

# Dell™ PowerConnect™ 5324 System-Benutzerhandbuch

[Einführung](#)

[Beschreibung der Hardware:](#)

[Installation des PowerConnect-Geräts:](#)

[Starten und Konfigurieren des Geräts](#)

[Verwendung von Dell OpenManage Switch Administrator](#)

[Konfiguration der Systeminformationen](#)

[Konfiguration der Geräteinformationen](#)

[Anzeigen von Statistiken](#)

[Konfiguration von QoS \(Quality of Service\):](#)

[Gerätespezifikationen:](#)

[Glossar](#)

---

## Anmerkungen, Hinweise und Vorsichtshinweise



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



**HINWEIS:** Ein HINWEIS weist auf mögliche Schäden an der Hardware oder auf möglichen Datenverlust hin und beschreibt, wie Sie dieses Problem vermeiden können.



**VORSICHT:** VORSICHT weist auf Gefahren hin, die zu Sachschäden, Personenschäden oder lebensgefährlichen Verletzungen führen können.

---

**Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern.**

©2003 – 2007 Dell Inc. Alle Rechte vorbehalten.

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

Markenzeichen in diesem Text: *Dell*, *Dell OpenManage*, das *DELL*-Logo, *Inspiron*, *Dell Precision*, *Dimension*, *OptiPlex*, *PowerConnect*, *PowerApp*, *PowerVault*, *Axim*, *DellNet* und *Latitude* sind Marken von Dell Inc. *Microsoft* und *Windows* sind eingetragene Marken von Microsoft Corporation.

Alle anderen in dieser Dokumentation genannten Markenzeichen und Handelsbezeichnungen sind Eigentum der entsprechenden Hersteller und Firmen. Dell Inc. erhebt keinerlei Eigentumsansprüche auf Markenzeichen und Markennamen außer der eigenen Markenzeichen und Dienstleistungsmarken.

May 2007

[Zurück zum Inhaltsverzeichnis](#)

## Starten und Konfigurieren des Geräts

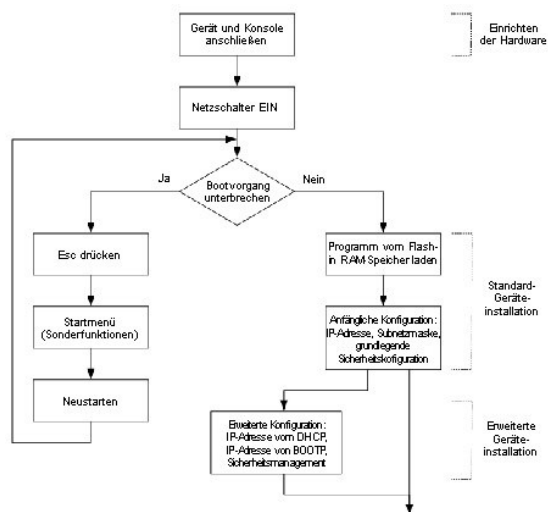
Benutzerhandbuch für das Dell™ PowerConnect™ 5324 System

- [Konfigurieren des Terminals](#)
- [Starten des Geräts](#)
- [Konfiguration - Übersicht](#)
- [Anfängliche Konfiguration](#)
- [Benutzername](#)
- [SNMP-Communityzeichenfolge](#)
- [Erweiterte Konfiguration](#)
- [Abrufen einer IP-Adresse von einem DHCP-Server](#)
- [Empfangen einer IP-Adresse von einem BOOTP-Server](#)
- [Sicherheitsmanagement und Kennwortkonfiguration](#)
- [Konfigurieren von Sicherheitskennwörtern](#)
- [Startanweisungen](#)

Nach Herstellung aller externen Anschlüsse stellen Sie die Verbindung des Geräts zu einem Terminal her, um das Gerät zu konfigurieren und um andere Verfahren durchzuführen. Die Anfangskonfiguration erfolgt im Rahmen der Standard-Gerätekonfiguration.

**ANMERKUNG:** Bevor Sie fortfahren, lesen Sie bitte die Versionshinweise für dieses Produkt. Die Versionshinweise können von [www.support.dell.com](http://www.support.dell.com) heruntergeladen werden.

Abb. 4-12. Installations- und Konfigurationsablauf




## Konfigurieren des Terminals

Zur Konfiguration des Geräts muss auf dem Terminal eine Terminal-Emulation-Software betrieben werden.

Stellen Sie sicher, dass die Terminal-Emulation-Software wie folgt eingestellt ist:

1. Wählen Sie den entsprechenden seriellen Port (serieller Port 1 oder serieller Port 2) zum Anschluss an die Konsole.
2. Setzen Sie die Datenübertragungsrate auf 9600 Baud.
3. Setzen Sie das Datenformat auf 8 Datenbits, 1 Stopbit und keine Parität.
4. Stellen Sie Datenflusssteuerung auf **none** ein.
5. Wählen Sie unter **Properties** (Eigenschaften) den Modus **VT100 for Emulation** (VT100 für Emulation).

6. Wählen Sie **Terminal keys** (Terminaltasten) für **Function, Arrow, and Ctrl keys** (Funktion, Pfeil, und Kontrolltasten). Stellen Sie sicher, dass **Terminal keys** (Terminaltasten) und nicht **Windows keys** (Windows-Tasten) gewählt ist.

 **HINWEIS:** Stellen Sie bei Verwendung von HyperTerminal mit Microsoft® Windows 2000 sicher, dass der Windows® 2000 Service-Pack 2 oder höher installiert ist. Beim Windows 2000 Service-Pack 2 funktionieren die Pfeiltasten ordnungsgemäß bei der HyperTerminal VT100 Emulation. Gehen Sie zu [www.microsoft.com](http://www.microsoft.com), um Informationen über Windows 2000 Service-Packs zu erhalten.

---

## Starten des Geräts

 **ANMERKUNG:** Es wird von den folgenden Startinformationen ausgegangen:

- n Das Gerät wird mit einer Standardkonfiguration geliefert.
- n Das Gerät ist nicht mit einem Standard-Benutzernamen und einem Kennwort konfiguriert.

Führen Sie folgende Schritte durch, um das Gerät zu starten:

1. Stellen Sie sicher, dass der serielle Port des Geräts an einem ASCII-Terminal oder dem seriellen Anschluss eines Desktopsystems, auf dem die Terminal-Emulation-Software ausgeführt wird, angeschlossen ist.
2. Suchen Sie nach einer Netzanschlussbuchse.
3. Schalten Sie die Netzanschlussbuchse aus.
4. Schließen Sie das Gerät an die Netzbuchse an. Siehe [„Anschließen eines Geräts an einer Stromversorgung“](#).
5. Schalten Sie die Netzanschlussbuchse ein.

Wenn der Strom eingeschaltet wird und das lokale Terminal bereits angeschlossen ist, durchläuft das Gerät einen Einschalt-Selbsttest (POST). POST wird jedesmal ausgeführt, wenn das Gerät initialisiert wird, und überprüft die Hardware-Komponenten, um festzustellen, ob das Gerät vor dem Start vollständig betriebsbereit ist. Wenn ein kritisches Problem entdeckt wird, wird der Programmfluss gestoppt. Wenn POST erfolgreich ausgeführt wurde, wird ein gültiges und ausführbares Bild in das RAM geladen. POST-Meldungen werden auf dem Terminal angezeigt und zeigen einen Erfolg oder einen Fehlschlag des Tests.

1. Stellen Sie sicher, dass das ASCII-Kabel am Terminal angeschlossen ist und dass die Parameter für SW- Emulation richtig konfiguriert sind.
2. Schließen Sie die Stromversorgung am Gerät an.
3. Schalten Sie das Gerät ein.
4. Beim Start des Geräts wird im Zuge des Bootup-Tests zuerst die verfügbare Speicherkapazität des Geräts festgestellt und der Startvorgang wird dann fortgesetzt. Der folgende Bildschirm illustriert eine POST-Anzeige:

```
----- Performing the Power-On Self Test (POST) -----  
  
UART Channel Loopback Test.....PASS  
  
Testing the System SDRAM.....PASS  
  
Boot1 Checksum Test.....PASS  
  
Boot2 Checksum Test.....PASS  
  
Flash Image Validation Test.....PASS  
  
BOOT Software Version 1.0.0.20 Built 22-Jan-2004 15:09:28  
  
Processor: FireFox 88E6218 ARM946E-S , 64 MByte SDRAM.
```

I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.

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

Preparing to decompress...

Das Booten dauert ca. 90 Sekunden.

Die am Ende des POST (siehe die letzten Zeilen) angezeigte Auto-Boot-Meldung teilt mit, dass während des Startvorgangs keine Probleme aufgetreten sind.

Während des Starts kann das **Startup**-Menü zur Ausführung spezieller Verfahren verwendet werden. Zum Aufruf des **Startup**-Menüs drücken Sie <Esc> oder die <Eingabetaste> innerhalb der ersten zwei Sekunden nach Anzeige der Auto-Boot-Meldung.

Wenn der Systemstartprozess nicht durch Drücken von <Esc> oder der <Eingabetaste> unterbrochen wird, wird der Prozess mit der Dekomprimierung und Laden des Codes im RAM fortgesetzt. Der Code wird dann vom RAM ausgeführt und die Liste der nummerierten Systemports und ihrer Zustände (ein oder aus) wird angezeigt.

Der folgende Bildschirm illustriert eine Konfiguration. Elemente wie Adressen, Versionen und Daten können abweichen.

Decompressing SW from image-2

78c000

OK

Running from RAM...

\*\*\*\*\*

\*\*\* Running SW Ver. 1.0.0.15 Date 03-Mar-2004 Time 10:41:14 \*\*\*

\*\*\*\*\*

HW version is 00.01.07

Base Mac address is: 00:00:07:77:77:77

Dram size is : 64M bytes

Dram first block size is : 40960K bytes

Dram first PTR is : 0x1800000

Flash size is: 16M

Device configuration:

Presteria based system

Slot 1 - Neyland24 HW Rev. 0.1

Tapi Version: v1.2.9

Core Version: v1.2.9

01-Jan-2000 01:01:32 %INIT-I-InitCompleted: Initialization task is completed

console> 01-Jan-2000 01:01:35 %LINK-W-Down: g1

01-Jan-2000 01:01:35 %LINK-W-Down: g2

01-Jan-2000 01:01:35 %LINK-W-Down: g3

01-Jan-2000 01:01:35 %LINK-W-Down: g4

01-Jan-2000 01:01:35 %LINK-W-Down: g5

01-Jan-2000 01:01:35 %LINK-W-Down: g6

01-Jan-2000 01:01:35 %LINK-W-Down: g7

01-Jan-2000 01:01:35 %LINK-W-Down: g8

01-Jan-2000 01:01:35 %LINK-W-Down: g9

01-Jan-2000 01:01:35 %LINK-W-Down: g10

01-Jan-2000 01:01:35 %LINK-W-Down: g11

01-Jan-2000 01:01:35 %LINK-W-Down: g12

01-Jan-2000 01:01:35 %LINK-W-Down: g13

01-Jan-2000 01:01:36 %LINK-W-Down: g14

01-Jan-2000 01:01:36 %LINK-W-Down: g15

01-Jan-2000 01:01:36 %LINK-W-Down: g16

01-Jan-2000 01:01:36 %LINK-W-Down: g17

01-Jan-2000 01:01:36 %LINK-W-Down: g18

01-Jan-2000 01:01:36 %LINK-W-Down: g19

01-Jan-2000 01:01:36 %LINK-W-Down: g20

01-Jan-2000 01:01:36 %LINK-W-Down: g21

01-Jan-2000 01:01:36 %LINK-W-Down: g22

01-Jan-2000 01:01:36 %LINK-I-Up: Vlan 3000

01-Jan-2000 01:01:36 %LINK-I-Up: Vlan 1

01-Jan-2000 01:01:36 %LINK-I-Up: g1

01-Jan-2000 01:01:36 %LINK-I-Up: g13

01-Jan-2000 01:01:36 %LINK-I-Up: g14

01-Jan-2000 01:01:36 %LINK-I-Up: g19

01-Jan-2000 01:01:36 %LINK-I-Up: g20

01-Jan-2000 01:01:36 %LINK-I-Up: g21

01-Jan-2000 01:01:36 %LINK-W-Down: g23

01-Jan-2000 01:01:36 %LINK-W-Down: g24

01-Jan-2000 01:01:36 %LINK-W-Down: chl

```
01-Jan-2000 01:01:36 %LINK-I-Up: Vlan 1000
```

```
01-Jan-2000 01:01:36 %TRUNK-I-PORTADDED: Port g24 added to chl
```

```
01-Jan-2000 01:01:36 %LINK-I-Up: g22
```

```
01-Jan-2000 01:01:36 %LINK-I-Up: g23
```

```
01-Jan-2000 01:01:36 %LINK-I-Up: g24
```

```
01-Jan-2000 01:01:36 %LINK-I-Up: chl
```

```
01-Jan-2000 01:01:36 %LINK-W-Down: g1
```

```
01-Jan-2000 01:03:42 %INIT-I-Startup: Cold Startup
```

```
console>
```

Nach erfolgreichem Start des Geräts wird eine System-Eingabeaufforderung angezeigt (`console>`), die zur Konfiguration des Geräts dient. Stellen Sie jedoch, bevor Sie das Gerät konfigurieren, sicher, dass die aktuelle Softwareversion auf dem Gerät installiert ist. Wenn es nicht die aktuellste Version ist, laden Sie diese herunter und installieren sie. Näheres zum Herunterladen der neuesten Version finden Sie unter [„Software-Download“](#).

---


## Konfigurationsübersicht

Holen Sie vor der Zuweisung einer statischen IP-Adresse für das Gerät die folgenden Informationen ein:

- 1 Eine spezifische IP-Adresse, die dem Gerät für seine Konfiguration zugewiesen wurde.
- 1 Standard-Route.
- 1 Netzwerkmaske für das Netzwerk.

Es gibt zwei Konfigurationsarten:


- 1 **Anfängliche Konfiguration** — umfasst Konfigurationsfunktionen mit grundlegenden Sicherheitsgesichtspunkten.
- 1 **Erweiterte Konfiguration** — umfasst eine dynamische IP-Konfiguration und erweiterte Sicherheitsgesichtspunkte.

 **ANMERKUNG:** Nachdem Konfigurationsänderungen vorgenommen wurden, muss die neue Konfiguration gespeichert werden, bevor ein Neustart durchgeführt wird. Geben Sie zum Speichern der Konfiguration Folgendes ein:

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

---

## Anfängliche Konfiguration

 **ANMERKUNG:** Bevor Sie fortfahren, lesen Sie bitte die Versionshinweise für dieses Produkt. Die Versionshinweise können von der Dell Support-Website auf [support.dell.com](http://support.dell.com) heruntergeladen werden.

 **ANMERKUNG:** Die einfache Anfangskonfiguration geht von der folgenden Ausgangssituation aus:

- n Das PowerConnect-Gerät wurde noch nie konfiguriert und ist in dem Zustand, in dem es geliefert wurde.
- n Das PowerConnect-Gerät wurde erfolgreich gestartet.
- n Der serielle Anschluss ist aufgebaut und der Konsolenprompt ist auf dem Bildschirm einer VT100-Terminalkomponente angezeigt. (Drücken Sie mehrmals die <Eingabetaste>, um zu überprüfen, dass das Anforderungszeichen erscheint.)
- n Das Gerät ist nicht mit einem Standard-Benutzernamen und einem Kennwort konfiguriert.

Die Anfangsgerätekonfiguration wird über den seriellen Port durchgeführt. Nach der ersten Konfiguration kann das Gerät entweder von dem bereits angeschlossenen seriellen Port verwaltet oder einer Schnittstelle fernverwaltet werden, die während der Anfangskonfiguration definiert wurde.

Die Anfangskonfiguration besteht aus Folgendem:

- 1 Einstellung des Benutzernamens 'admin', des Kennwortes 'dell' mit der höchsten Privilegstufe 15.
- 1 Konfiguration der statischen IP-Adresse und der Standard-Gateway.
- 1 Konfiguration der SNMP-Lese/Schreib-Community-Zeichenkette.
- 1 Zuordnung der vom DHCP-Server zugewiesenen IP-Adresse.

Vor Anwendung des ersten Konfigurationsverfahrens auf das PowerConnect-Gerät müssen die folgenden Informationen vom Netzwerkadministrator eingeholt werden:

- 1 Die IP-Adresse, die einem VLAN zugewiesen werden soll, über das das Gerät verwaltet wird.
- 1 Die IP-Subnetzmaske für das Netzwerk.
- 1 Die IP-Adresse der Standard-Gateway.
- 1 Die SNMP-Community.

## Statische IP-Adresse und Subnetzmaske

Eine IP-Adresse kann auf jeder Schnittstelle, einschließlich VLAN, LAG, und einem physikalischen Port konfiguriert werden. Nach der Eingabe des Konfigurationsbefehls wird empfohlen, durch Eingabe des Befehls **show ip interface** zu prüfen, ob ein Port mit der IP-Adresse konfiguriert wurde.


**Wichtig:** Wenn eine IP-Adresse auf einer LAG oder einem physikalischen Port konfiguriert wird (ex. g10), wird diese Schnittstelle aus VLAN 1 entfernt.

## Konfigurieren der statischen Route

Zur Verwaltung des Geräts von einem Remote-Netzwerk muss eine statische Route konfiguriert werden; darunter versteht man eine IP-Adresse, an die Datenpakete geschickt werden, wenn in den Gerätetabellen keine Einträge gefunden werden. Die konfigurierte IP-Adresse muss zum gleichen Subnetz gehören wie eine der IP-Geräteschnittstellen.

Zur Konfiguration einer statischen Route geben Sie den Befehl an der System-Prompt, wie im folgenden Konfigurationsbeispiel gezeigt, ein. In diesem Beispiel ist 100.1.1.1 (mask 24) die entsprechende Verwaltungsstation und 100.1.1.10 ist die statische Route, die als Standard-Gateway fungiert.

## Zuweisen einer statischen IP-Adresse auf einer bandinternen Schnittstelle

 **ANMERKUNG:** Dieses Beispiel illustriert die folgenden Annahmen:

- n Die IP-Adresse, die der PowerConnect VLAN-Schnittstelle zugewiesen wird, ist 192.168.1.123
- n Die IP-Teilnetzmaske für das Netzwerk ist 255.255.255.0
- n Die IP-Adresse der Standard-Route ist 192.168.1.1
- n Die SNMP-Lese/Schreib-Community-Zeichenkette ist „private“

```
console> enable
```



```

Console# configure

console(config)# username admin password dell level 15

Console(config)# interface vlan 1

console (config-if) # ip address 192.168.1.123 /24

console (config-if) # exit

console (config) # ip default-gateway 192.168.1.1

console (config) # snmp-server community private rw

Console(config)# exit

console#

```

## Verifizieren der IP- und Standard-Gateway-Adressen

Stellen Sie durch die Ausführung des folgenden Befehls und die Prüfung der Ausgabe sicher, dass die IP-Adresse und die Standard-Gateway korrekt zugewiesen wurden:


### Befehl

```
console# show ip interface vlan 1
```

### Output

Gateway IP Address	Activity status	
-----	-----	
192.168.1.1	Active	
IP address:	Interface	Type
-----	-----	-----
192.168.1.123 /24	Vlan 1	static

---

 **ANMERKUNG:** Es wird empfohlen, die neueste Version der Benutzerdokumentation von der Dell Support-Website [support.dell.com](http://support.dell.com) herunterzuladen.

---

## Benutzername

Zur Fernverwaltung des Geräts, zum Beispiel über SSH, Telnet oder die Web-Schnittstelle, muss ein Benutzername konfiguriert werden. Zur Gewährung umfassender Verwaltungskontrolle über das Gerät muss das höchste Benutzerprivileg (15) angegeben werden.

 **ANMERKUNG:** Nur der Verwalter (Super-User) mit der höchsten Privilegstufe (15) darf das Gerät über die Web-Browser-Schnittstelle verwalten.

Weitere Informationen zu Privilegstufen finden Sie im „CLI-Referenzhandbuch“.

Der konfigurierte Benutzername wird als Anmeldename für Fernverwaltungs-Sessions eingegeben. Zur Konfiguration des Benutzernamens und der Privilegstufe geben Sie den Befehl an der System-Prompt ein, wie im Konfigurationsbeispiel gezeigt:

```
console> enable
Console# configure
console(config)# username admin password abc level 15
```


---

## SNMPCommunityzeichenfolge

Simple Network Management Protocol (SNMP) stellt ein Verfahren zur Verwaltung von Netzwerkgeräten bereit. Geräte, die SNMP unterstützen, führen eine lokale Software (Agent) aus. Die SNMP-Agenten führen eine Liste von Variablen, die zur Verwaltung des Geräts dienen. Die Variablen werden in der Management Information Base (MIB) definiert. Die MIB präsentiert die vom Agenten gesteuerten Variablen. Der SNMP-Agent definiert das MIB-Spezifikationsformat sowie das Format, das zum Zugriff auf die Informationen über das Netzwerk verwendet wird. Die Zugriffsrechte für SNMP-Agenten werden durch Zugriffs-Zeichenfolgen und SNMP-Communityzeichenfolgen geregelt.

Das Gerät ist SNMP-konform und umfasst einen SNMP-Agenten, der einen Satz von Standard- und privaten MIB-Variablen unterstützt. Developer von Management-Stations benötigen den genauen MIB-Strukturbaum und erhalten die umfassenden privaten MIB-Informationen, bevor Sie die MIBs verwalten können.

Alle Parameter können von jeder SNMP-Verwaltungsplattform aus verwaltet werden, mit Ausnahme der IP-Adresse der SNMP-Verwaltungsstation, Community-Name und Zugriffsrechte. Der SNMP-Verwaltungszugriff ist deaktiviert, wenn keine Community-Zeichenfolgen existieren.

 **ANMERKUNG:** Das Gerät wird ohne konfigurierte Communityzeichenfolgen geliefert. SNMPv1 und SNMPv2 werden auf dem Gerät unterstützt. In diesem Abschnitt werden die SNMPv1/v2-Konfigurationsparameter beschrieben.

Der folgende Bildschirm zeigt die Standardgerätekonfiguration an:

Console# show snmp		
Community- String	Community-Access	IP-Adresse:
-----	-----	-----
Traps are enabled.		
Authentication trap is enabled.		

Trap-Rec- Address	Trap-Rec- Community	Version
System Contact:		
System Location:		

Während des ersten Konfigurationsverfahrens können die Communityzeichenfolge, Community-Zugriff und die IP-Adresse über den lokalen Terminal eingestellt werden.

Die SNMP-Konfigurationsoptionen sind:

- 1 Community string (Communityzeichenfolge).
  - o **Read Only** — Gibt an, dass die Community-Mitglieder die Konfigurationsinformationen nur ansehen, aber nicht ändern können.
  - o **Read/Write** — Gibt an, dass die Community-Mitglieder die Konfigurationsinformationen ansehen und ändern können.
  - o **Super** — Gibt an, dass die Community-Mitglieder Verwaltungszugriff haben.
- 1 Konfigurierbare IP-Adresse. Wenn keine IP-Adresse konfiguriert ist, haben alle Community-Mitglieder mit dem gleichen Community-Namen die gleichen Zugriffsrechte.

Häufig werden zwei Communityzeichenfolgen für das Gerät verwendet — eine (öffentliche Community) mit Nur-Lese-Zugriff und die andere (private Community) mit Lese/Schreib-Zugriff. Die öffentliche Zeichenfolge ermöglicht befugten Management-Stations den Abruf von MIB-Objekten, während die private Zeichenfolge es befugten Management-Stations ermöglicht, MIB-Objekte abzurufen und zu ändern.

Bei der ersten Konfiguration wird empfohlen, das Gerät entsprechend der Anforderungen der Netzwerkverwaltung, gemäß Verwendung einer SNMP-basierten Management-Station, zu konfigurieren.

## Konfigurieren von SNMP

Zur Konfiguration der IP-Adresse einer SNMP-Station und (einer) Communityzeichenfolge(n) für die allgemeinen Gerät-Router-Tabellen führen Sie folgende Schritte aus.

1. Geben Sie an der Konsolen-Prompt den Befehl **Enable** ein. Die Prompt wird als # angezeigt.
2. Geben Sie den Befehl **configure** ein und drücken Sie die <Eingabetaste>.
3. Geben Sie im Konfigurationsmodus den SNMP-Konfigurationsbefehl mit den Parametern ein, einschließlich Community-Name (privat), Community-Zugriffsrecht (Lese und Schreib) und IP- Adresse, wie im nachstehenden Beispiel gezeigt:

```
Console# configure

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

## Anzeigen der SNMP-Community-Tabellen

So zeigen Sie die IP-Adresse der SNMP-Station und Community-Tabellen an:

1. Geben Sie an der Konsolen-Prompt den Befehl **exit** ein. Die Prompt wird als # angezeigt.
2. Geben Sie im privilegierten EXEC-Modus den Show-Befehl, wie im nachstehenden Beispiel gezeigt, ein:

Die konfigurierten Parameter ermöglichen die weitere Gerätekonfiguration von jedem entfernten Standort aus.

Console# <b>show snmp</b>		
Community- String	Community-Access	IP-Adresse:
-----	-----	-----
private	read write	11.1.1.2
Traps are enabled.		
Authentication trap is enabled.		
Trap-Rec- Address	Trap-Rec- Community	Version
System Contact:		
System Location:		

---

## Erweiterte Konfiguration

Dieser Abschnitt enthält Informationen über die dynamische Zuweisung von IP-Adressen und Sicherheitsverwaltung auf der Grundlage der AAA-Mechanismen (Authentifizierung, Autorisierung und Abrechnung) und behandelt die folgenden Themen:

- 1 Konfiguration von IP-Adressen über DHCP
- 1 Konfiguration von IP-Adressen über BOOTP
- 1 Sicherheitsverwaltung und Kennwortkonfiguration

Bei Konfiguration/Empfang von IP-Adressen über DHCP und BOOTP enthält die von diesen Servern empfangene Information die IP-Adresse und sie kann auch die Subnetzmaske und Standard-Gateway enthalten.

---

## Abrufen einer IP-Adresse von einem DHCP-Server

Bei Verwendung des DHCP-Protokolls zum Abruf einer IP-Adresse fungiert das Gerät als DHCP-Client. Bei Rücksetzung des Geräts wird der DHCP-Befehl, nicht jedoch die IP-Adresse, in der Konfigurationsdatei gespeichert. Führen Sie die folgenden Schritte aus, um eine IP-Adresse von einem DHCP-Server abzurufen:

- 1. Wählen Sie und stellen Sie eine Verbindung irgendeines Ports mit einem DHCP-Server oder einem Subnetz, auf dem sich ein DHCP-Server befindet, her, um die IP-Adresse abzurufen.
- 2. Geben Sie die folgenden Befehle ein, um den ausgewählten Port zum Empfang der IP-Adresse auszuwählen. Im folgenden Beispiel beruhen die Befehle auf dem für die Konfiguration verwendeten Porttyp.
  - 1 Zuweisen dynamischer IP-Adressen:

```
Console# configure
```

```
console(config)# interface ethernet g1
```

```
console(config-if)# ip address dhcp hostname device
```

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

```
console(config)#
```

- 1 Zuweisen dynamischer IP-Adressen (auf einem VLAN):

```
Console# configure
```

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

```
console(config-if)# ip address dhcp hostname device
```


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

```
console(config)#
```

3. Geben Sie zur Überprüfung der IP-Adresse an der System-Prompt den Befehl **show ip interface** ein, wie im folgenden Beispiel gezeigt.

Console# <b>show ip interface</b>		
Gateway-IP-Adresse	Aktivitätsstatus	
-----	-----	
10.7.1.1	Active (Aktiv)	
IP-Adresse:	Schnittstelle	Typ
-----	-----	-----
10.7.1.192/24	Vlan 1	static
10.7.2.192/24	VLAN 2	DHCP

 **ANMERKUNG:** Zum Abruf einer IP-Adresse vom DHCP-Server ist es nicht erforderlich, die Gerätekonfiguration zu löschen.

 **ANMERKUNG:** Beim Kopieren von Konfigurationsdateien ist die Verwendung einer Konfigurationsdatei zu vermeiden, die eine Anweisung zur DHCP-Aktivierung auf einer Schnittstelle mit Verbindung zum gleichen DHCP-Server oder einem Server mit identischer Konfiguration enthält. In diesem Fall ruft das Gerät die neue Konfigurationsdatei ab und führt von ihr aus einen Neustart aus. Das Gerät aktiviert dann DHCP gemäß Anweisung in der neuen Konfigurationsdatei und der DHCP weist es an, die gleiche Datei erneut zu laden.

---


## Empfangen einer IP-Adresse von einem BOOTP-Server.

Das Standard-BOOTP-Protokoll wird unterstützt und aktiviert das Gerät zum automatischen Herunterladen seiner IP-Host-Konfiguration von jedem Standard-BOOTP-Server im Netzwerk. In diesem Fall fungiert das Gerät als BOOTP-Client.

Empfangen einer IP-Adresse von einem BOOTP-Server.

1. Wählen Sie und stellen Sie eine Verbindung irgendeines Ports mit einem BOOTP-Server oder einem Subnetz, auf dem sich ein solcher Server befindet, her, um die IP-Adresse abzurufen.
2. Geben Sie an der System-Prompt den Befehl **delete startup configuration** ein, um die Startkonfiguration aus dem Flash-Speicher zu löschen.

Das Gerät wird ohne Konfiguration neu gestartet und beginnt nach 60 Sekunden, BOOTP-Anforderungen auszusenden. Das Gerät erhält die IP-Adresse automatisch.

 **ANMERKUNG:** Nach Beginn des Neustarts des Geräts wird der BOOTP-Prozess durch irgendeine Eingabe am ASCII-Terminal oder über eine Tastatur automatisch abgebrochen und das Gerät erhält keine IP-Adresse vom BOOTP-Server.

Das folgende Beispiel illustriert diesen Prozess:

```
console> enable

console# delete startup-config

Startup file was deleted

console# reload

You haven't saved your changes. Are you sure you want to continue (y/n) [n]?

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

*****

/* the switch reboots */
```

Geben Sie zur Überprüfung der IP-Adresse den Befehl **show ip interface** ein.

Das Gerät ist jetzt mit einer IP-Adresse konfiguriert.

---

## Sicherheitsmanagement und Kennwortkonfiguration

Die Systemsicherheit wird über den AAA-Mechanismus (Authentifizierung, Authorisierung und Abrechnung), mit dem die Benutzerzugriffsrechte, Privilegien und Verwaltungsmethoden verwaltet werden, abgewickelt. AAA verwendet lokale und entfernte Benutzerdatenbanken. Die Datenverschlüsselung erfolgt mit dem SSH-Mechanismus.


Das System wird ohne konfiguriertes Standardkennwort geliefert. Alle Kennwörter sind benutzerdefiniert. Wenn ein benutzerdefiniertes Kennwort verlorengeht, kann ein Verfahren zur Wiederherstellung des Kennwortes im **Startmenü** aufgerufen werden. Das Verfahren gilt nur für den lokalen Terminal und ermöglicht einen einmaligen Zugriff auf das Gerät vom lokalen Terminal ohne Eingabe eines Kennwortes.


---

## Konfigurieren von Sicherheitskennwörtern

Die Sicherheitskennwörter können für die folgenden Dienste konfiguriert werden:

- 1 Terminal
- 1 Telnet
- 1 SSH
- 1 HTTP
- 1 HTTPS

 **ANMERKUNG:** Alle Kennwörter sind benutzerdefiniert.

 **ANMERKUNG:** Bei der Erstellung eines Benutzernamens ist die Standardpriorität 1. Sie überträgt Zugriffs- aber keine Konfigurationsrechte. Eine Priorität von 15 muss eingerichtet werden, um Zugriffs- und Konfigurationsrechte für das Gerät zu übertragen. Obwohl Benutzernamen die Privilegstufe 15 ohne ein Kennwort zugewiesen werden können, wird doch empfohlen, immer ein Kennwort zuzuweisen. Wenn kein Kennwort angegeben ist, können privilegierte Benutzer auf die Web-Schnittstelle ohne ein Kennwort zugreifen.

## Konfigurieren eines anfänglichen Terminal-Kennwortes

Zur Konfiguration eines anfänglichen Terminal-Kennwortes geben Sie die folgenden Befehle ein:

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line console
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password george
```

- 1 Wenn Sie sich erstmals über eine Terminal-Session bei einem Gerät anmelden, geben Sie an der Kennwort-Eingabeaufforderung **george** ein.
- 1 Wenn Sie den Modus eines Geräts auf „aktiviert“ abändern, geben Sie an der Kennwort-Eingabeaufforderung **george** ein.

## Konfigurieren eines anfänglichen Telnet-Kennwortes

Zur Konfiguration eines anfänglichen Telnet-Kennwortes geben Sie die folgenden Befehle ein:

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line telnet
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password bob
```

- 1 Wenn Sie sich erstmals über eine Telnet-Session bei einem Gerät anmelden, geben Sie an der Kennwort-Eingabeaufforderung **bob** ein.
- 1 Wenn Sie den Gerätestatus auf „aktiviert“ abändern, geben Sie **bob** ein.

## Konfigurieren eines anfänglichen SSH-Kennwortes

Zur Konfiguration eines anfänglichen SSH-Kennwortes geben Sie die folgenden Befehle ein:

```
console(config)# aaa authentication login default line
```

```
console(config)# aaa authentication enable default line
```

```
console(config)# line ssh
```

```
console(config-line)# login authentication default
```

```
console(config-line)# enable authentication default
```

```
console(config-line)# password jones.
```

- 1 Wenn Sie sich erstmals über eine SSH-Session bei einem Gerät anmelden, geben Sie an der Kennwort-Eingabeaufforderung `jones` ein.
- 1 Wenn Sie den Gerätemodus auf „aktiviert“ abändern, geben Sie `jones` ein.

## Konfigurieren eines anfänglichen HTTP-Kennwortes

Zur Konfiguration eines anfänglichen HTTP-Kennwortes geben Sie die folgenden Befehle ein:

```
console(config)# ip http authentication local
```

```
console(config)# username admin password user1 level 15
```


## Konfigurieren eines anfänglichen HTTPS-Kennwortes

Zur Konfiguration eines anfänglichen HTTPS-Kennwortes geben Sie die folgenden Befehle ein:

```
console(config)# ip https authentication local
```

```
console(config)# username admin password user1 level 15
```


Geben Sie die folgenden Befehle einmal ein, wenn Sie eine Konfiguration zur Verwendung einer Terminal-, Telnet- oder SSH-Session durchführen, um eine HTTPS-Session zu verwenden.

 **ANMERKUNG:** Aktivieren Sie im Web-Browser SSL 2.0 oder höher, damit der Seiteninhalt angezeigt werden kann.

```
console(config)# crypto certificate generate key_generate
```

```
console(config)# ip https server
```

Geben Sie bei der erstmaligen Aktivierung einer http- oder https-Session `admin` als Benutzernamen und `user1` als Kennwort ein.

 **ANMERKUNG:** Http- und Https-Dienste erfordern Zugriffslevel 15 und sind direkt mit dem Zugriff auf Konfigurationsstufe verbunden.

---

## Startanweisungen



## Verfahren des Startmenüs

Die vom Startmenü aufgerufenen Verfahren umfassen Software-Download, Flash-Handhabung und Kennwort-Wiederherstellung. Die Diagnoseverfahren sind für das technische Kundendienstpersonal reserviert und werden nicht im Dokument bekanntgegeben.

Das Startmenü kann beim Start des Geräts aufgerufen werden - dazu muss sofort nach dem POST-Test eine Benutzereingabe erfolgen.

So wird das Startmenü aufgerufen:

1. Schalten Sie das Gerät ein und warten Sie auf die Auto-Boot-Meldung.

\*\*\*\*\*

\*\*\*\*\* SYSTEM RESET \*\*\*\*\*

\*\*\*\*\*

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

UART Channel Loopback Test.....PASS

Testing the System SDRAM.....PASS

Boot1 Checksum Test.....PASS

Boot2 Checksum Test.....PASS

Flash Image Validation Test.....PASS

BOOT Software Version 1.0.0.20 Built 22-Jan-2004 15:09:28

Processor: FireFox 88E6218 ARM946E-S , 64 MByte SDRAM.

I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.

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

Preparing to decompress...

2. Drücken Sie, wenn die Auto-Boot-Meldung erscheint, die <Eingabetaste>, um das Startmenü aufzurufen. Die Startmenüverfahren können vom ASCII-Terminal oder Windows HyperTerminal erfolgen.

[1] Download Software (Software herunterladen)

[2] Erase Flash File (Flash-Datei löschen)

[3] Password Recovery Procedure (Kennwort-Wiederherstellung)


[4] Enter Diagnostic Mode (Diagnosemodus aufrufen)

[5] Set Terminal Baud-Rate (Terminal-Baudrate einstellen)

[6] Back (Zurück)

Enter your choice or press 'ESC' to exit (Geben Sie Ihre Wahl ein oder drücken Sie ESC um zu beenden)

In den folgenden Abschnitten werden die möglichen Startmenüoptionen beschrieben.

 **ANMERKUNG:** Bei der Auswahl einer Option im Startmenü ist das Zeitlimit zu beachten: Wenn nicht innerhalb von 35 Sekunden (Standard) eine Auswahl getroffen wird, tritt Zeitabschaltung ein. Dieser Standardwert kann über das CLI geändert werden.

## Download Software (Software herunterladen)


Das Software-Download-Verfahren wird durchgeführt, wenn eine neue Version als Ersatz beschädigter Dateien oder zur Aktualisierung bzw. Upgrade der Systemsoftware heruntergeladen werden muss. So wird Software im Startmenü heruntergeladen:

1. Wählen Sie [1] aus dem Startmenü. Daraufhin erscheint die folgende Prompt:

Downloading code using XMODEM

2. Wenn Sie HyperTerminal verwenden, klicken Sie auf **Transfer** auf der HyperTerminal Menüleiste.
3. Geben Sie im Feld **Filename** den Dateipfad für die Datei ein, die Sie herunterladen wollen.
4. Stellen Sie sicher, dass im Feld **Protocol** das Xmodem-Protokoll ausgewählt ist.
5. Wählen Sie **Send**. Die Software wird geladen.

 **ANMERKUNG:** Nachdem die Software heruntergeladen wurde, wird das Gerät automatisch neu gestartet.

 **ANMERKUNG:** Die Download-Dauer hängt von dem verwendeten Tool ab.

## Erase Flash File (Flash-Datei löschen)

In manchen Fällen muss die Gerätekonfiguration gelöscht werden. Wenn die Konfiguration gelöscht wird, müssen alle über CLI, EWS oder SNMP konfigurierten Parameter neu konfiguriert werden.

## Löschen der Gerätekonfiguration

1. Wählen Sie innerhalb von 2 Sekunden im Startmenü [2], um die Flash-Datei zu löschen. Die folgende Meldung erscheint:

Warning! About to erase a Flash file.

Are you sure (Y/N)? y

2. Drücken Sie auf Y. Die folgende Meldung wird angezeigt.

Write Flash file name (Up to 8 characters, Enter for none.):config

File config (if present) will be erased after system initialization

=====  
Press Enter To Continue  
=====

3. Geben Sie als Namen der Flash-Datei config ein. Die Konfiguration wird gelöscht und das Gerät wird neu gestartet.
4. Führen Sie die anfängliche Gerätekonfiguration erneut durch.

## Password Recovery (Kennwort-Wiederherstellung)

Wenn ein Kennwort verlorengeht, kann das Verfahren zur Wiederherstellung des Kennwortes im Startmenü aufgerufen werden. Das Verfahren ermöglicht den Zugang zum Gerät ohne Kennwort.

Wiederherstellung eines verlorenen Kennwortes nur für den lokalen Terminal:

1. Geben Sie im Startmenü 3 ein und drücken Sie die <Eingabetaste>.

Das Kennwort wird gelöscht.

 **ANMERKUNG:** Konfigurieren Sie die Kennwörter für die anwendbaren Verwaltungsmethoden neu, um die Sicherheit des Geräts zu gewährleisten.

## Software-Download über TFTP-Server

Dieser Abschnitt enthält eine Anleitung zum Herunterladen von Gerätesoftware (System- und Boot-Images) über einen TFTP-Server. Der TFTP-Server muss vor Beginn des Software-Downloadverfahrens konfiguriert werden.

### Herunterladen des System-Image

Das Gerät startet und wird betrieben, wenn das System-Image vom Flash-Speicherbereich, wo eine Kopie des System-Image gespeichert ist, dekomprimiert wird. Wenn ein neues Image heruntergeladen wird, wird es in dem anderen Bereich, der für die andere System-Image-Kopie reserviert ist, gespeichert.

Beim nächsten Start wird das derzeit aktive System-Image dekomprimiert und ausgeführt, wenn nicht ein anderes ausgewählt wird.

Herunterladen eines System-Image über den TFTP-Server:

1. Stellen Sie sicher, dass eine IP-Adresse auf einem der Geräteports konfiguriert ist und Pings an einen TFTP-Server übertragen werden können.

2. Stellen Sie sicher, dass die herunterzuladende Datei auf dem TFTP-Server (die .ros Datei) gespeichert wird.
3. Geben Sie „Show Version“ ein, um zu verifizieren, welche Softwareversion gegenwärtig auf dem System betrieben wird. Das folgende Beispiel illustriert die Informationen, die angezeigt werden:

```
console# show version

SW version 1.0.0.42 (date 22-Jul-2004 time 13:42:41)

Boot version 1.0.0.18 (date 01-Jun-2004 time 15:12:20)

HW version
```

4. Geben Sie „show bootvar“ ein, um zu verifizieren, welches System-Image gegenwärtig aktiv ist. Das folgende Beispiel illustriert die Informationen, die angezeigt werden:

```
console# sh bootvar

Images currently available on the Flash

Image-1 active (selected for next boot)

Image-2 not active

console#
```

5. Geben Sie copy tftp://{tftp address}/{file name} image ein, um ein neues System-Image auf das Gerät zu kopieren. Wenn das neue Image heruntergeladen wird, wird es in dem Bereich gespeichert, der für die andere Kopie des System-Image (image-2, wie im Beispiel angegeben) reserviert ist. Das folgende Beispiel illustriert die Informationen, die angezeigt werden:

```
console# copy tftp://176.215.31.3/file1.ros image

Accessing file `file1' on 176.215.31.3
Loading file1 from 176.215.31.3:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy took 00:01:11 [hh:mm:ss]
```

Die Ausrufezeichen zeigen an, dass ein Kopierprozess abläuft. Jedes Symbol (!) entspricht 512 Bytes, die erfolgreich übertragen wurden. Ein Punkt zeigt an, dass eine Zeitüberschreitung beim Kopierprozess eingetreten ist. Viele Punkte hintereinander zeigen an, dass der Kopierprozess fehlgeschlagen ist.

6. Wählen Sie das Image für den nächsten Start, indem Sie den Start-Systembefehl eingeben. Geben Sie im Anschluss „show bootvar“ ein, um zu überprüfen, dass die als Parameter im Start-Systembefehl angegebene Kopie für den nächsten Startvorgang ausgewählt ist.

Das folgende Beispiel illustriert die Informationen, die am Bildschirm angezeigt werden:

```
console# boot system image-2

console# sh boot

Images currently available on the Flash

Image-1 active

Image-2 not active (selected for next boot)
```

Wenn das Image für den nächsten Startvorgang nicht durch Eingabe des Befehls boot system ausgewählt wird, startet das System vom gegenwärtig aktiven Image.

7. Geben Sie den Befehl „reload“ ein. Die folgende Meldung erscheint:

```
console# reload

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

8. Geben Sie Y ein. Daraufhin wird das Gerät neu gestartet.

## Herunterladen des Start-Image

Das Laden eines neuen Start-Image vom TFTP-Server und dessen Programmierung im Flash aktualisiert das Start-Image. Das Start-Image wird beim Einschalten des Gerätes geladen. Ein Benutzer hat keine Kontrolle über die Start-Image-Kopien. Herunterladen eines Start-Image über den TFTP-



[Zurück zum Inhaltsverzeichnis](#)

## Glossar

Dell™ PowerConnect™ 5324 System-Benutzerhandbuch

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [Z](#)

Dieses Glossar enthält wichtige technische Begriffe.

---

### A

#### Abfrage

Extrahiert Informationen aus einer Datenbank und präsentiert diese zur Verwendung.

#### Aggregiertes VLAN

Gruppert mehrere VLANs in einem einzigen aggregierten VLAN. Die VLAN-Aggregation ermöglicht Routern, auf ARP-Anfragen für Knoten zu reagieren, die sich in verschiedenen Sub-VLANs befinden, die zum gleichen Super-VLAN gehören. Router antworten mit ihren MAC-Adressen.

#### ARP

Address Resolution Protocol. ARP ist ein TCP/IP-Protokoll, das IP-Adressen in physische Adressen konvertiert.

#### ASIC

Anwendungsspezifische integrierte Schaltung. Ein für eine bestimmte Anwendung speziell entwickelter Chip.

#### Asset Tag (Systemkennnummer)

Gibt die benutzerdefinierte Geräteferenz an.

#### Authentifizierungsprofile

Satz von Regeln, die Anmeldung und Authentifizierung von Benutzern und Anwendungen ermöglichen.

#### Auto-Negotiation (Automatische Verhandlung)

Ermöglicht die Einrichtung von 10/100 Mbps oder 10/100/1000 Mbps Ethernet-Ports für die folgenden Funktionen:

- 1 Duplex/Halbduplex-Modus
  - 1 Datenflusssteuerung
  - 1 Geschwindigkeit
- 

### B

### **Backup-Konfigurationsdateien**

Enthält eine Backup-Kopie zur Sicherung der Gerätekonfiguration. Die Sicherungsdatei wird geändert, wenn die Konfigurationsdatei ausgeführt wird oder die Startdatei in die Sicherungsdatei kopiert wird.

### **Bandbreite**

Die Bandbreite gibt die Datenmenge an, die in einer festgelegten Zeitspanne übertragen werden kann. Bei digitalen Geräten wird die Bandbreite in Bits pro Sekunde (bps) oder Bytes pro Sekunde angegeben.

### **Bandbreitenzuweisungen**

Der Bandbreiten-Umfang, der einer bestimmten Anwendung, Benutzer und/oder Schnittstelle zugewiesen wird.

### **Baud**

Die Anzahl der Signalelemente, die pro Sekunde übertragen werden.

### **Best Effort**

Der Datenverkehr wird in die Warteschlange mit der geringsten Priorität relegiert, und die Datenpaketzustellung ist nicht garantiert.

### **Bilddatei (Image-Datei)**

System-Images werden in zwei Flash-Sektoren, die als Images (Image 1 und Image 2) bezeichnet werden, gespeichert. Das aktive Image speichert die aktive Kopie, und das andere Image speichert eine zweite Kopie.

### **BootP**

BOOTP (Bootstrap-Protokoll) ermöglicht einer Workstation die Erkennung ihrer IP-Adresse, einer IP-Adresse auf einem BootP-Server in einem Netzwerk, oder einer Konfigurationsdatei, die im Startverzeichnis eines Geräts geladen ist.

### **BPDU**

Bridge Protocol Data Unit. Stellt Bridge-Informationen in Meldungsformat bereit. BPDUs werden über Geräteinformationen hinweg innerhalb von Spanning-Tree-Konfigurationen übertragen. BPDU-Pakete enthalten Informationen zu Ports, Adressen, Prioritäten und Weiterleitungskosten.

### **Bridge**

Ein Gerät, das zwei Netzwerke verbindet. Bridges sind hardware-spezifisch, aber protokollunabhängig. Bridges werden auf Layer-1 und Layer-2-Ebene betrieben.

### **Broadcast-Domäne**

Geräte-Sets, die Broadcast-Frames erhalten, die von irgendeinem Gerät innerhalb eines spezifizierten Sets ausgehen. Router verbinden Broadcast-Domänen, weil sie keine Broadcast-Frames weiterleiten.

### **Broadcasting**

Eine Methode der Übertragung von Datenpaketen an alle Ports in einem Netzwerk.

#### **Broadcast-Storm**

Eine Übermenge an Broadcast-Meldungen, die gleichzeitig über ein Netzwerk von einem einzigen Port übertragen werden. Das Netzwerk wird mit weitergeleiteten Antworten auf Meldungen überhäuft, was eine Überlastung von Netzwerkressourcen oder Überschreitung von Timelimits im Netzwerk zur Folge hat.

Weitere Informationen zu Broadcast-Storms finden Sie unter [„Definieren von LAG-Parametern“](#).

---

## **C**

#### **CDB**

Configuration Data Base (Konfigurationsdatenbank). Eine Datei, die die Konfigurationsinformationen eines Geräts enthält.

#### **Class of Service**

5:11 PM 6/9/2004 Class of Service ist der 802.1p-Prioritätsplan. CoS stellt eine Methode zur Kennung (Tagging) von Datenpaketen mit Prioritätsinformationen bereit. Ein CoS-Wert zwischen 0-7 wird dem Layer-II-Kopf von Paketen hinzugefügt. Dabei bedeutet Null die niedrigste und 7 die höchste Priorität.

#### **CLI**

Command Line Interface (Befehlszeilen-Schnittstelle). Ein Befehlszeilensatz zur Konfiguration des Systems. Weitere Informationen zur CLI-Verwendung finden Sie unter „Verwenden der CLI-Befehle“.

#### **Communities**

Gibt eine Gruppe von Benutzern mit den gleichen Systemzugriffsrechten an.

#### **CPU**

Central Processing Unit (Zentrale Verarbeitungseinheit). Der Teil des Computers, der Informationen verarbeitet. CPUs bestehen aus einer Kontrolleinheit und einer ALU.

---

## **D**

#### **Datenflusssteuerung**

Datenflusssteuerung ermöglicht Geräten mit niedrigerer Geschwindigkeit die Kommunikation mit Geräten höherer Geschwindigkeit, indem das Gerät mit der höheren Geschwindigkeit davon absieht, Pakete zu schicken.

#### **Datenpakete**



Informationsblöcke zur Übertragung in Packet-Switched-Systemen.

#### **DHCP-Client**

Ein Internet-Host, der DHCP verwendet, um Konfigurationsparameter zu erhalten, z.B. eine Netzwerkadresse.

#### **Domäne**

Eine Gruppe von Computern und Geräten in einem Netzwerk, die als eine Einheit mit gemeinsamen Regeln und Prozeduren verwaltet wird.

#### **DSCP**

DiffServe Code Point (DSCP). DSCP stellt eine Methode zur Kennung (Tagging) von IP-Datenpaketen mit QoS-Prioritätsinformationen bereit.

#### **Duplexmodus**

Ermöglicht simultane Übertragung und Empfang von Daten. Es gibt zwei Arten des Duplexmodus:

- 1 **Vollduplexmodus** — Ermöglicht bisynchrone Kommunikation, z.B. Telefon. Zwei Parteien können gleichzeitig Informationen übermitteln.
  - 1 **Halbduplexmodus** — Ermöglicht asynchrone Kommunikation, z.B. ein Walkie-Talkie (Kleinfunksprechgerät). Nur eine Partei kann jeweils Informationen übermitteln.
- 

## **E**

#### **Egress-Ports (Ausgangsports)**

Ports, von denen Netzwerkdatenverkehr übertragen wird.

#### **Endsystem**

Ein Endbenutzergerät in einem Netzwerk.

#### **Ethernet**

Ethernet ist gemäß IEEE 802.3 standardisiert. Ethernet ist der am häufigsten implementierte LAN-Standard. Unterstützung von Mbps-Datenübertragungsraten, wobei 10, 100 oder 1000 Mbps unterstützt werden.

#### **EWS**

Embedded Web-Server. Stellt Geräteverwaltung über einen Standard-Web-Browser bereit. Embedded Web-Server werden zusätzlich zu oder anstelle von CLI oder NMS verwendet.

---

## **F**

## FFT

Fast Forward Table. Stellt Informationen über Weiterleitungs-Routen bereit. Wenn ein Paket an einem Gerät mit einer bekannten Route (Strecke) eintrifft, wird das Paket über eine in der FFT aufgeführten Route weitergeleitet. Wenn keine Route bekannt ist, leitet die CPU das Datenpaket weiter und aktualisiert die FFT.

## FIFO

First In First Out. Ein Warteschlangenprozess, bei dem das erste in der Warteschlange eingereichte Paket als erstes aus der Warteschlange herauskommt.

## Flapping (ständiger Wechsel)

Flapping tritt auf, wenn ein Schnittstellenzustand ständig wechselt. Zum Beispiel ein STP-Port wechselt ständig zwischen Überwachen und Erfassen und Weiterleiten. Das kann Verlust von Datenverkehr verursachen.

## Fragment

Ethernet-Pakete von einer Größe unter 576 Bits.

## Frame

Datenpakete mit den Kopf- und Nachlaufinformationen, die vom physischen Medium benötigt werden.

---

## G

### GARP

General Attributes Registration Protocol. Dient zur Registrierung von Client-Stationen in einer Multicast-Domäne.

### Gigabit Ethernet

Gigabit-Ethernet arbeitet mit einer Übertragungsrates von 1000 Mbps und ist kompatibel mit bestehenden 10/100 Mbps- Ethernetstandards.

### GVRP

GARP VLAN Registration Protocol. Dient zur Registrierung von Client-Stationen in VLANs.

---

## H

### HOL

Head of Line. Datenpakete werden in Warteschlangen eingereiht. Pakete am Kopf der Warteschlange werden vor denen am Ende der Warteschlange

weitergeleitet.

## **Host**

Ein Computer, der für andere Computer als Informations- oder Dienstquelle fungiert.

## **HTTP**

HyperText Transport Protocol. Überträgt HTML-Dokumente zwischen Servern und Clients im Internet.

---

## **I**

## **IC**

Integrated Circuit (Integrierte Schaltung). Integrierte Schaltungen sind kleine elektronische Komponenten, die aus Halbleitermaterial bestehen.

## **ICMP**

Internet Control Message Protocol. Ermöglicht dem Gateway- oder Zielhost, mit einem Quellhost zu kommunizieren, z.B. um einen Verarbeitungsfehler zu melden.

## **IEEE**

Institute of Electrical and Electronics Engineers (Vereinigung der amerikanischen Elektro- und Elektronikingenieure). Eine Ingenieurvereinigung, die Kommunikations- und Netzwerkstandards entwickelt.

## **IEEE 802.1d**

Das im Spanning Tree-Protokoll verwendete IEEE 802.1d unterstützt MAC-Bridging, um Netzwerkschleifen zu verhindern.

## **IEEE 802.1p**

Priorisiert Netzwerk-Datenverkehr am Data-link/MAC-Sublayer.

## **IEEE 802.1Q**

Definiert den Betrieb von VLAN-Bridges, die die Definition, den Betrieb und die Verwaltung von VLANs innerhalb von Bridged-LAN-Infrastrukturen gestatten.

## **Ingress-Port (Eingangsport)**

Ports, von denen Netzwerkdatenverkehr übertragen wird.

## **IP**

Internet Protocol (Internet-Protokoll). Spezifiziert das Format von Paketen und ihre Adressierungsmethode. IP adressiert Pakete und leitet die Pakete an den richtigen Port weiter.

#### **IP-Adresse**

Internet-Protokoll(IP)-Adresse. Eine eindeutige Adresse, die einem Netzwerkgerät mit zwei oder mehreren untereinander verbundenen LANs oder WANs zugewiesen wird.

#### **IPX**

Internetwork Packet Exchange (Netzüberschreitender Datenpaketaustausch). Überträgt verbindungslose Kommunikationen.

---

## **J**

#### **Jumbo-Frames**

Jumbo-Frames ermöglichen die Übertragung von identischen Daten in weniger Frames. Jumbo-Frames reduzieren die Restkapazität und Verarbeitungszeit und sorgen für weniger Interrupts.

---

## **K**

#### **Knoten**

Ein Netzwerkverbindungs-Endpunkt oder eine gemeinsame Verbindungsstelle für mehrere Netzwerkleitungen. Knoten umfassen:

- 1 Prozessoren
- 1 Controller
- 1 Workstations

#### **Kombinations-Ports**

Ein logischer Port mit zwei physischen Anschlüssen, einschließlich ein RJ-45- und ein SFP-Anschluss.

---

## **L**

#### **LAG**

Link Aggregated Group. Zusammenschluss von Ports oder VLANs in einem einzigen virtuellen Port oder VLAN.

Weitere Informationen zu LAGs finden Sie unter **Definition von LAG-Zugehörigkeit**.

#### **LAN**

Local Area Networks. Ein Netzwerk, das auf einen Raum, Gebäude, Gelände oder sonstigen beschränkten geografischen Bereich beschränkt ist.

## Layer 2

Data-Link-Layer oder MAC-Layer. Enthält die physische Adresse eines Client oder einer Server-Station. Layer-2-Verarbeitung ist schneller als Layer-3-Verarbeitung, weil es weniger Informationen zu verarbeiten gibt.

## Layer 4

Stellt eine Verbindung her und stellt sicher, dass alle Daten an ihrem Ziel ankommen. Die auf Layer-4 kontrollierten Daten werden analysiert und die Weiterleitungsentscheidungen basieren auf ihren Anwendungen.

## Load Balancing (Lastverteilung)

Ermöglicht die gleichmäßige Verteilung von Daten- und/oder Verarbeitungspaketen auf die verfügbaren Netzwerkressourcen. Zum Beispiel kann Load-Balancing die eingehenden Pakete gleichmäßig auf alle Server verteilen oder die Pakete zum nächsten verfügbaren Server weiterleiten.

---

# M

## MAC-Adresse

Media Access Control-Adresse. Die MAC-Adresse ist eine hardware-spezifische Adresse, die jeden Netzwerkknoten identifiziert.

## MAC-Adressenlernen

MAC-Adressenlernen bezeichnet eine Lernbrücke, in der die MAC-Quelladresse des Pakets aufgezeichnet wird. Pakete, die für die Adresse bestimmt sind, werden nur an die Brückenschnittstelle weitergeleitet, auf der sich diese Adresse befindet. Pakete, die an unbekannte Adressen gerichtet sind, werden an jede Brückenschnittstelle weitergeleitet. MAC-Adressenlernen reduziert den Datenverkehr auf den verbundenen LANs.

## MAC-Layer

Ein Sublayer des Data Link Control (DTL)-Layers.

## MD5

Message Digest 5. Ein Algorithmus, der einen 128-Bit-Hash produziert. MD5 ist eine Variante von MD4 und erhöht die MD4-Sicherheit. MD5 verifiziert die Integrität der Kommunikation und authentifiziert den Ursprung der Kommunikation.

## MDI

Media Dependent Interface (medienabhängige Schnittstelle). Ein Kabel zur Verwendung für Endstationen.

## MDIX

Media Dependent Interface with Crossover (MDIX). Ein Kabel zur Verwendung mit Hubs und Schaltern.

## **MIB**

Management Information Base (Managementinformationsbasis). MIBs enthalten Informationen, die spezielle Aspekte von Netzwerkkomponenten beschreiben.

## **Multicast**

Überträgt Kopien eines einzelnen Datenpakets an mehrere Ports.

---

## **N**

### **NMS**

Network Management System. Eine Schnittstelle, die eine Methode zur Verwaltung eines Systems bereitstellt.

---

## **O**

### **OID**

Object Identifier (OID, Objektbezeichner). Wird von SNMP zur Identifikation von verwalteten Objekten verwendet. Im SNMP Manager/ Agent-Netzwerkverwaltungsparadigma muss jedes verwaltete Objekt eine dieses Objekt kennzeichnende OID besitzen.

---

## **P**

### **PDU**

Protocol Data Unit (Protokolldateneinheit). Eine in einem Layer-Protokoll spezifizierte Dateneinheit, die aus Protokoll-Kontrollinformationen und Layer-Benutzerdaten besteht.

### **PING**

Packet Internet Groper (Paketorientierter Internet-Taster). Überprüft, ob eine bestimmte IP-Adresse verfügbar ist. Ein Paket wird an eine andere IP-Adresse geschickt und wartet auf eine Antwort.

### **Port**

Physische Ports stellen Anschlusskomponenten dar, die es Mikroprozessoren ermöglichen, mit Peripheriegeräten zu kommunizieren.

### **Port-Geschwindigkeit**

Gibt die Geschwindigkeit des Ports an. Port-Geschwindigkeiten umfassen:

- 1 Ethernet 10 Mbps
- 1 Fast Ethernet 100Mbps
- 1 Gigabit Ethernet 1000 Mbps

### **Port-Mirroring (Port-Spiegelung)**

Port-Spiegelung überwacht und spiegelt Netzwerk-Datenverkehr durch Weiterleitung von Kopien der eingehenden und ausgehenden Pakete von einem überwachten Port zu einem Überwachungsport.

Weitere Informationen zur Port-Spiegelung finden Sie unter **Definieren von Port-Spiegelungssitzungen**.

### **Protokoll**

Ein Satz von Regeln, die festlegen, wie Geräte Informationen in Netzwerken austauschen.

---

## **Q**

### **QoS**

Quality of Service (Servicequalität). QoS ermöglicht Netzwerkverwaltern gemäß Prioritäten, Anwendungsarten und Quell- und Zieladressen zu entscheiden, welcher Netzwerkverkehr wie weitergeleitet wird.

---

## **R**

### **RADIUS**

Remote Authentication Dial-In User Service. Eine Methode zur Authentifizierung von Systembenutzern und Verfolgung von Verbindungszeiten.

### **RMON**

Remote Monitoring (Fernüberwachung). Stellt Netzwerkinformationen zur Erfassung durch eine Einzelworkstation bereit.

### **Router**

Ein Gerät, das mit separaten Netzwerken verbunden ist. Router leiten Datenpakete zwischen zwei oder mehreren Netzwerken weiter. Router arbeiten auf der Layer-3-Ebene.

### **RSTP**

Rapid Spanning Tree-Protokoll (RSTP). Erfasst und verwendet Netzwerktopologien, um eine schnellere Konvergierung des Spanning-Tree zu ermöglichen, ohne dass Weiterleitungsschleifen gebildet werden.

### **Running-Configuration-Datei**

Enthält alle Startdateibefehle sowie alle Befehle, die in der aktuellen Session eingegeben wurden. Nach Ausschalten oder Neustart des Geräts gehen alle Befehle, die in der Running-Configuration-Datei gespeichert sind, verloren.

---

## S

### Schalter

Filtert und leitet Datenpakete zwischen LAN-Segmenten weiter. Schalter unterstützen jeden Paketprotokolltyp.

### Segmentierung

Teilt LANs in separate LAN-Segmente für Bridging und Routing auf. Segmentierung eliminiert LAN-Bandbreitenbeschränkungen.

### Server

Ein zentraler Computer, der Dienste für andere Computer im Netzwerk bereitstellt. Zu diesen Diensten gehören Dateispeicherung und Zugriff auf Anwendungen.

### SNMP

Simple Network Management Protocol (Einfaches Netzwerk-Verwaltungsprotokoll). Verwaltet LANs. SNMP-basierte Software kommuniziert mit Netzwerkgeräten mit Embedded-SNMP-Agenten. SNMP-Agenten sammeln die Netzwerkaktivitäts- und Gerätestatusinformationen und senden sie an eine Workstation zurück.

### SNTP

Simple Network Management Protocol (Einfaches Netzwerk-Verwaltungsprotokoll). SNTP stellt die genaue Netzwerksschalter-Zeitsynchronisierung bis auf die Millisekunde sicher.

### SoC

System-on-a-Chip. Ein ASIC (Application Specific Integrated Circuit), der ein gesamtes System enthält. Zum Beispiel kann eine Telekommunikations-SoC-Anwendung einen Mikroprozessor, digitalen Signalprozessor, RAM, und ROM enthalten.

### Spanning Tree-Protokoll

Verhindert Schleifen im Netzwerkverkehr. Das Spanning Tree-Protokoll (STP) stellt eine Baumstruktur-Topografie für jede Brückenordnung bereit. STP stellt einen Pfad zwischen Endstationen im Netzwerk bereit und eliminiert so Schleifen.

### SSH

Meldet sich an einem Remote-Computer über ein Netzwerk an, führt Befehle aus und überträgt Dateien von einem Computer zum anderen.

### Startkonfiguration

Behält die genaue Gerätekonfiguration bei, wenn das Gerät ausgeschaltet und neu gestartet wird.



### **Startversion**

Die Startversion.

### **Subnet Mask (Subnetzmaske)**

Dient zur Maskierung aller oder eines Teils einer IP-Adresse, die in einer Subnetzadresse verwendet wird.

### **Subnetz**

Subnetzwerk. Subnetze sind Teile von Netzwerken, die einen gemeinsamen Adressenkomponenten haben. In TCP/IP-Netzwerken sind Geräte mit gemeinsamem Präfix Bestandteil des gleichen Subnetzes. Zum Beispiel gehören alle Geräte mit dem Präfix 157.100.100.100 dem gleichen Subnetz an.

---

## **T**

### **TCP/IP**

Transmissions Control-Protokoll. Ermöglicht die Kommunikation und den Austausch von Datenströmen zwischen zwei Hosts. TCP garantiert die Paketzustellung und garantiert, dass die Pakete in der Absende-Reihenfolge übertragen und empfangen werden.

### **Telnet**

Terminal-Emulation-Protokoll. Ermöglicht den Systembenutzern, sich auf Remote-Netzwerken anzumelden und deren Ressourcen zu verwenden.

### **TFTP**

Trivial File Transfer-Protokoll. Verwendet User Data-Protokoll (UDP) ohne Sicherheitsfunktionen zur Dateiübertragung.

### **Trap (Ereignismeldung)**

Eine vom SNMP versandte Meldung über das Auftreten eines Systemereignisses.

### **Trunking**

Link-Aggregation. Optimiert die Portausnutzung durch Verknüpfung einer Gruppe von Ports, so dass sie einen einzigen Trunk (aggregierte Gruppe) bilden.

---

## **U**

### **UDP**

User Data Protocol (Benutzerdatenprotokoll). Überträgt Pakete, ohne ihre Zustellung zu garantieren.

## Unicast

Eine Form des Routing, die einem Benutzer ein Paket überträgt.

---

## V

### VLAN

Virtual Local Area Network (Virtuelles Lokales Netzwerk). Logische Untergruppen innerhalb eines Local Area Network (LAN), die über Software hergestellt wurden (und keine Hardware-Lösung bezeichnen).

