Dell™ PowerConnect™ 3324/3348 Benutzerhandbuch

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

HINWEIS: Ein HINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und weist darauf hin, wie Probleme vermieden werden können.

VORSICHT: Unter VORSICHT werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

November 2003 Version A01

Zurück zum Inhalt

Konfigurieren des PowerConnect 3324/3348-Switches

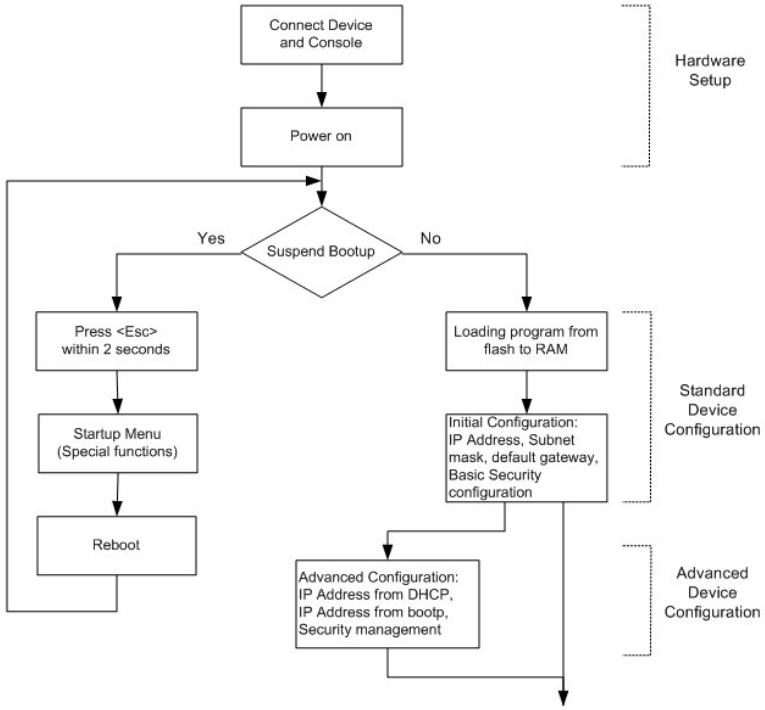
Dell™ PowerConnect™ 3324/3348 Benutzerhandbuch

Konfigurationsübersicht

In diesem Abschnitt werden folgende Schritte der Erstkonfiguration des Geräts beschrieben:

- Erster Gerätestart
- Vorbereitende Konfigurationsmaßnahmen
- Stacking-Konfiguration

Nachdem alle externen Verbindungen hergestellt wurden, muss zur Überwachung des Startvorgangs und anderer Prozeduren ein Terminal an das Gerät angeschlossen werden. Die Reihenfolge der Installations- und Konfigurationsschritte wird im folgenden Ablaufplan dargestellt:



In den vorhergehenden Abschnitten finden Sie Anweisungen zum Einrichten des Geräts und der Hardware. Bei erstmaliger Installation wird die Standard-Installation durchgeführt. Andere Sonderfunktionen sind ebenfalls möglich. Dadurch wird jedoch die Installation unterbrochen, und das System startet neu. Diese Option wird weiter unten in diesem Abschnitt beschrieben.

Allgemeine Konfigurationsinformationen

Der Dell™ PowerConnect™ 3324/3348 verfügt über vordefinierte Funktionen und Setup-Konfigurationen.

Auto-Negotiation

Mit Hilfe der Auto-Negotiation kann das Gerät Betriebsmodi mitteilen und Informationen mit einem anderen Gerät am gleichen Netzwerksegment austauschen. Dadurch werden beide Geräte automatisch so konfiguriert, dass sie ihre Fähigkeiten optimal nutzen können.

Auto-Negotiation wird während des Verbindungsaufrufs vollständig auf den physikalischen Schichten ausgeführt, und zwar ohne zusätzlichen Datenverkehr auf der MAC-Ebene oder auf höheren Netzwerkschichten. Auto-Negotiation ermöglicht den Anschlüssen

- Informationen über ihre Fähigkeiten mitzuteilen
- die Betriebsmodi, die von beiden Geräten genutzt werden, zu erkennen und festzulegen
- die Betriebsmodi abzulehnen, die nicht von beiden Geräten genutzt werden
- mit der höchstmöglichen Datenübertragungsrate konfiguriert zu werden, die von beiden Geräten unterstützt wird.

Sie können einen Switchanschluss auch mit solchen Netzwerkanschlüssen von Workstations oder Servern verbinden, die keine Auto-Negotiation unterstützen oder nicht darauf eingestellt sind. In diesem Fall müssen sowohl der Switch- als auch der Geräteanschluss manuell mit Hilfe Ihres Webbrowsers oder CLI-Befehlen auf gleiche Geschwindigkeits- und Duplexmodi eingestellt werden.

HINWEIS: Falls die Workstation am anderen Ende der Verbindung versucht, eine Auto- Negotiation mit einem Anschluss durchzuführen, der manuell auf Vollduplex-Modus konfiguriert wurde, bewirkt die Auto-Negotiation, dass die Workstation versucht, im Halbduplex-Modus zu arbeiten. Die daraus resultierende Fehlanpassung kann einen signifikanten Frame-Verlust verursachen. Dieser Umstand ist charakteristisch für den Auto-Negotiation-Standard.

Ändern der Standardeinstellungen von Anschlüssen

In der folgenden Tabelle werden die Standardeinstellungen von Anschlüssen beschrieben.

Standardeinstellungen von Anschlüssen

Funktion	Standardeinstellung
Anschlussgeschwindigkeit und Modus	10/100 Mbit/s Kupferanschlüsse: Auto-Negotiation 1000 Mbit/s Auto-Negotiation
Weiterleitungsstatus der Anschlüsse	Aktiviert
Anschlusskennzeichnung	Keine Kennzeichnung
Schutz vor Head-of-Line-Blocking	Aktiviert
Flow Control	Aus
Back Pressure	Aus

Im Folgenden sehen Sie ein Beispiel für die Änderung der Geschwindigkeit für den Anschluss `1/e5` mit den entsprechenden CLI-Befehlen:

```
console> enable

console# configure

Console(config)# interface ethernet 1/e5

Console (config-if)# speed 9600
```

Im Folgenden sehen Sie ein Beispiel für die Aktivierung der Flusskontrolle für den Anschluss `1/e5` mit den entsprechenden CLI-Befehlen:

```
console> enable

console# configure

Console(config)# interface ethernet 1/e5

Console (config-if)# flowcontrol on
```

Im Folgenden sehen Sie ein Beispiel für die Aktivierung des Backpressure für den Anschluss `1/e5` mit den entsprechenden CLI-Befehlen:

```
console> enable

console# configure

Console(config)# interface ethernet 1/e5

Console (config-if)# back-pressure
```

Baud Rate

Die Baudraten können manuell in einen der folgenden Werte geändert werden:

- 2400
- 4800
- 9600
- 19200
- 38400
- 57600
- 115200

ANMERKUNG: Die Standardbaudrate beträgt 9600.

ANMERKUNG: Wenn Sie das Gerät ausschalten, wird es nicht auf die Standardbaudrate zurückgesetzt. Die Standardbaudrate muss gesondert konfiguriert werden.

ANMERKUNG: Um in den Konfigurationsmodus zu gelangen, müssen Sie über Administratorenrechte der Ebene 15 verfügen.

Im Folgenden sehen Sie eine Beispielkonfiguration für die Änderung der Standardbaudrate mit den entsprechenden CLI-Befehlen:

```
console> enable

console# configure

console(config)# line console

console(config-line)# speed 9600

console (config-if)# exit

console(config)# exit
```

Konfiguration der Terminal-Verbindung

Für die Konfiguration des PowerConnect 3324/3348 sind die folgenden Terminalverbindungsparameter erforderlich:

- keine Parität
- 1 Stoppbit
- 8 Datenbits

Weitere Voraussetzungen für die Konfiguration

Zum Herunterladen der eingebetteten Software und zur Konfiguration des Geräts müssen folgende Voraussetzungen erfüllt sein:

- Das ASCII-Terminal (bzw. dessen Emulation) muss an den seriellen Anschluss hinten an der Einheit angeschlossen sein.
- Dem PowerConnect 3324/3348 muss eine IP-Adresse zugewiesen sein, um den Remote-Zugriff über Telnet, SSH u.a. zu ermöglichen.

ANMERKUNG: Pro Konfigurationsprozess wird jeweils ein Anschluss definiert.

Starten des Geräts

Wenn das Gerät mit dem lokalen Terminal verbunden ist und der Strom eingeschaltet wird, durchläuft das Gerät den POST (Power On Self Test - Einschalt-Selbsttest). Der integrierte Einschalt-Selbsttest wird jedes Mal ausgeführt, wenn das Gerät eingeschaltet wird. Während des POST-Tests werden die Hardwarekomponenten überprüft, um die vollständige Betriebsbereitschaft des Geräts sicherzustellen, bevor der Startvorgang ausgeführt wird.

Wenn ein kritischer Fehler festgestellt wird, wird der Programmablauf unterbrochen. Nach erfolgreicher Ausführung des POST wird der Code dekomprimiert und in den RAM-Speicher geladen.

Die Fehler- bzw. Erfolgsmeldungen des POST werden auf dem Terminal angezeigt.

So starten Sie das Gerät:

1. Stellen Sie sicher, dass das ASCII-Kabel an das Terminal angeschlossen ist.
2. Nachdem Sie das Gerät an die Stromversorgung angeschlossen haben, beginnt der Startvorgang. Beim Starttest wird zuerst ermittelt, ob Gerätearbeitsspeicher verfügbar ist. Anschließend wird der Startvorgang fortgesetzt. Folgende Informationen werden beispielsweise während eines POST angezeigt:

```
------ Performing the Power-On Self Test (POST) ------

UART Channel Loopback Test......PASS

Testing the System Cache.......PASS

Testing the System SDRAM.......PASS

Boot1 Checksum Test........PASS

Boot2 Checksum Test........PASS

Flash Image Validation Test......PASS

Testing CPU PCI Bus Device Configuration...PASS


BOOT Software Version 1.30.11 Built 27-JAN-2003 10:06:03

Processor: MPC8245 Rev 0.12, 250 MHz (Bus: 100MHz), 32 MByte SDRAM.

I-Cache 16 KB, linesize 32.D-Cache 16 KB, linesize 32.

Cache Enabled.
```

```
Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

Am Ende des POST wird eine Autoboot-Meldung (vergl. die letzten zwei Zeilen) angezeigt. Diese Meldung zeigt an, dass während des Startvorgangs keine Fehler aufgetreten sind.

An dieser Stelle können Sie per Tastatureingabe in das Menü Startup gelangen und wenn nötig spezielle Prozeduren ausführen, die von diesem Menü aus aufgerufen werden können. Um in das Menü Startup zu gelangen, drücken Sie innerhalb von zwei Sekunden nach Erscheinen der Autoboot-Meldung die Taste **<Esc>** oder **<Enter>**. Weitere Informationen zum Menü Startup finden Sie unter "Funktionen des Startmenüs".

Wenn keine Tastatureingaben erfolgen, wird der Code dekomprimiert in den RAM-Speicher geladen. Der Code wird im Arbeitsspeicher ausgeführt, und die Liste der verfügbaren Anschlüsse sowie deren Status (aktiviert/deaktiviert) wird angezeigt.

ANMERKUNG: Der folgende Bildschirm zeigt eine Beispielkonfiguration. Adressen, Versionen und Datumsangaben können je nach Gerät variieren.

```
Preparing to decompress.

Decompressing SW from RSCOD_2

85e000

OK

Running from RAM.

******************************************************Running SW Ver. 3.30 Date 03-Feb-2003 Time 10:10:37
******************************************************



HW version is X.X

Base Mac address is: 00:01:02:03:04:05

Dram size is: 32M bytes

Dram first block size is: 20M bytes

Dram first PTR is: 0xB70000

Flash size is: 8M



STAND ALONE

The BCM5625_A1 0 initiate successfully

The BCM5625_A1 1 initiate successfully
```

```
02-Jan-2000 01:01:11%SSHD-W-NOHOSTKEY: SSHG_init: The SSH daemon cannot listen

for incoming connections, because a host key has not been generated.

The service will start automatically when a host key is generated.

01-Jan-2000 01:01:11 %INIT-I-InitCompleted: Initialization task is completed



console> 01-Jan-2000 01:01:12 %PS-I-PSUP: Power Supply #1 is up

01-Jan-2000 01:01:12%PS-W-PSDOWN: Power Supply #2 is down

01-Jan-2000 01:01:12%LINK-W-Up: 1/e1

01-Jan-2000 01:01:12%LINK-W-UP: 1/e2

01-Jan-2000 01:01:12%LINK-W-Up: 1/e3

01-Jan-2000 01:01:12%LINK-W-UP: 1/e4

01-Jan-2000 01:01:12%LINK-W-Up: 1/e5

01-Jan-2000 01:01:13%LINK-W-Up: 1/e9
```

Nachdem das Gerät erfolgreich gestartet wurde, wird die Systemeingabeaufforderung (console>) angezeigt. Sie können jetzt mit dem Konfigurieren des Geräts beginnen. Für die Konfiguration kann das lokale Terminal verwendet werden.

Einführung in die Gerätekonfiguration

Die Konfiguration erfolgt in zwei Phasen. Die Erstkonfiguration enthält grundlegende Konfigurationsfunktionen und Sicherheitseinstellungen. Die erweiterte Konfiguration enthält die Konfiguration der dynamischen IP-Adresse sowie komplexere Sicherheitseinstellungen.

HINWEIS: Nach der Änderung von Konfigurationseinstellungen muss die neue Konfiguration gespeichert werden, bevor Sie das Gerät neu starten. Geben Sie zum Speichern der Konfiguration Folgendes ein:

```
console> enable

console# copy running-config startup-config
```

Erstkonfiguration

Die Erstkonfiguration des Gerätes beginnt, nachdem das Gerät gestartet wurde. Bei der Erstkonfiguration werden folgende Werte festgelegt:

- Die statische IP-Adresse und die Teilnetzmaske.
- Standard-Gateway
- Benutzername und Berechtigungsebenen für die Remote-Verwaltung.

Wenn das Gerät von einer SNMP-basierten Verwaltungsstation aus verwaltet werden soll, müssen hierfür auch die Community-Strings konfiguriert werden.

Statische IP-Adresse und Teilnetzmaske

Bei PowerConnect 3324/3348-Geräten können an jedem Anschluss beliebig viele IP-Schnittstellen eingerichtet werden. Es empfiehlt sich, nach Eingabe der Konfigurationsbefehle mit dem Befehl "show ip interface" zu überprüfen, ob der jeweilige Anschluss mit der entsprechenden IP-Adresse konfiguriert wurde.

HINWEIS: Es kann einer IP-Adresse jeweils nur ein VLAN zugewiesen werden. Wenn Sie eine Adresse einem anderen VLAN zuweisen, wird die ursprüngliche IP-Adresse von der neuen Adresse überschrieben.

Geben Sie zur Konfiguration einer IP-Schnittstelle in einem VLAN an der Systemeingabeaufforderung Folgendes ein:

```
console> enable

console# configure

console(config)# interface vlan 1

console(config-if)# ip address 100.1.1.1 /8

console (config-if)# exit

console(config)# exit

console# show ip interface


Gateway-IP-Adresse Aktivitätsstatus

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


IP Address I/F

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

100.1.1.1/8 vlan 1
```

```
console#
```

Geben Sie zur Konfiguration einer Schnittstelle für einen Anschluss an der Systemeingabeaufforderung folgende Befehle aus der Beispielkonfiguration ein:

```
console> enable

console# configure

console(config)# interface ethernet 1/e1

console(config-if)# ip address 10.1.1.1 255.0.0.0

console (config-if)# exit

console(config)# exit

console# show ip interface


Gateway IP Address Activity status

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


IP Address I/F

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

10.1.1.1/8 1/e1


console#
```

Standard-Gateway

Um einen PowerConnect 3324/3348 von einem Remote-Netzwerk aus zu verwalten, müssen Sie ein Standard-Gateway konfigurieren. Die konfigurierte Gateway-IP-Adresse muss dem gleichen Teilnetz angehören wie eine IP-Schnittstelle des Geräts.

Geben Sie zur Konfiguration eines Standard-Gateway an der Systemeingabeaufforderung die Befehle aus der Beispielkonfiguration ein:

```
console> enable

console# configure

console(config)# ip default-gateway

console(config)# exit
```

Benutzername, Passwort und Berechtigungsebene

WICHTIGER HINWEIS: Um ein Gerät von einem Remote-Terminal oder einer Webverwaltungsoberfläche aus zu verwalten, müssen Benutzername, Passwort sowie die höchste Berechtigungsebene (Ebene 15) eingegeben werden. (Um auf den Konfigurationskontext mit den CLI-Befehlen zugreifen zu können, müssen Benutzer über die höchste Berechtigungsebene verfügen.) Weitere Informationen zu den Berechtigungsebenen finden Sie im CLI Reference Guide.

Der konfigurierte Benutzername wird bei Remote-Verwaltungssitzungen als Login-Name eingegeben. Geben Sie zur Konfiguration von Benutzernamen und Berechtigungsebenen an der Systemeingabeaufforderung Folgendes ein:

```
console> enable

console# configure

console(config)# username admin password admin level 15

console(config)# exit
```

SNMP-Community-Strings

SNMP (Simple Network Management Protocol) bietet eine Methode zur Verwaltung von Netzwerkgeräten. Auf Geräten, die SNMP unterstützen, wird eine lokale Software (ein Agent) ausgeführt. Die SNMP-Agenten verwalten eine Liste von Variablen, die zur Verwaltung des Gerätes verwendet werden. Die Variablen werden in der MIB (Management Information Base) definiert. Die MIB stellt die vom Agenten gesteuerten Variablen dar. Der SNMP-Agent definiert das Format für die MIB-Spezifikationen sowie das Format für den Zugriff auf Daten über das Netzwerk. Die Zugriffsrechte auf die SNMP-Agenten werden über Zugriffszeichenfolgen und SNMP-Community-Strings gesteuert.

Das Gerät ist SNMP-konform. Das Gerät verfügt über einen SNMP-Agenten, der einen Satz Standard- und Privat-MIB-Variablen unterstützt. Entwickler von Verwaltungsstationen benötigen für das Verwalten der MIBs die genaue Struktur des MIB-Baums sowie sämtliche Informationen zu Privat-MIBs.

Fast alle Parameter können von jeder SNMP-basierten Verwaltungsplattform aus verwaltet werden. Ausgenommen sind die IP-Adresse der SNMP-basierten Verwaltungsplattform sowie die Community-Namen und -Zugriffsrechte. Der SNMP-Verwaltungszugriff auf das Gerät ist deaktiviert, wenn kein Community-String vorhanden ist. Der Switch wird ohne voreingestellte Community-Strings geliefert.

Auf dem folgenden Bildschirm wird eine Standardgerätekonfiguration gezeigt:

```
console#enable

console# show snmp
```

```
Community-String Community-Access IP address

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

Traps are enabled.

Authentication-failure trap is enabled.
```

IP-Adresse sowie Community-String und -Zugriff können während der Erstkonfiguration am lokalen Terminal festgelegt werden.

Die SNMP-Konfigurationsoptionen sind:

- Community-String
- Optionen bei Zugriffsrechten: ro (read only - Nur Lesen), rw (read-and-write - Schreiben und Lesen) oder su (super - Super-User).
- Die Option, eine IP-Adresse einzurichten: Wenn keine IP-Adresse eingerichtet wird, verfügen alle Mitglieder einer Community über die gleichen Zugriffsrechte.

Üblicherweise werden jedoch zwei Community-Strings für ein Gerät verwendet, und zwar einer mit ausschließlich Lese-Zugriff für das öffentliche Netzwerk (public community) und einer mit Schreib- und Lesezugriff für das private Netzwerk (private community).

- Public - Ermöglicht, dass entsprechend berechtigte Management-Stationen MIB-Objekte abrufen können.
- Private - Ermöglicht, dass entsprechend berechtigte Management-Stationen MIB-Objekte abrufen und ändern können.

Es empfiehlt sich, das Gerät während der Erstkonfiguration per SNMP-basierter Management-Station dem Bedarf des Netzwerkadministrators entsprechend zu konfigurieren.

So konfigurieren Sie IP-Adresse und Community-String(s) der SNMP-Station:

1. Geben Sie an der Eingabeaufforderung der Konsole **Enable** ein. Die Eingabeaufforderung wird als # angezeigt.
2. Geben Sie "configure" ein, und drücken Sie die **Eingabetaste**.
3. Geben Sie im Konfigurationsmodus wie unten dargestellt den SNMP- Konfigurationsbefehl mit den Parametern Community-Name (privat), Community-Zugriffsrechte (Schreib- und Lesezugriff) sowie die IP-Adresse ein:

```
console> enable

config# configure

console(config)# snmp-server community private rw 11.1.1.2

config(config)# exit

config# show snmp

Community-String Community-Access IP address

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

private readWrite 11.1.1.2
```

```
Traps are enabled.

Authentication-failure trap is enabled.

Trap-Rec-Address Trap-Rec-Community Version

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

System Contact :

System Location :
```

Damit ist die Erstkonfiguration des Geräts über das lokale Terminal abgeschlossen. Die konfigurierten Parameter ermöglichen die weitere Gerätekonfiguration von allen Remote-Standorten aus.

Fortgeschrittene Konfigurationen

In diesem Kapitel werden die dynamische Zuweisung von IP-Adressen sowie die Sicherheitsverwaltung nach dem AAA-Prinzip (Authentifizierung, Autorisierung und Accounting) erläutert. Dieses Kapitel enthält die folgenden Themen:

- IP-Adressen mittels DHCP konfigurieren.
- IP-Adressen mittels BOOTP konfigurieren.
- Sicherheitsverwaltung und Passwortkonfiguration.

Wenn Sie IP-Adressen mit Hilfe von DHCP und BOOTP konfigurieren oder abrufen, enthält die Konfiguration, die Sie von den entsprechenden Servern erhalten, die IP-Adresse sowie möglicherweise auch die Teilnetzmaske und den Standard-Gateway.

Abrufen einer IP-Adresse von einem DHCP-Server

Wenn eine IP-Adresse über das DHCP-Protokoll abgerufen wird, fungiert das Gerät als DHCP-Client.

So rufen Sie eine IP-Adresse von einem DHCP-Server ab:

1. Um eine IP-Adresse zu erhalten, verbinden Sie einen Anschluss mit einem DHCP- Server oder einem Teilnetz, das einen DHCP-Server enthält.
2. Um über den ausgewählten Anschluss die IP-Adresse zu empfangen, geben Sie folgende Befehle ein:

```
console> enable

console# configure

console(config)# interface vlan 1

console(config-if)# ip address dhcp hostname <string>

console (config-if)# exit
```

```
console(config)# exit
```

3. Die IP-Adresse wird vom Gerät automatisch empfangen.

So überprüfen Sie die IP-Adresse:

1. Geben Sie an der Systemeingabeaufforderung **show ip interface** ein. Nachfolgend finden Sie eine Beispielanzeige.

```
console> enable

console# show ip interface

Gateway IP Address Activity status

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

IP Address I/F

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

10.1.1.1/8 vlan1

console#
```

ANMERKUNG: Die Gerätekonfiguration muss nicht gelöscht werden, um eine IP-Adresse vom DHCP-Server abzurufen.

Empfangen einer IP-Adresse von einem BOOTP-Server

Mit Hilfe des BOOTP-Protokoll kann der Switch die IP-Host-Konfiguration automatisch von jedem Standard-BOOTP-Server im Internet laden. In dieser Konfiguration übernimmt der Switch die Rolle eines BOOTP-Clients.

So rufen Sie eine IP-Adresse von einem BOOTP-Server ab:

1. Um eine IP-Adresse zu erhalten, verbinden Sie einen Anschluss mit einem BOOTP- Server oder einem Teilnetz, das einen BOOTP-Server enthält.
2. Geben Sie an der Systemeingabeaufforderung den Befehl zum Löschen der Startkonfiguration ein. Mit diesem Befehl löschen Sie die Startkonfiguration aus dem Flash-Speicher. Der Switch startet ohne Konfiguration neu. Er beginnt nach einer Minute damit, BOOTP-Anfragen zu senden.
3. Die IP-Adresse wird vom Gerät automatisch empfangen.

ANMERKUNG: Während des Löschens der Startkonfiguration führt jede Eingabe am ASCII- Terminal oder über die Tastatur dazu, dass der Konfigurationsprozess vor dem Fertigstellen abgebrochen wird. Der Switch erhält in diesem Fall keine IP-Adresse von einem BOOTP-Server.

Im Folgenden finden Sie ein Beispiel für diesen Vorgang:

```
console> enable
```

```
console# delete startup-config
```

Im Folgenden finden Sie ein Beispiel für die Überprüfung einer IP-Adresse:

```
console> enable

console# show ip interface


Gateway IP Address Activity status

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


IP Address I/F

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

10.1.1.1/8 vlan1


console#
```

Now the device is configured with an IP address.

Die Gerätekonfiguration muss gelöscht werden, um eine IP-Adresse von einem BOOTP-Server zu erhalten.

Sicherheitsverwaltung und Passwortkonfiguration

Die Systemsicherheit wird mit Hilfe des AAA-Prinzips (Authentifizierung, Autorisierung und Accounting) gewährleistet. Nach diesem Prinzip werden Benutzerzugriffsrechte, Privilegien und Verwaltungsmethoden festgelegt. Bei der AAA-Methode werden Datenbanken sowohl für lokale als auch für Remote-Benutzer verwendet. Die Datenverschlüsselung erfolgt über das SSH-Protokoll.

Im Lieferzustand ist kein Standard-Benutzername oder -Passwort geladen. Alle Benutzernamen und Passwörter sind benutzerdefiniert. Wenn ein benutzerdefiniertes Passwort verloren gegangen ist, kann es vom Menü Startup aus über Passwortwiederherstellung wiederaufgerufen werden. Die Passwortwiederherstellung kann nur am lokalen Terminal ausgeführt werden. Vom lokalen Terminal aus kann einmalig und ohne Passworteingabe auf das Gerät zugegriffen werden.

ANMERKUNG: Stellen Sie sicher, dass Sie bei Eingabe Ihres Benutzernamens und Passworts stets die Administratorenrechte über die Ebene 15 einbeziehen.

Konfigurieren von Sicherheitspasswörtern

Sicherheitspasswörter können für folgende Dienste festgelegt werden:

- Console
- Telnet
- SSH
- HTTP
- HTTPS

ANMERKUNG: Passwörter sind benutzerdefiniert.

ANMERKUNG: Beim Erstellen eines Benutzernamens lautet die Standardpriorität "1", d. h., es ist Zugriff auf das Gerät möglich aber keine Konfiguration. Um den Zugriff auf das Gerät sowie dessen Konfiguration zu ermöglichen, muss ausdrücklich die Priorität "15" festgelegt werden.

Weitere Informationen zu Beschränkungen bei Passwörtern finden Sie unter "Konfigurieren der Netzwerksicherheit".

Konfigurieren eines ersten Konsolenpassworts

Zum Konfigurieren eines ersten Konsolenpassworts geben Sie die folgenden Befehle ein:

```
console> enable

console# configure

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 console

console (config-line)# exit

console(config)# exit
```

- Wenn Sie sich erstmalig über eine Konsolensitzung bei einem Gerät anmelden, geben Sie an der Passwort-Eingabeaufforderung console ein.
- Wenn Sie einen Modus des Gerätes erstmalig von deaktiviert in aktiviert ändern, geben Sie an der Passwort-Eingabeaufforderung console ein.

Konfigurieren eines ersten Telnet-Passworts

Zum Konfigurieren eines ersten Telnet-Passworts geben Sie die folgenden Befehle ein:

```
console> enable
```

```
console# configure

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 admin

console (config-line)# exit

console(config)# exit
```

- Wenn Sie sich erstmalig über eine Telnet-Sitzung bei einem Gerät anmelden, geben Sie `admin` ein.
- Wenn Sie einen Modus des Geräts in aktiviert ändern, geben Sie `admin`ein.

Konfigurieren eines ersten SSH-Passworts

Zum Konfigurieren eines ersten SSH-Passworts geben Sie die folgenden Befehle ein:

```
console> enable

console# configure

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 admin

console (config-line)# exit
```

```
console(config)# exit
```

- Wenn Sie sich erstmalig über eine SSH-Sitzung bei einem Gerät anmelden, geben Sie als Passwort `admin` ein.
- Wenn Sie einen Modus des Gerätes erstmalig von deaktiviert in aktiviert ändern, geben Sie als Passwort `admin` ein.

Konfigurieren eines ersten HTTP-Passworts

Zum Konfigurieren eines ersten HTTP-Passworts geben Sie die folgenden Befehle ein:

```
console> enable

console# configure

console(config)# ip http authentication local

console(config)# username admin password admin level 15

console(config)# exit
```

Konfigurieren eines ersten HTTPS-Passworts

Zum Konfigurieren eines ersten HTTPS-Passworts geben Sie die folgenden Befehle ein:

```
console> enable

console# configure

console(config)# ip https authentication local

console(config)# username admin password admin level 15

console(config)# exit
```

Geben Sie die folgenden Befehle einmal ein, wenn Sie eine Konsolen-, Telnet- oder SSH-Sitzung konfigurieren, um eine HTTPS-Sitzung zu verwenden.

ANMERKUNG: Aktivieren Sie in Ihrem Web-Browser SSL 2.0 oder höher, damit die Seiten angezeigt werden können.

```
console> enable

console# configure

console(config)# crypto certificate generate key-generate
```

```
console(config)# ip https server


console(config)# exit
```

Wenn Sie eine HTTP- oder HTTPS-Sitzung erstmalig aktivieren, geben Sie admin als Benutzernamen und user1 als Passwort ein.

ANMERKUNG: Für HTTP- und HTTPS-Dienste benötigen Sie die Zugriffsrechte für die Ebene 15, mit denen Sie auf die Konfigurationsebene zugreifen können.

Beispielkonfiguration

In diesem Kapitel werden die grundlegenden Schritte erläutert, mit denen Sie eine Remote-Verwaltungsverbindung zu einem PowerConnect 3324/3348 herstellen können. In diesem Kapitel finden Sie keine Informationen zu den verschiedenen Konfigurationsmöglichkeiten bzw. den entsprechenden Befehlen, über die der Switch verfügt.

In diesem Kapitel wird beschrieben, wie Sie erstmalig mit der werkseitigen Konfiguration und werkseitigen Definitionen auf den Switch zugreifen können. Wenn eine zuvor eingegebene Konfiguration Probleme verursacht, sollten Sie die Startkonfigurationsdatei löschen und das Gerät neu starten. Die Startkonfigurationsdatei enthält die Gerätekonfiguration, die bei Einschalten des Geräts besteht. Weitere Informationen finden Sie unter "Standardeinstellungen des Geräts".

Systemanforderungen für Hardware und Software

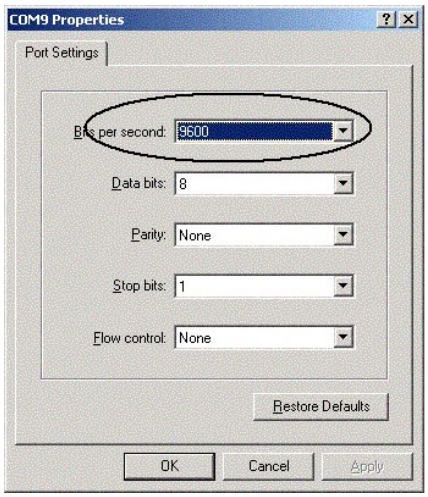
Für dieses Beispiel sind folgende Komponenten erforderlich:

- Ein PowerConnect 3324/3348-Switch
- Eine PC-Workstation mit folgender Hard- und Software:
  - Eine installierte Netzwerkkarte (NIC)
  - Eine ASCII-Terminal-Anwendung, beispielsweise Microsoft® Windows®, MS Hyper Terminal oder Procomm Plus Terminal.
  - Ein Browser
- Ein Nullmodem mit zwei weiblichen Steckern
- Gerade oder gekreuzte UTP-Kabel (Cat. 5)

Erstmalige Verbindung

Führen Sie dazu folgende Schritte durch:

1. Verbinden Sie den PowerConnect 3324/3348 mit dem RS232-Anschluss eines ASCII- Terminals.
2. Konfigurieren Sie folgende Einstellungen beim ASCII-Terminal, und wählen Sie den entsprechenden COM-Anschluss. In unserem Beispiel wird Windows Hyper Terminal verwendet:



ANMERKUNG: Für das neue Gerät ist die Standardbaudrate 9600. Wenn bei einer Baudrate von 9600 das Geräteterminal nicht angezeigt wird, stellen Sie eine andere Baudrate ein. Möglicherweise ist der Switch auf eine andere Baudrate eingestellt.

3. Verbinden Sie den ASCII-Terminal über ein Nullmodemkabel mit zwei weiblichen Steckern mit dem Switch.
4. Schließen Sie den Switch an die Stromversorgung an. Der folgende Bildschirm wird angezeigt:

```
**************************************************

***************** SYSTEM RESET *****************

**************************************************


Booting...


------ Performing the Power-On Self Test (POST( ------

UART Channel Loopback Test.....................PASS

Testing the System Cache.......................PASS

Testing the System SDRAM.......................PASS

Boot1 Checksum Test............................PASS

Boot1 Checksum Test............................PASS

Flash Image Validation Test....................PASS

Testing CPU PCI Bus Device Configuration.......PASS
```

```
BOOT Software Version 1.0.0.13 Built 11-May-2003 14:58:20

Processor: MPC8245 Rev 0.14, 250 MHz (Bus: 100MHz), 32 MByte SDRAM.

I-Cache 16 KB, linesize 32.D-Cache 16 KB, linesize 32.

Cache Enabled.

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.

Preparing to decompress...
```

Nach dem Dekomprimieren der Image-Datei wird der folgende Bildschirm angezeigt mit Informationen zum Gerät, Hard- und Software-Versionen sowie dem Status sämtlicher Schnittstellen (offen oder geschlossen):

```
Decompressing SW from image-2

8cc000

OK

Running from RAM...

Update Host params for stand-alone

****************************************************************

*** Running SW Ver. 1.0.0.52 Date 29-Jun-2003 Time 19:04:06 ***

****************************************************************

HW version is 00.00.01

Base Mac address is: 00:06:5b:ff:59:4d

Dram size is: 32M bytes
```

```
Dram first block size is: 20M bytes

Dram first PTR is: 0xB20000

Flash size is: 8M



STAND ALONE

The BCM5615_A1 0 initiate successfully

01-Jan-2000 01:01:10 %SSHD-W-NOHOSTKEY: SSH has been enabled but an encryption key was not found.

For key generation use the 'crypto key generate' commands. The service will start automatically when a host key is generated.

01-Jan-2000 01:01:11 %INIT-I-InitCompleted: Initialization task is completed



console> 01-Jan-2000 01:01:11 %BOX-I-PSUP: Power Supply #1 is up

01-Jan-2000 01:01:11 %BOX-W-PSNOTPRES: Power Supply #2 is not present

01-Jan-2000 01:01:11 %LINK-W-Down: 1/e1

01-Jan-2000 01:01:11 %LINK-W-Down: 1/e2

01-Jan-2000 01:01:11 %LINK-W-Down: 1/e3

.....

.....

Jan-2000 01:01:13 %LINK-W-Down: 1/e22

01-Jan-2000 01:01:13 %LINK-W-Down: 1/e23

01-Jan-2000 01:01:13 %LINK-W-Down: 1/e24

01-Jan-2000 01:01:13 %LINK-W-Down: 1/g1

01-Jan-2000 01:01:13 %LINK-W-Down: 1/g2
```

```
01-Jan-2000 01:01:14 %LINK-I-Up: Vlan 1

01-Jan-2000 01:01:14 %LINK-I-Up: 1/e1

console>
```

Der Switch kann jetzt konfiguriert werden.

Standardeinstellungen des Geräts

Um das Gerät auf die Standardeinstellungen zurückzusetzen, geben Sie an der Eingabeaufforderung für den Privileged Mode (#) den Befehl **delete startup-config** ein, und starten Sie es neu. Nach dem Neustart lädt das Gerät die Standardeinstellungen.

```
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 *****************

************************************************

.

.
```

.

.

Remote-Verwaltungszugriff

Um die Remote-Verwaltung des Geräts beispielsweise über Telnet oder Internet zu ermöglichen, führen Sie folgende Schritte aus:

1. Geben Sie an der Konsole den Befehl **enable** ein, um wie unten in den Privileged EXEC Mode zu gelangen:

```
console>enable
```

```
console#
```

2. Verbinden Sie die Management-Station über einen der Ethernet-Anschlüsse des Geräts wie nachfolgend dargestellt (Beispiel: e1). Die Verbindung kann auch über ein Netzwerk erfolgen, an das der Switch angeschlossen ist. Verwenden Sie für die Verbindung zwischen Management-Station (oder Netzwerk) und Switch ein CAT.5- Kabel. Stellen Sie über das ASCII-Terminal sicher, dass die Schnittstelle aktiviert ist und dass der STP-Status auf Weiterleitung (Forwarding) eingestellt ist (nach 30 s).

```
console>enable
```

```
Console#
```

```
01-Jan-2000 01:43:03 %LINK-I-Up: Vlan 1
```

```
01-Jan-2000 01:43:03 %LINK-I-Up: 1/e1
```

```
01-Jan-2000 01:43:34 %STP-I-PORTSTATUS: Port 1/e1: STP status Forwarding
```

3. Geben Sie an der Konsole den Befehl **configure** ein, um wie unten in den Konfigurationsmodus zu gelangen:

```
console> enable
```

```
console# configure
```

```
console(config)#
```

4. Geben Sie an der Konsole den Befehl **interface ethernet** ein, um wie unten in den Gerätekonfigurationsmodus über VLAN1 zu gelangen:

```
console> enable
```

```
console# configure
```

```
console(config)# interface vlan 1
```

```
console(config)# exit
```

5. Weisen Sie dem Switch-Anschluss, der mit der Management-Station verbunden ist, eine IP-Adresse zu. Auf diese Weise wird dem Switch eine IP-Adresse zugewiesen. In unserem Beispiel wurde die IP-Adresse 50.1.1.1 verwendet. Wenn die Management- Station direkt mit dem Switch verbunden ist, muss die IP-Adresse des Switches im gleichen Teilnetz liegen wie die IP-Adresse der Management-Station.

```
console> enable
```

```
console# configure
```

```
console(config)#
```

```
console(config-if)# ip address 50.1.1.2 /8
```

```
01-Jan-2000 01:48:37 %LINK-W-Down: Vlan 1
```

```
console (config-if)# exit
```

```
console(config)# exit
```

6. Wenn die Management-Station nicht direkt mit einem Anschluss, sondern mit einem Remote-Netzwerk verbunden ist, müssen Sie ein Standard-Gateway für den Switch definieren. Die zu konfigurierende Gateway-Adresse entspricht der IP-Adresse des Routers, an welchen der Switch angeschlossen ist.

```
console> enable
```

```
console# configure
```

```
console(config-if)#
```

```
console (config-if)# exit
```

```
console(config)# ip default-gateway 50.1.1.100
```

```
console(config)# exit
```

7. Senden Sie vom Switch aus einen Ping-Befehl an die Management-Station. Auf diese Weise stellen Sie sicher, dass die Verbindung hergestellt wurde. Warten Sie jedoch 30 Sekunden, bis der Switch in den Weiterleitungsmodus umgeschaltet hat. Die IP- Adresse der Management-Station lautet in diesem Beispiel 50.1.1.3:

```
console> enable
```

```
console# configure
```

```
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#
```

8. Definieren Sie einen Benutzernamen und ein Passwort mit der Berechtigungsebene 15, um einem Remote-Benutzer über Telnet oder Internet vollen Zugriff auf das Gerät zu ermöglichen. In unserem Beispiel lauten Benutzername und Passwort "Dell".

```
console#

console# configure

console(config)# username Dell password Dell level 15

console(config)#
```

9. Konfigurieren Sie Sicherheitspasswörter für Konsole, Telnet, SSH-, HTTP und HTTPS-Sitzungen:

```
console> enable

console# configure

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 admin
```

```
console (config-line)# exit

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 admin

console (config-line)# exit

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 admin

console (config-line)# exit

console(config)# ip http authentication local

console(config)# username admin password admin 15

console(config)# ip https authentication local

console(config)# username admin password admin 15

console(config)# crypto certificate generate key-generate

console(config)# ip https server
```

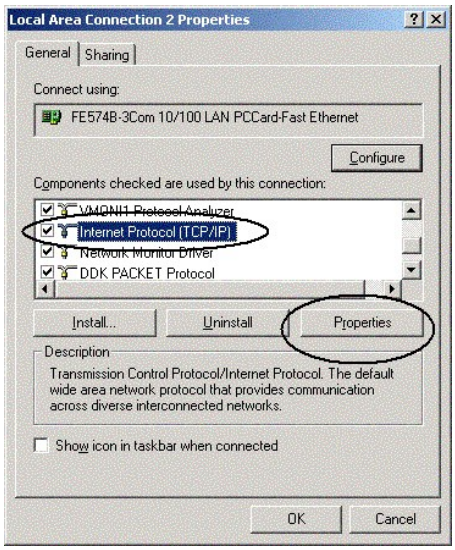
```
console(config)# exit


console# copy running-config startup-config
```

Das Gerät ist jetzt konfiguriert und kann von einer Webverwaltungsoberfläche aus verwaltet werden.

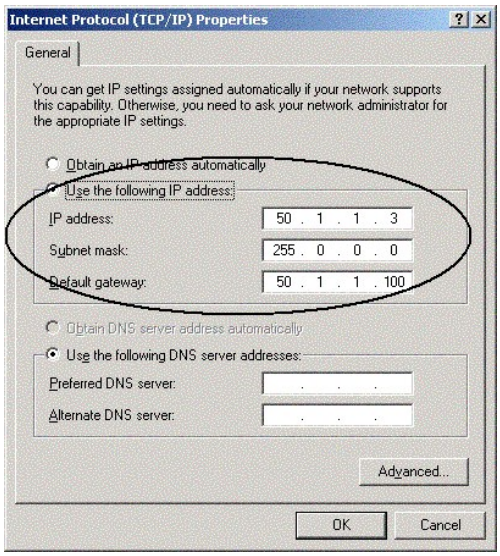
Die Management-Station konfigurieren

So konfigurieren Sie die Management-Station:

1. Weisen Sie dem PC, der als Remote-Management-Station fungieren soll, eine IP- Adresse zu. Klicken Sie unter Windows auf **Start > Einstellungen > Netzwerk- und DFÜ-Verbindungen.**
2. Klicken Sie mit der rechten Maustaste auf die Netzwerkverbindung, die für die Verwaltung verwendet wird. Wählen Sie "Eigenschaften".



3. Wählen Sie im Dialogfenster Eigenschaften von LAN-Verbindung den Eintrag für Internetprotokoll (TCP/IP), und klicken Sie auf **Eigenschaften**. Das Fenster Eigenschaften von Internetprotokoll (TCP/IP) wird angezeigt.



4. Wählen Sie **Folgende IP-Adresse verwenden**.
5. Definieren Sie im Fenster Eigenschaften von Internet Protokoll (TCP/IP) manuell (nicht über DHCP) eine statische IP-Adresse, Subnetzmaske und ein Standard- Gateway für den PC.

ANMERKUNG: Wenn der PC nicht direkt, sondern über einen Router an den PowerConnect 3324/3348 angeschlossen ist, muss als Standard-Gateway die IP-Adresse des Routers angegeben werden.

Telnet-Zugriff

Verwenden Sie Windows- oder DOS-Befehlszeilen bzw. eine Telnet-Anwendung, um über Telnet auf das Gerät zuzugreifen. Vergessen Sie nicht, das entsprechende Passwort einzugeben. Die Verbindung wird zu der für das Gerät festgelegten IP-Adresse hergestellt.

Nachdem Zugriff gewährt wurde, werden die Befehle genauso wie im direkten Gerätemanagement verwendet:

1. Gehen Sie im Windows-Menü auf **Start > Ausführen**, und geben Sie den Befehl "cmd" ein. Das Standardfenster für die Eingabeaufforderung wird angezeigt.
2. Geben Sie den Befehl **Telnet** und die IP-Adresse des Geräts ein.

```
Microsoft Windows 2000 [Version 5.00.2195]

(C) Copyright 1985-2000 Microsoft Corp.



C:\>telnet 50.1.1.2

01-Jan-2000 02:40:23 %MSCM-I-NEWTERM: New TELNET connection from 50.1.1.2

User Name:Dell

Password:****



console# show ip interface
```

```
Gateway IP Address Activity status

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

50.1.1.100 inactive


IP Address I/F

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

50.1.1.1/8 vlan 1


console#
```

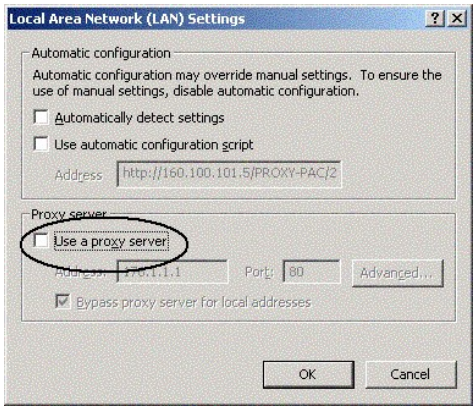
Beachten Sie, dass das Gerät über das ASCII-Terminal den Status der Telnet-Sitzung anzeigt:

```
console> 01-Jan-2000 02:39:04 %MSCM-I-NEWTERM: New TELNET connection from 50.1.1.3

01Jan-2000 02:39:11 %MSCM-I-TERMTERMINATED: TELNET connection from 50.1.1.3 terminated
```

Webzugriff (über einen HTTP-Server)

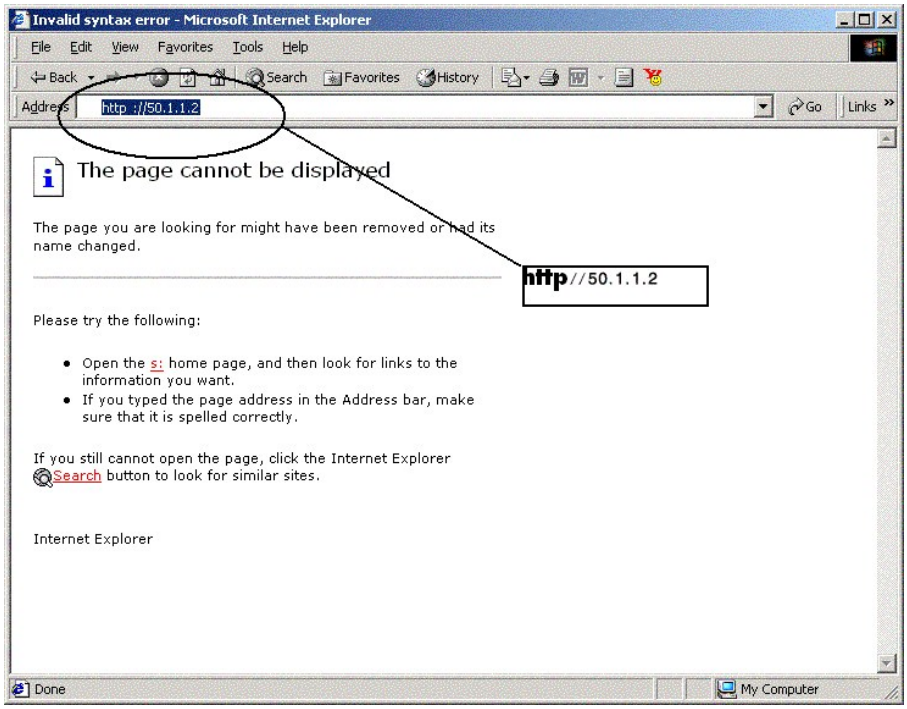
Für den Zugriff über das Internet führen Sie folgende Schritte durch:

1. Um bestimmte Probleme zu vermeiden, die während einer Sitzung mit einem HTTP- Proxy-Server auftreten können, deaktivieren Sie die Proxy-Server-Einstellung im Browser (in unserem Beispiel deaktiviert). Wählen Sie hierzu im Internet-Browser >Extras>Internetoptionen>Verbindungen>LAN-Einstellungen:



Deaktivieren Sie das Kontrollkästchen Proxyserver verwenden.

2. Geben Sie im Browserfenster die zuvor am Gerät konfigurierte IP-Adresse ein (mit oder ohne http://).

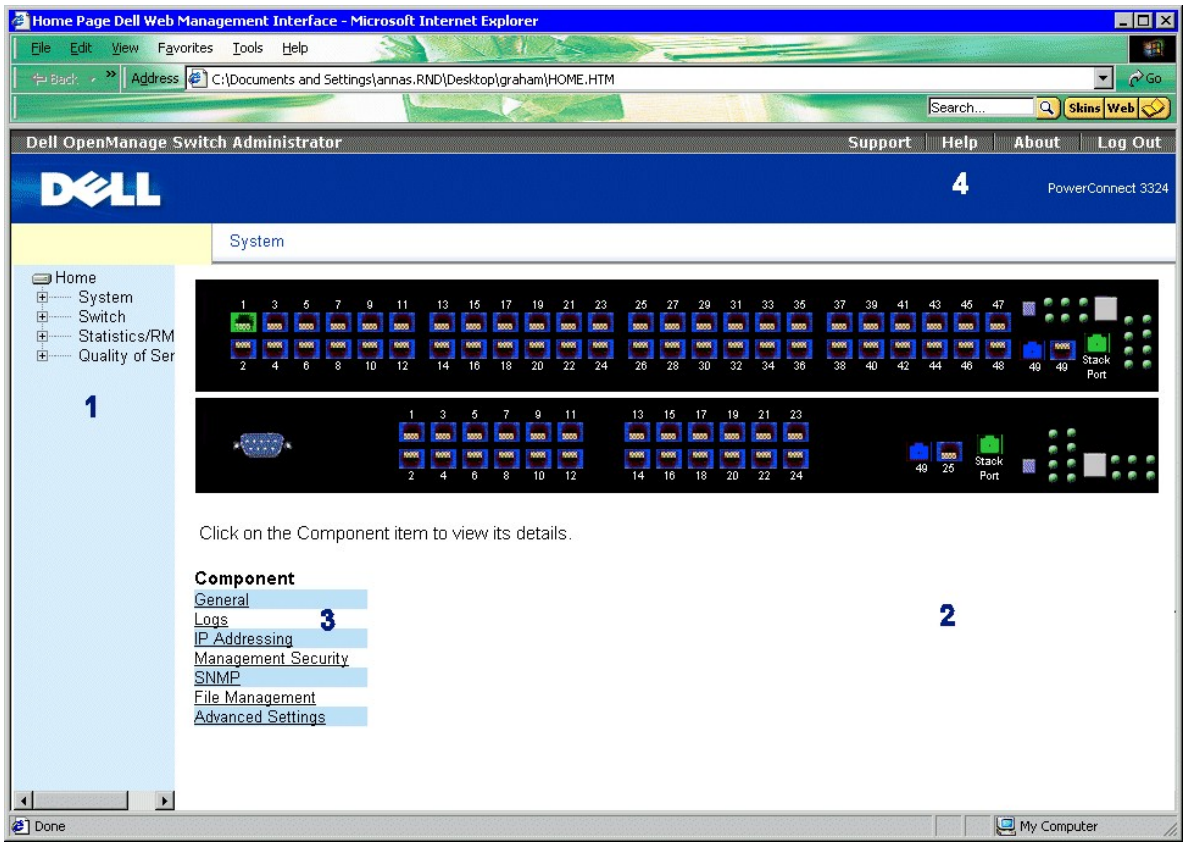


Anmelden auf der Schnittstelle

3. Wenn das Anmeldedialogfeld angezeigt wird, geben Sie Benutzernamen und Passwort ein:

Eingabeaufforderung für das Passwort

Die Webverwaltungsoberfläche für das Gerät wird angezeigt.



Webverwaltungsoberfläche des PowerConnect 3324/3348

In der **Oberflächenkomponenten-Tabelle zum PowerConnect 3324/3348** sind die Oberflächenkomponenten mit den dazugehörigen Nummern aufgelistet.

Stacking-Konfiguration

Einführung in das Stacking

PowerConnect 3324/3348-Stack-Einheiten fungieren als ein System. Jeder Stack verfügt über eine Mastereinheit und bis zu fünf Komponenten. Die Mastereinheit:

- verwaltet das Setup aller Komponenten
- konfiguriert Komponentenanschlüsse
- verwaltet im Komponentenkontext aufgetretene Ereignisse

Die Ereignisprotokolle aller Stack-Einheiten werden von der festgelegten Mastereinheit verwaltet und in Berichten zusammengefasst. Der Zugriff auf Komponenten erfolgt über die Mastereinheit, obwohl auch über das zugehörige ASCII-Terminal (RS-232-Anschluss) auf die einzelnen Einheiten zugegriffen werden kann.

Stacking-Voraussetzungen

Vor dem Aufbau eines Stacks müssen die folgenden Voraussetzungen erfüllt sein:

- Jede Einheit muss über ein Stack-Verbindungsmodul verfügen.

- Alle Kabel müssen ordnungsgemäß angeschlossen sein.
- Alle Einheiten müssen eingeschaltet sein. Nach wenigen Sekunden blinken die LEDs der Einheiten-IDs.
- Jede Komponente verfügt über eine Einheiten-ID. Weitere Informationen zur Auswahl von Einheiten-IDs finden Sie unter "Taste "Stack ID"".

Konfigurieren eines Stacks

Dieser Abschnitt enthält Anweisungen zum Konfigurieren eines Stacks. So konfigurieren Sie einen Stack:

ANMERKUNG: Die Stack-Einheiten-ID muss innerhalb von 15 Sekunden gewählt werden.

1. Schließen Sie die ausgewählte Mastereinheit an. Der Startvorgang des Gerätes beginnt.
2. Wählen Sie Einheit 1 über die Taste **Stack ID** aus, bis die Stack-LED 1 blinkt. Die LED hört innerhalb von 15 Sekunden auf zu blinken, wenn es sich bei der ausgewählten Einheit um den Stack-Master handelt.

ANMERKUNG: Wenn die Stack-LED weiterhin blinkt, gehört die Mastereinheit nicht der Gruppe an.

3. Schließen Sie die ausgewählte Komponente an. Der Startvorgang des Gerätes beginnt.
4. Wählen Sie innerhalb von 15 Sekunden über die Taste Stack ID **die Einheit 2.**
5. Wiederholen Sie Schritte 3 und 4 für alle Stack-Komponenten.

ANMERKUNG: Einheiten sollten nach ihrer Einheiten-ID in einem Stack angeordnet werden. Die Mastereinheit wird zuerst in den Stack aufgenommen, direkt gefolgt von Einheit 2.

Erweitern des Stacks

Dieser Abschnitt enthält Anweisungen zum Hinzufügen von Stack-Komponenten. So erweitern Sie einen Stack:

ANMERKUNG: Der Stack-Einheiten-ID muss innerhalb von 15 Sekunden gewählt werden.

1. Stellen Sie sicher, dass der Stack ordnungsgemäß funktioniert.
2. Verbinden Sie den unteren Stack-Anschluss mit der zusätzlichen Stack-Komponente.
3. Schließen Sie die neue Stack-Einheit an. Der Startvorgang des Gerätes beginnt.
4. Wählen Sie die Einheiten-ID innerhalb von 15 Sekunden über die Taste Stack ID **aus.**
5. Öffnen Sie für jede neue Komponente den vorhandenen Ring und schließen Sie das Stacking-Kabel an der neuen Komponente an.

Weitere Informationen zum Austauschen von Stack-Komponenten und zum Neuzuweisen von Einheiten-IDs finden Sie unter "Austauschen von Stack-Komponenten".

Neustart des Gerätes

ANMERKUNG: Vor dem Neustart des Gerätes sollte die Gerätekonfiguration gespeichert werden. Durch das Zurücksetzen des Gerätes werden nicht gespeicherte Konfigurationsänderungen verworfen.

1. Rufen Sie den CLI-Modus auf. Die folgende Eingabeaufforderung wird angezeigt:

```
Console > enable
```

2. Geben Sie Reload ein. Die folgende Meldung wird angezeigt:

```
>reload
```

```
This command will restart the whole system and disconnect your current session. Do you want to continue?
```

3. Geben Sie Y ein. Das Gerät wird neu gestartet.

Funktionen des Startmenüs

Über das Menü Startup werden zusätzliche Funktionen für die Gerätekonfiguration ausgeführt. Das Menü Startup enthält die folgenden Konfigurationsfunktionen:

- Herunterladen der Software
- Löschen der FLASH-Datei
- Löschen der FLASH-Sektoren

Der folgende Bildschirm zeigt das Menü Startup an:

```
[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: Startup Menu
```

Herunterladen der Software

Über das Menü Startup

Die Gerätesoftware kann über das Menü Startup heruntergeladen werden, auf das Sie während des Startvorgangs zugreifen können.

So starten Sie das Herunterladen der Software im CLI-Modus:

1. Rufen Sie den CLI-Modus auf. Die folgende Eingabeaufforderung wird angezeigt:

```
console>
```

2. Geben Sie reload ein. Die folgende Meldung wird angezeigt:

```
console>reload

This command will restart the whole system and disconnect your current session. Do you want to continue (y/n) [n]?
```

3. Geben Sie Y ein. Das Gerät wird neu gestartet.
4. Drücken Sie innerhalb von zwei Sekunden die Eingabetaste oder die ESC-Taste. Das Menü **Startup** wird angezeigt.

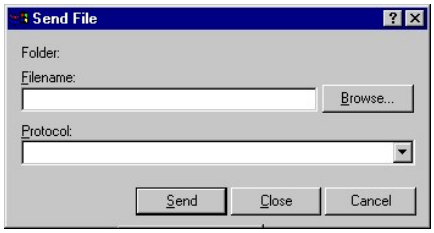
ANMERKUNG: Die Eingabetaste oder die Esc-Taste muss innerhalb von zwei Sekunden gedrückt werden, damit das Menü **Startup** angezeigt wird.

ANMERKUNG: Falls keine Auswahl erfolgt, läuft das Zeitlimit des Gerätes nach 35 Sekunden ab. Zeitlimits können über die CLI zurückgesetzt werden.

5. Geben Sie 1 ein. Die folgende Eingabeaufforderung wird angezeigt:

```
Downloading code using XMODEM.
```

6. Verwenden Sie ein beliebiges VT100-Emulationsprogramm, um die Option zum Herunterladen von Dateien auszuwählen. Das Fenster **Send File** wird angezeigt. klicken Sie auf die Schaltfläche **Send**.



Fenster "Send File"

7. Geben Sie den Dateipfad für die Konfigurationsdatei ein.
8. Stellen Sie sicher, dass das Protokoll als Xmodem definiert ist.
9. Klicken Sie auf **Send**. Die Software wird heruntergeladen.

Das Gerät wird automatisch neu gestartet.

ANMERKUNG: Vor dem Herunterladen der Software muss der TFTP-Server konfiguriert werden.

Löschen der FLASH-Datei

Die Gerätekonfiguration kann über das ASCII-Terminal gelöscht werden. Nach dem Löschen der Konfiguration müssen alle IP-Hostparameter sowie die über CLI, die Webverwaltungsoberfläche oder SNMP festgelegten Parameter neu konfiguriert werden.

So löschen Sie die Gerätekonfiguration:

1. Stellen Sie sicher, dass das ASCII-Terminal an das Gerät angeschlossen ist.
2. Schließen Sie das Netzkabel an. Das Gerät wird gestartet und das Menü **Startup** angezeigt. Der Startvorgang des Gerätes beginnt.
3. Drücken Sie innerhalb von zwei Sekunden die ESC-Taste, um den Vorgang abzubrechen, oder die Eingabetaste, um den Vorgang zu bestätigen. Das Menü **Startup** wird angezeigt.
4. Geben Sie die Nummer der gewünschten Menüoption ein, oder drücken Sie ESC, um den Vorgang abzubrechen. Geben Sie innerhalb von zwei Sekunden 2 ein. Die folgende Meldung wird angezeigt:

```
Warning! About to erase the file from flash Are you sure (Y/N)?
```

5. Geben Sie Y ein. Die folgende Meldung wird angezeigt.

```
? Flash file name (8 characters, Enter for none.)
```

6. Geben Sie config als Namen der FLASH-Datei ein. Die Konfiguration wird gelöscht und der Switch neu gestartet. Wie IP-Parameter bei einer Erstkonfiguration festgelegt werden, wird unter "Einführung in die Gerätekonfiguration" beschrieben.

Löschen der FLASH-Sektoren

Im FLASH-Speicher werden die ausführbare Image-, CDB- (MIB-Datei), Protokolldatei sowie weitere Dateien gespeichert.

HINWEIS: Falls der FLASH gelöscht wird, müssen alle Softwaredateien erneut heruntergeladen und installiert werden.

1. Stellen Sie sicher, dass das ASCII-Terminal an das Gerät angeschlossen ist.
2. Schließen Sie das Netzkabel an. Das Gerät wird gestartet und das Menü Startup angezeigt.
3. Geben Sie die Nummer der Menüoption ein, oder drücken Sie ESC, um den Vorgang abzubrechen. Geben Sie innerhalb von zwei Sekunden 3 ein. Die folgende Meldung wird angezeigt:

```
Warning! About to erase Flash Memory! FLASH size = 16252928. blocks = 64 Are you sure (Y/N)?
```

4. Bestätigen Sie durch Eingabe von Y. Die folgende Meldung wird angezeigt:

```
Enter First flash block (1 - 64):
```

5. Geben Sie den ersten zu löschenden FLASH-Block ein, und drücken Sie die Eingabetaste. Der Wertebereich umfasst die Werte 1 bis 64. Die folgende Meldung wird angezeigt:

```
Enter Last flash block (1 - 64):
```

6. Geben Sie den letzten zu löschenden FLASH-Block ein, und drücken Sie die Eingabetaste. Die folgende Meldung wird angezeigt:

```
Are you sure (Y/N)?
```

7. Bestätigen Sie durch Eingabe von Ys. Die folgende Meldung wird angezeigt:

```
Erasing flash blocks 1 - 1: Done.
```

Wiederherstellen von Passwörtern

So stellen Sie Passwörter für die Zugriffsmethode wieder her:

1. Starten Sie das Gerät (neu), und drücken Sie innerhalb von zwei Sekunden die <Eingabetaste>. Das Menü Startup wird angezeigt. Im Folgenden ist das Menü Startup dargestellt:

```
Startup menu

[1] Download sw

[2] Erase from flash

[3] Erase Flash

[4] Password Recovery Procedure
```

2. Geben Sie 4 ein, und drücken Sie die <Eingabetaste>. Die Zugriffsmethode wird zurückgesetzt.

ANMERKUNG: Definieren Sie die Passwörter für die Konsolenzugriffsmethode neu, um die Gerätesicherheit zu gewährleisten.

Weitere Informationen zur Konfiguration von Benutzerpasswörtern finden Sie unter *CLI User's Guide*.

Ausführen von Diagnoseprogrammen

Kontaktieren Sie vor Nutzung dieser Option den technischen Support von Dell. Siehe "Kontaktaufnahme mit Dell".

Herunterladen der Software auf die Stack-Einheiten

Die Software wird unter Verwendung einer der folgenden Methoden von einem TFTP-Server auf alle Stack-Einheiten heruntergeladen:

- Sequenzielles Herunterladen unter Verwendung der CLI
- Individuelles Herunterladen unter Verwendung der CLI
- Über Dell OpenManage™ Switch Administrator

Sequenzielles Herunterladen der Software unter Verwendung der CLI

1. Stellen Sie sicher, dass mindestens einem Anschluss der Mastereinheit eine IP-Adresse zugewiesen wurde.
2. Geben Sie `console# show version` ein, um zu überprüfen, welche Softwareversion derzeit auf den einzelnen Einheiten ausgeführt wird. Folgende Informationen werden beispielsweise angezeigt:

```
Unit SW version Boot version HW version

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

1 1.0.0.52 1.0.0.13 00.00.01

2 1.0.0.52 1.0.0.13 00.00.01
```

   Software-, Start- und Hardwareversion der einzelnen Einheiten werden angezeigt. Start- und Hardwareversion der Einheiten weichen im vorangehenden Beispiel voneinander ab, während die Softwareversion identisch ist.

3. Geben Sie `console# show bootvar` ein, um zu überprüfen, welche Image-Version auf den jeweiligen Einheiten aktiv ist. Folgende Informationen werden beispielsweise angezeigt:

```
Unit Active image Selected for next boot

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

1 image-2 image-2

2 image-1 image-1
```

   Sowohl die aktive Image-Datei als auch die Image-Datei, die nach dem Zurücksetzen des Gerätes aktiv ist, wird für alle Einheiten angezeigt.

4. Geben Sie `console# copy tftp://{tftp-Adresse}/{Dateiname} image` ein, um die Software auf die Mastereinheit zu kopieren. Die Datei wird zwar kopiert, muss jedoch noch als diejenige Image-Datei ausgewählt werden, die nach Zurücksetzen des Gerätes aktiv sein soll. Folgende Informationen werden beispielsweise angezeigt:

```
console# copy tftp://176.215.31.3/332448-10018.dos image
```

```
Erasing file image-1...done.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

ANMERKUNG: Jedes ! steht für die erfolgreiche Übertragung von 10 Paketen.

```
Copy: 2739187 bytes copied in 00:01:13 [hh:mm:ss]
```

5. Geben Sie console# copy tftp://50.1.1.2/332448-10018.dos unit://2/image ein. Die Gerätesoftware wird auf Stack-Komponente 2 kopiert: //2/image steht für die Einheiten-ID der Stack-Komponente, auf welche die Software kopiert wird. Folgende Informationen werden beispielsweise angezeigt:

```
...................Unit 2: Erased image-1

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!

Copy: 2744590 bytes copied in 00:01:41 [hh:mm:ss]

console# 01-Jan-2000 01:01:55 %COPY-W-TRAP: The copy operation was completed successfully
```

6. Wiederholen Sie Schritt 5 für jede Stack-Komponente. Stellen Sie sicher, dass die Software auf die Stack-Komponente mit der richtigen Einheiten-ID kopiert wird.
7. Geben Sie console# boot system image-2 ein, um die Image-Datei festzulegen, die nach Zurücksetzen des Gerätes verwendet werden soll.
8. Geben Sie console# boot system unit 2 image-1 ein. Dadurch wird angegeben, dass das Gerät beim Neustart Image 1 verwendet.
9. Geben Sie console# reload ein. Die folgende Meldung wird angezeigt:

```
This command will reset the whole system and disconnect your current session. Do you want to continue (y/n) [n]?
```

10. Geben Sie Y ein. Das Gerät wird neu gestartet.
11. Wiederholen Sie die Schritte 2 und 3, um zu überprüfen, welche Image-Dateien aktiv sind.

Individuelles Herunterladen der Software unter Verwendung der CLI

Dieser Abschnitt enthält Anweisungen dazu, wie Gerätesoftware auf folgende Weisen individuell für die einzelnen Stack-Komponenten heruntergeladen wird:

- von einem TFTP-Server auf eine Mastereinheit
- von der Mastereinheit auf Komponenten

1. Stellen Sie sicher, dass mindestens einem Anschluss der Mastereinheit eine IP-Adresse zugewiesen wurde.
2. Geben Sie console# show version ein, um zu überprüfen, welche Softwareversion derzeit auf den einzelnen Einheiten ausgeführt wird. Folgende Informationen werden beispielsweise angezeigt:

```
Unit SW version Boot version HW version

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

1 1.0.0.52 1.0.0.13 00.00.01

2 1.0.0.52 1.0.0.13 00.00.01
```

Software-, Start- und Hardwareversion der einzelnen Einheiten werden angezeigt. Start- und Hardwareversion der beiden Einheiten weichen im vorangehenden Beispiel voneinander ab, während die Softwareversion identisch ist.

3. Geben Sie console# show bootvar ein, um zu überprüfen, welche Image-Version auf den jeweiligen Einheiten aktiv ist. Folgende Informationen werden beispielsweise angezeigt:

```
Unit Active image Selected for next boot

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

1 image-2 image-2

2 image-1 image-1
```

Sowohl die aktive Image-Datei als auch die Image-Datei, die nach dem Zurücksetzen des Gerätes aktiv ist, wird für alle Einheiten angezeigt.

4. Geben Sie console# copy tftp://*{tftp-Adresse}*/*{Dateiname}* image ein, um die Software auf die Mastereinheit zu kopieren. Die Datei wird zwar kopiert, muss jedoch noch als diejenige Image-Datei ausgewählt werden, die nach Zurücksetzen des Gerätes aktiv sein soll. Folgende Informationen werden beispielsweise angezeigt:

```
console# copy tftp://176.215.31.3/332448-10018.dos image

Erasing file image-1...done.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Copy: 2739187 bytes copied in 00:01:13 [hh:mm:ss]
```

5. Geben Sie console# boot system image-1 ein, um die Image-Datei festzulegen, die nach Zurücksetzen des Gerätes verwendet werden soll.
6. Geben Sie console# reload ein. Die folgende Meldung wird angezeigt:

```
This command will reset the whole system and disconnect your current

session. Do you want to continue (y/n) [n]?
```

7. Geben Sie Y ein. Das Gerät wird neu gestartet.
8. Wiederholen Sie Schritt 3, um zu überprüfen, welche Image-Dateien aktiv sind.
9. Geben Sie console# copy image unit://2/image ein. Folgende Informationen werden beispielsweise angezeigt:

```
console# copy image unit://2/image

...................Unit 2: Erased image-2

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!

Copy: 2883576 bytes copied in 00:01:35 [hh:mm:ss]
```

```
console# 01-Jan-2000 01:08:59 %COPY-W-TRAP: The copy operation was completed successfully
```

10. Geben Sie `console# boot system unit {Einheiten-ID} image-{Dateiname}` ein.
11. Wiederholen Sie Schritt 9 für jede Stack-Einheit.
12. Geben Sie `console# reload` ein. Die folgende Meldung wird angezeigt:

```
This command will reset the whole system and disconnect your current

session. Do you want to continue (y/n) [n]?
```

13. Geben Sie `Y` ein. Das Gerät wird neu gestartet.
14. Wiederholen Sie die Schritte 2 und 3, um sicherzustellen, dass die richtige Image- Datei aktiv ist.

Herunterladen der Software über PowerConnect 3324/3348 Dell OpenManage Switch Administrator

Hinweise zum Herunterladen der Software über den Dell OpenManage Switch Administrator finden Sie unter "Verwalten von Dateien".

Definieren der SNMP-Einstellungen

SNMP (Simple Network Management Protocol) bietet eine Methode zur Verwaltung von Netzwerkgeräten. SNMP unterstützende Geräte führen lokale Software (einen Agenten) aus.

Die SNMP-Agenten verwalten eine Liste von Variablen, die zur Verwaltung des Gerätes verwendet werden. Die Variablen werden in der MIB (Management Information Base) definiert. Die MIB stellt die vom Agenten gesteuerten Variablen dar. Der SNMP-Agent definiert das Format für die MIB-Spezifikationen sowie das Format für den Netzwerkzugriff auf Daten.

Die Zugriffsrechte auf die SNMP-Agenten werden über Zugriffszeichenfolgen gesteuert. Um mit dem Gerät zu kommunizieren, übermittelt der integrierte Webserver zuerst eine gültige Community-Zeichenfolge für die Authentisierung.

Die Community-Standardzeichenfolgen für das PowerConnect-Gerät lauten:

- Public - Ermöglicht, dass entsprechend berechtigte Management-Stationen MIB-Objekte abrufen können.
- Private - Ermöglicht, dass entsprechend berechtigte Management-Stationen MIB-Objekte abrufen und ändern können.

Falls SNMP nicht verwendet wird:

- Ändern Sie die Community-Standardzeichenfolgen, um unberechtigte Zugriffe auf das PowerConnect-Gerät zu verhindern.
- Löschen Sie beide Community-Strings. Der SNMP-Verwaltungszugriff auf das PowerConnect-Gerät ist deaktiviert, wenn keine Community-Zeichenfolgen vorhanden sind.

So können Sie die Strings löschen:

ANMERKUNG: Um den Konfigurationskontext nutzen zu können, müssen Benutzer über die Berechtigungsebene 15 verfügen.

1. Geben Sie `Enable` ein. An der Eingabeaufforderung wird das Zeichen "#" angezeigt.
2. Geben Sie `configure` ein, und drücken Sie die Eingabetaste, falls der globale Konfigurationskontext auf Privileged Exec-Ebene nicht aktiviert ist.
3. Geben Sie `no snmp-server community private` ein, und drücken Sie anschließend die Eingabetaste, um den Community-String private zu löschen.

4. Geben Sie `no snmp-server community public` ein, und drücken Sie anschließend die Eingabetaste, um den Community-String **public** zu löschen.
5. Geben Sie `exit` ein. Der Konfigurationskontext wird beendet.
6. Geben Sie `copy running-config startup-config` ein, um die Konfigurationsänderungen zu speichern, und drücken Sie anschließend die Eingabetaste.

Geräte anschließen

Sobald dem PowerConnect IP-Adressen zugewiesen wurden, können Netzwerkverbindungen über die RJ45-Anschlüsse auf der Vorderseite des PowerConnect-Gerätes hergestellt werden.

HINWEIS: Wenn die Auto-Negotiation-Funktion für einen RJ-45-Anschluss deaktiviert ist, wird auch die automatische Konfiguration des MDI/MDI-X-Pin-Signals deaktiviert.

So verbinden Sie ein Gerät mit einem SFP-Transceiver-Anschluss:

1. Beachten Sie bei der Auswahl eines geeigneten SFP-Transceiver-Typs die Verkabelungsanforderungen.
2. Stecken Sie den (separat erhältlichen) SFP-Transceiver in den SFP Transceiver- Steckplatz.
3. Verwenden Sie die geeignete Netzwerkverkabelung, um ein Gerät mit den Anschlüssen am SFP-Transceiver zu verbinden.

HINWEIS: Wenn der SFP-Transceiver einen Link erhält, wird der zugewiesene integrierte 10/100/1000BASE-T-Anschluss deaktiviert.

Um alle Geräte auszuschalten, ziehen Sie das Kabel des Netzteils aus der Steckdose. Die Steckdose sollte sich in der Nähe der Geräte befinden und leicht zugänglich sein.

Das Prüfzeichen B besagt, dass das Gerät die Schutzanforderungen der Normen PN-93/T-42107 und PN-EN 55022:1996 erfüllt. 1996.

Zurück zum Inhalt

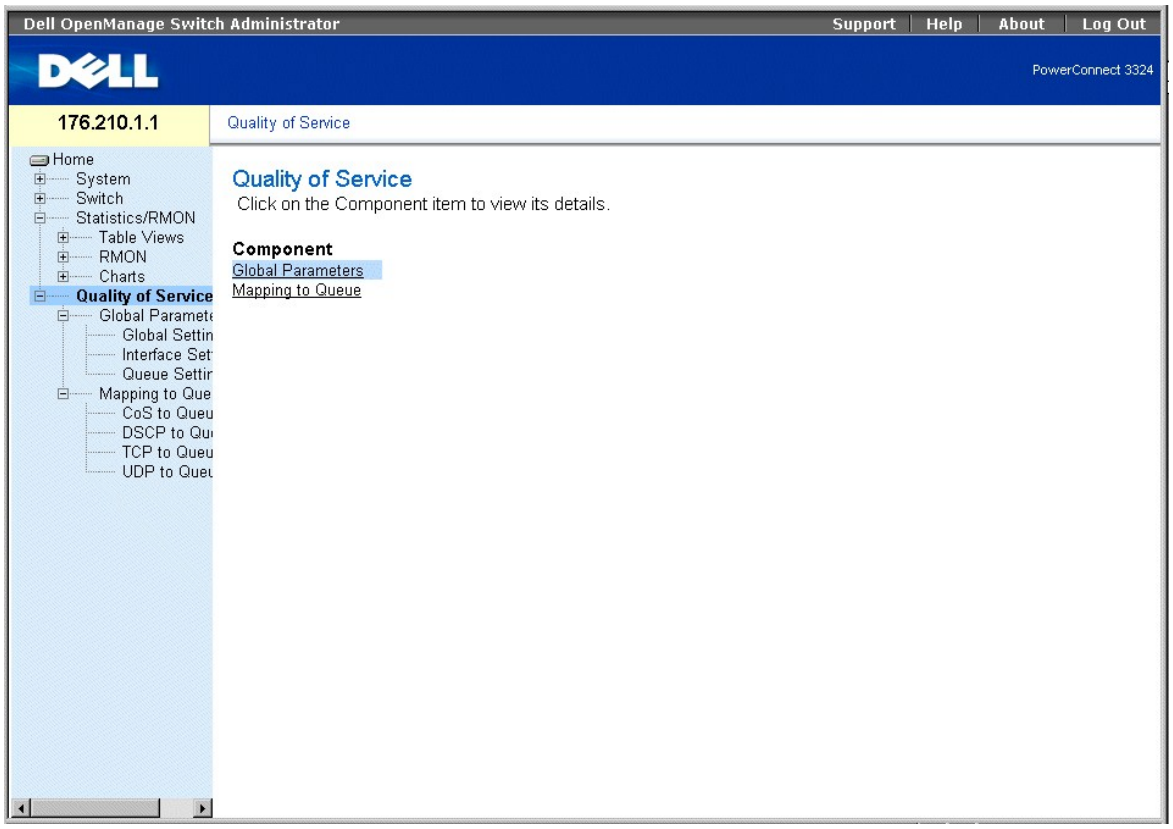
Zurück zum Inhalt

Konfigurieren von Quality of Service (QoS)

Dell™ PowerConnect™ 3324/3348 Benutzerhandbuch

Dieser Abschnitt enthält Informationen zum Definieren und Konfigurieren von QoS-(Quality of Service-)Parametern.

- Klicken Sie in der Strukturansicht auf **Quality of Service**. Die Seite **Quality of Service** wird geöffnet.



Seite "Quality of Service"

Dieser Abschnitt enthält die folgenden Themen:

Übersicht über Quality of Service (QoS)

Mittels Quality of Service (QoS) können innerhalb eines Netzwerks QoS- und Prioritätswarteschlangen implementiert werden. QoS optimiert den Fluss des Netzwerkverkehrs auf der Grundlage von Richtlinien, Frame-Zählern und Kontext.

QoS wirkt sich auf Sprach-, Video- und Echtzeitdatenverkehr aus, welcher einer Warteschlange mit hoher Priorität zugewiesen werden kann. Sonstiger Datenverkehr kann einer Warteschlange mit niedrigerer Priorität zugewiesen werden. Das Ergebnis ist ein optimierter Datenfluss in Hochleistungsnetzwerken.

QoS wird durch folgende Kriterien definiert:

- Klassifizierung - Legt fest, welchen Paketfeldern spezifische Werte zugewiesen werden. Alle mit den benutzerdefinierten Spezifikationen übereinstimmenden Pakete werden unter einer Kategorie zusammengefasst.
- Action - Definiert die Verwaltung des Datenverkehrs, wobei die Pakete auf der Grundlage von Paketinformationen und Paketfeldwerten, wie VLAN-Priorität (VPT) und DSCP (DiffServ Code Point), weitergeleitet werden.
- Prioritization - Dem Datenverkehr wird eine Priorität zugewiesen, und er wird zur Weiterleitung in die entsprechende Warteschlange eingereiht.

CoS-(Class of Service-)Informationen

Einer von vier Weiterleitungswarteschlangen (Warteschlangen 1 bis 4) können acht CoS-Werte zugewiesen werden. Jede Warteschlange verfügt über eine unterschiedliche Priorität. Die erste Warteschlange weist die niedrigste und die vierte Warteschlange die höchste Weiterleitungspriorität auf, wobei letztere standardmäßig nicht zugewiesen wird.

ANMERKUNG: In einer Stack-Konfiguration wird Warteschlange 4 für die Weiterleitung des Stack-Datenverkehrs verwendet. Folglich kann ein Konflikt mit der Stack-Steuerung entstehen, wenn Warteschlange 4 zusätzlicher Datenverkehr zugewiesen wird.

Die folgenden drei Zuweisungstabellen sind verfügbar:

- CoS to Queue Mapping Table.
- DSCP to Queue Mapping Table.
- TCP/UDP to Queue Mapping Table. Die TCP/UDP-Tabelle ist standardmäßig leer.

Die **CoS to Queue Mapping Table** enthält die CoS-Standardzuweisungen zu den Werten der Weiterleitungswarteschlangen:

CoS-Wert	Werte der Weiterleitungswarteschlangen
0	W2
1	W1 (Niedrigste Priorität = Best Effort)
2	W1 (Niedrigste Priorität = Best Effort)
3	W2
4	W2
5	W3
6	W3
7	W3

Standardwerte der CoS to Queue Mapping Table

Die CoS-Zuweisung wird auf Systembasis aktiviert. Die CoS-Werte reichen von 0 bis 7, wobei 0 der niedrigsten und 7 der höchsten Priorität entspricht.

DSCP-Werte können Prioritätswarteschlangen zugewiesen werden. Die **DSCP to Queue Mapping Table** enthält die DSCP-Standardzuweisungen zu den Werten der Weiterleitungswarteschlangen:

Standardwerte der "DSCP to Queue Mapping Table"

DSCP-Wert	Werte der Weiterleitungswarteschlangen
0-7	W1 (Niedrigste Priorität)
8-15	W1
16-23	W2
24-31	W2
32-39	W2
40-47	W3
48-55	W3

55-63	W3 (Höchste Priorität)

Die DSCP-Zuweisung wird auf Systembasis aktiviert.

QoS-Dienste

Nachdem Pakete einer bestimmten Warteschlange zugewiesen wurden, können der oder den Warteschlangen QoS-Dienste zugewiesen werden. Ausgabewarteschlangen werden unter Verwendung einer der folgenden Methoden mit einem Zeitplan konfiguriert:

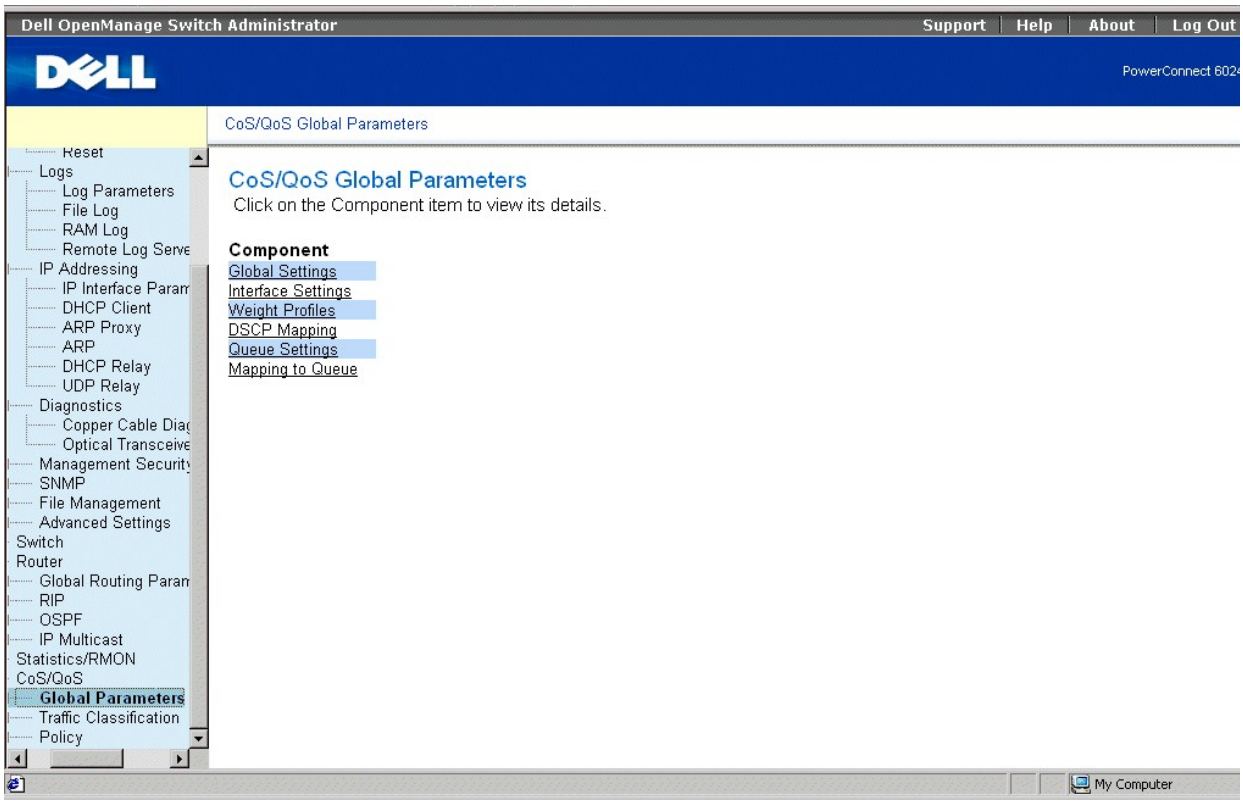
- Strict Priority - Stellt sicher, dass zeitkritische Anwendungsdaten immer beschleunigt weitergeleitet werden. Durch die "Strict Priority" können Netzwerkadministratoren unternehmenswichtigem, zeitkritischem Datenverkehr eine höhere Priorität als weniger zeitkritischen Anwendungen zuweisen. Bei Anwendung der "Strict Priority" wird "Voice-over-IP"-Datenverkehr beispielsweise vor FTP- oder E-Mail-(SMTP-)Datenverkehr weitergeleitet. Bevor der Datenverkehr der übrigen Warteschlangen weitergeleitet werden kann, muss die "Strict Priority"-Warteschlange leer sein.
- Weighted Round Robin - Stellt sicher, dass die Weiterleitungskapazität des PowerConnect 3324/3348 nicht vorrangig von einer einzelnen Anwendung beansprucht wird. Bei "Weighted Round Robin (WRR)" werden vollständige Warteschlangen nach dem Reigenmodell weitergeleitet. Warteschlangenprioritäten werden durch die Warteschlangenlänge definiert. Je länger die Warteschlange ist, desto höher ist die Weiterleitungspriorität der Warteschlange. Wenn vier Warteschlangen beispielsweise die Wertigkeit 1, 2, 3 und 4 haben, werden Pakete mit der höchsten Weiterleitungspriorität Warteschlange 4 und Pakete mit der niedrigsten Weiterleitungspriorität Warteschlange 1 zugewiesen. Indem Warteschlange 4 die höchste Weiterleitungspriorität zugewiesen wird, wird sichergestellt, dass Datenverkehr mit höherer Priorität nach dem WRR-(Weighted Round Robin-)Modell verarbeitet und Datenverkehr niedrigerer Priorität in angemessener Zeit weitergeleitet wird.

Die Zeitplanung wird für das gesamte System aktiviert. Warteschlangen, auf die die "Strict Priority"-Richtlinie angewendet wurde, werden automatisch der Warteschlange mit der höchsten Priorität zugewiesen. Standardmäßig wird für alle Werte "Strict Priority" festgelegt. Beim Wechsel zum WRR-Modus lautet die Standardwertigkeit 1. Wertigkeiten für Warteschlangen können mittels WRR in beliebiger Reihenfolge zugewiesen werden. WRR-Werte können auf Systembasis zugewiesen werden. Best Effort-Datenverkehr wird immer der ersten Warteschlange zugewiesen. Damit Warteschlange 1 Best Effort-orientiert bleibt, müssen WRR-Werte zugewiesen werden.

Definieren globaler QoS-Parameter

Globale QoS-(Quality of Service-)Parameter werden auf den Seiten **QoS Global Parameters** festgelegt. So öffnen Sie die Seite **QoS Global Parameters** :

- Wählen Sie in der Strukturansicht **Quality of Service** > **Global Parameters** aus. Die Seite **QoS Global Parameters** wird geöffnet.



Seite "QoS Global Parameters"

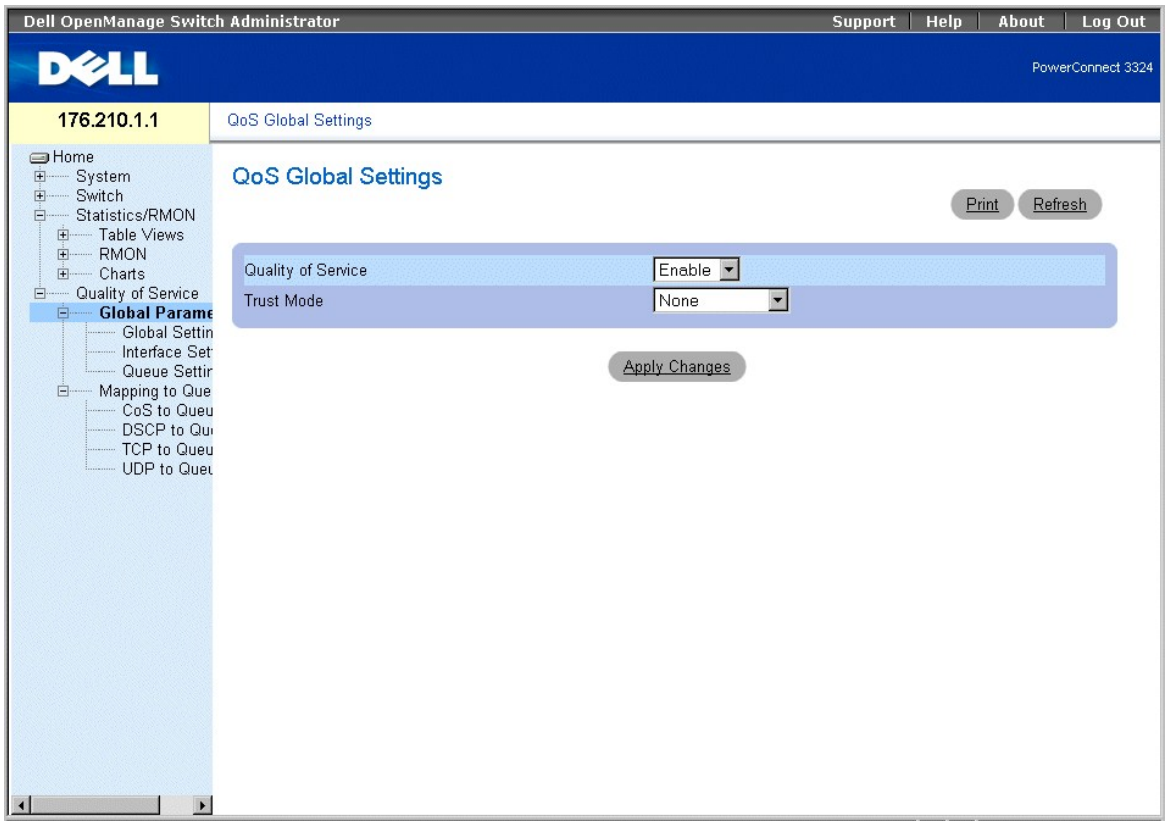
Die Seite **QoS Global Parameters** enthält Links zu:

- Konfigurieren globaler QoS-Einstellungen
- Definieren von QoS-Schnittstelleneinstellungen
- Definieren von Warteschlangeneinstellungen

Konfigurieren globaler QoS-Einstellungen

Auf der Seite **QoS Global Settings** kann der Benutzer QoS aktivieren oder deaktivieren. Zusätzlich kann der Benutzer den **Trust Mode** auswählen. In diesem Modus wird die Ausgangswarteschlange, und somit der Dienst für das Paket, auf der Basis vordefinierter Felder innerhalb des Pakets bestimmt. So öffnen Sie die Seite **QoS Global Settings**:

- Wählen Sie in der Strukturansicht **Quality of Service > Global Parameters > Global Settings**. Die Seite **QoS Global Settings** wird geöffnet.



Seite "QoS Global Settings"

Die Seite **QoS Global Settings** enthält folgende Felder:

- **Quality of Service** - Ermöglicht die Verwaltung des Netzwerkverkehrs mittels QoS. Die Optionen der Feldwerte lauten:
  - **Enable** - Aktiviert QoS für das Gerät.
  - **Disable** - Deaktiviert QoS für das Gerät.
- **Trust Mode** - Legt fest, anhand welcher Paketfelder auf dem Switch eingehende Pakete klassifiziert werden. Wenn keine Regeln definiert wurden, wird Datenverkehr, der das vordefinierte Paketfeld (CoS-Wert, DSCP-Wert oder TCP/UDP-Anschluss) enthält, entsprechend der relevanten Trust Mode-Tabelle zugewiesen. Datenverkehr, der kein vordefiniertes Paketfeld enthält, wird der Best Effort-Warteschlange zugewiesen. Die möglichen Feldwerte für den Trust Mode lauten:
  - **CoS** - Gibt an, dass die zugewiesene Ausgabewarteschlange über die IEEE802.1p VLAN-Prioritätskennung (VPT) oder die einem Anschluss zugewiesenen Standard-VPT ermittelt wird.
  - **DSCP** - Gibt an, dass die Zuweisung der Ausgangswarteschlange über das DSCP-Feld ermittelt wird.
  - **TCP/UDP** - Gibt an, dass die Ausgangswarteschlange über den TCP/UDP-Anschluss ermittelt wird.

ANMERKUNG: Die globale Einstellung **Trust** wird durch die Einstellung **Trust** der Schnittstelle überschrieben.

Aktivieren von Quality of Service:

1. Öffnen Sie die Seite **QoS Global Settings**.
2. Wählen Sie **Enable** im Feld **Quality of Service** aus.
3. Klicken Sie auf **Apply Changes**. Quality of Service wird für das Gerät aktiviert.

Aktivieren des Trust Mode:

1. Öffnen Sie die Seite **QoS Global Settings**.
2. Wählen Sie die Trust-Einstellung im Feld **Trust Mode** aus.
3. Klicken Sie auf **Apply Changes**. Trust Mode wird für das Gerät aktiviert/deaktiviert.

Aktivieren des Trust Mode mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zur Konfiguration von Feldern auf der Seite **QoS Global Settings** zusammengefasst.

CLI-Befehl	Beschreibung
qos trust [cos | dscp | tcp-udp-port]	Konfiguriert das System für den Basismodus und den Trust-Status.
qos	Aktiviert QoS für das Gerät.
no qos trust	Kehrt in den Nicht-Trust-Status zurück.

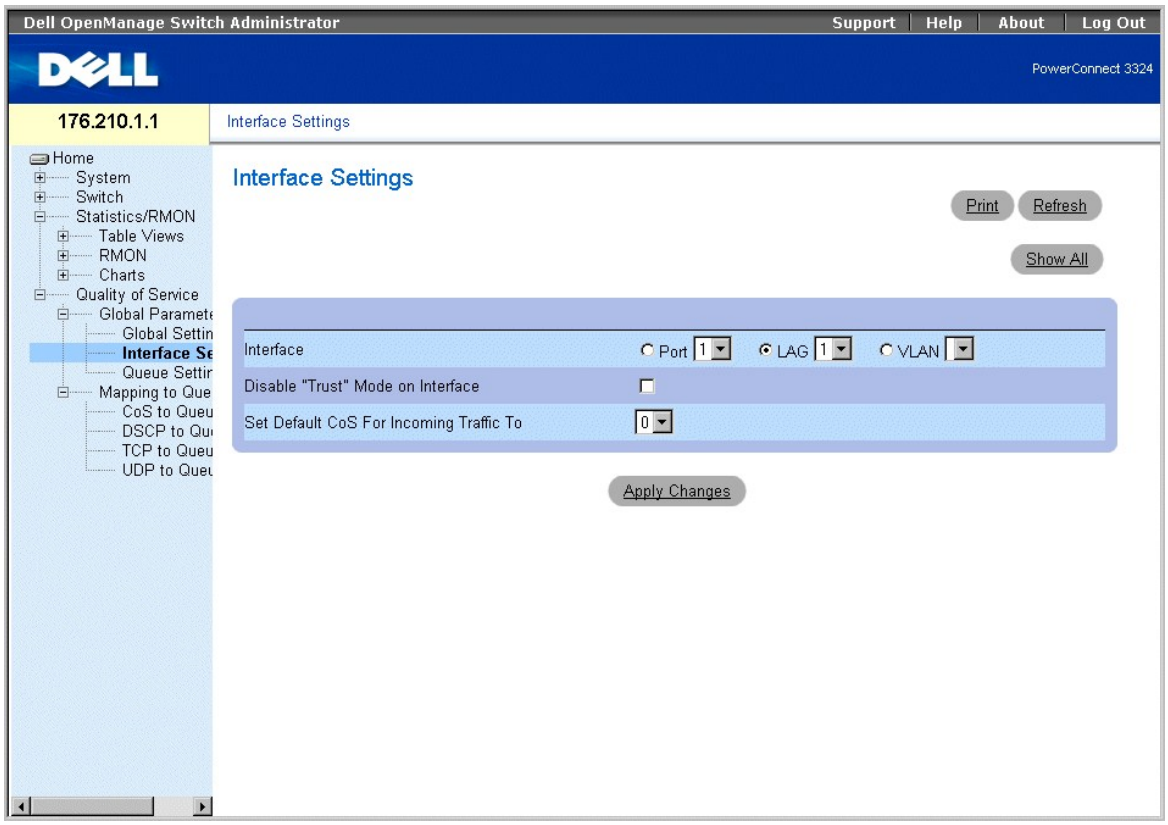
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# qos

Console (config)# qos trust dscp
```

Definieren von QoS-Schnittstelleneinstellungen

Auf der Seite **QoS Interface Settings** kann der Benutzer pro Schnittstelle definieren, ob der ausgewählte Trust Mode aktiviert werden soll. Darüber hinaus wird auf der Seite **QoS Interface Settings** die Standardpriorität für eingehende Pakete ohne Kennung ausgewählt. So öffnen Sie die Seite **QoS Interface Settings**:

- Klicken Sie in der Strukturansicht auf **Quality of Service > Global Parameters > Interface Settings**. Die Seite **QoS Interface Settings** wird geöffnet.



Seite "Interface Settings"

Die Seite **QoS Interface Settings** enthält folgende Felder:

- **Interface** - Gibt die spezifische Schnittstelle an, auf die der Trust Mode angewendet wird. Der Trust Mode wird auf folgende Elemente anwendet:
  - **Port** - Gibt die Anschlussnummer an.
  - **LAG** - Gibt die LAG-Nummer an.
  - **VLAN** - Gibt die VLAN-Nummer an.
- **Disable "Trust" Mode on Interface** - Deaktiviert Trust-Werte für das Gerät. Weitere Informationen zu den Trust-Einstellungen finden Sie unter "Konfigurieren globaler QoS-Einstellungen".
- **Set Default CoS For Incoming Traffic To** - Legt für Pakete ohne Kennung den Wert der CoS-Standardkennung fest. Die Werte der CoS-Kennung lauten 0 bis 7. Der Standardwert lautet **0**.

Zuweisen von QoS/CoS-Einstellungen für eine Schnittstelle:

1. Öffnen Sie die Seite **QoS Interface Settings**.
2. Wählen Sie eine Schnittstelle im Feld **Interface** aus.
3. Aktivieren Sie das Kontrollkästchen **Disable "Trust" Mode on Interface**, falls der Trust Mode für die jeweilige Schnittstelle deaktiviert werden soll.
4. Legen Sie den erforderlichen Wert für **Default CoS For Incoming Traffic** fest.
5. Klicken Sie auf **Apply Changes**. Die QoS/CoS-Einstellungen werden der Schnittstelle zugewiesen.

Zuweisen von QoS/CoS-Schnittstellen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zur Konfiguration von Feldern auf der Seite **QoS Interface Settings** zusammengefasst.

CLI-Befehl	Beschreibung
qos trust	Aktiviert den Trust-Status für die einzelnen Anschlüsse.

qos cos *Standard-CoS*	Konfiguriert den CoS-Standardwert des Anschlusses.
no qos trust	Deaktiviert den Trust-Status für die einzelnen Anschlüsse.

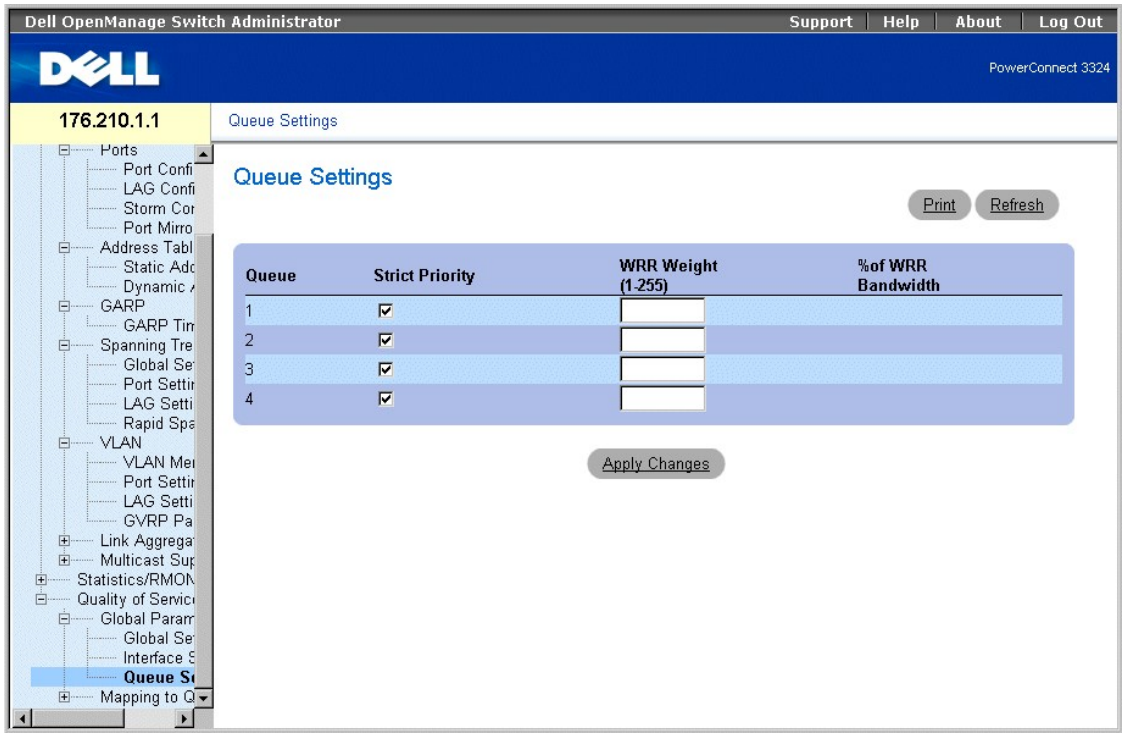
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# interface ethernet 1/e5

Console (config-if)# qos trust

Console (config-if)# qos cos 3
```

Definieren von Warteschlangeneinstellungen

Auf der Seite **Queue Settings** können Netzwerkadministratoren Weighted Round Robin (WRR) konfigurieren sowie Bandbreitenwerte für Warteschlangen zuweisen. Jede Warteschlange wird mit unterschiedlichen WRR- und WRED-(Weighted Random Early Detection-)Werten definiert. So öffnen Sie die Seite **Queue Settings**:

- Wählen Sie in der Strukturansicht **Quality of Service > Global Parameters > Queue Settings** aus. Die Seite **Queue Settings** wird geöffnet.



Seite "Queue Settings"

Die Seite **Queue Settings** enthält folgende Felder:

- **Queues** - Gibt die Warteschlangennummer an.

ANMERKUNG: Die Überlastung einer Warteschlange kann einen Netzwerkstau verursachen.

- **Strict Priority** - Gibt an, ob die Zeitplanung des Datenverkehrs strikt nach Warteschlangenpriorität erfolgt. Diese Option ist standardmäßig aktiviert.

- **WRR** - Gibt an, ob die Warteschlangen-Zeitplanung für den Datenverkehr auf dem WRR-Schema basiert.
- **WRR Weight** - Weist Egress-Warteschlangen WRR-Wertigkeiten zu. Die Feldwerte reichen von 1 bis 255, wobei 1 der niedrigste und 255 der höchste Wert ist.
- **% of WRR Bandwidth** - Gibt die dem WRR zugewiesene Bandbreitenkapazität an.

Definieren der Warteschlangeneinstellungen:

1. Öffnen Sie die Seite **Queue Settings**.
2. Definieren Sie die Felder **Scheduling, WRR Weight** und **Bandwidth**.
3. Klicken Sie auf **Apply Changes**. Die Seite **Queue Settings** und das Gerät werden aktualisiert.

Zuweisen von Warteschlangeneinstellung mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zur Konfiguration von Feldern auf der Seite **Queue Settings** zusammengefasst.

CLI-Befehl	Beschreibung
wrr-queue bandwidth *Wertigkeit1 Wertigkeit2. Wertigkeit_n*	Weist Egress-Warteschlangen WRR-(Weighted Round Robin-)Wertigkeiten zu.
show qos interface [*Schnittstellen-ID***] [queuing]**	Zeigt QoS-Daten der Schnittstelle an.

