-Paketen. Alle auf einem gemeinsamen Netzwerk verbundenen Geräte müssen das gleiche Hello-Intervall haben. Der Standardwert des Feldes ist 10 Sekunden.

Retransmit Interval (0-3600) (Übertragungsintervall) Zeit (in Sekunden) zwischen der erneuten Übertragung von Link State Advertisements (LSAs) für zur Schnittstelle gehörende Umgebungen. Der Wert muss höher sein als die erwartete Umlaufverzögerung (Round-Trip Delay) zwischen zwei beliebigen Routern auf dem verbundenen Netzwerk. Standard sind 5 Sekunden.

Transmit Delay (0-3600) (Übertragungsverzögerung) Erwartete Zeit (in Sekunden), die benötigt wird, um ein Update-Paket des Linkstatus auf der Schnittstelle zu senden. LSAs des Update-Pakets sind um diesen Zeitwert älter, bevor sie übertragen werden. Der Standardwert ist eine Sekunde.

Dead Interval (0-2147483647) (Totzeit) Zeit (in Sekunden), in der keine Hello-Pakete erkannt wurden und der Router für nicht verfügbar erklärt wird. Der Wert muss ein Vielfaches des Wertes für das **Hello-Intervall** sein. Alle an ein gemeinsames Netzwerk angeschlossenen Router müssen einen Wert für diesen Parameter festgelegt haben. Standard sind 60 Sekunden.

Virtual Interface State (Virtueller Schnittstellenstatus) Gibt den Status der virtuellen Schnittstelle an.

Authentication Mode (Authentifizierungsmodus) Der Authentifizierungstyp der Schnittstelle, Kennwort oder MD5-Schlüssel die verwendet werden, um OSPF-Link-Status-Meldungen zu authentifizieren.

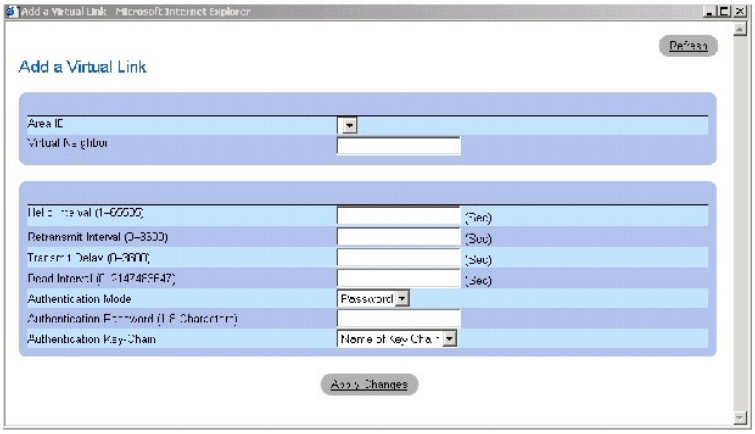
Authentication Password (1-8 Zeichen) Das Kennwort (maximal 8 Zeichen) für die Authentifizierung von OSPF-Link-Status-Meldungen.

Authentication Key-Chain (Authentifizierungsschlüsselkette) Die MD5-Schlüsselkette für die Authentifizierung von OSPF-Link-Status-Meldungen.

Hinzufügen eines virtuellen Links

1. Öffnen Sie die Seite **Virtual Links** (Virtuelle Links).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add a Virtual Link** (Virtuellen Link hinzufügen) anzuzeigen.

Abbildung 8-13. Virtuelle Links hinzufügen



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

Der neue virtuelle OSPF-Link wird hinzugefügt.

Ändernen virtueller Links

1. Öffnen Sie die Seite **Virtual Links** (Virtuelle Links).
2. Wählen Sie aus dem Drop-Down-Menü **Area ID** eine Area-ID.

Die Feldparameter werden angezeigt.

3. Ändern Sie die gewünschten Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Parameter des virtuellen OSPF-Links werden geändert und auf dem Gerät gespeichert.

Entfernen eines virtuellen OSPF-Links

1. Öffnen Sie die Seite **Virtual Links** (Virtuelle Links).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Tabelle **Virtual Links** (Virtuelle Links) anzuzeigen.
3. Wählen Sie einen virtuellen Link.

Die Feldparameter für den Tabelleneintrag werden angezeigt.

4. Klicken Sie das Kontrollkästchen **Remove** (Entfernen) an.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der virtuelle Link wird entfernt und das Gerät aktualisiert.

Anzeigen von virtuellen OSPF-Links mithilfe von CLI-Befehlen

Die folgende Tabelle beinhaltet die CLI-Befehle zum Definieren von OSPF-Areas.

Tabelle 8-10. CLI-Befehle für virtuelle OSPF-Links

CLI-Befehl	Beschreibung
`show ip ospf virtual-links [area area-id] [router router-id]`	Zeigt die Parameter und den aktuellen Status virtueller OSPF-Links an.
`router ospf area area-id virtual-link router-id`	Fügt einen virtuellen Link hinzu.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# show ip ospf virtual-links

Virtual Link to router 192.168.101.2 is up

Virtual link has simple password authentication

Transit area 0.0.0.1

Transmit Delay is 1 sec, State POINT_TO_POINT

Timer intervals configured, Hello 10, Dead 40, Retransmit 5

Adjacency State FULL

Console (config)#router ospf area 176.16.1.0 virtual-link 176.16.8.7

Console (config)#router ospf area 176.16.1.0 virtual-link 176.16.8.7
```

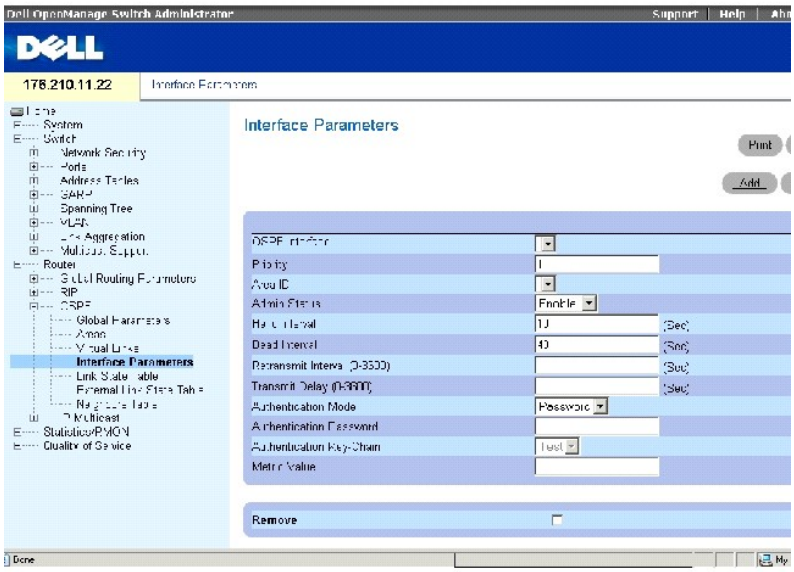
Konfigurieren von OSPF-Schnittstellenparametern

Wenn Sie die Definition der globalen OSPF-Parameter und Areas abgeschlossen haben, können Sie OSPF auf jeder Schnittstelle konfigurieren.

Die Funktion „Auto-creation" ermöglicht eine automatische Konfiguration von OSPF auf jeder Schnittstelle, wenn zuvor eine Area definiert worden ist. OSPF-Schnittstellen können auch benutzerbezogen definiert werden. Die OSPF-Schnittstellentabelle ermöglicht IP-Routing mithilfe von OSPF-spezifischen Informationen.

Um die Seite **Schnittstellenparameter** anzuzeigen, klicken Sie in der Strukturansicht auf **Router→ OSPF→ Interface Parameters**.

Abbildung 8-14. Schnittstellenparameter



OSPF Interface (OSPF-Schnittstelle) Die IP-Adresse der OSPF-Schnittstelle.

Priority (Priorität) Die Priorität der Schnittstelle. Der Wert 0 (Null) gibt an, dass das Gerät nicht als vorgesehenes Gerät auf dem aktuellen Netzwerk definiert werden kann. Wenn mehrere Geräte die gleiche Priorität haben, wird die Router-ID verwendet. Der Bereich der möglichen Feldwerte ist 0-255. Der Standardwert ist 1.

Area ID Die Area-ID der OSPF-Schnittstelle.

Admin Status (Verwaltungsstatus) Aktiviert oder deaktiviert den OSPF-Vorgang.

Hello Interval (Hello-Intervall) Zeitintervall (in Sekunden) zwischen den Hello-Paketen. Alle auf einem gemeinsamen Netzwerk verbundenen Geräte müssen das gleiche Hello-Intervall haben. Der Bereich der möglichen Feldwerte ist 1-65535. Der Standardfeldwert ist 10 Sekunden.

Dead Interval (Totzeit) Zeitintervall (in Sekunden), bis der Router für nicht verfügbar erklärt wird, nachdem keine Hello-Pakete erkannt worden sind. Der Wert muss ein Vielfaches des Wertes für das **Hello-Intervall** sein. Alle an ein gemeinsames Netzwerk angeschlossenen Router müssen einen Wert für diesen Parameter festgelegt haben. Der Bereich der möglichen Feldwerte ist **1-2147483647.** Der Standardfeldwert ist viermal höher als der Wert des **Hello-Intervalls**.

Retransmit Interval (0-3600) (Übertragungsintervall) Zeitintervall (in Sekunden) bis zur erneuten Übertragung von Link-State Advertisements (LSAs) für zur Schnittstelle gehörende Umgebungen. Der Wert muss höher sein als die erwartete Umlaufverzögerung (Round-Trip Delay) zwischen zwei beliebigen Routern auf dem verbundenen Netzwerk. Standard sind 5 Sekunden.

Transmit Delay (0-3600) (Übertragungsverzögerung) Erwartete Zeitspanne (in Sekunden), die erforderlich ist, um ein Update-Paket des Link-Status auf der Schnittstelle zu senden. LSAs des Update-Pakets sind um diesen Zeitwert älter, bevor sie übertragen werden. Der Standardwert ist eine Sekunde.

Authentication Mode (Authentifizierungsmodus) Der Authentifizierungstyp der Schnittstelle, Kennwort oder MD5-Schlüssel die verwendet werden, um OSPF-Link-Status-Meldungen zu authentifizieren.

Authentication Password (Authentifizierungskennwort) Kennwort für die Authentifizierung von OSPF-Link-Status-Meldungen. Das Kennwort darf aus maximal acht Zeichen bestehen.

Authentication Key-Chain (Authentifizierungsschlüsselkette) Die MD5-Schlüsselkette für die Authentifizierung von OSPF-Link Status Advertisements.

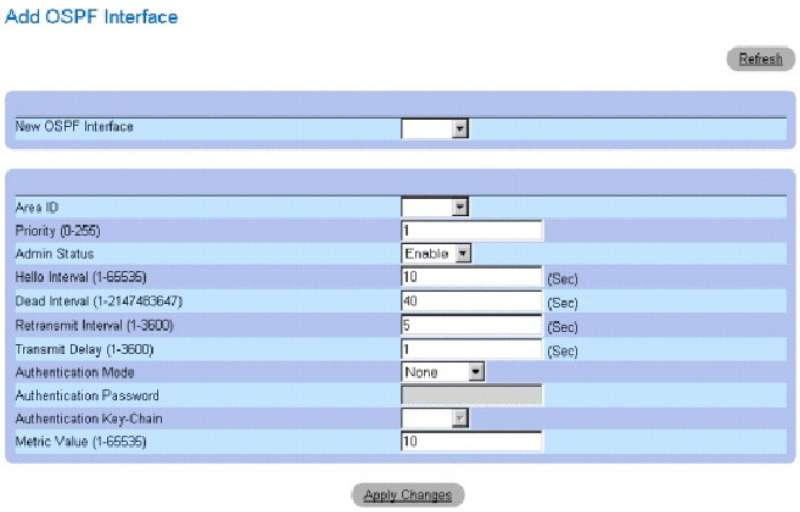
Metric Value (Metrikwert) Metrik für diesen Servicetyp auf der Schnittstelle. Der Bereich der möglichen Feldwerte ist **1-65535**.

Remove (Entfernen) Wenn diese Funktion ausgewählt ist, wird eine OSPF-Schnittstelle entfernt.

Hinzufügen einer OSPF-Schnittstelle

1. Öffnen Sie die Seite **Schnittstellenparameter**.
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add OSPF Interface** (OSPF-Schnittstelle hinzufügen) anzuzeigen.

Abbildung 8-15. OSPF-Schnittstelle hinzufügen



3. Geben Sie die Informationen in die Felder auf der Seite ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die neue OSPF-Schnittstelle wird dem Gerät hinzugefügt.

Ändern von OSPF-Parametern

1. Öffnen Sie die Seite **Schnittstellenparameter**.
2. Wählen Sie eine OSPF-Schnittstelle, um die Feldparameter für den Tabelleneintrag anzuzeigen.
3. Ändern Sie die gewünschten Parameter.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die OSPF-Parameter werden geändert und auf dem Gerät gespeichert.

Entfernen einer OSPF-Schnittstelle

1. Öffnen Sie die Seite **Schnittstellenparameter**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **OSPF-Schnittstellentabelle** anzuzeigen.
3. Wählen Sie eine OSPF-Schnittstelle
4. Klicken Sie das Kontrollkästchen **Remove** (Entfernen) an.

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

Die OSPF-Schnittstelle wird entfernt.

Definieren von OSPF-Schnittstellen mithilfe von CLI-Befehlen

Die folgende Tabelle beinhaltet CLI-Befehle zum Definieren von OSPF-Schnittstellen.

Table 8-11. CLI-Befehle für die OSPF-Schnittstelle

CLI-Befehl	Beschreibung
`ospf`	Erstellt einen OSPF-Routing-Vorgang auf einer Schnittstelle.
`ospf area area-id`	Definiert eine Schnittstellen-Area-ID.
`ospf enable`	Aktiviert OSPF auf einer Schnittstelle.
`ospf priority number-value`	Stellt die Routerpriorität ein, die verwendet wird, um den für das Netzwerk vorgesehenen Router zu wählen.
`ospf hello-interval seconds`	Legt das Zeitintervall zwischen den Hello-Paketen fest, die durch die Software auf einer Schnittstelle gesendet werden.
`ospf dead-interval seconds`	Stellt das Zeitintervall ein, in dem Hello-Pakete nicht gesendet werden dürfen, bis Nachbarn den Router als nicht verfügbar erklären.
`ospf retransmit-interval seconds`	Legt das Zeitintervall zwischen der erneuten Übertragung von Link-Satus Advertisements (LSAs) für zur Schnittstelle gehörende Schnittstellenadjazenzen fest.
`ospf transmit-delay seconds`	Stellt die geschätzte Zeit ein, die benötigt wird, um ein Update-Paket des Link-Status auf einer Schnittstelle zu senden.
`ospf authentication {text text | md5 name-of-chain}`	Ermöglicht die Authentifizierung von OSPF-Paketen und legt den Authentifizierungstypen fest.
`clear ip ospf process [interface]`	Löscht die Umverteilung auf OSPF-Routing-Basis.
`show ip ospf interface [interface]`	Zeigt OSPF-bezogene Schnittstelleninformationen an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface ip 1.100.100.100

Console (config-ip)# ospf

Console (config-ip)# ospf area 192.168.2.1

Console (config-ip)# ospf enable

Console (config-ip)# ospf priority 100
```

```
Console (config-ip)# ospf hello-interval 100

Console (config-ip)# ospf dead-interval 100

Console (config-ip)# ospf retransmit-interval 60

Console (config-if)# ospf retransmit-delay 60

Console (config-ip)# ospf authentication text abab

Console (config-ip)# ospf authentication md5 mychain

Console (config-ip)# exit

Console (config)# exit

Console# clear ip ospf process 192.168.3.1

Console# exit

Console# show ip ospf interface 192.168.1.1

IP interface 192.168.1.1/16 is up, OSPF is enabled

Area 0.0.0.0, Router ID 192.77.99.1, Network Type BROADCAST, Cost: 10

Interface has simple password authentication

Transmit Delay is 1 sec, State OTHER, Priority 1

Designated Router id 192.168.1.11, Interface address 192.168.1.11

Backup Designated router id 192.168.1.28, Interface addr 192.168.1.28

Timer intervals configured, Hello 10, Dead 60, Retransmit 5

Neighbor Count is 8, Adjacent neighbor count is 2

Adjacent with neighbor 192.168.1.28 (Backup Designated Router)
```

Anzeigen der Link-Status-Tabelle

Die Seite **OSPF Link State Table** (OSPF-Link-Status-Tabelle) beinhaltet Informationen über Link Status Advertisements für Areas, mit denen das Gerät verbunden ist. Klicken Sie in der Strukturansicht auf **Router→ OSPF→ Link State Table**.

Abbildung 8-16. OSPF-Link-Status-Tabelle

Area ID Die Area-ID.

Link Type Gibt den Link-Typ der Area an.

Link ID Bestandteil der in der Meldung beschriebenen Routing-Domäne. Dies ist entweder eine Router-ID oder eine IP-Adresse.

Router ID Der ursprüngliche Router im autonomen System.

Sequence Number (Folgennummer) Die Folgenummer des Links. Die Sequenznummer erkennt sowohl alte als auch duplizierte Link Status Advertisements. Je höher die Sequenznummer ist, desto aktueller ist die Bekanntgabe.

Age (Alter) Gibt das Alter der Link-Status-Meldungen in Sekunden an.

Checksum (Prüfsumme) Prüfsumme des vollständigen Inhalts der Meldung, mit Ausnahme des Werts für das **Alter**.

Anzeigen der OSPF-Link-Status-Tabelle mithilfe von CLI-Befehlen

Die folgende Tabelle beinhaltet die CLI-Befehle zum Anzeigen der OSPF-Link-Status-Tabelle.

Tabelle 8-12. CLI-Befehle für den OSPF-Link-Status

CLI-Befehl	Beschreibung
`show ip OSPF [area-id] database`	Zeigt OSPF-Datenbank-bezogene Informationslisten für einen bestimmten Router an.

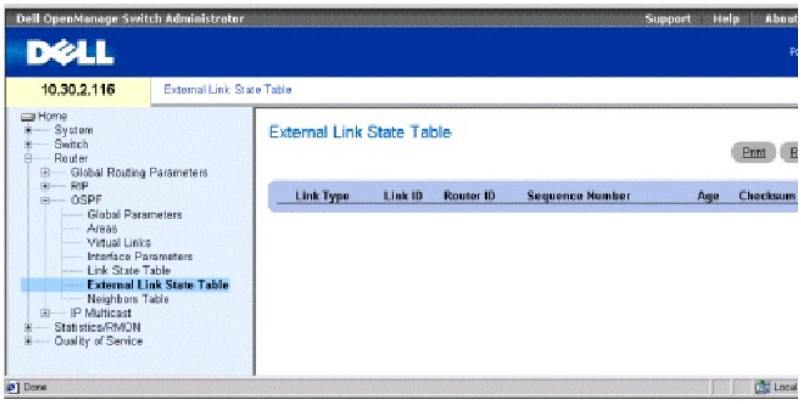
Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console> show ip ospf database

OSPF Router with ID 200.1.1.11

Router Link States(Area 0)

Link ID ADV Router Age Seq# Checksum Link count

200.1.1.8 200.1.1.8 1381 0x8000010D 0xEF60 2

200.1.1.11 200.1.1.11 1460 0x800002FE 0xEB3D 4

200.1.1.12 200.1.1.12 2027 0x80000090 0x875D 3

200.1.1.27 200.1.1.27 1323 0x800001D6 0x12CC 3



Net Link States(Area 0)

Link ID ADV Router Age Seq# Checksum

140.1.1.27 200.1.1.27 1323 0x8000005B 0xA8EE

141.1.1.11 200.1.1.11 1461 0x8000005B 0x7AC
```

Anzeigen der externen Link-Status-Tabelle

Die externe Link-Status-Tabelle beinhaltet Informationen über externe Link Status Advertisements. Die Informationen externer Link-Status-Tabellen werden von Quellen außerhalb der OSPF-Routen gelernt. Um die Seite „Externe Link-Status-Tabelle" anzuzeigen, klicken Sie in der Strukturansicht auf **Router→ OSPF→ External Link State Table**.

Abbildung 8-17. Externe Link-Status-Tabelle



Link Type Typ des externen Links. Jedes Link Status Advertisement hat ein bestimmtes Format. Dieses Feld ist immer der externe Link.

Link ID Bestandteil der in der Meldung beschriebenen Routing-Domäne. Dies ist entweder eine Router-ID oder eine IP-Adresse.

Router ID Der ursprüngliche Router im autonomen System.

Sequence Number (Folgenummer) Die Folgenummer des externen Links. Die Sequenznummer erkennt sowohl alte als auch duplizierte Link Status Advertisements. Je höher die Sequenznummer ist, desto aktueller ist die Bekanntgabe.

Age (Alter) Gibt das Alter der externen Link-Status-Meldung in Sekunden an.

Checksum (Prüfsumme) Prüfsumme des vollständigen Inhalts der Meldung, mit Ausnahme des Werts für das **Alter**.

Anzeigen der externen OSPF-Routentabelle mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Anzeigen der externen OSPF-Routentabelle.

Tabelle 8-13. CLI-Befehle für die externe Route-Tabelle

CLI-Befehl	Beschreibung
`show ip OSPF [area-id] database [external] [link-state-id]`	OSPF-Datenbank-bezogene Listen für einen bestimmten Router.

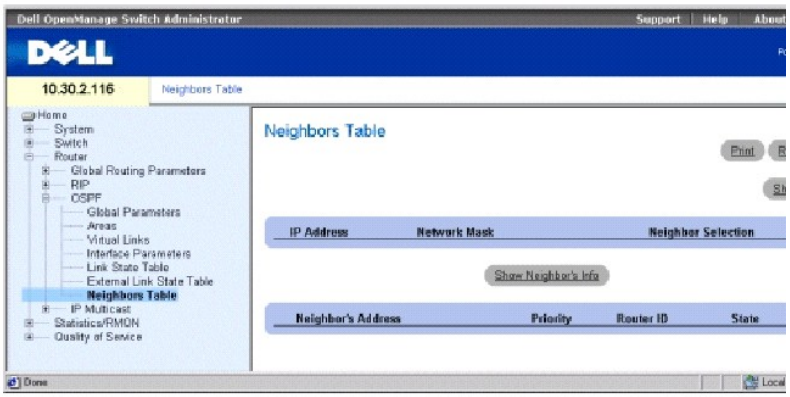
Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console> show ip ospf database
```

Anzeigen der OSPF-Nachbarntabelle

Die OSPF-Nachbarntabelle beschreibt alle Nachbarn am Ort des betreffenden Routers. Um die Seite **Nachbarntabelle** zu öffnen, klicken Sie in der Strukturansicht auf **Router→ OSPF→ Neighbors Table**.

Abbildung 8-18. Nachbarntabelle



IP Address IP-Adresse, die dieser Nachbar in seiner Quell-IP-Adresse verwendet.

Network Mask (Netzwerkmaske) Die Netzwerkmaske der benachbarten Schnittstelle.

Neighbor Selection (Nachbarnauswahl) Legt die anzuzeigenden Nachbarninformationen des Geräts fest.

Neighbor's Address Die IP-Adresse des Nachbarn.

Priority (Priorität) Die Priorität des Nachbarn.

Router ID Die Router-ID des Nachbarn.

State Der aktuelle Status des Nachbarn.

Anzeigen der Nachbarnliste

1. Öffnen Sie die Seite **OSPF Neighbors Table** (OSPF-Nachbarntabelle).
2. In der Spalte **Neighbor Selection** (Nachbarauswahl), klicken Sie auf die Taste Options" des Nachbarn, dessen Informationen Sie ansehen möchten.
3. Klicken Sie auf **Show Neighbor's Info** (Nachbarninformationen anzeigen).

Die Nachbarninformationen werden unten auf der Seite angezeigt.

Anzeigen der Tabelle Alle Nachbarn"

1. Öffnen Sie die Seite **Neighbors Table** (Nachbarntabelle).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Tabelle **All Neighbors** (Alle Nachbarn) anzuzeigen.

Anzeigen der OSPF-Nachbarninformationen mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Anzeigen der Tabelle „OSPF-Nachbarninformationen".

Tabelle 8-14. CLI-Befehle für OSPF-Nachbarn

CLI-Befehl	Beschreibung
`show ip ospf neighbor [interface]`	Zeigt OSPF-Nachbarninformationen schnittstellenbezogen an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console> show ip ospf neighbor

ID            Pri  State         Address       IP interface

------------  ---  ------------  ------------  ------------

192.168.1.11  1    FULL          /DR           192.168.1.11 192.168.1.1

192.168.1.12  2    FULL          /DROTHER      192.168.1.12 192.168.1.1

192.168.2.11  1    FULL          /DR           192.16 8.2.11 192.168.2.1

192.168.2.12  2    FULL          /DROTHER      192.168.2.12 192.168.2.1

Console> show ip ospf neighbor 192.168.1.1

Neighbor 192.168.1.11, Address 192.168.1.11

In the area 0.0.0.0

Neighbor priority is 1, State is FULL

Options 2

Neighbor 192.168.1.12, Address 192.168.1.12

In the area 0.0.0.0

Neighbor priority is 2, State is FULL

Options 2
```

Konfigurieren von IP-Multicast-Routing

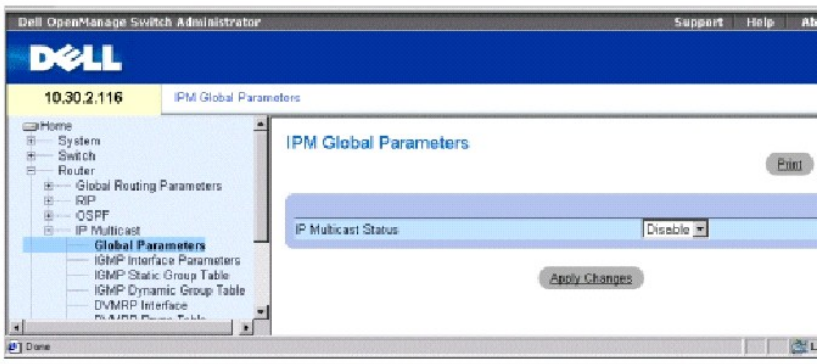
Multicast-Routing maximiert Netzwerkressourcen. Ein Host sendet im IP-Netzwerk Daten zu einer Hostgruppe (statt nur zu einem einzigen Host) und verwendet dabei die IP-Multicast-Gruppenadresse. IP Multicast-Routing ist im PowerConnect 6024/6024F implementiert und verwendet die folgenden Protokolle:

- **Internet Group Member Protocol** (IGMP) Bietet eine Methode an um herauszufinden, welche Clients am Empfang spezifischer Übertragungen interessiert sind.
- **Distance Vector Multicast Routing Protocol** (DVMRP) Ermöglicht es Routern, eine Übertragungsstruktur zu erzeugen und Pakete über den Routing-Übertragungsstruktur zu kopieren.

Definieren von globalen IPM-Parametern

IP Multicast-Routing wird über die Seite **IPM Global Parameters** (Globale IPM-Parameter) aktiviert. Um die Seite **Globale IPM-Parameter** anzuzeigen, klicken Sie in der Strukturansicht auf **Router→ IP Multicast→ Global Parameters**.

Abbildung 8-19. Globale IPM-Parameter



IP Multicast Status Aktiviert oder deaktiviert IPM-Routing auf dem Gerät.

Aktivieren von IPM-Routing auf dem Gerät

1. Öffnen Sie die Seite **IPM Global Parameters** (Globale IPM-Parameter).
2. Wählen Sie **Enable** (Aktivieren) im Feld **IPM Multicast Status**.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

IP Multicast-Routing ist auf dem Gerät aktiviert.

Aktivieren von Multicast-Routing mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Aktivieren von Multicast-Routing.

Tabelle 8-15. CLI-Befehle für Multicast-Routing

CLI-Befehl	Beschreibung
	Aktiviert IP Multicast-Routing.

ip multicast- routing	

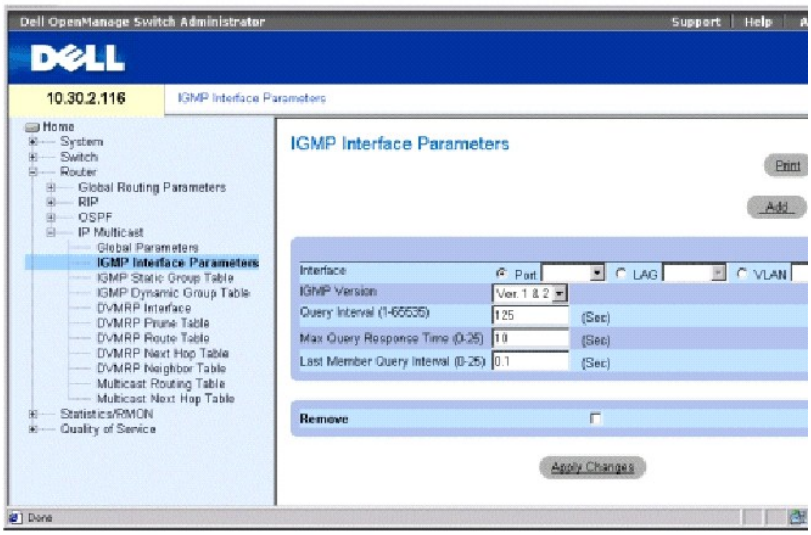
Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# ip multicast-routing
```

Definieren von IGMP-Schnittstellenparametern

Das Internet Group Membership Protocol (IGMP) baut Host-Mitgliedschaften innerhalb einer Multicast-Gruppe auf. Über IGMP teilen Hosts Routern mit, dass sie die an bestimmte Mulicast-Gruppen adressierte Multicast-Pakete empfangen können. Um die Seite **IGMP-Schnittstellenparameter** zu öffnen, klicken Sie in der Strukturansicht auf **Router→ IP Multicast→ IGMP Interface Parameters**.

Abbildung 8-20. IGMP-Schnittstellenparameter



Interface (Schnittstelle) Enthält eine Liste von IP-Adressen der Schnittstelle, für die IGMP aktiviert wurde.

IGMP Version Die aktuelle IGMP-Software-Version. Der Standard ist Version **1 & 2**.

Query Interval (1-65535) (Abfrageintervall) Zeitabstand (in Sekunden) für die Übertragung von Abfragemeldungen. Sie können die Anzahl der auf Teilnetzwerken gesendeten IGPM-Meldungen durch das Anpassen des Wertes Query Interval" einstellen. Je höher der Wert, desto seltener werden IGPM-Meldungen gesendet. Der Standardwert ist 125 Sekunden.

Max Query Response Time (0-25) (Maximale Antwortzeit) Maximale Antwortzeit, um IGMP-Abfragen bekanntzugeben. Die Antwortzeit regelt das Datenverkehrsaufkommen bezogen auf die Teilnetzwerke. Das Verändern der Antwortzeit beeinflusst den Stoßimpuls des Netzwerkdatenverkehrs. Je höher der Wert, desto größer ist die Zeitspanne zwischen den Host-Antworten. Der Standardwert lautet 10 Sekunden.

Last Member Query Interval (0-25) (Abfrageintervall des letzten Mitglieds) Ändert die sogenannte Leave Latency des Netzwerks. Ein geminderter Wert reduziert die Zeit, die notwendig ist, um den Verlust des letzten Gruppenmitglieds zu erkennen. Der Standardwert ist 0.1.

Remove (Entfernen) Wenn diese Funktion ausgewählt ist, wird die IGMP-Schnittstelle entfernt.

Hinzufügen einer IGPM-Schnittstelle

1. Öffnen Sie die Seite **IGPM Interface Parameters** (IGPM-Schnittstellenparameter).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add an IGPM Interface** (IGPM-Schnittstelle hinzufügen) anzuzeigen.
3. Wählen Sie aus dem Drop-Down-Menü **New Interface** (Neue Schnittstelle) eine Schnittstelle aus.
4. Geben Sie die Informationen in die Felder auf der Seite ein.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die neue IGPM-Schnittstelle wird dem Gerät hinzugefügt.

Ändern einer IGPM-Schnittstelle

1. Öffnen Sie die Seite **IGPM Interface Parameters** (IGPM-Schnittstellenparameter).
2. Wählen Sie die Schnittstelle, die Sie ändern möchten.
3. Ändern Sie die gewünschten Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die IGPM-Parameter werden geändert und auf dem Gerät gespeichert.

Entfernen einer IGPM-Schnittstelle

1. Öffnen Sie die Seite **IGPM Interface Parameters** (IGPM-Schnittstellenparameter).
2. Klicken Sie auf **Show All** (Alle anzeigen) um die Seite **IGPM Interface Table** (IGPM-Schnittstellentabelle) anzuzeigen.
3. Wählen Sie eine IGPM-Schnittstelle und aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die IGPM-Schnittstelle wird entfernt.

Konfigurieren von IGPM-Schnittstellenparametern mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Konfigurieren der IGPM-Schnittstellenparameter.

Tabelle 8-16. CLI-Befehle für IGMP-Schnittstellenparameter

CLI-Befehl	Beschreibung
`ip igmp`	Erzeugt IGPM auf einer Schnittstelle.
`ip igmp query-interval` *`seconds`*	Konfiguriert die Frequenz, in der die Software IGMP Host-Abfragen sendet.
`ip igmp query-max-response-time` *`seconds`* [*`tenths-of-seconds`*]	Konfiguriert die maximale in IGMP-Abfragen bekanntgegebene Antwortzeit.
`ip igmp last-member-query-interval` *`seconds`* [*`tenths-of-seconds`*]	Konfiguriert die Frequenz, in der der Router gruppenbezogene IGMP-Host-Abfragen sendet.
`show ip igmp interface [ethernet interface-number |` *`vlan vlan-id | port-channel number]`*	Zeigt IGMP-bezogene Informationen über eine Schnittstelle an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

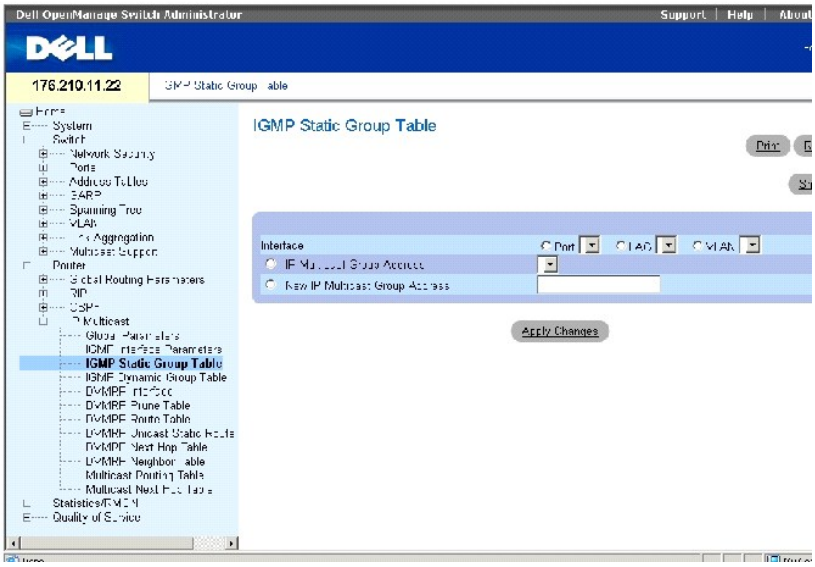
```
Console (config)# interface ethernet g1

Console (config-if)# ip igmp

Console (config-if)# ip igmp query-interval 60

Console (config-if)# ip igmp query-max-response-time 20

Console (config-if)# ip igmp last-member-query-interval 200

Console (config-if)# exit

Console (config)# exit

Console# disable

Console> show ip igmp interface

Interface  Version Query  Last     Max     Querier Interval     Member     response     router

           [sec]          [mSec]   [Sec]

---------  -------        -------  ------  --------             ---

eth g1     2              60       1000    10                   198.92.37.33

eth g2     60             1000     10                           198.92.36.131
```

Definieren von statischen IGMP-Schnittstellengruppen

Die **IGMP Static Group Table** (Statische IGMP-Gruppentabelle) ermöglicht die Definition statischer IGMP-Gruppen auf bestimmten Schnittstellen.

Um die Seite **Statische IGMP-Gruppentabelle zu öffnen**, klicken Sie in der Strukturansicht auf **Router→ IP Multicast→ IGMP Static Group Table**.

Abbildung 8-21. Statische IGMP-Gruppentabelle



Interface (Schnittstelle) Legt den Port, VLAN, oder LAG fest, dem die spezifische Multicast-Gruppe zugewiesen ist.

IP Multicast Group Address Die IP-Adresse der Multicast-Gruppe, die einer Schnittstelle zugewiesen ist.

New IP Multicast Group Address (Neue IP-Adresse der Multicast-Gruppe) Die neue IP-Adresse der Multicast-Gruppe, die einer Schnittstelle zugewiesen ist.

Zuweisen einer Schnittstelle zu einer Multicast-Gruppe

1. Öffnen Sie die **statische Gruppentabelle**.
2. Wählen Sie eine Schnittstelle im Feld **Interface**.
3. Wählen Sie eine IP-Adresse im Feld **Multicast Group Address** (Multicast-Gruppenadresse), oder definieren Sie eine neue Multicast-Gruppenadresse im Feld **New Multicast Group Address** (Neue Multicast-Gruppenadresse).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Anzeigen der Tabelle Statische Schnittstellengruppierung"

1. Öffnen Sie die **statische IGMP-Gruppentabelle**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **Static Interface Grouping Table** (Statische Schnittstellengruppierungstabelle) anzuzeigen.

Die Seite beinhaltet die folgenden Felder:

- **Interface** (Schnittstelle) Die IP-Adresse der Multicast-Gruppe, deren Mitglied der Port ist.
- **IP Multicast Group** (IP-Multicast-Gruppe) Die IP-Multicast-Gruppe, der diese Schnittstelle angehört.
- **Group Up Time** (Gruppe seit) Gibt die Zeittakte an, die seit Erzeugung des Eintrags vergangen sind. Das Format ist Stunde/Minute/Sekunde.
- **Last Reporter** (Letzter Reporter) Das letzte Mitglied, dass sich der IP-Multicast-Gruppe angeschlossen hat. Wenn sich der IP Multicast-Gruppe keine Mitglieder angeschlossen haben, ist der Wert 0.0.0.0.
- **Remove** (Entfernen) Wenn diese Funktion ausgewählt ist, wird eine IGMP-Schnittstelle entfernt.

Konfigurieren der statischen Schnittstellengruppierung mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet CLI-Befehle für die statische Schnittstellengruppierung.

Tabelle 8-17. CLI-Befehle für statische Schnittstellengruppierung

CLI-Befehl	Beschreibung
`ip igmp static-group group-address`	Konfiguriert den Router als statisch verbundenes Mitglied der festgelegten Gruppe auf der Schnittstelle.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface ethernet g5
```

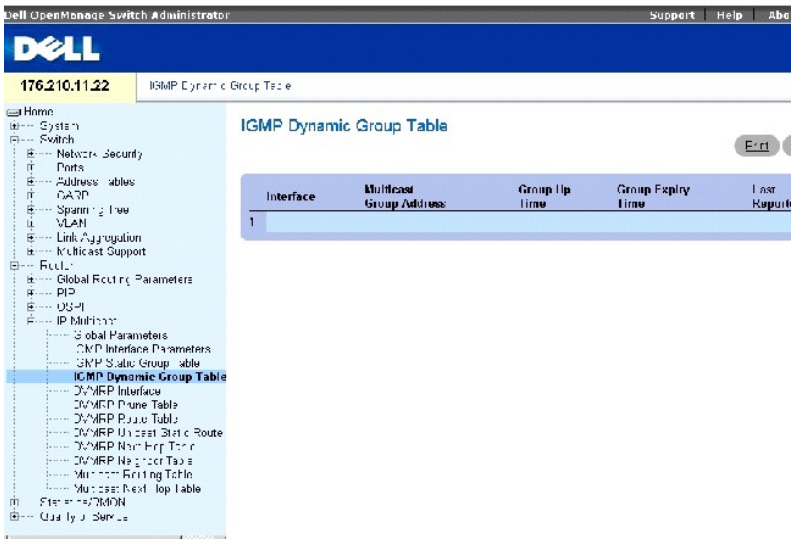
```
Console (config-if)# ip igmp static-group 192.168.4.1
```

Anzeigen der dynamischen IGMP-Gruppentabelle

Die Tabelle **Dynamische IGMP-Gruppe** zeigt IGMP-Informationen über jede IP-Multicast-Gruppe an, deren Mitglieder dynamisch einer Schnittstelle auf einem physikalischen Port zugewiesen wurden.

Um die Tabelle **Dynamische IGMP-Gruppe** zu öffnen, klicken Sie in der Strukturansicht auf **Router→ IP Multicast→ IGMP Dynamic Group Table**.

Abbildung 8-22. Dynamische IGMP-Gruppe



Interface (Schnittstelle) Legt eine zur IP-Multicast-Gruppe gehörenden Schnittstelle fest.

Multicast Group Address Die IGMP-Multicast-IP-Adresse.

Group Up Time (Gruppe seit) Gibt die Zeittakte an, die seit Erzeugung des Eintrags vergangen sind. Das Format ist Stunde/Minute/Sekunde.

Group Expiry Time (Gruppe bis) Zeit bis zum Ablauf des dynamischen Eintrags. Das Format ist Stunde/Minute/Sekunde.

Last Reporter (Letzter Reporter) Letztes Mitglied, das sich der IP Multicast-Gruppe angeschlossen hat. Wenn sich der IP Multicast-Gruppe keine Mitglieder angeschlossen haben, ist der Wert 0.0.0.0.

Anzeigen von IGMP-Gruppen mithilfe von CLI-Befehlen

Die folgende Tabelle beinhaltet die CLI-Befehle zum Anzeigen der IGPM-Gruppen.

Tabelle 8-18. CLI-Befehle der IGMP-Gruppe

CLI-Befehl	Beschreibung
`show ip igmp groups [group ip-address] [ethernet interface-number | vlan vlan-id | port-channel number]`	Zeigt die Multicast-Gruppen mit Empfängern an, die direkt an den Router angeschlossen sind und die durch das Internet Group Membership Protocol (IGMP) gelernt wurden.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console> show ip igmp groups

Group Address   Interface  Uptime    Expires    Last Reporter

---------------------------------------------------

239.255.255.254  eth g1     1w0d     00:02:19   172.21.200.159

224.0.1.40       eth g3     1w0d     00:02:15   172.21.200.1

224.0.1.40       eth g3     1w0d     00:02:1    static

224.0.1.1        eth g1     1w0d     00:02:11   172.21.200.11

224.9.9.2        eth g1     1w0d     00:02:17   172.21.200.155

232.1.1.1        eth g1     5d21h    00:02:11   172.21.200.206
```

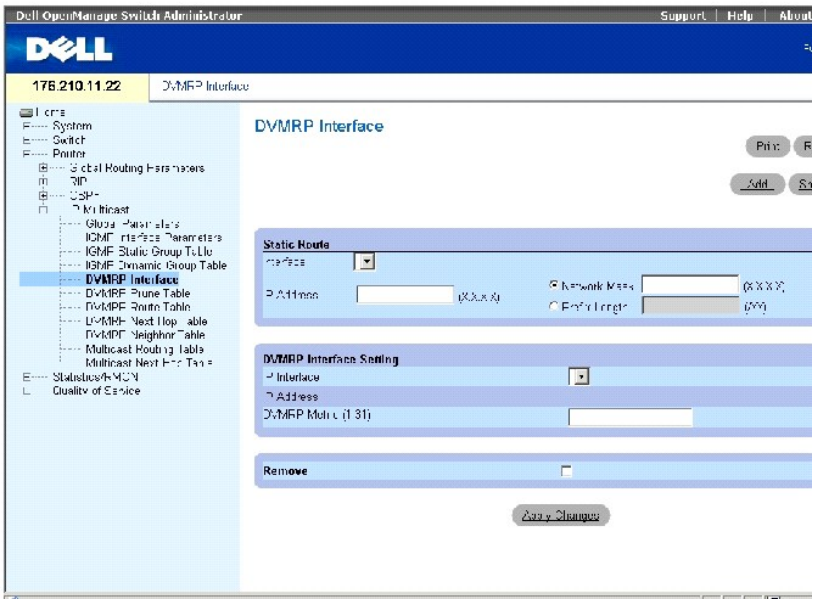
Konfigurieren von DVMRP-Schnittstellen

Das Distance Vector Multicast Routing Protocol (DVMRP) verwendet den Reverse Path Forwarding (RPF) Multicast-Algorithmus, um quellenbezogene Multicast-Lieferstrukturen zu bilden. DVMRP ist ein RPF-prüfendes Protokoll, das auf DVMRP Routing-Informationen basiert. Die Routing-Informationen werden während des Informationsaustausches zwischen den Routern gesammelt.

Die Seite **DVMRP Interface** (DVMRP-Schnittstelle) beinhaltet Informationen über DVMRP-Schnittstellenkonfigurationen.

Um die Seite **DVMRP-Schnittstelle** zu öffnen, klicken Sie in der Strukturansicht auf **Router→ IP Multicast→ DVMRP Interface**.

Abbildung 8-23. DVMRP-Schnittstelle



Die Seite **DVMRP-Schnittstelle** enthält die folgenden Felder, die in zwei Bereiche eingeteilt ist:

STATISCHE ROUTE

Interface (Schnittstelle) Legt die Anzahl der Schnittstellen fest, auf der DVMRP aktiviert ist.

IP Address (X.X.X.X) (IP-Adresse) Legt die Quell-IP-Adresse auf dem Port fest, auf dem DVMRP aktiviert ist.

Network Mask (X.X.X.X) (Netzwerkmaske) Legt die Teilnetzwerkmaske der Quell-IP-Adresse fest.

Prefix Length /XX (Präfixlänge) Gibt die Anzahl der Bits an, die das Präfix der Quell-IP-Adresse enthält, oder die Netzwerkmaske der Quell-IP-Adresse.

DVMRP INTERFACE SETTING (Einstellungen DVMRP-Schnittstelle)

IP Interface (IP-Schnittstelle) Legt die Anzahl der Schnittstellen fest, auf der DVMRP aktiviert ist.

IP Address (IP-Adresse) Legt die Quell-IP-Adresse auf dem Port fest, auf der DVMRP aktiviert ist.

DVMRP Metric (1-31) (DVMRP-Metrik) Gibt die Entfernung an, die zur Berechnung des Distanzvektors zugrunde gelegt wird. Die DVMRP-Metrik ist die Schnittstellenentfernung zwischen dem Router, der den Report erstellt und dem Quell-Netzwerk. Der Standardwert ist 1.

Remove (Entfernen) Wenn diese Option markiert ist, wird eine DVMRP-Schnittstelle entfernt.

Hinzufügen einer neuen DVMRP-Schnittstelle

1. Öffnen Sie die Seite **DVMRP-Schnittstelle**.
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add a DVMRP Interface** (DVMRP-Schnittstelle hinzufügen) anzuzeigen.
3. Definieren Sie die Schnittstellennummer und DVMRP-Metrik.

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

Die DVMRP-Schnittstelle wird der **IP Interfacelist** (IP-Schnittstellenliste) hinzugefügt, und das Gerät wird aktualisiert.

Ändern einer DVMRP-Schnittstelle

1. Öffnen Sie die Seite **DVMRP-Schnittstelle**.
2. Wählen Sie in der Liste **IP Interface** (IP-Schnittstelle) eine Schnittstelle aus.
3. Ändern Sie die gewünschten Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die ausgewählte DVMRP-Schnittstelle wird zur **DVMRP Interface list** (DVMRP-Schnittstellenliste) hinzugefügt, und das Geräte wird aktualisiert.

Entfernen einer DVMRP-Schnittstelle

1. Öffnen Sie die Seite **DVMRP-Schnittstelle**.
2. Wählen Sie in der Liste **IP Interface** (IP-Schnittstelle) eine Schnittstelle aus.
3. Klicken Sie das Kontrollkästchen **Remove** (Entfernen) an.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die geänderte DVMRP-Schnittstelle wird aus der **IP Interface list** (DVMRP-Schnittstellenliste) entfernt, und das Geräte wird aktualisiert.

Konfigurieren von DVMRP-Schnittstellen mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Konfigurieren und Anzeigen der DVMRP-Schnittstellen.

Tabelle 8-19. CLI-Befehle für DVMRP

CLI-Befehl	Beschreibung
`ip dvmrp`	Aktiviert DVMRP auf einer Schnittstelle.
`no ip dvmrp`	Deaktiviert DVMRP auf einer Schnittstelle.
`ip dvmrp metric` *`metric`*	Konfiguriert die Schnittstellenmetrik für DVMRP. Die Metrik kann sich im Bereich 1-31 bewegen.
`no ip dvmrp metric`	Deaktiviert die Schnittstellenmetrik für DVMRP.
`show ip dvmrp interface [ethernet` *`interface-number`* `| vlan` *`vlan-id`* `| port-channel` *`number`*`]`	Zeigt die Schnittstellentabelle.

Im Folgenden werden CLI-Befehle anhand eines Beispiels dargestellt:

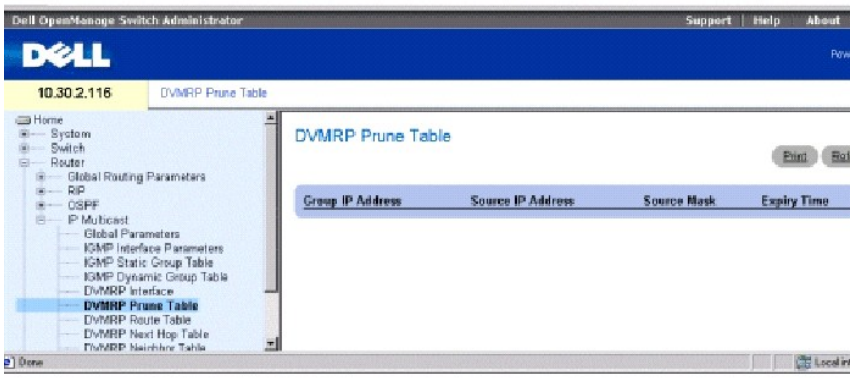
```
Console (config-if)# interface ethernet g5

Console (config-if)# ip dvmrp

Console (config-if)# ip dvmrp metric 15
```

```
Console (config-if)# exit

Console (config)# exit

Console> show ip dvmrp interface

Multicast routing enabled.

Multicast routing protocol is DVMRP.

Interface  IP address    Metric   RCV Bad  RCV Bad  Sent  Packets  Routes  Routes

---------  -----------   -------  -------  ------  ------

eth g1     172.16.1.1    10       0        12
```

DVMRP-Prune-Tabelle

Die Seite **DVMRP Prune Table** (DVMRP-Prune-Tabelle) listet den Upstream-Prune-Status des Routers auf. Um die Seite **DVMRP-Prune-Tabelle** zu öffnen, klicken Sie in der Strukturansicht auf **Router**→ **IP Multicast**→ **DVMRP Prune Table**.

Abbildung 8-24. DVMRP-Prune-Tabelle



Group IP Address IP-Adresse der Prune-Gruppe.

Source IP Address Zu kürzende Quell-IP-Adresse.

Source Mask (Quellmaske) Gekürzte Quell-IP-Maske.

Expiry Time (Ablaufzeit) Die verbleibende Zeit, bis der Upstream-Fluss gekürzt wird.