---

## W

### WAN

Wide Area Networks (WAN). Netzwerke, die ein großes geografisches Gebiet überspannen.

### Wildcard-Maske

Gibt an, welche IP-Adressen-Bits verwendet und welche ignoriert werden. Die Wildcard-Maske 255.255.255.255 zeigt an, dass kein Bit wichtig ist. Die Wildcard 0.0.0.0 zeigt an, dass alle Bits wichtig sind.

Wenn zum Beispiel die IP-Zieladresse 149.36.184.198 ist und die Wildcard-Maske 255.36.184.00 ist, werden die ersten beiden Bits der IP-Adresse verwendet und die letzten beiden ignoriert.

---

## Z

### Zugriffsmodus

Gibt die Methode an, mit der Benutzern Zugriff auf das System gewährt wird.

### Zugriffsprofile

Ermöglicht Netzwerkverwaltern die Definition von Profilen und Regeln zum Zugriff auf das Gerät. Der Zugriff auf Verwaltungsfunktionen kann auf Benutzergruppen beschränkt werden, die nach den folgenden Kriterien definiert werden:

- 1 Eingangsschnittstellen
- 1 Quell-IP-Adressen und/oder Quell-IP-Subnetze

### Zurückweisung (Backpressure)

Ein im Halbduplexmodus verwendeter Mechanismus, der es ermöglicht, dass ein Port keine Meldung erhält.

### Rückwandplatine

Der Haupt-Bus, der Informationen im Gerät befördert.

---

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Beschreibung der Hardware:

Dell™ PowerConnect™ 5324 System-Benutzerhandbuch

- [Konfigurationen der Geräteports](#)
- [Abmessungen](#)
- [LED-Definitionen](#)
- [Hardware-Komponenten](#)

## Konfigurationen der Geräteports

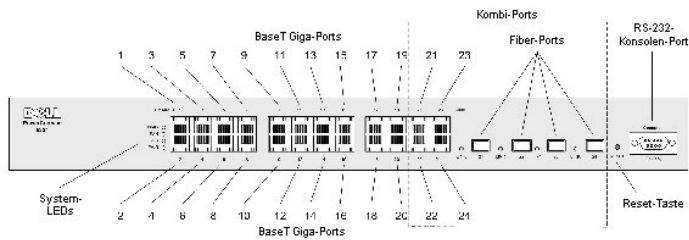
### Beschreibung der Ports an der Frontblende des PowerConnect 5324

Das PowerConnect 5324 Gerät ist mit den folgenden Ports konfiguriert:

- 1 24 Kupferports — RJ-45-Ports, ausgewiesen als 10/100/1000 BaseT Gigabit Ethernet-Ports
- 1 4 Fiber-Ports — ausgewiesen als Gigabit-Ports
- 1 Terminalport — konsolenbasierte RS-232-Port

Die folgende Abbildung zeigt die Frontblende des PowerConnect 5324.

Abb. 2-3. PowerConnect 5324 Frontblende



Auf der Frontblende befinden sich Ports 1-24, bei welchen es sich um kupferbasierte RJ-45-Ports handelt, die als 10/100/1000 Mbps ausgewiesen sind und Halb- und Voll duplexmodi unterstützen. Es gibt auch vier SFP-Fiber-Ports, die als Kombi-Ports 21-24 ausgewiesen sind. Ein Kombi-Port ist ein einzelner logischer Port mit zwei physischen Anschlüssen. Nur ein physischer Anschluss kann jeweils aktiv sein, d.h. entweder die Kupfer-Ports oder die äquivalenten Fiber-Ports 21-24 können aktiv sein, aber nicht beide gleichzeitig. Die obere Port-Reihe ist durch ungerade Zahlen 1-23 und die untere Port-Reihe ist mit geraden Zahlen 2-24 identifiziert.

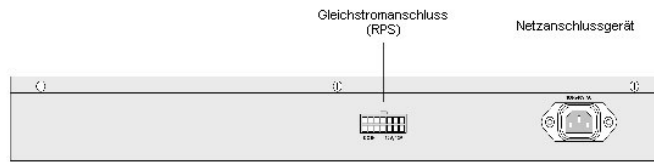
Auf der Frontblende befindet sich eine RS-232-Konsolen-Port, alle Geräte-LEDs und eine Reset-Taste, die zur manuellen Rücksetzung des Geräts dient.

Das Gerät erkennt automatisch, ob das an einer RJ-45-Port angeschlossene Kabel ein gekreuztes oder ein ungekreuztes Kabel ist; mit beiden ist die Funktion möglich.

### Beschreibung der Ports auf der Rückseite des PowerConnect

Auf der Rückseite des Geräts befinden sich die Netzanschlüsse, wie in [Abb. 2-4](#) gezeigt.

Abb. 2-4. Rückseite des Geräts



Auf der Rückseite befinden sich zwei Netzanschlüsse. Es gibt einen Wechselstromanschluss zur allgemeinen Verwendung, der entweder an 110 V oder 220 V Stromversorgungen angeschlossen werden kann.

Der Gleichstromanschluss dient zum Anschluss einer Redundant Power Supply (RPS), die automatisch im Falle eines Ausfalls der Wechselstromquelle aktiviert wird.

## Geräteports

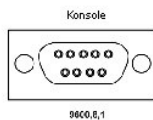
### SFP-Ports

Der Small Form Factor Pluggable (SFP)-Port ist ein hot-swappable optischer modularer Transceiver, der sich durch eine hohe Geschwindigkeit und Kompaktheit auszeichnet. Er ist als 1000Base-SX oder LX ausgewiesen.

### RS-232-Konsolen-Port

Ein DB-9-Anschluss für eine serielle Terminalverbindung, der zum Debuggen, Herunterladen von Software etc. verwendet wird. Die Standard-Baudrate ist 9600 bps. Die Baudrate kann von 2400 bps bis zu 38400 bps konfiguriert werden.

#### Abb. 2-5. Konsolen-Port



### Kombi-Port

Ein Kombi-Port ist ein logischer Port mit zwei physischen Anschlüssen:

- 1 Ein RJ-45-Anschluss für Twisted-Pair-Kupferkabel
- 1 Ein SFP-Anschluss für verschiedene Fiber-basierte Module

Es kann jeweils nur einer der beiden physischen Anschlüsse einem Kombi-Port verwendet werden. Die Portfunktionen und verfügbaren Portkontrollen hängen jeweils von der verwendeten physischen Verbindung ab.

Das System erkennt automatisch die an einem Kombi-Port verwendeten Medien und verwendet diese Informationen in allen Operationen und Kontrollschnittstellen.

Wenn sowohl RJ-45 und SFP vorhanden sind und ein Stecker am SFP-Port eingesteckt ist, ist die SFP-Port aktiv, außer wenn der Kupferanschluss des Base-T-Ports der gleichen Nummer eingesteckt ist und eine Verbindung hat.

Das System kann ohne einen Systemneustart oder Rücksetzen von RJ-45 zu SFP (oder umgekehrt) wechseln.

---

## Abmessungen

Das Gerät hat die folgenden Abmessungen:

- 1 Höhe — 44 mm
  - 1 Breite — 440 mm
  - 1 Tiefe — 255 mm
- 

## LED-Definitionen

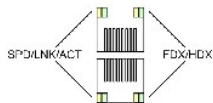
Auf der Frontblende befinden sich Leuchtdioden (LED), die den Status von Verbindungen, Stromversorgung, Lüftern und Systemdiagnose anzeigen.

### Port-LEDs

#### 10/100/1000 Base-T-Port-LEDs

Jeder 10/100/1000 Base-T-Port hat zwei LEDs. Auf der linken LED wird Geschwindigkeit/Verbindung/Aktivität und auf der rechten der Duplexmodus angezeigt.

**Abb. 2-6. Kupferbasierte RJ-45 10/100/1000 BaseT-LEDs**



Die Anzeigen der RJ-45-LED werden in der folgenden Tabelle beschrieben:

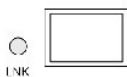
**Tabelle 2-1. Anzeigen der kupferbasierten RJ-45 10/100/1000BaseT-LED**

LED	Farbe	Beschreibung
Linke LED	Grün, ständig	Der Port ist mit 1000 Mbps verbunden.
	Grün blinkend:	Der Port überträgt oder empfängt Daten mit 1000 Mbps.
	Orange, ständig	Der Port ist entweder mit 10 oder 100 Mbps verbunden.
	Orange, blinkend	Der Port überträgt oder empfängt Daten mit 10 oder 100 Mbps.
	AUS	Der Port befindet sich im Halbduplexmodus.

### SFP-LEDs

Die SFP-Ports haben je eine LED, die als LNK ausgewiesen ist.

**Abb. 2-7.**



## SFP-Port-LED

Die Anzeigen der SFP-LED werden in der folgenden Tabelle beschrieben:

Tabelle 2-2. Anzeigen der SFP-Port-LED

LED	Farbe	Beschreibung
SFP	Grün, ständig	Der Port ist gegenwärtig aktiv.
	Grün blinkend:	Der Port überträgt oder empfängt Daten.
	AUS	Der Port ist gegenwärtig nicht aktiv.

Wenn der SFP-Port angeschlossen ist, leuchtet die Duplex-LED auf dem entsprechenden Kupfer-Kombi-Port grün auf.

## System-LEDs

Die System-LEDs, die sich links an der Frontblende befinden, liefern Informationen über die Stromversorgungen, Lüfter, Temperaturzustand und Diagnose. [Abb. 2-8](#) illustriert die System-LEDs.

Abb. 2-8. System-LEDs



Die Anzeigen der System-LEDs werden in der folgenden Tabelle beschrieben:

Tabelle 2-3. Anzeigen der System-LEDs

LED	Farbe	Beschreibung
Diagnose (DIAG)	Grün blinkend:	Das System führt einen Diagnosetest aus.
	Grün, ständig	Das System hat den Diagnosetest bestanden.
	Rot, ständig	Der Diagnosetest des Systems ist gescheitert.
Lüfter (FAN)	Grün, ständig	Die Lüfter des Geräts funktionieren normal.
	Rot, ständig	Funktionsausfall eines oder mehrerer Lüfter.
Redundant Power Supply (RPS)	Grün, ständig	Die redundante Stromversorgung ist gegenwärtig in Betrieb.
	Rot, ständig	Die redundante Stromversorgung ist gegenwärtig nicht in Betrieb.
	AUS	Die redundante Stromversorgung ist gegenwärtig nicht in Betrieb.
Main Power Supply (PWR)	Grün, ständig	Die Hauptstromversorgung funktioniert gegenwärtig normal.
	AUS	Die Hauptstromversorgung ist gegenwärtig nicht in Betrieb.
	Rot	Die Hauptstromversorgung ist ausgefallen.

---

## Hardwarekomponenten

### Netzteile

Das Gerät ist mit einem internen Netzteil (AC-Unit) und einem Steckplatz zum Anschluss des Geräts an einer externen Stromversorgung (DC-Unit) ausgerüstet. Die externe Einheit stellt Redundanz bereit und wird RPS-Einheit genannt. Zum Einschalten des Geräts ist nur eine Stromversorgung erforderlich. Der Betrieb mit beiden Stromversorgungseinheiten wird durch Load-Sharing geregelt.

Bei Load-Sharing wird der Strombedarf des Geräts auf die beiden Stromversorgungen verteilt. Wenn eine Stromversorgung ausfällt, arbeitet die zweite Stromversorgung automatisch weiter, um das gesamte Gerät mit Strom zu versorgen.

Die Stromversorgungs-LEDs zeigen den Stromversorgungsstatus an. Weitere Informationen zu den LEDs finden Sie unter [„LED-Definitionen“](#).

## AC-Netzteil

Die Netzteileneinheit wandelt Standard 220/110V AC 50/60 Hz in 5V DC bei 5A, 12V DC bei 3A um. Die Einheit erfasst automatisch die verfügbare Spannungsauslegung (110 oder 220V) und es ist keine Einstellung erforderlich.

Die Netzteileneinheit verwendet einen Standard-AC220/110V-Steckplatz. Die LED-Anzeige befindet sich an der Frontblende und zeigt an, ob die Netzeinheit angeschlossen ist.

## Gleichstrom-Netzteil

Ein externes DC-Netzteil dient als redundante Stromversorgung. Der Betrieb ist nur mit Stromversorgung von dieser Einheit möglich. Ein RPS600-Anschlussstyp wird verwendet. Es ist keine Konfiguration erforderlich. Die LED-Anzeige befindet sich an der Frontblende und zeigt an, ob die Gleichstrom-Einheit angeschlossen ist.

Bei Anschluss des Geräts an einer anderen Stromquelle nimmt die Wahrscheinlichkeit eines Ausfalls im Falle eines Stromausfalls ab.

## Reset-Taste

Die Reset-Taste, die sich auf der Frontblende befindet, dient zur manuellen Rücksetzung des Geräts.

## Belüftungssystem

Das Gerät wird durch ein Lüftersystem gekühlt. Der Betriebsstatus der Lüfter ist an den LEDs ersichtlich, die einen fehlerhaften Lüfter anzeigen. Weitere Informationen finden Sie unter [„LED-Definitionen“](#).

---

[Zurück zum Inhaltsverzeichnis](#)



[Zurück zum Inhaltsverzeichnis](#)

## Installation des PowerConnect:

Dell™ PowerConnect™ 5324 System-Benutzerhandbuch

- [Sicherheitshinweise zur Installation](#)
- [Standortanforderungen](#)
- [Auspacken](#)
- [Einbau des Geräts](#)
- [Anschließen des Geräts](#)
- [Portverbindungen, Kabel und Pinbelegung](#)
- [Standard-Porteinstellungen](#)

Dieser Abschnitt enthält Informationen zu Auspacken, Standort, Installation und Kabelanschlüsse.

---

### Sicherheitshinweise zur Installation

VORSICHT Lesen und befolgen Sie die Sicherheitshinweise in den Systeminformationen der Dell Dokumentation, bevor Sie die folgenden Schritte ausführen.

VORSICHT Beachten Sie die folgenden Punkte, bevor Sie die Verfahren in diesem Abschnitt ausführen:

- 1 Das Rack oder Gehäuse, in dem sich das Gerät befindet, sollte ausreichend gesichert werden, um Instabilität bzw. ein Umkippen zu verhindern.
  - 1 Stellen Sie sicher, dass die Schaltkreise der Stromversorgung ordnungsgemäß geerdet sind.
  - 1 Beachten und befolgen Sie die Wartungszeichen. Nehmen Sie an Geräten keine Wartungsarbeiten vor, die über die in der Systemdokumentation beschriebenen Arbeiten hinausgehen. Beim Öffnen bzw. Entfernen der mit einem Dreieckssymbol und einem Blitz gekennzeichneten Abdeckungen besteht die Gefahr eines Stromschlages. Diese Komponenten dürfen nur von qualifizierten Service-Technikern gewartet werden.
  - 1 Stellen Sie sicher, dass das Netzkabel, Verlängerungskabel und/oder der Stecker nicht beschädigt sind.
  - 1 Setzen Sie das Gerät keiner Feuchtigkeit aus.
  - 1 Stellen Sie sicher, dass das Gerät weder Heizgeräten noch anderen Wärmequellen ausgesetzt ist.
  - 1 Stellen Sie sicher, dass die Belüftungsöffnungen nicht blockiert sind.
  - 1 Achten Sie darauf, dass keine Objekte in das Gerät gelangen, da Brand- bzw. Stromschlaggefahr besteht.
  - 1 Verwenden Sie das Gerät ausschließlich mit zugelassenem Zubehör.
  - 1 Lassen Sie das Gerät abkühlen, bevor Sie Abdeckungen abnehmen oder interne Bauteile berühren.
  - 1 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.
  - 1 Installieren Sie den Switch nicht in einer Umgebung, in der die Umgebungstemperatur bei Betrieb 40°C überschreitet.
  - 1 Stellen Sie sicher, dass die Luftzirkulation an der Vorder- und Rückseite sowie an den Seitenbereichen des Geräts nicht behindert wird.
- 

### Standortanforderungen

Das Gerät kann in einem Standard-19-Zoll-Rack oder als Tischinstallation montiert werden. Stellen Sie vor der Montage sicher, dass der ausgewählte Standort die unten beschriebenen Standortanforderungen erfüllt.

- 1 Allgemein — Achten Sie darauf, dass das Gerät ordnungsgemäß mit Strom versorgt wird.
- 1 Stromversorgung — Der Abstand des Gerätes zu einer geerdeten, leicht zugänglichen Steckdose mit 220/110 V Wechselspannung und 50-60 Hz sollte maximal 1,5 m betragen.
- 1 Zugang — Der Bediener sollte an der Vorderseite des Gerätes ausreichend Bewegungsfreiheit haben. Auch Verkabelung, Stromanschlüsse und Belüftungsöffnungen sollten problemlos zugänglich sein.
- 1 Verkabelung — Die Kabel sollten so verlegt sein, dass elektromagnetische Einstrahlung durch Funksender, Funkverstärker, Stromleitungen sowie Leuchtstoffröhren vermieden wird.
- 1 Umgebungsanforderungen — Die Betriebstemperatur des Gerätes liegt zwischen 0 und 40 °C bei relativer Luftfeuchtigkeit von bis zu 95% (nicht kondensierend). Überprüfen Sie, dass kein Wasser oder Feuchtigkeit in das Gehäuse der Einheit eindringen kann.

---

## Auspacken

### Inhalt der Produktverpackung

Die folgenden Komponenten sollten nach dem Auspacken des Geräts vorhanden sein:

- 1 Die PowerConnect-Einheit
- 1 Wechselstromkabel
- 1 RS-232-gekreuztes Netzkabel
- 1 **Selbstklebende GummifüÙe**
- 1 Rackmontage-Kits
- 1 Dokumentations-CD

## Auspacken

Auspacken des Geräts:

 **ANMERKUNG:** Überprüfen Sie vor dem Auspacken des Geräts die Verpackung und melden Sie sofort jegliche Anzeichen von Beschädigung.

 **ANMERKUNG:** Es wird kein EGB-Handgelenkband bereitgestellt, aber für das folgende Verfahren für die Verwendung empfohlen.

1. Setzen Sie den Container auf eine flache, saubere Oberfläche und entfernen Sie alle Riemen am Container.
  2. Öffnen Sie den Container oder entfernen Sie die Abdeckung des Containers.
  3. Entnehmen Sie das Gerät vorsichtig aus dem Container und stellen Sie es auf eine sichere und saubere Oberfläche.
  4. Entfernen Sie das Verpackungsmaterial.
  5. Überprüfen Sie das Gerät auf Schäden. Melden Sie sofort jegliche Schäden.
- 

## Einbau des Geräts


### Übersicht

Die Stromanschlüsse für das Gerät befinden sich auf der Rückseite. Der Anschluss einer unterbrechungsfreien Gleichstromversorgung (USV) ist optional, wird jedoch empfohlen. Der UPS-DC-Anschluss befindet sich auf der Rückseite des Geräts.

## Einbau des Systems

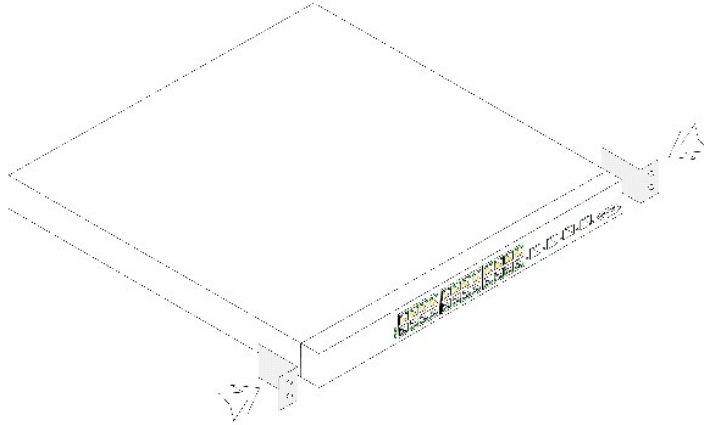
### Rack-Installation

 **VORSICHT:** Entfernen Sie alle Kabel von der Einheit, bevor Sie das Gerät in ein Rack oder Gehäuse einbauen.

 **VORSICHT:** Wenn mehrere Komponenten in ein Rack eingebaut werden, bauen Sie die Komponenten von unten nach oben ein.

1. Platzieren Sie das im Lieferumfang enthaltene Montageabdeckblech auf einer Seite des Geräts an, wobei sich die Montagebohrungen des Geräts mit den Montagebohrungen am Rackmontageblech decken müssen. [Abb. 3-9](#) illustriert die Anlage der Montagebleche.

**Abb. 3-9. Anbringen der Rackmontagebleche**



2. Führen Sie die mitgelieferten Schrauben in die Rackmontagebohrungen ein, und ziehen Sie diese mit einem Schraubendreher fest.
3. Wiederholen Sie dies beim Rackmontageblech auf der anderen Seite des Geräts.
4. Schieben Sie das Gerät in das 19-Zoll-Rack und stellen Sie dabei sicher, dass die Montagebohrungen am Gerät mit denen am Rack ausgerichtet sind.
5. Befestigen Sie die Einheit an das Rack mit den Rackschrauben (Im Lieferumfang nicht inbegriffen). Ziehen Sie zuerst die unteren Schrauben an, bevor die oberen Schrauben festgezogen werden. Dadurch wird sichergestellt, dass das Gewicht der Einheit während der Installation gleichmäßig verteilt ist. Stellen Sie sicher, dass die Lüftungslöcher nicht verstopft sind.

## Installation des Geräts ohne Rack

Das Gerät muss auf einer flachen Oberfläche installiert werden, wenn es nicht auf einem Rack installiert wird. Die Oberfläche muss in der Lage sein, das Gewicht des Geräts und der Gerätekabel zu tragen.

1. Befestigen Sie die mitgelieferten Gummifüße.
2. Stellen Sie das Gerät auf eine ebene Fläche, so dass auf auf jeder Seite 5 cm und hinten 13 cm Platz ist.
3. Es muss eine ausreichende Belüftung gewährleistet sein.

---

## Anschluss des Geräts

Zur Konfigurierung muss das Gerät an einem Terminal angeschlossen werden.

## Anschluss des Geräts an einem Terminal

Das Gerät ist mit einem Konsolenanschluss ausgerüstet; er ermöglicht den Anschluss an einem Terminal-Desktopsystem, auf dem eine Terminal-Emulationssoftware zur Überwachung und Konfiguration des Geräts ausgeführt wird. Der Konsolenanschluss ist ein DB9-Steckverbinder, der als Data Terminal Equipment (DTE)-Steckplatz angeschlossen wurde.

Für die Verwendung des Konsolenanschlusses ist Folgendes erforderlich:

- 1 VT100-kompatibler und über eine serielle Schnittstelle verfügbarer Terminal bzw. Desktop- oder portables System, auf dem VT100-Terminal-Emulationssoftware ausgeführt wird.
- 1 Ein gekreuztes RS-232-Kabel mit DB-9-Anschlussbuchse für die Konsolen-Port und entsprechendem Anschluss für den Terminal.

Führen Sie folgende Schritte durch, um einen Terminal an die Konsolenschnittstelle des Geräts anzuschließen:

1. Schließen Sie ein RS-232-gekreuztes Netzwerkabel an den Terminal an, auf dem eine VT100 Terminal-Emulation-Software ausgeführt wird.
2. Stellen Sie sicher, dass die Terminal-Emulation-Software wie folgt eingestellt ist:
  - a. Wählen Sie die entsprechende serielle Schnittstelle (serielle Schnittstelle 1 oder serielle Schnittstelle 2) zum Anschluss an die Konsole.

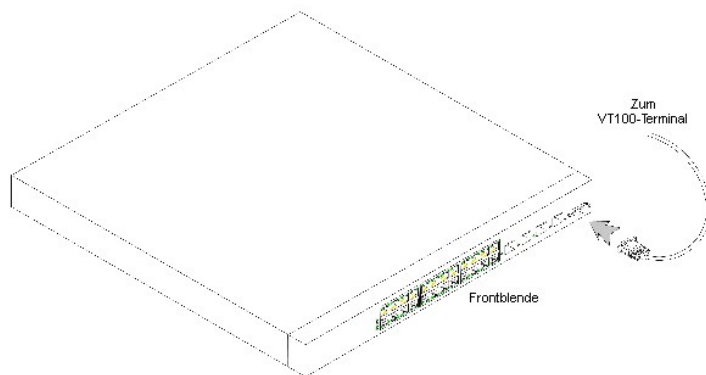
- b. Setzen Sie die Datenübertragungsrate auf 9600 Baud.
- c. Setzen Sie das Datenformat auf 8 Datenbits, 1 Stopbit und keine Parität.
- d. Stellen Sie Datenflusssteuerung auf keine (none) ein.
- e. Wählen Sie unter **Properties** (Eigenschaften) den Modus **VT100 for Emulation** (VT100 für Emulation) aus.
- f. Wählen Sie **Terminal keys** (Terminaltasten) für **Function, Arrow, and Ctrl keys** (Funktion, Pfeil und Strgs-Tasten). Stellen Sie sicher, dass **Terminal keys** (Terminaltasten) und nicht **Windows keys** (Windows-Tasten) eingestellt ist.

**HINWEIS:** Stellen Sie bei der Verwendung von HyperTerminal mit Microsoft® Windows 2000 sicher, dass Windows® 2000 Service-Pack 2 oder höher installiert ist. Beim Windows 2000 Service-Pack 2 funktionieren die Pfeiltasten korrekt bei der VT100-Emulation von HyperTerminal. Gehen Sie zu [www.microsoft.com](http://www.microsoft.com), um Informationen über Windows 2000 Service-Packs zu erhalten.

3. Schließen Sie die Anschlussbuchse des gekreuzten RS-232-Kabels direkt an dem Konsolen-Port des Geräts an und ziehen Sie die unverlierbaren Befestigungsschrauben fest.

Der Konsolen-Port der Einheit befindet sich an der Frontblende.

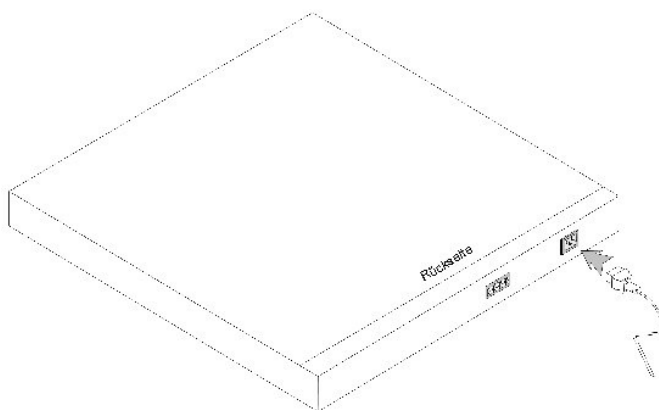
Abb. 3-10. Anschluss an der PowerConnect 5324 Konsolen-Port



### Anschließen eines Geräts an die Stromversorgung

1. Schließen Sie das Netzkabel (1,5 m Standardnetzkabel) mit angeschlossener Sicherheitserdung am AC-Netzanschluss auf der Rückseite der Einheit an.
2. Schließen Sie das Netzkabel an einer geerdeten Wechselstromsteckdose an.

Abb. 3-11. Anschluss am Netzanschlusses



Bestätigen Sie den Anschluss des Geräts und korrekten Betrieb durch eine Prüfung der Leuchtdioden auf der Frontblende.

## Portverbindungen, Kabel und Pinbelegung

In diesem Abschnitt werden die physischen Schnittstellen des Geräts erläutert und Informationen über Portverbindungen bereitgestellt. Die Steckplatzarten, Anschlüsse und Kabel sind im Abschnitt „Ports, Anschlüsse und Kabel“ zusammengefasst. Kupferkabel und Optical-Transceiver-Diagnose werden unterstützt.

## RJ-45-Anschlüsse für 10/100/1000BaseT-Ports

Bei den 10/100/1000BaseT-Ports handelt es sich um Twisted-Pair-Kupferschnittstellen.

Zur Herstellung einer Verbindung für die Twisted-Pair-Ports muss das Tx-Paar an einem Kabelende mit dem Rx-Paar am anderen Kabelende, und umgekehrt, verbunden werden. Bei einer Verkabelung, wo das Tx an einem Ende mit dem Tx am anderen Ende verbunden wird und Rx mit Rx verbunden wird, wird keine Verbindung hergestellt.

Bei der Auswahl von Kabeln zum Anschluss der Geräteports an ihren Networking-Peers ist zu beachten, dass Geradeauskabel zum Anschluss des Geräts an einer Station und gekreuzte Kabel zum Anschluss eines Übertragungsgeräts (Switch oder Hub) an einem anderen erforderlich sind. Sowohl Geradeaus- als auch gekreuzte Kabel müssen Kategorie 5 sein.

Nach Anschluss einer Schnittstelle leuchtet ihre LINK-LED auf.

**Tabelle 3-4. Ports, Anschlüsse und Kabel**

Steckplatz	Port/Schnittstelle	Kabel
RJ-45	10/100/1000BaseT-Port	Kat. 5

Die RJ-45-Pinbelegung für die 10/100/1000BaseT-Ports ist in der folgenden Tabelle aufgeführt.

**Tabelle 3-5. RJ-45-Pinbelegung für 10/100/1000BaseT-Ethernet-Port**

Pin-Nummer	Funktion
1	TxRx 1+
2	TxRx 1-
3	TxRx 2+
4	TxRx 2-
5	TxRx 3+
6	TxRx 3-
7	TxRx 4+
8	TxRx 4-

---

## Standard-Porteinstellungen

Die allgemeinen Informationen zur Konfiguration der Geräteports umfassen die Kurzbeschreibung der automatischen Verbindungsaushandlung (Auto-Negotiation) und der Standardeinstellungen für Switching-Ports.

### Automatische Verbindungsaushandlung (Auto-Negotiation)

Die automatische Verbindungsaushandlung (Auto-Negotiation) ermöglicht die automatische Erfassung von Geschwindigkeit, Duplexmodus und Datenflusssteuerung bei Switching-10/100/1000BaseT-Ports. Auto-Negotiation ist standardgemäß pro Port aktiviert.

Automatische Verbindungsaushandlung (Auto-Negotiation) ist ein Mechanismus, der zwischen zwei Verbindungspartnern hergestellt wird, um es einer Schnittstelle zu ermöglichen, ihrem Partner ihre Fähigkeiten in Bezug auf Übertragungsrate, Duplexmodus und Datenflusssteuerung (Datenflusssteuerung ist standardgemäß deaktiviert) bekanntzugeben. Die Funktion der Schnittstellen basiert dann auf ihrem höchsten gemeinsamen Nenner.

Beim Anschluss einer NIC, die keine automatische Verbindungsaushandlung unterstützt oder die nicht auf Auto-Negotiation eingestellt ist, müssen sowohl der Switching-Port des Geräts als auch die NIC manuell auf die gleiche Geschwindigkeit und Duplexmodus eingestellt werden.

Wenn die Station auf der anderen Seite der Verbindung eine automatische Verbindungsaushandlung mit einer 10/100/1000BaseT-Geräteschnittstelle versucht, die für Vollduplex konfiguriert ist, ist das Ergebnis von Auto-Negotiation, dass die Station den Betrieb im Halbduplex-Modus versucht.

## MDI /MDIX

Das Gerät unterstützt automatische Erkennung von Geradeaus- und gekreuzten Kabeln an allen Switching- 10/100/1000BaseT-Ports. Diese Funktion ist Teil der automatischen Verbindungsaushandlung (Auto-Negotiation) und sie wird zusammen mit Auto-Negotiation aktiviert.

Wenn MDI/MDIX (Media Dependent Interface with Crossover) aktiviert wird, ist die automatische Korrektur von Fehlern bei der Kabelauswahl möglich, womit die Unterscheidung von ungekreuztem und gekreuztem Kabel nicht mehr relevant ist. (die Standardverkabelung für Endstationen ist als MDI (Media Dependent Interface) und die Standardverkabelung für Hubs und Switches ist als MDIX bekannt.)

## Datenflusssteuerung

Dieses Gerät unterstützt 802.3x Datenflusssteuerung für Schnittstellen, die mit Vollduplexmodus konfiguriert wurden. Diese Funktion ist standardmäßig deaktiviert. Sie kann je Schnittstelle aktiviert werden. Der Datenflusssteuerungsmechanismus ermöglicht der empfangenden Seite, der übertragenden Seite zu signalisieren, dass die Datenübertragung vorübergehend eingestellt werden muss, um einen Pufferüberlauf zu vermeiden.

## Zurückweisung (Backpressure)

Das Gerät unterstützt Zurückweisung (Backpressure) für Schnittstellen, die für Halbduplexbetrieb konfiguriert wurden. Diese Funktion ist standardmäßig deaktiviert. Sie kann je Port aktiviert werden. Der Backpressure-Mechanismus verhindert, dass die übertragende Seite vorübergehend zusätzlichen Datenverkehr übermittelt. Die empfangende Seite kann auch eine Verbindung belegen, so dass sie nicht für zusätzlichen Datenverkehr zur Verfügung steht.

## Standardeinstellungen für Switching-Ports

Die folgende Tabelle gibt die Standard-Porteinstellungen wieder.

Tabelle 3-6. Standard-Porteinstellungen

Funktion	Standardeinstellung
Port-Geschwindigkeit und -modus	10/100/1000BaseT Kupfer: Auto-Negotiation 100 Vollduplex
Port-Forwarding-Zustand	Enabled (Aktiviert)
Port-Tagging	No tagging (ohne Tagging)
Flow Control (Datenflusssteuerung)	Off (disabled on ingress) (Aus [deaktiviert oder Eingang])
Backpressure (Zurückweisung)	Off (disabled on ingress) (Aus [deaktiviert oder Eingang])

---

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Einführung

Dell™ PowerConnect™ 5324 System-Benutzerhandbuch

- [PowerConnect 5324](#)
- [Funktionen](#)
- [Zusätzliche CLI-Dokumentation](#)

➔ **HINWEIS:** Bevor Sie fortfahren, lesen Sie bitte die Versionshinweise für dieses Produkt. Die Versionshinweise können von der Dell Support-Website auf [support.dell.com](http://support.dell.com) heruntergeladen werden.

Dieses Benutzerhandbuch enthält die notwendigen Informationen zur Installation, Konfiguration und Pflege des PowerConnect Geräts.

---

## PowerConnect 5324

Das PowerConnect 5324 verfügt über 24 Gigabit-Ethernet-Anschlüsse. Es gibt auch vier SFP-Fiber-Ports, die als Kombi-Schnittstellenalternativen zu den Ethernet-Anschlüssen 21-24 vorgesehen sind. Die Kombi-Anschlüsse sind einzelne Schnittstellen mit zwei physischen Anschlüssen. Wenn eine angeschlossen ist, ist die andere deaktiviert.

[Abb. 1-1](#) und [Abb. 1-2](#) illustrieren die Vorder- und Rückseite des PowerConnect 5324.

Abb. 1-1. PowerConnect 5324 Frontblende



Abb. 1-2. PowerConnect 5324 Rückseite



## Funktionen

Dieser Abschnitt beschreibt die vom Benutzer konfigurierten Funktionen. Eine vollständige Liste aller aktualisierten Gerätefunktionen finden Sie in den neusten Software-Versionshinweisen.

### Allgemeine Funktionen

#### Head of Line Blocking (HOL)

Head-of-Line (HOL)-Blocking resultiert in Verzögerungen im Datenverkehr und Frame-Verlust, die durch ein Konkurrieren des Datenverkehrs um die gleichen Ausgangs-Anschlussressourcen verursacht werden. HOL-Blocking reiht Pakete in Warteschlangen ein und die Pakete am Kopf der Warteschlange werden vor denen am Ende der Warteschlange weitergeleitet.

#### Virtual Cable Testing (VCT)

VCT erfasst und meldet Kupferverkabelungsereignisse, z.B. offene Kabel und Kabelkurzschlüsse.

## Unterstützung für Jumbo-Frames

Jumbo-Frames ermöglicht die Übertragung von identischen Daten in weniger Frames. Damit fallen weniger Restkapazität, geringere Verarbeitungszeit und weniger Interrupts an.

Weitere Informationen zur Aktivierung von Jumbo-Frames finden Sie unter [„Definieren der allgemeinen Geräteinformationen“](#).

## Unterstützung für MDI/MDIX

Das Gerät unterstützt automatische Erkennung zwischen gekreuzten und Geradeauskabeln.

Die Standardverkabelung für Endstationen ist als MDI (Media Dependent Interface) und die Standardverkabelung für Hubs und Switches ist als MDIX (Media-Dependent Interface with Crossover) bekannt.

Weitere Informationen zur Konfiguration von MDI/MDI für Ports oder Link Aggregate Groups (LAGs) finden Sie unter [„Definieren der Portparameter“](#) oder [„Definieren der LAG-Parameter“](#).

## Unterstützung der Datenflusssteuerung (IEEE 802.3X)

Datenflusssteuerung ermöglicht Geräten mit niedrigerer Geschwindigkeit die Kommunikation mit Geräten höherer Geschwindigkeit, indem das Gerät mit der höheren Geschwindigkeit davon absieht, Pakete zu schicken. Übertragungen werden vorübergehend unterbrochen, um Pufferüberläufe zu verhindern.

Weitere Informationen zur Konfiguration der Datenflusssteuerung für Schnittstellen oder LAGs finden Sie unter [„Definieren der Portparameter“](#) oder [„Definieren der LAG-Parameter“](#).

## Unterstützung für Backpressure

Bei Halbduplexverbindungen verhindert der empfangende Port Pufferüberläufe, indem die Verbindung belegt wird, so dass sie nicht für weiteren Datenverkehr zur Verfügung steht.

Weitere Informationen zur Konfiguration der Zurückweisung (Backpressure) für Ports oder LAGs finden Sie unter [„Definieren der Portparameter“](#) oder [„Definieren der LAG-Parameter“](#).

## Von MAC-Adressen unterstützte Funktionen

### Unterstützung für MAC-Adressenkapazität

Dieses Gerät unterstützt bis zu achttausend MAC-Adressen. Dieses Gerät reserviert bestimmte MAC-Adressen für die Verwendung durch das System.

### Selbstlernende MAC-Adressen

Das Gerät aktiviert das automatische Lernen von MAC-Adressen aus eingehenden Paketen. Die MAC-Adressen werden in der Bridging-Tabelle gespeichert.

### Automatische Alterung (Aging) für MAC-Adressen



MAC-Adressen, von denen über einen bestimmten Zeitraum kein Datenverkehr erhalten wird, werden gelöscht. Damit wird ein Überlauf der Bridging-Tabelle verhindert.

Weitere Informationen zur Konfiguration der Alterungszeit (Age-out-Time) für MAC-Adressen finden Sie unter [„Konfigurieren der Adresstabellen“](#).

## Statische MAC-Einträge

Die benutzerdefinierten statischen MAC-Einträge werden in der **Bridging-Tabelle** gespeichert.

Weitere Informationen finden Sie unter [„Konfigurieren der Adresstabellen“](#).

## VLAN-aware MAC-basiertes Switching

Von einer unbekanntenen Quelladresse ankommende Pakete werden an den Mikroprozessor gesandt, wo die Quelladressen zur Hardware-Tabelle hinzugefügt werden. Unter Verwendung der Hardware-Tabelle können Pakete von oder an diese Adresse effizienter weitergeleitet werden.

## Unterstützung für MAC-Multicast

Multicast-Service ist ein eingeschränkter Broadcast-Service, der One-to-Many- und Many-to-Many-Verbindungen zur Informationsverteilung ermöglicht. Bei Layer-2-Multicast-Service wird ein einzelner Frame an eine bestimmte Multicast-Adresse adressiert, von der aus Kopien des Frames an die entsprechenden Ports übertragen werden.

Weitere Informationen finden Sie unter [„Unterstützung für Multicast-Weiterleitung“](#).

## Layer-2-Funktionen

### IGMP-Snooping

Das Internet Group Membership Protocol (IGMP)-Snooping überprüft den Inhalt von IGMP-Frames, wenn diese durch das Gerät von den Workstations an einen vorgeschalteten Multicast-Router weitergeleitet werden. Anhand des Frames identifiziert das Gerät die Workstations, die für Multicast-Sessions konfiguriert wurden, und die Multicast-Router, die Multicast-Frames senden.

Weitere Informationen finden Sie unter [„IGMP-Snooping“](#).

### Port-Spiegelung (Mirroring)

Port-Spiegelung überwacht und spiegelt Netzwerk-Datenverkehr durch Weiterleitung von Kopien der eingehenden und ausgehenden Pakete von einem überwachten Port zu einem Überwachungsport. Die Angabe des Zielports, der Kopien des gesamten einen bestimmtem Quellport durchlaufenden Datenverkehrs erhält, erfolgt vom Benutzer.

Weitere Informationen finden Sie unter [„Definieren von Port-Spiegelungssitzungen“](#).

### Broadcast-Storm-Kontrolle

Storm-Kontrolle ermöglicht die Beschränkung der Menge der Multicast- und Broadcast-Frames, die vom Gerät angenommen und weitergeleitet werden.

Bei der Weiterleitung von Layer-2-Frames werden Broadcast- und Multicast-Frames an alle Ports im entsprechenden VLAN weitergeleitet. Das nimmt Bandbreite in Anspruch und belastet alle Knoten, die mit allen Ports verbunden sind.

Weitere Informationen finden Sie unter [„Aktivieren von Broadcast-Storm-Kontrolle“](#).

## VLAN-unterstützte Funktionen

### VLAN-Unterstützung

VLANs sind Sammlungen von Switching-Ports, die eine einzige Broadcast-Domain umfassen. Pakete werden entweder auf der Grundlage einer VLAN-Kennung oder aufgrund einer Kombination des Eingangsports und Paketinhalts als zu einem VLAN zugehörig klassifiziert. Pakete, die Attribute gemein haben, können im gleichen VLAN gruppiert werden.

Weitere Informationen finden Sie unter [„Konfigurieren von VLANs“](#).

### Port-basierte virtuelle LANs (VLANs)

Port-basierte VLANs klassifizieren eingehende Pakete an VLANs aufgrund ihres Eingangsports.

Weitere Informationen finden Sie unter [„Definieren von VLAN-Port-Einstellungen“](#).

### IEEE802.1V-protokollbasierte virtuelle LANs (VLANs)

VLAN-Klassifizierungsregeln werden aufgrund einer Data-Link-Layer (Layer 2) Protokoll-Kennung definiert. Protokollbasierte VLANs isolieren Layer-2-Datenverkehr für unterschiedliche Layer-3-Protokolle.

Weitere Informationen finden Sie unter [„Definieren von VLAN-Protokollgruppen“](#).

### Umfassende 802.1Q VLAN-Tagging-Konformität

IEEE 802.1Q definiert eine Architektur für virtuell überbrückte LANs, die in VLANs bereitgestellten Dienste und die an der Bereitstellung dieser Dienste beteiligten Protokolle und Algorithmen. Eine wichtige in diesem Standard enthaltene Anforderung ist die Fähigkeit, Frames mit einem gewünschten Class-of-Service (CoS)-Kennungswert (0-7) zu markieren.

### GVRP-Unterstützung

GARP VLAN Registration Protocol (GVRP) stellt IEEE 802.1Q-konformes VLAN-Pruning und dynamische VLAN-Erstellung auf 802.1Q-Trunk-Ports bereit. Bei Aktivierung von GVRP registriert und verbreitet das Gerät VLAN-Zugehörigkeit auf allen Ports, die Teil der aktiven zugrundeliegenden Topologie mit [„Spanning-Tree-Protokollmerkmalen“](#) sind.

Weitere Informationen finden Sie unter [„Konfigurieren von GVRP“](#).

## Merkmale des Spanning Tree-Protokolls (STP)

### Spanning Tree-Protokoll (STP)

802.1d Spanning Tree ist eine standardmäßige Layer-2-Switch-Anforderung, die es Brücken ermöglicht, automatisch L2-Weiterleitungsschleifen zu verhindern und aufzulösen. Switches tauschen Konfigurationsmeldungen unter Verwendung von speziell formatierten Frames aus und sie aktivieren und deaktivieren selektiv die Weiterleitung an Ports.

Weitere Informationen finden Sie unter [„Konfigurieren des Spanning Tree-Protokolls \(STP\)“](#).

## Fast Link

Die STP-Konvergenz kann bis zu 30-60 Sekunden dauern. Während dieser Zeit erfasst STP mögliche Schleifen, wobei Zeit zur Verbreitung von Zustandsänderungen und die Reaktionszeit der entsprechenden Geräte bleibt. 30-60 Sekunden gilt als zu lange Reaktionszeit für viele Applikationen. Die Fast Link-Option umgeht diese Verzögerung und kann in Netzwerktopologien verwendet werden, wo keine Weiterleitungsschleifen auftreten.

Weitere Informationen zur Aktivierung von Fast Link für Ports und LAGs finden Sie unter [„Definieren der STP-Porteinstellungen“](#) oder [„Definieren der STP LAG-Einstellungen“](#).

## IEEE 802.1w Rapid Spanning Tree

Bei Spanning Tree kann es 30-60 Sekunden dauern, bis jeder Host entschieden hat, ob seine Ports Datenverkehr aktiv weiterleiten. Rapid Spanning Tree (RSTP) erfasst die Verwendung von Netzwerktopologien, um eine schnellere Konvergenz zu ermöglichen, ohne dass Weiterleitungsschleifen gebildet werden.

Weitere Informationen finden Sie unter [„Konfigurieren des Rapid-Spanning-Tree-Protokolls \(RSTP\)“](#).

## Link Aggregation

Weitere Informationen finden Sie unter [„Aggregieren von Ports“](#).

### Link Aggregation

Es können bis zu acht Aggregated Links definiert werden, wobei jeder bis zu acht zugehörige Ports umfassen kann, um eine einzelne Link Aggregated Group (LAG) zu bilden. Damit wird Folgendes ermöglicht:

- 1 Fehlertoleranz-Schutz gegen Störung der physischen Verbindung
- 1 Verbindungen höherer Bandbreite
- 1 Verbesserte Bandbreitengranularität
- 1 Server-Konnektivität von höherer Bandbreite

LAG besteht aus Ports mit der gleichen Geschwindigkeit, die auf Vollduplex-Betrieb eingestellt sind.

Weitere Informationen finden Sie unter [„Definieren der LAG-Zugehörigkeit“](#).

### Link Aggregation und LACP

LACP verwendet Peer-Exchanges, d.h. Kontaktnahmen untereinander, über Verknüpfungen zur ständigen Feststellung der Aggregationskapazität der verschiedenen Links und stellt kontinuierlich die höchste Aggregationskapazität, die zwischen einem gegebenen Paar von Systemen erzielt werden kann, bereit. Durch LACP erfolgt die automatische Feststellung, Konfiguration, Bindung und Überwachung der Portbindung an Aggregatoren innerhalb des Systems.

Weitere Informationen finden Sie unter [„Definieren der LACP-Parameter“](#).

## Layer-3-Funktionen

### Address Resolution Protocol (ARP)

ARP ist ein TCP/IP-Protokoll, das IP-Adressen in physische Adressen konvertiert. ARP ermittelt automatisch die Device Next-Hop MAC-Adressen von Systemen, einschließlich direkt verbundene Endsysteme. Der Benutzer kann dies außer Kraft setzen und durch eine Definition von zusätzlichen ARP-Tabelleneinträgen ergänzen.

Weitere Informationen finden Sie unter [„Zuweisen von Domain-Hosts“](#).

### TCP (Übertragungssteuerungsprotokoll)

Transport Control Protocol (TCP)-Verbindungen werden zwischen 2 Ports durch einen anfänglichen Synchronisationsaustausch definiert. TCP-Ports werden durch eine IP-Adresse und eine 16-Bit-Portnummer identifiziert. Oktettströme werden in TCP-Pakete unterteilt, die jeweils eine Sequenznummer haben.

### BootP und DHCP Clients

Dynamic Host Configuration Protocol (DHCP) ermöglicht den Empfang von zusätzlichen Setup-Parametern von einem Netzwerk-Server nach dem Systemstart. DHCP-Service ist ein ständiger Prozess. DHCP ist eine Erweiterung von BootP.

Weitere Informationen zu DHCP finden Sie unter [„Definieren von DHCP-IP-Schnittstellenparametern“](#).

## QoS-Funktionen

### Unterstützung für Class Of Service 802.1p

Das IEEE 802.1p-Signalverfahren ist ein OSI-Layer-2-Standard zur Markierung und Priorisierung von Netzwerk-Datenverkehr auf der Datenlink-/MAC-Unterschicht. 802.1p-Datenverkehr wird klassifiziert und ans Ziel übertragen. Es werden keine Bandbreiten-Reservierungen oder Beschränkungen eingerichtet oder durchgesetzt. 802.1p ist ein Ableger des 802.1Q (VLANs) Standards. 802.1p legt acht Prioritätsebenen fest, ähnlich dem IP-Precedence-IP Header-Bitfeld.

Weitere Informationen finden Sie unter [„Konfigurieren von Quality of Service \(QoS\)“](#).

## Geräteverwaltungsfunktionen

### SNMP-Alarme und Trap-Protokolle

Das System protokolliert Ereignisse mit Schwerecodes und Zeitstempeln. Die Ereignisse werden als Simple Network Management Protocol (SNMP)-Traps an eine Trap-Empfängerliste gesendet.

Weitere Informationen über SNMP-Alarme und Traps finden Sie unter [„Definieren von SNMP-Parametern“](#).

### SNMP Version 1 und Version 2

Simple Network Management Protocol (SNMP) über dem UDP/IP-Protokoll. Zur Systemzugriffskontrolle wird eine Liste von Community-Einträgen definiert, die jede aus einer Community-Zeichenfolge und deren Zugriffsprivilegien bestehen. Es gibt 3 SNMP-Sicherheitsstufen: Schreibschutz, Lese- und Schreibzugriff und

Super. Nur ein Super-Benutzer hat Zugriff auf die Community-Tabelle.

## Web-basiertes Management

Mit web-basiertem Management kann das System von jedem Web-Browser aus verwaltet werden. Das System umfasst einen Embedded Web Server (EWS), der HTML-Seiten bereitstellt, über die das System überwacht und konfiguriert werden kann. Das System wandelt web-basierten Input intern in Konfigurationsbefehle, MIB-Variableneinstellungen und andere verwaltungsbezogene Einstellungen um.

## Herunterladen und Hochladen der Konfigurationsdatei

Die PowerConnect Gerätekonfiguration wird in einer Konfigurationsdatei gespeichert. Die Konfigurationsdatei umfasst sowohl die systemweite als auch die portspezifische Gerätekonfiguration. Das System kann Konfigurationsdateien in Form einer Sammlung von CLI-Befehlen, die als Textdateien gespeichert und manipuliert werden, anzeigen.

Weitere Informationen finden Sie unter [„Verwalten von Dateien“](#).

## Trivial File Transfer Protocol (TFTP)

Das Gerät unterstützt TFTP-basiertes Upload/Download von Boot-Image, Software und Konfiguration.

## Remote Monitoring (Fernüberwachung)

Remote Monitoring (RMON) ist eine Erweiterung von SNMP, welche eine umfassende Überwachungsfunktionalität für Netzwerk-Datenverkehr bereitstellt (im Gegensatz zu SNMP, welches Netzwerk-Geräteverwaltung und -überwachung ermöglicht). RMON ist eine Standard-MIB, die aktuelle und historische MAC-Layer-Statistiken und Kontrollobjekte definiert und somit die Erfassung von Echtzeitinformationen über das gesamte Netzwerk ermöglicht.

Weitere Informationen finden Sie unter [„Anzeigen von RMON-Statistiken“](#).

## Befehlszeilen-Schnittstelle

Die CLI (Command Line Interface)-Syntax und Semantik entsprechen so weit wie möglich der allgemeinen Industriepraxis. CLI besteht aus obligatorischen und optionalen Elementen. Der CLI-Interpreter stellt Befehls- und Stichwort-Vervollständigung zur Unterstützung des Benutzers und Verkürzung der Eingabezeit bereit.

## Syslog

Syslog ist ein Protokoll, das die Verschickung von Ereignismitteilungen an eine Reihe von Remote-Servern ermöglicht, wo sie gespeichert, geprüft und dementsprechende Maßnahmen ergriffen werden können. Mehrere Mechanismen werden implementiert, um eine Mitteilung von signifikanten Ereignissen in Echtzeit zu übertragen und um eine Aufzeichnung dieser Ereignisse für eine spätere Verwendung aufzubewahren.

Weitere Informationen über Syslog finden Sie unter [„Verwalten von Protokollen“](#).

## SNTP

Das Simple Network Time Protocol (SNTP) stellt eine präzise Zeitsynchronisation der Netzwerkgeräte bis auf die Millisekunde sicher. Die zeitliche Synchronisierung wird von einem Netzwerk-SNTP-Server ausgeführt. Zeitquellen werden durch Strata ermittelt. Strata definieren die Distanz von der Referenzuhr. Je höher das Stratum (Null ist am höchsten), desto genauer die Uhr.

Weitere Informationen finden Sie unter [„Konfigurieren der SNTP-Einstellungen“](#).

## Traceroute

Traceroute ermöglicht die Auffindung von IP-Routes, auf denen Datenpakete während des Weiterleitungsprozesses weitergeleitet wurden. Das CLI-Traceroute-Dienstprogramm kann vom User EXEC- oder vom privilegierten Modus ausgeführt werden.

## Sicherheitsfunktionen

### SSL

Secure Socket Layer (SSL) ist ein Protokoll auf Applikationsebene, das sichere Datentransaktionen mit Hilfe von Datenschutz, Authentifizierung und Datenintegrität ermöglicht. Es beruht auf Zertifikaten und öffentlichen und privaten Schlüsseln.

### Portbasierte Authentifizierung (802.1x)

Portbasierte Authentifizierung ermöglicht die Authentifizierung von Systembenutzern auf Portbasis über einen externen Server. Nur authentifizierte und genehmigte Systembenutzer können Daten übertragen und empfangen. Ports werden über den RADIUS (Remote Authentication Dial In User Service)-Server unter Einsatz des Extensible Authentication-Protokolls (EAP) authentifiziert.

Weitere Informationen finden Sie unter [„Konfigurieren der portbasierten Authentifizierung“](#).

## Unterstützung von Locked Port

Locked Port erhöht die Netzwerksicherheit durch Beschränkung bestimmter Ports ausschließlich auf Benutzer mit speziellen MAC-Adressen. Diese Adressen werden entweder manuell definiert oder an diesem Port gelernt. Wenn ein Frame auf einem gesperrten Port festgestellt wird und die MAC-Adresse der Frame-Quelle nicht mit dem Port verknüpft ist, wird der Schutzmechanismus aufgerufen.

Weitere Informationen finden Sie unter [„Konfigurieren der Portsicherheit“](#).

### RADIUS-Client

RADIUS ist ein Client/Server-basiertes Protokoll. Ein RADIUS-Server führt eine Benutzerdatenbank, die Authentifizierungsinformationen für jeden Benutzer enthält, z.B. Benutzername, Kennwort und Abrechnungsinformationen.

Weitere Informationen finden Sie unter [„Konfigurieren der globalen RADIUS-Parameter“](#).

### SSH

Secure Shell (SSH) ist ein Protokoll, das eine sichere Remote-Verbindung zu ein Gerät ermöglicht. SSH Version 1 ist derzeit erhältlich. Die SSH-Server-Funktion ermöglicht einem SSH-Client die Herstellung einer sicheren, verschlüsselten Verbindung mit einem Gerät. Die von dieser Verbindung gelieferte Funktionalität ähnelt der einer eingehenden Telnet-Verbindung. SSH verwendet RSA-Public-Key-Kryptographie für Geräteverbindungen und Authentifizierung.

### TACACS+

TACACS+ stellt eine zentralisierte Sicherheit zur Validierung von Benutzern, die auf das Gerät zugreifen, dar. TACACS+ stellt ein zentralisiertes Benutzerverwaltungssystem dar, das jedoch mit RADIUS und anderen Authentifizierungsprozessen konform ist.

Weitere Informationen finden Sie unter [„Definieren der TACACS+-Einstellungen“](#).

---

## **Zusätzliche CLI-Dokumentation**

Das CLI-Referenzhandbuch, welches sich auf der Dokumentations-CD befindet, enthält Informationen über die CLI-Befehle, die zur Konfiguration des Geräts verwendet werden. Das Dokument enthält auch eine CLI-Beschreibung und Informationen zur Syntax, Standardwerte, Richtlinien und Beispiele.

---

[Zurück zum Inhaltsverzeichnis](#)

## Konfiguration von QoS (Quality of Service):

Dell™ PowerConnect™ 5324 System-Benutzerhandbuch

- [Überblick: Quality of Service \(QoS\)](#)
- [Definition der globalen CoS-Parameter](#)

Dieser Abschnitt erläutert die Definition und Konfiguration der Quality of Service (QoS)-Parameter. Klicken Sie zum Öffnen auf „Quality of Service“ in der Strukturansicht.

---

### Überblick: Quality of Service (QoS)

Quality of Service (QoS) stellt die Fähigkeit zur Implementierung von QoS und Priority-Queuing (Einreihung in Warteschlangen nach Priorität) innerhalb eines Netzwerks bereit. QoS verbessert den Netzwerk-Datenfluss aufgrund von Grundsätzen, Frame-Zähler und Kontext.

Ein Implementierungsbeispiel, das QoS erfordert, umfasst bestimmte Verkehrsarten, z.B. Voice, Video und Echtzeit-Datenverkehr, denen eine Warteschlange mit hoher Priorität zugewiesen werden kann, während anderer Datenverkehr einer Warteschlange mit niedrigerer Priorität zugewiesen werden kann. Das Ergebnis ist ein verbesserter Datenverkehrsfluss bei hohem Verkehrsaufkommen.

QoS wird definiert durch:

- 1 Classification — Gibt an, welche Paketfelder mit bestimmten Werten abgestimmt werden. Alle Datenpakete, die den benutzerdefinierten Spezifikationen entsprechen, werden zusammen klassifiziert.
- 1 Action — Definiert eine Datenverkehrsverwaltung, in der weitergeleitete Pakete auf Paketinformationen und Paketfeldwerten basieren, z.B. VLAN-Priorität (VPT) und DSCP (DiffServ Code Point).

### VPT-Tag-Klassifikationsinformationen

VLAN-Prioritätskennungen werden zur Klassifikation der Datenpakete durch Zuweisung der Pakete zu einer der Ausgabewarteschlangen klassifiziert. VLAN-Prioritätskennungen zur Einreihung in eine Warteschlange sind ebenfalls benutzerdefinierbar. In der folgenden Tabelle sind die VPT-Einheiten zu den Warteschlangen-Standardinstellungen aufgeführt:

**Tabelle 9-92. Zuweisungstabelle: CoS zu Warteschlange, Standardwerte**

CoS-Wert	Werte der Weiterleitungs-Warteschlange
0	q2
1	q1 (Lowest Priority = Best Effort)
2	q1 (Lowest Priority = Best Effort)
3	q2
4	q3
5	q3
6	q4 (Highest Priority)
7	q4 (Highest Priority)

Ohne Kennungen ankommenden Paketen wird ein Standard-VPT zugewiesen, der auf Port-Basis eingestellt wird. Das zugewiesene VPT wird zur Zuweisung des Pakets in die Ausgabewarteschlange und als Ausgangs-VPT verwendet.

DSCP-Werte können Prioritäts-Warteschlangen zugewiesen werden. Die folgende Tabelle enthält die Standard-DSCP-Zuweisung zu Weiterleitungswarteschlangen-Werten:

**Tabelle 9-93. Zuweisungstabelle: DSCP zu Warteschlange, Standardwerte**

---



DSCP-Wert	Werte der Weiterleitungswarteschlange
0 - 7.	q2 (Lowest Priority)
8-15	q1
16 - 23	q1
24-31	q2
32-39	q3
40-47	q3
48-55	q4
55-63	q4 (Highest Priority)

Die DSCP-Zuweisung wird auf Systembasis aktiviert.

## CoS-Dienste

Nachdem die Pakete einer speziellen Warteschlange zugewiesen wurden, können der/den Warteschlange(n) CoS-Dienste zugewiesen werden. Ausgabewarteschlangen werden durch eine der folgenden Methoden mit einem Ablaufplan konfiguriert:

- 1 **Strict Priority (Strikte Priorität)** — Stellt sicher, dass zeitkritische („time-sensitive“) Applikationen immer über einen Express-Leitweg weitergeleitet werden. Die Strikte Priorität ermöglicht die Priorisierung des auftragsentscheidenden („mission-critical“) und zeitkritischen Datenverkehrs vor weniger zeitkritische Anwendungen. Zum Beispiel wird unter der strikten Priorität Voice über IP-Datenverkehr vor FTP oder E-Mail (SMTP)-Verkehr weitergeleitet. Die Warteschlange für strikte Priorität wird geleert, bevor der Datenverkehr in den übrigen Warteschlangen weitergeleitet wird.
- 1 **Weighted Round Robin [gewichteter Reihum-Algorithmus]** — Stellt sicher, dass nicht eine einzige Anwendung die Weiterleitungskapazität des Geräts dominiert. Weighted Round Robin (WRR) leitet gesamte Warteschlangen in einer Reihum-Reihenfolge weiter. Die Warteschlangenvorgangsprioritäten werden durch die Länge der Warteschlange definiert. Je länger die Warteschlangenlänge ist, desto höher ist ihre Weiterleitungspriorität. Wenn zum Beispiel vier Warteschlangen die Warteschlangengewichtungen 1, 2, 3 und 4 haben, dann werden Pakete mit der höchsten Weiterleitungspriorität der Warteschlange 4 zugewiesen und die Pakete mit der niedrigsten Weiterleitungspriorität werden der Warteschlange 1 zugewiesen. Durch die Übertragung der höchsten Weiterleitungspriorität auf Warteschlangen mit der Länge 4 verarbeiten die Round-Robin-Prozesse Datenverkehr mit höherer Priorität und stellen gleichzeitig sicher, dass der Datenverkehr mit niedrigerer Priorität zufriedenstellend weiterbefördert wird.

Der Ablaufplan wird systemweit aktiviert. Warteschlangen, die dem strikten Prioritätsgrundsatz unterliegen, wird automatisch die höchste Priorität zugewiesen. Alle Werte werden standardgemäß als Strict Priority eingestellt. Beim Wechsel auf den WRR-Modus ist der Gewichtung-Standardwert 1. Die Gewichtungswerte für Warteschlangen können mit WRR in jeder beliebigen Reihenfolge zugewiesen werden. WRR-Werte können systemweit zugewiesen werden. Best-Effort-Datenverkehr wird stets der ersten Warteschlange zugewiesen. WRR-Werte müssen so zugewiesen werden, dass Warteschlange 1 Best-Effort bleibt.

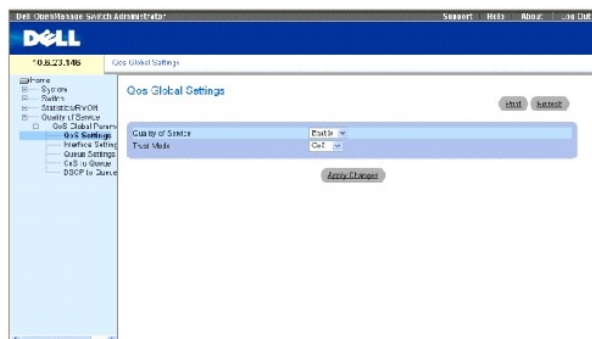
## Definition der globalen CoS-Parameter

Die globalen CoS (Class of Service)-Parameter werden auf den Seiten **CoS Global Parameter** eingestellt.

## Konfiguration der globalen QoS-Einstellungen

Die Seite „QoS Global Settings“ enthält Felder zur Aktivierung oder Deaktivierung von QoS. Außerdem kann der Trust-Modus ausgewählt werden. Der Trust-Modus beruht auf vordefinierten Feldern innerhalb des Datenpakets zur Ermittlung der Ausgabewarteschlange. Zum Öffnen der Seite [QoS Settings](#) klicken Sie auf Quality of Service → CoS Global Parameters → CoS Settings in der Strukturansicht.

Abb. 9-130. QoS-Einstellungen



**Quality of Service** — Aktiviert/deaktiviert die Verwaltung des Netzwerkverkehrs mit Quality of Service.

**Trust Mode**— Legt fest, welche Paketfelder für die Klassifikation von Paketen, die am Gerät eingehen, verwendet werden. Wenn keine Regeln definiert sind, wird der Datenverkehr mit dem vordefinierten Paketfeld (CoS oder DSCP) entsprechend der geltenden Trust-Modus-Tabelle zugewiesen. Datenverkehr, der kein vordefiniertes Paketfeld enthält, wird **Best-Effort** zugewiesen. Die möglichen Trust-Modus-Feldwerte sind:

**CoS** — Die Ausgabewarteschlangen-Zuordnung wird durch das IEEE802.1p VLAN Priority Tag (VPT) oder durch das einem Port zugewiesene Standard-VPT bestimmt.

**DSCP** — Die Ausgabewarteschlangen-Zuordnung wird durch das DSCP-Feld bestimmt.

 **ANMERKUNG:** Die Schnittstellen-Trust-Einstellungen setzen die globale Trust-Einstellung außer Kraft.

### Aktivieren von Quality of Service:

1. Öffnen Sie die Seite [QoS-Einstellungen](#).
2. Wählen Sie **Enable** im **CoS Mode**-Feld.
3. Klicken Sie auf Apply Changes.

Class of Service wird auf dem Gerät aktiviert.

### Aktivieren von Trust:

1. Öffnen Sie die Seite [QoS Settings](#).
2. Wählen Sie **Trust** im **Trust Mode**-Feld.
3. Klicken Sie auf Apply Changes.

Trust wird auf dem Gerät aktiviert.

### Aktivieren von Trust mit den CLI-Befehlen

In der folgenden Tabelle sind die entsprechenden CLI-Befehle zur Konfiguration von Feldern auf der Seite [QoS Settings](#) zusammengefasst.

**Tabelle 9-94. CLI-Befehle für CoS-Einstellungen**

CLI-Befehl	Beschreibung
<code>qos trust [cos   dscp]</code>	Konfiguriert das System mit Basic-Modus und Trust-Zustand.
<code>no cos trust</code>	Kehrt zum Non-Trust-Zustand zurück.