Im Folgenden ein Beispiel für die CLI-Befehle:

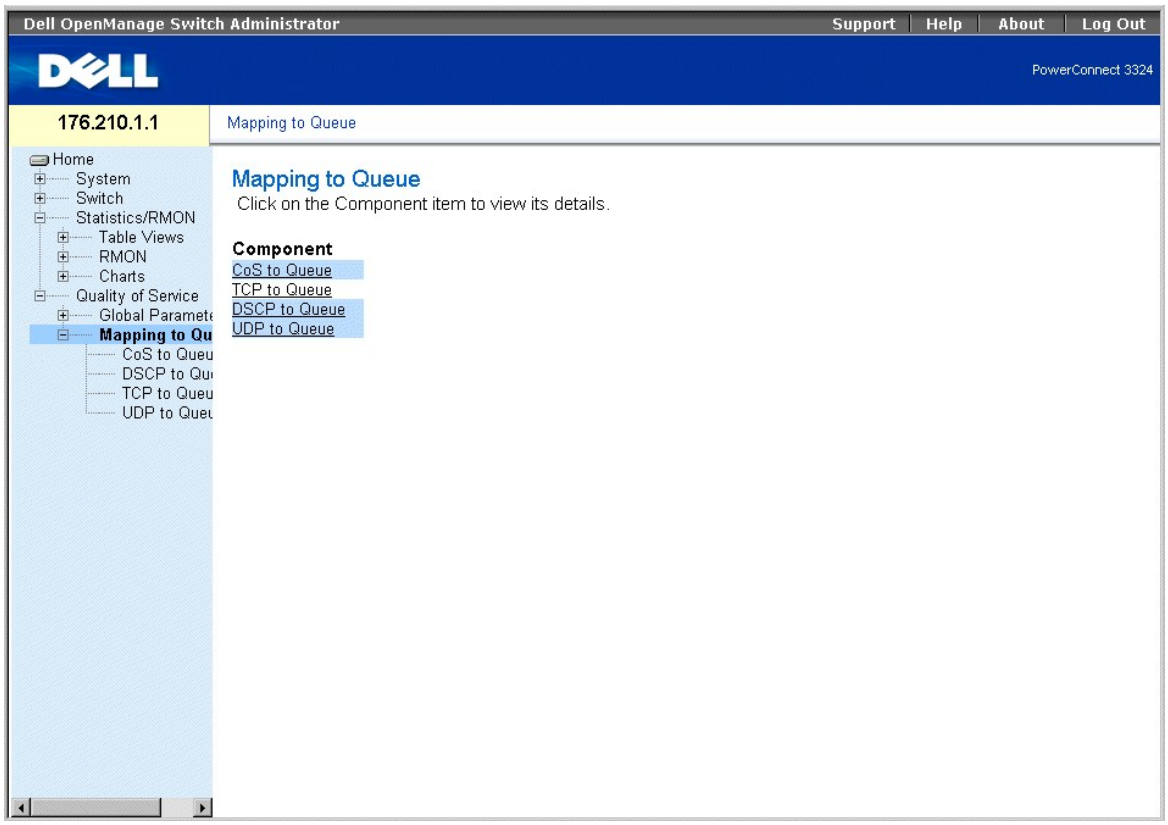
```
Console (config)# wrr-queue bandwidth 10 20 30 40

Console (config)# exit

Console # exit

Console> show qos interface ethernet 1/e3 queueing

Ethernet 1/e3

wrr bandwidth weights and EF priority:

qid-weights Ef - Priority

1 — 10 dis- N/A

2 — 20 dis- N/A

3 — 30 dis- N/A

4 — 1 dis- N/A

Cos-queue map:
```

```
cos-qid

0 - 2

1 - 1

2 - 1

3 - 2

4 - 2

5 - 3

6 - 3

7 - 3
```

Zuweisen zu Warteschlangen

Die Seite **Mapping to Queue** enthält Links zu Seiten, auf denen QoS-Warteschlangen CoS- und DSCP-Werte sowie TCP- und UDP-Anschlüsse zugewiesen werden können. So öffnen Sie die Seite **Mapping to Queue**:

- Wählen Sie **Quality of Service > Mapping to Queue**. Die Seite **Mapping to Queue** wird geöffnet.



Seite "Mapping to Queue"

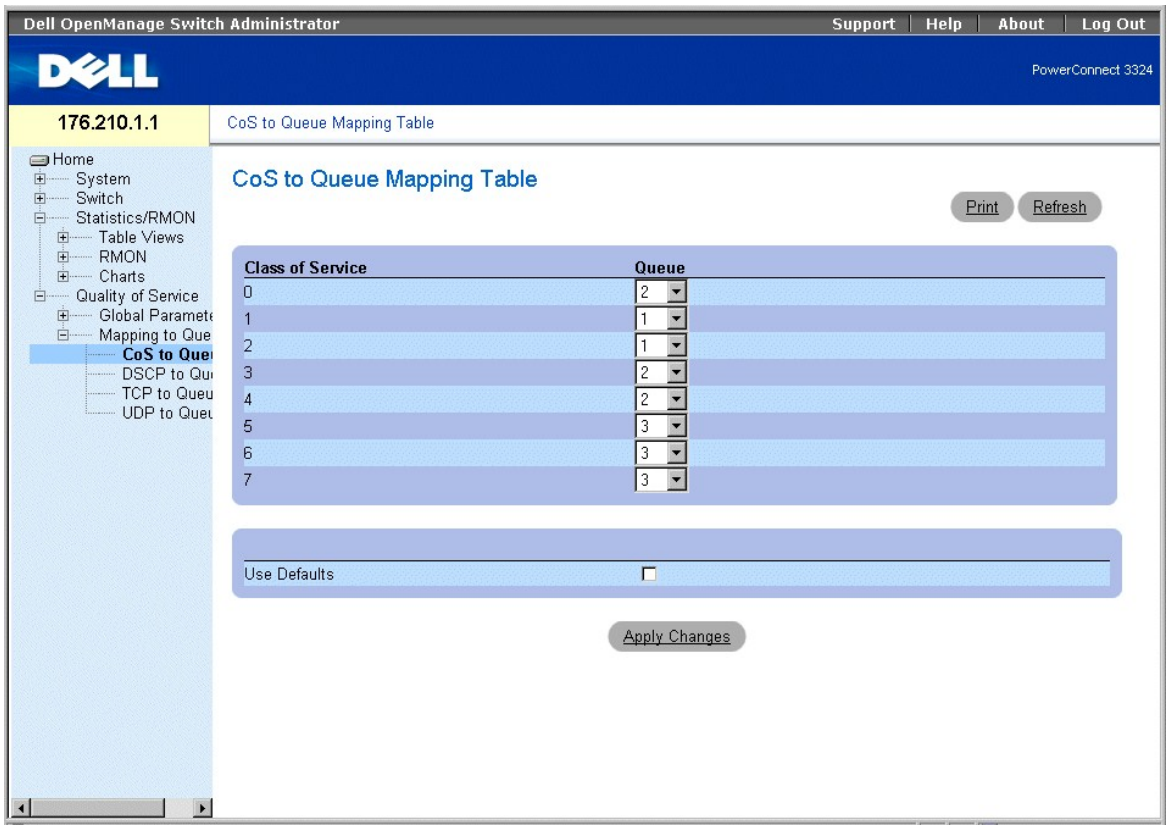
Die Seite **Mapping to Queue** enthält Links zu den folgenden Themen:

- Zuweisen von CoS-Werten zu Warteschlangen
- Zuweisen von TCP-Anschlusswerten zu Warteschlangen
- Zuweisen von DSCP-Werten zu Warteschlangen
- Zuweisen von UDP-Anschlusswerten zu Warteschlangen

Zuweisen von CoS-Werten zu Warteschlangen

Auf der Seite **CoS to Queue** können Netzwerkadministratoren CoS-Einstellungen für Netzwerkverkehrs-Warteschlangen klassifizieren. So öffnen Sie die Seite **CoS to Queue Mapping Table**:

- Wählen Sie in der Strukturansicht **Quality of Service >Mapping to Queue > CoS to Queue** aus. Die Seite **CoS to Queue Mapping Table** wird geöffnet.



Seite "CoS to Queue Mapping Table"

Die Seite **CoS to Queue Mapping Table** enthält folgende Felder:

- **Class of Service** - Gibt die Werte der CoS-Prioritätskennung an, wobei 0 der niedrigsten und 7 der höchsten Priorität entspricht.
- **Queue** - Gibt die Warteschlange für die Weiterleitung des Datenverkehrs an, der die CoS-Priorität zugewiesen wurde. Es werden vier Warteschlangen mit Datenweiterleitungsprioritäten unterstützt.

ANMERKUNG: In einer Stack-Konfiguration wird Warteschlange 4 für die Weiterleitung des Stack-Datenverkehrs verwendet. Folglich kann ein Konflikt mit der Stack-Steuerung entstehen, wenn Warteschlange 4 zusätzlicher Datenverkehr zugewiesen wird.

- **Use Defaults** - Verwendet die Gerätestandardwerte, um einer Weiterleitungswarteschlange CoS-Werte zuzuweisen.

Zuweisen eines CoS-Wertes zu einer Warteschlange:

1. Öffnen Sie die Seite **CoS to Queue**.
2. Wählen Sie einen CoS-Eintrag aus.
3. Definieren Sie die Warteschlangennummer im Feld **Queue**.
4. Klicken Sie auf **Apply Changes**. Der CoS-Wert wird einer Warteschlange zugewiesen und das Gerät aktualisiert.

Zuweisen von CoS-Werten zu Warteschlangen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Konfiguration von Feldern in der **Mapping CoS Values to Queues Table** zusammengefasst.

CLI-Befehl	Beschreibung
wrr-queue cos-map *Warteschlangen-ID* **cos1.cosn**	Weist den Egress-Warteschlangen festgelegte CoS-Werte zu.

Im Folgenden ein Beispiel für die CLI-Befehle:

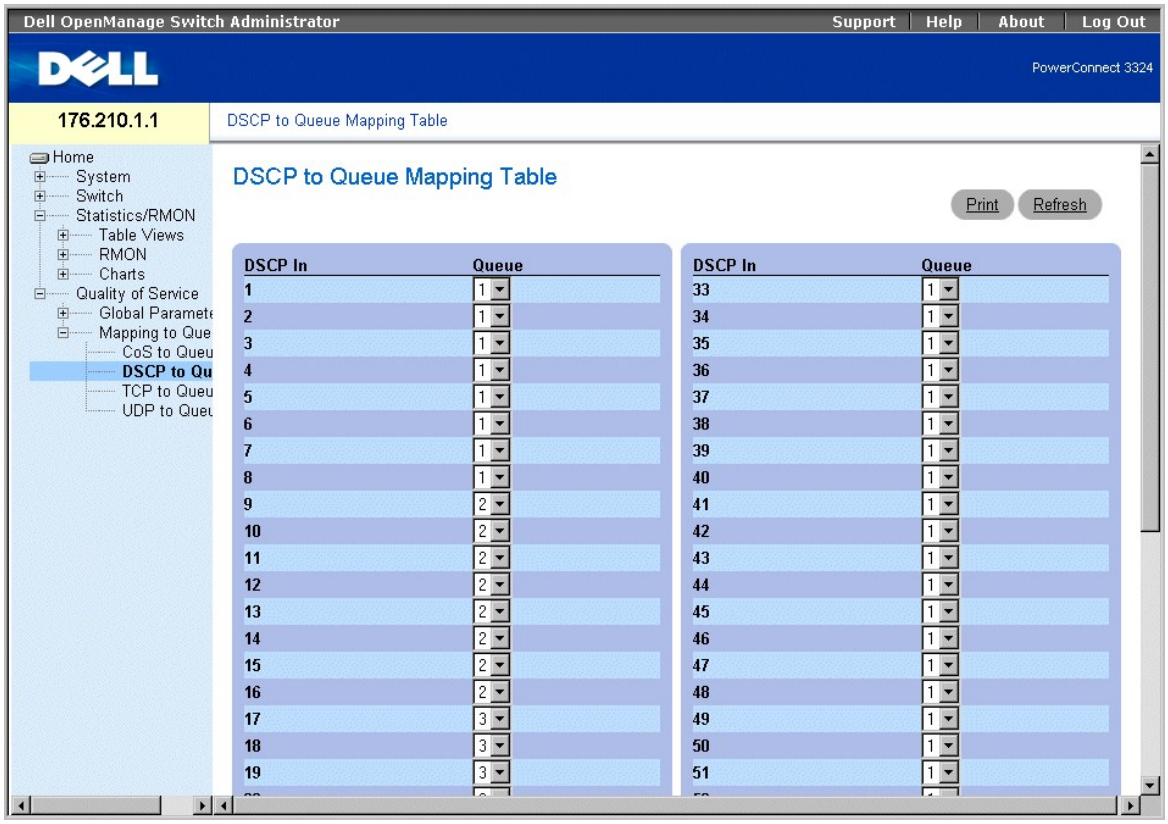
```
Console (config)# wrr queue cos-map 4 7
```

Zuweisen von DSCP-Werten zu Warteschlangen

Auf der Seite **DSCP Mapping** können Netzwerkverwalter die Ausgangswarteschlange bestimmen, die einem spezifischen DSCP-Feld zugewiesen wird. So öffnen Sie die Seite **DSCP Mapping**:

ANMERKUNG: Eine Auflistung der DSCP-Standardeinstellungen für Warteschlangen finden Sie unter den Standardwerten der DSCP to Queue Mapping Table Default Values.

- Wählen Sie in der Strukturansicht **Quality of Service > Global Parameters > Global Settings > DSCP Mapping.** Die Seite **DSCP Mapping** wird geöffnet.



Seite "DSCP Mapping"

Die Tabelle DSCP to Queue Mapping enthält die folgenden Felder:

ANMERKUNG: In einer Stack-Konfiguration wird Warteschlange 4 für die Weiterleitung des Stack-Datenverkehrs verwendet. Folglich kann ein Konflikt mit der Stack-Steuerung entstehen, wenn Warteschlange 4 zusätzlicher Datenverkehr zugewiesen wird.

- **DSCP In** - Gibt die Werte des DSCP-Feldes im eingehenden Paket an.
- **Queue** - Gibt die Warteschlange an, der Pakete mit dem spezifischen DSCP-Wert zugewiesen werden. Die Werte lauten 1 bis 4, wobei 1 der niedrigste und 4 der höchste Wert ist.

Zuweisen eines DSCP-Wertes und einer Prioritätswarteschlange:

1. Öffnen Sie die Seite **DSCP Mapping**.
2. Wählen Sie einen Wert in der Spalte **DSCP In** aus.
3. Wählen Sie einen zugehörigen Wert für **Queue**.
4. Klicken Sie auf **Apply Changes**. Der DSCP-Wert wird nicht außer Kraft gesetzt, und dem Wert wird eine Weiterleitungswarteschlange zugewiesen.

Zuweisen von DSCP-Werten mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zur Konfiguration von Feldern auf der Seite **DSCP Mapping** zusammengefasst.

CLI-Befehl	Beschreibung
qos map dscp-queue *DSCP-Liste zu Warteschlangen-ID*	Ändert die Zuweisung zwischen DSCP und Warteschlange.

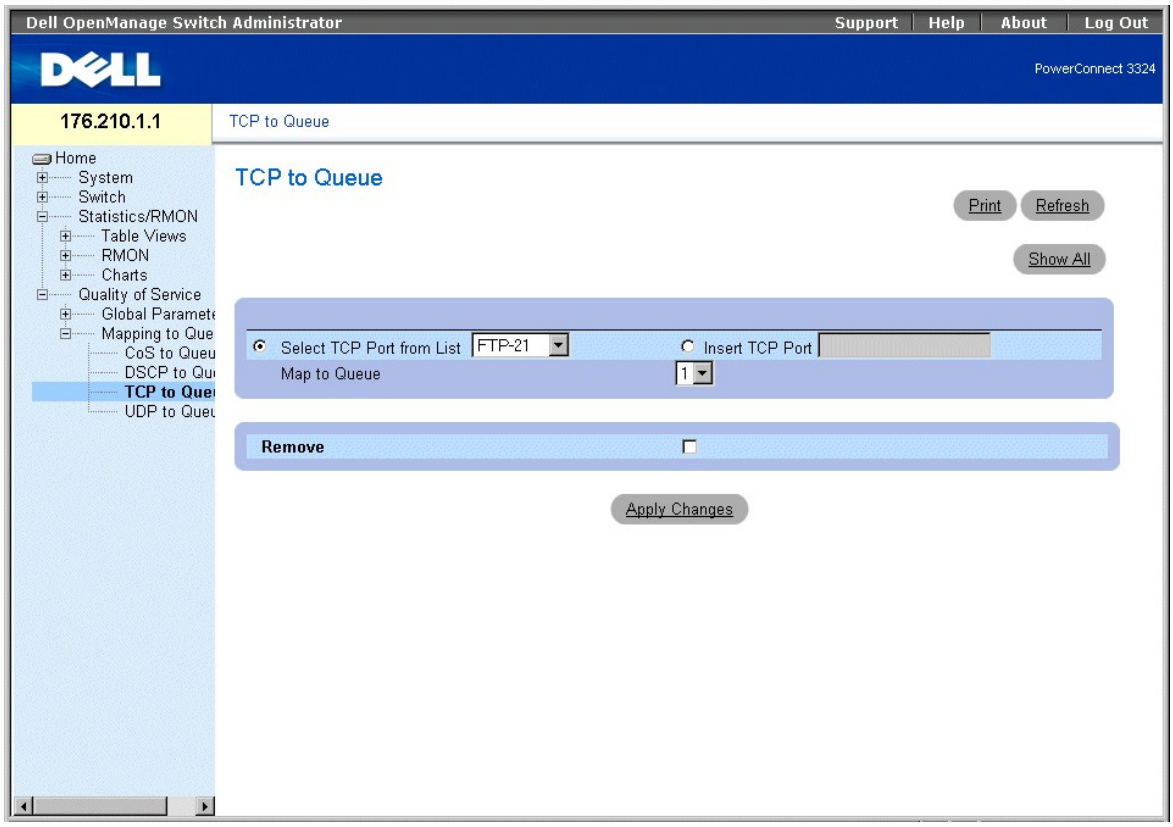
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# qos map dscp-queue 33 40 41 to 1
```

Zuweisen von TCP-Anschlusswerten zu Warteschlangen

Auf der Seite **TCP to Queue** können Netzwerkverwalter den Datenverkehr klassifizieren, der über spezifische TCP-Zielanschlüsse an Warteschlangen weitergeleitet wird. So öffnen Sie die Seite **TCP to Queue**:

- Wählen Sie in der Strukturansicht **Quality of Service >Mapping to Queue > TCP to Queue** aus. Die Seite **TCP to Queue** wird geöffnet.



Seite "TCP to Queue"

Die Seite **TCP to Queue** enthält folgende Informationen:

- **Select TCP Port from List** - Bietet eine Dropdown-Liste vordefinierter, häufig verwendeter TCP-Anschlüsse.
- **Insert TCP Port** - Ermöglicht die Definition eines neuen TCP-Anschlusses.
- **Map to Queue** - Gibt die Netzwerkverkehrs-Warteschlange an, welcher der TCP-Anschluss zugewiesen wird.

ANMERKUNG: In einer Stack-Konfiguration wird Warteschlange 4 für die Weiterleitung des Stack-Datenverkehrs verwendet. Folglich kann ein Konflikt mit der Stack-Steuerung entstehen, wenn Warteschlange 4 zusätzlicher Datenverkehr zugewiesen wird.

- **Remove** - Entfernt eine TCP-Anschlusszuweisung.
  - **Aktiviert** - Entfernt eine spezifische TCP-Anschlusszuweisung.
  - **Deaktiviert** - Behält eine TCP-Anschlusszuweisung bei.

Zuweisen eines TCP-Anschlusses zu einer Netzwerkverkehrs-Warteschlange:

1. Öffnen Sie die Seite **TCP to Queue**.
2. Wählen Sie einen Anschluss in der **TCP Port List** aus.

   Oder

   Aktivieren Sie das Kontrollkästchen **Insert TCP Port**. Das Feld **New TCP Port** wird aktiviert. Definieren Sie einen neuen TCP-Anschluss.
3. Wählen Sie eine Warteschlangennummer in der Dropdown-Liste **Map to Queue** aus.
4. Klicken Sie auf **Apply Changes**. Dem TCP-Anschluss wird eine Weiterleitungswarteschlange zugewiesen.

Ändern einer "TCP-Anschluss-zu-Netzwerkverkehrs-Warteschlange"-Zuweisung:

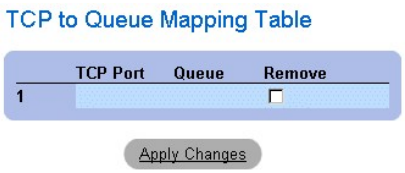
1. Öffnen Sie die Seite **TCP to Queue**.
2. Wählen Sie einen Anschluss in der Dropdown-Liste **TCP Port List** aus. Die Warteschlange, der der Anschluss zugewiesen ist, wird in der Dropdown-

Liste **Map to Queue** angezeigt.

3. Wählen Sie eine neue Netzwerkverkehrs-Warteschlange in der Dropdown-Liste **Map to Queue** aus.
4. Klicken Sie auf **Apply Changes**. Der TCP-Anschluss wird der neuen Netzwerkverkehrs-Warteschlange zugewiesen.

Anzeigen der TCP to Queue Mapping Table:

1. Öffnen Sie die Seite **TCP to Queue**.
2. Klicken Sie auf **Show All**. Die **TCP to Queue Mapping Table** wird geöffnet.



TCP to Queue Mapping Table

Entfernen einer TCP-Anschlusszuweisung aus der **TCP to Queue Mapping Table**:

1. Öffnen Sie die Seite **TCP to Queue**.
2. Klicken Sie auf **Show All**. Die **TCP to Queue Mapping Table** wird geöffnet.
3. Wählen Sie einen Anschluss in der Dropdown-Liste **TCP Port List** aus. Die Warteschlange, welcher der Anschluss zugewiesen ist, wird in der Dropdown-Liste **Map to Queue** angezeigt.
4. Aktivieren Sie das Kontrollkästchen **Remove**.
5. Klicken Sie auf **Apply Changes**. Der TCP-Anschluss wird aus der Netzwerkverkehrs- Warteschlange entfernt.

Zuweisen von TCP-Anschlüssen zu Warteschlangen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zur Konfiguration von Feldern auf der Seite **TCP to Queue** zusammengefasst.

CLI-Befehl	Beschreibung
qos map tcp-port-queue *Anschluss1.Anschluss8 to Warteschlangen-ID*	Ändert den der Warteschlange zugewiesenen TCP-Anschluss.
show qos map tcp-port-queue	Zeigt den der Warteschlange zugewiesenen TCP-Anschluss an.
no qos map tcp-port-queue	Entfernt den TCP-Anschluss aus einer Warteschlange.

Im Folgenden ein Beispiel für die CLI-Befehle:

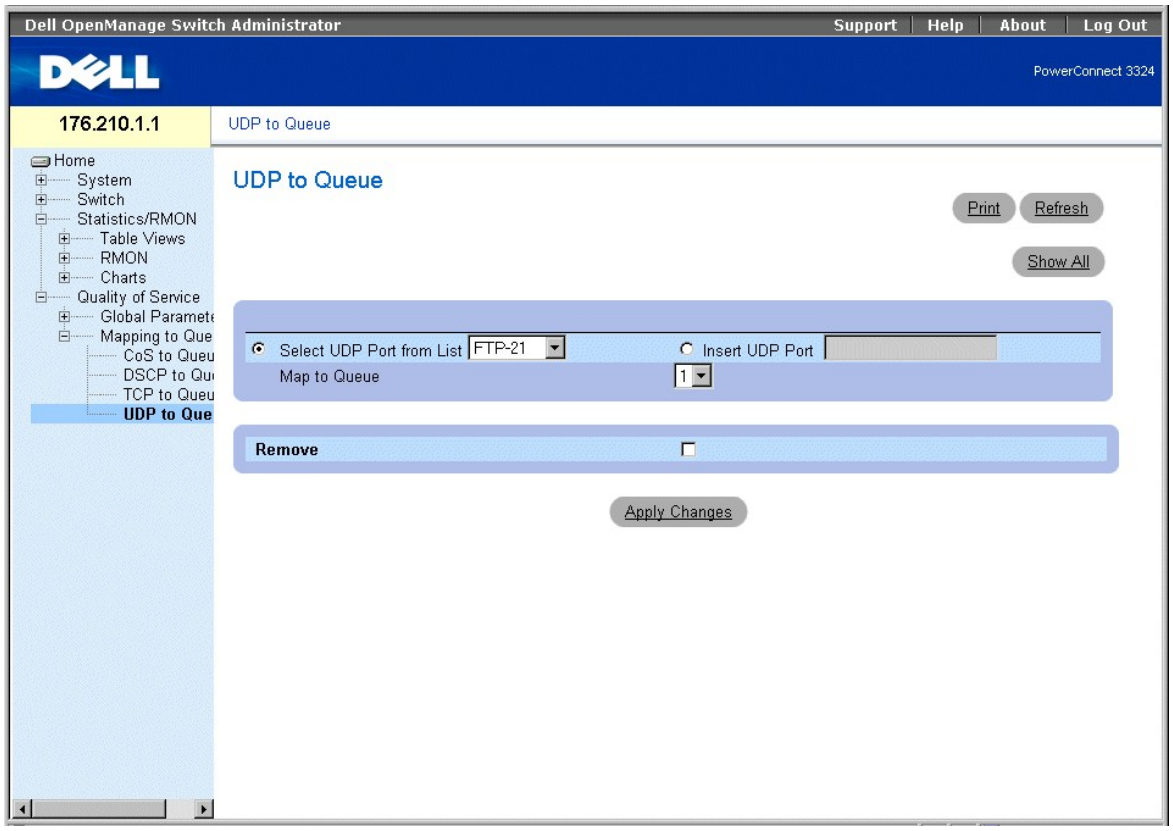
```
Console (config)# qos map tcp-port-queue 6001 to 2

Console (config)# exit

Console # exit

Console (config)# show qos map tcp-port-queue

Tcp port-queue map:
```

```
Port queue

----- ------

6000 1

6001 2

6002 3
```

Zuweisen von UDP-Anschlusswerten zu Warteschlangen

Auf der Seite **UDP to Queue** können Netzwerkverwalter den Datenverkehr klassifizieren, der über spezifische UDP-Anschlüsse an Warteschlangen weitergeleitet wird. So öffnen Sie die Seite **UDP to Queue**:

- Wählen Sie in der Strukturansicht **Quality of Service >Mapping to Queue > UDP to Queue** aus. Die Seite **UDP to Queue** wird geöffnet.



Seite "UDP to Queue"

Die Seite **UDP to Queue** enthält folgende Informationen:

- **Select UDP from the List** - Bietet eine Dropdown-Liste vordefinierter, häufig verwendeter UDP-Anschlüsse.
- **Insert UDP Port** - Ermöglicht die Definition eines neuen UDP-Anschlusses.

- **Map to Queue** - Gibt die Netzwerkverkehrs-Warteschlange an, der der UDP-Anschluss zugewiesen ist.

ANMERKUNG: In einer Stack-Konfiguration wird Warteschlange 4 für die Weiterleitung des Stack-Datenverkehrs verwendet. Folglich kann ein Konflikt mit der Stack-Steuerung entstehen, wenn Warteschlange 4 zusätzlicher Datenverkehr zugewiesen wird.

- **Remove** - Entfernt die UDP-Anschlusszuweisung.
  - **Aktiviert** - Entfernt eine UDP-Anschlusszuweisung.
  - **Deaktiviert** - Behält eine UDP-Anschlusszuweisung bei.

Zuweisen eines UDP-Anschlusses zu einer Netzwerkverkehrs-Warteschlange:

1. Öffnen Sie die Seite **UDP to Queue**.
2. Wählen Sie einen Anschluss in der **UDP Port List** aus.

   Oder

   Aktivieren Sie das Kontrollkästchen **Insert UDP Port**. Das Feld **New UDP Port** wird aktiviert.

   Definieren Sie einen neuen UDP-Anschluss.
3. Wählen Sie eine Warteschlangennummer in der Dropdown-Liste **Map to Queue** aus.
4. Klicken Sie auf **Apply Changes**. Der UDP-Anschluss wird einer Weiterleitungswarteschlange zugewiesen.

Ändern einer "UDP-Anschluss-zu-Netzwerkverkehrs-Warteschlange"-Zuweisung:

1. Die Seite **UDP to Queue** öffnen.
2. Wählen Sie eine Anschlusszuweisung in der Dropdown-Liste **UDP Port List** aus. Die Warteschlange, der der Anschluss zugewiesen ist, wird in der Dropdown-Liste **Map to Queue** angezeigt.
3. Wählen Sie eine neue Netzwerkverkehrs-Warteschlange in der Dropdown-Liste **Map to Queue** aus.
4. Klicken Sie auf **Apply Changes**. Der UDP-Anschluss wird einer anderen Netzwerkverkehrs-Warteschlange neu zugewiesen.

Entfernen einer UDP-Anschlusszuweisung aus einer UDP to Traffic Mapping Table:

1. Öffnen Sie die Seite **UDP to Queue**.
2. Wählen Sie eine Anschlusszuweisung in der Dropdown-Liste **UDP Port List** aus. Die Warteschlange, der der Anschluss zugewiesen ist, wird in der Dropdown-Liste **Map to Queue** angezeigt.
3. Aktivieren Sie das Kontrollkästchen **Remove**.
4. Klicken Sie auf **Apply Changes**. Die UDP-Anschlusszuweisung wird aus der UDP to Traffic Mapping Table entfernt.

Zuweisen von UDP-Anschlüssen zu Warteschlangen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zur Konfiguration von Feldern auf der Seite **UDP to Queue** zusammengefasst.

CLI-Befehl	Beschreibung
qos map udp-port-queue *Anschluss1.Anschluss8 zu Warteschlangen-ID*	Ändert den der Warteschlange zugewiesenen UDP-Anschluss.
show qos map udp-port-queue	Zeigt den der Warteschlange zugewiesenen UDP-Anschluss an.
no qos map udp-port-queue	Entfernt den UDP-Anschluss aus einer Warteschlange.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# qos map udp-port-queue 2000 80 to 2
```

```
Console (config)# show qos map udp-port-queue
```

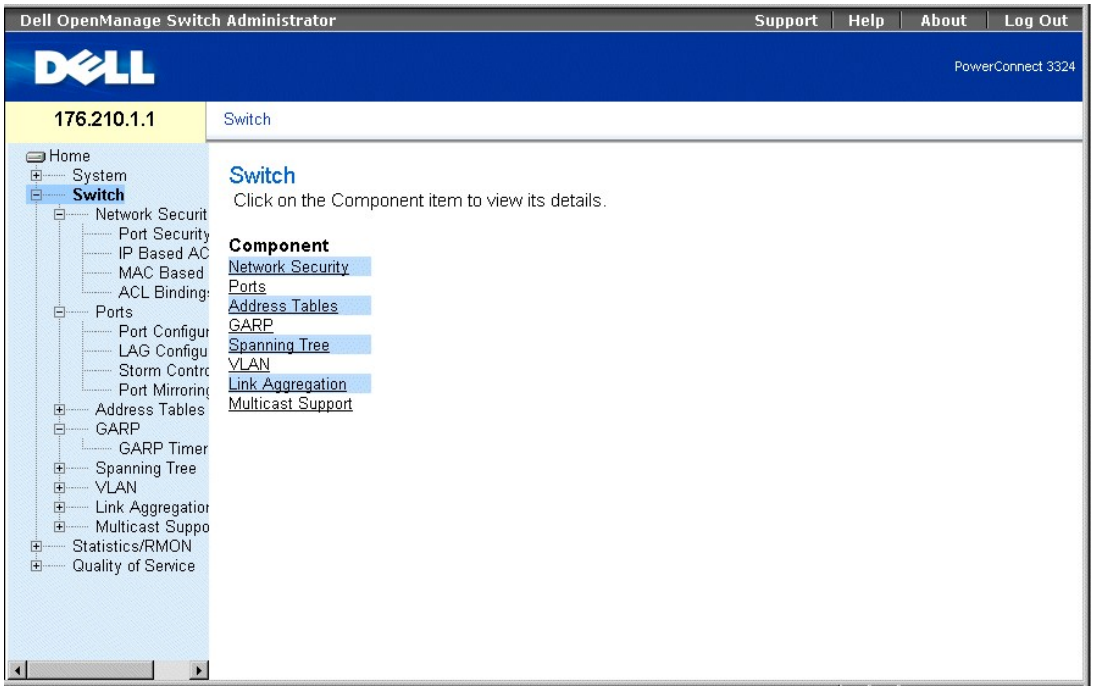
Zurück zum Inhalt

Zurück zum Inhalt

Konfigurieren von Switch-Informationen

Dell™ PowerConnect™ 3324/3348 Benutzerhandbuch

In diesem Abschnitt werden alle Systemoperationen sowie allgemeine Informationen im Zusammenhang mit der Konfiguration von Netzwerksicherheit, Anschlüssen, Adresstabellen, GARP, VLANs, Spanning Tree, Anschlussaggregation und Multicast-Unterstützung behandelt.



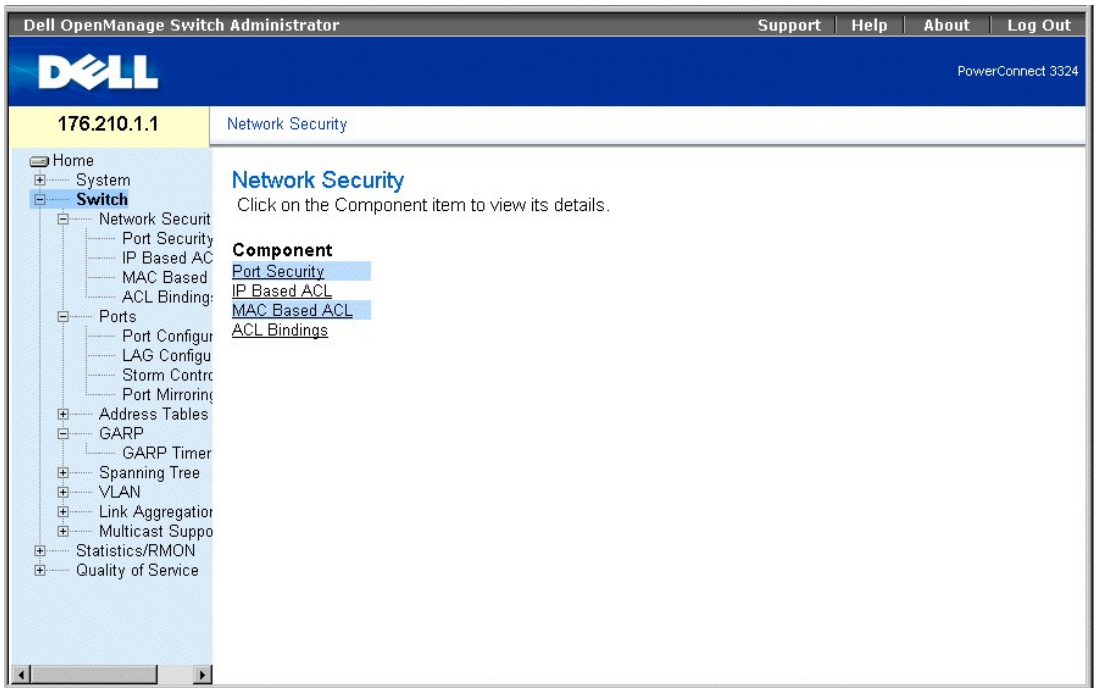
Seite "Switch"

Konfigurieren der Netzwerksicherheit

Auf dem Dell™ PowerConnect™ 3324/3348 können Netzwerkverwalter die Netzwerksicherheit wahlweise per ACL (Access Control Lists) oder Locked Ports (gesperrte Anschlüsse) einrichten.

So öffnen Sie die Seite **Network Security**:

- Wählen Sie Switch **> Network Security**. Die Seite **Network Security** wird geöffnet.



Seite "Network Security"

Die Seite **Network Security** enthält Links zu folgenden Themen:

- Übersicht über die Netzwerksicherheit
- Konfigurieren der Anschlusssicherheit
- Definieren IP-basierter ACLs
- Definieren MAC-basierter ACLs
- Verknüpfen von ACLs

Übersicht über die Netzwerksicherheit

Über ACLs können Netzwerkverwalter Klassifikationsaktionen und -regeln für spezifische Ingress-Anschlüsse festlegen. ACLs umfassen mehrere Klassifikationsregeln und -aktionen. Jede Klassifikationsregel und -aktion entspricht einem Access Control Element (ACE). Access Control Elements (ACEs) fungieren als Filter zur Ermittlung von Datenverkehrsklassifikationen. Pakete werden durch die folgenden Access Control Elements (ACEs) zugewiesen:

- Protokoll
- Destination Port
- IP-Quelladresse
- IP-Zieladresse
- Platzhaltermasken
- Zugewiesener DSCP-Wert
- Zugewiesene IP-Precedence
- MAC-Quelladresse
- MAC-Zieladresse
- VLAN-ID

Ein Netzwerkadministrator kann beispielsweise eine ACL-Regel definieren, durch die festgelegt wird, dass Anschluss Nummer 20 TCP-Pakete empfangen kann, wobei empfangene UDP-Pakete jedoch abgelehnt werden.

Eine einzelne ACL kann mehr als ein ACE enthalten. Die ACEs innerhalb einer ACL werden nach dem First-Fit-Verfahren (erste passende Stelle) angewendet.

Die ACEs werden ausgehend vom ersten ACE aufeinander folgend verarbeitet. Wenn ein Paket einer ACE-Klassifikation zugewiesen wurde, wird die entsprechende ACE-Aktion ausgeführt und die Verarbeitung der ACL unterbrochen. Wird keine Übereinstimmung gefunden, wird das Paket standardmäßig abgelehnt. Falls mehrere ACLs verarbeitet werden müssen, erfolgt die Standardaktion erst nach der Verarbeitung aller ACLs. Die standardmäßige Ablehnungsaktion sieht vor, dass der gesamte zulässige Datenverkehr, einschließlich Netzwerkverwaltungsdaten wie Telnet, HTTP oder SNMP, an den Switch weitergeleitet werden.

Netzwerkverwalter können zwei ACL-Typen definieren:

- IP-ACL - Bezieht sich nur auf IP-Pakete. Alle Klassifizierungsfelder beziehen sich auf IP-Pakete.
- MAC-ACL - Bezieht sich auf beliebige Pakete, einschließlich Nicht-IP-Paketen. Klassifizierungsfelder basieren lediglich auf L2-Feldern.

Über einen Ingress-Anschluss mit einer aktiven ACL eingehende Pakete werden:

- weitergeleitet
- verworfen, und ein Trap wird gesendet
- verworfen, ein Trap wird gesendet und der Ingress-Anschluss deaktiviert

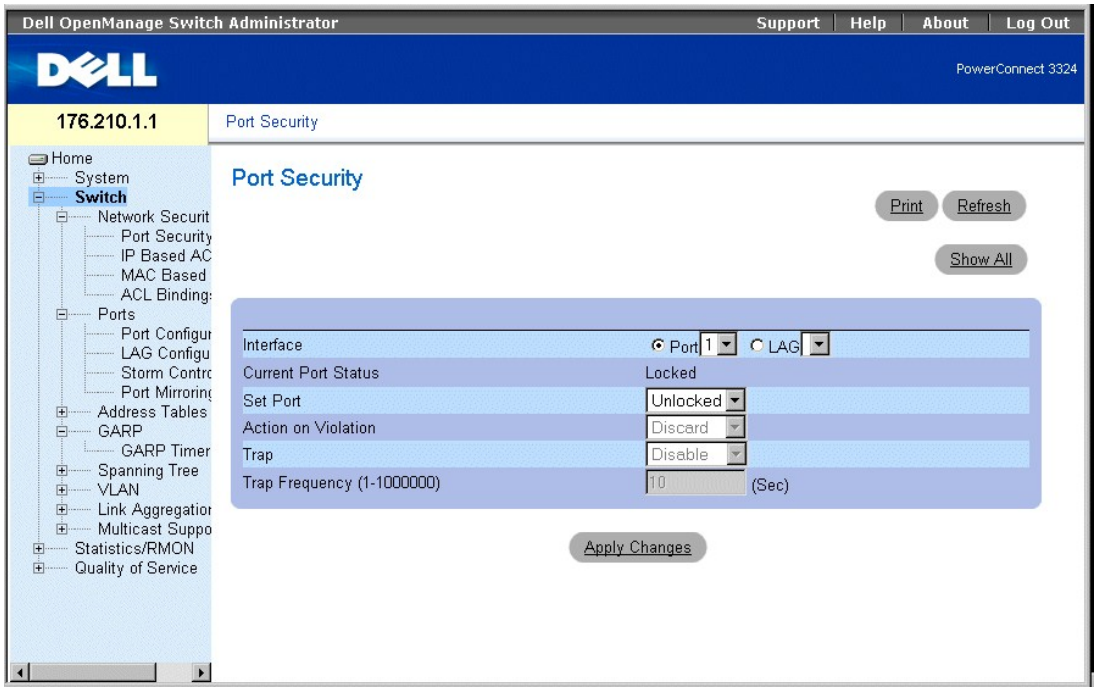
Der PowerConnect 3324/3348 unterstützt bis zu 128 ACLs. Der PowerConnect 3324/3348 unterstützt pro FE-Anschluss bis zu 248 ACEs, und pro GE-Anschluss können bis zu 120 ACEs definiert werden.

Konfigurieren der Anschlusssicherheit

Der Zugriff von Netzwerkbenutzern kann durch Locked Ports (gesperrte Anschlüsse) auf bestimmte Anschlüsse oder LAGs beschränkt werden. Locked Port bedeutet, dass nur Benutzer mit spezifischen MAC-Adressen Zugriff haben. Locked Ports können nur für statische MAC-Adressen aktiviert werden. Darüber hinaus bietet die Sicherheitsoption Locked Port die Möglichkeit, eine Liste von MAC-Adressen in der Konfigurationsdatei zu speichern. Die MAC-Adressliste kann nach dem Zurücksetzen des Gerätes wiederhergestellt werden. MAC-Adressen werden entweder dynamisch oder statisch erfasst.

Über einen Locked Port eingehende Pakete werden entweder weitergeleitet oder abgelehnt bzw. das Paket wird abgelehnt, ein Trap gesendet und der Ingress-Anschluss deaktiviert. Deaktivierte Anschlüsse werden über die Seite **Port Parameters** aktiviert. Siehe "Definieren von Anschlussparametern". So öffnen Sie die Seite **Port Security**:

- Wählen Sie **Switch > Network Security > Port Security**. Die Seite **Port Security** wird geöffnet.



Seite "Port Security"

Die Seite **Port Security** enthält folgende Felder:

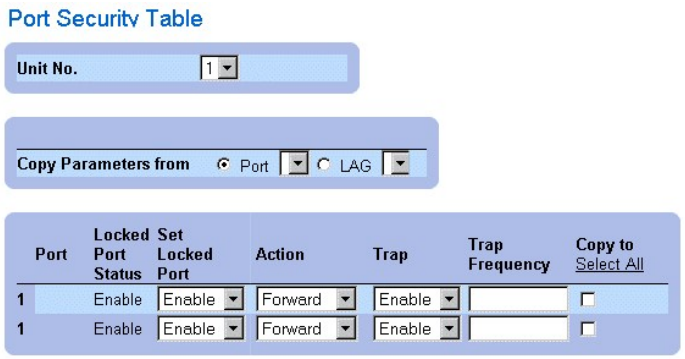
- **Interface** - Gibt den ausgewählten Schnittstellentyp an, für den der Locked Port aktiviert ist.
  - **Port** - Gibt an, dass es sich beim ausgewählten Schnittstellentyp um einen Anschluss handelt.
  - **LAG** - Gibt an, dass es sich beim ausgewählten Schnittstellentyp um eine Stack-Komponente handelt.
- **Current Port Status** - Gibt den aktuellen Anschlussstatus an.
- **Set Port** - Gibt an, ob der Anschluss gesperrt oder freigegeben ist. Folgende Feldwerte können ausgewählt werden:
  - **Unlocked** - Gibt den Anschluss frei. Dies ist der Standardwert.
  - **Locked** - Sperrt den Anschluss.
- **Action on Violation** - Gibt die Aktion für Pakete an, die über einen gesperrten Anschluss eingehen. Folgende Feldwerte können ausgewählt werden:
  - **Forward** - Leitet die aus einer unbekannten Quelle stammenden Pakete weiter; die MAC-Adresse wird jedoch nicht erfasst.
  - **Discard** - Verwirft die aus einer unbekannten Quelle stammenden Pakete. Dies ist der Standardwert.
  - **Shutdown** - Verwirft das aus einer beliebigen unbekannten Quelle stammende Paket und sperrt den Anschluss. Anschlüsse bleiben gesperrt, bis sie wieder aktiviert werden oder das Gerät zurückgesetzt wird.
- **Trap** - Aktiviert das Senden eines Traps. Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Aktiviert das Senden von Traps, wenn ein Paket über einen gesperrten Anschluss empfangen wird.
  - **Disable** - Deaktiviert das Senden von Traps, wenn ein Paket über einen gesperrten Anschluss empfangen wird. Dies ist der Standardwert.
- **Trap Frequency (1-1000000)** - Gibt das zwischen Traps liegende Zeitintervall (in Sekunden) an. Dieses Feld bezieht sich nur auf gesperrte Anschlüsse. Der Standardwert lautet 10 Sekunden.

Definieren eines Locked Port:

1. Öffnen Sie die Seite **Port Security**.
2. Wählen Sie den Typ und die Nummer einer Schnittstelle aus.
3. Definieren Sie die Felder **Set Port, Action on Violation** und **Trap**.
4. Klicken Sie auf **Apply Changes**. Der gesperrte Anschluss wird der **Port Security Table** hinzugefügt und das Gerät aktualisiert.

Anzeigen der Locked Port Table:

1. Öffnen Sie die Seite **Port Security**.
2. Klicken Sie auf **Show All**. Die Seite **Port Security Table** wird geöffnet. Die Felder in der **Port Security Table** entsprechen den Feldern auf der Seite **Port Security**. Locked Ports können sowohl über die **Locked Ports Table** als auch die Seite **Port Security** definiert werden.



Seite "Port Security Table"

Neben den auf der Seite Seite "Port Security" angezeigten Feldern enthält die Seite **Port Security Table** das folgende zusätzliche Feld:

- **Unit No.** - Gibt die Nummer der Einheit an, für die Anschlusssicherheitsinformationen angezeigt werden.

Konfigurieren der Locked Port-Sicherheit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zur Konfiguration der Locked Port-Sicherheit zusammengefasst, die auf der Seite Seite "Port Security" angezeigt werden.

CLI-Befehl	Beschreibung
shutdown	Deaktiviert Schnittstellen.
set interface active {ethernet *Schnittstelle* **| port-channel** *Anschlusskanalnummer***}**	Reaktiviert eine Schnittstelle, die aus Gründen der Anschlusssicherheit deaktiviert wurde.
port security <*Optionen***>** *Trapintervall*	Sperrt die Erfassung neuer Adressen für eine Schnittstelle.
show ports security	Zeigt den Sperrstatus von Anschlüssen an.

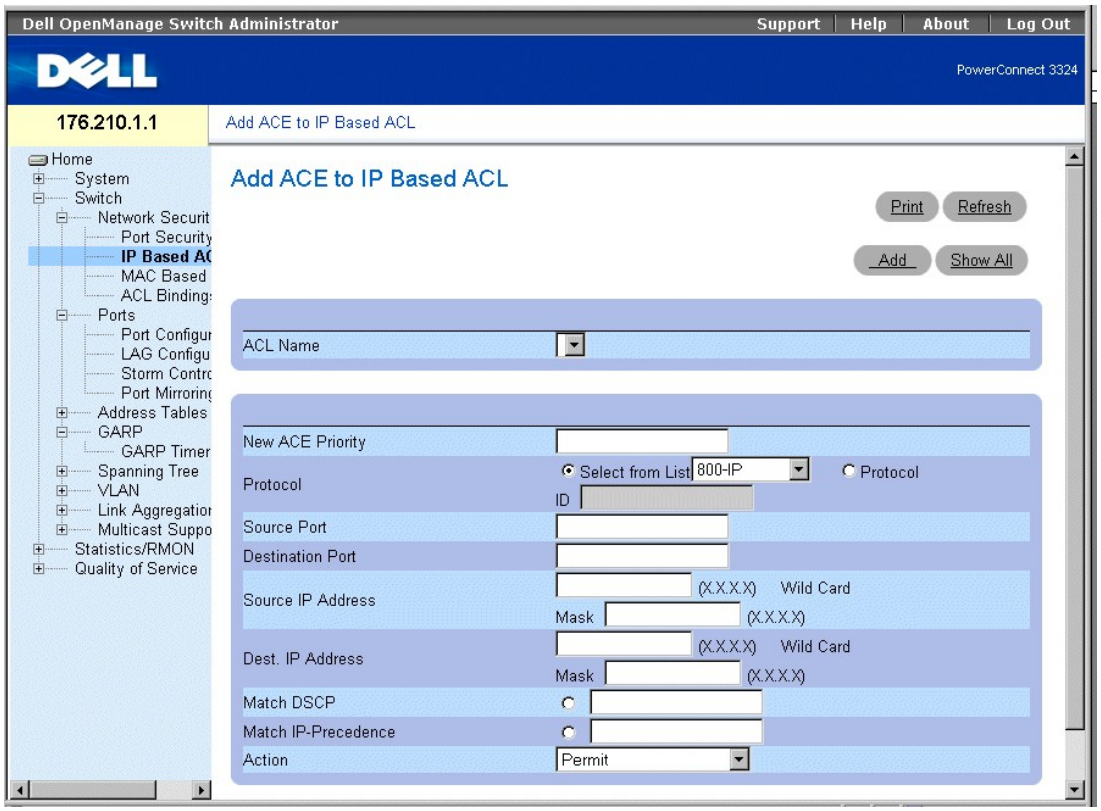
Im Folgenden ein Beispiel für die CLI-Befehle:

```
From 18.1.16 Console # show ports security

Port Action Trap Frequency Counter

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

5/7 Discard Enable 100 88

7/8 Discard Disable
```

Definieren IP-basierter ACLs

Auf der Seite **Add ACE to IP Based ACL** können Netzwerkadministratoren IP-basierte ACLs (Access Control Lists) sowie ACEs (Access Control Entries) definieren. ACEs fungieren als Filter, um Pakete mit Weiterleitungskriterien abzustimmen. So öffnen Sie die Seite **Add ACE to IP Based ACL**:

- Wählen Sie **Switch > Network Security > IP based ACL**. Die Seite **Add ACE to IP Based ACL** wird geöffnet.



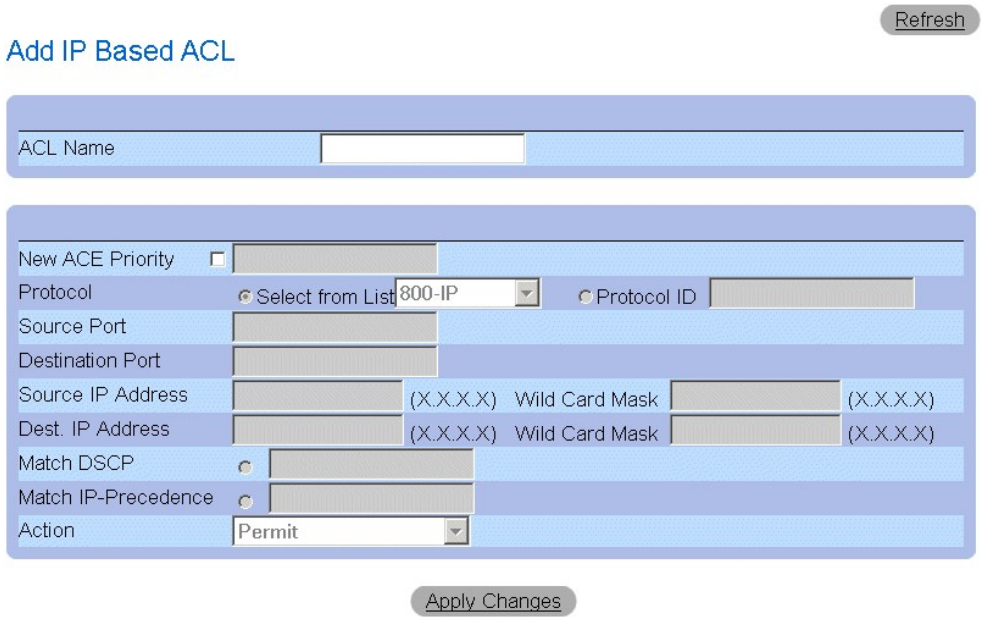
Seite "Add ACE to IP Based ACL"

Die Seite **Add ACE to IP Based ACL** enthält folgende Felder:

- **ACL Name** - Enthält eine Liste benutzerdefinierter ACLs.
- **New ACE Priority** - Definiert die ACE-Priorität. ACEs werden auf First-Fit-Basis (erste passende Stelle) überprüft. Die ACE-Reihenfolge in der ACL-Liste wird durch die ACE-Priorität definiert.
- **Protocol** - Aktiviert die Erstellung eines ACEs für ein spezifisches Protokoll.
- **Source Port** - Gibt den Quellanschluss an, der Paketen zugewiesen wurde. Die Option ist nur aktiviert, falls TCP oder UDP in der Liste Protocol ausgewählt wurde.
- **Destination Port** - Gibt den Zielanschluss an, der Paketen zugewiesen wurde. Die Option ist nur aktiviert, falls TCP oder UDP in der Liste Protocol ausgewählt wurde.
- **Source IP Address** - Weist dem ACE die IP-Quelladresse zu, an die Pakete adressiert werden.
- **Wild Card Mask** - Gibt die Platzhaltermaske der IP-Quelladresse an. Platzhalter werden verwendet, um eine IP-Quelladresse vollständig oder teilweise zu maskieren. Durch Platzhaltermasken wird festgelegt, welche Bits verwendet und welche ignoriert werden. Die Platzhaltermaske 255.255.255.255 gibt an, dass kein Bit von Bedeutung ist. Der Platzhalter 00.00.00.00 gibt an, dass alle Bits berücksichtigt werden. Wenn die IP-Quelladresse beispielsweise 149.36.184.198 und die Platzhaltermaske 255.36.184.00 lautet, werden die ersten beiden Bits der IP-Adresse ignoriert, während die letzten beiden Bits verwendet werden.
- **Dest. IP Address** - Weist dem ACE die IP-Zieladresse zu, an die Pakete adressiert werden.
- **Wild Card Mask** - Gibt die Platzhaltermaske der IP-Zieladresse an. Platzhalter werden verwendet, um eine IP-Zieladresse vollständig oder teilweise zu maskieren. Durch Platzhaltermasken wird festgelegt, welche Bits verwendet und welche ignoriert werden. Die Platzhaltermaske 255.255.255.255 gibt an, dass kein Bit von Bedeutung ist. Der Platzhalter 00.00.00.00 gibt an, dass alle Bits berücksichtigt werden. Wenn die IP-Zieladresse beispielsweise 149.36.184.198 und die Platzhaltermaske 255.36.184.00 lautet, werden die ersten beiden Bits der IP-Adresse verwendet, während die letzten beiden Bits ignoriert werden.
- **Match DSCP** - Weist dem ACE den DSCP-Wert des Pakets zu. Um ACEs Pakete zuzuweisen, wird entweder der DSCP-Wert oder der IP-Precedence-Wert verwendet.
- **Match IP-Precedence** - Weist dem ACE den IP-Precedence-Wert des Pakets zu. Um ACEs Pakete zuzuweisen, wird entweder der DSCP-Wert oder der IP-Precedence-Wert verwendet.
- **Action** - Gibt die ACE-Weiterleitungsaktion an. Folgende Feldwerte können ausgewählt werden:
  - **Permit** - Leitet Pakete weiter, die die ACE-Kriterien erfüllen.
  - **Deny** - Lehnt Pakete ab, die die ACE-Kriterien erfüllen.
  - **Deny and Disable Port** - Lehnt Pakete ab, die die ACE-Kriterien erfüllen und deaktiviert den Anschluss, an den die Pakete adressiert waren. Anschlüsse können über Port Configuration wieder aktiviert werden. Weitere Informationen siehe "Definieren von Anschlussparametern".

Hinzufügen IP-basierter ACLs:

1. Öffnen Sie die Seite **Add ACE to IP Based ACL**.
2. Klicken Sie auf **Hinzufügen**. Die Seite **Add ACE to IP Based ACL** wird geöffnet.



Seite "Add IP Based ACL"

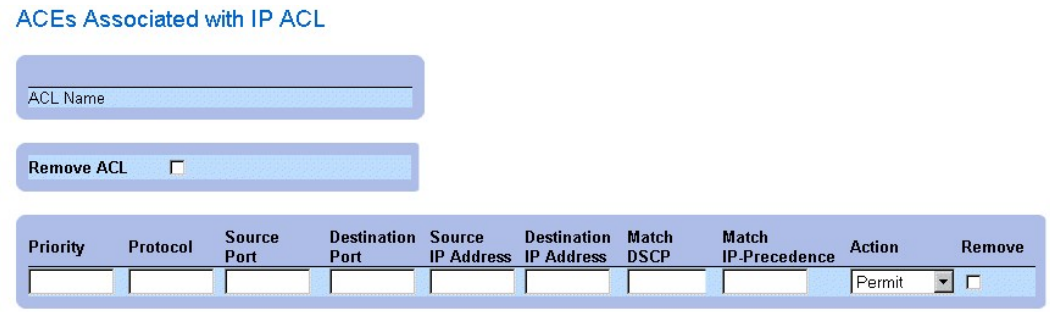
3. Definieren Sie die Felder **ACL Name**, **New Ace Priority**, **Protocol**, **Source und Destination Port**, **Source und Destination IP Address**, **Match DSCP** oder **Match IP Precedence** und **Action**.
4. Klicken Sie auf **Apply Changes**. Die IP-basierten ACLs werden definiert. Falls eine neue ACE-Priorität definiert wurde, wird diese der neuen ACL hinzugefügt.

Zuweisen von ACEs zu einer IP-basierten ACL:

1. Öffnen Sie die Seite **Add ACE to IP Based ACL**.
2. Wählen Sie eine ACL in der Dropdown-Liste **ACL Name** aus.
3. Definieren Sie das Feld **New ACE Priority**.
4. Definieren Sie die Felder **ACE No.**, **Protocol**, **Source und Destination Port**, **Source und Destination IP Address**, **Match DSCP** oder **Match IP Precedence** und/oder **Action**.
5. Klicken Sie auf **Apply Changes**. Der ACE wird der IP-basierten ACL zugewiesen.

Anzeigen ACL-spezifischer ACEs:

1. Öffnen Sie die Seite **Add ACE to IP Based ACL**.
2. Klicken Sie auf **Show All**. Die Seite **ACEs Associated with IP-ACL** wird geöffnet.



ACEs Associated with IP-ACL

Ändern eines IP-basierten ACEs:

1. Öffnen Sie die Seite **Add ACE to IP Based ACL**.
2. Klicken Sie auf Show All. Die Seite **ACEs Associated with IP-ACL** wird geöffnet.
3. Bearbeiten Sie die Felder **ACL Name**, **New Ace Priority**, **Protocol**, **Source und Destination Port**, **Source und Destination IP Address**, **Match DSCP** oder **Match IP Precedence** und **Action**.
4. Klicken Sie auf **Apply Changes**. Der IP-basierte ACE wird geändert und das Gerät aktualisiert.

Entfernen von ACLs:

1. Öffnen Sie die Seite **Add ACE to IP Based ACL**.
2. Klicken Sie auf **Show All**. Die Seite **ACEs Associated with IP-ACL** wird geöffnet.
3. Wählen Sie eine ACL aus.
4. Aktivieren Sie das Kontrollkästchen **Remove ACL**.
5. Klicken Sie auf **Apply Changes**. Die IP-basierte ACL wird entfernt und das Gerät aktualisiert.

Entfernen von ACEs:

1. Öffnen Sie die Seite **Add ACE to IP Based ACL**.
2. Klicken Sie auf **Show All**. Die Seite **ACEs Associated with IP-ACL** wird geöffnet.
3. Wählen Sie einen ACE aus.
4. Aktivieren Sie das Kontrollkästchen **Remove**.
5. Klicken Sie auf **Apply Changes**. Der IP-basierte ACE wird entfernt und das Gerät aktualisiert.

Zuweisen IP-basierter ACEs zu ACLs mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Zuweisung IP-basierter ACEs zu ACLs zusammengefasst, die auf der Seite **Add ACE to IP Based ACL** angezeigt werden.

CLI-Befehl	Beschreibung
ip access-list *Name*	Aktiviert den "IP Access List"-Konfigurationsmodus.
permit {any | *protocol*`}` **{any | {**`source source-wildcard`**}} {any | {**`destination destination-wildcard`**}} [dscp** `dscp number` **| ip-precedence** `ip-precedence`**]**	Akzeptiert Datenverkehr, wenn die in der permit-Anweisung definierten Bedingungen erfüllt sind.
deny [disable-port] {any| `protocol`**} {any | {**`source source-wildcard`**}} {any | {**`destination destination-wildcard`**}} [dscp** `dscp number` **| ip-precedence** `ip-precedence`**]**	Lehnt Datenverkehr ab, wenn die in der deny-Anweisung definierten Bedingungen erfüllt sind.

Im Folgenden ein Beispiel für die CLI-Befehle:

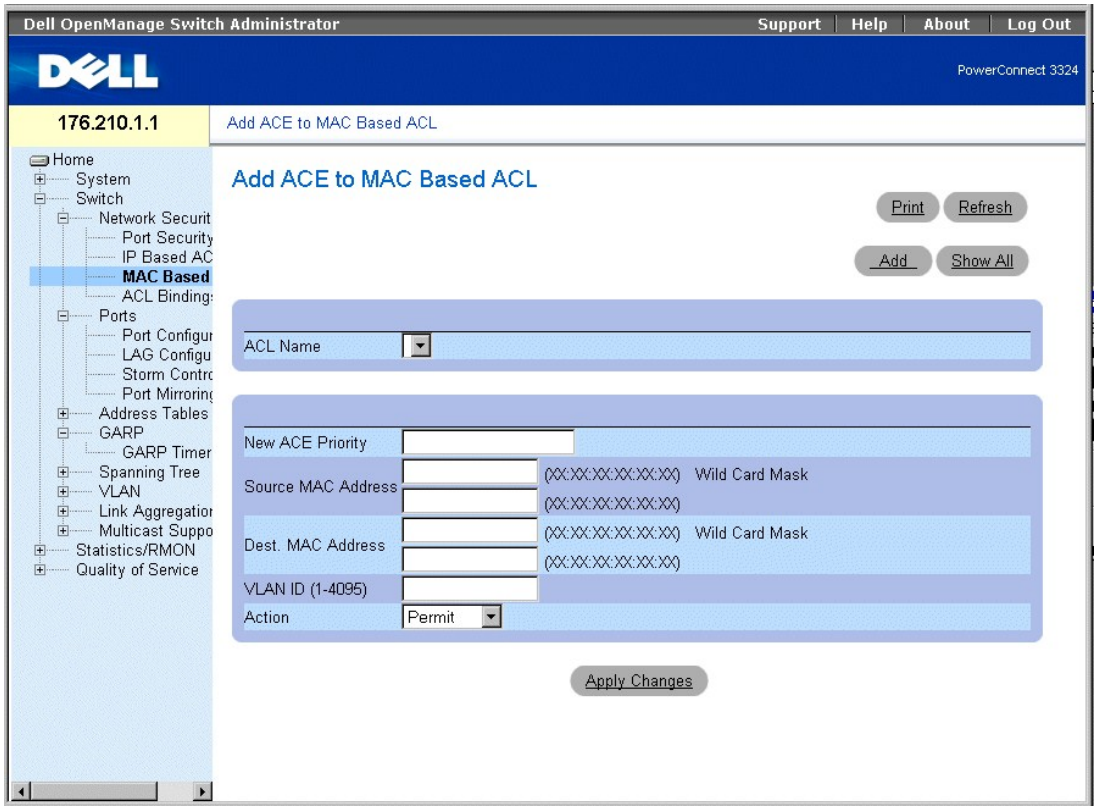
```
Permit 00:00:bo:11:11:11 0:0:0:0:0:0 any VLAN 4
```

```
deny 00:00:bo:11:11:11 0:0:0:0:0:0 any VLAN 4
```

Definieren MAC-basierter ACLs

Auf der Seite **Add ACE to MAC Based ACL** können Netzwerkadministratoren einen MAC-basierten **Access Control Entry** (ACE) sowie **Access Control Lists** (ACLs) definieren. ACEs fungieren als Filter, um Pakete mit Weiterleitungskriterien abzustimmen. So öffnen Sie die Seite **Add ACE to MAC Based ACL**:

- Wählen Sie **Switch > Network Security > MAC Based ACL**. Die Seite **Add ACE to MAC Based ACL** wird geöffnet.



Seite "Add ACE to MAC Based ACL"

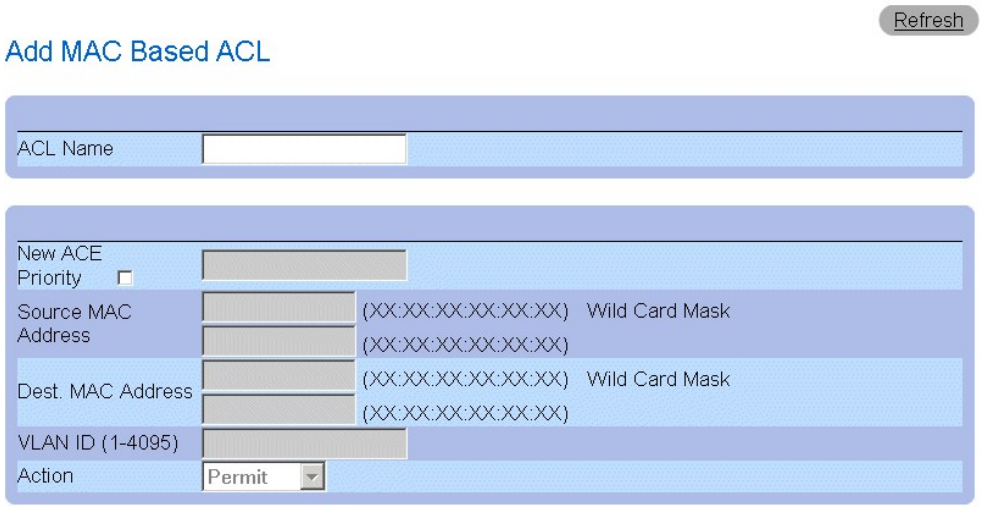
Die Seite **Add ACE to MAC Based ACL** enthält folgende Felder:

- **ACL Name** - Enthält eine Liste benutzerdefinierter ACLs.
- **New ACE Priority** - Ermöglicht die Erstellung eines neuen ACEs und gibt die ACE-Priorität an.
- **Source MAC Address** - Weist dem ACE die MAC-Quelladresse zu, von der aus die Pakete adressiert werden.
- **Wild Card Mask** - Gibt die Platzhaltermaske der MAC-Zieladresse an. Platzhalter werden verwendet, um eine MAC-Quelladresse vollständig oder teilweise zu maskieren. Durch Platzhaltermasken wird festgelegt, welche Bits verwendet und welche ignoriert werden. Die Platzhaltermaske FF:FF:FF:FF:FF:FF gibt an, dass kein Bit von Bedeutung ist. Der Platzhalter 00.00.00.00.00.00 gibt an, dass alle Bits berücksichtigt werden. Wenn die MAC-Quelladresse beispielsweise E0:3B:4A:C2:CA:E2 und die Platzhaltermaske 00:3B:4A:C2:CA:FF lautet, werden die ersten beiden Halbbytes der MAC-Adresse verwendet, während die letzten beiden ignoriert werden.
- **Destination MAC Address** - Weist dem ACE die MAC-Zieladresse zu, an die Pakete adressiert werden.
- **Wild Card Mask** - Gibt die Platzhaltermaske der MAC-Zieladresse an. Platzhalter werden verwendet, um eine MAC-Zieladresse vollständig oder teilweise zu maskieren. Durch Platzhaltermasken wird festgelegt, welche Bits verwendet und welche ignoriert werden. Die Platzhaltermaske FF:FF:FF:FF:FF:FF gibt an, dass kein Bit von Bedeutung ist. Die Platzhaltermaske 00.00.00.00.00.00 gibt an, dass alle Bits berücksichtigt werden. Wenn die MAC-Zieladresse beispielsweise E0:3B:4A:C2:CA:E2 und die Platzhaltermaske 00:3B:4A:C2:CA:FF lautet, werden die ersten beiden Halbbytes der MAC-Adresse verwendet, während die letzten beiden ignoriert werden.
- **VLAN ID** - Weist dem ACE die VLAN-ID des Pakets zu.
- **Action** - Gibt die ACE-Weiterleitungsaktion an. Folgende Feldwerte können ausgewählt werden:
  - **Permit** - Leitet Pakete weiter, die die ACE-Kriterien erfüllen.

- **Deny** - Lehnt Pakete ab, die die ACE-Kriterien erfüllen.
- **Shutdown** - Lehnt Pakete ab, die die ACE-Kriterien erfüllen und deaktiviert den Anschluss, an den die Pakete adressiert waren. Anschlüsse können über Port Configuration wieder aktiviert werden. Weitere Informationen siehe "Definieren von Anschlussparametern".

Hinzufügen einer MAC-basierten ACL:

1. Öffnen Sie die Seite **Add ACE to MAC Based ACL**.
2. Klicken Sie auf **Hinzufügen**. Die Seite **Add MAC Based ACL** wird geöffnet.



MAC-basierten ACLs zugewiesene ACEs

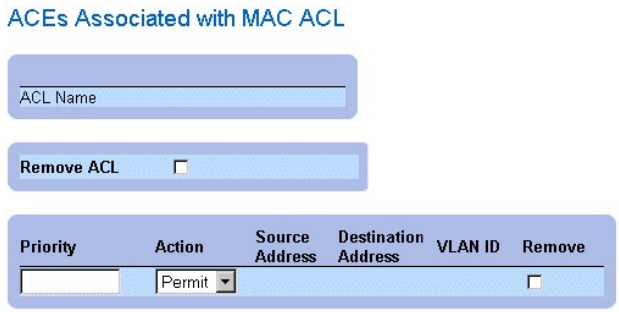
3. Definieren Sie die Felder **ACL Name**, **Source und Destination Address** sowie **Action**.
4. Klicken Sie auf **Apply Changes**. Die MAC-basierte ACL wird definiert und das Gerät aktualisiert.

Zuweisen von ACEs zu einer MAC-basierten ACL:

1. Öffnen Sie die Seite **Add ACE to MAC Based ACL**.
2. Wählen Sie eine ACL in der Dropdown-Liste **ACL Name** aus.
3. Definieren Sie das Feld **New ACE Priority**.
4. Definieren Sie die Felder **ACL Name**, **VLAN ID**, **Source und Destination Address** sowie **Action**.
5. Klicken Sie auf **Apply Changes**. Der ACE wird der MAC-basierten ACL zugewiesen.

Anzeigen ACL-spezifischer ACEs:

1. Öffnen Sie die Seite **Add ACE to MAC Based ACL**.
2. Klicken Sie auf **Show All**. Die Seite **ACEs Associated with MAC ACL** wird geöffnet.



ACEs Associated with MAC ACL

Ändern eines MAC-basierten ACEs:

1. Öffnen Sie die Seite **Add ACE to MAC Based ACL**.
2. Klicken Sie auf **Show All**. Die Seite **ACEs Associated with MAC ACL** wird geöffnet.
3. Bearbeiten Sie die Felder **ACL Name**, **Source und Destination Address** sowie **Action**.
4. Klicken Sie auf **Apply Changes**. Der MAC-basierte ACE wird geändert und das Gerät aktualisiert.

Entfernen von ACLs:

1. Öffnen Sie die Seite **Add ACE to MAC Based ACL**.
2. Klicken Sie auf **Show All**. Die Seite **ACEs Associated with MAC ACL** wird geöffnet.
3. Wählen Sie eine ACL aus.
4. Aktivieren Sie das Kontrollkästchen **Remove ACL**.
5. Klicken Sie auf **Apply Changes**. Die MAC-basierte ACL wird entfernt und das Gerät aktualisiert.

Entfernen von ACEs:

1. Öffnen Sie die Seite **Add ACE to MAC Based ACL**.
2. Klicken Sie auf **Show All**. Die Seite **ACEs Associated with MAC ACL** wird geöffnet.
3. Wählen Sie einen ACE aus.
4. Aktivieren Sie das Kontrollkästchen **Remove**.
5. Klicken Sie auf **Apply Changes**. Der MAC-basierte ACE wird entfernt und das Gerät aktualisiert.

Zuweisen MAC-basierter ACEs zu ACLs mit Hilfe der CLI-Befehle

Beachten Sie das folgende Beispiel: Station A ist mit Anschluss 5 und Station B mit Anschluss 9 verbunden. Station A besitzt die MAC-Adresse 00-0B-CD-35-6A-00 (IP-Adresse: 10.0.0.1 255.255.255.0). Station B verfügt über die MAC-Adresse 00-06-6B-C7-A1-D8 (IP-Adresse: 10.0.0.2 255.255.255.0).

Um eine MAC-ACL für Anschluss 5 zu implementieren, damit sämtlicher Datenverkehr von Station A zu Station B weitergeleitet werden kann, geben Sie die folgenden CLI-Befehle ein:

```
permit source mac address destination mac address
```

```
permit 00-0B-CD-35-6A-00 0.0.0.0.0.0 00-06-6B-C7-A1-D8 0.0.0.0.0.0
```

Sämtlicher Datenverkehr, der der ACL entspricht, wird akzeptiert und sonstiger Datenverkehr abgelehnt. (Es wird ein zusätzliches promiskuitives `deny all` am Ende der ACL eingegeben.)

Im vorangehenden Beispiel versucht Station A, ICMP ECHO an Station B zu senden. Das ICMP wird nicht erkannt, auch wenn es durch die MAC-ACL zugelassen ist. Das Problem liegt darin, dass Station A versucht, Station B das ICMP ECHO zu senden, ohne über einen Eintrag in der ARP-Tabelle zu verfügen. Station A versucht, die MAC-Adresse von Station B durch eine ARP-Anforderung abzurufen. Diese entspricht dem Broadcast-Frame mit der MAC-Quelladresse von Station A (00-0B-CD-35-6A-00) und der Broadcast-Zieladresse (FF.FF.FF.FF.FF.FF). Dieser Frame wird ohne Fehlermeldung abgelehnt, da er nicht mit der für Anschluss 5 eingerichteten MAC-ACL übereinstimmt.

Zur Lösung dieses Problems muss der Benutzer eine zusätzliche `permit`-Zeile eingeben, damit der Broadcast-Frame zulässig ist:

```
permit 00-0B-CD-35-6A-00 0.0.0.0.0.0 FF.FF.FF.FF.FF.FF 0.0.0.0.0.0
```

ANMERKUNG: Auch wenn ein Benutzer beabsichtigt, Datenverkehr von MAC-Adresse A zu MAC-Adresse B zuzulassen, wird einfacher Netzverkehr über das ICMP nicht weitergeleitet, da die zusätzliche Broadcast-Zeile nicht berücksichtigt wird.

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Zuweisung MAC-basierter ACEs zu ACLs zusammengefasst, die auf der Seite **Add ACE to MAC Based ACL** angezeigt werden.

CLI-Befehl	Beschreibung
mac access-list *Name*	Erstellt Layer 2-MAC-ACLs und ruft den "MAC Access List"-Konfigurationsmodus auf.
permit {any | {host *source source-wildcard***} any | {***destination destination-wildcard***}}[vlan** *vlan-id***]**	Akzeptiert Datenverkehr, wenn die in der permit-Anweisung definierten Bedingungen erfüllt sind.
deny [disable-port] {any | {*source source- wildcard***} any | {***destination destination- wildcard***}}[vlan** *vlan-id***]**	Akzeptiert Datenverkehr, wenn die in der permit-Anweisung definierten Bedingungen erfüllt sind.

Im Folgenden ein Beispiel für die CLI-Befehle:

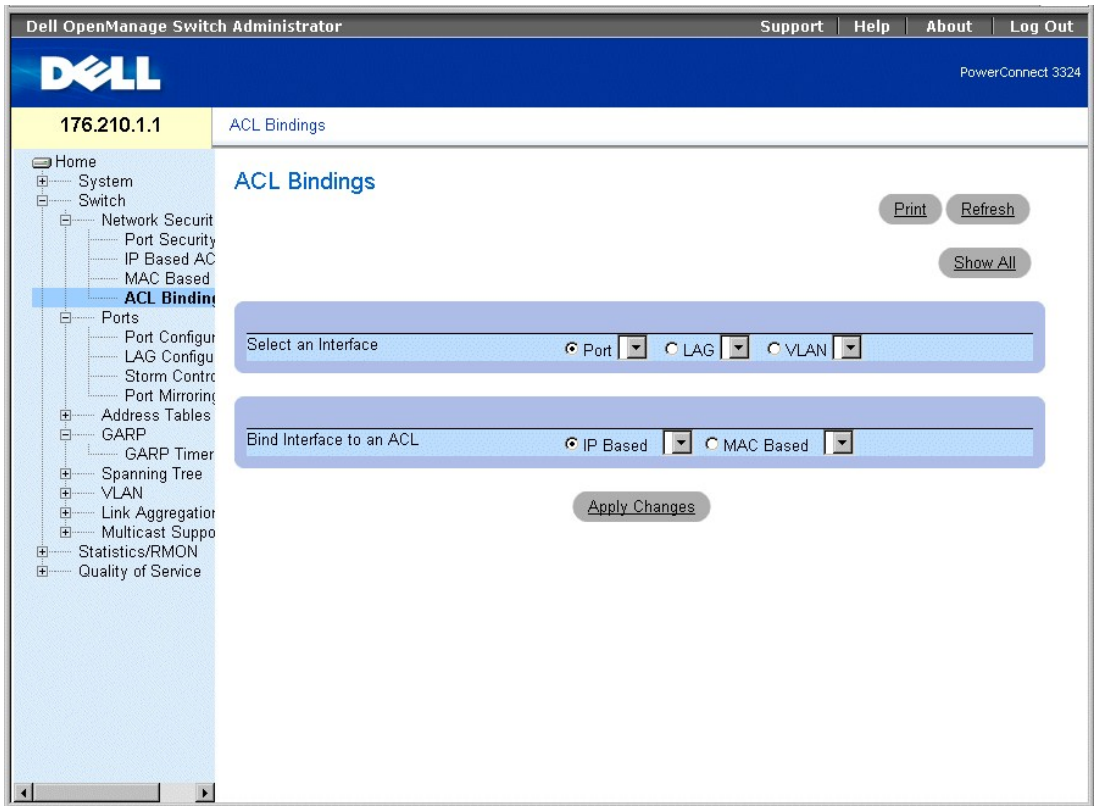
```
Console (config)# mac access-list dell

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
```

Verknüpfen von ACLs

Auf der Seite **ACL Bindings** können Netzwerkverwalter ACLs und Schnittstellen einander zuweisen. So öffnen Sie die Seite **ACL Bindings**:

- Wählen Sie **Switch > Network Security > ACL Bindings**. Die Seite **ACL Bindings** wird geöffnet.

ANMERKUNG: ACLs werden erst wirksam, wenn sie mit einer Schnittstelle verknüpft sind.



Seite "ACL Bindings"

Die Seite **ACL Bindings** enthält folgende Felder:

- **Select an Interface** - Gibt den Namen und den Typ der Schnittstelle an, mit der die ACL verbunden ist. Folgende Feldwerte können ausgewählt werden:
  - **Port** - Gibt die Nummer des Anschlusses an, mit dem die ACL verbunden ist.
  - **LAG** - Gibt die LAG an, mit der die ACL verbunden ist.
  - **VLAN** - Gibt das VLAN an, mit dem die ACL verbunden ist.
- **Bind Interface to ACL** - Gibt den Namen der ACL an, anhand welcher eingehende Pakete zugewiesen werden. Pakete können entweder IP-basierten ACLs oder auf MAC-Adressen basierenden ACLs zugewiesen werden. Folgende Feldwerte können ausgewählt werden:
  - **IP Based** - Gibt an, dass eingehende Pakete IP-basierten ACLs zugewiesen werden.
  - **MAC Based** - Gibt an, dass eingehende Pakete MAC-basierten ACLs zugewiesen werden.

Zuweisen einer ACL zu einer Schnittstelle:

1. Öffnen Sie die Seite **ACL Bindings**.
2. Wählen Sie den ACL-Typ in den Feldern Select ACL aus.
3. Definieren Sie im Feld **Attach ACL to an Interface** die Schnittstelle, der die ACL zugewiesen wird.
4. Klicken Sie auf **Apply Changes.** Die ACL wird mit der Schnittstelle verknüpft.

Zuweisen einer ACL-Mitgliedschaft mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Zuweisung einer ACL-Mitgliedschaft zusammengefasst, die auf der Seite **ACL Bindings** angezeigt wird.

CLI-Befehl	Beschreibung

class-map *Klassenzuweisungsname* **[match-all | match-any]**	Erstellt Klassenzuweisungen und aktiviert den "Class Map"-Konfigurationsmodus.
match access-group ACL *Name*	Definiert das Zuweisungskriterium für die Klassifizierung des Datenverkehrs.
show class-map [*Klassenzuweisungsname***]**	Zeigt alle für das Gerät konfigurierten Klassenzuweisungen an.

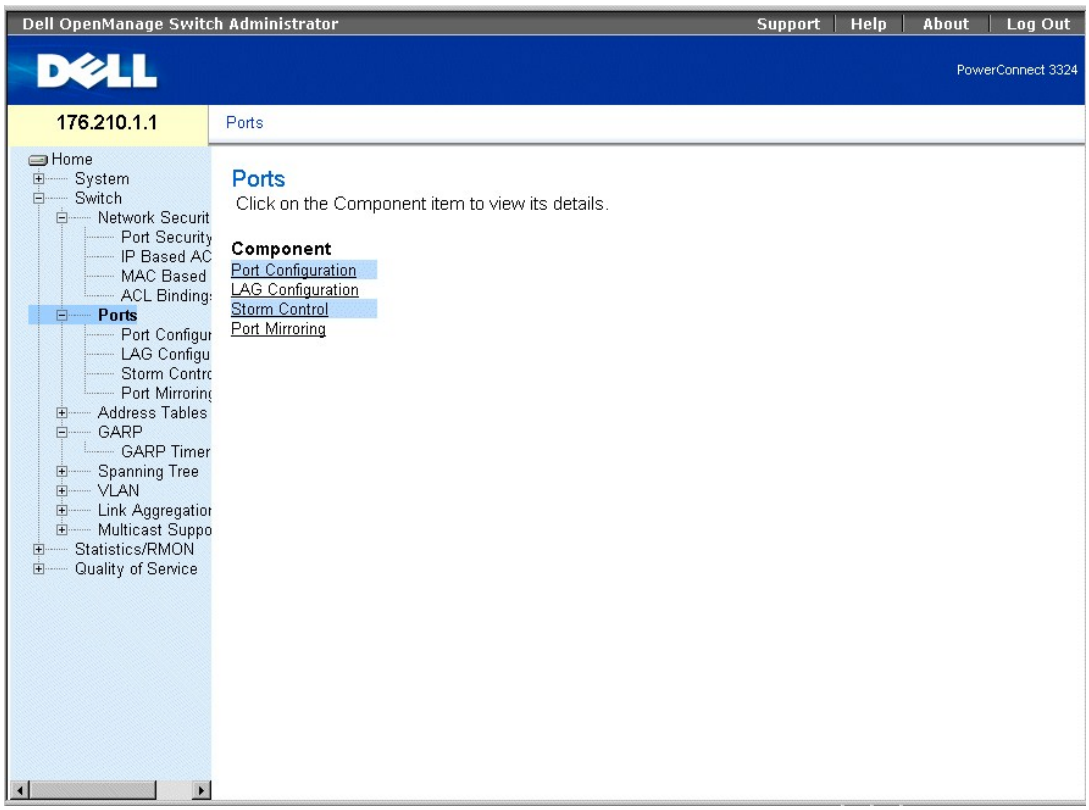
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# class-map class1 match-any

Console (config-cmap)# match access-group dell

Console (config-cmap)# exit

Console (config)# exit

Console # exit

Console> show class-map class1

Class Map match-any class1 (id4)
```

Konfigurieren von Anschlüssen

Dieser Abschnitt enthält eine Erläuterung sowie Anleitung zur Konfiguration der Anschlussfunktionalität, einschließlich erweiterter Funktionen wie Storm-Kontrolle und Anschlussspiegelung. So öffnen Sie die Seite **Ports**:

- Wählen Sie **Switch > Ports**. Die Seite **Ports** wird geöffnet.



Seite "Ports"

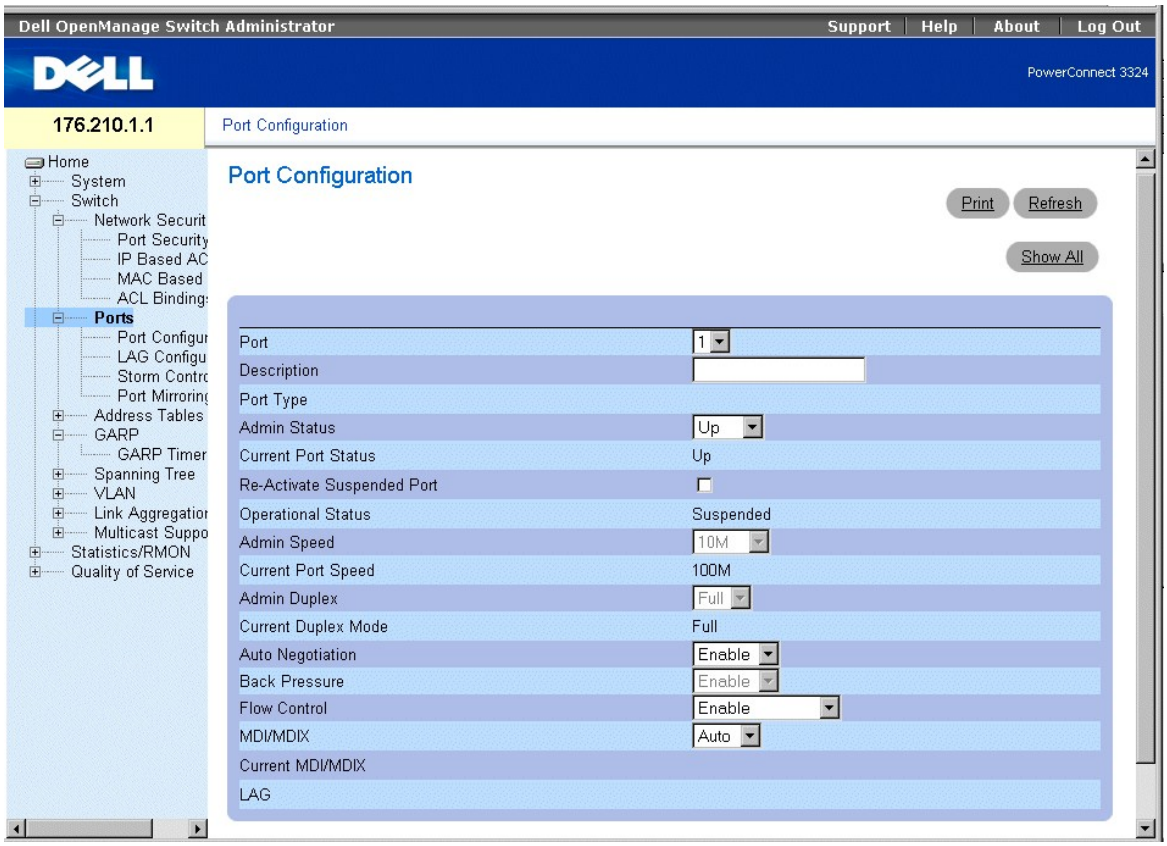
Dieser Abschnitt enthält die folgenden Themen:

- Definieren von Anschlussparametern
- Definieren von LAG-Parametern
- Aktivieren der Storm-Kontrolle
- Definieren von Anschluss-Spiegelsitzungen

Definieren von Anschlussparametern

Auf der Seite **Port Configuration** können Netzwerkadministratoren Anschlussparameter definieren. So öffnen Sie die Seite **Port Configuration**:

- Klicken Sie in der Strukturansicht auf **Switch > Ports > Port Configuration.** Die Seite **Port Configuration** wird geöffnet.



Port Configuration

Die Seite **Port Configuration** enthält folgende Felder:

- **Port** - Legt die Anschlussnummer fest.
- **Description** - Enthält eine kurze Schnittstellenbeschreibung, z. B. Ethernet.
- **Port Type** - Gibt den Anschlusstyp an. Folgende Feldwerte können ausgewählt werden:
  - Ethernet
  - Fast Ethernet
  - GE
- **Admin Status** - Steuert den über den Anschluss geleiteten Datenverkehr. Diese Option ist standardmäßig auf **Enable** gesetzt. Folgende Feldwerte können ausgewählt werden:
  - **Up** - Aktiviert die Weiterleitung des Datenverkehrs über den Anschluss.
  - **Down** - Deaktiviert die Weiterleitung des Datenverkehrs über den Anschluss.
- **Current Port Status** - Gibt den Betriebsstatus des Anschlusses an. Folgende Feldwerte können ausgewählt werden:
  - **Up** - Gibt an, dass der Anschluss derzeit betriebsbereit ist.
  - **Down** - Gibt an, dass der Anschluss derzeit nicht betriebsbereit ist.
- **Re-Activate Suspended Port** - Reaktiviert einen Anschluss, nachdem er über die Sicherheitsoptionen **Locked Port** oder **ACL** deaktiviert wurde.
- **Operational Status** - Gibt den Betriebsstatus des Anschlusses an.
- **Admin Speed** - Gibt die Geschwindigkeit an, mit der der Anschluss arbeitet. Dieser Wert kann nur festgelegt werden, wenn der Anschluss deaktiviert ist. Folgende Feldwerte können ausgewählt werden:
  - 10M
  - 100M
  - 1000M
- **Current Port Speed** - Gibt die Geschwindigkeit des synchronisierten Anschlusses in Bit/s an. Folgende Feldwerte können ausgewählt werden:
  - **10M**
  - **100M**

- **1000M**

- **Admin Duplex** - Legt den Duplexmodus für den synchronisierten Anschluss fest. Wenn für Admin Duplex der Wert Full festgelegt wurde, wird das Head-of-Line -Blocking für den ausgewählten Anschluss unterstützt. Folgende Feldwerte können ausgewählt werden:
  - **Full** - Die Schnittstelle unterstützt die simultane, beidseitig gerichtete Übertragung zwischen Gerät und Client. Dies ist der Standardwert.
  - **Half** - Die Schnittstelle unterstützt jeweils nur die einseitig gerichtete Übertragung zwischen Gerät und Client.
- **Current Duplex Mode** - Legt den Duplexmodus für den synchronisierten Anschluss fest. Folgende Feldwerte können ausgewählt werden:
  - **Full**
  - **Half**
- **Auto-Negotiation** - Aktiviert die Auto-Negotiation für das Gerät. Auto-Negotiation bezeichnet ein Protokoll zwischen zwei Verbindungspartnern, mit dessen Hilfe dem jeweils anderen Anschluss Übertragungsrate, Duplexmodus und Flusskontrollverhalten mitgeteilt werden. Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Aktiviert die Auto-Negotiation für den Anschluss.
  - **Disable** - Deaktiviert die Auto-Negotiation für den Anschluss. Dies ist der Standardwert.
  - **Current Auto Negotiation** - Gibt den Betriebsstatus der Auto-Negotiation an.
- **Back Pressure** - Aktiviert den Backpressure-Modus für das Gerät. Der Backpressure-Modus wird mit dem Halbduplexmodus verwendet, um den Empfang von Nachrichten über Anschlüsse zu deaktivieren. Wenn Backpressure aktiviert ist,, kann das Head-of-Line-Blocking nicht ausgeführt werden. Dies gilt auch für den Fall, dass es aktiviert ist.
- Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Aktiviert Backpressure für den Anschluss.
  - **Disable** - Deaktiviert Backpressure für den Anschluss. Dies ist der Standardwert.
  - **Current Back Pressure** - Gibt den Backpressure-Betriebsstatus an.
- **Flow Control** - Gibt an, ob die Flusskontrolle für den Anschluss aktiviert ist. Die Flusskontrolle ist aktiviert, wenn sich das Gerät im Duplexmodus befindet. Wenn die Flusskontrolle aktiviert ist, ist zusätzlich das Head-of-Line-Blocking für den ausgewählten Anschluss deaktiviert. Wenn die Flusskontrolle aktiviert ist, kann das Head-of-Line-Blocking nicht ausgeführt werden. Dies gilt auch für den Fall, dass es aktiviert ist. Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Gibt an, dass die Flusskontrolle für das Gerät aktiviert ist.
  - **Disable** - Gibt an, dass die Flusskontrolle für das Gerät deaktiviert ist. Dies ist der Standardwert.
  - **Current Flow Control** - Gibt den Betriebsstatus der Flusskontrolle an.
  - **Auto-negotiation** - Aktiviert die Auto-Negotiation der Flusskontrolle für den Anschluss.
  - **Tx Only** - Aktiviert die Auto-Negotiation für Egress-Anschlüsse.
  - **Rx Only** - Aktiviert die Auto-Negotiation für Ingress-Anschlüsse.
- **MDI/MDIX** - Ermöglicht dem Gerät die Erkennung gekreuzter und nicht gekreuzter Kabel. Hubs und Switches sind entgegengesetzt zu Endstationen verkabelt. Zur Verbindung von Hubs oder Switches mit Endstationen werden ungekreuzte Ethernet-Kabel verwendet. Wenn zwei Hubs/Switches bzw. zwei Endstationen miteinander verbunden werden, wird mit Hilfe eines Crossover-Kabels sichergestellt, dass die Paare richtig angeschlossen sind. Die Standardverkabelungen sind:
  - Media Dependent Interface with Crossover (MDIX) für Hubs und Switches
  - Media Dependent Interface (MDI) für Endstationen

ANMERKUNG: Die automatische MDIX-Unterstützung funktioniert nicht für FE-Anschlüsse, wenn die Auto-Negotiation deaktiviert ist.

In der folgenden Tabelle sind die Parameterkombinationen beschrieben, die für die Konfiguration von Anschlüssen erforderlich sind. Durch diese Einstellungen wird die Verfügbarkeit von Konfigurationsfunktionen sichergestellt.

	Auto-Negotiation	
	Aktiviert	**Deaktiviert**
Auto	zulässig	**unzulässig**
MDI	zulässig	zulässig
MDIX	zulässig	zulässig

- **Current MDI/MDIX** - Gibt den MDIX-Betriebsstatus an. Folgende Feldwerte können ausgewählt werden:
  - **MDI**
  - **MDIX**
  - **Auto** - Gibt an, dass der Wert automatisch festgelegt wird.
- **LAG** - Gibt an, ob der Anschluss einer LAG angehört.

Definieren von Anschlussparametern:

1. Öffnen Sie die Seite **Port Configuration**.
2. Wählen Sie einen Anschluss im Feld **Port** aus.

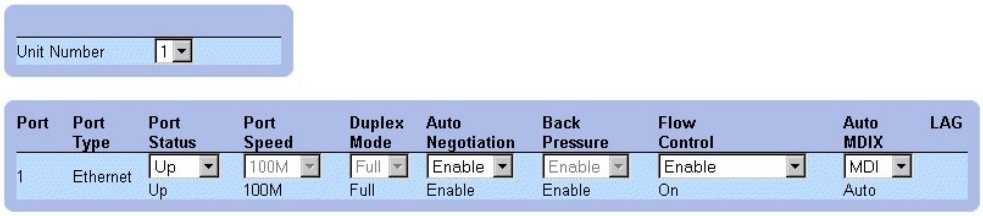
3. Definieren Sie die Felder **Description**, **Admin Status**, **Admin Speed**, **Admin Duplex**, **Auto Negotiation**, **Back Pressure**, **Admin Auto MDIX** und/oder **Admin Flow Control**.
4. Klicken Sie auf **Apply Changes.** Die Anschlussparameter werden im Gerät gespeichert.

Ändern von Anschlussparametern:

1. Öffnen Sie die Seite **Port Configuration**.
2. Wählen Sie einen Anschluss im Feld **Port** aus.
3. Bearbeiten Sie die Felder **Description**, **Admin Status**, **Admin Speed**, **Admin Duplex**, **Auto Negotiation**, **Back Pressure**, **Admin Auto MDIX** und/oder **Admin Flow Control**.
4. Klicken Sie auf **Apply Changes.** Die Anschlussparameter werden auf dem Gerät gespeichert.

Anzeigen der Port Configuration Table:

1. Öffnen Sie die Seite **Port Configuration**.
2. Klicken Sie auf **Show All**. Die **Port Configuration Table** wird geöffnet.



Port Configuration Table

Zusätzlich zu den Feldern auf der Seite **Port Configuration** enthält die **Port Configuration Table** das folgende Feld:

- **Unit Number** - Gibt die Nummer der Stack-Einheit an, für die Anschlussinformationen angezeigt werden.

Konfigurieren von Anschlüssen mit Hilfe der CLI-Befehle

In den folgenden Beispielen wird beschrieben, wie ein Anschluss in den MDIX- bzw. MDI-Modus geschaltet wird. Um für einen Anschluss den MDIX-Modus zu aktivieren, geben Sie an der Systemeingabeaufforderung Folgendes ein:

```
console(config-if)# mdix on
```

Die folgende Meldung wird angezeigt:

```
console # show inter config ethernet 1/e1


Flow Admin Back Mdix
Port Type Duplex Speed Neg Control State Pressure Mode


.....................................................


1/e1 100M-Copper Enabled Off Up Disabled On
```

Um für einen Anschluss den MDI-Modus zu aktivieren, geben Sie an der Systemeingabeaufforderung Folgendes ein:

```
console(config)# inter eth 1/e1

console(config-if)# no mdix
```

Die folgende Meldung wird angezeigt:

```
console # show inter config ethernet 1/e1

Flow Admin Back Mdix
Port Type Duplex Speed Neg Control State Pressure Mode

.....................................................

1/e1 100M-Copper Enabled Off Up Disabled Off
```

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zur Konfiguration der Anschlüsse zusammengefasst, die auf der Seite **Port Configuration** angezeigt werden.

CLI-Befehl	**Beschreibung**
interface ethernet *Schnittstelle*	Aktiviert den Schnittstellenkonfigurationsmodus, um eine Ethernet-Schnittstelle zu konfigurieren.
description *Zeichenfolge*	Fügt einer Schnittstellenkonfiguration eine Beschreibung hinzu.
shutdown	Deaktiviert Schnittstellen innerhalb des derzeit festgelegten Kontexts.
set interface active {ethernet *Schnittstelle* **| port-channel** *Anschlusskanalnummer***}**	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 | rx | tx}	Konfiguriert die Flusskontrolle für eine bestimmte Schnittstelle.
mdix {on | auto}	Aktiviert die automatische Kreuzkabel-Erkennung für eine bestimmte Schnittstelle bzw. einen bestimmten Anschlusskanal.
show interfaces configuration [ethernet *Schnittstelle* **| port-channel** *Anschlusskanalnummer***]**	Zeigt die Konfiguration aller konfigurierten Schnittstellen an.
show interfaces status [ethernet *Schnittstelle* **| port-channel** *Anschlusskanalnummer***]**	Zeigt den Status aller konfigurierten Schnittstellen an.
show interfaces description [ethernet Schnittstelle | port-channel *Anschlusskanalnummer***]**	Zeigt die Beschreibung aller konfigurierten Schnittstellen an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# interface ethernet 1/e5

Console(config-if)#

Console (config-if)# description RD SW#3

Console (config-if)# shutdown
```

```
Console (config-if)# no shutdown

Console (config-if)# speed 100

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# show interfaces configuration

Port Type Duplex Speed Neg Flow Back MDIX Admin

Cont Pres Mode State

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

1/e1 1g-combo-c Full 1000 Auto On Enable Auto Up

2/e1 100-copper Full 1000 Off Off Disable off Up

2/e2 1g-Fiber Full 1000 Off Off Disable on Up


Neg : Negotiation

Flow Cont: Flow Control

Back Pres: Back Pressure

Console# show interfaces status
```

```
Port Port Duplex Speed Neg Flow Back MDI Link

Cont Pres Mode State

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

2/e1 100-copper Full 1000 off Off Disable Off Down*



Legend

Neg : Negotiation

Flow Cont: Flow Control

Back Pres: Back Pressure

*: The interface was suspended by the system.

Router# show interfaces description



Port Description

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

1/e1 Port that should be used for management only

2/e1

2/e2



Port Channel Description

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

1 dell

2 projects
```

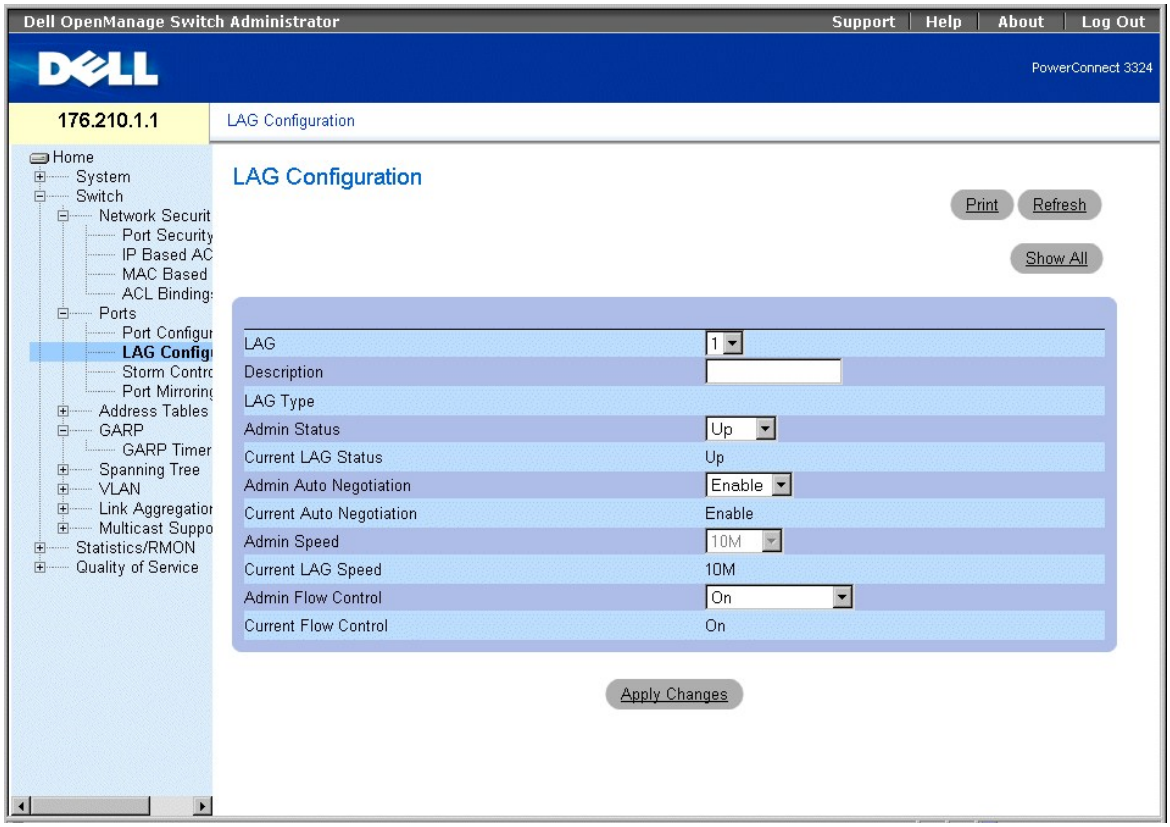
Definieren von LAG-Parametern

Auf der Seite **LAG Configuration** können Netzwerkverwalter Parameter für konfigurierte LAGs festlegen. Der PowerConnect 3324/3348 unterstützt bis zu acht Anschlüsse pro LAG sowie sechs LAGs pro System. Das System bietet sechs permanente LAGs. Weitere Informationen zu Link Aggregated Groups (LAGs) und zur Zuweisung von Anschlüssen zu LAGs finden Sie unter "Aggregieren von Anschlüssen".

So öffnen Sie die Seite **LAG Configuration**:

ANMERKUNG: Wenn die Anschlusskonfiguration geändert wird, während der Anschluss einer LAG angehört, werden die Konfigurationsänderungen erst wirksam, nachdem der Anschluss aus der LAG entfernt wurde.

- Klicken Sie in der Strukturansicht auf **Switch > Ports > LAG Configuration.** Die Seite LAG Configuration wird angezeigt.



Seite "LAG Configuration"

Die Seite **LAG Configuration** enthält folgende Felder:

- **LAG** - Gibt die LAG-Nummer an.
- **Description** - Zeigt eine benutzerdefinierte LAG-Beschreibung an.
- **LAG Type** - Gibt die maximale Geschwindigkeit der LAG an.
- **Admin Status** - Steuert den von der ausgewählten LAG gesendeten Datenverkehr. Dieser Parameter ist standardmäßig auf **Up** gesetzt. Folgende Feldwerte können ausgewählt werden:
  - **Up** - Aktiviert die Weiterleitung des Datenverkehrs über die LAG.
  - **Down** - Deaktiviert die Weiterleitung des Datenverkehrs über die LAG.
- **Current LAG Status** - Gibt den LAG-Status an. Folgende Feldwerte sind möglich:
  - **Up** - Gibt an, dass die LAG derzeit betriebsbereit ist.
  - **Down** - Gibt an, dass die LAG derzeit nicht betriebsbereit ist.
- **Admin Auto Negotiation** - Aktiviert 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. Folgende Feldwerte können ausgewählt werden:

- **Enable** - Aktiviert die Auto-Negotiation für die LAG.
- **Disable** - Deaktiviert die Auto-Negotiation für die LAG.