Anzeigen der DVMRP-Prune-Tabelle mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Anzeigen der Prune-Tabelle.

Tabelle 8-20. CLI-Befehle für die DVRMP-Tabelle

CLI-Befehl	Beschreibung
`show ip dvmrp prune [group group-address] [source-address]`	Zeigt die Tabelle.

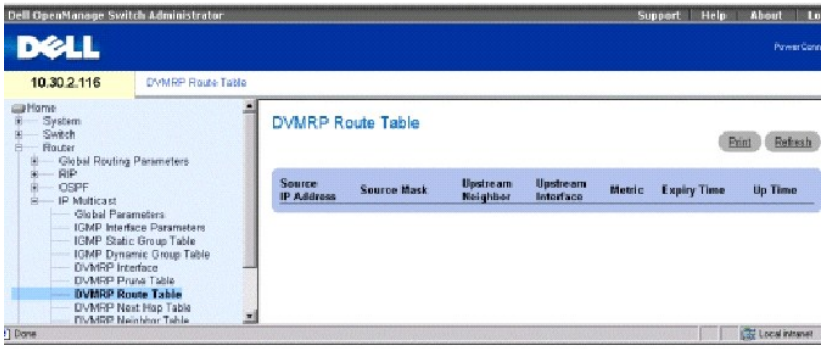
Im Folgenden werden CLI-Befehle anhand eines Beispiels dargestellt:

```
Console> show ip dvmrp prune

Group          Source         Expiry Time

-------------  ------------   --------

224.192.78.88  171.68.0.0/16  00:02:52

224.192.78.89  171.68.0.0/16  00:08:52
```

DVMRP-Routentabelle

Die Seite **DVMRP Route Table** (DVMRP-Routentabelle) beinhaltet Informationen über Routen, die über den DVMRP-Router-Datenaustausch gelernt wurden. Um die Seite **DVMRP-Routentabelle** zu öffnen, klicken Sie in der Strukturansicht auf **Router→ IP Multicast→ DVMRP Route Table**.

Abbildung 8-25. DVMRP-Routentabelle



Source IP Address (Quell-IP-Adresse) Quell-IP-Adresse der Multicast-Routing-Information.

Source Mask (Quellmaske) Quell-IP-Adresse der Netzwerkmaske.

Upstream Neighbor (Upstream-Nachbar) IP-Adresse des RPF-Upstream-Nachbarn, von dem Quell-IP-Datagramme empfangen werden.

Upstream Interface IP-Adresse der Upstream-Schnittstelle.

Metric (Metrik) Entfernung in Hops bis zum Quellteilnetz.

Expiry Time (Ablaufzeit) Zeitspanne bis zum Ablauf des Eintrags.

Up Time (Betriebszeit) Zeit, die vergangen ist, seit der Router den Router gelehrt hat.

Anzeigen der DVMRP-Routentabelle mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Anzeigen der DVMRP-Routentabelle.

Tabelle 8-21. CLI-Befehle für die DVRMP-Routentabelle

CLI-Befehl	Beschreibung
`show ip dvmrp route [ip-address] [ip-address]`	Zeigt die DVMRP-Routentabelle.

Im Folgenden werden CLI-Befehle anhand eines Beispiels dargestellt:

```
Console> show ip dvmrp route

Source          Neighbor        Interface       Metric       Expiry       Up Time       Time

------          --------        ---------       ------       ------       -------       ------------

171.68.0.0/16   192.168.1.2816  eth             g116         11016        100:02:5216   107:55:50
```

DVMRP-Next-Hop-Tabelle

Die Seite **DVMRP-Next-Hop-Tabelle** beinhaltet Informationen über den nächsten Hop der Datenausgangsschnittstelle für IP-Multicast-Pakete. Um die Seite **DVMRP-Next-Hop-Tabelle** zu öffnen, klicken Sie in der Strukturansicht auf **Router→ IP Multicast→ DVMRP Next Hop Table**.

Abbildung 8-26. DVMRP-Next-Hop-Tabelle

Source IP Address (Quell-IP-Adresse) Quell-IP-Adresse für den nächsten Hop einer Datenausgangsschnittstelle.

Source Mask (Quellmaske) Quellmaske für den nächsten Hop einer Datenausgangsschnittstelle.

Downstream Interface (Downstream-Schnittstelle) Die Datenausgangsschnittstelle des nächsten Hops.

Type Legt den nächsten Hop-Typ fest. Die möglichen Werte sind:

Branch (Zweig) Gibt an, dass nach diesem Hop ein weiterer folgt.

Leaf (Blatt) Gibt an, dass dies der letzte Hop auf der Route ist.

Anzeigen der DVMRP-Next-Hop-Tabelle mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Anzeigen der DVMRP-Next-Hop-Tabelle.

Tabelle 8-22. CLI-Befehle für die DVMRP-Next-Hop-Tabelle

CLI-Befehl	Beschreibung
show ip dvmrp next-hop [ethernet *interface-number* | vlan *vlan-id* | port-channel *number*]	Zeigt die DVMRP-Next-Hop-Tabelle.

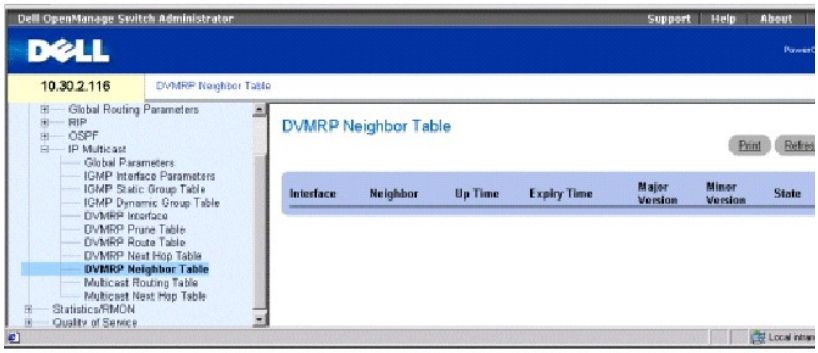
Im Folgenden werden CLI-Befehle anhand eines Beispiels dargestellt:

```
Console> show ip dvmrp next-hop

Source           Interface    Hop Type

---------------  -----------  ----------

198.92.37.100/32  eth g2       Leaf
```

DVMRP-Nachbarntabelle

Die Seite **DVMRP Neighbor Table** (DVMRP-Nachbarntabelle) beinhaltet Informationen über benachbarte Port-Schnittstellen. DVMRP-Nachbarn werden anhand von DVMRP-Meldungen erkannt. Um die Seite **DVMRP-Nachbarntabelle** zu öffnen, klicken Sie in der Strukturansicht auf **Router→ IP Multicast→ DVMRP Neighbor Table**.

Abbildung 8-27. DVMRP-Nachbarntabelle



Interface (Schnittstelle) Schnittstellennummer, auf der DVMRP aktiviert ist.

Neighbor (Nachbar) IP-Adresse der benachbarten Schnittstelle.

Up Time (Betriebszeit) Zeitspanne, seitdem die benachbarte Schnittstelle ein Nachbar ist.

Expiry Time (Ablaufzeit) Gibt die Mindestzeit an, die verbleibt, bis die Schnittstelle nicht mehr gültig ist.

Major Version (Hauptversion) Die Hauptversionsnummer des benachbarten Routers.

Minor Version (Nebenversion) Die Nebenversionsnummer des benachbarten Routers.

State (Status) Der Status des benachbarten Geräts.

Anzeigen der DVMRP-Nachbarntabelle mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Anzeigen der DVMRP-Nachbarntabelle.

Tabelle 8-23. CLI-Befehle für die DVMRP-Nachbarntabelle

CLI-Befehl	Beschreibung
`show ip dvmrp neighbor [ethernet` *`interface-number`* `| vlan` *`vlan-id`* `| port-channel` *`number`*`]`	Zeigt die DVMRP-Nachbarntabelle.

Im Folgenden werden CLI-Befehle anhand eines Beispiels dargestellt:

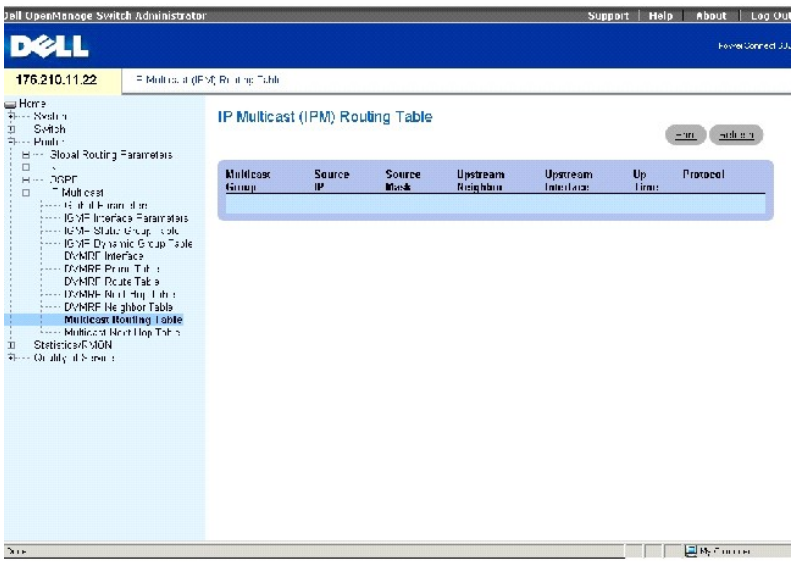
```
Console> show ip dvmrp neighbor ethernet g1

Interface  Neighbor      Up   Expiry            Version  Capabilities  RCV   Bad  State  Time  Time  Routes  Routes

---------  ------------  --   ---------------   -------  ------------  ---   ---  -----

eth g1     192.168.1.28  2    0:20:00 0:02:55   3.255    L,P,G,M       11    0    Active

eth g1     192.168.1.10  2    0:20:00 0:02:55   3.255    L,P,G,M       18    0    Active

eth g2     192.168.1.28  2    0:20:00 0:02:55   3.255    L,P,G,M       11    0    Active

eth g2     192.168.1.89  2    0:20:00 0:02:55   3.255    L,P,G,M       18    0    Active
```

Anzeigen der IP-Multicast-Routing-Tabelle

Die **IP-Multitask-Routing (IPM)** enthält Multicast-Routing-Informationen über IP-Pakete, die von einer bestimmten Quelle zu IP-Multicast-Gruppen gesendet wurden, die dem IP-Multicast-Router bekannt sind.

Um die Tabelle **IP-Multitask-Routing (IPM)** zu öffnen, klicken Sie in der Strukturansicht auf **Router**→ **IP Multicast**→ **Multicast Routing Table**.

Abbildung 8-28. IP-Multicast-Routing-Tabelle



Die Tabelle **IP-Multicast-Routing-Tabelle** enthält die folgenden Felder:

Multicast Group (Multicast-Gruppe) Die IP-Adresse der Multicast-Gruppe.

Source IP (Quell-IP) Quell-IP-Adresse des Geräts, auf das sich die Multicast-Informationen beziehen.

Source Mask (Quellmaske) Maskiert alle oder Teile der Quell-IP-Adresse.

Upstream Neighbor (Benachbarter Upstream) IP-Adresse des nächsten Upstream-Geräts, von dem Pakete an die IP-Adresse empfangen werden.

Upstream Interface (Upstream-Schnittstelle) Portnummer, auf der versendete Multicast-Pakete empfangen werden.

Up Time (Betriebszeit) Gibt die Zeitspanne an, die vergangen ist, seitdem der Router die Multicast-Informationen erlernt hat.

Protocol Identifiziert den Protokolltyp, der verwendet wird, um die Multicast-Information zu erlernen. In diesem Fall ist die einzige Möglichkeit **DVMRP**, d.h. dass das Distance Vector Multicast Routing Protocol verwendet wurde, um die Multicast-Information zu lernen.

Anzeigen der IP-Multicast Routingtabelle mithilfe der CLI-Befehle

Die folgende Tabelle beinhaltet die CLI-Befehle zum Anzeigen der IP-Multicast-Routingtabelle.

Tabelle 8-24. CLI-Befehle für die IP-Multicast-Routing-Tabelle

CLI-Befehl	Beschreibung
show ip mroute [group *group-address*] [source *source-address*] [ethernet *interface-number* | *vlan vlan-id* | *port-channel number*]	Zeigt den Inhalt der IP-Multicast-Routingtabelle an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

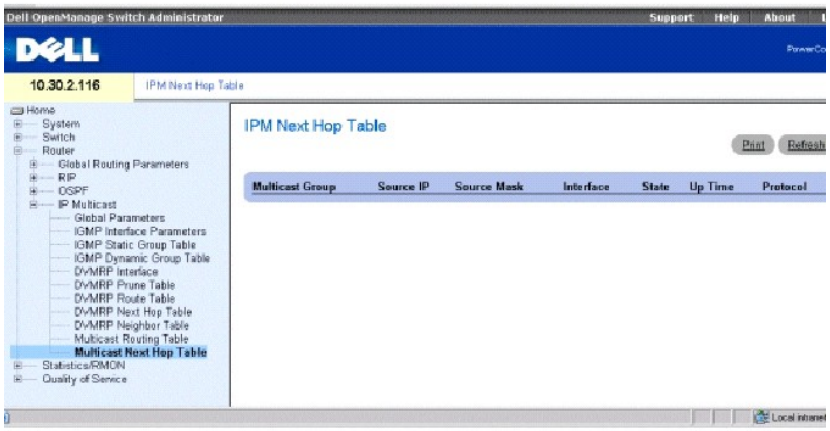
```
Console> show ip mroute

Group        Source           Upstream     Interface  Up Time    Expiry Time  Owner

-----        ------           --------     ---------  -------    -----------  --------

224.0.255.1  198.92.37.100/32  10.20.37.33  eth g1     20:20:00   0:02:55      dvmrp

224.0.255.1  199.92.37.100/32  10.20.37.33  eth g1     1d:4h:20m  0:02:55      dvmrp

224.1.255.1  198.92.37.100/32  10.20.37.33  eth g1     21:20:00   0:02:55      dvmrp

224.1.255.1  199.92.37.100/32  10.20.37.33  eth g1     1d:5h:20m  0:02:55      dvmrp

224.8.255.1  179.82.17.200/32  10.20.37.33  vlan 127   1w:1d:2h   0:02:55      dvmrp

224.8.255.1  179.82.17.200/32  10.20.37.33  vlan 128   3m:2w:2d   0:02:55      dvmrp
```

```
224.8.255.1   179.82.17.200/32  10.20.37.33  vlan 129   1y:2m:2w   0:02:55      dvmrp

224.9.255.1   179.82.17.200/32  10.20.37.33  p-c 7      1d:5h:20m 0:02:55      dvmrp
```

Anzeigen der IP-Multicast-Next-Hop-Tabelle

The Seite **IPM-Next-Hop-Tabelle** enthält Multicast-Informationen über den nächsten Hop. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Router→ IP Multicast→ Multicast Next Hop Table**.

Abbildung 8-29. IP-Multitask-Next-Hop-Tabelle



Multicast Group (Multicast-Gruppe) Die IP-Adresse der Multicast-Gruppe.

Source IP (Quell-IP) Quell-IP-Adresse des Geräts, auf das sich die Multicast-Informationen beziehen.

Source Mask (Quellmaske) Maskiert alle oder Teile der Quell-IP-Adresse.

Interface (Schnittstelle) Portnummer, auf der versendete Multicast-Pakete empfangen werden.

State (Status) Gibt an, ob der Port und der nächste Hop verwendet werden, um Multicast-Pakete zu befördern. Die möglichen Werte sind:

Pruned (Gekürzt) Der Port und der nächste Hop werden nicht verwendet, um Multicast-Pakete zu befördern.

Forwarding (Übermitteln) Der Port und der nächste Hop werden derzeit verwendet, um Multicast-Pakete zu übermitteln.

Up Time (Betriebszeit) Zeigt die Zeitspanne an die vergangen ist, seitdem der Router die Multicast-Informationen erlernt hat.

Protocol Protokolltyp, der verwendet wird, um die Multicast-Informationen zu erlernen. In diesem Fall ist die einzige Möglichkeit **DVMRP**, d. h. dass das Distance Vector Multicast Routing Protocol verwendet wurde, um die Multicast-Informationen zu lernen.

Anzeigen der IP-Multicast-Next-Hop-Tabelle mithilfe von CLI-Befehlen

Die folgende Tabelle beinhaltet die CLI-Befehle zum Anzeigen der IP-Multicast-Next-Hop-Tabelle.

Tabelle 8-25. CLI-Befehle für die IP-Multicast-Next-Hop-Tabelle

CLI-Befehl	Beschreibung
`show ip mroute-next-hop [group group-address] [source source-address]`	Zeigt den Inhalt der IP-Multicast Next-Hop Tabelle an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console> show ip mroute-next-hop


Group        Source            Interface   Up Time   Expiry Time  State    Owner

-----------  ----------------  -------     --------  -----------  -------  ----

224.0.255.1  198.92.37.100/32  eth g2 2     0:20:00  0:02:55      Forward  igmp

224.0.255.1  199.92.37.100/32  eth g2 1     :4d:20m  0:02:55      Forward  igmp

224.1.255.1  198.92.37.100/32  eth g2 2     1:20:00  0:02:55      Forward  dvmrp

224.1.255.1  199.92.37.100/32  eth g2 1     :4d:20m  0:02:55      Forward  dvmrp
```

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Konfigurieren von QoS (Diensteigenschaften)

Dell PowerConnect 6024/6024F Systeme

Die Seite **Quality of Service** (Servicequalität) enthält Verknüpfungen zu den wichtigsten QoS-Konfigurationsseiten. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service**.

Übersicht über Quality of Service (Diensteigenschaften)

Da der Datenverkehr im Netzwerk in der Regel unberechenbar ist, besteht die einzige Gewährleistung, die ein Netzwerkadministrator anbieten kann, darin, eine möglichst gute Übermittlung der Daten zu realisieren. Zur Überwindung dieses Problems wenden Netzwerkadministratoren das Konzept der Servicequalität (Quality of Service, QoS) innerhalb des gesamten Netzwerks an. Dadurch wird sichergestellt, dass der Netzwerk-Datenverkehr nach bestimmten Kriterien priorisiert wird, und dass bestimmter Datenverkehr bevorzugt behandelt wird. QoS im Netzwerk optimiert die Netzwerkleistung und enthält zwei grundlegende Funktionen:

- Klassifizieren des eingehenden Datenverkehrs in Behandlungsklassen auf der Basis eines Attributs, einschließlich:
  - Der Eintrittsschnittstelle
  - Paketinhalt
  - Einer Kombination aus diesen Attributen
- Bereitstellen verschiedener Mechanismen, mit denen die Zuordnung von Netzwerkressourcen zu verschiedenen Behandlungsklassen ermittelt wird, einschließlich:
  - Zuordnung des Netzwerk-Datenverkehrs zu einer bestimmten Hardware-Warteschlange
  - Zuordnung von internen Ressourcen
  - Datenverkehrsformung

In diesem Dokument werden die Begriffe Class of Service (CoS, Serviceklasse) and QoS (Diensteigenschaften) im folgenden Kontext verwendet:

- CoS bietet unterschiedliche Datenverkehrsservices der Schicht 2. CoS beschreibt die Klassifizierung von Datenverkehr in Datenverkehrsklassen, die als Gesamteinheit behandelt werden, ohne flussspezifische Einstellungen. CoS bezieht sich in der Regel auf den 802.1p-Dienst, der Flüsse entsprechend ihrer Schicht-2-Priorität klassifiziert, die im VLAN-Header festgelegt sind.
- QoS bezieht sich auf Datenverkehr der Schicht 2 und darüber. QoS verarbeitet flussspezifische Einstellungen, selbst innerhalb einer einzelnen Datenverkehrsklasse.

Die QoS-Funktion beinhaltet die folgenden Elemente:

- **Access Control Lists** (ACLs, Zugriffssteuerungsliste) Anhand von ACLs wird entschieden, welcher Datenverkehr in das System hineingelassen und welcher nicht zugelassen wird. Nur Datenverkehr, der diesen Kriterien entspricht, ist für CoS und QoS relevant. ACLs werden in QoS und der Netzwerksicherheit verwendet.
- **Traffic Classification** (Datenverkehrklassifizierung) Ordnet jedes eingehende Paket auf der Basis des Paketinhalts und/oder des Kontexts einer bestimmten Datenverkehrsklasse zu.
- **Assignment to Hardware Queues** (Zuordnung zu Hardware-Warteschlangen) Weist eingehende Pakete Weiterleitungswarteschlangen zu. Pakete werden an eine bestimmte Warteschlange zur Behandlung als Funktion der Datenverkehrsklasse gesendet, der sie angehören, entsprechend der Definition durch den Klassifizierungsmechanismus.
- **Traffic Class-Handling Attributes** (Attribute für die Behandlung der Datenverkehrsklasse) Wendet QoS/CoS-Mechanismen auf unterschiedliche Klassen an, darunter:
  - Bandbreitenmanagement
  - Formung
  - Überwachung

Zugriffssteuerungslisten

ACLs untersuchen eingehende Pakete und teilen diese auf der Basis verschiedener Kriterien in logische Gruppen ein. ACL-Gruppen verfügen über bestimmte Aktionen, die für jedes Paket ausgeführt werden, die der Gruppe zugeordnet ist. ACLs ermöglichen folgende Aktionen:

- Forward
- Verweigern
- Verweigern und Port deaktivieren

ACLs werden vorwiegend für folgende Zwecke eingesetzt:

- Als Sicherheitsmechanismus, der Paketen in einer Gruppe den Zugang entweder gewährt oder verweigert. Dieser Mechanismus wird im Abschnitt über Netzwerksicherheit erläutert.
- Als Mechanismus zur Klassifizierung von Paketen in Datenverkehrsklassen, für die verschiedene CoS/QoS-Behandlungsaktionen ausgeführt werden.

ACLs enthalten verschiedene Klassifizierungsregeln und -aktionen. Ein Zugriffssteuerungselement (ACE) besteht aus einer einzelnen Klassifizierungsregel und seiner Aktion. Eine einzelne ACL kann eine oder mehrere ACEs enthalten.

Die Reihenfolge der ACEs innerhalb einer ACL ist wichtig, da diese in chronologischer Reihenfolge angewendet werden. Die ACEs werden der Reihe nach verarbeitet, wobei mit der ersten ACE begonnen wird. Sobald ein Paket einer ACE-Klassifizierung entspricht, wird die ACE-Aktion ausgeführt und die ACL-Verarbeitung wird beendet. Falls mehrere ACLs verarbeitet werden müssen, wird die Standard-Zurückweisungsaktion erst nach Verarbeitung aller ACLs angewendet. Die Standard-Zurückweisungsaktion setzt voraus, dass der Benutzer explizit den gesamten gültigen Datenverkehr zulässt, einschließlich Management-Datenverkehr, z. B. telnet, HTTP oder SNMP, der an den Router selbst gerichtet ist.

Es werden zwei Arten von ACLs definiert:

- **IP ACL** Trifft nur auf IP-Pakete zu. Alle Klassifizierungsfelder beziehen sich auf IP-Pakete.
- **MAC ACL** Trifft auf jeden Paket zu, einschließlich Nicht-IP-Pakete. Klassifizierungsfelder basieren nur auf Ebene 2.

Es gibt zwei Möglichkeiten, ACLs auf eine Schnittstelle anzuwenden:

- **Policy** (Richtlinie) In dieser Form sind ACLs in einer komplexen Struktur zusammengefasst, die als Richtlinie bezeichnet wird. Die Richtlinie kann sowohl ACLs als auch QoS-Regeln enthalten. Benutzer können die Richtlinie auf eine Schnittstelle anwenden (siehe Erweiterter QoS-Modus").
- **Simple** (Einfach) In der einfachen Form wird eine einzelne (MAC- oder IP-) ACL auf eine Schnittstelle angewendet. Obwohl eine Richtlinie auf keine Schnittstelle angewendet werden kann, ist es möglich, grundlegende QoS-Regeln anzuwenden, die Pakete Ausgabewarteschlangen zuordnen (siehe Einfacher QoS-Modus").

Zuordnen zu Warteschlangen

Es kann entweder ein Trustverhalten ausgewählt werden, oder es lassen sich folgende Felder für den Ausgabeservice auswählen:

- **VLAN Priority Tags** (VPT, VLAN-Prioritäts-Tags) VPTs werden auf der Basis von VPT-Ausgabewarteschlangen zugeordnet. Während die Zuweisung zu Warteschlangen benutzerdefinierbar ist, wird die VPT-Standardzuweisung zur Ausgabewarteschlange wie folgt durchgeführt. Bei der VPT-Standardzuweisung hat Warteschlange 1 die niedrigste Priorität, wie in der folgenden Tabelle gezeigt:

Tabelle 10-1. Standardmäßige VPT-Zuweisungstabelle

VPT-Wert	Nummer der Warteschlange
0	3
1	1
2	2
3	4
4	5
5	6
6	7
7	8

ANMERKUNG: Die Zuweisung des VPT zur Ausgabewarteschlange erfolgt systemweit, und kann für einzelne Ports aktiviert oder deaktiviert werden.

- **802.1p Port-Based** (portbasiert) Ankommende Pakete ohne Tags werden einem Standard-VPT zugewiesen, der vom Benutzer für einzelne Ports eingestellt werden kann. Nach Zuweisung des VPT wird das Paket behandelt, als ob es mit diesem Tag angekommen wäre. Die VPT-Zuweisung zur Ausgabewarteschlange stützt sich auf dieselben benutzerdefinierten 802.1p tag-basierten Definitionen.

- **Layer 3 Predefined Field** (Ebene 3 Vordefiniertes Feld) Der Benutzer kann das System für die Verwendung der IP DSCP für die Zuordnung zur Ausgabe-Prioritätswarteschlange konfigurieren. Die Zuweisung des IP DSCP zu einer Prioritäts-Warteschlange erfolgt auf der Grundlage einzelner Systeme. Ist dieser Modus aktiv, wird ein Nicht-IP-Paket immer der Warteschlange mit dem Status Best Effort" (Bester Versuch) zugeordnet. Die Standardzuweisung wird in der folgenden Tabelle gezeigt:

Tabelle 10-2. Standardmäßige DSCP-Zuweisungstabelle

DSCP-Wert	Nummer der Warteschlange
0 - 7.	q1 (niedrigste Priorität)
8-15	q2
16 - 23	q3
24-31	q4
32-39	q5
40-47	q6
48-55	q7
55-63	q8 (höchste Priorität)

ANMERKUNG: Die DSCP-Werte 3, 11, 19, 27, 35, 43, 51 und 59 werden q1, q2 ... q8 zugewiesen. Diese Einstellungen lassen sich nicht ändern.

- **Layer 4 Predefined Fields** (Ebene 4 Vordefinierte Felder) Konfiguriert das System für die Verwendung des TCP/UDP-Zielports des eingehenden Pakets, um das Paket den Ausgabeprioritäts-Warteschlangen zuzuweisen. Die Zuweisung des TCP/UDP-Zielports zu einer Prioritäts-Warteschlange wird für jedes System einzeln in zwei unterschiedlichen Tabellen eingestellt. Sie kann pro Port aktiviert oder deaktiviert werden.
- **None** (Keiner) Der gesamte Verkehr wird dem Best Effort"-Service zugeordnet.

Nach der Zuweisung von Paketen zu einer bestimmten Warteschlange mithilfe der ausgewählten Klassifizierungsmethode können verschiedene Services angewendet werden. Für Ausgabewarteschlangen lassen sich folgende Schedulingschemata festlegen:

- Strikte Priorität.
- Weighted Round Robin (WRR).
- Eine Kombination aus diesen Methoden.

Planungsschemata werden für einzelne Systeme festgelegt. WRR-Bewertungen können den Warteschlangen in beliebiger Reihenfolge zugewiesen werden. Diese Bewertungseinstellungen stehen für einzelne Ports zur Verfügung.

Für jede Schnittstelle oder Warteschlange lässt sich außerdem die folgende Ausgabeformung konfigurieren:

- Burstgröße.
- Garantierte Datenrate (CIR).
- Aktionen für Datenverkehr, der das Limit überschreitet.

QoS-Modi

QoS wird beim PowerConnect 6024/6024F entweder im einfachen oder erweiterten Modus aktiviert.

einfachen QoS-Modus

Im einfachen QoS-Modus kann einer der Trustmodi aktiviert werden, einschließlich:

- VPT
- DSCP
- TCP (Übertragungssteuerungsprotokoll)
- UDP
- Kein Vorgang

Darüber hinaus kann eine einzelne MAC- oder IP-basierte ACL direkt an die Schnittstelle angehängt werden (weitere Informationen finden Sie unter

Konfigurieren der Netzwerksicherheit Nur Pakete mit einer **Forward**-Aktion können der Ausgabewarteschlange auf der Basis der angegebenen Klassifizierung zugewiesen werden.

Durch ordnungsgemäße Konfiguration der Ausgabewarteschlangen können Sie die folgenden Services des einfachen Modus einstellen:

- **Minimum Delay** (Minimale Verzögerung) Die Warteschlange wird einer Richtlinie mit einer strikten Priorität zugewiesen, und der Datenverkehr wird der Warteschlange mit der höchsten Priorität zugewiesen.
- **Best Effort** Der Datenverkehr wird der Warteschlange mit der niedrigsten Priorität zugewiesen.
- **Bandwidth Assignments** (Bandbreitenzuweisungen) Durch Konfiguration des WRR-Planungsschemas und Auswahl der richtigen Bewertungen können Sie Bandbreiten zuordnen.

Erweiterten QoS-Modus

Der erweiterte QoS-Modus legt Regeln für die Flussklassifizierung fest und weist Aktionsregeln zu, die sich auf das Bandbreitenmanagement beziehen. Die Regeln werden über die Klassifizierungskontrollliste (CCL) definiert.

CCLs werden gemäß in der ACL definierten Klassifizierung festgelegt, und Sie können nur dann festgelegt werden, wenn bereits eine gültige ACL definiert wurde. Wenn CCLs definiert werden, können ACLs und CCLs in einer komplexeren Struktur gruppiert werden, einer sogenannten Richtlinie". Richtlinien können auf eine Schnittstelle angewendet werden. Richtlinie-ACLs/CCLs werden in der Reihenfolge angewendet, wie sie in der Richtlinie organisiert sind. Einem Port kann nur eine Richtlinie zugewiesen werden.

Im erweiterten QoS-Modus können ACLs direkt auf eine Schnittstelle angewendet werden. Jedoch lassen sich eine Richtlinie und eine ACl nicht gleichzeitig auf eine Schnittstelle anwenden.

Nach der Zuweisung von Paketen zu einer bestimmten Warteschlange können Sie verschiedene Services anwenden, wie z. B.: Konfigurieren von Ausgabewarteschlangen für das Schedulingschema oder Konfigurieren der Ausgabeformung für die Burstgröße, CIR oder CBS pro Schnittstelle oder pro Warteschlange.

Konfiguration der Services - Beispiele

Mithilfe der Einstellungen des erweiterten QoS-Modus können Sie die folgenden Services auf den Netzwerk-Datenverkehr anwenden:

- **Best Effort** Der Datenverkehr wird der Warteschlange mit der niedrigsten Priorität zugewiesen.
- **802.1p** Der VPT-Wert wird entsprechend der Klassifizierung eingestellt.
- **IP DSCP** Der Wert wird entsprechend der Klassifizierung eingestellt.
- **Minimum Delay** (Minimale Verzögerung) Die Warteschlange wird einer Richtlinie mit einer strikten Priorität zugewiesen, und der Datenverkehr wird der Warteschlange mit der höchsten Priorität zugewiesen.
- **Ingress Metering/Rate Limiting** (Eintrittsmessung/Ratenbeschränkung) Es wird ein maximaler Wert für die Bandbreite angegeben, über dem der gesamte Datenverkehr zurückgewiesen wird. Dies erfolgt durch Festlegen eines Messpunkts beim Eingang für die maximale Bandbreite und Einstellen der Richtlinie, dass Datenverkehr bei Überschreitung zurückgewiesen wird. Für eine wirksame Konfiguration dieses Dienstes darf die vollständige Bandbreite eines bestimmten Ausgangsports nicht die Portrate übersteigen.

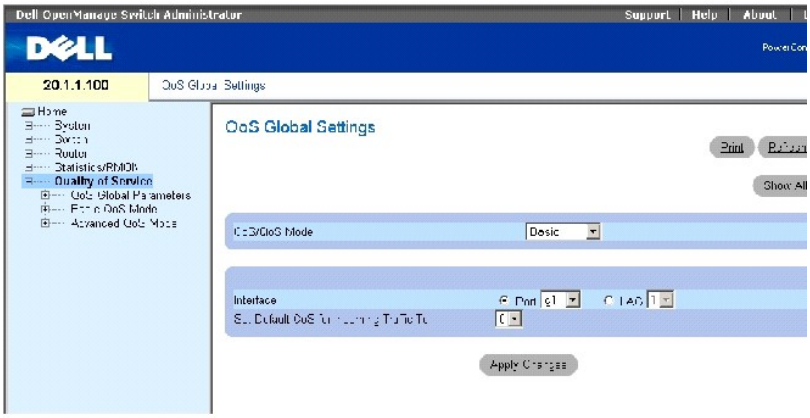
Konfigurieren von globalen QoS-Parametern

Die Seite **QoS Global Parameters** (Globale QoS-Parameter) enthält Verknüpfungen zu den QoS-Seiten, auf denen QoS aktiviert wird, DSCP-Werte und -Einstellungen umadressiert werden, Netzwerk-Datenverkehr in Warteschlangen eingereiht wird, und die Datenverkehrklassifizierung definiert wird. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service→ QoS Global Parameters**.

Definieren von QoS-Einstellungen

Auf der Seite **QoS Global Settings** (Globale QoS-Einstellungen) können Sie den QoS-Modus auswählen und die Standard-CoS für den eingehenden Datenverkehr auf einer ausgewählten Schnittstelle auswählen. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service→ QoS Global Parameters→ QoS Settings**.

Abbildung 10-1. Globale QoS-Einstellungen



QoS Mode (QoS-Modus) Deaktiviert oder aktiviert den einfachen oder erweiterten QoS-Modus. Der einfache Modus ist standardmäßig aktiviert.

ANMERKUNG: Beim Wechseln vom einfachen in den erweiterten QoS-Modus können einige Einstellungen verloren gehen.

Interface (Schnittstelle) Der Port oder die LAG, für die die CoS-Standardrichtlinie definiert werden.

Set Default CoS for Incoming Traffic To (Standard-CoS für eingehenden Datenverkehr einstellen auf) Legt den Standard-CoS-Wert für eingehende Pakete fest, für die kein VLAN-Tag definiert ist. Die möglichen Feldwerte sind **0-7**. Die Standard-CoS lautet **0**.

Auswählen eines Servicemodus

1. Öffnen Sie die Seite **QoS-Einstellungen**.
2. Wählen Sie im Feld **QoS Mode** (QoS-Modus) einen Servicemodus aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der QoS-Modus wird ausgewählt und das Gerät aktualisiert.

Einstellen des CoS-Standardwerts für eingehenden Datenverkehr an einer Schnittstelle

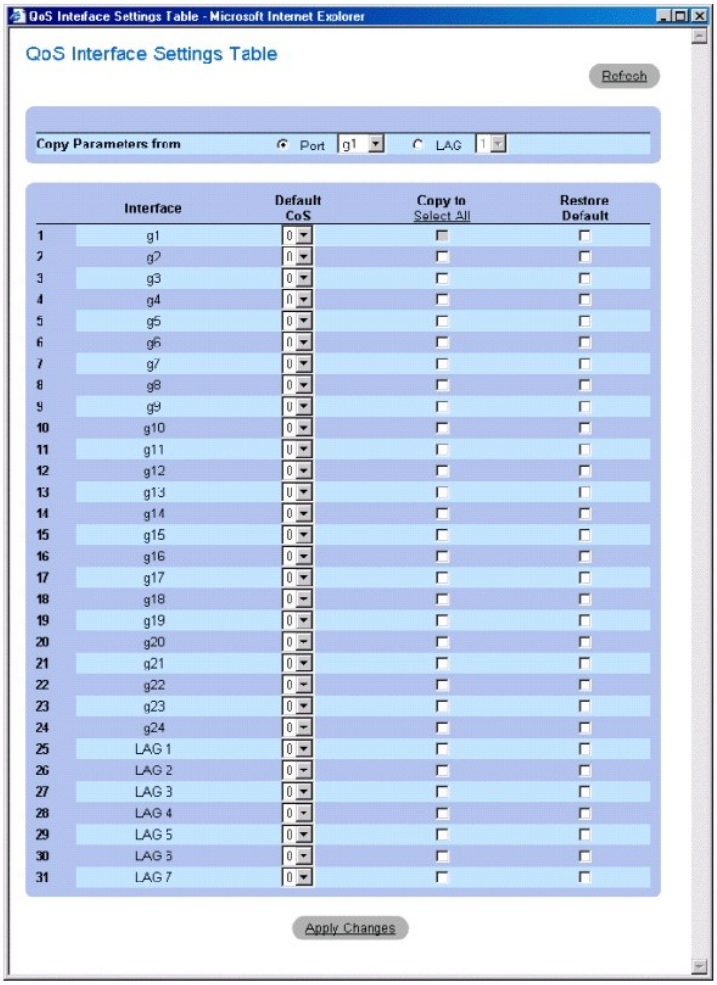
1. Öffnen Sie die Seite **QoS-Einstellungen**.
2. Wählen Sie eine Schnittstelle aus, und legen Sie den CoS-Standardwert für eingehenden Datenverkehr über das Drop-Down-Menü fest.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der CoS-Standardwert für eingehenden Datenverkehr an der Schnittstelle wird ausgewählt und das Gerät aktualisiert.

Kopieren von QoS-Schnittstelleneinstellungen

1. Öffnen Sie die Seite **QoS-Einstellungen**.
2. Klicken Sie auf **Show All** (Alles anzeigen), um die Seite **QoS Interface Settings Table** (Tabelle mit QoS-Schnittstelleneinstellungen) anzuzeigen.
3. Wählen Sie eine Schnittstelle aus, aus der Sie QoS-Einstellungen auf alle oder bestimmte der Schnittstellen kopieren möchten, die in der Tabelle mit QoS-Schnittstelleneinstellungen aufgelistet sind.
4. Aktivieren Sie das Kontrollkästchen **Copy to** (Kopieren nach) für jede Schnittstelle, auf die die QoS-Einstellungen kopiert werden sollen, oder klicken Sie auf **Select All** (Alle auswählen), um die QoS-Einstellungen auf alle aufgelisteten Schnittstellen zu kopieren.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Abbildung 10-2. Tabelle mit QoS-Schnittstelleneinstellungen



Definieren von QoS-Einstellungen mithilfe der CLI-Befehle

Tabelle 10-3. CLI-Befehle für das Definieren von QoS-Einstellungen

CLI-Befehl	Beschreibung
`qos [advanced]`	Aktiviert/deaktiviert QoS im einfachen /erweiterten Modus für das gesamte Gerät.
`show qos`	Zeigt den QoS-Modus für das gesamte Gerät an.
`qos cos default-cos`	Konfiguriert den CoS-Standardwert für die Schnittstelle.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

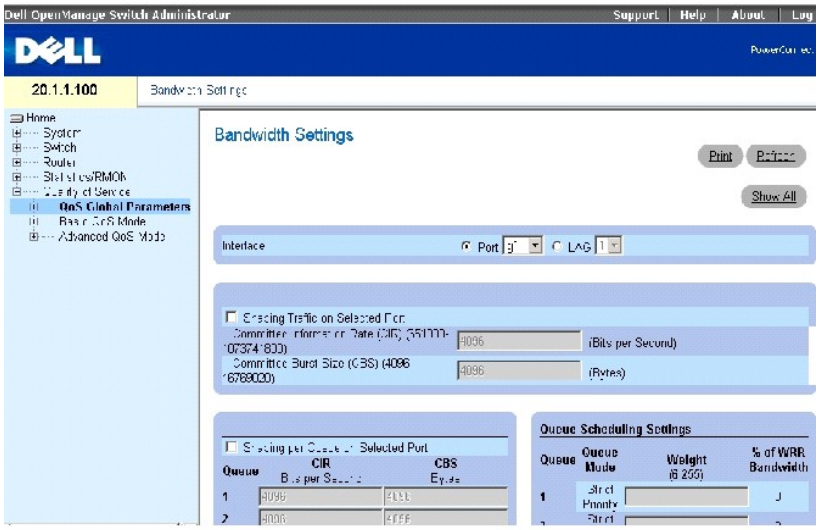
```
Console (config)# qos
```

```
Console (config)# interface ethernet g5

Console (config-if)# qos cos 3

Console (config-if)# exit

Console (config)# exit

Console# show qos

QoS: basic

Basic trust: vpt
```

Definieren von Bandbreiteneinstellungen

Auf der Seite **Bandwidth Settings** (Bandbreiteneinstellungen) legen Sie die Bandbreiteneinstellungen für eine bestimmte Eintrittsschnittstelle fest. Durch eine Änderung des Warteschlangen-Scheduling werden die Warteschlangeneinstellungen global betroffen. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service→ QoS Global Parameters→ Bandwidth Settings**.

Abbildung 10-3. Bandbreiteneinstellungen



Die Seite **Bandbreiteneinstellungen** enthält die folgenden Felder:

Interface (Schnittstelle) Der Port oder die LAG, für die die Bandbreiteneinstellungen gelten.

Shaping Traffic on Selected Port (Formung von Datenverkehr auf ausgewählten Ports) Konfiguriert die garantierte Datenrate (CIR) und die garantierte Burstgröße (CBS) auf der Schnittstelle. Es ist möglich, die Formung pro Warteschlange und pro Schnittstelle gleichzeitig anzugeben. Die Formung wird vom niedrigeren angegebenen Wert bestimmt.

Shaping per Queue on Selected Port (Formung pro Warteschlange an ausgewähltem Port) Konfiguriert CIR und CBS für einzelne Warteschlangen. Es ist möglich, die Formung pro Warteschlange und pro Schnittstelle gleichzeitig anzugeben. Die Formung wird vom niedrigeren angegebenen Wert bestimmt.

Queue Scheduling Settings (Einstellungen für Warteschlangen-Scheduling) Konfiguriert die Bewertung für jede WRR-Warteschlange (Weighted Round Robin).

WRR Weight (0-255) (WRR-Bewertung) Weist Bewertungen für jede Weighted Round Robin-Warteschlange zu. Die WRR-Warteschlangen werden pro Port definiert und decken einen Bereich von 6-255 ab. Jede Warteschlange kann einer Bewertung von 0 zugewiesen werden; in diesem Fall ist die Warteschlange nicht in Betrieb und gewissermaßen geschlossen.

Formen des Datenverkehrs an einer ausgewählten Schnittstelle

1. Öffnen Sie die Seite **Bandwidth Settings** (Bandbreiteneinstellungen).
2. Wählen Sie eine Schnittstelle.
3. Aktivieren Sie das Kontrollkästchen **Shaping Traffic on Selected Port** (Formen des Datenverkehrs an ausgewähltem Anschluss).
4. Geben Sie die CIR- und CBS-Werte für die Schnittstelle ein.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die CIR und CBS für die ausgewählte Schnittstelle werden konfiguriert und das Gerät aktualisiert.

Formen des Datenverkehrs für einzelne Warteschlangen

1. Öffnen Sie die Seite **Bandwidth Settings** (Bandbreiteneinstellungen).
2. Wählen Sie eine Schnittstelle.
3. Aktivieren Sie das Kontrollkästchen **Shaping per Queue on Selected Port** (Formen pro Warteschlange an ausgewähltem Port).
4. Geben Sie CIR- und CBS-Werte für jede Warteschlange ein.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die CIR und CBS für jede Warteschlange an der ausgewählten Schnittstelle werden konfiguriert und das Gerät aktualisiert.

Konfigurieren der Einstellungen für das Warteschlangen-Scheduling pro Port

1. Öffnen Sie die Seite **Bandwidth Settings** (Bandbreiteneinstellungen).

ANMERKUNG: Auf der Seite **Global Queue Settings** (Globale Warteschlangen-Einstellungen) können Sie die Einstellungen für das Warteschlangen-Scheduling global ändern.

2. Konfigurieren Sie für jede der acht Warteschlangen die Einstellung **Strict Priority** (Strikte Priorität), oder geben Sie einen Wert für **Weight** (Bewertung) ein.
3. Geben Sie für jede Warteschlange, die systemweit als WRR-Warteschlange eingestellt wurde, eine Bewertung ein.

Das Bewertungsverhältnis legt die Frequenz fest, mit der der Paket-Scheduler Pakete aus den einzelnen Warteschlangen ausgliedert. Das Verhältnis für jede Warteschlange definiert sich aus der Warteschlangenbewertung geteilt durch die Summe aller Bewertungen (normalisierte Bewertung), wodurch die Bandbreitenzuordnung für jede Warteschlange eingestellt wird.

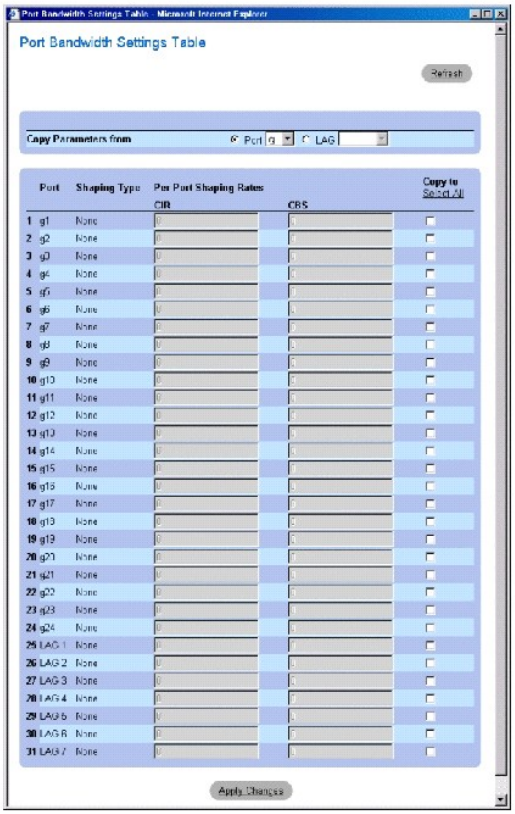
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das Gerät wird aktualisiert.

Anzeigen der Tabelle mit Bandbreiteneinstellungen für Port

1. Öffnen Sie die Seite **Bandwidth Settings** (Bandbreiteneinstellungen).
2. Klicken Sie auf **Show All** (Alles anzeigen), um die Seite **Port Bandwidth Settings Table** (Tabelle mit Bandbreiteneinstellungen für Port) anzuzeigen.

Abbildung 10-4. Tabelle für die Port-Bandbreiteneinstellungen



Shaping Type (Formungstyp) Kann entweder pro Port, pro Warteschlange, beide oder keiner von beiden sein.

Per Port Shaping Rates (Formungsraten pro Port) CIR und CBS werden pro Port angewendet. Wenn Sie die Formung pro Warteschlange anzeigen möchten, verwenden Sie die Bearbeitungsseite.

Kopieren von Bandbreiteneinstellungen für Port

1. Öffnen Sie die Seite **Bandwidth Settings** (Bandbreiteneinstellungen).
2. Klicken Sie auf **Show All** (Alles anzeigen), um die Seite **Port Bandwidth Settings Table** (Tabelle mit Bandbreiteneinstellungen für Port) anzuzeigen.
3. Wählen Sie eine Schnittstelle aus, aus der Sie die Bandbreiteneinstellungen pro Port auf alle oder bestimmte der Schnittstellen kopieren möchten, die in der Tabelle mit Bandbreiteneinstellungen für Port aufgelistet sind.
4. Aktivieren Sie das Kontrollkästchen **Copy to** (Kopieren nach) für jede Schnittstelle, auf die die Bandbreiteneinstellungen für den Port kopiert werden sollen, oder klicken Sie auf **Select All** (Alle auswählen), um die Bandbreiteneinstellungen für den Port auf alle aufgelisteten Schnittstellen zu kopieren.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Definieren von Bandbreiteneinstellungen mithilfe der CLI-Befehle

Tabelle 10-4. CLI-Befehle für die Bandbreiteneinstellung

CLI-Befehl	Beschreibung
`traffic-shape {committed-rate committed-burst} [queue-id]`	Stellt den Formgeber für den Ausgangsport oder die Warteschlange ein.
`wrr-queue bandwidth weight1 weight2 ... weight_n`	Weist Weighted Round Robin (WRR)-Gewichtungen zu Ausgangswarteschlangen zu.
	Konfiguriert die Anzahl der Warteschlangen mit strikter

priority-queue out num-of-queues *number-of-queues*	Priorität.
show qos interface [ethernet *interface-number* | vlan *vlan-id* | port-channel *number*] [buffers | queuing | policers | shapers]	Zeigt die QoS-Schnittstelleninformationen an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface ethernet g5

Console (config-if)# traffic-shape 124000 96000

Console (config-if)# wrr-queue bandwidth 1 2 3 4 5 6 7 8

Console (config-if)# exit

Console (config)# priority-queue out num-of-queues 2

Console (config)# exit

Console> show qos interface ethernet g1 buffers

Ethernet g1

Notify Q depth:

qid-size

1 - 125

2 - 125

3 - 125

4 - 125

5 - 125

125 - 6

7 - 125

8 - 125
```

qid	WRED	thresh0	thresh1	thresh2
1	dis	100	100	100
2	dis	100	100	100
3	dis	100	100	100
4	dis	100	100	100
5	Ena	N/A	N/A	N/A
6	Ena	N/A	N/A	N/A
7	Ena	N/A	N/A	N/A
8	Ena	N/A	N/A	N/A

qid	MinDP0	MaxDP0	ProbDP0	MinDP1	MaxDP1	ProbDP1	MinDP2	MaxDP2	ProbDP2	weight
1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5	50	60	13	65	80	6	85	95	4	2
6	50	60	13	65	80	6	85	95	4	2
7	50	60	13	65	80	6	85	95	4	2
8	50	60	13	65	80	6	85	95	4	2

```
Console> show qos interface ethernet g1 queueing

Ethernet g1

wrr bandwidth weights and EF priority:
```

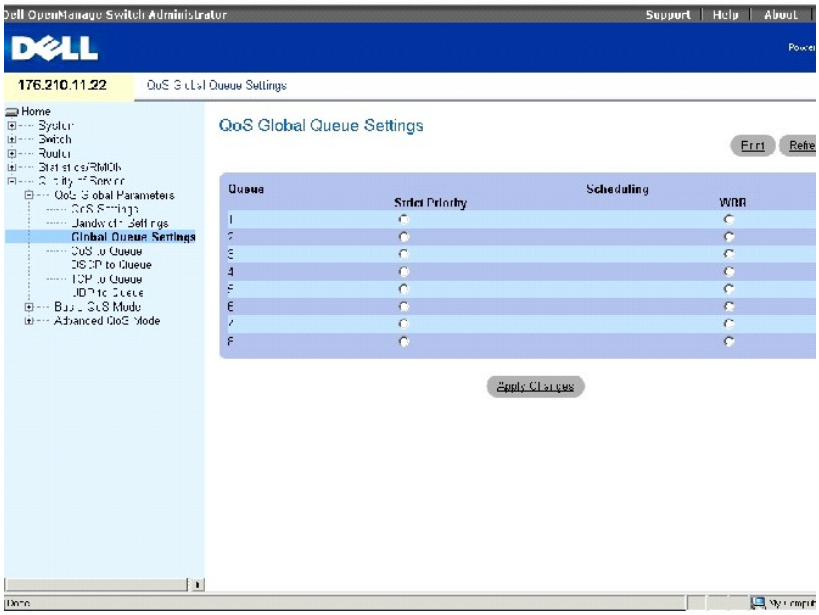
```
qid-weights Ef - Priority

1 - 125 dis- N/A

2 - 125 dis- N/A

3 - 125 dis- N/A

4 - 125 dis- N/A

5 - N/A ena- 5

6 - 125 dis- N/A

7 - 125 dis- N/A

8 - N/A ena- 8

Cos-queue map:

cos-qid

0 - 3

1 - 1

2 - 2

3 - 4

4 - 5

5 - 6

6 - 7
```

Definieren von globalen Warteschlangeneinstellungen

Auf der Seite **Globale Warteschlangen-Einstellungen** können Sie Warteschlangenzeitpläne global ändern.

Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service→ QoS Global Parameters→ Queue Settings**.

Abbildung 10-5. Globale Warteschlangen-Einstellungen



Die Seite **Globale Warteschlangen-Einstellungen** enthält die folgenden Felder:

Queue (Warteschlange) Zeigt die Nummer der Warteschlange an.

Strict Priority Gibt an, dass die Verkehrsablaufplanung strikt auf der Warteschlangenpriorität basiert. Dies ist die Standardeinstellung für Warteschlangen.

WRR Legt fest, ob der Zeitplan des Datenverkehrs bei den zugewiesenen Egress-Warteschlangen auf den Weighted Round Robin (WRR)-Wertigkeiten basiert. WRR-Bewertungen werden auf der Seite **Bandbreiteneinstellungen** definiert.

Konfigurieren globaler Einstellungen für das Warteschlangen-Scheduling

1. Öffnen Sie die Seite **Global Queue Settings** (Globale Warteschlangeneinstellungen).
2. Klicken Sie für jede der Warteschlangen auf **Strict Priority** (Strikte Priorität) oder **WRR** (Weighted Round Robin)**.**

   Die tatsächlichen WRR-Einstellungen werden pro Port auf der Seite **Bandbreiteneinstellungen** eingestellt.

   Die Aktivierung einer Optionsschaltfläche für eine beliebige Warteschlange markiert automatisch den Schedulingtyp für die Warteschlangen nach dieser Warteschlange. Jede Warteschlange vor der ausgewählten Warteschlange verwendet den entgegengesetzten Typ des Prioriätsscheduling. Wenn Sie beispielsweise für Warteschlange 6 auf **Strict Priority** (Strikte Priorität) klicken, wird für Warteschlangen 7 und 8 ebenfalls die Option **Strict Priority** markiert. Warteschlangen 1-5 werden hingegen als **WRR** markiert.

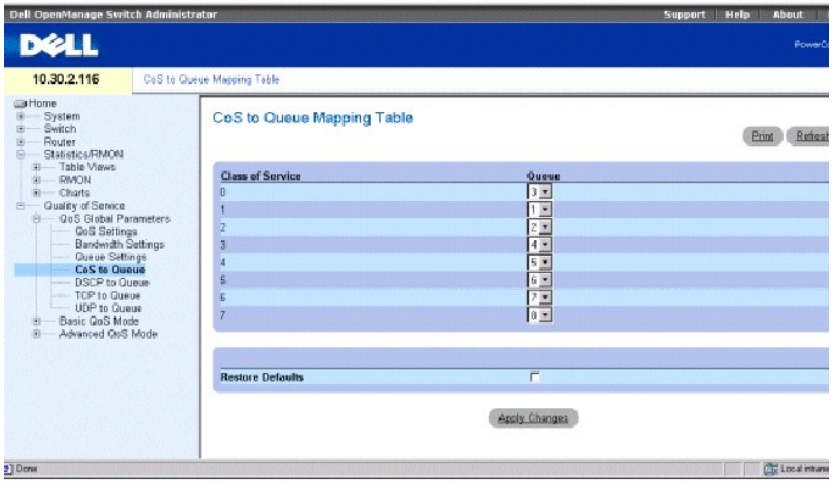
ANMERKUNG: Es müssen mindestens zwei Warteschlangen als WRR-Warteschlangen konfiguriert werden.

3. Klicken Sie auf **Apply Changes**, um das Gerät zu aktualisieren.

Definieren der Zuweisung von CoS auf eine Warteschlange

Auf der Seite **CoS to Queue Mapping Table** (Zuweisungstabelle CoS/Warteschlange) können Sie CoS-Werte bestimmten Warteschlangen zuweisen. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service→ QoS Global Parameters→ CoS to Queue**.

Abbildung 10-6. Zuordnen von CoS zu einer Warteschlange



Class of Service (Serviceklasse) Der 802.1Q-VLAN-Prioritäts-Tag im eingehenden Paket.

Queue (Warteschlange) Ordnet CoS der ausgewählten Warteschlange zu. Die möglichen Werte für die Warteschlangen sind **1-8**.

Eingehende Pakete mit dem angegebenen CoS-Wert werden der definierten Warteschlange zugeordnet, falls **Trust** für CoS aktiviert wurde.

Restore Defaults (Standardeinstellungen wiederherstellen) Stellt für alle Warteschlangen die Standardeinstellung für die Serviceklasse wieder her.

Zuordnen von CoS zu Warteschlangen

1. Öffnen Sie die Seite **CoS to Queue Mapping Table** (Zuweisungstabelle CoS/Warteschlange).
2. Wählen Sie für jeden Eintrag unter **Class of Service** (Serviceklasse) eine Warteschlange aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die CoS wird den Warteschlangen zugewiesen und das Gerät aktualisiert.

Zurücksetzen der CoS-Zuweisung auf die Standard-Warteschlangen:

1. Öffnen Sie die Seite **CoS to Queue Mapping Table** (Zuweisungstabelle CoS/Warteschlange).
2. Aktivieren Sie das Kontrollkästchen **Restore Defaults** (Standardeinstellungen wiederherstellen).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Zuweisung CoS/Warteschlangen wird auf die Standardeinstellung zurückgesetzt und das Gerät aktualisiert.

Zuweisen der CoS zu Warteschlangen mithilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für die Zuweisung der CoS zu Warteschlangen.

Tabelle 10-5. CLI-Befehle für das Zuweisen von CoS-Warteschlangen

CLI-Befehl	Beschreibung
`wrr-queue cos-map` *queue-id cos1 ... cos8*	Weist zugewiesene CoS-Werte zu, um eine der Ausgangswarteschlangen auszuwählen.
`show qos map [dscp-queue | tcp-port-queue | udp-port-queue | dscp-policed | dscp-mutation]`	Zeigt alle Maps für QoS an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# wrr-queue cos-map 7 246

Console (config)# show qos map dscp-queue

Dscp-queue map:

d1 : d2   0   1   2   3   4   5   6   7   8   9

-----------------------------------------

0  : 01   01  01  01  01  01  01  01  02  02

1  : 02   02  02  02  02  02  03  03  03  03

2  : 03   03  03  03  04  04  04  04  04  04

3  : 04   04  05  05  05  05  05  05  05  05

4  : 06   06  06  06  06  06  06  06  07  07

5  : 07   07  07  07  07  07  08  08  08  08

6  : 08   08  08  08

Console (config)# show qos map tcp-port-queue

Tcp port-queue map:

Port queue

----- ------

6000    1
```

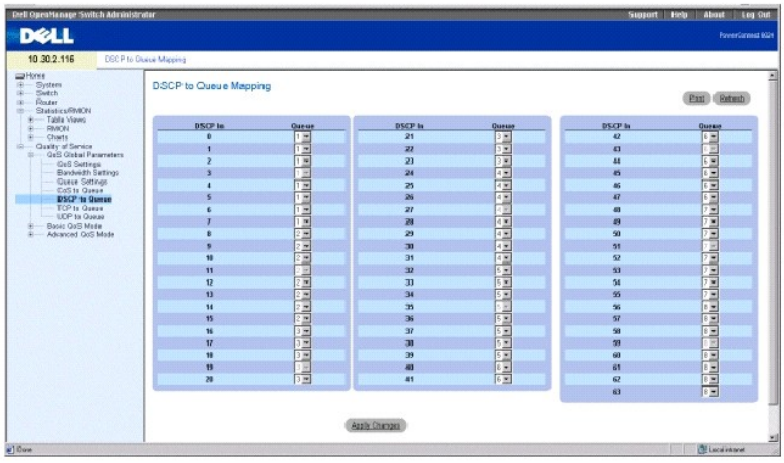
```
6001    2

6002    3

Console (config)# show qos map udp-port-queue

Udp port-queue map:

Port queue

----- -----

8000    1

8001    2

Console (config)# show qos map dscp-policed

Policed-dscp map:

d1 :  d2  0   1   2   3   4   5   6   7   8   9

----------------------------------------

0  :  00  01  02  03  04  05  06  07  08  09

1  :  10  11  12  13  14  15  16  17  18  19

2  :  20  21  22  23  24  25  26  27  28  29

3  :  30  31  32  33  34  35  36  37  38  39

4  :  40  41  42  43  44  45  46  47  48  49

5  :  50  51  52  53  54  55  56  57  58  59

6  :  60  61  62  63

Console (config)# show qos map dscp-mutation

Dscp-dscp mutation map:
```

```
d1 :  d2  0   1   2   3   4   5   6   7   8   9

-----------------------------------------

0  :  00  01  02  03  04  05  06  07  08  09

1  :  10  11  12  13  14  15  16  17  18  19

2  :  20  21  22  23  24  25  26  27  28  29

3  :  30  31  32  33  34  35  36  37  38  39

4  :  40  41  42  43  44  45  46  47  48  49

5  :  50  51  52  53  54  55  56  57  58  59

6  :  60  61  62  63
```

Definieren der Zuordnung von DSCP zu einer Warteschlange

Auf der Seite **DSCP to Queue Mapping** (Zuweisung DSCP/Warteschlange) können Sie DSCP-Werte bestimmten Warteschlangen zuweisen. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service→ QoS Global Parameters→ DSCP to Queue**.

Abbildung 10-7. Zuordnen von DSCP zu Warteschlangen



DSCP In Gibt den DSCP-Wert (Differentiated Services Code Point) im eingehenden Paket an.

Queue (Warteschlange) Ordnet den DSCP-Wert der ausgewählten Warteschlange zu.

Eingehende Pakete mit dem angegebenen DSCP-Wert werden der angegebenen Warteschlange zugeordnet, falls der **Trust** modus für DSCP aktiviert wurde

Die DSCP-Werte 3, 11, 19, 27, 35, 43, 51 und 59 werden q1, q2 ... q8 zugewiesen. Diese Einstellungen lassen sich nicht ändern.

Zuweisen von DSCP zu Warteschlangen

1. Öffnen Sie die Seite **DSCP to Queue Mapping** (Zuweisung DSCP/Warteschlange).
2. Wählen Sie eine Warteschlange für jede DSCP-Ebene aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

DSCP wird den Warteschlangen zugewiesen und das Gerät aktualisiert.

Zuweisen von DSCP zu Warteschlangen mithilfe der CLI-Befehle

Tabelle 10-6. CLI-Befehle für DSCP zu Warteschlangen

CLI-Befehl	Beschreibung
`qos map dscp-queue` *`dscp-list`* `to` *`queue-id`*	Ändert die DSCP/CoS-Zuweisung.
`show qos map [dscp-queue | tcp-port-queue | udp-port-queue | dscp-policed | dscp-mutation]`	Zeigt alle QoS-Maps an.

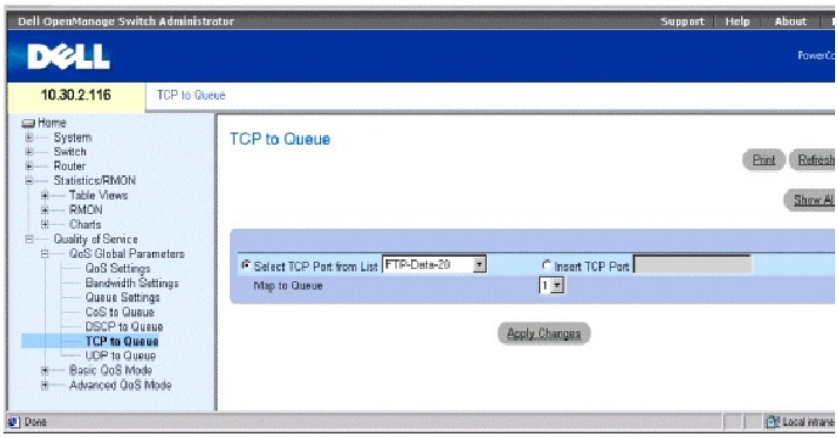
Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# qos map dscp-queue 33 40 41 to 1

Console (config)# exit

Console# show qos map dscp-queue

Dscp-queue Map

d1:  d2 0  1  2  3  4  5  6  7  8  9

---------------------------

0:   01 01 01 01 01 01 02 02

1:   02 02 02 02 02 03 03 03

2:   03 03 03 04 04 04 04 04

3:   04 04 05 05 05 05 05 05

4:   06 06 06 06 06 06 07 07

5:   07 07 07 07 08 08 08 08
```

Definieren der Zuordnung von QoS TCP zu einer Warteschlange

Die QoS-Seite **TCP to Queue** (TCP/Warteschlange) ermöglicht die Zuweisung eines TCP-Ports zu einer Warteschlange. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service→ QoS Global Parameters→ TCP to Queue**.

Abbildung 10-8. QoS TCP / Warteschlange



Select TCP Port from List (TCP-Port aus Liste auswählen) Ermöglicht die Auswahl eines bekannten TCP-Ports für die Zuweisung zu einer Warteschlange.

Insert TCP Port (TCP-Port einfügen) Ermöglicht die manuelle Eingabe eines TCP-Ports für die Zuweisung zu einer Warteschlange.

Map to Queue (Warteschlange zuweisen) Gibt die Warteschlange an, der der angegebene TCP-Port zugewiesen wird.

Zuweisen eines bekannten TCP-Ports zu einer Warteschlange

1. Öffnen Sie die Seite **TCP to Queue** (TCP zu Warteschlange).
2. Wählen Sie die Option **Select TCP Port from List** (TCP-Port aus Liste auswählen) aus.
3. Wählen Sie einen TCP-Port aus.
4. Wählen Sie eine Warteschlange aus der Liste **Map to Queue** (Warteschlange zuweisen) aus.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der TCP-Port wird der angegebenen Warteschlange zugewiesen und das Gerät aktualisiert.

Zuweisen eines nicht aufgelisteten TCP-Ports zu einer Warteschlange

1. Öffnen Sie die QoS-Seite **TCP to Queue** (TCP zu Warteschlange).
2. Wählen Sie die Option **Insert TCP Port** (TCP-Port einfügen) aus.
3. Geben Sie die TCP-Portnummer und die Beschreibung in das Feld **Insert TCP Port** (TCP-Port einfügen) ein.
4. Wählen Sie eine Warteschlange aus der Liste **Map to Queue** (Warteschlange zuweisen) aus.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der TCP-Port wird der angegebenen Warteschlange zugewiesen und das Gerät aktualisiert.

Entfernen der Zuweisung TCP/Warteschlange

1. Öffnen Sie die QoS-Seite **TCP to Queue** (TCP zu Warteschlange).
2. Klicken Sie auf **Show All** (Alles anzeigen), um die Seite **TCP to Queue Mapping Table** (Zuweisungstabelle TCP/Warteschlange) anzuzeigen.
3. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen) für jeden der TCP-Ports, für die die Warteschlangenzuweisung entfernt wird.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Zuweisen von TCP-Anschlüssen zu Warteschlangen mithilfe der CLI-Befehle

Tabelle 10-7. CLI-Befehle für die Zuordnung von TCP/Warteschlange

CLI-Befehl	Beschreibung
`qos map tcp-port-queue`*`port1 ... port 8 to queue-id`*	Ändert die Zuweisung des TCP-Ports zur Warteschlange.
`show qos map [dscp-queue | tcp-port-queue | udp-port-queue | dscp-policed | dscp-mutation]`	Zeigt alle QoS-Maps an.

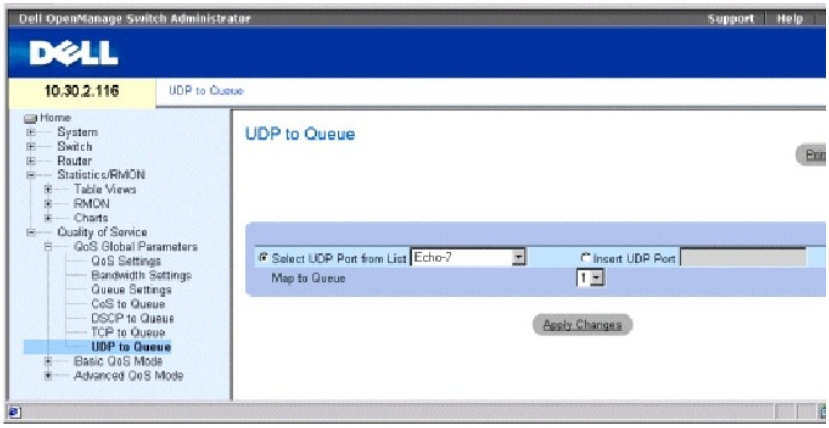
Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# qos map tcp-port-queue 2000 80 to 2

Console (config)# exit

Console# show qos map tcp-port-queue

Tcp port - queue map

Port        queue

--------------------

6000        1

6001        2

6002        3
```

Definieren der Zuordnung von QoS UDP zu einer Warteschlange

Die QoS-Seite **UDP to Queue** (UDP/Warteschlange) ermöglicht die Zuweisung eines UDP-Ports zu einer Warteschlange. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service→ QoS Global Parameters→ UDP to Queue**.

Abbildung 10-9. UDP/Warteschlange



Select UDP Port from List (UDP-Port aus Liste auswählen) Ermöglicht die Auswahl eines bekannten UDP-Ports für die Zuweisung zu einer Warteschlange.

Insert UDP Port (UDP-Port einfügen) Ermöglicht die manuelle Eingabe eines UDP-Ports für die Zuweisung zu einer Warteschlange.

Map to Queue (Warteschlange zuweisen) Gibt die Warteschlange an, der der angegebene UDP-Port zugewiesen wird.

Zuweisen eines bekannten UDP-Ports zu einer Warteschlange

1. Öffnen Sie die Seite **UDP to Queue** (UDP zu Warteschlange).
2. Wählen Sie die Option **Select UDP Port from List** (UDP-Port aus Liste auswählen) aus.
3. Wählen Sie einen UDP-Port aus.
4. Wählen Sie eine Warteschlange aus der Liste **Map to Queue** (Warteschlange zuweisen) aus.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der UDP-Port wird der angegebenen Warteschlange zugewiesen und das Gerät aktualisiert.

Zuweisen eines nicht aufgelisteten UDP-Ports zu einer Warteschlange.

1. Öffnen Sie die Seite **UDP to Queue** (UDP zu Warteschlange).
2. Wählen Sie die Option **Insert UDP Port** (UDP-Port einfügen) aus.
3. Geben Sie die UDP-Portnummer in das Feld **Insert UDP Port** (UDP-Port einfügen) ein.
4. Wählen Sie eine Warteschlange aus der Liste **Map to Queue** (Warteschlange zuweisen) aus.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der UDP-Port wird der angegebenen Warteschlange zugewiesen und das Gerät aktualisiert.

Entfernen der Zuweisung UDP/Warteschlange

1. Öffnen Sie die Seite **UDP to Queue** (UDP zu Warteschlange).
2. Klicken Sie auf **Show All** (Alles anzeigen), um die Seite **UDP to Queue Mapping Table** (Zuweisungstabelle UDP/Warteschlange) anzuzeigen.
3. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen) für jeden der UDP-Ports, für die die Warteschlangenzuweisung entfernt werden soll.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Zuweisen von UDP-Anschlüssen zu Warteschlangen mithilfe der CLI-Befehle

Tabelle 10-8. CLI-Befehle für die Zuordnung UDP/Warteschlange

CLI-Befehl	Beschreibung
`qos map udp-port-queue` *`port1 ... port 8 to queue-id`*	Ändert die Zuweisung des UDP-Ports zur Warteschlange.
`show qos map [dscp-queue | tcp-port-queue | udp-port-queue | dscp-policed | dscp-mutation]`	Zeigt alle QoS-Maps an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# qos map udp-port-queue 68 to 1

Console (config)# exit

Console# show qos map udp-port-queue

Udp port-queue map:

Port      queue

-----     -----

8000      1

8001      2
```

Konfigurieren des einfachen QoS-Modus

Die Seite **Basic QoS Mode** (Einfacher QoS-Modus) enthält Verknüpfungen zu QoS-Seiten, auf denen der Trustmodus und die DSCP-Umschreibung konfiguriert werden. Um die Seite **Einfacher QoS-Modus** zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service→ Basic QoS Mode**.

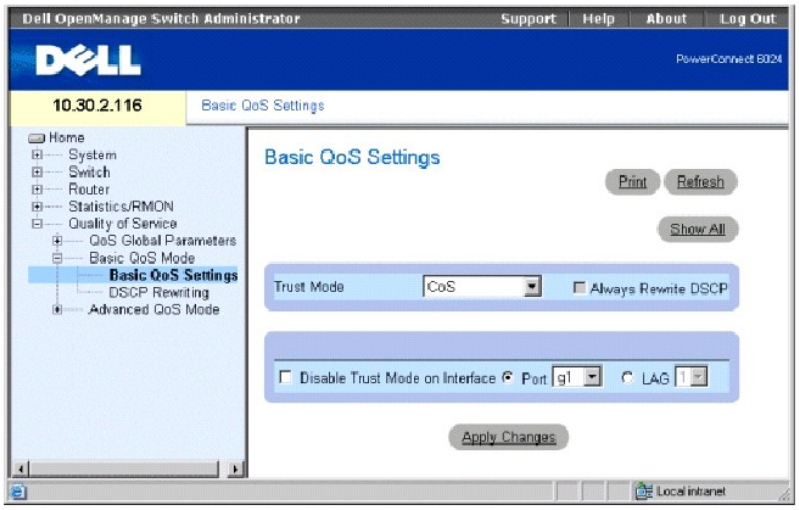
Definieren von Einstellungen einer einfachen QoS

Auf der Seite **Einfache QoS-Einstellungen** können Sie den globalen Trust-Modus konfigurieren, der auf bestimmten Schnittstellen eingestellt wird. Pakete, die in eine QoS-Domäne gelangen, werden am Rand der QoS-Domäne klassifiziert. Werden die Pakete am Rand klassifiziert, kann der Trustmodus an den Ports konfiguriert werden.

DSCP-Werte können am Rand der QoS-Verwaltungsdomäne umgeschrieben werden. Verfügen zwei QoS-Domänen über unterschiedliche DSCP-Definitionen, können die DSCP-Werte umgeschrieben werden. Die DSCP-Map wird nur auf eingehende, DSCP-trusted Ports angewendet

Um die Seite **Einfache QoS-Einstellungen** zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service→ Basic QoS Mode→ Basic QoS Settings**.

Abbildung 10-10. Einfache QoS-Einstellungen



Trust Mode (Trustmodus) Wählt den Trust-Modus aus. Falls CoS-Tag, DSCP-Tag und TCP/UDP-Zuweisung eines Pakets unterschiedlichen Warteschlangen zugewiesen sind, legt der **Trust Mode** die Warteschlange fest, der das Paket zugewiesen wird. Die möglichen Werte sind:

CoS Stellt den Trustmodus auf dem Gerät auf CoS ein. Die CoS-Zuweisung legt die Paketwarteschlange fest.

DSCP Stellt den Trustmodus auf dem Gerät auf DSCP ein. Die DSCP-Zuweisung legt die Paketwarteschlange fest.

TCP/UDP Port Stellt den Trustmodus auf dem Gerät auf TCP/UDP-Port ein. Die TCP/UDP Port-Zuweisung legt die Paketwarteschlange fest.

Always Rewrite DSCP (DSCP immer neu schreiben) Schreibt den DSCP-Tag des Pakets immer entsprechend der QoS-Konfiguration für die DSCP-Neuschreibung neu. Die Option **Always Rewrite DSCP** (DSCP immer neu schreiben) kann nur aktiviert werden, wenn der **Trust Mode** (Trustmodus) auf **DSCP** eingestellt ist.

Disable Trust Mode on Interface (Trustmodus auf Schnittstelle deaktivieren) Deaktiviert den Trustmodus für den ausgewählten Port oder die LAG.

Interface (Schnittstelle) Port oder LAG, auf denen der Trustmodus deaktiviert ist.

Festlegen des Trustmodus

1. Öffnen Sie die Seite **Basic QoS Settings** (Einfache QoS-Einstellungen).
2. Wählen Sie einen **Trust Mode** (Trustmodus) aus.
3. Falls der **Trust Mode** (Trustmodus) **DSCP** lautet, aktivieren Sie die Option **Always Rewrite DSCP** (DSCP immer neu schreiben), damit DSCP-Tags entsprechend ihrer Zuweisung neu geschrieben werden.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Trustmodus wird ausgewählt und das Gerät aktualisiert.

Deaktivieren des Trustmodus für Schnittstellen

1. Öffnen Sie die Seite **Basic QoS Settings** (Einfache QoS-Einstellungen).
2. Klicken Sie auf **Show All** (Alles anzeigen), um die Seite **Basic QoS Settings Table** (Tabelle mit einfachen QoS-Einstellungen) anzuzeigen.
3. Aktivieren Sie die Option **Disable Trust Mode** (Trustmodus deaktivieren) für alle Schnittstellen, auf denen der Trustmodus aktiviert werden soll.

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

Definieren von einfachen QoS-Einstellungen mithilfe der CLI-Befehle

Tabelle 10-9. CLI-Befehle für einfache QoS-Einstellungen

CLI-Befehl	Beschreibung
`qos trust cos | dscp | tcp-udp-port`	Im globalen Kontext wird dieser Befehl zur Konfiguration des Systems für den einfachen Modus und den Truststatus verwendet.
`qos trust`	Im Kontext der Schnittstellenkonfiguration dient dieser Befehl zur Aktivierung des Truststatus der einzelnen Ports.
`qos dscp-mutation`	Wendet die DSCP-Umwandlungsmap auf einen DSCP-trusted Port des Systems an (DSCP wird an diesem Port immer neu geschrieben).

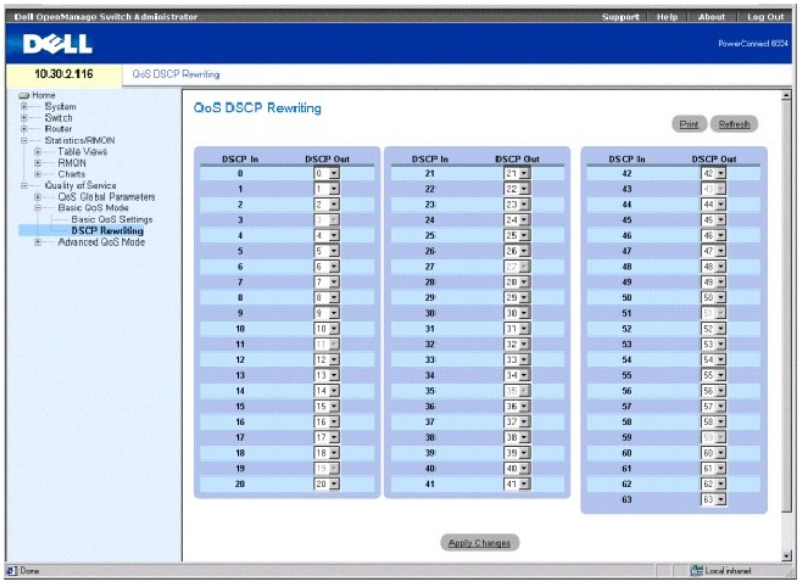
Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# qos trust dscp

Console (config)# qos dscp-mutation

Console (config)# interface ethernet g5

Console (config-if) qos trust
```

Definieren von QoS DSCP-Umschreibungseinstellungen

Auf der Seite **QoS DSCP Rewriting** (DSCP-Neuschreibung für QoS) konfigurieren Sie die Methode für das Neuschreiben von DSCP-Tags. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service→ Basic QoS Settings→ DSCP Rewriting**.

Abbildung 10-11. QoS DSCP-Umschreibung



DSCP In (DSCP eingehend) DSCP-Tag eines eingehenden Pakets.

DSCP Out (DSCP ausgehend) DSCP-Tag von ausgehenden Paketen.

Konfigurieren von DSCP-Neuschreibung

1. Öffnen Sie die Seite **QoS DSCP Rewriting** (QoS DSCP-Neuschreibung).
2. Wählen Sie für jeden der **DSCP In**-Tags einen **DSCP Out**-Wert aus der Drop-Down-Liste.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

DSCP-Neuschreibung wird konfiguriert und das Gerät aktualisiert.

Konfigurieren von DSCP-Neuschreibung mithilfe von CLI-Befehlen

Tabelle 10-10. CLI-Befehle für DSCP-Umschreibungen

CLI-Befehl	Beschreibung
`qos map dscp-mutation` *in-dscp* `to` *out-dscp*	Ändert die DSCP-Umwandlungsmap.

Im Folgenden werden CLI-Befehle für die Definition der DSCP-Umwandlungsmap anhand eines Beispiels dargestellt:

```
Console (config)# qos map dscp-mutation 1 2 4 5 6 to 63
```

Konfigurieren des erweiterten QoS-Modus

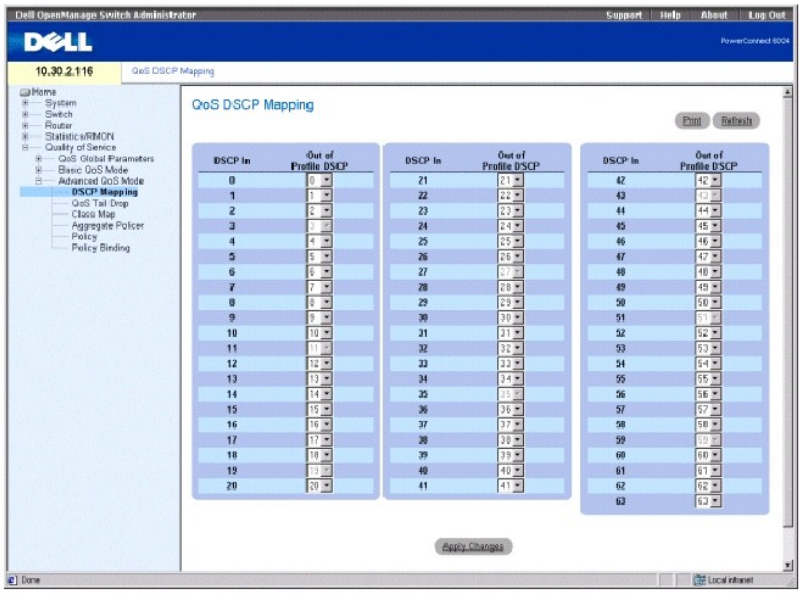
Die Seite **Advanced QoS Mode** (Erweiterter QoS-Modus) enthält Verknüpfungen zu QoS-Seiten für die Konfiguration erweiterter Einstellungen. Um die Seite zu

öffnen, klicken Sie in der Strukturansicht auf **Quality of Service**→ **Advanced QoS Mode**.

Definieren von QoS DSCP-Zuordnungseinstellungen

Sobald der Datenverkehr eine benutzerdefinierte Obergrenze erreicht, können Sie auf der Seite **QoS DSCP Mapping** (QoS DSCP-Zuweisung) den DSCP-Tag konfigurieren, der anstelle des eingehenden DSCP-Tags verwendet wird. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service**→ **Advanced QoS Mode**→ **DSCP Mapping**.

Abbildung 10-12. QoS DSCP-Zuordnung



DSCP In (DSCP eingehend) DSCP-Tag eines eingehenden Pakets.

Out of Profile DSCP (Profilexternes DSCP) Legt einen neuen DSCP-Tag für den eingehenden Tag fest.

Konfigurieren der DSCP-Zuweisung

1. Öffnen Sie die Seite **QoS DSCP Mapping** (QoS DSCP-Zuweisung).
2. Wählen Sie einen Wert aus dem Drop-Down-Menü **Out of Profile DSCP** (Profilexternes DSCP).

   Dieser Wert ersetzt den Wert des **DSCP In**-Tags.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die DSCP-Zuweisung wird konfiguriert und das Gerät aktualisiert.

Konfigurieren der DSCP-Zuweisung mithilfe von CLI-Befehlen

Tabelle 10-11. CLI-Befehle für die DSCP-Zuordnung

CLI-Befehl	Beschreibung
	Modifiziert die überwachte DSCP-Map für die Kommentierung.

qos map policed-*dscp dscp-list to dscp-mark-down*

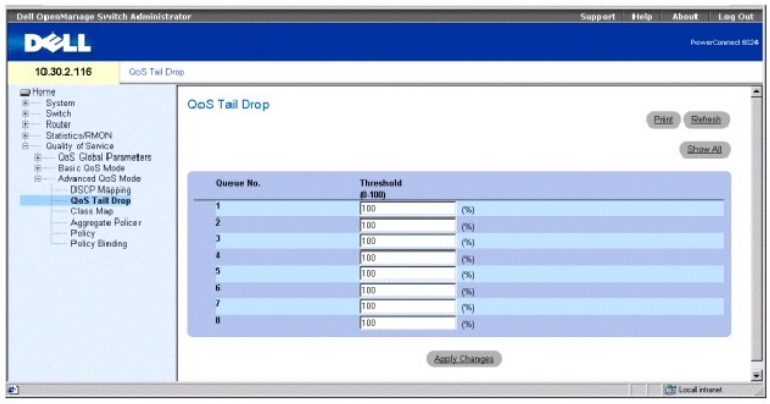
Das folgende Beispiel zeigt die CLI-Befehle für die Zuweisung der DSCP-Werte 12 und 18 zum Wert 56, wenn sich diese außerhalb des Profils befinden.

```
Console (config)# qos map policed-dscp 12 18 to 56
```

Definieren von QoS-Taildrop-Einstellungen

Taildrop (Fallenlassen der letzten Daten) tritt auf, wenn ein Paketburst einen Pufferspeicher füllt. Die letzten paar Pakete im Burst werden aufgrund des fehlenden Speicherplatzes im Pufferspeicher zurückgewiesen. Mithilfe der Seite **QoS Tail Drop** legen Sie die Taildrop-Einstellungen für alle Warteschlangen fest. Klicken Sie zum Öffnen der Seite **QoS-Taildrop** in der Strukturansicht auf **Quality of Service→ Advanced QoS Mode→ QoS Tail Drop**.

Abbildung 10-13. QoS-Taildrop



Queue No. (Warteschlangennummer) Gibt die Warteschlange an, für die die Taildrop-Einstellungen gelten.

Threshold (1-100) (Schwellenwert) Der Prozentsatz des Taildrop-Schwellenwerts für die Warteschlange. Das Paket bezieht sich auf diesen Schwellenwert. Bei seiner Überschreitung werden Pakete solange zurückgewiesen, bis der Schwellenwert wieder unterschritten wird.

Einstellen eines Taildrop-Schwellenwerts

1. Öffnen Sie die Seite **QoS Tail Drop**.
2. Wählen Sie einen Schwellenwert für jede Warteschlange aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Taildrop-Schwellenwert wird konfiguriert und das Gerät aktualisiert.

Einstellen der Taildrop-Parameter für eine Schnittstelle:

1. Öffnen Sie die Seite **QoS Tail Drop**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **Tail Drop Table** (Taildrop-Tabelle) anzuzeigen.
3. Wählen Sie einen Status für jede Schnittstelle aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).
5. Der Taildrop-Status wird für die Schnittstellen definiert.

Festlegen von QoS-Taildrop-Einstellungen mithilfe der CLI-Befehle

Tabelle 10-12. CLI-Befehle für Taildrop-Einstellungen

CLI-Befehl	Beschreibung
`qos wrr-queue threshold` *queue-id threshold-percentage*	Weist Taildrop-Schwellenwerte zu.

Im Folgenden werden die CLI-Befehle für die Definition von Taildrop-Einstellungen anhand eines Beispiels dargestellt:

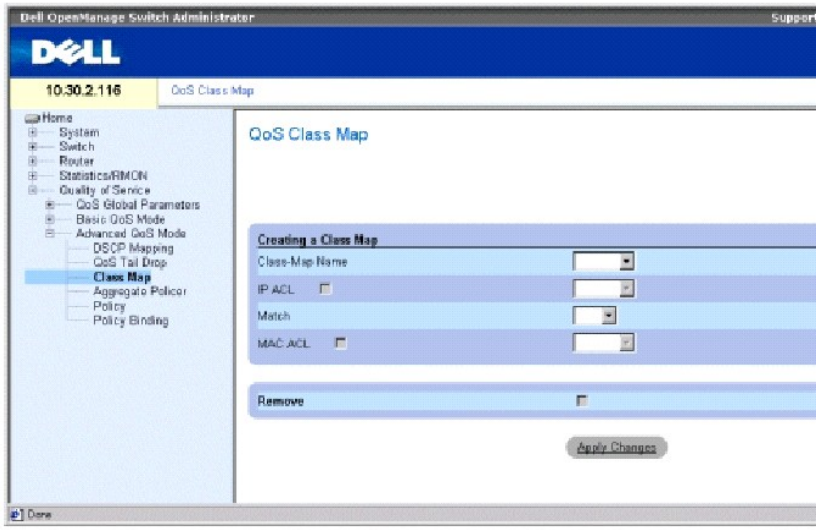
```
Console (config)# qos wrr-queue threshold 8 80
```

Definieren von QoS-Klassenmaps

Eine IP-ACL und/oder eine MAC-ACL enthalten eine Klassenmap. Klassenmaps werden für die Übereinstimmung mit Paketkriterien konfiguriert und mit Paketen auf der Grundlage einer ersten Übereinstimmung verglichen. So werden beispielsweise der Klassenmap A Pakete nur auf der Basis einer IP-basierten ACL oder einer MAC-basierten ACL zugewiesen. Die Klassenmap B wird Paketen sowohl auf der Basis einer IP-basierten ACL als auch einer MAC-basierten ACL zugewiesen.

Auf der Seite **QoS-Klassenmaps** können Sie die Zuweisung und Bearbeitung von Klassenmaps aktivieren. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service**→ **Advanced QoS Mode**→ Class Map.

Abbildung 10-14. QoS-Klassenmaps



Class-Map Name (Name der Klassenmap) Der benutzerdefinierte Name der Klassenmap.

IP ACL Die IP-ACL aus der IP-Zugriffssteuerungsliste (ACL). Weitere Informationen über das Definieren von IP-basierten ACLs finden Sie unter Definieren von IP-basierten ACLs".

Match (Übereinstimmung) Kriterien für den Vergleich von IP-Adressen und/oder MAC-Adressen mit einer Adresse von ACL. Die möglichen Werte sind:

And (Und) Sowohl die MAC-basierte als auch die IP-basierte ACL muss mit einem Paket übereinstimmen.

Or (Oder) Es muss entweder die MAC-basierte ACL oder die IP-basierte ACL mit einem Paket übereinstimmen.

MAC ACL Die MAC-ACL aus der MAC-Zugriffssteuerungsliste. Weitere Informationen über das Definieren von MAC-basierten ACLs finden Sie unter "Definieren von MAC-basierten ACLs".

Remove (Entfernen) Wenn diese Option markiert ist, wird die Klassenmap aus der Klassenmap-Tabelle entfernt.

Hinzufügen einer Klassenmap

1. Öffnen Sie die Seite **QoS Class Map** (QoS-Klassenmap).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add a Class-Map** (Hinzufügen einer Klassenmap) anzuzeigen.
3. Geben Sie in das Feld **Class-Map Name** einen Namen für die Klassenmap ein.
4. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine IP-ACL mit der Klassenmap zu verknüpfen, aktivieren Sie das Kontrollkästchen **IP ACL**, und wählen Sie eine IP-ACL aus dem Drop-Down-Menü aus.
   - Um eine MAC-ACL mit der Klassenmap zu verknüpfen, aktivieren Sie das Kontrollkästchen **MAC ACL**, und wählen Sie eine MAC-ACL aus dem Drop-Down-Menü aus.
5. Wählen Sie entweder **And** (Und) oder **Or** (Oder) aus der Drop-Down-Menü **Match** (Übereinstimmung) aus, wenn sowohl das Kontrollkästchen **IP ACL** als auch das Kontrollkästchen **MAC ACL** markiert sind.
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Klassenmap wird erstellt und das Gerät aktualisiert.

Bearbeiten einer Klassenmap

1. Öffnen Sie die Seite **QoS Class Map** (QoS-Klassenmap).
2. Wählen Sie eine Klassenmap aus dem Drop-Down-Menü **Class-Map Name** aus.
3. Bearbeiten Sie die restlichen Felder auf der Seite nach Bedarf.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).
5. Die Klassenmap wird bearbeitet und das Gerät aktualisiert.

Löschen einer Klassenmap

1. Öffnen Sie die Seite **QoS Class Map** (QoS-Klassenmap).
2. Wählen Sie eine Klassenmap aus dem Drop-Down-Menü **Class-Map Name** aus.
3. Klicken Sie das Kontrollkästchen **Remove** (Entfernen) an.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Klassenmap wird gelöscht und das Gerät aktualisiert.

Anzeigen der Klassenmap-Tabelle

1. Öffnen Sie die Seite **QoS Class Map** (QoS-Klassenmap).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **Class Map Table** (Klassenmap-Tabelle) anzuzeigen.

Definieren von QoS-Klassenmaps mithilfe der CLI-Befehle

Tabelle 10-13. CLI-Befehle für QoS-Klassenmap

CLI-Befehl	Beschreibung

`class-map class-map- name [match-all | match-any]`	Erstellt eine Klassenmap und startet den Klassenmap-Konfigurationsmodus.
`match access-group acl- name`	Definiert das Vergleichskriterium, nach dem Datenverkehr klassifiziert wird. Nur im Klassenmap-Konfigurationsmodus aktiv.
`show class-map [class- map-name]`	Zeigt alle Klassenmaps an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# class-map class1 match-all

Console (config-cmap)# match access-group dell

Console (config-cmap)# exit

Console (config)# exit

Console> show class-map class1

Class Map match-all class1 (id4)
```

Definieren von QoS-Sammelüberwachungsfunktionen

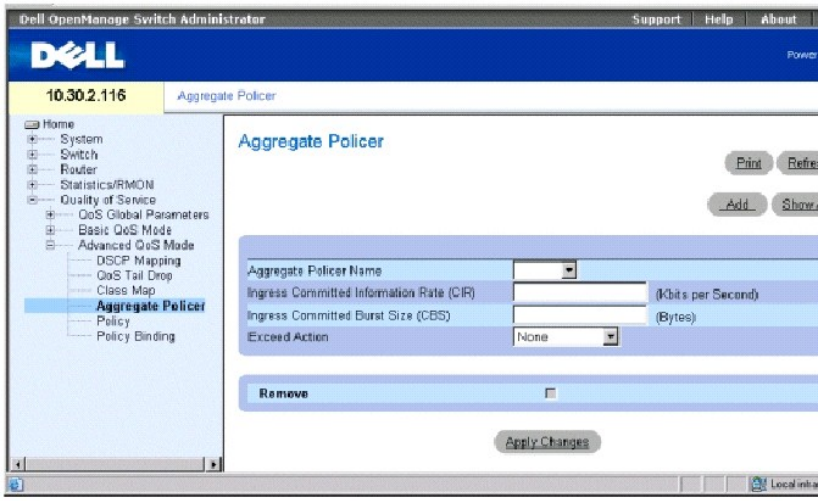
Nach der Klassifizierung eines Pakets beginnt der Überwachungsprozess. Eine Überwachungsfunktion legt die Bandbreitenobergrenze für eingehenden Datenverkehr innerhalb des klassifizierten Flusses fest und definiert Aktionen für Pakete, die die Obergrenze überschreiten. Zu diesen Aktionen gehören die Weiterleitung von Paketen, die Zurückweisung von Paketen oder das Kommentieren von Paketen mit einem neuen DSCP-Wert.

Ihr Switch unterstützt flussbasierte und gebündelte Überwachungsfunktionen.

Sammelüberwachungsfunktionen legen Grenzwerte für Flussgruppen fest. Eine Sammelüberwachungsfunktion lässt sich nicht löschen, falls diese in einer Richtlinienmap verwendet wird. Löschen Sie zuerst die Sammelüberwachungsfunktion aus allen Richtlinienmaps mit dem Befehl **no police aggregate**, bevor Sie den Befehl **no QoS aggregate-policer** verwenden.

Geben Sie auf der Seite **Sammelüberwachungsfunktion** die Bandbreitenobergrenzen ein und definieren Sie die Aktionen für Pakete, die den Anforderungen nicht entsprechen. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service→ Advanced QoS Mode→ Aggregate Policer**.

Abbildung 10-15. QoS-Sammelüberwachungsfunktion



Aggregate Policer Name (Name der Sammelüberwachungsfunktion) Gibt den Namen der Sammelüberwachungsfunktion an.

Ingress Committed Information Rate (CIR) (Garantierte Datenrate, eingehend) CIR in Bits pro Sekunde.

Ingress Committed Burst Size (CBS) (garantierte Spitzenrate, eingehend) CBS in Bytes pro Sekunde.

Exceed Action (Überschreitungsaktion) Die Aktion, die eingehenden Informationen zugeordnet wird, überschreitet die Obergrenzen im Datenverkehr. Die möglichen Werte sind:

Drop (Zurückweisen) Pakete, die die Obergrenze überschreiten, gehen verloren.

Remark DSCP (Kommentierter DSCP) Paket, die die Obergrenzen überschreiten, werden mit einem markierten/kommentierten DSCP-Wert weitergeleitet.

None (Keine) Pakete, die die Obergrenzen überschreiten, werden weitergeleitet.

Remove (Entfernen) Wenn diese Option markiert ist, wird die Sammelüberwachungsfunktion aus der Tabelle der Sammelüberwachungsfunktionen entfernt.

Hinzufügen einer Sammelüberwachungsfunktion

1. Öffnen Sie die Seite QoS-**Sammelüberwachungsfunktion**.
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add Aggregate Policer** (Sammelüberwachungsfunktion hinzufügen) anzuzeigen.
3. Füllen Sie die Felder in dem Dialogfeld aus und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Sammelüberwachungsfunktion wird erstellt und das Gerät aktualisiert.

Löschen einer Sammelüberwachungsfunktion

1. Öffnen Sie die Seite QoS-**Sammelüberwachungsfunktion**.
2. Wählen Sie aus dem Drop-Down-Menü eine Sammelüberwachungsfunktion aus.
3. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen), und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Sammelüberwachungsfunktion wird gelöscht und das Gerät aktualisiert.