Das folgende Beispiel illustriert die CLI-Befehle:

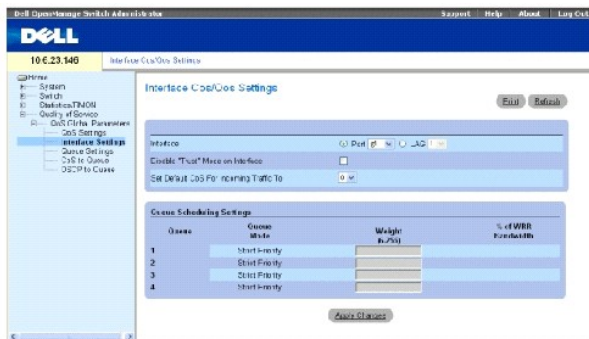
```
Console (config)# cos trust
dscp
```

### Definieren der QoS-Schnittstelleneinstellungen

Die Seite [Interface Cos/QoS Settings](#) enthält Felder zur Definition, jeweils für eine Schnittstelle, wenn der ausgewählte Trust-Modus aktiviert werden soll. Die

Standardpriorität für eingehende Pakete ohne Kennung wird ebenfalls auf der Seite [Interface Cos/QoS Settings](#) ausgewählt; klicken Sie dazu auf Quality of Service → CoS Global Parameters→ Interface Settings in der Strukturansicht.

Abb. 9-131. Cos/QoS-Schnittstelleneinstellungen



Interface — Der entsprechende zu konfigurierende Port oder LAG:

Disable „Trust“ Mode on Interface — Deaktiviert den Trust-Modus an der angegebenen Schnittstelle. Diese Einstellung setzt den auf dem Gerät global konfigurierten Trust-Modus außer Kraft.

Set Default CoS For Incoming Traffic To — Stellt den CoS-Standardkennungswert für Pakete ohne Kennung ein. Die CoS-Kennungswerte sind 0-7. Der Standardwert ist 0.

Queue — Die Nummer der Warteschlange.

Queue Mode — Gibt an, ob die Warteschlange Strict Priority oder WRR ist. Das wird auf dem Bildschirm **Queue Settings** definiert.

- 1 SP kann auf allen Warteschlangen 1 - 4 konfiguriert werden.
- 1 WRR kann auf allen Warteschlangen 1 - 4 konfiguriert werden.
- 1 SP-Modus kann auf Warteschlangen 1 - 2, mit WRR auf Warteschlangen 3 - 4 konfiguriert werden.
- 1 WRR-Modus kann auf Warteschlangen 1 - 2, mit SP auf Warteschlangen 3 - 4 konfiguriert werden.

Weight (6-255) — Weist den Warteschlangen WRR-Gewichtungen zu. Dieses Feld wird nur für Warteschlangen im WRR-Warteschlangenmodus aktiviert.

% of WRR Bandwidth — Die prozentuale Umsetzung der Gewichtung, die im Feld Weight (6-255) definiert wurde.

### Zuweisen von QoS/CoS-Einstellungen an eine Schnittstelle:

1. Öffnen Sie die Seite [Interface Cos/QoS Settings](#).
2. Wählen Sie eine Schnittstelle im Feld **Interface**.
3. Definieren Sie die Felder.
4. Klicken Sie auf **Apply Changes**

Die CoS-Einstellungen werden der Schnittstelle zugewiesen.

### Zuweisen von CoS-Schnittstellen mit den CLI-Befehlen

In der folgenden Tabelle sind die entsprechenden CLI-Befehle zur Konfiguration von Feldern auf der Seite [Interface Cos/QoS Settings](#) zusammengefasst.

Tabelle 9-95. CLI - Befehle für CoS-Schnittstellen

CLI - Befehl	Beschreibung
qos trust	Aktiviert für alle den Trust-Zustand.
qos cos default-cos	Konfiguriert den Standardport-CoS-Wert.
no qos trust	Deaktiviert den Trust-Zustand an jedem Port.

Das folgende Beispiel illustriert die CLI-Befehle:

```

Console (config)# interface ethernet g5

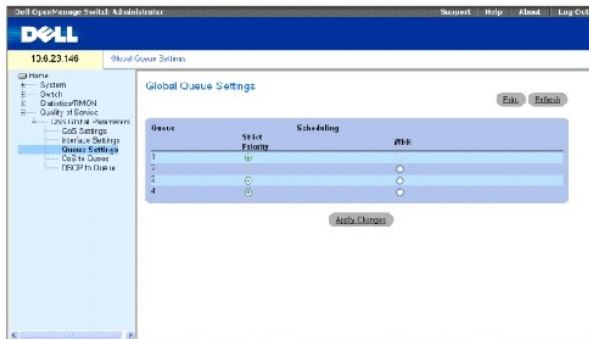
Console (config-if)# qos trust

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

## Definieren der Warteschlangeneinstellungen

Die Seite [Global Queue Setting](#) (Globale Warteschlangeneinstellungen) enthält Felder für die Konfiguration der Ablaufmethode, nach denen die Warteschlangen geführt werden. Zum Öffnen der Seite [Global Queue Setting](#) klicken Sie auf Quality of Service → CoS Global Parameters → Queue Settings in der Strukturansicht.

Abb. 9-132. Globale Warteschlangeneinstellung



Queues — Die Nummer der Warteschlange.

Strict Priority — Gibt an, dass die Verkehrsablaufplanung strikt auf der Warteschlangenpriorität basiert. Diese Einstellung ist standardgemäß aktiviert.

WRR — Gibt an, ob der Verkehrsablaufplan auf Weighted Round Robin (WRR)-Gewichtungen für Ausgangswarteschlangen basiert.

## Definieren der Warteschlangeneinstellungen

1. Öffnen Sie die Seite [Global Queue Setting](#).
2. Definieren Sie die Felder.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Warteschlangeneinstellungen werden definiert und das Gerät wird aktualisiert.

## Zuweisen von Warteschlangeneinstellungen mit den CLI-Befehlen

In der folgenden Tabelle sind die entsprechenden CLI-Befehle zur Konfiguration von Feldern auf der Seite [Global Queue Setting](#) zusammengefasst.

**Tabelle 9-96. CLI-Befehle für Warteschlangeneinstellungen**

CLI-Befehl	Beschreibung
wrr-queue bandwidth weight1 weight2 . weight_n	Weist Weighted Round Robin (WRR)-Gewichtungen zu Ausgangswarteschlangen zu.
show qos interface [ethernet interface-number] [queuing]	Zeigt QoS-Schnittstellendaten an.

Das folgende Beispiel illustriert die CLI-Befehle:

```

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

Console(config)# exit

Console # exit

Console> show qos interface ethernet g1 queuing

Ethernet g1

wrr bandwidth weights and EF priority:

```

```

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

Console(config)# exit

Console # exit

Console> show qos interface ethernet g1 queuing

Ethernet g1

wrr bandwidth weights and EF priority:

```

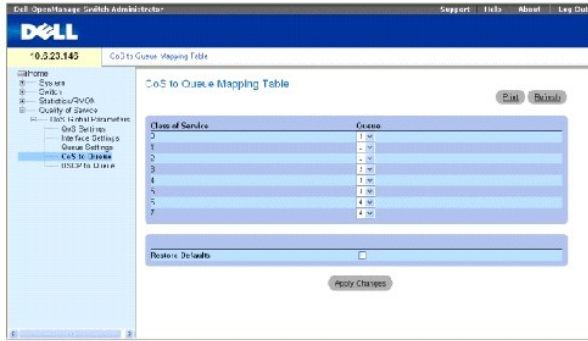
qid	weights	EF	Priority

-----	-----	-----	-----
-			
1	125	Disable	-
2	125	Disable	-
3	125	Disable	-
4	125	Disable	-
<p>Cos queue map:</p> <p>Cos qid</p> <p>0 2</p> <p>1 1</p> <p>2 1</p> <p>3 2</p> <p>4 3</p> <p>5 3</p> <p>6 4</p> <p>7 4</p>			

## Zuweisen von CoS-Werten zu Warteschlangen

Die Seite [CoS to Queue Mapping Table](#) enthält Felder zur Klassifikation von CoS-Einstellungen zu Datenverkehrs-Warteschlangen. Zum Öffnen der Seite [CoS to Queue Mapping Table](#) klicken Sie auf Quality of Service→ CoS Global Parameters→ CoS to Queue in der Strukturansicht.

Abb. 9-133. Zuweisungstabelle: CoS zu Warteschlange



Class of Service — Gibt die CoS-Prioritätskennungs-Werte an, wobei Null der niedrigste und 7 der höchste Wert ist.

Queue — Die Warteschlange zur Weiterleitung des Datenverkehrs, der die CoS-Priorität zugewiesen wurde. Es werden vier Prioritätswarteschlangen für Datenverkehr unterstützt.

Restore Defaults — Stellt die Werkzeugeinstellungen des Geräts zur Zuweisung von CoS-Werten zu einer Weiterleitungswarteschlange wieder her.

### Zuweisen eines CoS-Werts an eine Warteschlange

1. Öffnen Sie die Seite [CoS to Queue Mapping Table](#) (CoS an Warteschlangen-Zuweisungstabelle).
2. Wählen Sie einen CoS-Eintrag.
3. Definieren Sie die Warteschlangennummer im Feld **Queue** (Warteschlange).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der CoS-Wert wird einer Warteschlange zugewiesen und das Gerät wird aktualisiert.

### Zuweisen von CoS-Werten zu Warteschlangen mit den CLI-Befehlen

In der folgenden Tabelle sind die entsprechenden CLI-Befehle zur Konfiguration von Feldern auf der Seite [CoS to Queue Mapping Table](#) zusammengefasst.

**Tabelle 9-97. CLI-Befehle für die Zuweisung von CoS zu Warteschlangeneinstellungen**

CLI-Befehl	Beschreibung
wrr-queue cos-map queue-id cos1..cos8	Weist den Ausgangswarteschlangen die zugewiesenen CoS-Werte zu.

Das folgende Beispiel illustriert die CLI-Befehle:

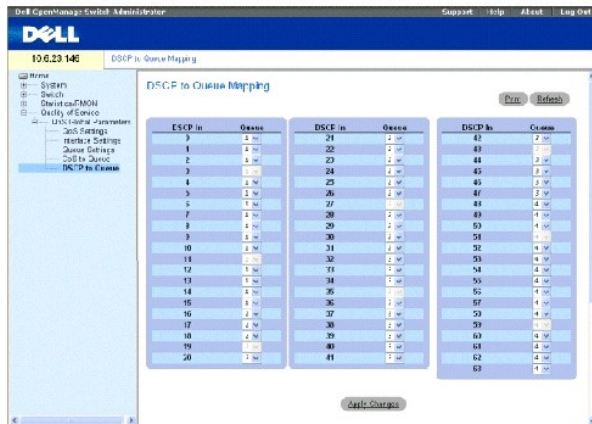
```
Console (config)# wrr-queue cos-map 4 7
```

### Zuweisen von DSCP-Werten zu Warteschlangen

Die Seite [DSCP Mapping](#) stellt Felder bereit zur Definition von spezifischen DSCP-Feldern für die Ausgangswarteschlange. Zum Öffnen der Seite [DSCP Mapping](#) klicken Sie auf Quality of Service → CoS Global Parameters → DSCP Mapping in der Strukturansicht.

 **ANMERKUNG:** Eine Liste der DSCP-Standard-Warteschlangeneinstellungen finden Sie unter [„Zuweisungstabelle: DSCP zu Warteschlange, Standardwerte“](#).

Abb. 9-134. DSCP-Zuweisung



DSCP In – Die Werte des DSCP-Feldes im eingehenden Paket.

Queue – Die Warteschlange, der Pakete mit dem jeweiligen DSCP-Wert zugewiesen werden. Die Werte sind 1-4, wobei 1 der niedrigste und 4 der höchste Wert ist.

### Zuweisen eines DSCP-Wertes und Zuordnung einer Prioritätswarteschlange:

1. Öffnen Sie die Seite [DSCP Mapping](#) (DSCP-Zuweisung).
2. Wählen Sie einen Wert in der die Spalte **DSCP In** (DSCP ein).
3. Definieren Sie die Felder **Queue** (Warteschlange).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen)

Der DSCP wird überschrieben und der Wert wird einer Weiterleitungswarteschlange zugewiesen.

### Zuweisen von DSCP-Werten mit den CLI-Befehlen

In der folgenden Tabelle sind die entsprechenden CLI-Befehle zur Konfiguration von Feldern auf der Seite [DSCP Mapping](#) zusammengefasst.

Tabelle 9-98. CLI-Befehle für Zuweisung eines DSCP-Wertes zu Warteschlangen

CLI-Befehl	Beschreibung
<code>qos map dscp-queue dscp-list to queue-id</code>	Ändert die DSCP-Zuweisung zu einer Warteschlange.

Das folgende Beispiel illustriert die CLI-Befehle:

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





[Zurück zum Inhaltsverzeichnis](#)

## Gerätespezifikationen:

Dell™ PowerConnect™ 5324 System-Benutzerhandbuch

- [Anschluss- und Kabelspezifikationen](#)
- [Betriebsbedingungen](#)
- [Gerätespezifikationen](#)
- [Angaben zum Gerätespeicher](#)
- [Angaben zu den Funktionen](#)

Dieser Anhang enthält die zum Betrieb des Geräts erforderlichen Informationen.

---

## Schnittstellen- und Kabelspezifikationen

Dieser Abschnitt beschreibt die Anschlussspezifikationen.

### Portspezifikationen

Die folgende Tabelle beschreibt die Anschlussarten des Geräts.

Tabelle 10-99.

Gerät	Spezifikation
PowerConnect 5324	<ul style="list-style-type: none"><li>1 24 GE-Ports</li><li>1 4 SFP-Ports</li><li>1 RS-232-Konsolen-Port</li></ul>
<b>Porttypen</b>	
RJ-45	<ul style="list-style-type: none"><li>1 10 Base-T</li><li>1 100 Base-T</li><li>1 1000 Base-T</li></ul>
SFP	Unterstützt Standard Small Form-Factor Gigabit Plug-Transceiver
<b>Porteinstellungen</b>	
	<ul style="list-style-type: none"><li>1 Auto-Negotiation (automatische Verbindungsaushandlung) für Geschwindigkeit, Duplexmodus und Datenflusssteuerung</li><li>1 Backpressure (Zurückweisung)</li><li>1 Head of Line Blocking (HOL)</li><li>1 Automatisches MDI/MDIX</li><li>1 Portspiegelung</li><li>1 Broadcast Storm-Kontrolle</li></ul>

Portspezifikationen

---

## Betriebsbedingungen

Dieser Abschnitt enthält eine detaillierte Beschreibung der Betriebsbedingungen, einschließlich Betriebstemperatur und relative Luftfeuchtigkeit.

Tabelle 10-100.

Funktion	Spezifikation
Betriebstemperatur	0 °C bis 40 °C
Relative Luftfeuchtigkeit bei Betrieb	10 % bis 90 % nicht-kondensierend

Betriebsbedingungen

---

## Gerätespezifikationen

Dieser Abschnitt enthält eine detaillierte Beschreibung der Gerätespezifikationen.

Tabelle 10-101.

Funktion	Spezifikation
Größe des Geräts	1 Breite 19 Zoll (48,3 cm) 1 Höhe der Einheit
Belüftung	Zwei Lüfter pro Einheit.

Gerätespezifikationen

---

## Spezifikationen des Gerätespeichers

In diesem Abschnitt werden die Spezifikationen des Gerätespeichers beschrieben.

Tabelle 10-102.

Speichertyp	Kapazität
CPU DRAM	64 MB
Flash-Speicher	16 MB
Paket-Pufferspeicher	2 Mb

Spezifikationen des Gerätespeichers

---

## Angaben zu den Funktionen

### VLAN

- 1 VLAN-Unterstützung für Tagging (Kennung) und portbasiert gemäß IEEE 802.1Q
- 1 Bis zu 4094 VLANs unterstützt
- 1 Reservierte VLANs für interne Systemverwendung
- 1 Dynamische VLANs mit GVRP-Unterstützung
- 1 Protokollbasierte VLANs

### Quality of Service (Servicequalität)

- 1 Layer-2-Trust-Modus (IEEE 802.1p Tagging)
- 1 Layer-3-Trust-Modus (DSCP)
- 1 Einstellbares Weighted Round Robin (WRR)
- 1 Einstellbares Strict Queue Scheduling

### Layer-2-Multicast

- 1 Dynamische Multicast-Unterstützung - bis zu 256 Multicast-Gruppen unterstützt in IGMP Snooping oder statischem Multicast

### Gerätesicherheit

- 1 Kennwortschutz für Switch-Zugriff
- 1 Portbasierte MAC-Adressen-Warnung und Sperre

- 1 RADIUS-Remote-Authentifizierung für Switch-Verwaltungszugriff
- 1 TACACS+
- 1 Verwaltungszugriff-Filterung mit Verwaltungs-Zugriffsprofilen
- 1 SSH/SSL-Verwaltungsverschlüsselung

## Weitere Switching-Funktionen

- 1 Link Aggregation mit Unterstützung von bis zu 8 Aggregated Links pro Gerät und bis zu 8 Ports pro Aggregated Link (IEEE 802.3ad)
- 1 LACP-Unterstützung
- 1 Unterstützung für Jumbo-Frames bis zu 10K
- 1 Broadcast Storm-Kontrolle
- 1 Portspiegelung

## Geräteverwaltung

- 1 Web-basierte Verwaltungsschnittstelle
- 1 CLI-Zugänglichkeit über Telnet
- 1 SNMPv1 und SNMP v2 werden unterstützt
- 1 4 RMON-Gruppen werden unterstützt
- 1 TFTP-Übertragungen von Firmware- und Konfigurationsdateien
- 1 Doppelte integrierte Firmware-Images
- 1 Unterstützung von Upload/Download mehrerer Konfigurationsdateien
- 1 Statistiken für Fehlerüberwachung und Leistungsoptimierung
- 1 BootP/DHCP IP-Adressenverwaltung unterstützt
- 1 Syslog Remote-Logging-Funktionalität
- 1 SNMP-Unterstützung
- 1 Layer-3-Traceroute
- 1 Telnet-Client
- 1 DNS-Client

---

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Konfigurieren von Geräteinformationen:

Dell PowerConnect 5324 System-Benutzerhandbuch

- [Konfigurieren der Netzwerksicherheit](#)
- [Konfigurieren von Ports](#)
- [Konfigurieren von Adresstabellen](#)
- [Konfigurieren von GARP](#)
- [Konfigurieren des Spanning Tree-Protokolls](#)
- [Konfigurieren von VLANs](#)
- [Aggregieren von Ports](#)
- [Unterstützung von Multicast-Weiterleitung](#)

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

---

## Konfigurieren der Netzwerksicherheit

Auf diesem Gerät kann die Netzwerksicherheit wahlweise per ACL (Access Control Lists) oder Locked Ports (gesperrte Anschlüsse) eingerichtet werden. Öffnen Sie die Seite **Network Security** (Netzwerksicherheit), indem Sie Switch → Network Security auswählen.

## Übersicht über die Netzwerksicherheit

In diesem Abschnitt werden die Netzwerksicherheitsfunktionen beschrieben.

### Portbasierte Authentifizierung (802.1x)

Portbasierte Authentifizierung ermöglicht die Authentifizierung von Systembenutzern auf Port-Basis über einen externen Server. Nur authentifizierte und genehmigte Systembenutzer können Daten übertragen und empfangen. Ports werden über den RADIUS (Remote Authentication Dial In User Service)-Server unter Einsatz des Extensible Authentication-Protokolls (EAP) authentifiziert. Die Port-Authentifizierung umfasst:

- 1 **Authenticators** Gibt den Port an, der authentifiziert wird, bevor ein Systemzugriff gewährt wird.
- 1 **Supplicants** Gibt den Host an, der mit dem authentifizierten Port verbunden ist, der Zugriff auf Systemdienste anfordert.
- 1 **Authentication Server (Authentifizierungs-Server)** Gibt den externen Server an, z.B. den RADIUS-Server, der die Authentifizierung für den Authenticator durchführt, und gibt an, ob der Benutzer zum Zugriff auf Systemdienste autorisiert ist.

Die portbasierte Authentifizierung erzeugt zwei Zugriffszustände:

- 1 **Controlled Access** Ermöglicht die Kommunikation zwischen dem Benutzer und dem System, wenn der Benutzer autorisiert ist.
- 1 **Uncontrolled Access** Ermöglicht freie Kommunikation, unabhängig vom Portstatus.

Das Gerät unterstützt zurzeit die portbasierte Authentifizierung über den RADIUS-Server.

### Erweiterte portbasierte Authentifizierung

Die erweiterte portbasierte Authentifizierung ermöglicht die Verbindung mehrerer Hosts an einem Port. Die erweiterte portbasierte Authentifizierung erfordert lediglich, dass ein Host autorisiert ist, damit alle Hosts Systemzugriff haben. Wenn der Port nicht autorisiert ist, wird allen angeschlossenen Hosts der Zugriff auf das Netzwerk verweigert.

Die erweiterte portbasierte Authentifizierung ermöglicht auch eine benutzerbasierte Authentifizierung. Bestimmte VLANs im Gerät sind immer verfügbar, selbst

wenn bestimmte am VLAN angeschlossene Ports nicht autorisiert sind. Zum Beispiel ist für Voice über IP keine Authentifizierung erforderlich, während diese jedoch für Datenverkehr erforderlich ist. VLANs, für die keine Authentifizierung erforderlich ist, können definiert werden. Den Benutzern stehen nicht authentifizierte VLANs zur Verfügung, selbst wenn die am VLAN angeschlossenen Ports als autorisiert definiert sind.

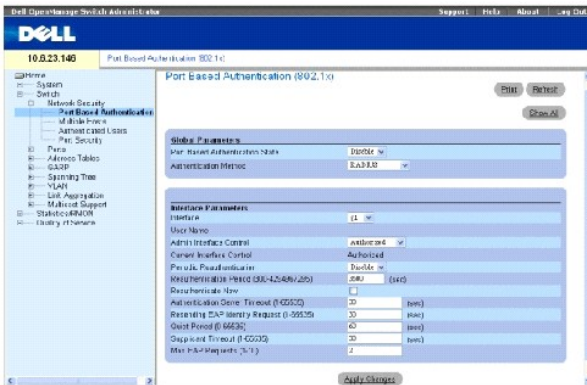
Die erweiterte portbasierte Authentifizierung wird in den folgenden Modi implementiert:

- 1 **Single Host Mode** Ermöglicht nur dem autorisierten Host Zugriff auf den Port.
- 1 **Multiple Host Mode** Ermöglicht die Verbindung mehrerer Hosts an einem Port. Nur ein Host muss autorisiert sein, um allen Hosts Netzwerkzugriff zu geben. Wenn die Host-Authentifizierung fehlschlägt oder eine EAPOL-Logoff-Meldung erhalten wird, wird allen angeschlossenen Clients der Netzwerkzugriff verwehrt.

## Konfigurieren der portbasierten Authentifizierung

Die Seite [Portbasierte Authentifizierung](#) enthält Felder zur Konfiguration der portbasierten Authentifizierung. Öffnen Sie die Seite [Portbasierte Authentifizierung](#), indem Sie auf Switch → Network Security → Port Based Authentication klicken.

Abb. 7-80. Portbasierte Authentifizierung



**Port Based Authentication State** Ermöglicht die portbasierte Authentifizierung für das Gerät. Folgende Feldwerte können ausgewählt werden:

**Enable** Aktiviert die portbasierte Authentifizierung für das Gerät.

**Disable** Deaktiviert die portbasierte Authentifizierung für das Gerät.

**Authentication Method** Gibt die verwendete Authentifizierungsmethode an. Folgende Feldwerte können ausgewählt werden:

**None** Es wird keine Authentifizierungsmethode zur Authentifizierung des Ports verwendet.

**RADIUS** Die Authentisierung des Ports wird über den RADIUS-Server durchgeführt.

**RADIUS, None** Die Authentisierung des Ports wird zuerst über den RADIUS-Server durchgeführt. Wenn der Port nicht authentifiziert wird, wird keine Authentifizierungsmethode verwendet und die Sitzung wird zugelassen.

**Interface** Enthält eine Schnittstellenliste.

**User Name** Gibt den Benutzernamen, wie er im RADIUS-Server konfiguriert ist, an.

**Admin Interface Control** Definiert den Port-Autorisierungsstatus. Folgende Feldwerte können ausgewählt werden:

**Authorized** Stellt den Schnittstellenstatus auf autorisiert ein (Verkehr zulassen).

**Unauthorized** Stellt den Schnittstellenstatus auf nicht autorisiert ein (Verkehr verweigern).

**Auto** Der Autorisierungszustand wird durch die Autorisierungsmethode eingestellt.

**Current Interface Control** Gibt den gegenwärtig konfigurierten Autorisierungszustand des Ports an.

**Periodic Reauthentication** Führt, wenn aktiviert, periodisch eine erneute Authentifizierung des Ports durch. Das Intervall für die erneute Authentifizierung wird im Feld **Reauthentication Period (300-4294967295)** festgelegt.

**Reauthentication Period (300-4294967295)** Zeigt die Zeitspanne an, nach der der ausgewählte Port erneut authentifiziert wird. Der Feldwert wird in Sekunden angegeben. Der Standardwert des Feldes ist 3600 Sekunden.

**Reauthenticate Now** Ermöglicht, wenn ausgewählt, die sofortige Reauthentifizierung des Ports.

**Authentication Server Timeout (1-65535)** Legt die Zeit fest, die vergeht, bevor das Gerät eine Anforderung an den Authentifizierungsserver erneut sendet. Der Feldwert wird in Sekunden angegeben. Der Standardwert des Feldes ist 30 Sekunden.

**Resending EAP Identity Request (1-65535)** Legt die Zeit fest, die vergeht, bevor eine EAP-Anforderung erneut gesendet wird. Der Standardwert des Feldes ist 30 Sekunden.

**Quiet Period (0-65535)** Die Anzahl der Sekunden, die das Gerät im Untätigkeitszustand verbleibt, nachdem eine Authentifizierungskommunikation fehlgeschlagen ist. Der mögliche Feldbereich ist 0-65535. Der Standardfeldwert ist 60 Sekunden.

**Supplicant Timeout (1-65535)** Legt die Zeit fest, die vergeht, bevor EAP-Anforderungen erneut an den Benutzer gesendet werden. Der Feldwert wird in Sekunden angegeben. Der Standardwert des Feldes ist 30 Sekunden.

**Max EAP Requests (1-10)** Gibt die Gesamtzahl der gesendeten EAP-Anforderungen an. Wenn nicht nach der angegebenen Zeit eine Antwort erhalten wird, wird der Authentifizierungsprozess neu gestartet. Der Standardfeldwert ist 2 Neuversuche.

## Anzeigen der portbasierten Authentifizierungstabelle

1. Öffnen Sie die Seite [Port Based Authentication](#).
2. Klicken Sie auf Show All (Alle anzeigen).

Die [Port Based Authentication Table](#) wird geöffnet:

**Abb. 7-81. Portbasierte Authentifizierungstabelle**

**Termination Cause** Zeigt den Grund für den Abbruch der Port-Authentifizierung an.

**Copy To Checkbox** Kopiert Portparameter von einem Port zu den ausgewählten Ports.

**Select All** Dient zur Auswahl aller Ports in der [Port Based Authentication Table](#).

### Kopieren von Parametern in die [Portbasierte Authentifizierungstabelle](#)

1. Öffnen Sie die Seite [Port Based Authentication](#).
2. Klicken Sie auf Show All (Alle anzeigen).

Die [Port Based Authentication Table](#) wird geöffnet.

3. Wählen Sie die Schnittstelle im Feld **Copy Parameters from** (Kopieren der Parameter von).
4. Wählen Sie eine Schnittstelle in der [Port Based Authentication Table](#).
5. Aktivieren Sie das Kontrollkästchen **Copy to** (Kopieren von), um die Schnittstellen zu definieren, auf die die portbasierten Authentifizierungsparameter kopiert werden.
6. Klicken Sie auf Apply Changes (Änderungen übernehmen).

Die Parameter werden auf den ausgewählten Port in der [Port Based Authentication Table](#) kopiert und das Gerät wird aktualisiert.

### Aktivieren der portbasierten Authentifizierung mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Aktivierung der portbasierten Authentifizierung, wie auf der Seite [Port Based Authentication](#) angezeigt, zusammen.

Tabelle 7-49. CLI-Befehle zur Port-Authentifizierung

CLI-Befehl	Beschreibung
<code>aaa authentication dot1x default method1 [method2]</code>	Gibt eine oder mehrere AAA (Authentifizierung, Autorisierung und Abrechnung)-Methoden zur Verwendung auf Schnittstellen, die IEEE 802.1X entsprechen, an.
<code>dot1x max-req count</code>	Stellt die maximale Anzahl der EAP-Sendeveruche des Geräts an den Client ein, bevor der Authentifizierungsprozess neu gestartet wird.
<code>dot1x re-authenticate [ethernet interface]</code>	Initiiert eine manuelle Reauthentifizierung aller 802.1X-aktivierten Ports oder des angegebenen 802.1X-aktivierten Ports.
<code>dot1x re-authentication</code>	Aktiviert die periodische Reauthentifizierung eines Clients.
<code>dot1x timeout quiet-period seconds</code>	Stellt die Anzahl der Sekunden ein, die das Gerät im Untätigkeitszustand verbleibt, nachdem ein Authentifizierungsaustausch fehlgeschlagen ist.
<code>dot1x timeout re-authperiod seconds</code>	Stellt die Anzahl der Sekunden zwischen Reauthentifizierungsversuchen ein.
<code>dot1x timeout server-timeout</code>	Stellt die Zeit für die erneute Übertragung von Paketen an den Authentifizierungsserver ein.



<i>seconds</i>	
<b>dot1x timeout supp-timeout</b> <i>seconds</i>	Stellt die Zeit für die erneute Übertragung eines EAP-Anforderungs-Frame an den Client ein.
<b>dot1x timeout tx-period</b> <i>seconds</i>	Stellt die Anzahl der Sekunden ein, die das Gerät auf eine Antwort auf einen EAP-Anforderungs-/Identitäts-Frame vom Client wartet, bevor die Anforderung erneut gesendet wird.
<b>show dot1x</b> [ <i>ethernet interface</i> ]	Zeigt den 802.1X-Status für das Gerät oder für die angegebene Schnittstelle ein.
show dot1x users [ <i>username username</i> ]	Zeigt 802.1X-Benutzer für das Gerät an.

Das folgende Beispiel illustriert die CLI-Befehle:

```

Console> enable

Console# show dot1x

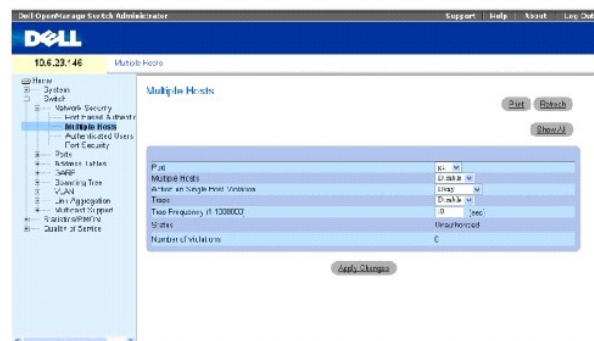
```

Schnittstelle	Admin Mode	Oper Mode	Reauth Control	Reauth Period	Benutzername
-----	-----	-----	-----	-----	-----
g1	Auto	Authorized	Ena	3600	Bob
g2	Auto	Authorized	Ena	3600	John
g3	Auto	Unauthorized	Ena	3600	Clark
g4	Force-auth	Authorized	Dis	3600	Nicht verfügbar

## Konfigurieren der erweiterten portbasierten Authentifizierung

Die Seite [Mehrere Hosts](#) enthält Informationen zur Definition der Einstellungen für die erweiterte portbasierte Authentifizierung für bestimmte Ports. Öffnen Sie die Seite [Mehrere Hosts](#), indem Sie auf Switch → Network Security → Multiple Hosts klicken.

Abb. 7-82. Mehrere Hosts



**Port** Gibt die Anschlussnummer, für die die erweiterte portbasierte Authentifizierung aktiviert wird, an.

**Multiple Hosts** Aktiviert/deaktiviert einen Host zur Autorisierung des Systemzugriffs mehrerer Hosts. Diese Einstellung muss aktiviert werden, um entweder

den EingangsfILTER zu aktivieren oder die Port-Lock-Sicherheitsfunktion am ausgewählten Port zu verwenden.

**Action on Single Host Violation** Definiert die Aktion, die auf im Single-Host-Modus eingehende Pakete angewendet wird, die von einem Host kommen, dessen MAC-Adresse nicht der Client (Supplicant)-MAC-Adresse entspricht. Das Feld **Action on Single Host Violation** kann nur dann definiert werden, wenn das Feld **Multiple Hosts** als **Disable** definiert ist. Folgende Feldwerte können ausgewählt werden:

**Permit** Leitet die Pakete unbekanntem Ursprungs weiter, jedoch wird die MAC-Adresse nicht gelernt.

**Deny** Lehnt die Pakete von einer nicht gelernten Quelle ab. Dies ist die Standardeinstellung.

**Shutdown** Lehnt das Paket von einer nicht gelernten Quelle ab und sperrt den Port. Die Ports bleiben gesperrt, bis sie aktiviert werden oder das Gerät zurückgesetzt wird.

**Traps** Aktiviert/deaktiviert das Senden von Traps an den Host bei Auftreten eines Verstoßes.

**Trap Frequency (1-1000000) (Sec)** Legt das Intervall fest, in dem Traps an den Host gesandt werden. Das Feld **Trap Frequency (1-1000000)** kann nur dann definiert werden, wenn das Feld **Multiple Hosts** als **Disable** definiert ist. Der Standardwert des Feldes ist 10 Sekunden.

**Status** Gibt den Hoststatus an. Folgende Feldwerte können ausgewählt werden:

**Unauthorized** Client (Supplicants) haben umfassenden Portzugriff.

**Authorized** Client (Supplicants) haben eingeschränkten Portzugriff.

**No single-host** **Multiple Hosts** ist aktiviert.

**Number of Violations** Gibt die Anzahl der im Single-Host-Modus an der Schnittstelle eingegangenen Pakete an, die von einem Host kommen, dessen MAC-Adresse nicht der Client (Supplicant)-MAC-Adresse entspricht.

### Anzeigen der [Multiple Hosts Table](#)

1. Öffnen Sie die Seite [Multiple Hosts](#).
2. Klicken Sie auf Show All (Alle anzeigen).

Die [Multiple Hosts Table](#) wird geöffnet:

Abb. 7-83. Multiple Hosts-Tabelle

Multiple Hosts Table

Default

Port	Enable Multiple Hosts	Action on Violation	Enable Traps	Trap Frequency	Status	Number of Violations
1	g1	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
2	g2	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
3	g3	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
4	g4	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
5	g5	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
6	g6	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
7	g7	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
8	g8	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
9	g9	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
10	g10	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
11	g11	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
12	g12	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
13	g13	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
14	g14	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
15	g15	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
16	g16	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
17	g17	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
18	g18	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
19	g19	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
20	g20	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
21	g21	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
22	g22	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
23	g23	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
24	g24	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0

Apply Changes

### Aktivieren mehrerer Hosts mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Aktivierung der erweiterten portbasierten Authentifizierung, wie auf der Seite [Multiple Hosts](#) angezeigt, zusammen.

Tabelle 7-50. CLI-Befehle für mehrere Hosts

CLI-Befehl	Beschreibung
<code>dot1x multiple-hosts</code>	Ermöglicht mehrere Hosts (Clients) für einen 802.1X-authorized Port, bei dem der Schnittstellenkonfigurationsbefehl <code>dot1x port-control</code> auf <code>auto</code> gesetzt ist.
<code>dot1x single-host-violation {forward  discard  discard-shutdown} [trap seconds]</code>	Legt die Aktion fest, die erfolgt, wenn eine Station, deren MAC-Adresse nicht die Client (Supplicant)-MAC-Adresse ist, einen Zugriff auf die Schnittstelle versucht.

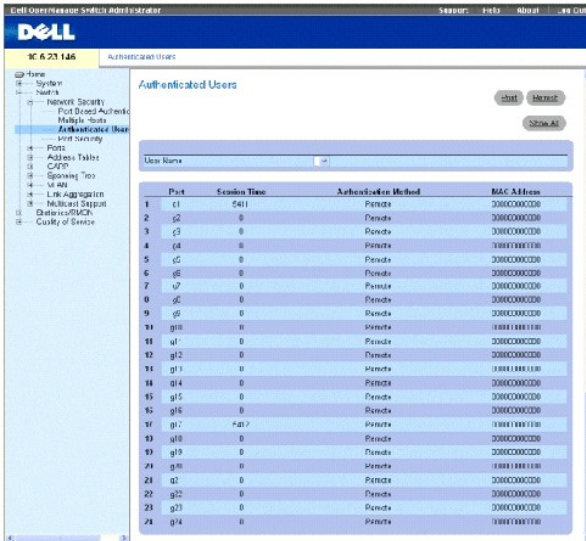
Das folgende Beispiel illustriert die CLI-Befehle:

```
Neyland# configure
Neyland(config)# interface ethernet g1
Neyland(config-if)# dot1x multiple-hosts
```

### Authentifizieren von Benutzern

Die Seite [Authenticated Users](#) zeigt Benutzer-Portzugriffslisten an. Die Benutzerzugriffslisten werden auf der Seite Add User Name definiert. Öffnen Sie die Seite [Authenticated Users](#), indem Sie auf Switch → Network Security → Authenticated Users klicken.

Abb. 7-84. Authentifizierte Benutzer



**User Name** Zeigt die Liste der Benutzer an, die über den RADIUS-Server autorisiert wurden.

**Port** Zeigt den/die für die Authentifizierung verwendeten Port(s) an - nach dem Benutzernamen.

**Session Time** Die Zeitdauer, die der Benutzer am Gerät angemeldet war. Das Feldformat lautet **Tage:Stunden:Minuten:Sekunden**, z.B. 3 Tage:2 Stunden: 4 Minuten: 39 Sekunden.

**Last Authentication** Die Zeit, die seit der letzten Authentifizierung des Benutzers vergangen ist. Das Feldformat lautet **Tage:Stunden:Minuten:Sekunden**, z.B. 3 Tage:2 Stunden 4 Minuten: 39 Sekunden.

**Authentication Method** Die Methode, mit der die letzte Sitzung authentifiziert wurde. Folgende Feldwerte sind möglich:

**Remote** Der Benutzer wurde von einem Remote-Server authentifiziert.

**None** Der Benutzer wurde nicht authentifiziert.

**MAC Address** Gibt die MAC-Adresse des Client (Supplicant) an.

## Anzeigen der Tabelle authentifizierter Benutzer

1. Öffnen Sie die Seite Add User Name.
2. Klicken Sie auf Show All (Alle anzeigen).

Die **Authenticated Users Table** wird geöffnet:

**Abb. 7-85. Tabelle authentifizierter Benutzer**

Authenticated Users Table Reset

User Name	Port	Session Time	Authentication Method	MAC Address
-----------	------	--------------	-----------------------	-------------

## Authentifizierung von Benutzern mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Authentifizierung von Benutzern, wie auf der Seite Add User Name angezeigt, zusammen.

Tabelle 7-51. CLI-Befehle zum Hinzufügen von Benutzernamen

CLI-Befehl	Beschreibung
<code>show dot1x users [username username]</code>	Zeigt 802.1X-Benutzer für das Gerät an.

Das folgende Beispiel illustriert die CLI-Befehle:

console# show dot1x users					
Benutzername	Session Time	Last Auth	Auth Method	MAC-Adresse	Schnittstelle
-----	-----	-----	-	-----	-----
Bob	1d3h	58m	Fern	00:08:3b:79:87:87	g1
John	8h19m	2m	Keine	00:08:3b:89:31:27	g2

## Konfigurieren der Port-Sicherheit

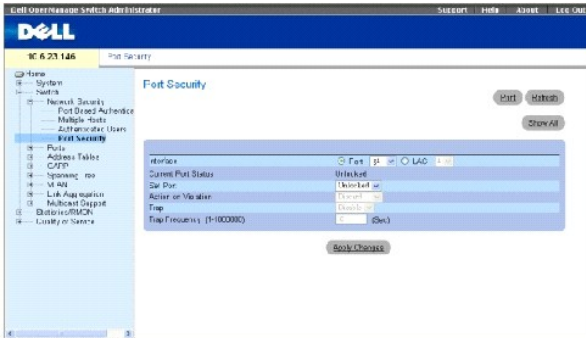
Die Netzwerksicherheit kann erhöht werden, indem der Zugriff auf bestimmte Ports auf Benutzer mit bestimmten MAC-Adressen beschränkt wird. Die MAC-Adressen können bis zu dem Punkt dynamisch gelernt werden oder sie können statisch konfiguriert werden. Bei Verwendung der Locked-Port-Sicherheitsfunktion werden sowohl eingegangene als auch erfasste Pakete, die an bestimmten Ports eingehen, überwacht. Der Zugriff auf die gesperrten Ports ist auf Benutzer mit bestimmten MAC-Adressen beschränkt. Diese Adressen werden entweder manuell für den Port definiert oder sie werden an dem Port bis zu dem Zeitpunkt, an dem der Port gesperrt wird, erfasst. Wenn ein Paket an einem gesperrten Port eingeht und die MAC-Quelladresse des Pakets nicht mit dem Port verknüpft ist (d.h. sie wurde entweder an einem anderen Port erfasst oder ist dem System nicht bekannt), wird der Schutzmechanismus ausgelöst, der verschiedene Optionen bietet. Nicht autorisierte Pakete, die an einem gesperrten Port eingehen, werden entweder:

- 1 Weitergeleitet
- 1 Ohne Trap abgelehnt
- 1 Mit Trap abgelehnt
- 1 Der Eingangsport wird deaktiviert

Die Locked-Port-Sicherheitsfunktion ermöglicht auch das Speichern einer Liste von MAC-Adressen in der Konfigurationsdatei. Die MAC-Adressliste kann nach einem Zurücksetzen des Geräts wiederhergestellt werden.

Deaktivierte Ports werden von der Seite **Port Parameters** aus aktiviert - siehe [„Definieren von Portparameter“](#). Öffnen Sie die Seite [Port Security](#), indem Sie auf Switch→ Network Security→ Port Security klicken.

### Abb. 7-86. Port-Sicherheit



**Interface** Gibt den Typ der ausgewählten Schnittstelle an, an der die Locked-Port-Funktion aktiviert wird.

**Port** Der Typ der ausgewählten Schnittstelle ist ein Port.

**LAG** Der Typ der ausgewählten Schnittstelle ist eine LAG.

**Current Port Status** Gibt den gegenwärtig konfigurierten Portzustand an.

**Set Port** Der Port ist entweder gesperrt oder nicht gesperrt. Folgende Feldwerte können ausgewählt werden:

**Unlocked** Entsperrt den Port. Dies ist der Standardwert.

**Locked** Sperrt den Port.

**Action on Violation** Die Aktion, die auf Pakete angewandt wird, die an einem gesperrten Port ankommen. Folgende Feldwerte können ausgewählt werden:

**Forward** Leitet die Pakete unbekanntem Ursprungs weiter, ohne dass jedoch die MAC-Adresse erfasst wird.

**Discard** Lehnt die Pakete von einer nicht erfassten Quelle ab. Dies ist die Standardeinstellung.

**Shutdown** Lehnt das Paket von einer nicht erfassten Quelle ab und sperrt den Port. Die Ports bleiben gesperrt, bis sie aktiviert werden oder das Gerät zurückgesetzt wird.

**Trap** Aktiviert das Senden von Traps, wenn ein Paket an einem gesperrten Port eingeht.

**Trap Frequency (1-1000000)** Die Zeit (in Sekunden) zwischen Traps. Dieses Feld gilt nur für gesperrte Ports. Der Standardwert lautet 10 Sekunden.

## Definieren eines gesperrten Ports

1. Öffnen Sie die Seite [Port Security](#).
2. Wählen Sie einen Schnittstellentyp und -nummer.
3. Definieren Sie die Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der gesperrte Port wird der [Port Security Table](#) hinzugefügt und das Gerät wird aktualisiert.

### Anzeigen der Locked Port-Tabelle

1. Öffnen Sie die Seite [Port Security](#).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die [Port Security Table](#) wird geöffnet:

Gesperrte Ports können auch von der Locked Ports Table und der Seite [Port Security](#) aus definiert werden.

Abb. 7-87. Port Security-Tabelle

Port	Current Port Status	Set Port	Action	Trap	Trap Frequency	Copy to Select All
1	g1	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
2	g2	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
3	g3	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
4	g4	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
5	g5	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
6	g6	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
7	g7	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
8	g8	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
9	g9	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
10	g10	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
11	g11	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
12	g12	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
13	g13	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
14	g14	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
15	g15	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
16	g16	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
17	g17	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
18	g18	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
19	g19	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
20	g20	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
21	g21	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
22	g22	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
23	g23	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
24	g24	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>

Global System LAGs						
Port	Current Port Status	Set Port	Action	Trap	Trap Frequency	Copy to Select All
25	LAG 1	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
26	LAG 2	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
27	LAG 3	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
28	LAG 4	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
29	LAG 5	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
30	LAG 6	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
31	LAG 7	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>
32	LAG 8	Unlocked	Unlocked	Discard	10	<input type="checkbox"/>

### Konfigurieren der Locked Port Security mit CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Konfiguration der Locked Port Security, wie auf der Seite [Port Security](#) angezeigt, zusammen.

Tabelle 7-52. CLI-Befehle zur Port-Sicherheit

CLI-Befehl	Beschreibung
<b>Shutdown</b>	Deaktiviert Schnittstellen.
<b>set interface active</b> { ethernet <i>interface</i>   port-channel <i>port-channel-number</i> }	Reaktiviert eine Schnittstelle, die aus Sicherheitsgründen deaktiviert wurde.
<b>port security</b> [forward   discard   discard-shutdown] [trap <i>seconds</i> ]	Sperrt das Erfassen (Lernen) neuer Adressen an einer Schnittstelle.
<b>show ports security</b> { ethernet <i>interface</i>   port-channel <i>port-channel-number</i> }	Zeigt den Sperrstatus eines Ports an.

Das folgende Beispiel illustriert die CLI-Befehle:

Console # show ports security					
Port	Status	Korrekturmaßnahme	Trap	Frequenz	Zähler
---	-----	-----	-----	-----	-----
-				-	--
g7	Unlocked	Discard	Enable	100	88
g8	Unlocked	Discard, Shutdown	disable		
g3	Unlocked	-	-	-	-

## Konfigurieren von Ports

Die Seite **Ports** enthält Links zu Seiten über Portfunktionalität, darunter erweiterte Funktionen wie Storm-Kontrolle und Port-Spiegelung. Öffnen Sie die Seite **Ports**, indem Sie auf Switch → Ports klicken.

## Definieren von Portparametern

Die Seite **Port Configuration** enthält Felder zur Definition der Portparameter. Öffnen Sie die Seite **Port Configuration**, indem Sie auf Switch → Ports → Portkonfiguration in der Strukturansicht klicken.

Abb. 7-88. Portkonfiguration



**Port** Gibt die Anschlussnummer an, für die Portparameter definiert werden.

**Description** (0-64 Characters) Enthält eine kurze Schnittstellenbeschreibung, z. B. Ethernet.

**Port Type** Gibt den Porttyp an.



**Admin Status** Aktiviert/deaktiviert den über den Port geleiteten Datenverkehr. Der neue Portstatus wird im Feld **Current Port Status** angezeigt.

**Current Port Status** Gibt den Betriebsstatus des Ports an.

**Re-Activate Port** Reaktiviert einen Port, nachdem er über die Sicherheitsoption **Locked Port** deaktiviert wurde.

**Operational Status** Gibt den Betriebsstatus des Ports an. Folgende Feldwerte können ausgewählt werden:

**Suspended** Der Port ist gegenwärtig aktiv und empfängt oder überträgt gegenwärtig keinen Verkehr.

**Active** Der Port ist gegenwärtig aktiv und empfängt und überträgt gegenwärtig Verkehr.

**Disable** Der Port ist gegenwärtig deaktiviert und empfängt oder überträgt gegenwärtig keinen Verkehr.

**Admin Speed** Gibt die konfigurierte Geschwindigkeit an, mit der der Port arbeitet. Der Porttyp bestimmt, welche Geschwindigkeitseinstellungen verfügbar sind. Admin speed kann nur angegeben werden, wenn Auto-Negotiation am konfigurierten Port deaktiviert ist.

**Current Port Speed** Die gegenwärtig konfigurierte Portgeschwindigkeit (bps).

**Admin Duplex** Der Duplexmodus des Ports kann entweder **Full** oder **Half** sein. **Full** zeigt an, dass die Schnittstelle eine Übertragung zwischen dem Gerät und seinem Verbindungspartner in beiden Richtungen gleichzeitig unterstützt. **Half** zeigt an, dass die Schnittstelle eine Übertragung zwischen dem Gerät und dem Client nur in jeweils eine Richtung unterstützt.

**Current Duplex Mode** Die aktuelle Konfiguration des Ports im Duplexmodus.

**Auto Negotiation** Aktiviert Auto-Negotiation für den Port. Auto-Negotiation (Automatische Verbindungsaushandlung) ist ein Protokoll zwischen zwei Verbindungspartnern, die es einem Port ermöglicht, seinem Partner seine Fähigkeiten in Bezug auf Übertragungsrate, Duplexmodus und Datenflusssteuerung bekanntzugeben.

**Current Auto Negotiation** Die gegenwärtige Auto-Verhandlungs-Einstellung.

**Back Pressure** Aktiviert den Backpressure-Modus (Zurückweisung) am Port. Der Backpressure-Modus wird im Halbduplexmodus verwendet, um den Eingang von Meldungen am Port zu verhindern.

**Current Back Pressure** Die aktuelle Backpressure-Einstellung.

**Flow Control** Aktiviert oder deaktiviert Datenflusssteuerung oder aktiviert Auto-Negotiation der Datenflusssteuerung für den Port. Diese wird wirksam, wenn der Port im **Vollduplex**modus arbeitet.

**Current Flow Control** Die gegenwärtige Datenflusssteuerungseinstellung.

**MDI /MDIX** Ermöglicht dem Gerät die Erkennung gekreuzter und nicht gekreuzter Kabel.

Hubs und Schalter sind entgegengesetzt zu Endstationen verkabelt, so dass, wenn ein Hub oder Schalter mit einer Endstation verbunden ist, ein ungekreuztes Ethernetkabel verwendet werden kann und sichergestellt wird, dass die Paare richtig angeschlossen sind. Wenn zwei Hubs/Schalter bzw. zwei Endstationen miteinander verbunden werden, wird mit Hilfe eines gekreuzten Kabels sichergestellt, dass die Paare richtig angeschlossen sind. Folgende Feldwerte können ausgewählt werden:

**Auto** Wird zur automatischen Erkennung des Kabeltyps verwendet.

**MDI (Media Dependent Interface)** Wird für Endstationen verwendet.

**MDIX (Media Dependent Interface with Crossover)** Wird für Hubs und Schalter verwendet.

**Current MDI/MDIX** Gibt die gegenwärtigen MDI/MDIX-Geräteinstellungen an.

**LAG** Gibt an, ob der Port Teil einer LAG ist.

### Definieren von Portparametern

1. Öffnen Sie die Seite [Port Configuration](#).
2. Wählen Sie einen Port im Feld **Port**.
3. Definieren Sie die restlichen Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen) **Verhandlung**.

Die Portparameter werden im Gerät gespeichert.

### Ändern von Portparametern

1. Öffnen Sie die Seite [Port Configuration](#).
2. Wählen Sie einen Port im Feld **Port**.
3. Ändern Sie die restlichen Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Portparameter werden im Gerät gespeichert.

### Anzeigen der Port-Konfigurationstabelle:

1. Öffnen Sie die Seite [Port Configuration](#).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die [Ports Configuration Table](#) wird geöffnet:

Abb. 7-89. Port-Konfigurationstabelle

Port Configuration Table

The screenshot shows a table with columns: Port, Port Type, Port Status, Port Speed, Duplex Mode, Auto Negotiation, Back Pressure, Flow Control, MDI/MDIX, and LAC. The table lists configurations for various ports (e.g., g0/1, g0/24, g1/0) with settings such as 1000 Mbps speed, Full Duplex, and Auto Negotiation enabled.

### Konfigurieren von Ports mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Konfiguration von Ports, wie auf der Seite [Ports Configuration Table](#) angezeigt, zusammen.

Tabelle 7-53. CLI-Befehle zur Portkonfiguration

CLI-Befehl	Beschreibung
<code>interface ethernet interface</code>	Aktiviert den Schnittstellenkonfigurationsmodus, um eine Ethernet-Schnittstelle zu konfigurieren.
<code>description string</code>	Fügt einer Schnittstellenkonfiguration eine Beschreibung hinzu.
<code>shutdown</code>	Deaktiviert Schnittstellen innerhalb des derzeit festgelegten Kontexts.
<code>set interface active {ethernet interface   port-channel port-channel-number}</code>	Reaktiviert eine Schnittstelle, die aus Sicherheitsgründen deaktiviert wurde.
<code>speed bps</code>	Konfiguriert die Geschwindigkeit einer bestimmten Ethernet-Schnittstelle, wenn keine Auto-Negotiation verwendet wird.
<code>autobaud</code>	Stellt die Leitung auf automatische Baudrate-Erkennung ein.
<code>duplex {half   full}</code>	Konfiguriert den Voll-/Halbduplexbetrieb einer bestimmten Ethernet-Schnittstelle, wenn keine Auto-Negotiation verwendet wird.
<code>negotiation</code>	Aktiviert die Auto-Negotiation für Geschwindigkeit und Duplexparameter einer bestimmten Schnittstelle.
<code>back-pressure</code>	Aktiviert Backpressure für eine bestimmte Schnittstelle.
<code>flowcontrol {auto   on   off   rx   tx}</code>	Konfiguriert die Flusskontrolle für eine bestimmte Schnittstelle.
<code>mdix {on   auto}</code>	Aktiviert die automatische Kreuzkabel-Erkennung für eine bestimmte Schnittstelle bzw. einen bestimmten Portkanal.
<code>show interfaces configuration [ethernet interface   port-channel port-channel-number]</code>	Zeigt die Konfiguration aller konfigurierten Schnittstellen an.
<code>show interfaces status [ethernet interface   port-channel port-channel-number]</code>	Zeigt den Status aller konfigurierten Schnittstellen an.
<code>show interfaces description [ethernet interface   port-channel port-channel-number]</code>	Zeigt die Beschreibung aller konfigurierten Schnittstellen an.

Das folgende Beispiel illustriert die CLI-Befehle:

```

Console (config)# interface ethernet g5

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 ethernet g5

```

Port	Typ	Duplex	Speed	Neg	Flow Control	Admin State	Back Pressure	Mdix
----	---	-----	-----	----	-----	-----	-----	----
g5	1G	Full	100	Enabled (Aktiviert)	auf	Up (Eingeschaltet)	aktivieren	Auto
console#								

```

console# show interfaces status ethernet g5

```

Port	Typ	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	Mdix
----	---	-----	-----	----	-----	-----	-----	----
g5	1G	Full	100	Enabled (Aktiviert)	auf	Up (Eingeschaltet)	Disabled (Deaktiviert)	auf

console#								

Console# show interfaces status									
Port	Typ	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	Mdix	Modus
----	----	-----	-----	----	-----	-----	-----	----	----
g1	1G	Full	100	Auto	auf	Up (Eingeschaltet)	aktivieren	auf	
g1	100	Full	100	Aus	Aus	Down (Abgeschaltet)	disable	Aus	
g2	100	Full	1000	Aus	Aus	Up (Eingeschaltet)	disable	auf	
Ch	Typ	Duplex	Speed	Neg	Flow Control	Back Pressure	Link State		
---	----	-----	---	----	-----	-----	-----		
1	1000	Full	1000	Aus	Aus	disable	Up (Eingeschaltet)		

## Definieren von LAG-Parametern

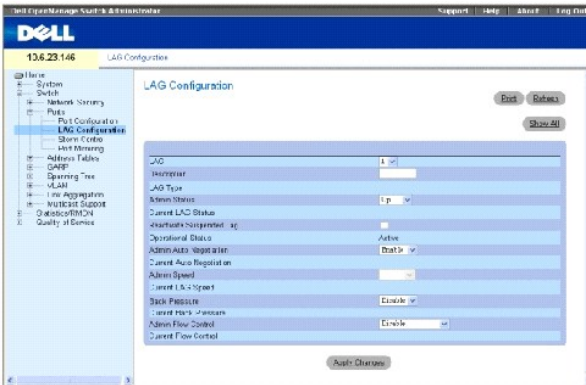
Die Seite [LAG Configuration](#) enthält Felder zur Configuration von Parametern für konfigurierte LAGs. Das System unterstützt bis zu acht Ports pro LAG sowie sechs LAGs pro System.

Weitere Informationen zu Link Aggregated Groups (LAGs) und zur Zuweisung von Ports zu LAGs finden Sie unter [Aggregieren von Ports](#).

Öffnen Sie die Seite [LAG Configuration](#), indem Sie auf Switch→ Ports→ LAG Configuration in der Strukturansicht klicken.

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

Abb. 7-90. LAG-Konfiguration



**LAG** Gibt die LAG-Nummer an.

**Description** (0-64 Characters) Zeigt eine benutzerdefinierte Beschreibung der konfigurierten LAG an.

**LAG Type** Gibt die Porttypen an, die in der LAG enthalten sind.

**Admin Status** Aktiviert/deaktiviert den über die ausgewählte LAG geleiteten Datenverkehr.

**Current LAG Status** Gibt den LAG-Status an.

**Re-Activate Suspended LAG** Reaktiviert eine ausgesetzte LAG.

**Operational Status** Gibt den Betriebsstatus der LAG an.

**Admin Auto Negotiation** Aktiviert/deaktiviert die Auto-Negotiation für die LAG. Auto-Negotiation bezeichnet ein Protokoll zwischen zwei Verbindungspartnern, mit dessen Hilfe der jeweils anderen LAG Übertragungsrate, Duplexmodus und Flusskontrollverhalten (standardmäßig deaktiviert) mitgeteilt werden.

**Current Auto Negotiation** Die gegenwärtige Auto-Negotiation-Einstellung.

**Admin Speed** Gibt die Betriebsgeschwindigkeit der LAG an.

**Current LAG Speed** Gibt die gegenwärtig konfigurierte Betriebsgeschwindigkeit der LAG an.

**Admin Back Pressure** Aktiviert/deaktiviert den Backpressure-Modus in der LAG. Der Backpressure-Modus ist wirksam an den Ports, die innerhalb der LAG im Halbduplex arbeiten.

**Current Back Pressure** Die aktuelle Backpressure-Einstellung.

**Admin Flow Control** Aktiviert/deaktiviert Datenflusssteuerung oder aktiviert Auto-Negotiation der Datenflusssteuerung in der LAG. Der Flusskontrollmodus ist wirksam an den Ports, die innerhalb der LAG im Vollduplex arbeiten.

**Current Flow Control** Die benutzerdefinierte Datenflusssteuerungseinstellung.

## Definieren von LAG-Parametern

1. Öffnen Sie die Seite [LAG Configuration](#).
2. Wählen Sie eine LAG im Feld **LAG**.
3. Definieren Sie die Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

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

Die LAG-Parameter werden im Gerät gespeichert.

## Anzeigen der LAG-Konfigurationstabelle:

1. Öffnen Sie die Seite [LAG Configuration](#).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die Seite [LAG Configuration Table](#) wird geöffnet:

Abb. 7-91. LAG-Konfigurationstabelle

LAG Configuration Table

Refresh

LAG	Description	LAG Type	LAG Status	LAG Speed	Auto Negotiation	Eth Port	Flow Control
1	1	Up			Enable	Disable	Disable
2	2	Up			Enable	Disable	Disable
3	3	Up			Enable	Disable	Disable
4	4	Up			Enable	Disable	Disable
5	5	Up			Enable	Disable	Disable
6	6	Up			Enable	Disable	Disable
7	7	Up			Enable	Disable	Disable
8	8	Up			Enable	Disable	Disable

Apply Changes

## Konfigurieren von LAGs mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Konfiguration von LAGs, wie auf der Seite [LAG Configuration](#) angezeigt, zusammen.

Tabelle 7-54. CLI-Befehle zur LAG-Konfiguration

CLI-Befehl	Beschreibung
<code>interface port-channel port-channel-number</code>	Aktiviert den Schnittstellenkonfigurationsmodus eines spezifischen Portkanals.
<code>description string</code>	Fügt einer Schnittstellenkonfiguration eine Beschreibung hinzu.
<code>shutdown</code>	Deaktiviert Schnittstellen innerhalb des derzeit festgelegten Kontexts.
<code>speed bps</code>	Konfiguriert die Geschwindigkeit einer bestimmten Ethernet-Schnittstelle, wenn keine Auto-

	Verhandlung verwendet wird.
<b>autobaud</b>	Stellt die Leitung auf automatische Baudrate-Erkennung ein.
<b>negotiation</b>	Aktiviert die Auto-Negotiation für Geschwindigkeit und Duplexparameter einer bestimmten Schnittstelle.
<b>back-pressure</b>	Aktiviert Backpressure für eine bestimmte Schnittstelle.
<b>flowcontrol {auto   on   off   rx   tx}</b>	Konfiguriert die Datenflusssteuerung für eine bestimmte Schnittstelle.
<b>show interfaces configuration</b> [ethernet <i>interface</i>   <b>port-channel</b> <i>port-channel-number</i> ]	Zeigt die Konfiguration aller konfigurierten Schnittstellen an.
<b>show interfaces status</b> [ethernet <i>interface</i>   <b>port-channel</b> <i>port-channel-number</i> ]	Zeigt den Status aller konfigurierten Schnittstellen an.
<b>show interfaces description</b> [ethernet <i>interface</i>   <b>port-channel</b> <i>port-channel-number</i> ]	Zeigt die Beschreibung aller konfigurierten Schnittstellen an.
<b>show interfaces port-channel</b> [ <i>port-channel-number</i> ]	Zeigt Portkanalinformationen an (welche Ports einem Portkanal angehören und ob sie derzeit aktiv sind oder nicht).

Das folgende Beispiel illustriert die CLI-Befehle:

<pre> console(config-if)# channel-group 1 mode on  Console(config-if)# exit  console(config)# interface range e g21-24  console(config-if)# channel-group 1 mode on  console(config-if)# ex  console(config)# interface ethernet g5  console(config-if)# channel-group 2 mode on  Console(config-if)# exit  Console(config)# exit </pre>	
<pre> console# show interfaces port-channel </pre>	
Channel-	Ports
-----	-----
ch1	Inactive: g(21-24)
ch2	Active: g5
ch3	



ch4	
ch5	
ch6	
ch7	
ch8	
console#	

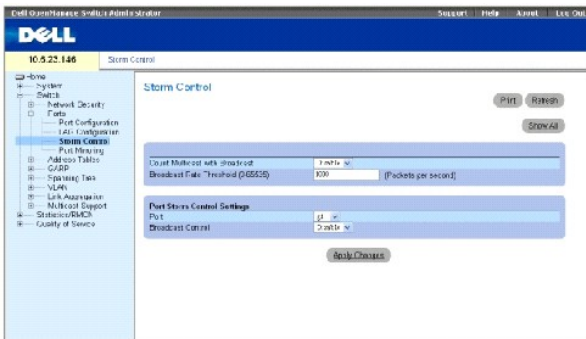
## Aktivieren der Storm-Kontrolle

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

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

Die Seite [Storm Control](#) enthält Felder zur Aktivierung und Konfiguration der Sturmkontrolle. Öffnen Sie die Seite [Storm Control](#), indem Sie auf Switch→ Ports→ Storm Control in der Strukturansicht klicken.

Abb. 7-92. Sturmkontrolle



**Count Multicast with Broadcast** Zählt Broadcast- und Multicast-Verkehr. Folgende Feldwerte können ausgewählt werden:

- o **Enable** Zählt Broadcast- und Multicast-Verkehr.
- o **Disable** Zählt nur Broadcast-Verkehr.

**Broadcast Rate Threshold (1-1000000)** Legt die max. Rate (Pakete pro Sekunde) für die Weiterleitung unbekannter Pakete fest. Der Wertebereich ist 0-1000000. Der Standardwert ist Null. Alle Werte werden auf die nächsten 64Kbps gerundet. Ein Feldwert unter 64 Kbps wird auf 64 Kbps aufgerundet; eine Ausnahme bildet der Wert Null.

**Port** Der Port, von welchem die Sturmkontrolle aktiviert wird.

**Broadcast Control** Aktiviert/deaktiviert die Weiterleitung von Broadcast-Paketen für das Gerät.

## Aktivieren der Sturmkontrolle für das Gerät

1. Öffnen Sie die Seite [Storm Control](#).
2. Wählen Sie eine Schnittstelle, für die die Sturmkontrolle aktiviert wird.
3. Definieren Sie die Felder.
4. Klicken Sie auf **Show All** (Alle anzeigen).

Die Sturmkontrolle wird für das Gerät aktiviert.

## Ändern der Portparameter für die Sturmkontrolle

1. Öffnen Sie die Seite [Storm Control](#).
2. Ändern Sie die entsprechenden Felder.
3. Klicken Sie auf **Show All** (Alle anzeigen).

Die Portparameter für die Sturmkontrolle werden im Gerät gespeichert.

## Anzeigen der Portparameter-Tabelle

1. Öffnen Sie die Seite [Storm Control](#).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die [Storm Control Settings Table](#) wird geöffnet:

Abb. 7-93. Tabelle der Sturm-Kontrolleinstellungen

Port	Storm Control
g1	Disable ▾
g2	Disable ▾
g3	Disable ▾
g4	Disable ▾
g5	Disable ▾
g6	Disable ▾
g7	Disable ▾
g8	Disable ▾
g9	Disable ▾
g10	Disable ▾
g11	Disable ▾
g12	Disable ▾
g13	Disable ▾
g14	Disable ▾
g15	Disable ▾
g16	Disable ▾
g17	Disable ▾
g18	Disable ▾
g19	Disable ▾
g20	Disable ▾
g21	Disable ▾
g22	Disable ▾
g23	Disable ▾
g24	Disable ▾

## Konfigurieren der Sturmkontrolle mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Konfiguration der Sturmkontrolle, wie auf der Seite [Storm Control](#) angezeigt, zusammen.

Tabelle 7-55. CLI - Befehle für Sturmkontrolle

CLI - Befehl	Beschreibung
--------------	--------------

<code>port storm-control include-multicast</code>	Aktiviert die Zählung von Multicast- und Broadcast-Paketen im Gerät.
<code>port storm-control broadcast enable</code>	Aktiviert die Broadcast Sturmkontrolle.
<code>port storm-control broadcast rate rate</code>	Konfiguriert die maximale Broadcast-Rate.
<code>show ports storm-control [ethernet interface]</code>	Zeigt die Konfiguration der Sturmkontrolle an.

Das folgende Beispiel illustriert die CLI-Befehle:

```

console> enable

Console# configure

Console(config)# port
storm-control include-
multicast

Console(config)# port
storm-control broadcast
rate 8000

console(config)# interface
ethernet g1

Console(config-if)# port
storm-control broadcast
enable

Console(config-if)# end

Console# show ports storm-
control

```

Port	Broadcast Storm control [Packets/sec]
----	-----
-	-----
g1	8000
g2	Disabled (Deaktiviert)
g4	Disabled (Deaktiviert)

## Definieren von Port-Spiegelsitzungen

Port-Spiegelung (Port-Mirroring) überwacht und spiegelt Netzwerk-Datenverkehr durch Weiterleitung von Kopien der eingehenden und ausgehenden Pakete von einem überwachten Port zu einem Überwachungsport.

Die Portspiegelung wird konfiguriert, indem ein bestimmter Port zum Kopieren aller Pakete und andere Ports ausgewählt werden, von denen die Pakete kopiert werden. Vor dem Konfigurieren der Portspiegelung sollten Sie Folgendes beachten:

- 1 Überwachte Ports können nicht schneller betrieben werden als die Überwachungsports.
- 1 Alle RX/TX-Pakete sollten auf demselben Port überwacht werden.


Die folgenden Beschränkungen gelten für Ports, die als Zielports konfiguriert sind:

- 1 Ports dürfen nicht als Quellport konfiguriert werden.
- 1 Ports dürfen keine LAG-Komponente sein.
- 1 IP-Schnittstellen dürfen nicht auf dem Port konfiguriert werden.
- 1 GVRP darf nicht für den Port aktiviert werden.
- 1 Der Port darf keine VLAN-Komponente sein.
- 1 Es darf nur ein Zielport definiert sein.

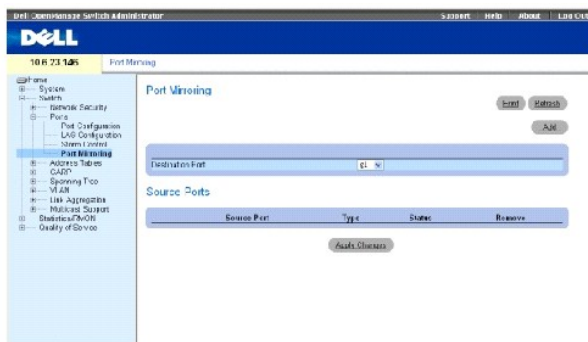
Die folgenden Beschränkungen gelten für Ports, die als Quellports konfiguriert sind:

- 1 Quellports dürfen keine LAG-Komponente sein.
- 1 Ports dürfen nicht als Zielport konfiguriert werden.
- 1 Alle Pakete werden mit Kennung (Tagging) vom Zielport aus übertragen.
- 1 Alle RX/TX-Pakete sollten auf demselben Port überwacht werden.

Öffnen Sie die Seite [Port Mirroring](#), indem Sie auf **Switch**→ **Ports**→ **Port Mirroring** in der Strukturansicht klicken.

 **ANMERKUNG:** Wenn ein Port als Zielport für eine Spiegelsitzung festgelegt wird, werden alle normalen Operationen auf diesem Port ausgesetzt. Diese Operationen umfassen Spanning Tree und LACP.

**Abb. 7-94. Portspiegelung**



**Destination Port** Definiert die Nummer des Ports, auf den der Datenverkehr kopiert wird.

**Source Port** Definiert die Nummer des Ports, von dem der Datenverkehr gespiegelt wird.

**Type** Zeigt an, ob der Quellport RX, TX oder beides ist.

**Status** Gibt an, ob der Port gegenwärtig überwacht (**Active**) oder nicht überwacht (**Ready**) wird.

**Remove** Entfernt, wenn ausgewählt, die Portspiegelsitzung.

### Hinzufügen einer Port-Spiegelsitzung

- 1. Öffnen Sie die Seite [Port Mirroring](#).

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

Die Seite **Add Source Port** (Quellport hinzufügen) wird geöffnet.

3. Wählen Sie den Zielport aus dem Drop-Down-Menü **Destination Port**.
4. Wählen Sie den Quellport aus dem Drop-Down-Menü **Source Port**.
5. Definieren Sie das Feld **Type**.
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der neue Quellport wird definiert und das Gerät wird aktualisiert.

### Löschen eines Zielports aus einer Port-Spiegelsitzung

1. Öffnen Sie die Seite [Port Mirroring](#).
2. Wählen Sie das Kontrollkästchen **Remove** (Entfernen).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die ausgewählte Port-Spiegelsitzung wird gelöscht und das Gerät aktualisiert.

### Konfigurieren einer Port-Spiegelsitzung mit den CLI -Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Konfiguration einer Port-Spiegelsitzung, wie auf der Seite [Port Mirroring](#) angezeigt, zusammen.

**Tabelle 7-56. CLI -Befehle zur Port-Spiegelung**

CLI -Befehl	Beschreibung
<code>port monitor src-interface [rx   tx]</code>	Startet eine Port-Spiegelsitzung.

Das folgende Beispiel illustriert die CLI-Befehle:

```

Console(config)# interface ethernet g1

Console(config-if)# port monitor g8

Console# show ports monitor

```

Source Port	Destination Port	Type	Status	VLAN Tagging
-----	-----	---	-----	-----
g8	g1	RX, TX	Active (Aktiv)	Nein
g2	g8	RX, TX	Active (Aktiv)	Nein

g18	g8	Rx	Active (Aktiv)	Nein
-----	----	----	-------------------	------

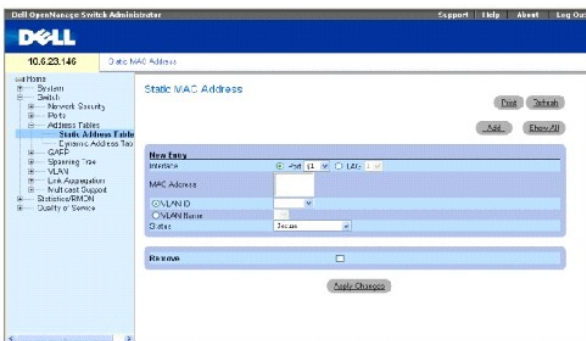
## Konfigurieren von Adresstabellen

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 Port weitergeleitet. Die Tabellen mit statischen und dynamischen Adressen können nach Schnittstelle, VLAN und Schnittstellentyp sortiert werden. MAC-Adressen werden dynamisch erfasst („gelernt“), sobald Pakete aus einer Quelle auf dem Gerät eingeht. Adressen werden mit Ports verknüpft, indem die Ports aus der Quelladresse des Frames ausgelesen werden. Frames, die an eine MAC-Zieladresse adressiert sind, die mit keinem Port verknüpft ist, werden an alle Ports 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. Öffnen Sie die Seite **Address Tables**, indem Sie auf **Switch** → **Address Table** in der Strukturansicht klicken.

## 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 Port definiert werden. Öffnen Sie die Seite [Static MAC Address](#), indem Sie auf **Switch** → **Address Table** → **Static Address** in der Strukturansicht klicken.

Abb. 7-95. Statische MAC-Adressen



**Interface** Gibt den spezifischen Port bzw. LAG an, für die eine statische MAC-Adresse hinzugefügt wird.

**MAC Address** Die MAC-Adresse, die in der aktuellen Liste statischer Adressen aufgeführt ist.

**VLAN ID** Gibt den Wert der mit der MAC-Adresse verknüpften VLAN-ID an.

**VLAN Name** Gibt den benutzerdefinierten VLAN-Namen an.

**Status** Status der MAC-Adresse. Mögliche Werte sind:

**Secure** Stellt sicher, dass eine mit der Locked-Port-Sicherheitsoption konfigurierte MAC-Adresse nicht gelöscht wird.

**Permanent** Gibt an, dass es sich um eine dauerhafte MAC-Adresse handelt.

**Delete on Reset** Gibt an, dass die MAC-Adresse beim Zurücksetzen des Gerätes gelöscht wird.

**Delete on Timeout** Gibt an, dass die MAC-Adresse gelöscht wird, nachdem das Zeitlimit des Gerätes erreicht wurde.

**Remove** Entfernt, wenn ausgewählt, die MAC-Adresse aus der MAC-Adresstabelle.

### Hinzufügen einer statischen MAC-Adresse

1. Öffnen Sie die Seite [Static MAC Address](#).
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite **Add Static MAC Address** wird geöffnet.

3. Geben Sie die Informationen in den Feldern ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die neue statische Adresse wird der **Static MAC Address Table** hinzugefügt und das Gerät aktualisiert.

### Ändern einer statischen Adresse in der Static MAC Address Table

1. Öffnen Sie die Seite [Static MAC Address](#).
2. Ändern Sie die entsprechenden Felder.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die statische MAC-Adresse wird geändert und das Gerät aktualisiert.

### Entfernen einer statischen Adresse aus der Static Address Table

1. Öffnen Sie die Seite [Static MAC Address](#).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die **Static MAC Address Table** wird geöffnet.

3. Wählen Sie einen Tabelleneintrag.
4. Wählen Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die ausgewählte statische Adresse wird gelöscht und das Gerät aktualisiert.

### Konfigurieren der Parameter statischer Adressen mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Konfiguration der Parameter statischer Adressen, wie auf der Seite [Static MAC Address](#) angezeigt, zusammen.

Tabelle 7-57. CLI-Befehle für statische Adressen

CLI-Befehl	Beschreibung
<code>bridge address mac-address {ethernet interface   port-channel port-channel-number} [permanent   delete-on-reset   delete-on-timeout   secure]</code>	Fügt der Bridge-Tabelle die statische Quelladresse einer Station auf MAC-Schicht hinzu.
<code>show bridge address-table [vlan vlan] [ethernet interface   port-channel port-channel-number]</code>	Zeigt Einträge in der Datenbank für die Bridge-Weiterleitung an.

Das folgende Beispiel illustriert die CLI-Befehle:

```
Console# show bridge address-table
```

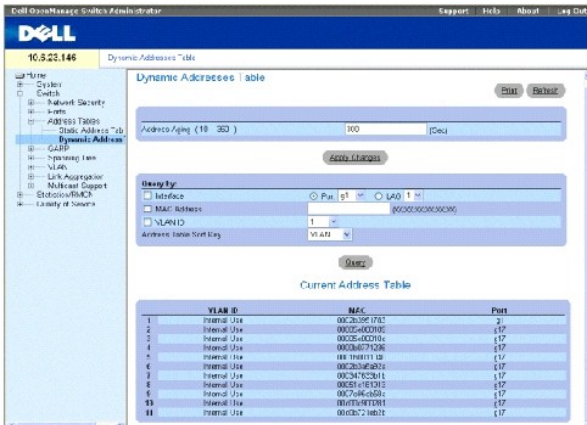
Aging time is 300 sec			
vlan	mac address	port	type
----	-----	----	-----
1	00:60:70:4C:73:FF	g8	dynamic
1	00:60:70:8C:73:FF	g8	dynamic
200	00:10:0D:48:37:FF	g9	static
g8	00:10:0D:98:37:88	g8	dynamic

## Anzeigen dynamischer Adressen

Die Seite [Dynamic Address Table](#) enthält Felder für die Abfrage von Informationen in der Dynamic Address-Tabelle, 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 Ports weitergeleitet. Die [Dynamic Address Table](#) enthält auch Informationen zur Speicherdauer (Aging Time), bevor dynamische MAC-Adressen gelöscht werden, einschließlich Parameter zur Abfrage und Anzeige der Liste dynamischer Adressen. Die Current Address Table enthält dynamische Adressparameter, gemäß denen Pakete direkt an die Ports weitergeleitet werden.

Öffnen Sie die Seite [Dynamic Address Table](#), indem Sie auf **Switch**→ **Address Table**→ **Dynamic Addresses Table** in der Strukturansicht klicken.

Abb. 7-96. Tabelle dynamischer Adressen



**Address Aging (10-360)** 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.

**Interface** Gibt die Schnittstelle an, für die die Tabelle abgefragt wird. Zwei Schnittstellentypen stehen zur Auswahl.

**Port** Gibt die Nummern der Ports an, für welche die Tabelle abgefragt wird.

**LAG** Gibt die LAG an, für die die Tabelle abgefragt wird.

**MAC Address** Gibt die MAC-Adresse an, 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-Tabelle sortiert wird.

### Neudefinieren der Speicherdauer:

1. Öffnen Sie die Seite [Dynamic Address Table](#).
2. Definieren Sie das Feld **Aging Time**.
3. Klicken Sie auf Apply Changes (Änderungen übernehmen).

Die Speicherdauer wird geändert und das Gerät aktualisiert.

### Abfragen der Dynamic Address-Tabelle

1. Öffnen Sie die Seite [Dynamic Address Table](#).
2. Definieren Sie die Parameter, nach denen die **Dynamic Address Table** abgefragt wird.

Die Einträge können nach **Port**, **MAC Address** oder **VLAN ID** abgefragt werden.

3. Klicken Sie auf **Query** (Abfragen).

Die [Dynamic Address Table](#) wird abgefragt.

### Sortieren der Dynamic Address-Tabelle

1. Öffnen Sie die Seite [Dynamic Address Table](#).
2. Wählen Sie im Drop-Down-Menü **Address Table Sort Key** aus, ob die Adressen nach Adresse, VLAN ID oder Schnittstelle geordnet werden sollen.
3. Klicken Sie auf **Query** (Abfragen).

Die [Dynamic Address Table](#) wird sortiert.

### Abfragen und Sortieren von dynamischen Adressen mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zum Abfragen und Sortieren dynamischer Adressen, wie auf der Seite [Dynamic Address Table](#) gezeigt, zusammen.

Tabelle 7-58. CLI-Befehle für Abfragen und Sortieren

CLI-Befehl	Beschreibung
<code>bridge aging-time seconds</code>	Stellt die Speicherdauer der Adresstabelle ein.
<code>show bridge address-table [vlan vlan] [ethernet interface   port-channel port-channel-number]</code>	Zeigt Klassen dynamisch erstellter Einträge in der Datenbank für die Bridge-Weiterleitung an.

Das folgende Beispiel illustriert die CLI-Befehle:

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

Console(config)# exit

Console# show bridge address-table
```

Aging time is 250 sec			
VLAN	MAC-Adresse	Port	Typ
----	-----	----	----
1	00:60:70:4C:73:FF	g8	dynamic
1	00:60:70:8C:73:FF	g8	dynamic
200	00:10:0D:48:37:FF	g8	static

## Konfigurieren von GARP

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

Bei der GARP-Konfiguration müssen Sie Folgendes sicherstellen:

- 1 Die Leave-Zeit muss größer oder gleich der dreifachen Join-Zeit sein.
- 1 Die Leave-all-Zeit muss größer als die Leave-Zeit sein.

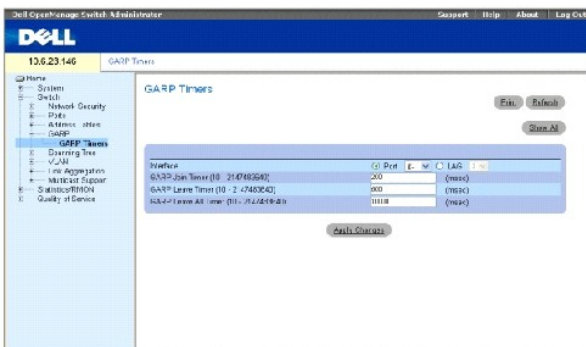
Stellen Sie die gleichen GARP-Timer-Werte für alle auf Layer 2 verbundenen Geräte ein. Wenn für die auf Layer 2 verbundenen Geräte die GARP-Timer verschieden eingestellt werden, funktioniert die GARP-Anwendung nicht ordnungsgemäß.

Öffnen Sie die Seite **GARP**, indem Sie auf **Switch** → **GARP** in der Strukturansicht klicken.

## Definieren von GARP-Timern

Die Seite [GARP Timers](#) enthält Felder zur Aktivierung von GARP für das Gerät. Öffnen Sie die Seite [GARP Timers](#), indem Sie auf **Switch** → **GARP** → **GARP Timers** in der Strukturansicht klicken.

Abb. 7-97. GARP-Timer



**Interface** Legt fest, ob die Aktivierung für einen Port oder eine LAG gilt.

**GARP Join Timer (10 - 2147483640)** Gibt die Zeit für die Übertragung von PDUs in Millisekunden an. Der Wertebereich ist 10-2147483640. Der Standardwert ist 200 Millisekunden.

**GARP Leave Timer (10 - 2147483640)** Gibt die Zeit in Millisekunden an, die ein Gerät vor Beenden seines GARP-Status wartet. Die Leave-Time wird durch eine gesendete/empfangene Leave All Time-Nachricht aktiviert und durch die empfangene Join-Nachricht beendet. Die Leave-Zeit muss größer oder gleich der dreifachen Join-Zeit sein. Der Wertebereich ist 0-2147483640. Der Standardwert ist 600 Millisekunden.

**GARP Leave All Timer (10 - 2147483640)** Gibt die Zeit in Millisekunden an, die ein Gerät vor Beenden seines GARP-Status wartet. Die Leave-all-Zeit muss größer als die Leave-Zeit sein. Der Wertebereich ist 0-2147483640. Der Standardwert ist 10000 Millisekunden.

## Definieren von GARP-Timern

1. Öffnen Sie die Seite [GARP Timers](#).
2. Geben Sie die Informationen in den Feldern ein.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die GARP-Parameter werden im Gerät gespeichert.

## Kopieren von Parametern in die GARP Timers-Tabelle

1. Öffnen Sie die Seite [GARP Timers](#).
2. Klicken Sie auf **Show All** (Alle anzeigen).

The **GARP Timers Table** wird geöffnet.

3. Wählen Sie den Schnittstellentyp im Feld **Copy Parameters from** (Kopieren der Parameter von).
4. Wählen Sie eine Schnittstelle im Drop-Down-Menü **Port** oder **LAG**.
5. Die Definitionen dieser Schnittstelle werden auf die ausgewählten Schnittstellen kopiert. Siehe Schnitt 6.
6. Wählen Sie das Kontrollkästchen **Copy to**, um die Schnittstellen zu definieren, auf die die GARP-Timer-Definitionen kopiert werden, oder klicken Sie auf **Select All** (Alle auswählen), um die Definitionen auf alle Ports oder LAGs zu kopieren.
7. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Parameter werden auf die ausgewählten Ports oder LAGs in der **GARP Timers Table** kopiert und das Gerät wird aktualisiert.

## Definieren von GARP-Timern mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Definition der GARP-Timer, wie auf der Seite [GARP Timers](#) angezeigt, zusammen.

Tabelle 7-59. CLI - Befehle für GARP-Timer

CLI-Befehl	Beschreibung
<code>garp timer {join   leave   leaveall} timer_value</code>	Legt die Join-, Leave- und Leaveall-GARP-Timer-Werte der GARP-Anwendung fest.

Das folgende Beispiel illustriert die CLI-Befehle:

```
Console(config)# interface ethernet g1

console(config-if)# garp timer leave 900

console(config-if)# end
```

```

console# show gvrp configuration ethernet g1

GVRP Feature is currently Disabled on the device.

Maximum VLANs: 223

```

Port (s)	GVRP-	Registration	Dynamic VLAN	Timers (milliseconds)		
	Status		Creation	Join	Leave	Leave All
---	-----	-----	-----	-----	-----	-----
---	-----	-----	-----	-----	-----	-----
g1	Disabled (Deaktiviert)	Normal	Enabled (Aktiviert)	200	900	10000
console#						

## Konfigurieren des Spanning Tree-Protokolls

Das Spanning Tree-Protokoll (STP) stellt eine Baumstruktur-Topografie für jede Brückenordnung bereit. STP stellt auch einen einzelnen Pfad zwischen Endstationen in einem Netzwerk bereit und vermeidet so Netzwerkschleifen.

Schleifen treten auf, wenn zwischen Hosts alternative Leitwege existieren. Schleifen in einem erweiterten Netzwerk können dazu führen, dass Datenverkehr über Brücken auf unbegrenzte Zeit weitergeleitet wird, was zu erhöhtem Datenaufkommen und einer Minderung der Netzwerkleistung führt.

Die Geräte unterstützen die folgenden Spanning Tree-Protokolle:

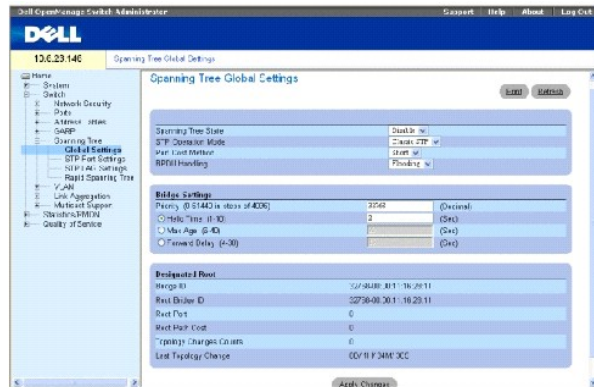
- 1 Classic STP Bietet einen einzelnen Leitweg zwischen Endstationen und vermeidet so Netzwerkschleifen. Weitere Informationen zur Konfiguration von Classic STP finden Sie unter [„Definieren globaler STP-Einstellungen“](#).
- 1 Rapid STP Erfasst und verwendet Netzwerktopologien, die eine schnellere Konvergenz des Spanning-Tree ermöglichen, ohne dass Weiterleitungsschleifen geschaffen werden. Weitere Informationen zur Konfiguration von Rapid STP finden Sie unter [„Konfigurieren von Rapid Spanning Tree“](#).

Öffnen Sie die Seite **Spanning Tree**, indem Sie auf **Switch**→ **Spanning Tree** in der Strukturansicht klicken.

## Definieren globaler STP-Einstellungen

Die Seite [STP Global Settings](#) enthält Parameter zur Aktivierung und Konfiguration von STP-Betrieb auf dem Gerät. Öffnen Sie die Seite [STP Global Settings](#), indem Sie auf **Switch**→ **Spanning Tree**→ **Global Settings** in der Strukturansicht klicken.

Abb. 7-98. Globale STP-Einstellungen



**Spanning Tree State** Aktiviert/deaktiviert STP für das Gerät. Folgende Feldwerte können ausgewählt werden:

- Enable** Aktiviert STP.
- Disable** Deaktiviert STP.

**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. Dies ist die Standardeinstellung.

**Rapid STP** Aktiviert Rapid STP für das Gerät.

**Port Cost Method** Legt die Kostenmethode für den Spanning Tree-Standardpfad fest. Folgende Feldwerte können ausgewählt werden:

**Short** Gibt den Bereich 1 bis 65535 für die Kosten des Portpfades an. Dies ist der Standardwert.

**Long** Gibt den Bereich 1 bis 200000000 für die Kosten des Portpfades an.

**BPDUs Handling** Legt die Verwaltung von BPDUs bei Deaktivierung von STP an dem Port/Gerät fest. BPDUs werden zur Übertragung von Spanning Tree-Informationen verwendet. Folgende Feldwerte können ausgewählt werden:

**Filtering** Filtert BPDUs-Pakete, wenn Spanning Tree an einer Schnittstelle deaktiviert ist.

**Flooding** Leitet BPDUs-Pakete weiter, wenn Spanning Tree an einer Schnittstelle deaktiviert ist. Dies ist die Standardeinstellung.

**Priority (0-61440, in steps of 4096)** Gibt den Wert der Bridge-Priorität an. Wenn auf Schaltern oder Brücken STP ausgeführt wird, wird jedem Element eine Priorität zugewiesen. Nach dem Auswechseln der BPDUs wird der Schalter mit der niedrigsten Priorität zur Root-Bridge. Der Standardwert lautet 32768. Die Wert der Bridge-Priorität wird in Inkrementen von 4096 (4K-Inkremente) angegeben. Beispiel: 0, 4096, 8192 etc.

**Hello Time (1-10)** Legt die Hello Time für das Gerät 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 das Gerät fest. Die maximale Speicherdauer entspricht der Zeit in Sekunden, die eine Bridge vor dem Senden von Konfigurationsnachrichten abwartet. Der Standardwert für die maximale Speicherdauer beträgt 20 Sekunden.

**Forward Delay (4-30)** Legt die Weiterleitungsverzögerung für das Gerät 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 Ports 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 seit dem letzten Neustart aufgetretenen STP-Statusänderungen an.

**Last Topology Change** Gibt die Zeit an, die seit der letzten topographischen Änderung und 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 der globalen STP-Parameter

1. Öffnen Sie die Seite [STP Global Settings](#).
2. Wählen Sie den zu aktivierenden Port im Drop-Down-Menü **Select a Port** aus.
3. Wählen Sie **Enable** im Feld **Spanning Tree State** aus.
4. Wählen Sie den Modus **STP** im Feld **STP Operation Mode** aus und definieren Sie die Bridge-Einstellungen.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

STP wird für das Gerät aktiviert.

## Ändern globaler STP-Parameter

1. Öffnen Sie die Seite [STP Global Settings](#).
2. Definieren Sie die Felder im Dialogfeld.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die STP-Parameter werden geändert und das Gerät aktualisiert.

## Definieren globaler STP-Parameter mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Definition globaler STP-Parameter, wie auf der Seite [STP Global Settings](#) angezeigt, zusammen.

Tabelle 7-60. CLI-Befehle für globale STP-Parameter

CLI-Befehl	Beschreibung
<code>spanning-tree</code>	Aktiviert die Spanning Tree-Funktion.
<code>spanning-tree mode {stp   rstp}</code>	Konfiguriert das Spanning Tree-Protokoll.
<code>spanning-tree priority <i>priority</i></code>	Konfiguriert die Spanning Tree-Priorität.
<code>spanning-tree hello-time <i>seconds</i></code>	Konfiguriert die Hello Time der Spanning Tree-Bridge, die angibt, wie häufig das Gerät Hello-Nachrichten an andere Schalter sendet.
<code>spanning-tree max-age <i>seconds</i></code>	Konfiguriert die maximale Speicherdauer für die Spanning Tree-Bridge.
<code>spanning-tree forward-time <i>seconds</i></code>	Konfiguriert die Weiterleitungszeit für die Spanning Tree-Bridge. Diese entspricht der Dauer, die ein Port vor Aktivierung des Weiterleitungsstatus im Überwachungs- und Erfassungsstatus verbleibt.
<code>show spanning-tree [ethernet <i>interface</i>  </code>	Zeigt den Identifier der Spanning Tree-Konfiguration an.

<code>port-channel</code> <i>port-channel-number</i>	
<code>show spanning-tree</code> [ <i>detail</i> ] [ <i>active</i>   <i>blockedports</i> ]	Zeigt die Spanning Tree-Konfiguration an - detaillierte Informationen zu aktiven oder gesperrten Ports.

Das folgende Beispiel illustriert die CLI-Befehle:

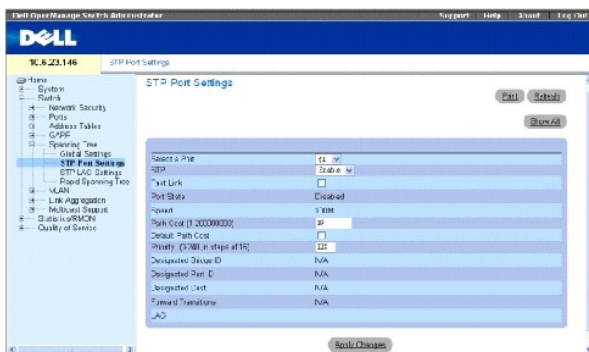
<pre> console(config)# spanning-tree  console(config)# spanning-tree mode rstp  console(config)# spanning-tree priority 12288  console(config)# spanning-tree hello-time 5  console(config)# spanning-tree max-age 15  console(config)# spanning-tree forward-time 25  Console(config)# exit  console# show spanning-tree  Spanning tree enabled mode RSTP  Default port cost method: short </pre>							
Root ID		Priority		12288			
		Adresse		00:e8:00:b4:c0:00			
		This switch is the root					
		Hello Time 5 sec Max Age 15 sec Forward Delay 25 sec					
<pre> Number of topology changes 5 last change occurred 00:05:28 ago  Times: hold 1, topology change 40, notification 5  hello 5, max age 15, forward delay 25 </pre>							

Interfaces							
Name	Status	Prio. Nbr	Cost	Sts	Role	PortFast	Typ
-----	-----	-----	-----	-----	-----	-----	-----
g1	Enabled (Aktiviert)	128.1	100	DSBL	DSBL	Nein	P2p (STP)
g2	Enabled (Aktiviert)	128.2	100	DSBL	DSBL	Nein	P2p (STP)
g3	Enabled (Aktiviert)	128.3	100	DSBL	DSBL	Nein	P2p (STP)

## Definieren von STP-Einstellungen für Ports

Die Seite [STP Port Settings](#) enthält Felder zur Zuweisung von STP-Eigenschaften zu einzelnen Ports. Öffnen Sie die Seite [STP Port Settings](#), indem Sie auf **Switch** → **Spanning Tree** → **Port Settings** in der Strukturansicht klicken.

Abb. 7-99. STP-Porteinstellungen



**Select a Port** Der Port, für den STP aktiviert wird.

**STP** Aktiviert/deaktiviert STP für den Port.

**Fast Link** Aktiviert, wenn ausgewählt, den Fast Link-Modus für den Port. Falls der Fast Link-Modus für einen Port aktiviert ist, wird der **Port** automatisch in den **Weiterleitungsstatus** versetzt, sobald die Portverbindung aktiv ist. Der Fast Link-Modus optimiert die Zeit, die zur Konvergenz des STP-Protokolls erforderlich ist. Die STP-Konvergenz kann in großen Netzwerken 30 bis 60 Sekunden dauern.

**Port State** Gibt den aktuellen STP-Status eines Ports an. Falls aktiviert, wird durch den Portstatus die Weiterleitungsaktion für den Datenverkehr bestimmt. Folgende Portzustände sind möglich:

**Disabled** Zeigt an, dass die Portverbindung derzeit inaktiv ist.

**Blocking** Der Port ist derzeit blockiert und kann nicht für die Weiterleitung von Datenverkehr oder die Erfassung von MAC-Adressen verwendet werden. Blocking wird angezeigt, wenn Classic STP aktiviert ist.

**Listening** Der Port befindet sich derzeit im Überwachungsmodus. Der Port kann weder Datenverkehr weiterleiten noch MAC-Adressen erfassen.



**Learning** Der Port befindet sich derzeit im Erfassungsmodus. Der Port kann zwar keinen Datenverkehr weiterleiten, jedoch neue MAC-Adressen erfassen.

**Forwarding** Der Port befindet sich derzeit im Weiterleitungsmodus. Der Port kann Datenverkehr weiterleiten und neue MAC-Adressen erfassen.

**Speed** Gibt die Portgeschwindigkeit an.

**Path Cost (1-200000000)** Gibt an, welchen Anteil dieser Port an den Root-Pfadkosten hat. Die Pfadkosten können an einen höheren oder niedrigeren Wert angepasst werden, und außerdem werden sie zur Weiterleitung des Datenverkehrs bei einem Pfad-Rerouting verwendet.

**Default Path Cost** Die Standardpfadkosten des Ports werden automatisch durch die Portgeschwindigkeit und die Pfadkosten-Standardmethode eingestellt.

Die Standardwerte für die Kosten langer Pfade sind:

**Ethernet - 2000000**

**Fast Ethernet - 200000**

**Gigabit Ethernet - 20000**

Die Standardwerte für die Kosten kurzer Pfade (kurze Pfadkosten sind Standard) sind:

**Ethernet - 100**

**Fast Ethernet - 19**

**Gigabit Ethernet - 4**

**Priority (0-240, in steps of 16)** Der Prioritätswert des Ports. Durch den Prioritätswert kann Einfluss auf die Portauswahl genommen werden, wenn eine Bridge über zwei Ports verfügt, die sich in einer Schleifenkonfiguration befinden. Der Prioritätswert liegt zwischen 0 und 240. Der Prioritätswert wird in Inkrementen von 16 angegeben.

**Designated Bridge ID** Gibt die Bridge-Priorität und die MAC-Adresse der designierten Bridge an.

**Designated Port ID** Die Priorität und Schnittstelle des ausgewählten Ports.

**Designated Cost** Gibt die Kosten des Ports an, der Bestandteil der STP-Topologie ist. Bei Ports mit niedrigeren Kosten ist die Wahrscheinlichkeit einer Blockierung geringer, wenn STP Schleifen erfasst.

**Forward Transitions** Gibt an, wie häufig der Port vom **Blockierungs-**in den **Weiterleitungsstatus** gewechselt hat.

**LAG** Gibt die LAG an, mit der der Port verknüpft ist.

## **Aktivieren von STP für einen Port**

1. Öffnen Sie die Seite [STP Port Settings](#).
2. Wählen Sie **Enabled** im Feld **STP Port Status**.
3. Definieren Sie die Felder **Fast Link**, **Path Cost** und **Priority**.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

STP wird für den Port aktiviert.

### Ändern der STP-Eigenschaften für Ports

1. Öffnen Sie die Seite [STP Port Settings](#).
2. Ändern Sie die Felder **Priority**, **Fast Link**, **Path Cost** und **Fast Link**.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die STP-Portparameter werden geändert und das Gerät aktualisiert.

### Anzeigen der STP-Port-Tabelle

1. Öffnen Sie die Seite [STP Port Settings](#).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die **STP Port Table** wird geöffnet.

### Definieren von STP-Portparametern mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Definition von STP-Portparametern, wie auf der Seite [STP Port Settings](#) angezeigt, zusammen.

Tabelle 7-61. CLI-Befehle für STP-Porteinstellungen

CLI-Befehl	Beschreibung
<code>spanning-tree disable</code>	Deaktiviert Spanning Tree für einen spezifischen Port.
<code>spanning-tree cost <i>cost</i></code>	Konfiguriert den Spanning Tree-Kostenbeitrag für einen Port.
<code>spanning-tree port-priority <i>priority</i></code>	Konfiguriert die Portpriorität.
<code>spanning-tree portfast</code>	Aktiviert den PortFast-Modus.
<code>show spanning-tree [ethernet <i>interface</i>   port-channel <i>port-channel-number</i>]</code>	Zeigt die Spanning Tree-Konfiguration an.

Das folgende Beispiel illustriert die CLI-Befehle:

```

console(config)# interface ethernet g5

console(config-if)# spanning-tree disable

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

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

```

```

Console(config-if)# exit

Console(config)# exit

console# show spanning-tree ethernet g5

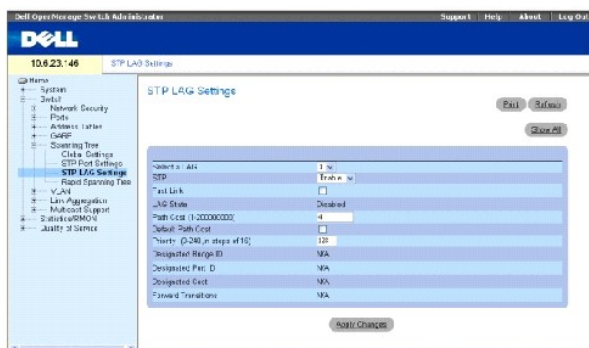
```

Port g5 disabled		
Bundesstaat: Deaktiviert	Rolle: Deaktiviert	
Port id: 96.5	Port cost: 35000	
Typ: P2p (configured: Auto) STP	Port Fast: No (configured: No)	
Designated bridge Priority : 32768	Adresse: 00:e8:00:b4:c0:00	
Designated port id: 96.5	Designated path cost: 19	
Number of transitions to forwarding state: 0		
BPDU: sent 0, received 0		
console#		

## Definieren von STP-Einstellungen für LAGs

Die Seite [STP LAG Settings](#) enthält Felder zur Zuweisung von STP-Portaggregations-Parametern. Öffnen Sie die Seite [STP LAG Settings](#), indem Sie auf **Switch** → **Spanning Tree** → **LAG Settings** in der Strukturansicht klicken.

Abb. 7-100. STP-Einstellungen für LAGs



**Select a LAG** Gibt die benutzerdefinierte LAG an. Weitere Informationen finden Sie unter [„Definition der LAG-Komponenten“](#).

**STP** Aktiviert/deaktiviert STP für die LAG.

**Fast Link** Aktiviert den Fast Link-Modus für die LAG. Falls der Fast Link-Modus für eine LAG aktiviert ist, wird der **Port** automatisch in den **Weiterleitungs**status versetzt, sobald die LAG-Verbindung aktiv ist. Der Fast Link-Modus optimiert die Zeit, die zur Konvergenz des STP-Protokolls erforderlich ist. Die STP-Konvergenz kann in großen Netzwerken 30 bis 60 Sekunden dauern.

**LAG State** Gibt den aktuellen STP-Status für eine LAG an. Falls aktiviert, wird durch den LAG-Status die Weiterleitungsaktion für den Datenverkehr bestimmt. Wenn die Bridge eine fehlerhaft arbeitende LAG identifiziert, wird die LAG in den Status **Broken** versetzt. Folgende LAG-Zustände sind möglich:

**Disabled** Zeigt an, dass die LAG-Verbindung derzeit inaktiv ist.

**Blocking** Die LAG ist derzeit blockiert und kann nicht für die Weiterleitung von Datenverkehr oder die Erfassung von MAC-Adressen verwendet werden.

**Listening** Die LAG befindet sich derzeit im Überwachungsmodus und ist nicht in der Lage, Datenverkehr weiterzuleiten oder MAC-Adressen zu erfassen.

**Learning** Die LAG befindet sich derzeit im Erfassungsmodus und kann zwar keinen Datenverkehr weiterleiten, jedoch neue MAC-Adressen erfassen.

**Forwarding** Die LAG befindet sich derzeit im Weiterleitungsmodus und kann Datenverkehr weiterleiten und neue MAC-Adressen erfassen.

**Broken** Die LAG ist derzeit defekt und kann nicht für die Weiterleitung von Datenverkehr verwendet werden.

**Path Cost (1-200000000)** Gibt an, welchen Anteil diese LAG an den Root-Pfadkosten hat. Die Pfadkosten können an einen höheren oder niedrigeren Wert angepasst werden, und außerdem werden sie zur Weiterleitung des Datenverkehrs bei einem Pfad-Rerouting verwendet. Die Pfadkosten haben einen Wert zwischen 1 und 200000000. Bei der kurzen Pfadkostenmethode ist der Standardkostenwert der LAG 4. Bei der langen Pfadkostenmethode ist der Standardkostenwert der LAG 20000.

**Default Path Cost** Falls ausgewählt, werden die LAG-Pfadkosten auf ihren Standardwert zurückgesetzt.

**Priority (0-240, in steps of 16)** Gibt den Prioritätswert der LAG an. Durch den Prioritätswert kann Einfluss auf die LAG-Auswahl genommen werden, wenn eine Bridge über zwei Ports verfügt, die sich in einer Schleifenkonfiguration befinden. Der Prioritätswert liegt zwischen 0 und 240. Der Prioritätswert wird in Inkrementen von 16 angegeben.

**Designated Bridge ID** Gibt die Bridge-Priorität und die MAC-Adresse der designierten Bridge an.

**Designated Port ID** Gibt die Priorität und die Schnittstellennummer des ausgewählten Ports an.

**Designated Cost** Gibt die Kosten der designierten Bridge an.

**Forward Transitions** Gibt an, wie häufig die LAG vom **Blockierungs**-in den **Weiterleitungs**status gewechselt hat.

### Ändern der STP-Parameter für LAGs:

1. Öffnen Sie die Seite [STP LAG Settings](#).
2. Wählen Sie eine LAG aus dem Drop-Down-Menü **Select a LAG** aus.

3. Ändern Sie die Felder wie gewünscht.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die STP-Parameter der LAG werden geändert und das Gerät aktualisiert.

## Definieren von STP-Einstellungen für LAGs mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Definition der STP-Einstellungen für LAGs zusammen.

Tabelle 7-62. CLI-Befehle für STP-Einstellungen für LAGs

CLI-Befehl	Beschreibung
<code>spanning-tree</code>	Aktiviert die Spanning Tree-Funktion.
<code>spanning-tree disable</code>	Deaktiviert Spanning Tree für eine spezifische LAG.
<code>spanning-tree cost cost</code>	Konfiguriert den Spanning Tree-Kostenbeitrag für eine LAG.
<code>spanning-tree port-priority priority</code>	Konfiguriert die Portpriorität.
<code>show spanning-tree [ethernet interface   port-channel port-channel-number]</code>	Zeigt die Spanning Tree-Konfiguration an.
<code>show spanning-tree [detail] [active   blockedports]</code>	Zeigt detaillierte Spanning Tree-Informationen zu aktiven oder blockierten Ports an.

Das folgende Beispiel illustriert 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 Konvergenz kann jedoch 30 bis 60 Sekunden dauern. Diese Konvergenzzeit gilt für viele Anwendungen als zu lang. Bei entsprechender Unterstützung durch die Netzwerktopologie kann die Konvergenz beschleunigt werden. Das Rapid Spanning Tree Protocol (RSTP) erkennt und verwendet Netzwerktopologien, die eine schnellere Spanning Tree-Konvergenz ohne Bildung von Weiterleitungsschleifen ermöglichen.

RSTP verfügt über die folgenden verschiedenen Statuswerte für Ports:

- 1 Disabled (Deaktiviert)
- 1 Überwachung (Learning)
- 1 Blockierung (Discarding)
- 1 Forwarding (Weiterleitung)

Rapid Spanning Tree wird auf der Seite [STP Global Settings](#) aktiviert. Öffnen Sie die Seite [Rapid Spanning Tree \(RSTP\)](#), indem Sie auf **Switch** → **Spanning Tree** → **Rapid Spanning Tree** in der Strukturansicht klicken.

Abb. 7-101. Rapid Spanning Tree (RSTP)



**Interface** Gibt die Nummer des Ports oder der LAG an, für die RSTP aktiviert wird.

**Role** Gibt die Rolle des Ports an, die vom STP-Algorithmus zur Bereitstellung von STP-Pfaden zugewiesen wird. Folgende Feldwerte können ausgewählt werden:

**Root** Stellt den Pfad mit den niedrigsten Kosten zur Weiterleitung von Paketen an das Root-Gerät bereit.

**Designated** Der Port oder die LAG, über die das designierte Gerät mit dem LAN verbunden ist.

**Alternate** Stellt einen alternativen Pfad zum Root-Gerät von der Root-Schnittstelle bereit.

**Backup** Stellt einen Backup-Pfad für den designierten Portpfad zu den Spanning Tree-Endpunkten bereit. Backup-Ports kommen nur dann vor, wenn zwei Ports in einer Schleife verbunden sind. Backup-Ports treten auch dann auf, wenn in einem LAN mindestens zwei Verbindungen zu einem gemeinsamen Segment anliegen.

**Disabled** Gibt an, dass der Port kein Bestandteil des Spanning Tree ist (die Verbindung des Ports ist deaktiviert).

**Fast Link Operational Status** Gibt an, ob Fast Link für den Port oder die LAG aktiviert oder deaktiviert ist. Wenn Fast Link für einen Port aktiviert ist, wird der Port automatisch in den Weiterleitungszustand versetzt.

**Point-to-Point Admin Status** Aktiviert/deaktiviert die Fähigkeit des Geräts zur Herstellung einer Punkt-zu-Punkt-Verbindung oder legt die automatische Herstellung einer Punkt-zu-Punkt-Verbindung für das Gerät fest.

Zur Herstellung von Kommunikation über eine Punkt-zu-Punkt-Verbindung sendet die Quell-PPP zuerst Link Control Protocol (LCP)-Pakete zur Konfiguration und Testen der Datenverbindung. Nachdem eine Verbindung hergestellt wurde und optionale Einrichtungen gemäß den Erfordernissen des LCP ausgehandelt wurden, sendet das Quell-PPP Network Control Protocols (NCP)-Pakete zur Auswahl und Konfiguration eines oder mehrerer Netzwerk-Layer-Protokolle aus. Wenn jedes der gewählten Netzwerk-Layer-Protokolle konfiguriert wurde, können Pakete von jedem Netzwerk-Layer-Protokoll über die Verbindung übertragen werden. Die Verbindung bleibt zur Kommunikation konfiguriert, bis sie durch ausdrückliche LCP- oder NCP-Pakete geschlossen wird bzw. bis ein externes Ereignis auftritt. Dieses ist der tatsächliche Verbindungstyp des Geräteports. Sie kann vom Verwaltungszustand abweichen.

**Point-to-Point Operational Status** Gibt den Punkt-zu-Punkt-Betriebsstatus an.

**Activate Protocol Migration Test** Ermöglicht, falls ausgewählt, dem PPP das Versenden von Link Control Protocol (LCP)-Paketen zur Konfiguration und zum Testen der Datenverbindung.

## Aktivieren von Rapid STP

1. Öffnen Sie die Seite [Rapid Spanning Tree \(RSTP\)](#).
2. Definieren Sie die Felder **Point-to-Point Admin**, **Point-to-Point Oper** und **Activate Protocol Migration**.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

RSTP wird aktiviert und das Gerät aktualisiert.

## Definieren von Rapid STP-Parametern mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Definition von Rapid STP-Parametern, wie auf der Seite [Rapid Spanning Tree \(RSTP\)](#) angezeigt, zusammen.

Tabelle 7-63. CLI-Befehle für RSTP-Einstellungen

CLI-Befehl	Beschreibung
<code>spanning-tree link-type { point-to-point   shared }</code>	Setzt die Einstellung für den Standardverbindungstyp außer Kraft.
<code>spanning tree mode { stp   rstp }</code>	Konfiguriert das derzeit ausgeführte STP.
<code>clear spanning-tree detected-protocols [ ethernet <i>interface</i>   port-channel <i>port-channel-number</i> ]</code>	Startet den Protokollmigrationsprozess neu.
<code>show spanning-tree [ ethernet <i>interface</i>   port-channel <i>port-channel-number</i> ]</code>	Zeigt die STP-Konfiguration an.

Das folgende Beispiel illustriert die CLI-Befehle:

```
console(config)# interface ethernet g5

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.

<sup>24</sup> ÄÄNs verfügen über eine unbegrenzte Anzahl von Ports und können pro Gerät oder einer anderen logischen Verbindungskombination erstellt werden, da sie softwarebasiert und nicht durch physische Attribute definiert sind.

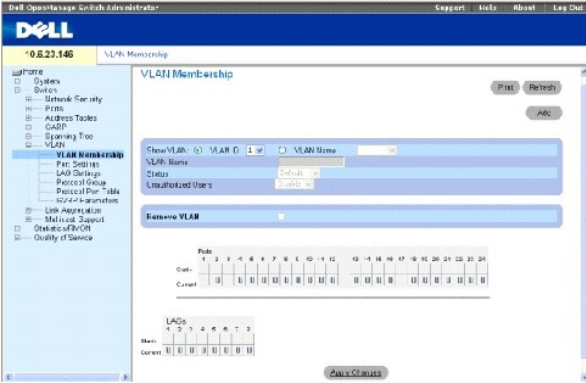
VLANs arbeiten auf Layer 2. Da der Datenverkehr bei VLAN-Verbindungen innerhalb des VLANs isoliert wird, wird ein Layer 3-Router benötigt, um den Datenfluss zwischen VLANs zu ermöglichen. Layer 3-Router dienen zur Identifikation von Segmenten und kooperieren mit VLANs. Bei VLANs handelt es sich um Broadcast- 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 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 die automatische Verteilung von VLAN-Informationen. Öffnen Sie die Seite [VLAN](#), indem Sie auf **Switch** → **VLAN** in der Strukturansicht klicken.

## Definieren von VLAN-Komponenten

Die Seite VLAN Membership enthält Felder zur Definition von VLAN-Gruppen. Das Gerät unterstützt die Zuordnung von 4094 VLAN IDs zu 256 VLANs. Alle Ports müssen eine vordefinierte PVID haben. Wenn keine anderer Wert konfiguriert ist, wird die Standard-VLAN-PVID verwendet. VLAN 1 ist das Standard-VLAN, das nicht vom System gelöscht werden kann. Öffnen Sie die Seite VLAN Membership, indem Sie auf **Switch** → **VLAN** → **VLAN Membership** in der Strukturansicht klicken.

Abb. 7-102. VLAN-Komponenten



**Show VLAN** Listet spezifische VLAN-Informationen nach VLAN-ID oder VLAN-Name auf und zeigt sie an.

**VLAN Name** Der benutzerdefinierte VLAN-Name.

**Status** Der VLAN-Typ. Mögliche Werte sind:

**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.

**Unauthorized Users** Aktiviert/deaktiviert den VLAN-Zugriff durch nicht autorisierte Benutzer.

**Remove VLAN** Entfernt, wenn ausgewählt, das VLAN aus der VLAN Membership-Tabelle.

## Hinzufügen neuer VLANs

1. Öffnen Sie die Seite VLAN Membership.
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite **Create New VLAN** wird geöffnet.

3. Geben Sie die VLAN ID und den VLAN-Namen ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das neue VLAN wird hinzugefügt und das Gerät aktualisiert.

## Ändern von VLAN-Membership-Gruppen

1. Öffnen Sie die Seite VLAN Membership.
2. Wählen Sie ein VLAN im Drop-Down-Menü **Show VLAN** aus.
3. Ändern Sie die Felder wie gewünscht.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).



Die VLAN-Membership-Informationen werden geändert und das Gerät aktualisiert.

### Löschen von VLAN-Membership-Gruppen

1. Öffnen Sie die Seite VLAN Membership.
2. Wählen Sie ein VLAN im Feld **Show VLAN** aus.
3. Wählen Sie das Kontrollkästchen **Remove VLAN** (VLAN entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das ausgewählte VLAN wird gelöscht und das Gerät aktualisiert.

### Definieren von VLAN-Membership-Gruppen mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Definition von VLAN-Membership-Gruppen, wie auf der Seite VLAN Membership angezeigt, zusammen.

Tabelle 7-64. CLI-Befehle für VLAN-Mitgliedschaftsgruppen

CLI-Befehl	Beschreibung
<code>vlan database</code>	Ruft den Schnittstellenkonfigurationsmodus (VLAN) auf.
<code>vlan {vlan-range}</code>	Erstellt ein VLAN.
<code>name string</code>	Fügt einem VLAN einen Namen hinzu.

Das folgende Beispiel illustriert die CLI-Befehle:

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

### VLAN-Port-Membership-Tabelle

Die VLAN Port Membership Table enthält eine Port-Tabelle für die Zuweisung von Ports zu VLANs. Um Ports eine VLAN-Mitgliedschaft zuzuweisen, müssen die Einstellungen für die Port-Steuerung geändert werden. Ports können über die folgenden Werte verfügen:

Tabelle 7-65. VLAN-Port-Membership-Tabelle

Port-Kontrolle	Definition
T	Die Schnittstelle gehört einem VLAN an. Alle über die Schnittstelle weitergeleitete Pakete verfügen über eine Kennung. Die Pakete enthalten VLAN-Informationen.
U	Die Schnittstelle gehört dem VLAN an. Über die Schnittstelle weitergeleitete Pakete besitzen keine Kennung.
F	Der Schnittstelle wird die Mitgliedschaft in einem VLAN verweigert.
Keine	Die Schnittstelle gehört diesem VLAN nicht an. Mit der Schnittstelle verknüpfte Pakete werden nicht weitergeleitet.

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

In der VLAN Port Membership Table werden die Ports und der Portstatus sowie die LAGs angezeigt.

### Zuweisen von Ports zu einer VLAN-Gruppe

1. Öffnen Sie die Seite VLAN Membership.
2. Klicken Sie auf die Optionsschaltfläche **VLAN ID** oder **VLAN Name** und wählen Sie ein VLAN aus dem Drop-Down-Menü aus.
3. Wählen Sie einen Port in der **Port Membership Table** und weisen Sie dem Port einen Wert zu.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Port wird der VLAN-Gruppe zugewiesen und das Gerät wird aktualisiert.

### Löschen von VLANs

1. Öffnen Sie die Seite VLAN Membership.
2. Klicken Sie auf die Optionsschaltfläche **VLAN ID** oder **VLAN Name** und wählen Sie ein VLAN aus dem Drop-Down-Menü aus.
3. Wählen Sie das Kontrollkästchen **Remove VLAN**.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das ausgewählte VLAN wird gelöscht und das Gerät aktualisiert.

### Zuweisen von Ports zu VLAN-Gruppen mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Zuweisung von Ports zu VLAN-Gruppen zusammen.

Tabelle 7-66. CLI-Befehle für die Zuweisung von Ports zu VLAN-Gruppen

CLI-Befehl	Beschreibung
<code>switchport general acceptable-frame-types tagged-only</code>	Aktiviert die EingangsfILTERUNG für Frames ohne Kennung.
<code>switchport forbidden vlan {add vlan-list   remove vlan-list}</code>	Verhindert das Hinzufügen spezifischer VLANs zum Port.
<code>switchport mode {access   trunk   general}</code>	Konfiguriert den VLAN-Mitgliedschaftsmodus eines Ports.
<code>switchport access vlan vlan-id</code>	Konfiguriert die VLAN ID, wenn sich die Schnittstelle im Zugriffsmodus befindet.
<code>switchport trunk allowed vlan {add vlan-list   remove vlan-list}</code>	Entfernt oder fügt VLANs zu einem Trunk-Port hinzu.
<code>switchport trunk native vlan vlan-id</code>	Definiert den Port als Mitglied des angegebenen VLAN und die VLAN ID als die „port default VLAN ID (PVID)“.
<code>switchport general allowed vlan add vlan-list [tagged   untagged]</code>	Entfernt oder fügt VLANs zu einem allgemeinen Port hinzu.
<code>switchport general pvid vlan-id</code>	Konfiguriert die PVID, während sich die Schnittstelle im allgemeinen Modus befindet.

Das folgende Beispiel illustriert die CLI-Befehle:

```
Console (config)# vlan database

Console (config-vlan)# vlan 23-25

Console (config-vlan)# exit

Console(config)# interface vlan 23

Console (config-if)# name Marketing

Console(config-if)# exit

Console (config)# interface ethernet g8

Console (config-if)# switchport mode access

Console (config-if)# switchport access vlan 23

Console(config-if)# exit

Console (config)# interface ethernet g9

Console (config-if)# switchport mode trunk

Console (config-if)# switchport mode trunk allowed vlan add 23-25

Console(config-if)# exit

Console (config)# interface ethernet g10

Console (config-if)# switchport mode general

Console (config-if)# switchport general allowed vlan add 23,25 tagged

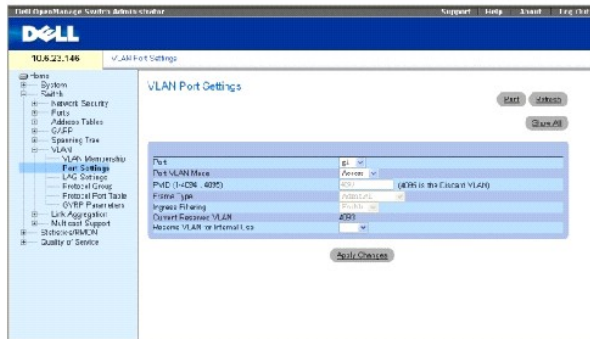
Console (config-if)# switchport general pvid 25
```

## Definieren von VLAN-Einstellungen für Ports

Die Seite [VLAN Port Settings](#) enthält Felder zur Verwaltung von Ports, die einem VLAN angehören. Die Standard-VLAN-ID (PVID) wird auf der Seite [VLAN Port Settings](#) konfiguriert. Alle über das Gerät eingehenden Pakete ohne Kennung werden mit der PVID des Ports versehen.

Öffnen Sie die Seite [VLAN Port Settings](#), indem Sie auf **Switch**→ **VLAN**→ **Port Settings** in der Strukturansicht klicken.

Abb. 7-103. VLAN-Einstellungen für Ports



**Port** Die Nummer des Ports, der Teil des VLAN ist.

**Port VLAN Mode** Der Port-Modus. Mögliche Werte sind:

**General** Gibt an, dass der Port VLANs angehört und dass jedes VLAN vom Benutzer als VLAN mit oder ohne Kennung definiert wurde (voller 802.1Q-Modus).

**Access** Gibt an, dass der Port zu einem einzelnen VLAN ohne Kennung gehört. Wenn der Port im Zugriffsmodus ist, können keine am Port akzeptierten Pakettypen designiert werden. Die Eingangsfilterung kann für den Zugriffsport nicht aktiviert/deaktiviert werden.

**Trunk** Gibt an, dass der Port VLANs angehört, in dem alle Ports über eine Kennung verfügen (mit Ausnahme von einem Port, der nicht gekennzeichnet sein darf).

**PVID** Weist Paketen ohne Kennung eine VLAN-ID zu. Die möglichen Werte sind 1-4094. VLAN 4095 ist gemäß Standard und Industriepraxis als Discard-VLAN definiert. Nach Discard-VLAN klassifizierte Pakete werden abgelehnt.

**Frame Type** Der am Port akzeptierte Pakettyp. Mögliche Werte sind:

**Admit Tag Only** Gibt an, dass nur Pakete mit Kennung am Port akzeptiert werden.

**Admit All** Gibt an, dass Pakete mit und ohne Kennung am Port akzeptiert werden.

**Ingress Filtering** Aktiviert/deaktiviert die Eingangsfilterung für den Port. Bei der Eingangsfilterung werden Pakete abgelehnt, die an VLANs gerichtet sind, denen die angegebene LAG nicht angehört.

**Current Reserve VLAN** Gibt das VLAN an, das derzeit vom System als reserviertes VLAN ausgewiesen ist.

**Reserve VLAN for Internal Use** Gibt das vom Benutzer als reserviertes VLAN ausgewählte VLAN an, wenn es nicht vom System verwendet wird.

## Zuweisen von Porteinstellungen

1. Öffnen Sie die Seite [VLAN Port Settings](#).
2. Wählen Sie den Port, dem Einstellungen zugewiesen werden, aus dem Drop-Down-Menü **Port**.
3. Geben Sie die Informationen in die restlichen Felder auf der Seite ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die VLAN-Portparameter werden definiert und das Gerät aktualisiert.

### Anzeigen der VLAN Port-Tabelle

1. Öffnen Sie die Seite [VLAN Port Settings](#).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die **VLAN Port Table** wird geöffnet.

### Zuweisen von Ports zu VLAN-Gruppen mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Zuweisung von Ports zu VLAN-Gruppen zusammen.

Tabelle 7-67. CLI - Befehle für VLAN-Ports

CLI-Befehl	Beschreibung
<code>switchport mode { access   trunk   general }</code>	Konfiguriert den VLAN-Mitgliedschaftsmodus für einen Port.
<code>switchport trunk native vlan <i>vlan-id</i></code>	Definiert den Port als Mitglied des angegebenen VLAN und die VLAN ID als die „port default VLAN ID (PVID)“.
<code>switchport general pvid <i>vlan-id</i></code>	Konfiguriert die PVID (Port VLAN ID), während sich die Schnittstelle im allgemeinen Modus befindet.
<code>switchport general allowed vlan add <i>vlan-list</i> [ tagged   untagged ]</code>	Entfernt oder fügt VLANs zu einem allgemeinen Port hinzu.
<code>switchport general acceptable-frame-types tagged-only</code>	Aktiviert die Eingangsfilterung für Frames ohne Kennung.
<code>switchport general ingress-filtering disable</code>	Deaktiviert die Eingangsfilterung für einen Port.
<b>Herunterfahren</b>	Deaktiviert Schnittstellen.
<code>set interface active { ethernet <i>interface</i>   port-channel <i>port-channel-number</i> }</code>	Reaktiviert eine Schnittstelle, die aus Sicherheitsgründen deaktiviert wurde.

Das folgende Beispiel illustriert die CLI-Befehle:

```

Console (config)# interface range ethernet g18-20

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

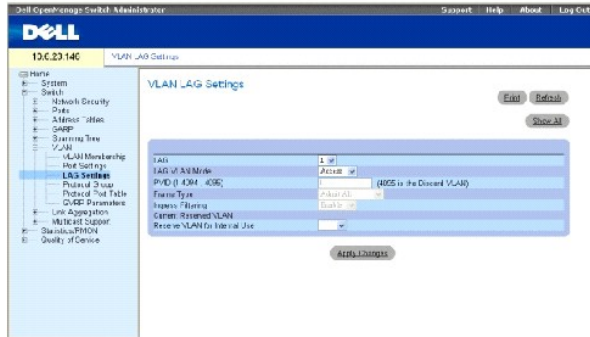
Console (config-if)# switchport general ingress-filtering disable

```

### Definieren von VLAN-Einstellungen für LAGs

Die Seite [VLAN LAG Setting](#) stellt Parameter zur Verwaltung von LAGs bereit, die einem VLAN angehören. VLANs setzen sich entweder aus einzelnen Ports oder LAGs zusammen. Auf dem Gerät eingehende Pakete ohne Kennung werden mit der PVID-Kennung der LAG versehen. Öffnen Sie die Seite [VLAN LAG Setting](#), indem Sie auf **Switch**→**VLAN**→**LAG Settings** in der Strukturansicht klicken.

**Abb. 7-104. VLAN-Einstellungen für LAGs**



**LAG** Gibt die Nummer der im VLAN enthaltenen LAG an.

**LAG VLAN Mode** Gibt den VLAN-Modus der LAG an. Mögliche Werte sind:

**General** Gibt an, dass die LAG VLANs angehört und dass jedes VLAN vom Benutzer als VLAN mit oder ohne Kennung definiert wird (voller 802.1Q-Modus).

**Access** Gibt an, dass die LAG zu einem einzelnen VLAN ohne Kennung gehört.

**Trunk** Gibt an, dass die LAG VLANs angehört, in der alle Ports über eine Kennung verfügen (mit Ausnahme von einem einzigen optionalen nativen VLAN).

**PVID** Weist Paketen ohne Kennung eine VLAN-ID zu. Die möglichen Feldwerte sind 1-4095. VLAN 4095 ist gemäß Standard und Industriepraxis als Discard-VLAN definiert. Nach Discard-VLAN klassifizierte Pakete werden abgelehnt.

**Frame Type** Gibt den von der LAG akzeptierten Pakettyp an. Mögliche Werte sind:

**Admit Tag Only** Gibt an, dass nur Pakete mit Kennung von der LAG akzeptiert werden.

**Admit All** Gibt an, dass Pakete sowohl mit als auch ohne Kennung von der LAG akzeptiert werden.

**Ingress Filtering** Aktiviert/deaktiviert die Eingangsfilterung für die LAG. Bei der Eingangsfilterung werden Pakete abgelehnt, die an VLANs gerichtet sind, denen die angegebene LAG nicht angehört.

**Current Reserve VLAN** Gibt das VLAN an, das derzeit als reserviertes VLAN ausgewiesen ist.

**Reserve VLAN for Internal Use** Gibt das VLAN an, das nach einer Rücksetzung des Geräts als reserviertes VLAN designiert ist.

Zuweisen von VLAN-Einstellungen zu LAGs:

1. Öffnen Sie die Seite [VLAN LAG Setting](#).

2. Wählen Sie eine LAG aus dem Drop-Down-Menü **LAG** und geben Sie die Informationen in den Feldern auf der Seite ein.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die VLAN-Parameter der LAG werden geändert und das Gerät aktualisiert.

### Anzeigen der VLAN LAG-Tabelle

1. Öffnen Sie die Seite [VLAN LAG Setting](#).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die **VLAN LAG Table** wird geöffnet.

### Zuweisen von LAGs zu VLAN-Gruppen mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Zuweisung von LAGs zu VLAN-Gruppen, wie auf der Seite [VLAN LAG Setting](#) angezeigt, zusammen.

**Tabelle 7-68. CLI-Befehle für die Zuweisung von LAGs zu VLAN-Gruppen**

CLI-Befehl	Beschreibung
<code>switchport mode { access   trunk   general }</code>	Konfiguriert den VLAN-Mitgliedschaftsmodus für einen Port.
<code>switchport trunk native vlan <i>vlan-id</i></code>	Definiert den Port als Mitglied des angegebenen VLAN und die VLAN ID als die „port default VLAN ID (PVID)“.
<code>switchport general pvid <i>vlan-id</i></code>	Konfiguriert die PVID (Port VLAN ID), während sich die Schnittstelle im allgemeinen Modus befindet.
<code>switchport general allowed vlan add <i>vlan-list</i> [ tagged   untagged ]</code>	Entfernt oder fügt VLANs zu einem allgemeinen Port hinzu.
<code>switchport general acceptable-frame-type tagged-only</code>	Aktiviert die Eingangsfilterung für Frames ohne Kennung.
<code>switchport general ingress-filtering disable</code>	Deaktiviert die Eingangsfilterung für einen Port.

Das folgende Beispiel illustriert die CLI-Befehle:

```

console(config)# interface port-channel 1

console(config-if)# switchport mode access

console(config-if)# switchport access vlan 2

Console(config-if)# exit

console(config)# interface port-channel 2

console(config-if)# switchport mode general

console(config-if)# switchport general allowed vlan add 2-3 tagged

```

```

console(config-if)# switchport general pvid 2

console(config-if)# switchport general acceptable-frame-type tagged-
only

console(config-if)# switchport general ingress-filtering disable

Console(config-if)# exit

console(config)# interface port-channel 3

console(config-if)# switchport mode trunk

console(config-if)# switchport trunk native vlan 3

console(config-if)# switchport trunk allowed vlan add 2

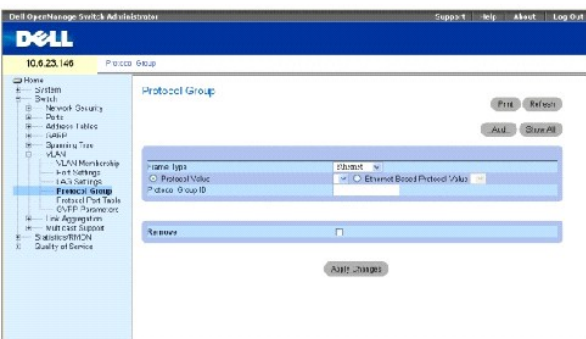
Console(config-if)# exit

```

## Definieren von VLAN-Protokollgruppen

Die Seite [Protocol Group](#) stellt Parameter zur Konfiguration von Frame-Typen für bestimmte Protokollgruppen bereit. Öffnen Sie die Seite [Protocol Group](#), indem Sie auf **Switch** → **VLAN** → **Protocol Group** in der Strukturansicht klicken.

Abb. 7-105. Protokollgruppe



**Frame Type** Gibt den Pakettyp an. Mögliche Feldwerte sind **Ethernet**, **RFC1042** und **LLC Other**.

**Protocol Value** Gibt den benutzerdefinierten Protokollnamen an.

**Ethernet-Based Protocol Value** Gibt den Typ der Ethernet-Protokollgruppe an. Die möglichen Feldwerte sind **IP**, **IPX** und **IPV6**.

**Protocol Group ID** Gibt die ID-Nummer der VLAN-Gruppe an.



**Remove** Entfernt, wenn ausgewählt, die Zuordnung von Frames zu Protokollgruppen, wenn die entfernte Protokollgruppe nicht für diesen Protokollport konfiguriert ist.

### Hinzufügen einer Protokollgruppe

1. Öffnen Sie die Seite [Protocol Group](#).
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite **Add Protocol to Group** wird geöffnet.

3. Geben Sie die Informationen in die Felder auf der Seite ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Protokollgruppe wird zugewiesen und das Gerät wird aktualisiert.

### Zuweisung von VLAN-Protokollgruppeneinstellungen

1. Öffnen Sie die Seite [Protocol Group](#).
2. Geben Sie die Informationen in die Felder auf der Seite ein.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die VLAN-Protokollgruppen-Parameter werden definiert und das Gerät aktualisiert.

### Entfernen von Protokollen aus der Protokollgruppen-Tabelle

1. Öffnen Sie die Seite [Protocol Group](#).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die **Protocol Group Table** wird geöffnet.

3. Wählen Sie **Remove** (Entfernen) für die zu entfernenden Protokollgruppen aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das Protokoll wird entfernt und das Gerät wird aktualisiert.

### Definieren von VLAN-Protokollgruppen mit den CLI-Befehlen

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

Tabelle 7-69. CLI-Befehle für VLAN-Protokollgruppen

CLI-Befehl	Beschreibung
<code>map protocol protocol [encapsulation] protocols-group group</code>	Ordnet einer Protokollgruppe ein Protokoll zu. Protokollgruppen werden zur protokollbasierten VLAN-Zuordnung verwendet.

Im folgenden Beispiel wird das ip-arp-Protokoll der Gruppe „213“ zugeordnet:

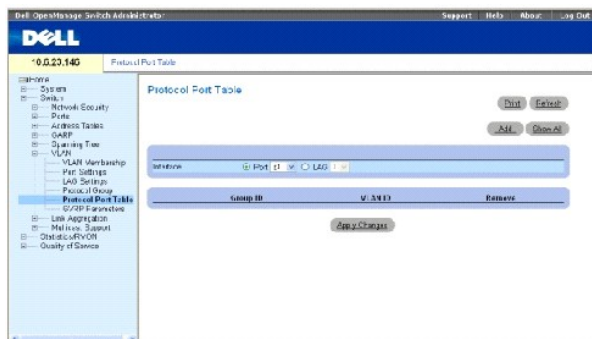
```
Console (config)# vlan
database

Console (config-vlan)#
map protocol ip-arp
protocols-group 213
```

## Hinzufügen von Protokoll-Ports

Auf der Seite [Protocol Port](#) können Schnittstellen zu Protokollgruppen hinzugefügt werden. Öffnen Sie die Seite [Protocol Port](#), indem Sie auf **Switch**→ **VLAN**→ **Protocol Port** in der Strukturansicht klicken.

Abb. 7-106. Protokoll-Port




**Interface** Gibt die einer Protokollgruppe hinzugefügte Port- oder LAG-Nummer an.

**Group ID** Gibt die Protokollgruppen-ID an, der die Schnittstelle hinzugefügt wird. Protokollgruppen-IDs werden in der Protokollgruppen-Tabelle definiert.

**VLAN ID (1-4095)** Fügt die Schnittstelle einer benutzerdefinierten VLAN ID hinzu. Die VLAN ID wird auf der Seite [Create a New VLAN](#) definiert. Protokoll-Ports können entweder einer VLAN ID oder einem VLAN-Namen angefügt werden.

 **ANMERKUNG:** VLAN 4095 ist das Discard-VLAN.

## Hinzufügen eines neuen Protokoll-Ports

 **ANMERKUNG:** Protokoll-Ports können nur auf Ports definiert werden, die auf der Seite [VLAN Port Settings](#) als General definiert sind.

1. Öffnen Sie die Seite [Protocol Port](#).
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite **Add Protocol Port** wird geöffnet.

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

Die neue VLAN-Protokollgruppe wird der **Protocol Port Table** hinzugefügt und das Gerät wird aktualisiert.

## Definieren von Protokoll-Ports mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Definition von Protokoll-Ports zusammen.

Tabelle 7-70. CLI-Befehle für Protokoll-Ports

CLI-Befehl	Beschreibung
<code>switchport general map protocols-group group vlan <i>vlan-id</i></code>	Richtet eine protokollbasierte Klassifikationsregel ein.

Im folgenden Beispiel wird eine protokollbasierte Klassifikationsregel für Protokollgruppe 1 und VLAN 8 festgelegt:

```
Console (config-if)#
switchport general map
protocols-group 1 vlan 8
```

## Konfigurieren von GVRP

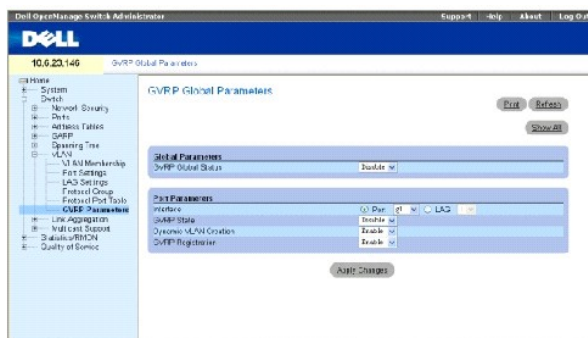
Das GARP VLAN Registration Protocol (GVRP) ist speziell für die automatische Verteilung von VLAN-Mitgliedschaftsinformationen an VLAN-orientierte Bridges konzipiert. Mittels GVRP können VLAN-orientierte Bridges VLANs automatisch erfassen und Portzuweisungen ohne Konfiguration einzelner Bridges überbrücken sowie die VLAN-Mitgliedschaft registrieren.

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:

- 1 Die Anzahl aller statischen VLANs, die bereits ordnungsgemäß konfiguriert sind oder demnächst konfiguriert werden.
- 1 Die Anzahl aller dynamischen an GVRP-Operationen beteiligten VLANs, die bereits konfiguriert sind (die anfängliche Anzahl aller GVRP-VLANs beträgt 128) oder demnächst konfiguriert werden.

Auf der Seite **GVRP Global Parameters** kann GVRP global aktiviert werden. GVRP kann auch jeweils für bestimmte Schnittstellen aktiviert werden. Öffnen Sie die Seite [GVRP Parameters](#), indem Sie auf **Switch** → **VLAN** → **GVRP Parameters** in der Strukturansicht klicken.

Abb. 7-107. GVRP-Parameter



**GVRP Global Status** Aktiviert/deaktiviert GVRP für das Gerät. GVRP ist standardgemäß deaktiviert.

**Interface** Gibt die Nummer des Ports oder der LAG an, für die GVRP aktiviert wird.

**GVRP State** Aktiviert/deaktiviert GVRP für eine Schnittstelle.

**Dynamic VLAN Creation** Aktiviert/deaktiviert die VLAN-Erstellung über GVRP.

**GVRP Registration** Gibt den GVRP-Registrierungsstatus an.

### Aktivieren von GVRP für das Gerät

1. Öffnen Sie die Seite GVRP Global Parameters.
2. Wählen Sie **Enable** im Feld **GVRP Global Status**.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

GVRP wird für das Gerät aktiviert.

### Aktivieren der VLAN-Registration über GVRP

1. Öffnen Sie die Seite GVRP Global Parameters.
2. Wählen Sie **Enable** im Feld **GVRP Global Status** für die gewünschte Schnittstelle aus.
3. Wählen Sie **Enable** im Feld **GVRP Registration** aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die VLAN-Registrierung über GVRP wird für den Port aktiviert und das Gerät wird aktualisiert.

### Konfigurieren von GVRP mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Konfiguration von GVRP, wie auf der Seite GVRP Global Parameters angezeigt, zusammen.

Tabelle 7-71. CLI-Befehle für globale GVRP-Parameter

CLI-Befehl	Beschreibung
<code>gvrp enable (global)</code>	Aktiviert GVRP global.
<code>gvrp enable (interface)</code>	Aktiviert GVRP für eine Schnittstelle.
<code>gvrp vlan-creation-forbid</code>	Aktiviert/deaktiviert dynamische VLAN-Erstellung.
<code>gvrp registration-forbid</code>	Deregistriert alle dynamischen VLANs und verhindert die dynamische VLAN-Registrierung für den Port.
<code>show gvrp configuration [ethernet interface] port-channel port-channel-number]</code>	Zeigt GVRP-Konfigurationsinformationen an, einschließlich Timer-Werte, Aktivierungsstatus von GVRP und dynamischer VLAN-Erstellung und Angabe der Ports, die GVRP ausführen.
<code>show gvrp error-statistics [ethernet interface] port-channel port-channel-number]</code>	Zeigt GVRP-Fehlerstatistiken an.
<code>show gvrp statistics [ethernet interface] port- channel port-channel-number]</code>	Zeigt GVRP-Statistiken an.
<code>clear gvrp statistics [ethernet interface] port- channel port-channel-number]</code>	Löscht alle GVRP-Statistikinformationen.

Das folgende Beispiel illustriert die CLI-Befehle:

```
console(config)# gvrp enable

Console(config)# interface ethernet g1

console(config-if)# gvrp enable

console(config-if)# gvrp vlan-creation-forbid

console(config-if)# gvrp registration-forbid

console(config-if)# end

console# show gvrp configuration
```

GVRP Feature is currently Enabled on the device.						
Maximum VLANs: 223						
Port (s)	GVRP- Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
---	-----	-----	-----	-----	-----	-----
g1	Enabled (Aktiviert)	Forbidden	Disabled (Deaktiviert)	200	900	10000
g2	Disabled (Deaktiviert)	Normal	Enabled (Aktiviert)	200	600	10000

## Aggregieren von Ports

Durch die Port-Aggregation wird die Portnutzung optimiert, indem eine Gruppe von Ports zu einer Link Aggregated Group (LAG) zusammengefasst wird. Die Portaggregation erhöht die Bandbreite zwischen Geräten um ein Vielfaches, steigert die Portflexibilität und gewährleistet die Verbindungsredundanz. Das System unterstützt bis zu acht LAGs pro System sowie acht Ports LAG pro Gerät.

Jede LAG besteht aus Ports mit der gleichen Geschwindigkeit, die auf Vollduplex-Betrieb eingestellt sind. Die Ports 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 Link Aggregation Control Protocol (LACP) aktiviert wird. Das Gerät unterstützt das LAG Load Balancing, das sowohl auf MAC-Quell- als auch auf MAC-Zieladressen basiert.

Aggregierte Verbindungen werden vom System als ein einziger logischer Port behandelt. Konkret bedeutet dies, dass die aggregierte Verbindung über ähnliche Portattribute verfügt wie ein nicht aggregierter Port, z. B. Auto-Negotiation, Geschwindigkeit, Duplexeinstellung usw.

Das Gerät unterstützt sowohl statische LAGs als auch LACP-(Link Aggregation Control Protocol-)LAGs. LACP-LAGs handeln mit anderen LACP-Ports, die sich an einem anderen Gerät befinden, Verbindungen mit aggregierten Ports aus. Wenn es sich bei den Ports des anderen Gerätes ebenfalls um LACP-Ports handelt, richten die Geräte eine LAG für diese Ports ein.

Um Ports einer LAG hinzuzufügen, sollten Sie die folgenden Richtlinien beachten:

- 1 Für den Port darf keine Layer 3-Schnittstelle definiert werden.
- 1 Der Port darf keinem VLAN angehören.
- 1 Der Port darf keiner anderen LAG angehören.
- 1 Der Port darf nicht gespiegelt werden.
- 1 Die 802.1p-Priorität des Ports muss der 802.1p-Priorität der LAG entsprechen.
- 1 Für den Port darf QoS Trust nicht deaktiviert sein.
- 1 GVRP darf nicht aktiviert sein.

 **ANMERKUNG:** Ports dürfen nur als LACP-Ports konfiguriert werden, wenn sie keiner zuvor konfigurierten LAG angehören.

Das Gerät 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 Gerät als ein logischer Port angesehen.

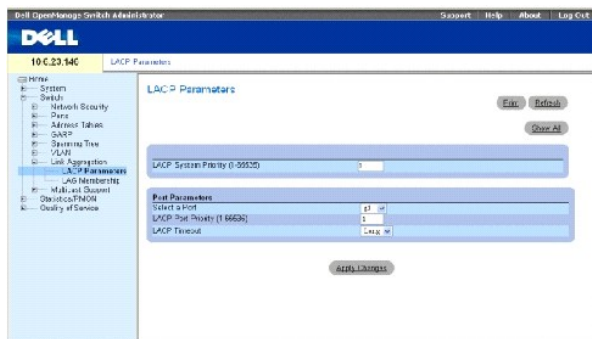
Jede aggregierte Verbindung verfügt über einen aggregierten Verbindungsanschlusstyp, einschließlich Gigabit Ethernet-Ports. Ports können einer aggregierten Verbindung nur hinzugefügt werden, wenn sie denselben Porttyp aufweisen. Wenn Ports aus einer aggregierten Verbindung entfernt werden, werden die ursprünglichen Porteinstellungen wiederhergestellt. Öffnen Sie die Seite **Link Aggregation**, indem Sie auf **Switch** → **Link Aggregation** in der Strukturansicht klicken.

## Definieren von LACP-Parametern

Die Seite **LACP Parameters** enthält Felder zur Konfiguration von LACP-LAGs. Aggregierte Ports können in Gruppen für die Verbindungsaggregation zusammengefasst werden. Jede Gruppe besteht aus Ports mit derselben Geschwindigkeit.

Aggregierte Verbindungen können manuell oder automatisch eingerichtet werden, indem für die relevanten Verbindungen das Link Aggregation Control Protocol (LACP) aktiviert wird. Öffnen Sie die Seite [LACP Parameters](#), indem Sie auf **Switch** → **Link Aggregation** → **LACP Parameters** in der Strukturansicht klicken.

Abb. 7-108. LACP-Parameter



**LACP System Priority** (1-65535) Gibt den LACP-Prioritätswert für globale Einstellungen an. Der zulässige Bereich liegt zwischen 1 und 65.535. Der Standardwert lautet 1.

**Select a Port** Gibt die Portnummer an, der Timeout- und Prioritätswerte zugewiesen werden.

**LACP Port Priority** (1-65535) Gibt den LACP-Prioritätswert für den Port an.

**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 globaler Verbindungsaggregations-Parameter

1. Öffnen Sie die Seite [LACP Parameters](#).
2. Geben Sie die Informationen im Feld **LACP System Priority** ein.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Parameter werden definiert und das Gerät aktualisiert.

### Definieren von Verbindungsaggregations-Parametern für Ports

1. Öffnen Sie die Seite [LACP Parameters](#).
2. Vervollständigen Sie die Felder im Bereich **Port Parameters**.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Parameter werden definiert und das Gerät aktualisiert.

### Anzeigen der LACP-Parameter-Tabelle

1. Öffnen Sie die Seite [LACP Parameters](#).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die **LACP Parameters Table** wird geöffnet.

### Konfigurieren von LACP-Parametern mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Konfiguration von LACP-Parametern, wie auf der Seite [LACP Parameters](#) angezeigt, zusammen.

Tabelle 7-72. CLI-Befehle für LACP-Parameter

CLI-Befehl	Beschreibung
<code>lACP system-priority value</code>	Konfiguriert die Systempriorität.
<code>lACP port-priority value</code>	Konfiguriert den Prioritätswert für physische Anschlüsse
<code>lACP timeout {long   short}</code>	Weist ein administratives LACP-Zeitlimit zu.
<code>show lACP ethernet interface [parameters   statistics   protocol-state]</code>	Zeigt LACP-Informationen für Ethernet-Ports an.

Das folgende Beispiel illustriert die CLI-Befehle:

```
Console (config)# lACP system-priority 120

Console (config)# interface ethernet g1

Console (config-if)# lACP port-priority 247

Console (config-if)# lACP timeout long

Console (config-if)# end

Console# show lACP ethernet g1 statistics

Port g1 LACP Statistics:

LACP PDUs sent:2
```

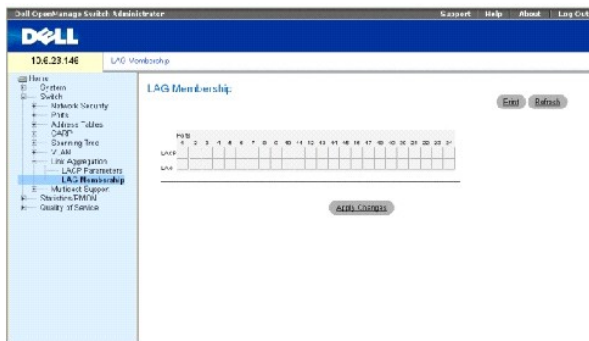
LACP PDUs received:2

## Definieren von LAG-Mitgliedschaften

Die Seite [LAG Membership](#) enthält Felder zur Zuweisung von Ports zu LAGs. LAGs können bis zu acht Ports umfassen. Beim Hinzufügen eines Ports zu einer LAG erwirbt der Port die Eigenschaften der LAG. Wenn der Port nicht mit den LAG-Eigenschaften konfiguriert werden kann, wird ein Trap erzeugt und der Port arbeitet mit seinen Standardeinstellungen.

Die Seite [LAG Membership](#) enthält Felder zur Zuweisung von Ports zu LAGs. Öffnen Sie die Seite [LAG Membership](#), indem Sie auf **Switch** → **Link Aggregation** → **LAG Membership** in der Strukturansicht klicken.

Abb. 7-109. LAG-Mitgliedschaft



**LACP** Fügt den Port über LACP einer LAG hinzu.

**LAG** Fügt einer LAG einen Port hinzu und gibt die spezifische LAG an, welcher der Port angehört.

## Konfiguration eines Ports für eine LAG oder LACP

1. Öffnen Sie die Seite [LAG Membership](#).
2. Stellen Sie in der LAG-Zeile (zweite Zeile) eine spezifische Zahl ein, um den Port der LAG-Nummer hinzuzufügen oder von ihr zu entfernen.
3. Stellen Sie in der LACP-Zeile (erste Zeile) den Knopf unter der Portnummer so ein, dass Sie entweder das LACP oder die statische LAG zuweisen.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Port wird der LAG oder LACP hinzugefügt und das Gerät wird aktualisiert.

## Zuweisen von Ports zu LAGs mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Zuweisung von Ports zu LAGs, wie auf der Seite [LAG Membership](#) angezeigt, zusammen.

Tabelle 7-73. CLI-Befehle für LAG-Mitgliedschaft

CLI-Befehl	Beschreibung
<code>interface port-channel port-channel-number</code>	Aktiviert den Schnittstellenkonfigurationsmodus eines spezifischen Portkanals.
<code>channel-group port-channel-number mode {on   auto}</code>	Weist einen Port einem Portkanal zu. Verwenden Sie die no-Form dieses Befehls, um die Kanalgruppenkonfiguration von der Schnittstelle zu entfernen.
<code>show interfaces port-channel [port-</code>	Zeigt Portkanal-Informationen an.



channel-number]

Das folgende Beispiel illustriert die CLI-Befehle:

```
console# config
console(config)# interface ethernet g1
console(config-if)# channel-group 1 mode on
console(config-if)# 01-Jan-2000 01:47:18 %LINK-W-Down: chl


console(config-if)#
```

## Unterstützung von 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 die Pakete an die relevanten Ports übertragen.

Das Gerät unterstützt die folgenden beiden Einstellungen:

- 1 **Forwarding L2 Multicast Packets** Standardmäßig aktiviert und nicht konfigurierbar.

 **ANMERKUNG:** Das System unterstützt Multicast-Filtern für 320 Multicastgruppen.

- 1 **Filtering L2 Multicast Packets** Aktiviert die Weiterleitung von L2-Paketen an Schnittstellen. Wenn Multicast-Filtern deaktiviert ist, werden Multicast-Pakete an alle relevanten VLAN-Ports weitergeleitet.

Öffnen Sie die Seite **Multicast Support**, indem Sie auf **Switch** → **Multicast Support** in der Strukturansicht klicken.

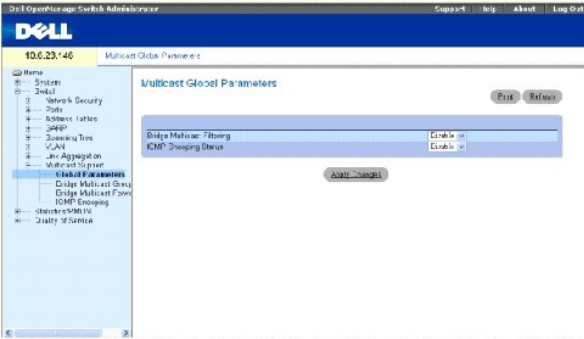
## Definieren von globalen Multicast-Parametern

Beim Layer 2-Switching werden Multicast-Pakete standardmäßig an alle relevanten VLAN-Ports weitergeleitet, wobei die Pakete als Multicast-Pakete behandelt werden. Diese Art der Datenweiterleitung ist prinzipiell funktionsfähig (alle relevanten Ports/Knoten erhalten eine Kopie des Frame). Da jedoch Ports/Knoten irrelevante Frames erhalten können, die nur von einer Untermenge der Ports dieses VLANs benötigt werden, ist sie aber potentiell unwirtschaftlich. Multicast-Weiterleitungsfilter ermöglichen die Weiterleitung von Layer-2-Paketen an Port-Untergruppen, die in der Multicast-Filterdatenbank definiert 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 Ports welchen Multicast-Gruppen beitreten sollen, welche Ports Multicast-Router zur Generierung von IGMP-Abfragen veranlassen und welche Routing-Protokolle Pakete und Multicast-Datenverkehr weiterleiten. Ein Port, der einer bestimmten Multicast-Gruppe beitreten will, gibt einen IGMP-Bericht aus, in dem diese Multicast-Gruppe angegeben ist. Dies führt zur Erstellung der Multicast-Filterdatenbank.

Die Seite [Multicast Global Parameters](#) enthält Felder zur Aktivierung von IGMP-Snooping auf dem Gerät. Öffnen Sie die Seite [Multicast Global Parameters](#), indem Sie auf **Switch** → **Multicast Support** → **Global Parameters** in der Strukturansicht klicken.

**Abb. 7-110. Globale Multicast-Parameter**



**Bridge Multicast Filtering** Aktiviert/deaktiviert die Bridge-Multicast-Filterung. Die Standardeinstellung ist Disabled (Deaktiviert). IGMP-Snooping kann nur aktiviert werden, wenn die Bridge-Multicast-Filterung aktiviert ist.

**IGMP Snooping Status** Aktiviert/deaktiviert IGMP-Snooping auf dem Gerät. Die Standardeinstellung ist Disabled (Deaktiviert).

Aktivieren der Bridge-Multicast-Filterung für das Gerät

1. Öffnen Sie die Seite [Multicast Global Parameters](#).
2. Wählen Sie **Enable** (Entfernen) im Feld **Bridge Multicast Filtering**.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Bridge 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** (Entfernen) im Feld **IGMP Snooping Status**.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

IGMP-Snooping wird für das Gerät aktiviert.

### Aktivieren von Multicast-Weiterleitung und IGMP-Snooping mit den CLI -Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Aktivierung von Multicast-Weiterleitung und IGMP- Snooping, wie auf der Seite [Multicast Global Parameters](#) angezeigt, zusammen.

Tabelle 7-74. CLI -Befehle für Multicast-Weiterleitung und Snooping

CLI -Befehl	Beschreibung
<code>bridge multicast filtering</code>	Aktiviert die Filterung von Multicastadressen.
<code>ip igmp snooping</code>	Aktiviert das IGMP-(Internet Group Management Protocol)-Snooping.

Das folgende Beispiel illustriert die CLI-Befehle:

```

Console (config)# bridge
multicast filtering

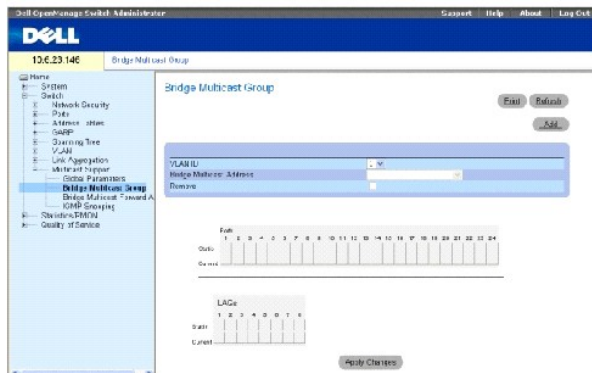
Console (config)# ip igmp
snooping
  
```

## Hinzufügen von Komponenten zu einer Bridge-Multicastadresse

Die Seite [Bridge Multicast Group](#) zeigt die Ports und LAGs an, die mit den Multicast-Dienstgruppen in den **Ports** und **LAGs**-Tabellen verknüpft sind. In den Port- und LAG-Tabellen wird auch angegeben, wie der Port oder die LAG der Multicast-Gruppe hinzugefügt wird. Ports können entweder vorhandenen Gruppen oder einer neuen Multicast-Dienstgruppe hinzugefügt werden. Auf der Seite [Bridge Multicast Group](#) können neue Multicast-Dienstgruppen erstellt werden. Auf der Seite [Bridge Multicast Group](#) werden einer spezifischen Multicast-Dienst-Adressgruppe darüber hinaus Ports zugewiesen.

Öffnen Sie die Seite **Bridge Multicast Group**, indem Sie auf **Switch**→ **Multicast Support**→ **Bridge Multicast Address** in der Strukturansicht klicken.

Abb. 7-111. Bridge-Multicastgruppe



**VLAN ID** Identifiziert ein VLAN und enthält Informationen über die Multicast-Gruppenadresse.

**Bridge Multicast Address** Identifiziert die MAC-Adresse/IP-Adresse der Multicast-Gruppe.

**Remove** Entfernt, wenn ausgewählt, eine Bridge-Multicastadresse.

**Ports** Listet den Port auf, der einem Multicast-Dienst hinzugefügt werden kann.

**LAGs** Listet die LAGs auf, die einem Multicast-Dienst hinzugefügt werden können.

Die folgende Tabelle enthält die Einstellungen für die Verwaltung von IGMP-Port und LAG-Komponenten:

Tabelle 7-75. Tabelle der Kontrolleinstellungen für IGMP-Port/LAG-Mitglieder

Port-Kontrolle	Definition
D	Gibt in der Zeile <i>Current</i> an, dass der Port/die LAG der Multicast-Gruppe dynamisch beigetreten ist.
S	Verknüpft den Port in der Zeile <i>Statics</i> statische Komponente mit der Multicast-Gruppe. Gibt in der Zeile <i>Current</i> an, dass der Port/die LAG der Multicast-Gruppe statisch beigetreten ist.
F	Forbidden.
Keine	Gibt an, dass der Port keiner Multicast-Gruppe angefügt ist.

## Hinzufügen von Bridge-Multicastadressen

1. Öffnen Sie die Seite [Bridge Multicast Group](#).
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite [Add Bridge Multicast Group](#) wird geöffnet:

Abb. 7-112. Hinzufügen einer Bridge-Multicastgruppe

3. Definieren Sie die Felder **VLAN ID** und **New Bridge Multicast Address**.
4. Stellen Sie einen Port auf **S** ein, um ihn zur ausgewählten Multicastgruppe hinzuzufügen.
5. Stellen Sie einen Port auf **F** ein, um das Hinzufügen spezifischer Multicastadressen zu einem spezifischen Port zu untersagen.
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Bridge-Multicastadresse wird der Multicastgruppe zugewiesen und das Gerät wird aktualisiert.

### Definieren von Ports für den Empfang eines Multicast-Dienstes:

1. Öffnen Sie die Seite [Bridge Multicast Group](#).
2. Definieren Sie die Felder **VLAN ID** und **Bridge Multicast Address**.
3. Stellen Sie einen Port auf **S** ein, um ihn zur ausgewählten Multicastgruppe hinzuzufügen.
4. Stellen Sie einen Port auf **F** ein, um das Hinzufügen spezifischer Multicastadressen zu einem spezifischen Port zu untersagen.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Port wird der Multicast-Gruppe zugewiesen und das Gerät wird aktualisiert.

### Definieren von LAGs für den Empfang eines Multicast-Dienstes:

1. Öffnen Sie die Seite [Bridge Multicast Group](#).
2. Definieren Sie die Felder **VLAN ID** und **Bridge Multicast Address**.
3. Stellen Sie eine LAG auf **S** ein, um sie zur ausgewählten Multicastgruppe hinzuzufügen.
4. Stellen Sie eine LAG auf **F** ein, um das Hinzufügen spezifischer Multicastadressen zu einer spezifischen LAG zu untersagen.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die LAG wird der Multicast-Gruppe zugewiesen und das Gerät wird aktualisiert.

### Verwalten von Multicast-Dienstkomponenten mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Verwaltung von Multicast-Dienstkomponenten, wie auf der Seite [Bridge Multicast Group](#) angezeigt, zusammen.

Tabelle 7-76. CLI-Befehle für Multicast-Dienstmitgliedschaft

---

CLI-Befehl	Beschreibung
<b>bridge multicast address</b> { <i>mac-multicast-address</i>   <i>ip-multicast-address</i> }	Registriert MAC-Layer-Multicastadressen in der Bridge-Tabelle und fügt der Gruppe statische Ports hinzu.
<b>bridge multicast forbidden address</b> { <i>mac-multicast-address</i>   <i>ip-multicast-address</i> } [ <b>add</b>   <b>remove</b> ] { <b>ethernet</b> <i>interface-list</i>   <b>port-channel</b> <i>port-channel-number-list</i> }	Verbietet das Hinzufügen einer spezifischen Multicastadresse zu spezifischen Ports. Verwenden Sie die no-Form dieses Befehls, um zur Standardeinstellung zurückzukehren.
<b>show bridge multicast address-table</b> [ <i>vlan</i> <i>vlan-id</i> ] [ <b>address</b> <i>mac-multicast-address</i>   <i>ip-multicast-address</i> ] [ <b>format</b> <b>ip</b>   <b>mac</b> ]	Zeigt Informationen der Multicast-MAC-Adresstabelle an.

Das folgende Beispiel illustriert die CLI-Befehle:

```

Console> enable

console# config

console(config)#vlan database

console(config-if)#vlan 8

Console(config-if)# exit

console(config)#interface range ethernet g1-9

console(config-if)# switchport mode general

console(config-if)# switchport general allow vlan add 8

Console(config)# interface vlan 8

Console(config-if)# exit

Console(config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1,g2

Console(config-if)# exit

Console(config)# exit

Console # show bridge multicast address-table

```

VLAN	MAC-Adresse	Typ	Ports
----	-----	----	-----
1	0100.5e02.0203	static	g1, g2

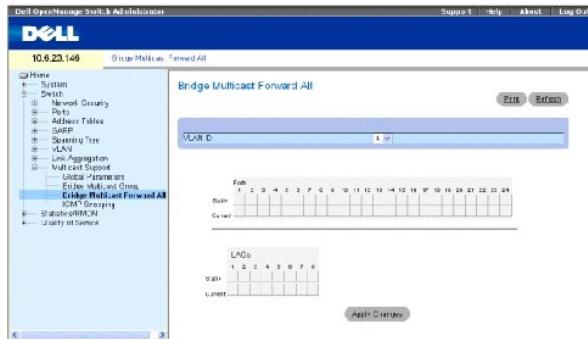
19	0100.5e02.0208	static	g1-8
19	0100.5e02.0208	Dynamisch	g9-11
Verbotene Ports für Multicast Adressen:			
VLAN	MAC-Adresse	Ports	
----	-----	-----	
1	0100.5e02.0203	g8	
19	0100.5e02.0208	g8	
Console # <code>show bridge multicast address-table format ip</code>			
VLAN	IP-Adresse	Typ	Ports
----	-----	----	-----
1	224-239.130 2.2.3	static	g1, g2
19	224-239.130 2.2.8	static	g1-8
19	224-239.130 2.2.8	Dynamisch	g9-11
Verbotene Ports für Multicast Adressen:			
VLAN	IP-Adresse	Ports	
----	-----	-----	
1	224-239.130 2.2.3	g8	
19	224-239.130 2.2.8	g8	

**Zuweisen von Parametern für die globale Multicast-Weiterleitung**

Die Seite [Bridge Multicast Forward All](#) enthält Felder zur Verknüpfung von Ports oder LAGs mit einem Gerät, das mit einem angrenzenden Multicast-Router/-Switch verbunden ist. Nachdem das IGMP-Snooping aktiviert wurde, werden die Multicast-Pakete an den entsprechenden Port bzw. das entsprechende VLAN weitergeleitet.

Öffnen Sie die Seite [Bridge Multicast Forward All](#), indem Sie auf **Switch** → **Multicast Support** → **Bridge Multicast** → [Bridge Multicast Forward All](#) in der Strukturansicht klicken.

**Abb. 7-113. Globale Bridge-Multicastweiterleitung**



**VLAN ID** Identifiziert ein VLAN.

**Ports** Listet Ports auf, die einem Multicast-Dienst hinzugefügt werden können.

**LAGs** Listet die LAGs auf, die einem Multicast-Dienst hinzugefügt werden können.

Die Seite [Bridge Multicast Forward All Router/Port Control Settings Table](#) enthält die Einstellungen zur Verwaltung von Router- und Porteeinstellungen.

**Tabelle 7-77. Tabelle der Einstellungen für globale Bridge-Multicastweiterleitung/Port-Kontrolle**

Port-Kontrolle	Definition
D	Fügt den Port dem Multicast-Router oder Schalter als dynamischen Port hinzu.
S	Fügt den Port dem Multicast-Router oder Schalter als statischen Port hinzu.
F	Verboten (Verboten).
Keine	Der Port ist keinem Multicast-Router oder Schalter angefügt.

### Anfügen eines Ports an einen Multicast-Router oder Schalter

1. Öffnen Sie die Seite [Bridge Multicast Forward All](#).
2. Definieren Sie das Feld **VLAN ID**.
3. Wählen Sie einen Port in der **Ports**-Tabelle und weisen Sie dem Port einen Wert zu.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Port wird dem Multicast-Router oder Schalter angefügt.

### Anfügen einer LAG an einen Multicast-Router oder Schalter

1. Öffnen Sie die Seite [Bridge Multicast Forward All](#).
2. Definieren Sie das Feld **VLAN ID**.
3. Wählen Sie eine LAG in der **LAGs**-Tabelle und weisen Sie der LAG einen Wert zu.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die LAG wird dem Multicast-Router oder Schalter angefügt.

## Verwaltung von an Multicast-Router angeschlossene LAGs und Ports mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Verwaltung von LAGs und Ports, die an Multicast-Router angeschlossen sind, wie auf der Seite [Bridge Multicast Forward All](#) angezeigt, zusammen.

Tabelle 7-78. CLI-Befehle zur Verwaltung von LAGs und Ports, die an Multicast- Router angeschlossen sind

CLI -Befehl	Beschreibung
<code>show bridge multicast filtering</code> <i>vlan-ld</i>	Zeigt die Multicast-Filterungskonfiguration an.
<code>no bridge multicast forbidden forward-all</code>	Deaktiviert die Weiterleitung von Multicast-Paketen für einen Port.
<code>bridge multicast forward-all</code> { <code>add</code>   <code>remove</code> } { <code>ethernet</code> <i>interface-list</i>   <code>port-channel</code> <i>port-channel-number-list</i> }	Aktiviert die Weiterleitung aller Multicast-Pakete für einen Port. Verwenden Sie die <code>no</code> -Form dieses Befehls, um zur Standardeinstellung zurückzukehren.

Das folgende Beispiel illustriert die CLI-Befehle:

```
console(config)#vlan database

console(config-if)#vlan 8

console(config-vlan)#exit

console(config)#interface range ethernet g1-9

console(config-if)# switchport mode general

console(config-if)# switchport general allow vlan add 8

Console(config-if)# exit

Console(config)# interface vlan 8

Console(config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1-9

Console(config-if)# exit

Console(config)# interface vlan 1

Console (config-if)# bridge multicast forward-all add ethernet g8
```



```

Console(config-if)# end

Console # show bridge multicast filtering 1

```

Filtering: Enabled (Aktiviert)		
VLAN:	Forward-All	
Port	static	Status
g1	Forbidden	Filter
g2	Vorwärts	Forward(s)
g3	-	Forward(d)

## IGMP-Snooping

Die Seite [IGMP Snooping](#) enthält Felder zum Hinzufügen von IGMP-Mitgliedern. Öffnen Sie die Seite [IGMP Snooping](#), indem Sie auf **Switch** → **Multicast Support** → **IGMP Snooping** in der Strukturansicht klicken.

Abb. 7-114. IGMP-Snooping



**VLAN ID** Gibt die VLAN ID an.

**IGMP Snooping Status** Aktiviert/deaktiviert IGMP-Snooping auf dem VLAN.

**Auto Learn** Aktiviert/deaktiviert Auto Learn auf dem Gerät.

**Host Timeout (1-2147483647)** Speicherdauer, bevor ein IGMP-Snooping-Eintrag gelöscht wird. Die Standardzeit ist 260 Sekunden.

**Multicast Router Timeout (1-2147483647)** Speicherdauer, bevor ein Multicast-Router-Eintrag gelöscht wird. Der Standardwert lautet 300 Sekunden.

**Leave Timeout (0-2147483647)** Speicherdauer (in Sekunden) nach Eingang einer Port-Leave-Meldung, bevor der Eintrag gelöscht wird. **User-defined** ermöglicht ein benutzerdefiniertes Zeitlimit und **Immediate Leave** gibt ein sofortiges Zeitlimit an. Das Standard-Zeitlimit ist 10 Sekunden.

### Aktivieren von IGMP-Snooping für das Gerät

1. Öffnen Sie die Seite [IGMP Snooping](#).
2. Wählen Sie die VLAN ID für das Gerät, auf dem IGMP-Snooping aktiviert werden soll.
3. Wählen Sie **Enable** (Aktivieren) im Feld **IGMP Snooping Status**.
4. Geben Sie die Informationen in die Felder auf der Seite ein.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

IGMP-Snooping wird auf dem Gerät aktiviert.

### Anzeigen der IGMP-Snooping-Tabelle

1. Öffnen Sie die Seite [IGMP Snooping](#).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die **IGMP Snooping Table** wird geöffnet.

### Konfigurieren von IGMP-Snooping mit den CLI-Befehlen

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Konfiguration von [IGMP Snooping](#) für das Gerät zusammen:

Tabelle 7-79. CLI-Befehle für IGMP-Snooping

CLI-Befehl	Beschreibung
<code>ip igmp snooping</code>	Aktiviert das IGMP (Internet Group Membership Protocol)-Snooping.
<code>ip igmp snooping mrouter learn-pim-dvmrp</code>	Aktiviert die automatische Erkennung von Multicast-Router-Ports innerhalb eines spezifischen VLAN-Kontexts.
<code>ip igmp snooping host-time-out time-out</code>	Konfiguriert das Host-Zeitlimit.
<code>ip igmp snooping mrouter-time-out time-out</code>	Konfiguriert das Multicast-Router-Zeitlimit.
<code>ip igmp snooping leave-time-out {time-out   immediate-leave}</code>	Konfiguriert das Leave-Zeitlimit.
<code>show ip igmp snooping groups [vlan vlan-id] [address ip-multicast-address]</code>	Zeigt die Multicast-Gruppen an, die über IGMP-Snooping erfasst (gelernt) wurden.
<code>show ip igmp snooping interface vlan-id</code>	Zeigt die IGMP-Snooping-Konfiguration an.
<code>show ip igmp snooping mrouter [interface vlan-id]</code>	Zeigt Informationen zu dynamisch erfassten Multicast-Router-Schnittstellen an.

Das folgende Beispiel illustriert die CLI-Befehle:

```
Console> enable

console# config

Console (config)# ip igmp snooping

Console(config)# interface vlan 1
```

```
Console (config-if)# ip igmp snooping mrouter learn-pim-dvmrp
```

```
Console (config-if)# ip igmp snooping host-time-out 300
```

```
Console (config-if)# ip igmp snooping mrouter-time-out 200
```

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

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

```
Console (config-if)# ip igmp snooping leave-time-out 60
```

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

```
Console(config)# exit
```

```
Console # show ip igmp snooping groups
```

```
Vlan IP Address Querier Ports
```

```
-----
```

```
1 224-239.130|2.2.3 Yes g1, g2
```

```
19 224-239.130|2.2.8 Yes g9-11
```

```
Console # show ip igmp snooping interface 1
```

```
IGMP Snooping is globally enabled
```

```
IGMP Snooping is enabled on VLAN 1
```

```
IGMP host timeout is 300 sec
```

```
IGMP Immediate leave is disabled. IGMP leave timeout is 60 sec
```

```
IGMP mrouter timeout is 200 sec
```

```
Automatic learning of multicast router ports is enabled
```

```
Console # show ip igmp snooping mrouter
```

VLAN	Ports
----	-----
1	g1

[Zurück zum Inhaltsverzeichnis](#)

## Konfigurieren von Systeminformationen:

Dell™ PowerConnect™ 5324 System-Benutzerhandbuch

- [Definieren allgemeiner Geräteinformationen](#)
- [Konfigurieren von SNMP-Einstellungen](#)
- [Verwalten von Protokollen](#)
- [Definieren von IP-Geräteadressen](#)
- [Ausführen von Kabeldiagnose](#)
- [Verwalten der Gerätesicherheit](#)
- [Definieren von SNMP-Parametern](#)
- [Verwalten von Dateien](#)
- [Definieren erweiterter Einstellungen](#)

Dieser Abschnitt enthält Informationen zur Definition von Systemparametern, einschließlich Sicherheitsfunktionen, zum Herunterladen von Gerätesoftware sowie zum Zurücksetzen des Gerätes. Um die System-Seite zu öffnen, klicken Sie auf „System“ in der Strukturansicht.

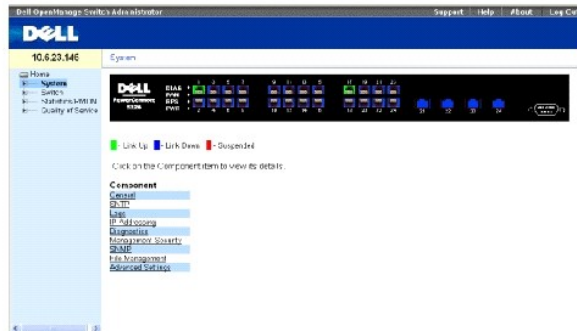


Abb. 6-15. System

## Definieren allgemeiner Geräteinformationen

Die Seite **General** (Allgemeines) enthält Links zu Seiten für die Konfiguration von Geräteparametern.

## Anzeigen der Seite „Asset“ (Bestand)

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. Öffnen Sie die Seite [Asset](#), indem Sie auf System → General → Asset in der Strukturansicht klicken.



Abb. 6-16. Asset

System Name (**0-160 Zeichen**) — Gibt den benutzerdefinierten Gerätenamen an.

System Contact (**0-160 Zeichen**) — Legt den Namen der Kontaktperson fest.

System Location (System-Standort) (**0-160 Zeichen**) — Gibt den Standort an, an dem das System derzeit betrieben wird.

MAC Address — Legt die MAC-Adresse des Geräts fest.

Sys Object ID — Gibt die maßgebende ID des Lieferanten des Netzwerk-Verwaltungssubsystems an, das in der Einheit enthalten ist.

Service Tag (Service-Kennnummer) — Gibt die Wartungsreferenznummer bei der Wartung des Geräts an.

Asset Tag (Systemkennnummer) (**0-16 Zeichen**) — Gibt die benutzerdefinierte Geräteferenz an.

Serial No. (Seriennummer) — Gibt die Seriennummer des Gerätes an.

Date (DD/MM/YY) (Datum) — 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) (Zeit) — 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 (Systembetriebszeit) — 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.

### Definieren von Systeminformationen:

1. Öffnen Sie die Seite [Asset](#) (Bestand).
2. Definieren Sie die entsprechenden Felder.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Systemparameter werden definiert und das Gerät aktualisiert.

### Starten einer Telnet-Sitzung:

1. Öffnen sie die Seite [Asset](#) (Bestand).
2. Klicken Sie auf **Telnet**.

Eine Telnet-Sitzung wird gestartet.

### Konfigurieren von Geräteinformationen mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Anzeige und Einstellung der Felder zusammengefasst, die auf der Seite [Asset](#) angezeigt werden.

**Tabelle 6-11. CLI-Befehle für Asset (Bestand)**

---

CLI-Befehl	Beschreibung
hostname name	Legt den Hostnamen des Gerätes fest oder ändert ihn.
snmp-server contact text	Richtet eine Kontaktperson für das System ein.
snmp-server location text	Fügt Informationen zum Gerätestandort ein.
<b>show clock [detail]</b>	Zeigt Systemuhrzeit und -datum an.
show system id	Zeigt die Service-Kennnummer an.
show system	Zeigt Systeminformationen an.
asset-tag	Stellt die Systemkennnummer des Gerätes ein.

Das folgende Beispiel illustriert 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 Dec 2004

Console> show clock

13:32:00 (UTC+0) Dec 7
2004

No time source

```

DELL Switch# <b>show system</b>		
System Description:		Ethernet Routing Switch
System Up Time (days, hour:min:sec):		0,00:04:17
System Contact:		spk
System Name:		DELL Switch
System Location:		R&D

System MAC Address:		00:10:b5:f4:00:01
Sys Object ID:		1.3.6.1.4.1.674.10895.3000
Type: PowerConnect 5324		
Netzteil	Status	
-----	-----	
Main	OK	
Redundant	OK	
FAN	Status	
-----	-----	
1	OK	
2	OK	
DELL Switch#		

## Definieren von Systemzeiteinstellungen

Die Seite [Time Synchronization](#) (Zeitsynchronisierung) enthält Felder zur Definition von Systemzeitparametern sowohl für die lokale Hardware-Uhr als auch die externe SNTP-Uhr. Wenn sich die Systemzeit nach einer externen SNTP-Uhr richtet und diese externe SNTP-Uhr ausfällt, kehrt die Systemzeit zur lokalen Hardware-Uhr zurück. Die Zeitumstellung auf Sommerzeit kann auf dem Gerät aktiviert werden. In der nachstehenden Liste sind die Start- und Enddaten der Sommerzeit in verschiedenen Ländern angegeben:

- 1 Ägypten — Letzter Freitag im April bis letzter Donnerstag im September.
- 1 Albanien — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Armenien — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Australien — Von Ende Oktober bis Ende März.
- 1 Australien - Tasmanien — Von Anfang Oktober bis Ende März.
- 1 Bahamas — Von April bis Oktober, zusammen mit der Sommerzeit in den USA.
- 1 Belarus — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Belgien — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Brasilien — Vom dritten Sonntag im Oktober bis zum dritten Samstag im März. Während der Sommerzeit werden die Uhren im Großteil des Südostens in Brasilien um eine Stunde vorgestellt.
- 1 Chile — Osterinsel 9. März bis 12. Oktober. Erster Sonntag im März oder nach dem 9. März.
- 1 China — In China gibt es keine Sommerzeit.
- 1 Dänemark — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Deutschland — Letztes Wochenende im März bis letztes Wochenende im Oktober.



- 1 Estland — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Finnland — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Frankreich — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Griechenland — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Großbritannien — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Indien — In Indien gibt es keine Sommerzeit.
- 1 Iran — Vom ersten Farvardin bis zum ersten Mehr.
- 1 Iraq — Vom ersten April bis zum ersten Oktober.
- 1 Irland — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Israel — Jedes Jahr verschieden.
- 1 Italien — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Japan — In Japan gibt es keine Sommerzeit.
- 1 Jordanien — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Kanada — Vom ersten Sonntag im April bis zum letzten Sonntag im Oktober. Die Sommerzeit wird in der Regel von den Regierungen der Provinzen und Hoheitsgebiete festgelegt. In manchen Gemeinden können Ausnahmeregelungen bestehen.
- 1 Kuba — Vom letzten Sonntag im März bis zum letzten Sonntag im Oktober.
- 1 Lettland — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Libanon — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Litauen — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Luxemburg — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Mazedonien — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Mexiko — Vom ersten Sonntag im April um 2.00 Uhr bis zum letzten Sonntag im Oktober um 2.00 Uhr.
- 1 Moldawien — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Montenegro — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Neuseeland — Vom letzten Sonntag im Oktober bis zum letzten Sonntag am oder nach dem 15. März.
- 1 Niederlande — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Norwegen — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Österreich — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Paraguay — Vom 6. April bis zum 7. September.
- 1 Polen — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Portugal — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Rumänien — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Russland — Vom 29. März bis 25. Oktober.
- 1 Schweden — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Schweiz — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Serbien — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Slowakien — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Spanien — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Südafrika — In Südafrika gibt es keine Sommerzeit.
- 1 Syrien — Vom 31. März bis 30. Oktober.
- 1 Taiwan — In Taiwan gibt es keine Sommerzeit.
- 1 Türkei — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 Ungarn — Letztes Wochenende im März bis letztes Wochenende im Oktober.
- 1 USA — Vom ersten Sonntag im April um 2.00 Uhr bis zum letzten Sonntag im Oktober um 2.00 Uhr.
- 1 Zypern — Letztes Wochenende im März bis letztes Wochenende im Oktober.

Weitere Informationen zu SNTP finden Sie unter [Konfigurieren der SNTP-Einstellungen](#).

Öffnen Sie die Seite [Time Synchronization](#) (Zeitsynchronisierung), indem Sie auf **System** → **General** → **Time Synchronization** in der *Strukturansicht* klicken.

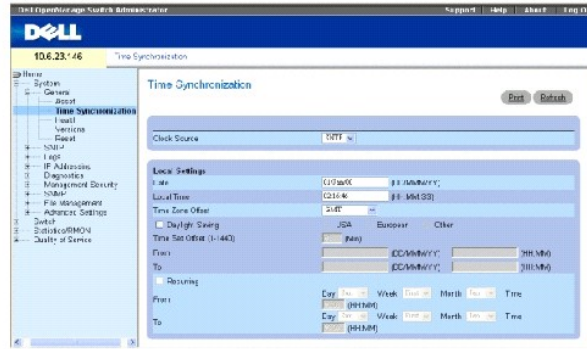


Abb. 6-17. Zeitsynchronisierung

## Zeitquelle

Clock Source (Zeitquelle) — Die der Systemzeit zugrundeliegende Zeitquelle. Folgende Feldwerte können ausgewählt werden:

**SNTP** — Gibt an, dass die Systemzeit über einen SNTP-Server eingestellt wird. Weitere Informationen finden Sie unter [Konfigurieren der SNTP-Einstellungen](#).

**None** (Keine) — Gibt an, dass die Systemzeit nicht nach einer externen Zeitquelle eingestellt wird.

## Lokale Einstellungen

**Date** (Datum) — Legt das Systemdatum fest. Das Feldformat ist: Tag:Monat:Jahr, beispielsweise 04 Mai 2010.

**Local Time** (Ortszeit) — Legt die Systemuhrzeit fest. Das Feldformat ist HH:MM:SS, beispielsweise, 21:15:03.

**Time Zone Offset** (Zeitzonendifferenz) — Die Differenz zwischen Greenwich Mean Time (GMT) und Ortszeit. Zum Beispiel ist die Zeitdifferenz zwischen Zonenzeit und Greenwich-Zeit für Paris GMT +1, während die lokale Zeit in New York GMT -5 ist.

Es gibt zwei Arten der Sommerzeiteinstellung: bestimmtes Datum in einem bestimmten Jahr oder eine periodisch wiederkehrende Einstellung unabhängig vom Jahr. Wenn Sie eine bestimmte Einstellung für ein bestimmtes Jahr vornehmen wollen, füllen Sie den Bereich **Daylight Savings** (Sommerzeit) aus. Für eine periodische Einstellung füllen Sie den Bereich **Recurring** (Wiederkehrend) aus.

**Daylight Savings** (Sommerzeit) — Aktiviert die Sommerzeit (DST) im Gerät aufgrund des Gerätestandorts. Folgende Feldwerte können ausgewählt werden:

**USA** — Das Gerät wird um 2 Uhr am ersten Sonntag im April auf Sommerzeit umgestellt und kehrt am letzten Sonntag im Oktober um 2 Uhr wieder zur Standardzeit zurück.

**European** (Europäisch) — Das Gerät schaltet am letzten Sonntag im März um 1 Uhr auf Sommerzeit um und kehrt am letzten Sonntag im Oktober um 1 Uhr wieder zur Standardzeit zurück. Die europäische Option gilt für EU-Mitglieder und andere europäische Länder, die den EU-Standard verwenden.

**Other** (Andere) — Die Sommerzeitangaben sind benutzerdefiniert aufgrund des Gerätestandorts. Bei Auswahl von „Other“ müssen die Felder **From** (Von) und **To** (Bis) definiert werden.

**From** (Von) — Legt den Zeitpunkt fest, an dem die Sommerzeit in Ländern außerhalb der USA und Europa beginnt. Das Format ist TagMonatJahr in einem Feld und Uhrzeit im anderen. Wenn zum Beispiel die Sommerzeit am 25. Oktober 2007 um 5 Uhr beginnt, lauten die beiden Felder 25Oct07 und 5:00. Die möglichen Feldwerte sind:

**Date** (Datum) — Das Datum, an dem die Sommerzeit beginnt. Es sind Werte im Feldbereich von 1-31 möglich.

**Month** (Monat) — Der Monat, in dem die Sommerzeit beginnt. Es sind Werte im Feldbereich von Jan bis Dez möglich.

**Year** (Jahr) — Das Jahr, in dem die konfigurierte Sommerzeit beginnt.

**Time** (Zeit) — Die Uhrzeit, an der die Sommerzeit beginnt. Das Feldformat ist HH:MM, beispielsweise 05:30.

**To (Bis)** — Legt den Zeitpunkt fest, an dem die Sommerzeit in Ländern außerhalb der USA und Europa endet. Das Format ist TagMonatJahr in einem Feld und Uhrzeit im anderen. Wenn zum Beispiel die Sommerzeit am 23. März 2008 um 12 Uhr endet, lauten die beiden Felder 23Mar07 und 12:00. Die möglichen Feldwerte sind:

**Date** (Datum) — Das Datum, an dem die Sommerzeit endet. Es sind Werte im Feldbereich von 1-31 möglich.

**Month** (Monat) — Der Monat, in dem die Sommerzeit endet. Es sind Werte im Feldbereich von Jan bis Dez möglich.

**Year** (Jahr) — Das Jahr, in dem die konfigurierte Sommerzeit endet.

**Time** (Zeit) — Die Uhrzeit, an der die Sommerzeit beginnt. Das Feldformat ist HH:MM, beispielsweise 05:30.

**Recurring** (Wiederkehrend) — Legt die Uhrzeit fest, an der die Sommerzeit in Ländern außerhalb der USA und Europa beginnt, wo die Sommerzeit jedes Jahr gleich ist. Folgende Feldwerte können ausgewählt werden:

**From** (Von) — Legt die Uhrzeit fest, an der die Sommerzeit jedes Jahr beginnt. Beispiel: Die örtliche Sommerzeit beginnt an jedem zweiten Sonntag im April um 5.00 Uhr. Folgende Feldwerte können ausgewählt werden:

**Day** (Tag) — Der Wochentag, an dem die Sommerzeit jedes Jahr beginnt. Feldwerte im Bereich von Sonntag - Samstag sind möglich.

**Week** (Woche) — Die Woche innerhalb eines Monats, in der die Sommerzeit jedes Jahr beginnt. Es sind Werte im Feldbereich von 1-5 möglich.

**Month** (Monat) — Der Monat, in dem die Sommerzeit jedes Jahr beginnt. Es sind Werte im Feldbereich von Jan bis Dez möglich.

**Time** (Zeit) — Die Uhrzeit, an der die Sommerzeit jedes Jahr beginnt. Das Feldformat ist HH:MM, beispielsweise 02:10.

**To** (Bis) — Legt die periodisch wiederkehrende Uhrzeit fest, an der die Sommerzeit jedes Jahr endet. Beispiel: Die örtliche Sommerzeit endet an jedem vierten Freitag im Oktober um 5.00 Uhr. Folgende Feldwerte können ausgewählt werden:

**Day** (Tag) — Der Wochentag, an dem die Sommerzeit jedes Jahr endet. Feldwerte im Bereich von Sonntag - Samstag sind möglich.

**Week** (Woche) — Die Woche innerhalb eines Monats, in der die Sommerzeit jedes Jahr endet. Es sind Werte im Feldbereich von 1-5 möglich.

**Month** (Monat) — Der Monat, in dem die Sommerzeit jedes Jahr endet. Es sind Werte im Feldbereich von Jan bis Dez möglich.

**Time** (Zeit) — Die Uhrzeit, an der die Sommerzeit jedes Jahr endet. Das Feldformat ist HH:MM, beispielsweise 05:30.

## Auswählen einer Zeitquelle

1. Öffnen Sie die Seite [Time Synchronization](#) (Zeitsynchronisierung). >
2. Definieren Sie das Feld **Clock Source** (Zeitquelle).
3. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen).

Die ausgewählte Zeitquelle wird ausgewählt und das Gerät wird aktualisiert.

### Festlegen von Ortszeiteinstellungen

1. Öffnen Sie die Seite [Time Synchronization](#) (Zeitsynchronisierung).
2. Legen Sie die Felder **Recurring** (Wiederkehrend) fest.
3. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen).

Die Ortszeiteinstellungen werden übernommen.

### Definieren der externen SNTP-Uhr-Einstellungen

1. Öffnen Sie die Seite [Time Synchronization](#) (Zeitsynchronisierung).
2. Legen Sie die Felder fest.
3. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen).

Die externen Zeiteinstellungen werden übernommen.

### Definieren der Zeiteinstellungen mit den CLI-Befehlen

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

**Tabelle 6- 12. CLI - Befehle für Zeiteinstellung**

CLI	Beschreibung
<code>clock source {sntp}</code>	Konfiguriert eine externe Zeitquelle für die Systemuhr.
<code>clock timezone hours-offset [minutes minutes-offset][zone acronym]</code>	Stellt die Zeitzone für Anzeigezwecke ein.
<code>clock summer-time</code>	Konfiguriert das System automatisch für Umstellung auf Sommerzeit (Daylight Savings Time).
<code>clock summer-time recurring {usa   eu} { week day month hh:mm week day month hh:mm} [offset offset] [zone acronym]</code>	Konfiguriert das System automatisch für Umstellung auf Sommerzeit (gemäß US- und europäischen Standards.)
<code>clock summer-time date date month year hh:mm date month year hh:mm [offset offset] [zone acronym]</code>	Konfiguriert das System automatisch für Umstellung auf Sommerzeit (Daylight Savings Time) für einen bestimmten Zeitraum - Format: Tag/Monat/Jahr.

Das folgende Beispiel illustriert die CLI-Befehle:

```

Console(config)# clock
timezone -6 zone CST

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

```


### Anzeigen von Informationen zum Systemzustand


Die Seite [System Health](#) (Systemzustand) enthält Informationen zu physischer Gerätehardware. Öffnen Sie die Seite [System Health](#) (Systemzustand), indem Sie auf System→ General→ Health in der Strukturansicht klicken.

**Abb. 6-18. Systemzustand (System Health)**




**Power Supply Status** – Zustand der Hauptstromversorgung. Folgende Feldwerte können ausgewählt werden:


 – Gibt an, dass die Hauptstromversorgung der angegebenen Einheit ordnungsgemäß funktioniert.

 – Gibt an, dass die Hauptstromversorgung der angegebenen Einheit nicht ordnungsgemäß funktioniert.

Not Present (Nicht vorhanden) – Gibt an, dass die Stromversorgung für das angegebene Gerät nicht vorhanden ist.

**Fan (Lüfter)** – Der Status des Lüfters des Geräts. Folgende Feldwerte können ausgewählt werden:

 – Gibt an, dass die Lüfter der angegebenen Einheit ordnungsgemäß funktionieren.

 – Gibt an, dass die Lüfter der angegebenen Einheit nicht ordnungsgemäß funktionieren.

Not Present (Nicht vorhanden) – Gibt an, dass die Lüfter für das angegebene Gerät nicht vorhanden sind.

## Anzeigen von Informationen zum Systemzustand mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Anzeige der Felder zusammengefasst, die auf der Seite [System Health](#) (Systemzustand) angezeigt werden.

**Tabelle 6-13. CLI-Befehle für Systemzustand**

CLI-Befehl	Beschreibung
show system	Zeigt Systeminformationen an.

DELL Switch# <b>show system</b>		
System Description:		Ethernet Routing Switch
System Up Time (days, hour:min:sec):		0,00:04:17
System Contact:		spk

System Name:		DELL Switch
System Location:		R&D
System MAC Address:		00:10:b5:f4:00:01
Sys Object ID:		1.3.6.1.4.1.674.10895.3000
Type: PowerConnect 5324		
Power Supply	Status	
-----	-----	
Main	OK	
Redundant	OK	
FAN	Status	
-----	-----	
1	OK	
2	OK	
DELL Switch#		

## Anzeigen der Seite „Versions“ (Versionen)

Die Seite [Versions](#) (Versionen) enthält Informationen zu den Versionen der derzeit ausgeführten Hardware und Software. Öffnen Sie die Seite [Versions](#), indem Sie auf System→ General→ Versions in der Strukturansicht klicken.

Abb. 6-19. Versionen



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

Boot Version — Die auf dem Gerät derzeit ausgeführte Startversion.

Hardware Version — Die Version der derzeit auf dem Gerät betriebenen Hardware.

## Anzeigen von Geräteversionen mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Anzeige der Felder zusammengefasst, die auf der Seite [Versions](#) (Versionen) angezeigt werden.

Tabelle 6-14. CLI-Befehle für die Versionsanzeige

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

Das folgende Beispiel illustriert die CLI-Befehle:

```

Console> show version

SW version x.xxx (date 23-Jul-xxxx time 17:34:19)

Boot version x.xxx (date 17-Jan-xxxx time 11:48:21)

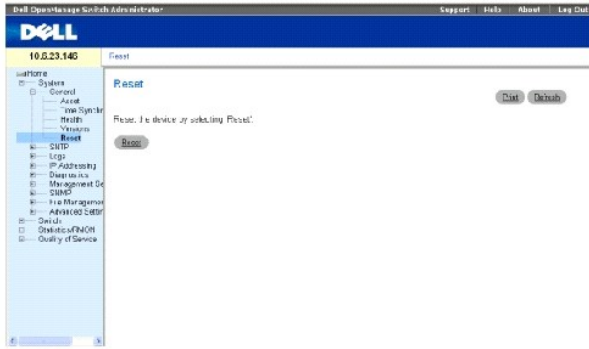
HW version x.x.x

```

## Zurücksetzen des Gerätes

Auf der Seite [Reset](#) (Zurücksetzen) können Benutzer das Gerät von einem Remote-Standort aus zurücksetzen. Öffnen Sie die Seite [Reset](#) (Zurücksetzen), indem Sie auf System→ General→ Reset in der Strukturansicht klicken.

Abb. 6-20. Zurücksetzen



**ANMERKUNG:** Speichern Sie vor dem Zurücksetzen des Gerätes sämtliche Änderungen an der Running-Configuration-Datei (Datei mit laufender Einstellung). Damit wird verhindert, dass die aktuelle Gerätekonfiguration verlorengeht. Weitere Informationen zum Speichern von Konfigurationsdateien finden Sie unter [„Verwalten von Dateien“](#).

### Zurücksetzen des Gerätes

1. Öffnen Sie die Seite [Reset](#) (Zurücksetzen).
2. Klicken Sie auf „Reset“.

Eine Bestätigungsmeldung wird angezeigt.

3. Klicken Sie auf „OK“.

Das Gerät wird zurückgesetzt. Nachdem das Gerät zurückgesetzt wurde, wird der Benutzer aufgefordert, Benutzernamen und Kennwort anzugeben.

4. Geben Sie einen Benutzernamen und Kennwort ein, um die Verbindung mit der Web-Schnittstelle wiederherzustellen.

### Zurücksetzen des Gerätes mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Zurücksetzung des Geräts mit CLI zusammengefasst:

Tabelle 6-15. CLI-Befehl zum Zurücksetzen

CLI-Befehl	Beschreibung
reload	Lädt das Betriebssystem neu.