- **Current Auto Negotiation** - Gibt die aktuelle Einstellung für die Auto-Negotiation an. Folgende Feldwerte sind möglich:
  - **Enable**
  - **Disable**
- **Admin Speed** - Gibt die Geschwindigkeit der LAG an. Dieser Wert kann nur festgelegt werden, wenn die LAG deaktiviert ist. Folgende Feldwerte können ausgewählt werden:
  - **10M**
  - **100M**
  - **1000M**
- **Current LAG Speed** - Gibt die Geschwindigkeit der synchronisierten LAG in Bit/s an. Folgende Feldwerte können ausgewählt werden:
  - **10M**
  - **100M**
  - **1000M**
- **Current Duplex Mode** - Legt den LAG-Konversationstyp fest. Die aktuellen Feldwerte lauten:
  - **Full** - Die Schnittstelle unterstützt die simultane, beidseitig gerichtete Übertragung zwischen Gerät und Client.
  - **Half** - Die Schnittstelle unterstützt jeweils nur die einseitig gerichtete Übertragung zwischen Gerät und Client.
- **Admin Current Duplex Mode** - Legt den LAG-Konversationstyp fest. Die aktuellen Feldwerte lauten:
  - **Full** - Die Schnittstelle unterstützt die simultane, beidseitig gerichtete Übertragung zwischen Gerät und Client.
  - **Half** - Die Schnittstelle unterstützt jeweils nur die einseitig gerichtete Übertragung zwischen Gerät und Client.
- **Flow Control** - Gibt an, ob die Flusskontrolle für die LAG aktiviert ist. Die möglichen Werte lauten:
  - **Off** - Deaktiviert die Flusskontrolle für die LAG. Dies ist der Standardwert.
  - **On** - Aktiviert die Flusskontrolle für die LAG.
  - **Auto-negotiation** - Aktiviert die Auto-Negotiation der Flusskontrolle für die LAG.
- **Current Flow Control** - Gibt die aktuelle Einstellung der Flusskontrolle an. Die möglichen Werte lauten:
  - **Off**
  - **On**
  - **Auto-negotiation**

Definieren von LAG-Parametern:

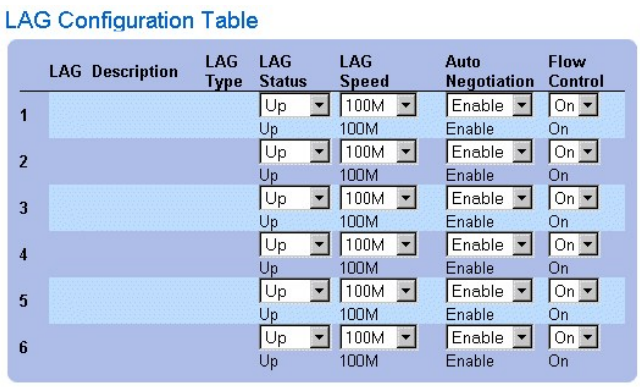
1. Öffnen Sie die Seite **LAG Configuration**.
2. Wählen Sie eine LAG im Feld **LAG** aus.
3. Definieren Sie die Felder **Description**, **Admin Status**, **Port Speed**, **Admin Auto Negotiation**, **Admin Speed** und/oder **Admin Flow Control**.
4. Klicken Sie auf **Apply Changes**. Die LAG-Parameter werden im Gerät gespeichert.

Ändern von LAG-Parametern:

1. Öffnen Sie die Seite **LAG Configuration**.
2. Wählen Sie eine LAG im Feld **LAG** aus.
3. Bearbeiten Sie die Felder **Description**, **Admin Status**, **Port Speed**, **Admin Auto Negotiation**, **Admin Speed** und/oder **Admin Flow Control**.
4. Klicken Sie auf **Apply Changes**. Die LAG-Parameter werden im Gerät gespeichert.

Anzeigen der LAG Configuration Table:

1. Öffnen Sie die Seite **LAG Configuration**.
2. Klicken Sie auf **Show All**. Die **LAG Configuration Table** wird geöffnet.



LAG Configuration Table

Konfigurieren von LAGs mit Hilfe der CLI-Befehle

Das folgenden Beispiel zeigt, wie die LAG mit den Parametern Auto-Negotiation deaktiviert, 100, Full eingerichtet wird.

Geben Sie an der Systemeingabeaufforderung Folgendes ein, um die statische Verbindungsaggregation einzurichten:

```
console> en

console# config

console(config)# interface port-channel 1

console(config-if)# no neg

console(config-if)# speed 100

console(config-if)# exit

console(config)# interface range ethernet 1/e23-24

console(config-if)# no mdix

console(config-if)# no neg

console(config-if)# speed 100

console(config-if)# duplex full

console(config-if)# channel-group 1 mode on
```

```
console(config-if)# end
```

Die folgende Meldung wird angezeigt:

```
console# sh interfaces status port-channel 1

Flow Link Back
ch Type Duplex Speed Neg Control State Pressure

.....................................................

ch1 100M Full 100 Disabled Off Up Disabled
```

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zur Konfiguration der LAGs zusammengefasst, die auf der Seite **LAG Configuration** angezeigt werden.

CLI-Befehl	**Beschreibung**
interface port-channel *Anschlusskanalnummer*	Erstellt einen Anschlusskanal und aktiviert den "Port Channel"-Konfigurationsmodus.
channel-group *Anschlusskanalnummer* **mode {on | auto}**	Verknüpft einen Anschluss mit einem Anschlusskanal.
show interfaces port-channel [*Anschlusskanalnummer***]**	Zeigt Anschlusskanalinformationen an (welche Anschlüsse einem Anschlusskanal angehören und ob sie derzeit aktiv sind oder nicht).

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console(config)# interface ethernet 1/e5

Console (config-if)# channel-group 1 mode on

Console (config-if)# exit

Console (config-if)# exit

Console # show interfaces port-channel

Channel Port

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

1 Active 1/e5, 2/e2 Inactive 3/e3

2 Active 1/e2

3 Inactive 3/e8
```

Aktivieren der Storm-Kontrolle

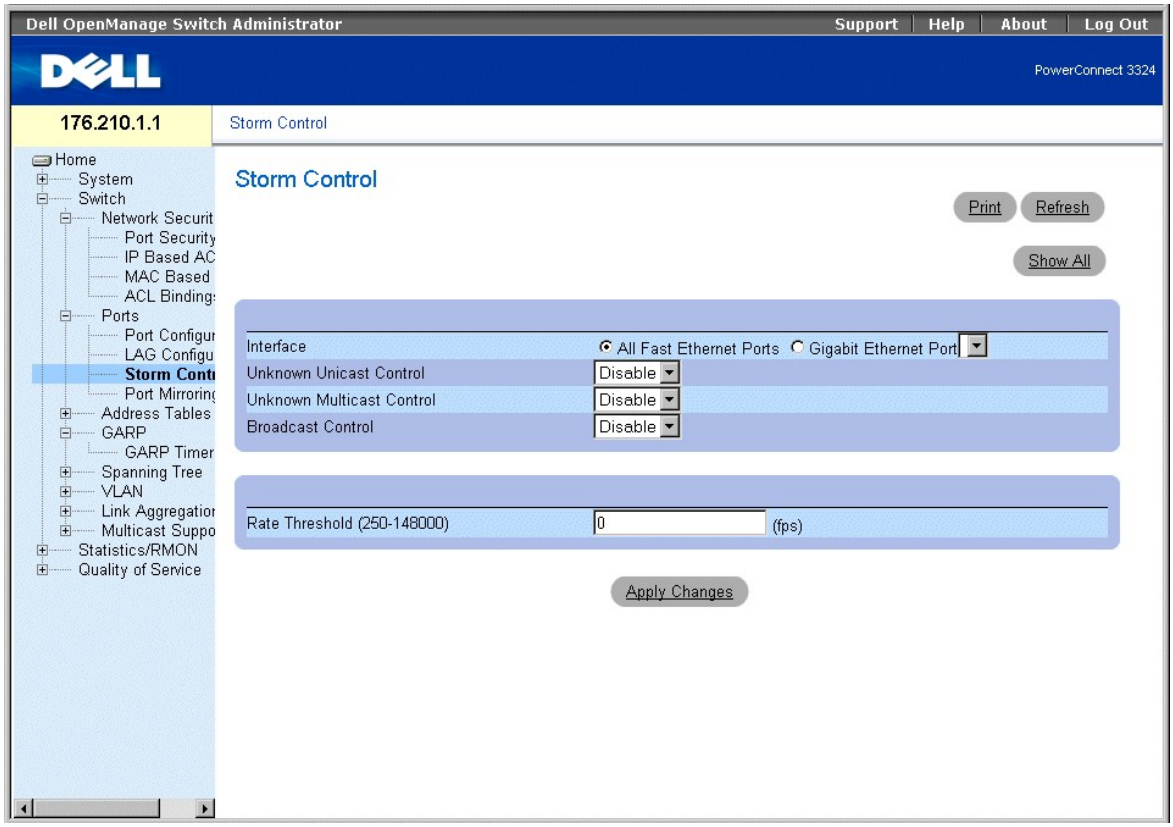
Ein Broadcast-Storm resultiert aus einem sehr hohen Aufkommen von Broadcast-Nachrichten, die gleichzeitig über einen einzelnen Anschluss im Netzwerk übertragen werden. Rückmeldungen auf weitergeleitete Nachrichten belasten das Netzwerk, wodurch Netzwerkressourcen strapaziert bzw. Netzwerkausfälle verursacht werden.

Die Storm-Kontrolle wird für alle Fast Ethernet- oder Giga-Anschlüsse aktiviert, indem der Pakettyp und die Übertragungsrate der Pakete definiert wird. Anschlüsse können auch gruppiert werden, um Storm-Schutz für die gesamte Gruppe zu gewährleisten.

Die Geschwindigkeit der eingehenden Broadcast-, Multicast- und unbekannten Frames wird pro Anschluss vom System gemessen. Sobald eine benutzerdefinierte Rate überschritten wird, werden Frames abgelehnt.

Auf der Seite **Storm Control** können Netzwerkverwalter die Storm-Kontrolle aktivieren und konfigurieren. So öffnen Sie die Seite **Storm Control**:

- Klicken Sie in der Strukturansicht auf **Switch > Ports > Storm Control,** um die Seite **Storm Control** zu öffnen.



Seite "Storm Control"

Die Seite **Storm Control** enthält folgende Felder:

- **Interface** - Gibt die Schnittstelle an, für welche die Storm-Kontrolle konfiguriert wird.
  - **All Fast Ethernet Ports** - Gibt an, dass die Storm-Kontrolle für alle FE-Anschlüsse aktiviert ist. Die Storm-Kontrolle kann auf einzelne GE-Anschlüsse angewendet werden.
  - **Gigabit Ethernet Port** - Gibt an, dass die Storm-Kontrolle für den ausgewählten Gigabit Ethernet-Anschluss aktiviert ist. Die Storm-Kontrolle ist für ALLE FE-Anschlüsse entweder aktiviert oder deaktiviert.
- **Unknown Unicast Control** - Aktiviert die Eindämmung unbekannter Unicast-Pakete für das Gerät. Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Aktiviert die Eindämmung unbekannter Unicast-Pakete für das Gerät.
  - **Disable** - Deaktiviert die Eindämmung unbekannter Unicast-Pakete für das Gerät.

- **Unknown Multicast Control** - Aktiviert die Eindämmung unbekannter Multicast-Pakete für das Gerät. Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Aktiviert die Eindämmung unbekannter Multicast-Pakete für das Gerät.
  - **Disable** - Deaktiviert die Eindämmung unbekannter Multicast-Pakete für das Gerät.
- **Broadcast Control** - Aktiviert die Eindämmung unbekannter Broadcast-Pakete. Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Aktiviert die Eindämmung von Broadcast-Paketen.
  - **Disable** - Deaktiviert die Eindämmung von Broadcast-Paketen.
- **Rate Threshold (250-148000)** - Legt die Beschränkung der Broadcast-Paketrate für die Storm-Kontrolle fest. Bei FE-Anschlüssen liegt die Rate zwischen 250 und 148.000 und bei GE-Anschlüssen zwischen 250 und 262.143 Paketen. Der Standardwert für FE-Anschlüsse beträgt 148.000 und der für GE-Anschlüsse 262.143 Pakete.

Aktivieren der Storm-Kontrolle für das Gerät:

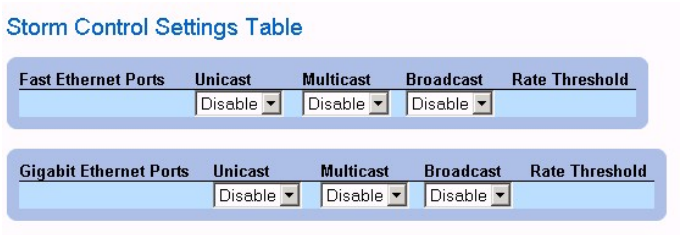
1. Öffnen Sie die Seite **Storm Control**.
2. Wählen Sie eine Schnittstelle aus, für welche die Storm-Kontrolle implementiert wird.
3. Definieren Sie die Felder **Unknown Unicast Control**, **Unknown Multicast Control**, **Broadcast Control** und **Rate Threshold (250-148000)**.
4. Klicken Sie auf **Apply Changes**. Die Storm-Kontrolle wird für das Gerät aktiviert.

Ändern der Anschlussparameter für die Storm-Kontrolle:

1. Öffnen Sie die Seite **Storm Control**.
2. Bearbeiten Sie die Felder **Unknown Unicast Control**, **Unknown Multicast Control**, **Broadcast Control** und **Rate Threshold (250-148000)**.
3. Klicken Sie auf **Apply Changes.** Die Anschlussparameter für die Storm-Kontrolle werden im Gerät gespeichert.

Anzeigen der Port Parameters Table:

1. Öffnen Sie die Seite **Storm Control**.
2. Klicken Sie auf **Show All**. Die **Storm Control Settings Table** wird geöffnet.



Storm Control Settings Table

Konfigurieren der Storm-Kontrolle mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zur Konfiguration der Storm-Kontrolle zusammengefasst wie auf der Seite **Storm Control** gezeigt.

CLI-Befehl	Beschreibung
port storm-control enable {unknown | broadcast | multicast} {fastethernet | gigaethernet *Schnittstelle*}	Aktiviert die Broadcast Storm-Kontrolle für Unicast-, Multicast- und Broadcast-Pakete.
port storm-control rate gigaethernet *Schnittstellenrate*.	Konfiguriert die maximale Broadcast-Rate.
show ports storm-control	Zeigt die Konfiguration der Storm-Kontrolle an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console(config)# port storm-control rate fastethernet 300
```

```
Console(config)# port storm-control enable fastethernet

Console# show ports storm-control

Port Unknown Broadcast Multicast Rate

[Packets/sec]

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

Gigaethernet 1 Enabled Disabled Enabled 2000

Gigaethernet 2 Enabled Enabled Enabled 2000

FastEthernet Enabled Enabled Enabled 1000
```

Definieren von Anschluss-Spiegelsitzungen

Durch die Anschlussspiegelung wird der Netzwerkdatenverkehr überwacht und gespiegelt, indem Kopien eingehender und ausgehender Pakete von einem Anschluss an einen Überwachungsanschluss weitergeleitet werden. Die Anschlussspiegelung kann als Diagnosetool und/oder Debuggingfunktion verwendet werden. Darüber hinaus ermöglicht sie die Leistungsüberwachung des Switches.

Netzwerkadministratoren konfigurieren die Anschlussspiegelung, indem sie einen spezifischen Anschluss zum Kopieren aller Pakete und andere Anschlüsse auswählen, von denen die Pakete kopiert werden. Vor dem Konfigurieren der Anschlussspiegelung sollten Sie Folgendes beachten:

- Überwachte Anschlüsse können nicht schneller betrieben werden als die Überwachungsanschlüsse.
- Alle RX/TX-Pakete sollten auf demselben Anschluss überwacht werden.
- Der PowerConnect 3348 führt die Spiegelung zwischen den Anschlüssen 1 bis 24 und 25 bis 48 derselben Einheit durch. Die Spiegelung kann auch zu und von den Anschlüssen 25 bis 48 sowie zu und von den Anschlüssen 25 bis 48 eines anderen PowerConnect 3348- bzw. eines beliebigen PowerConnect 3324-Anschlusses erfolgen.
- Der PowerConnect 3348 kann Pakete auf eine beliebige PowerConnect 3324-Einheit spiegeln, solange es sich beim Quellanschluss nicht um den G2-Anschluss handelt. Der PowerConnect 3348 kann Pakete auf und von einer anderen PowerConnect 3348-Einheit spiegeln, solange sich der Anschluss im Bereich 25 bis 48 des PowerConnect befindet.

Die folgenden Beschränkungen gelten für Anschlüsse, die als Zielanschlüsse konfiguriert sind:

- Anschlüsse dürfen nicht als Quellanschluss konfiguriert werden.
- Anschlüsse dürfen keine LAG-Komponente sein.
- IP-Schnittstellen werden nicht auf dem Anschluss konfiguriert.
- GVRP wird nicht für den Anschluss aktiviert.
- Der Anschluss ist keine VLAN-Komponente.
- Es darf nur ein Zielanschluss definiert sein.

Die folgenden Beschränkungen gelten für Anschlüsse, die als Quellanschlüsse konfiguriert werden:

- Quellanschlüsse dürfen keine LAG-Komponente sein.
- Anschlüsse dürfen nicht als Zielanschluss konfiguriert werden.
- Alle Pakete werden gekennzeichnet, wenn sie vom Zielanschluss aus übertragen werden.

Die folgende Beschränkung gilt für Anschlüsse, die als Quellanschlüsse konfiguriert sind:

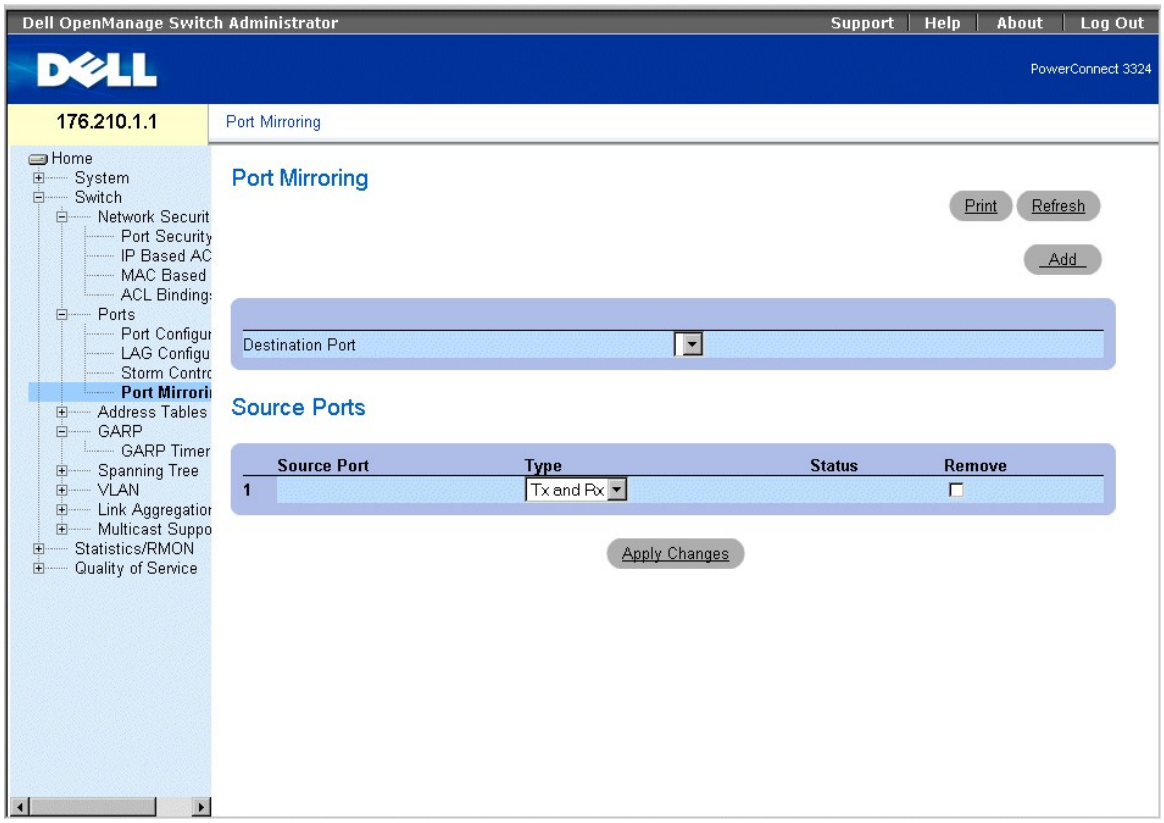
- Wird ein nicht gekennzeichnetes Paket vom Quellanschluss empfangen, erhält das Paket die Standard-PVID des Quellanschlusses, sobald es an den Zielanschluss der Spiegelung gesendet wird.

Alle RX/TX-Pakete sollten auf demselben Anschluss überwacht werden.

So öffnen Sie die Seite **Port Mirroring**:

- Klicken Sie in der Strukturansicht auf **Switch > Ports > Port Mirroring.** Die Seite Port Mirroring wird geöffnet.

ANMERKUNG: Wenn ein Anschluss als Ziel für eine Spiegelung festgelegt wird, werden alle normalen Operationen auf diesem Anschluss ausgesetzt. Diese Operationen umfassen Spanning Tree und LACP.



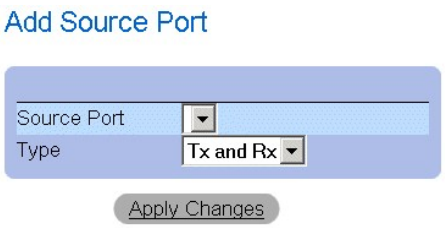
Seite "Port Mirroring"

- **Destination Port** - Definiert die Nummer des Anschlusses, auf den der Datenverkehr gespiegelt wird. Ein Zielanschluss kann sich nicht selbst spiegeln, er darf keinem anderen VLAN als dem des Quellanschlusses angehören und nicht mit einer IP-Schnittstelle konfiguriert werden. Sämtlicher Datenverkehr auf dem Quellanschluss wird gekennzeichnet.
- **Source Port** - Definiert die Nummer des Anschlusses, von dem der Datenverkehr kopiert wird. Auf einen Zielanschluss können maximal acht Quellanschlüsse gespiegelt werden.
- **Type** - Legt den Datenverkehrstyp des gespiegelten Anschlusses fest. Folgende Feldwerte können ausgewählt werden:
  - **RX** - Gibt an, dass der eingehende Datenverkehr gespiegelt wird.
  - **TX** - Gibt an, dass der ausgehende Datenverkehr gespiegelt wird.
  - **Both** - Gibt an, dass sowohl eingehender als auch ausgehender Datenverkehr gespiegelt wird.
- **Status** - Gibt den Anschlussstatus an. Folgende Feldwerte können ausgewählt werden:
  - **Active** - Gibt an, dass der Anschluss aktiviert ist und Netzwerkverkehr empfängt/weiterleitet.
  - **Not Active** - Gibt an, dass der Anschluss deaktiviert ist und keinen Netzwerkverkehr empfängt/weiterleitet.
- **Remove** - Entfernt die Anschluss-Spiegelsitzung. Folgende Feldwerte können ausgewählt werden:
  - **Aktiviert** - Entfernt die Anschluss-Spiegelsitzung.

- **Deaktiviert** - Behält die Anschluss-Spiegelsitzung bei.

Hinzufügen einer Anschluss-Spiegelsitzung:

1. Öffnen Sie die Seite **Port Mirroring**.
2. Klicken Sie auf **Hinzufügen**. Die Seite **Add Source Port** wird geöffnet.



Add Source Port

3. Definieren Sie die Felder **Source Port** und **Type**.
4. Klicken Sie auf **Apply Changes**. Der neue Quellanschluss wird definiert und das Gerät aktualisiert.

Löschen eines Zielanschlusses aus einer Anschluss-Spiegelsitzung:

1. Öffnen Sie die Seite **Port Mirroring**.
2. Aktivieren Sie das Kontrollkästchen **Remove**.
3. Klicken Sie auf **Apply Changes**. Die Anschluss-Spiegelsitzung wird gelöscht und das Gerät aktualisiert.

Konfigurieren einer Anschluss-Spiegelsitzung mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Konfiguration der Anschluss-Spiegelsitzung zusammengefasst, die auf der Seite **Port Mirroring** angezeigt wird.

CLI-Befehl	Beschreibung
port monitor *SRC-Schnittstelle* **[rx | tx]**	Zeigt den Kopierstatus des Anschlusses an.
show ports monitor	Startet eine Anschluss-Spiegelsitzung.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console(config)# interface ethernet 1/e1

Console(config-if)# port monitor 1/e8

Console# show ports monitor

Source port Destination Port Type Status

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

1/e1 1/e8 RX, TX Active
```

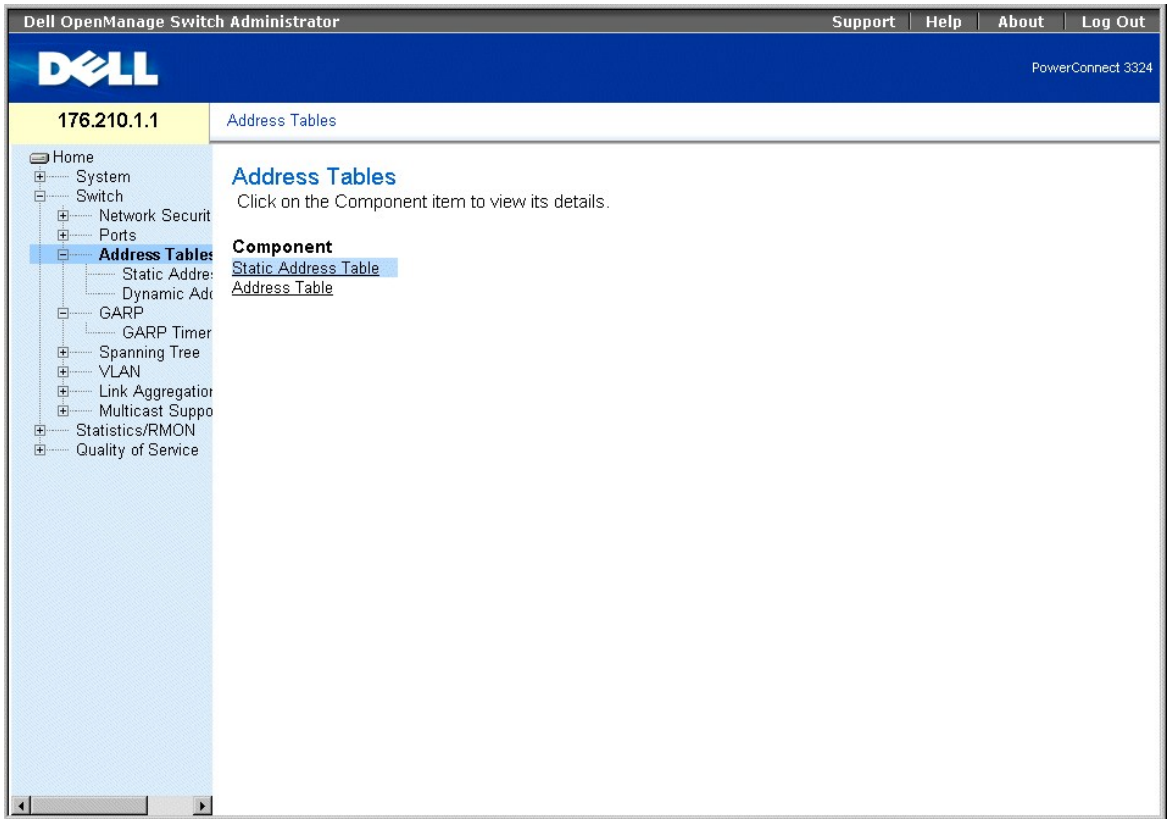
```
1/e2 1/e8 RX Active
```

Konfigurieren von Adresstabellen

MAC-Adressen werden entweder in Datenbanken mit statischen oder mit dynamischen Adressen gespeichert. Ein Paket, das an eine Zieladresse gerichtet ist, die in einer der Datenbanken gespeichert ist, wird sofort an den Anschluss weitergeleitet. Die Tabellen mit statischen und dynamischen Adressen können nach Schnittstelle, VLAN und Schnittstellentyp sortiert werden. MAC-Adressen werden dynamisch erfasst, sobald Pakete aus einer Quelle auf dem Switch eingehen. Adressen werden mit Anschlüssen verknüpft, indem die Anschlüsse aus der Quelladresse des Frames ausgelesen werden. Frames, die an eine MAC-Zieladresse adressiert sind, die mit keinem Anschluss verknüpft ist, werden an alle Anschlüsse des relevanten VLANs weitergeleitet. Statische Adressen werden manuell vom Benutzer konfiguriert. Damit in der Bridging-Tabelle kein Überlauf auftritt, werden dynamische MAC-Adressen gelöscht, nachdem über einen gewissen Zeitraum kein Datenverkehr verzeichnet wurde.

So öffnen Sie die Seite **Address Tables**:

- Klicken Sie in der Strukturansicht auf **Switch > Address Tables.** Die Seite **Address Tables** wird geöffnet.



Seite "Address Tables"

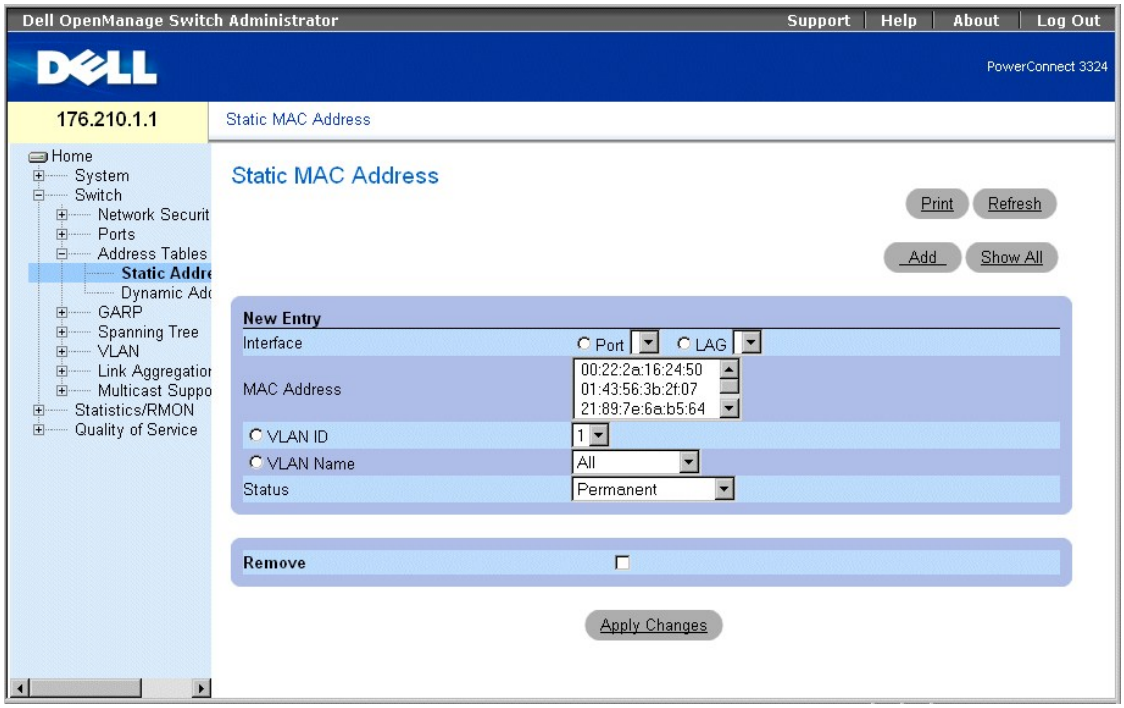
Die Seite **Address Tables** enthält Links zu folgenden Themen:

- Definieren statischer Adressen
- Anzeigen dynamischer Adressen

Definieren statischer Adressen

Die Seite **Static MAC Address** enthält eine Liste statischer MAC-Adressen. Statische Adressen können über die Seite **Static MAC Address** hinzugefügt und entfernt werden. Zusätzlich können mehrere MAC-Adressen für einen einzelnen Anschluss definiert werden. So öffnen Sie die Seite **Static MAC Address**:

- Klicken Sie in der Strukturansicht auf **Switch > Address Tables > Static Address.** Die Seite **Add Static MAC Address** wird geöffnet.



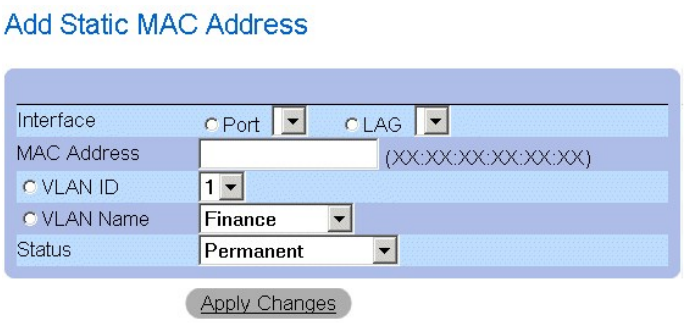
Seite "Add Static MAC Address"

Die Seite **Add Static MAC Address** enthält folgende Felder:

- **Interface** - Gibt die spezifische Schnittstelle an, für die eine statische MAC-Adresse hinzugefügt wird. Folgende Feldwerte können ausgewählt werden:
  - **Port** - Gibt den spezifischen Anschluss an, für den eine MAC-Adresse hinzugefügt wird.
  - **LAG** - Gibt die spezifische LAG an, für die eine MAC-Adresse hinzugefügt wird.
- **MAC Address** - Legt die in der **Current Static Address List** aufgeführte MAC-Adresse fest.
- **VLAN ID** - Gibt den Wert der mit der MAC-Adresse verknüpften VLAN-ID an.
- **VLAN Name** - Gibt den benutzerdefinierten VLAN-Namen an.
- **Status** - Definiert den Status der statischen MAC-Adresse. Folgende Feldwerte können ausgewählt werden:
  - **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.
  - **Timeout** - Gibt an, dass die MAC-Adresse gelöscht wird, nachdem das Zeitlimit des Gerätes erreicht wurde.
  - **Secure** - Stellt sicher, dass eine mit der Sicherheitsoption Locked Port konfigurierte MAC-Adresse nicht gelöscht wird. Eine sichere MAC-Adresse wird von der Seite "Port Security" aus gelöscht.

Hinzufügen einer statischen Adresse zur Static Address Table:

1. Öffnen Sie die **Static Address Table**.
2. Klicken Sie auf **Add**. Die Seite **Add Static MAC Address** wird geöffnet.



Seite "Add Static MAC Address"

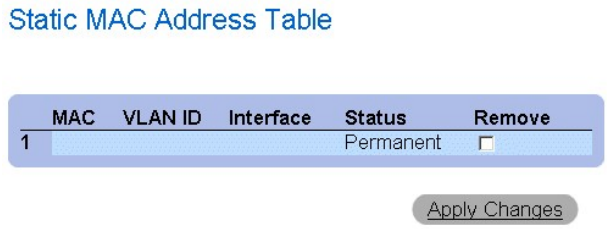
3. Definieren Sie die Felder **Interface**, **MAC Address**, **VLAN ID** oder **VLAN Name** und **Status**.
4. Klicken Sie auf **Apply Changes**. Die neue statische Adresse wird der Static Address Table hinzugefügt und das Gerät aktualisiert.

Ändern einer statischen Adresse in der Static Address Table:

1. Öffnen Sie die **Static Address Table**.
2. Ändern Sie die Felder **Port**, **MAC Address** und **VLAN**.
3. Klicken Sie auf **Apply Changes**. Die statische Adresse wird geändert und das Gerät aktualisiert.

Anzeigen der Static MAC Address Table:

1. Öffnen Sie die **Static Address Table**.
2. Klicken Sie auf **Show All**. Die **Static MAC Address Table** wird geöffnet.



Static MAC Address Table

Entfernen einer statischen Adresse aus der Static Address Table:

1. Öffnen Sie die **Static Address Table**.
2. Klicken Sie auf **Show All**, um die **Static MAC Address Table** zu öffnen.
3. Wählen Sie einen einzelnen oder mehrere Tabelleneinträge aus.
4. Aktivieren Sie das Kontrollkästchen **Remove**.
5. Klicken Sie auf **Apply Changes**. Die ausgewählten statischen Adressen werden gelöscht und das Gerät aktualisiert.

Konfigurieren von Parametern statischer Adressen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zur Konfiguration der Parameter statischer Adressen zusammengefasst, die auf der Seite **Add Static MAC Address** angezeigt werden.

CLI-Befehl	Beschreibung

bridge address *MAC-Adresse* **{ethernet** *Schnittstelle* **| port-channel** *Anschlusskanalnummer***} [permanent | delete-on-reset | delete-on-timeout| secure]**	Fügt der Bridge-Tabelle die statische Quelladresse einer Station auf MAC-Schicht hinzu.
show bridge address-table static [vlan *VLAN***] [ethernet** *Schnittstelle* **| port-channel** *Anschlusskanalnummer***]**	Zeigt Klassen von Einträgen an, die statisch in die Datenbank für die Bridge-Weiterleitung eingegeben wurden.

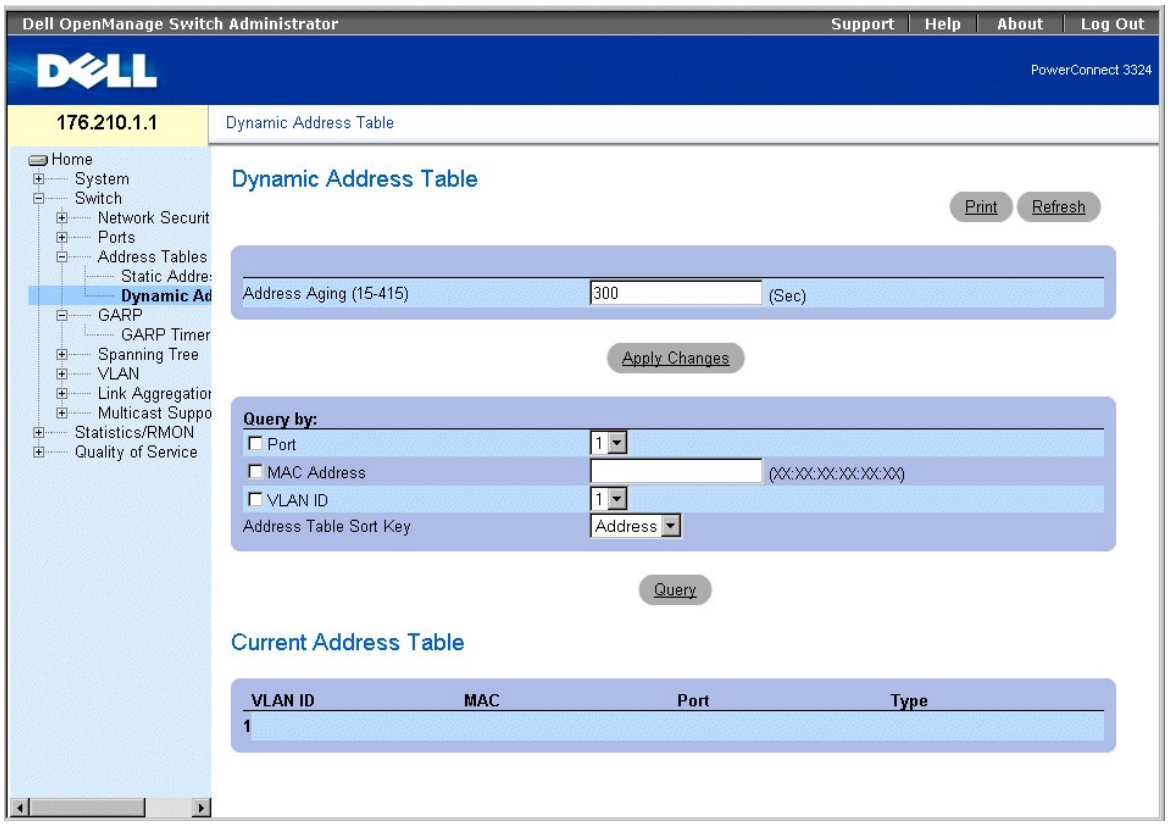
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config-vlan)# bridge address 168.210.0.10 ethernet 1/e8 permanent

Console# show bridge address table static

Aging time is 300 sec

vlan mac address port type

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

200 0010.0D48.37FF 5/9 delete-on-reset
```

Anzeigen dynamischer Adressen

Die Seite **Dynamic Address** enthält Informationen für die Abfrage der **Dynamic Address Table**, einschließlich des Schnittstellentyps, der MAC-Adressen, des VLANs und der Tabellensortierung. Pakete, die an eine in der Adresstabelle gespeicherte Adresse weitergeleitet werden, werden direkt an diese Anschlüsse gesendet. So öffnen Sie die **Dynamic Address Table**:

- Klicken Sie in der **Strukturansicht** auf **Switch > Address Tables > Dynamic Address.** Die Seite **Dynamic Address Table** wird geöffnet.



Seite "Dynamic Address Table"

Die Seite **Dynamic Address** enthält folgende Felder:

- **Address Aging** - Legt die Zeitdauer fest, die die MAC-Adresse bis zum Erreichen des Zeitlimits in der **Dynamic Address Table** verbleibt, falls keine Daten von der Quelle erfasst werden. Der Standardwert lautet 300 Sekunden.
- **Port** - Legt die Nummern der Anschlüsse fest, für welche die Tabelle abgefragt wird.
- **MAC Address** - Legt die MAC-Adresse fest, für die die Tabelle abgefragt wird.
- **VLAN ID** - Gibt die VLAN-ID an, für die die Tabelle abgefragt wird.
- **Address Table Sort Key** - Legt die Methode fest, nach der die Dynamic Address Table sortiert wird. Folgende Feldwerte können ausgewählt werden:
  - **Address** - Sortiert die Abfrageergebnisse für eine designierte MAC-Adresse.
  - **VLAN** - Sortiert die Abfrageergebnisse nach VLAN-ID.
  - **Interface** - Sortiert die Abfrageergebnisse nach Schnittstelle und zeigt alle MAC-Adressen an, die auf dem designierten Anschluss erfasst wurden.

Die **Query Results Table** enthält folgende Spalten:

- **VLAN ID** - Gibt den Wert der VLAN-Kennung an.
- **MAC** - Gibt die MAC-Adresse an.
- **Port** - Gibt den mit der dynamischen MAC-Adresse verknüpften Anschluss an.
- **Type** - Gibt den Typ der MAC-Adresse an.

Neudefinieren der Speicherdauer:

1. Öffnen Sie die **Dynamic Address Table**.
2. Definieren Sie das Feld **Aging Time**.
3. Klicken Sie auf **Apply Changes**. Die Speicherdauer wird geändert und das Gerät aktualisiert.

Abfragen der Dynamic Address Table:

1. Öffnen Sie die **Dynamic Address Table**.
2. Definieren Sie die Parameter, nach denen die **Dynamic Address Table** abgefragt wird. Die Einträge der **Dynamic Address Table** können nach Schnittstelle, MAC-Adresse oder VLAN abgefragt werden.
3. Klicken Sie auf **Query**. Die **Dynamic Address Table** wird abgefragt. Die Abfrageergebnisse werden nach dem im Feld **Address Table Sort Key** ausgewählten Wert sortiert.

Abfragen und Sortieren von dynamischen Adressen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Abfrage und Sortierung dynamischer Adressen zusammengefasst, die auf der Seite **Dynamic Address Table** angezeigt werden.

CLI-Befehl	Beschreibung
bridge aging-time *Sekunden*	Legt die Speicherdauer der Adresstabelle fest.
show bridge address-table [vlan *VLAN*] **[ethernet** *Schnittstelle* **| port-channel** *Anschlusskanalnummer*]	Zeigt Klassen dynamisch erstellter Einträge in der Datenbank für die Bridge-Weiterleitung an.

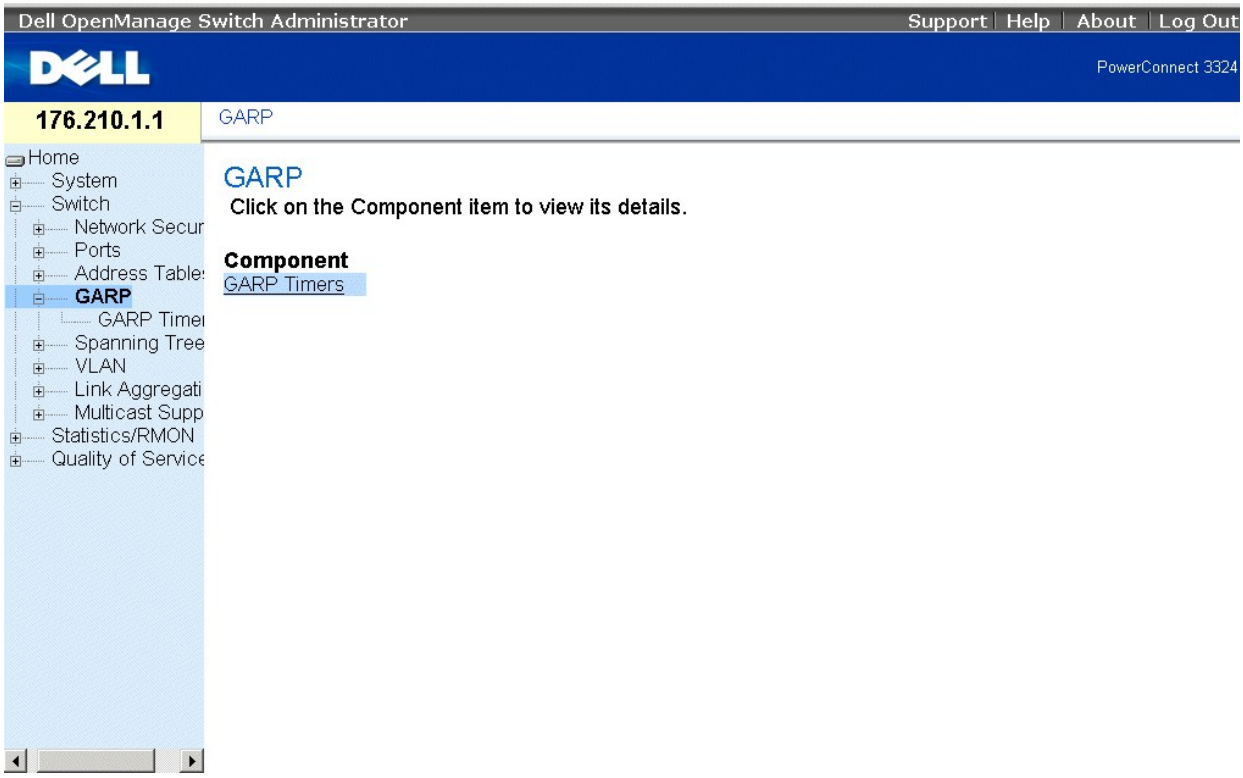
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# bridge aging-time 250

Console (config)# exit

Console# show bridge address table


Aging time is 250 sec


vlan mac address port type

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

1 0060.704C.73FF 5/e8 dynamic

1 0060.708C.73FF 5/e8 dynamic

200 0010.0D48.37FF 5/e9 static
```

Konfigurieren von GARP

Das Generic Attribute Registration Protocol (GARP) ist ein Universalprotokoll, durch das beliebige Informationen zur Netzwerkkonnektivität und zum Mitgliedschaftstyp registriert werden. Das GARP definiert eine Gruppe von Geräten, die gemeinsam an einem bestimmten Netzwerkattribut interessiert sind, beispielsweise an einer VLAN- oder Multicastadresse. So öffnen Sie die Seite **GARP**:

- Klicken Sie in der Strukturansicht auf **Switch > GARP.** Die Seite **GARP** wird geöffnet.



Seite "GARP"

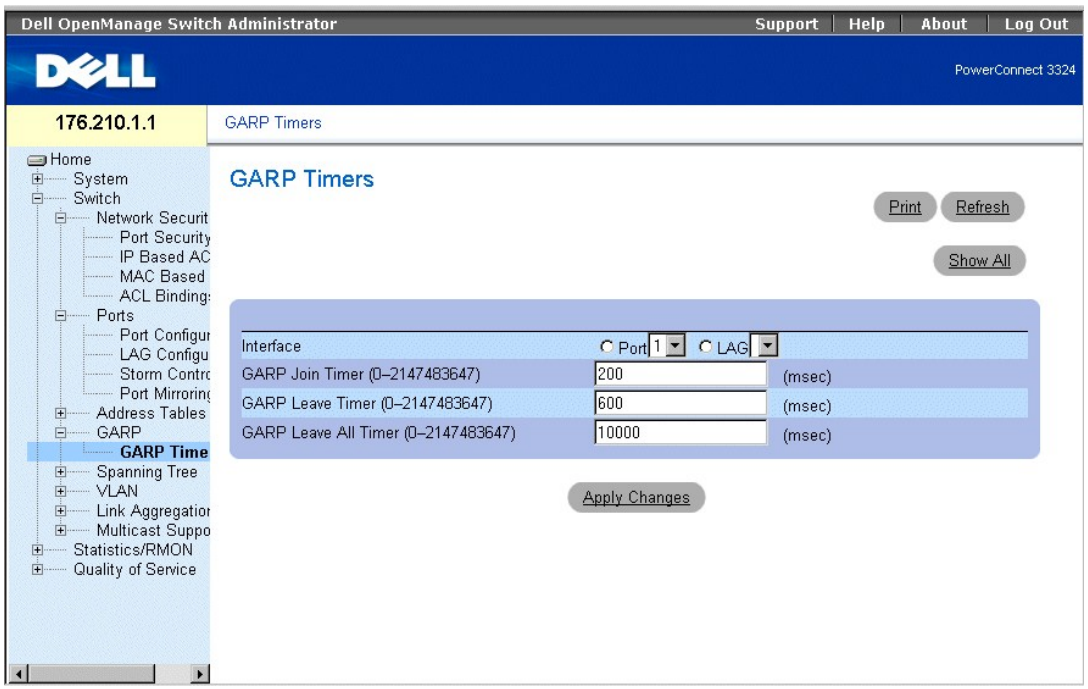
Dieser Abschnitt enthält das folgende Thema:

- Definieren von GARP-Timern

Definieren von GARP-Timern

Die Seite **GARP Timers** enthält Parameter zur GARP-Aktivierung für das Gerät. So öffnen Sie die Seite **GARP Timers**:

- Klicken Sie in der Strukturansicht auf **Switch > GARP > GARP Timers.** Die Seite **GARP Timers** wird geöffnet.



Seite "GARP Timers"

Die Seite **GARP Timers** enthält folgende Felder:

- **Interface** - Gibt den Schnittstellentyp an, für den GARP-Timer angezeigt werden. Folgende Feldwerte können ausgewählt werden:
  - **Port** - Gibt den Anschluss an, für den GARP-Timer angezeigt werden.
  - **LAG** - Gibt die LAG an, für die GARP-Timer angezeigt werden.
- **GARP Join Timer (10-2147483647)** - Gibt die Zeit für die Übertragung von PDUs in Millisekunden an.
- **GARP Leave Timer (10-2147483647)** - 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. Der Standardwert lautet 600 Millisekunden.
- **GARP Leave All Timer (10-2147483647)** - Wird zur Bestätigung des Anschlusses innerhalb des VLANs verwendet. Die zwischen dem Senden von Nachrichten vergangene Zeit in Millisekunden. Der Standardwert lautet 10000 Millisekunden.

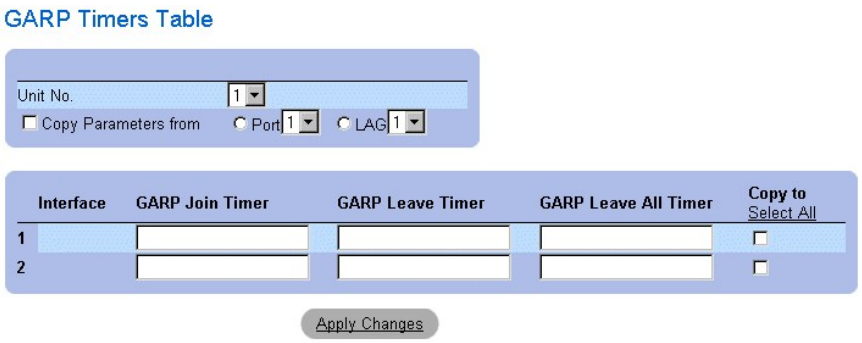
ANMERKUNG: Die folgenden Verhältnismäßigkeiten zwischen den verschiedenen Timer- Werten müssen beibehalten werden: Die Leave-Zeit muss größer oder gleich der dreimaligen Join-Zeit sein. Die Leave-all-Zeit muss größer als die Leave-Zeit sein.

Definieren von GARP-Timern:

1. Öffnen Sie die Seite **GARP Timers**.
2. Definieren Sie **Interface**, **GARP Join Time**, **GARP Leave Timer**, und **GARP Leave All Timer**.
3. Klicken Sie auf **Apply Changes**. Die GARP-Parameter werden auf dem Gerät gespeichert.

Anzeigen der GARP Timers Table:

1. Öffnen Sie die Seite **GARP Timers**.
2. Klicken Sie auf **Show All**. Die **GARP Timers Table** wird geöffnet.



GARP Timers Table

Zusätzlich zu den Feldern auf der Seite **GARP Timers** werden auf der Seite **GARP Timers Table** die folgenden Felder angezeigt:

- **Unit No.** - Gibt die Nummer der Stack-Einheit an.
- **Copy From** - Kopiert die GVRP-Anschlussparameter auf die im Feld **Copy to** angegebenen Schnittstellen.
- **Copy To** - Gibt die Schnittstellen an, auf die die GVRP-Timer kopiert werden.

Kopieren von GARP-Informationen:

1. Öffnen Sie die Seite **GARP Timers**.
2. Klicken Sie auf **Show All**. Die **GARP Timers Table** wird geöffnet.
3. Wählen Sie eine Schnittstelle im Feld **Copy Parameters from** aus.
4. Wählen Sie die Schnittstellen, auf die die GARP-Timer-Informationen kopiert werden, in den Feldern **Copy To** aus.

Definieren von GARP-Timern mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Definition von GARP-Timern zusammengefasst, die auf der Seite **GARP Timers** angezeigt werden.

CLI-Befehl	Beschreibung
garp timer {join | leave | leaveall} *Timerwert*	Legt die Join-, Leave- und Leaveall-GARP-Timer-Werte der GARP-Anwendung fest.

Im Folgenden ein Beispiel für die CLI-Befehle:

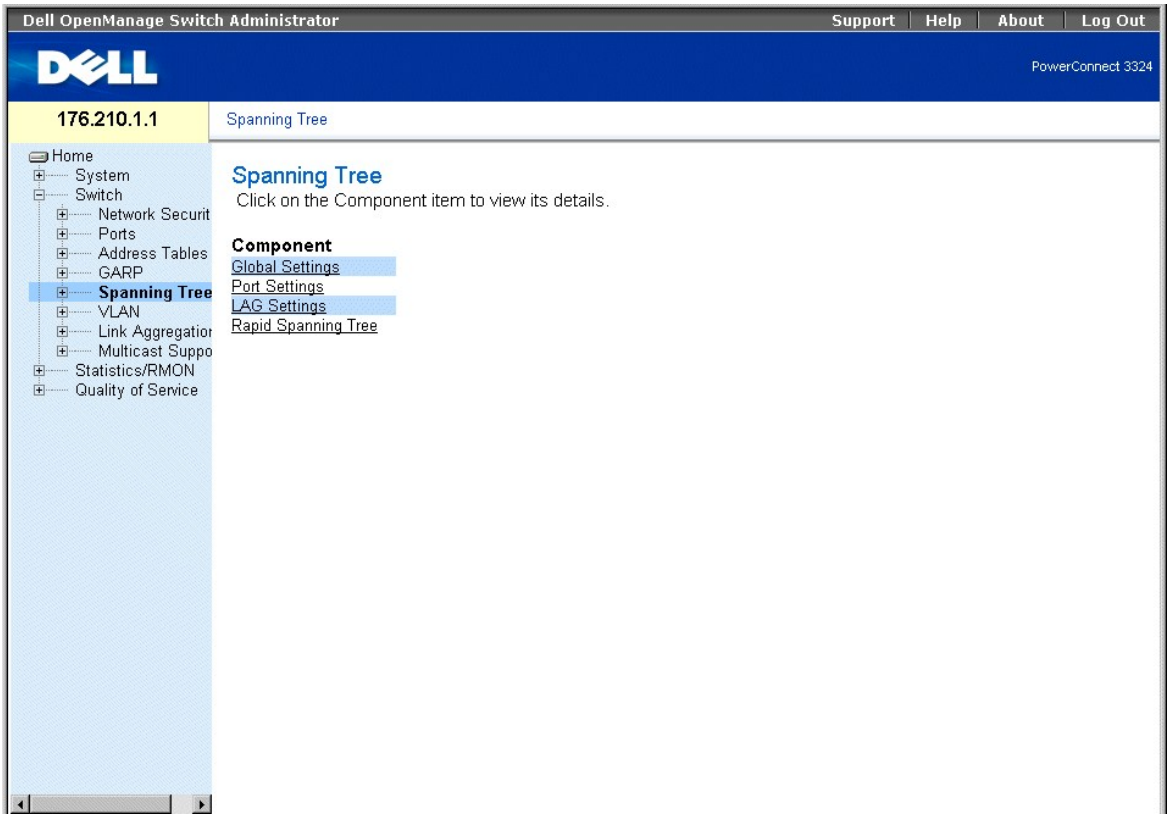
```
Console (config)# interface ethernet 1/e8

Console (config-if)# garp timer leave 900
```

Konfigurieren des Spanning Tree-Protokolls

Das Spanning Tree Protocol (STP) bietet einen einzelnen Pfad zwischen Endstationen in einem Layer 2-Netzwerk und vermeidet dadurch Netzwerkschleifen.

Schleifen treten auf, wenn zwischen Hosts alternative Leitwege existieren. Schleifen in einem erweiterten Netzwerk können dazu führen, dass Datenverkehr über Bridges unbestimmt weitergeleitet wird. Dies führt zu erhöhtem Datenaufkommen und einer Minderung der Netzwerkleistung. So öffnen Sie die Seite **Spanning Tree**:

- Klicken Sie in der Strukturansicht auf **Switch > Spanning Tree**. Die Seite **Spanning Tree** wird geöffnet.



Seite "Spanning Tree"

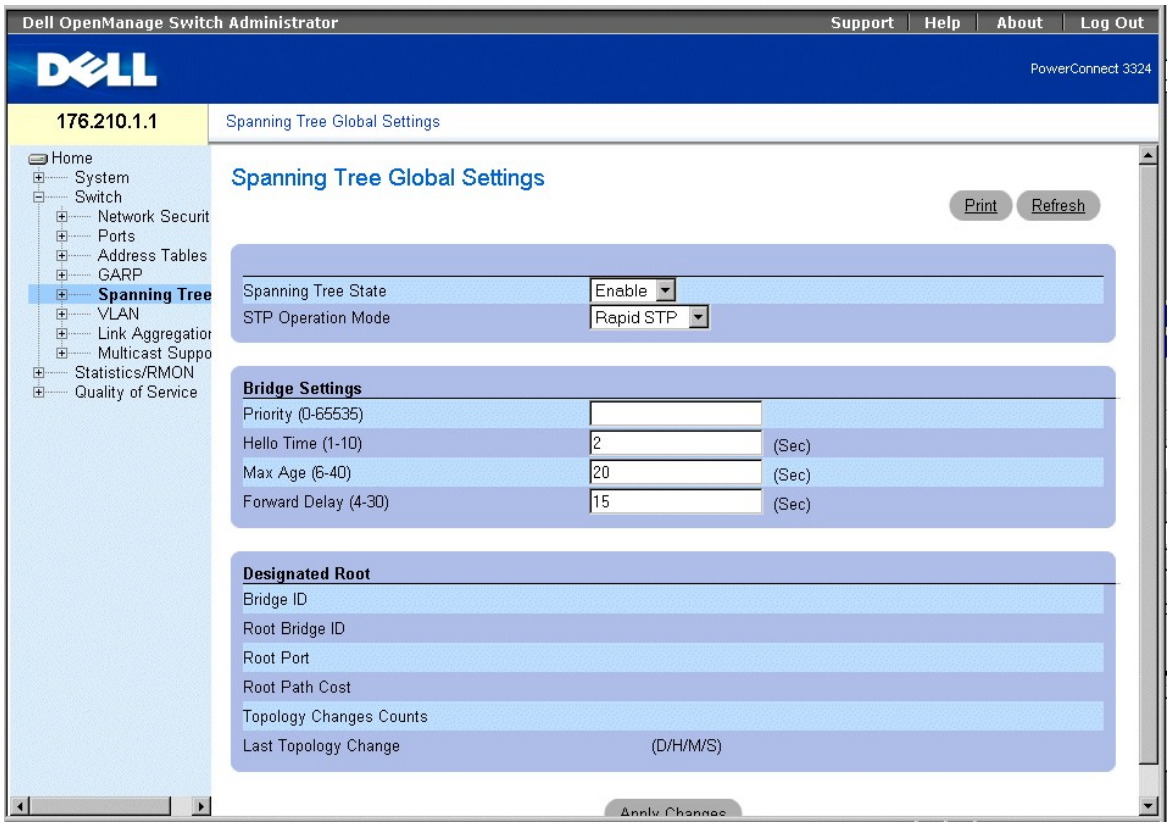
Dieser Abschnitt umfasst die folgenden Themen:

- Definieren globaler STP-Einstellungen
- Definieren von STP-Einstellungen für Anschlüsse
- Definieren von STP-Einstellungen für LAGs
- Konfigurieren von Rapid Spanning Tree

Definieren globaler STP-Einstellungen

Die Seite **Spanning Tree Global Settings** enthält Parameter zur Aktivierung und Konfiguration von STP-Operationen für das Gerät. So öffnen Sie die Seite **Spanning Tree Global Settings**:

- Klicken Sie in der Strukturansicht auf **Switch > Spanning Tree > Global Settings.** Die Seite **Spanning Tree Global Settings** wird geöffnet.



Seite "Spanning Tree Global Settings"

Die Seite **Spanning Tree Global Settings** enthält folgende Felder:

- **Spanning Tree State** - Aktiviert STP für das Gerät. Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Aktiviert STP für das Gerät.
  - **Disable** - Deaktiviert STP für das Gerät.
- **STP Operation Mode** - Gibt den STP-Modus an, nach dem STP für das Gerät aktiviert wird. Folgende Feldwerte können ausgewählt werden:
  - **Classic STP** - Aktiviert klassisches STP für das Gerät (IEEE 802.1D).
  - **Rapid STP** - Aktiviert RSTP für das Gerät (IEEE 802.1w). Weitere Informationen zu Rapid STP finden Sie unter "Konfigurieren von Rapid Spanning Tree".
- **Priority (0-65535)** - Legt den Wert für die Bridge-Priorität fest. Wenn auf Switches oder Bridges STP ausgeführt wird, wird jedem Element eine Priorität zugewiesen. Nach dem Auswechseln der BPDUs wird der Switch mit der niedrigsten Priorität zur Root-Bridge. Der Standardwert lautet 32768. Der Wert für die Anschlusspriorität wird in Einheiten von 16 erhöht, beispielsweise 16, 32, 64, 80 usw.
- **Hello Time (1-10)** - Legt die Hello Time für den Switch fest. Die Hello Time gibt die Dauer in Sekunden an, die eine Root-Bridge zwischen Konfigurationsnachrichten abwartet. Der Standardwert beträgt zwei Sekunden.
- **Max Age (6-40**) - Legt die maximale Speicherdauer für den Switch fest. Die maximale Speicherdauer entspricht der Zeit in Sekunden, die eine Bridge vor dem Senden von Konfigurationsnachrichten wartet. Der Standardwert für die maximale Speicherdauer beträgt 20 Sekunden.
- **Forward Delay (4-30)** - Legt die Weiterleitungsverzögerung für den Switch fest. Die Weiterleitungsverzögerung gibt die Zeit in Sekunden an, die eine Bridge in einem Überwachungs- und Erfassungsstatus verbleibt, bevor Pakete weitergeleitet werden. Der Standardwert beträgt 15 Sekunden.
- **Bridge ID** - Identifiziert die Bridge-Priorität und die MAC-Adresse.
- **Root Bridge ID** - Identifiziert die Root-Bridge-Priorität und die MAC-Adresse.
- **Root Port** - Gibt die Nummer des Anschlusses an, der die niedrigsten Pfadkosten von dieser Bridge zur Root-Bridge bietet. Dies ist von Bedeutung, wenn es sich bei der Bridge nicht um die Root-Bridge handelt. Der Standardwert lautet 0.
- **Root Path Cost** - Die Kosten für den zwischen dieser Bridge und der Root-Bridge verlaufenden Pfad.
- **Topology Changes Counts** - Gibt die Gesamtanzahl der aufgetretenen STP-Statusänderungen an.
- **Last Topology Change** - Gibt die Zeit an, die seit der letzten topographischen Änderung nach Initialisierung oder Zurücksetzung der Bridge verstrichen ist. Die Zeit wird im Format "Tage Stunden Minuten Sekunden" angezeigt, z. B. 2 Tage 5 Stunden 10 Minuten und 4 Sekunden.

Definieren globaler STP-Parameter:

1. Öffnen Sie die Seite **Spanning Tree Global Settings**.
2. Wählen Sie **Enable** im Feld **Spanning Tree State** aus.
3. Wählen Sie die STP-Option **Classic** im Feld **STP Operation Mode** aus.
4. Klicken Sie auf **Apply Changes.** STP wird für das Gerät aktiviert.

Ändern globaler STP-Parameter:

1. Öffnen Sie die Seite **Spanning Tree Global Settings**.
2. Definieren Sie die Felder **STP Operation Mode**, **Bridge Priority**, **Hello Time (Sec)**, **Max Age (Sec)** und **Forward Delay (Sec)**.
3. Klicken Sie auf **Apply Changes**. Die STP-Parameter werden geändert und das Gerät aktualisiert.

Definieren globaler STP-Parameter mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Definition globaler STP-Parameter zusammengefasst, die auf der Seite **Spanning Tree Global Settings** angezeigt werden.

CLI-Befehl	Beschreibung
spanning-tree	Aktiviert die Spanning Tree-Funktion.
spanning-tree mode {stp | rstp}	Konfiguriert das derzeit ausgeführte Spanning Tree-Protokoll.
spanning-tree priority *Priorität*	Konfiguriert die Spanning Tree-Priorität.
spanning-tree hello-time *Sekunden*	Konfiguriert die Hello Time der Spanning Tree-Bridge, die angibt, wie häufig der Switch Hello-Nachrichten an andere Switches sendet.
spanning-tree max-age *Sekunden*	Konfiguriert die maximale Speicherdauer für die Spanning Tree-Bridge, die angibt, wie lange auf einem Anschluss eingegangene Protokollinformationen vom Switch gespeichert werden.
spanning-tree forward-time Sekunden	Konfiguriert die Weiterleitungszeit für die Spanning Tree-Bridge. Diese entspricht der Dauer, die ein Anschluss vor Aktivierung des Weiterleitungsstatus im Überwachungs- und Erfassungsstatus verbleibt.
show spanning-tree [ethernet *Schnittstelle* **| port-channel** *Anschlusskanalnummer***]**	Zeigt die Spanning Tree-Konfiguration an.

Im Folgenden ein Beispiel für die CLI-Befehle:

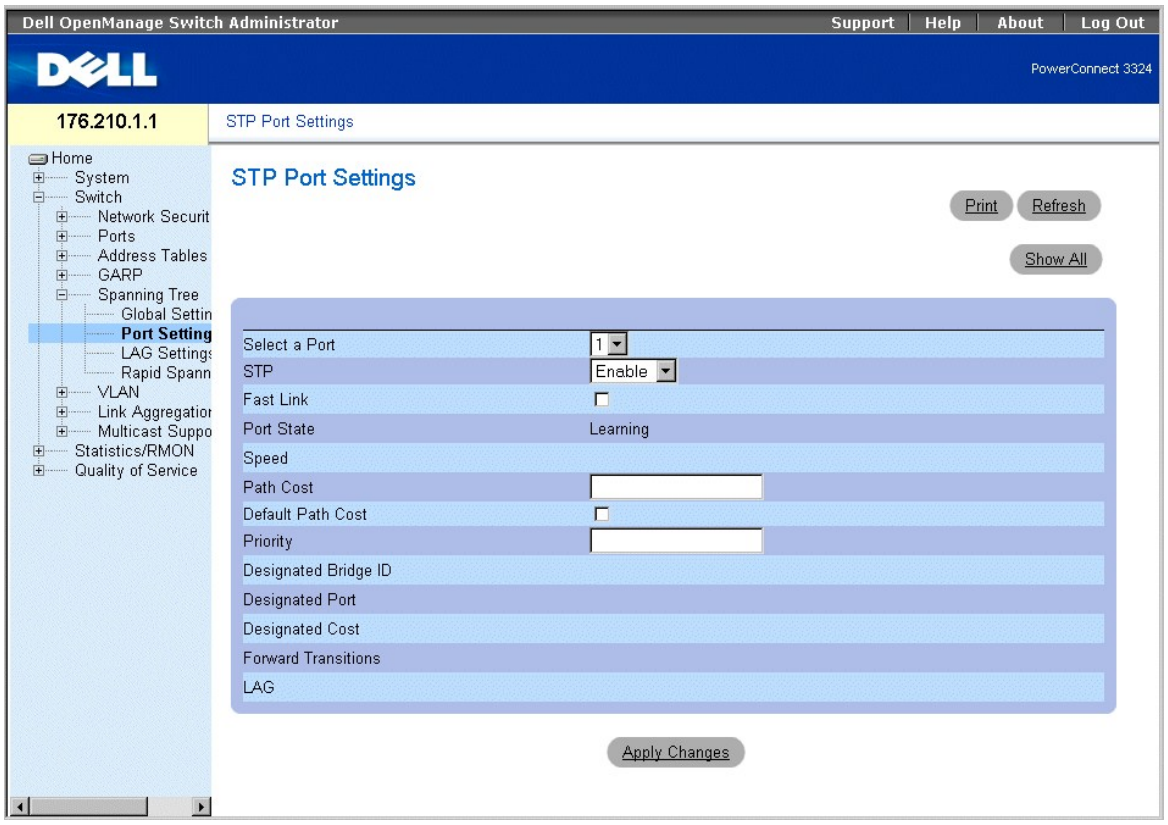
```
Console(config)# spanning-tree

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 X.X.X.X.X.X

Cost 57

Port 1/e1

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769

Address X.X.X.X.X.X

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Number of topology changes 2 last change occurred 00:23:56 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 Cost Sts Cost Bridge ID Prio.Nbr

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

1/e1 128 19 FWD 38 8000 00:30:94:41:62c1 80 001

1/e2 128 19 FWD 57 8000 00:02:4b:29:7a:00 80 002

ch1 128 19 FWD 57 8000 00:02:4b:29:7a:00 80 003
```

Definieren von STP-Einstellungen für Anschlüsse

Auf der Seite **STP Port Settings** können Netzwerkverwalter einzelnen Anschlüssen STP-Eigenschaften zuweisen. So öffnen Sie die Seite **STP Port Settings**:

- Klicken Sie in der Strukturansicht auf **Switch > Spanning Tree > Port Settings.** Die Seite **STP Port Settings** wird geöffnet.



Seite "STP Port Settings"

Die Seite **STP Port Settings** enthält folgende Felder:

- **Select a Port** - Gibt den Anschluss an, für den STP-Statistikwerte angezeigt werden.
- **STP** - Aktiviert STP für den Anschluss. Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Aktiviert STP für den Anschluss.
  - **Disable** - Deaktiviert STP für den Anschluss.
- **Fast Link** - Aktiviert den Fast Link-Modus für den Anschluss. Falls der Fast Link-Modus für einen Anschluss aktiviert ist, wird der Anschluss automatisch in den **Weiterleitungsstatus** versetzt, sobald die Anschlussverbindung 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** - Gibt den aktuellen STP-Status eines Anschlusses an. Falls aktiviert, wird durch Port State die Weiterleitungsaktion für den Datenverkehr bestimmt. Folgende Feldwerte sind möglich:
  - **Disabled** - Zeigt an, dass die Anschlussverbindung derzeit inaktiv ist.
  - **Blocking** - Der Anschluss ist derzeit blockiert und kann nicht für die Weiterleitung von Datenverkehr oder die Erfassung von MAC-Adressen verwendet werden.
  - **Listening** - Der Anschluss befindet sich derzeit im Überwachungsmodus. Der Anschluss kann weder Datenverkehr weiterleiten noch MAC-Adressen erfassen.
  - **Learning** - Der Anschluss befindet sich derzeit im Erfassungsmodus. Der Anschluss kann zwar keinen Datenverkehr weiterleiten, jedoch neue MAC-Adressen erfassen.
  - **Forwarding** - Der Anschluss befindet sich derzeit im Weiterleitungsmodus. Der Anschluss kann Datenverkehr weiterleiten und neue MAC-Adressen erfassen.
- **Speed** - Gibt die Anschlussgeschwindigkeit an. Folgende Feldwerte können ausgewählt werden:
  - **10M**
  - **100M**
  - **1000M**
- Path Cost - Gibt an, welchen Anteil dieser Anschluss an den Root-Pfadkosten hat. Die Pfadkosten können an einen höheren oder niedrigeren Wert angepasst werden. Außerdem kann der Datenverkehr umgeleitet werden, indem er zu einem Pfad hin oder von ihm weg geleitet wird. Die Pfadkosten können einen Wert zwischen 1 und 65.535 haben.
- **Default Path Cost** - Gibt die Standardpfadkosten an.
- **Priority** - Gibt den Prioritätswert des Anschlusses an. Durch den Prioritätswert kann Einfluss auf die Anschlussauswahl genommen werden, wenn eine Bridge über zwei Anschlüsse verfügt, die sich im selben LAN in einer Schleifenkonfiguration befinden. Der Prioritätswert liegt zwischen 0 und 255.

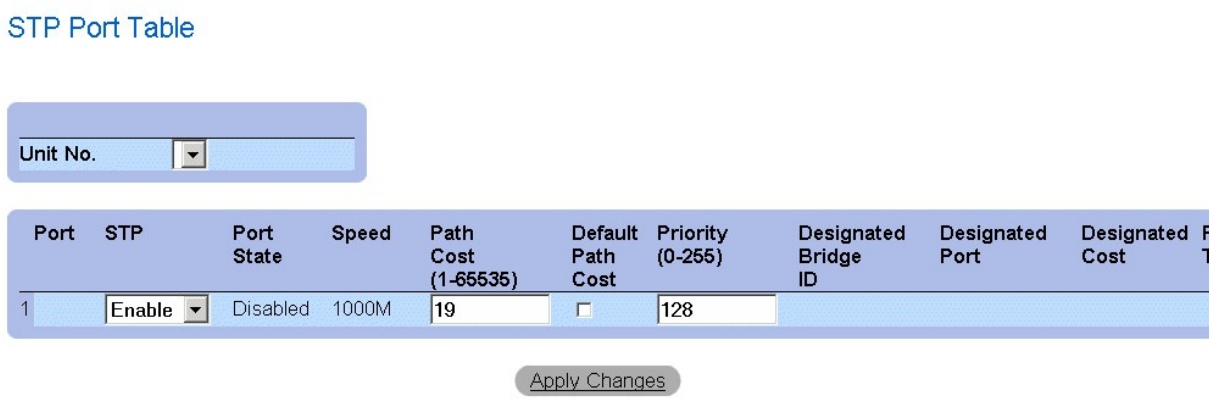
- **Designated Bridge ID** - Gibt die Priorität und die MAC-Adresse der designierten Bridge an.
- **Designated Port** - Gibt die Priorität und die MAC-Adresse für den ausgewählten Anschluss der designierten Bridge an.
- **Designated Cost** - Gibt die Kosten des designierten Anschlusses an, der Bestandteil der STP-Topologie ist.
- **Forward Transitions** - Gibt an, wie häufig der Anschluss vom **Blockierungs**- in den **Weiterleitungsstatus** gewechselt hat.
- **LAG** - Gibt die LAG an, mit der der Anschluss verknüpft ist.

Aktivieren von STP für einen Anschluss:

1. Öffnen Sie die Seite **STP Port Settings.**
2. Wählen Sie **Enabled** im STP -Feld.
3. Definieren Sie die Felder **Priority**, **Path Cost**, **Default Path Cost** und **Fast Link**.
4. Klicken Sie auf **Apply Changes.** STP wird für den Anschluss aktiviert.

Ändern der STP-Eigenschaften für Anschlüsse:

1. Öffnen Sie die Seite **STP Port Settings.**
2. Bearbeiten Sie die Felder **Priority**, **Path Cost**, **Default Path Cost** und **Fast Link**.
3. Klicken Sie auf **Apply Changes**. Die STP-Anschlussparameter werden geändert und das Gerät aktualisiert.



Seite "STP Port Table"

Definieren von STP-Anschlussparametern mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Definition von STP-Anschlussparametern zusammengefasst, die auf der Seite **STP Port Settings** angezeigt werden.

CLI-Befehl	Beschreibung
spanning-tree disable	Deaktiviert Spanning Tree für einen spezifischen Anschluss.
spanning-tree cost *Kosten*	Konfiguriert die Spanning Tree-Anschlusskosten für einen Anschluss.
spanning-tree port-priority Priorität	Konfiguriert die Anschlusspriorität.
show spanning-tree [ethernet *Schnittstelle* **| port-channel** *Anschlusskanalnummer***]**	Zeigt die Spanning Tree-Konfiguration an.
spanning-tree portfast	Aktiviert den PortFast-Modus.

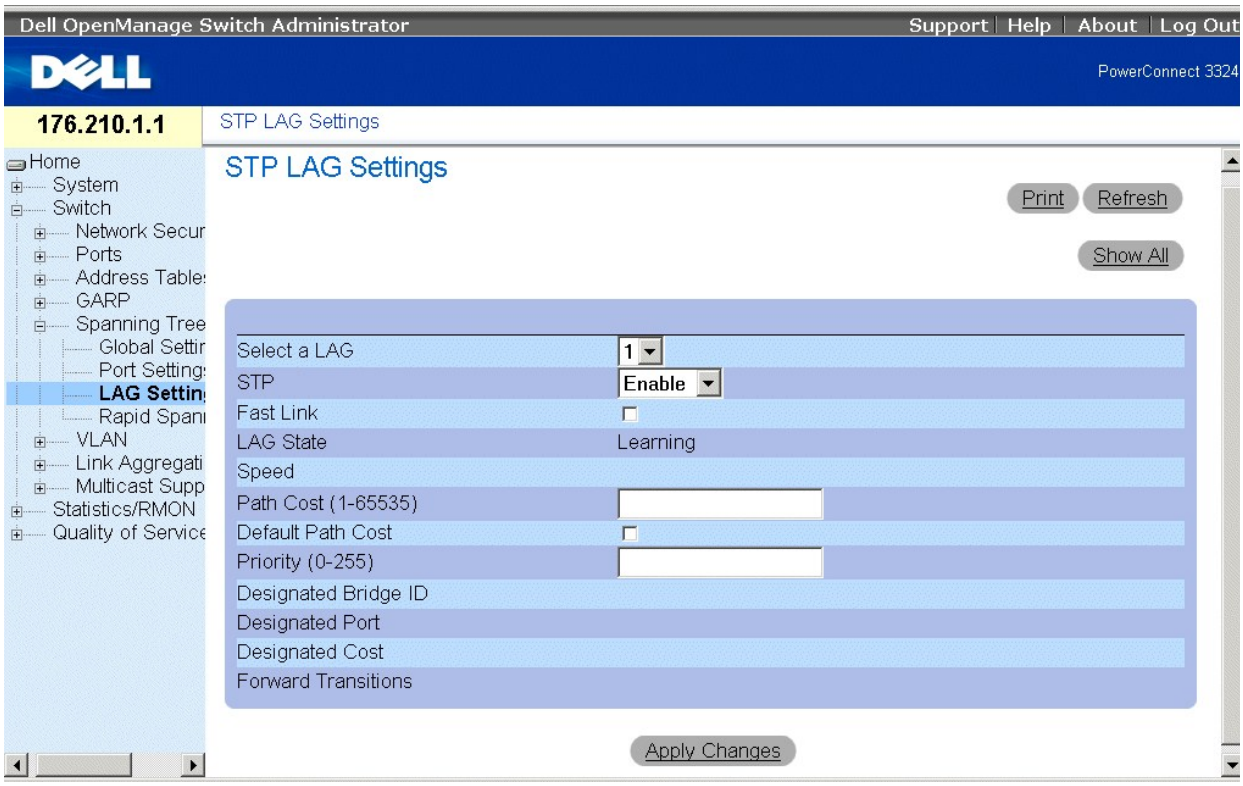
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console(config)# interface ethernet 1/e5

Console(config-if)# spanning-tree disable

Console(config-if)# spanning-tree cost 35000

Console(config-if)# spanning-tree port-priority 96

Console (config-if)# exit

Console (config)# exit

Console# show spanning-tree ethernet 1/e5

Console# show spanning-tree ethernet 1/e5

Interface Port ID Designated Port ID

Name Prio Sts Enb Cost Cost Bridge ID Prio.Nbr

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

1/e5 128 DSBL True 100 0 8000 xx.xx.xx.xx.xx.xx 80 001

Spanning tree enabled

Port Fast: no (configured: no)

Type: point-to-point (configured: auto)

Number of transitions to forwarding state: 1

BPDU: sent 2, received 120638
```

Definieren von STP-Einstellungen für LAGs

Auf der Seite **STP LAG Settings** können Netzwerkverwalter STP-Parameter für LAGs zuweisen. So öffnen Sie die Seite **STP LAG Settings** :

- Klicken Sie in der Strukturansicht auf **Switch > Spanning Tree > LAG Settings**. Die Seite **STP LAG Settings** wird geöffnet.



Seite "STP LAG Settings"

Die Seite **STP LAG Settings** enthält folgende Felder:

- **Select a LAG** - Gibt die benutzerdefinierte LAG an. Weitere Informationen zum Definieren von LAGs finden Sie unter "Definieren von LAG-Mitgliedschaften".
- **STP** - Aktiviert STP für die LAG. Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Aktiviert STP für die LAG.
  - **Disable** - Deaktiviert STP für die LAG.
- **Fast Link** - Aktiviert den Fast Link-Modus für die LAG. Falls Fast Link für eine LAG aktiviert ist, wird die LAG automatisch in den **Weiterleitungsstatus** versetzt. Fast Link verkürzt die Zeit, die zur Konvergierung des STP-Protokolls erforderlich ist (die STP-Konvergierung kann in großen Netzwerken 30 bis 60 Sekunden dauern).

ANMERKUNG: Verwenden Sie die Option **Fast Link** nur in geeigneten Fällen, beispielsweise, wenn das Gerät ein Objekt innerhalb der STP-Netzwerktopologie für Endstationen darstellt.

- **LAG State** - Gibt den aktuellen STP-Status für eine LAG an. Falls aktiviert, wird durch LAG State die Weiterleitungsaktion für den Datenverkehr bestimmt. Wenn die Bridge eine fehlerhaft arbeitende LAG identifiziert, wird die LAG in den Status **Disabled** versetzt. Folgende Feldwerte sind möglich:
  - **Disabled** - Die Verbindung ist derzeit inaktiv.
  - **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. Die LAG ist nicht in der Lage, Datenverkehr weiterzuleiten oder MAC-Adressen zu erfassen.
  - **Learning** - Die LAG befindet sich derzeit im Erfassungsmodus. Die LAG kann zwar keinen Datenverkehr weiterleiten, jedoch neue MAC-Adressen erfassen.
  - **Forwarding** - Die LAG befindet sich derzeit im Weiterleitungsmodus. Die LAG kann Datenverkehr weiterleiten und neue MAC-Adressen erfassen.
- **Speed** - Die Geschwindigkeit der zur LAG gehörenden Anschlüsse.
- **Path Cost (1-65535)** - Gibt an, welchen Anteil diese LAG an den Root-Pfadkosten hat. Die Pfadkosten können an einen höheren oder niedrigeren Wert angepasst werden. Außerdem kann der Datenverkehr umgeleitet werden, indem er zu einem Pfad hin oder von ihm weg geleitet wird. Die Pfadkosten können einen Wert zwischen 1 und 65.535 haben.
- **Default Path Cost** - Gibt die Standardpfadkosten an. Der Standardwert für die Pfadkosten einer LAG lautet 4.
- **Priority (0-255)** - Gibt den Prioritätswert der LAG an. Durch den Prioritätswert kann Einfluss auf die LAG-Auswahl genommen werden, wenn eine Bridge über zwei Anschlüsse verfügt, die sich im selben LAN in einer Schleifenkonfiguration befinden. Der Prioritätswert liegt zwischen 0 und 255.
- **Designated Bridge ID** - Gibt die Priorität und die MAC-Adresse der designierten Bridge an.

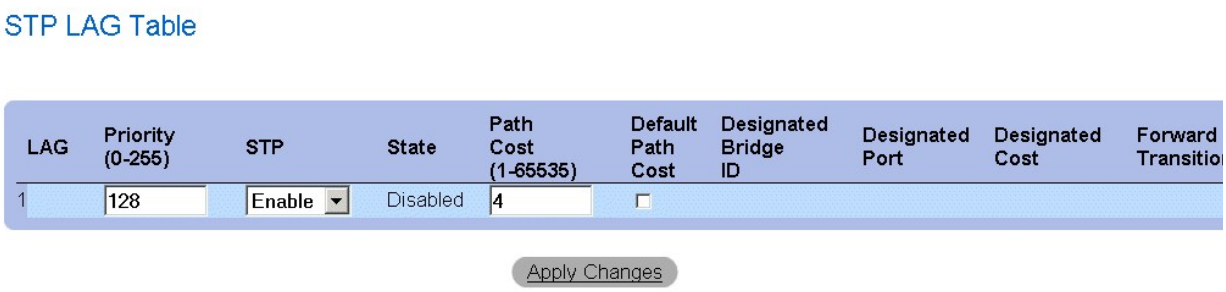
- **Designated Port** - Gibt die Priorität und die MAC-Adresse für den ausgewählten Anschluss an.
- **Designated Cost** - Gibt die designierten Kosten an.
- **Forward Transitions** - Gibt an, wie häufig der Anschluss vom **Blockierungs**- in den **Weiterleitungsstatus** gewechselt hat.

Aktivieren von STP für eine LAG:

1. Öffnen Sie die Seite **STP LAG Settings**.
2. Wählen Sie **Enable** im STP-Field.
3. Definieren Sie die Felder **Priority**, **Path Cost** und **Fast Link**.
4. Klicken Sie auf **Apply Changes**. STP wird für die LAG aktiviert und das Gerät aktualisiert.

Ändern der STP-Parameter für die LAG:

1. Öffnen Sie die Seite **STP LAG Settings**.
2. Bearbeiten Sie die Felder **Priority**, **Path Cost** und **Fast Link**.
3. Klicken Sie auf **Apply Changes**. Die STP-Parameter für die LAG werden geändert und das Gerät aktualisiert.



Seite "STP LAG Table"

Definieren von STP-Parametern für LAGs mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Definition von STP-Parametern für LAGs zusammengefasst, die auf der Seite **STP LAG Settings** angezeigt werden.

CLI-Befehl	Beschreibung
interface port-channel *Anschlusskanalnummer*	Aktiviert den "Port Channel"-Konfigurationsmodus.
spanning-tree port-priority *Priorität*	Konfiguriert die LAG-Priorität.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# interface port-channel 1

console(config-if)# spanning-tree port-priority 16
```

Konfigurieren von Rapid Spanning Tree

Das klassische Spanning Tree verhindert L2-Weiterleitungsschleifen in einer allgemeinen Netzwerktopologie. Die Konvergierung kann jedoch 30 bis 60 Sekunden dauern. Diese Konvergierungszeit gilt für viele Anwendungen als zu lang. Bei entsprechender Unterstützung durch die Netzwerktopologie kann die Konvergierung beschleunigt werden. Das Rapid Spanning Tree Protocol (RSTP) erkennt und verwendet Netzwerktopologien, die eine schnellere Spanning Tree-Konvergierung ohne Bildung von Weiterleitungsschleifen ermöglichen.

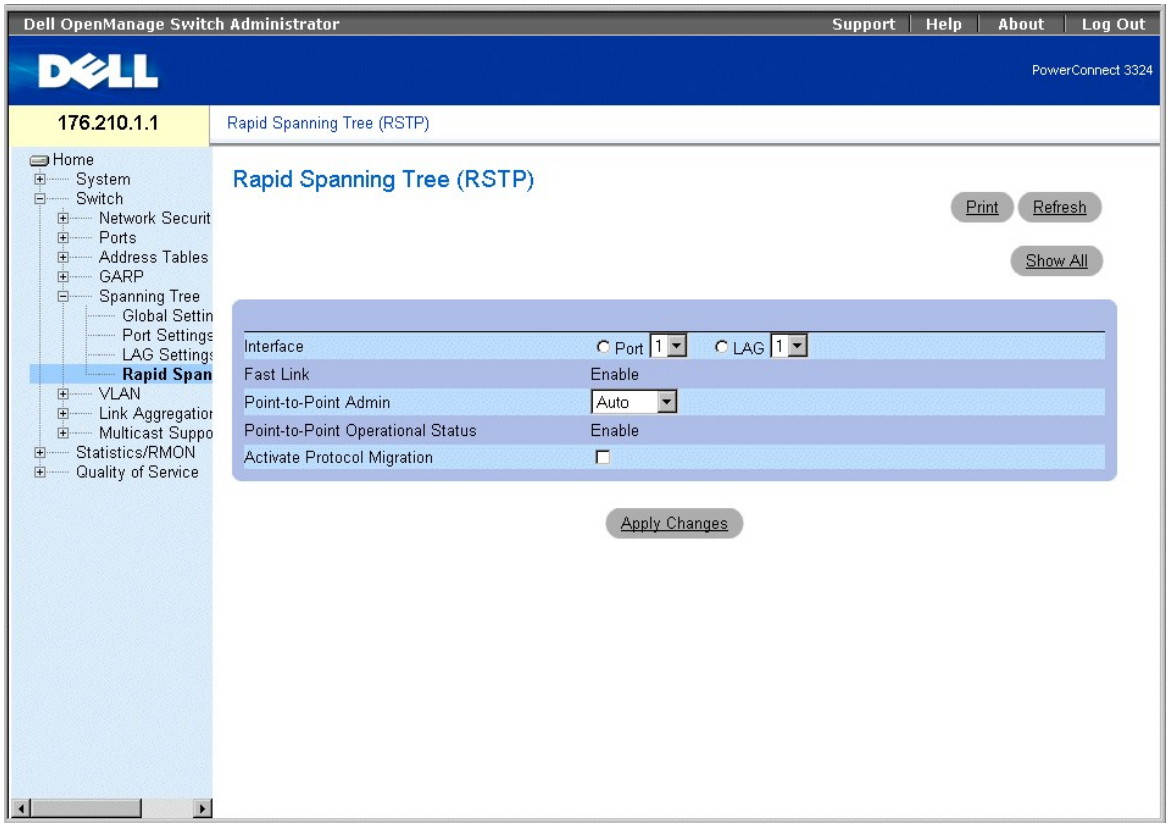
STP verfügt über die folgenden verschiedenen Statuswerte für Anschlüsse:

- Überwachung
- Erfassung
- Blockierung
- Weiterleitung

Bei einem Überwachungsanschluss handelt es sich entweder um einen designierten oder um einen Root-Anschluss, der vor dem Wechsel in den Weiterleitungsstatus steht. Nachdem der Anschluss sich im Weiterleitungsstatus befindet, kann jedoch nicht mehr festgestellt werden, ob es sich um einen designierten oder einen Root-Anschluss handelt. RSTP löst dieses Problem, indem es Funktion und Status des Anschlusses voneinander trennt. Verwenden Sie die Seite **Spanning Tree Global Settings**, um RSTP zu aktivieren.

So öffnen Sie die Seite **Rapid Spanning Tree (RSTP)**:

- Klicken Sie in der Strukturansicht auf **Switch > Spanning Tree > Rapid Spanning Tree.** Die Seite **Rapid Spanning Tree (RSTP)** wird geöffnet.



Seite "Rapid Spanning Tree (RSTP)"

Die Seite **Rapid Spanning Tree (RSTP)** enthält folgende Felder:

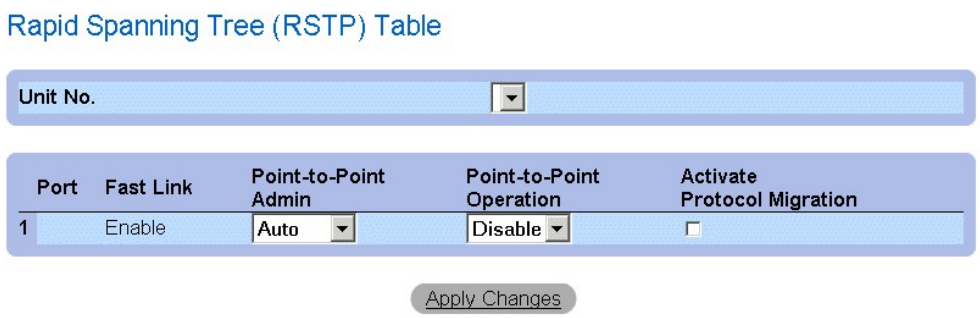
- **Interface** - Gibt die Nummer der Schnittstelle an, für die RSTP aktiviert wird.
- **Fast Link** - Gibt an, ob Fast Link aktiviert ist.

ANMERKUNG: Fast Link wird auf der Seite **STP Port Settings** page oder **STP LAG Settings** aktiviert. Weitere Informationen zur Aktivierung von Fast Link finden Sie unter "Definieren von STP-Einstellungen für Anschlüsse" oder "Definieren von STP-Einstellungen für LAGs".

- **Point-to-Point Admin** - Gibt als Anschlussverbindungstyp "Punkt-zu-Punkt" an. Folgende Feldwerte können ausgewählt werden:
  - **Auto** - Ermöglicht die automatische Erkennung einer "Punkt-zu-Punkt"-Verbindung durch das Gerät.
  - **Enable** - Aktiviert die Einrichtung einer "Punkt-zu-Punkt"-Verbindung.
  - **Disable** - Deaktiviert die Einrichtung einer "Punkt-zu-Punkt"-Verbindung.
- **Point-to-Point Operational Status** - Gibt den "Punkt-zu-Punkt"-Betriebsstatus an.
- **Activate Protocol Migration** - Aktiviert die Protokollmigration. Die Protokollmigration ermöglicht es Protokollen, eine neue Verbindung mit angrenzenden Switches auszuhandeln. Dabei werden die Anschlüsse daraufhin getestet, ob sie die Migration auf RSTP unterstützen. Folgende Feldwerte können ausgewählt werden:
  - **Aktiviert** - Aktiviert die Protokollmigration.
  - **Deaktiviert** - Deaktiviert die Protokollmigration.

Aktivieren von Rapid STP:

1. Öffnen Sie die Seite **Rapid Spanning Tree (RSTP).**
2. Definieren Sie die Felder **Point-to-Point Admin**, **Protocol Operation** und **Activate Protocol Migration**.
3. Klicken Sie auf **Apply Changes**. RSTP wird aktiviert und das Gerät aktualisiert.



Rapid Spanning Tree (RSTP) Table

Definieren von Rapid STP-Parametern mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Definition von RSTP-Parametern zusammengefasst, die auf der Seite **Rapid Spanning Tree (RSTP)** angezeigt werden.

CLI-Befehl	Beschreibung
spanning-tree link-type {point-to-point | shared}	Setzt die durch den Duplexmodus des Anschlusses definierte Einstellung für den Standardverbindungstyp außer Kraft und aktiviert den RSTP-(Rapid Spanning-Tree Protocol-)Wechsel in den Weiterleitungsstatus.
spanning tree mode {stp |rstp}	Konfiguriert das derzeit ausgeführte RSTP.
clear spanning-tree detected-protocols	Startet den Protokollmigrationsprozess neu.
show spanning-tree [ethernet Schnittstelle | port-channel Anschlusskanalnummer]	Zeigt die RSTP-Konfiguration an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console(config)# interface ethernet 1/e5

Console(config-if)# spanning-tree link-type shared
```

Konfigurieren von VLANs

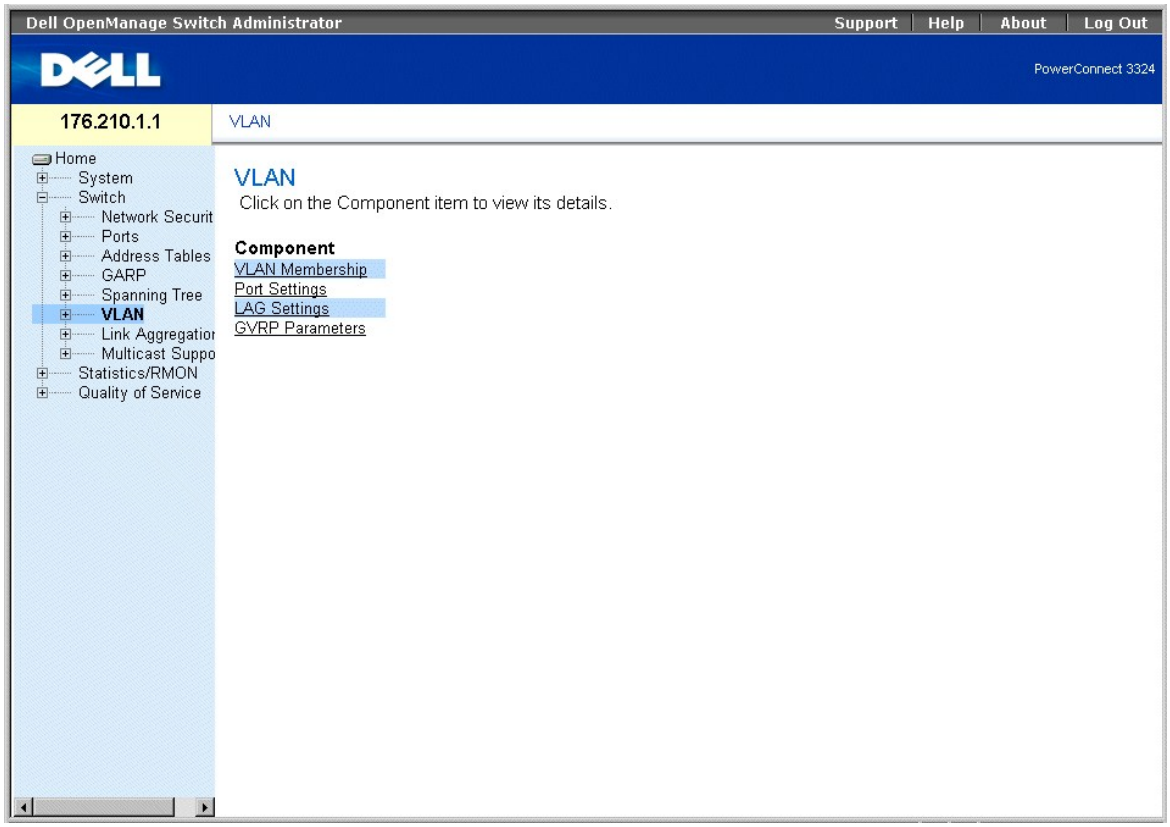
VLANs sind logische Untergruppen eines Local Area Networks (LAN), die softwarebasiert und nicht durch eine Hardwarelösung erstellt werden. In VLANs werden Benutzerstationen und Netzwerkgeräte in einer einzigen Domäne kombiniert, und zwar unabhängig von dem physischen LAN-Segment, mit dem sie verbunden sind. VLANs schaffen die Voraussetzung für einen effizienteren Netzdatenverkehrsfluss durch Untergruppen. Mittels Software verwaltete VLANs verkürzen die Zeit für die Implementierung von Netzwerkänderungen.

VLANs sind softwarebasiert und werden nicht durch physische Attribute definiert. Folglich verfügen VLANs über eine unbegrenzte Anzahl von Anschlüssen und können pro Einheit, pro Gerät, pro Stack bzw. einer anderen logischen Verbindungskombination erstellt werden.

VLANs arbeiten auf Layer 2. Da der Datenverkehr bei VLAN-Verbindungen innerhalb des VLANs isoliert wird, wird ein Layer 3-Router benötigt, um den Datenfluss zwischen VLANs zu ermöglichen. Layer 3-Router dienen zur Identifikation von Segmenten und kooperieren mit VLANs. Bei VLANs handelt es sich um Broadcast- und Multicast-Domänen. Broadcast- und Multicast-Datenverkehr wird nur innerhalb des VLANs übertragen, in dem die Daten generiert werden.

VLAN-Kennungen bieten eine Methode, um VLAN-Informationen zwischen VLAN-Gruppen zu übertragen. Für eine VLAN-Kennung wird eine aus vier Bytes bestehende Datenkennung an den Paketheader angehängt. Die VLAN-Kennung gibt das VLAN an, dem das Paket angehört. VLAN-Kennungen werden entweder von der Endstation oder dem Netzwerkgerät an das Paket angehängt. VLAN-Kennungen enthalten darüber hinaus Informationen zur Priorität von VLAN-Netzwerken. Die Kombination von VLANs und GVRP ermöglicht Netzwerkverwaltern die automatische Verteilung von VLAN-Informationen. So zeigen Sie die Seite **VLAN** an:

- Klicken Sie in der Strukturansicht auf **Switch > VLAN.** Die Seite **VLAN** wird geöffnet.



Seite "VLAN"

Die Seite **VLAN** enthält Links zur Definition folgender Elemente:

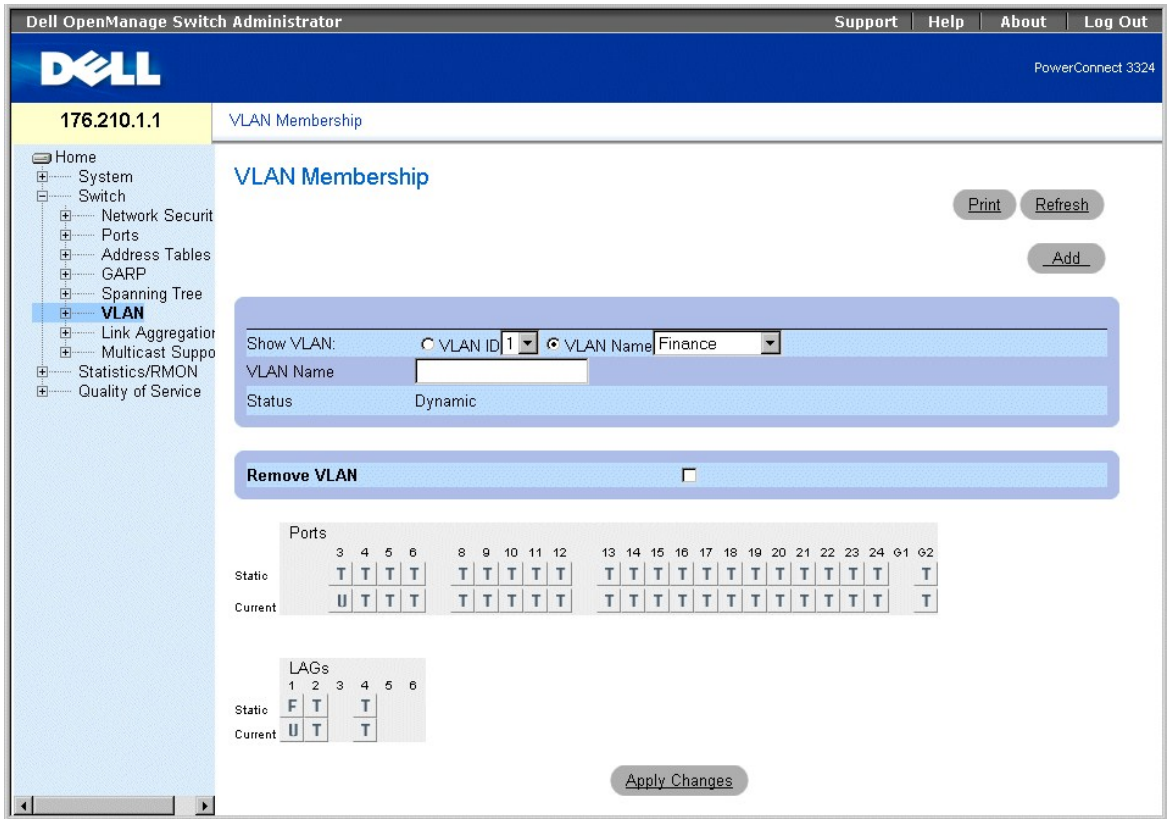
- Definieren von VLAN-Komponenten
- Definieren von VLAN-Einstellungen für Anschlüsse

- Definieren von VLAN-Einstellungen für LAGs
- Konfigurieren von GVRP

Definieren von VLAN-Komponenten

Auf der Seite **VLAN Membership** können Netzwerkverwalter VLAN-Gruppen definieren. So öffnen Sie die Seite **VLAN Membership**:

- Klicken Sie in der Strukturansicht auf **Switch > VLAN > VLAN Membership.** Die Seite **VLAN Membership** wird geöffnet.



Seite "VLAN Membership"

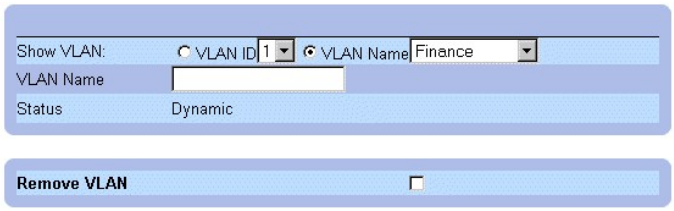
Die Seite **VLAN Membership** ist in folgende Bereiche untergliedert:

- VLAN Membership Section
- VLAN Port Membership Table
- Definieren von VLAN-Einstellungen für LAGs

VLAN Membership Section

Der Abschnitt VLAN Membership enthält Parameter für die Zuweisung von VLAN-Mitgliedschaften zu Anschlüssen. Der PowerConnect 3324/3348 unterstützt bis zu 256 VLANs.

ANMERKUNG: Für alle Anschlüsse muss eine PVID definiert werden. Falls kein anderer Wert konfiguriert wird, verwenden Sie die Standard-PVID des VLANs.



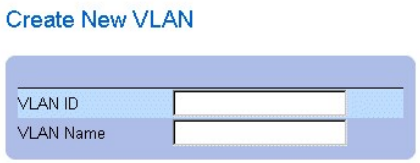
VLAN Membership Section

Der Abschnitt **VLAN Membership** enthält folgende Felder:

- **Show VLAN** - Listet spezifische VLAN-Informationen nach folgenden Kategorien auf und zeigt sie an:
  - **VLAN ID** - Zeigt VLANs nach VLAN-ID an. Die Standard-ID für das VLAN lautet 1. Falls das VLAN über eine ID verfügt, die der Standard-PVID (Port VLAN ID) des aktuellen Anschlusses entspricht und die Anschluss-ID gelöscht wird, wird die PVID des Anschlusses auf 1 gesetzt. VLAN Nummer 1 kann nicht aus dem System gelöscht werden. Der Wertebereich für VLAN-IDs reicht von 1 bis 4095. VLAN 4095 entspricht dem "Discard VLAN".
  - **VLAN Name** - Zeigt VLANs nach ihrem VLAN-Namen an.
- **VLAN Name** - Definiert einen Benutzernamen für das VLAN oder zeigt ihn an.
- **Status** - Gibt den VLAN-Typ an. VLANs sind entweder benutzerdefiniert (permanent), werden mittels GVRP erstellt oder entsprechen Standard-VLANs. Folgende Feldwerte sind möglich:
  - **Dynamic** - Gibt an, dass das VLAN dynamisch über GVRP erstellt wurde.
  - **Static** - Gibt an, dass das VLAN benutzerdefiniert ist.
  - **Default** - Gibt an, dass es sich bei dem VLAN um das Standard-VLAN handelt.
- **Remove** - Entfernt das VLAN aus der **VLAN Membership Table.** Folgende Feldwerte können ausgewählt werden:
  - **Aktiviert** - Entfernt die VLAN-Gruppe aus der VLAN Membership Table.
  - **Deaktiviert** - Behält die VLAN-Gruppe in der VLAN Membership Table bei.