Bearbeiten einer Sammelüberwachungsfunktion

1. Öffnen Sie die Seite QoS-**Sammelüberwachungsfunktion**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **Aggregate Policer Table** (Tabelle mit Sammelüberwachungsfunktionen) anzuzeigen.
3. Bearbeiten Sie in der Tabelle die Informationen der gewünschten Sammelüberwachungsfunktionen.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Definieren von Sammelüberwachungsfunktionen mithilfe von CLI-Befehlen

Tabelle 10-14. CLI-Befehle für die Sammelüberwachungsfunktion

CLI-Befehl	Beschreibung
qos aggregate-policer *aggregate-policer-name committed-rate-bps excess-burst-byte exceed-action* {drop | policed-dscp-transmit}	Definiert die Überwachungsparameter, die auf mehrere Datenverkehrsklassen mit derselben Richtlinienmap angewendet werden können.
show qos aggregate police [*aggregate-policer-name*]	Zeigt den Parameter für die Sammelüberwachungsfunktion an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console# qos aggregate policer policer1 124000 96000 exceed-action drop
```

```
Console> show qos aggregate police policer1
```

```
aggregate-policer policer1 96000 4800 exceed-action drop
```

```
not used by any policy map
```

Definieren von Richtlinien

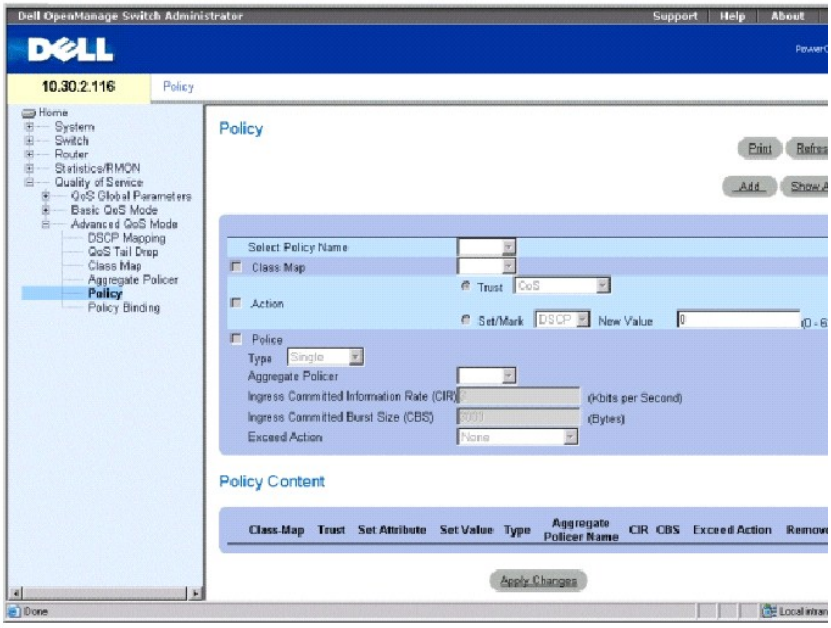
Eine Richtlinie ist eine Klassensammlung, wobei jede eine Kombination aus einer Klassenmap und einer QoS-Aktion ist, die auf übereinstimmenden Datenverkehr anzuwenden ist. Klassen werden gemäß dem Prinzip der ersten Übereinstimmung innerhalb einer Richtlinie angewendet.

Vor dem Konfigurieren von Richtlinien für Klassen, deren Übereinstimmungskriterien in einer Klassenmap definiert sind, müssen Sie eine Klassenmap festlegen oder den Namen der Richtlinienmap angeben, die erstellt, hinzugefügt oder bearbeitet werden soll. Klassenrichtlinien lassen sich nur in einer Richtlinienmap konfigurieren, falls die Klassen über definierte Übereinstimmungskriterien verfügen.

Es ist möglich, eine Sammelüberwachungsfunktion auf mehrere Klassen innerhalb derselben Richtlinienmap anzuwenden, jedoch nicht über verschiedene Richtlinienmaps hinweg. Legen Sie eine Sammelüberwachungsfunktion fest, falls die Überwachungsfunktion für mehrere Klassen freigegeben ist. Überwachungsfunktionen an einem Port können nicht für andere Überwachungsfunktionen in einem anderen Gerät freigegeben werden. Datenverkehr aus zwei unterschiedlichen Ports lässt sich für Überwachungszwecke zusammenfassen.

Um die Seite **QoS-Richtlinie**" zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service**→ **Advanced QoS Mode**→ **Policy**.

Abbildung 10-16. QoS-Richtlinie



Select Policy Name (Richtliniennamen auswählen) Wählt einen Richtliniennamen aus.

Class Map (Klassenmap) Wählt eine Klassenmap für eine Klasse aus.

Action (Aktion) Optionale Aktion für die Klasse. Die möglichen Werte sind:

Trust Aktiviert den Trust-Modus für die Klasse. Dieser Befehl dient der Unterscheidung des QoS-Trustverhaltens für den jeweiligen Datenverkehr. Wenn einem bestimmten Typ vertraut wird, ordnet der QoS-Mechanismus ein Paket einer Warteschlange mithilfe des empfangenen oder Standardwerts und der entsprechenden Map zu, entsprechend der Definition auf der Seite **QoS Global Parameters** (Globale QoS-Parameter). Durch Zuordnung von Trust ist es möglich, nur eingehendem Datenverkehr mit bestimmten DSCP-Werten zu vertrauen.

Set / Mark (Festlegen/Markieren) Konfiguriert den Trust manuell.

New Value (Neuer Wert) Wert für die ausgewählte Methode **Set / Mark** (Festlegen/Markieren).

Police Type (Überwachungsfunktionstyp) Typ der Überwachungsfunktion für die Klasse. Die möglichen Werte sind:

Aggregate (Sammel-) Konfiguriert die Klasse für die Verwendung einer konfigurierten Sammelüberwachungsfunktion, die aus dem Drop-Down-Menü ausgewählt wird. Eine Sammelüberwachungsfunktion wird definiert, falls die Überwachungsfunktion für mehrere Klassen freigegeben ist. Datenverkehr aus zwei unterschiedlichen Ports lässt sich für Überwachungszwecke konfigurieren. Es ist möglich, eine Sammelüberwachungsfunktion auf mehrere Klassen innerhalb derselben Richtlinienmap anzuwenden, jedoch nicht über verschiedene Richtlinienmaps hinweg.

Single (Einzeln) Konfiguriert die Klasse für die Verwendung manuell konfigurierter Informationsraten und Überschreitungsaktionen.

Aggregate Policer (Sammelüberwachungsfunktion) Benutzerdefinierte Sammelüberwachungsfunktionen.

Ingress Committed Information Rate (CIR) (Garantierte Datenrate, eingehend) CIR in Bits pro Sekunde. Dieses Feld ist nur relevant, wenn der Wert für **Police** (Überwachungsfunktion) **Single** (Einzeln) lautet.

Ingress Committed Burst Size (CBS) (garantierte Spitzenrate, eingehend) CBS in Bytes pro Sekunde. Dieses Feld ist nur relevant, wenn der Wert für **Police** (Überwachungsfunktion) **Single** (Einzeln) lautet.

Exceed Action (Überschreitungsaktion) Die Aktion, die eingehenden Paketen zugeordnet wird, die die garantierte Datenrate (CIR) überschreiten. Dieses Feld ist nur relevant, wenn der Wert für **Police** (Überwachungsfunktion) **Single** (Einzeln) lautet. Die möglichen Werte sind:

Drop (Zurückweisen) Weist Pakete zurück, die den definierten CIR-Wert überschreiten.

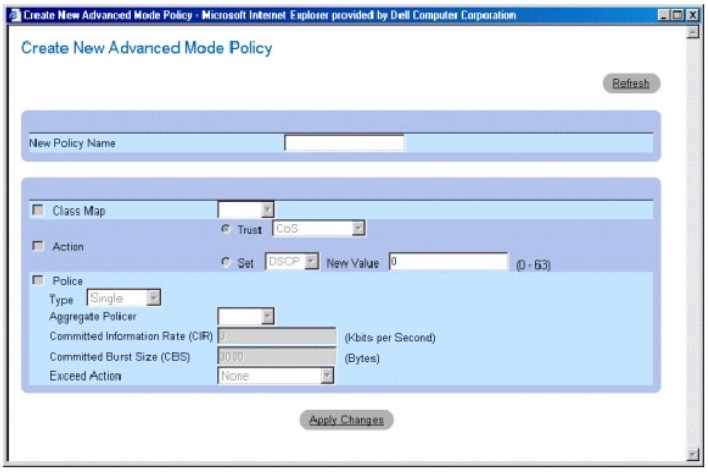
Remark DSCP (DSCP markieren) Kommentiert die DSCP-Werte von Paketen, die den definierten CIR-Wert überschreiten.

None (Keine) Leitet Pakete weiter, die den definierten CIR-Wert überschreiten.

Hinzufügen einer Richtlinie und ihrer ersten Klasse

1. Öffnen Sie die Seite QoS-**Richtlinie**.
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Create New Advanced Mode Policy** (Neue Richtlinie für den erweiterten Modus erstellen) zu öffnen.

Abbildung 10-17. Erstellen einer neuen Richtlinie für den erweiterten Modus



3. Geben Sie im Feld **New Policy Name** (Neuer Richtlinienname) einen Namen für die Richtlinie ein.
4. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine Klassenmap für die Klasse zu konfigurieren, klicken Sie auf **Class Map** (Klassenmap), und wählen Sie eine Klassenmap aus dem Drop-Down-Menü aus.
   - Um eine Trustaktion für die Klasse zu konfigurieren, klicken Sie auf **Action** (Aktion), dann auf **Trust** (Vertrauen), und wählen Sie eine Trustmethode aus dem Drop-Down-Menü aus.
   - Um Set/Mark-Aktionen zu konfigurieren, klicken Sie auf **Set** (Festlegen), wählen Sie eine Methode aus dem Drop-Down-Menü aus, und geben Sie einen Wert im Feld **New Value** (Neuer Wert) ein.
5. Wenn Sie die Überwachung für die Klasse konfigurieren möchten, klicken Sie auf **Police** (Überwachung), und wählen Sie eine Überwachungsfunktion aus dem Drop-Down-Menü.
   - Wählen Sie bei Sammelüberwachungsfunktionen eine Sammelüberwachungsfunktion aus dem Drop-Down-Menü **Aggregate Policer**.
   - Füllen Sie bei einzelnen Überwachungsfunktionen die Informationen in den Feldern **Committed Information Rate (CIR)** (Garantierte Datenrate), **Committed Burst Size (CBS)** (Garantierte Spitzenrate) und **Exceed Action** (Überschreitungsaktion) aus.
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Richtlinie und ihre erste Klasse werden erstellt und das Gerät aktualisiert.

Hinzufügen einer Klasse

1. Öffnen Sie die Seite QoS **Richtlinie**.
2. Wählen Sie aus dem Drop-Down-Menü eine Richtlinie aus.
3. Bearbeiten Sie die Informationen in den Feldern auf der Seite, und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Klasse wird der Richtlinie hinzugefügt und das Gerät aktualisiert.

Löschen von Richtlinien

1. Öffnen Sie die Seite QoS-**Richtlinie**.
2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **Policy Table** (Richtlinientabelle) anzuzeigen.
3. Klicken Sie für jede der zu löschenden Richtlinien auf **Remove** (Entfernen) und anschließend auf **Apply Changes** (Änderungen übernehmen).

Die Richtlinien werden aus dem System gelöscht und das Gerät aktualisiert.

Definieren von Richtlinien mithilfe von CLI-Befehlen

Tabelle 10-15. CLI-Befehle für die Richtlinie

CLI-Befehl	Beschreibung
`policy-map` *`policy-map-name`*	Erstellt eine Richtlinienmap und startet den Richtlinienmap-Konfigurationsmodus.
`class` *`class-map-name`* `[access-group` *`acl-name`*`]`	Definiert die Datenverkehrsklassifizierung, und startet den Richtlinienmap-Klassenkonfigurationsmodus.
`trust [cos | dscp | tcp-udp-port]`	Konfiguriert den Truststatus, wodurch der Wert ausgewählt wird, den QoS als Quelle des internen DSCP-Werts verwendet.
`set {dscp` *`new-dscp`* `| queue` *`queue-id`* `| cos` *`new-cos`*`}`	Legt neue Werte im IP-Paket fest. Anmerkung: Dieser Befehl und der Trustbefehl heben sich gegenseitig auf.
`police` *`committed-rate-bps committed-burst-byte`* `[exceed-action {drop | policed-dscp-transmit}]`	Legt eine einzelne Überwachungsfunktion für den klassifizierten Datenverkehr fest.
`qos aggregate-policer` *`aggregate-policer-name committed-rate-bps excess-burst-byte`* `exceed-action {drop | policed-dscp-transmit}`	Definiert die Überwachungsparameter, die auf mehrere Datenverkehrsklassen mit derselben Richtlinienmap angewendet werden können.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

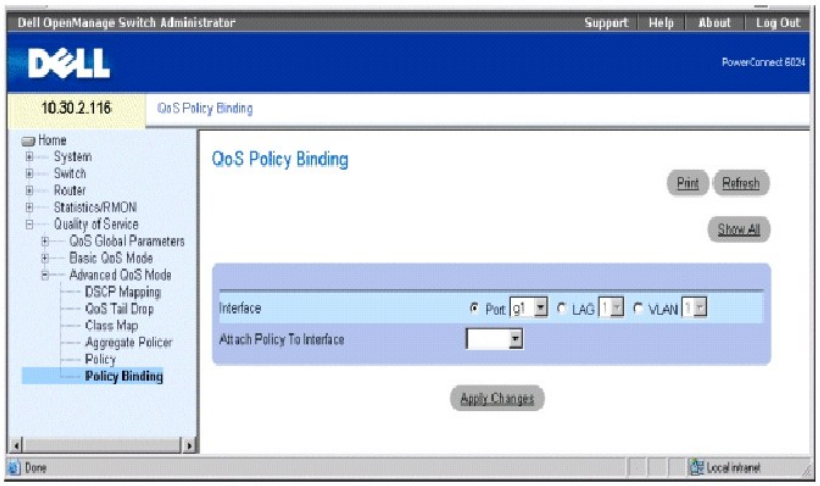
```
Console (config)# policy map policy1

Console (config-pmap)# class class1 access-group dell

Console (config-pmap)# trust cos

Console (config-pmap)# set dscp 56

Console (config-pmap)# police 124000 96000 exceed-action drop
```

```
Console (config-pmap)# exit


Console (config)# qos aggregate-policer policer1 124000 96000 exceed-action drop
```

Anwenden von Richtlinien auf Schnittstellen

Auf der Seite **QoS-Richtlinienbindung** können Sie Richtlinien an Schnittstellen implementieren. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Quality of Service→ Advanced QoS Mode→ Policy Binding**.

Abbildung 10-18. QoS-Richtlinienbindung



Interface (Schnittstelle) Wählt eine Schnittstelle aus.

Attach Policy to Interface (Richtlinie mit Schnittstelle verknüpfen) Die an der Schnittstelle implementierte Richtlinie.

ANMERKUNG: Eine Richtlinienmap, die einen set"- oder trust"-Klassenkonfigurationsbefehl für Richtlinienmaps enthält, oder die über eine ACL-Klassifizierung verfügt, die nicht an eine ausgehende Schnittstelle angehängt werden kann.

Verknüpfen einer Richtlinie mit einer Schnittstelle

1. Öffnen Sie die Seite **QoS Policy Binding** (QoS-Richtlinienbindung).
2. Wählen Sie einen Schnittstellentyp aus.

   Nur eine Richtlinienmap pro Schnittstelle pro Richtung wird unterstützt. Jedoch kann dieselbe Richtlinienmap auf mehrere Schnittstellen und Richtungen angewendet werden.
3. Wählen Sie aus dem entsprechenden Drop-Down-Menü den Port, die LAG oder die VLAN-Nummer aus.
4. Wählen Sie aus dem Drop-Down-Menü **Attach Policy to Interface** (Richtlinie mit Schnittstelle verknüpfen) eine Richtlinie aus.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die ausgewählte Richtlinie wird an der ausgewählten Schnittstelle implementiert und das Gerät aktualisiert.

Entfernen von Richtlinien von Schnittstellen

1. Öffnen Sie die Seite **QoS Policy Binding** (QoS-Richtlinienbindung).

2. Klicken Sie auf **Show All** (Alle anzeigen), um die Seite **PTI-Kennungstabelle** anzuzeigen.
3. Klicken Sie für jede der Schnittstellen, aus denen Sie Richtlinien entfernen möchten, auf **Remove** (Entfernen), und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Richtlinie wird vom Port entfernt, verbleibt jedoch weiterhin im System.

Anwenden von Richtlinien auf Schnittstellen mithilfe von CLI-Befehlen

Tabelle 10-16. CLI-Befehle für Richtlinien auf Schnittstellen

CLI-Befehl	Beschreibung
`service-policy input` *`policy-map-name`*	Wendet eine Richtlinienmap auf die Eingabe oder Ausgabe einer bestimmten Schnittstelle an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config-if)# service-policy input policy1
```

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Konfigurieren des Switch

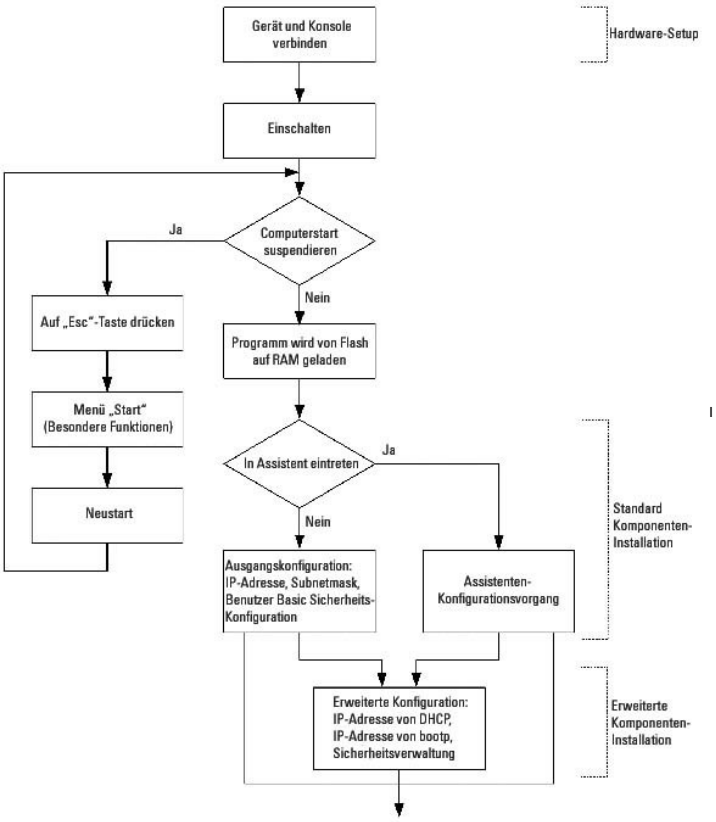
Dell PowerConnect 6024/6024F Systeme

Dieser Abschnitt beschreibt die Ausgangsgerätekonfiguration.

Wenn alle externen Verbindungen bestehen, müssen Sie einen Terminal an das Gerät anschließen, um die Startsequenz und andere Vorgänge überwachen zu können. Die Installationsreihenfolge und das Konfigurationsverfahren werden in Abbildung 5-1 dargestellt. Bei der ursprünglichen Konfiguration wird die Standard-Gerätekonfiguration ausgeführt. Sie können auch andere Funktionen ausführen, dies führt jedoch dazu, dass das Installationsverfahren unterbrochen wird und ein Systemneustart erfolgt. Die Ausführung anderer Funktionen wird weiter unten in diesem Abschnitt beschrieben.

HINWEIS: Bevor Sie fortfahren, lesen Sie bitte die Versionshinweise für dieses Produkt. Die Versionshinweise stehen unter **support.dell.com** zum Herunterladen zur Verfügung.

Abbildung 5-1. Installations- und Konfigurationsablauf



Allgemeine Informationen zur Konfiguration

Ihr Switch verfügt über vordefinierte Funktionen und Setup-Konfiguration.

Automatische Verbindungsaushandlung (Auto-Negotiation)

Die automatische Verbindungseinstellung ermöglicht es einem Gerät, einem anderen Gerät, das ein gemeinsames Punkt-zu-Punkt-Verbindungssegment verwendet, Betriebsmodi mitzuteilen und mit diesem Informationen auszutauschen. Dadurch werden beide Geräte automatisch konfiguriert, was eine bessere Ausnutzung ihrer Merkmale und Fähigkeiten ermöglicht.

Die automatische Verbindungseinstellung findet während der Verbindungseinführung vollständig auf der physischen Ebene statt, ohne dass weitere Zugriffe auf MAC oder höhere Protokollebenen erforderlich wären. Die automatische Verbindungseinstellung ermöglicht den Ports die Ausführung der folgenden Aufgaben:

- Mitteilung ihrer Fähigkeiten
- Bestätigung des Empfangs und der Kenntnisnahme der gemeinsamen Betriebsmodi der Geräte
- Ablehnung von Betriebsmodi, die nicht von beiden Geräten gemeinsam verwendet werden können
- Konfigurieren jedes Ports für den Betriebsmodus der höchsten Ebene, der von beiden Ports unterstützt wird

Wenn ein Port des Switch an die Netzwerk-Schnittstellenkarte (NIC) einer Workstation oder eines Servers angeschlossen wird, der die automatische Verbindungseinstellung nicht unterstützt oder nicht darauf eingestellt ist, müssen sowohl dieser Port als auch die NIC manuell mithilfe der Web-Browser-Schnittstelle oder mithilfe von CLI-Befehlen auf die gleiche Geschwindigkeit und denselben Duplex-Modus eingestellt werden.

HINWEIS: Wenn die Endstelle auf der anderen Seite der Verbindung den Versuch einer automatischen Verbindungseinstellung mit einem Port unternimmt, der manuell auf Vollduplex eingestellt ist, führt die automatische Verbindungseinstellung dazu, dass die Endstelle versucht, in Halbduplex zu arbeiten. Der daraus resultierende mangelnde Abgleich kann zu erheblichen Frame-Verlusten führen, was für den Standard der automatischen Verbindungseinstellung systemimmanent ist.

Standardeinstellungen für Switchports

Die folgende Tabelle beschreibt die Standardeinstellungen des Switchports.

Tabelle 5-1. Standard-Porteinstellungen

Funktion	Standardeinstellung
Port-Geschwindigkeit und -modus	1000M Automatische Verbindungseinstellung
Port-Forwarding-Zustand	Enabled (Aktiviert)
Verhindern einer Blockade des Leitungskopfes	Ein (aktiviert)
Flow Control (Datenflusssteuerung)	Aus
Backpressure (Zurückweisung)	Aus

Nachstehend ein Beispiel für den Wechsel der Portgeschwindigkeit auf Port g1 mithilfe von CLI-Befehlen:

```
Console (config)# interface ethernet g1

Console (config-if)# speed 100
```

Nachstehend ein Beispiel für die Aktivierung der Datenflusssteuerung auf Port g1 mithilfe von CLI-Befehlen:

```
Console (config)# interface ethernet g1
```

```
Console (config-if)# flowcontrol on
```

Nachstehend ein Beispiel für die Rückstau-Aktivierung auf Port g1 mithilfe von CLI-Befehlen. Rückstau (Backpressure) funktioniert nur im Betriebsmodus 10-Mbps.

```
Console (config)# interface ethernet g1

Console (config-if)# speed 10

Console (config-if)# back-pressure
```

Konfiguration der Terminalverbindung

Für die Konfiguration Ihres Switch sind die folgenden Parameter der Terminal-Verbindung erforderlich:

- keine Parität
- ein Stopbit
- 8 Datenbits

Baudrate

Die Baudrate kann manuell auf einen der folgenden Werte eingestellt werden:

- 2400
- 4800
- 9600
- 19200
- 115.200

ANMERKUNG: Die Standard-Baudrate beträgt 115.200.

ANMERKUNG: Durch das Ausschalten des Geräts wird die Standard-Baudrate nicht wieder hergestellt, da diese ausdrücklich eingestellt werden muss.

ANMERKUNG: Die Baudraten-Einstellung der Konsole wird nicht in der Konfigurationsdatei des Switch gespeichert. Sie wird direkt im nichtflüchtigen Speicher des Switch gespeichert.

Im Folgenden eine Beispielkonfiguration für die Änderung der Standard-Baudrate mithilfe von CLI-Befehlen:

```
Console# configure

Console (config)# line console

Console (config-line)# speed 115200
```

Weitere Konfigurationsanforderungen

Für das Herunterladen der Software und für das Konfigurieren des Geräts ist Folgendes erforderlich:

- ASCII-Terminal (oder Emulation), angeschlossen an den seriellen Port (Kreuzkabel) an der Vorderseite des Geräts
- Dem Switch zugewiesene IP-Adresse für Gerätefernsteuerung über Telnet, SSH usw.

ANMERKUNG: Das Konfigurationsverfahren definiert nur einen Port.

Starten des Switch

Wenn der Strom eingeschaltet wird und der lokale Terminal bereits angeschlossen ist, durchläuft der Switch einen Einschalt-Selbsttest (POST). POST wird jedes Mal ausgeführt, wenn das Gerät initialisiert wird und überprüft die Hardware-Komponenten, um festzustellen, ob das Gerät vor dem Booten vollständig betriebsbereit ist.

Wenn ein kritisches Problem entdeckt wird, wird der Programmfluss gestoppt. Wenn POST erfolgreich ausgeführt wurde, wird ein gültiges und ausführbares Bild in das RAM geladen.

POST-Meldungen werden auf dem Terminal angezeigt und zeigen einen Erfolg oder einen Fehlschlag des Tests.

Führen Sie Folgendes durch, um den Switch zu starten:

1. Stellen Sie sicher, dass das ASCII-Kabel mit dem Terminal verbunden ist.
2. Schließen Sie die Stromversorgung des Switch an.
3. Schalten Sie den Switch ein.

Beim Hochfahren des Switch wird in der Startsequenz zuerst der verfügbare Gerätespeicher getestet, danach wird die Startsequenz fortgesetzt. Im Folgenden ein Beispiel der POST-Anzeige:

```
Boot1 Checksum Test.............................PASS

Boot2 Checksum Test.............................PASS

Flash Image Validation Test.....................PASS

Testing CPU PCI Bus Device Configuration.........PASS



BOOT Version 1.0.0.13 Date 13-Aug-2003 Time 15:28:31



Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

Das Booten dauert ca. 30 Sekunden.

Die automatische Boot-Meldung, die am Ende des Einschalt-Selbsttests erscheint (siehe die letzten Zeilen) besagt, dass beim Starten keine Probleme aufgetreten sind.

Während der Startsequenz können Sie bei Bedarf das **Startup**-Menü (Startmenü) verwenden, um besondere Verfahren auszuführen. Um in das **Startup**-Menü zu gelangen, drücken Sie innerhalb der ersten beiden Sekunden nach Erscheinen der automatischen Boot-Meldung <Esc> oder <Enter>. Weitere Informationen über das **Startup**-Menü finden Sie unter Funktion im Startup-Menü".

Wenn Sie den Systemstart nicht durch Drücken der Tasten <Esc> oder <Enter> unterbrechen, setzt das System seine Arbeit fort, indem es den Code dekomprimiert und in den Arbeitsspeicher (RAM) lädt. Der Code wird aus dem Arbeitsspeicher ausgeführt, und eine Liste mit nummerierten Systemports einschließlich Portstatus (an oder aus) wird angezeigt.

ANMERKUNG: Im Folgenden wird einen Beispielkonfiguration gezeigt. Adressen, Versionen, Datumsangaben usw. können je nach Gerät anders sein.

```
Preparing to decompress...



Decompressing SW from image-1

d04000

OK

Running from RAM...



************************************************************ ****

** Running SW Ver. 1.0.1.06 Date 15-Sep-2003 Time 17:48:07 **

************************************************************ ****



HW version is 00.01.64

Base Mac address is: 00:00:b0:16:00:00

Dram size is : 256M bytes

Dram first block size is : 235520K bytes

Dram first PTR is : 0x1800000

Dram second block size is : 1984K bytes

Dram second PTR is : 0xFE00000

Flash size is: 16M

Tuning File info. Ver: 0.2.80 Creation date: Aug 20 2003 11:20:13

PowerConnect 6024
```

```
Tapi Version: v1.1a1-P18

Core Version: v1.1a1-P18

18-May-2003 16:24:41 %INIT-I-InitCompleted: Initialization task is completed


Start the sync process between devices 0 - 1


Sync OK


18-May-2003 16:24:41 %Box-W-PS-STAT-CHNG: PS# 1 status changed - not operational

.

18-May-2003 16:24:41 %Box-I-PS-STAT-CHNG: PS# 2 status changed - operational.

18-May-2003 16:24:41 %Box-W-FAN-STAT-CHNG: FAN# 1 status changed - operational.

18-May-2003 16:24:41 %Box-I-FAN-STAT-CHNG: FAN# 2 status changed - operational.

Console> 18-May-2003 16:24:41 %DELL-I-STATUS: Der globale Status des Produkts wurde um 9:00 Uhr von

OK auf nicht-kritisch geändert

18-May-2003 16:24:42 %LINK-W-Down: g1

18-May-2003 16:24:42 %LINK-W-Down: g2
```

Nachdem der Switch erfolgreich gestartet wurde, erscheint eine System-Eingabeaufforderung (Console>), und Sie können den Switch nun mithilfe des lokalen Terminals konfigurieren. Bevor Sie mit der Konfiguration des Switch beginnen, sollten Sie sich jedoch davon vergewissern, dass auf Ihrem Gerät die neueste Software-Version installiert ist. Wenn es nicht die aktuellste Version ist, laden Sie diese herunter und installieren Sie sie. Weitere Informationen finden Sie unter Herunterladen der Software und Neustart".

Konfigurationsübersicht

Ihr Switch unterstützt einen bandexternen 10/100 Mbps-Ethernet-Management-Port (OOB), welcher direkt an das Gerät angeschlossen ist. Dieser Port unterstützt Verwaltungsanwendungen für Systemadministratoren. Der OOB-Port wird als eine IP-Schnittstelle des Systems betrachtet, und alle Verwaltungsschnittstellen sind über diesen Port verfügbar. Der OOB-Port unterstützt jedoch keinen Benutzer-Datenverkehr. Pakete von einem bandinternen Port (einem anderen Ethernet-Port als OOB) werden nicht auf den OOB-Port geswitched oder geroutet.

Vor der Erstkonfiguration des Geräts müssen die folgenden Informationen vom Netzwerkadministrator eingeholt werden:

- IP-Adresse des OOB-Ports
- IP-Teilnetzmaske für das Netzwerk
- IP-Adresse des Standard-Gateways (Next-Hop-Router) für die Konfiguration der Standard-Route

Es gibt zwei Arten von Konfiguration: Die ursprüngliche Konfiguration besteht aus Konfigurationsfunktionen mit grundlegenden Sicherheitsmerkmalen, während die erweiterte Konfiguration eine dynamische IP-Konfiguration und erweiterte Sicherheitsmerkmale umfasst.

HINWEIS: Nachdem Konfigurationsänderungen vorgenommen wurden, muss die neue Konfiguration gespeichert werden, bevor ein Neustart durchgeführt wird. Geben Sie zum Speichern der Konfiguration Folgendes ein:

```
Console# copy running-config startup-config
```

Anfängliche Konfiguration

Die Ausgangskonfiguration kann mithilfe des Installationsassistenten oder über CLI-Befehle vorgenommen werden. Der Installationsassistent wird automatisch gestartet, wenn die Gerätekonfigurationsdatei leer ist. CLI kann durch die Eingabe von [ctrl+z] aufgerufen werden.

Dieses Handbuch enthält Informationen über die Erstkonfiguration des Geräts mithilfe des Installationsassistenten. Der Installationsassistent konfiguriert die folgenden Felder:

- IP-Adresse der SNMP-Communityzeichenfolge und des SNMP-Managementsystems (optional)
- Benutzername und Kennwort
- IP-Adresse des Geräts
- Bandexterne Standard-Gateway-Adresse

Nachdem das Gerät den Einschaltselbsttest (POST) und den Bootvorgang abgeschlossen hat, werden die folgenden Informationen angezeigt:

```
Herzlich willkommen beim  Easy Setup Wizard” (benutzerdefinierter Installationsassistent) von Dell!

Der Installationsassistent führt Sie durch die Erstkonfiguration des Switches und hilft Ihnen dabei, das System schnell und einfach in Betrieb zu nehmen. Sie können, falls Sie dies wünschen, den Installationsassistenten umgehen und stattdessen den CLI-Modus aktivieren, um den Switch manuell zu konfigurieren.

Sie können den Installationsassistenten jederzeit über die Tastenkombination [Strg+Z] beenden.

Das System zeigt Ihnen eine Standardantwort an. Wenn Sie die Eingabetaste drücken, nehmen Sie die Standardeinstellungen an.

Nachdem Sie die Grundeinstellungen über den Installationsassistent vorgenommen haben, können Sie das Gerät über den bandexternen Management-Port steuern.

Möchten Sie den Installationsassistenten starten? [Y/N] Y [J/N] J
```

1. Wenn Sie [N] eingeben, wird der Installationsassistent beendet und geschlossen. Wenn des System innerhalb von 60 Sekunden keinen Antwort erhält, wird der Installationsassistent automatisch geschlossen und die CLI-Konsolen-Eingabeaufforderung wird angezeigt. Wenn Sie [Y] (J) eingeben, führt Sie der Installationsassistent durch den gesamten Prozess der Erstkonfiguration des Geräts.

ANMERKUNG: Wenn das System innerhalb von 60Sekunden keine Antwort erhält und im Netzwerk kein BootP-Server installiert ist, wird eine Adresse vom BootP-Server abgerufen.

ANMERKUNG: Sie können den Installationsassistenten jederzeit über die Tastenkombination [ctrl+z] beenden.

Schritt 1

Wenn Sie [Y] (J) eingeben, wird die folgende Meldung angezeigt:

```
Das System ist nicht standardmäßig für eine Steuerung über SNMP konfiguriert. Führen Sie die folgenden Schritte aus, um den Switch über
SNMP zu steuern (erforderlich für den Dell Netzwerk-Manager):

l Eingangskonto für SNMP Version 2 jetzt einrichten.

l SNMP-Konto Version 2 später einrichten. (Weitere Informationen über die Einrichtung eines SNMP-Kontos der Version2 finden Sie in der
Benutzerdokumentation).


Möchten Sie die SNMP-Managementschnittstelle jetzt installieren? [Y/N] Y [J/N] J
```

2. Geben Sie [N] ein, wenn Sie Schritt 2 auslassen möchten, oder geben Sie [J] ein, um den Installationsassistenten fortzusetzen. Wenn Sie [Y] (J) eingeben, wir die folgende Meldung angezeigt:

```
Für das Einrichten eines SNMP-Steuerungskontos müssen Sie die Adresse des Verwaltungssystems und die Communityzeichenfolge oder das
Kennwort festlegen, die das Verwaltungssystem verwendet, um auf den Switch zuzugreifen. Der Assistent vergibt automatisch die höchste
Zugriffsklasse [Zugriffsstufe 15] für dieses Konto. Sie können den Netzwerk-Manager von Dell oder andere Managementschnittstellen
verwenden, um diese Einstellungen später zu ändern oder um ein zusätzliches Managementsystem zu installieren. Weitere Informationen zum
Hinzufügen von Managementsystemen finden Sie in Ihrer Benutzerdokumentation.


So fügen Sie eine Management-Station hinzu:


Geben Sie bitte die zu verwendende SNMP-Communityzeichenfolge ein


Geben Sie die IP-Adresse des Managementsystems (A.B.C.D) oder eine Wildcard (0.0.0.0) ein, um die Steuerung von jeder Management-Station
aus zu ermöglichen:
```

3. Geben Sie hier Folgendes ein:
   - SNMP-Communityzeichenfolge des Benutzers, z. B. MYSETUPWIZARD”
   - IP-Adresse des Managementsystems, z. B. 0.0.0.0”.
4. Drücken Sie erneut die Eingabetaste.

Schritt 2

Das Folgende wird angezeigt:

```
Richten Sie nun Ihr anfängliches Zugangsbenutzerkonto (Stufe15) ein. Dieses Konto wird für die Anmeldung an der
Befehlszeilenschnittstelle (CLI) und am Internet verwendet. Sie können später weitere Konten einrichten und Zugriffsstufen ändern.
Weitere Informationen zum Einrichten von Benutzerkonten und zum Ändern von Zugriffsstufen finden Sie in der Benutzerdokumentation.


So richten Sie ein Benutzerkonto ein:


Geben Sie den Benutzernamen ein:


Geben Sie das Benutzerkennwort ein:


Geben Sie das Benutzerkennwort noch einmal ein:
```

5. Geben Sie hier Folgendes ein:
   - Benutzername, z. B. admin”.
   - Kennwort und Kennwortbestätigung.

ANMERKUNG: Wenn die Eingaben des ersten und des zweiten Kennworts nicht übereinstimmen, wird der Benutzer dazu aufgefordert, übereinstimmende Kennwörter einzugeben.

6. **Eingabe** drücken.

Schritt 3

7. Das Folgende wird angezeigt:

```
Als Nächstes wird eine IP-Adresse eingerichtet. Diese IP-Adresse ist auf dem OOB-Port definiert. Es ist die IP-Adresse, die Sie für den
Zugang zur Befehlszeilenschnittstelle (CLI), das Internet oder die SNMP-Schnittstelle für den Switch benötigen.

So richten Sie eine IP-Adresse ein:

Bitte geben Sie die IP-Adresse des Geräts ein (A.B.C.D):

Bitte geben Sie die IP-Teilnetzmaske (A.B.C.D oder /nn) ein:
```

8. Geben Sie die IP-Adresse und die IP-Teilnetzmaske ein, z. B. 192.168.1.100 als IP-Adresse und 255.255.255.0 als IP-Teilnetzmaske.

ANMERKUNG: Jeder Teil der IP-Adresse muss mit einer Zahl beginnen, die ungleich 0 (Null) ist. So sind die IP-Adressen 001.100.192.6 und 192.001.10.3 beispielsweise gültig.

9. **Eingabe** drücken.

Schritt 4

Das Folgende wird angezeigt:

```
Nun können Sie das Standard-Gateway einrichten. Bitte geben Sie IP-Adresse des Gateways ein, von dem aus dieses Netzwerk erreichbar ist
(z. B. 192.168.1.1):
```

10. Geben Sie das Standard-Gateway ein.
11. Drücken Sie erneut die Eingabetaste. Daraufhin werden die folgenden Informationen angezeigt (wie in den Beispielparametern beschrieben):

```
Es wurden die folgenden Konfigurationsdaten ermittelt:

SNMP-Schnittstelle = MYSETUPWIZARD@0.0.0.0

Setup Benutzerkonto = admin

Kennwort = **********

Management-IP-Adresse = 192.168.1.100 255.255.255.0

Standard-Gateway = 192.168.1.1
```

Schritt 5

Das Folgende wird angezeigt:

```
Wenn die Daten korrekt anzeigt werden, klicken Sie bitte auf (J), um die Konfiguration zu speichern und die Startup-Konfigurationsdatei
zu kopieren. Sollten die Daten nicht korrekt sein, klicken Sie bitte auf (N), um die Konfiguration zu verwerfen und den Assistenten
erneut aufzurufen: [J/N]
```

12. Geben Sie [N] ein, um den Neustart des Installationsassistenten zu übergehen, oder geben Sie [Y] (J) ein, um den Installationsassistenten zu beenden. Wenn Sie [Y] (J) eingeben, wir die folgende Meldung angezeigt:

```
Konfigurieren der SNMP-Managementschnittstelle.

Konfigurieren des Benutzerkontos.......

Konfigurieren von IP und Subnetz......

.............................

Vielen Dank, dass Sie den benutzerdefinierten Installationsassistenten von Dell verwendet haben. Sie gelangen jetzt in den CLI-Modus.
```

Schritt 6

```
Die CLI-Eingabeaufforderung wird angezeigt.
```

Das Gerät kann nun über den bereits verbundenen Konsolenport gesteuert werden. Alternativ ist auch eine Fernverwaltung über den OBB-Port möglich, der während der Erstkonfiguration definiert wurde.

Erweiterte Konfiguration

Dieser Abschnitt enthält Informationen über die dynamische Zuweisung von IP-Adressen und Sicherheitsverwaltung auf der Grundlage der AAA-Mechanismen (Authentifizierung, Authorisierung und Abrechnung).

Bei Konfiguration/Empfang von IP-Adressen über DHCP und BOOTP enthält die von diesen Servern empfangene Information die IP-Adresse und sie kann auch die Subnetzmaske und Standard-Gateway enthalten.

Abrufen einer IP-Adresse von einem DHCP-Server

Wenn die IP-Adresse mithilfe des DHCP-Protokolls abgerufen wird, arbeitet das Gerät als DHCP-Client.

Führen Sie die folgenden Schritte aus, um eine IP-Adresse von einem DHCP-Server abzurufen:

1. Wählen Sie und stellen Sie eine Verbindung irgendeines Ports mit einem DHCP-Server oder einem Subnetz, auf dem sich ein DHCP-Server befindet, her, um die IP-Adresse abzurufen.
2. Geben Sie die folgenden Befehle ein, um den ausgewählten Port zum Empfang der IP-Adresse auszuwählen. Im folgenden Beispiel beruhen die Befehle auf dem für die Konfiguration verwendeten Porttyp.
    - Zuweisen von dynamischen IP-Adressen (an einem bandinternen Port):

```
Console# configure

Console (config)# interface ethernet g1
```

```
Console (config-if)# ip address dhcp hostname <string>

Console (config-if)# exit
```

- Zuweisen von dynamischen IP-Adressen (an einem bandexternen Port)

```
Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip address dhcp hostname dell

Console (config-oob)# exit

Console (config)# exit
```

Die Schnittstelle ruft die IP-Adressen automatisch ab.

3. Geben Sie zur Überprüfung der IP-Adresse an der System-Prompt den Befehl **show ip interface** ein, wie im folgenden Beispiel gezeigt.

```
Console# show ip interface

Console# show ip interface

IP Address    I/F       Type      Directed Broadcast

------------  ------    ------    -----------------

100.1.1.1/24  vlan 1    static    disable


OOB ip interfaces


Gateway IP Address       Activity status

-----------------------  -----------------------

10.6.12.1                active


IP Address      I/F                    Type
```

```
-------------  ---------------------  ---------


10.6.12.20/24   Oob-eth 1              dhcp
```

ANMERKUNG: Sie müssen die Gerätekonfiguration nicht löschen, um eine IP-Adresse für den DHCP-Server zu empfangen.

ANMERKUNG: Beim Kopieren von Konfigurationsdateien ist die Verwendung einer Konfigurationsdatei zu vermeiden, die eine Anweisung zur DHCP-Aktivierung auf einer Schnittstelle mit Verbindung zum gleichen DHCP-Server oder einem Server mit identischer Konfiguration enthält. In diesem Fall ruft der Switch die neue Konfigurationsdatei ab und bootet von dieser. Der Switch aktiviert anschließend DHCP gemäß Anweisung in der neuen Konfigurationsdatei und erhält von DHCP die Anweisung zum erneuten Laden derselben Datei.

Empfangen einer IP-Adresse von einem BOOTP-Server

Das Standard-BOOTP-Protokoll wird unterstützt und ermöglicht dem Switch, die IP-Hostkonfiguration automatisch von jedem beliebigen Standard-BOOTP-Server im Netzwerk zu laden. In diesem Fall arbeitet das Gerät als BOOTP-Client.

Empfangen einer IP-Adresse von einem BOOTP-Server.

1. Wählen Sie und stellen Sie eine Verbindung irgendeines Ports mit einem BOOTP-Server oder einem Subnetz, auf dem sich ein solcher Server befindet, her, um die IP-Adresse abzurufen.
2. Geben Sie bei Systemeingabeaufforderung den Befehl **delete startup configuration** (Startkonfiguration löschen) ein, um die Startkonfiguration aus dem Flash-Speicher zu löschen.

   Das Gerät führt einen Neustart ohne Konfiguration aus und sendet nach 60 Sekunden BOOTP-Anfragen.

   Das Gerät ruft die IP-Adresse automatisch ab.

ANMERKUNG: Nach Beginn des Neustarts des Geräts wird der BOOTP-Prozess durch irgendeine Eingabe am ASCII-Terminal oder über eine Tastatur automatisch abgebrochen und das Gerät erhält keine IP-Adresse vom BOOTP-Server.

Das folgende Beispiel illustriert diesen Prozess:

```
Console> enable


Console# delete startup-config


Startup file was deleted


Console# reload


You haven't saved your changes. Are you sure you want to continue (y/n) [n]?


This command will reset the whole system and disconnect your current session. Do you want to continue (y/n) [n]?


*****************************************************


/* the device reboots */
```

Geben Sie zur Überprüfung der IP-Adresse den Befehl **show ip interface** ein.

Das Gerät ist nun mit einer IP-Adresse konfiguriert.

Sicherheitsmanagement und Kennwortkonfiguration

Die Systemsicherheit wird nach dem AAA-Prinzip (Authentifizierung, Autorisierung und Accounting) gehandhabt, welches die Benutzer-Zugangsberechtigungen, Zugriffsrechte und Verwaltungsmethoden regelt. AAA verwendet lokale und entfernte Benutzerdatenbanken. Die Datenverschlüsselung erfolgt mit dem SSH-Mechanismus.

Bei Lieferung ist für das System kein Standard-Kennwort konfiguriert; sämtliche Kennwörter sind benutzerdefiniert. Wenn ein benutzerdefiniertes Kennwort verlorengeht, kann ein Verfahren zur Wiederherstellung des Kennwortes im Menü **Start** aufgerufen werden. Das Verfahren kann nur auf dem lokalen Terminal ausgeführt werden und ermöglicht den einmaligen Zugriff auf das Gerät vom lokalen Terminal ohne Kennworteingabe.

Konfigurieren von Sicherheitskennwörtern

Die Sicherheitskennwörter können für die folgenden Dienste konfiguriert werden:

- Console
- Telnet
- SSH
- HTTP
- HTTPS

ANMERKUNG: Alle Kennwörter sind benutzerdefiniert.

ANMERKUNG: Bei der Erstellung eines Benutzernamens ist die Standardpriorität 1. Sie überträgt Zugriffs-, aber keine Konfigurationsrechte. Für Zugangs- und Konfigurationsrechte zum Gerät muss eine Priorität von 15" eingestellt werden. Obwohl Benutzernamen die Privilegstufe 15 ohne ein Kennwort zugewiesen werden können, wird doch empfohlen, immer ein Kennwort zuzuweisen. Wenn kein Kennwort angegeben ist, können privilegierte Benutzer auf die Web-Schnittstelle ohne Eingabe eines Kennworts zugreifen.

Konfigurieren eines anfänglichen Konsolen-Kennworts

Geben Sie zum Konfigurieren eines anfänglichen Konsolen-Kennworts 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 george
```

- Wenn Sie sich über eine Konsolen-Sitzung erstmals bei einem Gerät anmelden, geben Sie bei Aufforderung zur Kennworteingabe **george** ein.
- Wenn Sie den Modus eines Geräts auf aktiviert" abändern, geben Sie an der Kennwort-Eingabeaufforderung george ein.

Konfigurieren eines anfänglichen Telnet-Kennwortes

Zur Konfiguration eines anfänglichen Telnet-Kennwortes 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 bob
```

- Wenn Sie sich erstmals über eine Telnet-Session bei einem Gerät anmelden, geben Sie an der Kennwort-Eingabeaufforderung bob ein.
- Wenn Sie den Gerätestatus auf aktiviert" abändern, geben Sie bob ein.

Konfigurieren eines anfänglichen SSH-Kennwortes

Zur Konfiguration eines anfänglichen SSH-Kennwortes geben Sie die folgenden Befehle ein:

```
Console (config)# aaa authentication login default line

Console (config)# aaa authentication enable default line

Console (config)# line ssh

Console (config-line)# login authentication default

Console (config-line)# enable authentication default

Console (config-line)# password jones.
```

- Wenn Sie sich erstmals über eine SSH-Session bei einem Gerät anmelden, geben Sie an der Kennwort-Eingabeaufforderung jones ein.
- Wenn Sie den Gerätemodus auf aktiviert" abändern, geben Sie jones ein.

Konfigurieren eines anfänglichen HTTP-Kennwortes

Zur Konfiguration eines anfänglichen HTTP-Kennwortes geben Sie die folgenden Befehle ein:

```
Console (config)# ip http authentication local

Console (config)# username admin password user1 level 15
```

Konfigurieren eines anfänglichen HTTPS-Kennworts

Zur Konfiguration eines anfänglichen HTTPS-Kennwortes geben Sie die folgenden Befehle ein:

```
Console (config)# ip https authentication local
```

```
Console (config)# username admin password user1 level 15
```

ANMERKUNG: Immer, wenn Sie die Steuerungssoftwareanwendung auf dem Gerät aktualisieren oder neu installieren, sollten Sie ein neues Crypto-Zertifikat erstellen.

Geben Sie beim Konfigurieren die folgenden Befehle ein Mal ein, um eine Konsolen-, eine Telnet- oder eine SSH-Sitzung zwecks Verwendung einer HTTPS-Sitzung zu verwenden.

Aktivieren Sie in Ihrem Web-Browser SSL 2.0 oder höher, um den Seiteninhalt anzuzeigen.

```
Console (config)# crypto certificate generate key_generate
```

```
Console (config)# ip https server
```

Geben Sie bei der erstmaligen Aktivierung einer http- oder https-Session admin als Benutzernamen und user1 als Kennwort ein.

ANMERKUNG: Http- und Https-Dienste erfordern Zugriffslevel 15 und sind direkt mit dem Zugriff auf die Konfigurationsstufe verbunden.

Herunterladen der Software und Neustart

Software herunterladen durch XModem

Dieser Abschnitt enthält Anweisungen zum Herunterladen der Gerätesoftware (System- und Boot-Abbilder) mithilfe von XModem, einem Datenübertragungsprotokoll zum Aktualisieren von Sicherungs-Konfigurationsdateien.

So laden Sie eine Boot-Datei mithilfe von XModem herunter:

1. Geben Sie den Befehl **Console# xmodem: boot** (Konsole# xmodem: booten) ein.

   Der Switch ist bereit für den Empfang der Datei über das XModem-Protokoll und zeigt einen Text wie im nachfolgenden Beispiel an:

   ```
   Console# copy xmodem: boot
   ```

   ```
   Please download program using XMODEM.
   ```

   ```
   Console#
   ```

2. Geben Sie binnen 20 Sekunden den Pfad zur Quelldatei ein.

   Wird der Pfad nicht binnen 20 Sekunden eingegeben, hat der Befehl das Zeitlimit überschritten und wird nicht ausgeführt.

So laden Sie eine Software-Abbilddatei mithilfe von XModem herunter:

1. Geben Sie den Befehl **Console# xmodem: image** (Konsole# xmodem: Abbild) ein.

   Der Switch ist bereit für den Empfang der Datei über das XModem-Protokoll.

2. Geben Sie den Quellpfad an, um den Transferprozess zu starten.

   Das folgende Beispiel illustriert die Informationen, die angezeigt werden:

```
Console# copy xmodem: image

Please download program using XMODEM.