Das folgende Beispiel illustriert 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] ?

```

### Konfigurieren von SNTP-Einstellungen

Das Gerät unterstützt das Simple Network Time Protocol (SNTP). SNTP stellt die genaue Netzwerkschalter-Zeitsynchronisierung bis auf die Millisekunde sicher.



Die zeitliche Synchronisierung wird von einem Netzwerk-SNTP-Server ausgeführt. Der Gerät wird nur als SNTP-Client betrieben. Es kann keine Zeitdienste für andere Systeme liefern.

Das Gerät kann die Serverzeit von den folgenden Servertypen abfragen:

- 1 Unicast
- 1 Anycast
- 1 Broadcast

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

Nachstehend ein Beispiel für Strata:

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

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

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

- 1 **T1** — Zeit, an der die ursprüngliche Anfrage vom Client gesendet wurde.
- 1 **T2** — Zeit, an der die ursprüngliche Anfrage vom Client erhalten wurde.
- 1 **T3** — Zeit, an der der Server dem Client eine Antwort geschickt hat.
- 1 **T4** — Zeit, an der der Client die Antwort des Servers erhalten hat.

## Abfrage von Unicast-Zeitinformationen

Die Abfrage von Unicast-Informationen wird zur Abfrage bei einem Server verwendet, dessen IP-Adresse bekannt ist. T1 - T4 werden zur Ermittlung der Serverzeit verwendet. Das ist die bevorzugte Methode zur Synchronisierung der Schalterzeit.

## Abfrage von Anycast-Zeitinformationen

Die Abfrage von Anycast-Informationen wird verwendet, wenn die IP-Adresse des Servers nicht bekannt ist. Der erste Anycast-Server, der eine Antwort liefert, wird zur Einstellung des Zeitwertes verwendet. Die Zeitlevels T3 and T4 werden zur Ermittlung der Serverzeit verwendet. Anycast-Zeitinformationen zur Synchronisierung der Schalterzeit werden Broadcast-Zeitinformationen vorgezogen.

## Broadcast-Zeitinformationen

Broadcast-Informationen werden verwendet, wenn die IP-Adresse des Servers nicht bekannt ist. Wenn von einem SNTP-Server eine Broadcast-Meldung ausgesandt wird, wartet der SNTP-Client auf eine Antwort. Der SNTP-Client sendet keine Anfragen zu Zeitinformationen aus und empfängt keine Antworten vom Broadcast-Server.

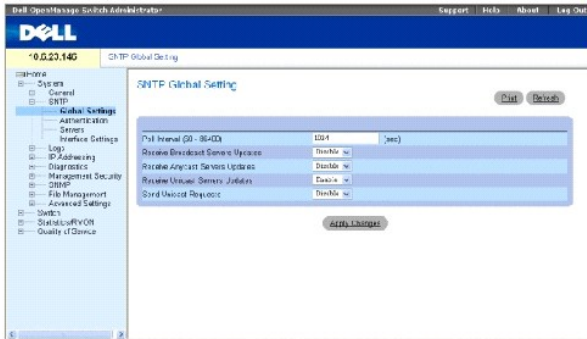
MD5 (Message Digest 5)-Authentifizierung schützt die Schalter-Synchronisierungspfade zu den SNTP-Servern. MD5 ist ein Algorithmus, der einen 128-Bit-Hash produziert. MD5 ist eine Variante von MD4 und bietet höhere Sicherheit als MD4. MD5 verifiziert die Integrität der Kommunikation und authentifiziert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

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

## Definieren globaler SNTP-Parameter

Die Seite **SNTP Global Settings** (Globale SNTP-Einstellungen) enthält Informationen zur globalen Definition von SNTP-Parametern. Öffnen Sie die Seite **SNTP Global Settings**, indem Sie auf **System** → **SNTP** → **SNTP Global Settings** in der Strukturansicht klicken.

Abb. 6-21. Globale SNTP-Einstellungen



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

**Receive Broadcast Servers Updates** (Aktualisierungen von Broadcast-Servern erhalten) — Fragt Broadcast-Server-Zeitinformationen an den ausgewählten Schnittstellen von den SNTP-Servern ab.

**Receive Anycast Servers Updates** (Aktualisierungen von Anycast-Servern erhalten) — Fragt, wenn aktiviert, Anycast-Server-Zeitinformationen vom SNTP-Server ab. Wenn sowohl das Feld **Receive Anycast Servers Update** als auch das Feld **Receive Broadcast Servers Update** aktiviert ist, wird die Systemzeit nach der Anycast-Server-Zeitinformation eingestellt.

**Receive Unicast Servers Updates** (Aktualisierungen von Unicast-Servern erhalten) — Fragt, wenn aktiviert, Unicast-Server-Zeitinformationen vom SNTP-Server ab. Wenn die Felder **Receive Broadcast Servers Updates**, **Receive Anycast Servers Updates** und **Receive Unicast Servers Updates** aktiviert sind, wird die Serverzeit nach den Unicast-Server-Zeitinformationen eingestellt.

**Poll Unicast Servers** (Unicast-Servern abfragen) — Sendet, wenn aktiviert, SNTP-Unicast-Weiterleitungsinformationen an den SNTP-Server.

## Definieren globaler SNTP-Parameter mit den CLI-Befehlen

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

Tabelle 6-16. CLI-Befehle für globale SNTP-Parameter

CLI-Befehl	Beschreibung
<code>sntp broadcast client enable</code>	Aktiviert SNTP-Broadcast-Clients
<code>sntp unicast client enable</code>	Aktiviert vordefinierte SNTP-Unicast-Clients

Das folgende Beispiel illustriert die CLI-Befehle:

```

console> enable

Console# configure

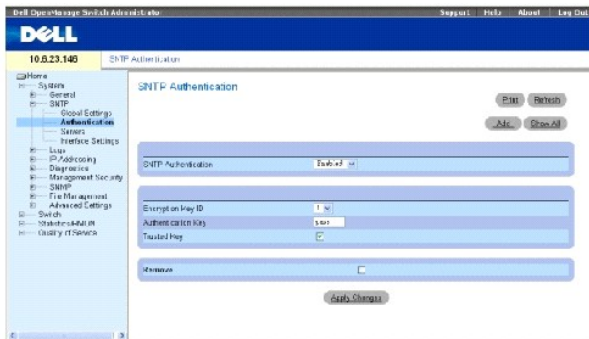
console(config)# sntp
    
```

anycast client enable

## Definieren von SNMP-Authentifizierungsmethoden

Die Seite **SNMP Authentication** (SNMP-Authentifizierung) ermöglicht die SNMP-Authentifizierung zwischen dem Gerät und einem SNMP-Server. Die Methode zur Authentifizierung des SNMP-Servers wird ebenfalls auf der Seite **SNMP Authentication** ausgewählt. Klicken Sie auf **System** → **SNMP** → **Authentication** in der Struktursicht, um die Seite **SNMP Authentication** zu öffnen.

Abb. 6-22. SNMP-Authentifizierung



SNMP Authentication (SNMP-Authentifizierung) — Ermöglicht, wenn aktiviert, die Authentifizierung einer SNMP-Session zwischen dem Gerät und einem SNMP-Server.

Encryption Key ID (Verschlüsselungs-ID) — Legt die Schlüssel-ID, die zur Authentifizierung des SNMP-Servers und des Geräts verwendet wird, fest. Der Feldwert kann bis zu 4294967295 Zeichen umfassen.

Authentication Key (Authentifizierungsschlüssel) (1-8 Zeichen) — Gibt den zur Authentifizierung verwendeten Schlüssel an.

Trusted Key (Zuverlässiger Schlüssel) — Gibt den zur Authentifizierung des SNMP-Servers verwendeten Verschlüsselungscode an.

Remove (Entfernen) — Entfernt, wenn markiert, den ausgewählten Schlüssel.

## Hinzufügen eines SNMP-Authentifizierungsschlüssels

1. Öffnen Sie die Seite [SNMP Authentication](#) (SNMP-Authentifizierung).
2. Klicken Sie auf „Add“ (Hinzufügen).

Die Seite [Add Authentication Key](#) (Authentifizierungsschlüssel hinzufügen) wird geöffnet:

Abb. 6-23. Hinzufügen eines Authentifizierungsschlüssels



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

Der SNMP-Authentifizierungsschlüssel wird hinzugefügt und das Gerät aktualisiert.

## Anzeigen der Authentifizierungsschlüssel-Tabelle

1. Öffnen Sie die Seite [SNTP Authentication](#) (SNTP-Authentifizierung).
2. Klicken Sie auf „Show All“ (Alles anzeigen).

Die Seite [Authentication Key Table](#) (Authentifizierungsschlüssel-Tabelle) wird geöffnet:

Abb. 6-24. Authentifizierungsschlüssel-Tabelle

Encryption Key ID	Authentication Key	Trusted Key	Remove
1	snmp	<input checked="" type="checkbox"/>	<input type="checkbox"/>

## Löschen des Authentifizierungsschlüssels

1. Öffnen Sie die Seite [SNTP Authentication](#) (SNTP-Authentifizierung).
2. Klicken Sie auf „Show All“ (Alles anzeigen).

Die Seite [Authentication Key Table](#) (Authentifizierungsschlüssel-Tabelle) wird geöffnet.

3. Wählen Sie einen Eintrag in der **Authentication Key Table**.
4. Wählen Sie das Kontrollkästchen „Remove“ (Entfernen).
5. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen).

Der Eintrag wird entfernt und das Gerät wird aktualisiert.

## Definieren der SNMP-Authentifizierungseinstellungen mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [SNTP Authentication](#) angezeigt werden.

Tabelle 6-17. CLI-Befehle für SNMP-Authentifizierung

CLI-Befehl	Beschreibung
<code>snmp authenticate</code>	Legt die Authentifizierung für von Servern empfangenen Netzwerk-Zeitprotokollverkehr fest.
<code>snmp authentication-key number md5 value</code>	Legt einen Authentifizierungsschlüssel für SNMP fest.

Das folgende Beispiel illustriert die CLI-Befehle:

```
console> enable

Console# configure

Console(config)# snmp
authentication-key 8 md5
ClkKey

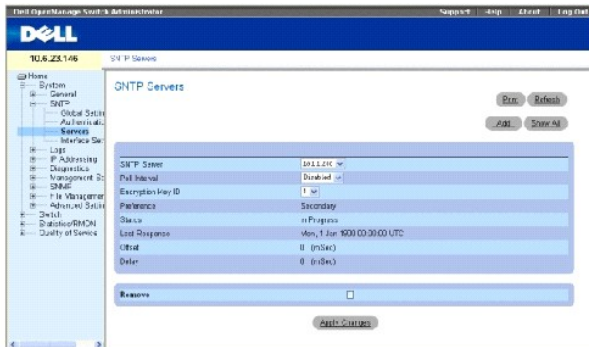
Console(config)# snmp
trusted-key 8
```

```
Console(config)# snmp
authenticate
```

## Definieren von SNMP-Servern

Die Seite [SNTP Servers](#) enthält Informationen zur Aktivierung von SNMP-Servern sowie zum Hinzufügen von neuen SNMP-Servern. Außerdem kann auf der Seite [SNTP Servers](#) die Fähigkeit des Geräts, SNMP-Verkehr von einem Server anzufordern und zu empfangen, eingestellt werden. *Öffnen Sie die Seite [SNTP Servers](#), indem Sie auf System → SNMP → SNTP Servers in der Strukturansicht klicken.*

Abb. 6-25. SNTP-Server



**SNTP Server** — Zur Eingabe einer benutzerdefinierten IP-Adresse oder Hostnamens eines SNMP-Servers. Bis zu acht SNMP-Server können definiert werden. Dieses Feld kann 1 - 158 Zeichen umfassen.

**Poll Interval (Abfragungsintervall)** — Ermöglicht, wenn aktiviert, die Abfrage von Systemzeitinformationen vom ausgewählten SNMP-Server.

**Encryption Key ID (Verschlüsselungs-ID)** — Legt die Schlüssel-ID, die zur Kommunikation zwischen dem SNMP-Server und dem Gerät verwendet wird, fest. Der Wert liegt im Bereich von 1 - 4294967295.

**Preference (Vorrang)** — Gibt den SNMP-Server an, der die SNMP-Systemzeitinformation bereitstellt. Folgende Feldwerte können ausgewählt werden:

**Primary (Primär)** — Der primäre Server liefert SNMP-Informationen.

**Secondary (Sekundär)** — Der Backup-Server liefert SNMP-Informationen.

**Status Up (Zustand: In Betrieb)** — Gibt den Betriebsstatus des SNMP-Servers an. Die möglichen Feldwerte sind:

**Up (In Betrieb)** — Der SNMP-Server funktioniert gegenwärtig normal.

**Down (Außer Betrieb)** — Der SNMP-Server funktioniert gegenwärtig nicht normal.

**Unknown (Unbekannt)** — Der Status des SNMP-Servers ist gegenwärtig nicht bekannt.

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

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

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

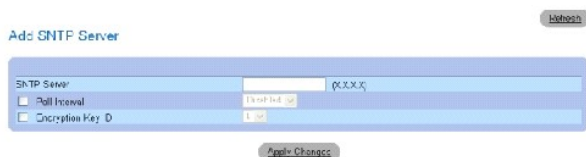
Remove (Entfernen) — Entfernt, wenn ausgewählt, einen bestimmten SNTP-Server von der **SNTP Server** -Liste.

### Hinzufügen eines SNTP-Servers

1. Öffnen Sie die Seite [SNTP Servers](#).
2. Klicken Sie auf „Add“ (Hinzufügen).

Die Seite [Add SNTP Server](#) (SNTP-Server hinzufügen) wird geöffnet:

**Abb. 6-26. Hinzufügen eines SNTP-Servers**



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

Der SNTP-Server wird hinzugefügt und das Gerät aktualisiert.

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite **Add SNTP Server** (SNTP-Server hinzufügen) angezeigt werden.

**Tabelle 6-18.**

CLI-Befehl	Beschreibung
<code>sntp server ip-address hostname [poll] [key keyid]</code>	Konfiguriert das Gerät zur Verwendung von SNTP, um NTP-Verkehr von einem Server anzufordern und anzunehmen.

CLI-Befehle für SNTP-Server

Das folgende Beispiel illustriert die CLI-Befehle:

```
console> enable

Console# configure

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

Anzeigen der SNTP-Server-Tabelle

1. Öffnen Sie die Seite [SNTP Servers](#).
2. Klicken Sie auf „Show All“ (Alles anzeigen).

Die Seite [SNTP Servers Table](#) (SNTP-Server-Tabelle) wird geöffnet:

**Abb. 6-27. SNTP-Server-Tabelle**

SNTP Servers Table [Edit]

SNTP Server	Poll interval	Encryption Key ID	Preference	Status	Last Response	Offset	Delay	Reserved
1	15.1..220	Disabled	Secondary	In Progress	Mon, 1 Jun '30 09:30:00 UTC	0	0	<input type="checkbox"/>

[Apply Changes]

## Ändern eines SNTP-Servers

1. Öffnen Sie die Seite [SNTP Servers](#).
2. Klicken Sie auf „Show All“ (Alles anzeigen).

Die Seite [SNTP Servers Table](#) (SNTP-Servers-Tabelle) wird geöffnet.

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

Die SNTP-Serverinformationen werden aktualisiert.

## Löschen des SNTP-Servers

1. Öffnen Sie die Seite [SNTP Servers](#).
2. Klicken Sie auf „Show All“ (Alles anzeigen).

Die Seite [SNTP Servers Table](#) (SNTP-Servers-Tabelle) wird geöffnet.

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

Der Eintrag wird entfernt und das Gerät wird aktualisiert.

## Definieren der SNTP-Servereinstellungen mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [SNTP Servers](#) angezeigt werden.

Tabelle 6-19. CLI-Befehle für SNTP-Server

CLI-Befehl	Beschreibung
<code>sntp server ip-address hostname [poll] [key keyid]</code>	Konfiguriert das Gerät zur Verwendung von SNTP, um NTP-Verkehr von einem Server anzufordern und anzunehmen.

Das folgende Beispiel illustriert die CLI-Befehle:

```

console> enable

Console# configure

Console(config)# sntp server 100.1.1.1 poll key 10

```

```

Console# show sntp status

```

Clock is synchronized, stratum 4, reference is 176.1.1.8					
Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 1993)					
Unicast servers:					
Server	Preference	Status	Last response	Offset [mSec]	Delay [mSec]
-----	-----	-----	-----	-----	-----
176.1.1.8	Primary	Up	AFE252C1.6DBDDFF2	7.33	117.79
176.1.8.179	Secondary	Unknown	AFE21789.643287C9	8.98	189.19
Anycast server:					
Server	Preference	Status	Last response	Offset [mSec]	Delay [mSec]
-----	-----	-----	-----	-----	-----
VLAN 119	Secondary	Up	19:53:21.789 PDT Feb 19 2002	7.19	119.89
Broadcast:					
Interface	IP address:	Last response			
-----	-----	-----			
176.1.1.8	Primary	AFE252C1.6DBDDFF2			
176.1.8.179	Secondary	AFE21789.643287C9			

## Definieren von SNTP-Schnittstellen

Die **SNTP Broadcast Interface Table** (SNTP-Broadcast-Schnittstellentabelle) enthält Felder zur Einstellung von SNTP auf verschiedenen Schnittstellen. Öffnen Sie die Seite **SNTP Broadcast Interface Table** (SNTP-Broadcast-Schnittstellentabelle), indem Sie auf System→ **SNTP**→ Interfaces Settings klicken.





Authentication is required for synchronization.		
Trusted Keys: 8,9		
Unicast Clients Polling: Enabled.		
Server	Polling	Encryption Key
-----	-----	-----
176.1.1.8	Enabled (Aktiviert)	9
176.1.8.179	Disabled	Disabled
Broadcast Clients: Enabled		
Broadcast Clients Poll: Enabled		
Broadcast Interfaces: g1, g3		

## Verwalten von Protokollen

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

Die Seite **Logs** enthält Links zu verschiedenen Protokollseiten.

## Definieren der globalen Protokollparameter

Mithilfe des Systemprotokolls können Sie Geräteereignisse in Echtzeit anzeigen lassen und diese Ereignisse zur späteren Verwendung aufzeichnen. Das Systemprotokoll bietet die Möglichkeit, Ereignisse zu protokollieren und zu verwalten sowie Fehlerberichte oder Informationsmeldungen zu erstellen.

Ereignismeldungen verfügen gemäß SYSLOG RFC-Empfehlung für die gesamte Fehlerberichterstellung über ein eindeutiges SYSLOG-Meldungsformat. Zum Beispiel wird Syslog und Meldungen über lokale Geräte ein Schweregrad-Code sowie ein mnemonisches Zeichen zugewiesen, durch das die Quellenanwendung identifiziert wird, von der die Meldung ausgegeben wurde. Dadurch wird es ermöglicht, Meldungen aufgrund ihrer Dringlichkeit oder Relevanz zu filtern. Der Schweregrad der jeweiligen Meldung legt fest, an welche Gruppe von Ereignisprotokollgeräten die Meldungen für die einzelnen Protokollierungsereignisse gesendet werden.

In der folgenden Tabelle sind die Schweregrade von Protokollen aufgeführt:

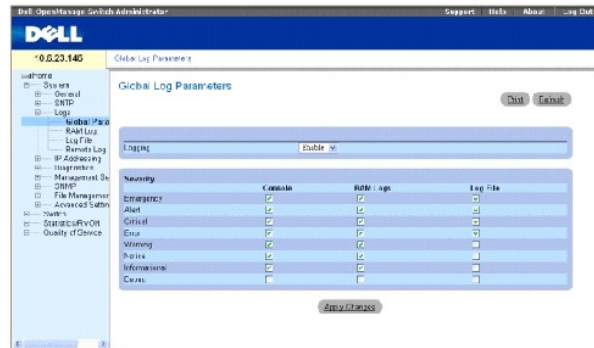
**Tabelle 6-21. Schweregrade von Protokollen**

Art des Schweregrads	Schweregrad	Beschreibung
Emergency (Notfall)	0	Gibt an, dass das System nicht funktionsfähig ist.
Alert (Alarm)	1	Gibt an, dass das System umgehend gewartet werden muss.
Critical (Kritisch)	2	Gibt an, dass sich das System in einem kritischen Zustand befindet.
Fehler	3	Weist auf einen Systemfehler hin.

Warning (Warnung)	4	Weist auf eine Systemwarnung hin.
Notice (Hinweis)	5	Gibt an, dass das System zwar ordnungsgemäß arbeitet, jedoch eine Systemmeldung ausgegeben wurde.
Informational (Zur Information)	6	Zeigt Geräteinformationen an.
Debug (Fehlerbeseitigung)	7	Zeigt ausführliche Informationen zum Protokoll an. Wenden Sie sich bei Auftreten eines Debug-Fehlers an den Dell Technischen Support online.

Die Seite [Global Log Parameters](#) (Globale Protokollparameter) enthält Felder zur Festlegung, welche Ereignisse in welchen Protokollen aufgezeichnet werden. Sie 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. Öffnen Sie die Seite [Global Log Parameters](#) (Globale Protokollparameter), indem Sie auf System→ Logs→ Global Parameters in der Strukturansicht klicken.

Abb. 6-29. Globale Protokollparameter



**Logging** (Protokollführung) – Ermöglicht die Erstellung globaler Geräteprotokolle in Form von Cache-, Datei- und Serverprotokollen. Konsolenprotokolle sind standardmäßig aktiviert.

**Severity** (Schweregrad) – Die folgenden Schweregrade sind für Protokolle verfügbar:

**Emergency** (Notfall) – 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** (Alarm) – Stellt die zweithöchste Warnstufe dar. Ein Warnprotokoll wird bei einem schwerwiegenden Geräteausfall gespeichert, beispielsweise wenn sämtliche Gerätefunktionen ausfallen.

**Critical** (Kritisch) – 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** (Fehler) – Gibt an, dass ein Gerätefehler aufgetreten ist, beispielsweise wenn ein einzelner Port offline geschaltet ist.

**Warning** (Warnung) – Entspricht der niedrigsten Gerätewarnstufe. Das Gerät funktioniert zwar, bei seinem Betrieb ist jedoch ein Problem aufgetreten.

**Notice** (Hinweis) – Liefert Geräteinformationen.

**Informational** (Zur Information) – Liefert Geräteinformationen.

**Debug** (Fehlerbehebung) – Liefert Meldungen zur Fehlerbehebung.

 **ANMERKUNG:** Bei Auswahl eines Schweregrades werden alle über dieser Auswahl befindlichen Schweregrade automatisch mit aktiviert.

Die Seite [Global Log Parameters](#) (Globale Protokollparameter) enthält zusätzlich Kontrollkästchen, die jeweils einem bestimmten Protokollierungssystem entsprechen:

Console (Konsole) — Gibt den geringsten Schweregrad an, bei dessen Auftreten Protokolle an die Konsole gesendet werden.

RAM Logs (RAM-Protokolle) — Gibt den geringsten Schweregrad an, bei dessen Auftreten Protokolle an die im RAM (Cache) enthaltene Protokolldatei gesendet werden.

Log File (Protokolldatei) — 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](#) (Globale Protokollparameter).
2. Wählen Sie **Enable** (Aktivieren) in der Dropdown-Liste **Logging** (Protokollführung).
3. Wählen Sie mithilfe der Kontrollkästchen unter **Global Log Parameters** Protokolltyp und Protokollschweregrad aus.
4. Klicken Sie auf „**Apply Changes**“ (Änderungen übernehmen).

Die Protokolleinstellungen werden gespeichert und das Gerät wird aktualisiert.

### Aktivierung von Protokollen mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [Global Log Parameters](#) angezeigt werden.

Tabelle 6-22. CLI-Befehle für globale Protokollparameter

CLI-Befehl	Beschreibung
logging on (Protokollführung läuft)	Aktiviert die Protokollierung von Fehlermeldungen.
logging {ip-address   hostname} [port port] [severity level] [facility facility] [description text]	Protokolliert Meldungen auf einem Syslog-Server. Eine Liste der Schweregrade finden Sie unter <a href="#">„Schweregrade von Protokollen“</a> .
logging console level (Protokollierung auf Konsolenebene)	Beschränkt die Protokollierung auf der Konsole auf Fehlermeldungen des angegebenen Schweregrads.
logging buffered level (Protokollierung auf Pufferspeicherebene)	Beschränkt die Anzeige von Syslog-Meldungen aus einem internen Pufferspeicher (RAM) auf Meldungen des angegebenen Schweregrads.
logging file level (Protokollierung auf Dateiebene)	Beschränkt das Senden von Syslog-Meldungen an die Protokolldatei auf Meldungen des angegebenen Schweregrads.
clear logging (Protokollierung löschen)	Löscht den Protokollinhalt.
clear logging file (Protokollierungsdatei löschen)	Löscht die Meldungen aus der Protokolldatei.

Das folgende Beispiel illustriert 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
```

```
Console(config)# exit

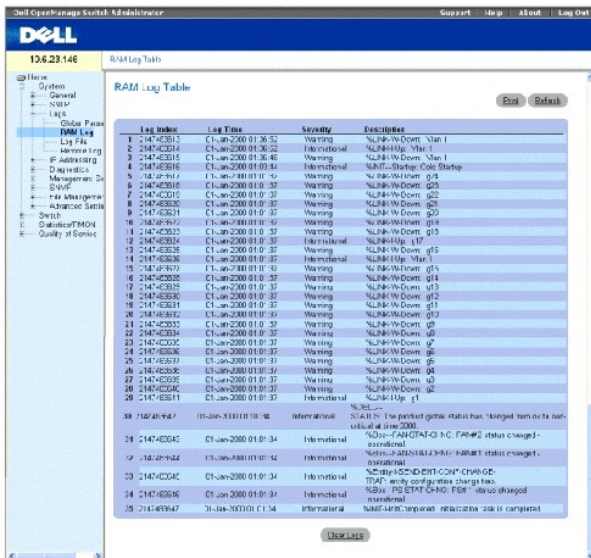
Console# clear logging
file

Clear Logging File [y/n]
```

## Anzeigen der RAM-Protokolltabelle

Die [RAM Log Table](#) (RAM-Protokolltabelle) enthält Informationen zu Protokolleinträgen im RAM, einschließlich der Uhrzeit, zu der das Protokoll aufgezeichnet wurde, des Protokollschweregrads sowie einer Beschreibung des Protokolls. Öffnen Sie die Seite [RAM Log Table](#) (RAM-Protokolltabelle), indem Sie auf System → Logs → RAM Log in der Strukturansicht klicken.

Abb. 6-30. RAM-Protokolltabelle



Log Index	Log Time	Severity	Description
1 2147E313	Cl Jan 2000 01:36:52	Warning	N/A/N/W/Down: Vlan 1
2 2147E314	Cl Jan 2000 01:36:52	Informational	N/A/N/W/Down: Vlan 1
3 2147E315	Cl Jan 2000 01:36:48	Warning	N/A/N/W/Down: Vlan 1
4 2147E316	Cl Jan 2000 01:09:34	Informational	N/A/N/W/Start: Core Startup
5 2147E317	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g15
6 2147E318	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g23
7 2147E319	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g22
8 2147E320	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g21
9 2147E321	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g14
10 2147E322	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g15
11 2147E323	Cl Jan 2000 01:09:35	Informational	N/A/N/W/Up: g17
12 2147E324	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g15
13 2147E325	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g15
14 2147E326	Cl Jan 2000 01:09:35	Informational	N/A/N/W/Up: Vlan 1
15 2147E327	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g15
16 2147E328	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g14
17 2147E329	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g13
18 2147E330	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g12
19 2147E331	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g11
20 2147E332	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g13
21 2147E333	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g12
22 2147E334	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g11
23 2147E335	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g7
24 2147E336	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g6
25 2147E337	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g5
26 2147E338	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g4
27 2147E339	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g3
28 2147E340	Cl Jan 2000 01:09:35	Warning	N/A/N/W/Down: g2
29 2147E341	Cl Jan 2000 01:09:35	Informational	N/A/N/W/Up: g1
30 2147E342	Cl Jan 2000 01:09:35	Informational	N/A/N/W/Up: g1
31 2147E343	Cl Jan 2000 01:09:35	Informational	N/A/N/W/Up: g1
32 2147E344	Cl Jan 2000 01:09:35	Informational	N/A/N/W/Up: g1
33 2147E345	Cl Jan 2000 01:09:35	Informational	N/A/N/W/Up: g1
34 2147E346	Cl Jan 2000 01:09:35	Informational	N/A/N/W/Up: g1
35 2147E347	Cl Jan 2000 01:09:35	Informational	N/A/N/W/Up: g1

Log Index (Protokollverzeichnis) — Gibt die Protokollnummer in der [RAM Log Table](#) (RAM-Protokolltabelle) an.

Log Time (Protokollzeit) — Gibt die Uhrzeit an, zu der das Protokoll in die [RAM Log Table](#) (RAM-Protokolltabelle) eingefügt wurde.

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

Description (Beschreibung) — Zeigt die benutzerdefinierte Protokollbeschreibung an.

### Entfernen von Protokollinformationen:

1. Öffnen Sie die Seite [RAM Log Table](#) (RAM-Protokolltabelle).
2. Klicken Sie auf „Clear Log“ (Protokoll löschen).

Die Protokollinformationen werden aus der [RAM Log Table](#) (RAM-Protokolltabelle) entfernt und das Gerät aktualisiert.

## Anzeigen und Löschen der RAM-Protokolltabelle mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zum Anzeigen und Löschen der Felder zusammengefasst, die auf der Seite [RAM Log Table](#) angezeigt werden.

Tabelle 6-23. CLI-Befehle für die RAM-Protokolltabelle

CLI-Befehl	Beschreibung
show logging	Zeigt den Protokollierungsstatus und die im internen Pufferspeicher enthaltenen Syslog-Meldungen an.
clear logging	Löscht den Protokollinhalt.

Das folgende Beispiel illustriert die CLI-Befehle:

```
console# show logging

Logging is enabled.

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

Buffer Logging: Level
info. Buffer Messages: 26
Logged, 26 Displayed, 200
Max.

File Logging: Level error.
File Messages: 157 Logged,
26 Dropped.

1 messages were not logged

01-Jan-2000 01:03:42 :%
INIT-I-Startup: Cold
Startup

01-Jan-2000 01:01:36 :%
LINK-W-Down: g24

01-Jan-2000 01:01:36 :%
LINK-W-Down: g23

01-Jan-2000 01:01:36 :%
LINK-W-Down: g22

01-Jan-2000 01:01:36 :%
LINK-W-Down: g21

01-Jan-2000 01:01:36 :%
LINK-W-Down: g20

01-Jan-2000 01:01:36 :%
LINK-W-Down: g19
```

```

01-Jan-2000 01:01:36 :%
LINK-W-Down: g18

01-Jan-2000 01:01:36 :%
LINK-W-Down: g17

01-Jan-2000 01:01:36 :%
LINK-W-Down: g13

1-Jan-2000 01:01:36 :%
LINK-W-Down: g2

01-Jan-2000 01:01:36 :%
LINK-W-Down: g1

01-Jan-2000 01:01:32 :%
INIT-I-InitCompleted:
Initialization task is
completed

Console # clear logging

clear logging buffer
[y/n]?

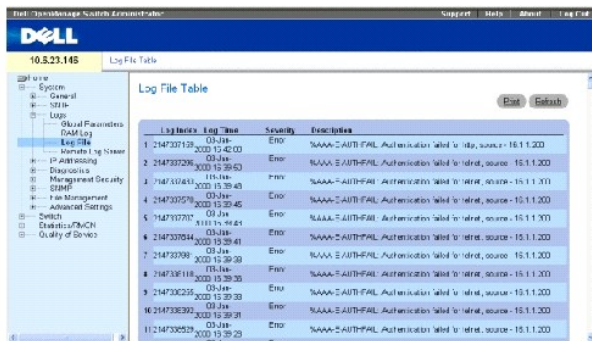
Console #

```

## Anzeigen der Protokolldatei-Tabelle

Die Seite [Log File Table](#) (Protokolldatei-Tabelle) 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. Öffnen Sie die Seite [Log File Table](#), indem Sie auf System→ Logs→ Log File in der Strukturansicht klicken.

Abb. 6-31. Protokolldatei-Tabelle (Log File Table)



Log Index (Protokollverzeichnis)— Gibt die Protokollnummer in der **Log File Table** an.

Log Time (Protokollzeit) — Gibt die Uhrzeit an, zu der das Protokoll in die **Log File Table**eingefügt wurde.

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

Description (Beschreibung) — Zeigt den Text der Protokollmeldung an.

## Anzeigen der Protokolldatei-Tabelle mit den CLI -Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Anzeige und Einstellung der Felder zusammengefasst, die auf der Seite [Log File Table](#)angezeigt werden.

**Tabelle 6-24. CLI -Befehle für die Protokolldatei-Tabelle (Log File Table)**

CLI-Befehl	Beschreibung
show logging file	Zeigt den Protokollierungsstatus und die in der Protokolldatei enthaltenen Syslog-Meldungen an.
clear logging file	Löscht die Meldungen aus den Protokolldateien.

Das folgende Beispiel illustriert die CLI-Befehle:

```
Console # show
logging file

Logging is enabled.

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

Buffer Logging: Level
info. Buffer
Messages: 62 Logged,
62 Displayed, 200
Max.

File Logging: Level
debug. File Messages:
11 Logged, 51
Dropped.

SysLog server
12.1.1.2 Logging:
warning. Messages: 14
Dropped.

SysLog server 1.1.1.1
Logging: info.
Messages: 0 Dropped.

1 messages were not
logged

01-Jan-2000
01:12:01 :%COPY-W-
TRAP: The copy
operation was
completed
successfully
```



```
01-Jan-2000
01:11:49 :%LINK-I-Up:
g21

01-Jan-2000
01:11:49 :%2SWPHY-I-
CHNGCOMBOMEDIA: Media
changed from copper
media

to fiber media
(1000BASE-SX) on port
g21.

01-Jan-2000
01:11:48 :%2SWPHY-I-
CHNGCOMBOMEDIA: Media
changed from fiber
media to copper media
on port g21.

01-Jan-2000
01:11:48 :%LINK-W-
Down: g21

01-Jan-2000
01:11:46 :%LINK-I-Up:
g19

01-Jan-2000
01:11:42 :%LINK-W-
Down: g14

01-Jan-2000
01:11:41 :%LINK-I-Up:
g14

01-Jan-2000
01:11:36 :%LINK-W-
Down: g9

01-Jan-2000
01:11:35 :%LINK-I-Up:
g1

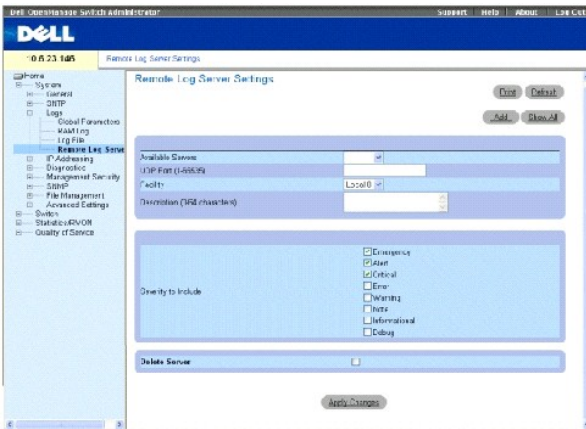
01-Jan-2000
01:11:34 :%LINK-W-
Down: g1

console#
```

### Konfiguration der Einstellungen des Remote-Protokollservers

Die Seite [Remote Log Server Settings](#) (Remote-Protokollserver-Einstellungen) enthält Felder zur Anzeige und Konfiguration der verfügbaren Protokollserver. Außerdem können neue Protokollserver und der Schweregrad der an die einzelnen Server gesendeten Protokolle definiert werden. Öffnen Sie die Seite [Remote Log Server Settings](#), indem Sie auf System→ Logs→ Remote Log Server in der Strukturansicht klicken.

Abb. 6-32. Einstellungen des Remote-Protokollservers



Available Servers (Verfügbare Server) — Enthält eine Liste der Server, an die Protokolle gesendet werden können.

UDP Port (1-65535) — Gibt den UDP-Port 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 (Anlage) — Gibt eine benutzerdefinierte Anwendung an, von der Systemprotokolle an den Remote-Server geschickt werden. Nur eine Anlage kann jeweils einem Server zugewiesen werden. Wenn eine zweite Anlagenebene zugewiesen wird, wird die erste aufgehoben. Alle für ein Gerät definierten Anwendungen verwenden die gleiche Anlage auf einem Server. Folgende Feldwerte können ausgewählt werden:

Local 0 - Local 7.

Description (Beschreibung) (0-64 Zeichen) — Zeigt die benutzerdefinierte Serverbeschreibung an.

Delete Server (Server löschen) — Löscht, wenn ausgewählt, den derzeit ausgewählten Server aus der Liste der verfügbaren Server.

Die Seite [Remote Log Server Settings](#) (Remote-Protokollserver-Einstellungen) enthält ferner eine Liste der Schweregrade. Die Definitionen der Schweregrade sind identisch mit denen auf der Seite [Global Log Parameters](#) (Globale Protokollparameter).

### Senden von Protokollen an einen Server:

1. Öffnen Sie die Seite [Remote Log Server Settings](#).
2. Wählen Sie einen Server aus der Dropdown-Liste **Available Servers** (Verfügbare Server) aus.
3. Definieren Sie die Felder.
4. Wählen Sie mithilfe der Kontrollkästchen **Severity to Include** (Einzubeziehen in den Schweregrad) den Protokollschweregrad aus.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Protokolleinstellungen werden gespeichert und das Gerät wird aktualisiert.

### Definieren eines neuen Servers:

1. Öffnen Sie die Seite [Remote Log Server Settings](#) (Remote-Protokollserver-Einstellungen).
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite [Add a Log Server](#) (Einen Protokollserver hinzufügen) wird geöffnet:

Abb. 6-33. Hinzufügen eines Protokollservers

Add a Log Server

Refresh

New Log Server IP Address

UDP Port (1-65535) 514

Facility Local 7

Description (64 characters)

Severity to include

- Emergency
- Alert
- Critical
- Error
- Warning
- Note
- Information
- Debug

Apply Changes

New Log Server IP Address (IP-Adresse von neuem Protokollserver-) — Gibt die IP-Adresse des neuen Protokollservers an.

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

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

#### Anzeigen der Remote-Protokollserver-Tabelle:

1. Öffnen Sie die Seite [Remote Log Server Settings](#) (Remote-Protokollserver-Einstellungen).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die Seite [Remote Log Servers Table](#) (Remote-Protokollserver-Tabelle) wird geöffnet:

Abb. 6-34. Remote-Protokollserver-Tabelle

Remote Log Servers Table

Refresh

Servers	UDP Port	Facility	Description	Minimum Severity	Remove
---------	----------	----------	-------------	------------------	--------

Apply Changes

#### Entfernen eines Protokollservers von der Seite „Log Servers Table“ (Protokollserver-Tabelle):

1. Öffnen Sie die Seite [Remote Log Server Settings](#) (Remote-Protokollserver-Einstellungen).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die Seite [Remote Log Servers Table](#) (Remote-Protokollserver-Tabelle) wird geöffnet.

3. Wählen Sie einen Eintrag aus der [Remote Log Servers Table](#) (Remote-Protokollserver-Tabelle) aus.
4. Wählen Sie das Kontrollkästchen **Remove** (Entfernen), um den/die Server zu entfernen.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag aus der [Remote Log Servers Table](#) (Remote-Protokollserver-Tabelle) wird entfernt und das Gerät wird aktualisiert.

#### Arbeiten mit Remote-Serverprotokollen mithilfe der CLI-Befehle

Die folgende Tabelle fasst die entsprechenden CLI-Befehle zur Arbeit mit Remote-Serverprotokollen zusammen.

**Tabelle 6-25. CLI - Befehle für Remote-Serverprotokolle**

CLI - Befehl	Beschreibung
<b>logging</b> ( <i>ip-address   hostname</i> ) [ <b>port</b> <i>port</i> ] [ <b>severity</b> <i>level</i> ] [ <b>facility</b> <i>facility</i> ] <b>description</b> <i>text</i>	Protokolliert Meldungen auf einem Remote-Server.
<b>no logging</b> (Keine Protokollierung)	Löscht einen Syslog-Server.
<b>show logging</b> (Protokollierung anzeigen)	Zeigt den Protokollierungszustand und die Syslog-Meldungen an.

Das folgende Beispiel illustriert die CLI-Befehle:

```
console> enable

Console# configure

console (config) # logging
10.1.1.1 severity critical

Console# show logging

Logging is enabled.

Console Logging: Level
debug. Console Messages: 5
Dropped.

Buffer Logging: Level
debug. Buffer Messages: 16
Logged, 16 Displayed, 200
Max.

File Logging: Level error.
File Messages: 0 Logged,
209 Dropped.

SysLog server 31.1.1.2
Logging: error. Messages:
22 Dropped.

SysLog server 5.2.2.2
Logging: info. Messages: 0
Dropped.

SysLog server 10.2.2.2
Logging: critical.
Messages: 21 Dropped.

SysLog server 10.1.1.1
Logging: critical.
Messages: 0 Dropped.
```

```
1 messages were not logged
```

```
03-Mar-2004 12:02:03 :%  
LINK-I-Up: g1
```

```
03-Mar-2004 12:02:01 :%  
LINK-W-Down: g2
```

```
03-Mar-2004 12:02:01 :%  
LINK-I-Up: g3
```

## 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. Öffnen Sie die Seite „IP Addressing“, indem Sie auf System → IP Addressing in der Strukturansicht klicken.

## Definieren von Standardgateways

Die Seite **Default Gateway** (Standardgateway) enthält Felder zur Zuweisung 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. Öffnen Sie die Seite **Default Gateway** (Standardgateway), indem Sie auf System → IP Addressing → Default Gateway in der Strukturansicht klicken.

Die Seite **Default Gateway** (Standardgateway) enthält die folgenden Felder:

Default Gateway (Standardgateway) — Gibt die IP-Adresse des Gatewaygerätes an.

Remove (Entfernen) — Entfernt, wenn ausgewählt, Gatewaygeräte aus der Dropdown-Liste **Default Gateway**.

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

Das Gatewaygerät wird ausgewählt und das Gerät wird aktualisiert.

### Entfernen eines Standardgatewaygerätes:

1. Öffnen Sie die Seite **Default Gateway** (Standardgateway).
2. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen), um die Standardgateways zu entfernen.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Standardgateway-Eintrag wird entfernt und das Gerät wird aktualisiert.

## Definieren von Gatewaygeräten mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite **Default Gateway** (Standardgateway) angezeigt werden.

**Tabelle 6-26. CLI-Befehle für Standardgateway**

CLI-Befehl	Beschreibung
ip default-gateway ip-address	Definiert eine Standardgateway.
no ip default-gateway	Entfernt eine Standardgateway.

Das folgende Beispiel illustriert die CLI-Befehle:

```

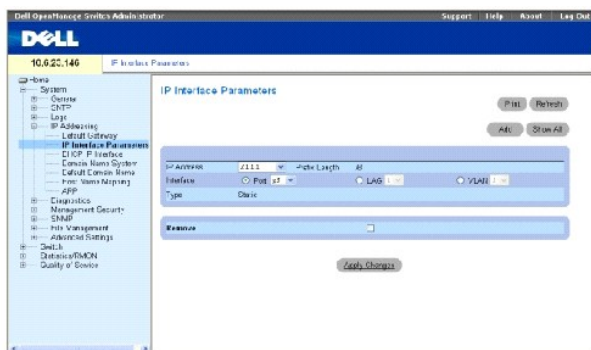
Console(config)# ip
default-gateway
196.210.10.1

Console (config)# no ip
default-gateway
    
```

## Definieren von IP-Schnittstellen

Die Seite [IP Interface Parameters](#) (IP-Schnittstellenparameter) enthält Parameter zum Zuweisen von IP-Adressen zu Schnittstellen. Öffnen Sie die Seite [IP Interface Parameters](#), indem Sie auf **System** → **IP Addressing** → **Interface Parameters** in der Strukturansicht klicken.

**Abb. 6-35. IP-Schnittstellenparameter**



**IP Address** — Gibt die IP-Adresse der Schnittstelle an.

**Prefix Length (Präfixlänge)** — Gibt die Anzahl der Bits an, die das IP-Quelladress-Präfix enthält, oder die Netzwerkmaske der IP-Quelladresse.

**Interface** — Legt den Schnittstellentyp fest, für den die ausgewählte IP-Adresse definiert ist. Folgende Feldwerte sind möglich: **Port**, **LAG** oder **VLAN**.

Weitere Informationen finden Sie unter [„Konfigurieren von VLANs“](#).

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

**Forward Directed IP Broadcasts (Vorwärtsgerichtete IP-Broadcasts)** — Ermöglicht die Umsetzung einer adressierten Broadcast in physische Broadcasts. Bei Deaktivierung werden IP-adressierte Broadcasts nicht bearbeitet und nicht weitergeleitet.

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

**One Fill** (Eine Füllung) — Die Broadcast-Adresse der Schnittstelle weist die gleiche Besetzung auf (255.255.255.255).

**Zero Fill** (Nullfüllung) — Die Broadcast-Adresse der Schnittstelle ist mit Nullen belegt (0.0.0.0).

**Remove** — Bei Aktivierung wird die Schnittstelle aus dem **IP Address** Dropdown-Menü entfernt.

## Hinzufügen einer IP-Schnittstelle

1. Öffnen Sie die Seite [IP Interface Parameters](#) (IP-Schnittstellenparameter).
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite [Add a Static Interface](#) (Eine statische Schnittstelle hinzufügen) wird geöffnet:

Abb. 6-36. Hinzufügen einer statischen Schnittstelle

Source IP Address: (x.X.X.X) Network Mask: (x.X.X.X)  
Prefix Length: 1/20  
Interface: g1 LAN VLAN: 1  
Apply Changes

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

**Network Mask** (Netzwerkmaske) gibt die Subnetzmaske der IP-Quelladresse an.

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

Die neue Schnittstelle wird hinzugefügt und das Gerät aktualisiert.

## Ändern von IP-Adressenparametern

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

Die Parameter werden geändert und das Gerät aktualisiert.

## Löschen von IP-Adressen

1. Öffnen Sie die Seite [IP Interface Parameters](#) (IP-Schnittstellenparameter).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die **Interface Parameters Table** (Schnittstellenparameter-Tabelle) wird geöffnet:

IP Interface Parameter Table

	IP Address	Prefix Length	Interface	Type	Remove
1	2.1.1.1	/8	g3	Static	<input type="checkbox"/>
2	10.8.254.146	/24	g17	DHCP	<input type="checkbox"/>
3	16.1.1.3	/8	g1	Static	<input type="checkbox"/>

Apply Changes

Abb. 6-37. IP-Schnittstellenparameter-Tabelle

3. Wählen Sie eine IP-Adresse und aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die ausgewählte IP-Adresse wird gelöscht und das Gerät wird aktualisiert.

## Definieren der IP-Schnittstellen mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [IP Interface Parameters](#) (IP-Schnittstellenparameter) angezeigt werden.

**Tabelle 6-27. CLI-Befehle für IP-Schnittstellen**

CLI-Befehl	Beschreibung
ip address ip-address {mask   prefix-length}	Stellt eine IP-Adresse ein.
no ip address [ip-address]	Entfernt eine IP-Adresse
show ip interface [ethernet interface-number   vlan vlan-id   port-channel number]	Zeigt den Nutzbarkeitsstatus von Schnittstellen an, die für IP konfiguriert wurden.

Das folgende Beispiel illustriert 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

Output

Gateway IP Address Activity
status

-----
---

192.168.1.1 Active

IP address Interface Type

-----
-----

```



```
192.168.1.123 /24 VLAN 1
Static
```

## Definieren von DHCP IP-Schnittstellenparametern

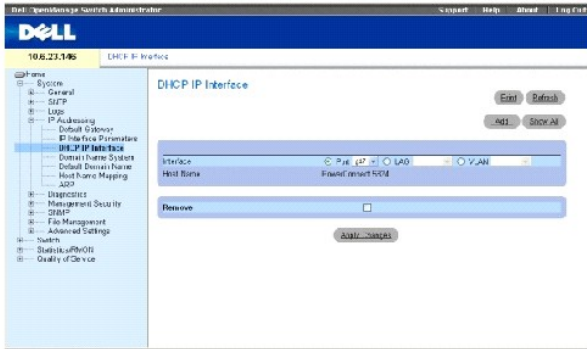
```
console# show ip interface vlan 1
```

### Ausgabe

Gateway-IP-Adresse	Aktivitätsstatus	
-----	-----	
	-	
192.168.1.1	Aktiv	
IP address:	Interface	Type
-----	-----	-----
		-
192.168.1.123 /24	VLAN 1	static

Die Seite [DHCP IP Interface](#) (DHCP IP-Schnittstelle) enthält Felder zur Angabe der am Gerät angeschlossenen DHCP-Clients. Klicken Sie auf **System** → **IP Addressing** → **DHCP IP Interface** in der Strukturansicht. Öffnen Sie die Seite [DHCP IP Interface](#).

Abb. 6-38. DHCP IP-Schnittstelle



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

**Host Name** — Gibt den Systemnamen an. Dieses Feld kann bis zu 20 Zeichen umfassen.

**Remove (Entfernen)** — Entfernt, wenn ausgewählt, DHCP-Clients.

### Hinzufügen von DHCP-Clients

1. Öffnen Sie die Seite [DHCP IP Interface](#) (DHCP IP-Schnittstelle).
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite **Add DHCP IP Interface** (DHCP IP-Schnittstelle hinzufügen) wird geöffnet.

3. Geben Sie die Informationen auf der Seite ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die DHCP-Schnittstelle wird hinzugefügt und das Gerät aktualisiert.

### Ändern einer DHCP IP-Schnittstelle

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

Der Eintrag wird geändert und das Gerät wird aktualisiert.

### Löschen einer DHCP IP-Schnittstelle

1. Öffnen Sie die Seite [DHCP IP Interface](#) (DHCP IP-Schnittstelle).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die **DHCP Client Table** (DHCP Client-Tabelle) wird geöffnet.

3. Wählen Sie einen DHCP-Client-Eintrag aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der ausgewählte Eintrag wird gelöscht und das Gerät wird aktualisiert.

## Definieren der DHCP IP-Schnittstellen mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Definition von DHCP-Clients.

Tabelle 6-28. CLI-Befehle für DHCP IP-Schnittstelle

CLI-Befehl	Beschreibung
<code>ip address dhcp [hostname host-name]</code>	Dient zum Bezug einer IP-Adresse auf einer Ethernet-Schnittstelle vom Dynamic Host Configuration Protocol (DHCP).

Das folgende Beispiel illustriert die CLI-Befehle:

```

console> enable

console# config

console (config#)
interface ethernet g1

console (config-if)# ip
address dhcp 10.0.0.1 /8
    
```

## Konfigurieren von Domännennamensystemen (DNS)

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

Die Seite **Domain Naming System (DNS)** enthält Felder zur Aktivierung von speziellen DNS-Servern. Öffnen Sie die Seite **Domain Naming System (DNS)**, indem Sie auf **System** → **IP Addressing** → **Domain Name System** in der *Strukturansicht* klicken.

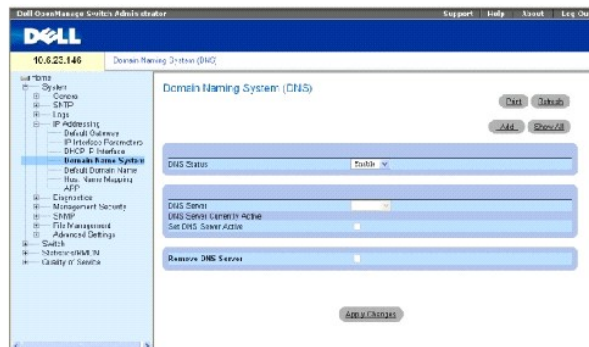


Abb. 6-39. Domain Naming System (DNS)

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

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

**DNS Server Currently Active** (Gegenwärtig aktiver DNS-Server) — Der gegenwärtig aktive DNS-Server.

**Set DNS Server Active** (DNS-Server auf aktiv einstellen) — Aktiviert den im Feld **DNS Server** ausgewählten DNS-Server.

**Remove DNS Server** (DNS-Server entfernen) — Entfernt, wenn ausgewählt, DNS-Server.

## Hinzufügen eines DNS-Servers

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

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

Abb. 6-40. Hinzufügen eines DNS-Servers

Das Bild zeigt ein Web-Formular mit dem Titel 'Add DNS Server' und einem 'Refresh'-Button oben rechts. Das Formular hat drei Zeilen mit Eingabefeldern: 'DNS server' (ein Textfeld), 'DNS Server Currently Active' (ein Kontrollkästchen) und 'Set DNS Server Active' (ein Kontrollkästchen). Unten rechts befindet sich ein 'Apply Changes'-Button.

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

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

## Anzeigen der DNS-Server-Tabelle

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

Die Seite **DNS Server Table** (DNS-Server-Tabelle) wird geöffnet:

Abb. 6-41. DNS-Server-Tabelle

Das Bild zeigt eine Tabelle mit dem Titel 'DNS Server Table' und einem 'Refresh'-Button oben rechts. Die Tabelle hat drei Spalten: 'DNS Server', 'Active Server' und 'Remove Set: All'. Unten rechts befindet sich ein 'Apply Changes'-Button.

## Entfernen von DNS-Servern

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

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

## Konfigurieren von DNS-Servern mit den CLI-Befehlen

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

Tabelle 6-29. CLI-Befehle für DNS-Server

CLI-Befehl	Beschreibung
<code>ip name-server server-address</code>	Stellt die verfügbaren DNS-Namensserver ein. Bis zu acht DNS-Namensserver können eingestellt werden.
<code>no ip name-server server-address</code>	Entfernt einen DNS-Namensserver.
<code>ip domain-name name</code>	Definiert einen Standarddomänennamen, mit dem die Software nicht-qualifizierte Hostnamen vervollständigt.
<code>clear host {name   *}</code>	Löscht Einträge aus dem „host name-to-address“-Cache.
<code>show hosts [name]</code>	Zeigt den Standarddomänennamen, eine Liste der DNS-Namensserver-Hosts, die statische und die gecachte Liste der Hostnamen und Adressen an.

Das folgende Beispiel illustriert die CLI-Befehle:

```

console> enable

Console# configure

console (config)# ip name-
server 176.16.1.18

```

## Definieren von Standarddomänen

Die Seite **Default Domain Name** (Standard-Domänennamen) enthält Informationen zur Definition der Standard-DNS-Domänennamen. Öffnen Sie die Seite **Default Domain Name**, indem Sie auf **System** → **IP Addressing** → **Default Domain Name** in der *Strukturansicht* klicken.

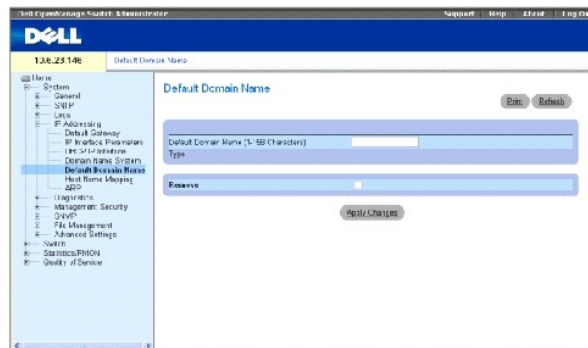


Abb. 6-42. Standard-Domänennamen

**Default Domain Name (1-158 Zeichen)** — Enthält einen benutzerdefinierten DNS-Server. Bei Auswahl ist der DNS-Domänennamen die Standarddomäne.

**Type** — Der Domäentyp, falls die Domäne statisch oder dynamisch erstellt wurde.

**Remove (Entfernen)** — Entfernt, wenn ausgewählt, eine ausgewählte Domäne.

## Definieren von DNS-Domänennamen mit den CLI-Befehlen

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

Tabelle 6-30. CLI-Befehle für DNS-Domänennamen

CLI-Befehl	Beschreibung
<code>ip domain-name name</code>	Definiert einen Standard-Domänennamen, mit dem die Software nicht-qualifizierte Hostnamen vervollständigt.
<code>no ip domain-name</code>	Deaktiviert die Verwendung des Domänennamensystems (DNS).
<code>show hosts [name]</code>	Zeigt den Standard-Domänennamen, eine Liste der DNS-Namensserver-Hosts, die statische und die gecachte Liste der Hostnamen und Adressen an.

Das folgende Beispiel illustriert die CLI-Befehle:

```
console> enable

Console# configure

console (config)# ip
domain-name www.dell.com
```

## Zuweisung des Domänenhosts

Die Seite **Host Name Mapping** (Zuweisung von Hostnamen) enthält Parameter zur Zuweisung von IP-Adressen zu statischen Hostnamen. Die Seite **Host Name Mapping** stellt bis zu acht IP-Adressen pro Host bereit. Öffnen Sie die Seite **Host Name Mapping**, indem Sie auf **System** → **IP Addressing** → **Host Name Mapping** klicken.

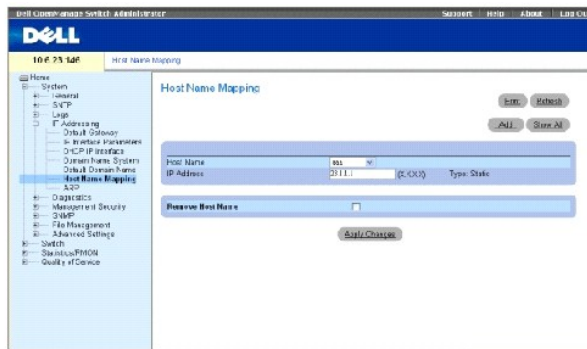


Abb. 6-43. Zuweisung von Hostnamen

**Host Name** — Enthält eine Liste von Hostnamen. Hostnamen werden auf der Seite **Add Host Name Mapping** (Zuweisen von Hostnamen) definiert. Jeder Host stellt bis zu acht IP-Adressen bereit. Die Feldwerte für das Hostnamen-Feld sind wie folgt:

**IP Address (X.X.X.X)** — Stellt bis zu acht IP-Adressen bereit, die dem angegebenen Hostnamen zugewiesen werden.

**Type** — Der IP-Adressentyp. Folgende Feldwerte können ausgewählt werden:

**Dynamic** — Die IP-Adresse wurde dynamisch erstellt.

**Static** — Die IP-Adresse ist statisch.

**Remove Host Name Mapping** (Hostnamenzuweisung entfernen) — Entfernt, wenn aktiviert, die DNS-Hostzuweisung.

## Hinzufügen von Host-Domännennamen

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

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

Refresh

Add Host Name Mapping

Host Name (1-126 Characters)	<input type="text"/>
IP Address	<input type="text" value="X.X.X.X"/>

Apply Changes

Abb. 6-44. Zuweisen von Hostnamen

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

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

### Anzeigen der Zuweisungstabelle für Hostnamen

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

Die Seite **Hosts Name Mapping Table** (Zuweisungstabelle für Hostnamen) wird geöffnet:

Refresh

Hosts Name Mapping Table

	Host Name	IP Address	Remove Select All
1	aaa	191.1.1.1	<input type="checkbox"/>
2	www.com	231.1.1.1	<input type="checkbox"/>

Apply Changes

Abb. 6-45. Host-Zuweisungstabelle

### Entfernen von Hostnamen aus der IP-Adressenzuweisung

1. Öffnen Sie die Seite **Host Name Mapping** (Zuweisung von Hostnamen).
2. Klicken Sie auf **Show All** (Alles anzeigen)
3. Die Seite **Host Mapping Table** (Host-Zuweisungstabelle) wird geöffnet.
4. **Wählen Sie einen Eintrag in der Hostzuweisungstabelle aus.**
5. **Aktivieren Sie das Kontrollkästchen Remove** (Entfernen).
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag in der Seite **Host Mapping Table** wird gelöscht und das Gerät wird aktualisiert.

### Zuweisung von IP-Adressen zu Domänenhostnamen mit den CLI-Befehlen

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

Tabelle 6-31. CLI - Befehle für für Domänenhostnamen

CLI - Befehl	Beschreibung
ip host name address1 [address2 ... address8]	Definiert die statische Zuweisung von Hostnamen zu Adressen im Hostcache.
no ip host name	Entfernt die Name-Adresse-Zuweisung.
clear host { name   * }	Löscht Einträge aus dem Hostname-Adresse-Cache.
show hosts [name]	Zeigt den Standard-Domännennamen, eine Liste der Serverhosts, die statische und die gecachte Liste der Hostnamen und Adressen an.

Das folgende Beispiel illustriert die CLI-Befehle:

```
console# enable
```

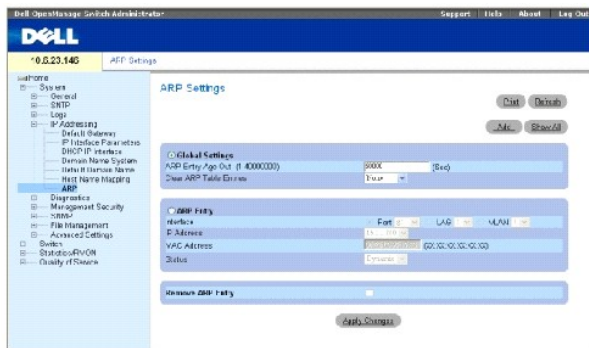
Console# **configure**

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

## 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. Öffnen Sie die Seite [ARP Settings](#) (ARP-Einstellungen), indem Sie auf System→ IP Addressing→ ARP in der Strukturansicht klicken.

Abb. 6-46. ARP-Einstellungen



**Global Settings** (Globale Einstellungen) — Diese Option wird gewählt, um die Felder für globale ARP-Einstellungen zu aktivieren.

**ARP Entry Age Out (1-4000000)** (ARP-Eintragsalter bei Ausgabe (1-4000000)) — Die Zeitspanne (in Sekunden), die zwischen ARP-Anforderungen zu einem Eintrag in der ARP-Tabelle vergeht - gilt für alle Geräte. Nach diesem Zeitraum wird der Eintrag aus der Tabelle gelöscht. Der Bereich ist 1 - 4000000, wobei Null anzeigt, dass Einträge nie aus dem Cache gelöscht werden. Der Standardwert lautet 60000 Sekunden.

**Clear ARP Table Entries** (ARP-Tabelleneinträge löschen) — Gibt die Art der auf allen Geräten zu löschenden ARP-Einträge an. Folgende Feldwerte können ausgewählt werden:

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

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

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

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

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

**Interface** (Schnittstelle) — Die Schnittstellenummer des am Gerät angeschlossenen Ports, LAG oder VLAN.

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

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



**Status** — Gibt den Status des Eintrags in der ARP-Tabelle an. Folgende Feldwerte können ausgewählt werden:

**Dynamic** — Der ARP-Eintrag wird dynamisch erfasst.

**Static** — Der ARP-Eintrag ist statisch.

**Remove ARP Entry** (ARP-Eintrag entfernen) — Entfernt, wenn ausgewählt, einen ARP-Eintrag.

### Hinzufügen eines statischen Eintrags in die ARP-Tabelle:

1. Öffnen Sie die Seite [ARP Settings](#) (ARP-Einstellungen).
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite **Add ARP Entry** (ARP-Eintrag hinzufügen) wird geöffnet:

Abb. 6-47. Hinzufügen eines ARP-Eintrags

The screenshot shows the 'Add ARP Entry' configuration page. At the top right is a 'Refresh' button. Below it is a form with three rows: 'Interface' with radio buttons for 'Port' (selected), 'LAG', and 'VLAN'; 'IP Address' with the value '0.0.0.0' and a '(X.X.X.X)' hint; and 'MAC Address' with a hexadecimal mask 'XXXXXXXXXX'. At the bottom center is an 'Apply Changes' button.

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

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

### Anzeigen der ARP-Tabelle:

1. Öffnen Sie die Seite [ARP Settings](#) (ARP-Einstellungen).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die Seite **ARP Table** (ARP-Tabelle) wird geöffnet:

Abb. 6-48. ARP-Tabelle

The screenshot shows the 'ARP Table' page with a 'Refresh' button at the top right. Below it is a table with the following data:

	Interface	IP Address	MAC Address	Status	Remove
1	g1	15.1.1.200	000b395179b3	Dynamic	<input type="checkbox"/>
2	g7	10.6.23.129	00026e00010d	Dynamic	<input type="checkbox"/>

At the bottom center is an 'Apply Changes' button.

### Löschen von Einträgen in der ARP-Tabelle

1. Öffnen Sie die Seite [ARP Settings](#) (ARP-Einstellungen).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die Seite **ARP Table** (ARP-Tabelle) wird geöffnet.

3. Wählen Sie einen Tabelleneintrag.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der ausgewählte Eintrag in der **ARP Table** wird gelöscht und das Gerät aktualisiert.

## Konfigurieren von ARP mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [ARP Settings](#) (ARP-Einstellungen) angezeigt werden.

Tabelle 6-32. CLI-Befehle für ARP-Einstellungen

CLI-Befehl	Beschreibung
arp ip_addr hw_addr { ethernet interface-number   vlan vlan-id   port-channel number }	Fügt einen permanenten Eintrag im ARP-Cache hinzu.
arp timeout seconds	Konfiguriert, wie lange ein Eintrag im ARP-Cache verbleibt.
clear arp-cache	Löscht alle dynamischen Einträge aus dem ARP-Cache
show arp	Zeigt Einträge in der ARP-Tabelle an.
no arp	Entfernt einen ARP-Eintrag aus der ARP-Tabelle.

Das folgende Beispiel illustriert die CLI-Befehle:

```
Console(config)# arp 198.133.219.232 00-00-0c-40-0f-bc

Console(config)# exit

Console# arp timeout 12000

Console# show arp

ARP timeout: 80000 Seconds
```

Interface	IP address:	HW address	Status
-----	-----	-----	-----
g1	10.7.1.102	00:10:B5:04:DB:4B	Dynamic
g2	10.7.1.135	00:50:22:00:2A:A4	Static

## Ausführen der Kabeldiagnose

Die Seite **Diagnostics** enthält Links zu Seiten, die die Ausführung virtueller Kabeltests an Kupfer- oder Glasfaserkabeln ermöglichen. Öffnen Sie die Seite **Diagnostics**, indem Sie auf **System** → **Diagnostics** in der Strukturansicht klicken.

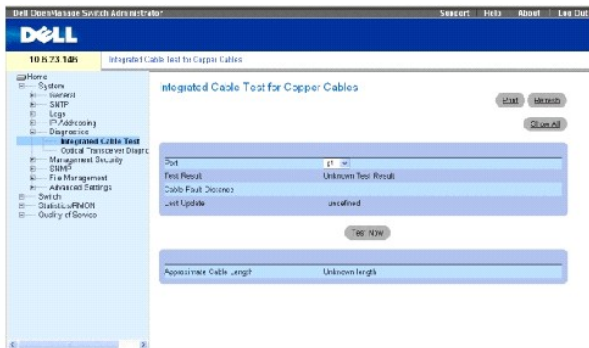
## Anzeigen der Kupferkabel-Diagnostik

Die Seite [Integrated Cable Test for Copper Cables](#) (Integrierter Kabeltest für Kupferkabel) enthält Felder zur Ausführung von Tests an Kupferkabeln.