Hinzufügen neuer VLANs:

1. Öffnen Sie die Seite **VLAN Membership**.
2. Klicken Sie auf **Add**. Die Seite **Create New VLAN** wird geöffnet:



Seite "Create New VLAN"

3. Definieren Sie die Felder **VLAN ID** und **VLAN Name**.
4. Klicken Sie auf **Apply Changes.** Das neue VLAN wird hinzugefügt und das Gerät aktualisiert.

Ändern von VLAN-Namensgruppen:

1. Öffnen Sie die Seite **VLAN Membership**.
2. Wählen Sie ein VLAN im Feld **Show VLAN** aus.
3. Bearbeiten Sie das Feld **VLAN Name**.
4. Klicken Sie auf **Apply Changes**. Die VLAN-Mitgliedschaftsinformationen werden geändert und das Gerät aktualisiert.

Löschen eines VLANs:

1. Öffnen Sie die Seite **VLAN Membership**.
2. Wählen Sie ein VLAN im Feld **Show VLAN** aus.
3. Aktivieren Sie das Kontrollkästchen **Remove**.

4. Klicken Sie auf **Apply Changes**. Das VLAN wird gelöscht und das Gerät aktualisiert.

Definieren von VLAN-Mitgliedschaftsgruppen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Definition der VLAN-Mitgliedschaftsgruppen zusammengefasst, die auf der Seite **VLAN Membership** angezeigt werden.

CLI-Befehl	Beschreibung
vlan database	Ruft den Schnittstellenkonfigurations-Modus (VLAN) auf.
vlan {*VLAN-Bereich***}**	Erstellt ein VLAN.
name *Zeichenfolge*	Fügt einem VLAN einen Namen hinzu.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console # vlan database

Console (config-switch)#

Console (config-switch)# vlan 1972

Console (config-switch)# exit

Console (config)# interface vlan 19

Console (config-if)# name Marketing
```

VLAN Port Membership Table

Die **VLAN Port Membership Table** enthält eine Anschlusstabelle für die Zuweisung von Anschlüssen zu VLANs. Um Anschlüssen eine VLAN-Mitgliedschaft zuzuweisen, müssen die Einstellungen für die Anschlusssteuerung geändert werden. Anschlüsse können über die folgenden Werte verfügen:

Steuerungseinstellungen für die VLAN-Mitgliedschaft von Anschlüssen

Anschlusssteuerung	Definition
T	Die Schnittstelle gehört einem VLAN an. Alle über die Schnittstelle weitergeleiteten Pakete verfügen über eine Kennung. Die Pakete enthalten VLAN-Informationen.
U	Die Schnittstelle gehört dieser Komponente an. Über die Schnittstelle weitergeleitete Pakete besitzen keine Kennung.
F	Der Schnittstelle wird über GVRP die Mitgliedschaft in einem VLAN verweigert.
Leer	Die Schnittstelle gehört diesem VLAN nicht an. Mit dem VLAN verknüpfte Pakete werden nicht weitergeleitet.

ANMERKUNG: Anschlüsse, die einer LAG angehören, werden in der VLAN Port Membership Table nicht angezeigt.

In der **VLAN Port Membership Table** werden die Anschlüsse und der Anschlussstatus sowie die LAGs angezeigt.

VLAN Port Membership Table

Zuweisen von Anschlüssen zu einer VLAN-Gruppe:

1. Öffnen Sie die Seite **VLAN Membership**.
2. Wählen Sie ein VLAN aus der Dropdown-Liste **Show VLAN** aus.
3. Wählen Sie Anschlüsse in der **Port Membership Table**, und weisen Sie den Anschlüssen Werte zu (**v**, **t**, **f** oder **b**).
4. Klicken Sie auf **Apply Changes**. Die Anschlüsse werden der VLAN-Gruppe zugewiesen, und das Gerät wird aktualisiert.

Löschen von VLANs:

1. Öffnen Sie die Seite **VLAN Membership**.
2. Wählen Sie ein VLAN aus der Dropdown-Liste **Show VLAN**aus.
3. Aktivieren Sie das Kontrollkästchen **Remove**.
4. Klicken Sie auf **Apply Changes**. Die VLAN-Gruppe wird gelöscht und das Gerät aktualisiert.

Zuweisen von Anschlüssen zu VLAN-Gruppen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Zuweisung von Anschlüssen zu VLAN-Gruppen zusammengefasst, die auf der Seite **VLAN Membership** angezeigt werden.

CLI-Befehl	**Beschreibung**
vlan database	Ruft den Schnittstellenkonfigurations-Modus (VLAN) auf.
vlan {*VLAN-Bereich***}**	Erstellt oder löscht ein VLAN.
interface vlan *VLAN-ID*	Ruft den Schnittstellenkonfigurations-Modus (VLAN) auf, um ein vorhandenes VLAN zu konfigurieren.
name *Zeichenfolge*	Fügt einem VLAN einen Namen hinzu.
interface range ethernet {*Anschlussbereich* **| all}**	Aktiviert die gleichzeitige Befehlsausführung für mehrere Anschlüsse.
switchport forbidden vlan {add vlan-list | remove vlan-list}	Verhindert das Hinzufügen spezifischer VLANs zum Anschluss.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console # vlan database

Console (config-vlan)# vlan 1972
```

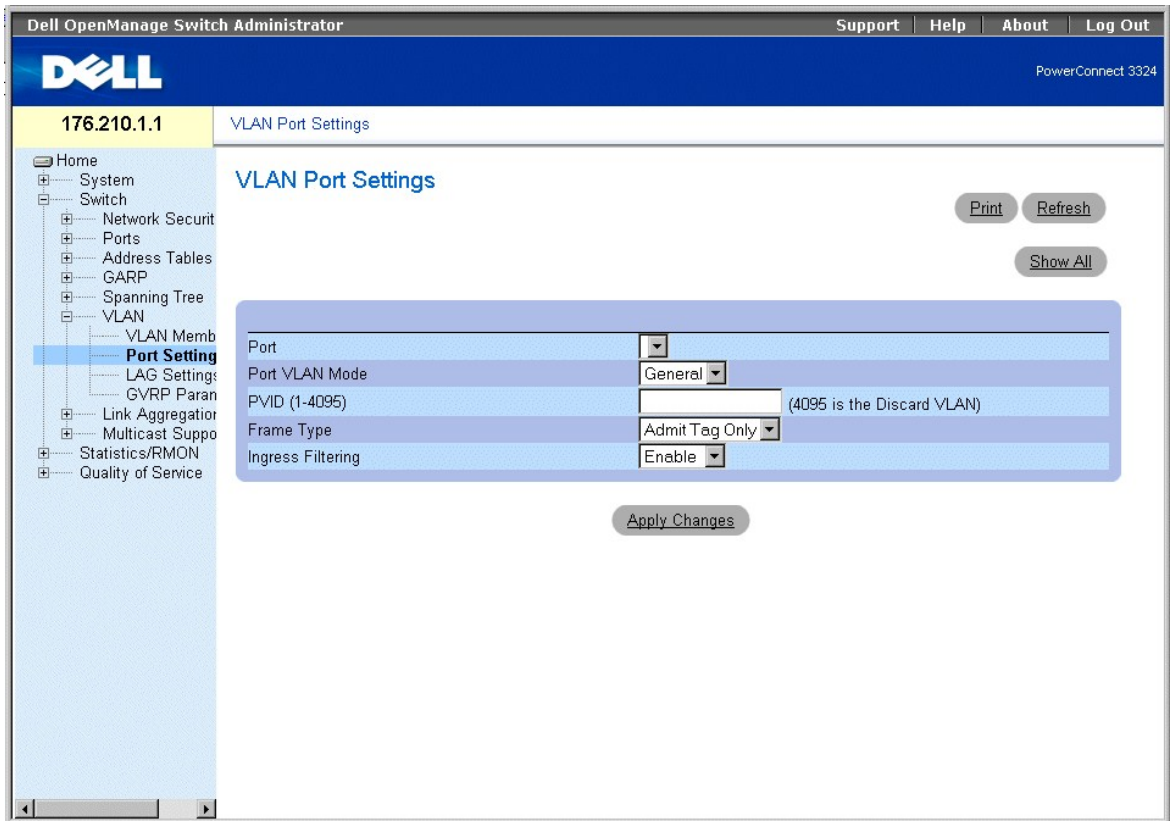
```
Console (config-vlan)# exit

Console (config)# interface vlan 1972

Console (config-if)# name Marketing

Console (config-if)# exit

Console (config)# interface range ethernet 1/e18 - e20
```

Definieren von VLAN-Einstellungen für Anschlüsse

Die Seite **VLAN Port Settings** enthält Parameter für die Verwaltung von Anschlüssen, die Teil eines VLANs sind.

Die **Port Default VLAN ID** (PVID) wird auf der Seite **VLAN Port Settings** konfiguriert. Alle über das Gerät eingehenden Pakete ohne Kennung werden mit der PVID des Anschlusses versehen. So öffnen Sie die Seite **VLAN Port Settings**:

- Klicken Sie in der Strukturansicht auf **Switch > VLAN > Port Settings.** Die Seite **VLAN Port Settings** wird geöffnet.



Seite "VLAN Port Settings"

Die Seite **VLAN Port Settings** enthält folgende Felder:

- **Port** - Gibt die Nummer des im VLAN enthaltenen Anschlusses an.
- **Port VLAN Mode** - Gibt den VLAN-Modus des Anschlusses an. Folgende Feldwerte können ausgewählt werden:
  - **General** - Gibt an, dass der Anschluss einem oder mehreren VLANs angehört und dass jedes VLAN vom Benutzer als VLAN mit oder ohne Kennung definiert wurde (voller 802.1Q-Modus). Die Ingress-Filterung kann nur für Anschlüsse deaktiviert werden, die sich in einem allgemeinen Modus befinden.
  - **Access** - Gibt an, dass der Anschluss zu einem einzelnen VLAN ohne Kennung gehört. Wenn der VLAN-Modus des Anschlusses als Zugriffsmodus definiert wird, impliziert dies, dass die Anschlüsse sowohl alle Frames ohne Kennung akzeptieren als auch solche mit der VID-Kennung, die der derzeitigen PVID des Anschlusses entspricht. Anschlüsse im Zugriffsmodus sind dazu konzipiert, Endstationen mit dem System zu verbinden, insbesondere dann, wenn die Endstationen keine VLAN-Kennungen generieren können. Die Ingress-Filterung ist aktiviert.
  - **Trunk** - Gibt an, dass der Anschluss einem VLAN angehört, in dem alle Frames über eine Kennung verfügen. Die Ingress-Filterung ist für Anschlüsse im Trunk-Modus aktiviert.
- **PVID (1-4095)** - Weist Paketen ohne Kennung eine VLAN-ID zu. Diese Option wird nur für Anschlüsse im allgemeinen Modus implementiert. Als Feldwerte können die Werte 1 bis 4095 festgelegt werden.

ANMERKUNG: Bei VLAN 4095 handelt es sich um das "Discard VLAN".

- **Frame Type** - Gibt den vom Anschluss akzeptierten Pakettyp an. Folgende Feldwerte können ausgewählt werden:
  - **Admit Tag Only** - Gibt an, dass nur Pakete mit Kennung vom Anschluss akzeptiert werden.
  - **Admit All** - Gibt an, dass sowohl Pakete mit als auch ohne Kennung vom Anschluss akzeptiert werden.
- **Ingress Filtering** - Aktiviert die Ingress-Filterung für den Anschluss. Bei der Ingress-Filterung werden Pakete abgelehnt, die mit einem VLAN verknüpft sind, das den Ingress-Anschluss nicht enthält. Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Aktiviert die Ingress-Filterung für den Anschluss.
  - **Disable** - Deaktiviert die Ingress-Filterung für den Anschluss.

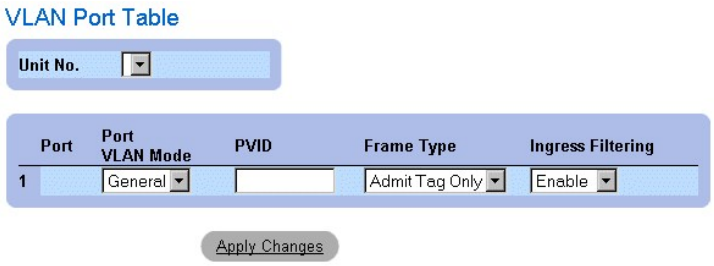
Zuweisen von Anschlusseinstellungen:

ANMERKUNG: Die Ingress-Filterung kann nur für Anschlüsse deaktiviert werden, für die ein allgemeiner VLAN-Modus festgelegt wurde.

1. Öffnen Sie die Seite **VLAN Port Settings**.
2. Definieren Sie die Felder **Port Mode**, **PVID**, **Frame Type** und **Ingress Filtering**.
3. Klicken Sie auf **Apply Changes**. Die VLAN-Anschlussparameter werden definiert und das Gerät aktualisiert.

Anzeigen der VLAN Port Table:

1. Öffnen Sie die Seite **VLAN Port Settings**.
2. Klicken Sie auf **Show All**. Die **VLAN Port Table** wird geöffnet.



VLAN Port Table

Zusätzlich zu den Feldern auf der Seite **VLAN Port Settings** wird auf der Seite **VLAN Port Table** das folgende Feld angezeigt:

- **Unit** - Gibt die Nummer der Stack-Einheit an, für die VLAN-Anschlussinformationen angezeigt werden.

Zuweisen von Anschlüssen zu VLAN-Gruppen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Zuweisung von Anschlüssen zu VLAN-Gruppen zusammengefasst, die auf der Seite **VLAN Port Settings** angezeigt werden.

CLI-Befehl	Beschreibung
interface ethernet *Schnittstelle*	Aktiviert den Schnittstellenkonfigurationsmodus, um eine Ethernet-Schnittstelle zu konfigurieren.
switchport mode {access | trunk | general}	Konfiguriert den VLAN-Mitgliedschaftsmodus für einen Anschluss.
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-Liste* **[tagged | untagged]**	Fügt einem Anschluss im allgemeinen Modus VLANs hinzu.
switchport general allowed vlan remove *VLAN-Liste*	Entfernt VLANs von einem Anschluss im allgemeinen Modus.
switchport general ingress-filtering disable	Deaktiviert die Ingress-Filterung für einen Anschluss.

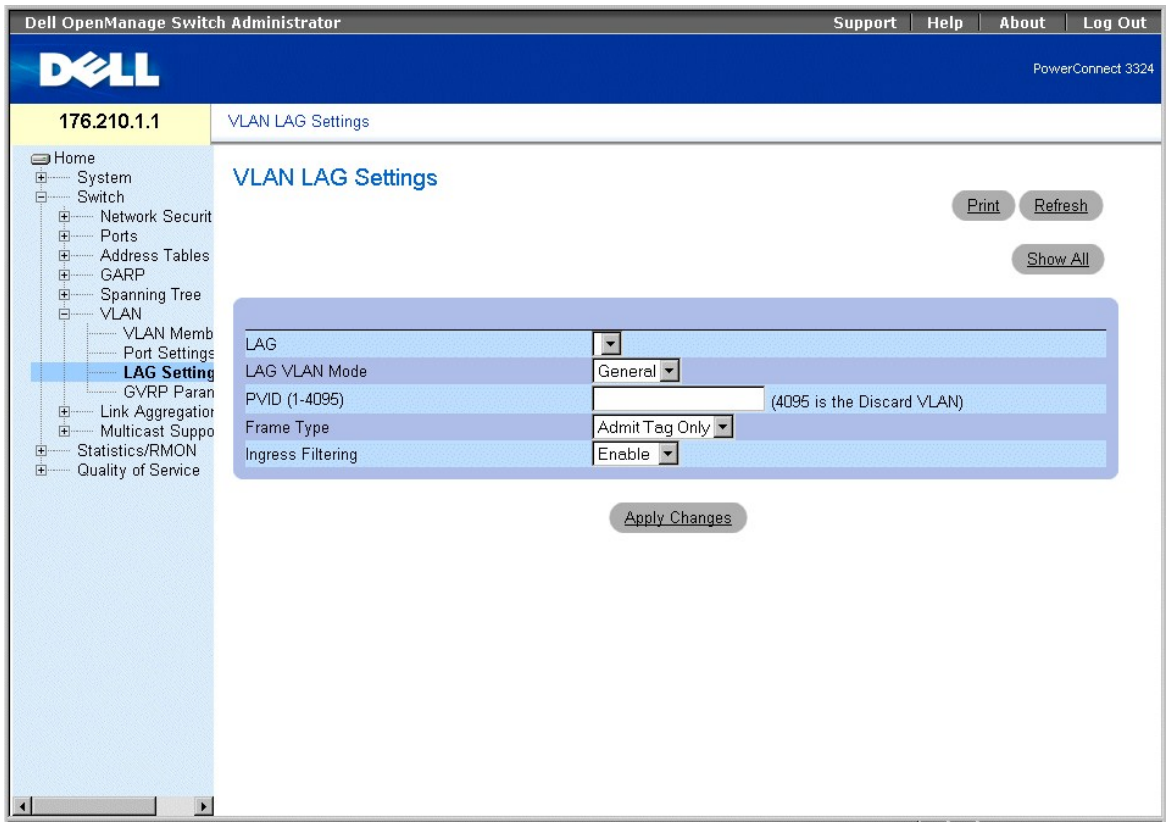
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# interface range ethernet 1/e18 - e20

Console (config-if)# switchport mode access

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 ingress-filtering disable
```

Definieren von VLAN-Einstellungen für LAGs

Die Seite **VLAN LAG Settings** enthält Parameter für die Verwaltung von LAGs, die Teil eines VLANs sind. VLANs setzen sich aus einzelnen Anschlüssen oder LAGs zusammen. Auf dem Switch einer LAG eingehende Pakete ohne Kennung werden mit der PVID-Kennung der LAG versehen. So öffnen Sie die Seite **VLAN LAG Settings**:

- Klicken Sie in der Strukturansicht auf **Switch > VLAN > LAG Settings.** Die Seite **VLAN LAG Settings** wird geöffnet.



Seite "VLAN LAG Settings"

Die Seite **VLAN LACP Parameters** enthält folgende Felder:

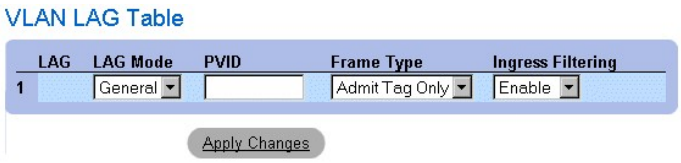
- **LAG** - Gibt die Nummer der im VLAN enthaltenen LAG an.
- **Port Mode** - Gibt den Anschlussmodus an. Folgende Feldwerte können ausgewählt werden:
  - **General** - Gibt an, dass die LAG einem oder mehreren VLANs angehört und dass jedes VLAN vom Benutzer als VLAN mit oder ohne Kennung definiert wird (volle 802.1Q-Konformität).
  - **Access** - Gibt an, dass die LAG einem einzelnen VLAN ohne Kennung angehört.
  - **Trunk** - Gibt an, dass die LAG einem VLAN angehört, in dem alle Frames über eine Kennung verfügen (außer bei optionalen, einzelnen nativen VLANs).
- **PVID** - Weist Paketen ohne Kennung eine VLAN-ID zu. Damit LAGs in der Lage sind, PVIDs zuzuweisen, muss die LAG in der **VLAN Port Membership Table** als LAG ohne Kennung definiert sein.
- **Frame Type** - Gibt den von der LAG akzeptierten Pakettyp an. Folgende Feldwerte können ausgewählt werden:
  - **Admit Tag Only** - Gibt an, dass nur Pakete mit Kennung von der LAG akzeptiert werden.
  - **Admit All** - Gibt an, dass sowohl Pakete mit als auch ohne Kennung von der LAG akzeptiert werden.
- **Ingress Filtering** - Aktiviert die Ingress-Filterung durch die LAG. Durch die Ingress-Filterung werden Pakete abgelehnt, in denen kein Ingress-Anschluss angegeben ist. Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Aktiviert die Ingress-Filterung durch die LAG.
  - **Disable** - Deaktiviert die Ingress-Filterung durch die LAG.

Zuweisen von LAG-Einstellungen:

1. Öffnen Sie die Seite **VLAN LAG Settings**.
2. Definieren Sie die Felder **Port Mode**, **PVID**, **Frame Type** und **Ingress Filtering**.
3. Klicken Sie auf **Apply Changes**. Die VLAN-Parameter für die LAG werden definiert und das Gerät aktualisiert.

Anzeigen der VLAN LAG Table:

1. Öffnen Sie die Seite **VLAN LAG Settings** öffnen.
2. Klicken Sie auf **Show All**. Die **VLAN LAG Table** wird geöffnet.



VLAN LAG Table

Zuweisen von LAGs zu VLAN-Gruppen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Zuweisung von LAGs zu VLAN-Gruppen zusammengefasst, die auf der Seite **VLAN LAG Settings** angezeigt werden.

CLI-Befehl	Beschreibung
switchport mode {access | LAG | general}	Konfiguriert den VLAN-Mitgliedschaftsmodus für einen Anschluss.
switchport LAG native vlan *VLAN-ID*	Definiert die LAG als Komponente des angegebenen VLANs und die VLAN-ID als Standard-PVID (Port VLAN ID).
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-Liste* **[tagged | untagged]**	Fügt einem Anschluss im allgemeinen Modus VLANs hinzu.
switchport general allowed vlan remove *VLAN-Liste* **[tagged | untagged]**	Entfernt VLANs von einem Anschluss im allgemeinen Modus.
switchport general acceptable-frame-types tagged-only	Lehnt Frames ohne Kennung bei der Ingress-Filterung ab.
switchport general ingress-filtering off	Deaktiviert die Ingress-Filterung für einen Anschluss.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# interface port channel 1 1/e8

Console (config-if)# switchport mode access

console (config-if)# switchport LAG 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-types tagged-only

Console (config-if)# switchport general ingress-filtering disable
```

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 Anschlusszuweisungen ohne Konfiguration einzelner Bridges überbrücken sowie die VLAN-Mitgliedschaft registrieren.

Um die Speichervoraussetzungen für die Ausführung von GVRP zu minimieren, wurden den Standardvariablen zwei firmeneigene Abstimmungsvariablen hinzugefügt:

- **Maximum number of GVRP VLANs** - Zeigt die Anzahl der GVRP-VLANs an, die an der GVRP-Operation beteiligt sein dürfen.
- **Maximum number of GVRP VLANs after Reset** - Legt einen anderen Wert für GVRP-VLANs fest und wird zur Optimierung verwendet. Dieser Wert wird erst nach dem Zurücksetzen wirksam.

Die maximale Anzahl von GVRP-VLANs umfasst alle an GVRP-Operationen beteiligten VLANs, die entweder statisch oder dynamisch sein können.

Folgendes ist zu beachten, wenn Sie die maximale Anzahl der an GVRP-Operationen beteiligten VLANs über die Option Maximum number of GVRP VLANs after Reset festlegen:

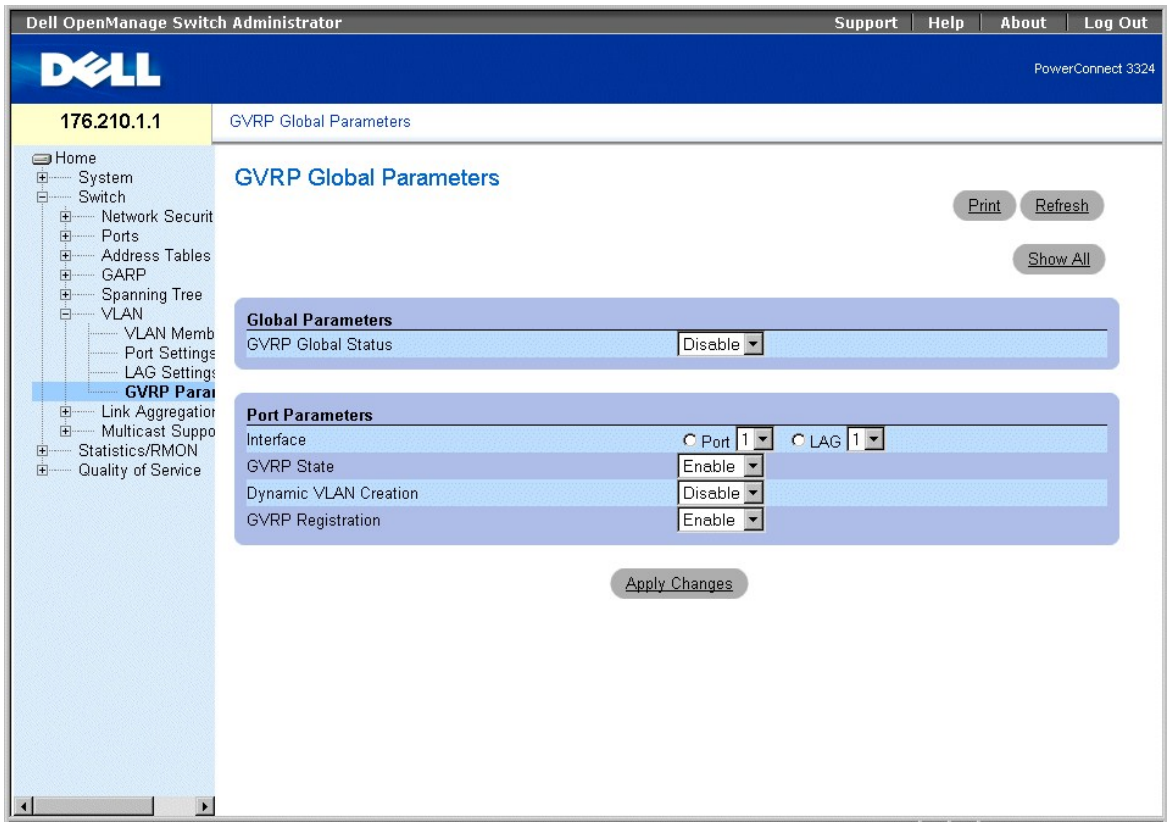
- Die Standard-Maximalanzahl von GVRP-VLANs beträgt aufgrund geltender Speicherbeschränkungen 128.
- Die maximale Anzahl von GVRP-VLANs wird durch die maximale Anzahl (der über die Variable Max VLANs MIB) verwalteten VLANs beschränkt.

Um den reibungslosen Betrieb des GVRP-Protokolls zu gewährleisten, sollten Benutzer die maximale Anzahl von GVRP-VLANs entsprechend einem Wert festlegen, der die Summe der folgenden Elemente deutlich übersteigt:

- Die Anzahl aller statischen VLANs, die bereits ordnungsgemäß konfiguriert sind oder demnächst konfiguriert werden.
- Die Anzahl aller dynamischen an GVRP-Operationen beteiligten VLANs, die bereits ordnungsgemäß konfiguriert sind (die anfängliche Anzahl aller GVRP-VLANs beträgt 128) oder demnächst konfiguriert werden.

Wenn die maximale Anzahl der GVRP-VLANs auf einen Wert gesetzt wird, der diese Summen übersteigt, können Benutzer GVRP ausführen, ohne hierzu das Gerät zurücksetzen zu müssen, um eine größere Anzahl von GVRP-VLANs zuzulassen. Wenn beispielsweise drei VLANs vorhanden sind und zwei weitere infolge einer statischen oder dynamischen VLAN-Registrierung konfiguriert werden sollen, setzen Sie die maximale Anzahl der GVRP-VLANs nach dem Zurücksetzen auf "10". So öffnen Sie die Seite **GVRP Parameters**:

- Klicken Sie in der Strukturansicht auf **Switch > VLAN > GVRP Parameters.** Die Seite **GVRP Parameters** wird geöffnet.



Seite "GVRP Parameters"

Die Seite **GVRP Parameters** enthält folgende Felder:

- **GVRP Global Status** - Aktiviert GVRP für das Gerät. Folgende Feldwerte können ausgewählt werden:
  - **Enabled** - Gibt an, dass GVRP für das Gerät aktiviert ist.
  - **Disabled** - Gibt an, dass GVRP für das Gerät deaktiviert ist. Dies ist der Standardfeldwert.
- **Interface** - Gibt die spezifische Schnittstelle an, für die GVRP aktiviert wird. Folgende Feldwerte können ausgewählt werden:
  - **Port** - Gibt den spezifischen Anschluss an, für den GVRP aktiviert wird.
  - **LAG** - Gibt die spezifische LAG an, für die GVRP aktiviert wird.
- **GVRP State** - Gibt an, ob GVRP für einen Anschluss aktiviert ist. Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Aktiviert GVRP für die Schnittstelle.
  - **Disable** - Deaktiviert GVRP für die Schnittstelle. Dies ist der Standardwert.
- **Dynamic VLAN Creation** - Aktiviert die VLAN-Erstellung über GVRP. Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Aktiviert die VLAN-Erstellung über GVRP.
  - **Disable** - Deaktiviert die VLAN-Erstellung über GVRP.
- **GVRP Registration** - Aktiviert den GVRP-Registrierungsstatus. Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Aktiviert die VLAN-Registrierung über GVRP.
  - **Disable** - Deaktiviert die VLAN-Registrierung über GVRP.

Aktivieren von GVRP für das Gerät:

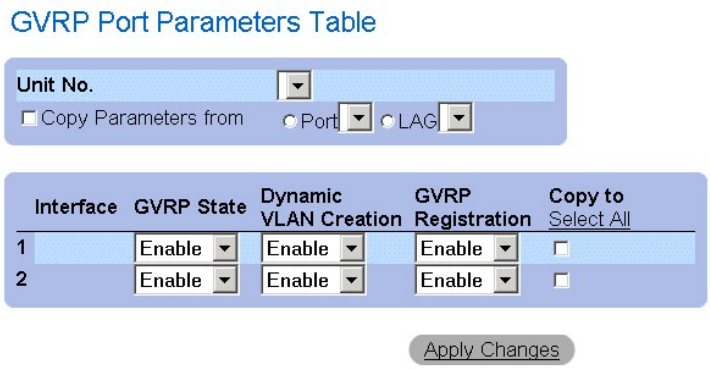
1. Öffnen Sie die Seite **GVRP Parameters.**
2. Wählen Sie **Enable** im Feld **GVRP Global Status** aus.
3. Klicken Sie auf **Apply Changes**. GVRP wird für das Gerät aktiviert.

Definieren von GVRP-Anschlüssen:

1. Öffnen Sie die Seite **GVRP Parameters.**
2. Klicken Sie auf **Show All**. Die Seite **GVRP Parameters** wird geöffnet. Die **GVRP Port Parameters** umfassen Parameter, durch die GVRP für einen Anschluss aktiviert und der Anschluss für die VLAN-Registrierung über GVRP zugelassen wird. Zusätzlich enthält die **GVRP Port Parameters Table** Informationen über den VLAN- Registrierungsmodus. Darüber hinaus können spezifische Anschlüsse für die Registrierung oder Verwendung in einem VLAN gesperrt werden.
3. Wählen Sie einen Anschluss aus.
4. Definieren Sie die Felder **GVRP State**, **Dynamic VLAN Creation**, **VLAN Registration** und **GVRP Registration**.
5. Klicken Sie auf **Apply Changes**. GVRP wird für den Anschluss aktiviert, die Parameter werden definiert, und das Gerät wird aktualisiert.

Anzeigen der GVRP Port Parameters Table:

1. Öffnen Sie die Seite **GVRP Parameters.**
2. Klicken Sie auf **Show All**. Die **GVRP Port Parameters Table** wird geöffnet.



GVRP Port Parameters Table

Zusätzlich zu dem auf der Seite **GVRP Parameters** angezeigten Feld enthält die Seite **GVRP Port Parameters Table** die folgenden Felder:

- **Unit** - Gibt die Nummer der Stack-Einheit an, für die GVRP-Informationen angezeigt werden.
- **Copy Parameters From** - Gibt die spezifische Schnittstelle an, von der die GVRP-Parameter kopiert werden.
- **Copy To** - Gibt die Anschlüsse an, auf welche die GVRP-Parameter kopiert werden.

Konfigurieren von GVRP mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zur GVRP-Konfiguration zusammengefasst, die auf der Seite **GVRP Parameters** verfügbar ist.

CLI-Befehl	**Beschreibung**
gvrp enable	Aktiviert GVRP global.
gvrp enable	Aktiviert GVRP für eine Schnittstelle.
gvrp vlan-creation-forbid	Aktiviert oder deaktiviert die dynamische VLAN-Erstellung.
gvrp registration-forbid	Hebt alle VLAN-Registrierungen auf und verhindert die dynamische VLAN-Erstellung oder -Registrierung für den Anschluss.
show gvrp configuration [ethernet Schnittstelle | port-channel *Anschlusskanalnummer*]	Zeigt GVRP-Konfigurationsinformationen an, darunter Timer-Werte, ob GVRP und die dynamische VLAN-Erstellung aktiviert ist und auf welchen Anschlüssen GVRP ausgeführt wird.
gvrp max-vlan number	Konfiguriert die maximale Anzahl von VLANs, falls GVRP aktiviert ist.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# gvrp enable
```

```
Console (config)# interface ethernet 1/e8

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 switch.

Maximum VLANs: 256, Maximum VLANs after reset: 256.

Port(s)Status Registration Dynamic VLAN Timers (milliseconds)

Creation Join Leave Leave All

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

2/1 Enabled Normal Enabled 200 600 10000

4/4 Enabled Normal Enabled 200 600 10000
```

Aggregieren von Anschlüssen

Durch die Anschlussaggregation wird die Anschlussnutzung optimiert, indem eine Gruppe von Anschlüssen zu einer Link Aggregated Group (LAG) zusammengefasst wird. Die Anschlussaggregation erhöht die Bandbreite zwischen Geräten um ein Vielfaches, steigert die Anschlussflexibilität und gewährleistet die Leitungsredundanz. Sowohl der PowerConnect 3324 als auch der PowerConnect 3348 unterstützen bis zu sechs LAGs sowie pro Stack oder eigenständiger Einheit acht Anschlüsse.

Jede LAG besteht aus vier Anschlüssen mit derselben Geschwindigkeit, die für den Vollduplexbetrieb konfiguriert sind. Die Anschlüsse innerhalb einer LAG können unterschiedliche Medientypen (UTP/Glasfaser bzw. verschiedene Glasfasertypen) aufweisen, solange sie mit derselben Geschwindigkeit arbeiten.

Aggregierte Verbindungen können manuell oder automatisch zugewiesen werden, indem für die relevanten Verbindungen das the Link Aggregation Control Protocol (LACP) aktiviert wird. Die PowerConnect 3324- und 3348-Geräte unterstützen das LAG Load Balancing, das sowohl auf MAC-Quell- als auch auf MAC-Zieladressen basiert.

Aggregierte Verbindungen werden vom System als ein einziger logischer Anschluss behandelt. Konkret bedeutet dies, dass die aggregierte Verbindung über ähnliche Anschlussattribute verfügt wie ein nicht aggregierter Anschluss, z. B. Auto-Negotiation, Geschwindigkeit, Duplexeinstellung usw.

Die PowerConnect 3324- und 3348-Geräte unterstützen sowohl statische LAGs als auch LACP-(Link Aggregation Control Protocol-)LAGs. LACP-LAGs handeln mit anderen LACP-Anschlüssen, die sich an einem anderen Gerät befinden, Verbindungen mit aggregierten Anschlüssen aus. Wenn es sich bei den Anschlüssen des anderen Gerätes ebenfalls um LACP-Anschlüsse handelt, richten die Geräte eine LAG für diese Anschlüsse ein.

Um Anschlüsse einer LAG in einer eigenständigen oder Stack-Konfiguration hinzuzufügen, sollten Sie die folgenden Richtlinien beachten:

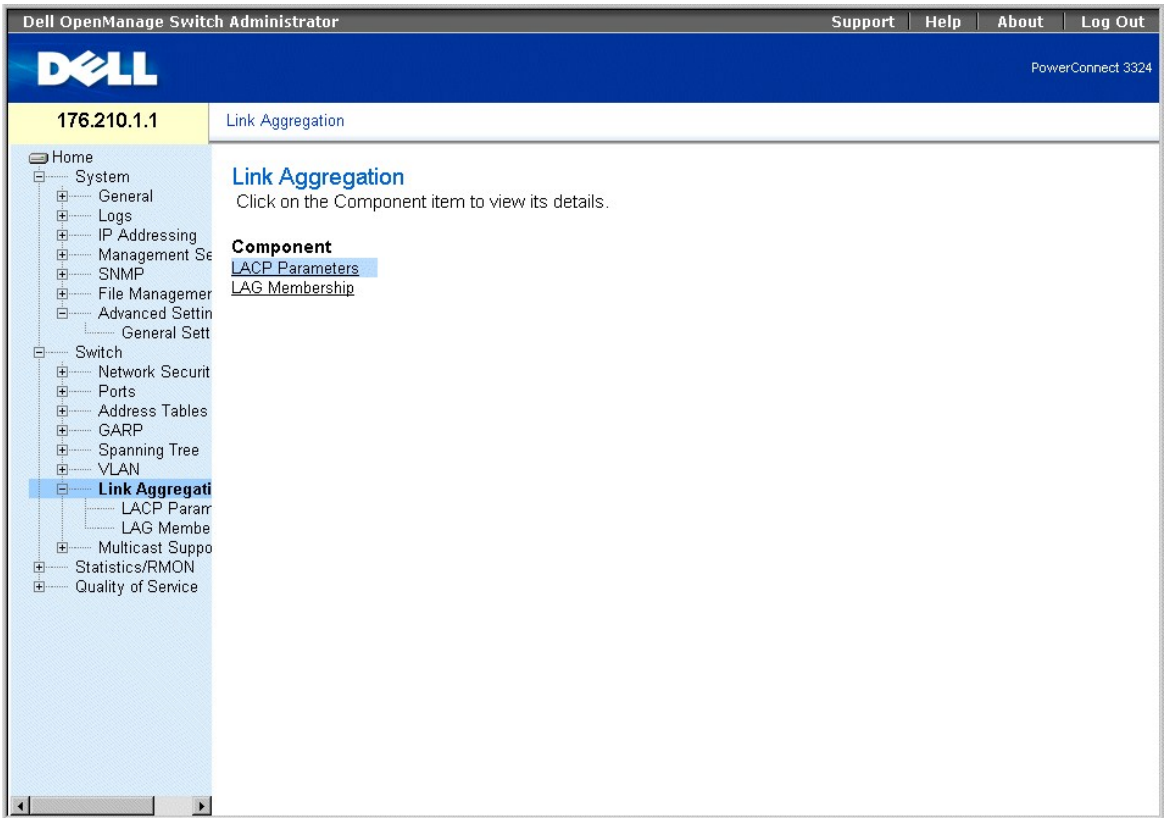
- Für den Anschluss darf keine Layer 3-Schnittstelle definiert werden.
- Der Anschluss darf keinem VLAN angehören.
- Der Anschluss darf keiner anderen LAG angehören.
- Der Anschluss darf nicht gespiegelt werden.
- Die 802.1p-Priorität des Anschlusses muss der 802.1p-Priorität der LAG entsprechen.
- Für den Anschluss darf keine ACL definiert sein.
- Für den Anschluss darf QoS Trust nicht deaktiviert sein.
- GVRP darf nicht aktiviert sein.

ANMERKUNG: Anschlüsse dürfen nur als LACP-Anschlüsse konfiguriert werden, wenn sie keiner zuvor konfigurierten LAG angehören.

Der PowerConnect 3324/3348 ermittelt über eine Hash-Funktion, welche Frames über welche aggregierte Verbindungskomponente übertragen werden. Die Hash-Funktion berechnet den statistischen Lastenausgleich für aggregierte Verbindungskomponenten. Eine aggregierte Verbindung wird vom PowerConnect 3324/3348 als ein logischer Anschluss angesehen.

Jede aggregierte Verbindung verfügt über einen aggregierten Verbindungsanschlusstyp, einschließlich Gigabit Ethernet- und Fast Ethernet-Anschlüssen. Anschlüsse können einer aggregierten Verbindung nur hinzugefügt werden, wenn sie denselben Anschlusstyp aufweisen. Wenn Anschlüsse aus einer aggregierten Verbindung entfernt werden, werden die ursprünglichen Anschlusseinstellungen wiederhergestellt. So öffnen Sie die Seite **Link Aggregation**:

- Klicken Sie in der Strukturansicht auf **Switch > Link Aggregation.** Die Seite **Link Aggregation** wird geöffnet.



Seite "Link Aggregation"

Dieser Abschnitt enthält die folgenden Themen:

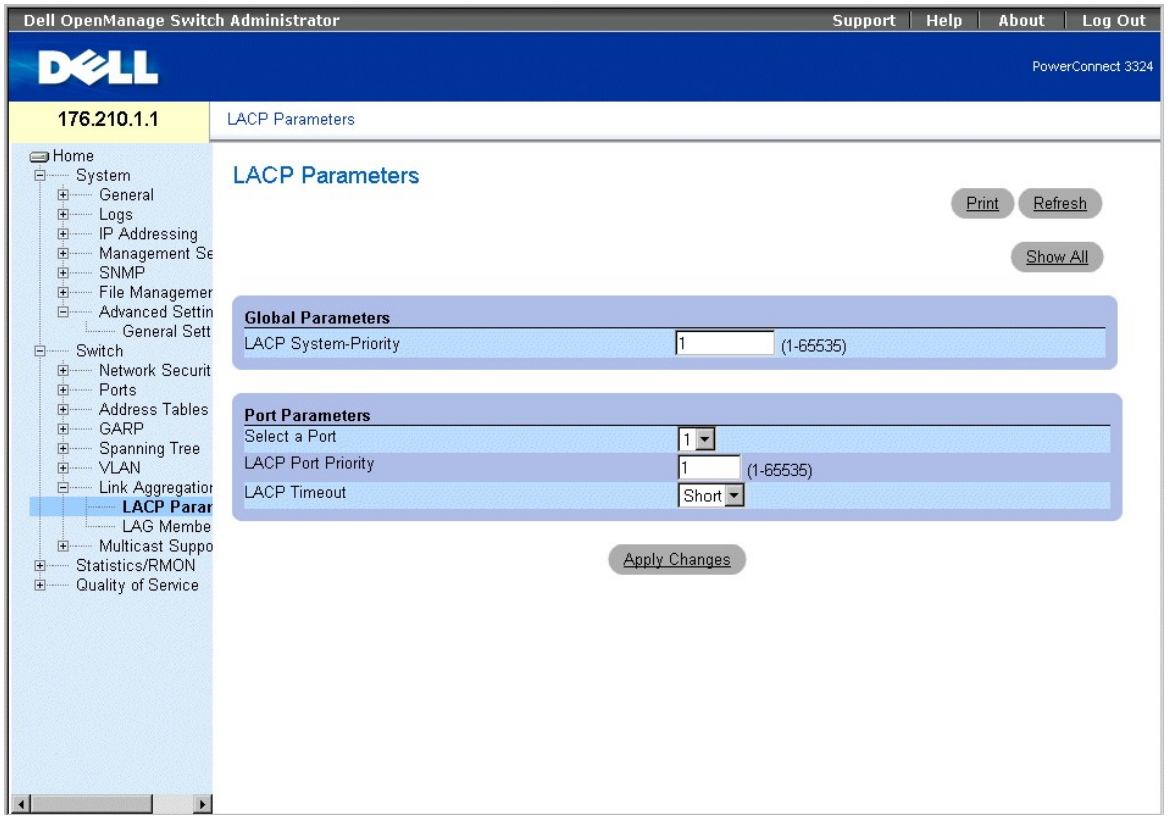
- Definieren von LACP-Parametern
- Definieren von LAG-Mitgliedschaften

Definieren von LACP-Parametern

Die Seite **LACP Parameters** enthält Informationen zur Konfiguration von LACP-LAGs. Aggregierte Anschlüsse können in Gruppen für die Verbindungsaggregation zusammengefasst werden. Jede Gruppe besteht aus Anschlüssen mit derselben Geschwindigkeit.

Aggregierte Verbindungen können manuell oder automatisch eingerichtet werden, indem für die relevanten Verbindungen das Link Aggregation Control Protocol (LACP) aktiviert wird. So öffnen Sie die Seite **LACP Parameters** :

- Klicken Sie in der Strukturansicht auf **Switch > Link Aggregation > LACP Parameters.** Die Seite **LACP Parameters** wird geöffnet.



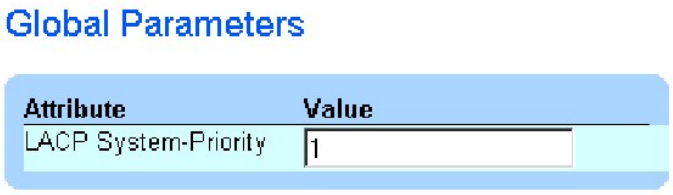
Seite "LACP Parameters"

Die Seite **LACP Parameters** enthält folgende Bereiche:

- Global Parameters
- Port Parameters Table

Global Parameters

Global Parameters enthält Informationen für die Zuweisung der LACP-Priorität. Aggregierte Anschlüsse können in Gruppen für die Verbindungsaggregation zusammengefasst werden. LAGs können manuell, durch explizite Benutzerzuweisung oder automatisch eingerichtet werden, indem das Link Aggregation Control Protocol (LACP) für die relevanten LAGs aktiviert wird.



Global Parameters

Der Bereich **Global Parameters** enthält das folgende Feld:

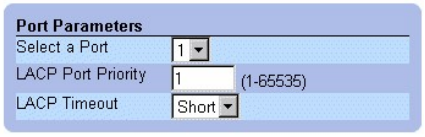
- **LACP System Priority** - Gibt den LACP-Prioritätswert an. Der Wertebereich umfasst die Werte 1 bis 65535. Der Standardwert lautet 1.

Definieren globaler Parameter:

1. Öffnen Sie die Seite **LACP Parameters.**
2. Führen Sie einen Bildlauf zum Bereich **Global Parameters** durch.
3. Definieren Sie die Felder **LACP System Priority** und **LACP Timeout**.
4. Klicken Sie auf **Apply Changes.** Die globalen Parameter werden definiert und das Gerät aktualisiert.

Port Parameters Table

Die **Port Parameters Table** enthält Informationen für die Zuweisung der LACP-Priorität und der Zeitlimitwerte zu Anschlüssen:



Port Parameters Table

Die **Port Parameters Table** enthält folgende Felder:

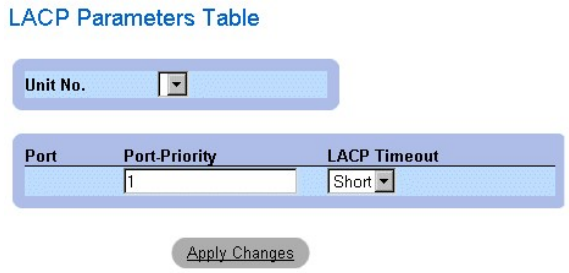
- **Select Port** - Gibt die Anschlussnummer an.
- **LACP Port Priority** - Gibt den LACP-Prioritätswert für den Anschluss an. Der Standardwert lautet 1.
- **LACP Timeout** - Weist ein administratives LACP-Zeitlimit zu. Folgende Feldwerte können ausgewählt werden:
  - **Short** - Legt ein kurzes Zeitlimit fest.
  - **Long** - Legt ein langes Zeitlimit fest.

Definieren von Anschlussparametern:

1. Öffnen Sie die Seite **LACP Parameters.**
2. Führen Sie einen Bildlauf zur **Link Aggregation Port Parameters Table** durch.
3. Definieren Sie die Felder **LACP System Priority** und **LACP Timeout**.
4. Klicken Sie auf **Apply Changes.** Die globalen Parameter für die Verbindungsaggregation werden definiert und das Gerät aktualisiert.

Anzeigen der LACP Parameters Table:

1. Öffnen Sie die Seite **LACP Parameters.**
2. Klicken Sie auf **Show All**. Die **LACP Parameters Table** wird geöffnet.



LACP Parameters Table

Zusätzlich zu den Feldern auf der Seite **LACP Parameters** wird auf der Seite **LACP Parameters Table** das folgende Feld angezeigt:

- **Unit** - Gibt die Nummer der Stack-Einheit an, für die LACP-Informationen angezeigt werden.

Konfigurieren von LACP-Parametern mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zur Konfiguration von LACP-Parametern zusammengefasst, die auf der Seite **Link Aggregation** angezeigt werden.

CLI-Befehl	**Beschreibung**
lacp system-priority *Wert*	Konfiguriert die Systempriorität.
lacp port-priority *Wert*	Konfiguriert den Prioritätswert für physische Anschlüsse.
lacp timeout {long | short}	Weist ein administratives LACP-Zeitlimit zu.
show lacp ethernet *Schnittstelle* **[parameters | statistics | protocol-state]**	Zeigt LACP-Informationen für Ethernet-Anschlüsse an.
show lacp port-channel **[Anschlusskanalnummer]**	Zeigt LACP-Informationen für einen Anschlusskanal an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# lacp system-priority 120

Console (config)# interface ethernet 1/e8

Console (config-if)# lacp port-priority 247

Console (config-if)# lacp timeout long

Console (config-if)# exit

Console# show lacp ethernet 1/e1 statistics

Port 1/e1 LACP Statistics:

LACP PDUs sent:2
```

```
LACP PDUs received:2
```

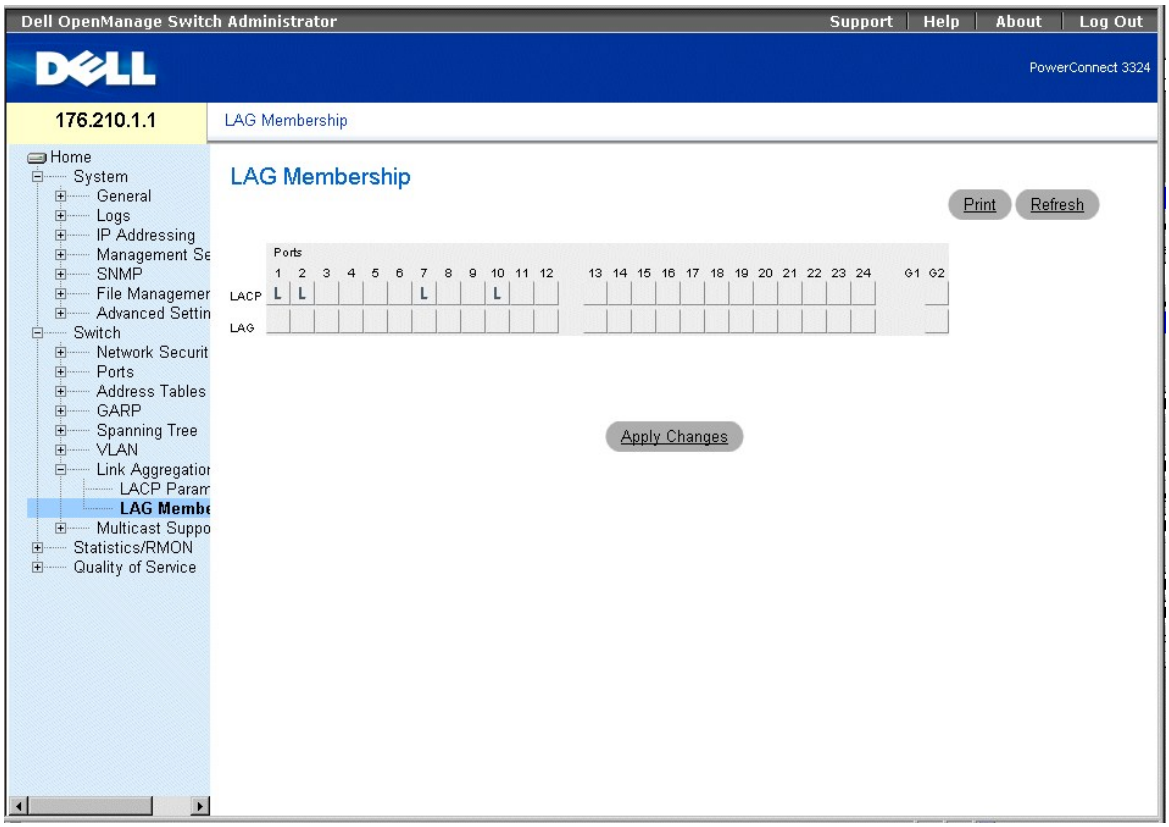
Definieren von LAG-Mitgliedschaften

Auf der Seite **LAG Membership** haben Netzwerkverwalter die Möglichkeit, LAGs Anschlüsse zuzuweisen. LAGs können bis zu acht Anschlüsse umfassen. Der PowerConnect 3324/3348 unterstützt derzeit sechs LAGs pro System, unabhängig davon, ob das Gerät eigenständig ist oder einem Stack angehört. Die **LAG Membership Table** enthält folgende Zeilen:

- **LACP** - Gibt an, ob der Anschluss dynamisch ist, indem er als LAG-Komponente zugelassen wird.
- **LAG** - Fügt einer LAG einen Anschluss hinzu und gibt die spezifische LAG an, welcher der Anschluss angehört.

So öffnen Sie die Seite **LAG Membership**:

- Klicken Sie in der Strukturansicht auf Switch > Link Aggregation > LAG Membership Tab. Die Seite **LAG Membership** wird geöffnet.



Seite "LAG Membership"

Hinzufügen eines Anschlusses zur einer LAG:

1. Öffnen Sie die Seite **LAG Membership**.
2. Ändern Sie den unter der Anschlussnummer angezeigten Wert, um LAG-Einstellung und -Nummer zuzuweisen.
3. Klicken Sie auf **Apply Changes**. Der Anschluss wird der LAG hinzugefügt und das Gerät aktualisiert.

Zuweisen von Anschlüssen zu LAGs mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Zuweisung von Anschlüssen zu LAGs zusammengefasst, die auf der Seite **LAG**

Membership angezeigt werden.

CLI-Befehl	Beschreibung
channel-group port-channel-number mode {on | auto}	Konfiguriert einen Anschluss für einen Anschlusskanal.
show interface port_channel	Zeigt die mit einer LAG verknüpften Schnittstellen an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console# channel-group port-channel-number mode on auto 1

Port-Channel 1:Port Type 1000 Ethernet

Actor

System Priority:1

MAC Address: 000285:0E1C00

Admin Key: 29

Oper Key: 29

Partner

System Priority:0

MAC Address: 000000:000000

Oper Key: 14
```

Unterstützung für die Multicast-Weiterleitung

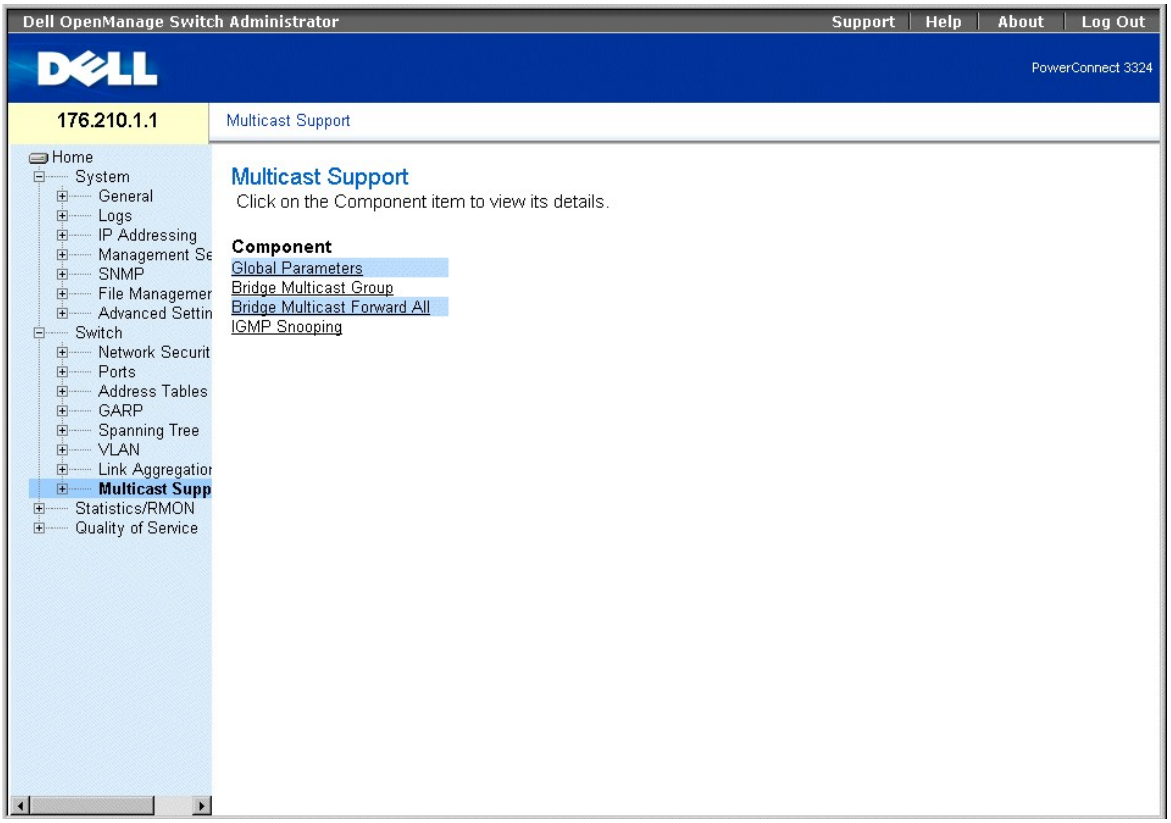
Bei der Multicast-Weiterleitung können einzelne Pakete an mehrere Ziele weitergeleitet werden. Der L2-Multicastdienst basiert auf einem L2-Switch, der ein an eine spezifische Multicastadresse adressiertes Einzelpaket empfängt. Bei der Multicast-Weiterleitung werden Kopien der Pakete erstellt und Pakete an die relevanten Anschlüsse übertragen.

Der PowerConnect 3324/3348 unterstützt die folgenden beiden Einstellungen:

- **Forwarding L2 Multicast Packets** - Standardmäßig aktiviert.
- **Filtering L2 Multicast Packets** - Aktiviert die Weiterleitung von L2-Paketen zum VLAN des Anschlusses. Wenn die Multicast-Filterung deaktiviert ist, werden Multicast-Pakete an alle relevanten VLAN-Anschlüsse weitergeleitet.

So öffnen Sie die Seite **Multicast Support** :

- Klicken Sie in der Strukturansicht auf **Switch > Multicast Support.** Die Seite **Multicast Support** wird geöffnet.



Seite "Multicast Support"

Die Seite **Multicast Support** enthält Links zu den folgenden Themen:

- Definieren von IGMP-Snooping-Einstellungen
- Hinzufügen von Komponenten zu einer Bridge-Multicast-Gruppe
- Zuweisen von Parametern für die globale Multicast-Weiterleitung
- Aktivieren von IGMP-Snooping

Definieren von IGMP-Snooping-Einstellungen

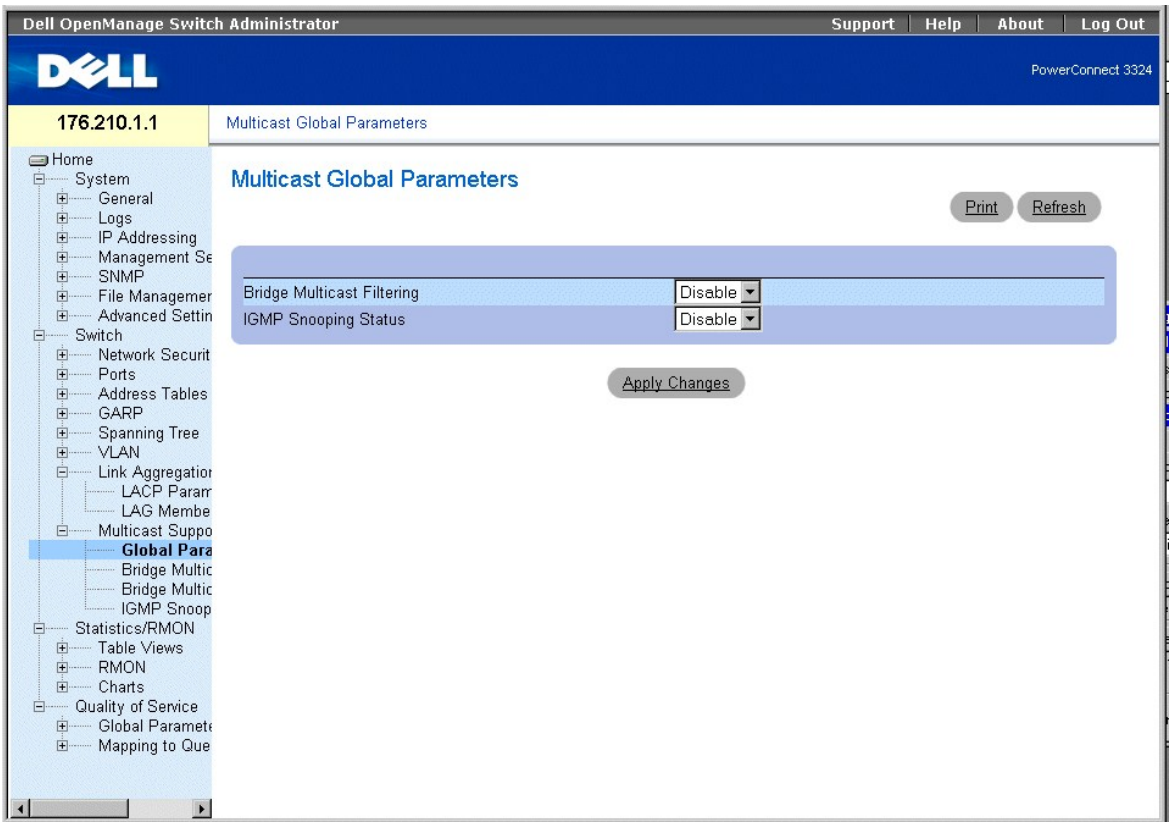
Beim Layer 2-Switching werden Multicast-Pakete standardmäßig an alle relevanten VLAN-Anschlüsse weitergeleitet, wobei die Pakete als Multicast-Pakete behandelt werden. Diese Art der Datenweiterleitung ist prinzipiell funktionsfähig. Der Multicast-Datenverkehr wird jedoch auch auf nicht beabsichtigten Anschlüssen empfangen, was zu einem erhöhten Aufkommen von Netzwerkverkehrsdaten führt.

Beim IGMP-Snooping wird unnötiger Multicast-Datenverkehr unterdrückt, indem IGMP-Frames überprüft werden, während sie von den Stationen an Multicast-Router weitergeleitet werden.

Wenn IGMP-Snooping global aktiviert ist, ist der Switching-ASIC für die Weiterleitung aller IGMP-Frames an die CPU programmiert. Die CPU analysiert die eingehenden Frames und ermittelt, welche Anschlüsse welchen Multicast-Gruppen beitreten sollen, welche Anschlüsse Multicast-Router zur Generierung von IGMP-Abfragen veranlassen und welche Routing-Protokolle Pakete und Multicast-Datenverkehr weiterleiten. Ein Anschluss, der einer bestimmten Multicast-Gruppe beitreten soll, gibt einen IGMP-Bericht aus, in dem diese Multicast-Gruppe angegeben ist.

Auf der Seite **Multicast Global Parameters** können Netzwerkverwalter IGMP-Snooping und Multicast-Filterung generell für das Gerät aktivieren. So öffnen Sie die Seite **Multicast Global Parameters** :

- Klicken Sie in der Strukturansicht auf **Switch > Multicast Support > Global Parameters.** Die Seite **Multicast Global Parameters** wird geöffnet.



Seite "Multicast Global Parameters"

Die Seite **Multicast Global Parameters** enthält folgende Felder:

- **Bridge Multicast Filtering** - Gibt an, ob die Bridge-Multicast-Filterung für das Gerät aktiviert ist. Folgende Feldwerte können ausgewählt werden:
  - **Enabled** - Aktiviert die Bridge-Multicast-Filterung für das Gerät.
  - **Disabled** - Deaktiviert die Bridge-Multicast-Filterung für das Gerät. Dies ist der Standardwert.
- **IGMP Snooping Status** - Gibt an, ob das IGMP-Snooping für das Gerät aktiviert ist. Folgende Feldwerte können ausgewählt werden:
  - **Enabled** - Aktiviert das IGMP-Snooping für das spezifische VLAN.
  - **Disabled** - Deaktiviert das IGMP-Snooping für das spezifische VLAN. Dies ist der Standardwert.

Aktivieren der Bridge-Multicast-Filterung für das Gerät:

1. Öffnen Sie die Seite **Multicast Global Parameters**.
2. Wählen Sie **Enable** im Feld **bridge multicast filtering** aus.
3. Klicken Sie auf **Apply Changes**. **Bridge Multicast** wird für das Gerät aktiviert.

Aktivieren von IGMP-Snooping für das Gerät:

1. Öffnen Sie die Seite **Multicast Global Parameters**.
2. Wählen Sie **Enable** im Feld **IGMP Snooping Status** aus.
3. Klicken Sie auf **Apply Changes**. IGMP-Snooping wird für das Gerät aktiviert.

Aktivieren von Multicast-Weiterleitung und IGMP-Snooping mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Aktivierung von Multicast-Weiterleitung und IGM-Snooping zusammengefasst, die auf der Seite **Multicast Support** angezeigt werden.

CLI-Befehl	Beschreibung
bridge multicast filtering	Aktiviert die Filterung von Multicastadressen.
ip igmp snooping	Aktiviert das IGMP-(Internet Group Management Protocol-)Snooping.

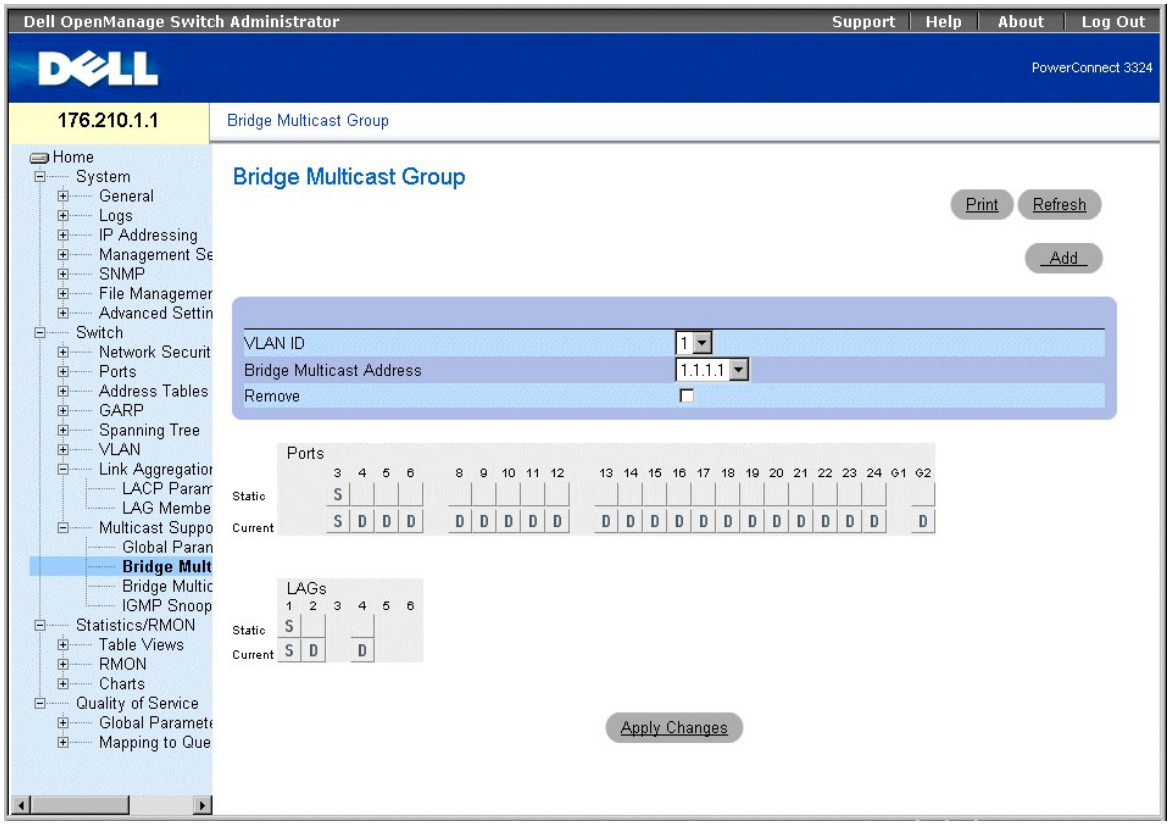
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# bridge multicast filtering

Console (config)# ip igmp snooping
```

Hinzufügen von Komponenten zu einer Bridge-Multicast-Gruppe

Auf der Seite **Bridge Multicast Group** werden die Anschlüsse und LAGs angezeigt, die mit den Multicast-Dienstgruppen in den **Anschluss-**- und **LAG-Tabellen** verknüpft sind. In den Anschluss- und LAG-Tabellen wird auch angegeben, wie der Anschluss oder die LAG der Multicast-Gruppe hinzugefügt wird. Anschlüsse können entweder vorhandenen Gruppen oder einer neuen Multicast-Dienstgruppe hinzugefügt werden. Auf der Seite **Bridge Multicast Group** können neue Multicast-Dienstgruppen erstellt werden. Auf der Seite **Bridge Multicast Group** werden einer spezifischen Multicast-Dienst-Adressgruppe darüber hinaus Anschlüsse zugewiesen. So öffnen Sie die Seite **Bridge Multicast Group**:

- Klicken Sie in der Strukturansicht auf **Switch > Multicast Support > Bridge Multicast Group.** Die Seite **Bridge Multicast Group** wird geöffnet.



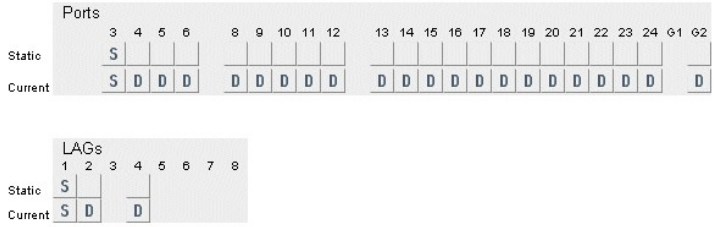
Seite "Bridge Multicast Group"

Die Seite **Bridge Multicast Group** enthält folgende Felder:

- **VLAN ID** - Identifiziert ein VLAN.

- **Bridge Multicast Address** - Identifiziert die IP-Adresse einer Multicast-Gruppe.
- **Remove** - Entfernt eine durch ihre Adresse angegebene Bridge-Multicast-Gruppe.
  - **Aktiviert** - Entfernt die Bridge-Multicastadresse.
  - **Deaktiviert** - Behält die Bridge-Multicastadresse bei.
- **Ports Table** - Listet den Anschluss auf, der einem Multicast-Dienst hinzugefügt werden kann.
- **LAGs Table** - Listet die LAGs auf, die einem Multicast-Dienst hinzugefügt werden können.

In der Abbildung **IGMP Port/LAG Members Table** wird der Zugehörigkeitsstatus von IGMP-Anschlüssen/LAGs angezeigt.



IGMP Port/LAG Members Table

Die **IGMP Port/LAG Members Table Control Settings Table** enthält die Einstellungen für die Verwaltung von IGMP-Anschluss und LAG-Komponenten.

IGMP Port/LAG Members Table Control Settings

Anschlusssteuerung	Definition
D	Gibt in der Zeile **Current** an, dass der Anschluss/die LAG der Multicast-Gruppe dynamisch beigetreten ist.
S	Verknüpft den Anschluss in der Zeile **Static** als statische Komponente mit der Multicast-Gruppe. Gibt in der Zeile **Current** an, dass der Anschluss/die LAG der Multicast-Gruppe statisch beigetreten ist.
F	Gibt an, dass der Anschluss dieser Multicast-Gruppe nicht beitreten darf.
Leer	Gibt an, dass der Anschluss nicht mit der Multicast-Gruppe verknüpft ist.

Definieren von Anschlüssen für den Empfang eines Multicast-Dienstes:

1. Öffnen Sie die Seite **Bridge Multicast**.
2. Definieren Sie die Felder **VLAN ID** und **Bridge Multicast Address.**
3. Aktivieren Sie **S** für einen Anschluss, damit dieser einer ausgewählten Multicast- Gruppe beitreten kann oder **F**, um dessen Beitritt zu dieser Multicast-Gruppe zu verhindern.
4. Klicken Sie auf **Apply Changes**. Der Anschluss wird der Multicast-Gruppe zugewiesen und das Gerät aktualisiert.

Zuweisen von LAGs für den Empfang des Multicast-Dienstes:

1. Öffnen Sie die Seite **Bridge Multicast**.
2. Definieren Sie die Felder **VLAN ID** und **Bridge Multicast Address.**
3. Aktivieren Sie **S** für die LAG, damit diese der ausgewählten Multicast-Gruppe beitreten kann, oder aktivieren Sie **F** für einen Anschluss, um den Beitritt des Anschlusses zu dieser Multicast-Gruppe zu verhindern.
4. Klicken Sie auf **Apply Changes**. Die LAG wird der Multicast-Gruppe zugewiesen und das Gerät aktualisiert.

Verwalten von Multicast-Dienstkomponenten mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Verwaltung von Multicast-Dienstkomponenten zusammengefasst, die auf der Seite **Bridge Multicast Group** angezeigt werden.

CLI-Befehl	Beschreibung
bridge multicast address {*MAC-Multicast-Addresse* **|** *IP-Multicast-Addresse***} {add | remove} {ethernet** *Schnittstellenliste* **| port-channel** *Anschlusskanal-Liste***}**	Registriert MAC-Layer-Multicastadressen in der Bridge-Tabelle und fügt der Gruppe statische Anschlüsse hinzu.
show bridge multicast address-table [vlan *VLAN-ID***] [address** *MAC-Multicastadresse* **|** *IP-Multicastadresse***] [format ip | mac]**	Zeigt Informationen der MAC-Multicast-Adresstabelle an.

Im Folgenden ein Beispiel für die CLI-Befehle:

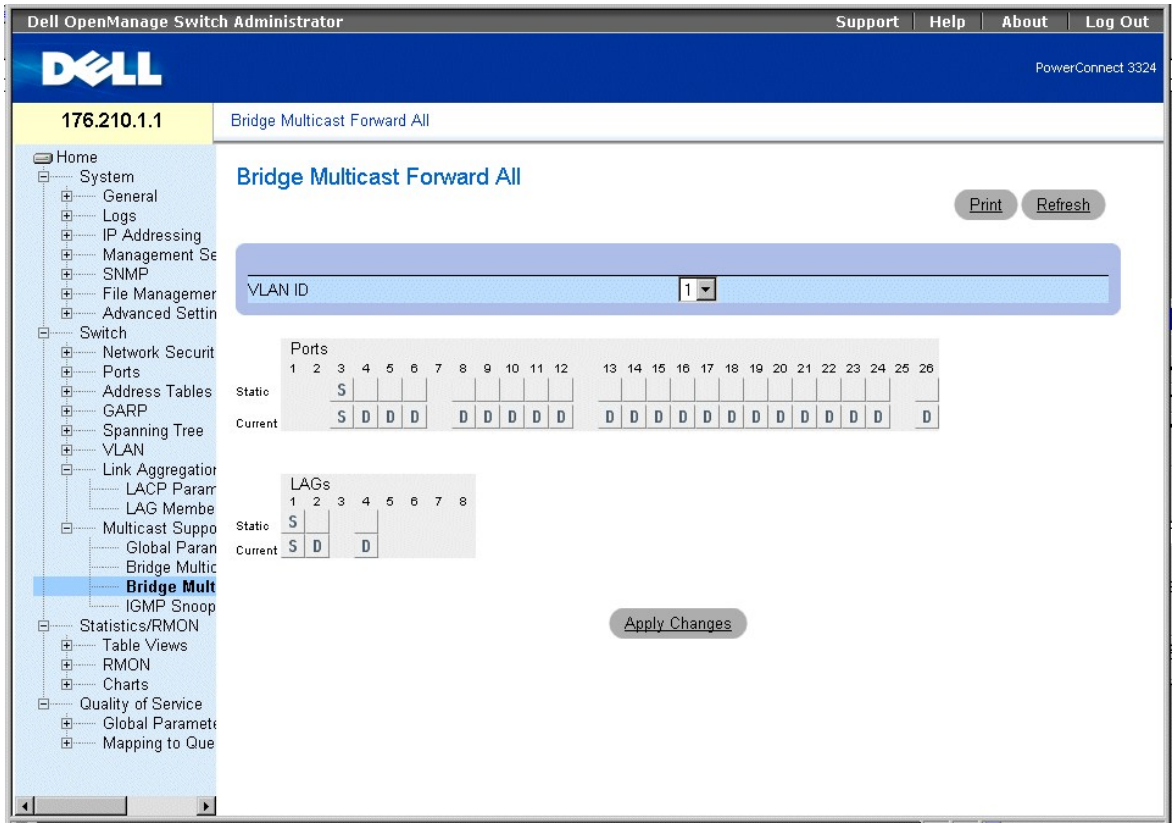
```
Console (config)# interface vlan 8

bridge multicast address 0100.5e02.0203

bridge multicast address 0100.5e02.0203 add ethernet 1/e1, 2/e2

Console (config-if)# Exit

Console # show bridge multicast address-table



Vlan MAC Address type Ports

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

1 0100.5e02.0203 static 1/e1, 2/e2

19 0100.5e02.0208 static 1/e1-8

19 0100.5e02.0208 dynamic 1/e9-11



Forbidden ports for multicast addresses:

Vlan MAC Address Ports

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

1 0100.5e02.0203 2/e8

19 0100.5e02.0208 2/e8
```

Zuweisen von Parametern für die globale Multicast-Weiterleitung

Auf der Seite **Bridge Multicast Forward All** können Netzwerkverwalter die Verknüpfung von Anschlüssen oder LAGs mit einem Switch aktivieren, der mit einem angrenzenden Multicast-Router/-Switch verbunden ist. Nachdem das IGMP-Snooping aktiviert wurde, werden die Multicast-Pakete an den entsprechenden

Anschluss bzw. das entsprechende VLAN weitergeleitet.

- Klicken Sie in der Strukturansicht auf **Switch > Multicast Support > Bridge Multicast > Bridge Multicast Forward All Tab.** Die Seite **Bridge Multicast Forward All** wird geöffnet.



Seite "Bridge Multicast Forward All"

Die Seite **Bridge Multicast Forward All** enthält folgende Felder:

- **VLAN ID** - Identifiziert das einem Frame zugewiesene VLAN und enthält Informationen zur Adresse der Multicast-Gruppe.
- **Ports Table** - Listet den Anschluss auf, der einem Multicast-Dienst hinzugefügt werden kann.
- **LAGs Table** - Listet die LAGs auf, die einem Multicast-Dienst hinzugefügt werden können.

Die Seite **Bridge Multicast Forward All** enthält die Einstellungen für die Verwaltung von Switch- und Anschlusseinstellungen.

Router- / Anschlusssteuerungs-Einstellungen unter "Bridge Multicast Forward All"

Anschlusssteuerung	Definition
D	Verknüpft den Anschluss als dynamischen Anschluss mit dem Multicast-Router oder -Switch.
S	Verknüpft den Anschluss als statischen Anschluss mit dem Multicast-Router oder -Switch.
F	Gibt an, dass der Anschluss keiner Multicast-Gruppe beitreten darf.
Leer	Gibt an, dass der Anschluss mit keinem Multicast-Router oder -Switch verknüpft ist.

Verbinden eines Anschlusses mit einem Multicast-Router oder -Switch:

1. Öffnen Sie die Seite **Bridge Multicast Forward All**.
2. Definieren Sie das Feld **VLAN ID**.
3. Wählen Sie einen Anschluss in der **Multicast Router Port Table** aus, und weisen Sie ihm einen Wert zu.

4. Klicken Sie auf **Apply Changes**. Der mit dem Multicast-Router oder der Multicast- Gruppe verknüpfte Anschluss wird aktualisiert.

Verbinden einer LAG mit einem Multicast-Router oder -Switch:

1. Öffnen Sie die Seite **Bridge Multicast Forward All**.
2. Definieren Sie das Feld **VLAN ID**.
3. Wählen Sie eine LAG in der **Multicast Router Port Table** aus, und weisen Sie ihr einen Wert zu.
4. Klicken Sie auf **Apply Changes**. Die mit dem Multicast-Router oder der Multicast- Gruppe verknüpfte LAG wird aktualisiert.

Verwalten von mit Multicast-Routern verbundenen LAGs und Anschlüssen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Verwaltung von mit Multicast-Routern verbundenen LAGs und Anschlüssen zusammengefasst, die auf der Seite **Bridge Multicast Forward All** angezeigt werden.

CLI-Befehl	Beschreibung
show bridge multicast filtering *VLAN-ID*	Zeigt die Multicast-Konfiguration an.
bridge multicast forbidden forward-all	Deaktiviert die Weiterleitung von Multicast-Paketen für einen Anschluss.
bridge multicast forward-all {add | remove} {ethernet interface-list | port-channel port-channel-number-list}	Aktiviert die Weiterleitung aller Multicast-Pakete für einen Anschluss.

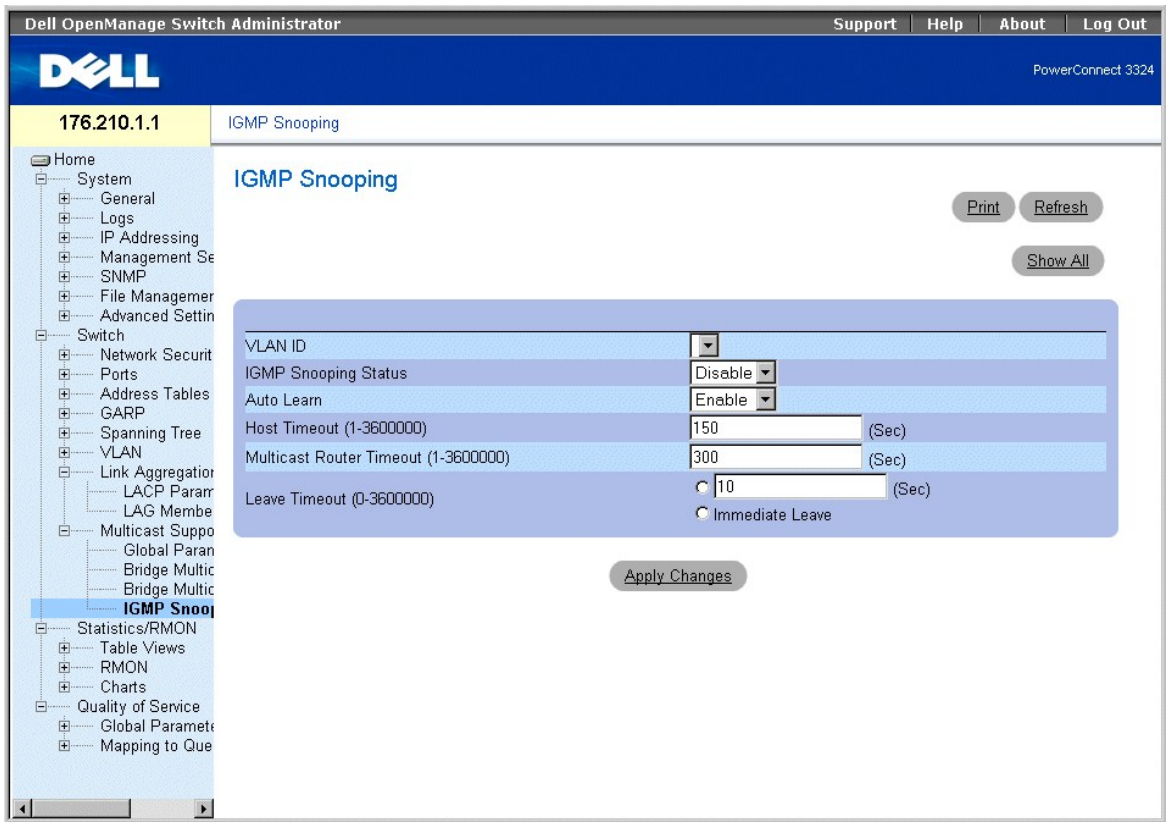
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console # show bridge multicast filtering

Filtering: Aktiviert

VLAN: 1

Port Forward-All

Static Status

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

1/e1 Forbidden Filter

1/e2 Forward Forward(s)

1/e3 - Forward(s)
```

Aktivieren von IGMP-Snooping

Auf der Seite **IGMP Snooping** können Netzwerkverwalter IGMP-Komponenten hinzufügen. So öffnen Sie die Seite **IGMP Snooping**:

- Klicken Sie in der Strukturansicht auf **Switch > Multicast Support > IGMP Snooping.** Die Seite **IGMP Snooping** wird geöffnet.



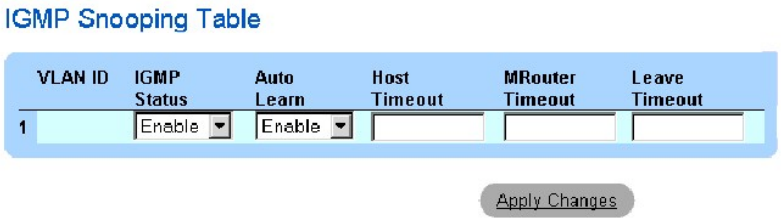
Seite "IGMP Snooping"

Die Seite **IGMP Snooping** enthält folgende Informationen:

- **VLAN ID** - Gibt die VLAN-ID an.
- **IGMP Snooping Status** - Aktiviert IGMP-Snooping für das Gerät. Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Aktiviert IGMP-Snooping für das Gerät.
  - **Disable** - Deaktiviert IGMP-Snooping für das Gerät.
- **Auto Learn** - Aktiviert die automatische Erfassung neuer Multicast-Gruppenkomponenten. Folgende Feldwerte können ausgewählt werden:
  - **Enable** - Aktiviert die automatische Erfassung neuer Multicast-Gruppenkomponenten.
  - **Disable** - Deaktiviert die automatische Erfassung neuer Multicast-Gruppenkomponenten.
- **Host Timeout (1-3600000)** - Gibt an, nach welcher Zeit die Speicherdauer eines IGMP-Snooping-Eintrags abläuft. Der Standardwert lautet **150** Sekunden.
- **Multicast Router Timeout (1-3600000)** - Gibt an, nach welcher Zeit die Speicherdauer eines Multicast-Router-Eintrags abläuft. Der Standardwert lautet **300** Sekunden.
- **Leave Time Out (1-3600000)** - Gibt die Zeit in Sekunden nach dem Empfang einer Leave-Nachricht für einen Anschluss an, bevor die Speicherdauer für den Eintrag abläuft. Folgende Feldwerte können ausgewählt werden:
  - **User-Defined** - Gibt das benutzerdefinierte Leave-Zeitlimit an.
  - **Immediate Leave** - Gibt ein sofortiges Leave-Zeitlimit an.

Anzeigen der IGMP Snooping Table:

1. Öffnen Sie die Seite **IGMP Snooping**.
2. Klicken Sie auf **Show All**. Die **IGMP Snooping Table** wird geöffnet.



IGMP Snooping Table

Konfigurieren von IGMP-Snooping mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zur Konfiguration des IGMP-Snoopings zusammengefasst, das auf der Seite **IGMP Snooping** angezeigt wird.

CLI-Befehl	**Beschreibung**
ip igmp snooping	Aktiviert das IGMP-(Internet Group Management Protocol-)Snooping für ein spezifisches VLAN.
ip igmp snooping mrouter learn-pim-dvmrp	Aktiviert die automatische Erkennung von Multicast-Router-Anschlüssen innerhalb eines spezifischen VLAN-Kontexts.
ip igmp snooping host-time-out *Zeitlimit*	Konfiguriert das Host-Zeitlimit.
ip igmp snooping mrouter-time-out *Zeitlimit*	Konfiguriert das Multicast-Router-Zeitlimit.
ip igmp snooping leave-time-out {*Zeitlimit* **| immediate-leave}**	Konfiguriert das Leave-Zeitlimit.
show ip igmp snooping mrouter [interface *VLAN-ID***]**	Zeigt Informationen zu dynamisch erfassten Multicast-Router-Schnittstellen an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# interface vlan 2

Console (config-if)# ip igmp snooping

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 300

Console (config-if)# exit

Console (config)# interface vlan 2

Console (config-if)# ip igmp snooping leave-time-out 60

Console (config-if)# exit

Console (config)# exit
```

```
Console # show igmp snooping mrouter interface 1000

VLAN Ports

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

200 1/e1, 2/e1
```

Zurück zum Inhalt

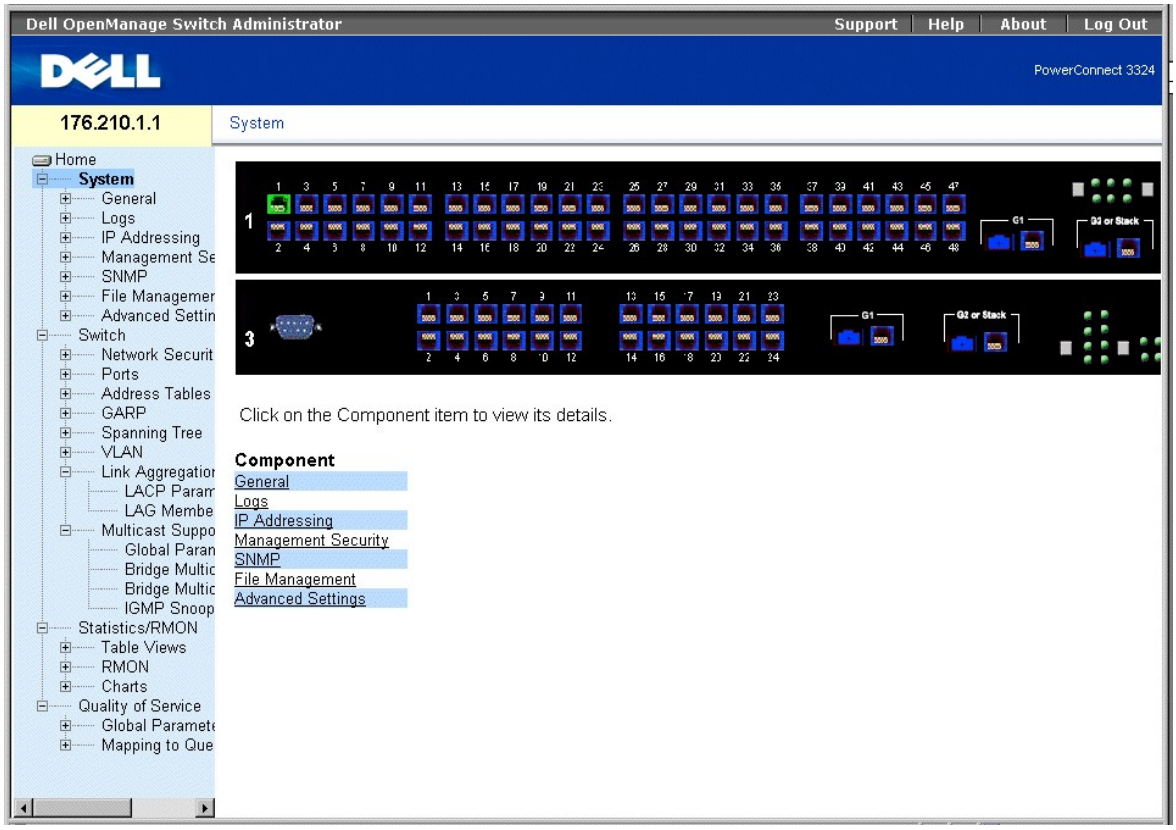
Zurück zum Inhalt

Konfigurieren von Systeminformationen

Dell™ PowerConnect™ 3324/3348 Benutzerhandbuch

Dieser Abschnitt bietet Informationen zur Definition von Systemparametern, einschließlich Sicherheitsfunktionen, zum Herunterladen von Gerätesoftware sowie zum Zurücksetzen des Gerätes. So öffnen Sie die Seite**System**:

- Klicken Sie in der Strukturansicht auf **System**. Die Seite **System** wird geöffnet.



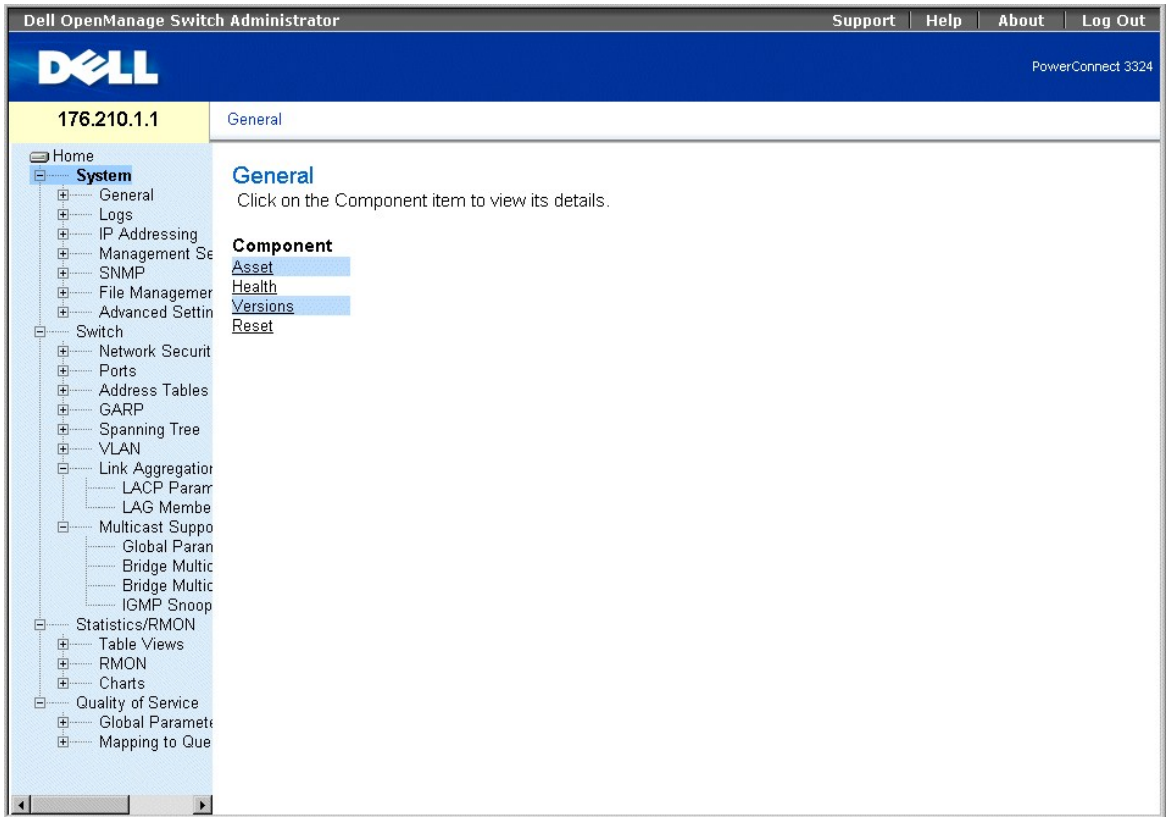
Seite "System"

Definieren allgemeiner Geräteinformationen

Die Seite **General** enthält Links zu Seiten, über die Netzwerkverwalter Geräteparameter konfigurieren können, darunter:

- Anzeigen der Seite "Asset"
- Anzeigen von Informationen zum Systemzustand

- Anzeigen der Seite "Versions"
- Zurücksetzen des Gerätes

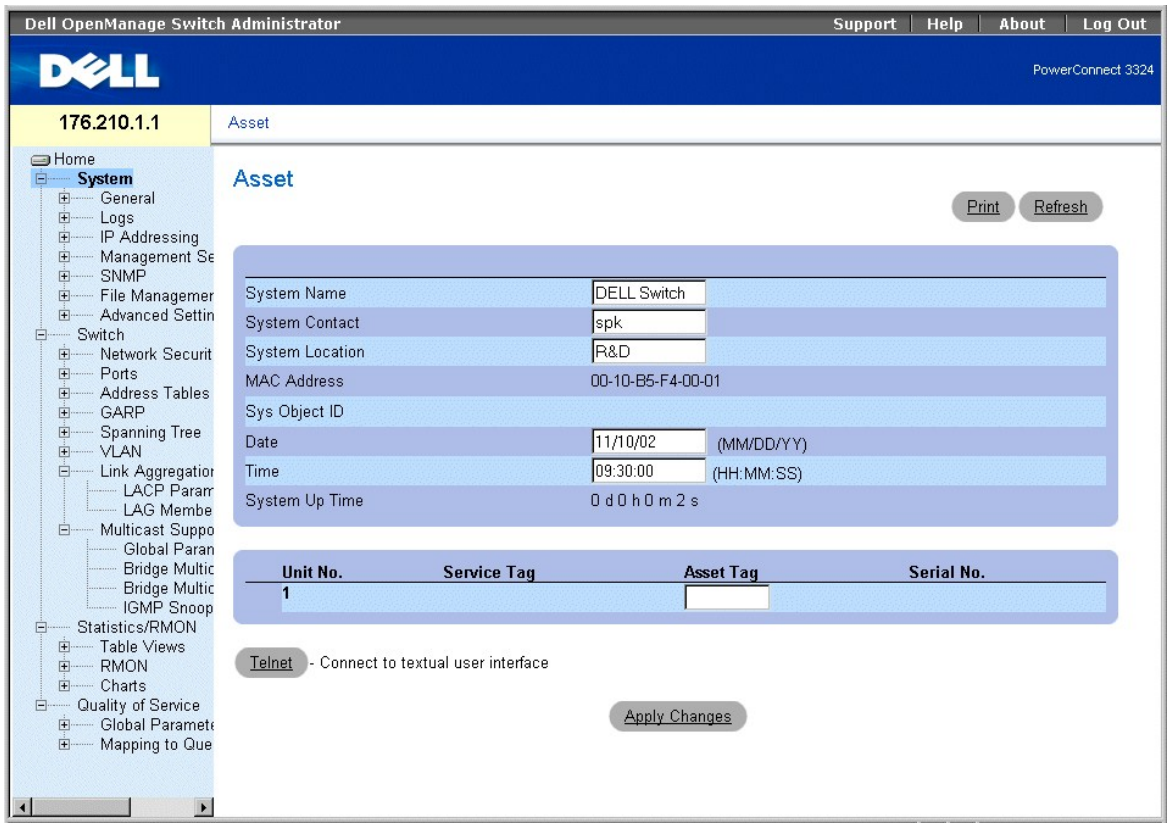


Seite "General"

Anzeigen der Seite "Asset"

Die Seite **Asset** enthält Parameter für die Konfiguration allgemeiner Geräteinformationen, einschließlich Systemname, -standort und -kontaktperson, MAC-Adresse und Objekt-ID des Systems sowie Datum, Uhrzeit und Systembetriebszeit. So öffnen Sie die Seite **Asset**:

- Klicken Sie in der Strukturansicht auf **System** > **General** > **Asset**. Die Seite**Asset** wird geöffnet.



Seite "Asset"

Die Seite **Asset** enthält folgende Felder:

- **System Name** - Gibt den benutzerdefinierten Gerätenamen an.
- **System Contact** - Legt den Namen der Kontaktperson fest.
- **System Location** - Gibt den Standort an, an dem das System derzeit betrieben wird.
- **MAC Address** - Legt die MAC-Adresse des Switches fest.
- **Sys Object ID** - Gibt die Objekt-ID der MIB an.
- **Date (MM/DD/YY)** - Gibt das aktuelle Datum an. Es wird im Format Monat, Tag, Jahr angezeigt. 11/10/02 entspricht beispielsweise dem 10. November 2002.
- **Time (HH:MM:SS)** - Legt die Uhrzeit fest. Sie wird im Format Stunde, Minute, Sekunde angezeigt. 20:12:03 entspricht beispielsweise zwölf Minuten und drei Sekunden nach zwanzig Uhr.
- **System Up Time** - Gibt die Gerätebetriebszeit seit dem letzten Zurücksetzen an. Die Systembetriebszeit wird im folgenden Format angezeigt: Tage, Stunden, Minuten und Sekunden, beispielsweise 41 Tage 2 Stunden 22 Minuten 15 Sekunden.
- **Unit No.** - Gibt die Nummer der Stack-Einheit an.
- **Service Tag** - Gibt die Wartungsreferenz des Geräts an.
- **Asset Tag** - Gibt die benutzerdefinierte Gerätereferenz an.
- **Serial No.** - Gibt die Seriennummer des Gerätes an.

Definieren von Systeminformationen:

1. Öffnen Sie die Seite **Asset**.
2. Definieren Sie die Felder **System Name**, **System Contact, System Location, Date, Asset Tag** und **Time**.
3. Klicken Sie auf **Apply Changes**. Die Systemparameter werden definiert und das Gerät aktualisiert.

Starten einer Telnet-Sitzung:

1. Öffnen Sie die Seite **Asset**.

2. Klicken Sie auf **Telnet**. Eine Telnet-Sitzung wird gestartet.

Konfigurieren von Geräteinformationen mit Hilfe der CLI-Befehle

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

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*	Fügt Informationen zum Gerätestandort ein.
clock set *hh:mm:ss Tag Monat Jahr*	Legt Systemuhrzeit und -datum manuell fest. Beachten Sie das abweichende Datumsformat.
show clock	Zeigt Uhrzeit und Datum der Systemuhr an.
show system id	Zeigt Informationen zur Wartungsreferenz an.
show system	Zeigt Systeminformationen an.
asset tag	Zeigt die benutzerdefinierte Gerätereferenz an.

Im Folgenden ein Beispiel für die CLI-Befehle:

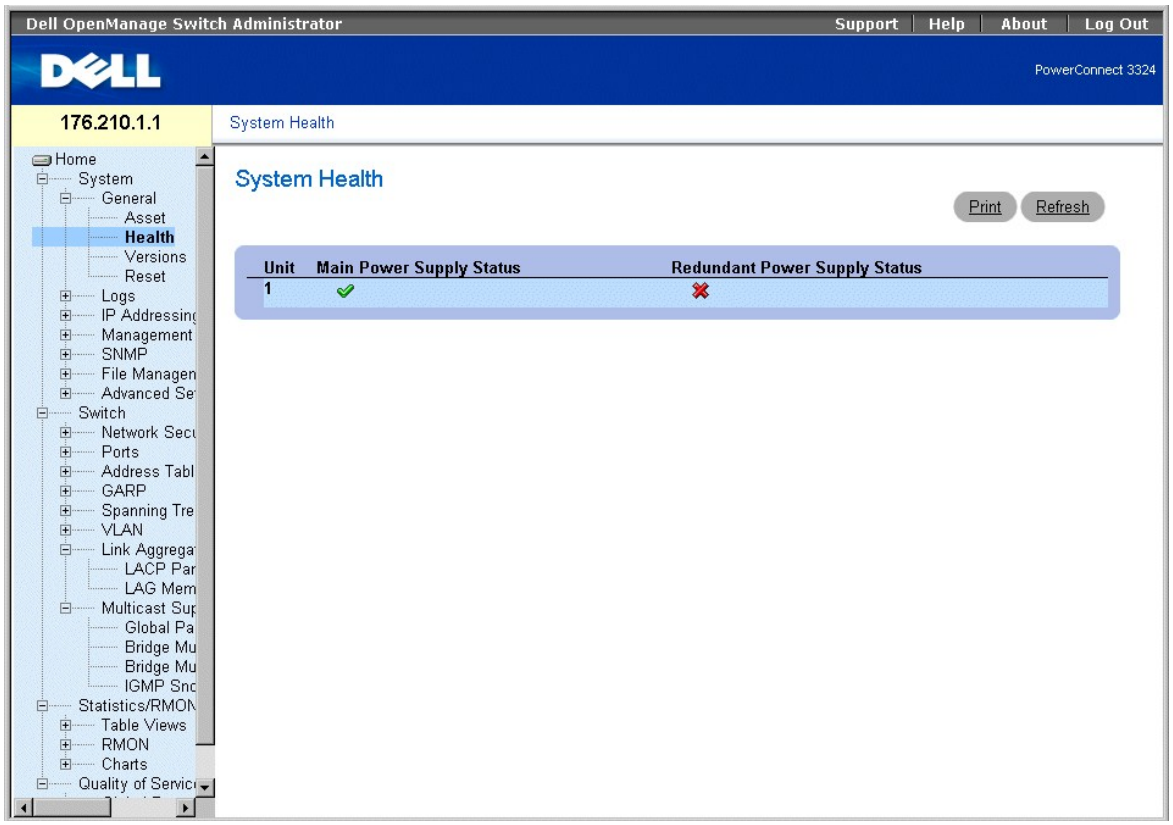
```
Console (config)# hostname dell

Console (config)# snmp-server contact Dell_Tech_Supp

Console (config)# snmp-server location New_York

Console (config)# exit

Console # exit

Console (config)# asset-tag lqwepot

Console> clock set 13:32:00 7 Mar 2002

Console> show clock

13:32:00 7 Mar 2002

console# show system

System Description: Ethernet Stackable Switching System

System Up Time (days,hour:min:sec): 0,00:30:58

System Contact : Dell_Tech_Supp
```

```
      System Name : Dell

      System Location : New_York

MAC Address: 00:00:b0:22:33:44

      Sys Object ID: 1.3.6.1.4.1.674.10895.3004

      Power supply Source Status

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

      Internal Power Supply Internal redundant OK unit1

      External Power Supply External OK unit1

      Internal PowerSupply Internal redundant OK unit2

      External PowerSupply External OK unit2

      Internal PowerSupply Internal redundant OK unit3

      External PowerSupply External OK unit3

      Internal PowerSupply Internal redundant OK unit6

      External PowerSupply External OK unit3
```

Anzeigen von Informationen zum Systemzustand

Die Seite **System Health** enthält Informationen zu physischer Gerätehardware. So öffnen Sie die Seite **System Health**:

- Klicken Sie in der Strukturansicht auf **System** > **General** > **Health**. Die Seite **System Health** wird geöffnet.