Console#
```

Software-Download über TFTP-Server

Dieser Abschnitt enthält Anweisungen zum Herunterladen der Switch-Software (System- und Boot-Abbilder) über einen TFTP-Server. Vor dem Herunterladen der Software muss der TFTP-Server konfiguriert werden.

Der Switch startet und läuft, wenn das Systemabbild vom Flash-Speicherbereich dekomprimiert wird, in dem eine Kopie des Systemabbilds gelagert ist. Wird ein neues Abbild heruntergeladen, so wird dieses im zweiten für die zusätzliche Kopie des Systemabbilds zugewiesenen Bereich gespeichert.

Beim nächsten Bootvorgang dekomprimiert der Switch das aktive Systemabbild und führt dieses aus, sofern nichts anderes ausgewählt wird.

So laden Sie ein Abbild über den TFTP-Server herunter:

1. Stellen Sie sicher, dass eine IP-Adresse auf einem der Geräteports konfiguriert ist und Pings an einen TFTP-Server übertragen werden können.
2. Stellen Sie sicher, dass die Datei (die DOS-Datei) vor dem Herunterladen auf dem TFTP-Server gespeichert ist.
3. Geben Sie den Befehl **Console# show version** (Konsole# Version anzeigen) ein, um zu überprüfen, welche Softwareversion derzeit auf dem Gerät ausgeführt wird.

   Das folgende Beispiel illustriert die Informationen, die angezeigt werden:

```
Console# show version
SW version 3.31.42 ( date 22-Jul-2003 time 13:42:41 )
Boot version 1.31.03 (date 01-Jun-2003 time 15:12:20 )
HW version
```

4. Geben Sie den Befehl **Console# show bootvar** (Konsole# Bootvar anzeigen) ein, um zu überprüfen, welches Systemabbild derzeit aktiv ist. Das folgende Beispiel illustriert die Informationen, die angezeigt werden:

```
Console# show bootvar
Images currently available on the Flash
Image-1 active (selected for next boot)
Image-2 not active
Console#
```

5. Geben Sie den Befehl **Console# copy tftp://{tftp address}/{file name} image** (Konsole# kopiere tftp://{tftp-Adresse}/{Dateiname} Abbild) ein, um ein neues Systemabbild auf das Gerät zu kopieren.

   Wenn das neue Abbild heruntergeladen ist, wird es in dem der zweiten Kopie des Systemabbilds zugewiesenen Bereich gespeichert (im Beispiel image-2″). Das folgende Beispiel illustriert die Informationen, die angezeigt werden:

```
Console# copy tftp://176.215.31.3/file1 image
Accessing file file1 on 176.215.31.3...
```

```
Loading file1 from
176.215.31.3: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy took 00:01:11 [hh:mm:ss]
```

Die Ausrufezeichen zeigen an, dass ein Kopierprozess abläuft. Ein Punkt zeigt an, dass eine Zeitüberschreitung beim Kopierprozess eingetreten ist. Viele Punkte hintereinander zeigen an, dass der Kopierprozess fehlgeschlagen ist.

6. Wählen Sie das Image für den nächsten Start, indem Sie den **Start**-Systembefehl eingeben. Geben Sie nach diesem Befehl den Befehl **Console# show bootvar** (Konsole# bootvar anzeigen) ein, um sicherzustellen, dass die als Parameter im Boot-Systembefehl angegebene Kopie für den nächsten Bootvorgang ausgewählt ist.

   Das folgende Beispiel illustriert die Informationen, die angezeigt werden:

```
Console# boot system image-2
Console# sh bootvar
Images currently available on the Flash
Image-1 active
Image-2 not active (selected for next boot)
```

   Wenn das Abbild für den nächsten Bootvorgang nicht durch Eingabe des Boot-Systembefehls ausgewählt wird, bootet das System vom derzeit aktiven Abbild (im Beispiel image-1").

7. Geben Sie den Befehl **reload** (neu laden) ein. Die folgende Meldung erscheint:

```
Console# reload
This command will reset the whole system and disconnect your current session. Do you want to continue (y/n) [n]?
```

8. Geben Sie **Y** (Ja) ein, um einen Neustart des Switch auszuführen.

Herunterladen des Start-Image

Das Laden eines neuen Start-Image vom TFTP-Server und dessen Programmierung im Flash aktualisiert das Start-Image. Das Boot-Abbild wird beim Einschalten des Switch geladen.

So laden Sie eine Boot-Datei über den TFTP-Server herunter:

1. Stellen Sie sicher, dass eine IP-Adresse auf einem der Geräteports konfiguriert ist und Pings an einen TFTP-Server übertragen werden können.
2. Stellen Sie sicher, dass die Datei (die **.rfb**-Datei) vor dem Herunterladen auf dem TFTP-Server gespeichert ist.
3. Geben Sie den Befehl **Console# show version** (Konsole# Version anzeigen) ein, um zu überprüfen, welche Boot-Version derzeit auf dem Gerät ausgeführt wird.

   Das folgende Beispiel illustriert die Informationen, die angezeigt werden:

```
Console# show version
SW version 3.31.42 ( date 22-Jul-2003 time 13:42:41 )
Boot version 1.31.03 (date 01-Jun-2003 time 15:12:20 )
HW version 00.00.01 (date 01-May-2003 time 12:12:20 )
```

4. Geben Sie den Befehl **Console# copy tftp://{tftp address}/{file name} boot** (Konsole# kopiere tftp://{tftp-Adresse}/{Dateiname} Boot) ein, um ein neues Boot-Abbild auf den Schalter zu kopieren.

   Das folgende Beispiel illustriert die Informationen, die angezeigt werden:

```
Console# copy tftp://176.215.31.3/6024_boot-10013.rfb
Erasing
```

```
file ...done. !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy: 393232 bytes copied in 00:00:05 [hh:mm:ss]
```

5. Geben Sie den Befehl **reload** (neu laden) ein.

   Die folgende Meldung erscheint:

```
Console# reload
This command will reset the whole system and disconnect your current session. Do you want to continue (y/n) [n]?
```

6. Geben Sie **Y** (Ja) ein, um einen Neustart des Switch auszuführen.

Beispiel für ein Konfigurationsverfahren

Dieser Abschnitt beschreibt die grundlegenden Schritte zur Einrichtung einer Remote-Netzwerkverwaltungsverbindung zum Switch. Die unterschiedlichen auf dem Switch verfügbaren Konfigurationen sowie die zugehörigen Befehle werden in diesem Abschnitt jedoch nicht behandelt.

In diesem Abschnitt wird auch das Vorgehen beim erstmaligen Zugriff auf den Switch mit den Standardkonfigurationen und -definitionen beschrieben. Wenn eine zuvor eingegebene Konfiguration Probleme verursacht, muss die Startkonfigurationsdatei d. h. die Konfiguration des Geräts beim Einschalten gelöscht und das Gerät neu gestartet werden. Weitere Informationen finden Sie unter Gerätestandardeinstellungen”.

Anforderung für die Einrichtung des Geräts

Für dieses Beispiel sind die folgenden Komponenten erforderlich:

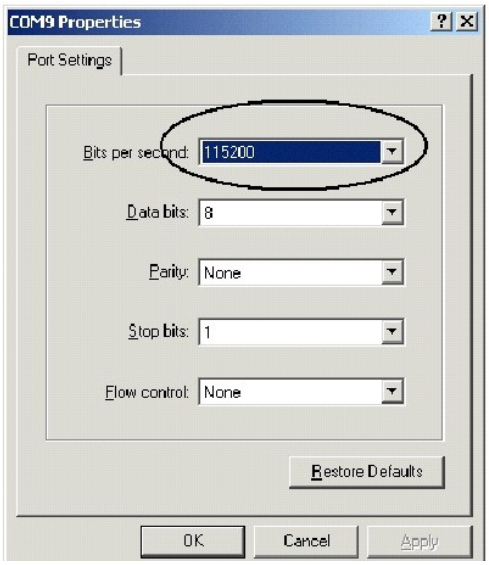
- PowerConnect 6024/6024F Switch.
- Eine Workstation, auf der die folgenden Komponenten installiert sind:
  - Netzwerkadapterkarte.
  - ASCII-Terminalanwendung (z. B. Microsoft® Windows® HyperTerminal oder Procomm Plus Terminal).
  - Ein Internet-Browser.
- Ein F2F-Nullmodemkabel.
- UTP-Kabel (Kategorie 5), gerades Kabel oder Kreuzkabel.

Erstmalige Verbindung

1. Verbinden Sie den Switch mithilfe des RS-232-Ports mit der Workstation.
2. Richten Sie den ASCII-Terminal mit den folgenden Einstellungen ein und wählen Sie den zugehörigen COM-Port aus.

   Der Beispiel-Bildschirm verwendet den HyperTerminal.

Abbildung 5-2. Eigenschaftsfenster des HyperTerminal



ANMERKUNG: 115.200 ist die Standard-Baudrate des neuen Geräts. Das Gerät kann eine andere Baudrate verwenden. Wenn der Geräteterminal bei einer Baudrate von 115.200 nicht erscheint, versuchen Sie es mit einer anderen Baudrate.

3. Schließen Sie die Workstation mithilfe eines F2F-Nullmodemkabels an den Switch an.
4. Schließen Sie das Netzkabel des Geräts an und schalten Sie das Gerät ein.

Der folgende Bildschirm wird angezeigt:

```
************************************************

*************** SYSTEM RESET ****************

************************************************


Booting...


Boot1 Checksum Test.............................PASS

Boot2 Checksum Test.............................PASS

Flash Image Validation Test.....................PASS

Testing CPU PCI Bus Configuration...............PASS


BOOT Version 1.0.0.13 Date 13-Aug-2003 Time 15:28:31
```

```
Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

An diesem Punkt können Sie bei Bedarf das **Startup**-Menü (Startmenü) aufrufen, um besondere Verfahren auszuführen. Wenn Sie das **Startup**-Menü nicht aufrufen, arbeitet das System weiter und dekomprimiert den Code in den Arbeitsspeicher. Der Code wird aus dem Arbeitsspeicher ausgeführt, und eine Liste der verfügbaren Portnummern einschließlich Portstatus (an oder aus) wird angezeigt.

ANMERKUNG: Im Folgenden wird eine Beispielkonfiguration gezeigt. Adressen, Versionen, Datumsangaben usw. können je nach Gerät anders sein.

```
Preparing to decompress...



Decompressing SW from image-1

d04000

OK

Running from RAM...



************************************************************ *******

*** Running SW Ver. 1.0.1.06 Date 15-Sep-2003 Time 17:48:07 ***

************************************************************ *******



HW version is 00.01.64

Base Mac address is: 00:00:b0:16:00:00

Dram size is : 256M bytes

Dram first block size is : 235520K bytes

Dram first PTR is : 0x1800000

Dram second block size is : 1984K bytes

Dram second PTR is : 0xFE00000

Flash size is: 16M

Tuning File info. Ver: 0.2.80 Creation date: Aug 20 2003 11:20:13
```

```
PowerConnect 6024

Tapi Version: v1.1a1-P18

Core Version: v1.1a1-P18

18-May-2003 16:24:41 %INIT-I-InitCompleted: Initialization task is completed




Start the sync process between devices 0 - 1


Sync OK


18-May-2003 16:24:41 %Box-W-PS-STAT-CHNG: PS# 1 status changed - not operational

.

18-May-2003 16:24:41 %Box-I-PS-STAT-CHNG: PS# 2 status changed - operational.

18-May-2003 16:24:41 %Box-W-FAN-STAT-CHNG: FAN# 1 status changed - operational.

18-May-2003 16:24:41 %Box-I-FAN-STAT-CHNG: FAN# 2 status changed - operational.

Console> 18-May-2003 16:24:41 %DELL-I-STATUS: The product global status has chan

ged from ok to non-critical at time 900.

18-May-2003 16:24:42 %LINK-W-Down: g1

18-May-2003 16:24:42 %LINK-W-Down: g2
```

Das Gerät ist konfigurationsbereit.

Gerätestandardeinstellungen

Wenn Sie die Standard-Geräteeinstellungen wieder herstellen möchten, geben Sie bei der Eingabeaufforderung im privilegierten Modus (#) den Befehl `delete startup-config` (Startkonfiguration löschen) ein und starten Sie das Gerät neu. Nach dem Neustart sind die Standardeinstellungen des Geräts wieder hergestellt.

```
Console>


Console> enable


Console# delete startup-config


Startup file was deleted


Console# reload


This command will reset the whole system and disconnect your current


session. Do you want to continue (y/n) [n]?


y



************************************************


*************** SYSTEM RESET ****************


************************************************


.


.


.


.
```

Aktivieren der Remote-Verwaltung

1. Geben Sie auf der Konsole den Befehl **enable** (aktivieren) ein, um den privilegierten Bildschirmmodus Privileged EXEC aufzurufen, siehe folgendes Beispiel:

```
Console> enable


Console#
```

2. Schließen Sie die Management-Station (PC) mithilfe eines CAT5-Kabels über einen der Ethernet-Ports oder über ein Netzwerk an das Gerät an.

   Bei diesem Beispiel wird Port g1 verwendet.

3. Stellen Sie (auf dem ASCII-Terminal) sicher, dass der Schnittstellenstatus ein" lautet und überprüfen Sie nach 30 Sekunden, dass der STP-Status auf Weiterleiten" (forwarding) steht, wie im unten stehenden Beispiel angegeben:

   ```
   Console#


   01-Jan-2000 01:43:03 %LINK-I-Up: Vlan 1


   01-Jan-2000 01:43:03 %LINK-I-Up: g1


   01-Jan-2000 01:43:34 %STP-I-PORTSTATUS: Port g1: STP status Forwarding
   ```

4. Geben Sie auf der Konsole den Befehl **config** (konfigurieren) ein, um den Konfigurationsmodus aufzurufen, siehe folgendes Beispiel:

   ```
   Console# config
   ```

5. Geben Sie auf der Konsole den Befehl **interface vlan** (Schnittstelle VLAN) ein, um den VLAN-Konfigurationsmodus über das Standard-VLAN 1 (tag = 1) aufzurufen, siehe folgendes Beispiel:

   ```
   Console (config)# interface vlan 1


   Console (config-if)#
   ```

6. Definieren Sie auf dem Gerät eine IP-Adresse, indem Sie eine IP-Adresse (in diesem Beispiel 50.1.1.1) jenem VLAN zuweisen, welches die an die Management-Station angeschlossene Schnittstelle enthält. Wenn die Management-Station direkt an die Schnittstelle angeschlossen ist, muss die IP-Adresse auf dem VLAN das gleiche Subnetz haben wie die Management-Station.

   ```
   Console (config)#


   Console (config-if) # ip address 50.1.1.1 225.0.0.0


   Console (config-if)#
   ```

7. Ist die Management-Station Mitglied eines Remote-Netzwerks und nicht direkt an die Schnittstelle angeschlossen, konfigurieren Sie eine statische Route.

   Die konfigurierte IP-Adresse muss zum gleichen Subnetz gehören wie eine der IP-Geräteschnittstellen. In diesem Beispiel lautet die statische Adresse 50.1.1.100.

   ```
   Console (config-if)# exit


   Console (config)# ip route 0.0.0.0.0.0.0.0 50.1.1.100


   Console (config)#
   ```

8. Senden Sie ein Ping vom Switch zur Management-Station, um sicherzustellen, dass die Konnektivität gewährleistet ist.

   Warten Sie 30 Sekunden, bis sich der Port im STP-Weiterleitungsmodus befindet, bevor Sie ein Ping an die Management-Station senden. Die IP-Adresse der Management-Station lautet (in diesem Beispiel) 50.1.1.2:

```
Console (config)#

Console (config)# exit

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

round-trip (ms) min/avg/max = 0/0/0

Console#
```

9. Definieren Sie Benutzernamen und Kennwort, um einem Remote-Benutzer (über HTTP und HTTPS) privilegierten Zugang der Stufe 15 zu ermöglichen.

In diesem Beispiel lautet der Benutzername „Dell" und das Kennwort ist „Dell", und die Zugriffsstufe beträgt 15. Es gibt die Zugriffsstufen 1-15, wobei 15 die höchste Stufe ist. 15 ist die einzige Zugriffsstufe, die den Zugang über die Web-Schnittstelle ermöglicht.

```
Console# config

Console (config)# username Dell password Dell privilege 15

Console (config)# lip 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. Definieren Sie Benutzernamen und Kennwort, um einem lokalen Benutzer den Zugang über Konsole, Telnet oder Webserver zu ermöglichen. Beispiel:

In diesem Beispiel lauten Benutzername und Kennwort „Dell" und die Zugriffsstufe ist 15.

```
Console (config)# username Dell password Dell privilege 15

Console (config)#

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 tom

Console (config-line)# exit

Console (config)# line telnet

Console (config-line)# login authentication default

Console (config-line)# enable authentication default

Console (config-line)# password bob

Console (config-line)# exit

Console (config)# line ssh

Console (config-line)# login authentication default

Console (config-line)# enable authentication default

Console (config-line)# password jones

Console (config-line)# exit
```

11. Speichern Sie die Datei **running-config** in die Datei **startup-config**.

Dadurch wird sichergestellt, dass die soeben beendete Konfiguration beim Neustart des Geräts die gleiche ist.

```
Console (config-line)# exit

Console (config)# exit

Console# copy running-config startup-config
```

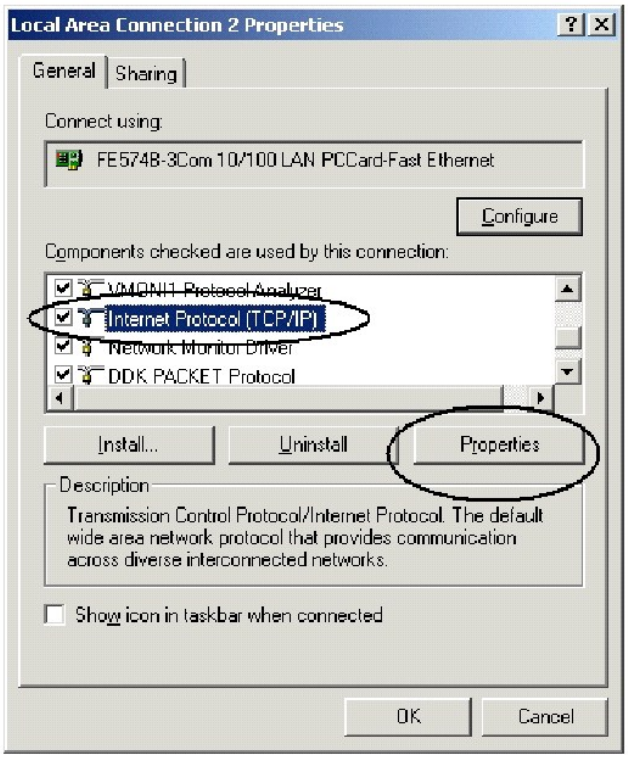
Das Gerät ist nun konfiguriert und kann über die verschiedenen Optionen, z. B. Telnet, Web-Browser u.a. verwaltet werden.

Einstellen der IP-Adresse der Management-Station

1. Klicken Sie auf der Management-Station auf **Start**→ **Settings**→ **Network and Dial-up Connections**.
2. Klicken Sie mit der rechten Maustaste auf die Netzwerkverbindung, die für Verwaltung verwendet wird, und wählen Sie **Eigenschaften** aus.

Das Fenster mit den Verbindungseigenschaften wird angezeigt.

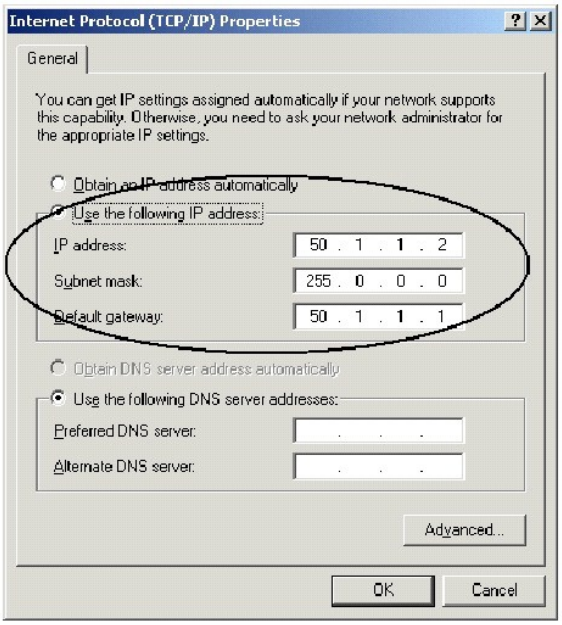
Abbildung 5-3. Fenster mit den LAN-Verbindungseigenschaften



3. Klicken Sie auf **Internet-Protokoll (TCP/IP)** und dann auf **Eigenschaften**.

Das Fenster mit den Eigenschaften von **Internet-Protokoll (TCP/IP)** wird angezeigt.

Abbildung 5-4. Fenster mit den Eigenschaften von Internet Protocol (TCP/IP)



4. Klicken Sie auf **Folgende IP-Adresse verwenden**.
5. Geben Sie die entsprechenden Adressen der Management-Station in den Feldern **IP-Adresse**, **Subnetzmaske** und **Standard-Gateway** ein.

ANMERKUNG: Wenn die Management-Station an einen Router und nicht direkt an den 6024/6024F-Switch angeschlossen ist, muss das Standard-Gateway als IP-Adresse der an die Management-Station angeschlossenen Router-Schnittstelle (welche zum 6024/6024F-Switch führt) konfiguriert werden.

Aktivieren des Telnet-Zugangs

Verwenden Sie die Windows/DOS-Befehlszeile oder eine Telnet-Anwendung, um über Telnet auf das Gerät zuzugreifen. Denken Sie daran, das richtige Kennwort einzugeben. Die Verbindung erfolgt mit der auf dem Gerät definierten IP-Adresse.

Wird der Zugang gewährt, so ist die Verwendung der Befehle die gleiche wie beim direkten Gerätemanagement:

1. Klicken Sie auf der Management-Station auf **Start**→ **Run.**
2. Geben Sie unter **Ausführen** den Befehl cmd ein und klicken Sie auf **OK**.

   Die Standard-Windows-Befehlszeilenschnittstelle wird angezeigt.
3. Geben Sie den Befehl **Telnet** und die IP-Adresse des Geräts ein, siehe folgendes Beispiel:

```
Microsoft Windows 2000 [Version 5.00.2195]

(C) Copyright 1985-2000 Microsoft Corp.

C:\>telnet 50.1.1.1

11-Aug-20 03 11:14:06 %MSCM-I-NEWTERM: New TELNET connection from 50.1.1.2

Password:***
```

```
Console> enable

Password:***

Console# show ip interface

Proxy ARP is disabled

IP Address     I/F        Type      Directed Broadcast

-------------  -------    ------    ---------------

100.1.1.1/24   vlan 1     static    disable



OOB ip interfaces

Gateway IP Address       Activity status

-----------------------  -----------------------

10.6.12.1                active



IP Address               I/F                    Type

-----------------------  ---------------------  ---------

10.6.12.20/24            Oob-eth 1              dhcp
```

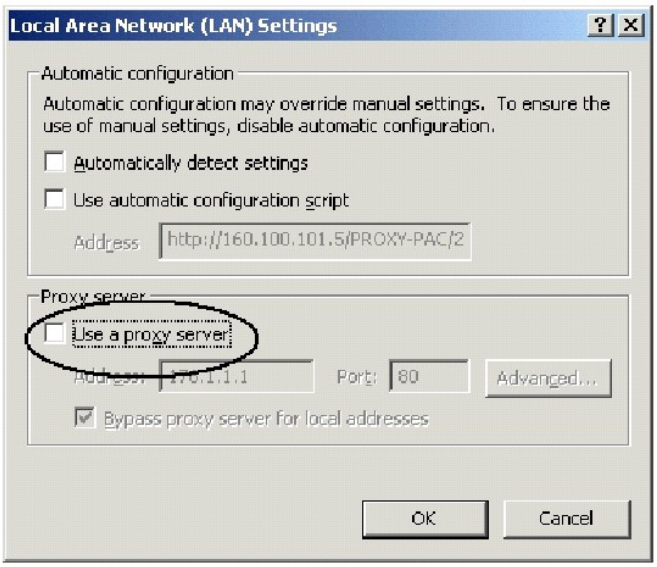
Le commutateur indique l'état de la session Telnet :

```
Console> 01-Jan-2000 02:39:04 %MSCM-I-NEWTERM: New TELNET connection from 50.1.1.2

01Jan-2000 02:39:11 %MSCM-I-TERMTERMINATED: TELNET connection from 50.1.1.2 terminated
```

Aktivieren des Web-Zugangs (HTTP-Server)

1. Zur Vermeidung von Problemen bei der Nutzung eines HTTP-Proxy-Servers können Sie die Proxy-Einstellung im Browser deaktivieren (d. h. die Markierung des entsprechenden Kontrollkästchens löschen).
    a. Klicken Sie im Microsoft Internet Explorer auf **Extras→ Internetoptionen**.
    b. Klicken Sie auf die Registerkarte **Verbindungen** und dann auf **LAN-Einstellungen**, um das Fenster **Einstellungen von Local Area Network (LAN)** aufzurufen.
    c. Stellen Sie sicher, dass das Kontrollkästchen **Proxy-Server verwenden** nicht aktiviert ist, und klicken Sie dann auf **OK**.

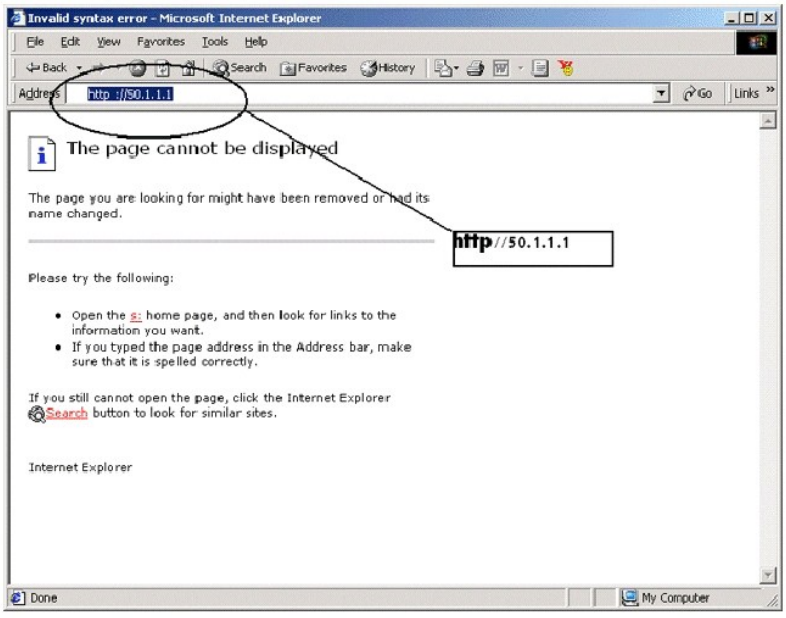
Abbildung 5-5. Fenster der LAN-Einstellungen



d. Klicken Sie auf **OK**, um das Fenster **Internetoptionen** zu schließen.

2. Geben Sie im Browser-Fenster die zuvor konfigurierte IP-Adresse des Geräts ein (mit oder ohne das http://-Präfix).

Abbildung 5-6. Anmelden am Internet



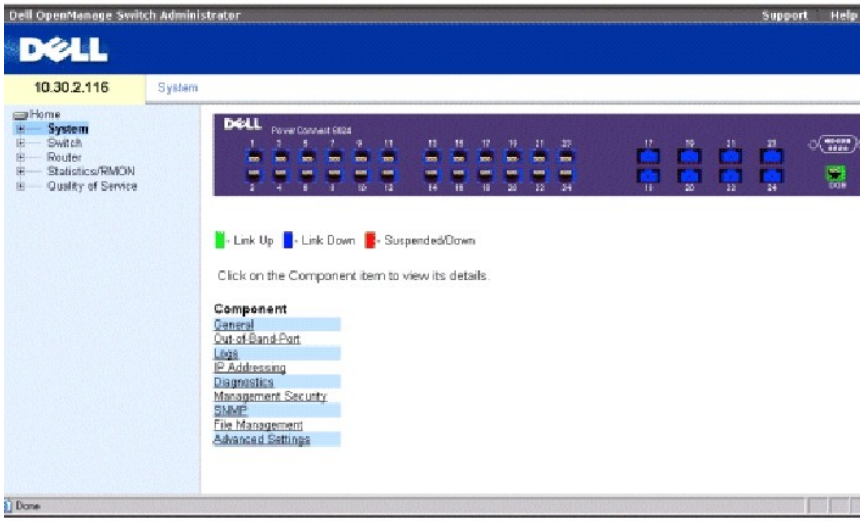
Das Kennwort-Authentifizierungsfenster wird angezeigt.

3. Geben Sie den Benutzernamen und das Kennwort ein.

Der Dell OpenManage-Switch-Administrator wird angezeigt.

ANMERKUNG: Wenn kein Kennwort definiert ist, kann jedes beliebige Kennwort verwendet werden.

Abbildung 5-7. Dell OpenManage Switch-Administrator



Konfigurieren von Secure Management Access (Sicherer Verwaltungszugang - HTTPS)

Wenn das Gerät mithilfe eines Standard-Web-Browsers gesichert verwaltet werden soll, so kommt das Sicherheitsprotokoll SSL (Secure Socket Layer) zur Anwendung.

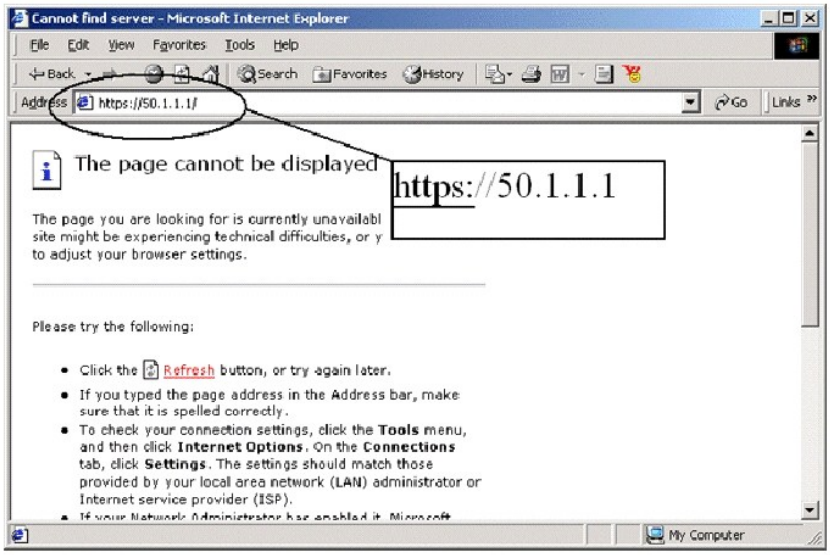
Führen Sie die folgenden Schritte aus, um das Gerät mithilfe eines Standard-Web-Browsers gesichert zu verwalten:

1. Konfigurieren Sie den Switch so, dass die Verwendung eines HTTPS-Servers ermöglicht wird, und erstellen Sie einen Sicherheitsschlüssel mithilfe der Befehle **ip https server** (IP-HTTPS-Server) und **crypto certificate generate key-generate** (Generierung Verschlüsselungszertifikat - Schlüssel):

```
Console# configure

Console (config)# ip https server

Console (config)# crypto certificate generate key-generate

Generating RSA private key, 1024 bit long modulus

Console (config)#
```

2. Konfigurieren Sie die Management-Station so, wie für eine normale HTTP-Verbindung üblich (weitere Informationen finden Sie unter Aktivieren des Web-Zugangs (HTTP-Server))".
3. Verbinden Sie sich über HTTPS mit dem Gerät, indem Sie die Adresse `https://<device IP address>` in das Browser-Fenster eingeben (das Präfix muss dabei eingegeben werden):

Abbildung 5-8. Anmelden am Internet mit einer sicheren Verbindung



Das Fenster **Sicherheitshinweis** wird angezeigt.

4. Klicken Sie auf **Ja**, um die Annahme des Sicherheitszertifikats zu bestätigen (sofern dieses nicht von einem Dritten authentifiziert ist).
5. Das Fenster **Netzwerkkennwort eingeben** wird angezeigt.
6. Geben Sie den Benutzernamen und das Kennwort ein.

Der Dell OpenManage-Switch-Administrator wird angezeigt.

Startup-Menüfunktionen

Weitere Konfigurationen können Sie im **Startup**-Menü ausführen.

So rufen Sie das **Startup**-Menü auf:

1. Drücken Sie während des Startvorgangs, nachdem der erste Teil des Einschaltselbsttests abgeschlossen ist, binnen zwei Sekunden die Taste <Esc> oder <Enter>, nachdem die folgende Meldung angezeigt wurde:

```
Autoboot in 2 seconds -press RETURN or Esc.to abort and enter prom.
```

Das **Startup**-Menü wird angezeigt und enthält die folgenden Konfigurationsfunktionen:

```
[1] Download Software

[2] Erase Flash File

[3] Erase Flash Sectors

[4] Password Recovery Procedure
```

```
[5] Enter Diagnostic Mode


[6] Back Enter your choice or press 'ESC' to exit:
```

Im folgenden Abschnitt werden die Optionen des **Startup**-Menüs beschrieben. Wenn innerhalb von 25 Sekunden (Standardeinstellung) keine Auswahl getroffen wird, erfolgt die Zeitüberschreitung des Switch.

Der Diagnosemodus darf nur vom Technischen Support bedient werden. Aus diesem Grund wird die Option **Enter Diagnostic Mode** (Diagnosemodus aufrufen) des **Startup**-Menüs in diesem Handbuch nicht beschrieben.

Software herunterladen

Verwenden Sie die Option zum Herunterladen von Software, wenn Sie eine neue Softwareversion herunterladen müssen, um beschädigte Dateien zu ersetzen oder um die Systemsoftware zu aktualisieren oder auf eine neue Version umzustellen.

So laden Sie Software vom **Startup**-Menü aus herunter:

1. Drücken Sie im **Startup**-Menü auf <1>.

   Es erscheint die folgende Eingabeaufforderung:

   ```
   Downloading code using XMODEM
   ```

2. Wenn Sie den HyperTerminal verwenden, klicken Sie in der **HyperTerminal**-Menüleiste auf **Transfer**.
3. Klicken Sie dann im **Transfer**-Menü auf **Datei senden**.

   Das Fenster **Datei senden** wird angezeigt.

4. Geben Sie den Pfad der herunterzuladenden Datei ein.
5. Stellen Sie sicher, dass das Protokoll als Xmodem definiert ist.
6. Klicken Sie auf **Senden**.

   Die Software wird geladen. Das Herunterladen der Software dauert mehrere Minuten. Unter Umständen zeigt die Terminal-Emulationsanwendung, z. B. HyperTerminal, eine Fortschrittsanzeige an.

   Nach dem Herunterladen der Software nimmt das Gerät automatisch einen Neustart vor.

Erase Flash File (Flash-Datei löschen)

In bestimmten Fällen muss die Gerätekonfiguration gelöscht werden. Wenn die Konfiguration gelöscht wird, müssen alle über CLI, Web-Browser-Schnittstelle oder SNMP konfigurierten Parameter neu konfiguriert werden.

So löschen Sie die Konfiguration des Geräts:

1. Drücken Sie innerhalb von 6 Sekunden im **Startup**-Menü auf <2>, um die Flash-Datei zu löschen.

   Die folgende Meldung erscheint:

   ```
   Warning! About to erase a Flash file.
   ```

```
Are you sure (Y/N)? y
```

2. Drücken Sie auf <Y>.

ANMERKUNG: Drücken Sie nicht die <Enter>-Taste.

Die folgende Meldung wird angezeigt

```
Write Flash file name (Up to 8 characters, Enter for none.):config File config (if present) will be erased after system initialization


======== Press Enter To Continue ========
```

3. Geben Sie **config** als Namen der Flash-Datei ein.

Die Konfiguration wird gelöscht und das Gerät nimmt einen Neustart vor.

4. Führen Sie die Anfangskonfiguration des Switch aus.

FLASH-Sektoren löschen

Bei der Behebung von Störungen ist es unter Umständen erforderlich, Flash-Sektoren zu löschen. Wird der Flash-Speicher gelöscht, so müssen alle Software-Dateien erneut heruntergeladen und installiert werden.

So löschen Sie den FLASH-Speicher:

1. Drücken Sie binnen 6 Sekunden im **Startup**-Menü auf <3>.

Die folgende Meldung erscheint:

```
Warning! About to erase Flash Memory! FLASH size = 16252928. blocks = 64 Are you sure (Y/N)
```

2. Bestätigen Sie Ihre Auswahl, indem Sie auf <Y> klicken.

Die folgende Meldung erscheint:

```
Enter First flash block (1 - 63):
```

3. Geben Sie den als erstes zu löschenden Flash-Block ein und drücken Sie die Taste <Enter>.

Der Wertebereich beträgt 1-64. Die folgende Meldung wird angezeigt:

```
Enter Last flash block (1 - 63):
```

4. Geben Sie den als letztes zu löschenden Flash-Block ein und drücken Sie auf die Taste <Enter>.
5. Die folgende Meldung erscheint:

```
Are you sure (Y/N)
```

6. Bestätigen Sie Ihre Auswahl, indem Sie auf <Y> klicken.

Die folgende Meldung erscheint:

```
Erasing flash blocks 1 - 63: Done.
```

Password Recovery (Kennwort-Wiederherstellung)

Wenn ein Kennwort verloren gegangen ist, können Sie es aus dem **Startup**-Menü mithilfe der Option **Password Recovery** (Kennwort-Wiederherstellung) wieder herstellen. Bei diesem Verfahren kann der Benutzer ohne Kennwort auf das Gerät zugreifen, jedoch nur für ein einziges Mal.

Wiederherstellung eines verlorenen Kennwortes nur für den lokalen Terminal:

1. Wählen Sie aus dem **Startup**-Menü **[4]** aus und drücken Sie auf <Enter>.

   Das Kennwort wird gelöscht.

2. Konfigurieren Sie die Kennwörter für die anwendbaren Verwaltungsmethoden neu, um die Sicherheit des Geräts zu gewährleisten.

Out of Band-Management-Port

Der OBB-Management-Port ist ein 10/100-Mbps-Ethernet-Port, der zur Ausführung von Systemadministrator-Verwaltungsfunktionen für die direkte Verbindung mit dem Switch verwendet werden kann. Dieser Port gilt als reguläre IP-Schnittstelle des Systems, und alle Verwaltungsschnittstellen sind über diesen Anschluss verfügbar.

Über den OOB-Port kann nicht auf bandinterne Ports zugegriffen werden. Ebenfalls ist der OOB-Port nicht über bandinterne Ports zugänglich. Weil Netzwerkverwaltungsfunktionen mithilfe von OOB ausgeführt werden können, sollten Sie den OOB-Port für alle Netzwerkverwaltungsfunktionen verwenden, einschließlich Web-Management, Abbild, Boot und Konfiguration von Download/Upload, Telnet, SNMP-Management usw.

Im Unterschied zu den bandinternen Ports wird OOB nicht für Routing oder Switching verwendet. Indem Sie den OOB-Port anstelle eines bandinternen Ports für die Netzwerkverwaltung verwenden, stellen Sie sicher, dass ein zusätzlicher bandinterner 1-GB-Port für das Routing aktiv bleibt.

Der folgende Abschnitt enthält Beispiele für OOB-Befehle.

Zuweisen von dynamischen IP-Adressen (an einem bandexternen Port)

```
Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip address dhcp hostname dell

Console (config-oob)# exit

Console (config)# exit

Console#
```

Zuweisen von statischen IP-Adressen (an einem bandexternen Port)

```
Console> enable

Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip address 10.1.1.1 255.0.0.0