Kabeltests liefern Informationen zu Orten im Kabel, wo Fehler aufgetreten sind, den letzten Kabeltest-Ausführungszeitpunkt und die Art des aufgetretenen Kabelfehlers. Die Tests bedienen sich der Time Domain Reflectometry (TDR)-Technologie, um die Qualität und Eigenschaften eines an einem Port angeschlossenen Kupferkabels zu testen. Kabel von bis zu 120 Meter Länge können getestet werden. Kabel werden getestet, wenn die Ports nicht in Betrieb sind, mit Ausnahme des Approximated Cable Length-Tests (Test für geschätzte Kabellänge).

Öffnen Sie die Seite [Integrated Cable Test for Copper Cables](#) (Integrierter Kabeltest für Kupferkabel), indem Sie auf System → Diagnostics → Integrated Cable Test in der Strukturansicht klicken.

Abb. 6-49. Integrierter Kabeltest für Kupferkabel



**Port** — Der Port, an dem das Kabel angeschlossen ist.

**Test Result** (Testergebnis) — Die Ergebnisse des Kabeltests. Mögliche Werte sind:

**No Cable** (Kein Kabel) — Am Port ist kein Kabel angeschlossen.

**Open Cable** (Offenes Kabel) — Das Kabel ist nur an einer Seite angeschlossen.

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

**OK** — Das Kabel hat den Test bestanden.

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

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

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

**Approximate Cable Length** (Ungefähre Kabellänge) — Die ungefähre Kabellänge. Dieser Test kann nur ausgeführt werden, wenn der Port aktiv ist und mit einer Geschwindigkeit von 1 Gbps arbeitet.

## Durchführung eines Kabeltests

1. Stellen Sie sicher, dass beide Enden des Kupferkabels an einem Gerät angeschlossen sind.
2. Öffnen Sie die Seite [Integrated Cable Test for Copper Cables](#) (Integrierter Kabeltest für Kupferkabel).
3. Klicken Sie auf **Test Now** (Jetzt testen).

Der Kupferkabeltest wird ausgeführt und die Ergebnisse werden auf der Seite [Integrated Cable Test for Copper Cables](#) angezeigt.

## Anzeigen der Ergebnistabelle für den virtuellen Kabeltest

1. Öffnen Sie die Seite [Integrated Cable Test for Copper Cables](#) (Integrierter Kabeltest für Kupferkabel).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die Seite **Virtual Cable Test Results Table** (Ergebnistabelle für virtuellen Kabeltest) wird geöffnet.

## Durchführung der Kupferkabeltests mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Ausführung der Kupferkabeltests.

Tabelle 6-33. CLI - Befehle für Kupferkabeltests

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

Das folgende Beispiel illustriert die CLI-Befehle:


```
console> enable

Console# test copper-port tdr g3

Cable is open at 100 meters.

Console> show copper-ports tdr
```

Port	Result	Length [meters]	Date
----	-----	-----	----
g1	OK		
g2	Short	50	13:32:00 15 January 2004
g3	Test has not been performed		
g4	Open	64	13:32:00 15 January 2004
g5	Fiber	-	-

 **ANMERKUNG:** Die angezeigte Kabellänge ist ein Annäherungswert im Bereich von bis zu 50 m, 50 - 80 m, 80 - 110 m, 110 - 120 m oder mehr als 120 m. Die Abweichung kann bis zu 20 m betragen.

## Anzeigen der Diagnostik für optische Transceiver

Die Seite [Optical Transceiver Diagnostics](#) (Diagnostik für optische Transceiver) enthält Felder zur Ausführung von Tests an Glasfaserkabeln. Öffnen Sie die Seite [Optical Transceiver Diagnostics](#), indem Sie auf **System**→ **Diagnostics**→ **Optical Transceiver Diagnostics** in der Strukturansicht klicken.


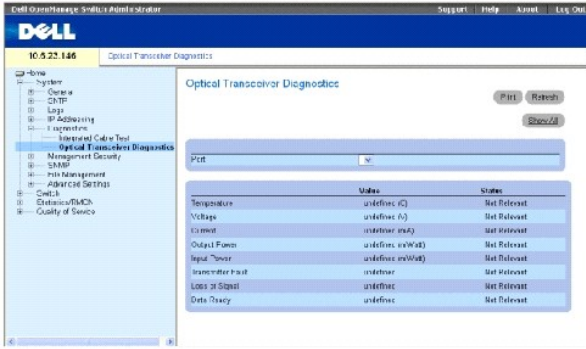
 **ANMERKUNG:** Die Diagnose für optische Transceiver kann nur bei vorhandener Verbindung durchgeführt werden.

Abb. 6-50. Diagnostik für optische Transceiver



**Port** — Der Port, an dem das Glasfaserkabel angeschlossen ist.

**Temperature** — Die Betriebstemperatur (in Celsius) des Kabels.

**Voltage** (Spannung) — Die Betriebsspannung des Kabels.

**Current** (Strom) — Der Betriebsstrom des Kabels.

**Output Power** (Ausgangsstrom) — Die Übertragungsrate des Ausgangsstroms.

**Input Power** (Eingangsstrom) — Die Übertragungsrate des Eingangsstroms.

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

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

**Data Ready** (Daten bereit) — Der Transceiver wurde erfolgreich eingeschaltet und Daten sind bereit.

## Anzeigen der Diagnosetest-Ergebnistabelle für optische Transceiver

1. Öffnen Sie die Seite [Optical Transceiver Diagnostics](#) (Diagnostik für optische Transceiver).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Der Test wird ausgeführt und die Seite **Virtual Cable Test Results Table** (Ergebnistabelle für virtuellen Kabeltest) wird geöffnet.

## Durchführung der Glasfaserkabeltests mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Ausführung der Glasfaserkabeltests.

Tabelle 6-34. CLI-Befehle für Glasfaserkabel-Tests

CLI-Befehl	Beschreibung
<code>show fiber-ports optical-transceiver [<i>interface</i>] [detailed]</code>	Zeigt die Optical-Transceiver-Diagnostik an.

Das folgende Beispiel illustriert die CLI-Befehle:

```


```

```
console> enable
```

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

Port	Temp	Voltage	Current	Power		TX	LOS
				Output	Input		
	(C)	(Volt)	(mA)	(mWatt)	(mWatt)	Fault	
g1	W	OK	E	OK	OK	OK	OK
g2	OK	OK	OK	OK	OK	E	OK
g3	Copper						

Temp - Internally measured transceiver temperature.

Voltage - Internally measured supply voltage.

Current - Measured TX bias current.

Output Power - Measured TX output power.


Input Power - Measured RX received power.

Tx Fault - Transmitter fault


LOS - Loss of signal

Die Seite **Optical Transceiver Diagnostics Table** (Diagnostiktabelle für optische Transceiver) **enthält die folgenden Spalten:**

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

 **ANMERKUNG:** Finisair-Transceiver unterstützen den Senderfehler-Diagnosetest nicht.

- 1 **LOS** — Signalverlust.
- 1 **Data Ready** (Daten bereit) — Der Transceiver wurde erfolgreich eingeschaltet und Daten sind bereit.
- 1 **N/A** — Nicht verfügbar, N/S - Nicht unterstützt, W - Warnung, E - Fehler.

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

## Verwalten der Gerätesicherheit

Die Seite **Management Security** (Verwalten der Gerätesicherheit) bietet Zugriff auf Sicherheitsseiten, die Felder zur Einstellung der Sicherheitsparameter für Ports, Geräteverwaltungsmethoden, Benutzer- und Serversicherheit enthalten. Öffnen Sie die Seite **Management Security**, indem Sie auf System→Management Security in der Strukturansicht klicken.

## Definieren von Zugriffsprofilen

Die Seite **Access Profiles** (Zugriffsprofile) enthält Felder zur Definition von Profilen und Regeln für den Gerätezugriff. Der Zugriff auf Verwaltungsmethoden kann durch Ingress-Schnittstellen, IP-Quelladressen und/oder IP-Quellsubnetze auf spezifische Benutzergruppen beschränkt werden.

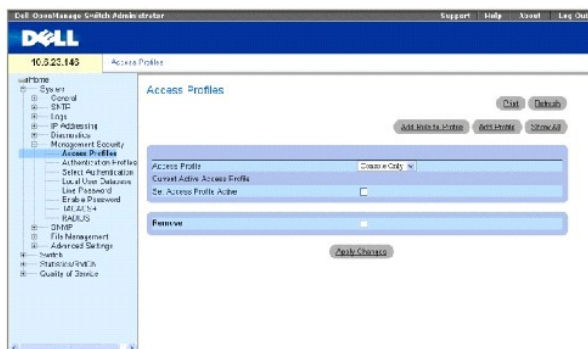
Verwaltungszugriffe können für jede der folgenden Methoden getrennt definiert werden, einschließlich Webzugriff (HTTP), Sicherer Webzugriff (HTTPS), Telnet, Secure Telnet und SNMP.

Es besteht die Möglichkeit, dass Benutzergruppen Zugriff auf unterschiedliche Verwaltungsdienste haben. Beispielsweise ist es möglich, dass Benutzergruppe 1 nur über eine HTTPS-Session auf das Gerät zugreifen kann, während Benutzergruppe 2 sowohl über HTTPS- als auch Telnet-Sessions Zugriff auf das Gerät hat.

Die Verwaltungszugriffslisten umfassen Regeln, die festlegen, auf welche Weise Geräte von welchem Benutzer verwaltet werden. Der Gerätezugriff kann auch für bestimmte Benutzer blockiert werden.

Die Seite **Access Profiles** (Zugriffsprofile) enthält Felder für die Konfiguration der Verwaltungslisten und ihre Anwendung auf bestimmte Schnittstellen. Öffnen Sie die Seite **Access Profiles**, indem Sie auf System→Management Security→Access Profiles in der Strukturansicht klicken.

Abb. 6-51. Zugriffsprofile



**Access Profile** — Benutzerdefinierte Zugriffsprofilnamen. Die Liste **Access Profile** enthält einen Standardwert für **Console List** (Konsolenliste), zu dem benutzerdefinierte Zugriffsprofile hinzugefügt werden. Bei Auswahl von **Console Only** (nur Konsole) als **Access Profile**-Name wird die Verbindung der Session getrennt und ausschließlicher Zugriff auf das Gerät von der Konsole aktiviert.

**Current Active Access Profile** (Derzeit aktives Zugriffsprofil) — Zeigt das derzeit aktive Zugriffsprofil an.

**Set Access Profile Active** (Zugriffsprofil auf Aktiv einstellen) — Aktiviert das ausgewählte Zugriffsprofil.

**Remove** (Entfernen) — Entfernt, wenn ausgewählt, das ausgewählte Zugriffsprofil aus der Liste **Access Profile Name** (Zugriffsprofilname).

## Aktivieren eines Profils

1. Öffnen Sie die Seite [Access Profiles](#) (Zugriffsprofile).
2. Wählen Sie ein Zugriffsprofil im Feld **Access Profile**.
3. Aktivieren Sie das Kontrollkästchen **Set Access Profile Active** (Zugriffsprofil auf Aktiv einstellen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das Zugriffsprofil wird aktiviert.

## Hinzufügen eines Zugriffsprofils

Bei der Bestimmung der Priorität von Regeln, 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. Priorität von Regeln legt die Reihenfolge fest, in der die Regeln in einem Profil angewendet werden.

### Definieren der Regeln für ein Zugriffsprofil:

1. Öffnen Sie die Seite **Access Profiles** (Zugriffsprofile).
2. Klicken Sie auf **Add an Access Profile** (Ein Zugriffsprofil hinzufügen).

Die Seite **Add An Access Profile** wird geöffnet:


Abb. 6-52. Hinzufügen eines Zugriffsprofils

**Access Profile Name** (Zugriffsprofilname) (1-32 Zeichen) — Benutzerdefinierter Name für das Zugriffsprofil.

**Rule Priority (1-65535)** (Regelpriorität (1-65535)) — Die Priorität der Regeln. Wenn das Paket mit einer Regel abgeglichen wird, wird Benutzergruppen der Verwaltungszugriff auf das Gerät entweder gewährt oder verwehrt. Die Reihenfolge der Regeln wird durch Definition einer Regelnnummer in der **Profile Rules Table** (Tabelle der Profilregeln) eingestellt. Die Regelnnummer ist wesentlich für die Abgleichung von Paketen mit Regeln, da Pakete nach dem First-Fit-Prinzip abgeglichen werden. Die Prioritäten der Regeln werden in der **Profile Rules Table** zugewiesen.

**Management Method** (Verwaltungsmethode) — Gibt die Verwaltungsmethode an, für die das Zugriffsprofil definiert wurde. Benutzer mit diesem Zugriffsprofil können mit der ausgewählten Verwaltungsmethode auf das Gerät zugreifen.

**Interface** (Schnittstelle) — Gibt den Schnittstellentyp an, auf die die Regel angewendet wird. Dieses Feld ist optional. Diese Regel kann auf einen ausgewählten Port, LAG oder VLAN angewandt werden, indem das Markierungskästchen aktiviert wird und die entsprechende Optionsschaltfläche und Schnittstelle ausgewählt werden.

 **ANMERKUNG:** Bei Zuweisung des Zugriffsprofils zu einer Schnittstelle wird der Zugriff über andere Schnittstellen verwehrt. Wenn keiner Schnittstelle ein Zugriffsprofil zugewiesen wird, ist der Gerätezugang von allen Schnittstellen möglich.

**Source IP Address** (IP-Quelladresse) — Gibt die IP-Quelladresse der Schnittstelle an, für die die Regel gilt. Dieses Feld ist optional und zeigt an, dass die Regel für ein Subnetzwerk gültig ist.



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


**Prefix Length** (Präfixlänge) — Gibt die Anzahl der Bits an, die das IP-Quelladress-Präfix enthält, oder die Netzwerkmaske der IP-Quelladresse.

**Action** — Legt fest, ob der angegebenen Schnittstelle Verwaltungszugriff gewährt oder verwehrt werden soll.

3. Definieren Sie das Feld **Access Profile Name**.
4. Definieren Sie die relevanten Felder.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das neue Zugriffsprofil wird hinzugefügt und das Gerät wird aktualisiert.

### Hinzufügen von Regeln zu Zugriffsprofilen:

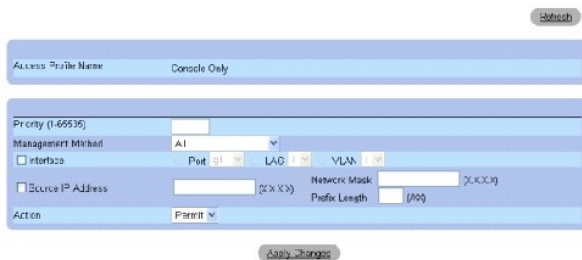
 **ANMERKUNG:** Die erste Regel muss definiert werden, damit der Datenverkehr mit Zugriffsprofilen abgeglichen werden kann.

1. Öffnen Sie die Seite **Access Profiles** (Zugriffsprofile).
2. Klicken Sie auf **Add Profile to Rule** (Profil der Regel hinzufügen).

Die Seite **Add An Access Profile Rule** (Eine Regel zum Zugriffsprofil hinzufügen) wird geöffnet:

**Abb. 6-53. Hinzufügen einer Regel zum Zugriffsprofil**


Add an Access Profile Rule



3. Geben Sie die Informationen in den Feldern ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Regel wird zum Zugriffsprofil hinzugefügt und das Gerät wird aktualisiert.

### Anzeigen der Profilregeln-Tabelle:

 **ANMERKUNG:** Die Reihenfolge, in der Regeln in der Profile Rules Table (Profilregeln-Tabelle) 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** (Zugriffsprofile).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die Seite **Profile Rules Table** (Profilregeln-Tabelle) wird geöffnet:

**Abb. 6-54. Profilregeln-Tabelle**



## Entfernen einer Regel

1. Öffnen Sie die Seite **Access Profiles** (Zugriffsprofile).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die Seite **Profile Rules Table** (Profilregeln-Tabelle) wird geöffnet.

3. Wählen Sie eine Regel.
4. Wählen Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die ausgewählte Regel wird gelöscht und das Gerät wird aktualisiert.

## Definieren der Zugriffsprofile mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [Access Profiles](#) (Zugriffsprofile) angezeigt werden.

Tabelle 6-35. CLI-Befehle für Zugriffsprofile

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

Das folgende Beispiel illustriert die CLI-Befehle:

```

Console (config)#
management access-list
m1ist

Console (config-macl)#
permit ethernet g1

Console (config-macl)#
permit ethernet g9

Console (config-macl)#
deny ethernet g2

```

```
Console (config-macl)#
deny ethernet g10

Console (config-macl)#
exit

Console (config)#
management access-class
m1ist

Console(config)# exit

Console# show management
access-list

m1ist

-----

permit ethernet g1

permit ethernet g9

! (Note: all other access
implicitly denied)

Console> show management
access-class

Management access-class is
enabled, using access list
m1ist
```

## Definieren von Authentifizierungsprofilen

Die Seite [Authentication Profiles](#) (Authentifizierungsprofile) enthält Felder für die Auswahl der Benutzer-Authentifizierungsmethode für das Gerät. Die Benutzer-Authentifizierung erfolgt:

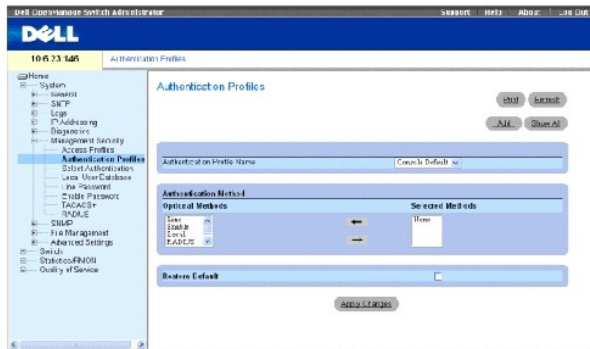
- 1 Lokal
- 1 Über einen externen Server

Außerdem kann die Benutzer-Authentifizierung auf None (Keine) gesetzt werden.

Die Benutzer-Authentifizierung 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 Authentifizierung ein Fehler auftritt, wird die nächste ausgewählte Methode verwendet. Öffnen Sie die Seite [Authentication Profiles](#), indem Sie auf System→ Management Security→ Authentication Profiles in der Strukturansicht klicken.

**Abb. 6-55. Authentifizierungsprofile**



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

**Optional Methods** (Optionale Methoden) — Listet die Benutzer-Authentifizierungsmethoden auf. Die möglichen Optionen lauten:

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

**Local** (Lokal) — Gibt an, dass die Benutzerauthentifizierung auf der Geräteebene erfolgt. Das Gerät überprüft den Benutzernamen und das Kennwort zur Authentifizierung.

**RADIUS** — Gibt an, dass die Benutzer-Authentifizierung auf dem RADIUS-Server erfolgt. Weitere Informationen finden Sie unter [„Konfigurieren von globalen RADIUS-Parametern“](#).

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

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

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

**Restore Default** (Standard wiederherstellen) — Stellt die Standardmethode zur Benutzer-Authentifizierung auf dem Gerät wieder her.

### Auswählen eines Authentifizierungsprofils:

1. Öffnen Sie die Seite [Authentication Profiles](#) (Authentifizierungsprofile).
2. Wählen Sie ein Profil im Feld **Authentication Profile Name** (Authentifizierungsprofilname) aus.
3. Wählen Sie eine Authentifizierungsmethode mit den Navigationspfeilen aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das Benutzer-Authentifizierungsprofil für das Gerät wird aktualisiert.

### Hinzufügen eines Authentifizierungsprofils:

1. Öffnen Sie die Seite [Authentication Profiles](#) (Authentifizierungsprofile).
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite **Add Authentication Method Profile Name** (Profilname für Authentifizierungsmethode hinzufügen) wird geöffnet:

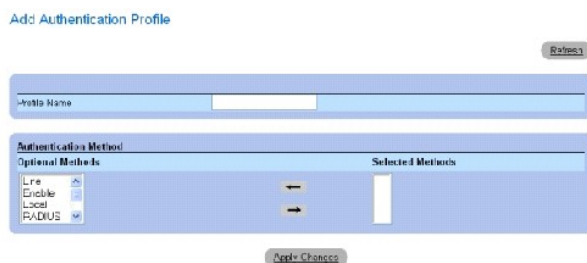


Abb. 6-56.

### Hinzufügen eines Authentifizierungsprofils

3. Konfigurieren Sie das Profil.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das Authentifizierungsprofil für das Gerät wird aktualisiert.

### Anzeigen der Seite „Show All Authentication Profiles“ (Alle Authentifizierungsprofile anzeigen):

1. Öffnen Sie die Seite [Authentication Profiles](#) (Authentifizierungsprofile).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die Seite **Authentication Profile** (Authentifizierungsprofil) wird geöffnet:

Abb. 6-57. Authentifizierungsprofile



### Löschen eines Authentifizierungsprofils:

1. Öffnen Sie die Seite [Authentication Profiles](#) (Authentifizierungsprofile).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die Seite **Authentication Profile** wird geöffnet.

3. Wählen Sie ein Authentifizierungsprofil.
4. Wählen Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das ausgewählte Authentifizierungsprofil wird gelöscht.

### Konfigurieren eines Authentifizierungsprofils mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [Authentication Profiles](#) angezeigt werden.

Tabelle 6-36. CLI-Befehle für Authentifizierungsprofile

CLI-Befehl	Beschreibung
aaa authentication login {default   list-name} method1 [method2.]	Konfiguriert die Anmeldungs-Authentifizierung.

no aaa authentication login { default | list-name } Entfernt ein Anmeldungs-Authentifizierungsprofil.

Das folgende Beispiel illustriert die CLI-Befehle:

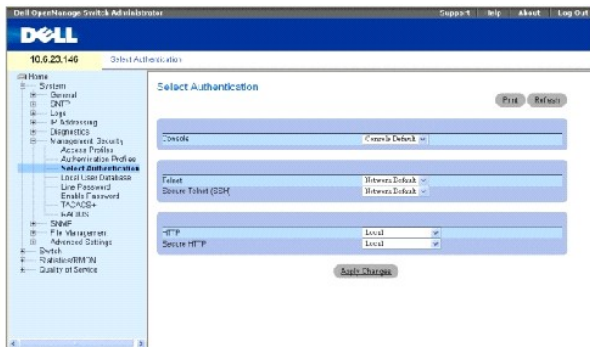
```
Console (config)# aaa
authentication login
default radius local
enable none

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

## Zuweisen von Authentifizierungsprofilen

Nach der Definition der Authentifizierungsprofile können diese auf Verwaltungszugriffsmethoden angewendet werden. Beispielsweise können Konsolenbenutzer durch Authentifizierungsmethodenliste 1 und Telnet-Benutzer durch Authentifizierungsmethodenliste 2 authentisiert werden. Öffnen Sie die Seite [Select Authentication](#) (Authentifizierung auswählen), indem Sie auf System → Management Security → Select Authentication in der Strukturansicht klicken.

Abb. 6-58. Auswählen einer Authentifizierung



**Console** — Zeigt die zur Authentifizierung von Konsolenbenutzern verwendeten Authentifizierungsprofile an.

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

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

**HTTP and Secure HTTP** — Zeigt die jeweils für den HTTP-Zugriff und sicheren HTTP-Zugriff verwendeten Authentifizierungsmethoden an. Folgende Feldwerte können ausgewählt werden:

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

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

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

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

## Anwenden einer Authentifizierungsliste auf Konsolensitzungen

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

Konsolensitzungen wird eine Authentifizierungsliste zugewiesen.

## Anwenden eines Authentifizierungsprofils auf Telnet-Sitzungen

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

Telnet-Sitzungen wird eine Authentifizierungsliste zugewiesen.

## Anwenden eines Authentifizierungsprofils auf Secure Telnet- (SSH-)Sitzungen:

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

Secure Telnet-(SSH-)Sitzungen wird ein Authentifizierungsprofil zugewiesen.

## Zuweisen einer Authentifizierungssequenz zu HTTP-Sitzungen

1. Öffnen Sie die Seite [Select Authentication](#) (Authentifizierung auswählen).
2. Wählen Sie eine Authentifizierungssequenz im Feld **HTTP**.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

HTTP-Sitzungen wird eine Authentifizierungssequenz zugewiesen.

## Zuweisen einer Authentifizierungssequenz zu Secure HTTP-Sitzungen

1. Öffnen Sie die Seite [Select Authentication](#) (Authentifizierung auswählen).
2. Wählen Sie eine Authentifizierungssequenz im Feld **Secure HTTP**.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Secure HTTP-Sitzungen wird eine Authentifizierungssequenz zugewiesen.

## Zuweisen von Zugriffs-Authentifizierungsprofilen oder -sequenzen mit den CLI -Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [Select Authentication](#) angezeigt werden.

Tabelle 6-37. CLI -Befehle für die Auswahl der Authentifizierung

CLI -Befehl	Beschreibung
enable authentication [default   list-name]	Legt die Authentifizierungsmethodenliste für Zugriffe auf eine höhere Berechtigungsebene über eine Remote-Telnet- oder -Konsolensitzung fest.
login authentication [default   list-name]	Legt die Liste der Anmeldungs-Authentifizierungsmethoden für eine Remote-Telnet- oder -Konsolensitzung fest.
ip http authentication method1	Legt die Authentifizierungsmethoden für HTTP-Server fest.

[method2.]	
ip https authentication method1 [method2.]	Legt die Authentifizierungsmethoden für HTTPS-Server fest.
show authentication methods	Zeigt Informationen zu den Authentifizierungsmethoden an.

Das folgende Beispiel illustriert 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
```

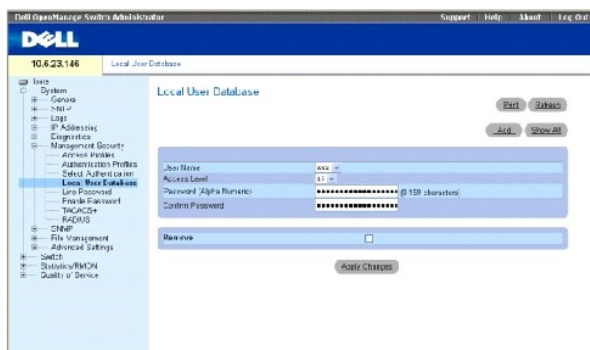
```
HTTPS: Radius, local
```

```
Dot1x: Radius
```

## Definieren der lokalen Benutzerdatenbanken

Die Seite [Local User Database](#) (Lokale Benutzerdatenbank) enthält Felder zur Definition von Benutzern, Kennwörtern und Zugriffsebenen. Öffnen Sie die Seite [Local User Database](#) (Lokale Benutzerdatenbank), indem Sie auf System > Management Security > Local User Database in der Strukturansicht klicken.

Abb. 6-59. Lokale Benutzerdatenbank



User Name (Benutzername) — Enthält eine Benutzerliste.

**Access Level** (Zugriffsebene) — Legt die Zugriffsebene für Benutzer fest. 1 steht für die niedrigste und 15 für die höchste Benutzerzugriffsebene.

**Password** (Kennwort) (0-159 Zeichen) — Legt das Benutzerkennwort fest. Kennwörter für lokale Benutzerdatenbanken können max. 159 Zeichen umfassen.

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

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

### Zuweisen von Zugriffsrechten zu einem Benutzer:

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

Die Benutzerzugriffsrechte und Kennwörter werden definiert und das Gerät aktualisiert.

### Definieren eines neuen Benutzers:

1. Öffnen Sie die Seite [Local User Database](#) (Lokale Benutzerdatenbank).
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite **Add User** (Benutzer hinzufügen) wird geöffnet:

#### Abb. 6-60. Hinzufügen von Benutzern

Attribute	Value
User Name (Alpha Numeric)	<input type="text"/> 1: 23 characters
Access Level (1-15)	1
Password (Alpha Numeric)	<input type="text"/> 0-159 characters
Confirm Password	<input type="text"/>

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

Der neue Benutzer wird definiert und das Gerät wird aktualisiert.

### Anzeigen der lokalen Benutzertabelle:

1. Öffnen Sie die Seite [Local User Database](#) (Lokale Datenbank).
2. Klicken Sie auf **Show All** (Alles anzeigen).

The Local User Table (Lokale Benutzertabelle) wird geöffnet:

#### Abb. 6-61. Lokale Benutzer-Tabelle



### Löschen von Benutzern:

1. Öffnen Sie die Seite [Local User Database](#) (Lokale Benutzerdatenbank).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die **Local User Table** (Lokale Benutzer-Tabelle) wird geöffnet.

3. Wählen Sie einen **User Name** (Benutzernamen).
4. Wählen Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der ausgewählte Benutzer wird gelöscht und das Gerät wird aktualisiert.

### Zuweisen von Benutzern mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [Local User Database](#) (Lokale Benutzerdatenbank) angezeigt werden.

Tabelle 6-38. CLI-Befehle für Datenbank der lokalen Benutzer

CLI-Befehl	Beschreibung
username name [password password] [level level] [encrypted]	Richtet ein auf Benutzernamen basierendes Authentifizierungssystem ein.

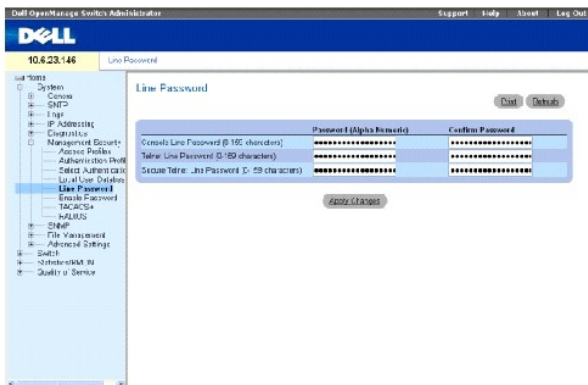
Das folgende Beispiel illustriert die CLI-Befehle:

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

### Definieren von Leitungskennwörtern

Die Seite [Line Password](#) (Leitungskennwort) enthält Felder zur Definition von Leitungskennwörtern für Verwaltungsmethoden. Öffnen Sie die Seite [Line Password](#), indem Sie auf System → Management Security → Line Passwords in der Strukturansicht klicken.

Abb. 6-62. Leitungskennwort



**Line Password for Console/Telnet/Secure Telnet** (Leitungskennwort für Konsole/Telnet/Secure Telnet) (0-159 Zeichen) — Gibt das Leitungskennwort für den Gerätezugriff über eine Konsolen-, Telnet- oder Secure Telnet-Sitzung an. Das Kennwort kann maximal 159 Zeichen enthalten.

**Confirm Password** (Kennwort bestätigen) — Bestätigt das neue Leitungskennwort. Das Kennwort wird als \*\*\*\*\* angezeigt.

### Definieren von Leitungskennwörtern für Konsolensitzungen

1. Öffnen Sie die Seite [Line Password](#) (Leitungskennwort).
2. Definieren Sie das Feld **Line Password for Console** (Leitungskennwort für Konsole).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das Leitungskennwort für Konsolensitzungen wird definiert und das Gerät aktualisiert.

### Definieren von Leitungskennwörtern für Telnet-Sitzungen

1. Öffnen Sie die Seite [Line Password](#) (Leitungskennwort).
2. # Definieren Sie das Feld „Line Password for Telnet“ (Leitungskennwort für Telnet).
3. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen).

Das Leitungskennwort für Telnet-Sitzungen wird definiert und das Gerät aktualisiert.

### Definieren von Leitungskennwörtern für Secure Telnet-Sitzungen

1. Öffnen Sie die Seite [Line Password](#) (Leitungskennwort).
2. Definieren Sie das Feld **Line Password for Secure Telnet** (Leitungskennwort für Secure Telnet).
3. Klicken Sie auf „Apply Changes“ (Änderungen übernehmen).

Das Leitungskennwort für Secure Telnet-Sitzungen wird definiert und das Gerät aktualisiert.

### Zuweisen von Leitungskennwörtern mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [Line Password](#) (Leitungskennwort) angezeigt werden.

Tabelle 6-39. CLI - Befehle für Leitungskennwort

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

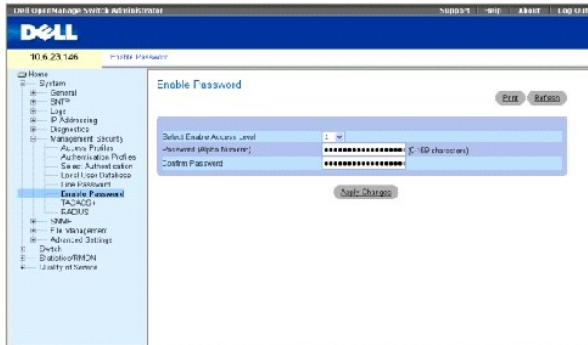
Das folgende Beispiel illustriert die CLI-Befehle:

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

### Definieren von Aktivierungskennwörtern

Auf der Seite [Modify Enable Password](#) (Ändern von Aktivierungskennwort) wird ein lokales Kennwort festgelegt, um den Zugriff auf den normalen, privilegierten und globalen Konfigurationsmodus zu steuern. Öffnen Sie die Seite [Modify Enable Password](#) (Ändern von Aktivierungskennwort), indem Sie auf System → Management Security → Enable Passwords in der Strukturansicht klicken.

**Abb. 6-63. Ändern eines Aktivierungskennworts:**



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

**Password** (Kennwort) (0-159 Zeichen) — Gibt das gegenwärtig konfigurierte Aktivierungskennwort an. Das Aktivierungskennwort kann maximal 159 Zeichen enthalten.

**Confirm Password** (Kennwort bestätigen) — Bestätigt das neue Aktivierungskennwort. Das Kennwort wird als \*\*\*\*\* angezeigt.

### Definieren eines neuen Aktivierungskennworts:

1. Öffnen Sie die Seite [Modify Enable Password](#) (Ändern des Aktivierungskennworts).
2. Definieren Sie die entsprechenden Felder.
3. Klicken Sie auf Apply Changes (Änderungen übernehmen.)

Das neue Aktivierungskennwort wird definiert und das Gerät aktualisiert.

### Zuweisen von Aktivierungskennwörtern mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [Modify Enable Password](#) (Ändern des Aktivierungskennworts) angezeigt werden.

Tabelle 6-40. CLI-Befehle für Ändern des Aktivierungskennwortes

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

Das folgende Beispiel illustriert die CLI-Befehle:

```

Console (config)# enable
password level 15 secret

Console# show users
accounts

Username Privilege
-----

```

## Definition der TACACS+-Einstellungen

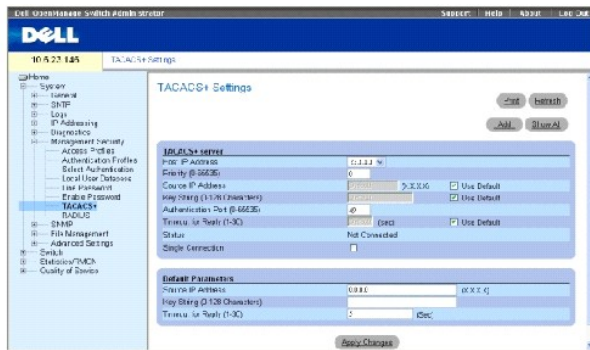
Die Geräte stellen Terminal Access Controller Access Control System (TACACS+)-Client-Support bereit. TACACS+ stellt eine zentralisierte Sicherheit zur Validierung von Benutzern, die auf das Gerät zugreifen, dar.

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

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

Das TACACS+-Protokoll stellt die Netzwerkintegrität mittels verschlüsselter Protokollaustausche zwischen dem Gerät und dem TACACS+-Server sicher. Öffnen Sie die Seite [TACACS+ Settings](#) (TACACS+-Einstellungen), indem Sie auf **System**→**Management Security**→**TACACS+** in der Strukturansicht klicken.

Abb. 6-64. TACACS+-Einstellungen



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

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

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

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

Authentication Port (0-65535) — Die Anschlussnummer, über die die TACACS+-Sitzung erfolgt. Port 49 ist der Standardanschluss.

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

Status — Der Verbindungsstatus zwischen dem Gerät und dem TACACS+-Server. Folgende Feldwerte können ausgewählt werden:

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

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

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

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

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

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

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

## Hinzufügen eines TACACS+-Servers

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

Die Seite [Add TACACS+ Host](#) (TACACS+-Host hinzufügen) wird geöffnet:

**Abb. 6-65. Hinzufügen eines TACACS+-Hosts**

Host IP Address	<input type="text"/>	(0-255.255.255)
Priority (0-25535)	<input type="text"/>	
Source IP Address	<input type="text"/>	(0-255.255.255) <input type="checkbox"/> Use Default
Key String (0-128 Characters)	<input type="text"/>	<input type="checkbox"/> Use Default
Authent Level (0-25535)	<input type="text"/>	
Timeout for Reply (1-30)	<input type="text"/>	(0-30) <input type="checkbox"/> Use Default
Single Connection	<input type="checkbox"/>	

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

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

## Anzeigen der TACACS+-Tabelle

1. Öffnen Sie die Seite [TACACS+ Settings](#) (TACACS+-Einstellungen).
2. Klicken Sie auf Show All (Alles anzeigen).

Die Seite [TACACS+ Table](#) (TACACS+-Tabelle) wird geöffnet:

**Abb. 6-66. TACACS+-Tabelle**

## TACACS+ Table

Host IP Address	Priority	Source IP Address	Authentication Port	Timeout for Reply	Single Connection	Status	Remove
1 23.1.1.1	0	Default	40	Default	<input type="checkbox"/>	Not Connected	<input type="checkbox"/>

## Entfernen eines TACACS+-Servers

1. Öffnen Sie die Seite [TACACS+ Settings](#) (TACACS+-Einstellungen).
2. Klicken Sie auf Show All (Alles anzeigen).

Die Seite [TACACS+ Table](#) (TACACS+-Tabelle) wird geöffnet.

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

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

## Definieren der TACACS+-Einstellungen mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [TACACS+ Settings](#) (TACACS+-Einstellungen) angezeigt werden.

Tabelle 6-41. CLI-Befehle für TACACS+

CLI-Befehl	Beschreibung
<b>TACACS-server host</b> ( <i>ip-address</i>   <i>hostname</i> ) [ <b>single-connection</b> ] [ <b>port</b> <i>port-number</i> ] [ <b>timeout</b> <i>timeout</i> ] [ <b>key</b> <i>key-string</i> ] [ <b>source</b> <i>source</i> ] [ <b>priority</b> <i>priority</i> ]	Gibt einen TACACS+-Host an.
<b>no TACACS-server host</b> ( <i>ip-address</i>   <i>hostname</i> )	Löscht einen TACACS+-Host.
<b>tacacs-server key</b> <i>key-string</i>	Legt den Authentifizierungs- und Verschlüsselungscode für die gesamte TACACS+-Kommunikation zwischen dem Gerät und dem TACACS+-Server fest. Dieser Schlüssel muss mit der auf dem TACACS+-Daemon verwendeten Verschlüsselung übereinstimmen. (Bereich: 0 - 128 Zeichen.)
<b>tacacs-server timeout</b> <i>timeout</i>	Gibt den Zeitlimit-Wert in Sekunden an. (Bereich: 1 - 30.)
<b>tacacs-server source-ip</b> <i>source</i>	Gibt eine IP-Quelladresse an. (Bereich: Gültige IP-Adresse.)
<b>show TACACS</b> [ <i>ip-address</i> ]	Zeigt die Konfiguration und Statistiken für einen TACACS+-Server an.

Das folgende Beispiel illustriert die CLI-Befehle:

Console# <b>show tacacs</b>						
Router Configuration						
-----	-----	-----	-----	-----	-----	-----
-	-	-	-	-	-	-
IP- Address:	Status	Port	Single	TimeOut	Source IP	Priority



		Connection			
-----	-----	---	-----	-----	-----
-		-	-	-	-
12.1.1.2	Not  Connected	49	Yes	1	12.1.1.1 1
Global values					
-----					
TimeOut :					
5					
Router Configuration					
-----					
Source IP : 0.0.0.0					
console#					

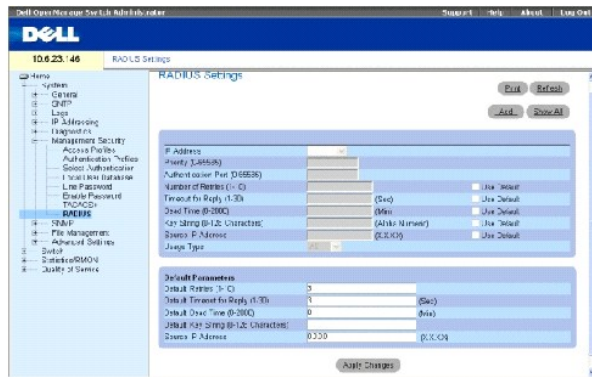
## Konfigurieren globaler RADIUS-Parameter

Remote Authorization Dial-In User Service (RADIUS)-Server (Server mit Anwahl-Benutzer-Service für Remote-Authorisierung) stellen zusätzliche Sicherheit für Netzwerke bereit. RADIUS-Server stellen eine zentralisierte Authentifizierungsmethode für folgende Zugriffsarten bereit:

- 1 Telnet-Zugriff
- 1 Webzugriff
- 1 Konsolenzugriff auf Geräte

Öffnen Sie die Seite [„RADIUS Settings“](#) (RADIUS-Einstellungen), indem Sie auf System → Management Security → RADIUS in der Strukturansicht klicken.

**Abb. 6-67. RADIUS-Einstellungen**



**IP Address** — Gibt die Liste der IP-Adressen für Authentifizierungsserver an.

**Priority (1-65535) ((Priorität) (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. Diese Angabe wird zur Konfiguration der Reihenfolge, in der die Server abgefragt werden, verwendet.

**Authentication Port** — Gibt den Authentifizierungs-Port an. Der Authentifizierungs-Port wird zur Überprüfung der RADIUS-Server-Authentifikation verwendet.

**Number of Retries (1-10) ((Anzahl der Versuche) (1-10))** — Gibt die Anzahl der Anforderungen an, die an den RADIUS-Server gesendet werden können, bevor ein Fehler auftritt. Die möglichen Feldwerte sind 1 - 10. Der Standardwert ist 3.

**Timeout for Reply (1-30) ((Antwort-Zeitlimit) (1-30))** — 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. Die möglichen Feldwerte sind 1 - 30. Der Standardwert ist 3.

**Dead Time (0-2000) ((Besetzzeit, 0-2000))** — Gibt die Zeit (in Sekunden) an, während der ein RADIUS-Server für Dienstanforderungen umgangen wird. Der Bereich ist 0-2000.

**Key String (Schlüssel-Zeichenkette) (1-128 Zeichen)** — Gibt die Schlüsselzeichenkette an, die für die Authentifizierung und Verschlüsselung der gesamten RADIUS-Kommunikation zwischen Gerät und RADIUS-Server verwendet wird. Dieser Schlüssel ist verschlüsselt.

**Source IP Address (IP-Quelladresse)** — Gibt die IP-Quelladresse an, die für das Gerät, das auf den RADIUS-Server zugreift, verwendet wird.

Durch die folgenden Felder werden die RADIUS-Standardwerte festgelegt:

**Default Timeout for Reply (1-30) (Standard-Antwort-Zeitlimit (1-30))** — Gibt das Standardzeitintervall (in Sekunden) an, das ein Gerät auf eine Antwort vom RADIUS-Server wartet, bevor das Zeitlimit erreicht ist.

**ANMERKUNG:** Falls für host-spezifische Timeouts, Retries oder Dead Time keine Werte angegeben sind, werden die globalen (Standard-) Werte auf die einzelnen Hosts angewendet.

**Number of Retries (1-10) (Anzahl von Versuchen (1-10))** — Gibt die Anzahl der Anforderungen an, die an den RADIUS-Server gesendet werden können, bevor ein Fehler auftritt.

**Default Dead time (0-2000) (Standard-Besetzzeit (0-2000))** — Gibt die Zeit (in Sekunden) an, während der ein RADIUS-Server für Dienstanforderungen umgangen wird. Der Bereich ist 0-2000.

**Default Key String (Standard-Schlüssel-Zeichenkette) (1-128 Zeichen)** — Gibt die Schlüsselzeichenfolge an, die für die Authentifizierung und Verschlüsselung der gesamten RADIUS-Kommunikation zwischen Gerät und RADIUS-Server verwendet wird. Dieser Schlüssel ist verschlüsselt.

**Source IP Address (IP-Quelladresse)** — Gibt die IP-Quelladresse an, die für das Gerät, das auf den RADIUS-Server zugreift, verwendet wird.

Usage Type (Verwendungsart) — Gibt die Server-Verwendungsart an. Mögliche Werte sind: login, 802.1x oder all. Wenn keine Angabe gemacht wurde, wird „alle“ als Standardwert angenommen.

### Definieren von RADIUS-Parametern:

1. Öffnen Sie die Seite [RADIUS Settings](#) (RADIUS-Einstellungen).
2. Definieren Sie die Felder.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die RADIUS-Einstellungen werden auf dem Gerät aktualisiert.

### Hinzufügen eines RADIUS-Servers

1. Öffnen Sie die Seite [RADIUS Settings](#) (RADIUS-Einstellungen).
2. Klicken Sie auf Add (Hinzufügen).

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

Abb. 6-68. Hinzufügen eines RADIUS-Servers

IP Address	<input type="text"/>	(0.X.X.X)
Priority (0-65535)	<input type="text" value="0"/>	
Authentication Port (0-65535)	<input type="text" value="1812"/>	
Number of Retries (1-10)	<input type="text" value="3"/>	<input checked="" type="checkbox"/> Use Default
Timeout for Reply (1-30)	<input type="text" value="5"/>	<input checked="" type="checkbox"/> Use Default
Dead time (0-200)	<input type="text" value="0"/>	<input checked="" type="checkbox"/> Use Default
Key String (0-120 Characters)	<input type="text" value="alpha numeric"/>	<input checked="" type="checkbox"/> Use Default
Source IP Address	<input type="text" value="0.0.0.0"/>	<input checked="" type="checkbox"/> Use Default
Usage Type	<input type="text" value="All"/>	

**Apply Changes**

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

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

### Anzeigen der RADIUS-Server-Liste:

1. Öffnen Sie die Seite [RADIUS Settings](#) (RADIUS-Einstellungen).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die Seite [Show all RADIUS Servers](#) (Alle RADIUS-Servers anzeigen) wird geöffnet:

Abb. 6-69. Anzeigen aller RADIUS-Server

IP Address	Priority	Authentication Port	Number of Retries	Timeout for Reply	Dead Time	Source IP Address	Usage Type	Remove
------------	----------	---------------------	-------------------	-------------------	-----------	-------------------	------------	--------

**Apply Changes**

### Ändern der RADIUS-Servereinstellungen:

1. Öffnen Sie die Seite [RADIUS Settings](#) (RADIUS-Einstellungen).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die Seite **RADIUS Servers List** (RADIUS-Server-Liste) wird geöffnet.

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

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

### Löschen eines RADIUS-Servers aus der RADIUS-Server-Liste:

1. Öffnen Sie die Seite [RADIUS Settings](#) (RADIUS-Einstellungen).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die Seite **RADIUS Servers List** (RADIUS-Server-Liste) wird geöffnet.

3. Wählen Sie einen RADIUS-Server in der **RADIUS Servers List**.
4. Wählen Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der RADIUS-Server wird aus der **RADIUS Servers List** entfernt.

### Definieren der RADIUS-Servereinstellungen mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [RADIUS Settings](#) (RADIUS-Einstellungen) angezeigt werden.

Tabelle 6-42. CLI-Befehle für RADIUS-Einstellungen

CLI-Befehl	Beschreibung
radius-server timeout timeout	Legt das Standardintervall fest, während dessen ein Gerät auf die Antwort eines Server-Hosts wartet.
radius-server retransmit retries	Legt fest, wie häufig die Liste der RADIUS-Server-Hosts standardmäßig von der Software durchsucht wird.
radius-server deadtime deadtime	Legt fest, dass nicht verfügbare Standardserver übersprungen werden.
radius-server key [key-string]	Legt den Standardschlüssel für die Authentifizierung und Verschlüsselung der gesamten RADIUS-Kommunikation zwischen dem Gerät und der RADIUS-Umgebung fest.
radius-server host { ip-address   hostname} [auth-port auth-port-number] [timeout timeout] [retransmit retries] [deadtime deadtime] [key key-string] [source source] [priority priority] [usage type]	Legt einen RADIUS-Server-Host sowie beliebige Einstellungen fest, die nicht den Standardeinstellungen entsprechen.
show radius-servers	Zeigt die RADIUS-Servereinstellungen an.

Das folgende Beispiel illustriert 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	Source IP	Priority	Verwendung
-----	----	----	-----	-----	-----	-----	-----	-----
33.1.1.1	1812	1813	6	4	10	0.0.0.0 (Versant- Produktversion: 6.0.0.1)	0	All
172.16.1.2	1645	1646	11	8	Global	Global	2	All

```

Global values
-----

TimeOut: 5

Retransmit: 5

Deadtime: 10

Source IP: 0.0.0.0 (Versant-Produktversion: 6.0.0.1)

```

## Definieren von SNMP-Parametern

Simple Network Management Protocol (SNMP) stellt ein Verfahren zur Verwaltung von Netzwerkgeräten bereit. Geräte, die SNMP unterstützen, führen eine lokale Software (Agent) aus.

Die SNMP-Agenten führen eine Liste von Variablen, die zur Verwaltung des Geräts dienen. Die Variablen werden in der Management Information Base (MIB) definiert. Die MIB enthält die vom Agenten gesteuerten Variablen. Das SNMP-Protokoll definiert das MIB-Spezifikationsformat sowie das Format, das zum Zugriff auf die Informationen über das Netzwerk verwendet wird.

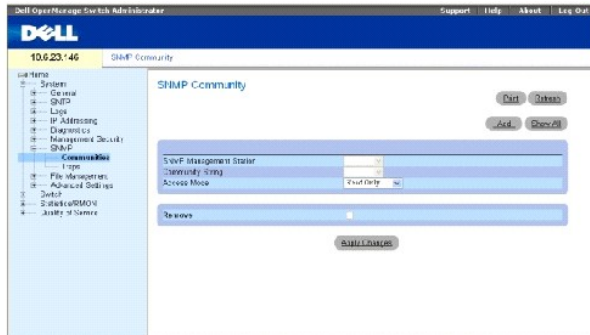
Die Zugriffsrechte für die SNMP-Agenten werden durch Zugriffs-Zeichenfolgen geregelt. Zur Kommunikation mit dem Gerät präsentiert der Embedded-Web-Server eine gültige Communityzeichenfolge zur Authentifizierung. Öffnen Sie die Seite SNMP, indem Sie auf System → SNMP in der Strukturansicht klicken.

Dieser Abschnitt enthält Informationen zur Verwaltung der SNMP-Konfiguration.

## Definieren von Communities

Zugriffsrechte werden durch Definieren von Communities in der **Community Table** (Community-Tabelle) verwaltet. Sobald der Name einer Community geändert wird, ändern sich auch die Zugriffsrechte. Öffnen Sie die Seite [SNMP Community](#), indem Sie auf System → SNMP → Communities in der Strukturansicht klicken.

Abb. 6-70. SNMP-Community



SNMP Management Station — Enthält eine Liste mit IP-Adressen von Management-Stationen.

Community String (Community-Zeichenkette) — Hat die Funktion eines Passworts und wird zur Authentifizierung der ausgewählten Management-Station gegenüber dem Gerät verwendet.

Access Mode (Zugriffsmodus) — Definiert die Zugriffsrechte der Community. Folgende Feldwerte können ausgewählt werden:

**Read Only** (Nur Lesezugriff) — Gibt an, dass sich der Verwaltungszugriff auf Lesezugriffe beschränkt, und zwar für alle MIBs außer der Community-Tabelle, auf die nicht zugegriffen werden kann.

**Read Write** (Lese- und Schreibzugriff) — Gibt an, dass Verwaltungszugriffe in Form von Lese- und Schreibzugriffen möglich sind und zwar für alle MIBs außer der Community-Tabelle, auf die nicht zugegriffen werden kann.

**SNMP Admin** (SNMP-Verwaltung) — Gibt an, dass der Benutzer Lese-Schreib-Zugriff auf sämtliche MIBs hat, einschließlich die Community-Tabelle.

Remove (Entfernen) — Entfernt, wenn ausgewählt, eine Community.

## Definieren einer neuen Community

1. Öffnen Sie die Seite [SNMP Community](#).
2. Klicken Sie auf Add (Hinzufügen).

Die Seite **Add SNMP Community** (SNMP-Community hinzufügen) wird geöffnet:

Add SNMP Community

Refresh

SNMP Management  Management Station   All (0.0.0.0)

Community String (1-20 Characters)

Access Mode

Apply Changes

Abb. 6-71. Hinzufügen einer SNMP-Community

3. Wählen Sie eine der folgenden Optionen aus:

**Management Station** — Definiert eine SNMP-Community für eine bestimmte Management-Station. (Der Wert 0.0.0.0 steht für sämtliche Management-Stationen.

**All** — Definiert eine SNMP-Community für alle Management-Stationen.

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

Die neue Community wird gespeichert und das Gerät wird aktualisiert.

### Anzeigen aller Communities

1. Öffnen Sie die Seite [SNMP Community](#).
2. Klicken Sie auf **Show All** (Alles anzeigen).

Die [Community Table](#) (Community-Tabelle) wird geöffnet:

Abb. 6-72. Community-Tabelle

Community Table

Refresh

Management Station	Community String	Access Mode	Remove

Apply Changes

### Löschen von Communities

1. Öffnen Sie die Seite [SNMP Community](#).
2. Klicken Sie auf Show All (Alles anzeigen).

Die [Community Table](#) (Community-Tabelle) wird geöffnet.

3. Wählen Sie eine Community aus [Community Table](#) (Community-Tabelle) aus.
4. Wählen Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die ausgewählte Community wird gelöscht und das Gerät wird aktualisiert.

### Konfigurieren von Communities mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [SNMP Community](#) angezeigt werden.

Tabelle 6-43. CLI-Befehle für SNMP-Community

---

CLI-Befehl	Beschreibung
snmp-server community string [ro   rw   su] [ip-address]	Konfiguriert die Community-Zugriffszeichenkette so, dass SNMP-Protokollzugriffe zulässig sind.
snmp-server host {ip-address   hostname} community-string [1   2]	Legt den an den ausgewählten Empfänger übertragenen Trap-Typ fest.
show snmp	Überprüft den Status der SNMP-Kommunikation.

Das folgende Beispiel illustriert die CLI-Befehle:

console(config)# snmp-server community public_1 su 1.1.1.1		
console(config)# snmp-server community public_2 rw 2.2.2.2		
console(config)# snmp-server community public_3 ro 3.3.3.3		
console(config)# snmp-server host 1.1.1.1 public_1 1		
console(config)# snmp-server host 2.2.2.2 public_2 2		
console(config)#		
console#		
show snmp		
Community-String	Community-Access	IP-Adresse:
-----		
-----		
-----		
public_1	super	1.1.1.1
public_2	readwrite	2.2.2.2
public_3	readonly	3.3.3.3
Traps are enabled.		
Authentication-failure trap is enabled.		
Trap-Rec-Address	Trap-Rec-Community	Version
-----	-----	-----
-----	-----	-
1.1.1.1	public_1	1
2.2.2.2	public_2	2

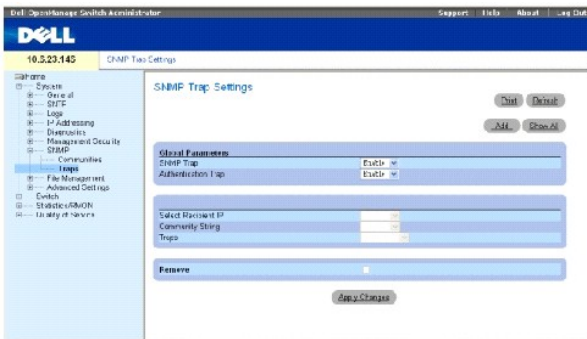


System Contact: 345 6789		
System Location: 1234 5678		
console#		

## Definieren von Traps

Über die Seite [SNMP Trap Settings](#) (Trap-Einstellungen) kann der Benutzer das Senden von SNMP-Traps oder -Benachrichtigungen durch das Gerät aktivieren oder deaktivieren. Öffnen Sie die Seite [SNMP Trap Settings](#) (SNMP-Trap-Einstellungen), indem Sie auf System → SNMP → Traps in der Strukturansicht klicken.

Abb. 6-73. SNMP-Trap-Einstellungen



**SNMP Trap** — Aktiviert das Senden von SNMP-Traps oder SNMP-Benachrichtigungen vom Gerät zu festgelegten Trap-Empfängern.

**Authentication Trap (Authentifizierungs-Trap)** — Aktiviert das Senden von SNMP-Traps, wenn festgelegte Empfänger nicht authentisiert werden können.

**Select Recipient IP (IP-Empfänger auswählen)** — Legt die IP-Adresse des Empfängers fest, an den die Traps gesendet werden.

**Community String (Community-Zeichenkette)** — Gibt die Community-Zeichenfolge des Trap Managers an.

**Traps** — Legt den an den ausgewählten Empfänger übertragene Trap-Typ fest. Folgende Feldwerte können ausgewählt werden:

**SNMP V1** — SNMP-Version-1-Traps werden übertragen

**SNMP V2** — SNMP-Version-2-Traps werden übertragen

**Remove (Entfernen)** — Entfernt, wenn ausgewählt, Einträge aus der **Trap Manager Table** (Trap-Verwalter-Tabelle).

## Aktivieren von SNMP-Traps für das Gerät

1. Öffnen Sie die Seite [SNMP Trap Settings](#) (SNMP-Trap-Einstellungen).
2. Wählen Sie **Enable** (Aktivieren) in der Dropdown-Liste **SNMP Trap**.
3. Definieren Sie die Felder.

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

Die SNMP-Traps werden für das Gerät aktiviert.

### Aktivieren von Authentifizierungs-Traps für das Gerät

1. Öffnen Sie die Seite [SNMP Trap Settings](#) (SNMP-Trap-Einstellungen).
2. Wählen Sie **Enable** (Aktivieren) in der Dropdown-Liste **Authentication Trap** (Authentifizierungs-Trap).
3. Definieren Sie die Felder.
4. Klicken Sie auf Apply Changes (Änderungen übernehmen).

Die Authentifizierungs-Traps werden für das Gerät aktiviert.

### Hinzufügen eines neuen Trap-Empfängers:

1. Öffnen Sie die Seite [SNMP Trap Settings](#) (SNMP-Trap-Einstellungen).
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite [Add Trap Receiver/Manager](#) (Trap-Empfänger/Manager hinzufügen) wird geöffnet:

**Abb. 6-74. Hinzufügen eines Trap-Empfängers/Managers**

Add Trap Recipient

Refresh

Recipient IP Address (0.0.0.0)

Community String (1-20 Characters)

Trap Enable SNMPV1

Apply Changes

3. Definieren Sie die Felder. 0.0.0.0 steht für „Alle“ und die Traps werden an alle Empfänger weitergeleitet (Broadcast). Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Trap-Empfänger/Manager wird hinzugefügt und das Gerät aktualisiert.

### Anzeigen der Trap-Managers-Tabelle:

Die Seite **Trap Managers Table** (Trap-Managers-Tabelle) enthält Felder zur Konfiguration von Trap-Typen.

1. Öffnen Sie die Seite [SNMP Trap Settings](#) (SNMP-Trap-Einstellungen).
2. Klicken Sie auf Show All (Alles anzeigen).

Die Seite [Trap Managers Table](#) (Trap-Managers-Tabelle) wird geöffnet:

**Abb. 6-75. Trap-Managers-Tabelle**

Trap Recipients Table

Refresh

Recipient IP	Trap	Community String	Remove
--------------	------	------------------	--------

Apply Changes

## Löschen eines Eintrags aus der Trap-Manager-Tabelle:

1. Öffnen Sie die Seite [SNMP Trap Settings](#) (SNMP-Trap-Einstellungen).
2. Klicken Sie auf Show All (Alles anzeigen).

Die Seite [Trap Managers Table](#) (Trap-Manager-Tabelle) wird geöffnet.

3. Wählen Sie einen Eintrag in der **Trap Managers Table**.
4. Wählen Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der ausgewählte Trap-Manager wird gelöscht und das Gerät aktualisiert.

## Konfigurieren von Traps mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [SNMP Trap Settings](#) (SNMP-Trap-Einstellungen) angezeigt werden.

Tabelle 6-44. CLI-Befehle für SNMP-Trap-Einstellungen

CLI-Befehl	Beschreibung
<code>snmp-server enable traps</code>	Aktiviert den Versand von SNMP-Traps oder SNMP-Benachrichtigungen durch das Gerät.
<code>snmp-server trap authentication</code>	Aktiviert den Versand von SNMP-Traps durch das Gerät, wenn die Authentifizierung fehlschlägt.
<code>snmp-server host host-addr community-string [1   2]</code>	Legt den Typ des an den ausgewählten Empfänger gesendeten Traps fest.
<code>show snmp</code>	Zeigt den SNMP-Kommunikationsstatus an.

Das folgende Beispiel illustriert die CLI-Befehle:

console(config)# snmp-server community public_1 su 1.1.1.1		
console(config)# snmp-server community public_2 rw 2.2.2.2		
console(config)# snmp-server community public_3 ro 3.3.3.3		
console(config)# snmp-server host 1.1.1.1 public_1 1		
console(config)# snmp-server host 2.2.2.2 public_2 2		
console(config)# snmp-server enable traps		
console(config)# snmp-server trap authentication		
console(config)#		
console#		
show snmp		

Community-String	Community-Access	IP-Adresse:
----- ----- -----		
public_1	super	1.1.1.1
public_2	readwrite	2.2.2.2
public_3	readonly	3.3.3.3
Traps are enabled.		
Authentication-failure trap is enabled.		
Trap-Rec-Address	Trap-Rec-Community	Version
----- -----	----- -----	----- -----
1.1.1.1	public_1	1
2.2.2.2	public_2	2
System Contact: 345 6789		
System Location: 1234 5678		
console#		

## Verwalten von Dateien

Die Seite „File Management“ (Dateiverwaltung) enthält Felder zur Verwaltung der Gerätesoftware, Image-Dateien und Konfigurationsdateien. Die Dateien können von einem TFTP-Server heruntergeladen werden.

## Übersicht über die Dateiverwaltung

Die Konfigurationsdateistruktur umfasst die folgenden Dateien:

- 1 Startup Configuration File (Startup-Konfigurationsdatei) — In dieser Datei sind alle Befehle gespeichert, die zur Neukonfiguration des Gerätes mit den gleichen Einstellungen erforderlich sind, wenn das Gerät ausgeschaltet oder neu gestartet wird. Die Startup-Datei wird erstellt, indem die Konfigurationsbefehle aus der Running-Konfigurationsdatei oder der Backup-Konfigurationsdatei kopiert werden.
- 1 Running Configuration File (Running-Konfigurationsdatei) — Enthält sämtliche Befehle aus der Startup-Konfigurationsdatei sowie alle während der aktuellen Sitzung eingegebenen Befehle. Nach Ausschalten oder Neustart des Geräts gehen alle Befehle, die in der Running-Konfigurationsdatei gespeichert sind, verloren. Während des Startvorgangs werden alle Befehle aus der Startup-Datei in die Running-Konfigurationsdatei kopiert und auf das Gerät angewendet. Während der Sitzung werden alle neu eingegebenen Befehle den in der Running-Konfigurationsdatei bereits enthaltenen Befehlen hinzugefügt. Befehle werden nicht überschrieben. Um die Startup-Konfigurationsdatei zu aktualisieren, muss die Running-Konfigurationsdatei in die Startup-Konfigurationsdatei kopiert werden, bevor das Gerät ausgeschaltet wird. Wenn das Gerät das nächste Mal neu gestartet wird, werden die

Befehle von der Startup-Konfigurationsdatei zurück in die Running-Konfigurationsdatei kopiert.

- 1 Backup Configuration File (Backup-Konfigurationsdatei)— Enthält eine Sicherungskopie der Gerätekonfiguration. Die Sicherungsdatei wird erzeugt, wenn die Running-Konfigurationsdatei oder die Startup-Datei in die Sicherungsdatei kopiert wird. Die in der Backup-Konfigurationsdatei enthaltenen Befehle werden durch die in die Datei kopierten Befehle ersetzt. Der Inhalt der Backup-Konfigurationsdatei kann sowohl in die Running-Konfigurationsdatei als auch in die Startup-Konfigurationsdatei kopiert werden.
- 1 Image files (Imagedateien) — 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.

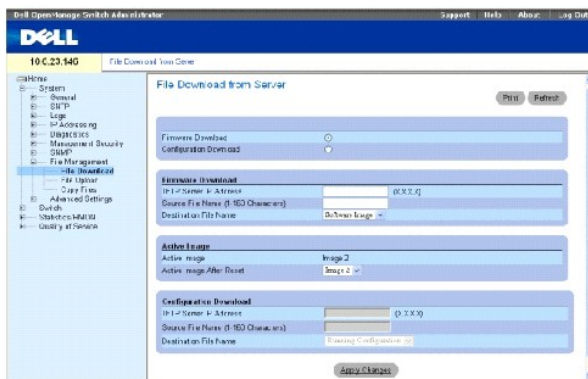
Öffnen Sie die Seite „File Management“, indem Sie auf System→ File Management in der Strukturansicht klicken. Die Seite „File Management“ (Dateiverwaltung) enthält Links zum:

- 1 Herunterladen von Dateien
- 1 Hochladen von Dateien
- 1 Kopieren von Dateien

## Herunterladen von Dateien

Die Seite [File Download From Server](#) (Herunterladen von Dateien vom Server) enthält Felder zum Herunterladen von Image- und Konfigurationsdateien vom TFTP-Server auf das Gerät. Öffnen Sie die Seite [File Download From Server](#) (Herunterladen von Dateien vom Server), indem Sie auf System → File Management → File Download in der Strukturansicht klicken.