Seite "System Health"

Die Seite **System Health** enthält folgende Felder:

- **Unit** - Gibt die Nummer der Stack-Einheit an.
- **Main Power Supply Status** - Gibt den Zustand der Hauptstromversorgung an. Folgende Feldwerte sind möglich:
  -  - Gibt an, dass die Hauptstromversorgung der angegebenen Einheit ordnungsgemäß funktioniert.
  -  - Gibt an, dass die Hauptstromversorgung der angegebenen Einheit nicht ordnungsgemäß funktioniert.
  - **Not Present** - Gibt an, dass die Stromversorgung für das angegebene Gerät nicht vorhanden ist.
- **Redundant Power Supply Status** - Gibt den Zustand der redundanten Stromversorgung an. Folgende Feldwerte sind möglich:
  -  - Gibt an, dass die redundante Stromversorgung der angegebenen Einheit ordnungsgemäß funktioniert.
  -  - Gibt an, dass die redundante Stromversorgung der angegebenen Einheit nicht ordnungsgemäß funktioniert.
  - **Not Present** - Gibt an, dass diese Stromversorgung für das angegebene Gerät nicht vorhanden ist.

Anzeigen von Informationen zum Systemzustand mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
show system	Zeigt Systeminformationen an.

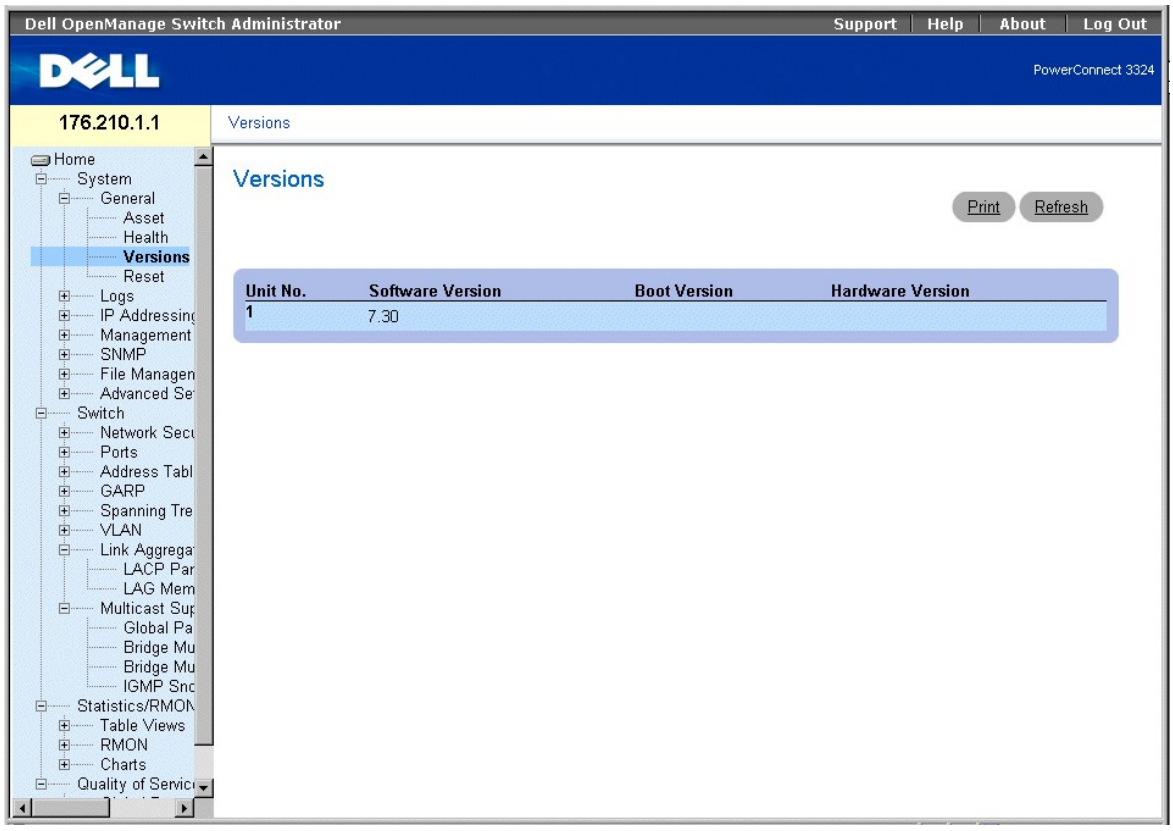
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console> show system

System Description: Ethernet Stackable Switching System

System Up Time (days,hour:min:sec): 0,00:08:56

System Contact : Dell_Tech_Supp

System Name : Dell

System Location : New_York
```

Anzeigen der Seite "Versions"

Die Seite **Versions** enthält Informationen zu den Versionen der derzeit ausgeführten Hardware und Software. So öffnen Sie die Seite **Versions**:

- Klicken Sie in der Strukturansicht auf **System** > **General** > **Versions**. Die Seite **Versions** wird geöffnet.



Seite "Versions"

Die Seite **Versions** enthält folgende Informationen:

- **Unit No.** - Gibt die Nummer der Stack-Einheit an.
- **Software Version** - Zeigt die Version der aktuellen, auf einer bestimmten Stack-Einheit ausgeführten Software an.
- **Boot Version** - Zeigt die aktuelle, auf einer bestimmten Stack-Einheit ausgeführte Startversion an.
- **Hardware Version** - Zeigt die Version der aktuellen, in einer bestimmten Stack-Einheit betriebenen Hardware an.

Anzeigen von Geräteversionen mit Hilfe der CLI-Befehle

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

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

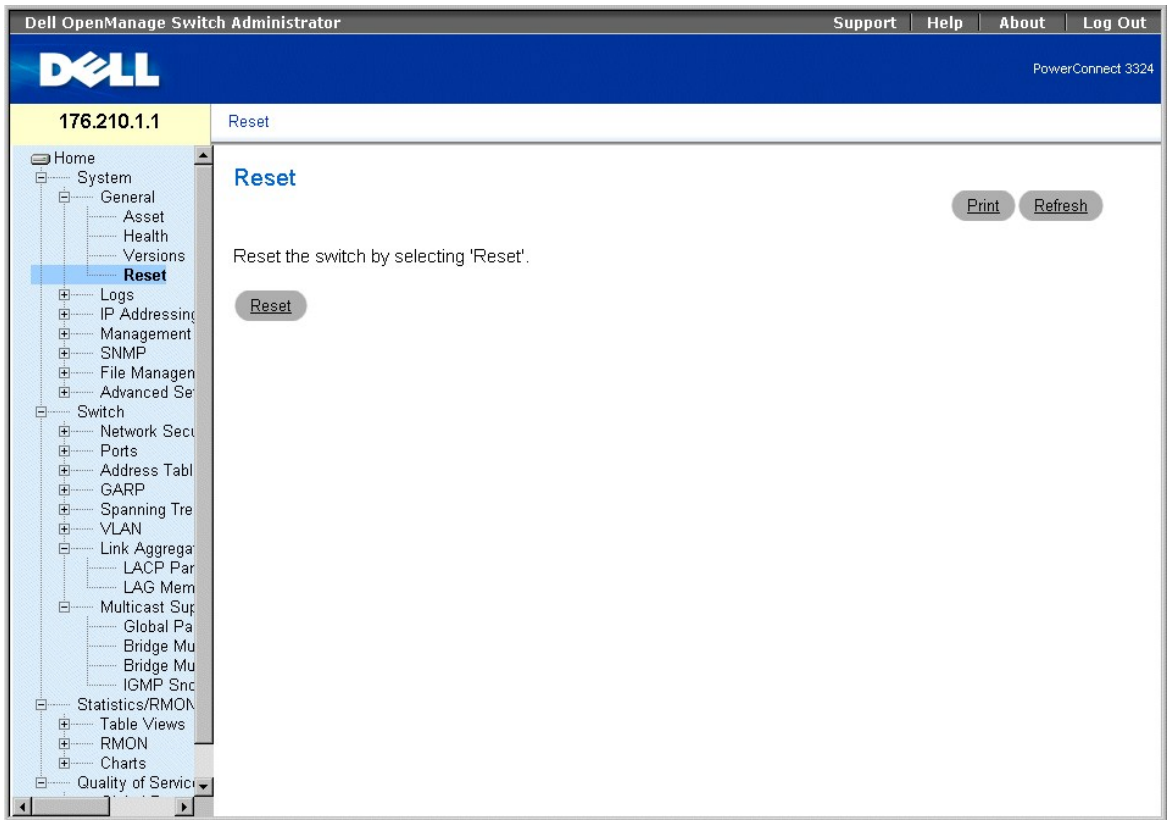
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console> show version

SW version 1.0.0.01 (date 14-Feb-2003 time 14:42:16 )

Boot version 1.30.11 ( date 27-Jan-2003 time 10:06:02 )

HW version 01.01.01
```

Zurücksetzen des Gerätes

Auf der Seite **Reset** können Benutzer das Gerät von einem Remote-Standort aus zurücksetzen. So öffnen Sie die Seite **Reset**:

- Klicken Sie in der Strukturansicht auf **System** > **General** > **Reset**. Die Seite **Reset** wird geöffnet.



Seite "Reset"

ANMERKUNG: Speichern Sie vor dem Zurücksetzen des Gerätes sämtliche Änderungen an der Datei **Running Configuration**, um zu verhindern, dass die aktuelle Gerätekonfiguration verloren geht. Weitere Informationen zum Speichern von Konfigurationsdateien finden Sie unter "Verwalten von Dateien".

Zurücksetzen des Gerätes:

1. Öffnen Sie die Seite **Reset.**
2. Klicken Sie auf **Reset**. Eine Bestätigungsmeldung wird angezeigt:

Bestätigungsmeldung zum Zurücksetzen des Gerätes

3. Klicken Sie auf **OK**. Das Gerät wird zurückgesetzt. Nachdem das Gerät zurückgesetzt wurde, wird der Benutzer aufgefordert, Benutzernamen und Passwort anzugeben.

Zurücksetzen des Gerätes mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
reload	Lädt das Betriebssystem neu.

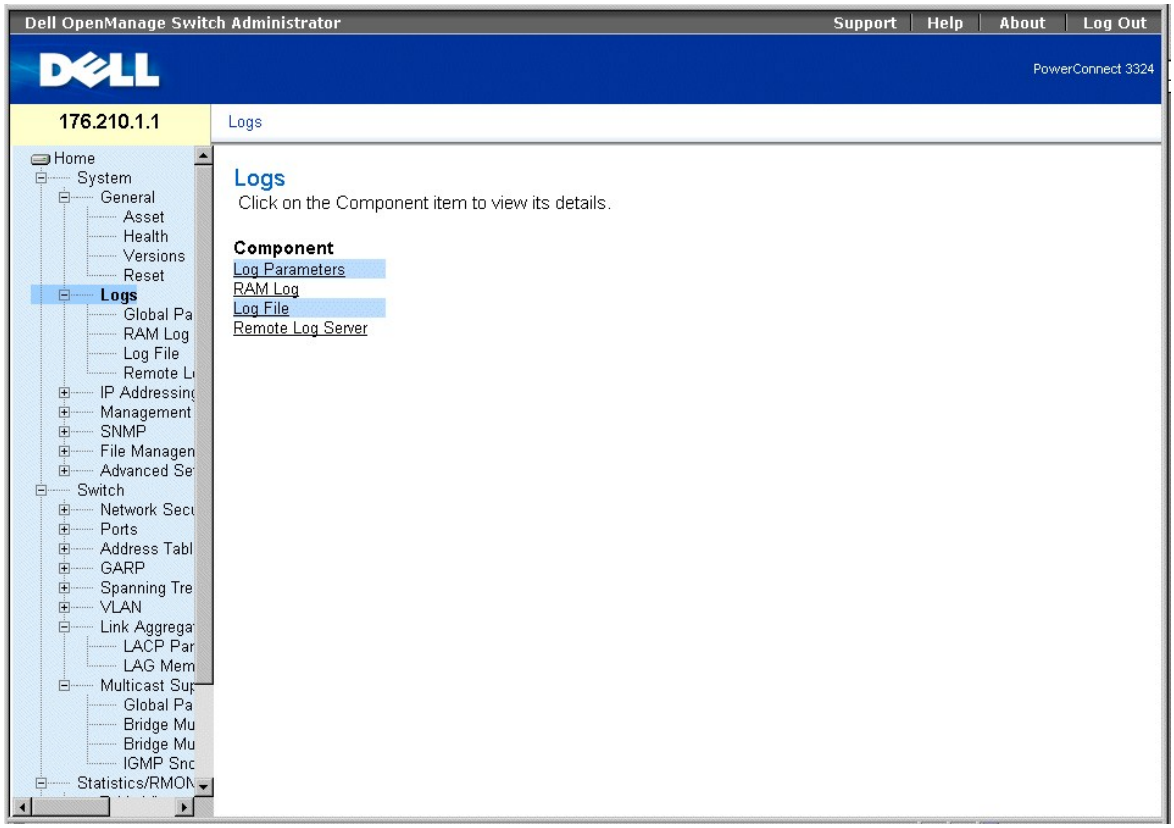
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console >reload

This command will reset the whole system and disconnect your current

session. Do you want to continue (y/n) [n]?
```

Verwalten von Protokollen

Die Seite **Logs** enthält Links zu verschiedenen Protokollseiten. So öffnen Sie die Seite **Logs**:

- Klicken Sie in der Strukturansicht auf **System** > **Logs**. Die Seite **Logs** wird geöffnet.



Seite "Logs"

Die Seite **Logs** enthält Links zu folgenden Seiten:

- Definieren globaler Protokollparameter
- Anzeigen der "RAM Log Table"
- Anzeigen der "Log File Table"
- Anzeigen der Seite "Remote Log Server Settings"

Definieren globaler Protokollparameter

Mit Hilfe des Systemprotokolls können Sie signifikante Ereignisse in Echtzeit anzeigen lassen und diese Ereignisse zur späteren Verwendung aufzeichnen. Diese Funktion bietet die Möglichkeit, Ereignisse zu protokollieren und zu verwalten sowie Fehlerberichte zu erstellen.

Ereignismeldungen verfügen gemäß RFC-Empfehlung für die gesamte Fehlerberichterstellung über ein eindeutiges SYSLOG-Meldungsformat, z. B. "Syslog+ lokaler Gerätebericht". Meldungen wird ein Schweregrad-Code sowie ein mnemonisches Zeichen zugewiesen, durch das die Quellanwendung identifiziert wird, von der die Meldung ausgegeben wurde. Die Meldungen werden auf der Grundlage ihrer Dringlichkeit bzw. Wichtigkeit gefiltert. Der Schweregrad der jeweiligen Meldung legt fest, an welche Gruppe von Ereignisprotokollgeräten die Meldungen für die einzelnen Ereignisprotokollgeräte gesendet werden. In der folgenden Tabelle sind die Schweregrade von Protokollen aufgeführt:

Schweregrade von Protokollen

Art des Schweregrads	Schweregrad	Beschreibung
Emergency	0	Gibt an, dass das System nicht funktionsfähig ist.
Warnung	1	Gibt an, dass das System umgehend gewartet werden muss.
Kritisch	2	Gibt an, dass sich das System in einem kritischen Zustand befindet.
Fehler	3	Deutet auf einen Systemfehler hin.
Warning	4	Deutet auf eine Systemwarnung hin.
Notice	5	Gibt an, dass das System ordnungsgemäß arbeitet, jedoch eine Systemmeldung ausgegeben wurde.
Informativ	6	Zeigt Geräteinformationen an.
Debug	7	Zeigt ausführliche Informationen zum Protokoll an.

The **Global Log Parameters** page enables you to define which events are recorded to which logs. Die Seite **Global Log Parameters** enthält Felder, mit denen Protokolle global aktiviert werden können sowie Parameter für die Definition von Protokollparametern. Die unter dem Schweregrad aufgeführten Protokollmeldungen sind vom höchsten bis zum niedrigsten Schweregrad angeordnet. So öffnen Sie die Seite **Global Log Parameters**:

- Klicken Sie in der Strukturansicht auf **System** > **Logs** > **Global Parameters**. Die Seite **Global Log Parameters** wird geöffnet.

Seite "Global Log Parameters"

Die Seite **Global Log Parameters** enthält folgende Felder:

- **Logging** - Ermöglicht die Erstellung globaler Geräteprotokolle in Form von Cache-, Datei- und Serverprotokollen. Konsolenprotokolle sind standardmäßig aktiviert und können nicht deaktiviert werden. Folgende Feldwerte sind möglich:
  - **Enable** - Aktiviert die Speicherung von Protokollen im Cache (RAM), in Dateien (FLASH) sowie auf einem externen Server.
  - **Disable** - Deaktiviert die Protokollspeicherung. Konsolenprotokolle können nicht deaktiviert werden.
- **Severity** - Die folgenden Schweregrade sind für Protokolle verfügbar:
  - **Emergency** - Stellt die höchste Warnstufe dar. Falls keine Verbindung zum Gerät besteht oder das Gerät nicht ordnungsgemäß funktioniert, wird eine Notfall-Protokollmeldung am angegebenen Protokollspeicherort gespeichert.
  - **Alert** - Stellt die zweithöchste Warnstufe dar. Ein Warnprotokoll wird bei einem schwerwiegenden Geräteausfall gespeichert, beispielweise wenn sämtliche Gerätefunktionen ausfallen.
  - **Critical** - Stellt die dritthöchste Warnstufe dar. Ein kritisches Protokoll wird bei einem Geräteausfall gespeichert, beispielsweise wenn zwei Geräteanschlüsse nicht arbeiten, während die übrigen Anschlüsse weiterhin funktionsfähig sind.
  - **Error** - Gibt an, dass ein Gerätefehler aufgetreten ist, beispielsweise wenn ein einzelner Anschluss offline geschaltet ist.
  - **Warning** - Entspricht der niedrigsten Gerätewarnstufe. Das Gerät funktioniert zwar, bei seinem Betrieb ist jedoch ein Problem aufgetreten.
  - **Notice** - Liefert dem Netzwerkadministrator Geräteinformationen.
  - **Informational** - Zeigt Geräteinformationen an.
  - **Debug** - Zeigt ausführliche Informationen zum Protokoll an. Falls ein Debug-Fehler auftritt, wenden Sie sich an den technischen Online-Support von Dell (**www.support.euro.dell.com**).

ANMERKUNG: Bei Auswahl eines Schweregrades werden alle über dieser Auswahl befindlichen Schweregrade automatisch mit aktiviert.

Die Seite **Global Log Parameters** enthält zusätzlich Kontrollkästchen, die jeweils einem bestimmten Protokollierungssystem entsprechen:

- **Console** - Gibt den geringsten Schweregrad an, bei dessen Auftreten Protokolle an die Konsole gesendet werden.
- **RAM Logs** - Gibt den geringsten Schweregrad an, bei dessen Auftreten Protokolle an die im RAM (Cache) enthaltene Protokolldatei gesendet werden.
- **Log File** - Gibt den geringsten Schweregrad an, bei dessen Auftreten Protokolle an die im FLASH-Speicher enthaltene Protokolldatei gesendet werden.

Aktivieren von Protokollen:

1. Öffnen Sie die Seite **Global Log Parameters**.
2. Wählen Sie **Enable** in der Dropdown-Liste **Logging**.
3. Wählen Sie mit Hilfe der Kontrollkästchen unter**Global Log Parameters** Protokolltyp und Protokollschweregrad aus.
4. Klicken Sie auf **Apply Changes**. Die Protokolleinstellungen werden gespeichert und das Gerät aktualisiert.

Aktivieren von Protokollen mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
logging on	Aktiviert die Protokollierung von Fehlermeldungen.
logging IP-Adresse [port Port] [severity Schweregrad] [facility Anlage] [description Text]	Protokolliert Meldungen auf einem Syslog-Server. Eine Liste der Schweregrade finden Sie unter "Schweregrade von Protokollen".
logging console Schweregrad	Beschränkt die Protokollierung auf der Konsole auf Fehlermeldungen des angegebenen Schweregrads.
logging buffered Schweregrad	Beschränkt die Anzeige von Syslog-Meldungen aus einem internen Pufferspeicher (RAM) auf Meldungen des angegebenen Schweregrads.
logging file Schweregrad	Beschränkt das Senden von Syslog-Meldungen an die Protokolldatei auf Meldungen des angegebenen Schweregrads.
clear logging	Löscht den Protokollinhalt.

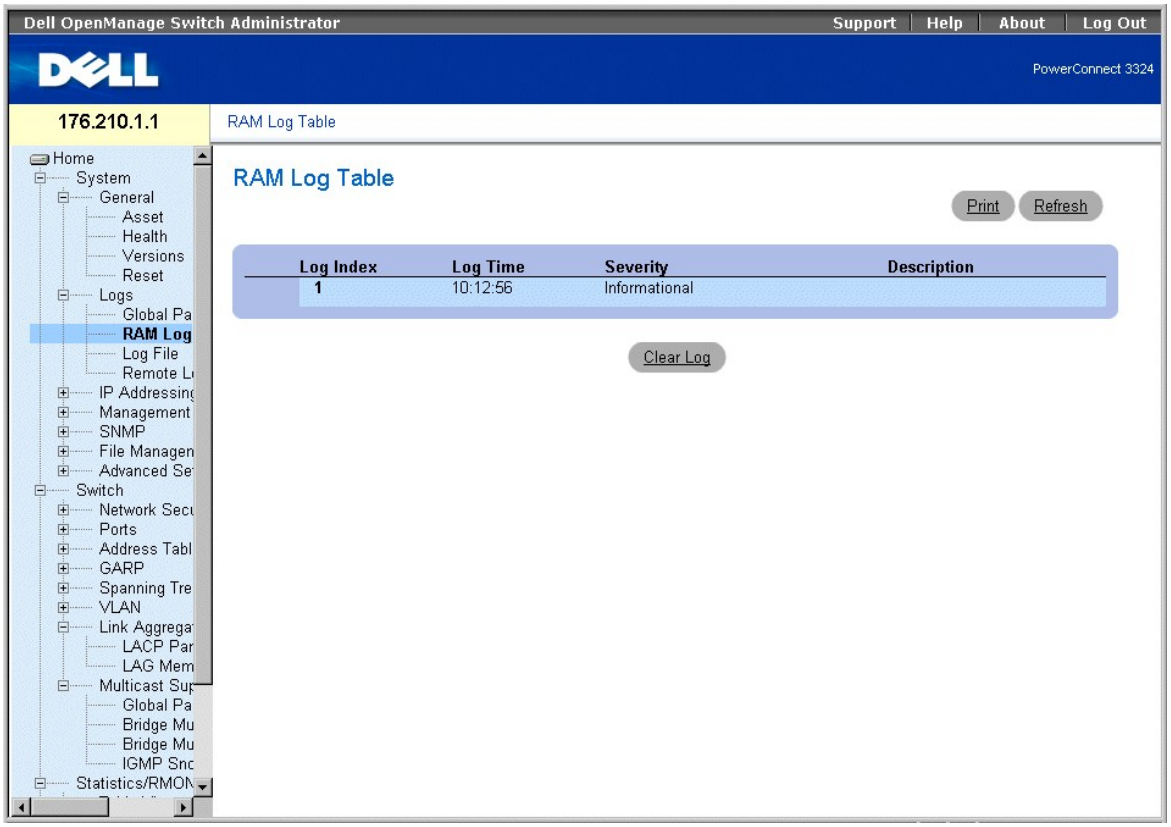
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# logging on

Console (config)# logging console errors

Console (config)# logging buffered debugging

Console (config)# logging file alerts

Console (config)# clear logging
```

Anzeigen der "RAM Log Table"

Die **RAM Log Table** enthält Informationen zu Protokolleinträgen im RAM, einschließlich der Uhrzeit, zu der das Protokoll aufgezeichnet wurde, des Protokollschweregrads sowie einer Beschreibung des Protokolls. So öffnen Sie die Seite **RAM Log Table**:

- Klicken Sie in der Strukturansicht auf **System** > **Logs** > **RAM Log**. Die Seite **RAM Log Table** wird geöffnet.



Seite "RAM Log Table"

Die Seite **RAM Log Table** enthält folgende Felder:

- **Log Index** - Gibt die Protokollnummer in der **RAM Log Table** an.
- **Log Time** - Gibt die Uhrzeit an, zu der das Protokoll in die **RAM Log Table** eingefügt wurde.
- **Severity** - Gibt den Schweregrad des Protokolls an.
- **Description** - Zeigt die benutzerdefinierte Protokollbeschreibung an.

Entfernen von Protokollinformationen:

1. Öffnen Sie die Seite **RAM Log Table**.
2. Klicken Sie auf **Clear Log**. Die Protokollinformationen werden aus der **RAM Log Table/Log File Table** entfernt und das Gerät aktualisiert.

Anzeigen der "RAM Log Table" mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
show logging	Zeigt den Protokollierungsstatus und die im internen Pufferspeicher enthaltenen Syslog-Meldungen an.
clear logging	Löscht den Protokollinhalt.

Im Folgenden ein Beispiel für die CLI-Befehle:

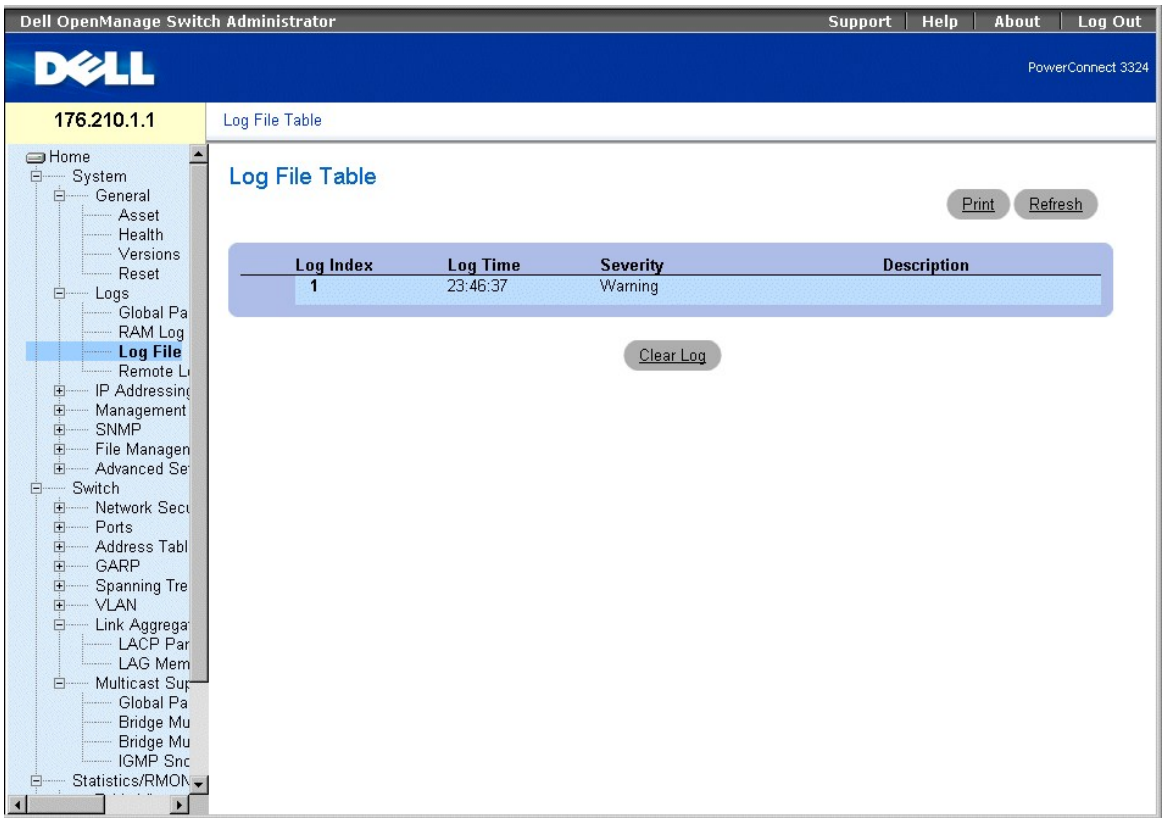
```
Console # show logging

Console logging: level debugging. Console Messages: 0 Dropped (severity).

Buffer logging: level debugging. Buffer Messages: 11 Logged, 200 Max.

File logging: level notifications. File Messages: 0 Dropped (severity).

Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped (severity).

Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped (severity).

2 messages were not logged (resources)

Buffer log:

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e0, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e1, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e2, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e3, changed state to up

11-Aug-2002 15:41:43: %SYS-5-CONFIG_I: Configured from memory by console
```

```
11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e0, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e1, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e2, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e3, changed state to down

Console # clear logging

clear logging buffer [confirm]

Console#



Console # clear logging file

clear logging buffer [confirm]

Console#
```

Anzeigen der "Log File Table"

Die **Log File Table** enthält Informationen zu Protokolleinträgen, die in der Protokolldatei im FLASH-Speicher abgelegt wurden, einschließlich der Uhrzeit, zu der das Protokoll aufgezeichnet wurde, des Protokollschweregrads sowie einer Beschreibung der Protokollmeldung. So öffnen Sie die Seite **Log File Table**:

- Klicken Sie in der Strukturansicht auf **System** > **Logs** > **Log File**. Die Seite **Log File Table** wird geöffnet.



Log File Table

Die **Log File Table** enthält folgende Felder:

- **Log Index** - Gibt die Protokollnummer in der **Log File Table** an.
- **Log Time** - Gibt die Uhrzeit an, zu der das Protokoll in die **Log File Table** eingefügt wurde.
- **Severity** - Gibt den Schweregrad des Protokolls an.
- **Description** - Zeigt den Text der Protokollmeldung an.

Anzeigen der "Log File Table" mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
show logging file	Zeigt den Protokollierungsstatus und die in der Protokolldatei enthaltenen Syslog-Meldungen an.
clear logging	Löscht sämtliche Protokolldateien.

Im Folgenden ein Beispiel für die CLI-Befehle:

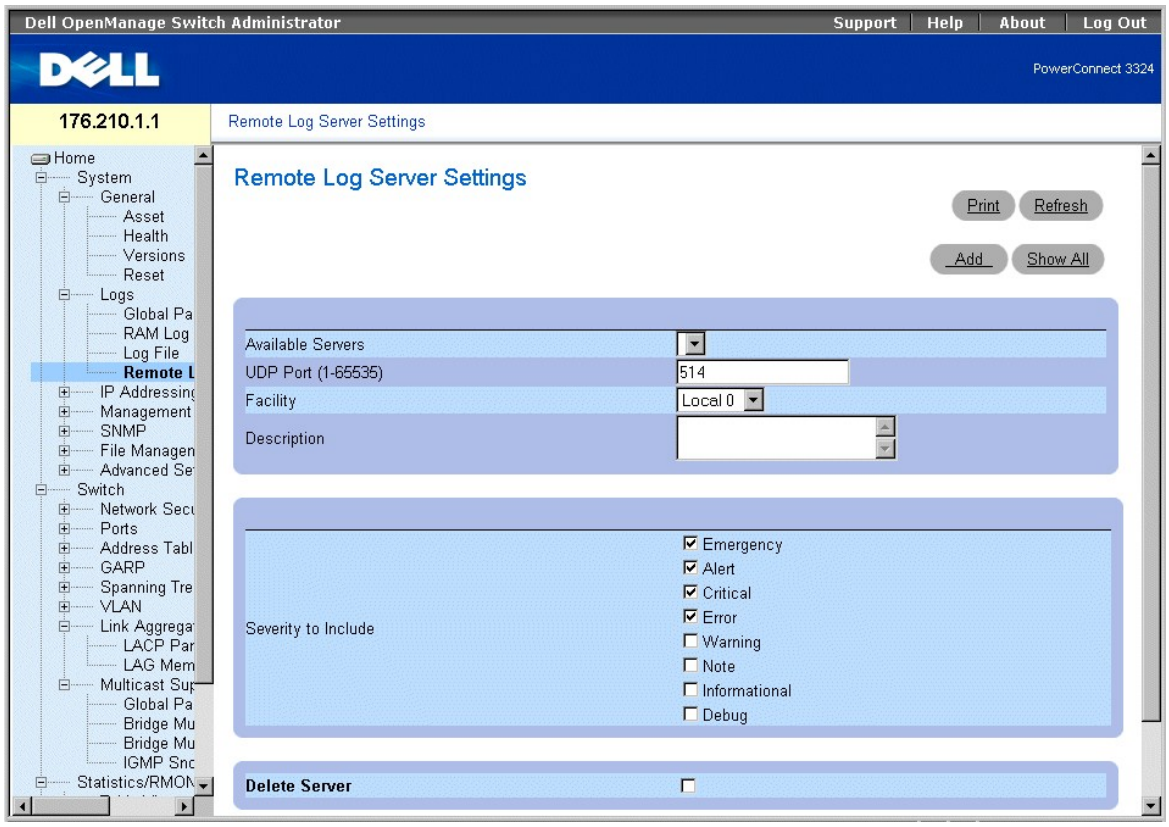
```
Console # show logging file

Console logging: level debugging. Console Messages: 0 Dropped (severity).
```

```
Buffer logging: level debugging. Buffer Messages: 11 Logged, 200 Max.

File logging: level notifications. File Messages: 0 Dropped (severity).

Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped (severity).

Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped (severity).

2 messages were not logged (resources)

File log:

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e0, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e1, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e2, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e3, changed state to up

11-Aug-2002 15:41:43: %SYS-5-CONFIG_I: Configured from memory by console

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e0, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e1, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e2, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e3, changed state to down
```

Anzeigen der Seite "Remote Log Server Settings"

Die Seite **Remote Log Server Settings** enthält Felder zur Anzeige der verfügbaren Protokollserver. Außerdem können neue Protokollserver und der Schweregrad der an die einzelnen Server gesendeten Protokolle definiert werden. So öffnen Sie die Seite **Remote Log Server Settings**:

- Klicken Sie in der Strukturansicht auf **System** > **Logs** > **Remote Log Server**. Die Seite **Remote Log Server Settings** wird geöffnet.



Seite "Remote Log Server Settings"

Die Seite **Remote Logs Server Settings** enthält folgende Felder:

- **Available Servers** - Enthält eine Liste der Server, an die Protokolle gesendet werden können.
- **UDP Port (1-65535)** - Gibt den UDP-Anschluss an, an den die Protokolle für den jeweiligen Server gesendet werden. Der zulässige Bereich liegt zwischen 1 und 65.535. Der Standardwert lautet 514.
- **Facility** - Gibt die Anlagenzuweisungsebene für den ausgewählten Server an. Der Standardwert lautet "Local 0". Die möglichen Werte sind:
  - **Local 0 - Local 7.**
  - **No Map.**
- **Description** - Zeigt die benutzerdefinierte Serverbeschreibung an.
- **Delete Server** - Löscht den derzeit ausgewählten Server aus der Liste **Available Servers**. Folgende Feldwerte sind möglich:
  - **Aktiviert** - Löscht den Server aus der Liste **Available Servers**.
  - **Deaktiviert** - Behält den Server in der Liste **Available Servers** bei.

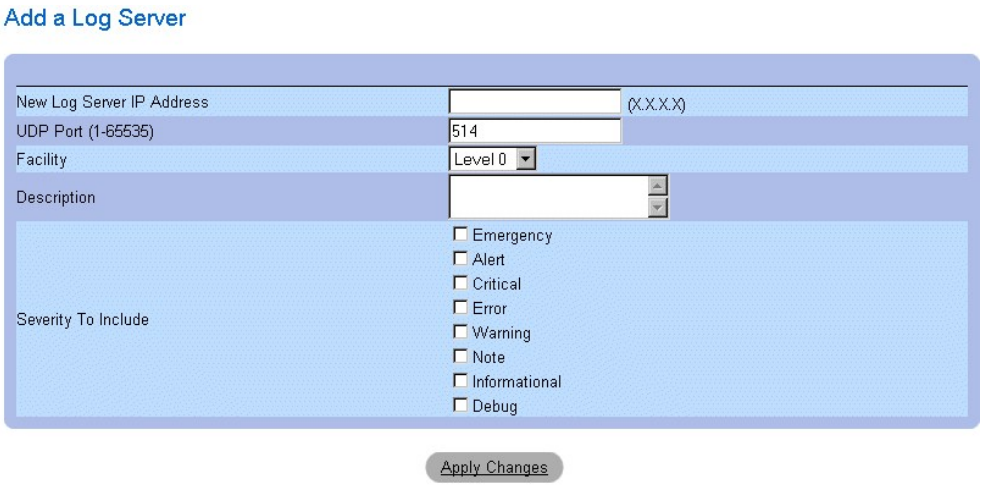
Darüber hinaus enthält die Seite **Remote Logs Server Settings** eine Liste der Schweregrade. Die Definitionen der Schweregrade sind identisch mit denen auf der Seite "Seite "Global Log Parameters"".

Senden von Protokollen an einen Server:

1. Öffnen Sie die Seite **Remote Logs Server Settings**.
2. Wählen Sie einen Server aus der Dropdown-Liste **Available Servers** aus.
3. Definieren Sie die Felder **UDP Port**, **Facility** und **Description**.
4. Wählen Sie mit Hilfe der Kontrollkästchen **Severity to Include** den Protokollschweregrad aus.
5. Klicken Sie auf **Apply Changes**. Die Protokolleinstellungen werden gespeichert und das Gerät aktualisiert.

Definieren eines neuen Servers:

1. Öffnen Sie die Seite **Remote Logs Server Settings**.
2. Klicken Sie auf **Add**. Die Seite **Add a Log Server** wird geöffnet.



Seite "Add a Log Server"

Neben den auf der Seite **Remote Logs Server Settings** verfügbaren Feldern enthält die Seite **Add a Log Server** folgendes Feld:

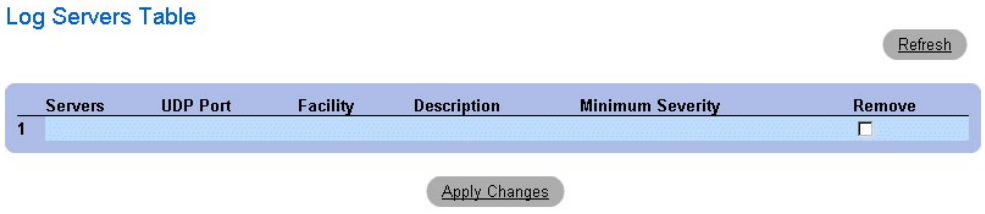
- **New Log Server IP Address** - Gibt die IP-Adresse des neuen Protokollservers an.

So fügen Sie einen Protokollserver hinzu:

1. Definieren Sie die Felder **New Log Server IP Address, UDP Port, Facility** und **Description,** und aktivieren Sie die Kontrollkästchen unter **Severity to Include**.
2. Klicken Sie auf **Apply Changes**. Der Server wird definiert und der Liste **Available Servers** hinzugefügt.

Anzeigen der "Log Servers Table":

1. Öffnen Sie die Seite **Remote Logs Server Settings**.
2. Klicken Sie auf **Show All**. Die Seite **Log Servers Table** wird geöffnet.



Seite "Log Servers Table"

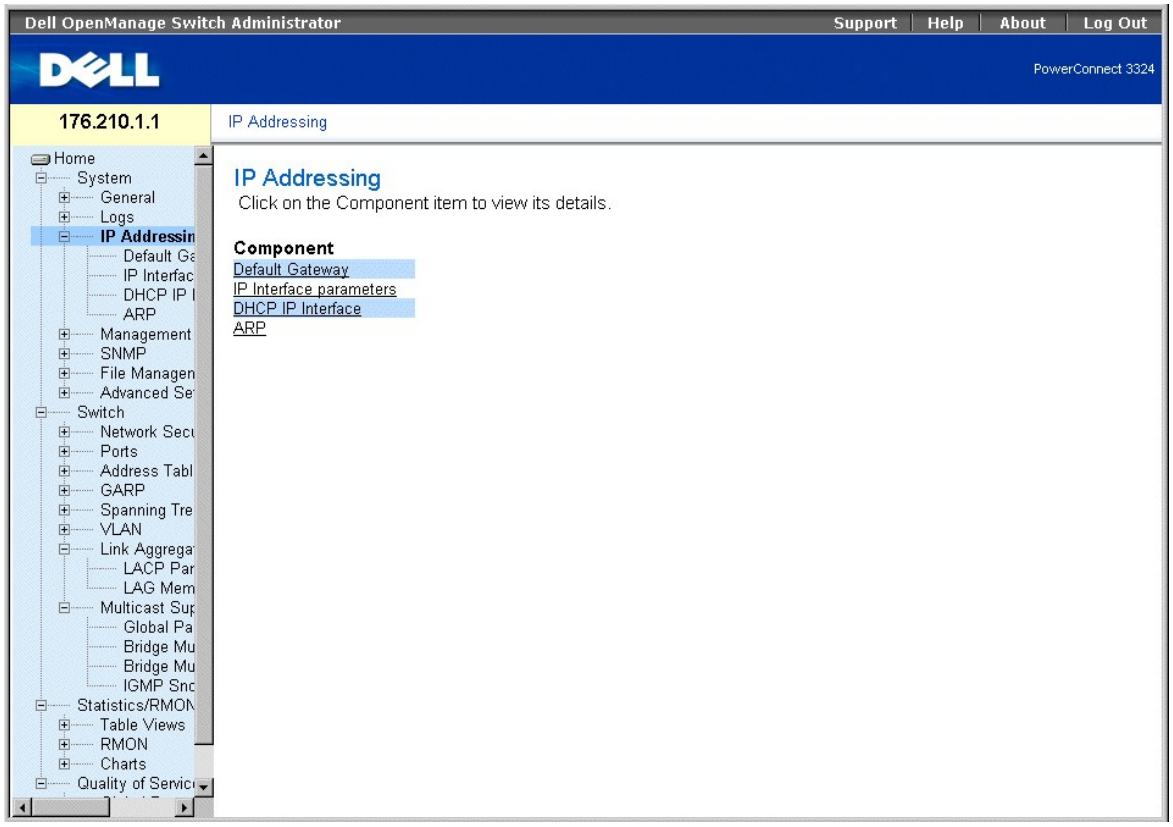
Entfernen eines Protokollservers von der Seite **Log Servers Table**:

1. Öffnen Sie die Seite **Remote Logs Server Settings**.
2. Klicken Sie auf **Show All**. Die Seite **Log Servers Table** wird geöffnet.
3. Wählen Sie einen Eintrag in der **Log Servers Table** aus.
4. Aktivieren Sie das Kontrollkästchen **Remove**, um den/die Server zu entfernen.
5. Klicken Sie auf **Apply Changes**. Der Eintrag in der **Log Servers Table** wird entfernt und das Gerät aktualisiert.

Definieren von IP-Geräteadressen

Die Seite **IP Addressing** enthält Links, über die Schnittstellen- und Standardgateway-IP-Adressen zugewiesen sowie ARP- und DHCP-Parameter für die Schnittstellen definiert werden können. So öffnen Sie die Seite **IP Addressing**:

- Klicken Sie in der Strukturansicht auf **System** > **IP Addressing**. Die Seite **IP Addressing** wird geöffnet.



Seite "IP Addressing"

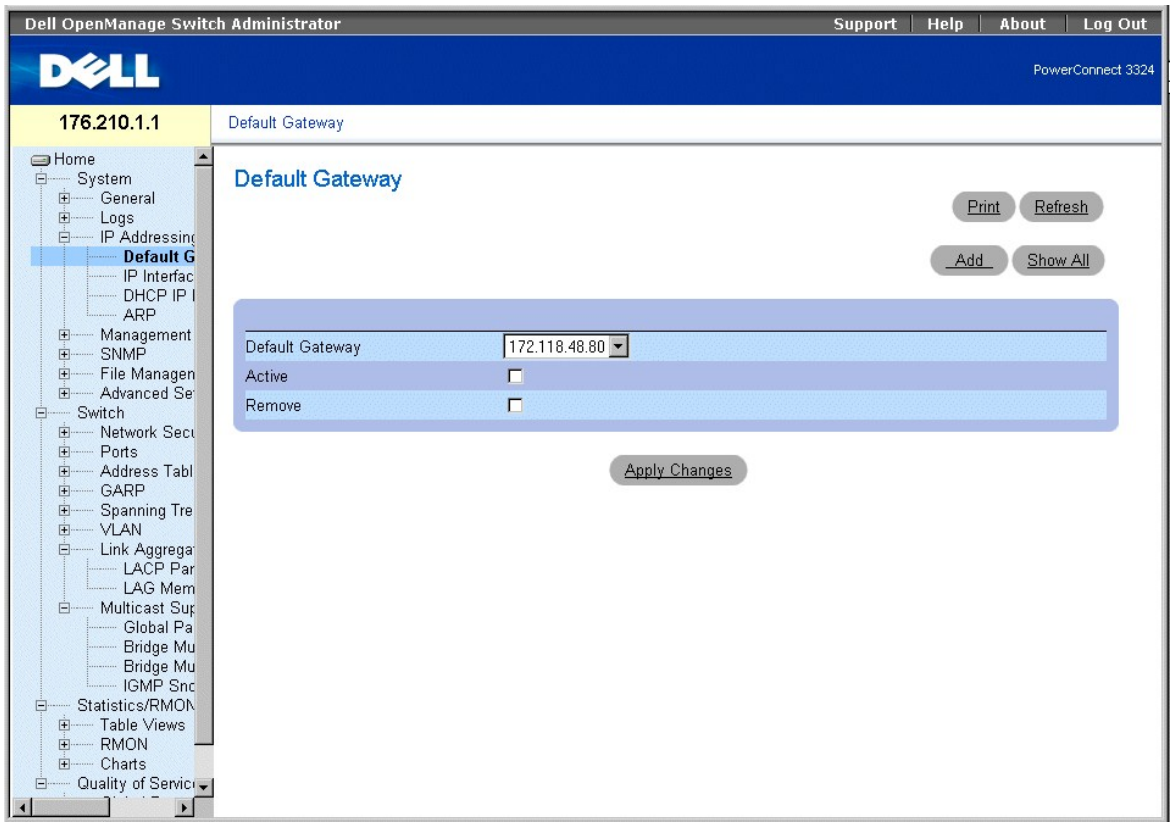
Die Seite **IP Addressing** enthält Links zu folgenden Seiten:

- Definieren von Standardgateways
- Definieren von IP-Schnittstellen
- Definieren von DHCP IP-Schnittstellen
- Konfigurieren von ARP

Definieren von Standardgateways

Die Seite **Default Gateway** ermöglicht Netzwerkverwaltern das Zuweisen von Gatewaygeräten. Pakete werden an die IP-Standardadresse weitergeleitet, wenn Frames an ein Remote-Netzwerk gesendet werden. Die konfigurierte IP-Adresse muss dem IP-Adressen-Subnetz einer der IP-Schnittstellen angehören. So öffnen Sie die Seite **Default Gateway** :

- Klicken Sie in der Strukturansicht auf **System** > **IP Addressing** > **Default Gateway**. Die Seite **Default Gateway** wird geöffnet.



Seite "Default Gateway"

Die Seite **Default Gateway** enthält folgende Felder:

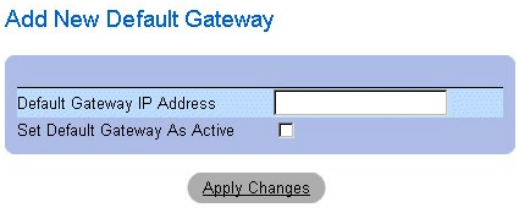
- **Default Gateway** - Gibt die IP-Adresse des Gatewaygerätes an.
- **Active** - Gibt an, ob das in der Dropdown-Liste **Default Gateway** angegebene Standardgatewaygerät derzeit aktiv ist. Folgende Feldwerte sind möglich:
  - **Aktiviert** - Gibt an, dass das Gatewaygerät momentan aktiv ist.
  - **Deaktiviert** - Gibt an, dass das Gatewaygerät momentan nicht aktiv ist.
- **Remove** - Entfernt Gatewaygeräte aus der Dropdown-Liste **Default Gateway**.
  - **Aktiviert** - Entfernt die ausgewählten Gatewaygeräte aus der Dropdown-Liste **Default Gateway.**
  - **Deaktiviert** - Behält Gatewaygeräte in der Dropdown-Liste **Default Gateway** bei.

Auswählen eines Gatewaygerätes:

1. Öffnen Sie die Seite **Default Gateway.**
2. Wählen Sie in der Dropdown-Liste **Default Gateway** eine IP-Adresse aus.
3. Aktivieren Sie das Kontrollkästchen **Active**.
4. Klicken Sie auf **Apply Changes.** Das Gatewaygerät wird ausgewählt und sein Status im Feld **Active** angezeigt.

Hinzufügen eines Gatewaygerätes:

1. Öffnen Sie die Seite **Default Gateway**.
2. Klicken Sie auf **Add**. Die Seite **Add New Default Gateway** wird geöffnet.



Hinzufügen eines neuen Standardgateways

3. Definieren Sie das Feld **Default Gateway IP Address**.

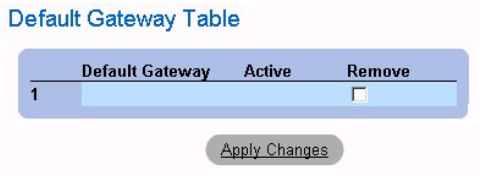
   ODER

   Legen Sie das neue Gateway durch Aktivieren des entsprechenden Kontrollkästchens als aktiv fest.

4. Klicken Sie auf **Apply Changes**. Das neue Gatewaystandardgerät wird definiert und das Gerät aktualisiert.

Anzeigen der "Default Gateway Table":

1. Öffnen Sie die Seite **Default Gateway**.
2. Klicken Sie auf **Show All**. Die **Default Gateway Table** wird geöffnet.



Seite "Default Gateway Table"

Entfernen eines Standardgatewaygerätes:

1. Öffnen Sie die Seite **Default Gateway**.
2. Klicken Sie auf **Show All**. Die Seite **Default Gateway Table** wird geöffnet.
3. Wählen Sie einen Eintrag in der **Default Gateway Table** aus.
4. Aktivieren Sie das Kontrollkästchen **Remove**, um Standardgateways zu entfernen.
5. Klicken Sie auf **Apply Changes**. Der Eintrag in der Default Gateway Table wird entfernt und das Gerät aktualisiert.

Definieren von Gatewaygeräten mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
ip default-gateway ip-address1 [ip-address2.]	Definiert ein Standardgateway.
no ip default-gateway [ip-address]	Entfernt ein Standardgateway.

Im Folgenden ein Beispiel für die CLI-Befehle:

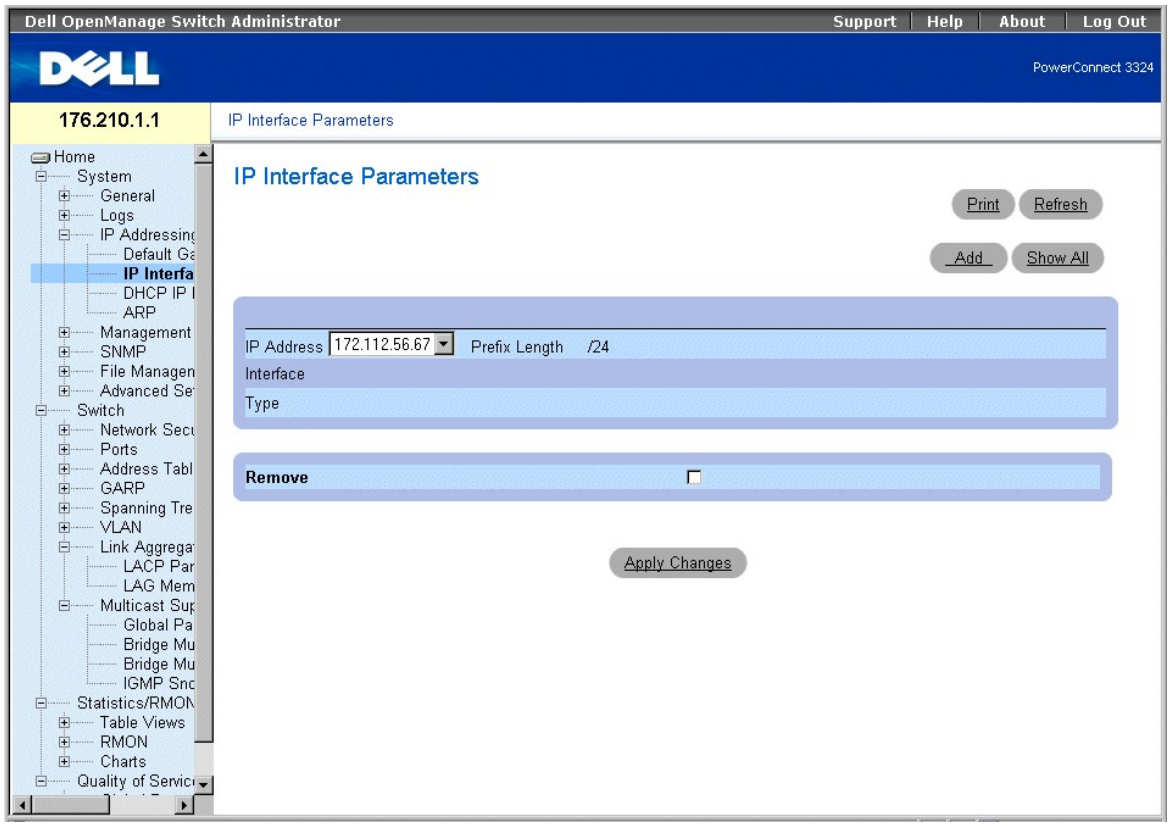
```
Console (config)# ip default-gateway 196.210.10.1
```

```
Console (config)# no ip default-gateway 196.210.10.1
```

Definieren von IP-Schnittstellen

Die Seite **IP Interface Parameters** enthält Parameter zum Zuweisen von IP-Adressen zu Schnittstellen. So öffnen Sie die Seite **IP Interface Parameters**:

- Klicken Sie in der Strukturansicht auf **System** > **IP Addressing** > **IP Interface Parameters**. Die Seite **IP Interface Parameters** wird geöffnet.



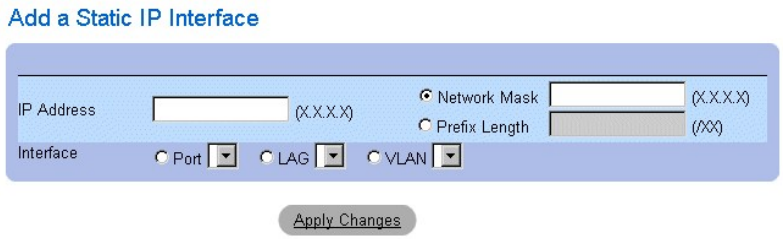
Seite "IP Interface Parameters"

Die Seite **IP Interface Parameters** enthält folgende Felder:

- **IP Address** - Gibt die Liste der IP-Schnittstellenadressen an.
- **Interface** - Legt den Schnittstellentyp fest, für den die ausgewählte IP-Adresse definiert ist. Folgende Feldwerte sind möglich:
  - **Port** - Gibt an, dass die IP-Adresse einem Anschluss zugewiesen wurde.
  - **LAG** - Gibt an, dass die IP-Adresse einer LAG (Link Aggregated Group) zugewiesen wurde.
  - **VLAN** - Gibt an, dass die IP-Adresse einem VLAN zugewiesen wurde.
- **Type** - Gibt an, ob die IP-Adresse manuell als statische IP-Adresse oder automatisch über DHCP definiert wurde.
- **Remove** - Entfernt die ausgewählte Schnittstelle aus der Dropdown-Liste **IP Address**.
  - **Aktiviert** - Entfernt die Schnittstelle aus der Dropdown-Liste **IP Address**.
  - **Deaktiviert** - Behält die Schnittstelle in der Dropdown-Liste **IP Address** bei.

Hinzufügen einer IP-Schnittstelle:

1. Öffnen Sie die Seite **IP Interface Parameters**.
2. Klicken Sie auf **Add**. Die Seite **Add a Static IP Interface** wird geöffnet:

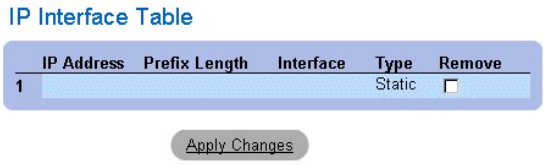


Seite "Add A Static IP Interface"

3. Definieren Sie die Felder **IP Address, Interface, Network Mask** oder **Prefix Length**.
4. Wählen Sie die Schnittstelle aus, der die IP-Schnittstelle zugewiesen werden soll.
5. Klicken Sie auf **Apply Changes.** Die neue Schnittstelle wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der "IP Interface Table":

1. Öffnen Sie die Seite **IP Interface Parameters**.
2. Klicken Sie auf **Show All**. Die Seite **IP Interface Table** wird geöffnet. Die **IP Interface Table** verfügt über dieselben Felder wie die Seite "Definieren von IP-Schnittstellen".



Seite "IP Interface Table"

Löschen von IP-Adressen:

1. Öffnen Sie die Seite **IP Interface.**
2. Klicken Sie auf **Show All**. Die Seite **IP Interface Table** wird geöffnet.
3. Wählen Sie einen Eintrag in der **IP Interface Table**aus.
4. Aktivieren Sie das Kontrollkästchen **Remove**, um IP-Adressen zu entfernen.
5. Klicken Sie auf **Apply Changes**. Die IP-Adresse wird gelöscht und das Gerät aktualisiert.

Definieren von IP-Schnittstellen mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
ip address *IP-Adresse {Maske | Präfixlänge}*	Legt eine IP-Adresse fest.
no ip address [ip-address]	Entfernt eine IP-Adresse.
show ip interface [ethernet *Schnittstellennummer* **| vlan** *VLAN-ID* **| port-channel** *Nummer]*	Zeigt den Verwendungsstatus der für IP konfigurierten Schnittstellen an.

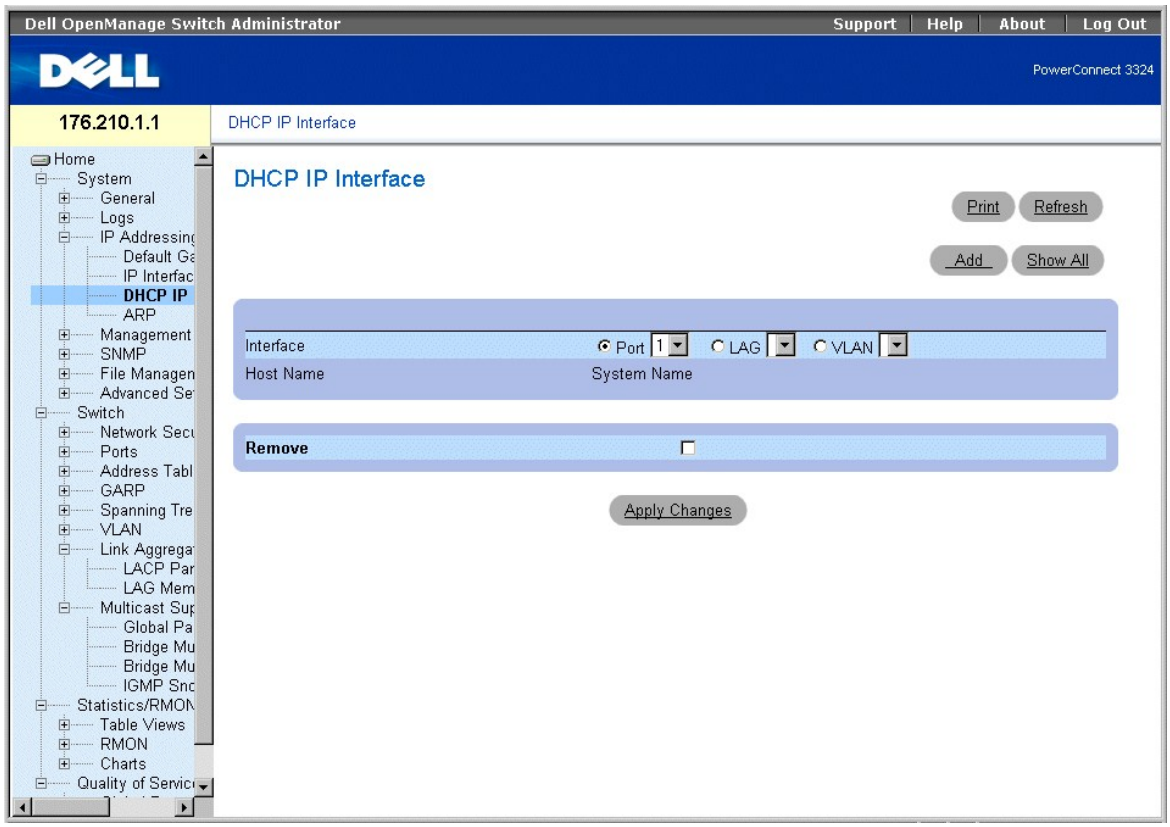
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# interface vlan 1

Console (config-if)# ip address 131.108.1.27 255.255.255.0

Console (config-if)# no ip address 131.108.1.27

Console (config-if)# exit

Console# show ip interface vlan 1

Internet address is 10.7.1.192/24

console# show ip interface vlan 204



IP Address Directed Broadcast

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

146.1.0.132/29 disable



console#
```

Definieren von DHCP IP-Schnittstellen

Auf der Seite **DHCP IP Interface** wird pro Schnittstelle die DHCP-Clienteinstellung für das Gerät festgelegt.

- Klicken Sie in der Strukturansicht auf **System** > **IP Addressing** > **DHCP IP Interface**. Die Seite **DHCP IP Interface** wird geöffnet.



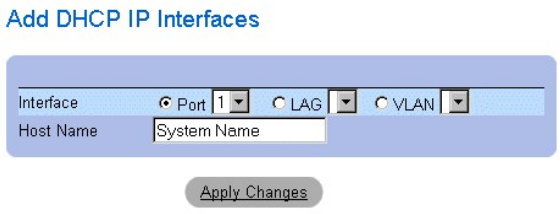
Seite "DHCP IP Interface"

Die Seite **DHCP IP Interface** enthält folgende Felder:

- Interface - Dient zur Auswahl einer Geräteschnittstelle.
  - **Port** - Legt fest, dass der Schnittstellentyp ein Anschluss ist und enthält die jeweilige Anschlussnummer, für die DHCP-Clienteinstellungen angezeigt werden.
  - **LAG** - Legt fest, dass der Schnittstellentyp eine LAG ist und enthält die jeweilige LAG-Nummer, für die DHCP-Clienteinstellungen angezeigt werden.
  - **VLAN** - Legt fest, dass der Schnittstellentyp ein VLAN ist und enthält die jeweilige VLAN-Nummer, für die DHCP-Clienteinstellungen angezeigt werden.
- **Host Name** - Gibt den Systemnamen an.
- **Remove** - Entfernt die DHCP-Clientinstanz der ausgewählten Schnittstelle aus der **DHCP IP Interfaces Table**.
  - **Aktiviert** - Entfernt die Schnittstelle aus der **DHCP IP Interfaces Table**.
  - **Deaktiviert** - Behält die Schnittstelle in der **DHCP IP Interfaces Table** bei.

Hinzufügen einer DHCP IP-Schnittstelle:

1. Öffnen Sie die Seite **DHCP IP Interface**.
2. Klicken Sie auf **Add**. Die Seite **Add DHCP IP Interfaces** wird geöffnet.



Hinzufügen von DHCP IP-Schnittstellen

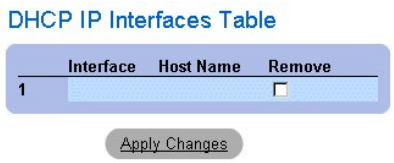
3. Wählen Sie das **Interface** aus und definieren Sie den **Host Name**.
4. Klicken Sie auf **Apply Changes**. Die neue DHCP IP-Schnittstelle wird hinzugefügt und das Gerät aktualisiert.

Ändern einer DHCP IP-Schnittstelle:

1. Öffnen Sie die Seite **DHCP IP Interface**.
2. Ändern Sie das Feld **Interface**.
3. Klicken Sie auf **Apply Changes**. Der Eintrag wird geändert und das Gerät aktualisiert.

Anzeigen der "DHCP IP Interfaces Table":

1. Öffnen Sie die Seite **DHCP IP Interface**.
2. Klicken Sie auf **Show All**. Die Seite **DHCP IP Interfaces Table** wird geöffnet.



Seite "DHCP IP Interfaces Table"

Löschen einer DHCP IP-Schnittstelle:

1. Öffnen Sie die Seite **DHCP IP Interface**.
2. Klicken Sie auf **Show All**. Die **DHCP IP Interfaces Table** wird geöffnet.
3. Wählen Sie einen DHCP-Clienteintrag aus.
4. Aktivieren Sie das Kontrollkästchen **Remove**, um DHCP-Clienteinträge zu entfernen.
5. Klicken Sie auf **Apply Changes**. Die Einträge in der **DHCP IP Interfaces Table** werden gelöscht und das Gerät aktualisiert.

Definieren von DHCP-Clients mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
ip address-dhcp [hostname *Hostname*]	Erhält eine IP-Adresse an einer Ethernet-Schnittstelle über DHCP.

Im Folgenden ein Beispiel für die CLI-Befehle:

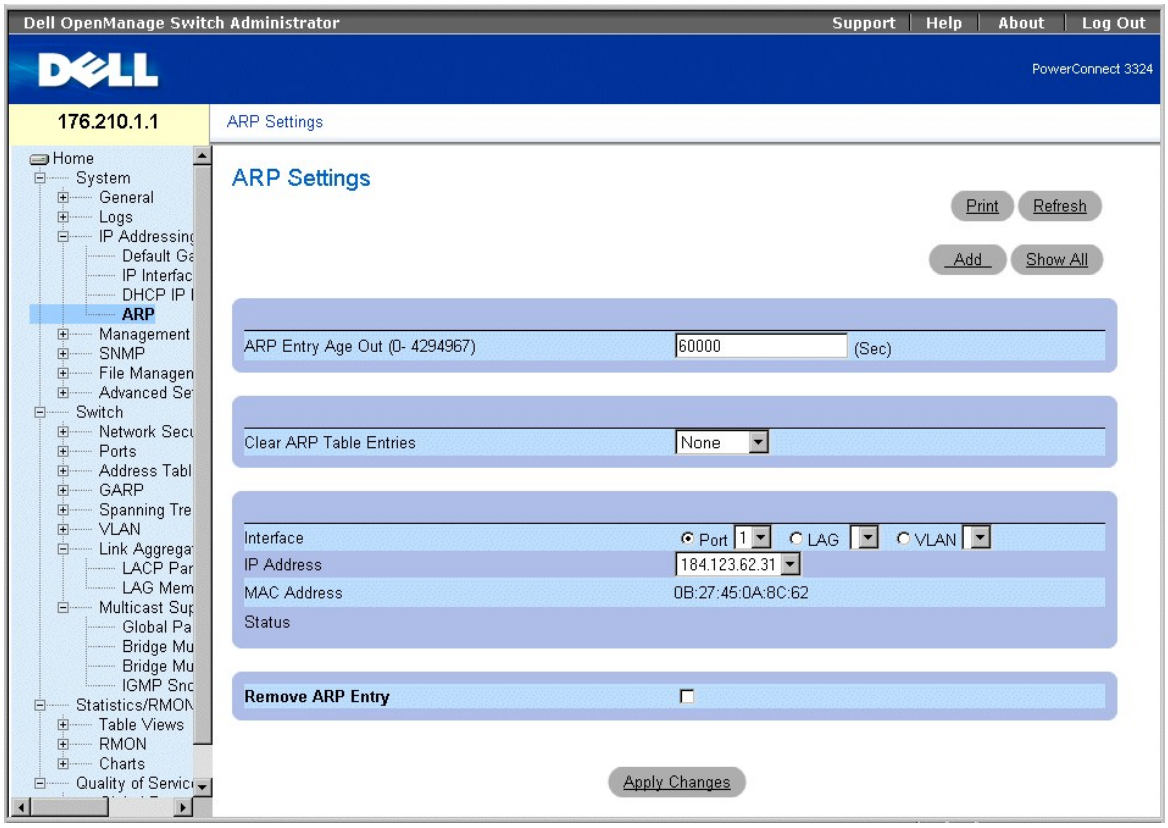
```
Console (config)# interface ethernet 1/e8

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

Konfigurieren von ARP

Das **Address Resolution Protocol** (ARP) ist ein TCP/IP-Protokoll, das IP-Adressen in physische Adressen konvertiert. Die statischen Einträge können in der ARP

Table definiert werden. Bei der Definition statischer Einträge wird ein permanenter Eintrag erfasst und zur Übersetzung von IP-Adressen in MAC-Adressen verwendet. So öffnen Sie die Seite **ARP Settings**:

- Klicken Sie in der Strukturansicht auf **System** > **IP Addressing** > **ARP**. Die Seite **ARP Settings** wird geöffnet.



Seite "ARP Settings"

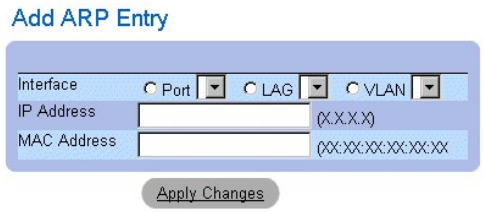
Die Seite **ARP Settings** enthält folgende Felder:

- **ARP Entry Age Out (0-4000000)** - Gibt an, wie viel Zeit (in Sekunden) vergeht, bis ein ARP-Eintrag verfällt. Nach diesem Zeitraum wird der Eintrag aus der Tabelle gelöscht. Der Standardwert lautet 60.000 Sekunden.
- **Clear ARP Table Entries** - Gibt die Art der zu löschenden ARP-Einträge an. Folgende Feldwerte sind möglich:
  - **None** - Gibt an, dass keine ARP-Einträge gelöscht werden.
  - **All** - Gibt an, dass alle ARP-Einträge gelöscht werden.
  - **Static** - Gibt an, dass lediglich statische ARP-Einträge gelöscht werden.
  - **Dynamic** - Gibt an, dass lediglich dynamische ARP-Einträge gelöscht werden.
- **Interface** - Dient zur Auswahl des Schnittstellentyps und der jeweiligen Schnittstellennummer. Folgende Feldwerte sind möglich:
  - **Port** - Enthält die Liste der Anschlüsse, für die ARP definiert werden kann.
  - **LAG** - Enthält die Liste der LAGs, für die ARP definiert werden kann.
  - **VLAN** - Enthält die Liste der VLANs, für die ARP definiert werden kann.
- **IP Address** - Dient zur Auswahl einer IP-Adresse, die mit der angegebenen Schnittstelle verknüpft ist.
- **MAC Address** - Gibt die verknüpfte MAC-Adresse an.
- **Status** - Gibt den Status des Eintrags in der **ARP Table** an. Folgende Feldwerte sind möglich:
  - **Other** - Gibt an, dass der ARP-Eintrag weder dynamisch erfasst wurde noch statisch ist.
  - **Invalid** - Gibt an, dass der ARP-Eintrag ungültig ist.
  - **Dynamic** - Gibt an, dass der ARP-Eintrag dynamisch erfasst wurde.
  - **Static** - Gibt an, dass es sich bei dem ARP-Eintrag um einen statischen Eintrag handelt.
- Remove ARP Entry - Entfernt einen ARP-Eintrag aus der **ARP Table**.

- **Aktiviert** - Entfernt einen bestimmten ARP-Eintrag.
- **Deaktiviert** - Behält ARP-Einträge bei.

Hinzufügen eines statischen Eintrags in die "ARP Table":

1. Öffnen Sie die Seite **ARP Settings**.
2. Klicken Sie auf **Add**. Die Seite **Add ARP Entry** wird geöffnet.

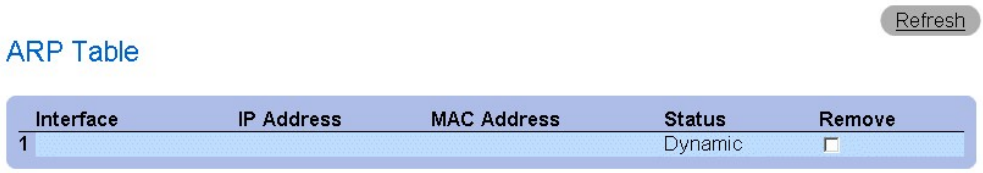


Seite "Add ARP Entry"

3. Wählen Sie eine **Interface** und definieren Sie die zugehörigen Felder **IP Address** und **MAC address**.
4. Klicken Sie auf **Apply Changes**. Der Eintrag wird der **ARP Table** hinzugefügt und das Gerät aktualisiert.

Anzeigen der "ARP Table":

1. Öffnen Sie die Seite **ARP Settings**.
2. Klicken Sie auf **Show All**. Die Seite **ARP Table** wird geöffnet.



Seite "ARP Table"

Löschen von Einträgen aus der "ARP Table":

1. Öffnen Sie die Seite **ARP Settings**.
2. Klicken Sie auf **Show All**. Die Seite **ARP Table** wird geöffnet.
3. Wählen Sie einen Tabelleneintrag aus.
4. Aktivieren Sie das Kontrollkästchen **Remove**
5. Klicken Sie auf **Apply Changes**. Der Eintrag in der **ARP Table** wird gelöscht und das Gerät aktualisiert.

Konfigurieren von ARP mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
arp *ip_addr hw_addr* **{ethernet** *interface-number* **| vlan** *vlan-id* **| port-channel** *number***}**	Fügt einen permanenten Eintrag in den ARP-Cache ein.
arp timeout seconds	Legt fest, wie lange ein Eintrag im ARP-Cache verbleibt.
show arp	Zeigt Einträge in der "ARP Table" an.
no arp	Entfernt einen ARP-Eintrag aus der "ARP Table".

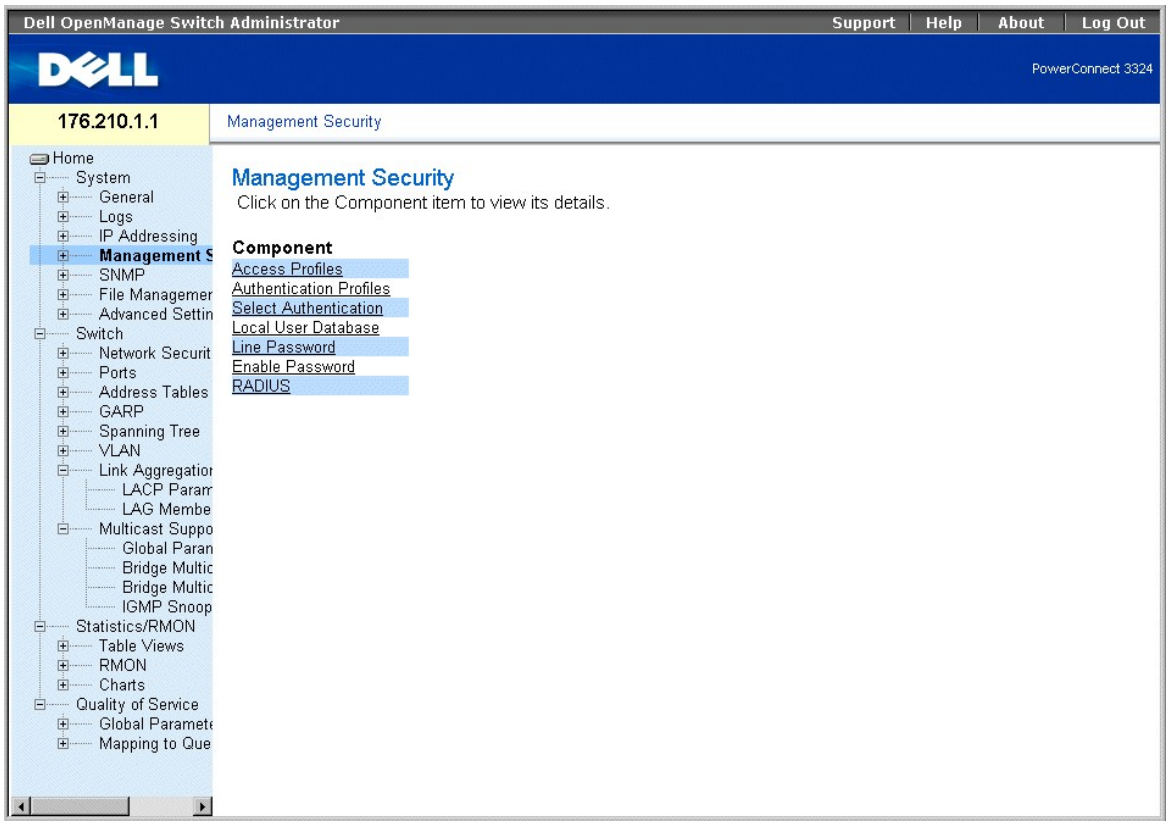
Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# arp 146.1.0.131 00-00-55-66-77-00 ethernet 1/e1

Console (config)# exit

Console# arp timeout 12000

Console# show arp

Interface IP address HW address Status

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

1/e1 10.7.1.102 00:10:B5:04:DB:4B Dynamic

2/e2 10.7.1.135 00:50:22:00:2A:A4 Static
```

Verwalten der Gerätesicherheit

Die Seite **Management Security** bietet Zugriff auf Sicherheitsseiten, auf denen Netzwerkadministratoren Sicherheitsparameter für Anschlüsse, Geräteverwaltungsverfahren sowie Benutzer- und Serversicherheit festlegen können. So öffnen Sie die Seite **Management Security**:

- Klicken Sie in der Strukturansicht auf **System** > **Management Security**. Die Seite **Management Security** wird geöffnet.



Seite "Management Security"

Dieser Abschnitt enthält die folgenden Themen:

- Definieren von Zugriffsprofilen
- Definieren von Authentisierungsprofilen
- Zuweisen von Authentisierungsprofilen
- Definieren der lokalen Benutzerdatenbanken
- Definieren von Leitungspasswörtern
- Definieren von Aktivierungspasswörtern
- Konfigurieren globaler RADIUS-Parameter

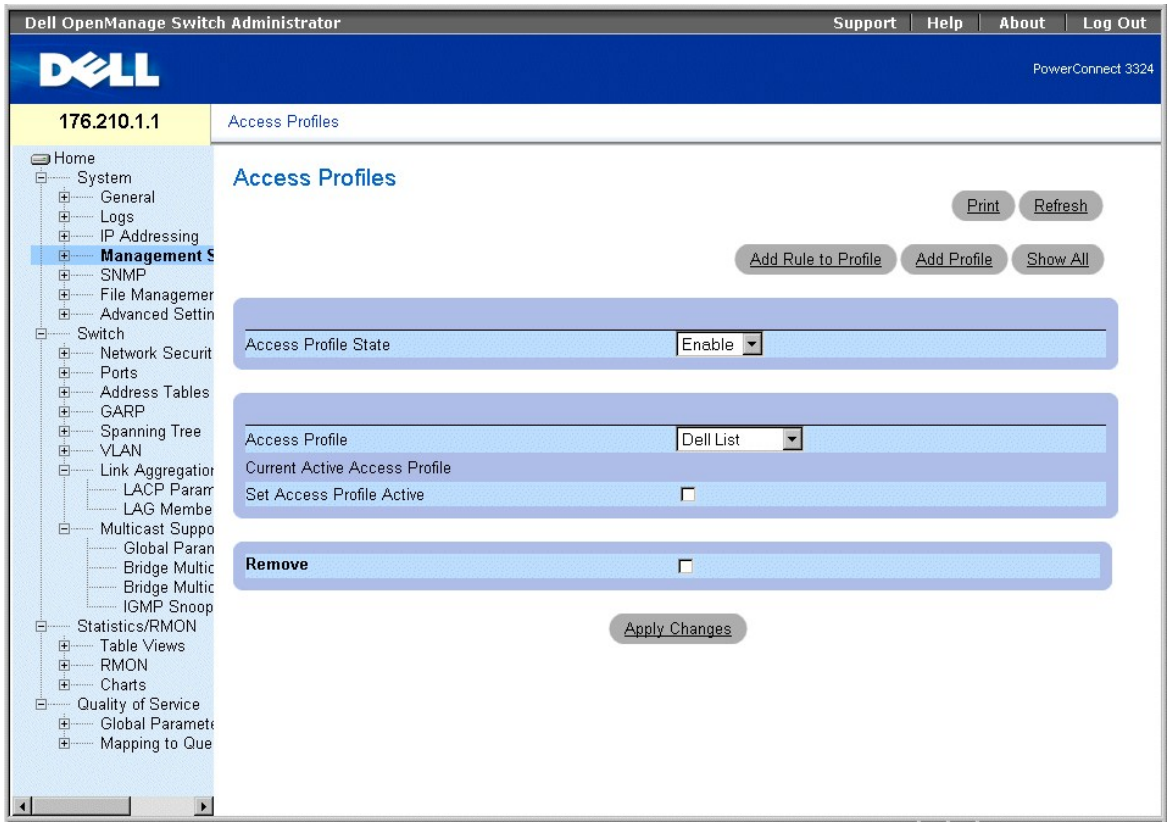
Definieren von Zugriffsprofilen

Auf der Seite **Access Profiles** können Netzwerkverwalter Profile und Regeln für den Gerätezugriff definieren. Der Zugriff auf Verwaltungsmethoden kann durch Ingress-Anschlüsse, IP-Quelladressen und/oder Subnetzmasken auf spezifische Benutzergruppen beschränkt werden. Verwaltungszugriffe können wie anschließend erläutert auf die folgenden Methoden beschränkt werden:

- Webzugriff (HTTP)
- Sicherer Webzugriff (HTTPS)
- Telnet
- SNMP
- Alle oben genannten Methoden

Es besteht die Möglichkeit, dass Benutzer Zugriff auf unterschiedliche Verwaltungsdienste haben. Daher umfassen die Verwaltungszugriffslisten Regeln, die festlegen, auf welche Weise Geräte von welchem Benutzer verwaltet werden. So öffnen Sie die Seite **Access Profiles**:

- Klicken Sie in der Strukturansicht auf **System** > **Management Security** > **Access Profiles**. Die Seite **Access Profiles** wird geöffnet.



Seite "Access Profiles"

Die Seite **Access Profiles** enthält folgende Felder:

- **Access Profile State** - Aktiviert das Zugriffsprofil für das Gerät. Folgende Feldwerte sind möglich:
  - **Enable** - Aktiviert die Sicherheitsverwaltung von Zugriffsprofilen für das Gerät.
  - **Disable** - Deaktiviert die Sicherheitsverwaltung von Zugriffsprofilen für das Gerät. Wenn die Sicherheitsverwaltung der Zugriffsprofile deaktiviert ist, kann von allen Stationen auf das Gerät zugegriffen werden.
- **Access Profiles** - Umfasst eine Liste benutzerdefinierter **Access Profile Lists**. Die Liste **Access Profile** enthält den folgenden Standardwert:
  - **Console Only** - Aktiviert den Zugriff ausschließlich über die Konsole. Durch Auswahl von "Console Only" werden Verbindungen über HTTP- und Telnet-Sitzungen getrennt. Dies ist der Standardwert, der nicht entfernt werden kann.
- **Current Active Access Profile** - Zeigt das derzeit aktive Zugriffsprofil an.
- **Set Access Profile Active** - Aktiviert das ausgewählte Zugriffsprofil.
- **Remove** - Entfernt das ausgewählte Zugriffsprofil aus der Liste **Access Profile Names**.
  - **Aktiviert** - Entfernt ein Zugriffsprofil.
  - **Deaktiviert** - Behält ein Zugriffsprofil bei.

ANMERKUNG: Aktive Profile können nicht entfernt werden.

Aktivieren eines Profils:

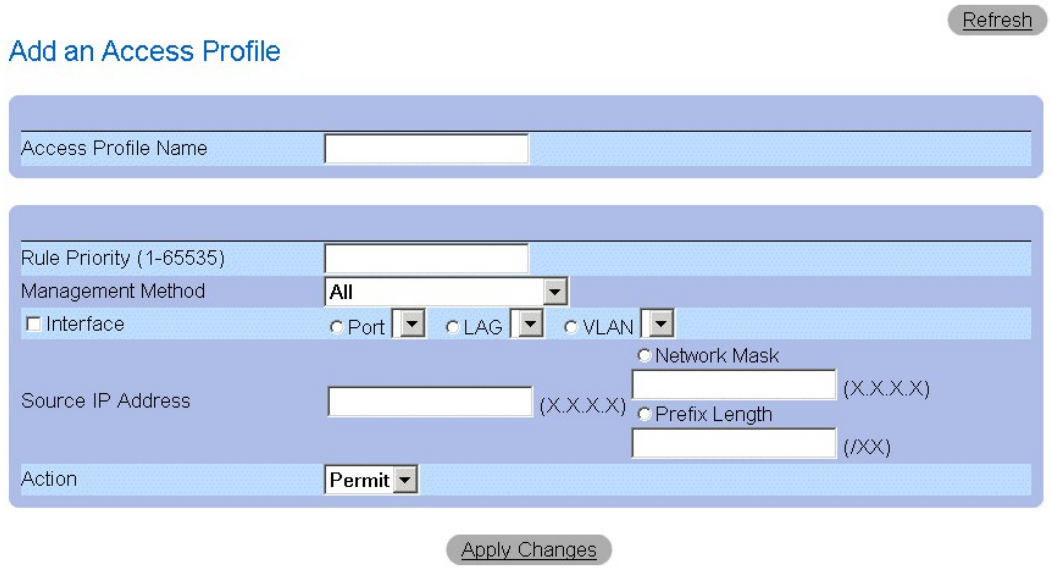
1. Öffnen Sie die Seite **Access Profiles**.
2. Wählen Sie ein Zugriffsprofil im Feld **Access Profile** aus.
3. Aktivieren Sie das Kontrollkästchen **Set Access Profile Active**.
4. Klicken Sie auf **Apply Changes**. Das Zugriffsprofil wird aktiviert.

Hinzufügen eines Zugriffsprofils:

Bei der Bestimmung der jeweiligen Priorität, der Geräteverwaltungsmethode, des Schnittstellentyps, der IP-Quelladresse sowie der Netzwerkmaske und des Zugriffs auf die Geräteverwaltung haben Regeln die Funktion von Filtern. Benutzern kann der Verwaltungszugriff gewährt oder verwehrt werden. Die Priorität von Regeln legt die Reihenfolge fest, in der die Regeln in einem Profil angewendet werden.

So definieren Sie Regeln für ein Zugriffsprofil:

1. Öffnen Sie die Seite **Access Profiles**.
2. Klicken Sie auf **Add Profile.** Die Seite **Add An Access Profile** wird geöffnet.



Seite "Add An Access Profile"

Die Seite **Add An Access Profile** enthält folgende Felder:

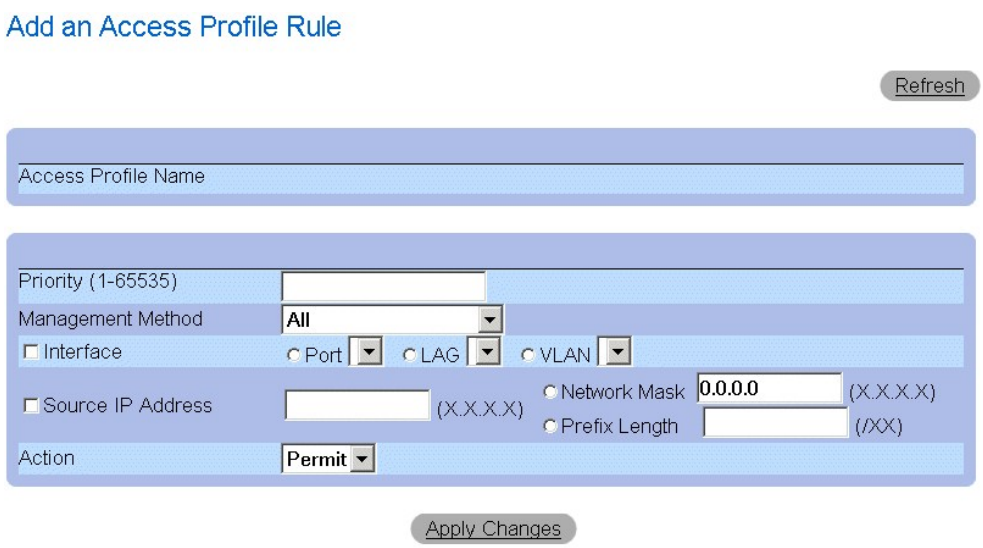
- **Access Profiles Name** - Gibt das Zugriffsprofil an, für das Regeln definiert werden.
- **Rule Priority (1-65535)** - Gibt die Priorität der Regeln an (falls eine optionale erste Regel im neuen Profil berücksichtigt werden soll).
- **Management Method** - Gibt die Verwaltungsmethode an, für die das Zugriffsprofil definiert wurde. Folgende Feldwerte sind möglich:
  - **All** - Gibt an, dass dem Zugriffsprofil alle Verwaltungsmethoden zugewiesen wurden.
  - **Telnet** - Gibt an, dass dem Zugriffsprofil alle Telnet-Sitzungen zugewiesen wurden.
  - **Secure Telnet** - Gibt an, dass dem Zugriffsprofil Secure Telnet-Sitzungen zugewiesen wurden.
  - **HTTP** - Gibt an, dass dem Zugriffsprofil HTTP-Sitzungen zugewiesen wurden.
  - **Secure HTTP** - Gibt an, dass dem Zugriffsprofil Secure HTTP-Sitzungen zugewiesen wurden.
  - **SNMP** - Gibt an, dass dem Zugriffsprofil SNMP-Sitzungen zugewiesen wurden.
- **Interface** - Gibt die Schnittstelle an, auf die die Regel angewendet wird. Folgende Feldwerte sind möglich:
  - **Port** - Weist darauf hin, dass die Schnittstelle ein Anschluss ist und gibt außerdem den jeweiligen Anschluss an, für den das Zugriffsprofil definiert wurde.
  - **LAG** - Weist darauf hin, dass die Schnittstelle eine LAG ist und gibt außerdem die jeweilige LAG an, für die das Zugriffsprofil definiert wurde.
  - **VLAN** - Weist darauf hin, dass die Schnittstelle ein VLAN ist und gibt außerdem das jeweilige VLAN an, für das das Zugriffsprofil definiert wurde.
- **Source IP Address** - Gibt die IP-Quelladresse der Schnittstelle an, mit der das Paket abgeglichen wird.
- **Network Mask** - Gibt die Netzwerkmaske der Schnittstelle an, mit der das Paket abgeglichen wird.
- **Prefix Length** - Gibt die Länge des Präfixes an, mit dem das Paket abgeglichen wird.
- **Action** - Definiert die Aktion, die bei Anwendung der Verwaltungssicherheitsregel in Kraft tritt. Folgende Feldwerte sind möglich:
  - **Permit** - Lässt den Verwaltungszugriff auf die definierte Schnittstelle zu.
  - **Deny** - Unterbindet den Verwaltungszugriff auf die definierte Schnittstelle.

3. Definieren Sie das Feld **Access Profile Name**.
4. Definieren Sie die Felder **Rule Priority, Management Method, Interface, Source IP, Network Mask, Prefix Length** und **Action**.
5. Klicken Sie auf **Apply Changes**. Das neue Zugriffsprofil wird hinzugefügt und das Gerät aktualisiert.

Hinzufügen von Regeln zu Zugriffsprofilen:

ANMERKUNG: Die erste Regel muss definiert werden, damit der Datenverkehr mit Zugriffsprofilen verglichen werden kann.

1. Öffnen Sie die Seite **Access Profiles**.
2. Klicken Sie auf **Add Rule to Profile**. Die Seite **Add An Access Profile Rule** wird geöffnet.



Seite "Add An Access Profile Rule"

Die Seite **Add An Access Profile Rule** enthält folgende Felder:

- **Access Profile Name** - Gibt den Namen des Zugriffsprofils an.
- **Rule Priority (1-65535)** - Gibt die Priorität der Regeln an.
- **Management Method** - Gibt die Verwaltungsmethode an, für die das Zugriffsprofil definiert wurde. Folgende Feldwerte sind möglich:
  - **All** - Gibt an, dass dem Zugriffsprofil alle Verwaltungsmethoden zugewiesen wurden. Benutzer mit diesem Zugriffsprofil können unter Verwendung sämtlicher Verwaltungsmethoden auf das Gerät zugreifen.
  - **Telnet** - Gibt an, dass dem Zugriffsprofil alle Telnet-Sitzungen zugewiesen wurden. Benutzer mit diesem Zugriffsprofil können unter Verwendung der Telnet-Verwaltungsmethode auf das Gerät zugreifen.
  - **Secure Telnet** - Gibt an, dass dem Zugriffsprofil Secure Telnet-Sitzungen zugewiesen wurden. Benutzer mit diesem Zugriffsprofil können unter Verwendung der Secure Telnet-Verwaltungsmethode auf das Gerät zugreifen.
  - **HTTP** - Gibt an, dass dem Zugriffsprofil HTTP-Sitzungen zugewiesen wurden. Benutzer mit diesem Zugriffsprofil können unter Verwendung der HTTP-Verwaltungsmethode auf das Gerät zugreifen.
  - **Secure HTTP** - Gibt an, dass dem Zugriffsprofil Secure HTTP-Sitzungen zugewiesen wurden. Benutzer mit diesem Zugriffsprofil können unter Verwendung der Secure HTTP-Verwaltungsmethode auf das Gerät zugreifen.
  - **SNMP** - Gibt an, dass dem Zugriffsprofil SNMP-Sitzungen zugewiesen wurden. Benutzer mit diesem Zugriffsprofil können unter Verwendung der SNMP-Verwaltungsmethode auf das Gerät zugreifen.
- **Interface** - Gibt die Schnittstelle an, auf die die Regel angewendet wird. Folgende Feldwerte sind möglich:
  - **Port** - Weist darauf hin, dass die Schnittstelle ein Anschluss ist und gibt außerdem den jeweiligen Anschluss an, für den das Zugriffsprofil definiert wurde.
  - **LAG** - Weist darauf hin, dass die Schnittstelle eine LAG ist und gibt außerdem die jeweilige LAG an, für die das Zugriffsprofil definiert wurde.
  - **VLAN** - Weist darauf hin, dass die Schnittstelle ein VLAN ist und gibt außerdem das jeweilige VLAN an, für das das Zugriffsprofil definiert wurde.
- **Source IP Address** - Gibt die IP-Quelladresse der Schnittstelle an, mit der das Paket abgeglichen wird.
- **Network Mask** - Gibt die Netzwerkmaske der Schnittstelle an, mit der das Paket abgeglichen wird.
- **Prefix Length** - Gibt die Länge des Präfixes an, mit dem das Paket abgeglichen wird.

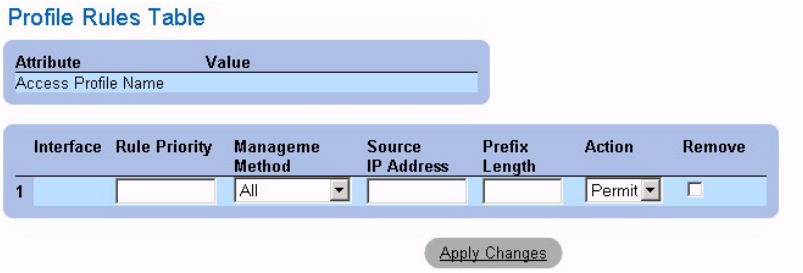
- **Action** - Definiert die Aktion, die bei Anwendung der Verwaltungssicherheitsregel in Kraft tritt. Folgende Feldwerte sind möglich:
  - **Permit** - Lässt den Verwaltungszugriff auf die definierte Schnittstelle zu.
  - **Deny** - Unterbindet den Verwaltungszugriff auf die definierte Schnittstelle.

3. Definieren Sie das Feld **Access Profile Name**.
4. Definieren Sie die Felder **Rule Priority, Management Method, Interface, Source IP, Network Mask, Prefix Length** und **Action**.
5. Klicken Sie auf **Apply Changes**. Die Regel wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der "Profile Rules Table":

ANMERKUNG: Die Reihenfolge, in der Regeln in der **Profile Rules Table** angezeigt werden, ist von Bedeutung. Pakete werden mit der ersten Regel abgeglichen, die die für die Regel festgelegten Kriterien erfüllt.

1. Öffnen Sie die Seite **Access Profiles**.
2. Klicken Sie auf **Show All**. Die Seite **Profile Rules Table** wird geöffnet.



Seite "Profile Rules Table"

3. Klicken Sie auf **Apply Changes**.

Entfernen einer Regel:

ANMERKUNG: Beim Löschen einer Regel wird zusätzlich der Profilname gelöscht.

1. Öffnen Sie die Seite **Access Profiles**.
2. Klicken Sie auf **Show All**. Die Seite **Profile Rules Table** wird geöffnet.
3. Wählen Sie eine Regel auf der Seite **Profile Rules Table** aus.
4. Aktivieren Sie das Kontrollkästchen **Remove**.
5. Klicken Sie auf **Apply Changes**. Die Regel wird gelöscht und das Gerät aktualisiert.

Definieren von Zugriffsprofilen mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
management access-list *Name*	Definiert eine Verwaltungszugriffsliste und erfasst den Zugriffslistenkontext zu Konfigurationszwecken.
permit [ethernet *Schnittstellennummer* **| vlan** *VLAN-ID* **| port-channel** *Nummer***] [service** *Dienst***]**	Legt Anschlusszugriffsbedingungen für die Verwaltungszugriffsliste fest.
permit ip-source *IP-Adresse* **[mask** *Maske* **|** *Präfixlänge***] [ethernet** *Schnittstellennummer* **| vlan** *VLAN-ID* **| port-channel** *Nummer***] [service** *Dienst***]**	Legt Anschlusszugriffsbedingungen für die Verwaltungszugriffsliste sowie die ausgewählte Verwaltungsmethode fest.
deny [ethernet *Schnittstellennummer* **| vlan** *VLAN-ID* **| port-channel** *Nummer***] [service** *Dienst***]**	Legt Anschlusssperrbedingungen für die Verwaltungszugriffsliste sowie die ausgewählte Verwaltungsmethode fest.
deny ip-source *IP-Adresse* **[mask** *Maske* **|** *Präfixlänge***] [ethernet** *Schnittstellennummer* **| vlan** *VLAN-ID* **| port-channel** *Nummer***] [service** *Dienst***]**	Legt Anschlusssperrbedingungen 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 zur Verwaltungszugriffsklasse an.

Im Folgenden ein Beispiel für die CLI-Befehle:

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

Console (config-macl)# permit ethernet 1/e1

Console (config-macl)# permit ethernet 2/e9

Console (config-macl)# deny ethernet 1/e2

Console (config-macl)# deny ethernet 2/e10

Console (config-macl)# exit

Console (config)# management access-class mlist

Console (config)# exit

Console# show management access-list

mlist

-----

permit ethernet 1/e1

permit ethernet 2/e9

! (Note: all other access implicitly denied)

Console> show management access-class

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

Definieren von Authentisierungsprofilen

Auf der Seite **Authentication Profiles** können Netzwerkverwalter die Benutzerauthentisierungsmethode für das Gerät auswählen. Die Benutzerauthentisierung erfolgt:

- lokal

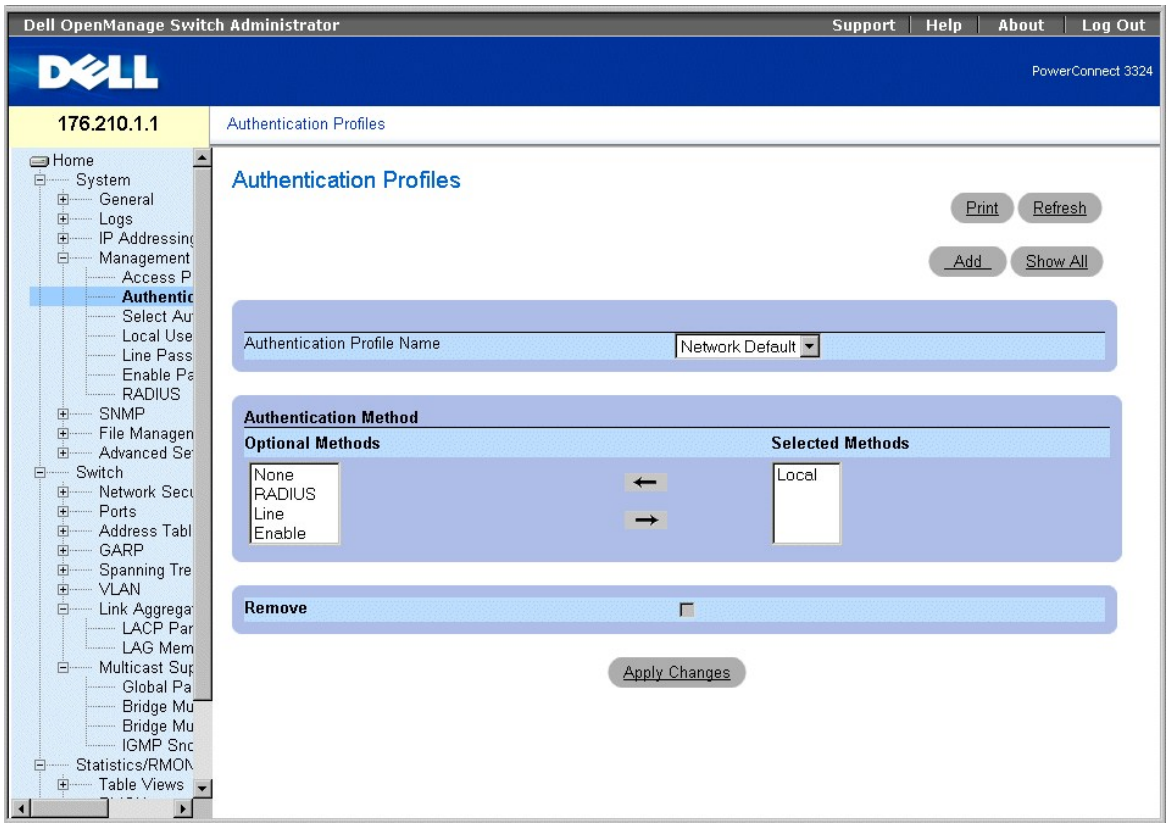
- über einen externen Server

Außerdem kann die Benutzerauthentisierung auf **None** gesetzt werden.

Die Benutzerauthentisierung erfolgt in der Reihenfolge, in der die Methoden ausgewählt werden. Wenn beispielsweise sowohl die Optionen **Local** als auch **RADIUS** ausgewählt werden, wird der Benutzer zuerst lokal authentisiert. Wenn die lokale Benutzerdatenbank keine Datensätze enthält, wird der Benutzer über den RADIUS-Server authentisiert.

Falls während der Authentisierung ein Fehler auftritt, wird die nächste ausgewählte Methode verwendet. So öffnen Sie die Seite **Authentication Profiles**:

- Klicken Sie in der Strukturansicht auf **System** > **Management Security** >**Authentication Profiles**. Die Seite **Authentication Profiles** wird geöffnet.



Seite "Authentication Profiles"

The Die Seite **Authentication Profiles** enthält folgende Optionslisten:

- **Authentication Profile Name** - Zeigt die Listen benutzerdefinierter Authentisierungsmethoden an und umfasst die folgenden Werte:
  - **Network Default**
  - **Console Default**
- **Optional Methods** - Listet die Benutzerauthentisierungsmethoden auf. Die möglichen Optionen lauten:
  - **Local** - Gibt an, dass die Authentisierung lokal erfolgt. Benutzername und Passwort werden zu Authentisierungszwecken vom Gerät überprüft.
  - **None** - Gibt an, dass keine Benutzerauthentisierung erfolgt.
  - **RADIUS** - Gibt an, dass die Benutzerauthentisierung auf dem RADIUS-Server erfolgt.
  - **Line** - Gibt an, dass das Leitungspasswort für die Authentisierung verwendet wird.
  - **Enable** - Gibt an, dass das Aktivierungspasswort für die Authentisierung verwendet wird.
- **Selected Methods** - Gibt die ausgewählten Authentisierungsmethoden und ihre Reihenfolge an.

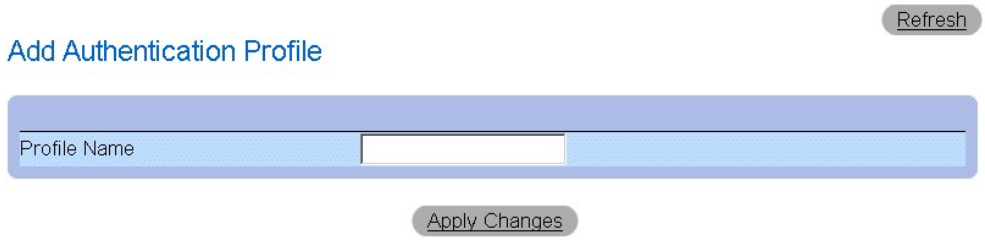
- **Remove** - Entfernt das ausgewählte Authentisierungsprofil aus der Liste **Access Profile Names**.
  - **Aktiviert** - Entfernt ein Authentisierungsprofil.
  - **Deaktiviert** - Behält ein Authentisierungsprofil bei.

Auswählen eines Authentisierungsprofils:

1. Öffnen Sie die Seite **Authentication Profiles**.
2. Wählen Sie ein Profil im Feld **Authentication Profile Name**.
3. Wählen Sie eine Authentisierungsmethode mit den Pfeilschaltflächen aus.
4. Klicken Sie auf **Apply Changes.** Das Benutzerauthentisierungsprofil für das Gerät wird aktualisiert.

Hinzufügen eines Authentisierungsprofils:

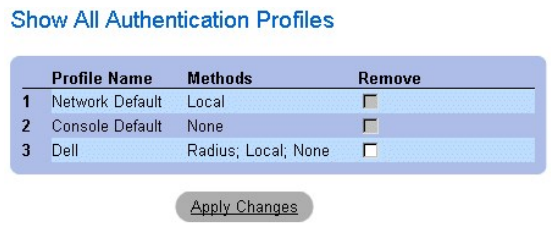
1. Öffnen Sie die Seite **Authentication Profile**.
2. Klicken Sie auf **Add**. Die Seite **Add Authentication Method Profile Name** wird geöffnet.



Seite "Add Authentication Profile"

Anzeigen der Seite "Show All Authentication Profiles":

1. Öffnen Sie die Seite **Authentication Profiles**.
2. Klicken Sie auf **Show All**. Die Seite **Open the Authentication Profile** wird geöffnet:



Seite "Authentication Profile"

Löschen eines Authentisierungsprofils:

1. Öffnen Sie die Seite **Authentication Profiles**.
2. Klicken Sie auf **Show All**. Die Seite **Open the Authentication Profile** wird geöffnet:
3. Wählen Sie ein Authentisierungsprofil aus.
4. Aktivieren Sie das Kontrollkästchen **Remove**.
5. Klicken Sie auf **Apply Changes.** Das Authentisierungsprofil wird gelöscht.

Konfigurieren eines Authentisierungsprofils mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
aaa authentication login {default | *Listenname***}** *Methode1* **[***Methode2***]**	Konfiguriert die Anmeldungsauthentisierung.
no aaa authentication login \{default | *Listenname*	Entfernt ein Anmeldungsauthentisierungsprofil.

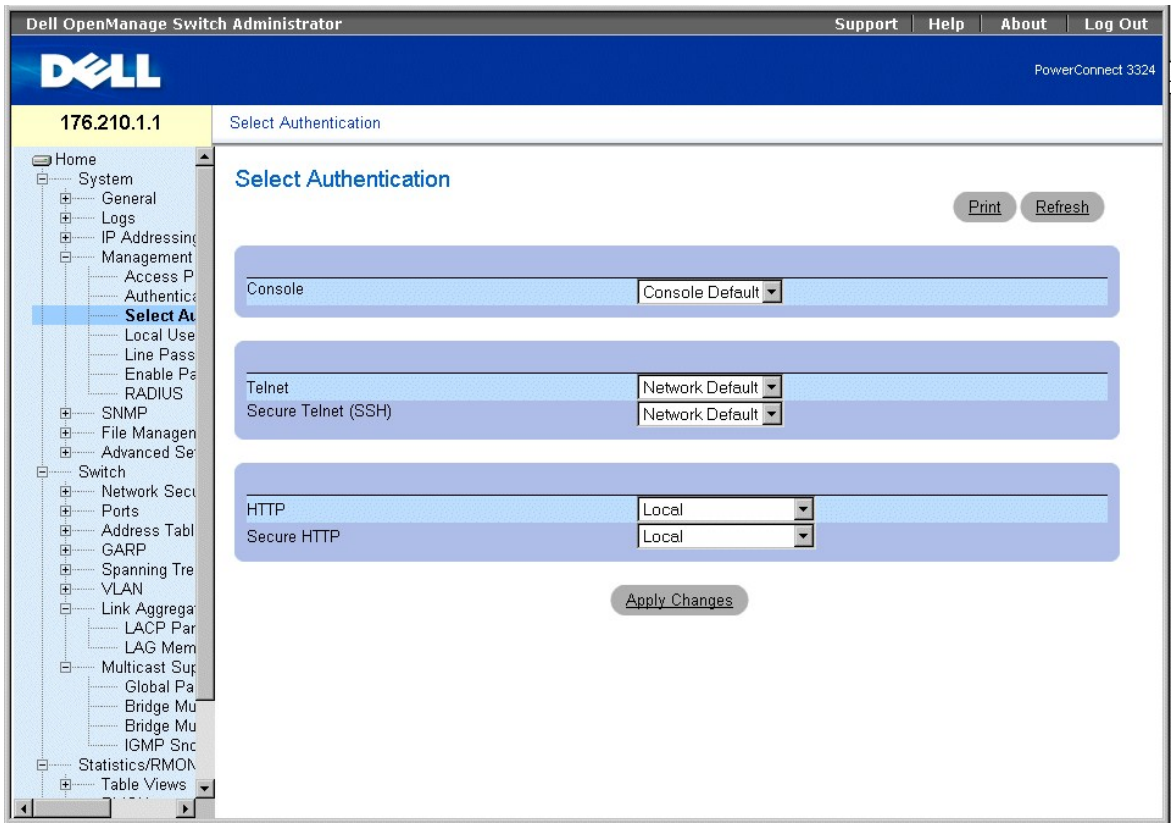
Im Folgenden ein Beispiel für die CLI-Befehle:

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

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

Zuweisen von Authentisierungsprofilen

Nach der Definition der Authentisierungsprofile können diese auf Verwaltungszugriffsmethoden angewendet werden. Beispielsweise können Konsolenbenutzer durch Authentisierungsmethodenliste 1 und Telnet-Benutzer durch Authentisierungsmethodenliste 2 authentisiert werden. So öffnen Sie die Seite **Management Authentication**:

- Klicken Sie in der Strukturansicht auf **System** > **Management Security** > **Select Authentication**. Die Seite **Select Authentication** wird geöffnet.



Seite "Select Authentication"

Die Seite **Select Authentication** enthält folgende Felder:

- **Console** - Zeigt die zur Authentisierung von Konsolenbenutzern verwendeten Authentisierungsprofile an. Authentisierungsprofile werden auf der Seite "Zuweisen von Authentisierungsprofilen" zugewiesen. Es gibt zwei vordefinierte Feldwerte, denen weitere Authentisierungsprofile hinzugefügt werden können. Die vordefinierten Werte können jedoch nicht gelöscht werden. Die vordefinierten Feldwerte lauten:
  - **Network Default**
  - **Console Default**
- **Telnet** - Zeigt die zur Authentisierung von Telnet-Benutzern verwendeten Authentisierungsprofile an. Authentisierungsprofile werden auf der Seite "Zuweisen von Authentisierungsprofilen" zugewiesen. Es gibt zwei vordefinierte Feldwerte, denen weitere Authentisierungsprofile hinzugefügt werden können. Die vordefinierten Werte können jedoch nicht gelöscht werden. Die vordefinierten Feldwerte lauten:
  - **Network Default**
  - **Console Default**
- **Secure Telnet (SSH)** - Zeigt die zur Authentisierung von SSH-Benutzern verwendeten Authentisierungsprofile an. Über Secure Shell (SSH) können sichere Remote-Verbindungen zu einem Gerät hergestellt werden. SSH ermöglicht es SSH-Clients, eine sichere, verschlüsselte Verbindung mit einem Gerät herzustellen. Authentisierungsprofile werden auf der Seite "Zuweisen von Authentisierungsprofilen" zugewiesen.
- **HTTP** - Zeigt die für den HTTP-Zugriff verwendeten Authentisierungsmethoden an. Folgende Feldwerte sind möglich:
  - **None** - Gibt an, dass kein Authentisierungsprofil für HTTP-Zugriffe verwendet wird.
  - **Local** - Gibt an, dass die HTTP-Authentisierung lokal erfolgt.
  - **Radius** - Gibt an, dass die HTTP-Authentisierung auf dem RADIUS-Server erfolgt und dass HTTP-Zugriffe zulässig sind.
  - **Local, None** - Gibt an, dass die HTTP-Authentisierung zunächst lokal erfolgt. Falls keine Authentisierungsmethode verwendet wird, bleibt die lokale Benutzerdatenbank leer und HTTP-Zugriffe sind zulässig.
  - **Radius, None** - Gibt an, dass die HTTP-Authentisierung zunächst auf dem RADIUS-Server erfolgt. Falls keine Authentisierungsmethode verwendet wird, kann nicht auf den RADIUS-Server zugegriffen werden.
  - **Local, Radius** - Gibt an, dass die HTTP-Authentisierung zunächst lokal erfolgt. Wenn der Benutzer vom RADIUS-Server authentisiert wird, ist die lokale Benutzerdatenbank leer. Wenn die Verwaltungsmethode nicht vom RADIUS-Server authentisiert werden kann, wird die HTTP-Sitzung gesperrt.
  - **Radius, Local**- Gibt an, dass die HTTP-Authentisierung zunächst auf dem RADIUS-Server erfolgt. Falls kein Zugriff auf den RADIUS-Server möglich ist, wird die HTTP-Sitzung lokal authentisiert. Wenn die HTTP-Sitzung nicht lokal authentisiert werden kann, wird die HTTP-Sitzung gesperrt.
  - **Local, Radius, None** - Gibt an, dass die HTTP-Authentisierung zunächst lokal erfolgt. Wenn die lokale Datenbank leer ist, wird die Verwaltungsmethode vom RADIUS-Server authentisiert. Falls kein Zugriff auf den RADIUS-Server möglich ist, wird die HTTP-Sitzung zugelassen.
  - **Radius, Local, None** - Gibt an, dass die HTTP-Authentisierung zunächst auf dem RADIUS-Server erfolgt. Falls kein Zugriff auf den RADIUS-Server möglich ist, wird die HTTP-Sitzung lokal authentisiert. Wenn die lokale Datenbank leer ist, wird die HTTP-Sitzung zugelassen.
- **Secure HTTP** - Gibt die für den Secure HTTP-Zugriff verwendeten Authentisierungsprofile an. Folgende Feldwerte sind möglich:
  - **None** - Gibt an, dass kein Authentisierungsprofil für Secure HTTP-Zugriffe verwendet wird.
  - **Local** - Gibt an, dass die Secure HTTP-Authentisierung lokal erfolgt.
  - **Radius** - Gibt an, dass die Secure HTTP-Authentisierung auf dem RADIUS-Server erfolgt.
  - **Local, None** - Gibt an, dass die Secure HTTP-Authentisierung zunächst lokal erfolgt. Falls die lokale Datenbank leer ist, wird keine Authentisierungsmethode verwendet und Secure HTTP-Zugriffe sind zulässig.
  - **Radius, None** - Gibt an, dass die Secure HTTP-Authentisierung zunächst auf dem RADIUS-Server erfolgt. Falls kein Zugriff auf den RADIUS-Server möglich ist, wird keine Authentisierungsmethode verwendet und Secure HTTP-Zugriffe sind zulässig.
  - **Local, Radius** - Gibt an, dass die Secure HTTP-Authentisierung zunächst lokal erfolgt. Wenn die lokale Datenbank leer ist, wird der Benutzer vom RADIUS-Server authentisiert. Wenn die Verwaltungsmethode nicht vom RADIUS-Server authentisiert werden kann, wird die Secure HTTP-Sitzung gesperrt.
  - **Radius, Local**- Gibt an, dass die Secure HTTP-Authentisierung zunächst auf dem RADIUS-Server erfolgt. Falls kein Zugriff auf den RADIUS-Server möglich ist, wird die Secure HTTP-Sitzung lokal authentisiert. Wenn die Secure HTTP-Sitzung nicht lokal authentisiert werden kann, wird die Secure HTTP-Sitzung gesperrt.
  - **Local, Radius, None** - Gibt an, dass die Secure HTTP-Authentisierung zunächst lokal erfolgt. Wenn die lokale Datenbank leer ist, wird die Verwaltungsmethode vom RADIUS-Server authentisiert. Falls der RADIUS-Server nicht auf die Datenbank zugreifen kann, wird die Secure HTTP-Sitzung zugelassen.
  - **Radius, Local, None** - Gibt an, dass die Secure HTTP-Authentisierung zunächst auf dem RADIUS-Server erfolgt. Falls kein Zugriff auf den RADIUS-Server möglich ist, wird die Secure HTTP-Sitzung lokal authentisiert. Wenn die lokale Datenbank leer ist, wird die Secure HTTP-Sitzung zugelassen.

Anwenden einer Authentisierungsliste auf Konsolensitzungen:

1. Öffnen Sie die Seite **Select Authentication**.
2. Wählen Sie ein Authentisierungsprofil im Feld **Console** aus.
3. Klicken Sie auf **Apply Changes**. Konsolensitzungen wird eine Authentisierungsliste zugewiesen.

Anwenden eines Authentisierungsprofils auf Telnet-Sitzungen:

1. Öffnen Sie die Seite **Select Authentication.**
2. Wählen Sie ein Authentisierungsprofil im Feld **Telnet** aus.
3. Klicken Sie auf **Apply Changes**. Telnet-Sitzungen wird eine Authentisierungsliste zugewiesen.

Anwenden eines Authentisierungsprofils auf Secure Telnet-(SSH-)Sitzungen:

1. Öffnen Sie die Seite **Select Authentication.**
2. Wählen Sie ein Authentisierungsprofil im Feld **Secure Telnet (SSH)** aus.
3. Klicken Sie auf **Apply Changes**. Secure Telnet-(SSH-)Sitzungen wird ein Authentisierungsprofil zugewiesen.

Zuweisen einer Authentisierungssequenz zu HTTP-Sitzungen:

1. Öffnen Sie die Seite **Select Authentication**.
2. Wählen Sie eine Authentisierungssequenz im Feld **HTTP** aus.
3. Klicken Sie auf **Apply Changes**. HTTP-Sitzungen wird eine Authentisierungssequenz zugewiesen.

Zuweisen einer Authentisierungssequenz zu Secure HTTP-Sitzungen:

1. Öffnen Sie die Seite **Select Authentication**.
2. Wählen Sie eine Authentisierungssequenz im Feld **Secure HTTP** aus.
3. Klicken Sie auf **Apply Changes**. Secure HTTP-Sitzungen wird eine Authentisierungssequenz zugewiesen.

Zuweisen von Zugriffsauthentisierungsprofilen oder -sequenzen mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
enable authentication [default | *Listenname*]	Legt die Authentisierungsmethodenliste für Zugriffe auf eine höhere Berechtigungsebene über eine Remote-Telnet- oder -Konsolensitzung fest.
login authentication [default | *Listenname*]	Legt die Liste der Anmeldungsauthentisierungsmethoden für eine Remote-Telnet- oder -Konsolensitzung fest.
ip http authentication *Methode1* [*Methode2*]	Legt die Authentisierungsmethoden für HTTP-Server fest.
ip https authentication *Methode1* [*Methode2*]	Legt die Authentisierungsmethoden für HTTPS-Server fest.
show authentication methods	Zeigt Informationen zu den Authentisierungsmethoden an.

Im Folgenden ein Beispiel für die CLI-Befehle:

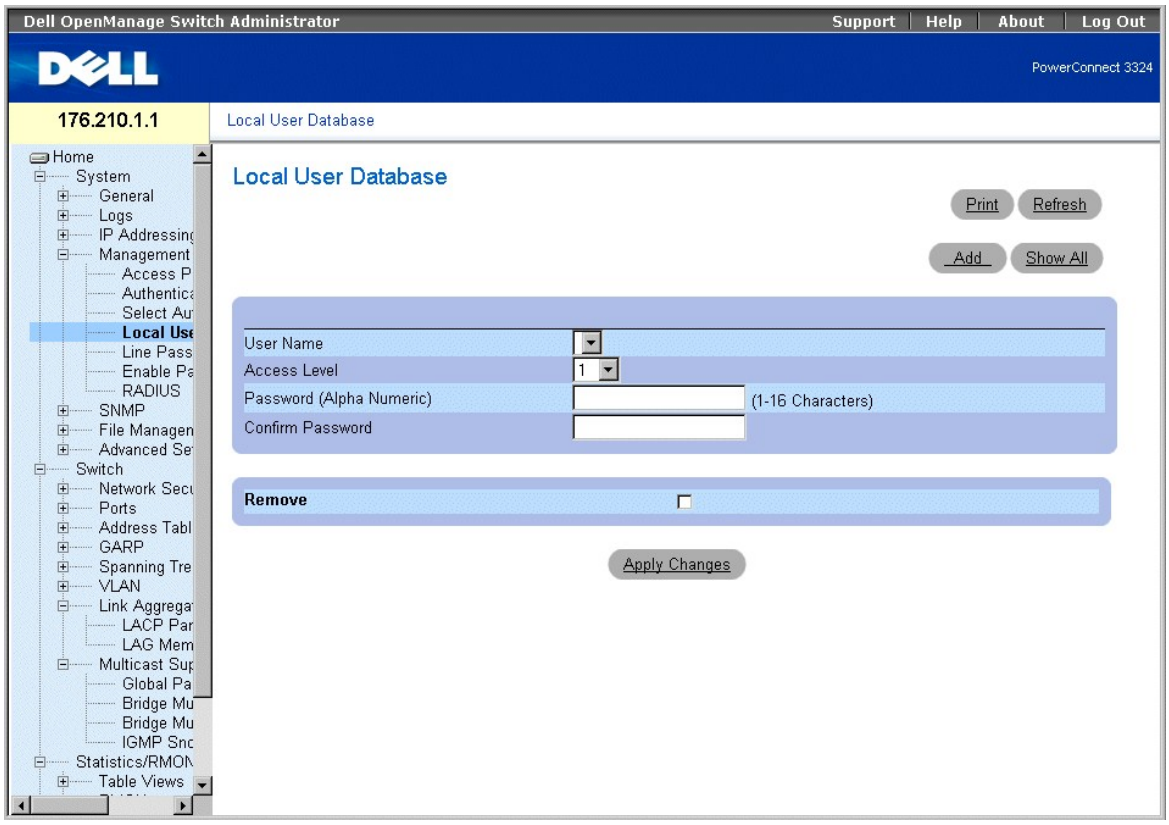
```
Console(config-line)# enable authentication default