Console (config-oob)# exit

Console (config) # ip default-gateway 10.1.1.10

Console (config)# exit

Console#
```

Zuweisen eines IP-Standard-Gateway

```
Console>

Console> enable

Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip address 10.0.0.1 /8

Console (config-oob)# ip default-gateway 10.1.1.1

Console (config-oob)#
```

Ping über OBB

```
Console# ping oob/ 10.6.12.25
```

Kopieren von Abbild/Boot

```
copy tftp://oob/10.6.12.25/ves_115.dos image

copy tftp://oob/10.6.12.25/boot_013.rfb boot
```

IP-Standard-Gateway auf OBB

```
Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip default-gateway 10.1.1.10
```

Zusätzliche Informationen

Weitere Informationen über das Konfigurieren von OBB finden Sie unter „Konfigurieren von bandexternen (OOB) Management-Ports".

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Wie Sie Hilfe bekommen

Dell™ PowerConnect™ 6024/6024F Systeme

Technische Unterstützung

Wenn Sie Unterstützung bei einem technischen Problem benötigen, können Sie die umfassenden Online-Dienste des Supports von Dell unter **support.dell.com** in Anspruch nehmen; dort finden Sie Vorgehensweisen zur Installation und Problembehebung. Weitere Informationen finden Sie unter „Online-Dienste".

Wenn Sie das Problem über die Online-Dienste nicht lösen können, wenden Sie sich direkt an Dell, um technische Hilfestellung zu erhalten. Die entsprechenden Informationen finden Sie unter „Kontaktaufnahme mit Dell".

ANMERKUNG: Rufen Sie den technischen Support über ein Telefon, das sich in der Nähe des Computers befindet, an, damit ein Techniker Sie bei den erforderlichen Schritten unterstützen kann.

ANMERKUNG: Der Expressdienst von Dell ist möglicherweise nicht in allen Ländern verfügbar.

Geben Sie den Express-Servicecode ein, wenn Sie vom automatischen Telefonsystem von Dell dazu aufgefordert werden, damit Ihr Anruf direkt zum zuständigen Support-Personal weitergeleitet werden kann. Wenn Sie keinen Express-Servicecode haben, öffnen Sie den Ordner **Dell Accessories** (Dell Zubehör), doppelklicken Sie auf das Symbol **Express Service Code**, und befolgen Sie die weiteren Anweisungen.

Anweisungen zur Nutzung des technischen Supports finden Sie unter „Technischer Support" und „Vor dem Anruf".

ANMERKUNG: Einige der im Folgenden genannten Dienste sind außerhalb der USA (Festland) möglicherweise nicht verfügbar. Informationen hierzu erhalten Sie bei Ihrem örtlichen Dell-Vertreter.

Online-Dienste

Unter **support.dell.com** können Sie auf die Dell Support-Website zugreifen. Wählen Sie auf der Seite **WELCOME TO DELL SUPPORT** (WILLKOMMEN BEIM DELL SUPPORT) Ihre Region aus, und geben Sie die geforderten Informationen ein, um auf Hilfetools und Informationen zugreifen zu können.

Dell kann elektronisch über die folgenden Adressen erreicht werden:

- World Wide Web

  www.dell.com

  www.dell.com/ap/ (nur für Länder in Asien und im Pazifikraum)

  www.dell.com/jp (Nur für Japan)

  www.euro.dell.com (nur für Länder in Europa)

www.dell.com/la (Lateinamerikanische Länder)

www.dell.ca (nur für Kanada)

- Anonymes FTP-Protokoll (File Transfer Protocol)

ftp.dell.com/

Geben Sie als Benutzerkennung anonymous an und verwenden Sie Ihre E-Mail-Adresse als Kennwort.

- Elektronischer Kundendienst

support@us.dell.com

apsupport@dell.com (Nur für Länder in Asien und im Pazifikraum)

support.jp.dell.com (nur für Japan)

support.euro.dell.com (nur für Länder in Europa)

- Elektronischer Vertriebsdienst

sales@dell.com

apmarketing@dell.com (Nur für Länder in Asien und im Pazifikraum)

sales_canada@dell.com (nur für Kanada)

- Elektronischer Informationsdienst

info@dell.com

AutoTech-Service

Der automatische technische Support von Dell AutoTech bietet Ihnen aufgezeichnete Antworten auf die Fragen, die Dell-Kunden am häufigsten zu tragbaren und Desktop-Computern stellen.

Wenn Sie AutoTech anrufen, können Sie mithilfe der Telefontasten das Thema auswählen, zu dem Sie Fragen haben.

Der AutoTech-Service steht täglich rund um die Uhr zur Verfügung. Sie können diesen Service auch über den technischen Support erreichen. Lesen Sie dazu die Kontaktinformationen zu Ihrer Region.

Automatisches Auftragsauskunftsystem

Um den Status der von Ihnen bestellten Dell™-Produkte abzufragen, können Sie die Webseite **support.dell.com** besuchen oder den automatischen Auftragsauskunftsdienst anrufen. Über eine Bandansage werden Sie zur Angabe bestimmter Informationen aufgefordert, die erforderlich sind, um Ihre Bestellung zu finden und darüber Auskunft zu geben. Lesen Sie dazu die Kontaktinformationen zu Ihrer Region.

Technischer Support

Der Technische Support-Service von Dell ist täglich rund um die Uhr erreichbar und beantwortet Ihre Fragen zur Hardware von Dell. Das Personal des technischen Supports verwendet computergestützte Diagnoseprogramme, um die Fragen schnell und exakt zu beantworten.

Lesen Sie „Vor dem Anruf", um den technischen Support-Service von Dell zu kontaktieren, und sehen Sie sich die für Ihre Region zutreffenden Kontaktinformationen an.

Dell Unternehmensschulungen und Zertifizierungen (Dell Enterprise Training and Certification)

Inzwischen sind auch Unternehmensschulungen und Zertifizierungen (Dell Enterprise Training und Certification) verfügbar. Nähere Informationen hierzu finden Sie unter **www.dell.com/training**. Dieser Service wird möglicherweise nicht an allen Stellen angeboten.

Probleme mit der Bestellung

Sollten sich Probleme mit der Bestellung ergeben (fehlende oder falsche Teile, inkorrekte Abrechnung), setzen Sie sich mit dem Kundendienst von Dell in Verbindung. Halten Sie beim Anruf Lieferschein oder Packzettel bereit. Lesen Sie dazu die Kontaktinformationen zu Ihrer Region.

Produktinformationen

Wenn Sie Informationen zu weiteren Produkten von Dell benötigen oder eine Bestellung aufgeben möchten, besuchen Sie die Website von Dell unter **www.dell.com**. Wenn Sie mit einem Verkaufsberater persönlich sprechen möchten, finden Sie die entsprechende Rufnummer in den Kontaktinformationen für Ihre Region.

Einsenden von Teilen zur Reparatur auf Garantie oder zur Gutschrift

Sämtliche Produkte, die zur Reparatur oder Gutschrift zurückgesendet werden, müssen wie folgt vorbereitet werden:

1. Wenden Sie sich telefonisch an Dell, um eine Rücksendegenehmigungsnummer zu erhalten. Schreiben Sie diese Nummer deutlich lesbar außen auf den Versandkarton.

   Die entsprechende Rufnummer finden Sie in den Kontaktinformationen für Ihre Region.
2. Legen Sie eine Kopie der Rechnung und ein Begleitschreiben bei, in dem der Grund der Rücksendung erklärt wird.
3. Legen Sie gegebenenfalls eine Kopie von Diagnose-Informationen bei.
4. Für eine Gutschrift müssen alle zugehörigen Einzelteile (wie z. B. Netzkabel, Datenträger wie CDs und Disketten sowie Handbücher) mitgeschickt werden.
5. Senden Sie die Geräte in der Originalverpackung (oder einer gleichwertigen Verpackung) zurück.

   Beachten Sie, dass Sie die Versandkosten tragen müssen. Außerdem sind Sie verantwortlich für die Transportversicherung aller zurückgeschickten Produkte und tragen das volle Risiko für den Versand an Dell. Nachnahmesendungen werden verweigert.

Rücksendungen, die diesen Voraussetzungen nicht entsprechen, werden an unserer Annahmestelle verweigert und an den Absender zurückgeschickt.

Vor dem Anruf

ANMERKUNG: Halten Sie bei einem Anruf den Express-Servicecode bereit. Mithilfe dieser Codenummer kann das automatische Telefonsystem von Dell Ihren Anruf gezielt weiterleiten.

Schalten Sie nach Möglichkeit das System vor dem Anruf bei Dell ein und benutzen Sie ein Telefon in der Nähe des Systems. Während des Anrufs sollten Sie in der Lage sein, einige Befehle einzugeben, detaillierte Informationen während des Betriebs zu übermitteln oder andere Schritte zur Fehlerbehebung zu versuchen, die nur am Computersystem durchgeführt werden können. Die Systemdokumentation sollte immer griffbereit sein.

⚠ **WARNUNG: Bevor Sie Arbeiten an Komponenten im Inneren des Computers durchführen, beachten Sie die wichtigen Sicherheitshinweise im *Systeminformationshandbuch*.**

Kontaktaufnahme mit Dell

Dell kann elektronisch über die folgenden Websites erreicht werden:

- **www.dell.com**
- **support.dell.com** (Technischer Support)
- **premiersupport.dell.com** (Technischer Support für Bildungswesen, Behörden, Gesundheitswesen sowie mittelständische Betriebe/Großkunden, einschließlich Premier-, Platin- und Gold-Kunden)

Die Web-Adressen für Ihr Land finden Sie im entsprechenden Abschnitt in der Tabelle unten.

ANMERKUNG: Die gebührenfreien Nummern gelten jeweils in dem Land, bei dem sie genannt werden.

Wenn Sie sich mit Dell in Verbindung setzen möchten, verwenden Sie die in der folgenden Tabelle angegebenen Telefonnummern, Codes und elektronischen Adressen. Im Zweifelsfall können Sie sich an die nationale oder internationale Auskunft wenden.

Land (Stadt) **Vorwahl für ein internationales Gespräch, Nationale Vorwahl** **Ortsvorwahl**	**Abteilungsname oder Dienst,** **Website und E-Mail-Adresse**	**Vorwahlnummern,** **örtliche Nummern und** **gebührenfreie Nummern**
Anguilla	Support (allgemein)	gebührenfrei: 800-335-0031
Antigua und Barbuda	Support (allgemein)	1-800-805-5924
Argentinien (Buenos Aires)	Website: **www.dell.com.ar**	
Internationale Vorwahl: **0 0**	Technischer Support und Kundenbetreuung	gebührenfrei: 0-800-444-0733
	Vertrieb	0-810-444-3355
Nationale Vorwahl: **5 4**	Technischer Support per Fax	11 4515 7139
Ortsvorwahl: **1 1**	Kundenbetreuung per Fax	11 4515 7138
Aruba	Support (allgemein)	gebührenfrei: 800-1578
Australien (Sydney)	E-Mail (Australien): au_tech_support@dell.com	
Internationale Vorwahl: **0 0 1 1**	E-Mail (Neuseeland): nz_tech_support@dell.com	
	Privatkunden und Kleinbetriebe	1-300-65-55-33
Nationale Vorwahl: **6 1**	Behörden und Unternehmen	gebührenfrei: 1-800-633-559
Ortsvorwahl: **2**	Abteilung Vorzugskonten (PAD)	gebührenfrei: 1-800-060-889
	Kundenbetreuung	gebührenfrei: 1-800-819-339
	Vertrieb Firmenkunden	gebührenfrei: 1-800-808-385
	Vertrieb (allgemein)	gebührenfrei: 1-800-808-312
	Fax	gebührenfrei: 1-800-818-341
Bahamas	Support (allgemein)	gebührenfrei: 1-866-278-6818
Barbados	Support (allgemein)	1-800-534-3066
Belgien (Brüssel)	Website: **support.euro.dell.com**	
Internationale Vorwahl: **0 0**	E-Mail: tech_be@dell.com	
Nationale Vorwahl: **3 2**	E-Mail für französischsprachige Kunden: **support.euro.dell.com / be / fr / emaildell /**	
Ortsvorwahl: **2**	Technischer Support	02 481 92 88
	Kundenbetreuung	02 481 91 19
	Vertrieb Firmenkunden	02 481 91 00
	Fax	02 481 92 99

	Zentrale	02 481 91 00
Bermuda	Support (allgemein)	1-800-342-0671
Bolivien	Support (allgemein)	gebührenfrei: 800-10-0238
Brasilien Internationale Vorwahl: **00** Nationale Vorwahl: **55** Ortsvorwahl: **51**	Website: **www.dell.com/br**	
	Kundenunterstützung, Technischer Support	0800 90 3355
	Technischer Support per Fax	51 481 5470
	Kundenbetreuung per Fax	51 481 5480
	Vertrieb	0800 90 3390
Britische Jungferninseln	Support (allgemein)	gebührenfrei: 1-866-278-6820
Brunei Nationale Vorwahl: **673**	Technischer Support für Kunden (Penang, Malaysia)	604 633 4966
	Kundendienst (Penang, Malaysia)	604 633 4949
	Vertrieb (allgemein) (Penang, Malaysia)	604 633 4955
Caymaninseln	Support (allgemein)	1-800-805-7541
Chile (Santiago) Nationale Vorwahl: **56** Ortsvorwahl: **2**	Vertrieb, Kundenunterstützung und technischer Support	gebührenfrei: 1230-020-4823
China (Xiamen) Nationale Vorwahl: **86** Ortsvorwahl: **592**	Website des Techn. Supports: **support.ap.dell.com/china**	
	Technischer Support per E-Mail: cn_support@dell.com	
	Technischer Support per Fax	818 1350
	Technischer Support für Privatkunden und Kleinbetriebe	gebührenfrei: 800 858 2437
	Technischer Support Firmenkunden	gebührenfrei: 800 858 2333
	Kundenerfahrungen	gebührenfrei: 800 858 2060
	Privatkunden und Kleinbetriebe	gebührenfrei: 800 858 2222
	Abteilung Vorzugskonten	gebührenfrei: 800 858 2557
	Großkunden – GCP	gebührenfrei: 800 858 2055
	Großkunden – Key Accounts	gebührenfrei: 800 858 2628
	Großkunden – Nord	gebührenfrei: 800 858 2999
	Großkunden – Nord, Behörden und Bildungswesen	gebührenfrei: 800 858 2955
	Großkunden – Ost	gebührenfrei: 800 858 2020
	Großkunden – Ost, Behörden und Bildungswesen	gebührenfrei: 800 858 2669
	Support-Team für Großkunden	gebührenfrei: 800 858 2222
	Großkunden – Süd	gebührenfrei: 800 858 2355
	Großkunden – West	gebührenfrei: 800 858 2811
	Großkunden – Ersatzteile	gebührenfrei: 800 858 2621
Costa Rica	Support (allgemein)	0800-012-0435
Dänemark (Kopenhagen) Internationale Vorwahl: **00** Nationale Vorwahl: **45**	Website: **support.euro.dell.com**	
	E-Mail-Support (Laptop-Computer): den_nbk_support@dell.com	
	E-Mail-Support (Desktop-Computer): den_support@dell.com	
	E-Mail-Support (Server): Nordic_server_support@dell.com	
	Technischer Support	7023 0182
	Kundenbetreuung (relational)	7023 0184
	Kundenbetreuung Privatkunden/Kleinbetriebe	3287 5505
	Zentrale (relational)	3287 1200
	Fax-Zentrale (relational)	3287 1201
	Zentrale (Privatkunden/Kleinbetriebe)	3287 5000
	Fax-Zentrale (Privatkunden/Kleinbetriebe)	3287 5001
Deutschland (Langen) Internationale Vorwahl: **00** Nationale Vorwahl: **49** Ortsvorwahl: **6103**	Website: **support.euro.dell.com**	
	E-Mail: tech_support_central_europe@dell.com	
	Technischer Support	06103 766-7200
	Kundenbetreuung Privatkunden/Kleinbetriebe	0180-5-224400
	Kundenbetreuung (global)	06103 766-9570
	Kundenbetreuung Vorzugskonten	06103 766-9420
	Kundenbetreuung Großkunden	06103 766-9560
	Kundenbetreuung Kunden der öffentlichen Hand	06103 766-9555
	Zentrale	06103 766-7000
Dominica	Support (allgemein)	gebührenfrei: 1-866-278-6821
Dominikanische Republik	Support (allgemein)	1-800-148-0530
Ecuador	Support (allgemein)	gebührenfrei: 999-119

El Salvador	Support (allgemein)	01-899-753-0777
Finnland (Helsinki) Internationale Vorwahl: **990** Nationale Vorwahl: **358** Ortsvorwahl: **9**	Website: **support.euro.dell.com**	
	E-Mail: fin_support@dell.com	
	E-Mail-Support (Server): Nordic_support@dell.com	
	Technischer Support	09 253 313 60
	Technischer Support per Fax	09 253 313 81
	Kundenbetreuung (relational)	09 253 313 38
	Kundenbetreuung Privatkunden/Kleinbetriebe	09 693 791 94
	Fax	09 253 313 99
	Zentrale	09 253 313 00
Frankreich (Paris) (Montpellier) Internationale Vorwahl: **00** Nationale Vorwahl: **33** Ortsvorwahlen: **(1) (4)**	Website: **support.euro.dell.com**	
	E-Mail: **support.euro.dell.com/fr/fr/emaildell/**	
	Privatkunden und Kleinbetriebe	
	Technischer Support	0825 387 270
	Kundenbetreuung	0825 823 833
	Zentrale	0825 004 700
	Zentrale (Anrufe von außerhalb nach Frankreich)	04 99 75 40 00
	Vertrieb	0825 004 700
	Fax	0825 004 701
	Fax (Anrufe von außerhalb nach Frankreich)	04 99 75 40 01
	Firmenkunden	
	Technischer Support	0825 004 719
	Kundenbetreuung	0825 338 339
	Zentrale	01 55 94 71 00
	Vertrieb	01 55 94 71 00
	Fax	01 55 94 71 01
Grenada	Support (allgemein)	gebührenfrei: 1-866-540-3355
Griechenland Internationale Vorwahl: 00 Nationale Vorwahl: 30	Website: **support.euro.dell.com**	
	E-Mail: support.euro.dell.com/gr/en/emaildell/	
	Technischer Support	080044149518
	Technischer Gold-Support	08844140083
	Zentrale	2108129800
	Vertrieb	2108129800
	Fax	2108129812
Großbritannien (Bracknell) Internationale Vorwahl: **00** Nationale Vorwahl: **44** Ortsvorwahl: **1344**	Website: **support.euro.dell.com**	
	Website für Kundenbetreuung: **support.euro.dell.com/uk/en/ECare/Form/Home.asp**	
	E-Mail: dell_direct_support@dell.com	
	Technischer Support (Firmenkunden/Vorzugskonten/PAD [ab 1000 Mitarbeiter])	0870 908 0500
	Technischer Support (Direkt/PAD und allgemein)	0870 908 0800
	Kundenbetreuung (global)	01344 373 186
	Kundenbetreuung Privatkunden/Kleinbetriebe	0870 906 0010
	Kundenbetreuung Firmenkunden	01344 373 185
	Kundenbetreuung Vorzugskonten (500–5000 Mitarbeiter)	0870 906 0010
	Kundenbetreuung Zentralbehörden	01344 373 193
	Kundenbetreuung Regionale Regierung & Bildungswesen	01344 373 199
	Kundenbetreuung Gesundheitswesen	01344 373 194
	Vertrieb Privatkunden und Kleinbetriebe	0870 907 4000
	Vertrieb Firmenkunden/Staatliche Einrichtungen	01344 860 456
	Fax Privatkunden und Kleinbetriebe	0870 907 4006
Guatemala	Support (allgemein)	1-800-999-0136
Guyana	Support (allgemein)	gebührenfrei: 1-877-270-4609
Hongkong Internationale Vorwahl: **001** Nationale Vorwahl: **852**	Website: **support.ap.dell.com**	
	E-Mail: ap_support@dell.com	
	Technischer Support (Dimension™ und Inspiron™)	2969 3189
	Technischer Support (OptiPlex™, Latitude™ und Dell Precision™)	2969 3191
	Technischer Support (PowerApp™ und PowerVault™)	2969 3196
	Gold Queue EEC Hotline	2969 3187

	Kundenbetreuung	3416 0910
	Großkunden	3416 0907
	Kundenprogramme (global)	3416 0908
	Mittlere Unternehmen	3416 0912
	Privatkunden und Kleinbetriebe	2969 3105
Indien	Technischer Support	1600 33 8045
	Vertrieb	1600 33 8044
Irland (Cherrywood)	Website: **support.euro.dell.com**	
Internationale Vorwahl: **16**	E-Mail: dell_direct_support@dell.com	
	Technischer Support	1850 543 543
Nationale Vorwahl: **353**	Technischer Support in Großbritannien (nur innerhalb von GB)	0870 908 0800
Ortsvorwahl: **1**	Kundenbetreuung Privatkunden	01 204 4014
	Kundenbetreuung Kleinbetriebe	01 204 4014
	Kundenbetreuung in Großbritannien (nur innerhalb von GB)	0870 906 0010
	Kundenbetreuung Firmenkunden	1850 200 982
	Kundenbetreuung Firmenkunden (nur innerhalb von GB)	0870 907 4499
	Vertrieb für Irland	01 204 4444
	Vertrieb in Großbritannien (nur innerhalb von GB)	0870 907 4000
	Fax/Vertrieb per Fax	01 204 0103
	Zentrale	01 204 4444
Italien (Mailand)	Website: **support.euro.dell.com**	
Internationale Vorwahl: **00**	E-Mail: **support.euro.dell.com/it/it/emaildell/**	
	Privatkunden und Kleinbetriebe	
Nationale Vorwahl: **39**	Technischer Support	02 577 826 90
Ortsvorwahl: **02**	Kundenbetreuung	02 696 821 14
	Fax	02 696 821 13
	Zentrale	02 696 821 12
	Firmenkunden	
	Technischer Support	02 577 826 90
	Kundenbetreuung	02 577 825 55
	Fax	02 575 035 30
	Zentrale	02 577 821
Jamaika	Support (allgemein, nur innerhalb von Jamaika)	1-800-682-3639
Japan (Kawasaki)	Website: **support.jp.dell.com**	
Internationale Vorwahl: **001**	Technischer Support (Server)	gebührenfrei: 0120-198-498
	Technischer Support außerhalb Japans (Server)	81-44-556-4162
Nationale Vorwahl: **81**	Technischer Support (Dimension™ und Inspiron™)	gebührenfrei: 0120-198-226
Ortsvorwahl: **44**	Technischer Support außerhalb Japans (Dimension und Inspiron)	81-44-520-1435
	Technischer Support (Dell Precision™, OptiPlex™ und Latitude™)	gebührenfrei:0120-198-433
	Technischer Support außerhalb Japans (Dell Precision, OptiPlex und Latitude)	81-44-556-3894
	Technischer Support (Axim™)	gebührenfrei: 0120-981-690
	Technischer Support außerhalb Japans (Axim)	81-44-556-3468
	Faxbox-Dienst	044-556-3490
	Automatischer Bestellservice (rund um die Uhr)	044-556-3801
	Kundenbetreuung	044-556-4240
	Vertrieb Geschäftskunden (bis 400 Mitarbeiter)	044-556-1465
	Vertrieb Vorzugskonten (über 400 Mitarbeiter)	044-556-3433
	Vertrieb Großkunden (über 3500 Mitarbeiter)	044-556-3430
	Vertrieb Öffentliche Einrichtungen (Behörden, Bildungs- und Gesundheitswesen)	044-556-1469
	Japan (global)	044-556-3469
	Einzelbenutzer	044-556-1760
	Zentrale	044-556-4300
Jungferninseln (USA)	Support (allgemein)	1-877-673-3355
Kanada (North York, Ontario)	Online-Bestellstatus: **www.dell.ca/ostatus**	
Internationale Vorwahl: **011**	AutoTech (Automatischer technischer Support)	gebührenfrei: 1-800-247-9362
	TechFax	gebührenfrei: 1-800-950-1329
	Kundenbetreuung (Privatkunden/Kleinbetriebe)	gebührenfrei: 1-800-847-4096
	Kundenbetreuung (mittlere/große Betriebe, Behörden)	gebührenfrei: 1-800-326-9463

	Technischer Support (Privatkunden/Kleinbetriebe)	gebührenfrei: 1-800-847-4096
	Technischer Support (mittlere/große Betriebe, Behörden)	gebührenfrei: 1-800-387-5757
	Vertrieb (Privatkunden/Kleinbetriebe)	gebührenfrei: 1-800-387-5752
	Vertrieb (mittlere/große Betriebe, Behörden)	gebührenfrei: 1-800-387-5755
	Ersatzteilverkauf & Erweiterter Vertriebsservice	1 866 440 3355
Kolumbien	Support (allgemein)	980-9-15-3978
Korea (Seoul) Internationale Vorwahl: **001** Nationale Vorwahl: **82** Ortsvorwahl: **2**	Technischer Support	gebührenfrei: 080-200-3800
	Vertrieb	gebührenfrei: 080-200-3600
	Kundendienst (Seoul, Korea)	gebührenfrei: 080-200-3800
	Kundendienst (Penang, Malaysia)	604 633 4949
	Fax	2194-6202
	Zentrale	2194-6000
Lateinamerika	Technischer Support für Kunden (Austin, Texas, USA)	512 728-4093
	Kundendienst (Austin, Texas, USA)	512 728-3619
	Fax (Technischer Support und Kundendienst) (Austin, Texas, USA)	512 728-3883
	Vertrieb (Austin, Texas, USA)	512 728-4397
	Vertrieb per Fax (Austin, Texas, USA)	512 728-4600 oder 512 728-3772
Luxemburg Internationale Vorwahl: **00** Nationale Vorwahl: **352**	Website: **support.euro.dell.com**	
	E-Mail: tech_be@dell.com	
	Technischer Support (Brüssel, Belgien)	3420808075
	Vertrieb Privatkunden/Kleinbetriebe (Brüssel, Belgien)	gebührenfrei: 080016884
	Vertrieb Firmenkunden (Brüssel, Belgien)	02 481 91 00
	Kundenbetreuung (Brüssel, Belgien)	02 481 91 19
	Fax (Brüssel, Belgien)	02 481 92 99
	Zentrale (Brüssel, Belgien)	02 481 91 00
Macao Nationale Vorwahl: **853**	Technischer Support	gebührenfrei: 0800 582
	Kundendienst (Penang, Malaysia)	604 633 4949
	Vertrieb (allgemein)	gebührenfrei: 0800 581
Malaysia (Penang) Internationale Vorwahl: **00** Nationale Vorwahl: **60** Ortsvorwahl: **4**	Technischer Support	gebührenfrei: 1 800 888 298
	Kundendienst	04 633 4949
	Vertrieb (allgemein)	gebührenfrei: 1800888202
	Vertrieb Firmenkunden	gebührenfrei: 1 800 888 213
Mexiko Internationale Vorwahl: **00** Nationale Vorwahl: **52**	Technischer Support für Kunden	001-877-384-8979 oder 001-877-269-3383
	Vertrieb	50-81-8800 oder 01-800-888-3355
	Kundendienst	001-877-384-8979 oder 001-877-269-3383
	Zentrale	50-81-8800 oder 01-800-888-3355
Montserrat	Support (allgemein)	gebührenfrei: 1-866-278-6822
Neuseeland Internationale Vorwahl: **00** Nationale Vorwahl: **64**	E-Mail (Neuseeland): nz_tech_support@dell.com	
	E-Mail (Australien): au_tech_support@dell.com	
	Privatkunden und Kleinbetriebe	0800 446 255
	Behörden und Unternehmen	0800 444 617
	Vertrieb	0800 441 567
	Fax	0800 441 566
Nicaragua	Support (allgemein)	001-800-220-1006
Niederlande (Amsterdam) Internationale Vorwahl: **00** Nationale Vorwahl: **31** Ortsvorwahl: **20**	Website: **support.euro.dell.com** E-Mail (Technischer Support): (Enterprise): nl_server_support@dell.com (Latitude): nl_latitude_support@dell.com (Inspiron): nl_inspiron_support@dell.com	

	(Dimension): nl_dimension_support@dell.com (OptiPlex): nl_optiplex_support@dell.com (Dell Precision): nl_workstation_support@dell.com	
	Technischer Support	020 674 45 00
	Technischer Support per Fax	020 674 47 66
	Kundenbetreuung Privatkunden/Kleinbetriebe	020 674 42 00
	Kundenbetreuung (relational)	020 674 4325
	Vertrieb Privatkunden/Kleinbetriebe	020 674 55 00
	Vertrieb (relational)	020 674 50 00
	Vertrieb Privatkunden/Kleinbetriebe per Fax	020 674 47 75
	Vertrieb per Fax (relational)	020 674 47 50
	Zentrale	020 674 50 00
	Fax-Zentrale	020 674 47 50
Niederländische Antillen	Support (allgemein)	001-800-882-1519
Norwegen (Lysaker) Internationale Vorwahl: **00** Nationale Vorwahl: **47**	Website: **support.euro.dell.com**	
	E-Mail-Support (Laptop-Computer): nor_nbk_support@dell.com	
	E-Mail-Support (Desktop-Computer): nor_support@dell.com	
	E-Mail-Support (Server): Nordic_server_support@dell.com	
	Technischer Support	671 16882
	Kundenbetreuung (relational)	671 17514
	Kundenbetreuung Privatkunden/Kleinbetriebe	23162298
	Zentrale	671 16800
	Fax-Zentrale	671 16865
Österreich (Wien) Internationale Vorwahl: **900** Nationale Vorwahl: **43** Ortsvorwahl: **1**	Website: **support.euro.dell.com**	
	E-Mail: tech_support_central_europe@dell.com	
	Vertrieb Privatkunden/Kleinbetriebe	0820 240 530 00
	Fax Privatkunden/Kleinbetriebe	0820 240 530 49
	Kundenbetreuung Privatkunden/Kleinbetriebe	0820 240 530 14
	Kundenbetreuung Vorzugskonten/Firmenkunden	0820 240 530 16
	Technischer Support Privatkunden/Kleinbetriebe	0820 240 530 14
	Technischer Support Vorzugskonten/Firmenkunden	0660 8779
	Zentrale	0820 240 530 00
Panama	Support (allgemein)	001-800-507-0962
Peru	Support (allgemein)	0800-50-669
Polen (Warschau) Internationale Vorwahl: **011** Nationale Vorwahl: **48** Ortsvorwahl: **22**	Website: **support.euro.dell.com**	
	E-Mail: pl_support@dell.com	
	Kundendienst per Telefon	57 95 700
	Kundenbetreuung	57 95 999
	Vertrieb	57 95 999
	Kundendienst per Fax	57 95 806
	Empfang – Fax	57 95 998
	Zentrale	57 95 999
Portugal Internationale Vorwahl: **00** Nationale Vorwahl: **351**	Website: **support.euro.dell.com**	
	E-Mail: **support.euro.dell.com/pt/en/emaildell/**	
	Technischer Support	707200149
	Kundenbetreuung	800 300 413
	Vertrieb	800 300 410 oder 800 300 411 oder 800 300 412 oder 21 422 07 10
	Fax	21 424 01 12
Puerto Rico	Support (allgemein)	1-800-805-7545
Schweden (Upplands Vasby) Internationale Vorwahl: **00** Nationale Vorwahl: **46**	Website: **support.euro.dell.com**	
	E-Mail: swe_support@dell.com	
	E-Mail-Support für Latitude und Inspiron: Swe-nbk_kats@dell.com	
	E-Mail-Support für OptiPlex: Swe_kats@dell.com	

Ortsvorwahl: **8**		
	E-Mail-Support für Server: Nordic_server_support@dell.com	
	Technischer Support	08 590 05 199
	Kundenbetreuung (relational)	08 590 05 642
	Kundenbetreuung Privatkunden/Kleinbetriebe	08 587 70 527
	Support für das Mitarbeiterprogramm (EPP)	20 140 14 44
	Fax-technischer Support	08 590 05 594
	Vertrieb	08 590 05 185
Schweiz (Genf)	Website: **support.euro.dell.com**	
Internationale Vorwahl: **00**	E-Mail: swisstech@dell.com	
Nationale Vorwahl: **41**	E-Mail für französischsprachige Privatkunden/Kleinbetriebe sowie Firmenkunden: **support.euro.dell.com/ch/fr/emaildell/**	
Ortsvorwahl: **22**	Technischer Support (Privatkunden/Kleinbetriebe)	0844 811 411
	Technischer Support (Firmenkunden)	0844 822 844
	Kundenbetreuung (Privatkunden/Kleinbetriebe)	0848 802 202
	Kundenbetreuung (Firmenkunden)	0848 821 721
	Fax	022 799 01 90
	Zentrale	022 799 01 01
Singapur(Singapur)	Technischer Support	gebührenfrei: 800 6011 051
Internationale Vorwahl: **005**	Kundendienst (Penang, Malaysia)	604 633 4949
Nationale Vorwahl: **65**	Vertrieb (allgemein)	gebührenfrei: 800 6011 054
	Vertrieb Firmenkunden	gebührenfrei: 800 6011 053
Spanien (Madrid)	Website: **support.euro.dell.com**	
Internationale Vorwahl: **00**	E-Mail: **support.euro.dell.com/es/es/emaildell/**	
Nationale Vorwahl: **34**	**Privatkunden und Kleinbetriebe**	
Ortsvorwahl: **91**	Technischer Support	902 100 130
	Kundenbetreuung	902 118 540
	Vertrieb	902 118 541
	Zentrale	902 118 541
	Fax	902 118 539
	Firmenkunden	
	Technischer Support	902 100 130
	Kundenbetreuung	902 118 546
	Zentrale	91 722 92 00
	Fax	91 722 95 83
St. Kitts und Nevis	Support (allgemein)	gebührenfrei: 1-877-441-4731
St. Lucia	Support (allgemein)	1-800-882-1521
St. Vincent und Grenadinen	Support (allgemein)	gebührenfrei: 1-877-270-4609
Südafrika (Johannesburg)	Website: **support.euro.dell.com**	
Internationale Vorwahl:	E-Mail: dell_za_support@dell.com	
09/091	Technischer Support	011 709 7710
Nationale Vorwahl: **27**	Kundenbetreuung	011 709 7707
Ortsvorwahl: **11**	Vertrieb	011 709 7700
	Fax	011 706 0495
	Zentrale	011 709 7700
Südostasien und Pazifikraum	Technischer Support für Kunden, Kundendienst und Vertrieb (Penang, Malaysia)	604 633 4810
Taiwan	Technischer Support (Laptop- und Desktop-Computer)	gebührenfrei: 00801 86 1011
Internationale Vorwahl: **002**	Technischer Support (Server)	gebührenfrei: 0080 60 1256
Nationale Vorwahl: **886**	Vertrieb (allgemein)	gebührenfrei: 0080 651 228
	Vertrieb Firmenkunden	gebührenfrei: 0080 651 227
Thailand	Technischer Support	gebührenfrei: 0880 060 07
Internationale Vorwahl: **001**	Kundendienst (Penang, Malaysia)	604 633 4949
Nationale Vorwahl: **66**	Vertrieb	gebührenfrei: 0880 060 09
Trinidad und Tobago	Support (allgemein)	1-800-805-8035
Tschechische Republik (Prag)	Website: **support.euro.dell.com**	
Internationale Vorwahl: **00**	E-Mail: czech_dell@dell.com	
Nationale Vorwahl: **420**	Technischer Support	02 2186 27 27
	Kundenbetreuung	02 2186 27 11
Ortsvorwahl: **2**	Fax	02 2186 27 14

	TechFax	02 2186 27 28
	Zentrale	02 2186 27 11
Turks- und Caicosinseln	Support (allgemein)	gebührenfrei: 1-866-540-3355
Uruguay	Support (allgemein)	gebührenfrei: 000-413-598-2521
USA (Austin, Texas) Internationale Vorwahl: **011** Nationale Vorwahl: **1**	Automatisches Auftragsauskunftsystem	gebührenfrei: 1-800-433-9014
	AutoTech (Laptop- und Desktop-Computer)	gebührenfrei: 1-800-247-9362
	Verbraucher (Privat und Home Office)	
	Technischer Support	gebührenfrei: 1-800-624-9896
	Kundendienst	gebührenfrei: 1-800-624-9897
	DellNet™ Service und Support	gebührenfrei: 1-877-Dellnet (1-877-335-5638)
	EPP-Kunden (Mitarbeiterprogramm)	gebührenfrei: 1-800-695-8133
	Website der Finanzierungsdienste: **www.dellfinancialservices.com**	
	Finanzierungsdienste (Leasing/Darlehen)	gebührenfrei: 1-877-577-3355
	Finanzierungsdienste (Dell Vorzugskonten [DPA])	gebührenfrei: 1 -800 -283 -2210
	Geschäftskunden	
	Kundendienst und technischer Support	gebührenfrei: 1-800-822-8965
	EPP-Kunden (Mitarbeiterprogramm)	gebührenfrei: 1-800-695-8133
	Technischer Support für Projektoren	gebührenfrei: 1-877-459-7298
	Öffentliche Kunden (Regierung, Bildungs- und Gesundheitswesen)	
	Kundendienst und technischer Support	gebührenfrei: 1-800-456-3355
	EPP-Kunden (Mitarbeiterprogramm)	gebührenfrei: 1-800-234-1490
	Dell-Vertrieb	gebührenfrei: 1-800-289-3355 oder gebührenfrei: 1-800-879-3355
	Dell Outlet-Verkauf (von Dell erneuerte Computer)	gebührenfrei: 1-888-798-7561
	Vertrieb von Software und Peripheriegeräten	gebührenfrei: 1-800-671-3355
	Ersatzteilvertrieb	gebührenfrei: 1-800-357-3355
	Vertrieb, erweiterter Service und Garantie	gebührenfrei: 1-800-247-4618
	Fax	gebührenfrei: 1-800-727-8320
	Dell-Dienste für Gehörlose, Schwerhörige oder Sprachbehinderte	gebührenfrei: 1-877-DELLTTY (1-877-335-5889)
Venezuela	Support (allgemein)	8001-3605

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Verwendung von Dell OpenManage Switch Administrator:

Dell™ PowerConnect™ 6024/6024F Systeme

Starten der Anwendung

1. Öffnen eines Web-Browsers.
2. Geben Sie die IP-Adresse des Switch (wie im CLI definiert) in der Adresszeile ein und drücken Sie die <Eingabetaste>.

   Weitere Informationen über die Zuordnung von IP-Adressen für ein Switch finden Sie unter „Initial Configuration" (Anfängliche Konfiguration).
3. Wenn das Fenster **Enter Network Password** (Netzwerk-Kennwort eingeben) erscheint, geben Sie einen Benutzernamen und ein Kennwort ein.

ANMERKUNG: Der Switch ist ohne Standard-Kennwort konfiguriert und kann auch ohne Eingabe eines Kennworts konfiguriert werden. Nähere Angaben zur Wiederherstellung eines verlorengegangenen Kennwortes finden Sie unter „Kennwort-Wiederherstellung ".

ANMERKUNG: Kennwörter sind alphanummerisch und es wird zwischen Groß- und Kleinschreibung unterschieden.

4. Klicken Sie auf **OK**.
5. Die Startseite von **Dell OpenManage Switch Administrator** wird angezeigt.

Wissenswertes zur Benutzeroberfläche

Die Startseite (siehe Abbildung 4-1) enthält die folgenden Ansichten:

- **Tree View** (Strukturansicht) – Die links auf der Startseite befindliche Strukturansicht bietet eine erweiterbare Ansicht der Funktionen und ihrer Komponenten.
- **Device View** (Geräteansicht) – Die rechts auf der Startseite befindliche Geräteansicht bietet eine Ansicht des Geräts, einen Informations- oder Tabellenbereich und Konfigurationsanweisungen.

Abb. 4-1. Switch Administrator-Komponenten

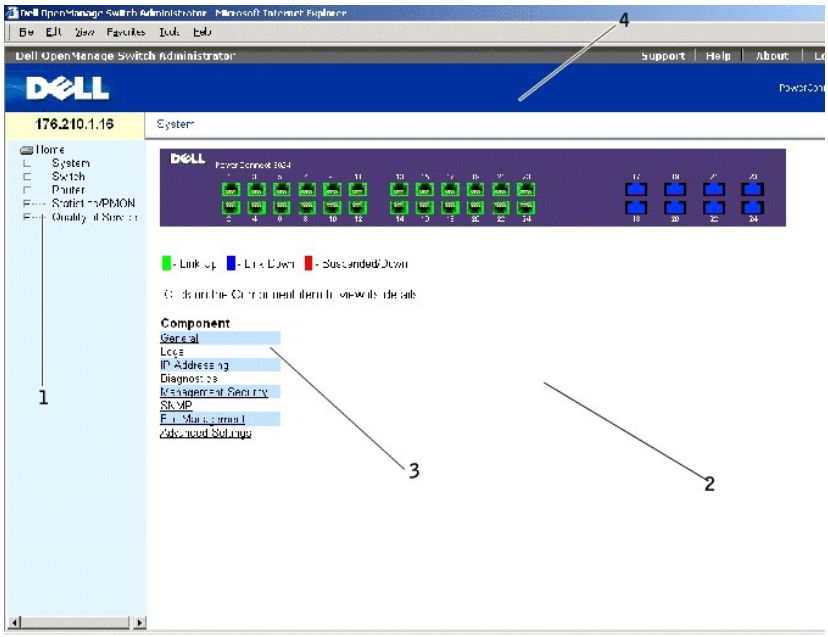


Tabelle 4-1 listet die Schnittstellenkomponenten mit den entsprechenden Nummern auf.

Tabelle 4-1. Schnittstellenkomponenten

Komponente	Name
1	Die Strukturansicht enthält eine Liste der verschiedenen Gerätefunktionen. Die Verzweigungen der Strukturansicht lassen sich erweitern, um alle Komponenten unter einer bestimmten Funktion anzuzeigen, bzw. lassen sich einziehen, um die Komponenten der Funktion auszublenden. Durch Verschieben des senkrechten Balkens kann der Ansichtsbereich vergrößert werden und der vollständige Name einer Komponente sichtbar gemacht werden.
2	Die Geräteansicht bietet Informationen über die Geräteports, aktuelle Konfiguration und Status, Tabelleninformationen und Komponenten von Funktionen. Die jeweilige Farbe des Ports zeigt an, ob der Port derzeit aktiv ist. Grün zeigt an, dass der Port aktiviert ist, rot zeigt an, dass ein Fehler am Port aufgetreten ist und blau zeigt an, dass die Verbindung deaktiviert wurde. **ANMERKUNG:** Die Leuchtdioden werden nicht in der Geräteansicht angezeigt. Der Status der Leuchtdioden kann nur durch Sichtung des jeweiligen Switch festgestellt werden. Weitere Informationen über LEDs finden Sie unter „LED-Definitionen". Je nach dem welche Option Sie auswählen, zeigt der untere Bereich der Geräteansicht weitere Geräteinformationen und/ oder Dialogfelder für das Konfigurieren von Parametern an.
3	Die Komponentenliste umfasst eine Liste der Funktionskomponenten. Sie können Komponenten auch durch das Aufklappen einer Funktion in der Strukturansicht ansehen.
4	Die Informations-Schaltflächen ermöglichen den Zugang zu Switch-Informationen und zum Dell Support. Weitere Informationen finden Sie unter Informationsschaltflächen.

Verwenden der Switch Administrator-Schaltflächen

Informationsschaltflächen

Tabelle 4-2. Informationsschaltflächen

Schaltfläche	Beschreibung
Support	Öffnet die Seite „Dell Support" unter **support.dell.com**

Help (Hilfe)	Online-Hilfe mit hilfreichen Informationen zur Konfiguration und Steuerung des Switch. Die Seiten der Online-Hilfe sind direkt mit den jeweiligen Seiten verbunden. Wenn beispielsweise die Seite **IP Addressing** (IP-Adressierung) geöffnet ist, erscheint die themenbezogene Hilfe zu dieser Seite, wenn Sie auf **Help** (Hilfe) klicken.
Info	**Beinhaltet** die Version und Bauartnummer sowie Informationen zum Dell Copyright.
Log Out (Abmelden)	Meldet den Benutzer aus der Anwendung ab und schließt das Browser-Fenster.

Schaltflächen zur Geräteverwaltung

Tabelle 4-3. Schaltflächen zur Geräteverwaltung

Schaltfläche	Beschreibung
Apply Changes (Änderungen übernehmen)	Übernimmt vorgenommene Änderungen auf dem Gerät.
Schaltfläche **Add** (Hinzufügen)	Fügt Informationen zu Tabellen oder Dialogfeldern hinzu.
Telnet	Startet eine Telnet-Sitzung.
Query (Abfragen)	Dient zur Tabellenabfrage.
Show all (Alle anzeigen)	Zeigt die Gerätetabellen an.
Links-/Rechtspfeil	Verschiebt Informationen zwischen Listen.
Refresh (Aktualisieren)	Aktualisiert Geräteinformationen.
Reset All Counters (Alle Zähler rücksetzen)	Löscht den Inhalt aller Statistikzähler.
Print (Drucken)	Druckt die Seite **Network Management System** und/oder Tabelleninformationen aus.
Show Neighbor's Info (Nachbarninformationen anzeigen)	Zeigt die **Neighbors List** (Nachbarliste) von der Seite **Neighbors Table** (Nachbartabelle) an.
Draw (Grafik)	Generiert Diagramme zu Statistiken dynamisch.
Protokoll löschen	Löscht Protokollmeldungen aus dem Protokollzwischenspeicher.
Reset-	Setzt den Switch zurück.
Test Now (Jetzt testen)	Führt eine Diagnosetest für die Kupferkabel aus.

Definieren von Feldern

Benutzerdefinierte Felder können 1-159 Zeichen enthalten, wenn es keine anderslautenden Informationen auf der Webseite von Dell OpenManage Switch Administrator gibt.

Es können alle Zeichen verwendet werden, mit Ausnahme der folgenden:

- \
- /
- :
- *
- ?
- <
- >
- |

Zugriff auf den Switch über CLI

Der Switch kann über eine direkte Verbindung zur Konsolenport oder eine Telnet-Verbindung gesteuert werden. Informationen über bandexterne Management-Ports finden Sie unter „Out of Band-Management-Port".

Die Verwendung von CLI ist mit der Eingabe von Befehlen auf einem Linux-System vergleichbar. Wenn der Zugriff über eine Telnet-Verbindung erfolgt, stellen Sie vor der Verwendung von CLI-Befehlen sicher, dass für das Gerät eine IP-Adresse definiert wurde und dass die zum Zugriff auf das Gerät verwendete Workstation mit dem Gerät verbunden ist.

Informationen über das Konfigurieren von ursprünglichen IP-Adressen finden Sie unter „Anfängliche Konfiguration”.

ANMERKUNG: Stellen Sie vor der CLI-Verwendung sicher, dass der Client geladen ist.

Konsolenverbindung

1. Schalten Sie den Switch ein und warten Sie bis der Startvorgang abgeschlossen ist.
2. Geben Sie nach Erscheinen der Eingabeaufforderung `Console>` `enable` ein und drücken Sie die <Eingabetaste>.
3. Konfigurieren Sie das Gerät und geben Sie die erforderlichen Befehle zur Durchführung der gewünschten Funktionen ein.
4. Beenden Sie anschließend die Session mit dem Befehl `quit` oder `exit`.

ANMERKUNG: Wenn sich ein anderer Benutzer im privilegierten EXEC-Befehlsmodus im System anmeldet, wird der aktuelle Benutzer abgemeldet und der neue Benutzer angemeldet.

Telnet-Verbindung

Telnet ist ein Terminal-Emulations-TCP/IP-Protokoll. ASCII-Terminals können virtuell über ein TCP/IP-Protokoll-Netzwerk am lokalen Gerät angeschlossen werden. Telnet ist eine Alternative zu einem lokalen Anmelde-Terminal, in der eine Fernanmeldung erforderlich ist.

Ihr Switch unterstützt bis zu vier simultane Telnet-Sitzungen. Alle CLI-Befehle können in einer Telnet-Session verwendet werden.

Starten einer Telnet-Sitzung:

1. Wählen Sie **Start** > **Run** (Ausführen).
2. Geben Sie im Fenster **Run** (Ausführen) `Telnet` *<IP address>* im Feld **Open** ein.
3. Klicken Sie auf **OK**, um die Telnet-Sitzung zu beginnen.

Verwenden der CLI-Befehle

Übersicht über den Befehlsmodus

CLI ist in Befehlsmodi unterteilt. Jeder Befehlsmodus umfasst einen bestimmten Befehlssatz. Nach Eingabe eines Fragezeichens an der Konsolen-Eingabeaufforderung wird eine Liste der möglichen Befehle für den jeweiligen Befehlsmodus angezeigt.

In jedem Modus wird ein spezieller Befehl zur Navigation von einem Befehlsmodus zum anderen verwendet.

In der Initialisierung der CLI-Sitzung ist der CLI-Modus der User EXEC-Modus. Im User EXEC-Modus ist nur eine begrenzte Untermenge der Befehle verfügbar. Dieser Level ist für Funktionen reserviert, die die Konsolenkonfiguration nicht verändern, und dient zum Zugriff auf Konfigurations-Subsysteme, wie das CLI. Zum Zugang zum nächsten Level, dem Privileged EXEC-Modus, ist ein Kennwort erforderlich (falls konfiguriert).

Der privilegierte EXEC-Modus ermöglicht Zugriff auf die globale Gerätekonfiguration. Für spezifische globale Konfigurationsoperationen innerhalb des Geräts müssen Sie den nächsten Level, den globalen Konfigurationsmodus, aufrufen. Ein Kennwort ist nicht erforderlich.

Der globale Konfigurationsmodus dient zur Verwaltung der Gerätekonfiguration auf globaler Ebene.

Der Schnittstellenkonfigurationsmodus dient zur Konfiguration des Geräts auf der physikalischen Schnittstellenebene. Bei Schnittstellenbefehlen, die Unterbefehle erfordern, gibt es oft einen weiteren Level, der Unterschnittstellen-Konfigurationsmodus (Subinterface Configuration) genannt wird. Ein Kennwort ist nicht erforderlich.

User EXEC-Modus

Nach Anmeldung am Gerät ist der EXEC-Befehlsmodus aktiviert. Die Benutzerlevel-Eingabeaufforderung besteht aus dem Hostnamen, gefolgt von einer spitzen Klammer (>). Zum Beispiel:

```
Console>
```

ANMERKUNG: Der Standard-Hostname ist die Konsole, außer wenn das in der Erstkonfiguration verändert wurde.

Die User EXEC-Befehle ermöglichen die Verbindungsaufnahme mit Remote-Geräten, vorübergehende Änderung von Terminal-Einstellungen, Ausführung von einfachen Tests und Auflistung von Systeminformationen.

Zur Auflistung der User EXEC-Befehle geben Sie ein Fragezeichen an der Eingabeaufforderung ein.

Privilegierter EXEC-Modus

Um unbefugten Zugriff zu verhindern und die Betriebsparameter zu sichern, kann der privilegierte Zugriff geschützt werden. Die Kennwörter werden auf dem Bildschirm angezeigt und berücksichtigen Groß- und Kleinschreibung.

Zugriff und Auflistung der Befehle im privilegierten EXEC-Modus:

1. Geben Sie an der Eingabeaufforderung `enable` (aktivieren) ein und drücken Sie die <Eingabetaste>.
2. Geben Sie bei Erscheinen der Kennwort-Eingabeaufforderung das Kennwort ein und drücken Sie die <Eingabetaste>.

Daraufhin erscheint die Eingabeaufforderung des privilegierten EXEC-Modus als Gerät-Hostname, gefolgt von `#`. Zum Beispiel:

```
Console#
```

Um die Befehle des privilegierten EXEC-Modus aufzulisten, geben Sie ein Fragezeichen an der Eingabeaufforderung ein drücken die <Eingabetaste>.

Zur Rückkehr vom privilegierten EXEC-Modus zum User EXEC-Modus können Sie einen der folgenden Befehle verwenden: `disable`, `exit/end`, or <Ctrl><Z>.

Das folgende Beispiel veranschaulicht den Zugriff auf den privilegierten EXEC-Modus und Rückkehr zum User EXEC-Modus:

```
Console>enable

Enter Password: ******

Console#

Console#disable

Console>
```

Der Befehl **exit** dient zur Rückkehr zu einem vorherigen Modus. Beispielsweise können Sie vom Interface Configuration Mode

(Schnittstellenkonfigurationsmodus) zum Global Configuration Mode (Globaler Konfigurationsmodus) und vom Global Configuration Mode (Globaler Konfigurationsmodus) zum Privileged EXEC Mode (Priviligierter EXEC-Modus) wechseln.

Globaler Konfigurationsmodus

Die Befehle im globalen Konfigurationsmodus gelten für Systemfunktionen, und nicht für bestimmte Protokolle oder Schnittstellen.

Zum Zugriff auf den globalen Konfigurationsmodus geben Sie an der Eingabeaufforderung im privilegierten EXEC-Modus `configure` (konfigurieren) ein und drücken dann die <Eingabetaste>. Der globale Konfigurationsmodus wird als Gerät-Hostname, gefolgt von (config) und #, angezeigt.

```
Console (config)#
```

Zur Auflistung der Befehle im globalen Konfigurationsmodus geben Sie ein Fragezeichen an der Eingabeaufforderung ein.

Zur Rückkehr vom globalen Konfigurationsmodus zum privilegierten EXEC-Modus geben Sie den Befehl `exit` ein oder verwenden den Befehl <Ctrl><Z>.

Das folgende Beispiel illustriert den Zugriff auf den globalen Konfigurationsmodus und Rückkehr zum privilegierten EXEC-Modus:

```
Console#

Console# configure

Console (config)# exit

Console#
```

Schnittstellen-Konfigurations-Modus

Schnittstellenkonfigurationsbefehle ändern bestimmte IP-Schnitttsellen-Einstellungen einschließlich Bridge-Gruppe, Beschreibung usw. Die Interface Configuration Modes (Schnittstellenkonfigurationsmodi) lauten wie folgt:

- **VLAN** – Enthält Befehle für das Erstellen und Konfigurieren von VLANs als Ganzes, beispielsweise für das Erstellen eines VLAN und die Zuweisung einer IP-Adresse für dieses VLAN.
- **Port Channel** (Portkanal) – Beinhaltet Befehle für das Konfigurieren von Link Aggregation Groups (LAG).
- **IP** – Enthält Befehle für die Steuerung von IP-Schnittstellen.
- **Out-of-Band-Ethernet** (OOB-Ethernet) – Enthält Befehle für das Steuern und Konfigurieren der Verwaltungsverbindungen.

CLI-Beispiele

CLI-Befehle werden hier als Konfigurationsbeispiele angeführt. Eine vollständige Beschreibung der CLI-Befehle einschließlich Beispiele finden Sie im CLI-Referenzhandbuch Ihres Switch.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Beschreibung der Hardware

Dell™ PowerConnect™ 6024/6024F Systeme

Dieser Abschnitt enthält Informationen über Geräteeigenschaften und Hardwarekonfigurationen des Moduls.

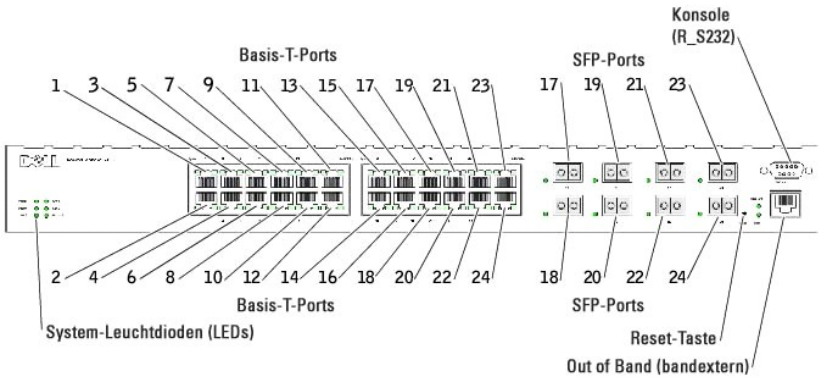
Beschreibung der Ports

PowerConnect 6024

Die Ports 1-16 werden als 10/100/1000-Ports bezeichnet und die Ports 17-24 als Kombi-Ports. Die Portnummern sind in der unteren Abbildung dargestellt.

Ein Kombi-Port ist ein logischer Port mit zwei physischen Anschlüssen – ein RJ-45- und ein SFP-Anschluss. Wird ein Stecker in den SFP-Port gesteckt, ist der SFP-Port aktiv, es sei denn, der Kupferstecker des Base-T-Ports der gleichen Nummer ist eingesteckt und hat eine Verbindung.

Abbildung 2-1. PowerConnect 6024 mit 24 10/100/1000 Base-T-Ports



Der Switch erkennt automatisch den Unterschied zwischen gekreuzten und 1:1 Kabeln auf den RJ-45-Ports. SFP-Ports unterstützen sowohl SX- als auch LX-Module.

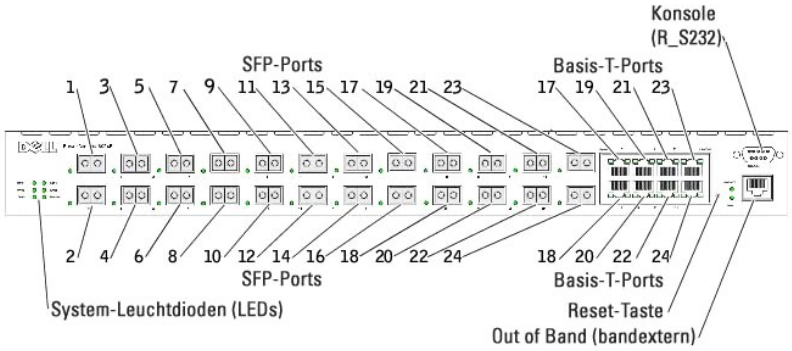
RJ-45-Ports unterstützen den Halb- und Vollduplexmodus 10/100/1000 Mbit/s.

PowerConnect 6024F

Die PowerConnect 6024F-Ports unterscheiden sich vom PowerConnect 6024 lediglich durch ihre Portbezeichnung: Die Ports -16 werden als SFP-Ports bezeichnet und die Ports 17-24 als Kombi-Ports. Die Portnummern sind in der unteren Abbildung dargestellt

Informationen über die Funktionsweise der Ports finden Sie in der Portbeschreibung des PowerConnect 6024.

Abbildung 2-2. PowerConnect 6024F mit 24 SFP-Ports



Out of Band-Management-Port

Der Out of Band (OOB)-Management-Port ist ein 10/100 Mbit/s-Ethernet-Port, den Sie direkt mit dem Switch verbinden können, um Systemadministrator- und Verwaltungsanwendungen durchzuführen. Der OOB-Port wird als reguläre IP-Schnittstelle des Systems betrachtet und alle Management-Schnittstellen sind über diese Port verfügbar.

Weitere Informationen über die OBB-Konfiguration finden Sie unter „Out of Band-Management-Port".

RS-232-Konsolen-Port

Der Konsolenport (RS-232) wird lediglich zur Steuerung über eine serielle Schnittstelle verwendet. Dieser Port ist direkt mit dem Switch verbunden und wird verwendet, um von einem Konsolenterminal, das mit einem EIA/TIA-232-Port verbunden ist, einen CLI-Zugang herzustellen.

Der Konsolenport unterstützt synchrone Daten von acht Datenbits, einem Stopbit und keinen Paritätsbit. Die Standardbaudrate beträgt 115.200.

Hardware-Komponenten

Abmessungen

Der Switch hat die folgenden Abmessungen:

- 440 x 460 x 44 mm (B x T x H).
- 17,32 x 18,11 x 1,73 Zoll (B x T x H).

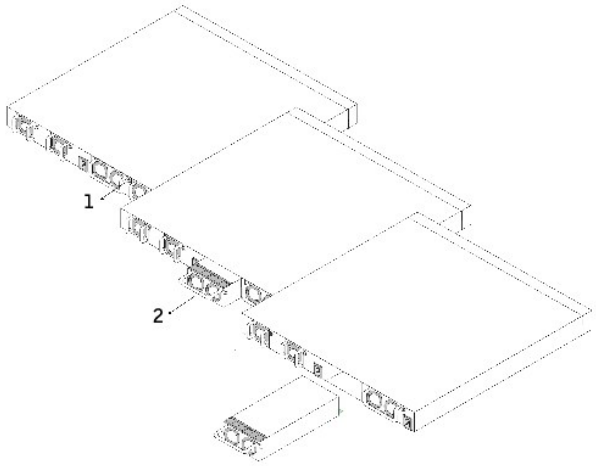
Netzteile

Ihr Switch wurde mit zwei internen Stromversorgungen geliefert. Sie können den Betrieb durch Beobachtung der Leuchtdioden überprüfen. Weitere Informationen finden Sie unter „System-LEDs".

So wechseln Sie eine Stromversorgung aus:

1. Entfernen Sie die fehlerhafte Stromversorgungseinheit, indem Sie diese, nach Entfernen der Schrauben auf der Rückseite, herausziehen.
2. Setzen Sie eine neue Stromversorgung in den Steckplatz ein und stellen Sie sicher, dass sich die Stromversorgung vollständig im Switch befindet.

Abbildung 2-3. Stromversorgung verbinden



3. Setzen Sie die Stromversorgung ein und ziehen Sie die Schraube fest.
4. Verbinden Sie jede Stromversorgung mit einer separaten externen Stromquelle.

Wenn Sie zwei unterschiedliche Stromquellen verwenden, ist das Risiko einer Störung am Switch bei einem Stromausfall geringer.

Reset-Taste

Die Reset-Taste, die sich auf der Frontblende befindet, dient zur manuellen Rücksetzung des Switch.

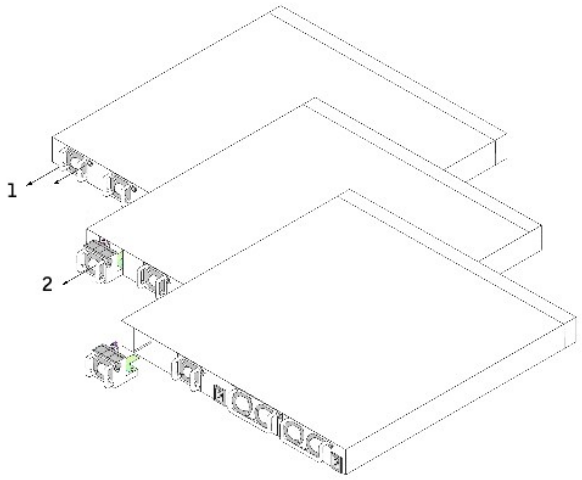
Belüftungssystem

Das System verfügt über zwei Lüfter. Sie können den Betrieb durch Beobachtung der Leuchtdioden überprüfen. Weitere Informationen finden Sie unter „System-LEDs".

So wechseln Sie einen Lüfter aus:

1. Entfernen Sie die beiden Schrauben und ziehen Sie den fehlerhaften Lüfter behutsam heraus.
2. Setzen Sie den neuen Lüfter vorsichtig in den Schlitz.

Abbildung 2-4. Lüfterinstallation/-auswechslung



3. Setzen Sie den Lüfter ein und ziehen Sie die Schraube fest.

LED-Definitionen

Auf der Frontblende befinden sich Leuchtdioden (LED), die den Status von Verbindungen, Stromversorgung, Lüftern und Systemdiagnose anzeigen.

LEDs am SFP-Port

Abbildung 2-5 zeigt die LEDs am SFP-Port, die sich neben dem jeweiligen SFP-Port befinden.

Abbildung 2-5. SFP-Port-LEDs

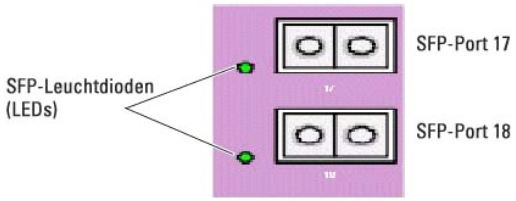


Tabelle 2-1 beinhaltet die Bedeutungen der LEDs des SFP-Ports:

Tabelle 2-1. beinhaltet die Bedeutungen der LEDs des SFP-Ports

LED	Farbe	Definition
SFP	Grün	Der Port ist gerade verbunden.
	Blinkt grün	Der Port sendet und/ oder empfängt gerade Netzwerkdatenverkehr.
	Aus	Der Port ist gerade nicht verbunden.

10/100/1000 Base-T-Port-LEDs

Jeder 10/100/1000 Base-T-Port hat zwei LEDs. Die Geschwindigkeits-LED befindet sich auf der linken Seite des Ports, während sich die Link/Duplex/Aktivitäts-LEDs auf der rechten Seite befinden. Die folgende Abbildung zeigt die LEDs des 10/100/100 Base-T-Ports:

Abbildung 2-6. LEDs des 10/100/1000 Base-T-Ports

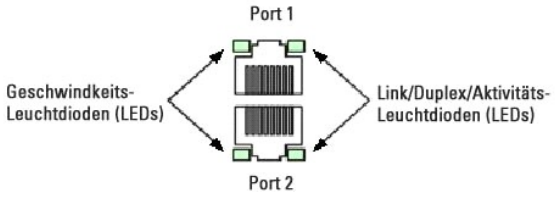


Tabelle 2-2 beinhaltet die Bedeutung der LEDs des 10/100/1000 Base-T-Ports.

Tabelle 2-2. Bedeutung des 10/100/1000 Base-T-Ports

LED	Farbe	Definition
Geschwindigkeit		
	Grün	Der Port arbeitet mit 1000 MBit/s.
	Gelb	Der Port arbeitet mit 100 MBit/s.
	Aus	Der arbeitet mit 10 MBit/s.
Zurück		
	Grün	Der Port läuft bei aktivem Vollduplexmodus.
	Blinkt grün	Der Port sendet oder empfängt Datenpakete und läuft im Vollduplexmodus.
	Gelb	Der Port läuft bei aktivem Halbduplexmodus.
	Blinkt gelb	Der Port sendet oder empfängt Datenpakete und läuft im Halbduplexmodus.
	Aus	Der Port ist nicht verbunden.

System-LEDs

Die System-LEDs, die sich links an der Frontblende befinden, liefern Informationen über die Stromversorgungen, Lüfter, Temperaturzustand und Diagnose.

Abbildung 2-7 stellt die LEDs des Systems dar.

Abb. 2-7. System-LEDs

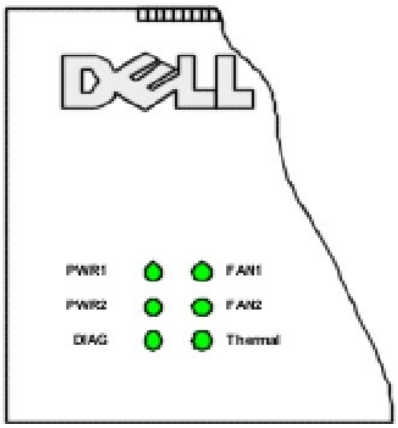


Tabelle 2-3 enthält die Bedeutungen der System-LEDs.

Tabelle 2-3. Bedeutungen der System-LEDs

LED	Farbe	Definition
Lüfter 1		
	Grün	Lüfter 1 ist vorhanden und arbeitet.
	Rot	Lüfter 1 ist vorhanden aber arbeitet nicht.
	Aus	Lüfter 1 ist nicht vorhanden.
Lüfter 2		
	Grün	Lüfter 2 ist vorhanden und arbeitet.
	Rot	Lüfter 2 ist vorhanden aber arbeitet nicht.
	Aus	Lüfter 2 ist nicht vorhanden.
PWR1		
	Grün	Stromversorgung 1 ist vorhanden und arbeitet.
	Rot	Stromversorgung 1 ist vorhanden aber arbeitet nicht.
	Aus	Stromversorgung 1 ist nicht vorhanden.
PWR2		
	Grün	Stromversorgung 2 ist vorhanden und arbeitet.
	Rot	Stromversorgung 2 ist vorhanden aber arbeitet nicht.
	Aus	Stromversorgung 2 ist nicht vorhanden.
Dia (Diagnose)		
	Blinkt grün	Ein Diagnosetest wird gerade durchgeführt.
	Grün	Der Diagnosetest wurde erfolgreich beendet.
	Rot	Der Diagnosetest ist fehlgeschlagen.
Thermal (Temperatur)		
	Rot	Das System hat die Maximaltemperatur überschritten.
	Aus	Die Systemtemperatur ist normal.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Einführung

Dell™ PowerConnect™ 6024/6024F Systeme

HINWEIS: Bevor Sie fortfahren, lesen Sie bitte die Versionshinweise für dieses Produkt. Die Versionshinweise stehen unter **support.dell.com** zum Download zur Verfügung.

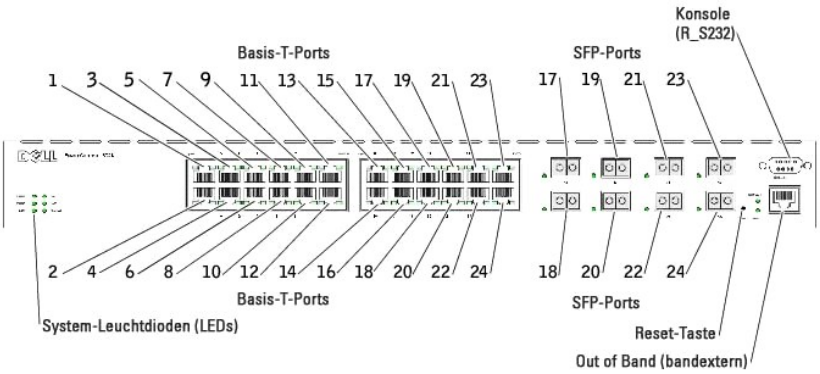
Der Dell™ PowerConnect™ 6024/6024F ist ein stand-alone Switch der Schicht 3, der die Produktreihe der Dell PowerConnect LAN-Switches erweitert. Der Switch umfasst folgende Ausstattungsmerkmale:

- 1U-Formfaktor, rack-montierbares Gehäuse.
- Out of Band-Management-Port für RJ-45- und RS-232-Verbindungen.
- Unterstützung aller Datenkommunikationsanforderungen an einen Multi-Schicht-Switch, einschließlich der vollen Funktionsbandbreite für Schicht 2, Schicht 3+, Sicherheit und Verwaltung.
- Hohe Verfügbarkeit durch Stromversorgungseinheiten und Kühlungslüfter, die während des Betriebs umgeschaltet werden können.

PowerConnect 6024

Der PowerConnect 6024 bietet 24 10/100/1000 Base-T RJ-45-Ports mit acht SFP-Kombiports, die über einen Auto-Sensor-Modus für Geschwindigkeit, Datenflusssteuerung und Duplex-Modus verfügen. SFP-Sender-Empfänger können separat erworben werden.

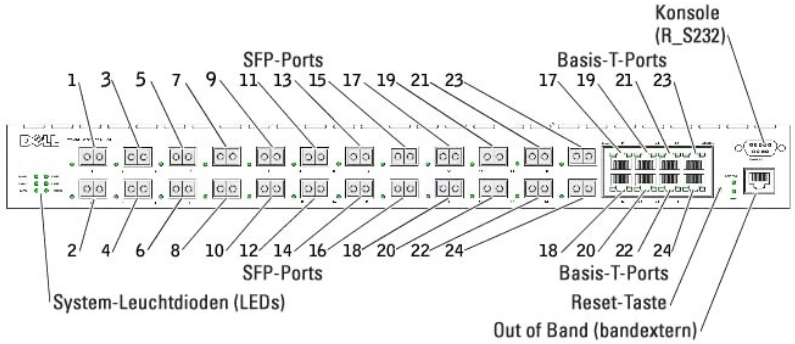
Abbildung 1-1. PowerConnect 6024



PowerConnect 6024F

Der PowerConnect 6024F bietet 24 SFP-Ports mit 8 10/100/1000 Base-T RJ-45-Kombiports, die über einen Auto-Sensor-Modus für Geschwindigkeit, Datenflusssteuerung und Duplex-Modus verfügen. SFP-Sender-Empfänger können separat erworben werden.

Abbildung 1-2. PowerConnect 6024F



CLI-Dokumentation

Das *CLI-Referenzhandbuch* enthält Informationen zu den CLI-Befehlen, die zum Konfigurieren des Switch verwendet werden. Das Dokument enthält CLI-Beschreibungen, Syntax und Standardwerte.

Funktionen

In diesem Abschnitt werden die vom Benutzer konfigurierbaren Switch-Funktionen beschrieben. Eine Liste aller Funktionen finden Sie in den Versionshinweisen zur Software.

Portbasierte Funktionen

Virtual Cable Testing (VCT)

VCT erkennt und meldet potenzielle Probleme an den Kupferverbindungskabeln, z. B. unterbrochene Stromkreise oder Kurzschlüsse.

Unterstützung für Jumbo-Frames

Die Verwendung von Jumbo-Frames ermöglicht den Transfer von identischen Daten in weniger Frames, was Aufwand und Verarbeitungszeit spart und zu einer Vermeidung von Unterbrechungen beiträgt.

Unterstützung für MDI/MDIX

Ihr Switch unterstützt die automatische Erkennung zwischen Kreuzkabeln und durchlaufenden Kabeln.

Die Standardverkabelung für Endstationen ist als MDI (Media Dependent Interface) und die Standardverkabelung für Hubs und Switches ist als MDIX (Media-Dependent Interface with Crossover) bekannt.

Informationen über das Konfigurieren von MDI/MDI für Ports oder LAGs finden Sie unter „Definieren der Portkonfiguration" oder „Definieren der LAG-Konfiguration".

Hardware-Watchdog-Unterstützung

Der Switch verwendet einen Hardware-Watchdog zur Problemerkennung und Problembehandlung, wenn die Software nicht mehr antwortet.

Automatische Verbindungsaushandlung (Auto-Negotiation)

Über Auto-Verhandlung wird das Gerät in die Lage versetzt, Operationsmodi mitzuteilen. Die Auto-Verhandlungsfunktion bietet die Mittel, um Informationen zwischen zwei Geräten auszutauschen, die ein Punkt-zu-Punkt-Verbindungselement gemeinsam benutzen, und beide Geräte automatisch zu konfigurieren, um die Übertragungskapazitäten optimal zu nutzen.

Der PowerConnect 6024/6024F erweitert die Auto-Verhandlung durch Portmitteilung. Portmitteilung ermöglicht es dem Systemadministrator, Portgeschwindigkeiten mitzuteilen.

Weitere Informationen über Auto-Verhandlung finden Sie unter „Definieren der Portkonfiguration" oder „Definieren der LAG-Konfiguration".

Unterstützung der Datenflusssteuerung (IEEE 802.3X)

Die Datenflusssteuerung ermöglicht Geräten mit geringerer Transferrate die Kommunikation mit schnelleren Geräten. Dies geschieht durch Anfragen an das schnellere Gerät, die Sendung von Paketen zurückzuhalten. Übertragungen werden vorübergehend unterbrochen, um Pufferüberläufe zu verhindern.

Weitere Informationen über das Konfigurieren von Datenflusssteuerung für Ports oder LAGs finden Sie unter „Definieren der Portkonfiguration" oder „Definieren der LAG-Konfiguration".

Verhindern einer Blockade des Leitungskopfes (Head of Line Blocking)

Head-of-Line (HOL)-Blocking verhindert Verzögerungen im Datenverkehr und Frame-Verlust, die durch ein Konkurrieren des Datenverkehrs um die gleichen Ausgangs-Port-Ressourcen verursacht werden. HOL-Blocking reiht Pakete in Warteschlangen ein und die Pakete am Kopf der Warteschlange werden vor denen am Ende der Warteschlange weitergeleitet.

Unterstützung für Backpressure

Auf Halbduplex-Verbindungen kann ein Receiver einen Überlauf des Zwischenspeichers verhindern, indem er die Verbindung besetzt, so dass sie für den weiteren Datenverkehr nicht verfügbar ist.

Weitere Informationen über das Konfigurieren von Back Pressure für Ports oder LAGs finden Sie unter „Definieren der Portkonfiguration" oder „Definieren der LAG-Konfiguration".

Von MAC-Adressen unterstützte Funktionen

MAC-Adress-Unterstützung

Der Switch unterstützt bis zu 16K MAC-Adressen und reserviert bestimmte MAC-Adressen für den systeminternen Bedarf.

Selbstlernende MAC-Adressen

Der Switch ermöglicht die automatische Erkennung von MAC-Adressen durch die eingehenden Pakete.

Automatische Alterung (Aging) für MAC-Adressen

MAC-Adressen, an denen für einen bestimmten Zeitraum kein Datenverkehr stattgefunden hat, veralten, so dass ein Überlaufen der Bridging-Tabelle vermieden wird.

Weitere Informationen über das Konfigurieren des Gültigkeitszeitraumes der MAC-Adresse finden Sie unter „Anzeigen von dynamischen Adressen".

Statische MAC-Einträge

Benutzerdefinierte MAC-Einträge werden zusammen mit der automatisch erkannten Adresse in der Bridging-Tabelle gespeichert.

Weitere Informationen über das Konfigurieren von statischen MAC-Adressen finden Sie unter „Definieren von statischen Adressen".

VLAN-aware MAC-basiertes Switching

Pakete, die von einer unbekannten Quelladresse stammen, werden an die CPU gesendet und der Hardware-Tabelle zugefügt. Die an oder von dieser Adresse gesendeten weiteren Pakete können dadurch effizienter weitergeleitet werden.

Unterstützung für MAC-Multicast

Der Multicast-Dienst ist ein eingeschränkter Broadcast-Dienst, der eine-zu-vielen und viele-zu-vielen Verbindungen ermöglicht. Bei Multicast-Diensten der Schicht 2 wird ein an eine bestimmte Multicast-Adresse adressierter Einzel-Frame empfangen, und an jedem zugehörigen Port werden Kopien des zu übertragenden Frames erstellt.

Weitere Informationen über das Konfigurieren der MAC-Multicast-Unterstützung finden Sie unter „Unterstützung von Multicast-Weiterleitung".

Layer-2-Funktionen

IGMP-Snooping

IGMP-Snooping untersucht den Inhalt von IGMP-Frames, wenn diese durch den Switch von Endstellen an einen vorgelagerten Multicast-Router weitergeleitet werden. Das Snooping ermöglicht es dem Switch, die an einer Multicast-Sitzung interessierten Endstellen zu identifizieren und festzustellen, welche Multicast-Router Multicast-Frames senden.

Weitere Informationen über das Konfigurieren des IGMP-Snooping finden Sie unter „IGMP-Snooping".

Port Mirroring (Portspiegelung)

Die Portspiegelung überwacht und spiegelt den Netzwerkverkehr, indem sie Kopien ein- und ausgehender Pakete von einem Port an einen Überwachungsport weiterleitet.

Weitere Informationen über das Konfigurieren von Portspiegelung finden Sie unter „Definieren von Portspiegelungssitzungen".

Broadcast-Sturmkontrolle

Bei der Weiterleitung von Frames der Schicht 2 werden Broadcast- und Multicast-Frames an alle Ports des entsprechenden VLAN geflutet. Das Fluten besetzt Bandbreite und lädt alle mit allen Ports verbundenen Knoten. Die Datensturmkontrolle begrenzt die Anzahl der Multicast- und Broadcast-Frames, die vom

Switch akzeptiert und weitergeleitet werden.

Weitere Informationen über das Konfigurieren der Datensturmkontrolle finden Sie unter „Aktivieren der Sturmkontrolle".

VLAN-unterstützte Funktionen

VLAN-Unterstützung

VLANs sind Sammlungen von Switchports, die eine einzige Broadcast-Domain umfassen. Pakete werden auf der Grundlage des VLAN-Tags oder einer Kombination der Eingangsport und des Paketinhalts als dem VLAN zugehörig klassifiziert. Pakete, die gemeinsame Attribute aufweisen, können Gruppen im selben VLAN sein.

Weitere Informationen über das Konfigurieren von VLANs finden Sie unter „Konfigurieren von VLANs".

Portbasierte VLANs

Portbasierte VLANs klassifizieren eingehende Pakete an VLANs aufgrund ihres Eingangsports.

Weitere Informationen über das Konfigurieren von VLANs finden Sie unter „Konfigurieren von VLANs".

IEEE802.1V-protokollbasierte VLANs

VLAN-Klassifizierungsregeln werden aufgrund einer Data-Link-Layer (Layer 2) Protokoll-Kennung definiert. Protokollbasierte VLANs werden zum Trennen des Datenverkehrs der Schicht 2 für unterschiedliche Protokolle der Schicht 3 verwendet.

Information zum Definieren von protokollbasierten VLANs finden Sie unter „Definieren von VLAN-Protokollgruppen".

Umfassende 802.1Q VLAN-Tagging-Konformität

IEEE 802.1Q definiert eine Architektur für virtuell überbrückte LANs, die in VLANs bereitgestellten Dienste und die bei der Bereitstellung dieser Dienste verwendeten Protokolle und Algorithmen.

Dieser Standard erfordert, dass Frames mit einem gewünschten Class-of- Service (CoS)-Kennungswert (0-7) markiert werden können.

GVRP-Unterstützung

GARP VLAN Registration Protocol (GVRP) stellt IEEE 802.1Q-konformes VLAN-Pruning und dynamische VLAN-Erstellung auf 802.1Q-Trunk-Ports bereit. Wenn GVRP aktiviert ist, registriert der Switch die VLAN-Mitgliedschaft und teilt diese an alle Ports mit, die Teil der aktiven unterliegenden Spanning Tree-Protokolltypologie sind.

Weitere Informationen über das Konfigurieren von GVRP finden Sie unter „Konfigurieren von GVRP".

Privates VLAN-Edge

Bei Private VLAN-Edge-Ports (PVE) handelt es sich um eine Sicherheitsfunktion der Schicht 2, die portbasierte Sicherheit zwischen benachbarten Ports innerhalb eines VLANs bietet. Es handelt sich dabei um eine Erweiterung des allgemeinen VLANs. Datenverkehr von geschützten Ports wird nur an die Uplink-

Ports gesendet und kann nicht an andere Ports innerhalb des VLANs gesendet werden.

Weitere Informationen über das Konfigurieren von PVE-Ports finden Sie unter „Konfigurieren von Ports".

Merkmale des Spanning Tree-Protokolls (STP)

Spanning Tree-Protokoll (STP) pro Gerät

802.1d STP ist eine standardmäßige Layer-2-Switch-Anforderung, die es Brücken ermöglicht, automatisch L2-Weiterleitungsschleifen zu verhindern und aufzulösen. Switches tauschen Konfigurationsmeldungen mithilfe speziell formatierter Frames aus und aktivieren oder deaktivieren wahlweise die Weiterleitung an Ports.

Weitere Informationen über das Konfigurieren von STP finden Sie unter „Konfigurieren des Spanning Tree Protocol".

Fast Link

STP braucht zum Konvergieren unter Umständen bis zu 30-60 Sekunden, da dieses Protokoll mögliche Schleifen erkennt und Zeit für die Umsetzung von Statusänderungen und für die Antworten der entsprechenden Geräte vorhält. Für viele Anwendungen ist diese Zeitdauer zu lang. Fast Link deaktiviert diese Zeitverzögerung, ohne dass mehrere Datenpfade für die Netzwerkelastizität erforderlich wären.

Informationen über das Aktivieren von Fast Link für Ports und LAGs finden Sie unter „Definieren der Portkonfiguration" oder „Definieren der LAG-Konfiguration".

IEEE 802.1w Rapid Spanning Tree

Das Rapid Spanning Tree Protocol (RSTP) verwendet Netzwerktopologien, um eine schnellere Konvergenz zu ermöglichen, ohne dass Weiterleitungsschleifen erstellt werden müssen.

Informationen über das Aktivieren von RSTP finden Sie unter „Definieren des Rapid Spanning Tree".

Mehrfacher Spanning Tree

Multiple Spanning Tree-Operationen (MSTP) verbinden VLANs mit ST-Instanzen. MSTP ermöglicht ein anderes Ladeausgleichsszenario. Pakete, die verschiedenen VLANs zugeordnet sind, werden auf unterschiedlichen Pfaden innerhalb der MSTP-Regionen (MST Regions) weitergeleitet. Unter einer Region versteht man eine oder mehrere miteinander verbundene MSTP-Brücken mit identischen MSTP-Einstellungen. Über den Standard können Administratoren VLAN-Datenverkehr auf eindeutigen Pfaden zuordnen.

Weitere Informationen über MSTP finden Sie unter „Definieren des Multiple Spanning Tree".

Link-Aggregation

Link-Aggregation

Bis zu sieben Ports können zu einer sogenannten Link Aggregated Group (LAG) zusammengefasst werden. Dies ermöglicht Schutz vor Fehlertoleranzen bedingt durch Störungen der physischen Verbindung, höhere Bandbreiten-Verbindungen und verbesserte Bandbreitengranularität.

LAG besteht aus Ports mit der gleichen Geschwindigkeit, die auf Vollduplex-Betrieb eingestellt sind.

Weitere Informationen über das Konfigurieren von LAGs finden Sie unter „Definieren der LAG-Konfiguration".

Link Aggregation und LACP

LACP verwendet Peer-Exchanges, d. h. Kontaktnahmen untereinander, über Verknüpfungen zur ständigen Feststellung der Aggregationskapazität der verschiedenen Links und stellt kontinuierlich die höchste Aggregationskapazität, die zwischen einem gegebenen Paar von Systemen erzielt werden kann, bereit. LACP bestimmt, konfiguriert, bindet und überwacht automatisch die Bindungsports an Aggregatoren innerhalb des Systems.

Informationen zu LACP finden Sie unter „Definieren von LACP-Parametern".

Routing-Funktionen

IP-Routing

IP-Routing leitet Pakete, die an die System-MAC-Adresse, nicht jedoch an eine System-IP-Adresse adressiert sind, an ein Gerät der nächsten Teilstrecke weiter.

Weitere Informationen über das Konfigurieren von IP-Routing finden Sie unter „Konfigurieren von globalem IP-Routing".

RIP-Versionen 1 und 2

RIP ist ein Routingprotokoll auf Basis von Distanzvektoren. RIP wählt Routen auf der Grundlage der Anzahl der Hops zum nächsten Zielort aus. RIP 2 erweitert die Effizienz, Nutzbarkeit und Authentifizierungsmethoden des RIP-Protokolls.

Weitere Informationen über das Konfigurieren von RIP finden Sie unter „Konfigurieren von RIP".

OSPF Version 2

Open Shortest Path First (OSPF, Kürzesten Pfad zuerst öffnen) ist ein internes Gateway-Routingprotokoll. In Netzwerken mit einer großen Anzahl von miteinander verbundenen Routern arbeitet OSPF effizienter als RIP, weil OSPF weniger Verbindungsbandbreite verwendet und schneller konvergiert.

Weitere Informationen über das Konfigurieren von OSPF finden Sie unter „Konfigurieren von Parametern und Filtern für OSPF".

Address Resolution Protocol (ARP)

Beim IP-Routing verwenden Router und Switches der Schicht 3 verschiedene Routingprotokolle, um die Netzwerktopologie zu ermitteln und Routing-Tabellen zu definieren. ARP ermittelt automatisch die Device Next-Hop MAC-Adressen von Systemen, einschließlich direkt verbundene Endsysteme. Benutzer können dies überschreiben und ergänzen, indem sie zusätzliche ARP-Tabelleneinträge erstellen.

Weitere Informationen über das Konfigurieren von ARP finden Sie unter „Definieren von ARP-Einstellungen".

ICMP-Meldungen

Meldungen des Internet Control Message Protocol (ICMP - Internet-Kontrollmeldungsprotokoll) werden für bandexterne Meldungen verwendet, die sich auf den Netzwerkbetrieb oder Fehlfunktionen des Netzwerks beziehen.

IGMPv2

IGMP ermöglicht es dem Router, IGMP-Anfragen in Form von L2-Broadcasts über jede Schnittstelle zu senden. Wenn ein Multicast-Paket an eine Multicast-MAC-Zieladresse gesendet wird, erhalten alle Hosts auf dieser Router-Schnittstelle eine Kopie. Hosts empfangen alle IGMP-Reports. Wenn interessierte Multicast-Gruppen bereits von einer Endstelle auf derselben Schnittstelle angefragt wurden, senden die verbleibenden Endstellen keine doppelten Anfragen.

Weitere Informationen über das Konfigurieren von IGMP finden Sie unter „Definieren von IGMP-Schnittstellenparametern".

Unterstützung der Übereinstimmung des längsten Präfix

Übereinstimmungen des längsten Präfix werden in erster Linie zur Bestimmung der besten nächsten Teilstrecke für ein Paket auf der alleinigen Grundlage der im Paketkopf enthaltenen Zieladresse verwendet. Da IP-Adressen im Allgemeinen unter Berücksichtigung der Netzwerktopologie zugewiesen werden, besteht das Ergebnis der Übereinstimmung des längsten Präfix in der Regel darin, dass die kürzeste Route zum Zielort bestimmt wird.

DVMRP

Das Distance Vector Multicast Routing Protocol (VMRP - Abstandsvektor-Multicast-Routing-Protokoll) teilt die kürzesten Routen zu Multicast-Quellnetzwerken mit Hosts mit, welche Multicast-IP-Datenverkehr übertragen können.

Weitere Informationen über das Konfigurieren von DVMRP finden Sie unter „Konfigurieren von DVMRP-Schnittstellen".

VRRP

Das Virtual Router Redundancy Protocol (VRRP - Protokoll für virtuelle Router-Redundanz) schließt Einzel-Fehlerpunkte in der Routing-Umgebung aus. VRRP verwendet ein Auswahlprotokoll, das die Verantwortung für den virtuellen Router dynamisch einem der VRRP-Router im LAN zuweist.

Der Auswahlvorgang bietet dynamisches Failover bei der Weiterleitung von Verantwortung, wenn der Master nicht verfügbar ist. Jede IP-Adresse des virtuellen Routers kann von End-Hosts als Standard-Router der ersten Teilstrecke verwendet werden.

Weitere Informationen über das Konfigurieren von VRRP finden Sie unter „Konfigurieren von VRRP".

Layer-3-Funktionen

TCP (Übertragungssteuerungsprotokoll)

Transport Control Protocol (TCP)-Verbindungen werden zwischen 2 Ports durch einen anfänglichen Synchronisationsaustausch definiert. TCP-Ports werden durch eine IP-Adresse und eine 16-Bit-Portnummer identifiziert. Oktettströme werden in TCP-Pakete unterteilt, die jeweils eine Sequenznummer haben.

UDP-Relais

UDP Relay ermöglicht es dem Gerät, bestimmte UDP-Broadcasts von einer Schnittstelle zur nächsten weiterzuleiten. IP-Broadcast-Pakete werden im Allgemeinen nicht von einer Schnittstelle an die nächste weitergeleitet. Bestimmte Anwendungen verwenden UDP-Broadcast jedoch, um die Verfügbarkeit eines Dienstes zu prüfen. Für andere Dienste ist es erforderlich, dass UDP-Broadcast-Pakete geroutet werden, um Clients auf einem anderen Subnetz Dienste bereitstellen zu können.

BootP und DHCP Clients

DHCP aktiviert zusätzliche Setup-Parameter, die von einem Netzwerkserver beim Systemstart empfangen werden. DHCP-Service ist ein ständiger Prozess.

DHCP ist eine Erweiterung von BootP.

Informationen über DHCP finden Sie unter „Definieren von DHCP-IP-Schnittstellenparametern".

BootP Relay

BootP ermöglicht es einem Gerät, Konfigurationsdaten von Servern anzufragen und zu empfangen. Ist der gewünschte BootP-Server nicht direkt an die Broadcast-Domäne des Clients angeschlossen, so ermöglicht ein BootP Relay-Dienst das Erreichen des Servers durch den Client.

von DHCP-Relais

DHCP ermöglicht es einem Gerät, Konfigurationsdaten von Servern anzufragen und zu empfangen. Ist der gewünschte DHCP-Server nicht direkt an die Broadcast-Domäne des Clients angeschlossen, so ermöglicht ein DHCP Relay-Dienst das Erreichen des Servers durch den Client.

Weitere Informationen über das Konfigurieren von DHCP-Relay-Parametern finden Sie unter „Definieren von DHCP-Relais-Parametern".

Quality of Service(Diensteigenschaften)-Merkmale

Unterstützung von Quality of Service (QoS)

Zur Bewältigung unvorhergesehenen Netzwerk-Datenverkehrs und zur Leistungsoptimierung können Sie im gesamten Netzwerk den Quality-of-Service (QoS) anwenden, um sicherzustellen, dass der Netzwerk-Datenverkehr gemäß bestimmten Kriterien priorisiert wird. Ihr Switch unterstützt zwei QoS-Betriebsarten: Einfache QoS und erweiterte QoS.

Unterstützung für Class Of Service 802.1p

Die IEEE 802.1p-Signalisierungstechnik ist ein OSI-Standard der Schicht 2 und wird zum Taggen und Priorisieren von Netzwerk-Datenverkehr auf der Datenverbindung-/MAC-Subschicht verwendet. Der 802.1p-Datenverkehr wird klassifiziert und an den Zielort gesendet; es erfolgt keine Bandbreitenreservierung oder Einrichtung von Limits. Der 802.1p-Standard richtet acht Prioritätsstufen ein, ähnlich dem IP-Präzedenz IP-Header Bit-Feld.

Einfache Quality of Service-Modus (QoS)

Im einfachen QoS-Modus kann ein Trustmodus (Vertrauen gegenüber VPT, DSCP, TCP/UDP oder keines) aktiviert werden. Darüber hinaus kann einer Schnittstelle eine einzelne Zugangskontrollliste beigefügt werden.

Informationen über die Aktivierung des einfachen QoS-Modus finden Sie unter „Konfigurieren des einfachen QoS-Modus".

Erweiterter Quality of Service-Modus

Der erweiterte Quality-of-Service-Modus legt die Flussklassifizierung fest und weist Aktionsregeln zu, die sich auf das Bandbreitenmanagement beziehen. Diese Regeln können gruppenweise zusammengefasst und auf eine Schnittstelle angewandt werden.

Informationen zum Aktivieren des erweiterten QoS-Modus finden Sie unter „Konfigurieren des erweiterten QoS-Modus".

Geräteverwaltungsfunktionen

SNMP-Alarme und Trap-Protokolle

Das System protokolliert Ereignisse mit Schwerecodes und Zeitstempeln. Die Ereignisse werden als SNMP-Traps an eine Trap-Empfängerliste gesendet.

Informationen über SNMP-Alarme und Traps finden Sie unter „Definieren von SNMP-Parametern".

Web-basiertes Management

Sie können das System mit jedem Web-Browser verwalten. Der Switch umfasst einen eingebetteten Web-Server, der HTML-Seiten bereitstellt, die Sie zum Überwachen und Konfigurieren des Systems verwenden können.

Herunterladen der Konfigurationsdatei

Die Konfigurationsdatei des Switch enthält systemweite und Port-spezifische Gerätekonfigurationsdaten. Sie können Konfigurationsdateien mithilfe von CLI-Befehlen anzeigen.

Informationen über das Herunterladen von Konfigurationsdateien finden Sie unter „Herunterladen von Dateien".

Software Download (Software-Download)

Der Software-Download ermöglicht das Speichern von Sicherungskopien der Firmware-Images. Informationen über das Herunterladen der Software finden Sie unter „Herunterladen der Software und Neustart".

Trivial File Transfer Protocol (TFTP)

PowerConnect 6024/6024F unterstützt das Laden und Herunterladen von Boot-Abbild, Firmware und Konfiguration über TFTP.

Remote Monitoring (Fernüberwachung)

Remote-Überwachung (RMON) ist eine Erweiterung zum SNMP und bietet umfassende Überwachungsmöglichkeiten für den *Netzwerk-Datenverkehr* (im Unterschied zu SNMP, welches *Geräte*-Management und -überwachung über das Netzwerk ermöglicht). RMON ist eine Standard-MIB, die aktuelle und historische MAC-Layer-Statistiken und Kontrollobjekte definiert und somit die Erfassung von Echtzeitinformationen über das gesamte Netzwerk ermöglicht.

Informationen über RMON finden Sie unter „Anzeigen der RMON-Statistik".

Simple Network Management Protocol (SNMP, Einfaches Netzwerkverwaltungsprotokoll (SNMP) Versionen 1, 2 und 3)

Zur Systemzugriffskontrolle wird eine Liste von Community-Einträgen definiert, die jede aus einer Community-Zeichenfolge und deren Zugriffsprivilegien bestehen. Es gibt drei SNMP-Sicherheitsstufen – Nur-Lese, Lesen-Schreiben und Super. Nur ein Super-User kann auf die eigentliche Community-Tabelle zugreifen.

Befehlszeilen-Schnittstelle

Die CLI (Command Line Interface)-Syntax und Semantik entsprechen so weit wie möglich der allgemeinen Industriepraxis. CLI besteht aus obligatorischen und

optionalen Elementen. Die kontextsensitive Hilfe bietet Format- und Wertebereiche, die für die aktuellen Befehle zulässig sind, der CLI-Interpreter bietet die automatische Vervollständigung von Befehlen und Stichwörtern.

Syslog

Syslog ist ein Protokoll, das die Versendung von Ereignismeldungen an eine Gruppe von Remote-Servern ermöglicht. Die Meldungen können dann auf den Servern gespeichert, untersucht und weiterverarbeitet werden.

Informationen über Syslog finden Sie unter „Verwalten von Protokollen".

SNTP

Das Simple Network Time Protocol (SNTP) stellt eine präzise Zeitsynchronisation der Netzwerkswitche bis auf die Millisekunde sicher. Die zeitliche Synchronisierung wird von einem Netzwerk-SNTP-Server ausgeführt.

Weitere Informationen über SNTP finden Sie unter „Konfigurieren von SNTP-Einstellungen".

Traceroute

Traceroute ermöglicht die Auffindung von IP-Routes, auf denen Datenpakete während des Weiterleitungsprozesses weitergeleitet wurden. Das CLI-Traceroute-Dienstprogramm kann vom User EXEC- oder vom privilegierten EXEC-Modus ausgeführt werden.

Unterstützung für bandexternen Management-Port

Ein bandexterner Management-Port ist ein externer Ethernet-Port, die nur Datenverkehr zwischen dem Systemadministrator und den Verwaltungsanwendungen trägt. Der bandexterne Management-Port bietet eine physisch gesicherte Verbindung sowie Fehlertoleranz.

Sicherheitsfunktionen

Zugriffssteuerungsliste (ACL)

Die ACL (Zugriffssteuerungsliste) bietet Regeln für das Weiterleiten bzw. Blockieren von Netzwerk-Datenverkehr. Sie können ACLs definieren, um Sicherheitserweiterungen durchzusetzen, indem Sie Klassifizierungsregeln definieren und den Regeln Aktionen zuweisen. Sie können eine ACL einer Eintritts-Schnittstelle (Port oder VLAN) zuweisen.

Informationen über das Definieren von ACLs finden Sie unter „Definieren von IP-basierten ACLs" und unter „Definieren von MAC-basierten ACLs".

Portbasierte Authentifizierung (802.1x)

Portbasierte Authentifizierung ermöglicht die Authentifizierung von Systembenutzern auf Portbasis über einen externen Server. Nur authentifizierte und genehmigte Systembenutzer können Daten übertragen und empfangen. Ports werden über den RADIUS (Remote Authentication Dial In User Service)-Server unter Einsatz des Extensible Authentication-Protokolls (EAP) authentifiziert.

Weitere Informationen finden Sie unter „Konfigurieren der portbasierten Authentifizierung".

Unterstützung von gesperrten Ports

Die Port-Sperre beschränkt den Zugang von Benutzern mit bestimmten MAC-Adressen auf nur einen Port. Diese Adressen werden manuell auf diesem Port definiert oder „erlernt". Wenn ein Frame auf einem gesperrten Port festgestellt wird und die MAC-Adresse der Frame-Quelle nicht mit dem Port verknüpft ist, wird der Schutzmechanismus aufgerufen.

Informationen über die Aktivierung der Port-Sperre finden Sie unter „Konfigurieren der Portsicherheit".

Kennwort-Managementsicherheit

Die Kennwortverwaltung bietet verbesserte Netzwerksicherheit und Kennwortkontrolle. Kennwörter für den Zugang zu SSH, Telnet, HTTP, HTTPS und SNMP unterliegen Sicherheitsfunktionen.

Weitere Informationen über Kennwortverwaltung finden Sie unter „Verwalten von Kennwörtern".

TACACS+

TACACS+ gewährleistet zentralisierte Sicherheit bei der Validierung von Benutzern beim Zugang zum Switch. TACACS+ stellt ein zentralisiertes Benutzerverwaltungssystem dar, das jedoch mit RADIUS und anderen Authentifizierungsprozessen konform ist.

Informationen über das Definieren von TACACS+-Einstellungen finden Sie unter „Konfigurieren von bandexternen TACACS+-Servern" und unter „Konfigurieren von TACACS+-Einstellungen".

RADIUS-Client

RADIUS ist ein Client-/Server-basiertes Protokoll, bei dem der Server eine Benutzerdatenbank führt, die Authentifizierungsangaben wie Benutzername, Kennwort und Kontoangaben über jeden einzelnen Benutzer enthält.

Informationen über das Definieren von RADIUS-Einstellungen finden Sie unter „Konfigurieren von RADIUS-Einstellungen".

SSH

Secure Shell (SSH) ist ein Protokoll, das eine sichere Remote-Verbindung zu ein Gerät ermöglicht. Die von dieser Verbindung gelieferte Funktionalität ähnelt der einer eingehenden Telnet-Verbindung.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Dell™ PowerConnect™ 6024/6024F Systeme

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

HINWEIS: Ein HINWEIS weist auf mögliche Schäden an der Hardware oder auf möglichen Datenverlust hin und beschreibt Ihnen, wie Sie dieses Problem vermeiden können.

VORSICHT: VORSICHT weist auf Gefahren hin, die zu Sachschäden, Personenschäden oder lebensgefährlichen Verletzungen führen können.

Januar 2005

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Anzeigen von Statistiken:

Dell PowerConnect 6024/6024F Systeme

Dieser Abschnitt enthält statistische Angaben über die Schnittstellen-, GVRP-, Etherlike-, RMON- und die Gerätenutzung.

ANMERKUNG: Für keine der Statistikseiten stehen CLI-Befehle zur Verfügung.

Anzeigen von Tabellen

Die Seite **Table Views** (Tabellenansichten) enthält Verknüpfungen zur Anzeige von Statistiken in Diagrammform.

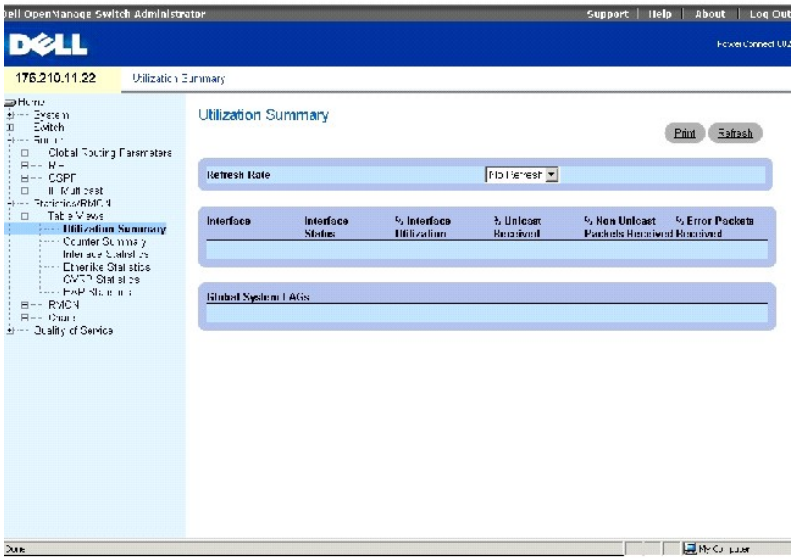
Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Statistics/RMON→ Table Views**.

Anzeigen der Nutzungsübersicht

Die Seite **Utilization Summary** (Nutzungsübersicht) umfasst Statistiken für die Schnittstellennutzung.

Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Statistics/RMON→ Table Views→ Utilization Summary**.

Abbildung 9-1. Nutzungsübersicht



Die Seite **Zusammenfassung der Nutzung** enthält die folgenden Felder:

Refresh Rate (Aktualisierungsrate) Zeit, die vergeht, bevor die Statistik aktualisiert wird. Die möglichen Feldwerte sind No Refresh (Keine Aktualisierung), 15, 30 und 60 Sekunden.

Interface Die Nummer der Schnittstelle.

Interface Status Status der Schnittstelle.

% Interface Utilization Prozentuale Netzwerkschnittstellen-Nutzung, basierend auf Duplexbetrieb der Schnittstelle. Der Bereich für diesen Wert ist von 0 bis 200 %. Der maximale Wert von 200 % für eine Vollduplexverbindung zeigt an, dass 100 % der Bandbreite von Eingangs- und Ausgangsverbindungen von Datenverkehr, der durch die Schnittstelle fließt, genutzt werden. Der maximale Wert für eine Halbduplexverbindung beträgt 100 %.

% Unicast Received Prozentsatz der Unicast-Pakete, die an der Schnittstelle erhalten wurden.

% Non Unicast Packets Received Prozentsatz der Nicht-Unicast-Pakete, die an dieser Schnittstelle erhalten wurden.

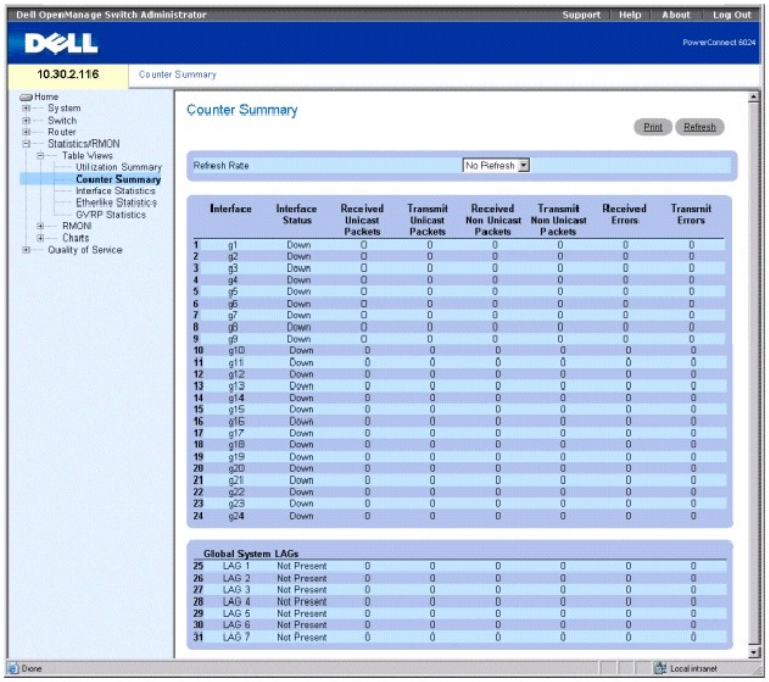
% Error Packets Received Anzahl der fehlerhaften Pakete, die an der Schnittstelle erhalten wurden.

Anzeigen der Zählerübersicht

Die Seite **Counter Summary** (Zählerübersicht) enthält Statistiken über die Portnutzung in nummerischen Summen im Gegensatz zu Prozentsätzen.

Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Statistics/RMON→ Table Views→ Counter Summary**.

Abbildung 9-2. Zählerzusammenfassung



Refresh Rate (Aktualisierungsrate) Zeit, die vergeht, bevor die Statistik aktualisiert wird. Die möglichen Feldwerte sind No Refresh (Keine Aktualisierung), 15, 30 und 60 Sekunden.

Interface Die Nummer der Schnittstelle.

Interface Status Status der Schnittstelle.

Received Unicast Packets Anzahl der Unicast-Pakete, die an dieser Schnittstelle erhalten wurden.

Transmit Unicast Packets Anzahl der von der Schnittstelle übertragenen Unicast-Pakete.

Received non-Unicast Packets Received Anzahl der Nicht-Unicast-Pakete, die an dieser Schnittstelle erhalten wurden.

Transmit non-Unicast Packets Anzahl der von der Schnittstelle übertragenen Nicht-Unicast-Pakete.

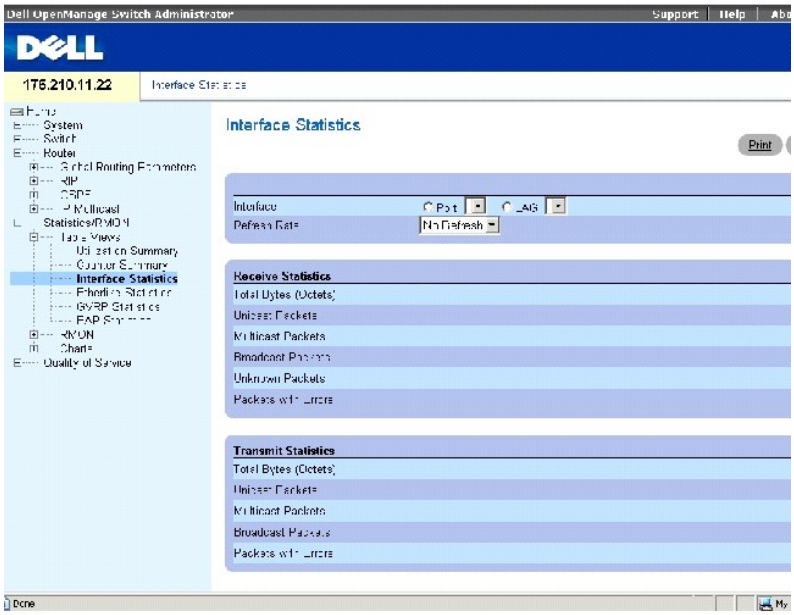
Received Errors (Eingegangene Fehler) Anzahl der an der Schnittstelle eingegangenen Fehler.

Transmit Errors (Übertragenen Fehler) Anzahl der von der Schnittstelle übertragenen Fehler.

Anzeigen der Schnittstellenstatistik

Die Seite **Interface Statistics** (SchnittstellenstatistikI) enthält Statistiken für die erhaltenen und übertragenen Datenpakete. Die Felder für empfangene und übertragene Pakete sind identisch. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Statistics/RMON→ Table Views→ Interface Statistics**.

Abbildung 9-3. Schnittstellenstatistik



Interface Gibt an, ob Statistiken für einen Port oder LAG angezeigt werden.

Refresh Rate (Aktualisierungsrate) Zeit, die vergeht, bevor die Statistik aktualisiert wird. Die möglichen Feldwerte sind No Refresh (Keine Aktualisierung), 15, 30 und 60 Sekunden.

Empfangsstatistik

Total Bytes (Octets) (Gesamtzahl Bytes (Oktetts) Die auf der ausgewählten Schnittstelle empfangene Oktettmenge.

Unicast Packets (Unicast-Pakete) Die auf der ausgewählten Schnittstelle empfangene Menge der Unicast-Pakete.

Multicast Packets (Multicast-Pakete) Die auf der ausgewählten Schnittstelle empfangene Menge der Multicast-Pakete.

Broadcast Packets (Broadcast-Pakete) Die auf der ausgewählten Schnittstelle empfangene Menge der Broadcast-Pakete.

Unknown Packets (Unbekannte Pakete) Die auf der ausgewählten Schnittstelle empfangene Menge der unbekannten Pakete.

Packets with Errors (Pakete mit Fehlern) Die von der ausgewählten Schnittstelle übermittelte Menge von fehlerhaften Paketen.

Übertragungsstatistiken

Total Bytes (Octets) (Gesamtzahl Bytes (Oktetts) Die auf der ausgewählten Schnittstelle übermittelte Oktettmenge.

Unicast Packets (Unicast-Pakete) Anzahl der an der Schnittstelle übertragenen Unicast-Pakete.

Multicast Packets (Multicast-Pakete) Anzahl der Multicast-Pakete, die an der ausgewählten Schnittstelle übertragen wurden.

Broadcast Packets (Broadcast-Pakete) Anzahl der Broadcast-Pakete, die an der ausgewählten Schnittstelle übertragen wurden.

Packets with Errors (Pakete mit Fehlern) Die von der ausgewählten Schnittstelle übermittelte Menge von fehlerhaften Paketen.

Anzeigen der Schnittstellenstatistik

1. Öffnen Sie die Seite **Interface Statistics** (Schnittstellenstatistik).
2. Wählen Sie eine Schnittstelle im Feld **Interface.**

Zurücksetzen der Zähler für Schnittstellenstatistiken

1. Öffnen Sie die Seite **Interface Statistics** (Schnittstellenstatistik).
2. Klicken Sie auf **Reset All Counters**.

Anzeigen der Schnittstellenstatistik mithilfe der CLI-Befehle

Die folgende Tabelle enthält CLI-Befehle für die Ansicht der Schnittstellenstatistik.

Tabelle 9-1. CLI-Befehle für Schnittstellenstatistiken

CLI-Befehl	Beschreibung
show interfaces counters [ethernet *interface* | port- channel *port-channel-number*]	Zeigt den über die physische Schnittstelle gelaufenen Datenverkehr an.

Das folgende Beispiel zeigt die CLI-Befehle.

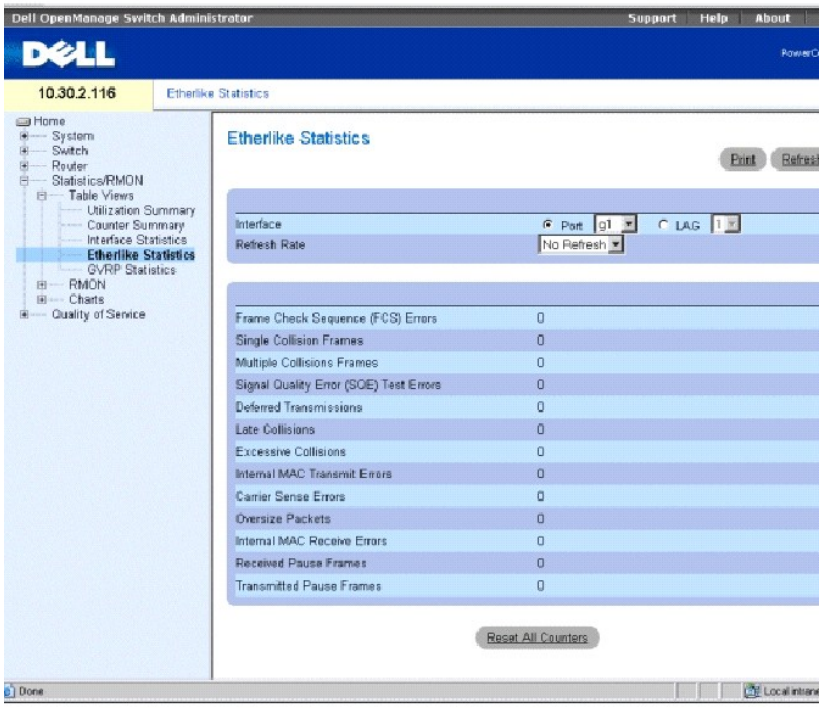
```
Console> show interfaces counters