Console(config-line)# login authentication default

Console (config-line)# exit

Console (config)# ip http authentication radius local

Console (config)# ip https authentication radius local

Console (config)# exit

Console# show authentication methods
```

```
Login Authentication Method Lists

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

Default: Radius, Local, Line

Console_Login: Line, None



Enable Authentication Method Lists

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

Default: Radius, Enable

console> enable: Enable, None



Line Login Method List Enable Method List

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

Console Console_Login Console_Enable

Telnet Default Default

SSH Default Default



HTTP: Radius, local

HTTPS: Radius, local
```

Definieren der lokalen Benutzerdatenbanken

Auf der Seite **Local User Database** können Netzwerkverwalter Benutzer, Passwörter und Zugriffsebenen definieren. Die Passwortlänge ist auf maximal 16 Zeichen beschränkt. So öffnen Sie die Seite **Local User Database**:

- Klicken Sie in der Strukturansicht auf **System** > **Management Security** > **Local User Database**. Die Seite **Local User Database** wird geöffnet.



Seite "Local User Database"

Die Seite **Local User Database** enthält folgende Felder:

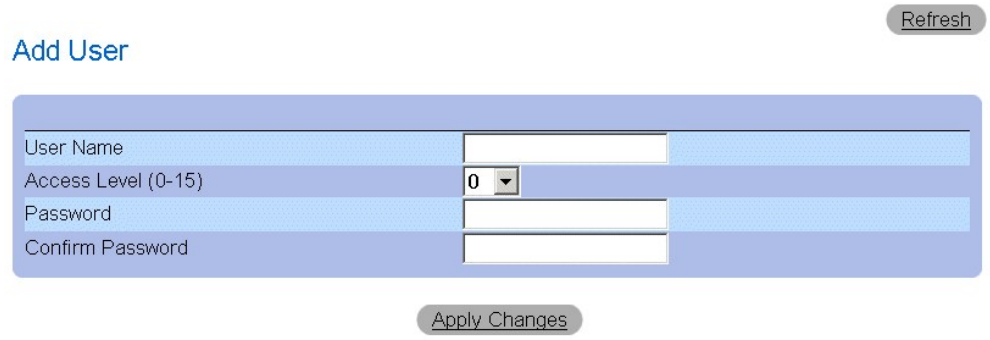
- **User Name** - Enthält eine Benutzerliste.
- **Access Level** - Legt die Zugriffsebene für Benutzer fest. Die möglichen Werte lauten:
  - **1-15** - Gibt die Benutzerzugriffsebene an. **1** steht für die niedrigste Benutzerzugriffsebene.
- **Password (Alpha Numeric)** - Legt das Benutzerpasswort fest. The password is displayed as *******.
- **Confirm Password** - Bestätigt das benutzerdefinierte Passwort. Das bestätigte Passwort wird als ******* angezeigt.
- **Remove** - Entfernt Benutzer aus der Liste **User Name**.
  - **Aktiviert**- Entfernt einen bestimmten Benutzer aus der **Local User Database**.
  - **Deaktiviert** - Behält den Benutzer in der **Local User Database** bei.

Zuweisen von Zugriffsrechten zu einem Benutzer:

1. Öffnen Sie die Seite **Local User Database**.
2. Wählen Sie einen Benutzer im Feld **User Name** aus.
3. Definieren Sie die Felder **Access Level** und **Password**.
4. Klicken Sie auf **Apply Changes.** Die Benutzerzugriffsrechte und Passwörter werden definiert und das Gerät aktualisiert.

Definieren eines neuen Benutzers:

1. Öffnen Sie die Seite **Local User Database**.
2. Klicken Sie auf **Add**. Die Seite **Add User** wird geöffnet:

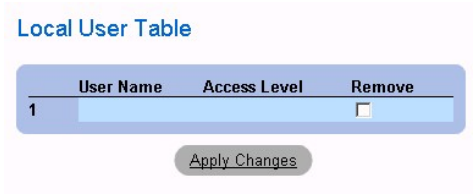


Seite "Add User"

3. Definieren Sie einen neuen Benutzernamen in den Feldern **User Name, Access Level (1-15), Password** und **Confirm Password**.
4. Klicken Sie auf **Apply Changes.** Der neue Benutzer wird definiert und das Gerät aktualisiert.

Anzeigen der "Local User Table":

1. Öffnen Sie die Seite **Local User Database**.
2. Klicken Sie auf **Show All**. Die Seite **Local User Table** wird geöffnet.



Seite "Local User Table"

Löschen von Benutzern:

1. Öffnen Sie die Seite **Local User Database**.
2. Klicken Sie auf **Show All**. Die Seite **Local User Table** wird geöffnet.
3. Wählen Sie einen **User Name** aus.
4. Aktivieren Sie das Kontrollkästchen **Remove**.
5. Click **Apply Changes**. Der Benutzer wird gelöscht und das Gerät aktualisiert.

Zuweisen von Benutzern mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
username *Name* **[password** *Passwort***] [privilege** *Ebene***] [encrypted]**	Richtet ein auf Benutzernamen basierendes Authentisierungssystem ein.

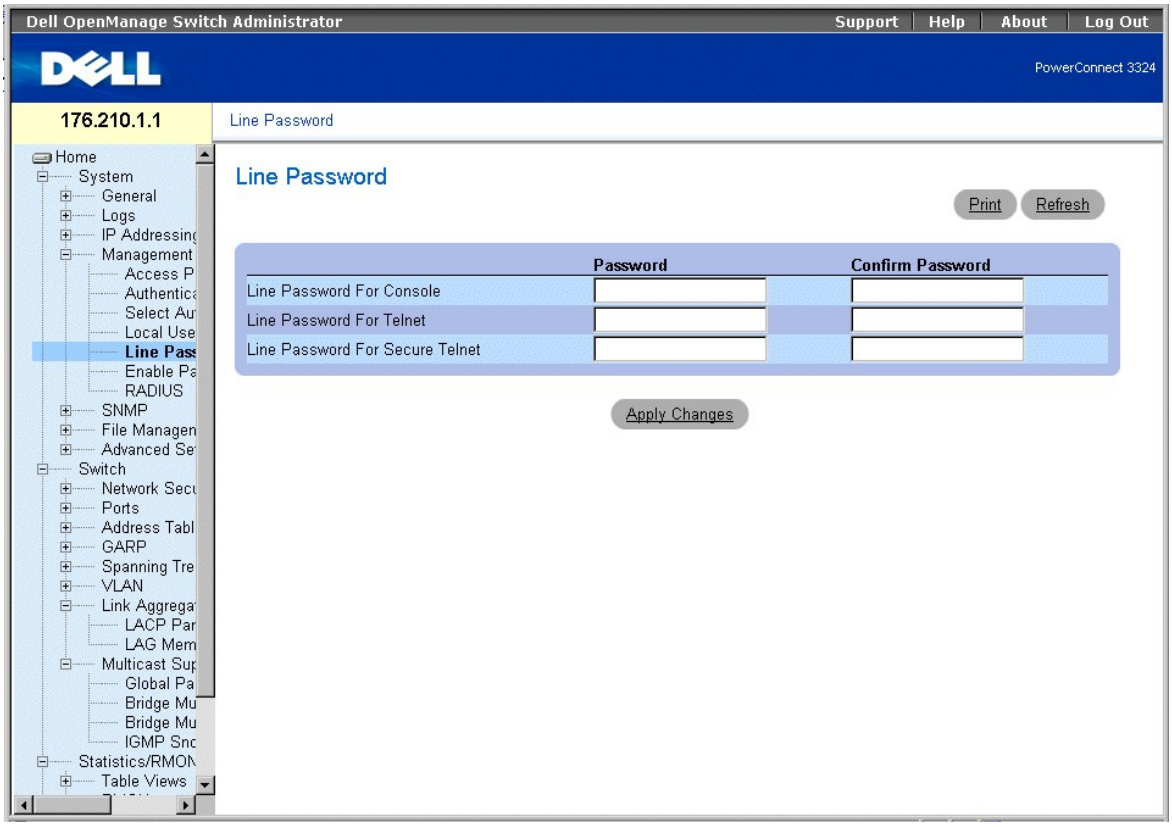
Im Folgenden ein Beispiel für die CLI-Befehle:

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

Definieren von Leitungspasswörtern

Auf der Seite **Line Passwords** können Netzwerkverwalter Leitungspasswörter für Verwaltungsmethoden definieren. Die Passwortlänge ist auf maximal 16 Zeichen beschränkt. So öffnen Sie die Seite **Line Passwords**:

- Klicken Sie in der Strukturansicht auf **System** > **Management Security** > **Line Passwords**. Die Seite **Line Password** wird geöffnet.



Seite "Line Password"

Die Seite **Line Password** enthält folgende Felder:

- **Line Password For Console** - Gibt das Leitungspasswort für den Gerätezugriff über eine Konsolensitzung an. Das Passwort wird als ******* angezeigt.
- **Line Password For Telnet** - Gibt das Leitungspasswort für den Gerätezugriff über eine Telnet-Sitzung an. Das Passwort wird als ******* angezeigt.
- **Line Password For Secure Telnet** - Gibt das Leitungspasswort für den Gerätezugriff über eine Secure Telnet-Sitzung an. Das Passwort wird als ******* angezeigt.

Definieren von Leitungspasswörtern für Konsolensitzungen:

1. Öffnen Sie die Seite **Line Password**.
2. Definieren Sie das Feld **Line Password for Console**.
3. Klicken Sie auf **Apply Changes**. Das Leitungspasswort für Konsolensitzungen wird definiert und das Gerät aktualisiert.

Definieren von Leitungspasswörtern für Telnet-Sitzungen:

1. Öffnen Sie die Seite **Line Password**.
2. Definieren Sie das Feld **Line Password for Telnet**.
3. Klicken Sie auf **Apply Changes**. Das Leitungspasswort für Telnet-Sitzungen wird definiert und das Gerät aktualisiert.

Definieren von Leitungspasswörtern für Secure Telnet-Sitzungen:

1. Öffnen Sie die Seite **Line Password**.
2. Definieren Sie das Feld **Line Password for Secure Telnet**.
3. Klicken Sie auf **Apply Changes**. Das Leitungspasswort für Secure Telnet-Sitzungen wird definiert und das Gerät aktualisiert.

Zuweisen von Leitungspasswörtern mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
password *Passwort* **[encrypted]**	Legt ein Passwort für eine Leitung fest.

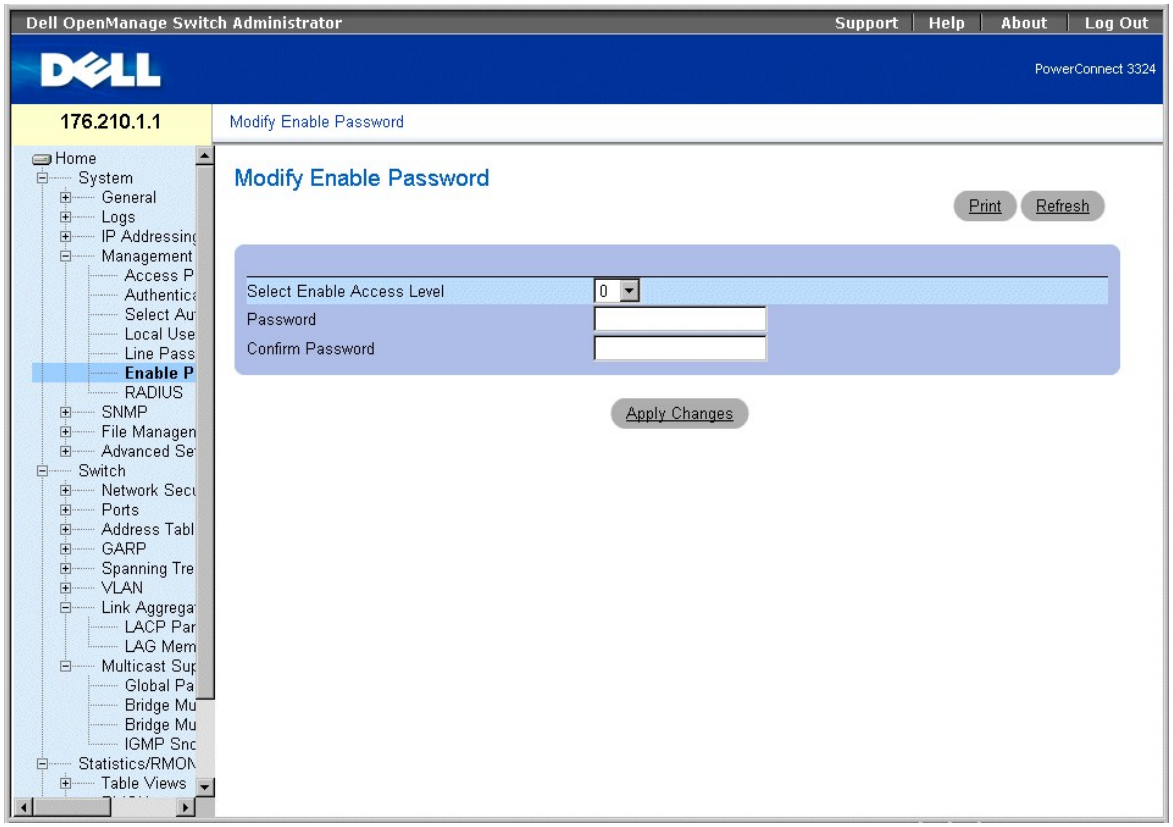
Im Folgenden ein Beispiel für die CLI-Befehle:

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

Definieren von Aktivierungspasswörtern

Auf der Seite **Modify Enable Password** wird ein lokales Passwort festgelegt, um den Zugriff auf den normalen, privilegierten und globalen Konfigurationsmodus zu steuern. So öffnen Sie die Seite **Modify Enable Password**.

- Klicken Sie in der Strukturansicht auf **System** > **Management Security** > **Enable Passwords**. Die Seite **Modify Enable Password** wird geöffnet.



Seite "Modify Enable Password"

Die Seite **Modify Enable Password** enthält folgende Felder:

- **Select Enable Access Level** - Legt die mit dem Aktivierungspasswort verknüpfte Zugriffsebene fest.
- **Password** - Gibt das Aktivierungspasswort an. Das Passwort wird als ******* angezeigt.
- **Confirm Password** - Bestätigt das neue Aktivierungspasswort. The confirmed password is displayed as *******.

Definieren eines neuen Aktivierungspassworts:

1. So öffnen Sie die Seite **Modify Enable Password**.
2. Definieren Sie die Felder **Select Enable Access Level, Password** und **Confirm Password**.
3. Click **Apply Changes**. Das neue Aktivierungspasswort wird definiert und das Gerät aktualisiert.

Zuweisen von Aktivierungspasswörtern mit Hilfe der CLI-Befehle

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

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

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# enable password level 15 dell

Console# show users accounts

Username Privilege

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

Bob 15

Robert 15
```

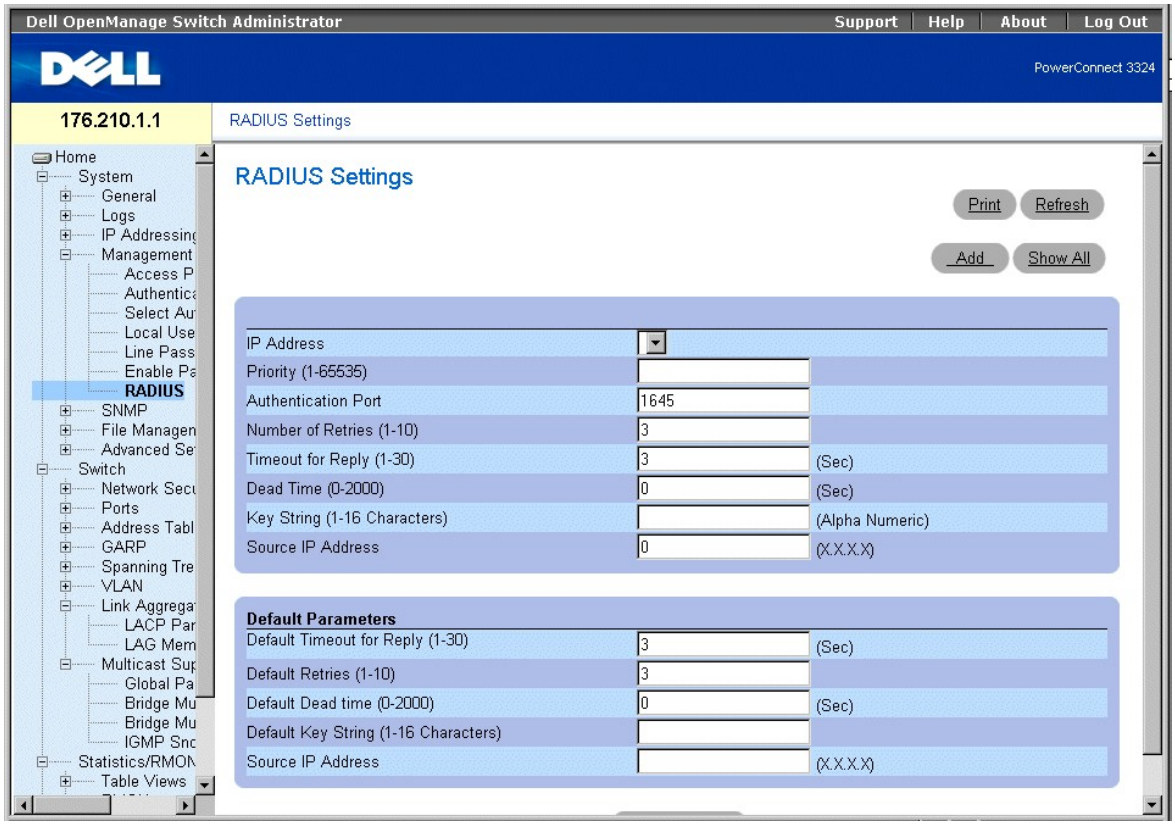
Konfigurieren globaler RADIUS-Parameter

Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. RADIUS-Server stellen eine zentralisierte Authentisierungsmethode für folgende Zugriffsarten bereit:

- Telnet-Zugriff
- Webzugriff
- Konsolenzugriff auf Switches

So öffnen Sie die Seite **RADIUS Settings**:

- Klicken Sie in der Strukturansicht auf **System** > **Management Security** >**RADIUS**. Die Seite **RADIUS Settings** wird geöffnet.



Seite "RADIUS Settings"

Die Seite **RADIUS Settings** enthält folgende Felder:

- **IP Address** - Gibt die Liste der IP-Adressen für Authentisierungsserver an.
- **Priority (1-65535)** - Gibt die Priorität der Server an. Die möglichen Werte liegen im Bereich von 1 bis 65.535, wobei 1 den höchsten Wert darstellt. This is used to configure the order in which servers are queried.
- **Authentication Port** - Gibt den Authentisierungsanschluss an. The authentication port is used to verify the RADIUS server authentication.
- **Number of Retries (1-10)** - Gibt die Anzahl der Anforderungen an, die an den RADIUS-Server gesendet werden können, bevor ein Fehler auftritt. The possible field values are 1-10. Three is the default value
- **Timeout for Reply (1-30)** &#
  - **Deny** - Unterbindet den Verwaltungszugriff auf die definierte Schnittstelle.-{}-
  - **Deny** - Unterbindet den Verwaltungszugriff auf die definierte Schnittstelle.-{}-; Gibt die Zeit in Sekunden an, die das Gerät auf eine Antwort vom RADIUS-Server wartet, bevor die Abfrage wiederholt oder der nächste Server abgefragt wird. The possible field values are 1-30. Three is the default value.
- **Dead Time (0-2000)** - Gibt die Zeit (in Sekunden) an, während der ein RADIUS-Server für Dienstanforderungen umgangen wird. The range is 0-2000.
- **Key String (1-16 Characters)** - Gibt die Schlüsselzeichenfolge an, die für die Authentisierung und Verschlüsselung der gesamten RADIUS-Kommunikation zwischen Gerät und RADIUS-Server verwendet wird. Dieser Schlüssel ist verschlüsselt.
- **Source IP Address** - Gibt die IP-Adresse an, die für das Gerät, das auf den RADIUS-Server zugreift, verwendet werden soll.

Durch die folgenden Felder werden die RADIUS-Standardwerte festgelegt:

- **Default Timeout for Reply (1-30)** - Gibt das Standardzeitintervall (in Sekunden) an, das ein Gerät auf eine Antwort vom RADIUS-Server wartet, bevor eine Zeitüberschreitung auftritt.

ANMERKUNG: If Falls für **Host Specific Timeouts, Retransmit, Dead Time** oder **Deny** keine Werte angegeben sind, werden die globalen Werte auf die einzelnen Hosts angewendet.

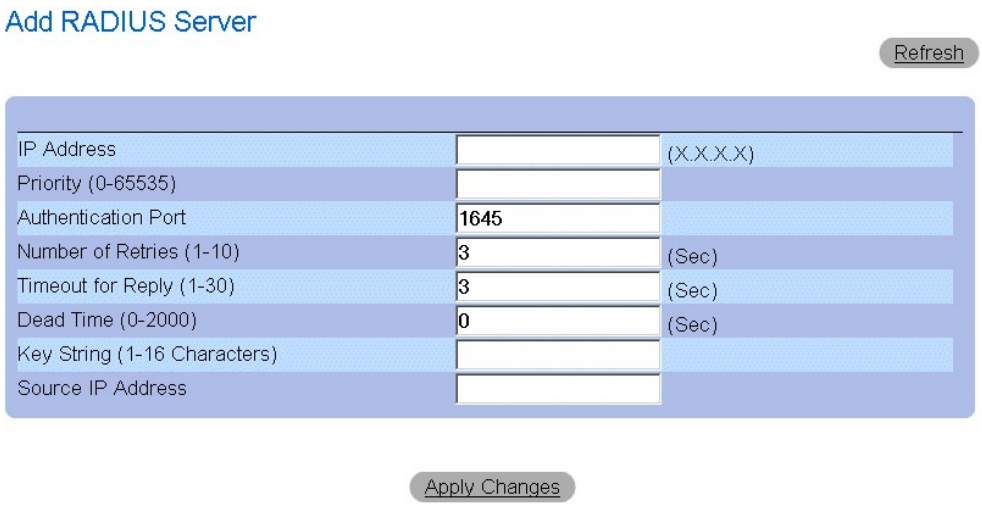
- **Default Retries (1-10)** - Gibt die Standardanzahl der Anforderungen an, die an den RADIUS-Server gesendet werden können, bevor ein Fehler auftritt.
- **Default Dead time (0-2000)** - Gibt das Standardzeitintervall (in Sekunden) an, während dem ein RADIUS-Server für Dienstanforderungen umgangen wird. Der Bereich liegt bei: 0 bis 2000.
- **Default Key String (1-16 Characters)** - Gibt die Standardschlüsselzeichenfolge an, die für die Authentisierung und Verschlüsselung der gesamten RADIUS-Kommunikation zwischen Gerät und RADIUS-Server verwendet wird. Dieser Schlüssel ist verschlüsselt.
- **Source IP Address** - Gibt die IP-Standardadresse für das Gerät an, das auf den RADIUS-Server zugreift.

Definieren von RADIUS-Parametern:

1. Öffnen Sie die Seite **RADIUS Settings**.
2. Definieren Sie die Felder **Default Timeout for Reply, Default Retries, Default Dead Time** und **Default Key Strings**.
3. Klicken Sie auf **Apply Changes**. Die RADIUS-Einstellungen für das Gerät werden aktualisiert.

Hinzufügen eines RADIUS-Servers:

1. Öffnen Sie die Seite **RADIUS Settings**.
2. Klicken Sie auf **Add**. Die Seite **Add RADIUS Settings** wird geöffnet:



Seite "Add RADIUS Server"

3. Definieren Sie die Felder **IP Address, Priority, Authentication Port, Number of Retries, Timeout for Reply, Dead Time, Key String** und **Source IP Address**.
4. Klicken Sie auf **Apply Changes**. Der neue RADIUS-Server wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der RADIUS Servers List:

1. Öffnen Sie die Seite **RADIUS Settings**.
2. Klicken Sie auf **Show All**. Die Seite **RADIUS Servers List** wird geöffnet.

Seite "RADIUS Servers List"

Ändern der RADIUS-Servereinstellungen:

1. Öffnen Sie die Seite **RADIUS Settings**.
2. Klicken Sie auf **Show All**. Die Seite **RADIUS Servers List** wird geöffnet.
3. Ändern Sie die Felder **Priority, Number of Retries, Timeout for Reply** oder **Dead Time**.
4. Klicken Sie auf **Apply Changes**. Die RADIUS-Servereinstellungen werden geändert und das Gerät aktualisiert.

Löschen eines RADIUS-Servers aus der RADIUS Servers List:

1. Öffnen Sie die Seite **RADIUS Settings**.
2. Klicken Sie auf **Show All**. Die Seite **RADIUS Servers List** wird geöffnet.
3. Wählen Sie einen RADIUS-Server in der Liste **RADIUS Servers List** aus.
4. Aktivieren Sie das Kontrollkästchen **Remove**. Der RADIUS-Server wird aus der **RADIUS Servers List** entfernt.

Definieren von RADIUS-Servern mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
radius-server timeout *Zeitlimit*	Legt das Standardintervall fest, während dem ein Gerät auf die Antwort eines Server-Hosts wartet.
radius-server retransmit *Wiederholungsversuche*	Legt fest, wie häufig die Liste der RADIUS-Server-Hosts standardmäßig von der Software durchsucht wird.
radius-server deadtime *Totzeit*	Legt fest, dass nicht verfügbare Standardserver übersprungen werden.
radius-server key *Schlüsselzeichenfolge*	Legt den Standardschlüssel für die Authentisierung und Verschlüsselung der gesamten RADIUS-Kommunikation zwischen dem Gerät und der RADIUS-Umgebung fest.
radius-server host *IP-Adresse* **[auth-port** *Auth.-Anschlussnummer***] [timeout** *Zeitlimit***] [retransmit** *Wiederholungsversuche***] [deadtime** *Totzeit***] [key** *Schlüsselzeichenfolge***] [source** *Quelle***] [priority** *Priorität***]**	Legt einen RADIUS-Server-Host sowie beliebige Einstellungen fest, die nicht den Standardeinstellungen entsprechen.
show radius-servers	Zeigt die RADIUS-Servereinstellungen an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
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 1645 timeout 20

Console# show radius-servers

Port

IP address Auth Acct TimeOut Retransmit deadtime Priority
```

```
---------- ---- ---- ------- ---------- -------- --------

172.16.1.1 1645 1646 3 3 0 1

172.16.1.2 1645 1646 11 8 0 2
```

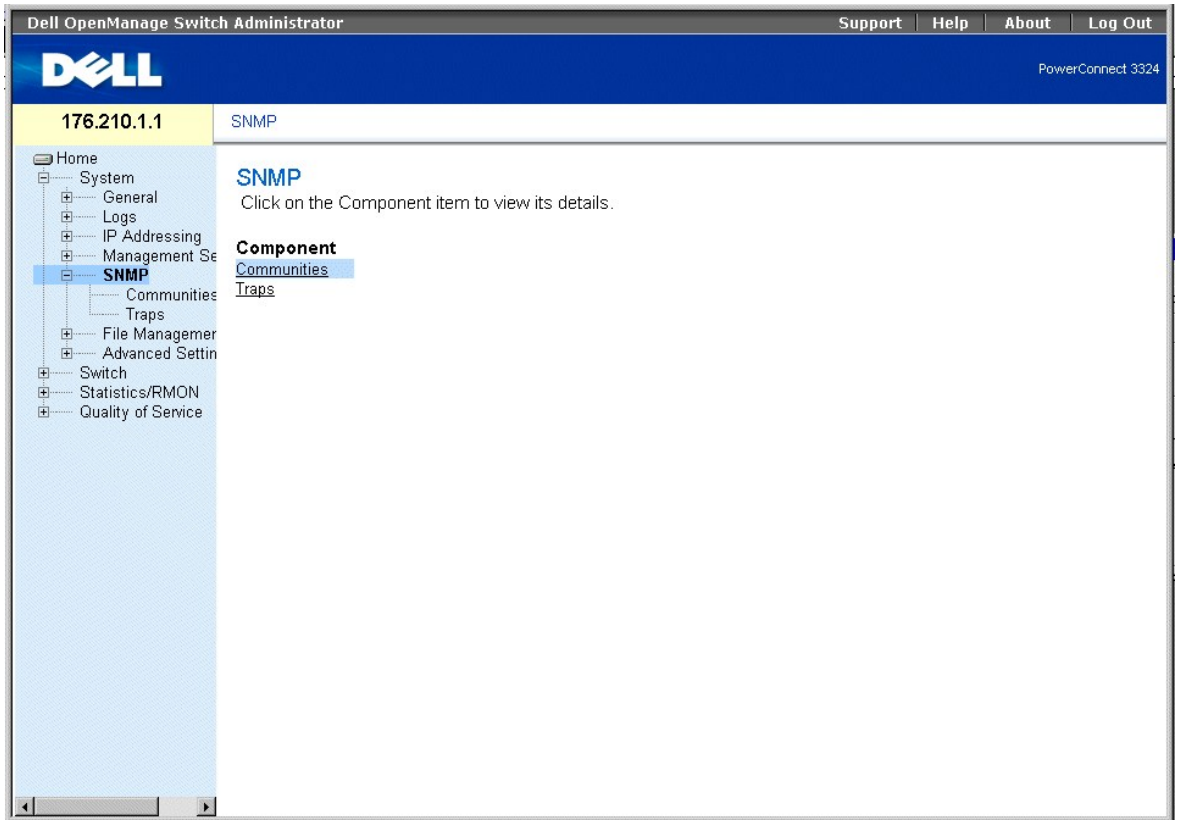
Definieren von SNMP-Parametern

Simple Network Management Protocol (SNMP) provides a method for managing network devices. Auf Geräten, die SNMP unterstützen, wird eine lokale Software (ein Agent) ausgeführt.

Die SNMP-Agenten verwalten eine Liste von Variablen, die zur Verwaltung des Gerätes verwendet werden. The variables are defined in the Management Information Base (MIB). Die MIB stellt die vom Agenten gesteuerten Variablen dar. Das SNMP-Protokoll definiert das Format für die MIB-Spezifikationen sowie das Format für den Netzwerkzugriff auf Daten.

Die Zugriffsrechte auf die SNMP-Agenten werden über Zugriffszeichenfolgen gesteuert. Um mit dem Gerät zu kommunizieren, übermittelt der integrierte Webserver zuerst eine gültige Community-Zeichenfolge für die Authentisierung. So öffnen Sie die Seite SNMP:

- Klicken Sie in der Strukturansicht auf **System** > **SNMP**. Die Seite **SNMP** wird geöffnet.



Seite "SNMP"

Dieser Abschnitt bietet Informationen zur Verwaltung der SNMP-Konfiguration und umfasst folgende Themen:

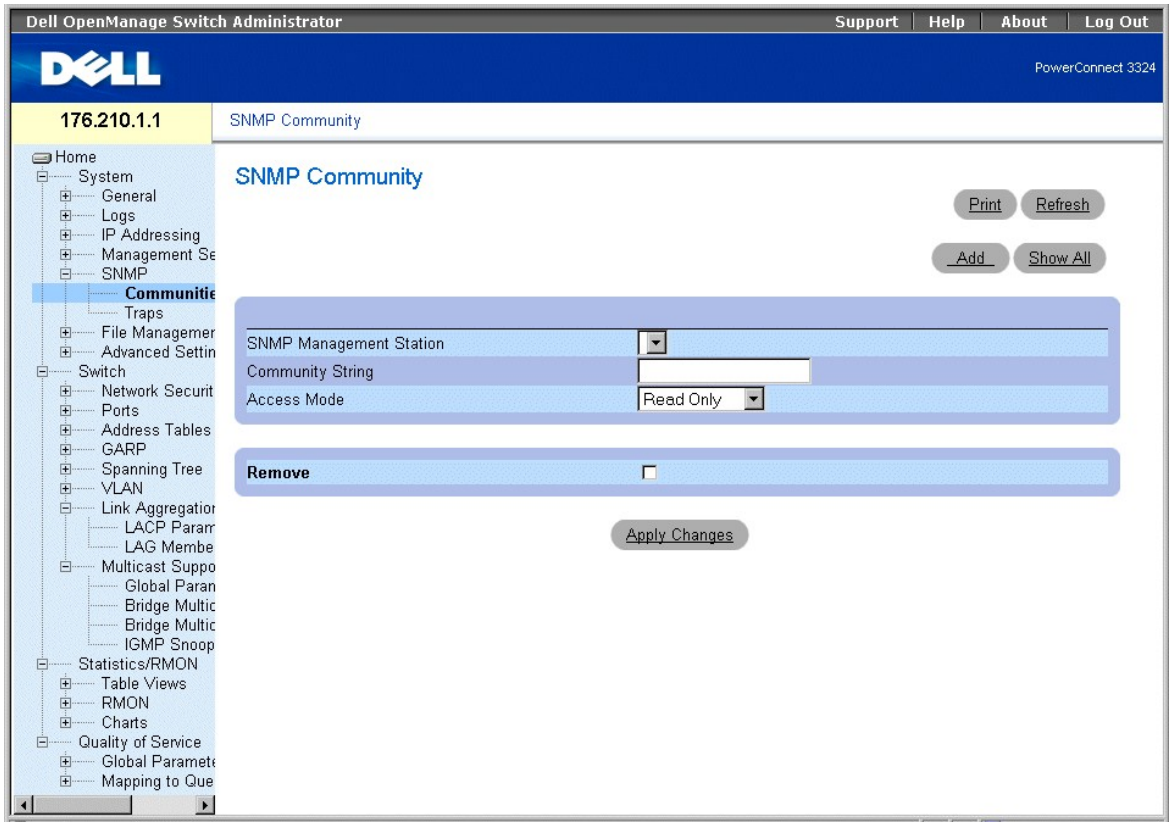
- Definieren von Communities

- Definieren von Traps

Definieren von Communities

Der Systemadministrator verwaltet Zugriffsrechte (Lese-/Schreibzugriff, Nur-Lese-Zugriff usw.), indem er Communities in der Community Table definiert. Sobald der Name einer Community geändert wird, ändern sich auch die Zugriffsrechte. So öffnen Sie die Seite **SNMP Community**:

- Klicken Sie in der Strukturansicht auf **System** > **SNMP** > **Communities**. Die Seite **SNMP Community** wird geöffnet.



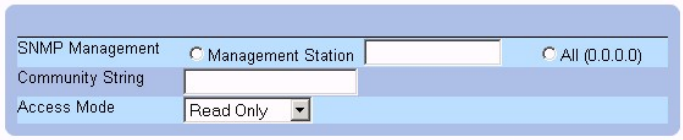
Seite "SNMP Community"

Die Seite **SNMP Community** enthält folgende Felder:

- **SNMP Management Station** - Enthält eine Liste mit IP-Adressen von Management-Stationen.
- **Community String** - Hat die Funktion eines Passworts und wird zur Authentisierung der ausgewählten Management-Station gegenüber dem Gerät verwendet.
- **Access Mode** - Definiert die Zugriffsrechte der Community. Folgende Feldwerte sind möglich:
  - **Read Only** - Gibt an, dass sich der Verwaltungszugriff auf Lesezugriffe beschränkt und dass keine Änderungen an der Community vorgenommen werden können.
  - **Read Write** - Gibt an, dass Verwaltungszugriffe in Form von Lese- und Schreibzugriffen möglich sind und dass zwar die Gerätekonfiguration, nicht aber die Community geändert werden kann.
  - **SNMP Admin** - Gibt an, dass der Benutzer Zugriff auf sämtliche Gerätekonfigurationsoptionen hat und auch die Community ändern kann.
- **Remove** - Entfernt eine Community. Folgende Feldwerte sind möglich:
  - **Aktiviert** - Entfernt die Community.
  - **Deaktiviert** - Behält die Community bei.

Definieren einer neuen Community:

1. Öffnen Sie die Seite **SNMP Community.**
2. Klicken Sie auf **Add**. Die Seite **Add SNMP Community** wird geöffnet.



Seite "Add SNMP Community"

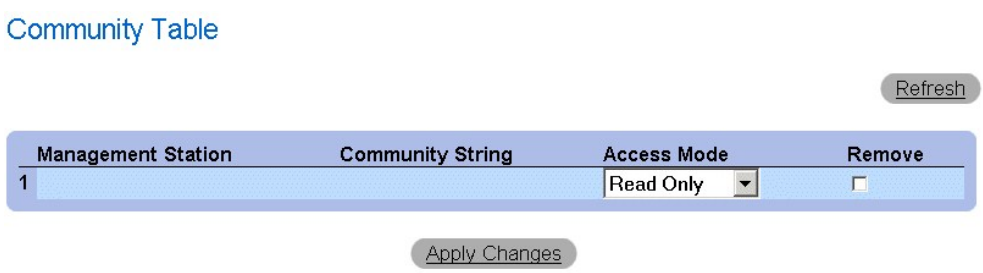
Neben den auf der Seite **SNMP Community** enthaltenen Feldern bietet die Seite **Add SNMP Community** folgende Felder:

- **SNMP Management** - Gibt an, ob eine SNMP-Community für eine bestimmte Management-Station oder für alle Management-Stationen definiert wurde. Folgende Feldwerte sind möglich:
  - **Management Station** - Gibt die IP-Adresse der Management-Station an. Der Wert 0.0.0.0 steht für sämtliche Management-Stationen.
  - **All** - Gibt an, dass die SNMP-Community für alle Management-Stationen definiert wurde.

3. Definieren Sie die Felder **SNMP Management, Management Station, Community String** und **Access Mode**.
4. Klicken Sie auf **Apply Changes.** Die neue Community wird gespeichert und das Gerät aktualisiert.

Anzeigen aller Communities

1. Öffnen Sie die Seite **SNMP Community.**
2. Klicken Sie auf **Show All**. Die Seite **Community Table** wird geöffnet.



Seite "Community Table"

Löschen von Communities:

1. Öffnen Sie die Seite **SNMP Community.**
2. Klicken Sie auf **Show All**. Die Seite **Community Table** wird geöffnet.
3. Wählen Sie eine Community aus der **Community Table** aus.
4. Aktivieren Sie das Kontrollkästchen **Remove**.
5. Klicken Sie auf **Apply Changes**. Der Community-Eintrag wird gelöscht und das Gerät aktualisiert.

Konfigurieren von Communities mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
snmp-server community *Zeichenfolge* **[ro | rw | su] [***IP-Adresse***]**	Konfiguriert die Community-Zugriffszeichenfolge so, dass SNMP-Protokollzugriffe zulässig sind.
show snmp	Überprüft den Status der SNMP-Kommunikation.

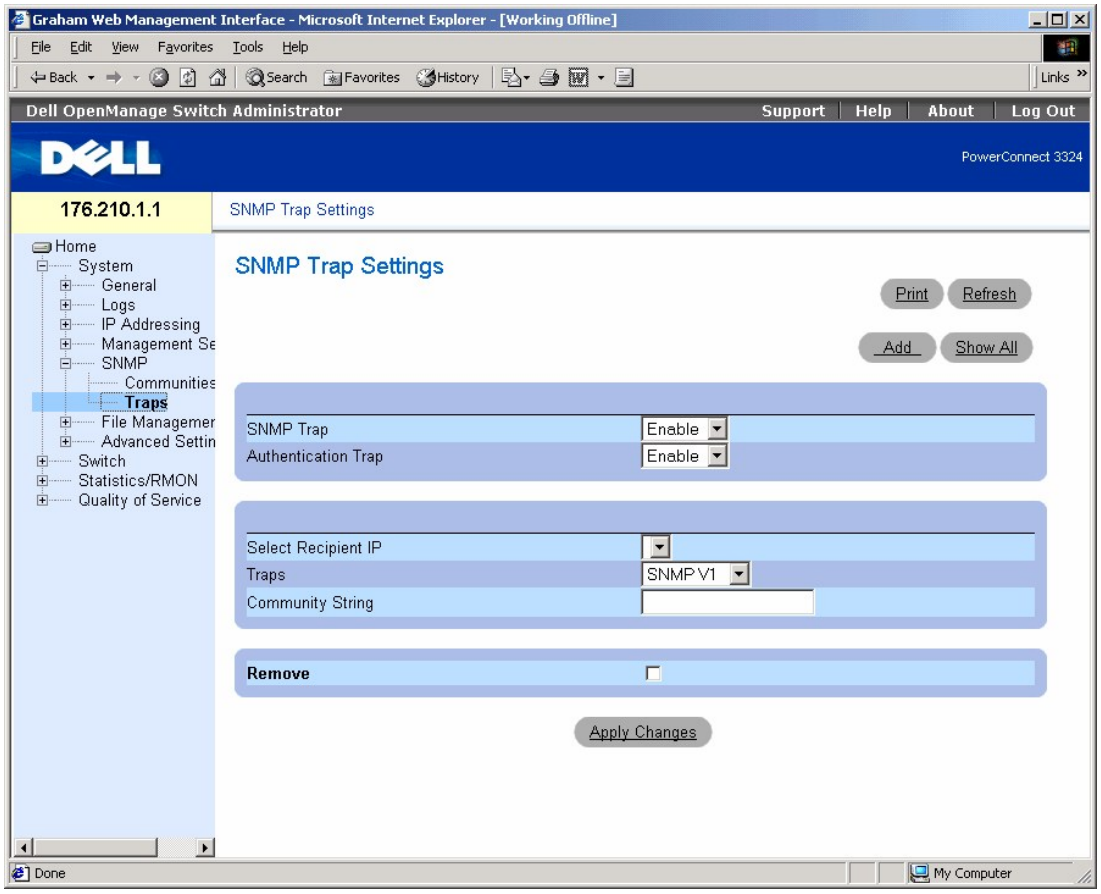
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# snmp-server community public su 0.0.0.0
```

Definieren von Traps

Über die Seite **SNMP Trap Settings** kann der Benutzer das Senden von SNMP-Traps oder -Benachrichtigungen durch das Gerät aktivieren oder deaktivieren. So öffnen Sie die Seite **SNMP Trap Settings**:

- Klicken Sie in der Strukturansicht auf **System** > **SNMP** > **Traps**. Die Seite **SNMP Trap Settings** wird geöffnet.



Seite "SNMP Trap Settings"

Die Seite **SNMP Trap Settings** enthält die folgenden Felder:

- **SNMP Trap** - Aktiviert das Senden von SNMP-Traps oder SNMP-Benachrichtigungen vom Switch zu festgelegten Trap-Empfängern. Folgende Feldwerte sind möglich:
  - **Enable** - Aktiviert das Senden von SNMP-Traps oder SNMP-Benachrichtigungen.
  - **Disable**
  - **Deny** - Unterbindet den Verwaltungszugriff auf die definierte Schnittstelle. Unterbindet das Senden jeglicher SNMP-Traps.
- **Authentication Trap** - Aktiviert das Senden von SNMP-Traps, wenn festgelegte Empfänger nicht authentisiert werden können. Folgende Feldwerte sind möglich:
  - **Enable** - Aktiviert das Senden von SNMP-Traps, wenn die Authentisierung fehlschlägt.

- **Disable** - Deaktiviert das Senden von SNMP-Traps, wenn die Authentisierung fehlschlägt.

- **Select Recipient IP** - Legt die IP-Adresse des Empfängers fest, an den die Traps gesendet werden.
- **Traps** - Legt den Typ des an den ausgewählten Empfänger gesendeten Traps fest. Folgende Feldwerte sind möglich:
  - **SNMP V1** - Gibt an, dass Traps von SNMP Version 1 gesendet werden.
  - **SNMP V2c** - Gibt an, dass Traps von SNMP Version 2 gesendet werden.
  - **Disable** - Deaktiviert das Senden von Traps an den Empfänger.
- **Community String** - Gibt die Community-Zeichenfolge des Trap Managers an.
- **Remove** - Entfernt Einträge aus der **Trap Manager Table**.
  - **Aktiviert** - Entfernt den Eintrag aus der **Trap Manager Table**.
  - **Unchecked**-Maintains the **Trap Manager Table** entry.

Aktivieren von SNMP-Traps für das Gerät:

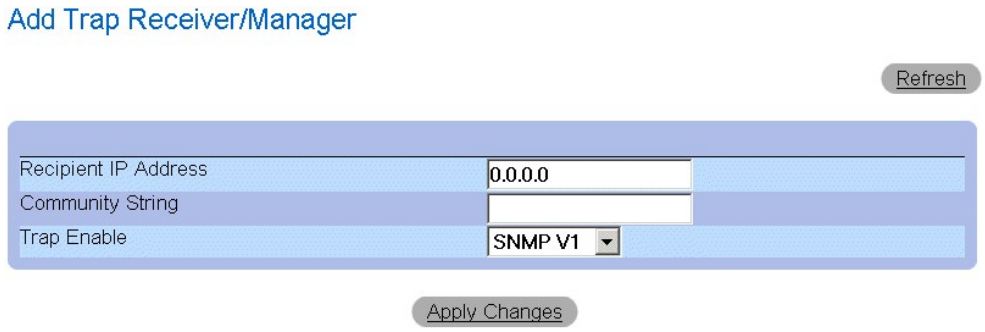
1. Öffnen Sie die Seite **SNMP Trap Settings**.
2. Wählen Sie **Enable** in der Dropdown-Liste **SNMP Trap**.
3. Definieren Sie die Felder **Select Recipient IP, Traps** und **Community String**.
4. Klicken Sie auf **Apply Changes**. Die SNMP-Traps werden für das Gerät aktiviert.

Aktivieren von Authentisierungs-Traps für das Gerät:

1. Öffnen Sie die Seite **SNMP Trap Settings**.
2. Wählen Sie **Enable** in der Dropdown-Liste **Authentication Trap**.
3. Definieren Sie die Felder **Select Recipient IP, Traps** und **Community String**.
4. Klicken Sie auf **Apply Changes**. Die Authentisierungs-Traps werden für das Gerät aktiviert.

Hinzufügen eines neuen Trap-Empfängers:

1. Öffnen Sie die Seite **SNMP Trap Settings**.
2. Klicken Sie auf **Add**. Die Seite **Add Trap Receiver / Manager** wird geöffnet.



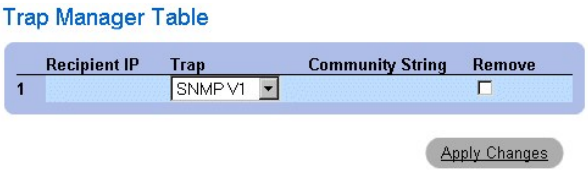
Seite "Add Trap Receiver / Manager"

3. Definieren Sie die Felder **Recipient IP Address, Community String** und **Trap Enable**. (Beachten Sie, dass 0.0.0.0 für "Alle" steht und dass die Traps an alle Empfänger weitergeleitet werden.)
4. Klicken Sie auf **Apply Changes**. Der Trap-Empfänger/Trap Manager wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der Trap Managers Table:

Die **Trap Managers Table** enthält Felder zum Konfigurieren von Trap-Typen.

1. Öffnen Sie die Seite **Traps**.
2. Klicken Sie auf **Show All**. Die Seite **Trap Manager Table** wird geöffnet.



Seite "Trap Manager Table"

Löschen eines Eintrags aus der Trap Manager Table:

1. Öffnen Sie die Seite **SNMP Trap Settings**.
2. Klicken Sie auf **Show All**. Die Seite **Trap Manager Table** wird geöffnet.
3. Wählen Sie einen Eintrag in der **Trap Managers Table** aus.
4. Aktivieren Sie das Kontrollkästchen **Remove**.
5. Klicken Sie auf **Apply Changes**. Der Trap Manager wird gelöscht und das Gerät aktualisiert.

Konfigurieren von Traps mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
snmp-server enable traps	Aktiviert den Versand von SNMP-Traps oder SNMP-Benachrichtigungen durch den Switch.
snmp-server trap authentication	Aktiviert den Versand von SNMP-Traps durch den Switch, wenn die Authentisierung fehlschlägt.
snmp-server host host-addr community-string [1 | 2]	Legt den Typ des an den ausgewählten Empfänger gesendeten Traps fest.
show snmp	Zeigt den SNMP-Kommunikationsstatus an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# snmp-server enable traps

Console (config)# snmp-server trap authentication

Console (config)# snmp-server host 10.1.1.1 trapRec 2

Console (config)# exit

Console# show snmp


Community-String Community-Access IP address

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

public read only All
```

```
private read write 172.16.1.1

private read write 172.16.1.1



Traps are enabled.

Authentication trap is enabled.



Trap-Rec-Address Trap-Rec-Community Version

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

192.122.173.42 public 2



System Contact : Robert

System Location : Marketing
```

Verwalten von Dateien

Auf der Seite **File Management** können Netzwerkverwalter Gerätesoftware, Image-Dateien und Konfigurationsdateien verwalten. Die Dateien können von einem TFTP-Server heruntergeladen werden.

Übersicht über die Dateiverwaltung

Die Konfigurationsdateistruktur umfasst die folgenden Dateien:

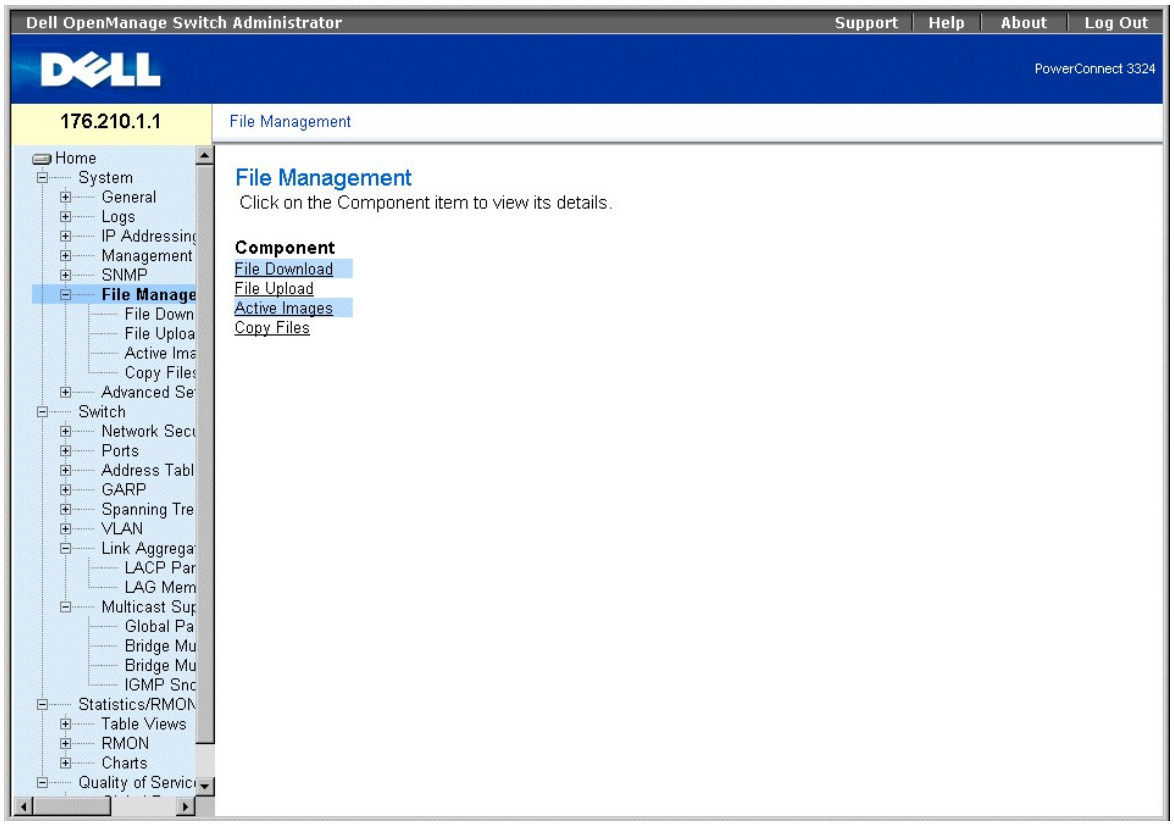
- Datei "Startup Configuration" - In dieser Datei wird die exakte Gerätekonfiguration gespeichert, wenn das Gerät ausgeschaltet oder neu gestartet wird. In der Datei "Startup Configuration" werden Konfigurationsbefehle verwaltet. Außerdem können Konfigurationsbefehle aus der Datei "Running Configuration" in der Datei "Startup Configuration" gespeichert werden.
- Datei "Running Configuration" - Enthält sämtliche Befehle aus der Datei "Startup Configuration" sowie alle während der aktuellen Sitzung eingegebenen Befehle. Nachdem das Gerät ausgeschaltet oder neu gestartet wurde, werden alle in der Datei "Running Configuration" gespeicherten Befehle verworfen. Während des Startvorgangs werden alle Befehle aus der Datei "Startup Configuration" in die Datei "Running Configuration" kopiert und auf das Gerät angewendet. Während der Sitzung werden alle neu eingegebenen Befehle den in der Datei "Running Configuration" bereits enthaltenen Befehlen hinzugefügt. Befehle werden nicht überschrieben. Um die Datei "Startup Configuration" zu aktualisieren, muss die Datei "Running Configuration" in die Datei "Startup Configuration" kopiert werden, bevor das Gerät ausgeschaltet wird. Wenn das Gerät das nächste Mal neu gestartet wird, werden die Befehle von der Datei "Startup Configuration" zurück in die Datei "Running Configuration" kopiert.

ANMERKUNG: Konfigurationsbefehle werden mit der Datei "Running Configuration" zusammengeführt und direkt auf das Gerät angewendet.

- Datei "Backup Configuration" - Enthält eine Sicherungskopie der Gerätekonfiguration. Die Datei "Backup Configuration" ändert sich, sobald die Datei "Running Configuration" oder "Startup Configuration" in die Datei "Backup Configuration" kopiert werden. Die in der Datei "Backup Configuration" enthaltenen Befehle werden durch die in die Datei kopierten Befehle ersetzt. Der Inhalt der Datei "Backup Configuration" kann sowohl in die Datei "Running Configuration" als auch in "Startup Configuration" kopiert werden.
- Image-Dateien - System-Images werden in zwei FLASH-Dateien gespeichert, die als Images (Image 1 und Image 2) bezeichnet werden. Im aktiven Image wird die aktive Kopie und im zweiten Image eine weitere Kopie gespeichert. Das Gerät wird vom aktiven Image aus gestartet und ausgeführt. Falls das aktive Image beschädigt ist, startet das System automatisch vom nicht aktiven Image aus. Hierbei handelt es sich um eine Sicherheitsfunktion zum Schutz vor Fehlern, die während der Softwareaktualisierung auftreten können.

So öffnen Sie die Seite **File Management**:

- Klicken Sie in der Strukturansicht auf **System** > **File Management**. Die Seite **File Management** wird geöffnet.



Seite "File Management"

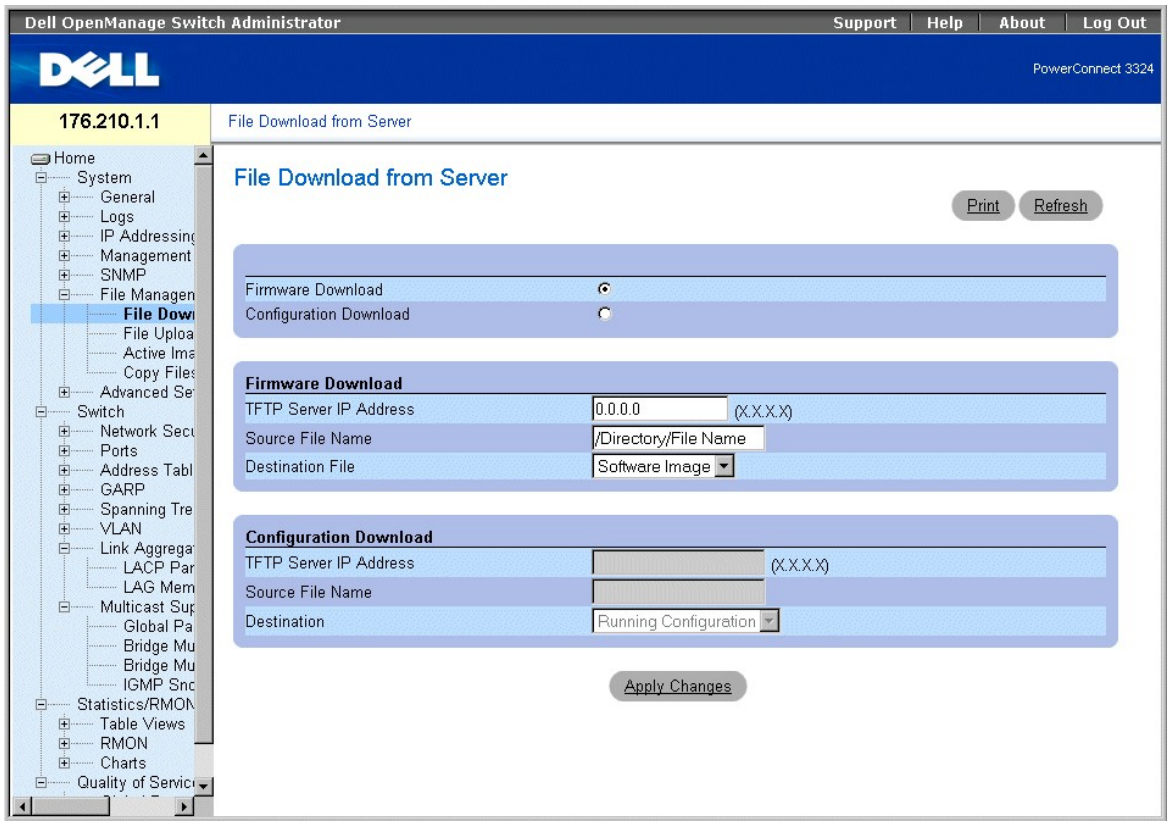
Die Seite **File Management** enthält Links zum:

- Herunterladen von Dateien
- Hochladen von Dateien
- Zurücksetzen des aktiven Images
- Kopieren und Löschen von Dateien

Herunterladen von Dateien

Die Seite **File Download from Server** enthält Felder zum Herunterladen von Image- und Konfigurationsdateien vom TFTP-Server auf das Gerät. So öffnen Sie die Seite **File Download from Server**:

- Klicken Sie in der Strukturansicht auf **System** > **File Management** > **File Download**. Die Seite **File Download from Server** wird geöffnet.



Seite "File Download From Server"

Die Seite **File Download from Server** enthält folgende Felder:

- **Firmware Download** - Gibt an, dass die Firmware-Datei heruntergeladen wird. If Bei Auswahl von **Firmware Download** werden die Felder unter **Configuration Download** grau dargestellt.
- **Configuration Download** - Gibt an, dass die Konfigurationsdatei heruntergeladen wird. Bei Auswahl von **Configuration Download** werden die Felder unter **Firmware Download** grau dargestellt.
- **Firmware Download TFTP Server IP Address** - Gibt die IP-Adresse des TFTP-Servers an, von dem die Dateien heruntergeladen werden.
- **Firmware Download Source File Name** - Legt die Datei fest, die heruntergeladen werden soll.
- **Firmware Download Destination File** - Gibt den Typ der Zieldatei an, in die die Datei heruntergeladen wird. Folgende Feldwerte sind möglich:
  - **Software Image** - Lädt die Image-Datei herunter.
  - **Boot Code** - Lädt die Startdatei herunter.
- **Configuration Download File TFTP Server IP Address** - Gibt die IP-Adresse des TFTP-Servers an, durch den die Konfigurationsdateien heruntergeladen werden.
- **Configuration Download File Source File Name** - Legt die Konfigurationsdateien fest, die heruntergeladen werden sollen.
- **Configuration Download File Destination** - Gibt die Zieldatei an, in die die Konfigurationsdateien heruntergeladen werden. Folgende Feldwerte sind möglich:
  - **Running Configuration** - Lädt Befehle in die Datei "Running Configuration" herunter.
  - **Startup Configuration** - Lädt die Datei "Startup Configuration" herunter und überschreibt die alte Datei.
  - **Backup Configuration** - Lädt die Datei "Backup Configuration" herunter und überschreibt die alte Datei.

Herunterladen von Dateien:

1. Öffnen Sie die Seite **File Download from Server** page.
2. Definieren Sie den Typ der herunterzuladenden Datei.
3. Definieren Sie die Felder **TFTP Server IP Address, Source File Name** und **Destination File**.
4. Klicken Sie auf **Apply Changes.** Die Software wird auf das Gerät heruntergeladen.

ANMERKUNG: Um die ausgewählte Image-Datei zu aktivieren, setzen Sie das Gerät zurück. Informationen zum Zurücksetzen des Gerätes finden Sie unter "Zurücksetzen des Gerätes".

Herunterladen von Dateien mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
copy *Quell-URL Ziel-URL* **[snmp]**	Kopiert eine beliebige Datei von einem Quellort an einen Zielort.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console# copy running-config tftp://11.1.1.2/pp.txt
```

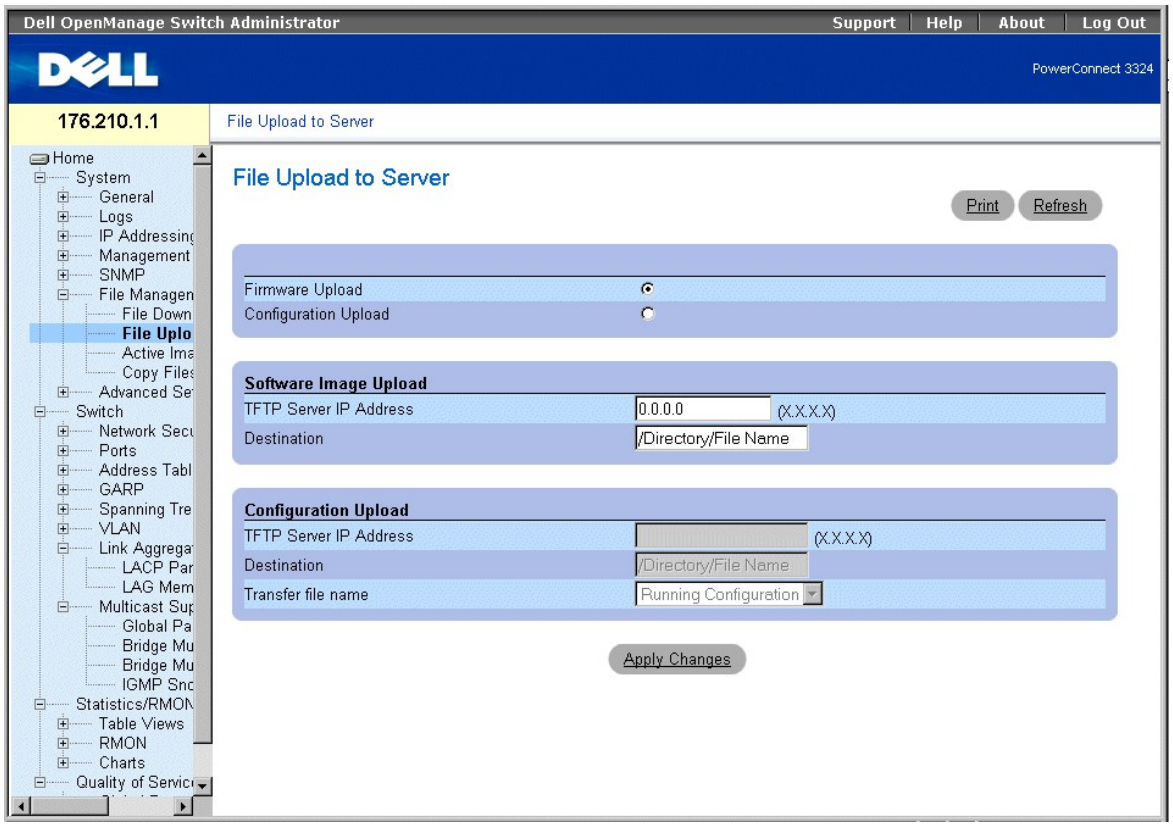
ANMERKUNG: Jedes ! steht für die erfolgreiche Übertragung von 10 Paketen.

```
Accessing file 'file1' on 172.16.101.101.

Loading file1 from 172.16.101.101: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!
[OK]

Copy took 0:01:11 [hh:mm:ss]
```

Hochladen von Dateien

Die Seite **File Upload to Server** enthält Felder zum Hochladen der Software vom TFTP-Server auf das Gerät. Die Image-Datei kann außerdem von der Seite **File Upload to Server** hochgeladen werden. So öffnen Sie die Seite **File Upload to Server**:

- Klicken Sie in der Strukturansicht auf **System** > **File Management** > **File Upload**. Die Seite **File Upload to Server** wird geöffnet:



Seite "File Upload to Server"

Die Seite **File Upload to Server** enthält folgende Felder:

- Firmware Upload - Gibt an, dass die Firmware-Datei hochgeladen wird. Bei Auswahl von **Firmware Upload** werden die Felder unter **Configuration Upload** grau dargestellt.
- **Configuration Upload** - Gibt an, dass die Konfigurationsdatei hochgeladen wird. Bei Auswahl von **Configuration Upload** werden die Felder unter **Software Image Upload** grau dargestellt.
- **Software Image Upload TFTP Server IP Address** - Gibt die IP-Adresse des TFTP-Servers an, auf den das Software-Image hochgeladen wird.
- **Software Image Upload Destination** - Gibt den Dateipfad an, auf den das Software-Image hochgeladen wird.
- **Configuration Upload TFTP Server IP Address** - Gibt die IP-Adresse des TFTP-Servers an, auf den die Konfigurationsdatei hochgeladen wird.
- **Configuration Upload Destination** - Gibt den Dateipfad an, auf den die Konfigurationsdatei hochgeladen wird.
- **Configuration Upload Transfer file name** - Gibt die Softwaredatei an, in die die Konfiguration hochgeladen wird. Folgende Feldwerte sind möglich:
  - **Running Configuration** - Lädt die Datei "Running Configuration" hoch.
  - **Startup Configuration** - Lädt die Datei "Startup Configuration" hoch.
  - **Backup Configuration** - Lädt die Datei "Backup Configuration" hoch.

Hochladen von Dateien:

1. Öffnen Sie die Seite **File Upload to Server.**
2. Definieren Sie den hochzuladenden Dateityp.
3. Definieren Sie die Felder **TFTP Server IP Address, Destination** und **Transfer file name**.
4. Klicken Sie auf **Apply Changes**. Die Software wird auf das Gerät hochgeladen.

Hochladen von Dateien mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Anzeige der Felder zusammengefasst, die auf der Seite **File Upload to Server**

angezeigt werden.

CLI-Befehl	Beschreibung
copy Quell-URL Ziel-URL [snmp]	Kopiert eine beliebige Datei von einem Quellort an einen Zielort.

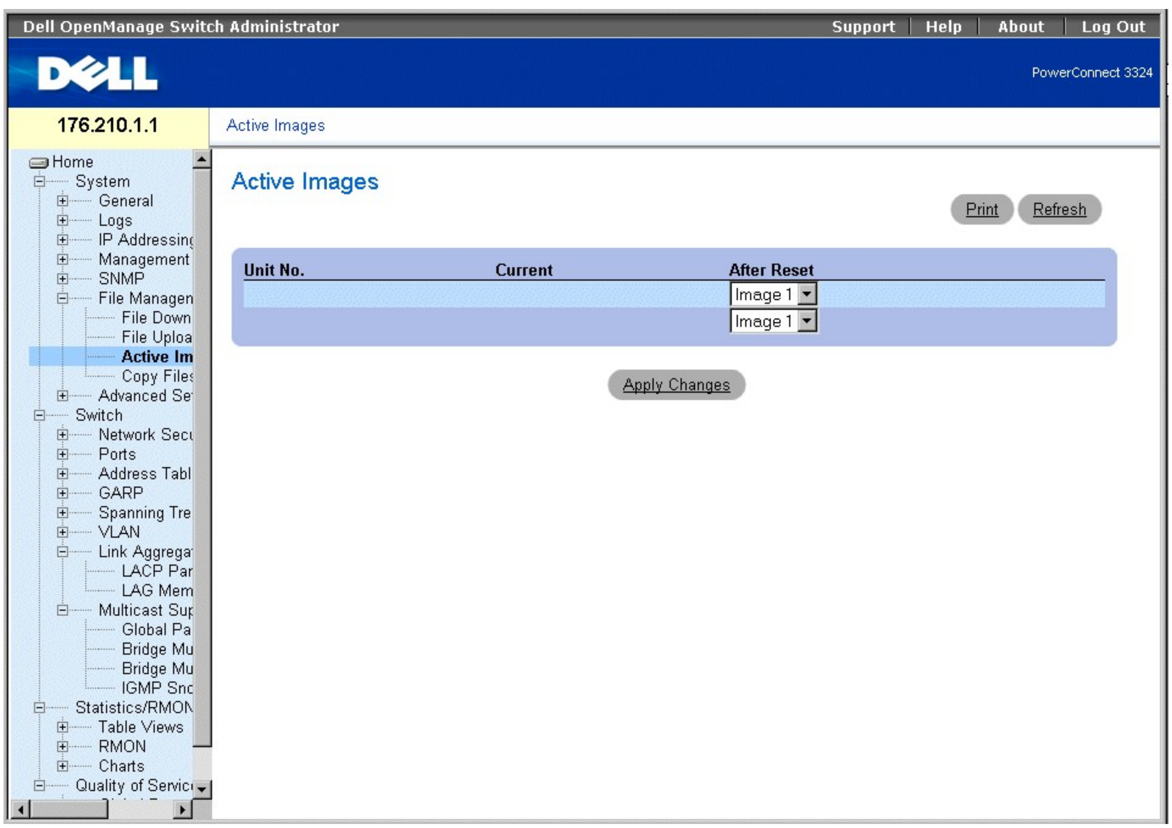
Im Folgenden ein Beispiel für die CLI-Befehle:

```
----------------------------------------------------

console# copy tftp://16.1.1.200/file1 image

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!
2883576 bytes copied in 00:00:10 [hh:mm:ss]
```

Zurücksetzen des aktiven Images

Auf der Seite **Active Images** können Netzwerkverwalter die Image-Dateien auswählen und zurücksetzen. Für jede Einheit in einer Stack-Konfiguration kann die aktive Image-Datei individuell ausgewählt werden. So öffnen Sie die Seite **Active Images**:

- Klicken Sie in der Strukturansicht auf **System** > **File Management** > **Active Images**. Die Seite **Active Images** wird geöffnet.



Seite "Active Images"

Die Seite **Active Images** enthält folgende Felder:

- **Unit No.** - Zeigt die Nummer der Einheit an, für die die Image-Datei ausgewählt wurde.
- **Current** - Zeigt die derzeit auf der Einheit aktive Image-Datei an.
- **After Reset** - Gibt die Image-Datei an, die nach dem Zurücksetzen des Gerätes auf der Einheit aktiv sein wird.

Auswählen einer Image-Datei:

1. Öffnen Sie die Seite **Active Images**.
2. Wählen Sie eine Image-Datei für eine bestimmte Einheit im Feld **After Reset** aus.
3. Klicken Sie auf **Apply Changes**. Die Image-Datei wird ausgewählt. Die Image-Datei wird erst nach dem nächsten Zurücksetzen neu geladen. Die derzeit ausgewählte Image-Datei wird so lange ausgeführt, bis das Gerät das nächste Mal zurückgesetzt wird. Informationen zum Zurücksetzen des Gerätes finden Sie unter "Zurücksetzen des Gerätes".

Verwalten der aktiven Image-Datei mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
boot system [unit | unit] {image-1 | image-2}	Gibt das System-Image an, das beim Start vom Gerät geladen wird.

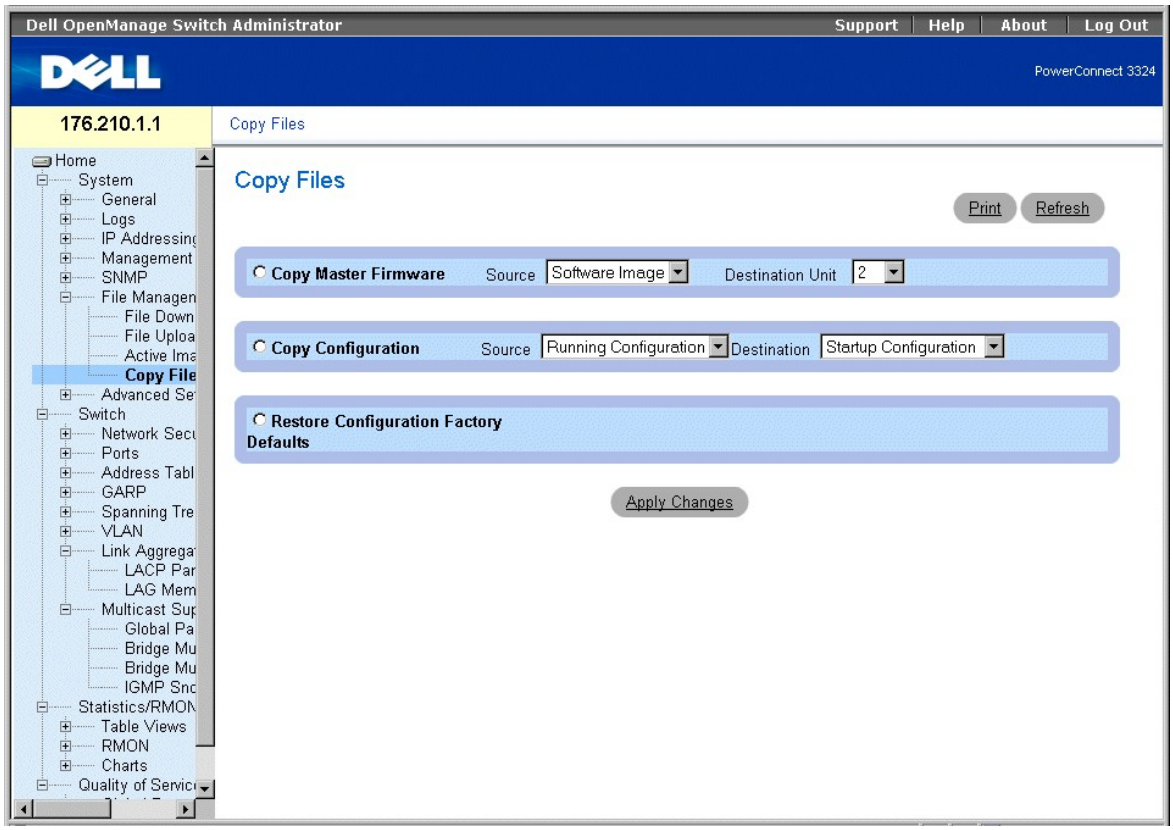
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console# boot system image-1
```

Kopieren und Löschen von Dateien

Dateien können über die Seite **Copy Files** kopiert und gelöscht werden. So öffnen Sie die Seite **Copy Files**:

- Klicken Sie in der Strukturansicht auf **System** > **File Management** > **Copy Files**. Die Seite **Copy Files** wird geöffnet.



Seite "Copy Files"

Die Seite **Copy Files** enthält folgende Felder:

- **Copy Master Firmware** - Kopiert entweder das Software-Image und/oder den Startcode von der Master-Einheit auf eine ausgewählte Stack-Einheit.
  - **Source** - Kopiert entweder die Software-Image- oder Startcodedatei auf die ausgewählte Stack-Einheit.
  - **Destination Unit** - Gibt die Stack-Einheit an, auf die das Software-Image oder der Startcode kopiert wird.
- **Copy Configuration** - Kopiert die Datei "Running Configuration", "Startup Configuration" oder "Backup Configuration" in die Datei "Startup Configuration" oder "Backup Configuration".
  - **Source** - Gibt an, dass entweder die Datei "Running Configuration", "Startup Configuration" oder "Backup Configuration" auf die ausgewählte Stack-Einheit kopiert wird.
  - **Destination** - Gibt die zu überschreibende Konfiguration an, entweder die Start- oder die Sicherungskonfiguration.
- Restore Configuration Factory Defaults - Stellt die werkseitigen Standardkonfigurationsdateien wieder her, indem die Datei "Startup Configuration" gelöscht wird. Beachten Sie, dass die Datei "Backup Configuration" nicht gelöscht wird. Folgende Feldwerte sind möglich:
  - **Aktiviert** - Stellt die werkseitigen Standardeinstellungen wieder her.
  - **Deaktiviert** - Behält die aktuellen Konfigurationseinstellungen bei.

Kopieren von Dateien:

1. Öffnen Sie die Seite **Copy Files**.
2. Wählen Sie entweder das Feld **Copy Configuration** oder **Copy Master Firmware** aus.
3. Wählen Sie die Felder **Source** und **Destination** für die Datei aus.
4. Klicken Sie auf **Apply Changes**. Die Datei wird kopiert und das Gerät aktualisiert.

Wiederherstellen der werkseitigen Standardeinstellungen:

1. Öffnen Sie die Seite **Copy Files**.
2. Wählen Sie die Felder unter **Restore Company Factory Defaults** aus.
3. Klicken Sie auf **Apply Changes**. Die werkseitigen Standardeinstellungen werden wiederhergestellt und das Gerät aktualisiert.

Kopieren und Löschen von Dateien mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
delete *Startkonfiguration*	Löscht die Datei "Startup Configuration".
copy *Quell-URL Ziel-URL [SNMP]*	Kopiert eine beliebige Datei von einem Quellort an einen Zielort.

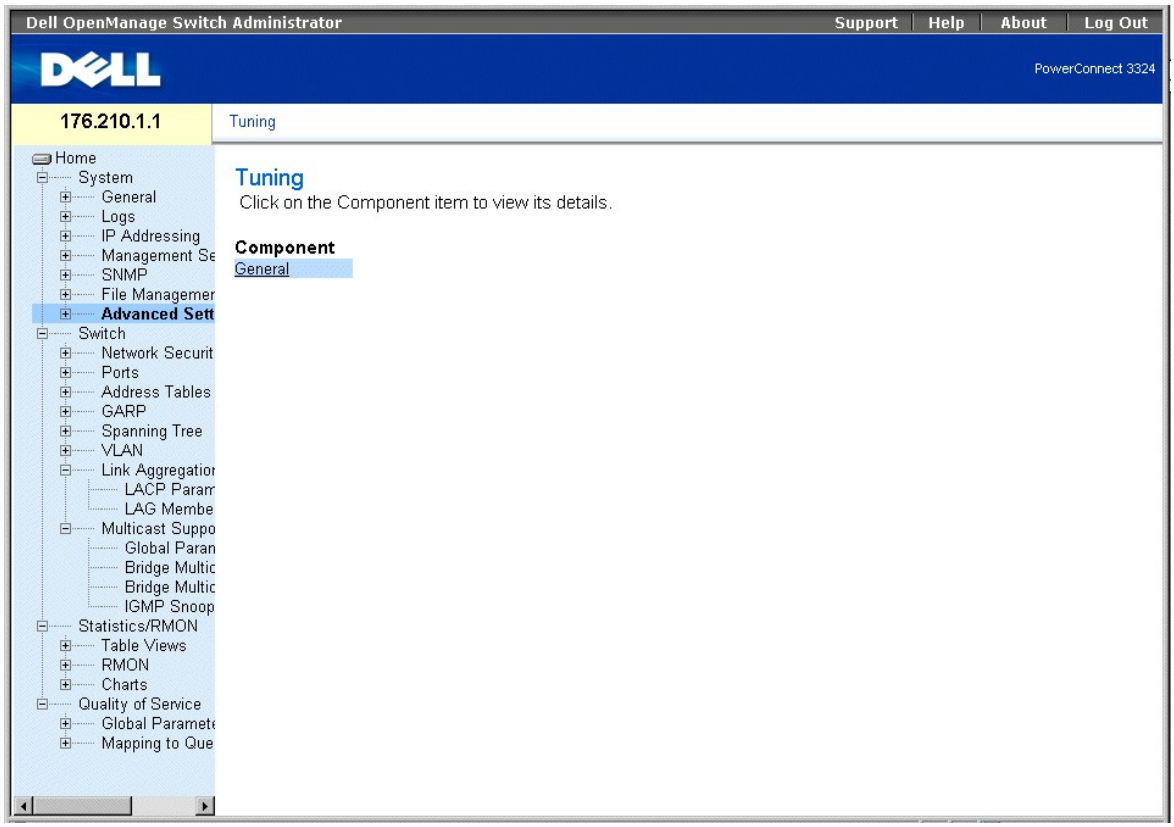
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console# delete startup-config

This command will reset the whole system and disconnect your Telnet session. Do you want to continue (y/n) [n]?

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]
```

Definieren erweiterter Einstellungen

Die Geräteabstimmung wird verwendet, um die maximale Anzahl zulässiger Einträge in den verschiedenen, aufgelisteten Tabellen zu ermitteln. Änderungen werden erst implementiert, nachdem das Gerät zurückgesetzt wurde. So öffnen Sie die Seite **Tuning**:

- Klicken Sie in der Strukturansicht auf **System** > **Advanced Settings**. Die Seite **Tuning** wird geöffnet.



Seite "Tuning"

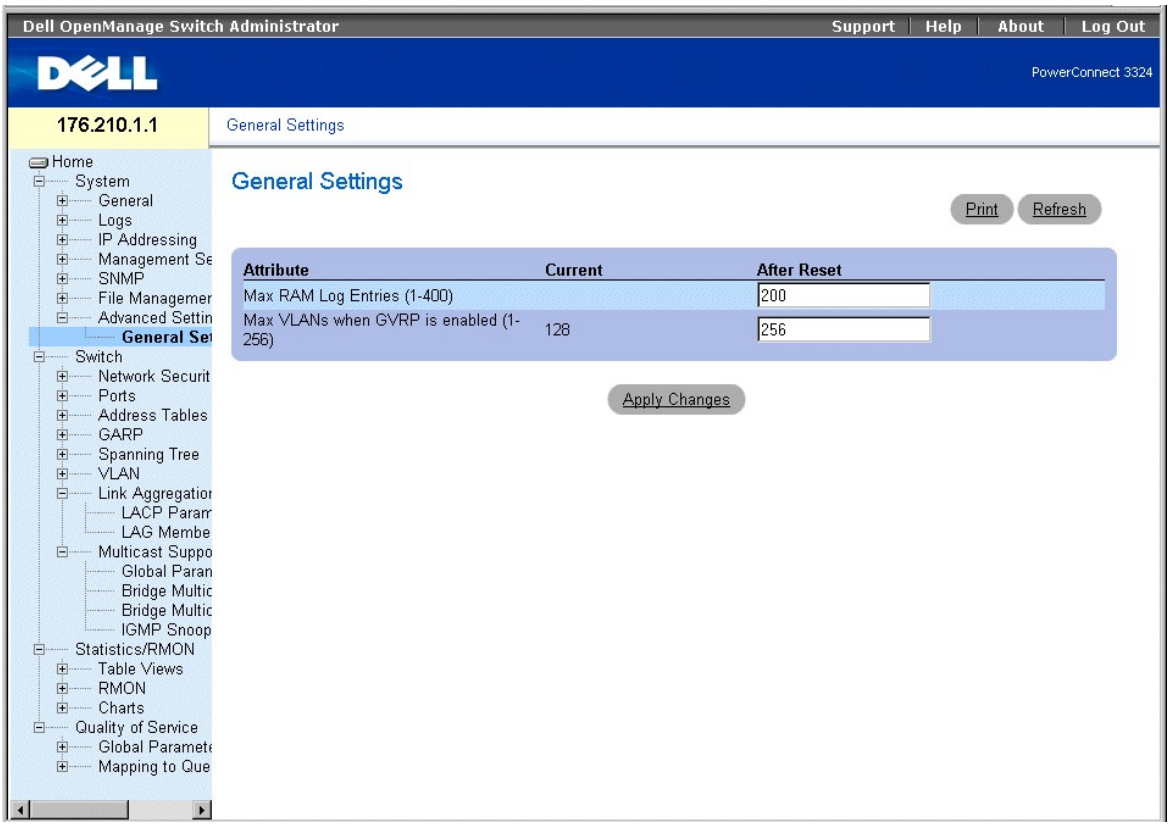
Die Seite **Tuning** enthält die folgenden Links:

- Konfigurieren allgemeiner Parameter für die Geräteabstimmung

Konfigurieren allgemeiner Parameter für die Geräteabstimmung

Auf der Seite **General Settings** können Netzwerkverwalter allgemeine Geräteparameter definieren. So öffnen Sie die Seite **General Settings**:

- Klicken Sie in der Strukturansicht auf **System** > **Advanced Settings** > **General**. Die Seite **General Settings** wird geöffnet.



Seite "General Settings"

Die Seite **General Settings** enthält folgende Spalten:

- **Attribute** - Das Attribut der allgemeinen Einstellung.
- **Current** - Der aktuelle Wert.
- **After Reset** - Der künftige Wert (nach dem Zurücksetzen). Durch Eingabe eines Wertes in die Spalte **After Reset** wird der Feldtabelle Arbeitsspeicher zugewiesen.

Die Seite **General Tuning** enthält folgende Felder:

- **Max RAM Log Entries (1-400)** - Gibt die maximale Anzahl von RAM Log-Einträgen an. Sobald die maximale Anzahl von Protokolleinträgen erreicht ist, wird der Protokollinhalt gelöscht und die Erfassung neu gestartet.
- **Max VLANs when GVRP is enabled (1-256)** - Definiert die Gesamtanzahl von VLANs, falls GVRP aktiviert ist.

ANMERKUNG: Die maximale Anzahl von GVRP-VLANs umfasst alle VLANs, die an GVRP- Operationen beteiligt sind, und zwar unabhängig davon, ob es sich um statische oder dynamische VLANs handelt.

Anzeigen des Zählers für RAM-Protokolleinträge mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
logging buffered size *Anzahl*	Legt die Anzahl der im internen Pufferspeicher (RAM) gespeicherten Syslog-Meldungen fest.
gvrp max vlan	Konfiguriert die maximale Anzahl von VLANs, falls GVRP aktiviert ist.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# logging buffered size 300
```

Zurück zum Inhalt

Zurück zum Inhalt

Weitere Hilfe

Dell™ PowerConnect™ 3324/3348 Benutzerhandbuch

Technische Unterstützung

Falls Sie Unterstützung bei einem technischen Problem benötigen, nutzen Sie die umfassenden Online-Dienste auf der Dell-Support-Website (**support.euro.dell.com**) für Fragen zur Verfahrensweise bei der Installation und Problembehandlung.

Weitere Informationen finden Sie unter "Online-Dienste".

Falls das Problem weiterhin besteht, wenden Sie sich telefonisch an die technische Unterstützung von Dell.

ANMERKUNG: Rufen Sie den technischen Support von einem Telefon in der Nähe des Systems an, damit Ihnen der technische Support bei allen notwendigen Verfahren helfen kann.

ANMERKUNG: Dells Express-Servicecode steht eventuell nicht in allen Ländern zur Verfügung.

Geben Sie den Express-Servicecode ein, wenn Dells automatisches Telefonsystem Sie dazu auffordert, damit Ihr Anruf direkt zum zuständigen Support-Personal weitergeleitet werden kann. Wenn Sie keinen Express-Servicecode haben, öffnen Sie das Verzeichnis **Dell Accessories** (Dell Zubehör), doppelklicken Sie auf das Symbol **Express Service Code**, und befolgen Sie die weiteren Anweisungen.

Anweisungen zur Verwendung des technischen Support-Service finden Sie unter "Technischer Support-Service" und "Vor dem Anruf"

ANMERKUNG: Einige der nachstehend aufgeführten Dienste sind nicht immer in allen Ländern verfügbar. Informationen hierzu erteilt Ihnen der örtliche Dell Verkaufsberater.

Online-Dienste

Sie können auf Dell Support unter **support.euro.dell.com** 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.euro.dell.com (nur für Länder in Europa)

www.dell.com/la (für lateinamerikanische Länder)

www.dell.ca (nur für Kanada)

- Anonymes FTP (File Transfer Protocol [Dateiübertragungsprotokoll])

ftp.dell.com/

Melden Sie sich als user:anonymous an, und verwenden Sie Ihre E-Mail-Adresse als Kennwort.

- Elektronischer Support-Service

support@us.dell.com

apsupport@dell.com (nur für Länder in Asien und im Pazifikraum)

support.euro.dell.com (nur für Länder in Europa)

- Elektronischer Kostenvoranschlagsservice

sales@dell.com

apmarketing@dell.com (nur für Länder in Asien und im Pazifikraum)

sales_canada@dell.com (Nur für Kanada)

- Elektronischer Informationsservice

info@dell.com

AutoTech Service

Dells automatisierter technischer Support-Service, AutoTech, bietet auf Band aufgezeichnete Antworten zu den Fragen, die von Dell Kunden zu ihren portablen und Desktop-Computersystemen am häufigsten gestellt werden.

Wenn Sie AutoTech anrufen, können Sie mit Hilfe der Telefontasten das Thema auswählen, das Ihre Fragen behandelt.

Der AutoTech-Service steht täglich rund um die Uhr zur Verfügung. Sie können diesen Service auch über den technischen Support-Service erreichen. Lesen Sie dazu die Kontaktinformationen zu Ihrer Region.

Automatischer Auftragsstatusdienst

Um den Status der von Ihnen bestellten Dell™-Produkte abzufragen, können Sie die Website **support.euro.dell.com** besuchen oder den automatischen Auftragsauskunftsdienst anrufen. Ein Band fordert Sie auf, die Informationen zu geben, die nötig sind, um die Bestellung zu finden und darüber Auskunft geben zu können. Lesen Sie dazu die Kontaktinformationen zu Ihrer Region.

Technischer Support-Service

Der technische Support-Service von Dell steht an allen Tagen der Woche rund um die Uhr zur Verfügung, um Ihre Fragen über Dell Hardware zu beantworten. 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 Ihr Land zutreffenden Kontaktinformationen an.

Dell Unternehmenstraining und Zertifizierung

Dell bietet Unternehmenstraining und Zertifizierung an. Weitere Informationen finden Sie unter **www.dell.com/training**. Dieser Service wird eventuell nicht an allen Stellen angeboten.

Probleme mit Ihrer Bestellung

Sollten sich Probleme mit der Bestellung ergeben (fehlende oder falsche Teile, unkorrekte 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

Um Informationen über die weitere Produktpalette von Dell einzuholen oder um eine Bestellung aufzugeben, besuchen Sie die Dell Website unter **www.dell.com/**. Wenn Sie mit einem Verkaufsberater persönlich sprechen möchten, finden Sie die entsprechende Rufnummer in den Kontaktnummern für Ihre Region.

Rücksendung von Teilen zur Garantiereparatur oder zur Gutschrift

Bereiten Sie alle zurückzuschickenden Produkte - zur Reparatur oder zur Gutschrift - wie folgt vor:

1. Rufen Sie bei Dell an, um eine Rücksendegenehmigungsnummer zu erhalten, und schreiben Sie diese deutlich lesbar außen auf den Versandkarton.

   Die entsprechende Rufnummer finden Sie in den Kontaktnummern für Ihre Region.

2. Legen Sie eine Kopie des Lieferscheins und ein Begleitschreiben bei, in dem der Grund der Rücksendung erklärt wird.
3. Fügen Sie Diagnoseinformationen bei, aus denen hervorgeht, welche Tests Sie durchgeführt haben und welche Fehlermeldungen vom Diagnoseprogramm ausgegeben wurden.
4. Für eine Gutschrift müssen alle zugehörigen Einzelteile (wie z. B. Netzkabel, Datenträger wie CDs und Disketten sowie Handbücher) mitgeschickt werden.
5. Schicken Sie die Geräte in der Originalverpackung (oder einer ähnlichen Verpackung) zurück.

   Sie sind für das Porto verantwortlich. 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 beim Anruf den Express-Servicecode griffbereit. Der Code hilft Dells automatischem Support-Telefonsystem, Ihren Anruf effizienter weiterzuleiten.

Schalten Sie nach Möglichkeit das System vor dem Anruf bei Dell ein, und benutzen Sie ein Telefon in der Nähe des Computers. Sie werden möglicherweise aufgefordert, einige Befehle über die Tastatur einzugeben, detaillierte Informationen während der Ausführung von Operationen zu übermitteln oder sonstige Verfahren für die Problembehandlung anzuwenden, die nur am System selbst durchgeführt werden können. Die Systemdokumentation sollte immer griffbereit sein.

⚠ **VORSICHT: Lesen Sie die wichtigen Sicherheitshinweise im *Systeminformationshandbuch*, bevor Sie Komponenten im Inneren des Computers warten.**

Kontaktaufnahme mit Dell

Dell kann elektronisch über die folgenden Websites erreicht werden:

- **www.dell.com**
- **support.euro.dell.com** (Technischer Support)
- **premiersupport.dell.com** (Technischer Support für Bildungswesen, Behörden und Gesundheitswesen sowie mittelständische Betriebe/Großkunden, einschließlich Premier-, Platin- und Gold-Kunden)

Spezifische Web-Adressen für Ihr Land finden Sie im entsprechenden Landesabschnitt in unten stehender Tabelle.

ANMERKUNG: Gebührenfreie Nummern gelten in den Ländern, für die sie aufgeführt werden.

Verwenden Sie die elektronischen Adressen, Telefonnummern und Vorwahlen, die in der folgenden Tabelle enthalten sind, wenn es notwendig ist, Dell zu kontaktieren. Wenn Sie Hilfe bei der Bestimmung der Nummern benötigen, können Sie sich an die örtliche bzw. internationale Telefonauskunft wenden.

Land (Stadt) Internationale Vorwahl Landesvorwahl Ortsvorwahl:	Abteilungsname oder Servicebereich, Website und E-Mail-Adresse	Vorwahlen, Rufnummern undgebührenfreie Nummern
Anguilla	Allgemeiner Support	gebührenfrei: 800-335-0031
Antigua und Barbuda	Allgemeiner Support	1-800-805-5924
Argentinien (Buenos Aires) Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **54** Ortskennzahl: **11**	Website: **www.dell.com.ar**	
	Technischer Support und Kundenbetreuung	gebührenfrei: 0-800-444-0733
	Verkauf	0-810-444-3355
	Tech-Support-Fax	11 4515 7139
	Kundenbetreuung - Fax	11 4515 7138
Aruba	Allgemeiner Support	gebührenfrei: 800-1578
Australien (Sydney) Vorwahl für ein internationales Gespräch: **0011** Landesvorwahl: **61** Ortskennzahl: **2**	E-Mail (Australien): au_tech_support@dell.com	
	E-Mail (Neuseeland): nz_tech_support@dell.com	
	Privatbenutzer und Kleinbetriebe	1-300-65-55-33
	Öffentliche Auftraggeber und Unternehmen	gebührenfrei: 1-800-633-559
	PAD (Vorzugskunden)	gebührenfrei: 1-800-060-889
	Kundenbetreuung	gebührenfrei: 1-800-819-339
	Firmenkunden - Verkauf	gebührenfrei: 1-800-808-385
	Transaktionsverkauf	gebührenfrei: 1-800-808-312
	Fax	gebührenfrei: 1-800-818-341
	Telefonzentrale	0820 240 530 00
Bahamas	Allgemeiner Support	gebührenfrei: 1-866-278-6818
Barbados	Allgemeiner Support	1-800-534-3066
Belgien (Brüssel) Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **32** Ortskennzahl: **2**	Website: **support.euro.dell.com**	
	E-Mail: tech_be@dell.com	
	E-Mail für Französisch sprechende Kunden: **support.euro.dell.com/be/fr/emaildell/**	
	Technischer Support	02 481 92 88
	Kundenbetreuung	02 481 91 19
	Firmenkunden - Verkauf	02 481 91 00
	Fax	02 481 92 99
	Telefonzentrale	02 481 91 00
Bermuda	Allgemeiner Support	1-800-342-0671
Bolivien	Allgemeiner Support	gebührenfrei: 800-10-0238

Brasilien Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **55** Ortskennzahl: **51**	Website: **www.dell.com/br**	
	Kunden-Support, Technischer Support	0800 90 3355
	Tech-Support-Fax	51 481 5470
	Kundenbetreuung - Fax	51 481 5480
	Verkauf	0800 90 3390
Britische Jungferninseln	Allgemeiner Support	gebührenfrei: 1-866-278-6820
Brunei Landesvorwahl: **673**	Technischer Support für Kunden (Penang, Malaysia)	604 633 4966
	Kundendienst (Penang, Malaysia)	604 633 4949
	Transaktionsverkauf (Penang, Malaysia)	604 633 4955
Caymaninseln	Allgemeiner Support	1-800-805-7541
Chile (Santiago) Landesvorwahl: **56** Ortskennzahl: **2**	Verkauf, Kunden-Support und technischer Support	gebührenfrei: 1230-020-4823
China (Xiamen) Landesvorwahl: **86** Ortskennzahl: **592**	Tech Support-Website: **support.ap.dell.com/china**	
	E-Mail-Tech-Support cn_support@dell.com	
	Tech-Support-Fax	818 1350
	Privatbenutzer und Kleinbetriebe - Technischer Support	gebührenfrei: 800 858 2437
	Firmenkunden - Technischer Support	gebührenfrei: 800.8582333
	Kundenerfahrungen	gebührenfrei: 800 858 2060
	Privatbenutzer und Kleinbetriebe	gebührenfrei: 800 858 2222
	Vorzugskundenbereich	gebührenfrei: 800 858 2557
	Große Unternehmenskunden - GCP	gebührenfrei: 800 858 2055
	Große Unternehmenskunden Großkunden	gebührenfrei: 800 858 2628
	Große Unternehmenskunden - Nord	gebührenfrei: 800 858 2999
	Große Unternehmenskunden Nord - Behörden und Schulen	gebührenfrei: 800 858 2955
	Große Unternehmenskunden - Ost	gebührenfrei: 800 858 2020
	Große Unternehmenskunden Ost - Behörden und Schulen	gebührenfrei: 800 858 2669
	Große Unternehmenskunden - Queue-Team	gebührenfrei: 800 858 2222
	Große Unternehmenskunden - Süd	gebührenfrei: 800 858 2355
	Große Unternehmenskunden - West	gebührenfrei: 800 858 2811
	Große Unternehmenskunden - Ersatzteile	gebührenfrei: 800 858 2621
Costa Rica	Allgemeiner Support	0800-012-0435
Dänemark (Kopenhagen) Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **45**	Website: **support.euro.dell.com**	
	E-Mail-Support (portable 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 (Stammkunden)	7023 0184
	Privatbenutzer/Kleinbetriebe - Kundenbetreuung	3287 5505
	Telefonzentrale (Stammkunden)	3287 1200
	Faxzentrale (Stammkunden)	3287 1201
	Telefonzentrale (Privatbenutzer/Kleinbetriebe)	3287 5000
	Faxzentrale (Privatbenutzer/Kleinbetriebe)	3287 5001
Deutschland (Langen) Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **49** Ortskennzahl: **6103**	Website: **support.euro.dell.com**	
	E-Mail: tech_support_central_europe@dell.com	
	Technischer Support	06103 766-7200
	Privatbenutzer/Kleinbetriebe - Kundenbetreuung	0180-5-224400
	Weltweite Kundenbetreuung	06103 766-9570
	Vorzugskunden - Kundenbetreuung	06103 766-9420
	Großkunden - Kundenbetreuung	06103 766-9560
	Öffentliche Kunden - Kundenbetreuung	06103 766-9555
	Telefonzentrale	06103 766-7000
Dominikanische Republik	Allgemeiner Support	gebührenfrei: 1-866-278-6821
Ecuador	Allgemeiner Support	gebührenfrei: 999-119
El Salvador	Allgemeiner Support	01-899-753-0777
Finnland (Helsinki) Vorwahl für ein internationales	Website: **support.euro.dell.com**	
	E-Mail: fin_support@dell.com	

Gespräch: **990** Landesvorwahl: **358** Ortskennzahl: **9**	E-Mail-Support (Server): Nordic_support@dell.com	
	Technischer Support	09 253 313 60
	Technischer Support - Fax	09 253 313 81
	Stammkundenbetreuung	09 253 313 38
	Privatbenutzer/Kleinbetriebe - Kundenbetreuung	09 693 791 94
	Fax	09 253 313 99
	Telefonzentrale	09 253 313 00
Frankreich (Paris) (Montpellier) Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **33** Ortskennzahlen: **(1) (4)**	Website: **support.euro.dell.com**	
	E-Mail: **support.euro.dell.com/fr/fr/emaildell/**	
	Privatbenutzer und Kleinbetriebe	
	Technischer Support	0825 387 270
	Kundenbetreuung	0825 823 833
	Telefonzentrale	0825 004 700
	Telefonzentrale (auswärtige Anrufe nach Frankreich)	04 99 75 40 00
	Verkauf	0825 004 700
	Fax	0825 004 701
	Fax (auswärtige Anrufe nach Frankreich)	04 99 75 40 01
	Firmenkunden	
	Technischer Support	0825 004 719
	Kundenbetreuung	0825 338 339
	Telefonzentrale	01 55 94 71 00
	Verkauf	01 55 94 71 00
	Fax	01 55 94 71 01
Grenada	Allgemeiner Support	gebührenfrei: 1-866-540-3355
Griechenland Vorwahl für ein internationales Gespräch: 00 Landesvorwahl: 30	Website: **support.euro.dell.com**	
	E-Mail: support.euro.dell.com/gr/en/emaildell/	
	Technischer Support	080044149518
	Technischer Gold-Support	08844140083
	Telefonzentrale	2108129800
	Verkauf	2108129800
	Fax	2108129812
Großbritannien (Bracknell) Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **44** Ortskennzahl: **1344**	Website: **support.euro.dell.com**	
	Kundenbetreuung - Website: **support.euro.dell.com/uk/en/ECare/Form/Home.asp**	
	E-Mail: dell_direct_support@dell.com	
	Technischer Support (Firmenkunden/Vorzugskunden/PAD [1000 Mitarbeiter und mehr])	0870 908 0500
	Technischer Support (Direkt/PAD und Allgemein)	0870 908 0800
	Globale Kunden - Kundenbetreuung	01344 373 186
	Privatbenutzer und Kleinbetriebe - Kundenbetreuung	0870 906 0010
	Firmenkunden - Kundenbetreuung	01344 373 185
	Vorzugskunden (500 - 5000 Mitarbeiter) - Kundenbetreuung	0870 906 0010
	Zentralregierung - Kundenbetreuung	01344 373 193
	Kommunalbehörden und Bildungseinrichtungen - Kundenbetreuung	01344 373 199
	Gesundheitseinrichtungen - Kundenbetreuung	01344 373 194
	Privatbenutzer und Kleinbetriebe - Verkauf	0870 907 4000
	Firmenkunden/Öffentlicher Sektor - Verkauf	01344 860 456
	Fax für Privatbenutzer und Kleinbetriebe	0870 907 4006
Guatemala	Allgemeiner Support	1-800-999-0136
Guyana	Allgemeiner Support	gebührenfrei: 1-877-270-4609
Hongkong Vorwahl für ein internationales Gespräch: **001** Landesvorwahl: **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
	Kundenberatung	3416 0910
	Große Konzernkunden	3416 0907
	Globale Kundenprogramme	3416 0908

	Bereich für mittelgroße Unternehmen	3416 0912
	Bereich für Privatbenutzer und Kleinbetriebe	2969 3105
Indien	Technischer Support	1600 33 8045
	Verkauf	1600 33 8044
Irland (Cherrywood) Vorwahl für ein internationales Gespräch: **16** Landesvorwahl: **353** Ortskennzahl: **1**	Website: **support.euro.dell.com**	
	E-Mail: dell_direct_support@dell.com	
	Technischer Support	1850 543 543
	Technischer Kundendienst Großbritannien (nur für innerhalb Großbritanniens)	0870 908 0800
	Privatbenutzer - Kundenbetreuung	01 204 4014
	Kleinbetriebe - Kundenbetreuung	01 204 4014
	Kundenbetreuung Großbritannien (nur für innerhalb Großbritanniens)	0870 906 0010
	Firmenkunden - Kundenbetreuung	1850 200 982
	Konzernkundenbetreuung (Anwahl der Nummer nur in Großbritannien)	0870 907 4499
	Irland - Verkauf	01 204 4444
	Vertrieb Großbritannien (Rufnummer nur für innerhalb Großbritannien)	0870 907 4000
	Fax/Verkaufsfax	01 204 0103
	Telefonzentrale	01 204 4444
Italien (Mailand) Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **39** Ortskennzahl: **02**	Website: **support.euro.dell.com**	
	E-Mail: **support.euro.dell.com/it/it/emaildell/**	
	Privatbenutzer und Kleinbetriebe	
	Technischer Support	02 577 826 90
	Kundenbetreuung	02 696 821 14
	Fax	02 696 821 13
	Telefonzentrale	02 696 821 12
	Firmenkunden	
	Technischer Support	02 577 826 90
	Kundenbetreuung	02 577 825 55
	Fax	02 575 035 30
	Telefonzentrale	02 577 821
Jamaika	Allgemeiner Support (Anwahl nur innerhalb von Jamaika)	1-800-682-3639
Japan (Kawasaki) Vorwahl für ein internationales Gespräch: **001** Landesvorwahl: **81** Ortskennzahl: **44**	Website: **support.jp.dell.com**	
	Technischer Support (Server)	gebührenfrei: 0120-198-498
	Technischer Support außerhalb von Japan (Server)	81-44-556-4162
	Technischer Support (Dimension™ und Inspiron™)	gebührenfrei: 0120-198-226
	Technischer Support außerhalb von Japan (Dimension und Inspiron)	81-44-520-1435
	Technischer Support (Dell Precision™, OptiPlex™ und Latitude™)	gebührenfrei: 0120-198-433
	Technischer Support außerhalb von Japan (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-Service	044-556-3490
	Automatisierter Bestelldienst (24 Stunden)	044-556-3801
	Kundenbetreuung	044-556-4240
	Unternehmen - Verkaufsabteilung (bis zu 400 Mitarbeiter)	044-556-1465
	Bereich für Vorzugskunden - Verkauf (über 400 Mitarbeiter)	044-556-3433
	Große Konzernkunden - Verkauf (über 3500 Mitarbeiter)	044-556-3430
	Öffentlicher Verkauf (Regierungsbehörden, Bildungsinstitutionen und Medizinische Institutionen)	044-556-1469
	Globales Segment Japan	044-556-3469
	Privatbenutzer	044-556-1760
	Telefonzentrale	044-556-4300
Kanada (North York, Ontario) Vorwahl für ein internationales Gespräch: **011**	Online-Bestellstatus: **www.dell.ca/ostatus**	
	AutoTech (automatisierter technischer Support)	gebührenfrei: 1-800-247-9362
	TechFax	gebührenfrei: 1-800-950-1329
	Kundenbetreuung (Privatbenutzer und Kleinbetriebe)	gebührenfrei: 1-800-847-4096
	Kundenbetreuung (mittlere/große Unternehmen, Regierung)	gebührenfrei: 1-800-326-9463
	Technischer Support (Privatbenutzer und Kleinbetriebe)	gebührenfrei: 1-800-847-4096
	Technischer Support (mittlere/große Unternehmen, Regierung)	gebührenfrei: 1-800-387-5757
	Verkauf (Privatbenutzer/Kleinbetriebe)	gebührenfrei: 1-800-387-5752

	Verkauf (mittlere/große Unternehmen, Behörden)	gebührenfrei: 1-800-387-5755
	Verkauf für Ersatzteile und erweiterten Service	1 866 440 3355
Kolumbien	Allgemeiner Support	980-9-15-3978
Korea (Seoul) Vorwahl für ein internationales Gespräch: **001** Landesvorwahl: **82** Ortskennzahl: **2**	Technischer Support	gebührenfrei: 080-200-3800
	Verkauf	gebührenfrei: 080-200-3600
	Kundendienst (Seoul, Korea)	gebührenfrei: 080-200-3800
	Kundendienst (Penang, Malaysia)	604 633 4949
	Fax	2194-6202
	Telefonzentrale	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
	Verkauf (Austin, Texas, USA)	512 728-4397
	Verkaufsfax (Austin, Texas, USA)	512 728-4600 oder 512 728-3772
Luxemburg Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **352**	Website: **support.euro.dell.com**	
	E-Mail: tech_be@dell.com	
	Technischer Support (Brüssel, Belgien)	3420808075
	Privatbenutzer/Kleinbetriebe - Verkauf (Brüssel, Belgien)	gebührenfrei: 080016884
	Firmenkunden - Verkauf (Brüssel, Belgien)	02 481 91 00
	Kundenbetreuung (Brüssel, Belgien)	02 481 91 19
	Fax (Brüssel, Belgien)	02 481 92 99
	Telefonzentrale (Brüssel, Belgien)	02 481 91 00
Macao Landesvorwahl: **853**	Technischer Support	gebührenfrei: 0800 582
	Kundendienst (Penang, Malaysia)	604 633 4949
	Transaktionsverkauf	gebührenfrei: 0800 581
Malaysia (Penang) Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **60** Ortskennzahl: **4**	Technischer Support	gebührenfrei: 1 800 888 298
	Kundendienst	04 633 4949
	Transaktionsverkauf	gebührenfrei: 1 800 888 202
	Firmenkunden - Verkauf	gebührenfrei: 1 800 888 213
Mexiko Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **52**	Technischer Support für Kunden	001-877-384-8979 oder 001-877-269-3383
	Verkauf	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	Allgemeiner Support	gebührenfrei: 1-866-278-6822
Neuseeland Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **64**	E-Mail (Neuseeland): nz_tech_support@dell.com	
	E-Mail (Australien): au_tech_support@dell.com	
	Privatbenutzer und Kleinbetriebe	0800 446 255
	Öffentliche Auftraggeber und Unternehmen	0800 444 617
	Verkauf	0800 441 567
	Fax	0800 441 566
Nicaragua	Allgemeiner Support	001-800-220-1006
Niederlande (Amsterdam) Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **31** Ortskennzahl: **20**	Website: **support.euro.dell.com** E-Mail-Support (Technische Unterstützung): (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 - Fax	020 674 47 66
	Privatbenutzer/Kleinbetriebe - Kundenbetreuung	020 674 42 00
	Stammkundenbetreuung	020 674 4325
	Privatbenutzer/Kleinbetriebe - Verkauf	020 674 55 00
	Relationaler Vertrieb	020 674 50 00
	Privatbenutzer/Kleinbetriebe - Verkaufsfax	020 674 47 75
	Fax Relationaler Vertrieb	020 674 47 50
	Telefonzentrale	020 674 50 00
	Fax-Telefonzentrale	020 674 47 50
Niederländische Antillen	Allgemeiner Support	001-800-882-1519
Norwegen (Lysaker) Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **47**	Website: **support.euro.dell.com**	
	E-Mail-Support (portable 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
	Stammkundenbetreuung	671 17514
	Privatbenutzer/Kleinbetriebe - Kundenbetreuung	23162298
	Telefonzentrale	671 16800
	Fax-Telefonzentrale	671 16865
Österreich (Wien) Vorwahl für ein internationales Gespräch: **900** Landesvorwahl: **43** Ortskennzahl: **1**	Website: **support.euro.dell.com**	
	E-Mail: tech_support_central_europe@dell.com	
	Privatbenutzer/Kleinbetriebe - Verkauf	0820 240 530 00
	Privatbenutzer/Kleinbetriebe - Fax	0820 240 530 49
	Privatbenutzer/Kleinbetriebe - Kundenbetreuung	0820 240 530 14
	Vorzugskunden/Firmenkunden - Kundenbetreuung	0820 240 530 16
	Privatbenutzer/Kleinbetriebe - Technischer Support	0820 240 530 14
	Vorzugskunden/Firmenkunden - Technischer Support	0660 8779
Panama	Allgemeiner Support	001-800-507-0962
Peru	Allgemeiner Support	0800-50-669
Polen (Warschau) Vorwahl für ein internationales Gespräch: **011** Landesvorwahl: **48** Ortskennzahl: **22**	Website: **support.euro.dell.com**	
	E-Mail: pl_support@dell.com	
	Kundendiensttelefon	57 95 700
	Kundenbetreuung	57 95 999
	Verkauf	57 95 999
	Kundendienstfax	57 95 806
	Empfangsfax	57 95 998
	Telefonzentrale	57 95 999
Portugal Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **351**	Website: **support.euro.dell.com**	
	E-Mail: **support.euro.dell.com/pt/en/emaildell/**	
	Technischer Support	707200149
	Kundenbetreuung	800 300 413
	Verkauf	800 300 410 oder 800 300 411 oder 800 300 412 oder 21 422 07 10
	Fax	21 424 01 12
Puerto Rico	Allgemeiner Support	1-800-805-7545
St. Kitts und Nevis	Allgemeiner Support	gebührenfrei: 1-877-441-4731
St. Lucia	Allgemeiner Support	1-800-882-1521
St.Vincent und die Grenadinen	Allgemeiner Support	gebührenfrei: 1-877-270-4609
Singapur (Singapur) Vorwahl für ein internationales Gespräch: **005** Landesvorwahl: **65**	Technischer Support	gebührenfrei: 800 6011 051
	Kundendienst (Penang, Malaysia)	604 633 4949
	Transaktionsverkauf	gebührenfrei: 800 6011 054
	Firmenkunden - Verkauf	gebührenfrei: 800 6011 053

Schweden (Upplands Vasby) Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **46** Ortskennzahl: **8**	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	
	E-Mail-Support für Server: Nordic_server_support@dell.com	
	Technischer Support	08 590 05 199
	Stammkundenbetreuung	08 590 05 642
	Privatbenutzer/Kleinbetriebe - Kundenbetreuung	08 587 70 527
	EPP-Support (Belegschaftskaufprogramm)	20 140 14 44
	Fax-Technischer Support	08 590 05 594
	Verkauf	08 590 05 185
Schweiz (Genf) Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **41** Ortskennzahl: **22**	Website: **support.euro.dell.com**	
	E-Mail: swisstech@dell.com	
	E-Mail für Französisch sprechende Privat-/Kleinbetriebe und Firmenkunden: **support.euro.dell.com/ch/fr/emaildell/**	
	Technischer Support (Privatbenutzer und Kleinbetriebe)	0844 811 411
	Technischer Support (Firmenkunden)	0844 822 844
	Kundenbetreuung (Privatbenutzer und Kleinbetriebe)	0848 802 202
	Kundenbetreuung (Firmenkunden)	0848 821 721
	Fax	022 799 01 90
	Telefonzentrale	022 799 01 01
Spanien (Madrid) Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **34** Ortskennzahl: **91**	Website: **support.euro.dell.com**	
	E-Mail: **support.euro.dell.com/es/es/emaildell/**	
	Privatbenutzer und Kleinbetriebe	
	Technischer Support	902 100 130
	Kundenbetreuung	902 118 540
	Verkauf	902 118 541
	Telefonzentrale	902 118 541
	Fax	902 118 539
	Firmenkunden	
	Technischer Support	902 100 130
	Kundenbetreuung	902 118 546
	Telefonzentrale	91 722 92 00
	Fax	91 722 95 83
Südafrika (Johannesburg) Vorwahl für ein internationales Gespräch: **09/091** Landesvorwahl: **27** Ortskennzahl: **11**	Website: **support.euro.dell.com**	
	E-Mail: dell_za_support@dell.com	
	Technischer Support	011 709 7710
	Kundenbetreuung	011 709 7707
	Verkauf	011 709 7700
	Fax	011 706 0495
	Telefonzentrale	011 709 7700
Südostasiatische und pazifische Länder	Technischer Support für Kunden, Kundendienst und Verkauf (Penang, Malaysia)	604 633 4810
Taiwan Vorwahl für ein internationales Gespräch: **002** Landesvorwahl: **886**	Technischer Support (portable und Desktop-Computer)	gebührenfrei: 00801 86 1011
	Technischer Support (Server)	gebührenfrei: 0080 60 1256
	Transaktionsverkauf	gebührenfrei: 0080 651 228
	Firmenkunden - Verkauf	gebührenfrei: 0080 651 227
Thailand Vorwahl für ein internationales Gespräch: **001** Landesvorwahl: **66**	Technischer Support	gebührenfrei: 0880 060 07
	Kundendienst (Penang, Malaysia)	604 633 4949
	Verkauf	gebührenfrei: 0880 060 09
Trinidad/Tobago	Allgemeiner Support	1-800-805-8035
Tschechische Republik (Prag) Vorwahl für ein internationales Gespräch: **00** Landesvorwahl: **420** Ortskennzahl: **2**	Website: **support.euro.dell.com**	
	E-Mail: czech_dell@dell.com	
	Technischer Support	02 2186 27 27
	Kundenbetreuung	02 2186 27 11
	Fax	02 2186 27 14
	TechFax	02 2186 27 28
	Telefonzentrale	02 2186 27 11

Turks- und Caicosinseln	Allgemeiner Support	gebührenfrei: 1-866-540-3355
Uruguay	Allgemeiner Support	gebührenfrei: 000-413-598-2521
USA (Austin, Texas) Vorwahl für ein internationales Gespräch: **011** Landesvorwahl: **1**	Automatischer Auftragsstatusdienst	gebührenfrei: 1-800-433-9014
	AutoTech (portable und Desktop-Computer)	gebührenfrei: 1-800-247-9362
	Kunden (Privatkunden und kleine Büros)	
	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-Support (Belegschaftskaufprogramm)	gebührenfrei: 1-800-695-8133
	Finanzierungen - Website: **www.dellfinancialservices.com**	
	Finanzierungen (Leasing/Kredit)	gebührenfrei: 1-877-577-3355
	Finanzierungen (DPA - Dell Vorzugskunden)	gebührenfrei: 1-800-283-2210
	Unternehmen	
	Kundendienst und Technischer Support	gebührenfrei: 1-800-822-8965
	EPP-Support (Belegschaftskaufprogramm)	gebührenfrei: 1-800-695-8133
	Projektoren - Technischer Support	gebührenfrei: 1-877-459-7298
	Öffentlicher Sektor (Verwaltung, Bildungs- und Gesundheitswesen)	
	Kundendienst und Technischer Support	gebührenfrei: 1-800-456-3355
	EPP-Support (Belegschaftskaufprogramm)	gebührenfrei: 1-800-234-1490
	Dell Verkauf	gebührenfrei: 1-800-289-3355 oder gebührenfrei: 1-800-879-3355
	Dell Fabrikverkaufsstelle (von Dell aufgearbeitete Computer)	gebührenfrei: 1-888-798-7561
	Software und Peripheriegeräte - Verkauf	gebührenfrei: 1-800-671-3355
	Ersatzteile - Verkauf	gebührenfrei: 1-800-357-3355
	Erweiterter Wartungsdienst und erweiterte Garantie - Verkauf	gebührenfrei: 1-800-247-4618
	Fax	gebührenfrei: 1-800-727-8320
	Dell Dienste für Gehör- und Sprachbehinderte	gebührenfrei: 1-877-DELLTTY (1-877-335-5889)
U.S. Virgin Islands	Allgemeiner Support	1-877-673-3355
Venezuela	Allgemeiner Support	8001-3605

Zurück zum Inhalt

Zurück zum Inhalt

Erste Schritte

Dell™ PowerConnect™ 3324/3348 Benutzerhandbuch

Starten von Switch Administrator

Auf den Dell OpenManage™ Switch Administrator des Dell™ PowerConnect™ 3324/3348 kann von jedem beliebigen PC mit Webbrowser zugegriffen werden. So starten Sie Switch Administrator:

1. Öffnen Sie einen Webbrowser.
2. Geben Sie in das Adressfeld des Browsers "http://{IP-Adresse des Geräts}/home.htm" ein, und drücken Sie <Eingabe>. Ein Anmeldefenster wird angezeigt.

Passwortseite für den PowerConnect 3324/3348

3. Geben Sie Benutzernamen und Passwort ein.

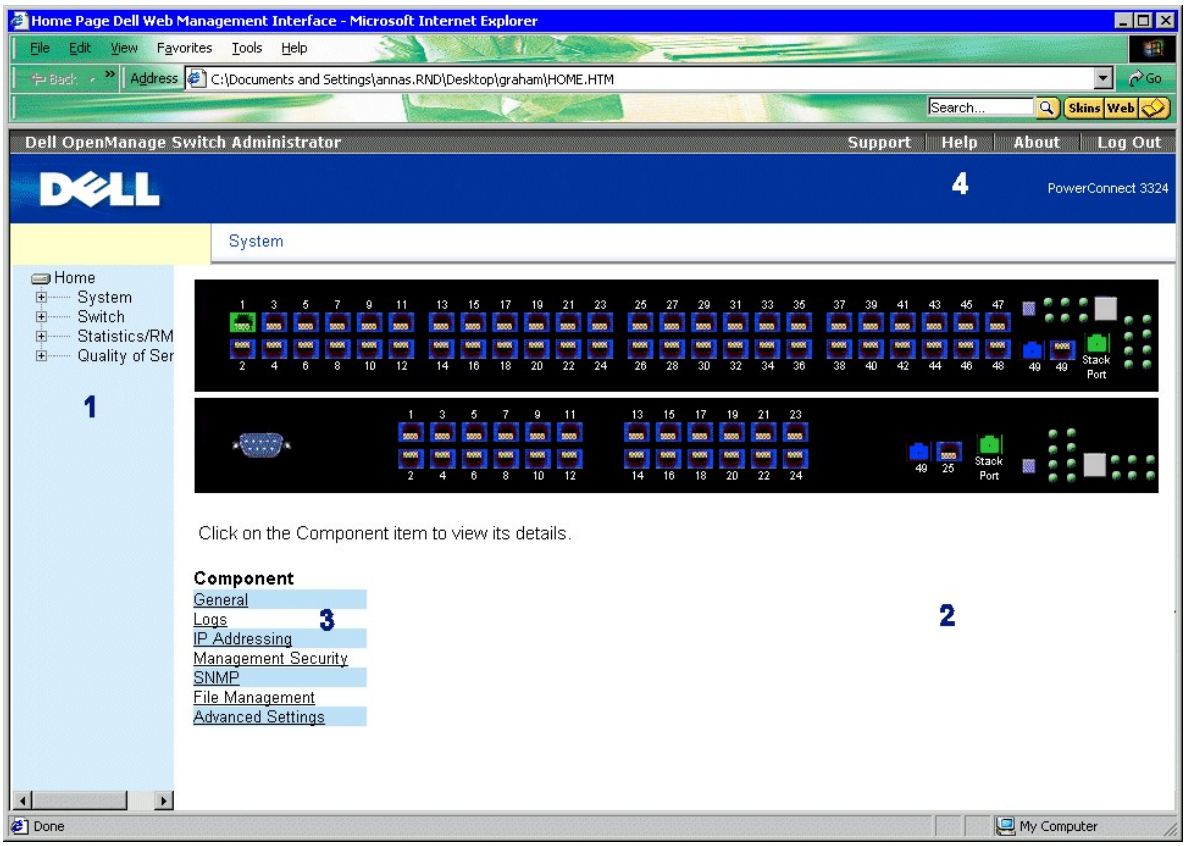
ANMERKUNG: Der PowerConnect 3324/3348 kann auch ohne Passworteingabe konfiguriert werden. Bei Passwörtern wird die Groß-/Kleinschreibung berücksichtigt, und sie können eine Kombination aus Buchstaben und Zahlen enthalten.

4. Klicken Sie auf **OK**. Die Startseite von **Switch Administrator** wird angezeigt.

Aufbau der Benutzeroberfläche

Die Startseite von **Switch Administrator** enthält die folgenden Ansichten:

- Strukturansicht - Sie befindet sich links auf der Startseite von **Switch Administrator** und bietet eine erweiterbare Strukturansicht der Funktionen und ihrer Komponenten (Komponentenliste).
- Geräteansicht - Sie befindet sich rechts auf der Startseite von **Switch Administrator** und enthält eine Ansicht des Gerätes, einen Informations- oder Tabellenbereich sowie Konfigurationsanweisungen.



Webverwaltungsoberfläche des PowerConnect 3324/3348

In der **Oberflächenkomponenten-Tabelle zum PowerConnect 3324/3348** sind die Oberflächenkomponenten mit den dazugehörigen Nummern aufgelistet:

Oberflächenkomponenten-Tabelle zum PowerConnect 3324/3348

Komponente	Name
1	Strukturansicht. Die Strukturansicht enthält eine Liste der verschiedenen Gerätefunktionen. Weitere Informationen zur Strukturansicht finden Sie unter "Strukturansicht".
2	Geräteansicht. Die Geräteansicht enthält Informationen zu Geräteanschlüssen, Tabelleninformationen sowie Funktionskomponenten. Weitere Informationen zur Strukturansicht finden Sie unter "Geräteansicht".
3	Komponentenliste Die Komponentenliste enthält eine Liste mit Funktionskomponenten. Weitere Informationen zur Verwendung der Komponentenliste finden Sie unter "Komponentenliste".
4	Informationsschaltflächen. Über die Informationsschaltflächen haben Sie Zugriff auf PowerConnect-Geräteinformationen und Dell-Dienste. Weitere Informationen zu den Informationsschaltflächen finden Sie unter "Verwenden der Schaltflächen in Switch Administrator".

Strukturansicht

Die Strukturansicht enthält eine Liste der verschiedenen, konfigurierbaren Funktionen, darunter Switching-Funktionen, Anschlüsse, Spanning Tree, VLANs, Class of Service (CoS), Verbindungsaggregation (LAG), Multicast-Unterstützung und Statistiken.

Die Verzweigungen der Strukturansicht können eingeblendet werden, um alle Komponenten unterhalb einer bestimmten Funktion anzuzeigen, bzw. ausgeblendet werden, um die Funktionskomponenten zu verbergen.

Geräteansicht

Im folgenden Abschnitt werden die verschiedenen Merkmale der Geräteansicht erläutert. Die Geräteansicht bietet Informationen zum PowerConnect 3324/3348-Switch. Die Geräteansicht umfasst die folgenden Komponenten:

- Komponentenliste
- Gerätedarstellung
- Arbeitsbereich

Komponentenliste

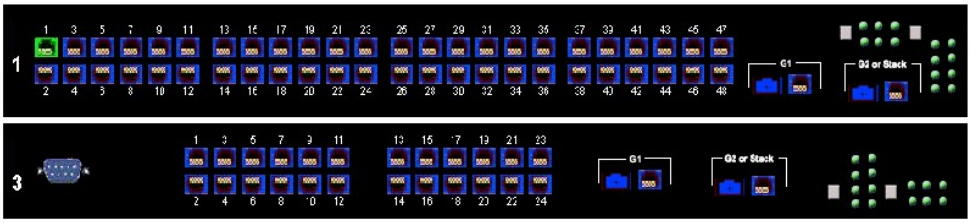
Auf der Startseite von **Switch Administrator** wird eine Komponentenliste mit den Menüoptionen der Funktion angezeigt. So zeigen Sie die Funktionen der Komponente an:

- Klicken Sie auf ein Element in der Komponentenliste. Die zur jeweiligen Komponente gehörige Seite wird geöffnet. Klicken Sie in der Strukturansicht beispielsweise auf **Switch**. Die folgende Seite wird geöffnet:

Komponentenliste

Gerätedarstellung

Die Startseite von **Switch Administrator** enthält eine grafische Darstellung von der Vorderseite des PowerConnect 3324/3348.



PowerConnect 3348

An der Farbgebung der Anschlüsse ist erkennbar, ob ein bestimmter Anschluss derzeit aktiv ist. Die Anschlüsse werden in den folgenden Farben dargestellt:

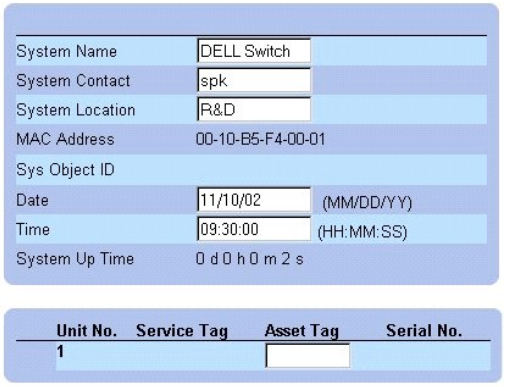
Anschlussanzeigen für den PowerConnect 3324/3348

Komponente	Name
Grün	Gibt an, dass eine Verbindung zum Anschluss besteht.
Blau	Gibt an, dass die Anschlussverbindung aufgrund einer Sicherheitsfunktion ausgesetzt ist.
Rot	Gibt an, dass keine Verbindung zum Anschluss besteht.

ANMERKUNG: Die LEDs auf der Vorderseite des PowerConnect 3324/3348 werden nicht in Switch Administrator angezeigt. Der LED-Status kann nur durch Anzeige des aktuellen Gerätes festgestellt werden. Weitere Informationen zu den LED-Definitionen finden Sie unter "LED-Definitionen".

Arbeitsbereich

Der Arbeitsbereich in der Geräteansicht bietet eine "Arbeitsplattform", die Gerätetabellen, allgemeine Geräteinformationen sowie konfigurierbare Geräteparameter enthält. In der Abbildung unten ist ein Beispiel für eine Tabelle zu sehen, so wie sie bei entsprechender Auswahl angezeigt wird:



Beispiel für Informationen im Arbeitsbereich

Verwenden der Schaltflächen in Switch Administrator

In diesem Abschnitt werden die verschiedenen Oberflächen-Schaltflächen von Dell OpenManage *Switch Administrator* beschrieben. Switch Administrator umfasst die folgenden Schaltflächen:

- Informationsschaltflächen - Bieten Zugriff auf Informationsdienste, einschließlich technischem Support, Onlinehilfe, Geräteinformationen, sowie eine Schaltfläche zum Schließen von *Switch Administrator*.
- Schaltflächen für die Geräteverwaltung - Bieten eine Erläuterung zu den Verwaltungsschaltflächen von *Switch Administrator*, die Befehle zum Hinzufügen, Löschen und Abfragen sowie zum Übernehmen von Änderungen bereitstellen.

Informationsschaltflächen

Die **Switch Administrator-** Startseite enthält die folgenden Informationsschaltflächen:

Taste	Beschreibung
Support	Öffnet die Seite für Dell-Support. Der URL für die technische Support-Seite von Dell lautet **www.support.euro.dell.com**
Help	Öffnet die Onlinehilfe.
About	Öffnet die Seite **About**.
Log Out	Meldet Sie von Switch Administratorab.

Informationsschaltflächen

Schaltfläche "Support"

Die Seite **Support** enthält Informationen zum Zugriff auf die technische Support-Seite von Dell.

1. Klicken Sie auf **Support**. Die **technische Support-Seite von Dell** wird geöffnet:

Technische Support-Seite von Dell

2. Wählen Sie den Bereich aus, in dem der gewünschte Support beschrieben wird. Die entsprechende Supportseite wird angezeigt.
3. Geben Sie Benutzernamen und Passwort ein.
4. Klicken Sie auf **Login**, und folgen Sie den Anweisungen.

ANMERKUNG: Abhängig vom gewünschten technischen Support sind u. U. Benutzername und Passwort erforderlich.

Schaltfläche "Help"

Die Seite **Online Help** enthält Informationen, die Sie bei der Konfiguration und Verwaltung des Switches unterstützen.

1. Auf **Hilfe** klicken. Die Seite **der Online-Hilfe** wird geöffnet.
2. Wählen Sie ein Hilfethema aus. Die Seite mit dem ausgewählten Hilfethema wird geöffnet.

ANMERKUNG: Jeder Bildschirm bietet eine kurze Hilfeseite. Um die Hilfe aufzurufen, klicken Sie auf der Switch Administrator-Seite auf **Help**.

Schaltfläche "About"

Die Schaltfläche**About** öffnet die Seite **About**. Auf der Seite **About** werden Gerätename, Software-Versionsnummer sowie Dell-Copyright-Informationen angezeigt. So öffnen Sie die Seite **About**:

- Klicken Sie auf **About**. Die Seite **About** wird geöffnet:

Schaltflächen für die Geräteverwaltung

Die Switch Administrator-Verwaltungsschaltflächen ermöglichen Netzwerkverwaltern die einfache PowerConnect-Konfiguration von Remote-Standorten aus. Switch Administrator umfasst die folgenden Verwaltungsschaltflächen:

Schaltflächen für die Geräteverwaltung

Taste	Beschreibung
Apply Changes	Übernimmt die festgelegten Änderungen für das Gerät.
Add	Fügt Tabellen oder Informationsfenstern Informationen hinzu.
Telnet	Startet eine Telnetsitzung.
Reset All Counters	Führt Tabellenabfragen durch.
Show All	Zeigt die Gerätetabellen an.
Transfer to Server	Überträgt die Firmware-Datei vom Gerät auf den Server.
← →	Verschiebt Informationen zwischen Listen.
Refresh	Aktualisiert Geräteinformationen.
	Öffnet die Seite **Log File Table**.
Show Log RAM	Öffnet die Seite **Log Ram Table**.

Restart DHCP	Startet die DHCP-Clientverbindungen neu.
Add ACE to ACL	Fügt ACLs ACEs hinzu.
Add ACL	Fügt ACLs hinzu.
Add List Name	Fügt neue Listen hinzu.
Attach to Interface	Verknüpft Schnittstellen mit verschiedenen Listen.
Reset All Counters	Setzt Statistikzähler zurück.
Print	Druckt die Seite **Network Management System** und/oder Tabelleninformationen.
Sort	Sortiert Tabelleninformationen.
Show Neighbors List	Zeigt die Neighbors List von der Seite **Neighbors Table** an.
Restore Defaults	Setzt das Gerät auf die Standardeinstellungen zurück.
Draw	Erstellt Ad-hoc-Statistiken in Diagrammform.

Verwenden des CLI-Programms

Dieser Abschnitt enthält eine Einführung in das CLI-(Command Line Interface-)Programm.

Befehlsmodus

Das CLI-Programm ist in Befehlsmodi unterteilt. Jeder Befehlsmodus verfügt über einen spezifischen Befehlssatz. Durch Eingabe eines Fragezeichens ? an der Systemeingabeaufforderung (Konsoleneingabeaufforderung) wird eine Liste der für den gerade aktiven Befehlsmodus verfügbaren Befehle angezeigt.

In jedem Modus wird ein spezifischer Befehl verwendet, um von einem Befehlsmodus zum anderen zu wechseln. Die Zugriffsstandards für die einzelnen Modi lauten wie folgt:

- User EXEC Mode
- Privileged EXEC Mode
- Global Configuration Mode
- Interface Configuration Mode

Während der Initialisierung der CLI-Sitzung ist der User EXEC Mode aktiv. Im User EXEC Mode ist nur eine Teilmenge der Befehle verfügbar. Diese Ebene ist für Vorgänge reserviert, die keinen Einfluss auf die Gerätekonfiguration haben; sie wird zum Zugriff auf Konfigurationsteilsysteme, wie das CLI-Programm, genutzt. Für den Zugriff auf die nächste Ebene, den Privileged EXEC Mode, ist ein Passwort erforderlich.

Der Privileged EXEC Mode bietet Zugriff auf die allgemeine Gerätekonfiguration. Für bestimmte globale Konfigurationen innerhalb des Gerätes wechseln Sie zur nächsten Ebene, dem Global Configuration Mode. Es ist kein Passwort erforderlich.

Im Global Configuration Mode wird die Gerätekonfiguration auf globaler Ebene verwaltet. Für individuelle Konfigurationen wechseln Sie wiederum zur nächsten Ebene, dem Interface Configuration Mode. Es ist kein Passwort erforderlich.

Im Interface Configuration Mode wird das Gerät auf der physischen Schnittstellenebene konfiguriert. Schnittstellenbefehle, die Unterbefehle erfordern, sind einer anderen Ebene zugeordnet, dem so genannten Subinterface Configuration Mode. Es ist kein Passwort erforderlich.

User EXEC Mode

Nach der Anmeldung beim Gerät wird der User EXEC-Befehlsmodus aktiviert. Mit Hilfe der User EXEC-Befehle werden Verbindungen zu Remote-Geräten hergestellt, Terminaleinstellungen temporär geändert, grundlegende Tests durchgeführt und Systeminformationen aufgelistet.

Um die User EXEC-Befehle aufzulisten, geben Sie den Befehl ? ein.

Die Eingabeaufforderung auf Benutzerebene besteht aus dem Hostnamen, gefolgt von einer spitzen Klammer (>).

```
console>
```

ANMERKUNG: Sofern er bei der Erstkonfiguration nicht geändert wurde, lautet der Standardhostname console.

Privileged EXEC Mode

In diesem Modus ist gewährleistet, dass der Privileged-Zugriff passwortgeschützt ist, um die unbefugte Nutzung zu vermeiden. Bei Passwörtern wird die Groß-/Kleinschreibung berücksichtigt. Passwörter werden als ***** auf dem Bildschirm angezeigt.

So können Sie auf die Befehle im Privileged EXEC Mode zugreifen und diese auflisten:

1. Geben Sie an der Eingabeaufforderung den Befehl enable ein, und drücken Sie <Eingabe>. Eine Passwort-Eingabeaufforderung wird angezeigt.
2. Geben Sie das Passwort ein, und drücken Sie <Eingabe>. Das Passwort wird als * angezeigt. Die Eingabeaufforderung für den Privileged EXEC Mode wird angezeigt. Die Eingabeaufforderung für den Privileged EXEC Mode besteht aus dem Gerätehostnamen, gefolgt von einer Raute (#).

```
console#
```

- Um die Privileged EXEC-Befehle aufzulisten, geben Sie den Befehl ? ein.

Um vom Privileged EXEC Mode in den User EXEC Mode zurückzukehren, verwenden Sie:

- enable
- disable
- exit/end
- STRG+Z

Das folgende Beispiel veranschaulicht, wie Sie den Privileged EXEC Mode aufrufen und zum User EXEC Mode zurückkehren:

```
console>enable

Enter Password: ******

console#

console#disable
```

```
console>
```

Der Befehl exit wird verwendet, um von einem beliebigen Modus zu einem Modus auf einer vorherigen Ebene zurückzukehren, beispielsweise vom Interface Configuration Mode zum Global Configuration Mode und vom Global Configuration Mode zum Privileged EXEC Mode.

Global Configuration Mode

Die Global Configuration-Befehle werden für Systemfunktionen und nicht für ein bestimmtes Protokoll bzw. eine Schnittstelle verwendet. Mit dem im Privileged EXEC Mode verwendeten Befehl configure wird der Global Configuration Mode aufgerufen.

So können Sie auf die Befehle im Global Configuration Mode zugreifen und diese auflisten:

- Geben Sie an der Eingabeaufforderung für den Privileged EXEC configure ein, und drücken Sie <Eingabe>. Die Eingabeaufforderung für den Global Configuration Mode wird angezeigt. Die Eingabeaufforderung für den Global Configuration Mode besteht aus dem Gerätehostnamen, gefolgt von einer Raute # und (config).

```
console(config)#
```

- Um die Global Configuration-Befehle aufzulisten, geben Sie den Befehl ? ein.

Um vom Global Configuration Mode zum Privileged EXEC Mode zurückzukehren, verwenden Sie einen der folgenden Befehle:

- exit
- STRG+Z

Das folgende Beispiel veranschaulicht, wie Sie den Global Configuration Mode aufrufen und zum Privileged EXEC Mode zurückkehren:

```
console#
```

```
console#configure
```

```
console(config)#exit
```

```
console#
```

Interface Configuration Mode

Mit Hilfe der Interface Configuration-Befehle wird eine bestimmte IP-Schnittstelle, einschließlich Bridge-Gruppe, Beschreibung usw., geändert. Die Interface Configuration Modes lauten:

- VLAN - Umfasst Befehle zum Erstellen und Konfigurieren eines vollständigen VLANs, beispielsweise um ein VLAN zu erstellen und eine IP-Adresse darauf anzuwenden.
- Port Channel - Umfasst Befehle zum Konfigurieren einzelner Anschlüsse, beispielsweise zum Zuweisen von Anschlüssen zu einer LAG.
- Line Interface - Umfasst Befehle zum Konfigurieren der Verwaltungsverbindungen. Dazu gehören beispielsweise Befehle zum Festlegen von Übertragungsrate und Zeitlimiteinstellungen.
- IP Access-List - Umfasst Befehle zum Verwalten von Zugriffslisten. Mit diesen Befehlen werden die Listen erstellt und verwaltet.
- Ethernet - Umfasst Befehle zum Verwalten der Anschlusskonfiguration.
- Management Access List - Umfasst Befehle zum Definieren von Zugriffslisten zu Verwaltungszwecken. Zugriffslisten werden zur Verwaltung von Zugriffsberechtigungen und Benutzerauthentifizierungen verwendet.
- MAC List - Konfiguriert die erforderlichen Bedingungen, um Datenverkehr auf der Grundlage von MAC-Adressen zuzulassen.

Starten des CLI-Programms

Der PowerConnect 3324/3348 kann über eine direkte Verbindung zum Konsolenanschluss oder über eine Telnet-Verbindung verwaltet werden. Der Switch wird durch die Eingabe von Befehlsschlüsselwörtern und -parametern an der Eingabeaufforderung verwaltet. Die Verwendung des CLI-Programms ist mit der Eingabe von Befehlen an einem UNIX-System vergleichbar.

Beim Zugriff über eine Telnet-Verbindung sollten Sie sicherstellen, dass eine IP-Adresse für das Gerät definiert wurde und dass die für den Gerätezugriff verwendete Workstation bereits vor Verwendung der CLI-Befehle mit dem Gerät verbunden ist.

Mehr Informationen zur Konfiguration einer ersten IP-Adresse finden Sie unter "Erstkonfiguration".

Konsolenverbindung

So starten Sie das CLI-Programm:

1. Starten Sie das Gerät, und warten Sie, bis die Starteingabeaufforderung `Console>` angezeigt wird.
2. Konfigurieren Sie das Gerät, und geben Sie die notwendigen Befehle ein, um die gewünschten Vorgänge auszuführen.
3. Beenden Sie abschließend die Sitzung durch Eingabe von `quit` oder `exit`.

Um den aktuellen Benutzer ab- und einen neuen Benutzer anzumelden, geben Sie den Anmeldebefehl im Privileged EXEC-Befehlsmodus ein.

ANMERKUNG: Eine Telnet-Sitzung wird automatisch getrennt, nachdem diese über einen benutzerdefinierten Zeitraum inaktiv war.

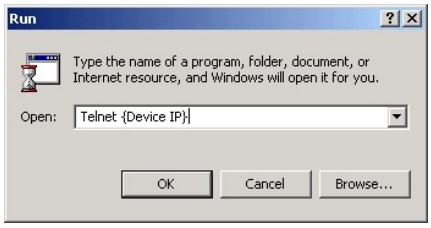
Telnet-Verbindung

Telnet ist ein Protokoll für die Terminal-Emulation über TCP/IP. ASCII-Terminals können über ein Netzwerk mit TCP/IP-Protokoll virtuell mit dem lokalen Gerät verbunden werden. Telnet stellt eine Alternative zur Anmeldung am lokalen Terminal dar, wenn eine Remote-Anmeldung erforderlich ist.

Der PowerConnect 3324/3348 unterstützt bis zu vier Telnet-Sitzungen gleichzeitig. In einer Telnet-Sitzung können sämtliche CLI-Befehle verwendet werden.

So starten Sie eine Telnet-Sitzung:

1. Wählen Sie **Start** > **Ausführen**. Das Fenster **Ausführen** wird geöffnet.



Fenster "Ausführen"

2. Geben Sie `Telnet` und die IP-Adresse des Gerätes im Feld **Öffnen**ein.
3. Klicken Sie auf **OK**. Die Telnet-Sitzung wird gestartet.

Telnet-Fenster

Zurück zum Inhalt

Zurück zum Inhalt

Hardwarebeschreibung

Dell™ PowerConnect™ 3324/3348 Benutzerhandbuch

PowerConnect 3324/3348 Beschreibung

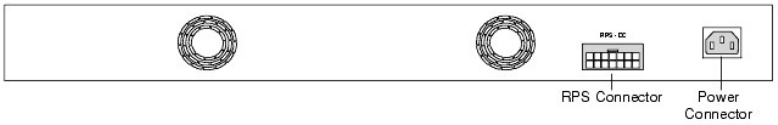
PowerConnect 3324/3348 Abmessungen

Dieses Gerät verfügt über folgende Abmessungen:

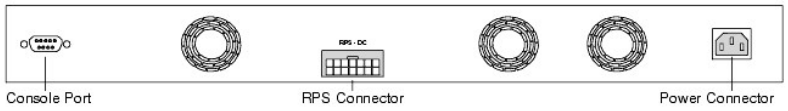
- Breite: 48,3 cm
- Höhe: 1U

PowerConnect 3324/3348 Rückseite

Die Rückseite des Dell™ PowerConnect™ 3324/3348 wird in der folgenden Abbildung angezeigt:



PowerConnect 3324 Rückseite



PowerConnect 3348 Rückseite

PowerConnect 3324/3348 Komponenten

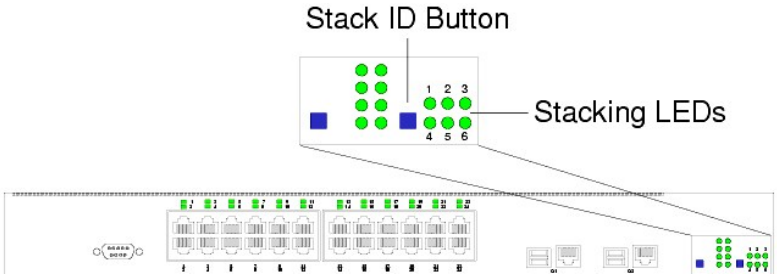
In diesem Abschnitt werden die verschiedenen PowerConnect 3324/3348-Hardwarekomponenten sowie folgende Themen beschrieben:

- Allgemeine Gerätekomponenten
- Taste "Mode"
- Taste "Stack ID"

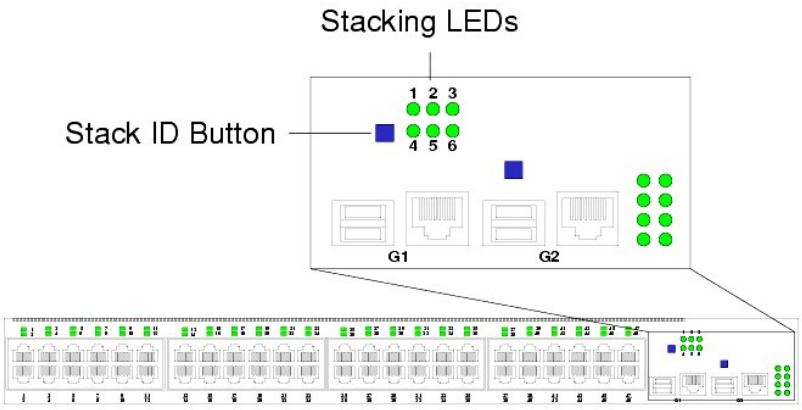
Allgemeine Gerätekomponenten

Der PowerConnect 3324/3348 enthält die folgenden Hardwarekomponenten:

- CPU - Basiert auf Motorolas MPC 8245.
- FLASH - Enthält 8 MB FLASH-Speicher.
- SDRAM - Enthält 32 MB.



PowerConnect 3324 Vorderseite



PowerConnect 3348 Vorderseite

Taste "Mode"

Über die Taste **Mode** ändern Sie die Einstellungen für Aktivität und Duplexbetrieb des Anschlusses.

Taste "Stack ID"

Auf der Vorderseite des PowerConnect 3324/3348 befindet sich die Taste **Stack ID**, über die Netzwerkadministratoren den Stack-Master und die Stack-Komponenten manuell auswählen können.

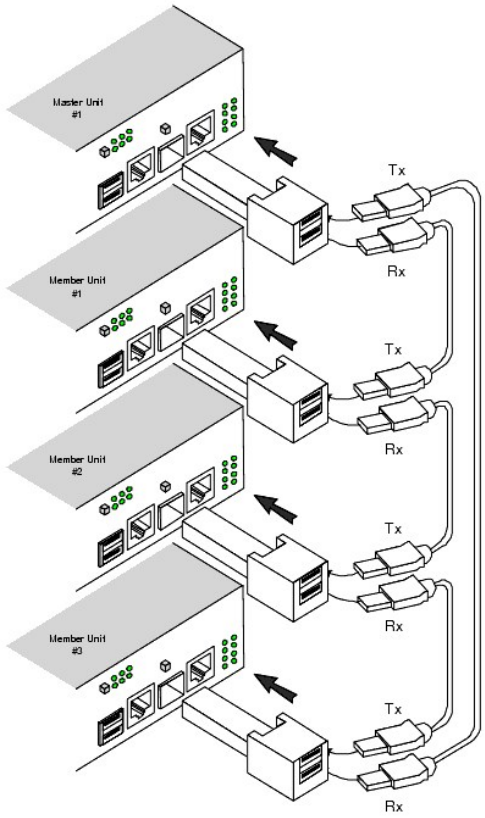
ANMERKUNG: Der Stack-Master und die Stack-Komponenten müssen innerhalb von 15 Sekunden nach dem Gerätestart ausgewählt werden. Wird der Stack-Master nicht innerhalb von 15 Sekunden ausgewählt, muss das Gerät zurückgesetzt werden, um die Einheiten-IDs auszuwählen.

Nachdem der Stack-Master ausgewählt wurde, werden die übrigen Geräte als Stack-Komponenten definiert. Mastereinheiten wird die Einheiten-ID 1 und Stack-Komponenten eine separate Einheiten-ID (2 bis 6) zugewiesen. Wenn ein Stack beispielsweise vier Einheiten enthält, hat die Mastereinheit den Wert 1, die zweite Stack-Komponente den Wert 2, die dritte den Wert 3, die vierte den Wert 4 usw.

Stack-Module und -Anschlüsse

Die PowerConnect 3324/3348-Stack-Module werden an den G2-Anschluss angeschlossen. Beim Stack-Modul handelt es sich um ein Mini-GBIC-Modul mit zwei Stack-Anschlüssen: RX und TX. RX entspricht dem unteren und TX dem oberen Verbindungsanschluss. Das Modul wird über eine Stacking-Kabelverbindung mit weiteren Stack-Einheiten verbunden. Der RX-Anschluss der oberen Einheit wird mit dem TX-Anschluss der unteren Einheit verbunden. Dadurch wird die

Ringtopologie gebildet. Diese Ringtopologie wird durch die Abbildung "Stack-Verbindungen" veranschaulicht.



Stack-Verbindungen

Weitere Informationen zum Verbinden von Stack-Kabeln finden Sie unter "Stacking-Kabel anschließen".

Anschlussbeschreibung

Beschreibung des Ethernet-Anschlusses

Der PowerConnect 3324 bietet 24 FE 10BaseT/100BaseTX UTP-Kupferanschlüsse (RJ45) pro Einheit sowie zwei Combo-Anschlüsse. Der PowerConnect 3348 bietet 48 FE 10BaseT/100BaseTX UTP-Kupferanschlüsse (RJ45) pro Einheit sowie zwei Combo-Anschlüsse. Jeder Combo-Anschluss stellt einen logischen Anschluss dar, der über die beiden folgenden physischen Schnittstellen verfügt:

- 1000Base-T-Anschlüsse
- Mini-GBIC-(SFP-)Anschlüsse

Es kann jeweils nur eine der beiden physischen Verbindungen eines Combo-Anschlusses verwendet werden.

Falls die automatische MDIX-Unterstützung aktiviert ist, erkennt der PowerConnect 3324/3348 auf allen Anschlüssen automatisch den Unterschied zwischen Crossover- und "Straight-Through"-Kabeln.

Der PowerConnect 3324/3348 unterstützt eine Geschwindigkeit von 10/100 Mbit/s für Kupferanschlüsse im Halb- oder Vollduplexmodus.

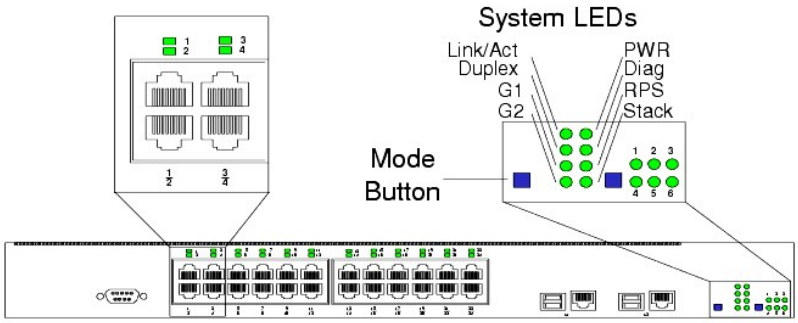
Beschreibung des Konsolenanschlusses

Die Schnittstelle des Konsolenanschlusses unterstützt die synchrone Datenübertragung mit folgenden Eigenschaften: acht Datenbits, ein Stoppbit und keine Parität. Alle 9 RS232-Kontakte sind zwecks Modemunterstützung belegt.

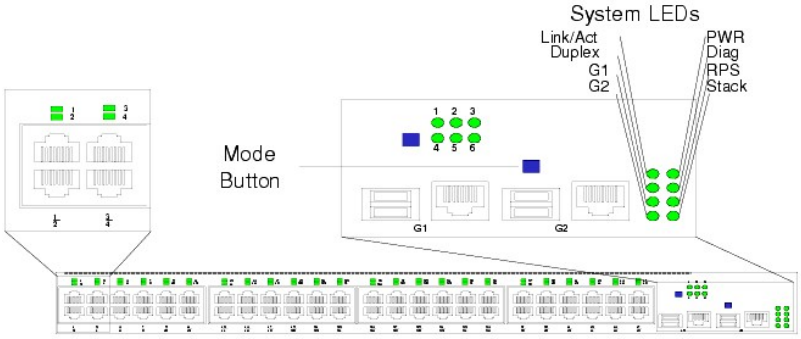
LED-Definitionen

Die in den folgenden Abbildungen angezeigten LEDs, die sich auf der Vorderseite befinden, zeigen den Status von Anschlussverbindungen und -modi, den Stromversorgungsstatus, den Stack-Status sowie Systemdiagnosewerte an. Folgende LED-Typen werden unterschieden:

- Anschluss-LEDs
- System-LEDs
- Stack-LEDs



LEDs an der Vorderseite: 24 Anschlüsse



LEDs an der Vorderseite: 48 Anschlüsse

Anschluss-LEDs

Jedem Anschluss ist eine LED zugewiesen, die sich oberhalb des Anschlusses befindet. Die LEDs zeigen je nach LED-Anzeigemodus des Anschlusses entweder die Verbindungsaktivität oder den Duplexmodus an. Weitere Informationen zum Festlegen des LED-Anzeigemodus finden Sie unter "System-LEDs".

Farbe	Aktivität	Definition
Grün	Static	Anschlussverbindung aktiv. Der Anschluss arbeitet mit einer Geschwindigkeit von 100 Mbit/s.
Grün	Blinkend	Anschlussverbindung aktiv mit Übertragungsaktivität. Der Anschluss arbeitet mit einer Geschwindigkeit von 100 Mbit/s.

Rot	Static	Anschlussverbindung aktiv. Der Anschluss arbeitet mit einer Geschwindigkeit von 10 Mbit/s.
Rot	Blinkend	Anschlussverbindung aktiv mit Übertragungsaktivität. Der Anschluss arbeitet mit einer Geschwindigkeit von 10 Mbit/s.
Aus	Aus	Anschlussverbindung inaktiv.

Aktivität der Anschlussverbindung

Farbe	Aktivität	Definition
Grün	Static	Anschluss im Vollduplexbetrieb.
Aus	Aus	Anschlussverbindung inaktiv oder im Halbduplexbetrieb.

Duplexmodus des Anschlusses

System-LEDs

Die acht System-LEDs geben den Status verschiedener Gerätefunktionen an:

- Wie in der Abbildung von der Vorderseite zu Beginn dieses Abschnitts dargestellt, zeigen die beiden System-LEDs oben links die Verbindungsaktivität und den Duplexmodus an. Diese LEDs zeigen an, ob die Anschluss-LEDs die Verbindungsaktivität oder den Duplexstatus angeben.
- Die beiden LEDs links unten in den Abbildungen zeigen den Verbindungsaktivitätsstatus der Giga-Anschlüsse 1 und 2 wie folgt an:

Farbe	Aktivität	Definition
Grün	Static	Anschlussverbindung aktiv. Der Anschluss arbeitet mit einer Geschwindigkeit von 1000 Mbit/s.
Grün	Blinkend	Anschlussverbindung aktiv mit Übertragungsaktivität. Der Anschluss arbeitet mit einer Geschwindigkeit von 1000 Mbit/s.
Rot	Static	Anschlussverbindung aktiv. Der Anschluss arbeitet mit einer Geschwindigkeit von 10/100 Mbit/s.
Rot	Blinkend	Anschlussverbindung aktiv mit Übertragungsaktivität. Der Anschluss arbeitet mit einer Geschwindigkeit von 10/100 Mbit/s.
Aus	Aus	Anschlussverbindung inaktiv.

Aktivität der Giga-Anschlussverbindung

- Über die neben den System-LEDs befindliche Taste **Mode** kann zwischen den beiden Anzeigemodi umgeschaltet werden. Eine Erläuterung der Anschluss-LEDs in den einzelnen Modi finden Sie unter "Anschluss-LEDs".

Nach einem Stromausfall werden eine Fehlermeldung und mehrere Traps generiert. Der Status der einzelnen Stromversorgungen wird durch die LEDs auf der Vorderseite angezeigt.

- Über die vier LEDs auf der rechten Seite wird der Status der Stromversorgungen, der Diagnosemodus sowie der Stack-Modus wie folgt angezeigt:

LED	Farbe	Aktivität	Definition
PWR	Grün	Static	Stromversorgung in Betrieb.
	Gelb	Static	Stromversorgung außer Betrieb.
RPS	Grün	Static	Redundante Stromversorgung in Betrieb.
	Gelb	Static	Redundante Stromversorgung außer Betrieb.
	Aus	Aus	Redundante Stromversorgung nicht vorhanden.
Diag	Grün	Blinkend	Das System befindet sich derzeit im Diagnosemodus.
Stack	Grün	Static	Stacking erfolgreich abgeschlossen.
	Aus	Aus	Unabhängiger Betrieb.

Stromversorgungs-, Diagnose- und Stack-LEDs

Stack-LEDs

Die Stack-LEDs geben die Position der Einheit im Stack an. Wie in den Abbildungen von der Vorderseite zu Beginn dieses Abschnitts dargestellt, sind die Stack-LEDs von 1 bis 6 durchnummeriert. Jede Einheit im Stack verfügt über eine leuchtende Stack-LED, die die Position der Einheit innerhalb des Stacks angibt. Wenn Stack-LED 1 leuchtet, handelt es sich dabei um die Mastereinheit. Wenn eine der Stack-LEDs mit der Nummer 2 bis 6 leuchtet, handelt es sich um die entsprechende Einheit der Stack-Komponente.

Zurück zum Inhalt

Zurück zum Inhalt

Installieren des PowerConnect 3324/3348-Switches

Dell™ PowerConnect™ 3324/3348 Benutzerhandbuch

Sicherheitshinweise zur Installation

⚠ **VORSICHT: Das Rack oder Gehäuse, in dem sich der Switch befindet, sollte ausreichend gesichert werden, um Instabilität bzw. ein Umkippen zu verhindern.**

⚠ **VORSICHT: Stellen Sie sicher, dass die Schaltkreise der Stromversorgung ordnungsgemäß geerdet sind.**

⚠ **VORSICHT: Beachten und befolgen Sie die Wartungszeichen. Nehmen Sie an Produkten keine Wartungsarbeiten vor, die über die in der Dokumentation zum System beschriebenen hinausgehen. Beim Öffnen bzw. Entfernen der mit einem Dreieckssymbol und einem Blitz gekennzeichneten Abdeckungen besteht die Gefahr eines Stromschlages. Diese Komponenten sollten nur von qualifizierten Servicetechnikern gewartet werden.**

⚠ **VORSICHT: Stellen Sie sicher, dass Netzkabel, Verlängerungskabel und/oder Stecker nicht beschädigt sind.**

⚠ **VORSICHT: Setzen Sie das Gerät keiner Feuchtigkeit aus.**

⚠ **VORSICHT: Achten Sie darauf, dass keine Objekte in das Gerät gelangen, da Brand- bzw. Stromschlaggefahr besteht.**

⚠ **VORSICHT: Lassen Sie das Gerät abkühlen, bevor Sie Abdeckungen abnehmen oder interne Bauteile berühren.**

⚠ **VORSICHT: Achten Sie darauf, dass Stromkreise, Verkabelung und Überstromschutz vom Switch nicht überlastet werden. Um eine mögliche Überlastung der Stromversorgung zu ermitteln, addieren Sie die Nennströme aller Switches, die vom selben Stromkreis wie der Switch gespeist werden. Anschließend vergleichen Sie dieses Gesamtergebnis mit der Nennstrombegrenzung für den Schaltkreis. Der maximale Nennstrom ist normalerweise neben den jeweiligen Wechselstromanschlüssen auf dem Switch angegeben.**

HINWEIS: Stellen Sie sicher, dass das Gerät weder Heizgeräten noch anderen Wärmequellen ausgesetzt ist.

HINWEIS: Stellen Sie sicher, dass die Belüftungsöffnungen nicht blockiert sind.

HINWEIS: Verwenden Sie das Gerät ausschließlich mit zugelassenem Zubehör.

HINWEIS: Installieren Sie den Switch nicht in einer Umgebung, in der die Umgebungstemperatur bei Betrieb 40ºC überschreitet.

HINWEIS: Stellen Sie sicher, dass die Luftzirkulation an der Vorder- und Rückseite sowie an den Seitenbereichen des Switches nicht behindert wird.

Standortvoraussetzungen

Geräte der Dell™ PowerConnect™ 3324/3348-Serie können in einem Standard-19-Zoll-Rack oder als Tischinstallation montiert werden. Stellen Sie vor der Montage sicher, dass der ausgewählte Standort die unten beschriebenen Standortvoraussetzungen erfüllt.

- Allgemein - Achten Sie darauf, dass das Gerät ordnungsgemäß mit Strom versorgt wird.
- Stromversorgung - Der Abstand des Gerätes zu einer geerdeten, leicht zugänglichen Steckdose mit 100-250 V Wechselspannung und 50-60 Hz sollte maximal 1,5 m betragen. Es sollten vorzugsweise zwei separate Stromversorgungen vorhanden sein, beispielsweise eine USV und eine getrennte, stufenweise Stromversorgung.
- Zugang - Der Bediener sollte an der Vorderseite des Gerätes ausreichend Bewegungsfreiheit haben. Auch Verkabelung, Stromanschlüsse und Belüftungsöffnungen sollten problemlos zugänglich sein.
- Verkabelung - Die Kabel sollten so verlegt sein, dass elektromagnetische Einstrahlung durch Funksender, Funkverstärker, Stromleitungen sowie Leuchtstoffröhren vermieden werden.
- Umgebungsvoraussetzungen - Die Betriebstemperatur des Gerätes liegt zwischen 0 und 40 ºC bei relativer Luftfeuchtigkeit von bis zu 95% (nicht kondensierend). Achten Sie darauf, dass kein Wasser bzw. keine Feuchtigkeit in das Gehäuse der Einheit eindringen kann.

Auspacken und Installieren

Inhalt des Softwarepakets

Die folgenden Komponenten sollten nach dem Auspacken des PowerConnect 3324/3348 vorhanden sein:

- PowerConnect 3324/3348-Einheit
- Wechselstromkabel
- Nullmodemkabel
- Selbstklebende Gummifüße
- Rack-Montage-Kits
- Dokumentations-CD

Auspacken

ANMERKUNG: Überprüfen Sie vor dem Auspacken des PowerConnect 3324/3348-Switches die Verpackung, und melden Sie mögliche Beschädigungen unverzüglich.

1. Legen Sie ein EGB-Handgelenkband an, und verbinden Sie die EGB-Klammer mit einer Metallfläche, um eine ausreichende Erdung zu gewährleisten.
2. Stellen Sie das Paket auf eine saubere, ebene Fläche, und zerschneiden Sie alle Befestigungsbänder.
3. Öffnen Sie die Verpackung, oder entfernen Sie die obere Abdeckung.
4. Nehmen Sie das Gerät vorsichtig aus der Verpackung, und stellen Sie es auf einer stabilen, sauberen Fläche ab.
5. Entfernen Sie das gesamte Verpackungsmaterial.
6. Untersuchen Sie das Produkt auf Beschädigungen. Schäden sollten unverzüglich gemeldet werden. Dell-Kontaktinformationen finden Sie unter "Weitere Hilfe".

Rackmontage des Gerätes

VORSICHT: Ziehen Sie alle Kabel vom Gerät ab, bevor Sie den PowerConnect 3324/3348-Switch in einem Rack oder Gehäuse montieren.

Montieren des PowerConnect 3324/3348:

1. Legen Sie ein EGB-Handgelenkband an, und verbinden Sie die EGB-Klammer mit einer Metallfläche, um eine ausreichende Erdung zu gewährleisten.
2. Setzen Sie den PowerConnect 3324/3348-Switch auf einer ebenen, stabilen Oberfläche ab.
3. Platzieren Sie das mitgelieferte Rackmontageblech auf einer Seite des PowerConnect 3324/3348, wobei sich die Montagebohrungen am PowerConnect 3324/3348 mit den Montagebohrungen am Rackmontageblech decken müssen.
4. Führen Sie die mitgelieferten Schrauben in die Rackmontagebohrungen ein, und ziehen Sie diese mit einem Kreuzschlitzschraubendreher fest.
5. Wiederholen Sie die Schritte für das Rackmontageblech auf der anderen Seite des PowerConnect 3324/3348.
6. Setzen Sie die Einheit in das 19-Zoll-Rack ein, und befestigen Sie diese mit den Rackschrauben (nicht im Lieferumfang des PowerConnect 3324/3348 enthalten) am Rack. Ziehen Sie das untere Schraubenpaar vor dem oberen an, so dass während der Montage das Gewicht der Einheit gleichmäßig verteilt wird. Die Belüftungsöffnungen dürfen nicht versperrt sein.

Montieren des Switches ohne Rack

Falls kein Rack verwendet wird, muss der PowerConnect 3324/3348 auf einer ebenen Fläche montiert werden. Die Tragfähigkeit der Fläche muss für das Gerät und die Gerätekabel ausreichen.

1. Stellen Sie den PowerConnect 3324/3348 auf einer ebenen Fläche ab, und lassen Sie an den Seiten 5 cm sowie auf der Rückseite 13 cm Platz.
2. Es muss eine ausreichende Belüftung gewährleistet sein.
3. Befestigen Sie die Gummifüße an der Unterseite des Gerätes, um ein Verrutschen des Gerätes zu verhindern.

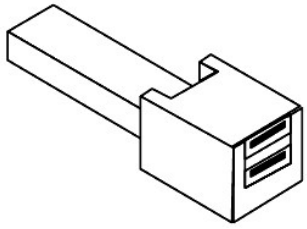
Stack-Montage des PowerConnect 3324/3348

Der PowerConnect 3324/3348 unterstützt die Stack-Montage von bis zu sechs PowerConnect 3324/3348-Geräten oder bis zu 192 Fast Ethernet- und sechs Giga-Anschlüssen. Jeder PowerConnect 3324/3348-Stack verfügt über eine einzelne Mastereinheit, während die übrigen Einheiten als Stack-Komponente betrachtet werden. Die gesamte Verwaltung erfolgt über die Mastereinheit. Der Stack kann sowohl Geräte mit 24 als auch mit 48 Anschlüssen umfassen.

Damit das Stacking unterstützt wird, müssen die Einheiten in einer Stack-Konfiguration mit einem Stack-Modul angeordnet werden, das mit dem G2-Anschluss im SFP-Steckplatz verbunden ist.

Stacking-Kabel anschließen

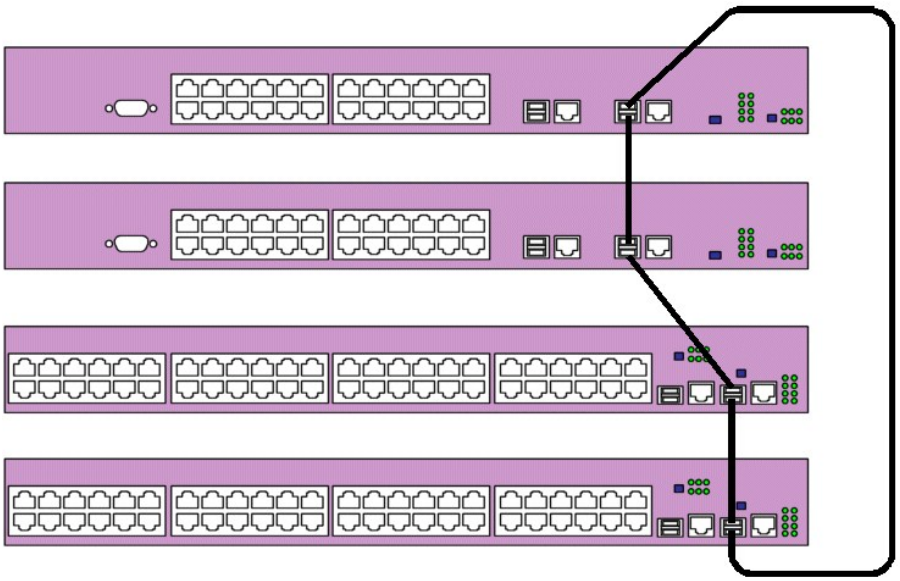
1. Platzieren Sie jedes Gerät im Rack oder auf einer ebenen Fläche.
2. Bringen Sie für jeden G2-Anschluss einen Stack-Anschluss an.



USB-Anschluss

3. Verbinden Sie den unteren RX-Stack-Anschluss der Mastereinheit mit dem oberen TX-Anschluss der ausgewählten Komponente.
4. Legen Sie die Stack-Verbindungen in einer Ringtopologie an, wobei die Stacking-Kabel vom unteren RX-Stack-Anschluss zum oberen TX-Stack-Anschluss führen.
5. Stellen Sie sicher, dass obere und untere Stack-Komponente über ein Stacking-Kabel verbunden sind. In der folgenden Abbildung ist ein ordnungsgemäß verbundener Stack zu sehen:

ANMERKUNG: Der Stacking-Ring muss geschlossen sein, damit der Stack funktionsfähig ist.



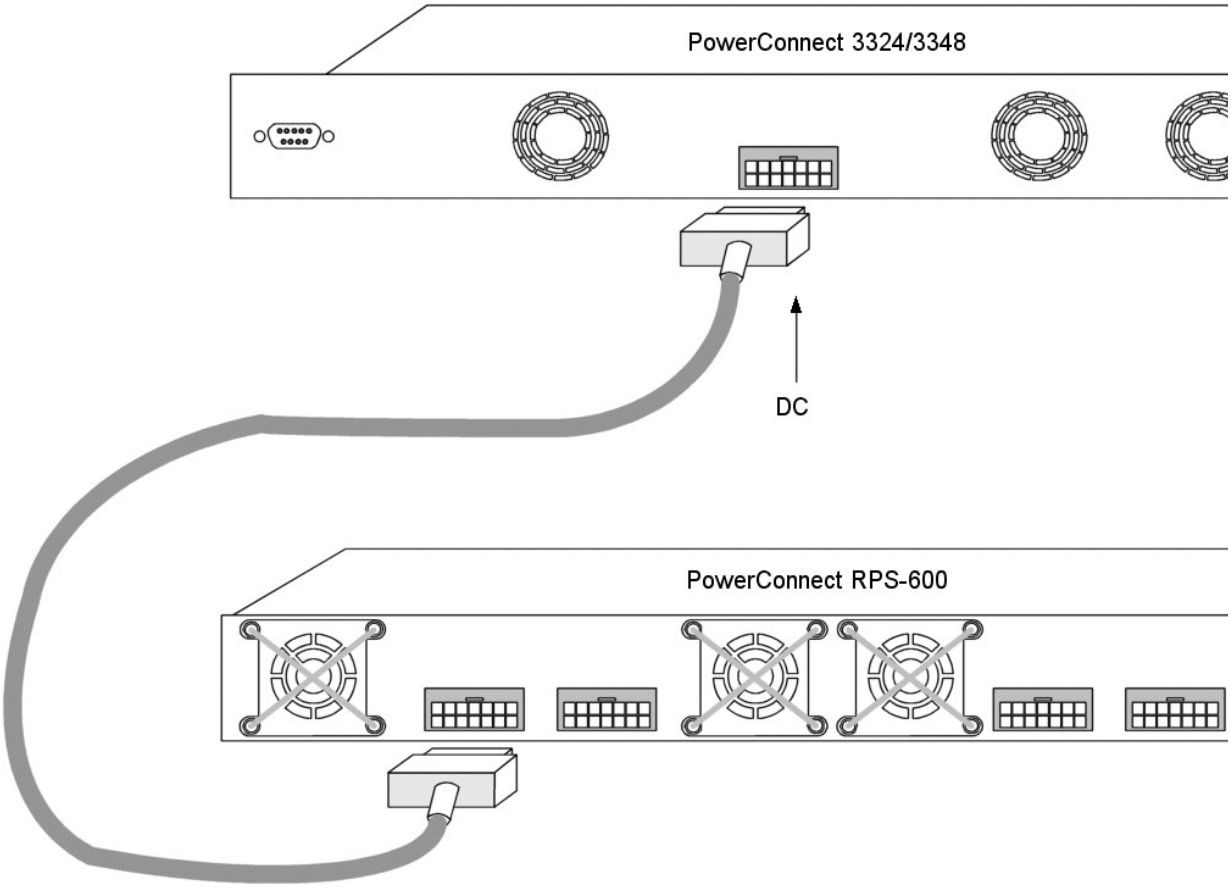
Verbundener Stack

Weitere Informationen zur Konfiguration von Stacks finden Sie unter "Stacking-Konfiguration".

Anschließen des PowerConnect 3324/3348 an die Stromversorgung

Der folgende Abschnitt enthält Anweisungen zum Anschluss des PowerConnect 3324/3348 an eine Netzstromquelle. Die Stromversorgung des PowerConnect 3324/3348 erfolgt über:

- Netzstromquelle
- Optionale, redundante PowerConnect RPS-600-Stromversorgung
- Sowohl Stromquellen mit Wechsel- als auch Gleichspannung



PowerConnect 3324/3348 an die Stromversorgung anschließen

- Verbinden Sie den PowerConnect 3324/3348 mit einer der zuvor aufgelisteten Stromquellen.

Anschluss an die Netzstromversorgung

Der Strom sollte über ein 1,5 m langes, geerdetes Standardkabel mit Schutzkontakt in das Gerät geleitet werden.

So schließen Sie den PowerConnect 3324/3348 an die Stromversorgung an:

1. Verbinden Sie das Netzkabel mit der Haupt-Netzanschlussbuchse auf dem rückseitigen Bedienfeld. Bei Verwendung einer redundanten Stromversorgung das dazugehörige Kabel an eine separate Stromquelle anschließen.
2. Das Stromkabel mit einer geerdeten Netzsteckdose verbinden.
3. Stellen Sie durch die Überprüfung der LEDs an der Vorderseite sicher, dass das Gerät angeschlossen ist und fehlerfrei funktioniert. Weitere Informationen zu den LEDs finden Sie unter "LED-Definitionen".

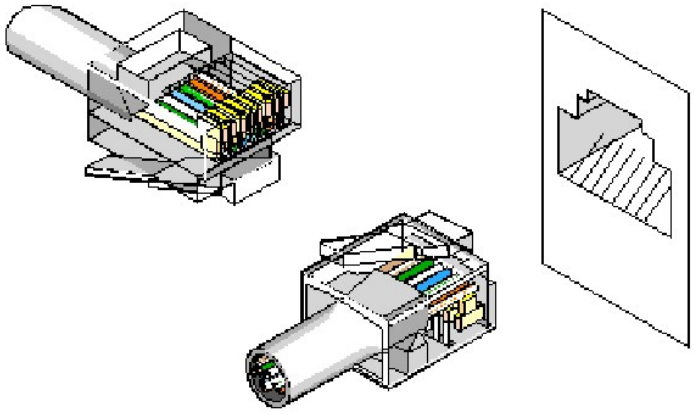
Informationen zu Kabeln, Anschlüssen und Kontaktbelegung

In diesem Abschnitt werden die physischen Schnittstellen des PowerConnect 3324/3348 sowie die Kabelverbindungen beschrieben. Die Stationen werden über die auf der Vorderseite befindlichen physischen Schnittstellenanschlüsse mit den Anschlüssen des PowerConnect 3324/3348 verbunden. Für jede Station wird der geeignete Modus (Halbduplex-, Vollduplex- bzw. automatischer Modus) eingestellt.

Anschlussverbindungen

Die Anschlüsse sind ausnahmslos RJ45-Ethernet-Standardanschlüsse. Unter Verwendung von "Straight-Through"-Kabeln können Switching-Anschlüsse mit Stationen verbunden werden, die gemäß dem RJ45-Ethernet-Standardstationsmodus verkabelt sind. Übertragungsgeräte werden mit Hilfe von Kreuzkabeln miteinander verbunden.

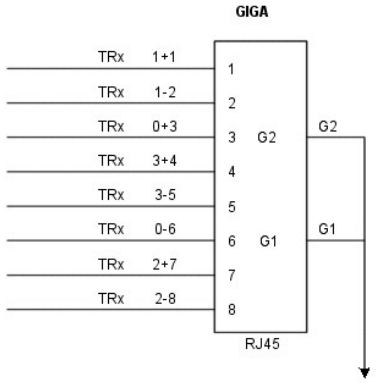
In der folgenden Abbildung wird die RJ45-Kontaktbelegung für 10/100 Mbit/s-Anschlüsse erläutert.



RJ45-Kontaktzuweisung

Pin	Verwendung
1	RX +
2	RX -
3	TX +
4	
5	--
6	TX -
7	-
8	-

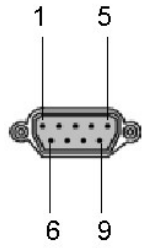
Die folgende Abbildung veranschaulicht den GigaPort-Anschluss:



GigaPort-Anschluss

Für Setup und Erstkonfiguration wird der PowerConnect 3324/3348 über ein serielles Kabel mit einem Terminal verbunden. (Hierzu kann auch ein PC mit Terminal-Emulationssoftware verwendet werden.) Bei dem seriellen Kabel handelt es sich um ein DB-9-Crossover-Kabel (Buchse/Buchse).

Die folgende Abbildung veranschaulicht den DB-9-Anschluss.



Serielles DB-9-Kabel

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

DB-9-Kontaktzuweisung

Kabelverbindungen

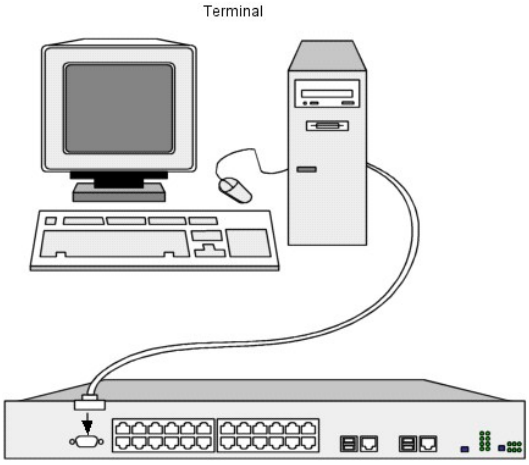
In diesem Abschnitt wird der Anschluss der verschiedenen Kabel an den PowerConnect 3324/3348 beschrieben.

ASCII-Terminalverbindung (seriell)

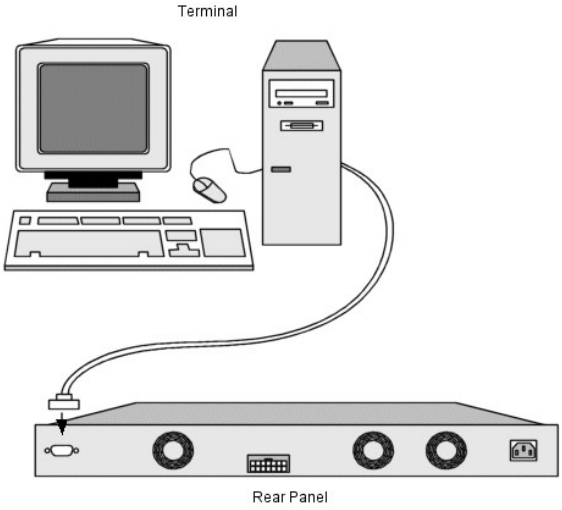
Für den seriellen Anschluss wird ein DB-9-Anschluss verwendet. Zum Anschluss des Gerätes ist das mitgelieferte Schnittstellenkabel erforderlich.

So schließen Sie das Gerät an:

1. Verbinden Sie das Schnittstellen-Kreuzkabel mit dem ASCII DTE RS-232-Anschluss am Terminal.
2. Verbinden Sie das Schnittstellen-Kreuzkabel mit dem seriellen Anschluss am Gerät.



Terminalverbindung mit dem PowerConnect 3324



Terminalverbindung mit dem PowerConnect 3348

Zurück zum Inhalt

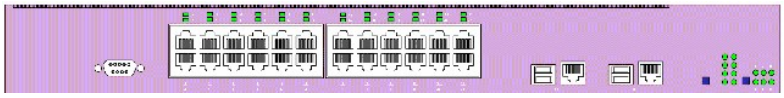
Zurück zum Inhalt

Übersicht

Dell™ PowerConnect™ 3324/3348 Benutzerhandbuch

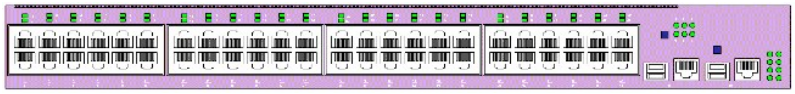
Systembeschreibung

Bei den Geräten Dell™ PowerConnect™ 3324 und 3348 handelt es sich um hoch entwickelte Layer 2-Switches, die einzeln oder im Stack eingesetzt werden können. Der PowerConnect 3324 und der PowerConnect 3348 können auch als eigenständige Layer 2-Switching-Systeme verwendet werden. Die PowerConnect 3324/3348-Geräte werden entweder per In-Band-Verwaltung (über die Netzwerkstation) oder über die Konsole verwaltet.



PowerConnect 3324

Beim Betrieb als Stack-Komponente bietet jede PowerConnect 3324-Einheit 24 10BaseT/100BaseTX Fast Ethernet-Anschlüsse, einen Gigabit Ethernet-Combo-Anschluss (10/100/1000 BaseT- oder Mini-GBIC-Anschluss) sowie einen Giga Ethernet-Stack-Anschluss.



PowerConnect 3348

Beim Betrieb als Stack-Komponente bietet jede PowerConnect 3348-Einheit 48 10BaseT/100BaseTX Fast Ethernet-Anschlüsse, einen Gigabit Ethernet-Combo-Anschluss (10/100/1000 BaseT- oder Mini-GBIC-Anschluss) sowie einen Giga Ethernet-Stack-Anschluss.

Beim Betrieb als eigenständige Einheit können die Stack-Anschlüsse des PowerConnect 3324/3348 als Giga Ethernet-Anschlüsse genutzt werden.

Übersicht über die Stack-Montage des PowerConnect 3324/3348

Die Verwendung des PowerConnect 3324/3348 im Stack ermöglicht die Verwaltung mehrerer Geräte von einem zentralen Punkt aus, so als bildeten sämtliche Stack-Komponenten eine Einheit. Der Zugriff auf sämtliche Komponenten erfolgt über eine einzige IP-Adresse für die SNMP-Verwaltung sowie eine Konsolen-/Telnet-Sitzung, über die der gesamte Stack verwaltet wird.

Der PowerConnect 3324/3348 unterstützt Stacks von jeweils maximal sechs Einheiten bzw. die Erweiterung auf 192 Fast Ethernet- und sechs Gigabit Ethernet-Anschlüsse. Die PowerConnect 3324- und PowerConnect 3348-Geräte können auch als eigenständige Einheiten verwendet werden.

Während des Stack-Setups wird ein Gerät vom Netzwerkadministrator als Stack-Master ausgewählt, während die übrigen Geräte als Stack-Komponenten konfiguriert und mit einer eindeutigen Einheiten-ID versehen werden.

PowerConnect 3324/3348-Stacks bieten Stack-übergreifende Layer 2-Funktionalität, darunter:

- Switching
- Trunking
- Port Mirroring
- VLANs

VLANs können beispielsweise über Anschlüsse unterschiedlicher Stack-Komponenten konfiguriert werden, und es besteht die Möglichkeit, die Anschlussspiegelung so zu konfigurieren, dass sie von einer zweiten zu einer dritten Stack-Komponente erfolgt. Anwendungen in einer Stack-Konfiguration werden zentral ausgeführt. So wird beispielsweise das Spanning Tree-Protokoll für den gesamten Stack auf der Mastereinheit ausgeführt. Gerätesoftware wird für jede Stack-Komponente separat heruntergeladen.

Die PowerConnect 3324/3348-Stack-Architektur unterstützt die dynamische Adressenerfassung für die Stack-Topologie. Außerdem können die Anschlüsse unter minimaler Beeinträchtigung des Stack-Betriebs ermittelt und neu konfiguriert werden, falls eines der folgenden Ereignisse auftritt:

- Ausfall einer Einheit
- Verbindungsunterbrechung zwischen Einheiten
- Einsetzen einer Einheit
- Entfernen einer Stack-Einheit

Stack-Komponenten und Einheiten-ID

Der Stack-Betriebsmodus wird während des Startvorgangs festgelegt.

PowerConnect 3324/3348-Einheiten werden mit der standardmäßigen Einheiten-ID 1 geliefert. Die Einheiten-ID ist eine wesentliche Voraussetzung für die Stack-Konfiguration. Wenn eine Stack-Komponente ohne Stack-Modul neu startet, arbeitet das Gerät im eigenständigen Modus, bis es zurückgesetzt wird. Wird eine PowerConnect 3324/3348-Einheit im eigenständigen Modus betrieben, leuchtet keine der Stack-LEDs. Wird die Einheit wieder an einen Stack angeschlossen, wird die Einheiten-ID nicht gelöscht und behält ihre Gültigkeit.

ANMERKUNG: Das Stack-Modul muss in Anschluss G2 eingesetzt werden, damit der Stack funktionsfähig ist. Bei Einsetzen des Stack-Moduls in Anschluss G1 erscheint eine Warnmeldung auf der Konsole.

Wird die Mastereinheit gestartet bzw. eine Stack-Komponente eingesetzt oder entfernt, wird von der Mastereinheit ein Stack-Erkennungsvorgang initiiert. Falls zwei Komponenten mit derselben Einheiten-ID erkannt werden oder keine Mastereinheit gefunden wird, ist der gesamte Stack nicht funktionsfähig. Die Stack-LED leuchtet in diesem Fall weiterhin rot.

Konfigurationsverwaltung

In einem funktionsfähigen PowerConnect 3324/3348-Stack ist der Stack-Master für die Stack-Konfiguration verantwortlich. Die Stack-Komponenten verfügen nicht über separate Konfigurationsdateien. Jeder Anschluss im Stack verfügt über eine spezifische Einheiten-ID sowie über einen eigenen Anschlusstyp und eine Anschlussnummer, die sowohl Teil der Konfigurationsbefehle als auch der Konfigurationsdateien sind. Konfigurationsdateien werden ausschließlich vom PowerConnect 3324/3348-Stack-Master verwaltet. Die Verwaltung umfasst:

- Speichern im FLASH
- Hochladen von Konfigurationsdateien auf einen externen TFTP-Server
- Herunterladen von Konfigurationsdateien von einem externen TFTP-Server

ANMERKUNG: Selbst wenn der Stack zurückgesetzt wird und/oder die Anschlüsse nicht mehr vorhanden sind, wird die Stack-Konfiguration für alle konfigurierten Anschlüsse gespeichert.

Konfigurationsdateien können nur explizit durch einen Benutzer geändert werden. Außerdem werden die Konfigurationsdateien in folgenden Fällen nicht automatisch geändert:

- Hinzufügen von Einheiten.
- Entfernen von Einheiten.
- Neuzuweisung von Einheiten-IDs
- Umschalten zwischen Stack-Modus und eigenständigem Modus einer Einheit.

Bei jedem Systemneustart wird die gespeicherte Konfiguration in die Startkonfigurationsdatei geschrieben.

Wenn eine PowerConnect 3324/3348-Stack-Komponente aus dem Stack entfernt und anschließend durch ein Gerät mit derselben Einheiten-ID ersetzt wird, wird die Stack-Komponente mit der ursprünglichen Gerätekonfiguration konfiguriert.

In Dell OpenManage™ Switch Administrator werden lediglich physisch vorhandene Anschlüsse angezeigt; diese können mit Hilfe des Webverwaltungssystems konfiguriert werden. Nicht vorhandene Anschlüsse werden über die CLI- bzw. SNMP-Schnittstellen konfiguriert.

Neuanordnen von Stacks

Die Stack-Reihenfolge kann geändert werden, indem entweder eine Stack-Komponente entfernt wird oder die Stacking-Kabel neu angeordnet werden. Die Reihenfolge von Stack-Komponenten wird nicht durch ihre physische Anordnung, sondern durch die zugewiesene Einheiten-ID festgelegt. Nachdem die Stack-Reihenfolge geändert und der Stack zurückgesetzt wurde, wird die Stack-Konfiguration im Stack-Master gespeichert.

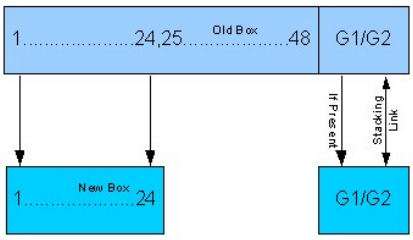
Wenn die PowerConnect 3324/3348-Einheit aus einem Stack entfernt bzw. ausgetauscht wird, wird die Stack-Konfiguration wie folgt wiederhergestellt:

- Falls die Stack-Unterbrechung länger als zwei Minuten dauert, stellt der gesamte Stack die Weiterleitung von Netzwerkdaten ein. Jede Stack-Komponente wird neu gestartet und wartet, bis der Stack wieder verbunden wird. Falls die Einheit nicht ersetzt wird, wird der Stack kontinuierlich von der Mastereinheit abgefragt.
- Falls die Stack-Verbindung in weniger als zwei Minuten wiederhergestellt wird, verbleiben alle Einheiten in der Stack-Konfiguration, und die Verbindung zu anderen Einheiten wird innerhalb von fünf Sekunden wieder aufgenommen. Eine neue Stack-Komponente wird mit der Mastereinheit verbunden, aber entsprechend der Konfiguration der Mastereinheit initialisiert. Falls eine Konfiguration nicht gespeichert wurde, wird das Gerät entsprechend der Standardkonfiguration eingerichtet.

Austauschen von Stack-Komponenten

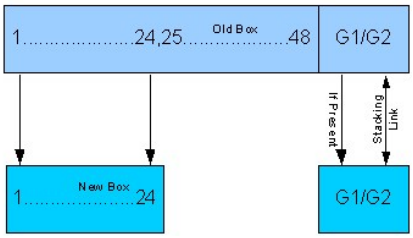
Wird eine Stack-Komponente durch ein neues Gerät ersetzt, wird die erforderliche Geräte-ID ausgewählt. Darüber hinaus wird die zuvor gültige Gerätekonfiguration auf die hinzugefügte Stack-Komponente angewendet. Sofern das neu hinzugefügte Gerät über mehr oder weniger Anschlüsse als das vorherige Gerät verfügt, wird die entsprechende Anschlusskonfiguration auf die neue Stack-Komponente angewendet. Beispielsweise:

- Wird ein PowerConnect 3324 durch einen PowerConnect 3324 ersetzt, wird für die neuen 24 10/100BaseT-Anschlüsse die Kofiguration der zuvor bestehenden 24 Anschlüsse übernommen. Für die Anschlüsse G1 und G2 wird die G1- und G2-Anschlusskonfiguration des vorherigen Gerätes verwendet.
- Wird ein PowerConnect 3348 durch einen PowerConnect 3324 ersetzt, wird für die 10/100BaseT-Anschlüsse 1 bis 24 die Konfiguration der Anschlüsse 1 bis 24 des vorherigen Gerätes verwendet. Dabei wird für die Anschlüsse G1 und G2 die G1- und G2-Anschlusskonfiguration des vorherigen Gerätes verwendet.



PowerConnect 3348 wird durch PowerConnect 3324 ersetzt

- Wird ein PowerConnect 3348 durch einen PowerConnect 3348 ersetzt, wird für die neuen 48 10/100BaseT-Anschlüsse die zuvor gültige 48 10/100BaseT-Anschlusskonfiguration übernommen. Für die Anschlüsse G1 und G2 wird die G1- und G2-Anschlusskonfiguration des vorherigen Gerätes verwendet.
- Wird ein PowerConnect 3324 durch einen PowerConnect 3348 ersetzt, wird für die 10/100 BaseT-Anschlüsse 1 bis 24 die Konfiguration des vorherigen Gerätes übernommen.
- Für die Anschlüsse 25 bis 48 wird die werkseitige Standardkonfiguration verwendet. Für die Anschlüsse G1 und G2 wird die G1- und G2-Anschlusskonfiguration des vorherigen Gerätes verwendet.



PowerConnect 3324 wird durch PowerConnect 3348 ersetzt

Übersicht über das PowerConnect Benutzerhandbuch

Das PowerConnect Benutzerhandbuch ist in zwei Bereiche gegliedert:

- Informationen zur Installation des PowerConnect 3324/3348-Switches
- Verwenden von OpenManage Switch Administrator

Installieren des PowerConnect 3324/3348-Switches

Dieser Abschnitt enthält die folgenden Unterabschnitte zum Auspacken sowie zur Installation und Konfiguration des PowerConnect 3324/3348:

- Hardwarebeschreibung - Enthält Informationen zur PowerConnect 3324/3348-Hardware, einschließlich einer Beschreibung der Anschlüsse und LED-Kategorien.
- Installieren des PowerConnect 3324/3348-Switches - Enthält Anweisungen zur Installation des PowerConnect 3324/3348 im Rack oder auf einer ebenen Fläche. Dieser Abschnitt enthält außerdem Sicherheitshinweise für die Installation sowie eine Beschreibung der Anschlüsse und Kabel.
- Konfigurieren des PowerConnect 3324/3348-Switches - Enthält Anweisungen zur Erstkonfiguration des Gerätes, einschließlich Informationen zum Herunterladen von Gerätesoftware, zum Startbildschirm des Gerätes sowie zu optionalen Konfigurationsfunktionen.

Verwenden von OpenManage Switch Administrator

Dieser Abschnitt enthält die folgenden Informationen zur Gerätekonfiguration mit Hilfe des Webverwaltungssystems und des CLI-(Command Line Interface-) Geräteverwaltungssystems:

- Erste Schritte - Enthält Informationen zum Einstieg in die Oberfläche des Webverwaltungssystems, einschließlich einer Erläuterung der Verwaltungs- und Informationsschaltflächen, der Komponentenliste sowie der Geräte- und Strukturansicht.
- Konfigurieren von Systeminformationen - Enthält Informationen zur Konfiguration allgemeiner Systeminformationen, darunter Festlegen von Systeminformationen, Konfigurieren einer IP-Standardadresse, Festlegen der Gerätesicherheit und der SNMP-Communities, Herunterladen von Gerätesoftware sowie Festlegen erweiterter Einstellungen.
- Konfigurieren von Switch-Informationen - Enthält Informationen zur Konfiguration von Anschlüssen und VLANs, zur Definition von statischen und dynamischen Adresstabellen, zur Konfiguration von GARP und GVRP, zur Definition von Spanning Tree-Parametern, zur Bündelung von Anschlüssen sowie zur Konfiguration der Unterstützung für die Multicastweiterleitung.
- Anzeigen von Statistiken - Enthält Informationen zur Anzeige von Tabellen- und Diagrammstatistiken für Anschlüsse, GVRP, Etherlike, RMON sowie Schnittstellenstatistiken.
- Konfigurieren von Quality of Service (QoS) - Enthält Informationen über die CoS-(Class of Service-)Konfiguration für Geräte.
- Weitere Hilfe - Enthält Informationen zur technischen Unterstützung, zu Problemen mit Bestellungen, zur Rücksendung von Teilen zur Reparatur oder zur Gutschrift sowie zur Kontaktaufnahme mit Dell.

PowerConnect 3324/3348 CLI-Dokumentation

Neben dem *PowerConnect 3324/3348 Benutzerhandbuch* bietet Dell das *PowerConnect 3324/3348 CLI Reference Guide* an. Das *PowerConnect 3324/3348 CLI Reference Guide* liefert detaillierte Informationen über die zur Konfiguration des PowerConnect 3324/3348 verwendeten CLI-Befehle.

Zurück zum Inhalt

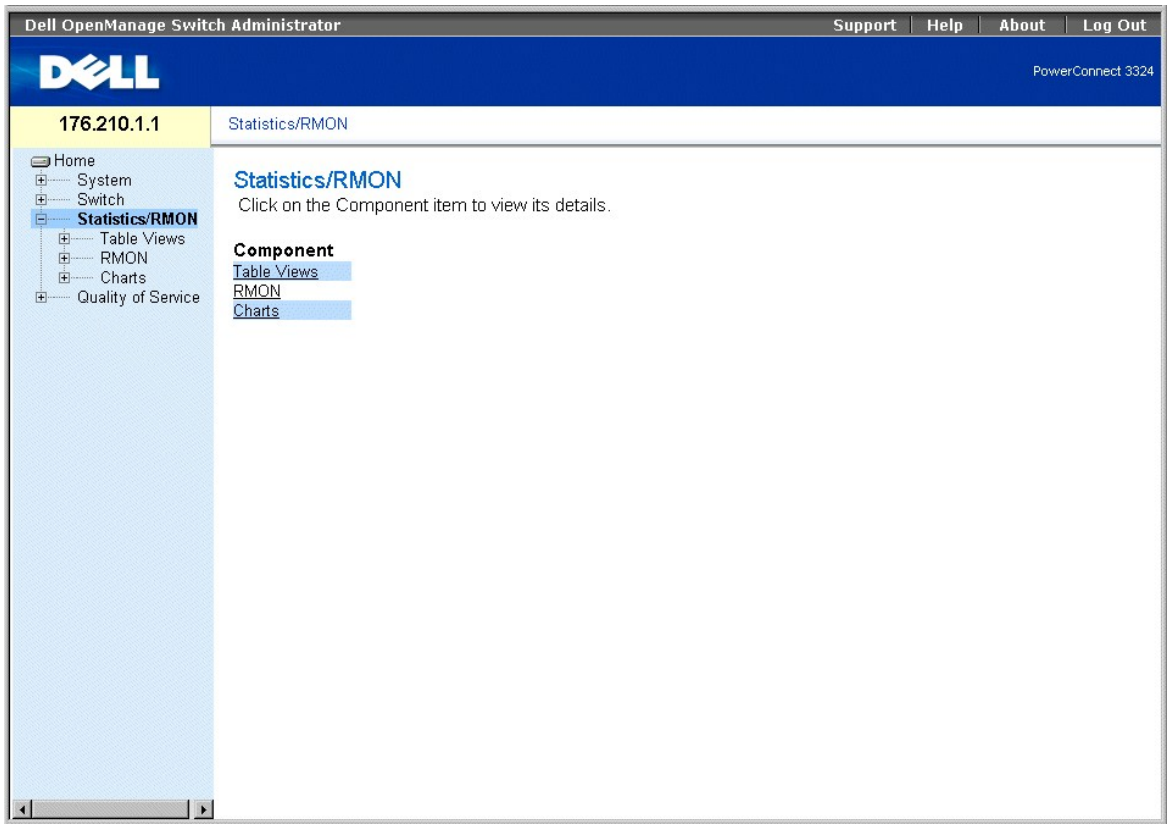
Zurück zum Inhalt

Anzeigen von Statistiken

Dell™ PowerConnect™ 3324/3348 Benutzerhandbuch

Die Statistikseiten enthalten Geräteinformationen zu Schnittstellen, GVRP, Etherlike, RMON sowie zur Gerätenutzung. So öffnen Sie die Seite **Statistics / RMON**:

- Klicken Sie in der Strukturansicht auf **Statistics / RMON**. Die Seite **Statistics / RMON** wird geöffnet.



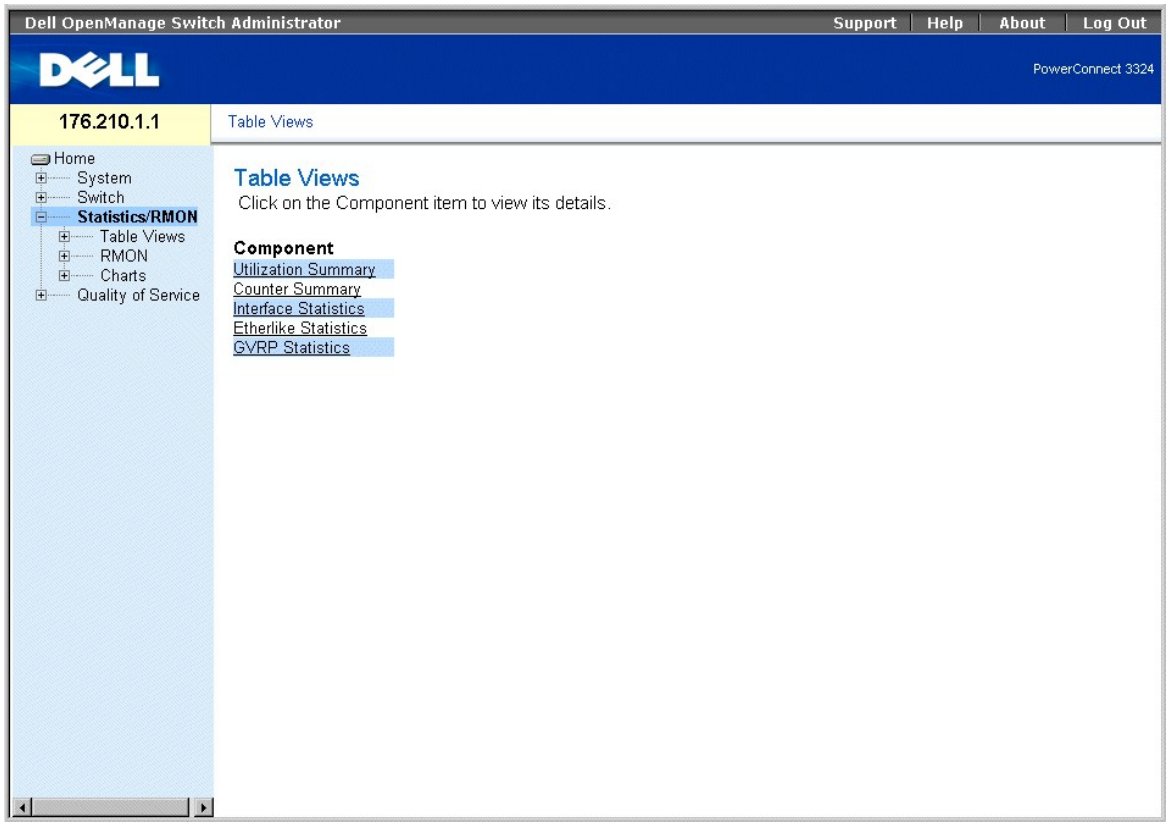
Seite "Statistics / RMON"

Dieser Abschnitt umfasst die folgenden Themen:

Anzeigen von Tabellen

Die Seite **Table View** enthält Links zur Anzeige von Statistiken in Tabellenform. So öffnen Sie die Seite **Table View**:

- Klicken Sie in der Strukturansicht auf **Statistics** > **Table**. Die Seite **Table View** wird geöffnet.



Seite "Table View"

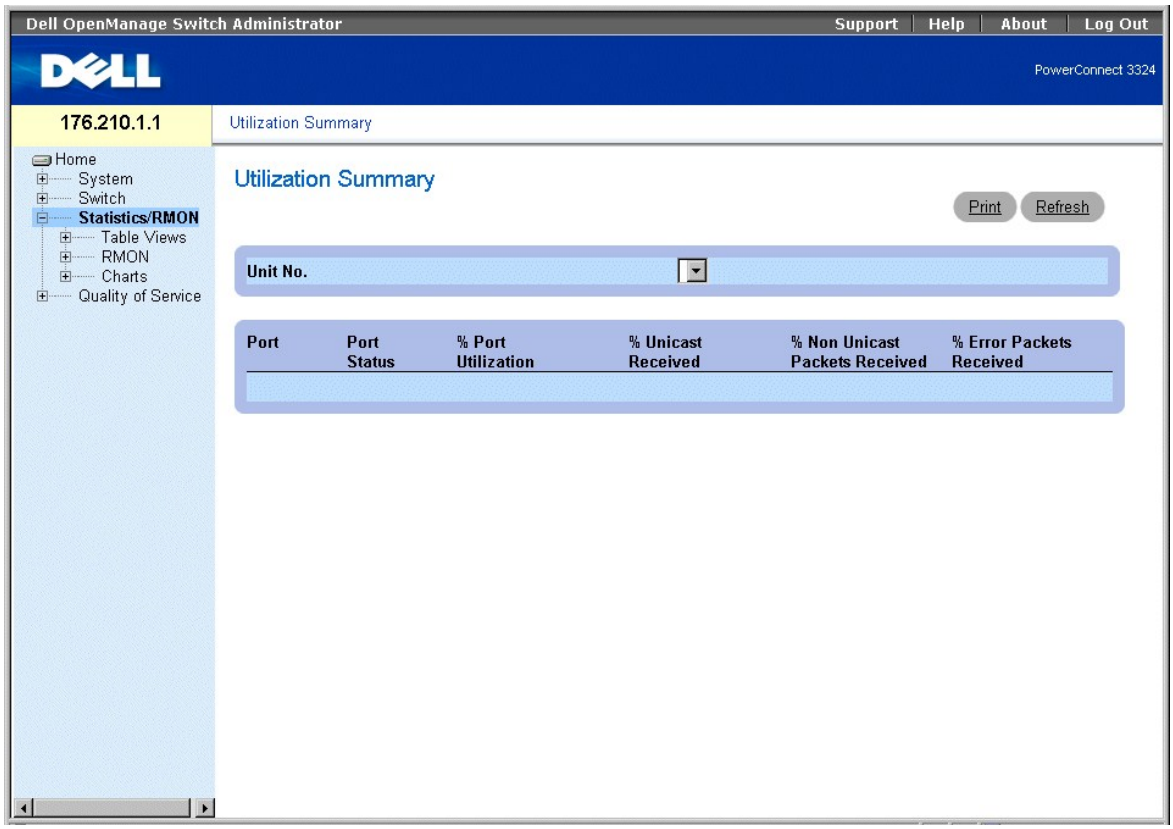
Die Seite **Table View** enthält die folgenden Links:

- Anzeigen der Seite "Utilization Summary"
- Anzeigen der Seite "Counter Summary"
- Anzeigen der Seite "Interface Statistics"
- Anzeigen der Seite "Etherlike Statistics"
- Anzeigen der Seite "GVRP Statistics"

Anzeigen der Seite "Utilization Summary"

Die Seite **Utilization Summary** enthält Statistiken zur Anschlussnutzung. So öffnen Sie die Seite **Utilization Summary**:

- Klicken Sie in der Strukturansicht auf **Statistics** > **Table View** > **Utilization Summary**. Die Seite **Utilization Summary** wird geöffnet:



Seite "Utilization Summary"

Die Seite **Utilization Summary** enthält folgende Felder:

- **Unit No.**- Gibt die Nummer der Einheit an, für welche die Anschlussstatistik angezeigt wird.
- **Port**- Gibt die Anschlussnummer an.
- **Port Status**- Gibt den Anschlussstatus an.
- **% Port Utilization**- Gibt die Anschlussnutzung an.
- **% Unicast Received**- Gibt den Prozentsatz der über die Anschlüsse empfangenen Unicast-Pakete an.
- **% Non Unicast Received**- Gibt die Anzahl der über den Anschluss empfangenen ungültigen Pakete an.
- **% Error Packets Received**- Gibt die Anzahl der über den Anschluss empfangenen fehlerhaften Pakete an.

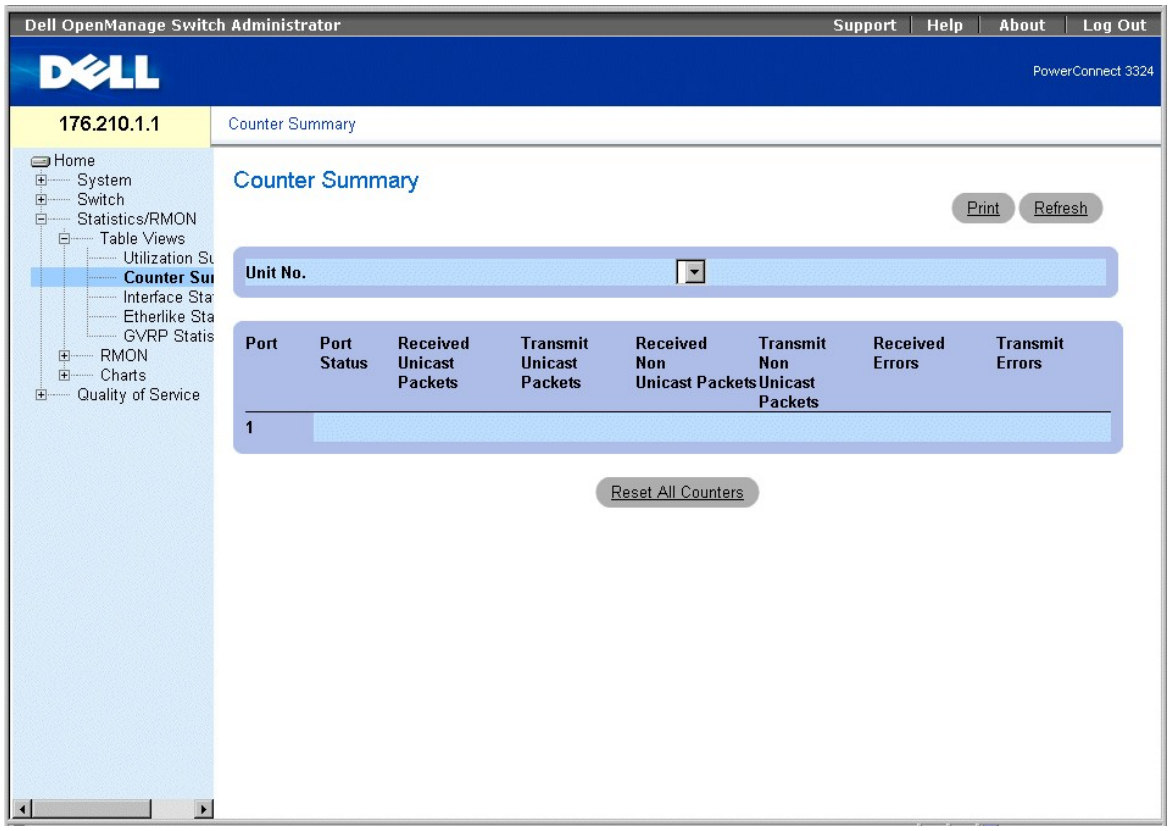
Anzeigen von Nutzungsstatistiken:

1. Öffnen Sie die Seite **Utilization Summary**.
2. Wählen Sie eine Einheit im Feld **Unit** aus. Für die ausgewählte Einheit wird die Nutzungsstatistik angezeigt.

Anzeigen der Seite "Counter Summary"

Die auf der Seite **Counter Summary** enthaltenen Statistiken geben die Anschlussnutzung in absoluten Zahlen und nicht in Prozentwerten wieder. So öffnen Sie die Seite **Counter Summary**:

- Klicken Sie in der Strukturansicht auf **Statistics/RMON** > **Table Views** > **Counter Summary**. Die Seite **Counter Summary** wird geöffnet:



Seite "Counter Summary"

Die Seite **Counter Summary** enthält folgende Felder:

- **Unit No.**- Gibt die Nummer der Einheit an, für welche die Anschlussstatistik angezeigt wird.
- **Port**- Gibt die Anschlussnummer an.
- **Port Status**- Gibt den Anschlussstatus an.
- **Received Unicast Packets**- Gibt die Anzahl der über den Anschluss empfangenen Unicast-Pakete an.
- **Transmit Unicast Packets**- Gibt die Anzahl der über den Anschluss gesendeten Unicast-Pakete an.
- **Received Non-Unicast Packets**- Gibt die Anzahl der über den Anschluss empfangenen Non-Unicast-Pakete an.
- **Transmit Non-Unicast Packets**- Gibt die Anzahl der über den Anschluss gesendeten Non-Unicast-Pakete an.
- **Received Errors**- Gibt die Anzahl der über den Anschluss empfangenen Fehler an.
- **Transmit Errors**- Gibt die Anzahl der über den Anschluss gesendeten Fehler an.

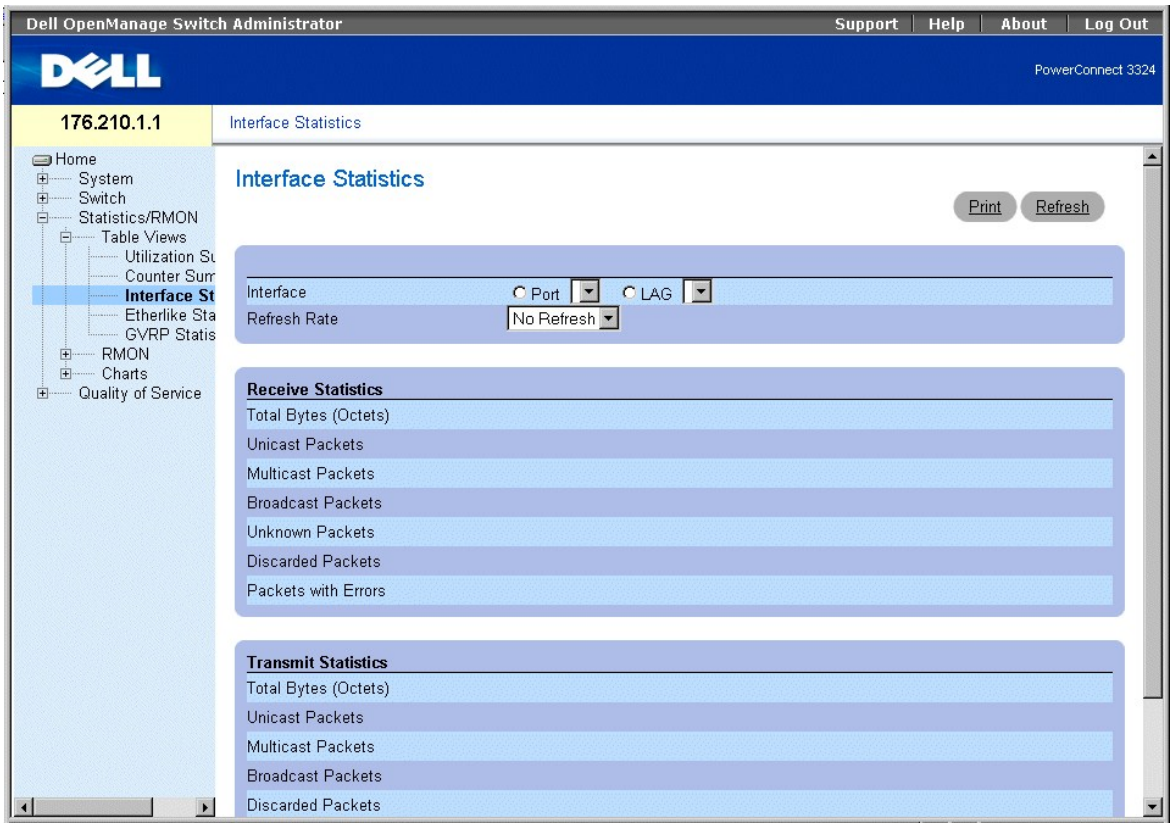
Anzeigen von Zählerübersichtsstatistiken:

1. Öffnen Sie die Seite **Counter Summary**.
2. Wählen Sie eine Einheit im Feld **Unit** aus. Für die ausgewählte Einheit wird die Zählerübersichtsstatistik angezeigt.

Anzeigen der Seite "Interface Statistics"

Die Seite **Interface Statistics** enthält Schnittstellenstatistiken. So öffnen Sie die Seite **Interface Statistics**:

- Klicken Sie in der Strukturansicht auf **Statistics/RMON** > **Table Views** > **Interface Statistics**. Die Seite **Interface Statistics** wird geöffnet.



Seite "Interface Statistics"

Die Seite **Interface Statistics** enthält folgende Felder:

- **Interface**- Gibt die Schnittstelle (Typ und Nummer) an, für welche die Statistik angezeigt wird.
  - **Port**- Gibt den Anschluss an, für den die Statistik angezeigt wird.
  - **LAG**- Gibt die LAG an, für welche die Statistik angezeigt wird.
- **Refresh Rate**- Gibt den Zeitraum bis zur Aktualisierung der Schnittstellenstatistiken an. Folgende Feldwerte können ausgewählt werden:
  - **15 Sec**- Gibt an, dass die Schnittstellenstatistiken alle 15 Sekunden aktualisiert werden.
  - **30 Sec**- Gibt an, dass die Schnittstellenstatistiken alle 30 Sekunden aktualisiert werden.
  - **60 Sec**- Gibt an, dass die Schnittstellenstatistiken alle 60 Sekunden aktualisiert werden.
  - **No Refresh**- Gibt an, dass die Schnittstellenstatistiken nicht automatisch aktualisiert werden.
- **Total Bytes (Octets) Received**- Zeigt die über die ausgewählte Schnittstelle empfangene Bytemenge an.
- **Received Unicast Packets**- Zeigt die Anzahl der über die ausgewählte Schnittstelle empfangenen Unicast-Pakete an.
- **Received Multicast Packets**- Zeigt die Anzahl der über die ausgewählte Schnittstelle empfangenen Multicast-Pakete an.
- **Received Broadcast Packets**- Zeigt die Anzahl der über die ausgewählte Schnittstelle empfangenen Broadcast-Pakete an.
- **Received Unknown Packets**- Zeigt die Anzahl der über die ausgewählte Schnittstelle empfangenen unbekannten Pakete an.
- **Received Discarded Packets**- Zeigt die Anzahl der Pakete an, die beim Empfang über die ausgewählte Schnittstelle verworfen wurden.
- **Received Packets with Errors**- Zeigt die Anzahl der über die ausgewählte Schnittstelle empfangenen fehlerhaften Pakete an.
- **Total Bytes (Octets) Transmitted**- Gibt die über die ausgewählte Schnittstelle gesendete Bytemenge an.
- **Transmitted Unicast Packets**- Zeigt die Anzahl der über die ausgewählte Schnittstelle gesendeten Unicast-Pakete an.
- **Transmitted Multicast Packets**- Zeigt die Anzahl der über die ausgewählte Schnittstelle gesendeten Multicast-Pakete an.
- **Transmitted Broadcast Packets**- Zeigt die Anzahl der über die ausgewählte Schnittstelle gesendeten Broadcast-Pakete an.
- **Transmitted Unknown Packets**- Zeigt die Anzahl der über die ausgewählte Schnittstelle gesendeten unbekannten Pakete an.
- **Transmitted Discarded Packets**- Zeigt die Anzahl der Pakete an, die beim Senden über die ausgewählte Schnittstelle verworfen wurden.
- **Transmitted Packets with Errors**- Zeigt die Anzahl der Pakete an, die während des Sendens über die ausgewählte Schnittstelle als fehlerhaft identifiziert wurden.

Anzeigen von Schnittstellenstatistiken für einen Anschluss:

1. Öffnen Sie die Seite **Interface Statistics**.
2. Wählen Sie **Port** im Feld **Interface** aus.
3. Klicken Sie auf **Reset All Counters**. Die Schnittstellenstatistiken für den Anschluss werden angezeigt.

Anzeigen von Schnittstellenstatistiken für eine LAG:

1. Öffnen Sie die Seite **Interface Statistics**.
2. Wählen Sie **LAG** im Feld **Interface** aus.
3. Klicken Sie auf **Reset All Counters**. Die Schnittstellenstatistiken für die LAG werden angezeigt.

Anzeigen von Schnittstellenstatistiken mit Hilfe der CLI-Befehle

Dieser Abschnitt enthält die CLI-Befehle für die Anzeige von Schnittstellenstatistiken.

CLI-Befehl	Beschreibung
show interfaces counters [ethernet Schnittstelle | Anschlusskanalnummer]	Zeigt den über eine physische Schnittstelle abgewickelten Datenverkehr an.

Im Folgenden ein Beispiel für die CLI-Befehle:

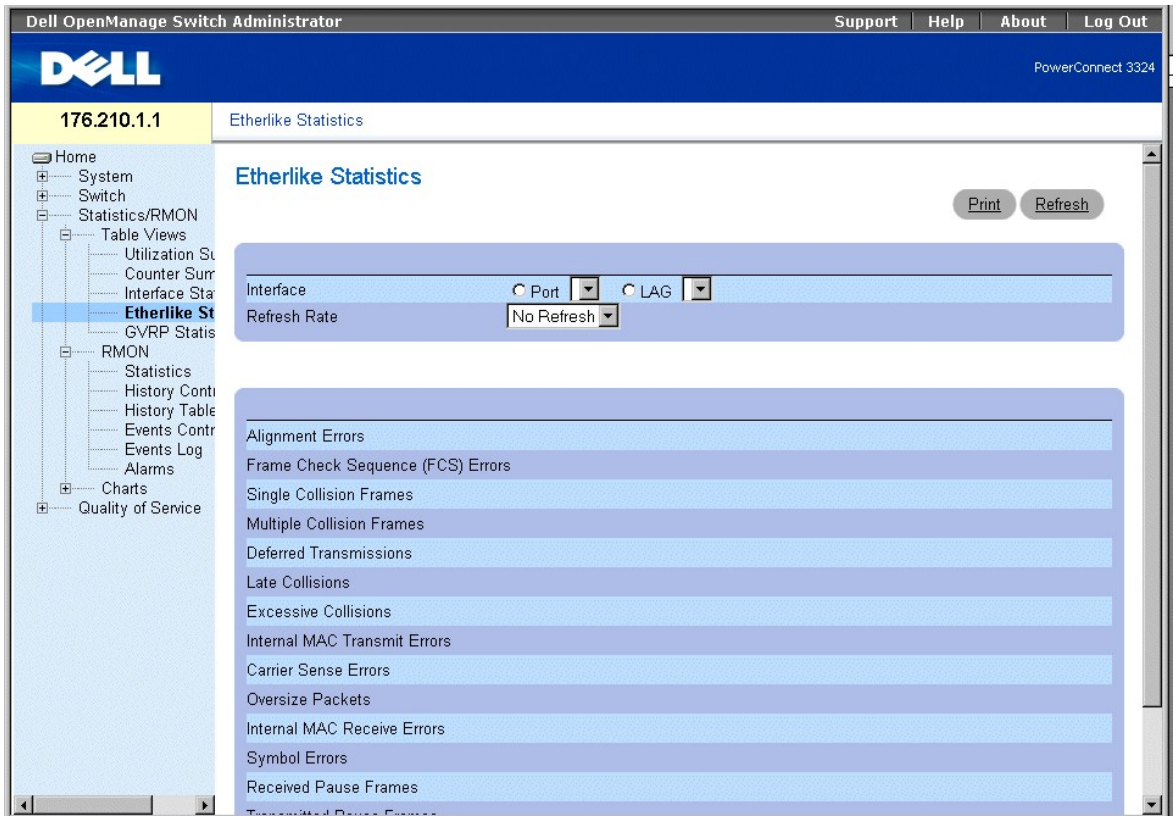
```
console# show interfaces counters ethernet 1/e1