Port    InOctets InUcastPkts InMcastPkts InBcastPkts

------ --------- ----------- ----------- -----------

g1          0         0          0          0

g2          0         0          0          0

g3          0         0          0          0

g4          0         0          0          0

g5          0         0          0          0

g6          0         0          0          0

g7          0         0          0          0

g8          0         0          0          0

g9          0         0          0          0

g10         0         0          0          0

g11         0         0          0          0

g12         10        685        290        32

g13         0         0          0          0

g14         0         0          0          0
```

g15	0	0	0	0
g16	0	0	0	0
g17	0	0	0	0
g18	0	0	0	0
g19	0	0	0	0
g20	0	0	0	0
g21	0	0	0	0
g22	0	0	0	0
g23	0	0	0	0
g24	0	0	0	0

Anzeigen von Etherlike-Statistiken

Die Seite **Etherlike Statistics** (Etherlike-Statistik) enthält Schnittstellenstatistiken. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Statistics/RMON→ Table Views→ Etherlike Statistics**.

Abbildung 9-4. Etherlike-Statistik



Interface Gibt an, ob Statistiken für einen Port oder LAG angezeigt werden.

Refresh Rate (Aktualisierungsrate) Zeit, die vergeht, bevor die Statistik aktualisiert wird. Die möglichen Feldwerte sind No Refresh (Keine Aktualisierung), 15, 30 und 60 Sekunden.

Frame Check Sequence (FCS) Errors (Frameprüfsequenz-Fehler) Die Anzahl der über die ausgewählte Schnittstelle empfangenen FCS-Fehler.

Single Collision Frames Anzahl der über die ausgewählte Schnittstelle empfangenen Single-Collision-Frame-Fehler.

Multiple Collision Frames Anzahl der über die ausgewählte Schnittstelle empfangenen Multiple-Collision-Frame-Fehler.

Signal Quality Error (SQE) Test Errors Die Anzahl der SQE-Testfehler, die an der ausgewählten Schnittstelle erhalten wurden.

Deferred Transmissions (Verzögerte Übertragungen) Anzahl der verzögerten Übertragungen auf der ausgewählten Schnittstelle.

Late Collisions (Verspätete Kollisionen) Anzahl der auf der ausgewählten Schnittstelle empfangenen verspäteten Kollisionen.

Excessive Collisions (Übermäßige Kollisionen) Anzahl der auf der ausgewählten Schnittstelle empfangenen übermäßigen Kollisionen.

Internal MAC Transmit Errors Anzahl interner MAC-Übertragungsfehler an der ausgewählten Schnittstelle.

Carrier Sense Errors Anzahl der bei der Leitungsüberwachung an der ausgewählten Schnittstelle aufgetretenen Fehler.

Oversize Packets (Übergroße Pakete) Anzahl der Fehler durch überlange Pakete auf der ausgewählten Schnittstelle.

Internal MAC Receive Errors Anzahl interner MAC-Empfangsfehler an der ausgewählten Schnittstelle.

Receive Pause Frames (Pause-Frame-Empfang) Anzahl der auf der ausgewählten Schnittstelle empfangenen Pausenfehler.

Transmitted Pause Frames (Pause-Frame-Übertragung) Anzahl der auf der ausgewählten Schnittstelle übertragenen Pausenfehler.

Anzeigen der Etherlike-Statistik für eine Schnittstelle

1. Öffnen Sie die Seite **Etherlike Statistics** (Etherlike-Statistik).
2. Wählen Sie eine Schnittstelle im Feld **Interface** aus.
3. Klicken Sie auf **Query** (Anfrage), um die Etherlike-Statistik der Schnittstelle anzuzeigen.

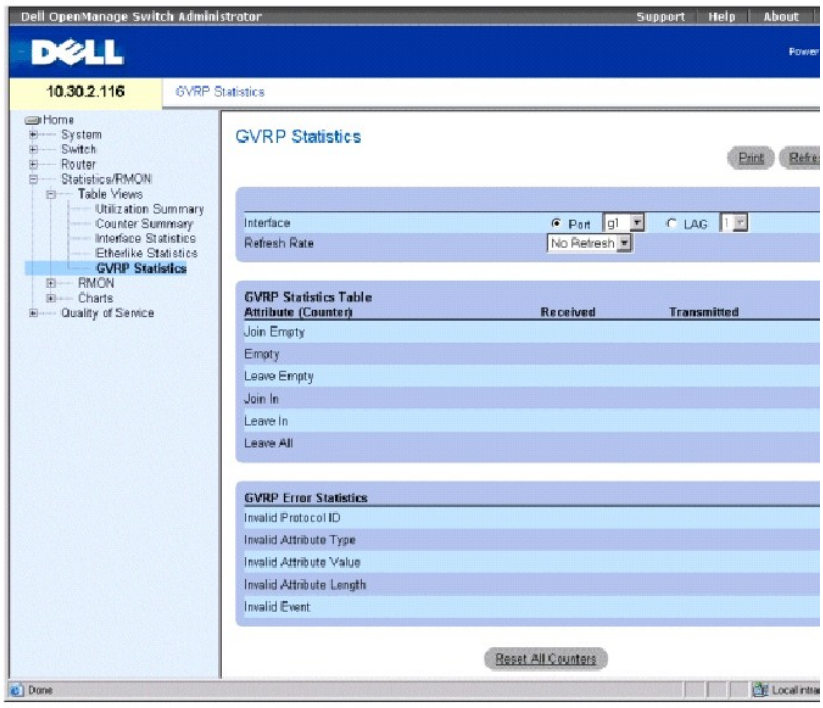
Zurücksetzen der Etherlike-Statistik

1. Öffnen Sie die Seite **Etherlike Statistics** (Etherlike-Statistik).
2. Klicken Sie auf **Reset All Counters**.

Anzeigen der GVRP-Statistiken

Die Seite **GVRP Statistics** (GVRP-Statistik) enthält die Gerätestatistik für GVRP. Öffnen Sie die Seite, indem Sie auf **Statistics/RMON→ Table Views→ GVRP Statistics** in der Strukturansicht klicken.

Abbildung 9-5. GVRP-Statistik



Interface Gibt an, ob Statistiken für einen Port oder LAG angezeigt werden.

Refresh Rate (Aktualisierungsrate) Zeit, die vergeht, bevor die Statistik aktualisiert wird. Die möglichen Feldwerte sind No Refresh (Keine Aktualisierung), 15, 30 und 60 Sekunden.

Join Empty Die GVRP Join Empty"-Statistik für das Gerät.

Empty Die GVRP Empty"-Statistik für das Gerät.

Leave Empty Die GVRP Leave"-Statistik für das Gerät.

Join In Die GVRP Join In"-Statistik für das Gerät.

Leave In Die GVRP Leave In"-Statistik für das Gerät.

Leave All Die GVRP Leave All"-Statistik für das Gerät.

Invalid Protocol ID Die GVRP-Gerätestatistik zu ungültigen Protokoll-IDs.

Invalid Attribute Type Die GVRP-Gerätestatistik zu ungültigen Attribut-IDs.

Invalid Attribute Value Die GVRP-Gerätestatistik zu ungültigen Attributwerten.

Invalid Attribute Length Die GVRP-Gerätestatistik zu ungültigen Attributlängen.

Invalid Event Die GVRP-Gerätestatistik zu ungültigen Ereignissen.

Anzeigen der GVRP-Statistiken für einen Port:

1. Öffnen Sie die Seite **GVRP Statistics** (GVRP-Statistik).
2. Wählen Sie eine Schnittstelle im Feld **Interface**.

Zurücksetzen der GVRP-Statistik

1. Öffnen Sie die Seite **GVRP Statistics** (GVRP-Statistik).
2. Klicken Sie auf **Reset All Counters**.

Anzeigen der GVRP-Statistiken mithilfe der CLI-Befehle

Die folgende Tabelle enthält CLI-Befehle für die Ansicht der GVRP-Statistiken.

Tabelle 9-2. CLI-Befehle für GVRP-Statistiken

CLI-Befehl	Beschreibung
`show gvrp statistics [ethernet interface | port-channel port- channel-number]`	Zeigt die GVRP-Statistiken an.
	Zeigt die GVRP-Fehlerstatistiken an.

show gvrp error- statistics [ethernet *interface* | port-channel *port-channel-number*]

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console# show gvrp statistics

GVRP statistics:

----------------

Legend:

rJE : Join Empty Received rJIn : Join In Received

rEmp : Empty Received rLIn : Leave In Received

rLE : Leave Empty Received rLA : Leave All Received

sJE : Join Empty Sent sJIn : Join In Sent

sEmp : Empty Sent sLIn : Leave In Sent

sLE : Leave Empty Sent sLA : Leave All Sent

Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE sLA

---- --- ---- ---- ---- --- --- --- --- --- ---- --- ---

g1    0    0    0    0   0   0   0   0   0    0   0   0

g2    0    0    0    0   0   0   0   0   0    0   0   0

g3    0    0    0    0   0   0   0   0   0    0   0   0

g4    0    0    0    0   0   0   0   0   0    0   0   0

g5    0    0    0    0   0   0   0   0   0    0   0   0

g6    0    0    0    0   0   0   0   0   0    0   0   0

g7    0    0    0    0   0   0   0   0   0    0   0   0
```

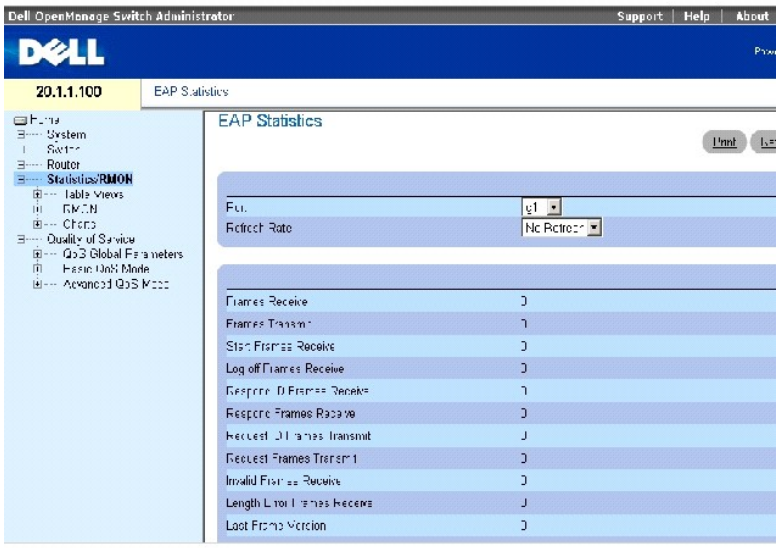
```
g8    0    0    0    0   0   0   0   0   0    0   0   0

Console# show gvrp error-statistics

GVRP error statistics:

----------------

Legend:

INVPROT : Invalid Protocol Id INVPLEN : Invalid PDU Length

INVATYP : Invalid Attribute Type INVALEN : Invalid Attribute Length

INVAVAL : Invalid Attribute Value INVEVENT : Invalid Event



Port INVPROT INVATYP INVAVAL INVPLEN INVALEN INVEVENT

---- ------- ------- ------- ------- ------- --------

g1      0       0       0       0       0       0

g2      0       0       0       0       0       0

g3      0       0       0       0       0       0

g4      0       0       0       0       0       0

g5      0       0       0       0       0       0

g6      0       0       0       0       0       0

g7      0       0       0       0       0       0

g8      0       0       0       0       0       0
```

Anzeigen von EAP-Statistiken

Die Seite **EAP Statistics** enthält Informationen zu EAP-Paketen, die an einem bestimmten Port erhalten wurden. Weitere Informationen zu EAP finden Sie unter „Portbasierte Authentifizierung (802.1x)".

Öffnen Sie die Seite **EAP Statistics**, indem Sie auf **Statistics / RMON→ Table Views→ EAP Statistics** in der Strukturansicht klicken.

Abbildung 9-6. EAP-Statistiken



Die Seite **EAP-Statistik** enthält die folgenden Felder:

Port Der Port, über den Statistiken abgefragt werden.

Refresh Rate Die Zeitspanne, die vergeht, bevor die Schnittstellenstatistiken aktualisiert werden.

Frames Receive Die Anzahl der am Port erhaltenen gültigen EAPOL-Frames.

Frames Transmit Die Anzahl der über den Port übertragenen EAPOL-Frames.

Start Frames Receive Die Anzahl der am Port erhaltenen EAPOL-Start-Frames.

Log off Frames Receive Die Anzahl der am Port erhaltenen EAPOL-Logoff-Frames.

Respond ID Frames Receive Die Anzahl der am Port erhaltenen EAP-Respond-ID-Frames.

Respond Frames Receive Die Anzahl der am Port erhaltenen gültigen EAP-Respond-Frames.

Request ID Frames Transmit Die Anzahl der über den Port übertragenen EAP-Requested-ID-Frames.

Request Frames Transmit Die Anzahl der über den Port übertragenen EAP-Request-Frames.

Invalid Frames Receive Die Anzahl der am Port erhaltenen unerkannten EAPOL-Start-Frames.

Length Error Frames Receive Die Anzahl der an diesem Port erhaltenen EAPOL-Frames mit einer ungültigen Paketkörperlänge.

Last Frame Version Die am zuletzt erhaltenen EAPOL-Frame angehängte Protokollversionsnummer.

Last Frame Version Die am zuletzt erhaltenen EAPOL-Frame angehängte MAC-Quelladresse.

Anzeigen der EAP-Statistiken für einen Port

1. Öffnen Sie die Seite **EAP Statistics**.
2. Wählen Sie eine Schnittstelle im Feld **Interface**.

Die EAP-Statistiken für die Schnittstelle werden angezeigt.

Anzeigen der EAP-Statistiken mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Anzeige der EAP-Statistiken.

Tabelle 9-3. CLI-Befehle für die EAP-Statistik

CLI-Befehl	Beschreibung
`show dot1x statistics ethernet` *`interface`*	Zeigt die 802.1X-Statistiken für die angegebene Schnittstelle an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console# show dot1x statistics ethernet g11

EapolFramesRx: 11

EapolFramesTx: 12

EapolStartFramesRx: 1

EapolLogoffFramesRx: 1

EapolRespIdFramesRx: 3

EapolRespFramesRx: 6

EapolReqIdFramesTx: 3

EapolReqFramesTx: 6

InvalidEapolFramesRx: 0
```

```
EapLengthErrorFramesRx: 0

LastEapolFrameVersion: 1

LastEapolFrameSource: 0008.3b79.8787
```

Anzeigen von RMON-Statistiken

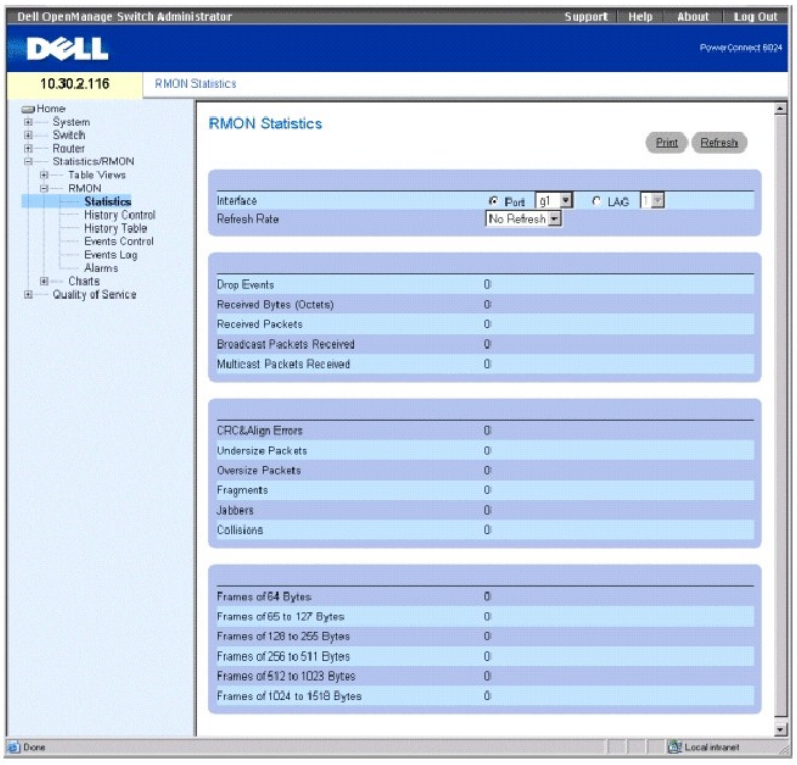
Fernüberwachung (RMON) ermöglicht es Netzwerkmanagern, Netzwerkinformationen von einem Remote-Standort anzusehen. Öffnen Sie die Seite **RMON**, indem Sie auf **Statistics / RMON→ RMON** in der Strukturansicht klicken.

Anzeigen der RMON-Statistikgruppe

Auf der Seite **RMON-Statistikgruppe** können Sie Informationen über die Gerätenutzung und die auf diesem Gerät auftretenden Fehler anzeigen.

Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Statistics / RMON→ RMON→ Statistics**.

Abbildung 9-7. RMON-Statistikgruppe



Interface Gibt den Port oder LAG an, für den Statistiken angezeigt werden.

Refresh Rate (Aktualisierungsrate) Zeit, die vergeht, bevor die Statistik aktualisiert wird. Die möglichen Feldwerte sind No Refresh (Keine Aktualisierung), 15, 30 und 60 Sekunden.

Drop Events Die Anzahl der Ereignisse, die seit dem letzten Aktualisieren des Geräts an der Schnittstelle abgewiesen wurden.

Received Bytes die Anzahl der Oktette, die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden. Diese Anzahl enthält fehlerhafte Pakete und FCS-Oktetts, aber keine Framing-Bits.

Received Packets (Eingegangene Pakete) Die Anzahl der Pakete, die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden, einschließlich fehlerhafte Pakete, Multicast- und Broadcast-Pakete.

Broadcast Packets Received Die Anzahl der fehlerlosen Pakete, die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden. Diese Anzahl enthält keine Multicast-Pakete.

Multicast Packets Received Die Anzahl der fehlerlosen Multicast-Pakete, die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden.

CRC & Align Errors Die Anzahl der CRC- und Ausrichtungsfehler, die seit dem letzten Aktualisieren des Geräts an der Schnittstelle aufgetreten sind.

Undersize Packets Die Anzahl der Pakete unter Normalgröße (unter 64 Oktette), die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden.

Oversize Packets Die Anzahl der Pakete über Normalgröße (über 1518 Oktette), die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden.

Fragments Die Anzahl der Fragmente (Pakete mit weniger als 64 Oktetten, ausschließlich Framing-Bits, aber einschließlich FCS-Oktette), die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden.

Jabbers (Hintergrundgeräusche) Die Anzahl der während der Probennahme empfangenen Pakete mit einer Länge von über 1.518 Oktetts und mit FCS.

Collisions Die Anzahl der Kollisionen, die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden.

Frames of *xx* Bytes Die Anzahl der *xx*-Byte-Frames, die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden.

Anzeigen der Schnittstellenstatistik

1. Öffnen Sie die Seite **RMON Statistics Group** (RMON-Statistikgruppe).
2. Wählen Sie eine Schnittstellenart und -nummer im Feld **Interface**.

Anzeigen der RMON-Statistiken mit den CLI-Befehlen

Die folgende Tabelle enthält die CLI-Befehle für die Ansicht der RMON-Statistiken.

Tabelle 9-4. CLI-Befehle für RMON-Statistiken

CLI-Befehl	Beschreibung
`show rmon statistics {ethernet` *`interface`* `| port-channel` *`port-channel- number`*`}`	Zeigt RMON-Ethernet-Statistiken an.

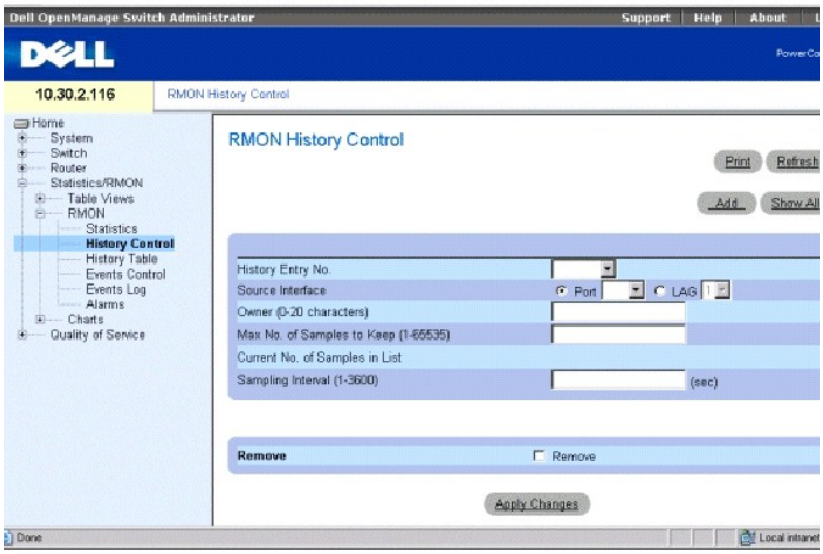
Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console# show rmon statistics ethernet g1

Port g1

Dropped: 8

Octets: 878128 Packets: 978

Broadcast: 7 Multicast: 1

CRC Align Errors: 0 Collisions: 0

Undersize Pkts: 0 Oversize Pkts: 0

Fragments: 0 Jabbers: 0

64 Octets: 98 65 to 127 Octets: 0

128 to 255 Octets: 0 256 to 511 Octets: 0

512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

Anzeigen von RMON-Verlaufssteuerungsstatistiken

Die Seite **RMON History Control** enthält Informationen zu Stichprobendaten, die an den Ports erfasst wurden. Die Proben können z. B.. Schnittstellendefinitionen oder Polling-Perioden enthalten. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Statistics / RMON→ RMON→ RMON History Control**.

Abbildung 9-8. RMON-Verlaufssteuerung



History Entry No. (Eintragsnummer) Die Eintragsnummer für die **RMON History Control Table** (RMON-Verlaufssteuerungstabelle).

Source Interface Der Port oder LAG, von der die Verlaufsstichproben erfasst wurden.

Owner (Eigentümer) RMON-Station oder RMON-Benutzer, die/der die RMON-Information angefordert hat.

Max No. of Samples to Keep (1-65535) Die Anzahl der zu speichernden Stichproben. Der Standardwert ist 50.

Current No. of Samples in List (Derzeitige Anzahl an Stichproben in der Liste) Zeigt die derzeitige Anzahl an erfassten Stichproben an.

Sampling Interval (1-3600) (Stichprobenintervall) Zeigt die Zeit (in Sekunden) an, in der Proben von den Ports genommen werden. Die möglichen Werte sind 1-3600 Sekunden. Der Standardwert ist 1800 Sekunden (30 Minuten).

Remove (Entfernen) Wenn diese Option markiert ist, wird der Eintrag aus der RMON **History Control Table** (RMON-Verlaufssteuerungstabelle entfernt.

Hinzufügen eines Verlaufssteuerungseintrags

1. Öffnen Sie die Seite **RMON History Control** (RMON-Verlaufssteuerung).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add History Entry** (Verlaufseintrag hinzufügen) anzuzeigen.
3. Füllen Sie die Felder in dem Dialogfeld aus und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag wird der RMON **History Control Table** (RMON-Verlaufssteuerungstabelle) hinzugefügt.

Ändern eines Eintrags in der RMON-Verlaufssteuerungtabelle

1. Öffnen Sie die Seite **RMON History Control** (RMON-Verlaufssteuerung).
2. Wählen Sie einen Eintrag im Feld **History Entry No.**.
3. Ändern Sie die Felder nach Wunsch und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Tabelleneintrag wird geändert und das Gerät aktualisiert.

Löschen eines Eintrags in der Verlaufssteuerungstabelle

1. Öffnen Sie die Seite **RMON History Control** (RMON-Verlaufssteuerung).
2. Wählen Sie einen Eintrag im Feld **History Entry No.**.
3. Klicken Sie auf **Remove** (Entfernen) und dann auf **Apply Changes** (Änderungen übernehmen).

Der Tabelleneintrag wird entfernt und das Gerät aktualisiert.

Ansicht der RMON-Verlaufssteuerung mithilfe der CLI-Befehle

Die folgende Tabelle enthält CLI-Befehle für die Ansicht der GVRP-Statistiken.

Tabelle 9-5. CLI-Befehle für RMON-History

CLI-Befehl	Beschreibung
`rmon collection history index [owner ownername | buckets bucket-number] [interval seconds]`	Aktiviert und konfiguriert RMON für eine Schnittstelle.
`show rmon collection history [ethernet interface | port-channel port-channel-number]`	Zeigt RMON-Verlaufssteuerungsstatistiken an.

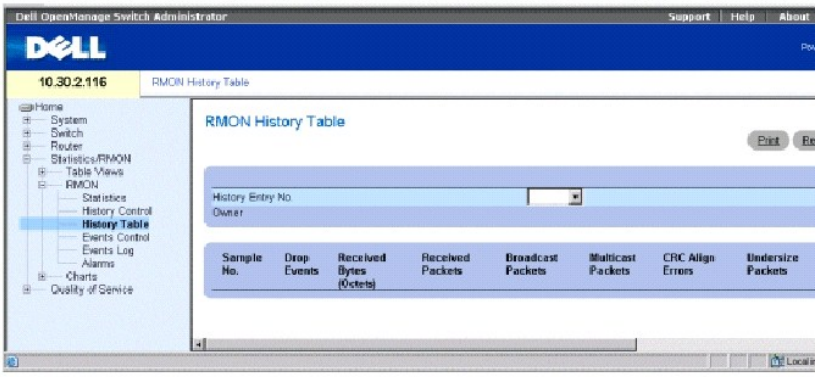
Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# interface ethernet g8

Console (config-if)# rmon collection history 1 interval 2400

Console (config-if)# exit

Console (config)#exit

Console# disable

Console> show rmon collection history

Index Interface Interval Requested Samples  Granted Samples   Owner

----- --------- -------- --------- -------- --------------- --------

1         1        10        0        50           50         CLI
```

Anzeigen der RMON-History-Tabelle

Die Seite RMON History Table (RMON-Verlaufstabelle) enthält Schnittstellen-spezifische statistische Netzwerkstichproben. Jeder Eintrag in der Tabelle stellt alle Zählerwerte dar, die während einer einzigen Stichprobe kompiliert wurden. Um die Seite **RMON History Table** (RMON-Verlaufstabelle), zu öffnen, klicken Sie in der Strukturansicht auf **Statistics/RMON→ RMON→ History Table**.

Figure 9-9. RMON History Table



ANMERKUNG: Nicht alle Felder werden in der RMON-Verlaufstabelle gezeigt.

History Entry No. (Nummer des Verlaufseintrags) Enthält eine Liste mit Eintragsnummern auf der RMON **History Control Table** (RMON-Verlaufssteuerungstabelle).

Owner (Eigentümer) Wenn diese Option verfügbar ist, wird der Name des Eigentümers der RMON-Statistikgruppe angezeigt.

Sample No. (Stichprobennummer) Zeigt die Nummer der spezifischen Stichprobe, die von den Informationen in der Tabelle widergespiegelt wird.

Drop Events Die Anzahl von Paketen, die aufgrund unzureichender Netzwerkressourcen während des Stichprobenintervalls abgewiesen wurden. Dies stellt möglicherweise nicht die genaue Anzahl abgewiesener Pakete dar, sondern wie oft abgewiesene Pakete festgestellt wurden.

Received Bytes (Octets) Die Anzahl der über das Netzwerk empfangenen Daten-Oktette, einschließlich ungültiger Pakete.

Received Packets Die Anzahl der während des Stichprobenintervalls empfangenen Pakete.

Broadcast Packets Die Anzahl der während des Stichprobenintervalls empfangenen gültigen Broadcast-Pakete.

Multicast Packets Die Anzahl der während des Stichprobenintervalls empfangenen gültigen Multicast-Pakete.

CRC Align Errors (CRC-Ausrichtungsfehler) Die Anzahl der während der Probennahme empfangenen Pakete mit einer Länge von 64-1.518 Oktetts. Allerdings haben die Pakete eine fehlerhafte Paketprüfsequenz (FCS) mit einer ganzzahligen Anzahl von Oktetts oder eine fehlerhafte FCS mit einer nicht ganzzahligen Anzahl.

Undersize Packets Die Anzahl der während der Stichprobensitzung empfangenen Pakete mit einer Länge von unter 64 Oktetten.

Oversize Packets Die Anzahl der während der Stichprobensitzung empfangenen Pakete mit einer Länge von über 1,518 Oktetten.

Fragments Die Anzahl der empfangenen Pakete mit einer Länge von unter 64 Oktetten, für die während der Stichprobensitzung eine Frameprüfsequenz generiert wurde.

Jabbers Die Anzahl der empfangenen Pakete mit einer Länge von über 1,518 Oktetten, für die während der Stichprobensitzung eine Frameprüfsequenz generiert wurde.

Collisions (Kollisionen) Schätzt die Gesamtzahl der Paketkollisionen, die während der Probennahme aufgetreten sind. Kollisionen werden erkannt, wenn Verstärkerschnittstelle feststellen, dass zwei oder mehr Stationen gleichzeitig übertragen werden.

Utilization Enthält einen Schätzwert zur Beschreibung physischer Netzwerkschichten für eine Schnittstelle während der Stichprobensitzung. Der Wert wird in Prozenten wiedergegeben.

Ansicht der Statistik für einen spezifischen Verlaufseintrag

1. Öffnen Sie die Seite **RMON History Table** (RMON-Verlaufstabelle).
2. Wählen Sie einen Eintrag im Feld **History Entry No.**.

In der RMON-Verlaufstabelle wird die Eintragsstatistik angezeigt.

Ansicht der RMON-Verlaufssteuerung mithilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für die Ansicht des RMON-Verlaufs.

Tabelle 9-6. CLI-Befehle für RMON-History

CLI-Befehl	Beschreibung
show rmon history index {throughput | errors | other} [period seconds]	Zeigt RMON-Ethernet-Verlaufsstatistiken an.

Im Folgenden werden CLI-Befehle für das Anzeigen der RMON-Ethernet-Statistik für den Datendurchsatz auf Index 1 an Hand eines Beispiels dargestellt:

```
Console# show rmon history 1 throughput

Sample Set: 5 Owner: cli

Interface: 24 interval: 10

Requested samples: 50 Granted samples: 50

Maximum table size: 270

Time                Octets Packets Broadcast Multicast  %

------------------- ------ ------- --------- --------- ---

09-Mar-2003 18:29:32    0      0        0         0      0

09-Mar-2003 18:29:42    0      0        0         0      0
```

09-Mar-2003 18:29:52 0 0 0 0 0

09-Mar-2003 18:30:02 0 0 0 0 0

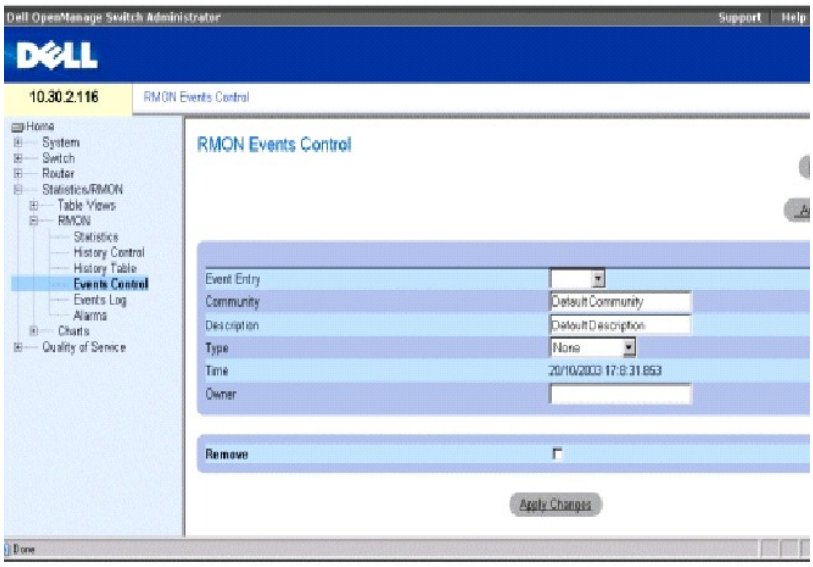
09-Mar-2003 18:30:12 0 0 0 0 0

09-Mar-2003 18:30:22 0 0 0 0 0

Definieren von RMON-Geräteereignissen

Verwenden Sie die Seite **RMON Events Control** (RMON-Ereignissteuerung), um RMON-Ereignisse zu definieren. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Statistics / RMON→ RMON→ Events Control**.

Abbildung 9-10. RMON-Ereignissteuerung



Event Entry (Ereigniseintrag) Zeigt das Ereignis an.

Community Die Community, der das Ereignis angehört.

Description Benutzerdefinierte Ereignisbeschreibung.

Type Beschreibt den Ereignistyp. Die möglichen Werte sind:

Log Der Ereignistyp ist ein Protokolleintrag.

Trap Der Ereignistyp ist ein Trap.

Log and Trap Der Ereignistyp ist sowohl ein Protokolleintrag als auch ein Trap.

None Es gibt kein Ereignis.

Time (Zeitpunkt) Uhrzeit, zu der das Ereignis aufgetreten ist.

Owner Das Gerät bzw. der Benutzer, von dem das Ereignis definiert wurde.

Remove (Entfernen) Wenn diese Option markiert ist, wird das Ereignis aus der Ereignistabelle entfernt.

Hinzufügen eines RMON-Ereignisses

1. Öffnen Sie die Seite **RMON Events Control** (RMON-Ereignissteuerung).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add an Event Entry** (Einen Ereigniseintrag hinzufügen) anzuzeigen.
3. Geben Sie die Informationen im Dialogfeld ein und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das **Ereignis wird der RMON Event Table** (RMON-Ereignistabelle) hinzugefügt, und das Gerät wird aktualisiert.

Ändern eines RMON-Ereignisses

1. Öffnen Sie die Seite **RMON Events Control** (RMON-Ereignissteuerung).
2. Wählen Sie einen Eintrag aus dem **Event Entry field** (Ereigniseintragsfeld) aus.
3. Ändern Sie die Felder auf dieser Seite und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die **RMON Events Table** (RMON-Ereignistabelle) wurde geändert, und das Gerät wurde aktualisiert.

Löschen von RMON-Ereigniseinträgen

1. Öffnen Sie die Seite **RMON Events Control** (RMON-Ereignissteuerung).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **RMON Events Table** (RMON-Ereignistabelle) anzuzeigen.
3. Klicken Sie auf **Remove** (Entfernen) für das/die Ereignis(se), das/die Sie löschen möchten, und klicken Sie dann auf **Apply Changes** (Änderungen übernehmen).

Der Tabelleneintrag wird entfernt und das Gerät aktualisiert.

ANMERKUNG: Sie können ein einzelnes Ereignis von der Seite **RMON Events Control** (RMON-Ereignissteuerung) löschen, indem Sie das Kontrollkästchen **Remove** (Entfernen) auf dieser Seite markieren.

Definieren von Geräteereignissen mithilfe der CLI-Befehle

Die folgende Tabelle enthält CLI-Befehle für das Definieren von Geräteereignissen.

Tabelle 9-7. CLI-Befehle für die Definition von Geräteereignissen

CLI-Befehl	Beschreibung
`rmon event` *`index type`* `[community` *`text`*`] [description` *`text`*`] [owner` *`name`*`]`	Konfiguriert RMON-Ereignisse.
`show rmon events`	Zeigt die RMON-Ereignistabelle an.

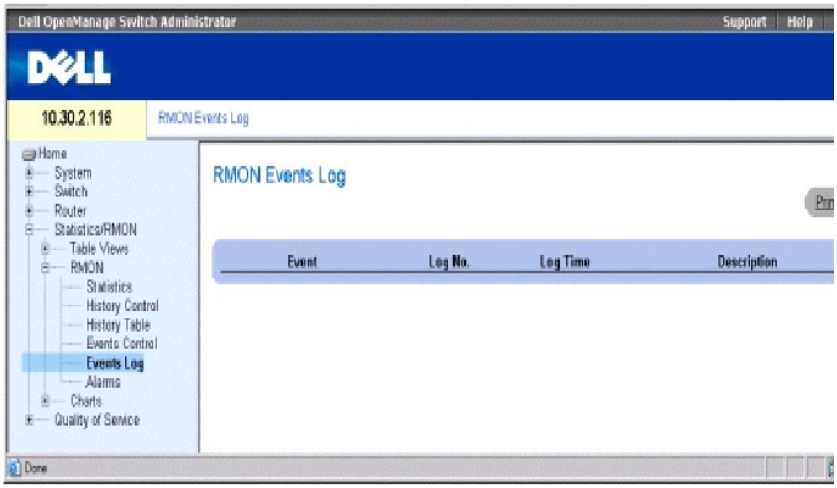
Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# rmon event 10 log

Console (config)# exit

Console# disable

Console> show rmon events

Index     Description     Type     Community     Owner     Last time sent

-----     -----------     ----     ---------     -----     ------------------------

1         Errors          Log      CLI                     Jan 18 2002 23:58:17

2         High Broadcast  Log-Trap router        Manager   Jan 18 2002 23:59:48
```

Anzeigen des RMON-Ereignisprotokolls

Die Seite **RMON Events Log** (RMON-Ereignisprotokoll) enthält eine Liste von RMON-Ereignissen. Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Statistics/RMON→ RMON→ Events Log**.

Abbildung 9-11. RMON-Ereignisprotokoll



Event Die Eintragsnummer im RMON-Ereignisprotokoll.

Log Nr. Die Protokollnummer.

Log Time Die Uhrzeit, zu welcher der Protokolleintrag erfasst wurde.

Description Beschreibt den Protokolleintrag.

Definieren von Geräteereignissen mithilfe der CLI-Befehle

Die folgende Tabelle enthält CLI-Befehle für das Definieren von Geräteereignissen.

Tabelle 9-8. CLI-Befehle für die Definition von Geräteereignissen

CLI-Befehl	Beschreibung
`show rmon log [event]`	Zeigt die RMON-Protokolltabelle an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

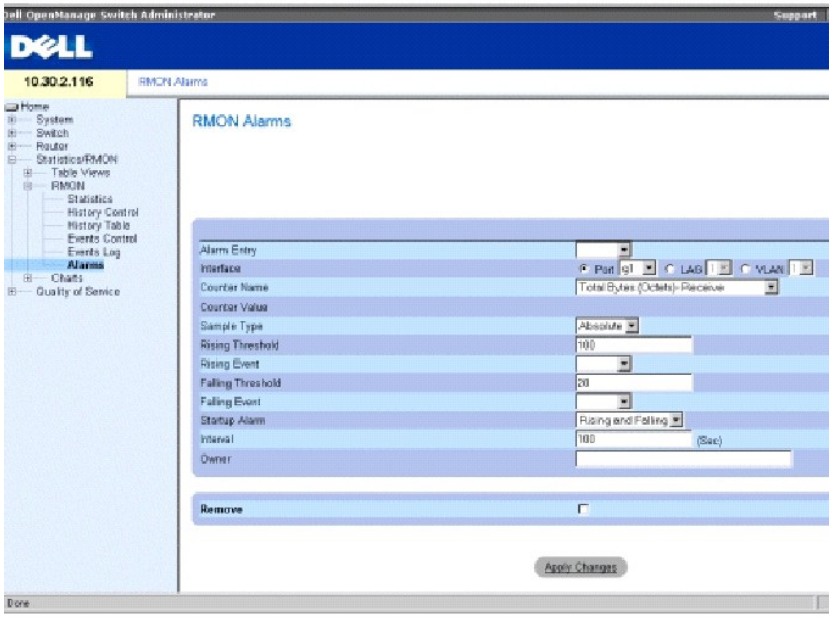
```
Console> show rmon log

Maximum table size: 500

Event   Description                  Time

-----   -----------                  ------------------

1       Errors                       Jan 18 2002 23:48:19

1       Errors                       Jan 18 2002 23:58:17

2       High Broadcast               Jan 18 2002 23:59:48
```

Definieren von RMON-Gerätealarmen

Verwenden Sie die Seite **RMON Alarm**, um Netzwerkalarmmeldungen einzustellen. Netzwerkalarme finden statt, wenn ein Netzwerkproblem oder ein Ereignis festgestellt wurde. Steigende und fallende Schwellenwerte generieren Ereignisse. Weitere Informationen über Ereignisse finden Sie unter Anzeigen des RMON-Ereignisprotokolls".

Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Statistics/RMON→ RMON→ Alarms**.

Abbildung 9-12. RMON-Alarme



Alarm Entry Zeigt einen spezifischen Alarm an.

Interface (Schnittstelle) Gibt die Schnittstelle an, für die die RMON-Statistik angezeigt wird.

Counter Name (Zählername) Zeigt die ausgewählte MIB-Variable an.

Counter Value Der Wert der ausgewählten MIB-Variablen.

Sample Type Gibt das Stichprobenverfahren für die ausgewählte Variable an und vergleicht den Wert mit den Schwellenwerten. Die möglichen Feldwerte sind:

Delta Subtrahiert den letzten Stichprobenwert vom aktuellen Wert. Die Differenz der Werte wird mit dem Schwellenwert verglichen.

Absolute Vergleicht die Werte am Ende des Stichprobenintervalls direkt mit den Schwellenwerten.

Rising Threshold Der obere Zählerwert, durch den der Alarm für die Überschreitung des oberen Schwellenwertes ausgelöst wird. Der steigende Schwellenwert wird oben auf den Diagrammbalken dargestellt. Jeder beobachteten Variable ist eine Farbe zugeordnet.

Rising /Falling Event (Oberes/Unteres Ereignis) Der Mechanismus, durch den ein Alarm gemeldet wird LOG, TRAP oder eine Kombination aus beiden. Wenn LOG ausgewählt ist, gibt es weder in dem Gerät noch in dem Managementsystem einen Speichermechanismus. Wenn das Gerät jedoch nicht zurückgesetzt wird, verbleibt das Ereignis in der LOG-Tabelle des Geräts. Wenn TRAP gewählt ist, wird eine SNMP-Trap generiert und über den Mechanismus der Trap gemeldet. Die TRAP kann mithilfe desselben Mechanismus gespeichert werden.

Falling Threshold Der untere Zählerwert, durch den der Alarm für die Unterschreitung des unteren Schwellenwertes ausgelöst wird. Der fallende Schwellenwert wird oben auf den Diagrammbalken grafisch dargestellt. Jeder beobachteten Variable ist eine Farbe zugeordnet.

Startup Alarm Der Auslöser, durch den der Alarm aktiviert wird. Steigend wird durch das Überschreiten des Schwellenwerts von einem niedrigen Schwellenwert zu einem höheren Schwellenwert definiert.

Interval (sec) Die Intervallzeit für den Alarm.

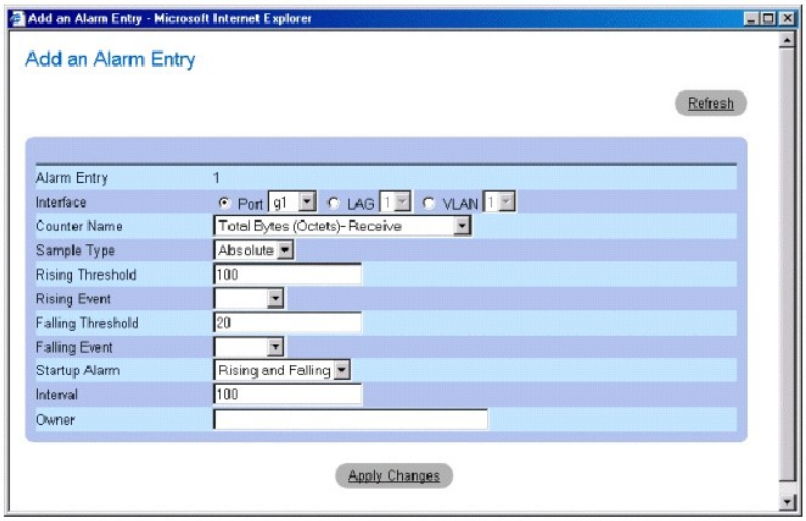
Owner Das Gerät bzw. der Benutzer, von dem der Alarm definiert wurde.

Remove (Entfernen) Wenn diese Funktion ausgewählt ist, wird ein RMON-Alarm entfernt.

Hinzufügen eines Alarmtabelleneintrags

1. Öffnen Sie die Seite **RMON Alarms** (RMON-Alarme).
2. Klicken Sie auf **Add** (Hinzufügen), um die Seite **Add an Alarm Entry** (Einen Alarmeintrag hinzufügen) anzuzeigen.

Abb. 9-13. Hinzufügen eines Alarmeintrags



3. Wählen Sie eine Schnittstelle.
4. Füllen Sie die Felder in dem Dialogfeld aus und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der RMON-Alarm wird hinzugefügt und das Gerät aktualisiert.

Modifizieren eines Alarmtabelleneintrags

1. Öffnen Sie die Seite **RMON Alarms** (RMON-Alarme).
2. Wählen Sie einen Eintrag im **Alarm Entry** Drop-Down-Menü.
3. Ändern Sie die Felder in dem Dialogfeld nach Wunsch und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag wird geändert und das Gerät aktualisiert.

Anzeigen der Alarmtabelle

1. Öffnen Sie die Seite **RMON Alarms** (RMON-Alarme).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **RMON Alarms Table** (RMON-Alarmtabelle) anzuzeigen.

Löschen eines Alarmtabelleneintrags

1. Öffnen Sie die Seite **RMON Alarms** (RMON-Alarme).

2. Wählen Sie einen Eintrag im Drop-Down-Menü **Alarm Entry**.
3. Markieren Sie das Kontrollkästchen **Remove** (Entfernen) und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag wird entfernt und das Gerät aktualisiert.

Definieren von Gerätealarmen mithilfe der CLI-Befehle

Die folgende Tabelle enthält CLI-Befehle für das Definieren von Gerätealarmen.

Tabelle 9-9. CLI-Befehle für Gerätealarm

CLI-Befehl	Beschreibung
rmon alarm *index MIB_Object_ID interval rthreshold fthreshold revent fevent* [type *type*] [startup *direction*] [owner *name*]	Konfiguriert die RMON-Alarmbedingungen.
show rmon alarm-table	Zeigt eine Übersicht der Alarmtabelle an.
show rmon alarm	Zeigt die RMON-Alarmkonfiguration an.

Im Folgenden sind CLI-Befehle anhand eines Beispiels dargestellt:

```
Console (config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1 360000 1000000 1000000 10 20

Console# show rmon alarm-table

Index  OID                      Owner

-----  -----------------------  -------

1      1.3.6.1.2.1.2.2.1.10.1   CLI

2      1.3.6.1.2.1.2.2.1.10.1   Manager

3      1.3.6.1.2.1.2.2.1.10.9   CLI
```

Anzeigen von Diagrammen

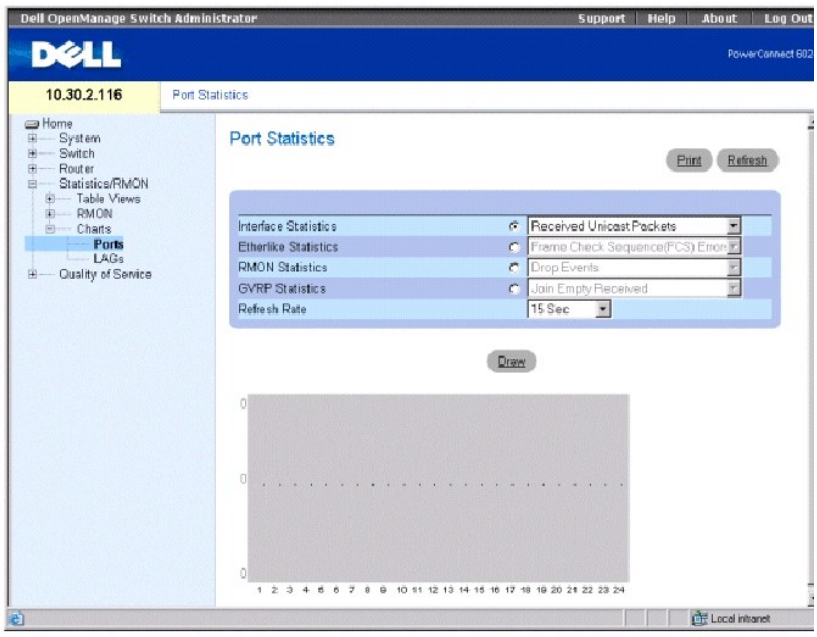
Die Seite **Chart** enthält Links zur Anzeige von Statistiken in Diagrammform. Öffnen Sie die Seite, indem Sie in der Strukturansicht auf **Statistics / RMON→ Charts** klicken.

Anzeigen der Portstatistiken

Auf der Seite **Portstatistik** können Sie eine Statistik in Diagrammformat für Portelemente anzeigen.

Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Statistics / RMON** → **Charts** → **Ports**.

Abbildung 9-14. Portstatistik



Interface Statistics (Schnittstellenstatistik) Wählt die anzuzeigende Schnittstellenstatistik aus.

Etherlike Statistics (Etherlike-Statistik) Wählt die anzuzeigende Etherlike-Statistik aus.

RMON Statistics (RMON-Statistik) Wählt den Typ der anzuzeigenden RMON-Statistik aus.

GVRP Statistics (GVRP-Statistik) Wählt den Typ der anzuzeigenden GVRP-Statistik aus.

Refresh Rate (Aktualisierungsrate) Zeit, die vergeht, bevor die Statistik aktualisiert wird. Die möglichen Feldwerte sind No Refresh (Keine Aktualisierung), 15, 30 und 60 Sekunden.

Anzeigen der Portstatistik

1. Öffnen Sie die Seite **Port Statistics** (Portstatistik).
2. Wählen Sie den anzuzeigenden Statistiktyp.
3. Wählen Sie die gewünschte Aktualisierungsrate aus dem Drop-Down-Menü **Refresh Rate** aus.
4. Klicken Sie auf **Draw**

Die Grafik für die gewählte Statistik wird angezeigt.

Anzeigen der Portstatistiken mit den CLI-Befehlen

Die folgende Tabelle enthält CLI-Befehle für die Ansicht der Portstatistiken.

Tabelle 9-10. CLI-Befehle für Portstatistiken

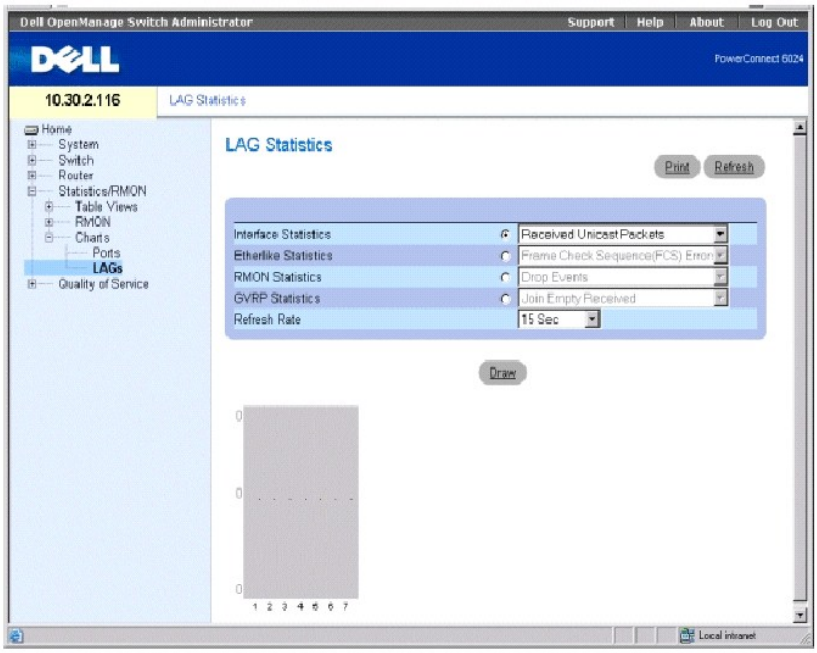
CLI-Befehl	Beschreibung
`show interfaces counters [ethernet` *`interface`* `| port- channel` *`port-channel-number`*`]`	Zeigt den an der physikalischen Schnittstelle abgewickelten Datenverkehr an.
`show rmon statistics {ethernet` *`interface`* `| port-channel` *`port- channel-number`*`}`	Zeigt die RMON-Ethernet-Statistiken an.
`show gvrp statistics {ethernet` *`interface`* `| port-channel` *`port- channel-number`*`}`	Zeigt die GVRP-Statistiken an.
`show gvrp-error statistics {ethernet` *`interface`* `| port- channel` *`port-channel-number`*`}`	Zeigt die GVRP-Fehlerstatistiken an.

Anzeigen der LAG-Statistiken

Verwenden Sie die Seite **LAG Statistics** (LAG-Statistik), um die Statistik für LAGs in Diagrammform anzuzeigen.

Um die Seite zu öffnen, klicken Sie in der Strukturansicht auf **Statistics/RMON**→ **Charts**→ **LAGs**.

Abbildung 9-15. LAG-Statistik



Interface Statistics (Schnittstellenstatistik) Wählt die anzuzeigende Schnittstellenstatistik aus.

Etherlike Statistics (Etherlike-Statistik) Wählt die anzuzeigende Etherlike-Statistik aus.

RMON Statistics (RMON-Statistik) Wählt den Typ der anzuzeigenden RMON-Statistik aus.

GVRP Statistics (GVRP-Statistik) Wählt den Typ der anzuzeigenden GVRP-Statistik aus.

Refresh Rate (Aktualisierungsrate) Zeit, die vergeht, bevor die Statistik aktualisiert wird. Die möglichen Feldwerte sind No Refresh (Keine Aktualisierung), 15, 30 und 60 Sekunden.

Anzeigen der LAG-Statistik

1. Öffnen Sie die Seite **LAG Statistics**.
2. Wählen Sie den anzuzeigenden Statistiktyp.
3. Wählen Sie die gewünschte Aktualisierungsrate aus dem Drop-Down-Menü **Refresh Rate** aus.
4. Klicken Sie auf **Draw** (Zeichnen).

Die Grafik für die gewählte Statistik wird angezeigt.

Anzeigen der LAG-Statistiken mithilfe der CLI-Befehle

Die folgende Tabelle enthält CLI-Befehle für die Ansicht der LAG-Statistiken.

Tabelle 9-11. CLI-Befehle für LAG-Statistiken

CLI-Befehl	Beschreibung
`show interfaces counters [ethernet` *`interface`* `| port- channel` *`port-channel-number`*`]`	Zeigt den über die physische Schnittstelle gelaufenen Datenverkehr an.
`show rmon statistics {ethernet` *`interface`* `| port-channel` *`port- channel-number`*`}`	Zeigt RMON-Ethernet-Statistiken an.
`show gvrp statistics {ethernet` *`interface`* `| port-channel` *`port- channel-number`*`}`	Zeigt die GVRP-Statistiken an.
`show gvrp-error statistics {ethernet` *`interface`* `| port- channel` *`port-channel-number`*`}`	Zeigt die GVRP-Fehlerstatistiken an.

Zurück zum Inhaltsverzeichnis