Port InOctets InUcastPkts InMcastPkts InBcastPkts

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

1/e1 1717 0 326 26



Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts

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

1/e1 21845 0 326 26



Alignment Errors: 0

FCS Errors: 0

Single Collision Frames: 0
```

```
Multiple Collision Frames: 0

Deferred Transmissions: 0

Late Collisions: 0

Excessive Collisions: 0

Internal MAC Tx Errors: 0

Carrier Sense Errors: 0

Oversize Packets: 0

Internal MAC Rx Errors: 0

Symbol Errors: 0

Received Pause Frames: 0

Transmitted Pause Frames: 0
```

Anzeigen der Seite "Etherlike Statistics"

Die Seite **Etherlike Statistics** enthält Schnittstellenstatistiken. So öffnen Sie die Seite **Etherlike Statistics**:

- Klicken Sie in der Strukturansicht auf **Statistics/RMON** > **Table Views** > **Etherlike Statistics**. Die Seite **Etherlike Statistics** wird geöffnet.



Seite "Etherlike Statistics"

Die Seite **Etherlike Statistics** enthält folgende Felder:

- **Interface**- Gibt den Typ der Schnittstelle an, für welche die Statistik angezeigt wird.
  - **Port**- Gibt den Anschluss an, für den die Statistik angezeigt wird.
  - **LAG**- Gibt die LAG an, für welche die Statistik angezeigt wird.
- **Refresh Rate**- Gibt den Zeitraum bis zur Aktualisierung der Schnittstellenstatistiken an. Folgende Feldwerte können ausgewählt werden:
  - **15 Sec**- Gibt an, dass die Etherlike-Statistiken alle 15 Sekunden aktualisiert werden.
  - **30 Sec**- Gibt an, dass die Etherlike-Statistiken alle 30 Sekunden aktualisiert werden.
  - **60 Sec**- Gibt an, dass die Etherlike-Statistiken alle 60 Sekunden aktualisiert werden.
  - **No Refresh**- Gibt an, dass die Etherlike-Statistiken nicht automatisch aktualisiert werden.
- **Alignment Errors**- Zeigt die Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen Ausrichtungsfehler an.
- **Frame Check Sequence (FCS) Errors**- Zeigt die Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen Frameprüfsequenz-Fehler an.
- **Single Collision Frames**- Zeigt die Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen "Single Collisions Frames"-Fehler an.
- **Multiple Collision Frames**- Zeigt die Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen "Multiple Collisions Frames"-Fehler an.
- **Deferred Transmissions**- Zeigt die Anzahl der verzögerten Übertragungen über die ausgewählte Schnittstelle an.
- **Late Collision**- Zeigt die Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen verspäteten Kollisionen an.
- **Excessive Collisions**- Zeigt die Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen übermäßigen Kollisionen an.
- **Internal MAC Transmit Errors**- Zeigt die Anzahl interner MAC-Übertragungsfehler an der ausgewählten Schnittstelle an.
- **Carrier Sense Errors**- Zeigt die Anzahl der bei der Leitungsüberwachung an der ausgewählten Schnittstelle aufgetretenen Fehler an.
- **Oversize Packets**- Zeigt die Anzahl der durch überlange Pakete verursachten Frame-Fehler an der ausgewählten Schnittstelle an.
- **Internal MAC Receive Errors**- Zeigt die Anzahl interner MAC-Empfangsfehler an der ausgewählten Schnittstelle an.
- **Symbol Errors**- Zeigt die Anzahl der Symbolfehler an der ausgewählten Schnittstelle an.
- **Receive Pause Frames**- Zeigt die Anzahl der über die ausgewählte Schnittstelle (IEEE 802.3X) empfangenen Pause-Frames an.
- **Transmitted Pause Frames**- Zeigt die Anzahl der über die ausgewählte Schnittstelle (IEEE 802.3X) gesendeten Pause-Frames an.

Anzeigen von Etherlike-Statistiken für einen Anschluss:

1. Öffnen Sie die Seite **Etherlike Statistics**.
2. Wählen Sie **Port** im Feld **Interface** aus.
3. Klicken Sie auf **Query**. Die Etherlike-Statistiken für den Anschluss werden angezeigt.

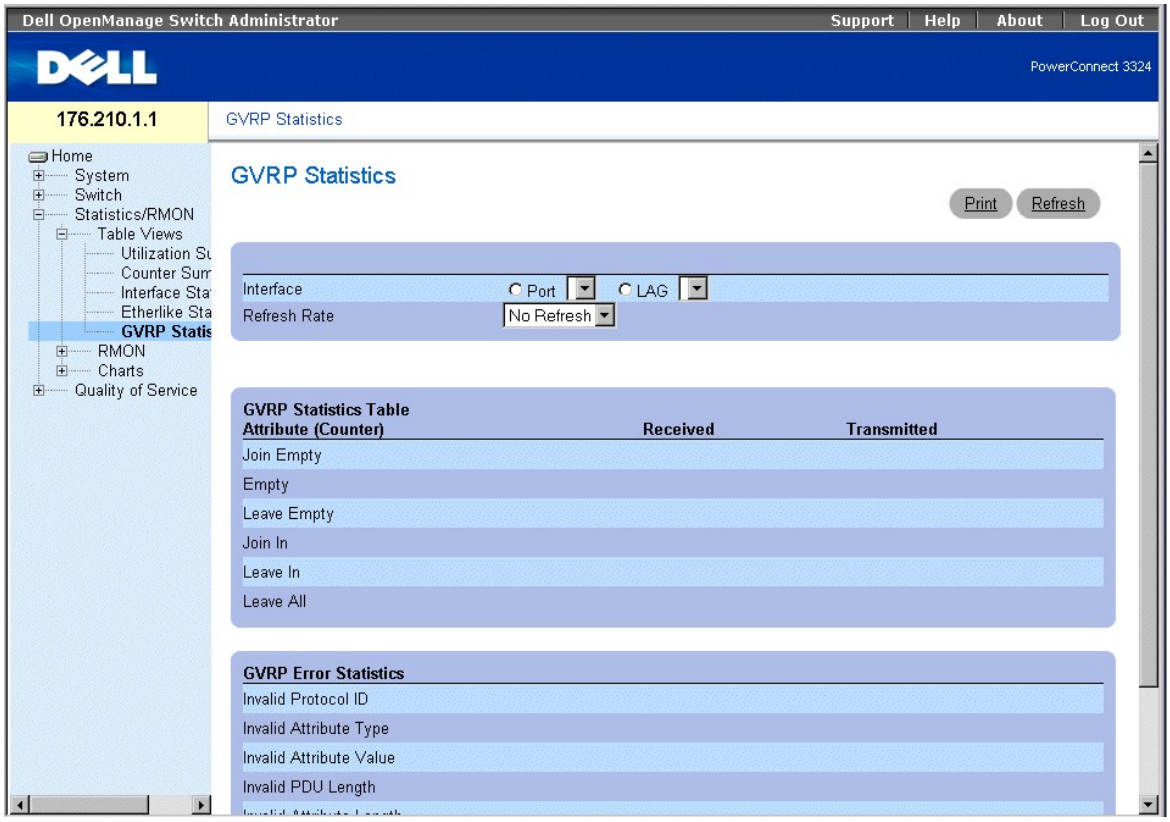
Anzeigen von Etherlike-Statistiken für eine LAG:

1. Öffnen Sie die Seite **Etherlike Statistics**.
2. Wählen Sie **LAG** im Feld **Interface** aus.
3. Klicken Sie auf **Query**. Die Etherlike-Statistiken für die LAG werden angezeigt.

Anzeigen der Seite "GVRP Statistics"

Die Seite **GVRP Statistics** enthält Gerätestatistiken für GVRP. So öffnen Sie die Seite **GVRP Statistics**:

- Klicken Sie in der Strukturansicht auf **Statistics/RMON** > **Table Views** > **GVRP Statistics**. Die Seite **GVRP Statistics** wird geöffnet:



Seite "GVRP Statistics"

Die Seite **GVRP Statistics** enthält folgende Felder:

- **Interface**- Gibt den Typ der Schnittstelle an, für welche die Statistik angezeigt wird.
  - **Port**- Gibt den Anschluss an, für den die Statistik angezeigt wird.
  - **LAG**- Gibt die LAG an, für welche die Statistik angezeigt wird.
- **Refresh Rate**- Gibt den Zeitraum bis zur Aktualisierung der GVRP-Statistiken an. Folgende Feldwerte können ausgewählt werden:

- **15 Sec**- Gibt an, dass die GVRP-Statistiken alle 15 Sekunden aktualisiert werden.
- **30 Sec**- Gibt an, dass die GVRP-Statistiken alle 30 Sekunden aktualisiert werden.
- **60 Sec**- Gibt an, dass die GVRP-Statistiken alle 60 Sekunden aktualisiert werden.
- **No Refresh**- Gibt an, dass die GVRP-Statistiken nicht automatisch aktualisiert werden.

- **Join Empty**- Zeigt die "GVRP Join Empty"-Statistik für das Gerät an.
- **Empty**- Zeigt die "GVRP Empty"-Statistik für das Gerät an.
- **Leave Empty**- Zeigt die "GVRP Leave"-Statistik für das Gerät an.
- **Join In**- Zeigt die "GVRP Join In"-Statistik für das Gerät an.
- **Leave In**- Zeigt die "GVRP Leave In"-Statistik für das Gerät an.
- **Invalid Protocol ID**- Zeigt die GVRP-Gerätestatistik zu ungültigen Protokoll-IDs an.
- **Invalid Attribute Type**- Zeigt die GVRP-Gerätestatistik zu ungültigen Attribut-IDs an.
- **Invalid Attribute Value**- Zeigt die GVRP-Gerätestatistik zu ungültigen Attributwerten an.
- **Invalid PDU Length**- Zeigt die GVRP-Gerätestatistik zu ungültigen PDU-Längen an.
- **Invalid Attribute Length**- Zeigt die GVRP-Gerätestatistik zu ungültigen Attributlängen an.
- **Invalid Events**- Zeigt die GVRP-Gerätestatistik zu ungültigen Ereignissen an.

Anzeigen von GVRP-Statistiken für einen Anschluss:

1. Öffnen Sie die Seite **GVRP Statistics**.
2. Wählen Sie **Port** im Feld **Interface** aus.
3. Klicken Sie auf **Query**. Die GVRP-Statistiken für den Anschluss werden angezeigt.

Anzeigen von GVRP-Statistiken für eine LAG:

1. Öffnen Sie die Seite **GVRP Statistics**.
2. Wählen Sie **LAG** im Feld **Interface** aus.
3. Klicken Sie auf **Query**. Die GVRP-Statistiken für die LAG werden angezeigt.

Anzeigen von GVRP-Statistiken mit Hilfe der CLI-Befehle

Informationen zur Anzeige der GVRP-Anweisungen pro Anschluss finden Sie auf der Seite **Port Statistics**. In der folgenden Tabelle werden die CLI-Befehle beschrieben.

CLI-Befehl	Beschreibung
show gvrp statistics [**ethernet** *Schnittstelle* | **port-channel** *Anschlusskanalnummer*]	Zeigt GVRP-Statistiken an.
show gvrp error-statistics [**ethernet** *Schnittstelle*| **port-channel** *Anschlusskanalnummer*]	Zeigt GVRP-Fehlerstatistiken an.

Im Folgenden ein Beispiel für die CLI-Befehle:

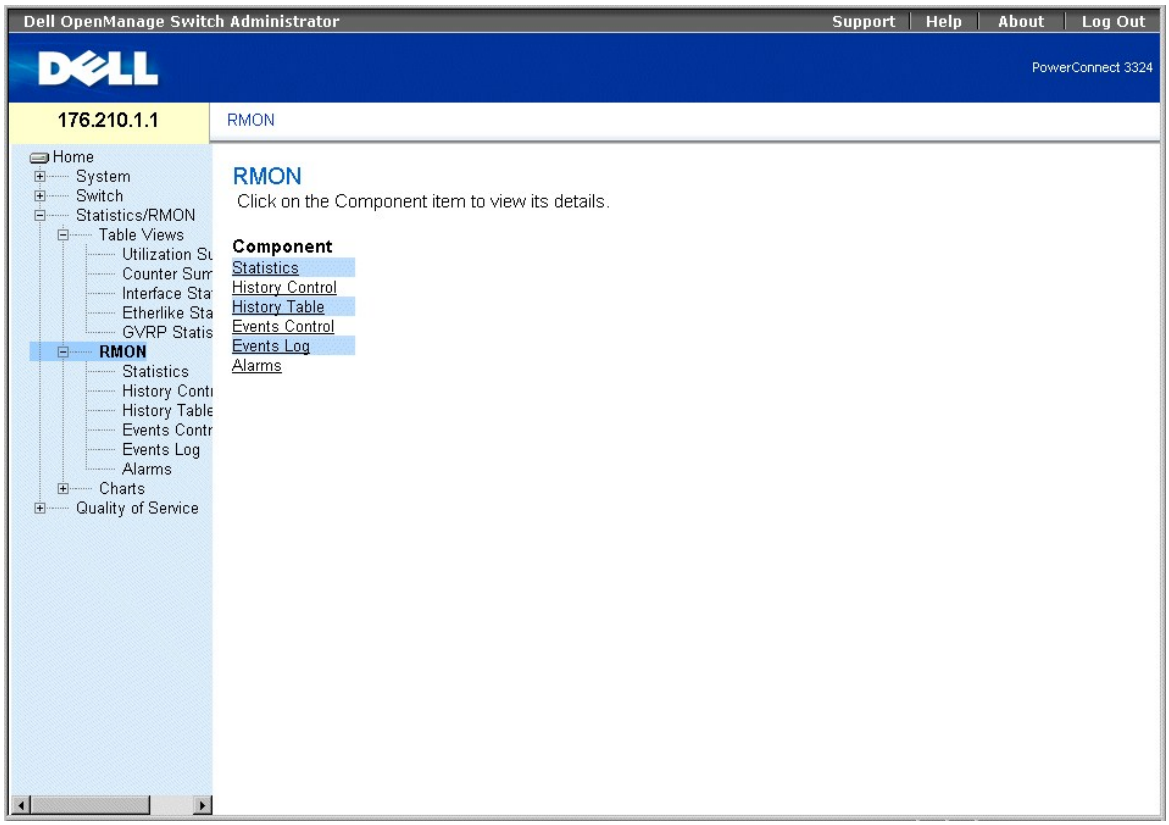
```
Console# show gvrp statistics


GVRP statistics:

---------------
```

```
Legend:

rJE: Join Empty Received . : 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

---- --- ---- ---- ---- --- --- --- --- --- ---- 1/e1 0 0 0 0 0 0 0 0 0 0 0 0

1/e2 0 0 0 0 0 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0 0 0 0 0 0

1/e4 0 0 0 0 0 0 0 0 0 0 0 0

1/e5 0 0 0 0 0 0 0 0 0 0 0 0

1/e6 0 0 0 0 0 0 0 0 0 0 0 0

1/e7 0 0 0 0 0 0 0 0 0 0 0 0

1/e8 0 0 0 0 0 0 0 0 0 0 0 0
```

Anzeigen von RMON-Informationen

Mit Hilfe von RMON (Remote Monitoring) können Netzwerkverwalter von einem Remote-Standort aus Informationen zum Netzwerkverkehr anzeigen lassen. So öffnen Sie die Seite **RMON**:

- Klicken Sie in der Strukturansicht auf **Statistics / RMON** > **RMON**. Die Seite **RMON** wird geöffnet.



Seite "RMON"

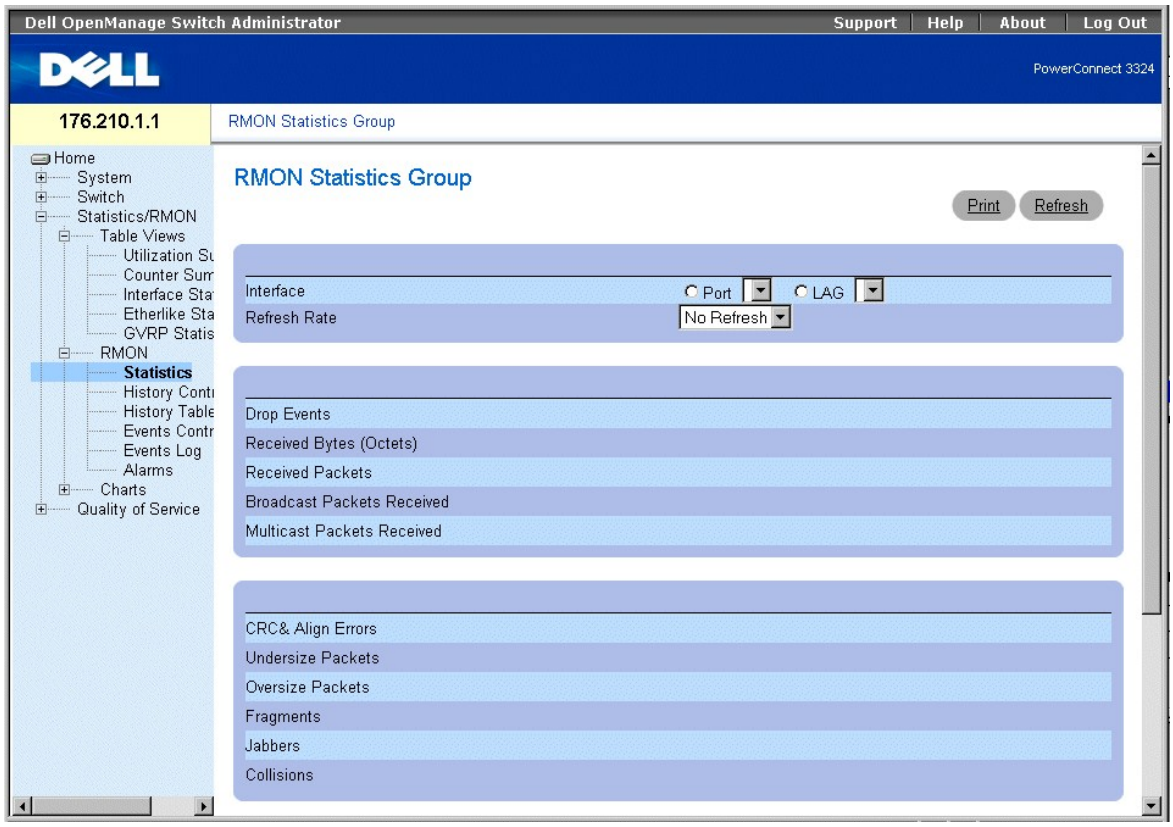
Dieser Abschnitt umfasst die folgenden Themen:

- Anzeigen von RMON-Statistiken
- Anzeigen von Verlaufssteuerungsstatistiken
- Anzeigen der "RMON History Table"
- Definieren von Geräteereignissen
- Anzeigen des Ereignisprotokolls
- Definieren von Gerätealarmen

Anzeigen von RMON-Statistiken

Auf der Seite **RMON Statistics Group** können Netzwerkverwalter RMON-Statistiken für eine Schnittstelle anzeigen. Schnittstellenstatistiken bieten Informationen zur Gerätenutzung sowie zu Gerätefehlern. So öffnen Sie die Seite **RMON Statistics Group**:

- Klicken Sie in der Strukturansicht auf **Statistics/RMON** > **RMON**> **Statistics**. Die Seite **RMON Statistics Group** wird geöffnet.



Seite "RMON Statistics Group"

Die Seite **RMON Statistics Group** enthält folgende Informationen:

- **Interface**- Gibt Typ und Nummer der Schnittstelle an, für welche die Statistik angezeigt wird. Folgende Feldwerte können ausgewählt werden:
  - **Port**- Gibt den Anschluss an, für den die jeweilige Statistik angezeigt wird.
  - **LAG**- Gibt die LAG an, für welche die jeweilige Statistik angezeigt wird.
- **Refresh Rate**- Gibt den Zeitraum bis zur Aktualisierung der RMON-Statistiken an. Folgende Feldwerte können ausgewählt werden:
  - **15 Sec**- Gibt an, dass die RMON-Statistiken alle 15 Sekunden aktualisiert werden.
  - **30 Sec**- Gibt an, dass die RMON-Statistiken alle 30 Sekunden aktualisiert werden.
  - **60 Sec**- Gibt an, dass die RMON-Statistiken alle 60 Sekunden aktualisiert werden.
  - **No Refresh**- Gibt an, dass die RMON-Statistiken nicht automatisch aktualisiert werden.
- **Drop Events**- Gibt die Anzahl der Ereignisse an, die seit dem letzten Zurücksetzen der Zähler an der Schnittstelle abgewiesen wurden.
- **Received Octets**- Gibt die Anzahl der Oktette an, die seit dem letzten Zurücksetzen der Zähler über die Schnittstelle empfangen wurden.
- **Received Packets**- Gibt die Anzahl der Pakete an, die seit dem letzten Zurücksetzen der Zähler über die Schnittstelle empfangen wurden.
- **Broadcast Packets Received**- Gibt die Anzahl der Broadcast-Pakete an, die seit dem letzten Zurücksetzen der Zähler über die Schnittstelle empfangen wurden.
- **Multicast Packets Received**- Gibt die Anzahl der Multicast-Pakete an, die seit dem letzten Zurücksetzen der Zähler über die Schnittstelle empfangen wurden.
- **CRC& Align Errors**- Gibt die Anzahl der CRC- und Ausrichtungsfehler an, die seit dem letzten Zurücksetzen der Zähler an der Schnittstelle aufgetreten sind.
- **Undersize Packets**- Gibt die Anzahl der Pakete unter Normalgröße an, die seit dem letzten Zurücksetzen der Zähler über die Schnittstelle empfangen wurden.
- **Oversize Packets**- Gibt die Anzahl der Pakete über Normalgröße an, die seit dem letzten Zurücksetzen der Zähler über die Schnittstelle empfangen wurden.
- **Fragments**- Gibt die Anzahl der Fragmente an, die seit dem letzten Zurücksetzen der Zähler über die Schnittstelle empfangen wurden.
- **Jabbers**- Gibt die Anzahl der Jabbers (Hintergrundgeräusche) an, die seit dem letzten Zurücksetzen der Zähler über die Schnittstelle empfangen wurden.
- **Collisions**- Gibt die Anzahl der Kollisionen an, die seit dem letzten Zurücksetzen der Zähler über die Schnittstelle empfangen wurden.

- **Frames of 64 Bytes**- Gibt die Anzahl der 64-Byte-Pakete an, die seit dem letzten Zurücksetzen der Zähler über die Schnittstelle empfangen wurden.
- **Frames of 65-127 Bytes**- Gibt die Anzahl der 65- bis 127-Byte-Pakete an, die seit dem letzten Zurücksetzen der Zähler über die Schnittstelle empfangen wurden.
- **Frames of 128-255 Bytes**- Gibt die Anzahl der 128- bis 255-Byte-Pakete an, die seit dem letzten Zurücksetzen der Zähler über die Schnittstelle empfangen wurden.
- **Frames of 256-511 Bytes**- Gibt die Anzahl der 256- bis 511-Byte-Pakete an, die seit dem letzten Zurücksetzen der Zähler über die Schnittstelle empfangen wurden.
- **Frames of 512-1023 Bytes**- Gibt die Anzahl der 512- bis 1023-Byte-Pakete an, die seit dem letzten Zurücksetzen der Zähler über die Schnittstelle empfangen wurden.
- **Frames of 1024-1518 Bytes**- Gibt die Anzahl der 1024- bis 1518-Byte-Pakete an, die seit dem letzten Zurücksetzen der Zähler über die Schnittstelle empfangen wurden.

Anzeigen von Schnittstellenstatistiken:

1. Öffnen Sie die Seite **RMON Statistics Group**.
2. Wählen Sie einen Schnittstellentyp sowie eine Schnittstellennummer im Feld **Interface** aus. Die Schnittstellenstatistiken werden im Abschnitt **RMON Statistics** angezeigt.

Anzeigen von RMON-Statistiken mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
show rmon statistics [**ethernet** *Schnittstelle* | **port-channel** *Anschlusskanalnummer*]	Zeigt RMON-Ethernet-Statistiken an.

Im Folgenden ein Beispiel für den CLI-Befehl:

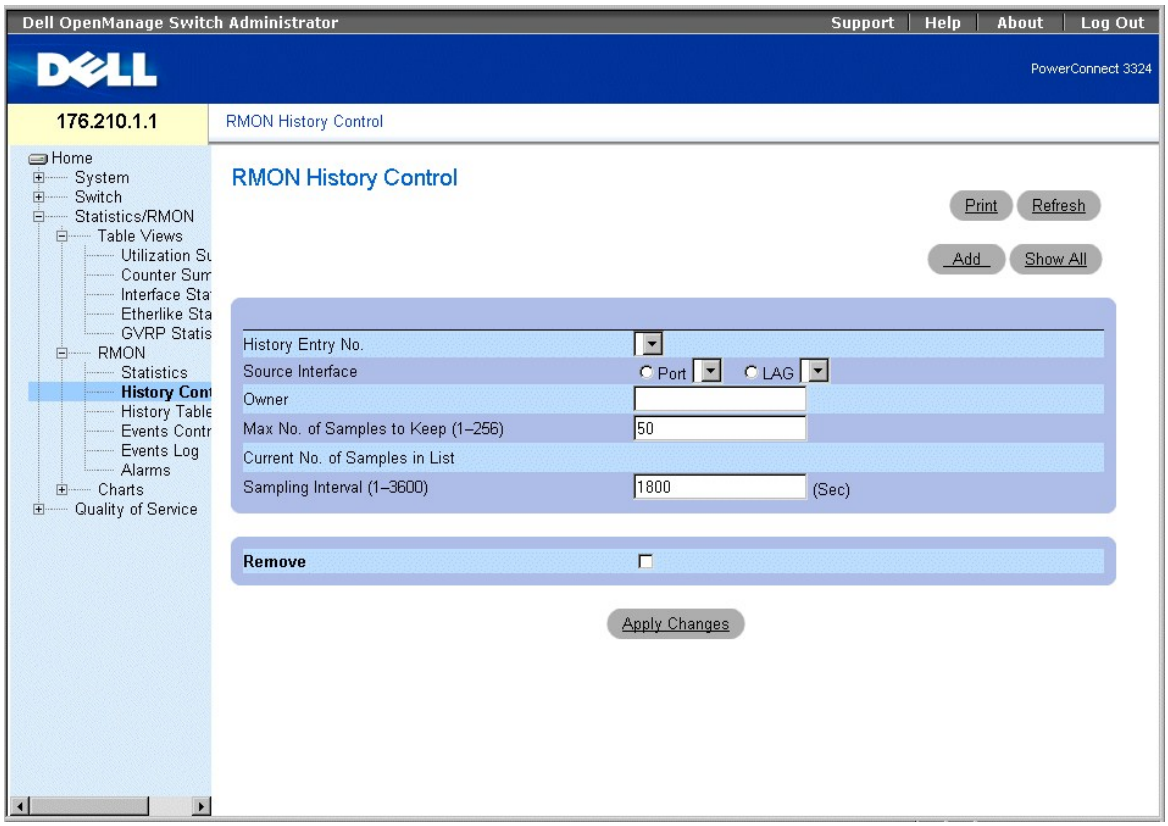
```
Console# show rmon statistics ethernet 1/e1

Port 1/e1

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: 256 to 511 Octets: 0
```

512 to 1023 Octets: 491 1024 to 1518 Octets: 389

Anzeigen von Verlaufssteuerungsstatistiken

Die Seite **RMON History Control** enthält Informationen zu RMON-Stichprobendaten, die an den Anschlüssen erfasst wurden. Die Erfassung dieser Stichproben wird über die Seite **RMON History Control** gesteuert.

- Klicken Sie in der Strukturansicht auf **Statistics/RMON** > **History Control**. Die Seite **RMON History Control** wird geöffnet.



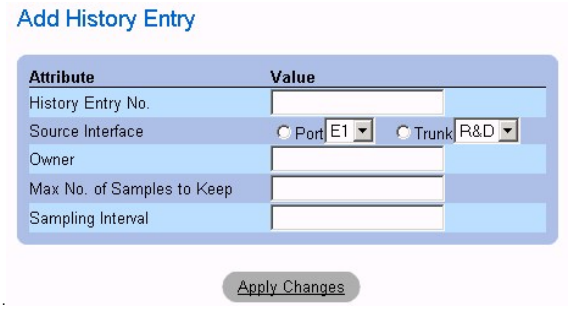
Seite "RMON History Control"

Die Seite **RMON History Control** enthält folgende Informationen:

- **History Entry No.**- Gibt den Eintrag in der **History Control Table** an.
- **Source Interface**- Gibt die Quelle an, von der die Verlaufsstichproben erfasst wurden. Folgende Feldwerte können ausgewählt werden:
  - **Port**- Gibt an, dass die Verlaufsstichproben von einem Anschluss erfasst wurden.
  - **LAG**- Gibt an, dass die Verlaufsstichproben von einer LAG erfasst wurden.
- **Owner**- Gibt die RMON-Station bzw. den Benutzer an, die oder der die RMON-Informationen angefordert hat.
- **Max Number of Samples to Keep**- Gibt die Anzahl der zu speichernden Stichproben an. Der Standardwert ist **50**.
- **Current Number of Samples**- Gibt die Anzahl der derzeit erfassten Stichproben an.
- **Sampling Interval**- Gibt die Zeit (in Sekunden) an, in der Stichproben von den Anschlüssen erfasst werden. Die möglichen Werte liegen zwischen 1 und 3.600 Sekunden. Der Standardwert lautet **1800** Sekunden (30 Minuten).
- **Remove**- Entfernt den Eintrag aus der **History Control Table**.
  - **Aktiviert**- Entfernt den Eintrag aus der **History Control Table**.
  - **Deaktiviert**- Behält den Eintrag in der **History Control Table** bei.

Hinzufügen eines Verlaufssteuerungseintrags:

1. Öffnen Sie die Seite **RMON History Control.**
2. Klicken Sie auf **Add**. Die Seite **Add History Entry** wird geöffnet.



Seite "Add History Entry"

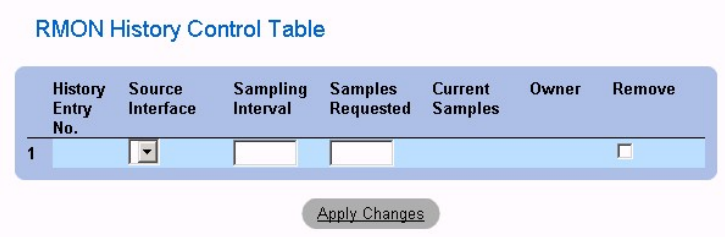
3. Definieren Sie die Felder **History Entry No., Source Interface, Owner, Max No. of Samples to Keep**, und **Sampling Interval**.
4. Klicken Sie auf **Apply Changes**. Der **History Control Entry** wird hinzugefügt.

Ändern eines Eintrags in der History Control Table:

1. Öffnen Sie die Seite **RMON History Control.**
2. Wählen Sie unter **RMON History Control Table** einen Eintrag im Feld **History Index**.
3. Ändern Sie die Felder **Source Interface, Owner, Max Number of Samples to Keep, Number of Current Samples** und/oder **Sampling Interval**.
4. Klicken Sie auf **Apply Changes**. Der Eintrag in der **RMON History Control Table** wird geändert und das Gerät aktualisiert.

Anzeigen der Verlaufssteuerungstabelle:

1. Öffnen Sie die Seite **RMON History Control.**
2. Klicken Sie auf **Show All**. Die **History Control Table** wird geöffnet.



Verlaufssteuerungstabelle

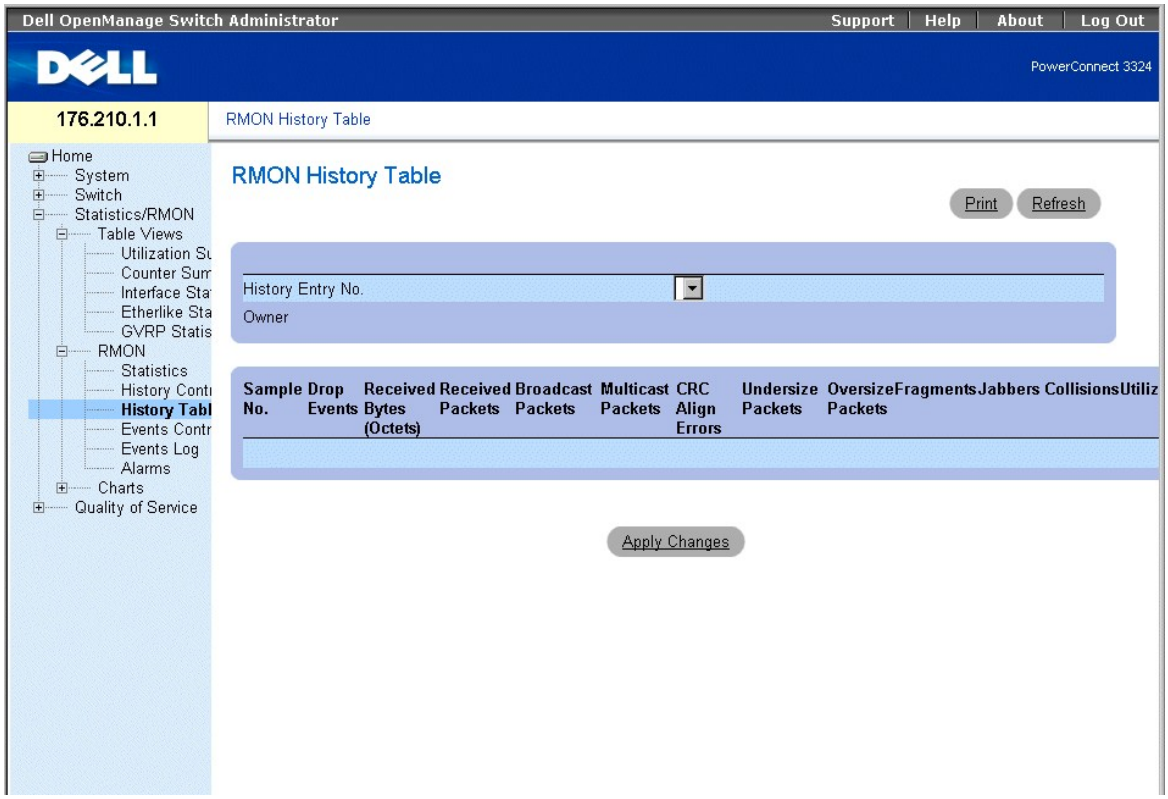
Löschen eines Eintrags aus der History Control Table:

1. Öffnen Sie die Seite **RMON History Control**.
2. Wählen Sie unter **History Control Table** einen Eintrag im Feld **History Index**.
3. Aktivieren Sie das Kontrollkästchen **Remove**.
4. Klicken Sie auf **Apply Changes**. Der Eintrag wird aus der **RMON History Control Table** gelöscht und das Gerät aktualisiert.

Anzeigen der "RMON History Table"

Die **RMON History Table** enthält schnittstellenspezifische, statistische RMON-Netzwerkstichproben. Jeder Tabelleneintrag repräsentiert alle während einer einzelnen Stichprobe erfassten Zählerwerte. So öffnen Sie die **RMON History Table**:

- Klicken Sie in der Strukturansicht auf **Statistics / RMON** > **RMON History** > **History Table**.



RMON History Table

ANMERKUNG: In der RMON History Table werden nicht alle Felder angezeigt.

Die **RMON History Table** enthält folgende Felder:

- **Sample No.**- Gibt die jeweilige Stichprobe an, welche durch die Informationen in der Tabelle dargestellt wird.
- **Drop Events**- Gibt die Anzahl von Paketen an, die aufgrund unzureichender Netzwerkressourcen während des Stichprobenintervalls abgewiesen wurden. Dieser Wert bezieht sich nicht unbedingt auf die genaue Anzahl abgewiesener Pakete, sondern auf die Häufigkeit, mit der abgewiesene Pakete identifiziert wurden.
- **Received Bytes (Octets)**- Gibt die Anzahl der über das Netzwerk empfangenen Daten-Oktette an, einschließlich ungültiger Pakete.
- **Received Packets**- Gibt die Anzahl der während des Stichprobenintervalls empfangenen Pakete an.
- **Broadcast Packets**- Gibt die Anzahl der während des Stichprobenintervalls empfangenen gültigen Broadcast-Pakete an.
- **Multicast Packets**- Gibt die Anzahl der während des Stichprobenintervalls empfangenen gültigen Multicast-Pakete an.
- **CRC Align Errors**- Gibt die Anzahl der während der Stichprobensitzung empfangenen Pakete mit einer Länge zwischen 64 und 1518 Oktetten an, die einen Frameprüfsequenz-Fehler verursacht haben und über eine ganzzahlige Oktettanzahl oder über eine nicht ganzzahlige Oktettanzahl verfügen.
- **Undersized Packets**- Gibt die Anzahl der während der Stichprobensitzung empfangenen Pakete mit einer Länge unter 64 Oktetten an.
- **Oversized Packets**- Gibt die Anzahl der während der Stichprobensitzung empfangenen Pakete mit einer Länge von über 1518 Oktetten an.
- **Fragments**- Gibt die Anzahl der empfangenen Pakete mit einer Länge unter 64 Oktetten an, für die während der Stichprobensitzung eine Frameprüfsequenz generiert wurde.
- **Jabbers**- Gibt die Anzahl der empfangenen Pakete mit einer Länge über 1518 Oktetten an, für die während der Stichprobensitzung eine Frameprüfsequenz generiert wurde.
- **Collisions**- Enthält einen Schätzwert zur Gesamtzahl der während der Stichprobensitzung aufgetretenen Paketkollisionen. Kollisionen treten auf, wenn von einem Zwischenverstärkeranschluss festgestellt wird, dass mindestens zwei Stationen gleichzeitig Daten übertragen.
- **Utilization**- Enthält einen Schätzwert zur Beschreibung physikalischer Netzwerkschichten für eine Schnittstelle während der Stichprobensitzung. Der Wert wird prozentual mit zwei Nachkommastellen angegeben.

Anzeigen von Statistiken für einen bestimmten Verlaufseintrag:

1. Öffnen Sie die Seite **RMON History Table**.
2. Wählen Sie einen Verlaufseintrag im Feld **History Table No.**. Die Eintragsstatistik wird in der **RMON History Table** angezeigt.

Anzeigen von RMON-Verlaufsstatistiken mit Hilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für die Anzeige von RMON-Verlaufsstatistiken.

CLI-Befehl	Beschreibung
rmon table-size history *Einträge*	Konfiguriert die maximale Anzahl von Verlaufstabelleneinträgen.
rmon collection history *index* [owner *Besitzername*] [**buckets** *Bucket-Nummer*] [**interva**l *Sekunden*]	Aktiviert eine RMON-(Remote Monitoring-)MIB-Verlaufsstatistikgruppe für eine Schnittstelle.
show rmon history *Index* {**throughput** | **errors** | **other**} [**period** *hh:mm:ss*]	Zeigt RMON-Ethernet-Verlaufsstatistiken an.

Im Folgenden ein Beispiel für die CLI-Befehle:

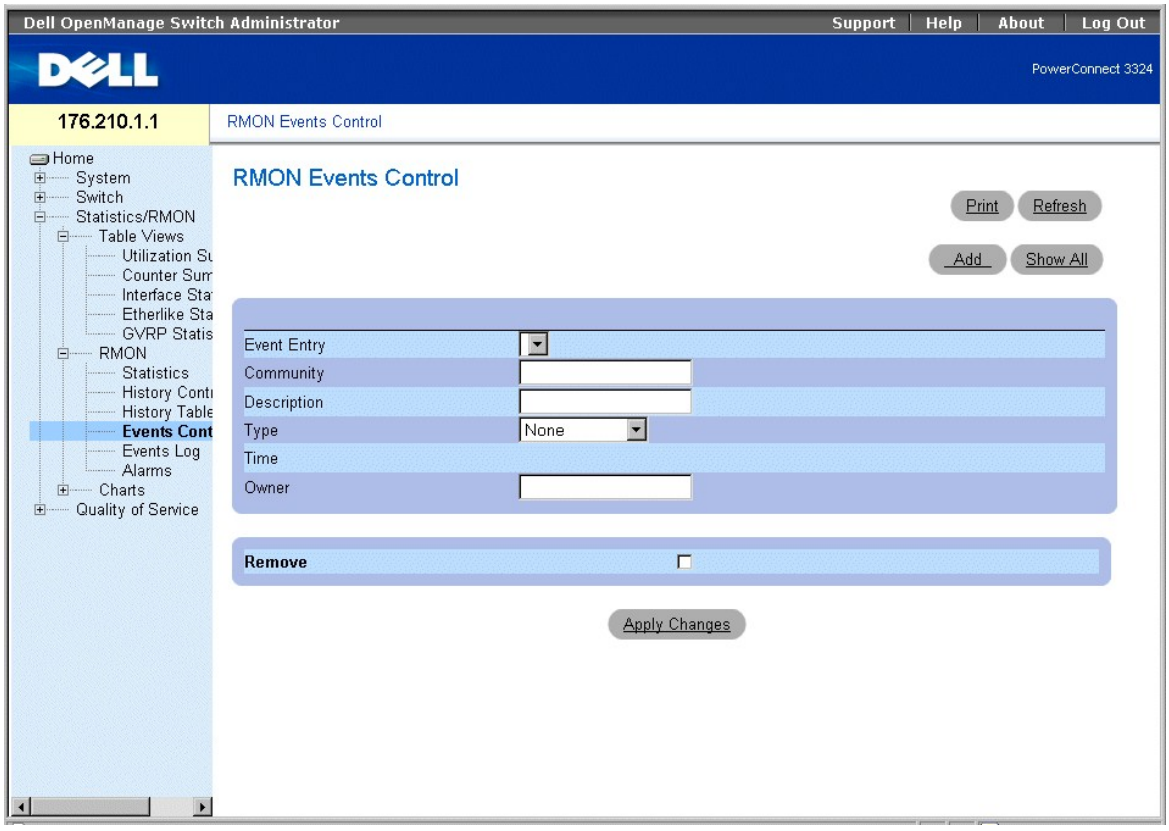
```
Console (config)# rmon table-size history 1000

Console (config)# interface ethernet 1/e8

Console (config-if)# rmon collection history 1 interval 2400

Console# show rmon history 1 throughput

Sample set: 1 Owner: CLI

Interface: 1/e1 Interval: 1800

Requested samples: 50 Granted samples: 50



Maximum table size: 500



Day: Jan 18 2002

Time Octets Packets Broadcast Multicast Utilization

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

23:58:30 878128 878 7 1 20.87%

23:59:00 75898768 91892 932 1723 19.27%
```

```
23:59:30 171797536 193784 1817 3289 19.82%


Day: Jan 19 2002

Time Octets Packets Broadcast Multicast Utilization

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

00:00:00 287696304 275686 2789 5878 20.17%

00:00:30 303595962 357568 3289 7287 19.98%
```

Definieren von Geräteereignissen

Auf der Seite **RMON Events Control** können Netzwerkverwalter RMON-Ereignisse anzeigen lassen. Die Tabelle **RMON Events** kann über die Tabelle **RMON Events Control** geöffnet werden. So öffnen Sie die Seite **RMON Events Control**:

- Klicken Sie in der Strukturansicht auf **Statistics / RMON** > **RMON** > **Events**. Die Seite **RMON Events Control** wird geöffnet.



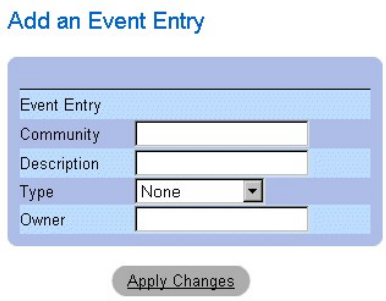
Seite "RMON Events Control"

Die Seite **RMON Events Control** enthält folgende Felder:

- **Event Entry**- Gibt das Ereignis an.
- **Community**- Gibt die SNMP-Community an, der das Ereignis angehört.
- **Description**- Enthält eine benutzerdefinierte Ereignisbeschreibung.
- **Type**- Beschreibt den Ereignistyp. Folgende Feldwerte können ausgewählt werden:
  - **Log**- Gibt an, dass der Ereignistyp ein Protokolleintrag ist.
  - **Trap**- Gibt an, dass der Ereignistyp ein Trap ist.
  - **Log** und **Trap**- Gibt an, dass der Ereignistyp sowohl ein Protokolleintrag als auch ein Trap ist.
- **Time**- Gibt die Uhrzeit an, zu der das Ereignis aufgetreten ist.
- **Owner**- Gibt das Gerät bzw. den Benutzer an, von dem das Ereignis definiert wurde.
- **Remove**- Entfernt das Ereignis aus der **Events Table**.
  - **Aktiviert**- Entfernt das Ereignis aus der **Events Table**.
  - **Deaktiviert**- Behält das Ereignis in der **Events Table** bei.

Hinzufügen eines RMON-Ereignisses:

1. Öffnen Sie die Seite **RMON Events Control**.
2. Klicken Sie auf **Add**. Die Seite **Add New RMON Event** wird geöffnet.



Hinzufügen eines neuen RMON-Ereignisses

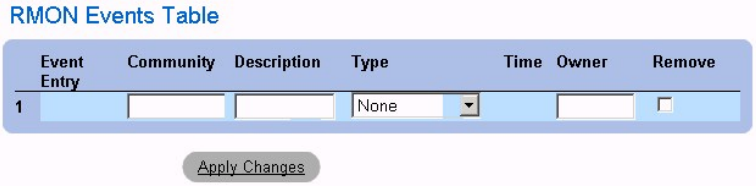
3. Definieren Sie die Felder **New Event Index, Community, Description, Type** und **Owner**.
4. Klicken Sie auf **Apply Changes**. Der Eintrag wird der **Event Table** hinzugefügt und das Gerät aktualisiert.

Ändern eines RMON-Ereignisses:

1. Öffnen Sie die Seite **RMON Events Control**.
2. Wählen Sie aus dem **Event Table** einen Eintrag im Feld **Event Entry** aus.
3. Ändern Sie die Felder **Community, Description, Type** und/oder **Owner**.
4. Klicken Sie auf **Apply Changes**. Der Eintrag in der **Event Table** wird geändert und das Gerät aktualisiert.

Anzeigen der RMON Event Table:

1. Öffnen Sie die Seite **RMON Events Control**.
2. Klicken Sie auf **Show All**. Die **Event Table** wird geöffnet.



RMON Events Table

Löschen mehrerer RMON-Ereigniseinträge:

1. Öffnen Sie die Seite **RMON Events Control**.
2. Wählen Sie im Feld **Event Index** einen Eintrag der **Event Table** aus.
3. Aktivieren Sie das Kontrollkästchen **Remove**.
4. Klicken Sie auf **Apply Changes**. Der Eintrag in der **Event Table** wird gelöscht und das Gerät aktualisiert.

ANMERKUNG: Ein einzelner **Ereignis**eintrag kann mit Hilfe des Kontrollkästchens **Remove** von der Seite **RMON Events** entfernt werden.

Definieren und Anzeigen der RMON-Ereignissteuerung mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Konfiguration und Anzeige der Felder auf der Seite **RMON Events Control** zusammengefasst.

CLI-Befehl	Beschreibung
rmon event *Indextyp* [**community** *Text*] [**description** *Text*] [*Besitzername*]	Konfiguriert ein RMON-Ereignis.
show rmon events	Zeigt die RMON-Ereignistabelle an.

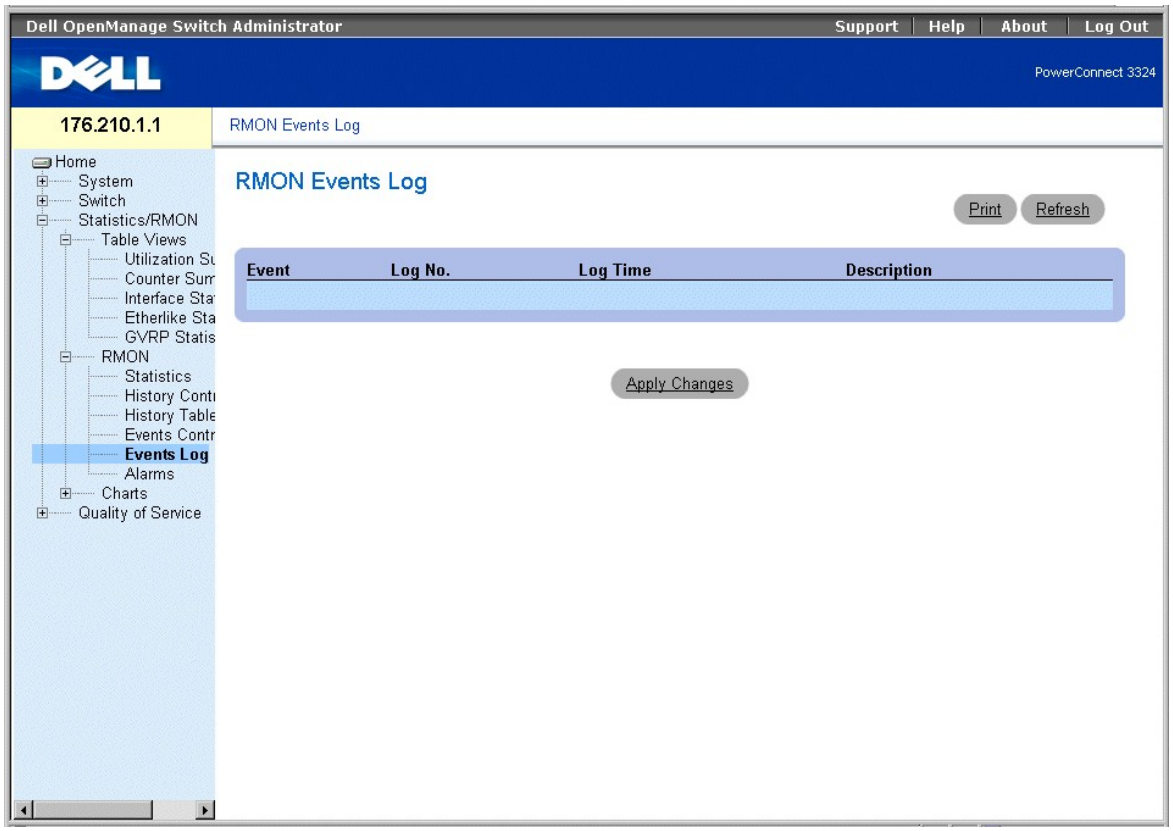
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# rmon event 10 log

Config (config)# exit

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 device Manager Jan 18 2002 23:59:48
```

Anzeigen des Ereignisprotokolls

Die Seite **RMON Events Log** enthält eine Liste der RMON-Ereignisse. So öffnen Sie das **RMON Events Log**:

- Klicken Sie in der Strukturansicht auf **Statistics / RMON** >RMON **Events**. Die Seite **RMON Events Log** wird geöffnet.



Seite "RMON Events Log"

Die Seite **RMON Events Log** enthält folgende Felder:

- **Event**- Gibt die Nummer des Eintrags im **RMON Event Log** an.
- **Log No.**- Gibt die Protokollnummer an.
- **Log Time**- Gibt die Uhrzeit an, zu welcher der Protokolleintrag erfasst wurde.
- **Description**- Beschreibt den Protokolleintrag.

Anzeigen des RMON-Ereignisprotokolls mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
rmon table-size log *Einträge*	Konfiguriert die maximale Anzahl von Protokolltabelleneinträgen.
show rmon log [*Ereignis*]	Zeigt die RMON-Protokolltabelle an.

Im Folgenden ein Beispiel für die CLI-Befehle:

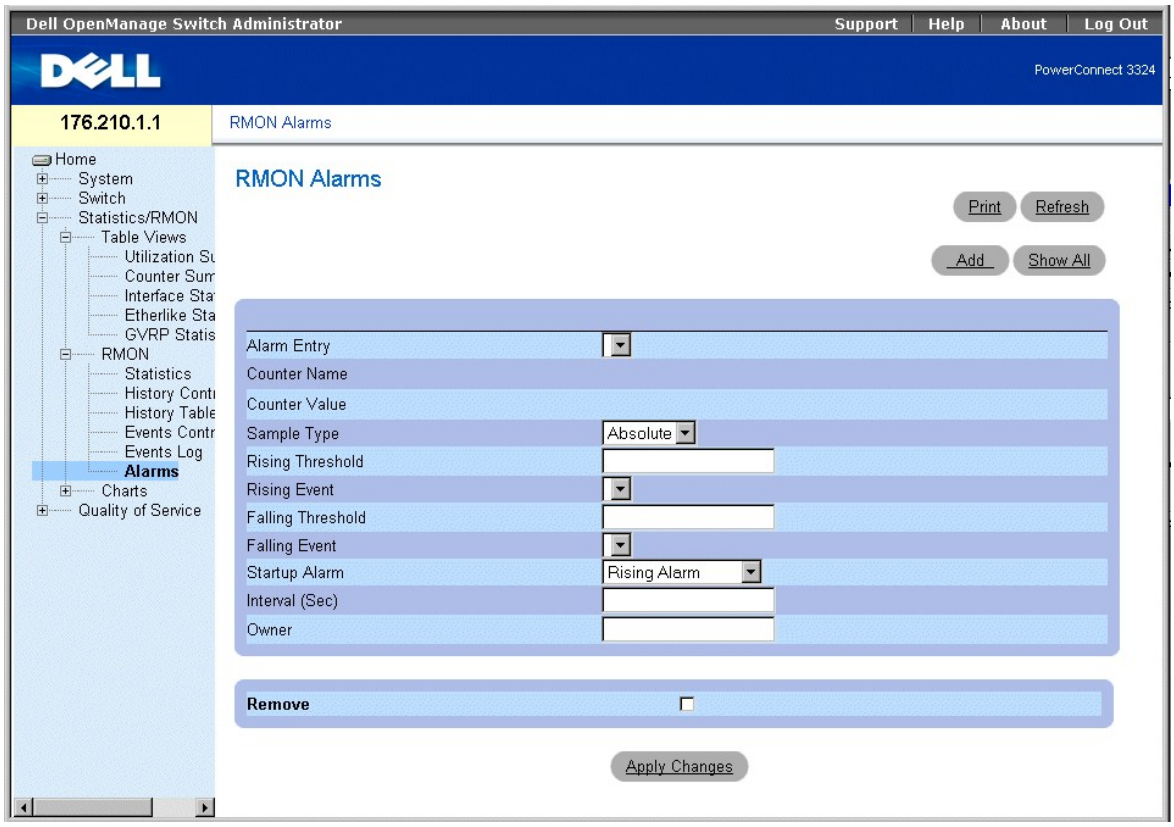
```
Console (config)# rmon table-size log 500

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



Console# show rmon log

Maximum table size: 500 (800 after reset)

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 Gerätealarmen

Auf der Seite **RMON Alarm** können Netzwerkadministratoren Netzwerkalarme einrichten. Ein Netzwerkalarm wird ausgegeben, wenn ein Netzwerkproblem vorliegt. Beim Über- oder Unterschreiten eines Schwellenwerts wird ein Alarm ausgegeben. So öffnen Sie die Seite **RMON Alarm**:

- Klicken Sie in der Strukturansicht auf **Statistics / RMON** > **RMON** > **Alarms**. Die Seite **RMON Alarm** wird geöffnet.



Seite "RMON Alarm"

Die Seite **RMON Alarm** enthält folgende Felder:

- **Alarm Entry**- Weist auf einen spezifischen Alarm hin.
- **Counter Name**- Gibt den ausgewählten RMON-Zähler an.
- **Counter Value**- Gibt den Wert des RMON-Zählers an.
- **Sample Type**- Gibt das Stichprobenverfahren für die ausgewählte Variable an und vergleicht den Wert mit den Schwellenwerten. Folgende Feldwerte können ausgewählt werden:
  - **Delta**- Subtrahiert den letzten Stichprobenwert vom aktuellen Wert. Die Differenz zwischen den Werten 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.
- **Rising/Falling Event**- Der Mechanismus, durch den ein Alarm gemeldet wird: Als Optionen kommen LOG bzw. TRAP oder eine Kombination aus beiden in Frage. Bei Auswahl von LOG verfügen weder das Gerät noch das Verwaltungssystem über einen Speichermechanismus. Wird das Gerät jedoch nicht zurückgesetzt, verbleibt sein Eintrag in der LOG-Gerätetabelle. Bei Auswahl von TRAP wird via SNMP ein TRAP generiert und über den grundlegenden TRAP-Mechanismus gemeldet. Der TRAP kann mit demselben Mechanismus gespeichert werden.
- **Falling Threshold**- Der untere Zählerwert, durch den der Alarm für die Unterschreitung des unteren Schwellenwertes ausgelöst wird.

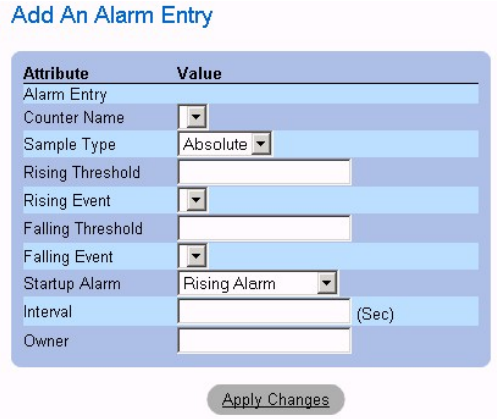
ANMERKUNG: Die oberen und unteren Schwellenwerte sind oben auf den Diagrammbalken grafisch dargestellt. Jeder überwachten Variablen wird eine eigene Farbe zugewiesen.

- **Startup Alarm**- Der Auslöser, durch den der Alarm aktiviert wird. Ein Anstieg wird wie folgt definiert: Das Überschreiten der Schwelle von einem niedrigeren zu einem höheren Schwellenwert. Folgende Feldwerte können ausgewählt werden:
  - **Rising Alarm**
  - **Falling Alarm**
  - **Rising and Falling Alarm**
- **Interval**- Gibt die Intervallzeit für den Alarm an.
- **Owner**- Gibt das Gerät bzw. den Benutzer an, von dem der Alarm definiert wurde.
- **Remove**- Entfernt einen RMON-Alarm.
  - **Aktiviert**- Entfernt einen Eintrag aus der **Alarm Table**.

- **Deaktiviert**- Behält einen Eintrag in der **Alarm Table** bei.

Hinzufügen eines Eintrags in die Alarmtabelle:

1. Öffnen Sie die Seite **RMON Alarm**.
2. Klicken Sie auf **Add**. Die Seite **New Alarm Entry** wird geöffnet.



New Alarm Entry

3. Definieren Sie die Felder **New Alarm Index, Sample Variable, Sample Type, Rising Threshold, Rising Event, Falling Threshold, Falling Event, Startup Alarm, Interval** und **Owner**.
4. Klicken Sie auf **Apply Changes**. Der RMON-Alarm wird hinzugefügt und das Gerät aktualisiert.

Ändern eines Eintrags in der Alarmtabelle:

1. Öffnen Sie die Seite **RMON Alarm**.
2. Wählen Sie aus der **RMON Alarm Table** einen Eintrag im Dropdown-Feld **Alarm Entry** aus.
3. Ändern Sie die Felder **Sample Type, Rising Threshold, Rising Event, Falling Threshold, Falling Event, Startup Alarm, Interval** und/oder **Owner**.
4. Klicken Sie auf **Apply Changes**. Der Eintrag in der **RMON Alarm Table** wird geändert und das Gerät aktualisiert.

Anzeigen der RMON Alarm Table:

1. Öffnen Sie die **RMON Alarm Table**.
2. Klicken Sie auf **Show All**. Die **RMON Alarm Table** wird geöffnet.

RMON Alarm Table

Löschen eines Eintrags aus der RMON Alarm Table:

1. Öffnen Sie die Seite **RMON Alarm**.
2. Wählen Sie einen **RMON Alarm** im Dropdown-Feld **Alarm Entry** aus.
3. Aktivieren Sie das Kontrollkästchen **Remove**.
4. Klicken Sie auf **Apply Changes**. Der Eintrag wird aus der **RMON Alarm Table** gelöscht und das Gerät aktualisiert.

Definieren und Anzeigen von Gerätealarmen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Konfiguration und Anzeige der Felder auf der Seite **RMON Alarms** zusammengefasst.

CLI-Befehl	Beschreibung
rmon alarm *index variable interval rthreshold fthreshold revent fevent* [**type** *type*] [**startup** *direction*] [**owner** *name*]	Konfiguriert Alarmbedingungen.
show rmon alarm-table	Zeigt die Alarmübersichtstabelle an.
show rmon alarm *Nummer*	Zeigt Alarmkonfigurationen an.

Im Folgenden ein Beispiel für den CLI-Befehl:

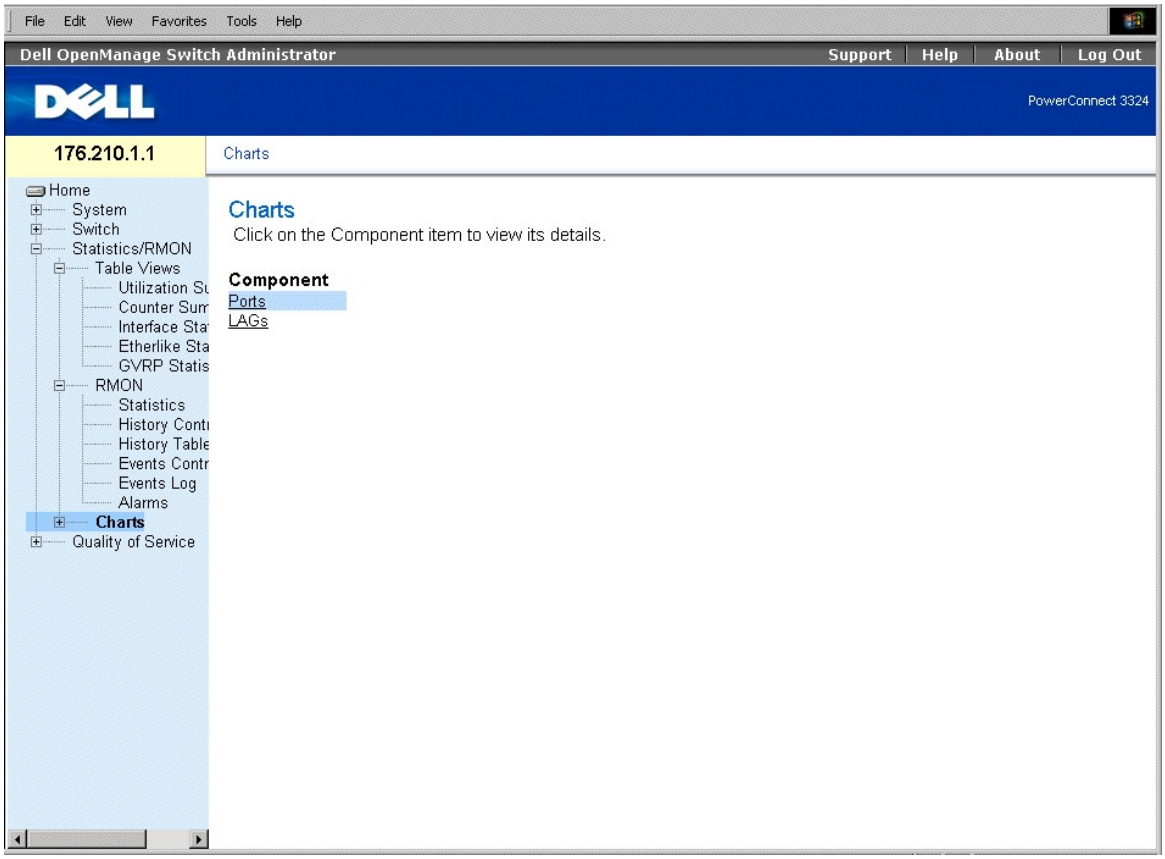
```
Console (config)# rmon alarm 1.3.6.1.2.1.2.2.1.10 1000000 10 20

Console (config)# exit

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

Console# show rmon alarm 1

Alarm 1

-------

OID: 1.3.6.1.2.1.2.2.1.10.1

Last sample Value: 878128

Interval: 30

Sample Type: delta

Startup Alarm: rising
```

```
Rising Threshold: 8700000

Falling Threshold: 78

Rising Event: 1

Falling Event: 1

Owner: CLI
```

Anzeigen von Diagrammen

Die Seite **Charts** enthält Links zur Anzeige von Statistiken in Tabellenform. So öffnen Sie die Seite **Charts**:

- Klicken Sie in der Strukturansicht auf **Statistics** > **Charts**. Die Seite **Charts** wird geöffnet.



Seite "Charts"

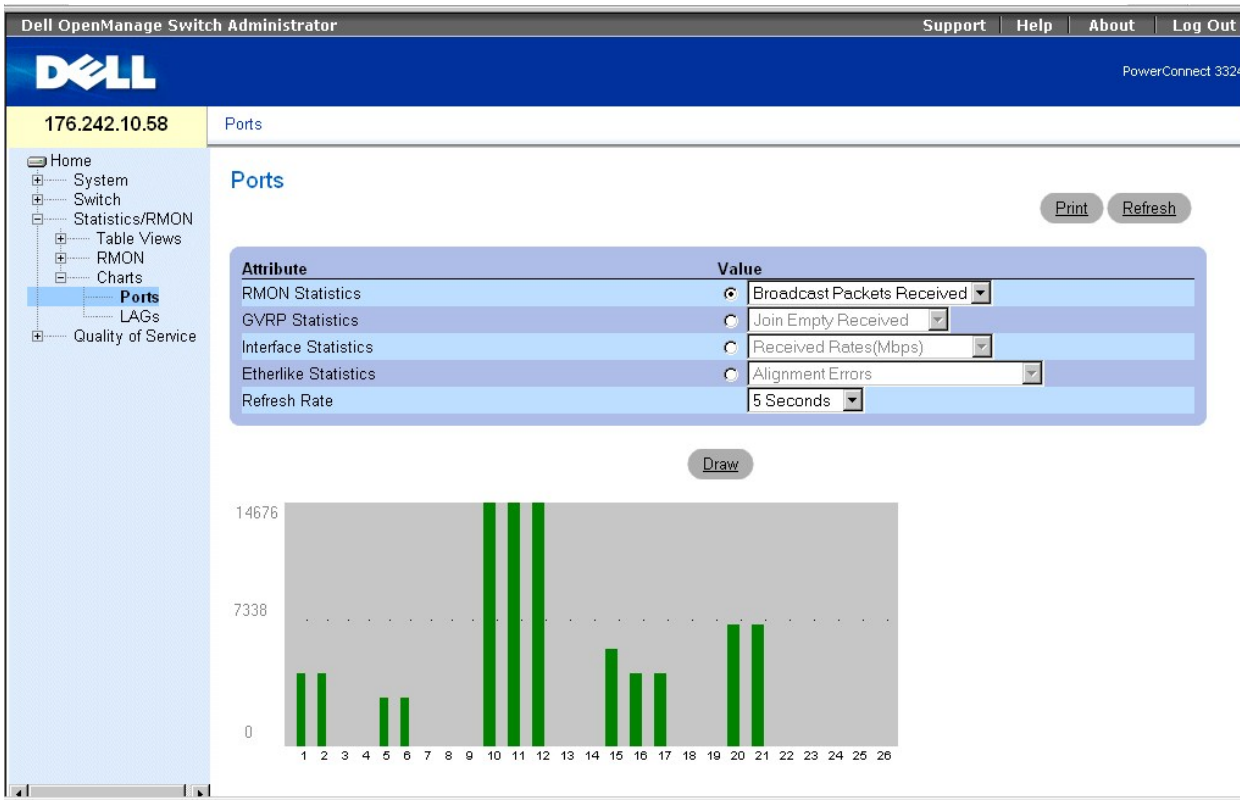
Die Seite **Charts** enthält die folgenden Links:

- Anzeigen von Anschlussstatistiken
- Anzeigen von LAG-Statistiken

Anzeigen von Anschlussstatistiken

Auf der Seite **Ports** werden Statistiken zu einem ausgewählten Anschluss in Diagrammform angezeigt. So öffnen Sie die Seite Port **Statistics**:

- Klicken Sie in der Strukturansicht auf **Statistics** >**Charts**> **Ports**. Die Seite Port **Statistics** wird geöffnet.



Seite "Port Statistics"

Die Seite **Port Statistics** enthält folgende Felder:

- **Interface Statistics**- Zeigt eine Schnittstellenstatistik für die ausgewählte Einheit an.
- **Etherlike Statistics**- Zeigt eine Etherlike-Statistik für die ausgewählte Einheit an.
- **RMON Statistics**- Zeigt eine RMON-Statistik für die ausgewählte Einheit an.
- **GVRP Statistics**- Zeigt eine GVRP-Statistik für die ausgewählte Einheit an.
- **Refresh Rate**- Gibt den Zeitraum bis zur Aktualisierung des Gerätes an. Folgende Feldwerte können ausgewählt werden:
  - **15 Sec**- Gibt an, dass die Anschlussstatistiken alle 15 Sekunden aktualisiert werden.
  - **30 Sec**- Gibt an, dass die Anschlussstatistiken alle 30 Sekunden aktualisiert werden.
  - **60 Sec**- Gibt an, dass die Anschlussstatistiken alle 60 Sekunden aktualisiert werden.
  - **No Refresh**- Gibt an, dass die Anschlussstatistiken nicht automatisch aktualisiert werden.

Anzeigen anschlussspezifischer Statistiken

1. Öffnen Sie die Seite Port **Statistics**.
2. Wählen Sie Kategorie und Anschluss für die Statistik aus.
3. Klicken Sie auf **Draw**. Die Statistik für die ausgewählte Schnittstelle wird angezeigt.

Anzeigen von Anschlussstatistiken mit Hilfe der CLI-Befehle

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

CLI-Befehl	Beschreibung
clear counters [ethernet *Schnittstelle* | **port-channel** *Anschlusskanalnummer*]	Löscht den Inhalt der Statistik für eine Schnittstelle.
show rmon statistics [ethernet *Schnittstelle* | **port-channel** *Anschlusskanalnummer*]	Zeigt RMON-Ethernet-Statistiken an.
clear gvrp statistics [**ethernet** *Schnittstelle* | **port-channel** *Anschlusskanalnummer*]	Löscht die gesamten GVRP-Statistikdaten.
show gvrp statistics [ethernet *Schnittstelle* | **port-channel** *Anschlusskanalnummer*]	Zeigt GVRP-Statistiken an.
show gvrp error-statistics [**ethernet** *Schnittstelle* | **port-channel** *Anschlusskanalnummer*]	Zeigt GVRP-Fehlerstatistiken an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console# clear counters ethernet 1/e1

Console# show rmon statistics ethernet 1/e1

Port 1/e1

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: 256 to 511 Octets: 0

512 to 1023 Octets: 491 1024 to 1518 Octets: 389

Console # configure

Console (config)# clear gvrp statistics ethernet 1/e8

Console (config)# exit
```

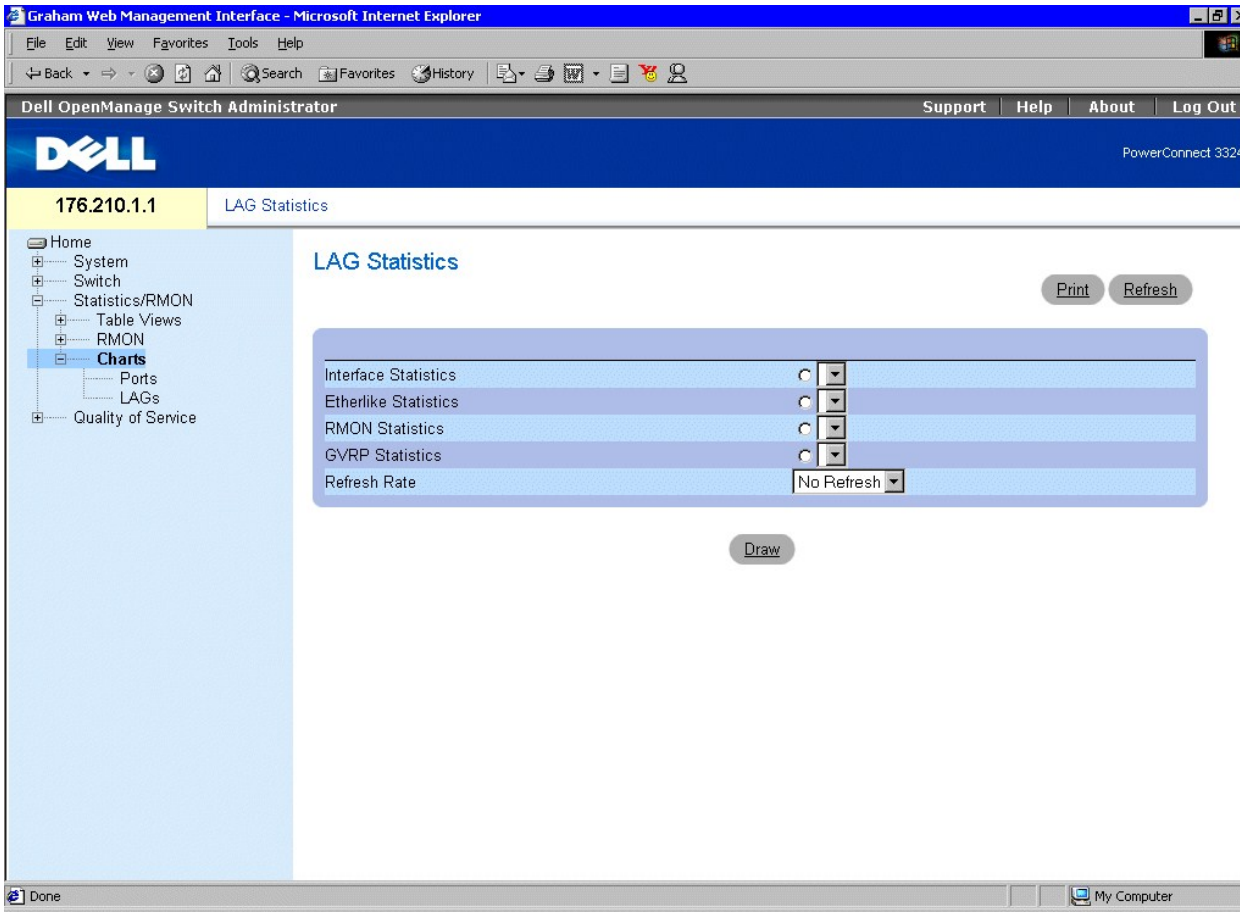
```
Console# show gvrp statistics

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

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

1/e1 0 0 0 0 0 0 0 0 0 0 0 0

1/e2 0 0 0 0 0 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0 0 0 0 0 0

1/e4 0 0 0 0 0 0 0 0 0 0 0 0

1/e5 0 0 0 0 0 0 0 0 0 0 0 0

1/e6 0 0 0 0 0 0 0 0 0 0 0 0

1/e7 0 0 0 0 0 0 0 0 0 0 0 0

1/e8 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

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

1/e1 0 0 0 0 0 0

1/e2 0 0 0 0 0 0

1/e3 0 0 0 0 0 0

1/e4 0 0 0 0 0 0

1/e5 0 0 0 0 0 0

1/e6 0 0 0 0 0 0

1/e7 0 0 0 0 0 0

1/e8 0 0 0 0 0 0
```

Anzeigen von LAG-Statistiken

Auf der Seite **LAG Statistics** werden Statistiken für Anschlusselemente in Diagrammform angezeigt. So öffnen Sie die Seite **LAG Statistics**:

- Klicken Sie in der Strukturansicht auf **Statistics** > **Charts** > **LAGs**. Die Seite **LAG Statistics** wird geöffnet.



Seite "LAG Statistics"

Die Seite **LAG Statistics** enthält folgende Felder:

- **Interface Statistics**- Bietet eine Schnittstellenstatistik für Trunks.
- **Etherlike Statistics**- Bietet eine Etherlike-Statistik für Trunks.
- **RMON Statistics**- Bietet eine RMON-Statistik für Trunks.
- **GVRP Statistics**- Bietet eine GVRP-Statistik für Trunks.
- **Refresh Rate**- Gibt den Zeitraum bis zur Aktualisierung des Gerätes an. Folgende Feldwerte können ausgewählt werden:
  - **15 Sec**- Gibt an, dass die LAG-Statistiken alle 15 Sekunden aktualisiert werden.
  - **30 Sec**- Gibt an, dass die LAG-Statistiken alle 30 Sekunden aktualisiert werden.
  - **60 Sec**- Gibt an, dass die LAG-Statistiken alle 60 Sekunden aktualisiert werden.
  - **No Refresh**- Gibt an, dass die LAG-Statistiken nicht aktualisiert werden.

Anzeigen anschlussspezifischer Statistiken:

1. Öffnen Sie die Seite **Port Statistics**.
2. Wählen Sie einen Schnittstellentyp aus.
3. Klicken Sie auf **Draw**. Die Statistik für die ausgewählte Schnittstelle wird angezeigt.

Anzeigen von LAG-Statistiken mit Hilfe der CLI-Befehle

Die folgende Tabelle enthält CLI-Befehle für die Anzeige von LAG-Statistiken.

CLI-Befehl	Beschreibung
show interfaces counters [**ethernet** *Schnittstelle* | **port-channel** *Anschlusskanalnummer*]	Zeigt Statistiken für eine physische Schnittstelle an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console# show interfaces counters

Port InOctets InUcastPkts InMcastPkts InBcastPkts

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

1/e1 183892 1289 987 8

2/e1 0 0 0 0

3/e1 123899 1788 373 19

Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts

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

1/e1 9188 9 8 0

2/e1 0 0 0 0

3/e1 8789 27 8 0

Ch InOctets InUcastPkts InMcastPkts InBcastPkts

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

1 27889 928 0 78

Ch OutOctets OutUcastPkts OutMcastPkts OutBcastPkts

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

1 23739 882 0 122
```

```
Console# show interfaces counters ethernet 1/e1

Port InOctets InUcastPkts InMcastPkts InBcastPkts

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

1/e1 183892 1289 987 8

Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts

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

1/e1 9188 9 8 0

Alignment Errors: 17

FCS Errors: 8

Single Collision Frames: 0

Multiple Collision Frames: 0

SQE Test Errors: 0

Deferred Transmissions: 0

Late Collisions: 0

Excessive Collisions: 0

Internal MAC Tx Errors: 0

Carrier Sense Errors: 0

Oversize Packets: 0

Internal MAC Rx Errors: 0

Symbol Errors: 0

Received Pause Frames: 0
```

```
     Transmitted Pause Frames: 0

----------------------------------------------------------------------------
```

Zurück zum Inhalt

Zurück zum Inhalt

Dell™ PowerConnect™ 3324/3348 Benutzerhandbuch

Modell PowerConnect 3324/3348

Anmerkungen, Hinweise und Vorsichtshinweise

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

HINWEIS: Ein HINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und weist darauf hin, wie Probleme vermieden werden können.

VORSICHT: Unter VORSICHT werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

November 2003 Version A01

Zurück zum Inhalt