Abb. 6-76. Herunterladen von Dateien vom Server



**Firmware Download** (Herunterladen von Firmware) — Gibt an, dass die Firmware-Datei heruntergeladen wird. Bei Auswahl von **Firmware Download** (Herunterladen von Firmware) werden die Felder unter **Configuration Download** (Herunterladen von Konfiguration) grau dargestellt.

**Configuration Download** (Herunterladen von Konfiguration) — Gibt an, dass die Konfigurationsdatei heruntergeladen wird. Bei Auswahl von **Configuration Download** (Herunterladen von Konfiguration) werden die Felder unter **Firmware Download** (Herunterladen von Firmware) grau dargestellt.

Firmware Download TFTP Server IP Address (TFTP-Server-IP-Adresse für das Herunterladen von Firmware) — Gibt die IP-Adresse des TFTP-Servers an, von dem die Dateien heruntergeladen werden.

Firmware Download Source File Name (Quelldateiname für das Herunterladen von Firmware) — Gibt die Datei an, die heruntergeladen werden soll.

Firmware Download **Destination File** (Zieldatei für das Herunterladen von Firmware) — Gibt den Typ der Zieldatei an, in die die Datei heruntergeladen wird. Folgende Feldwerte können ausgewählt werden:

**Software Image** — Lädt die Image-Datei herunter.

**Boot Code** (Startcode) — Lädt die Startdatei herunter.

Active Image (Aktives Image) — Die gegenwärtig aktive Image-Datei.

Active Image After Reset (Aktives Image nach Rücksetzung) — Gibt die Image-Datei an, die nach Rücksetzung des Geräts aktiv ist.

Configuration Download File TFTP Server IP Address (IP-Adresse des TFTP-Servers für Herunterladen von Konfiguration) — Gibt die IP-Adresse des TFTP-Servers an, von dem die Konfigurationsdateien heruntergeladen werden.

Configuration Download File Source File Name (Quelldateiname für herunterzuladende Konfigurationsdatei) — Legt die Konfigurationsdateien fest, die heruntergeladen werden.

Configuration Download File Destination (Ziel für herunterzuladende Konfigurationsdatei) — Gibt die Zieldatei an, in die die Konfigurationsdatei heruntergeladen wird. Folgende Feldwerte können ausgewählt werden:

**Running Configuration** (Running-Konfiguration) — Lädt Befehle in die Running-Konfiguration-Datei herunter.


**Startup Configuration** (Startup-Konfiguration) — Lädt die Startup-Konfiguration-Datei herunter und überschreibt die alte Datei.

**Backup Configuration** (Backup-Konfiguration) — Lädt die Backup-Konfiguration-Datei herunter und überschreibt die alte Datei.

### Herunterladen von Dateien:

1. Öffnen Sie die Seite [File Download From Server](#) (Herunterladen von Datei vom Server).
2. Definieren Sie den Typ der herunterzuladenden Datei.
3. Definieren Sie die Felder.
4. Klicken Sie auf Apply Changes (Änderungen übernehmen).

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 den CLI-Befehlen


In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [File Download From Server](#) (Herunterladen von Datei vom Server) angezeigt werden.

Tabelle 6-45. CLI-Befehle zum Herunterladen von Dateien

CLI-Befehl	Beschreibung
copy source-url destination-url [snmp]	Kopiert eine beliebige Datei von einem Quellort an einen Zielort.

Das folgende Beispiel illustriert 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: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```



**Backup Configuration** (Backup-Konfiguration) — Lädt die Backup-Konfiguration-Datei hoch

## Hochladen von Dateien

1. Öffnen Sie die Seite [File Upload to Server](#) (Hochladen von Dateien auf den Server).
2. Definieren Sie den Typ der hochzuladenden Datei.
3. Definieren Sie die Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Software wird auf das Gerät hochgeladen.

## Hochladen von Dateien mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [File Upload to Server](#) (Hochladen von Dateien auf den Server) angezeigt werden.

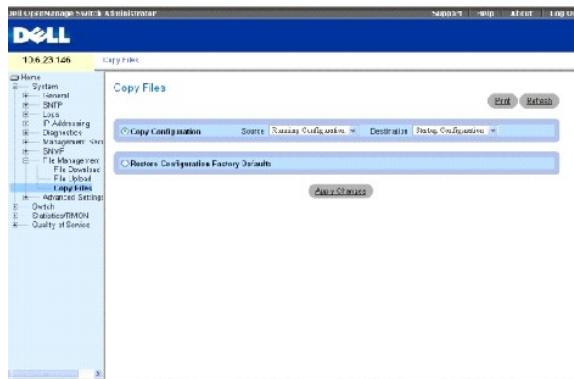
Tabelle 6-46. CLI-Befehle zum Hochladen von Dateien

CLI-Befehl	Beschreibung
copy source-url destination-url [snmp]	Kopiert eine beliebige Datei von einem Quellort an einen Zielort.

## Kopieren von Dateien

Dateien können von der Seite [Copy Files](#) (Dateien kopieren) aus kopiert und gelöscht werden. Öffnen Sie die Seite [Copy Files](#) (Dateien kopieren), indem Sie auf System→ File Management→ Copy Files in der Strukturansicht klicken.

Abb. 6-78. Kopieren von Dateien



**Copy Configuration** (Konfiguration kopieren) — Kopiert, wenn ausgewählt, die Running-Konfiguration-, Startup-Konfiguration- oder Backup-Konfiguration-Datei. Folgende Feldwerte können ausgewählt werden:

**Source** (Quellort) — Kopiert die Running-Konfiguration-, Startup-Konfiguration- oder Backup-Konfiguration-Datei.

**Destination** (Zielort) — Die Datei, in die die Running-Konfiguration-, Startup-Konfiguration- oder die Backup-Konfiguration-Datei kopiert wird.

**Restore Configuration Factory Defaults** (Konfiguration auf Herstellerstandard wiederherstellen) — Gibt an, wenn ausgewählt, dass eine Rücksetzung auf die Standardkonfigurationsdateien des Herstellers erfolgen soll. Wenn diese Option nicht gewählt ist, werden die aktuellen Konfigurationseinstellungen beibehalten.



## Kopieren von Dateien

1. Öffnen Sie die Seite [Copy Files](#) (Dateien kopieren).
2. Definieren Sie die Felder **Source** (Quellort) und **Destination** (Zielort).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Datei wird kopiert und das Gerät aktualisiert.

## Wiederherstellung der Standardeinstellungen des Herstellers

1. Öffnen Sie die Seite [Copy Files](#) (Dateien kopieren).
2. Klicken Sie auf **Restore Company Factory Defaults** (Originalstandard des Herstellers wiederherstellen).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Standardeinstellungen des Herstellers werden wiederhergestellt und das Gerät wird aktualisiert.

## Kopieren und Löschen von Dateien mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite [Copy Files](#) (Dateien kopieren) angezeigt werden.

Tabelle 6-47. CLI-Befehle zum Kopieren von Dateien

CLI-Befehl	Beschreibung
<code>copy source-url destination-url [snmp]</code>	Kopiert eine beliebige Datei von einem Quellort an einen Zielort.
<code>delete startup-config</code>	Löscht die Startup-Konfigurationsdatei.

Das folgende Beispiel illustriert die CLI-Befehle:

```
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]

Console# delete startup-config

Console# copy running-config startup-config

01-Jan-2000 01:55:03 %COPY-W-TRAP: The copy operation was completed successfully

Copy succeeded
```

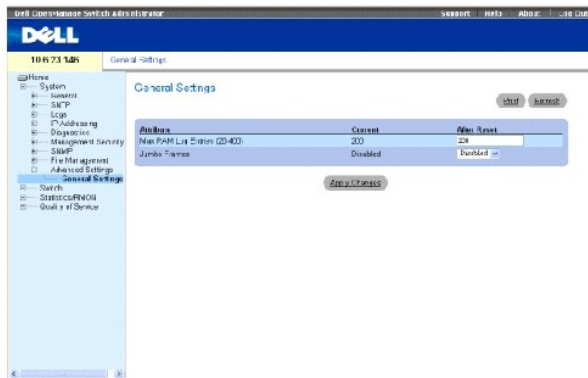
## Definieren erweiterter Einstellungen

Die Seite **Advanced Settings** (Erweiterte Einstellungen) enthält einen Link zur Konfiguration allgemeiner Einstellungen. Mit „Advanced Settings“ können verschiedene globale Attribute für das Gerät eingestellt werden. Die Änderung dieser Attribute tritt erst in Kraft, nachdem das Gerät zurückgesetzt wird. Öffnen Sie die Seite **Advanced Settings** (Erweiterte Einstellungen), indem Sie auf System → Advanced Settings in der Strukturansicht klicken.

## Konfigurieren allgemeiner Parameter für die Geräteabstimmung

Die Seite **General Settings** (Allgemeine Einstellungen) enthält Informationen zur Definition allgemeiner Geräteparameter. Öffnen Sie die Seite **General Settings** (Allgemeine Einstellungen), indem Sie auf System → Advanced Settings → General in der Strukturansicht klicken.

Abb. 6-79. Allgemeine Einstellungen



Attribute — Das Attribut der allgemeinen Einstellung.

Current (Aktuell) — Der aktuelle Wert.

After Reset (Nach Zurücksetzen) — Der künftige Wert (nach dem Zurücksetzen). Durch Eingabe eines Wertes in die Spalte „After Reset“ (Nach Zurücksetzen) wird der Feldtabelle Arbeitsspeicher zugewiesen.

Max RAM Log Entries (20-400) (Maximale Anzahl von RAM-Protokolleinträgen (20-400)) — Gibt die maximale Anzahl von RAM-Protokolleinträgen an. Sobald die maximale Anzahl von Protokolleinträgen erreicht ist, wird der Protokollinhalt gelöscht und die Erfassung neu gestartet.

Jumbo Frames — Aktiviert oder deaktiviert die Jumbo-Frames-Funktion. Jumbo-Frames ermöglicht die Übertragung von identischen Daten in weniger Frames. Damit fallen weniger Restkapazität, geringere Verarbeitungszeit und weniger Interrupts an.

## Anzeigen des Zählers für RAM-Protokolleinträge mit den CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle für die Einstellung der Felder zusammengefasst, die auf der Seite **General Settings** (Allgemeine Einstellungen) angezeigt werden.

Tabelle 6-48. CLI-Befehle für allgemeine Einstellungen

CLI-Befehl	Beschreibung
logging buffered size number	Legt die Anzahl der im internen Pufferspeicher (RAM) gespeicherten Syslog-Meldungen fest.
port jumbo-frame	Aktiviert Jumbo-Frames für das Gerät.

Das folgende Beispiel illustriert die CLI-Befehle:

```
Console (config)# logging
```

buffered size 300

---

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Dell™ PowerConnect™ 5324 System-Benutzerhandbuch



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



**HINWEIS:** Ein HINWEIS weist auf mögliche Schäden an der Hardware oder auf möglichen Datenverlust hin und beschreibt Ihnen, wie Sie dieses Problem vermeiden können.



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

**Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern.**

©2003 – 2004 Dell Inc. Alle Rechte vorbehalten.

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

Marken in diesem Text: *Dell*, *Dell OpenManage*, das *DELL*-Logo, *Inspiron*, *Dell Precision*, *Dimension*, *OptiPlex*, *PowerConnect*, *PowerApp*, *PowerVault*, *Axim*, *DellNet* und *Latitude* sind Marken von Dell Inc. *Microsoft* und *Windows* sind eingetragene Marken von Microsoft Corporation.

Alle anderen in dieser Dokumentation genannten Marken und Handelsbezeichnungen sind Eigentum der entsprechenden Hersteller und Firmen. Dell Inc. verzichtet auf alle Besitzrechte an Markenzeichen und Handelsbezeichnungen, die nicht Eigentum von Dell sind.

April 2004 Rev. A00

---

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Verwendung von Dell OpenManage Switch Administrator:

Dell™ PowerConnect™ 5324 System-Benutzerhandbuch

- [Verstehen der Schnittstelle](#)
- [Verwenden der Switch Administrator-Schaltflächen](#)
- [Starten der Anwendung](#)
- [Zugriff auf das Gerät über CLI](#)
- [Verwenden der CLI-Befehle](#)

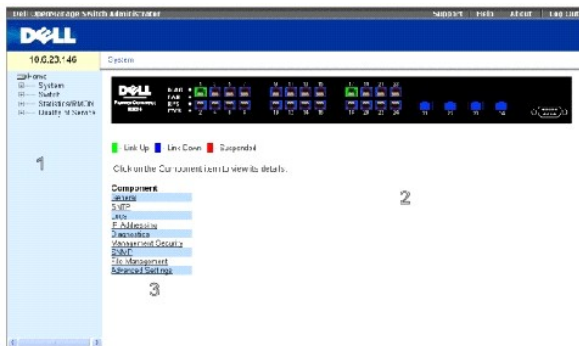
Dieser Abschnitt enthält eine Einführung in die Benutzeroberfläche.

### Verstehen der Schnittstelle

Die Startseite enthält die folgenden Anzeigen:

- 1 Tree View (Strukturansicht) — Die links auf der Startseite befindliche Strukturansicht bietet eine erweiterbare Ansicht der Funktionen und ihrer Komponenten.
- 1 Device View (Geräteansicht) — Die rechts auf der Startseite befindliche Geräteansicht bietet eine Ansicht des Geräts, einen Informations- oder Tabellenbereich und Konfigurationsanweisungen.

Abb. 5-13. Switch Administrator-Komponenten



[Tabelle 5-7](#) enthält eine Liste der Schnittstellenkomponenten mit ihren entsprechenden Nummern.

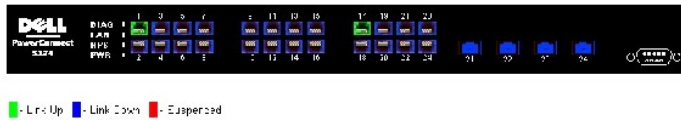
Tabelle 5-7. Schnittstellenkomponenten

Komponente	Name
1	Die Strukturansicht enthält eine Liste der verschiedenen Gerätefunktionen. Die Verzweigungen der Strukturansicht lassen sich erweitern, um alle Komponenten unter einer bestimmten Funktion anzuzeigen, bzw. lassen sich einziehen, um die Komponenten der Funktion auszublenden. Durch Ziehen des vertikalen Balkens nach rechts kann der Bereich der Strukturansicht erweitert werden, um den kompletten Namen einer Komponente anzuzeigen.
2	Die Geräteansicht bietet Informationen über die Geräteports, aktuelle Konfiguration und Status, Tabelleninformationen und Komponenten von Funktionen.  Je nach der ausgewählten Option zeigt der untere Bereich der Geräteansicht andere Geräteinformationen und/oder Dialogfelder zur Konfiguration von Parametern an.
3	Die Komponentenliste umfasst eine Liste der Funktionskomponenten. Die Komponenten können auch angezeigt werden, indem die Ansicht einer Funktion in der Strukturansicht erweitert wird.
4	Die Informationsschaltflächen ermöglichen Zugang zu Informationen über das Gerät und Dell-Support. Weitere Informationen finden Sie unter „ <a href="#">Informationsschaltflächen</a> “.

## Grafische Darstellung des Geräts

Die PowerConnect Startseite enthält eine grafische Darstellung der Vorderseite des Geräts.

Abb. 5-14. Portanzeigen



Die Port-Farbe zeigt an, ob ein bestimmter Port derzeit aktiv ist. Die Ports können die folgenden Farben aufweisen:

Tabelle 5-8. LED-Anzeigen

Komponente	Name
Portanzeigen	
Grün	Der Port ist gegenwärtig aktiviert.
Rot	Am Port ist ein Fehler aufgetreten.
Blau	Der Port ist gegenwärtig deaktiviert.

**ANMERKUNG:** Die Port-LEDs sind in der Darstellung der PowerConnect-Vorderseite im PowerConnect OpenManage Switch Administrator nicht wiedergegeben. Der LED-Status kann nur anhand des physischen Geräts ermittelt werden. Weitere Informationen zu LEDs finden Sie unter [„LED-Definitionen“](#).

## Verwenden der Switch Administrator-Schaltflächen

In diesem Abschnitt werden die Schaltflächen der OpenManage Switch Administrator-Benutzeroberfläche beschrieben.

### Informationsschaltflächen

Die Informationsschaltflächen ermöglichen Zugriff auf Online-Support und Online-Hilfe wie auch Informationen zu den OpenManage Switch Administrator-Benutzeroberflächen.

Tabelle 5-9. Informationsschaltflächen

Schaltfläche	Beschreibung
Support	Öffnet die Dell Support-Seite auf <a href="http://support.dell.com">support.dell.com</a> .
Help (Hilfe)	Die Online-Hilfe enthält Informationen zur Konfiguration und Verwaltung des Geräts. Die Seiten der Online-Hilfe sind direkt mit der aktuell geöffneten Seite verknüpft. Wenn zum Beispiel die Seite <b>IP Addressing</b> geöffnet ist, wird bei Klicken auf <b>Help</b> das Hilfethema für die Seite geöffnet.
Info	Zeigt die Version und Build-Nummer sowie Dell Urheberrechtsinformationen an.
Log Out (Abmelden)	Meldet den Benutzer aus der Anwendung ab und schließt das Browser-Fenster.

### Schaltflächen zur Geräteverwaltung

Die Schaltflächen zur Geräteverwaltung stellen ein einfaches Verfahren zur Konfiguration der Geräteinformationen dar und umfassen Folgendes:

Tabelle 5-10. Schaltflächen zur Geräteverwaltung

Schaltfläche	Beschreibung
<b>Apply Changes (Änderungen übernehmen)</b>	Übernimmt die Änderungen für das Gerät.
Schaltfläche <b>Add (Hinzufügen)</b>	Fügt Informationen zu Tabellen oder Dialogfeldern hinzu.


Telnet	Startet eine Telnet-Sitzung.
Query (Abfragen)	Dient zur Tabellenabfrage.
Show all (Alle anzeigen)	Zeigt die Gerätetabellen an.
Links-/Rechtspfeil	Verschiebt Informationen zwischen Listen.
Refresh (Aktualisieren)	Aktualisiert Geräteinformationen.
Reset All Counters (Alle Zähler rücksetzen)	Löscht den Inhalt aller Statistikzähler.
Print (Drucken)	Druckt die Seite <b>Network Management System</b> und/oder Tabelleninformationen aus.
Show Neighbors Info (Nachbarinfo anzeigen)	Zeigt die <b>Neighbors List</b> (Nachbarliste) von der Seite <b>Neighbors Table</b> (Nachbartabelle) an.
Draw (Grafik)	Generiert Diagramme zu Statistiken dynamisch.


## Starten der Anwendung

1. Öffnen eines Web-Browsers.
2. Geben Sie die IP-Adresse des Geräts (wie im CLI definiert) in der Adressenleiste ein und drücken Sie die <Eingabetaste>.

Näheres zur Zuweisung einer IP-Adresse an ein Gerät finden Sie unter „Statische IP-Adresse und Subnetzmaske“.

3. Geben Sie, wenn das Fenster **Enter Network Password** geöffnet wird, den Benutzernamen und das Kennwort ein.

 **ANMERKUNG:** Das Gerät ist nicht mit einem Standardkennwort konfiguriert und kann ohne Kennworteingabe konfiguriert werden. Nähere Angaben zur Wiederherstellung eines verlorengegangenen Kennwortes finden Sie unter „Kennwort-Wiederherstellung“.

 **ANMERKUNG:** Kennwörter sind alphanumerisch und es wird zwischen Groß- und Kleinschreibung unterschieden.

4. Klicken Sie auf **OK**.

Die **Dell PowerConnect OpenManage™ Switch Administrator** Startseite wird geöffnet.

## Zugriff auf das Gerät über CLI

Das Gerät kann über eine direkte Verbindung zum Konsolenport oder eine Telnet-Verbindung verwaltet werden. Die Verwendung von CLI ist mit der Eingabe von Befehlen auf einem Linux-System vergleichbar. Wenn der Zugriff über eine Telnet-Verbindung erfolgt, stellen Sie vor der Verwendung von CLI-Befehlen sicher, dass für das Gerät eine IP-Adresse definiert wurde und dass die zum Zugriff auf das Gerät verwendete Workstation mit dem Gerät verbunden ist.

Näheres zur Konfiguration einer anfänglichen IP-Adresse finden Sie unter „Statische IP-Adresse und Subnetzmaske“.

 **ANMERKUNG:** Stellen Sie vor der CLI-Verwendung sicher, dass der Client geladen ist.

## Konsolenverbindung

1. Schalten Sie das Gerät ein und warten Sie, bis der Startvorgang abgeschlossen ist.
2. Geben Sie nach Erscheinen der Eingabeaufforderung `console> enable` ein und drücken Sie die <Eingabetaste>.
3. Konfigurieren Sie das Gerät und geben Sie die erforderlichen Befehle zur Durchführung der gewünschten Funktionen ein.
4. Beenden Sie anschließend die Session mit dem Befehl `quit` oder `exit`.

 **ANMERKUNG:** Wenn sich ein anderer Benutzer im privilegierten EXEC-Befehlsmodus im System anmeldet, wird der aktuelle Benutzer abgemeldet und der neue Benutzer angemeldet.

## Telnet-Verbindung

Telnet ist ein Terminal-Emulations-TCP/IP-Protokoll. ASCII-Terminals können virtuell über ein TCP/IP-Protokoll-Netzwerk am lokalen Gerät angeschlossen werden. Telnet ist eine Alternative zu einem lokalen Anmelde-Terminal, in der eine Fernanmeldung erforderlich ist.

Das Gerät unterstützt bis zu vier simultane Telnet-Sessions. Alle CLI-Befehle können in einer Telnet-Session verwendet werden.

Starten einer Telnet-Sitzung:

1. Wählen Sie **Start > Run (Ausführen)**.

Daraufhin öffnet sich das Fenster **Run (Ausführen)**.

2. Geben Sie im Fenster **Run (Ausführen)** **Telnet <IP address>** im Feld **Open** ein.
3. Klicken Sie auf **OK**, um die Telnet-Sitzung zu beginnen.

---

## Verwendung des CLI

In diesem Abschnitt finden Sie Informationen zur Verwendung der CLI-Befehle.

## Überblick über den Befehlsmodus

CLI ist in Befehlsmodi unterteilt. Jeder Befehlsmodus umfasst einen bestimmten Befehlssatz. Nach Eingabe eines Fragezeichens an der Konsolen-Eingabeaufforderung wird eine Liste der möglichen Befehle für den jeweiligen Befehlsmodus angezeigt.

In jedem Modus wird ein spezieller Befehl zur Navigation von einem Befehlsmodus zum anderen verwendet.

In der Initialisierung der CLI-Sitzung ist der CLI-Modus der User EXEC-Modus. Im User EXEC-Modus ist nur eine begrenzte Untermenge der Befehle verfügbar. Dieser Level ist für Funktionen reserviert, die die Konsolenkonfiguration nicht verändern, und dient zum Zugriff auf Konfigurations-Subsysteme, wie das CLI. Zum Zugang zum nächsten Level, dem Privileged EXEC-Modus, ist ein Kennwort erforderlich (falls konfiguriert).

Der privilegierte EXEC-Modus ermöglicht Zugriff auf die globale Gerätekonfiguration. Für spezifische globale Konfigurationsoperationen innerhalb des Geräts müssen Sie den nächsten Level, den globalen Konfigurationsmodus, aufrufen. Ein Kennwort ist nicht erforderlich.

Der globale Konfigurationsmodus dient zur Verwaltung der Gerätekonfiguration auf globaler Ebene.

Der Schnittstellenkonfigurationsmodus dient zur Konfiguration des Geräts auf der physikalischen Schnittstellenebene. Bei Schnittstellenbefehlen, die Unterbefehle erfordern, gibt es oft einen weiteren Level, der Unterschnittstellen-Konfigurationsmodus (Subinterface Configuration) genannt wird. Ein Kennwort ist nicht erforderlich.

## User EXEC-Modus

Nach Anmeldung am Gerät ist der EXEC-Befehlsmodus aktiviert. Die Benutzerlevel-Eingabeaufforderung besteht aus dem Hostnamen, gefolgt von einer spitzen Klammer (>). Zum Beispiel:

```
console>
```



**ANMERKUNG:** Der Standard-Hostname ist die Konsole, außer wenn das in der Erstkonfiguration verändert wurde.

Die User EXEC-Befehle ermöglichen die Verbindungsaufnahme mit Remote-Geräten, vorübergehende Änderung von Terminal-Einstellungen, Ausführung von einfachen Tests und Auflistung von Systeminformationen.

Zur Auflistung der User EXEC-Befehle geben Sie ein Fragezeichen an der Eingabeaufforderung ein.



## Privilegierter EXEC-Modus

Um unbefugten Zugriff zu verhindern und die Betriebsparameter zu sichern, kann der privilegierte Zugriff geschützt werden. Kennwörter werden auf dem Bildschirm im \*\*\*\*\*-Format angezeigt und es wird zwischen Groß- und Kleinschreibung unterschieden.

Zugriff und Auflistung der Befehle im privilegierten EXEC-Modus:

1. Geben Sie an der Eingabeaufforderung `enable` (aktivieren) ein und drücken Sie die <Eingabetaste>.
2. Geben Sie bei Erscheinen der Kennwort-Eingabeaufforderung das Kennwort ein und drücken Sie die <Eingabetaste>.

Daraufhin erscheint die Eingabeaufforderung des privilegierten EXEC-Modus als `Gerät-Hostname`, gefolgt von `#`. Zum Beispiel:

```
console#
```

Um die Befehle des privilegierten EXEC-Modus aufzulisten, geben Sie ein Fragezeichen an der Eingabeaufforderung ein drücken die <Eingabetaste>.

Zur Rückkehr vom privilegierten EXEC-Modus zum User EXEC-Modus können Sie einen der folgenden Befehle verwenden: `disable`, `exit/end`, or `<Ctrl><Z>`.

Das folgende Beispiel veranschaulicht den Zugriff auf den privilegierten EXEC-Modus und Rückkehr zum User EXEC-Modus:

```
console>enable
```

```
Enter Password: *****
```

```
console#
```

```
console#disable
```

```
console>
```

Der Befehl `exit` dient zur Rückkehr zu einem vorherigen Modus. Zum Beispiel können Sie damit vom Schnittstellenkonfigurationsmodus zum globalen Konfigurationsmodus und vom globalen Konfigurationsmodus zum privilegierten EXEC-Modus zurückkehren.

## Globaler Konfigurationsmodus:

Die Befehle im globalen Konfigurationsmodus gelten für Systemfunktionen, und nicht für bestimmte Protokolle oder Schnittstellen.

Zum Zugriff auf den globalen Konfigurationsmodus geben Sie an der Eingabeaufforderung im privilegierten EXEC-Modus `configure` (konfigurieren) ein und drücken dann die <Eingabetaste>. Der globale Konfigurationsmodus wird als `Gerät-Hostname`, gefolgt von `(config)` und `#`, angezeigt.

```
console(config)#
```

Zur Auflistung der Befehle im globalen Konfigurationsmodus geben Sie ein Fragezeichen an der Eingabeaufforderung ein.

Zur Rückkehr vom globalen Konfigurationsmodus zum privilegierten EXEC-Modus geben Sie den Befehl `exit` ein oder verwenden den Befehl `<Ctrl><Z>`.

Das folgende Beispiel illustriert den Zugriff auf den globalen Konfigurationsmodus und Rückkehr zum privilegierten EXEC-Modus:

```
console#  
  
Console# configure  
  
Console(config)# exit  
  
console#
```

## Schnittstellenkonfigurationsmodus

Die Befehle zur Schnittstellenkonfiguration verändern bestimmte IP-Schnittstelleneinstellungen, einschließlich Bridge-Gruppe, Beschreibung etc..

### VLAN-Datenbankmodus

Der VLAN-Modus umfasst Befehle zur Erstellung und umfassenden Konfiguration eines VLAN, z.B. Erstellung eines VLAN und Anwendung einer IP-Adresse auf das VLAN. Das folgende Beispiel illustriert die Eingabeaufforderung im VLAN-Modus:

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

### Port-Kanalmodus

Der Port-Kanalmodus (Port Channel Mode) umfasst Befehle zur Konfiguration von Link Aggregation Groups (LAG). Das folgende Beispiel illustriert die Eingabeaufforderung im Port-Kanalmodus:

```
Console (config)# interface port-channel 1  
  
Console (config-if)#
```

### Schnittstellenmodus

Der Schnittstellenmodus umfasst Befehle zur Konfiguration der Schnittstelle. Der Befehl `interface ethernet` im globalen Konfigurationsmodus dient zum Aufruf des Schnittstellenkonfigurationsmodus. Das folgende Beispiel illustriert die Eingabeaufforderung im Schnittstellenmodus:

```
console> enable  
  
Console# configure
```

```
console(config)# interface ethernet g18
```

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

## Verwaltungszugriffsliste

Der Modus Verwaltungszugriffsliste umfasst Befehle zur Definition der Verwaltungszugriffslisten. Der Befehl `management access-list` im globalen Konfigurationsmodus dient zum Aufruf des Konfigurationsmodus für Verwaltungszugriffslisten.

Das folgende Beispiel illustriert die Erstellung einer Zugriffsliste mit dem Namen „m1ist“, die Konfiguration zweier Verwaltungsschnittstellen ethernet g1 und ethernet g9 und Designierung der Zugriffsliste als aktive Liste:

```
Console (config)# management access-list m1ist
```

```
Console (config-macl)# permit ethernet g1
```

```
Console (config-macl)# permit ethernet g9
```

```
Console (config-macl)# exit
```

```
Console (config)# management access-class m1ist
```

## SSH Public Key

Der Modus SSH Public Key umfasst Befehle zur manuellen Angabe anderer öffentlicher SSH-Geräteschlüssel.

Der Befehl `crypto key pubkey-chain ssh` im globalen Konfigurationsmodus dient zum Aufruf des Konfigurationsmodus für SSH Public Key-chain.

Das folgende Beispiel illustriert den Aufruf des Modus zur Konfiguration der SSH Public Key-chain:

```
Console(config)# crypto key pubkey-chain ssh
```

```
Console(config-pubkey-chain)#
```

## CLI -Beispiele

CLI-Befehle werden hier als Konfigurationsbeispiele angeführt. Eine umfassende Beschreibung der CLI-Befehle mit Beispielen finden Sie unter „CLI-Referenzhandbuch“ auf der Dokumentations-CD.

---

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Anzeigen von Statistiken:

Dell PowerConnect 5324 System-Benutzerhandbuch

- [Anzeigen von Tabellen](#)
- [Anzeigen von RMON-Statistiken](#)
- [Anzeigen von Diagrammen](#)

Die Seite **Statistics** enthält Geräteinformationen für die Schnittstellen-, GVRP-, etherlike-, RMON- und Geräteausnutzung. Um die Seite **Statistics** zu öffnen, klicken Sie auf **Statistics** in der Strukturansicht.

 **ANMERKUNG:** Für keine der Statistikseiten stehen CLI-Befehle zur Verfügung.

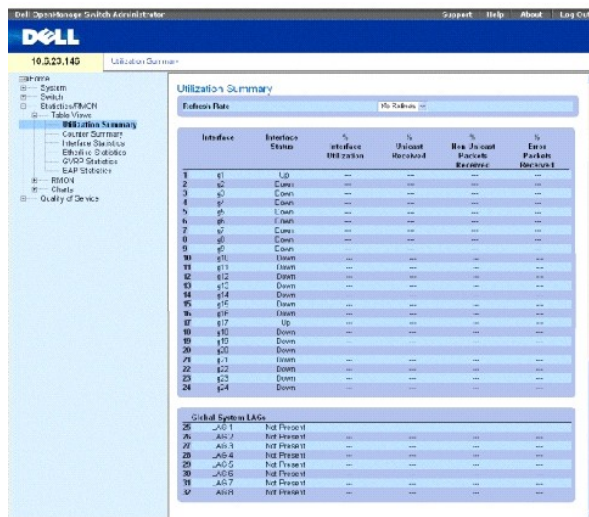
## Anzeigen von Tabellen

Die Seite **Table Views** (Tabellenansichten) enthält Verknüpfungen zur Anzeige von Statistiken in Diagrammform. Zum Öffnen der Seite klicken Sie auf **Statistics**→ **Table** in der Strukturansicht.

## Anzeigen der Nutzungsübersicht

Die Seite **Utilization Summary** (Nutzungsübersicht) umfasst Statistiken für die Schnittstellennutzung. Um die Seite zu öffnen, klicken Sie auf **Statistics**→ **Table Views**→ **Utilization Summary** in der Strukturansicht.

Abb. 8-115. Nutzungsübersicht



Refresh Rate	Interface	Interface Status	% Interface Utilization	% Packet Received	% Bytes Received	% Error Packets Received
1	e1	Up	---	---	---	---
2	e2	Down	---	---	---	---
3	e3	Down	---	---	---	---
4	e4	Down	---	---	---	---
5	e5	Down	---	---	---	---
6	e6	Down	---	---	---	---
7	e7	Down	---	---	---	---
8	e8	Down	---	---	---	---
9	e9	Down	---	---	---	---
10	e10	Down	---	---	---	---
11	e11	Down	---	---	---	---
12	e12	Down	---	---	---	---
13	e13	Down	---	---	---	---
14	e14	Down	---	---	---	---
15	e15	Down	---	---	---	---
16	e16	Down	---	---	---	---
17	e17	Up	---	---	---	---
18	e18	Down	---	---	---	---
19	e19	Down	---	---	---	---
20	e20	Down	---	---	---	---
21	e21	Down	---	---	---	---
22	e22	Down	---	---	---	---
23	e23	Down	---	---	---	---
24	e24	Down	---	---	---	---

Global System LAGs	LAG ID	LAG Name	LAG Status	% Utilization	% Packet Received	% Bytes Received	% Error Packets Received
25	JAG1	JAG1	Not Present	---	---	---	---
26	JAG2	JAG2	Not Present	---	---	---	---
27	JAG3	JAG3	Not Present	---	---	---	---
28	JAG4	JAG4	Not Present	---	---	---	---
29	JAG5	JAG5	Not Present	---	---	---	---
30	JAG6	JAG6	Not Present	---	---	---	---
31	JAG7	JAG7	Not Present	---	---	---	---
32	JAG8	JAG8	Not Present	---	---	---	---

**Refresh Rate** (Aktualisierungsrate) Die Zeitspanne, die vergeht, bevor die Schnittstellenstatistiken aktualisiert werden.

**Interface** Die Nummer der Schnittstelle.

**Interface Status** Status der Schnittstelle.



**Transmit Non Unicast Packets** Anzahl der von der Schnittstelle übertragenen Nicht-Unicast-Pakete.

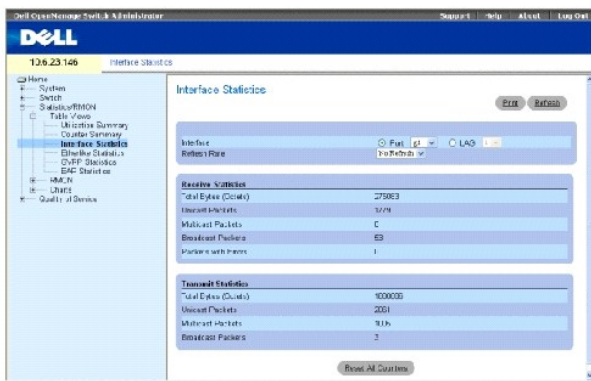
**Received Errors** Anzahl der fehlerhaften Pakete, die an der Schnittstelle erhalten wurden.

**Global System LAG**- Aktuelle LAG/Trunk-Leistung.

## Anzeigen der Schnittstellenstatistiken

Die Seite [Interface Statistics](#) enthält Statistiken für die erhaltenen und übertragenen Datenpakete. Die Felder für die erhaltenen und übertragenen Pakete sind identisch. Um die Seite [Interface Statistics](#) zu öffnen, klicken Sie auf **Statistics/RMON**→ **Table Views**→ **Interface Statistics** in der Strukturansicht.

Abb. 8-117. Schnittstellenstatistiken



Receive Statistics	
Total Bytes (Octets)	275923
Unicast Packets	3279
Multicast Packets	0
Broadcast Packets	53
Packets with Errors	1

Transmit Statistics	
Total Bytes (Octets)	1000000
Unicast Packets	2001
Multicast Packets	916
Broadcast Packets	3

**Interface** Gibt an, ob Statistiken für einen Port oder LAG angezeigt werden.

**Refresh Rate** Die Zeitspanne, die vergeht, bevor die Schnittstellenstatistiken aktualisiert werden.

## Statistiken für Paketeingang

**Total Bytes (Octets)** Anzahl der Oktette, die an der ausgewählten Schnittstelle erhalten wurden.

**Unicast Packets** Anzahl der Unicast-Pakete, die an der ausgewählten Schnittstelle erhalten wurden.

**Multicast Packets** Anzahl der Multicast-Pakete, die an der ausgewählten Schnittstelle erhalten wurden.

**Broadcast Packets** Anzahl der Broadcast-Pakete, die an der ausgewählten Schnittstelle erhalten wurden.

**Packets with Errors** Anzahl der fehlerhaften Pakete, die von der ausgewählten Schnittstelle erhalten wurden.

## Übertragungsstatistiken

**Total Bytes (Octets)** Anzahl der Oktette, die an der ausgewählten Schnittstelle übertragen wurden.

**Unicast Packets** Anzahl der an der Schnittstelle übertragenen Unicast-Pakete.

**Multicast Packets** Anzahl der Multicast-Pakete, die an der ausgewählten Schnittstelle übertragen wurden.

**Broadcast Packets** Anzahl der Broadcast-Pakete, die an der ausgewählten Schnittstelle übertragen wurden.

**Packets with Errors** Anzahl der fehlerhaften Pakete, die von der ausgewählten Schnittstelle übertragen wurden.

## Anzeigen der Schnittstellenstatistiken

1. Öffnen Sie die Seite [Interface Statistics](#).
2. Wählen Sie eine Schnittstelle im Feld **Interface**.

Die Schnittstellenstatistiken werden angezeigt.

## Rücksetzen des Schnittstellenstatistik-Zählers

1. Öffnen Sie die Seite [Interface Statistics](#).
2. Klicken Sie auf **Reset All Counters**.

Daraufhin werden die Schnittstellenstatistik-Zähler zurückgesetzt.

## Anzeigen der Schnittstellenstatistiken mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Anzeige der Schnittstellenstatistiken.

Tabelle 8-80. CLI-Befehle für Schnittstellenstatistiken

CLI-Befehl	Beschreibung
<code>show interfaces counters [ethernet interface   port-channel port-channel-number]</code>	Zeigt den über die physikalische Schnittstelle gelaufenen Datenverkehr an.

Das folgende Beispiel illustriert die CLI-Befehle:

```
Console> enable
Console# show interfaces counters
```

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
---	-----	-----	-----	-----
-	----	----	----	----
g1	183892	1289	987	8
g2	0	0	0	0
g3	123899	1788	373	19

Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
---	-----	-----	-----	-----
-				
g4	9188	9	8	0
g5	0	0	0	0
g6	8789	27	8	0
Ch	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
---	-----	-----	-----	-----
-				
1	27889	928	0	78
Ch	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
---	-----	-----	-----	-----
-				
1	23739	882	0	122

### Anzeigen von Etherlike-Statistiken

Die Seite [Etherlike Statistics](#) enthält Schnittstellenstatistiken. Um die Seite [Etherlike Statistics](#) zu öffnen, klicken Sie auf **Statistics/RMON** → **Table Views** → **Etherlike Statistics** in der Strukturansicht.

Abb. 8-118. Etherlike-Statistiken





**Interface** Gibt an, ob Statistiken für einen Port oder LAG angezeigt werden.

**Refresh Rate** Die Zeitspanne, die vergeht, bevor die Schnittstellenstatistiken aktualisiert werden.

**Frame Check Sequence (FCS) Errors** Die Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen Frameprüfsequenz-Fehler.

**Single Collision Frames** Die Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen Single Collision Frames-Fehler.

**Multiple Collision Frames** Die Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen Multiple Collisions Frames-Fehler.

**Single Quality Error (SQE) Test Errors** Die Anzahl der SQE-Testfehler, die an der ausgewählten Schnittstelle erhalten wurden.

**Deferred Transmissions** Die Anzahl der verzögerten Übertragungen über die ausgewählte Schnittstelle.

**Late Collisions** Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen verspäteten Kollisions-Frames. **Excessive Collisions** Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen übermäßigen Kollisionen.

**Internal MAC Transmit Errors** Anzahl interner MAC-Übertragungsfehler an der ausgewählten Schnittstelle.

**Carrier Sense Errors** Anzahl der bei der Leitungsüberwachung an der ausgewählten Schnittstelle aufgetretenen Fehler.

**Oversize Packets** Anzahl der durch überlange Pakete verursachten Fehler an der ausgewählten Schnittstelle.

**Internal MAC Receive Errors** Anzahl interner MAC-Empfangsfehler an der ausgewählten Schnittstelle.

**Single Quality Errors (SQE) Test Errors** Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen SQE-Testfehler.

**Receive Pause Frames** Anzahl der über die ausgewählte Schnittstelle empfangenen Pause-Frames.

**Transmitted Paused Frames** Anzahl der über die ausgewählte Schnittstelle gesendeten Pause-Frames.

## Anzeigen von Etherlike-Statistiken für eine Schnittstelle

1. Öffnen Sie die Seite [Etherlike Statistics](#).
2. Wählen Sie eine Schnittstelle im Feld **Interface** aus.

Die Etherlike-Statistiken für die Schnittstelle werden angezeigt.

## Rücksetzen von Etherlike-Statistiken

1. Öffnen Sie die Seite [Etherlike Statistics](#).
2. Klicken Sie auf **Reset All Counters**.

Die Ethernetlike-Statistiken werden zurückgesetzt.

## Anzeigen der Etherlike-Statistiken mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Anzeige der Etherlike-Statistiken.

**Tabelle 8-81. CLI - Befehle für Etherlike-Statistiken**

CLI-Befehl	Beschreibung
<code>show interfaces counters [ethernet interface   port-channel port-channel-number]</code>	Zeigt den über die physikalische Schnittstelle abgewickelten Datenverkehr an.

Das folgende Beispiel illustriert die CLI-Befehle:

```

Console> enable
Console# show interfaces counters ethernet g1

```

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
---	-----	-----	-----	-----
---	-----	-----	-----	-----
-				
g1	183892	1289	987	8

Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
---	-----	-----	-----	-----
---	-----	-----	-----	-----
-				
g1	9188	9	8	0

```

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

Received Pause Frames: 0

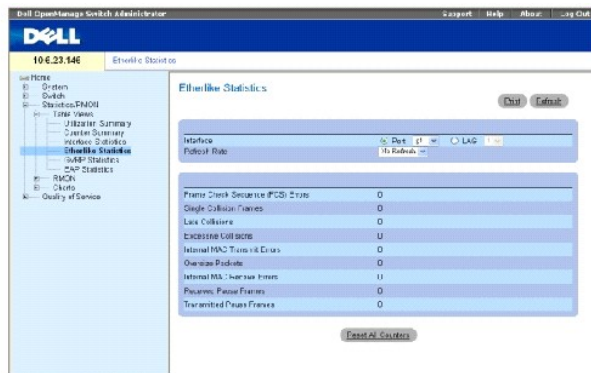
Transmitted Pause Frames: 0

```

## Anzeigen der GVRP-Statistiken

Die Seite [GVRP Statistics](#) enthält Gerätestatistiken für GVRP. Öffnen Sie die Seite, indem Sie auf **Statistics/RMON** → **Table Views** → **GVRP Statistics** in der Strukturansicht klicken.

Abb. 8-119. GVRP-Statistiken



**Interface** Gibt an, ob Statistiken für einen Port oder LAG angezeigt werden.

**Refresh Rate** Die Zeitspanne, die vergeht, bevor die Schnittstellenstatistiken aktualisiert werden.

**Join Empty** Die „GVRP Join Empty“-Statistik für das Gerät.

**Empty** Die „GVRP Empty“-Statistik für das Gerät.

**Leave Empty** Die „GVRP Leave“-Statistik für das Gerät.

**Join In** Die „GVRP Join In“-Statistik für das Gerät.

**Leave In** Die „GVRP Leave In“-Statistik für das Gerät.

**Leave All** Die „GVRP Leave All“-Statistik für das Gerät.

**Invalid Protocol ID** Die GVRP-Gerätestatistik zu ungültigen Protokoll-IDs.

**Invalid Attribute Type** Die GVRP-Gerätestatistik zu ungültigen Attribut-IDs.

**Invalid Attribute Value** Die GVRP-Gerätestatistik zu ungültigen Attributwerten.

**Invalid Attribute Length** Die GVRP-Gerätestatistik zu ungültigen Attributlängen.

**Invalid Events** Die GVRP-Gerätestatistik zu ungültigen Ereignissen.

### Anzeigen der GVRP-Statistiken für einen Port

1. Öffnen Sie die Seite [GVRP Statistics](#).
2. Wählen Sie eine Schnittstelle im Feld **Interface**.

Die GVRP-Statistiken für die Schnittstelle werden angezeigt.

### Rücksetzen von GVRP-Statistiken

1. Öffnen Sie die Seite [GVRP Statistics](#).
2. Klicken Sie auf **Reset All Counters**.

Die GVRP-Zähler werden zurückgesetzt.

### Anzeigen der GVRP-Statistiken mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Anzeige der GVRP-Statistiken.

**Tabelle 8-82. CLI-Befehle für GVRP-Statistiken**

CLI-Befehl	Beschreibung
<code>show gvrp statistics [ethernet interface   port-channel port-channel-number]</code>	Zeigt die GVRP-Statistiken an.
<code>show gvrp error-statistics [ethernet interface   port-channel port-channel-number]</code>	Zeigt die GVRP-Fehlerstatistiken an.

Das folgende Beispiel illustriert die CLI-Befehle:

```
:
Console# show gvrp statistics
GVRP statistics:
-----
```

rJE : Join Empty Received						rJIn : Join In Received						
rEmp : Empty Received						rLIn : Leave In Received						
rLE : Leave Empty Received						rLA : Leave All Received						
sJE : Join Empty Sent						sJIn : Join In Sent						
sEmp : Empty Sent						sLIn : Leave In Sent						
sLE : Leave Empty Sent						sLA : Leave All Sent						
Port	rJE	rJIn	rEmp	rLIn	rLE	rLA	sJE	sJIn	sEmp	sLIn	sLE	sLA
----	---	-----	-----	-----	---	----	---	-----	-----	-----	---	---
g1	0	0	0	0	0	0	0	0	0	0	0	0
g2	0	0	0	0	0	0	0	0	0	0	0	0
g3	0	0	0	0	0	0	0	0	0	0	0	0
g4	0	0	0	0	0	0	0	0	0	0	0	0
g5	0	0	0	0	0	0	0	0	0	0	0	0
g6	0	0	0	0	0	0	0	0	0	0	0	0
g7	0	0	0	0	0	0	0	0	0	0	0	0
g8	0	0	0	0	0	0	0	0	0	0	0	0

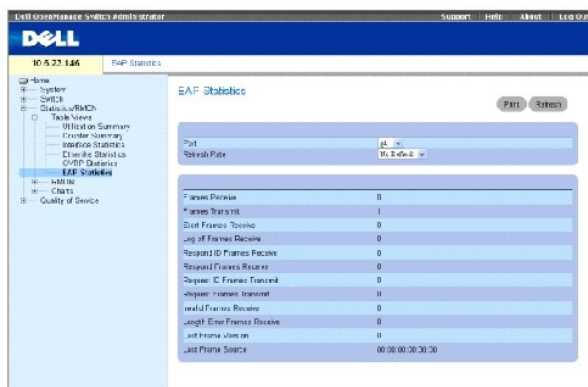
Console# show gvrp error-statistics	
GVRP error statistics:	
-----	
Legend:	
INVPROT : Invalid Protocol Id	INVPLEN : Invalid PDU Length
INVATYP : Invalid Attribute Type	INVALEN : Invalid Attribute Length

INVAVAL : Invalid Attribute Value			INVEVENT : Invalid Event		
Port	INVPROT	INVATYP	INVAVAL	INVALEN	INVEVENT
----	-----	-----	-----	-----	-----
g1	0	0	0	0	0
g2	0	0	0	0	0
g3	0	0	0	0	0
g4	0	0	0	0	0
g5	0	0	0	0	0
g6	0	0	0	0	0
g7	0	0	0	0	0
g8	0	0	0	0	0

## Anzeigen von EAP-Statistiken

Die Seite [EAP Statistics](#) enthält Informationen zu EAP-Paketen, die an einem bestimmten Port erhalten wurden. Weitere Informationen zu EAP finden Sie unter [„Portbasierte Authentifizierung \(802.1x\)“](#). Öffnen Sie die Seite [EAP Statistics](#), indem Sie auf Statistics/RMON > Table Views > EAP Statistics in der Strukturansicht klicken.

Abb. 8-120. EAP-Statistiken



**Port** Der Port, über den Statistiken abgefragt werden.

**Refresh Rate** Die Zeitspanne, die vergeht, bevor die Schnittstellenstatistiken aktualisiert werden.

**Frames Receive** Die Anzahl der am Port erhaltenen gültigen EAPOL-Frames.

**Frames Transmit** Die Anzahl der über den Port übertragenen EAPOL-Frames.

**Start Frames Receive** Die Anzahl der am Port erhaltenen EAPOL-Start-Frames.

**Log off Frames Receive** Die Anzahl der am Port erhaltenen EAPOL-Logoff-Frames.

**Respond ID Frames Receive** Die Anzahl der am Port erhaltenen EAP Resp/Id-Frames.

**Respond Frames Receive** Die Anzahl der am Port erhaltenen gültigen EAP-Response-Frames.

**Request ID Frames Transmit** Die Anzahl der über den Port übertragenen EAP-Requested-ID-Frames.

**Request Frames Transmit** Die Anzahl der über den Port übertragenen EAP-Request-Frames.

**Invalid Frames Receive** Die Anzahl der am Port erhaltenen unerkannten EAPOL-Start-Frames.

**Length Error Frames Receive** Die Anzahl der an diesem Port erhaltenen EAPOL-Frames mit einer ungültigen Paketkörperlänge.

**Last Frame Version** Die am zuletzt erhaltenen EAPOL-Frame angehängte Protokollversionsnummer.

**Last Frame Version** Die am zuletzt erhaltenen EAPOL-Frame angehängte MAC-Quelladresse.

### Anzeigen der EAP-Statistiken für einen Port

1. Öffnen Sie die Seite [EAP Statistics](#).
2. Wählen Sie eine Schnittstelle im Feld **Interface**.

Die EAP-Statistiken für die Schnittstelle werden angezeigt.

### Rücksetzen der EAP-Statistiken

1. Öffnen Sie die Seite [EAP Statistics](#).
2. Klicken Sie auf „Reset All Counters“, um den Zähler zurückzusetzen.

Die EAP-Statistiken werden zurückgesetzt.

### Anzeigen der EAP-Statistiken mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Anzeige der EAP-Statistiken.

Tabelle 8-83. CLI - Befehle für GVRP-Statistiken

CLI - Befehl	Beschreibung
<code>show dot1x statistics ethernet <i>interface</i></code>	Zeigt die 802.1X-Statistiken für die angegebene Schnittstelle an.

Das folgende Beispiel illustriert die CLI-Befehle:

```
Switch# show dot1x statistics ethernet g1

EapolFramesRx: 11

EapolFramesTx: 12

EapolStartFramesRx: 1

EapolLogoffFramesRx: 1

EapolRespIdFramesRx: 3

EapolRespFramesRx: 6

EapolReqIdFramesTx: 3

EapolReqFramesTx: 6

InvalidEapolFramesRx: 0

EapLengthErrorFramesRx: 0

LastEapolFrameVersion: 1

LastEapolFrameSource: 0008.3b79.8787
```

---

## Anzeigen von RMON-Statistiken

Remote Monitoring (RMON) enthält Verknüpfungen zur Anzeige von Netzwerkinformationen an einem entfernten Standort. Öffnen Sie die Seite **RMON**, indem Sie auf **Statistics/RMON** → **RMON** in der Strukturansicht klicken.

## Anzeigen der RMON-Statistikgruppe

Die Seite [RMON Statistics](#) enthält Felder zur Anzeige von Informationen zur Gerätenutzung und Fehlern, die bei diesem Gerät aufgetreten sind. Öffnen Sie die Seite [RMON Statistics](#), indem Sie auf **Statistics/RMON** → **RMON** → **Statistics** in der Strukturansicht klicken.

**Abb. 8-121. RMON-Statistiken**



RMON Statistics	
Interface	10.0.20.140
Refresh Rate	10.0.20.140
Drop Events	0
Received Bytes (Octets)	27751
Received Packets	1318
Broadcast Packets Received	65
Multicast Packets Received	0
CRC/Align Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	11
Frames of 64 Bytes	1159
Frames of 65 to 127 Bytes	361
Frames of 128 to 255 Bytes	24
Frames of 256 to 511 Bytes	11
Frames of 512 to 1023 Bytes	230
Frames of 1024 to 1518 Bytes	0

**Interface** Gibt den Port oder LAG an, für den Statistiken angezeigt werden.

**Refresh Rate** Die Zeitspanne, die vergeht, bevor die Schnittstellenstatistiken aktualisiert werden.

**Drop Events** Die Anzahl der Ereignisse, die seit dem letzten Aktualisieren des Geräts an der Schnittstelle abgewiesen wurden.

**Received Bytes (Octets)** Die Anzahl der Oktette, die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden. Diese Zahl umfasst fehlerhafte Pakete und FCS-Oktette, jedoch keine Framing-Bits.

**Received Packets** Die Anzahl der Pakete, die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden, einschließlich fehlerhafter Pakete, Multicast- und Broadcast-Pakete.

**Broadcast Packets Received** Die Anzahl der fehlerlosen Pakete, die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden. Diese Angabe umfasst keine Multicast-Pakete.

**Multicast Packets Received** Die Anzahl der fehlerlosen Multicast-Pakete, die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden.

**CRC & Align Errors** Die Anzahl der CRC- und Ausrichtungsfehler, die seit dem letzten Aktualisieren des Geräts an der Schnittstelle aufgetreten sind.

**Undersize Packets** Die Anzahl der Pakete unter Normalgröße (unter 64 Oktette), die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden.

**Oversize Packets** Die Anzahl der Pakete über Normalgröße (über 1518 Oktette), die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden.

**Fragments** Die Anzahl der Fragmente (Pakete mit weniger als 64 Oktetten, ausschließlich Framing-Bits, aber einschließlich FCS-Oktette), die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden.

**Jabbers** Die Anzahl der Jabbers (Pakete, die länger als 1518 Oktette sind), die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden.

**Collisions** Die Anzahl der Kollisionen, die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden.

**Frames of xx Bytes** Die Anzahl der xx-Byte-Frames, die seit dem letzten Aktualisieren des Geräts über die Schnittstelle empfangen wurden.

## Anzeigen der Schnittstellenstatistiken

1. Öffnen Sie die Seite [RMON Statistics](#).
2. Wählen Sie eine Schnittstellenart und -nummer im Feld **Interface**.

Die Schnittstellenstatistiken werden angezeigt.

## Anzeigen der RMON-Statistiken mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Anzeige der RMON-Statistiken.

**Tabelle 8-84. CLI - Befehle für RMON-Statistiken**

CLI - Befehl	Beschreibung
<code>show rmon statistics {ethernet <i>interface</i>   port-channel <i>port-channel-number</i>}</code>	Zeigt RMON-Ethernet-Statistiken an.

Das folgende Beispiel illustriert die CLI-Befehle:

```
console> enable
```

```
console> enable

Console# show rmon statistics ethernet g1

Port g1

Dropped: 8

Octets: 878128 Packets: 978

Broadcast: 7 Multicast: 1

CRC Align Errors: 0 Collisions: 0

Undersize Pkts: 0 Oversize Pkts: 0

Fragments: 0 Jabbers: 0

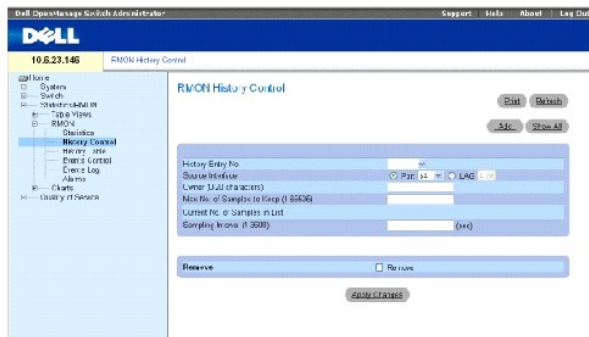
64 Octets: 98 65 to 127 Octets: 0
```

```
128 to 255 Octets: 0 256 to 511 Octets: 0
512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

## Anzeigen von RMON-Verlaufssteuerungsstatistiken

Die Seite [RMON History Control](#) enthält Informationen zu Stichprobendaten, die an den Ports erfasst wurden. Die Stichproben können zum Beispiel Schnittstellendefinitionen oder Abfragezeiträume umfassen. Öffnen Sie die Seite [RMON History Control](#), indem Sie auf **Statistics/RMON→ History Control** in der Strukturansicht klicken.

Abb. 8-122. RMON-Verlaufssteuerungsstatistiken



**History Entry No.** Eintragsnummer für die Seite **History Control Table**.

**Source Interface** Der Port oder LAG, von der die Verlaufsstichproben erfasst wurden.

**Owner (0-20 characters)** RMON-Station oder Benutzer, die/der die RMON-Informationen angefordert hat.

**Max No. of Samples to Keep (1-65535)** Die Anzahl der zu speichernden Stichproben. Der Standardwert ist 50.

**Current No. of Samples in List** Die derzeit erfasste Anzahl an Stichproben.

**Sampling Interval (1-3600)** Gibt die Zeit (in Sekunden) an, in denen Stichproben von den Ports erfasst werden. Die Werte liegen zwischen 1 und 3600 Sekunden. Der Standardwert ist 1800 Sekunden (30 Minuten).

**Remove** Entfernt, wenn aktiviert, den Eintrag aus der **History Control Table**.

### Hinzufügen eines Verlaufssteuerungseintrags

1. Öffnen Sie die Seite [RMON History Control](#).
2. Klicken Sie auf **Add**.

Die Seite **Add History Entry** wird geöffnet.

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

Der Eintrag wird in der **History Control Table** hinzugefügt.

### Ändern eines Eintrags in der Verlaufssteuerungstabelle (History Control Table)

1. Öffnen Sie die Seite [RMON History Control](#).
2. Wählen Sie einen Eintrag im Feld **History Entry No.**.
3. Ändern Sie die Felder wie gewünscht.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Tabelleneintrag wird geändert und das Gerät wird aktualisiert.

### Löschen eines Eintrags aus der Verlaufssteuerungstabelle (History Control Table)

1. Öffnen Sie die Seite [RMON History Control](#).
2. Wählen Sie einen Eintrag im Feld **History Entry No.**.
3. Klicken Sie auf **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der ausgewählte Tabelleneintrag wird gelöscht und das Gerät wird aktualisiert.

### Anzeigen der RMON-Verlaufssteuerung mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Anzeige der GVRP-Statistiken.

Tabelle 8-85. CLI - Befehle für RMON-History

CLI-Befehl	Beschreibung
<code>rmon collection history index [owner ownername   buckets bucket-number] [interval seconds]</code>	Aktiviert und konfiguriert RMON für eine Schnittstelle.
<code>show rmon collection history [ethernet interface   port-channel port-channel-number]</code>	Zeigt RMON-Verlaufssteuerungsstatistiken an.

Das folgende Beispiel illustriert die CLI-Befehle:

```
Console (config)#  
interface ethernet g8  
  
Console (config-if)# rmon  
collection history 1  
interval 2400  
  
Console(config-if)# exit  
  
Console(config)# exit
```

### Anzeigen der RMON-History-Tabelle

Die Seite [RMON History Table](#) enthält schnittstellenspezifische statistische Netzwerkstichproben. Jeder Tabelleneintrag repräsentiert alle Zählerwerte, die während einer einzigen Stichprobennahme erfasst wurden. Öffnen Sie die [RMON History Table](#), indem sie auf **Statistics/RMON** → **RMON** → **History Table** in der Strukturansicht klicken.

Abb. 8-123. RMON-History-Tabelle

**Sample No.** Die jeweilige Stichprobe, die durch die Informationen in der Tabelle dargestellt wird.

**Drop Events** Die Anzahl von Paketen, die aufgrund unzureichender Netzwerkressourcen während des Stichprobenintervalls abgewiesen wurden. Dieser Wert gibt nicht unbedingt die genaue Anzahl abgewiesener Pakete wieder, sondern bezieht sich auf die Häufigkeit, mit der abgewiesene Pakete identifiziert wurden.

**Received Bytes (Octets)** Die Anzahl der über das Netzwerk empfangenen Daten-Oktette, einschließlich ungültiger Pakete.

**Received Packets** Die Anzahl der während des Stichprobenintervalls empfangenen Pakete.

**Broadcast Packets** Die Anzahl der während des Stichprobenintervalls empfangenen gültigen Broadcast-Pakete.

**Multicast Packets** Die Anzahl der während des Stichprobenintervalls empfangenen gültigen Multicast-Pakete.

**CRC Align Errors** Die Anzahl der während der Stichprobensitzung empfangenen Pakete mit einer Länge zwischen 64 und 1518 Oktetten, einer ungültigen Frameprüfsequenz (FCS) mit einer ganzzahligen Oktettanzahl oder einer ungültigen FCS mit einer nicht ganzzahligen Oktettanzahl.

**Undersize Packets** Die Anzahl der während der Stichprobensitzung empfangenen Pakete mit einer Länge von unter 64 Oktetten.

**Oversize Packets** Die Anzahl der während der Stichprobensitzung empfangenen Pakete mit einer Länge von über 1518 Oktetten.

**Fragments** Die Anzahl der empfangenen Pakete mit einer Länge von unter 64 Oktetten, für die während der Stichprobensitzung eine Frameprüfsequenz generiert wurde.

**Jabbers** Die Anzahl der empfangenen Pakete mit einer Länge von über 1518 Oktetten, für die während der Stichprobensitzung eine Frameprüfsequenz generiert wurde.

**Collisions** Enthält einen Schätzwert der 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 Eintrag in der **History Table No.**

Die Eintragsstatistik wird in der RMON-History-Tabelle angezeigt.

## Anzeigen der RMON-Verlaufssteuerung mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Anzeige der RMON-History.

**Tabelle 8-86. CLI - Befehle für RMON-History**

CLI - Befehl	Beschreibung
show rmon history index {throughput   errors   other} [period seconds]	Zeigt RMON-Ethernet-Verlaufsstatistiken an.

Das folgende Beispiel illustriert die CLI-Befehle zur Anzeige von RMON-Ethernet-Statistiken für den Durchsatz am Index 1:

```

console> enable

Console# show rmon history 1 throughput

```

Sample Set: 1	Owner: CLI				
Interface: g1	Interval: 1800				
Requested samples: 50	Granted samples: 50				
Maximum table size: 500					
Time	Octets	Packets	Broadcast	Multicast	%
-----	-----	-----	-----	-----	-----
Jan 18 2004 21:57:00	303595962	357568	3289	7287	19.98%
Jan 18 2004 21:57:30	287696304	275686	2789	2789	20.17%

## Definieren von RMON-Geräteereignissen

Die Seite [RMON Events Control](#) enthält Felder zur Definition von RMON-Ereignissen. Öffnen Sie die Seite [RMON Events Control](#), indem Sie auf **Statistics/RMON→RMON→Events Control** in der Strukturansicht klicken.

**Abb. 8-124. RMON-Ereignissteuerung**



**Event Entry** Das Ereignis.

**Community** Die Community, der das Ereignis angehört.

**Description** Benutzerdefinierte Ereignisbeschreibung.

**Type** Beschreibt den Ereignistyp. Mögliche Werte sind:

**Log** Der Ereignistyp ist ein Protokolleintrag.

**Trap** Der Ereignistyp ist ein Trap.

**Log and Trap** Der Ereignistyp ist sowohl ein Protokolleintrag als auch ein Trap.

**None** Es gibt kein Ereignis.

**Time** Die Uhrzeit an, zu der das Ereignis aufgetreten ist, z.B. 29. März 2004, 11.00 Uhr, wird angezeigt als 29/03/2004 11:00:00.

**Owner** Das Gerät bzw. der Benutzer, von dem das Ereignis definiert wurde.

**Remove** Entfernt, falls ausgewählt, das Ereignis aus der RMON-Ereignistabelle.

### Hinzufügen eines RMON-Ereignisses

1. Öffnen Sie die Seite [RMON Events Control](#).
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite **Add an Event Entry** wird geöffnet.

3. Geben Sie die Informationen im Dialogfeld ein und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag wird in der **Event Table** hinzugefügt und das Gerät wird aktualisiert.

### Ändern eines RMON-Ereignisses

1. Öffnen Sie die Seite [RMON Events Control](#)
2. Wählen Sie einen Eintrag in der Event Table.
3. Ändern Sie die Felder im Dialogfeld und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag der **Event Table** wird geändert und das Gerät wird aktualisiert.


### Löschen von RMON-Ereigniseinträgen

1. Öffnen Sie die Seite [RMON Events Control](#).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die Seite **Events Table** wird geöffnet.

3. Wählen Sie **Remove** (Entfernen) für die/das Ereignis(se), die gelöscht werden sollen und klicken Sie dann auf **Apply Changes** (Änderungen übernehmen).

Der ausgewählte Tabelleneintrag wird gelöscht und das Gerät wird aktualisiert.

 **ANMERKUNG:** Ein einzelnes Ereignis kann aus der Seite **RMON Events Control** entfernt werden, indem Sie das Kontrollkästchen **Remove** (Entfernen) auf dieser Seite aktivieren.

### Definieren von Geräteereignissen mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Definition von Geräteereignissen.

**Tabelle 8-87. CLI - Befehle für die Definition von Geräteereignissen**

CLI - Befehl	Beschreibung
<code>rmon event index type [community text] [description text] [owner name]</code>	Konfiguriert RMON-Ereignisse.
<code>show rmon events</code>	Zeigt die RMON-Ereignistabelle an.

Das folgende Beispiel illustriert die CLI-Befehle:

```

console> enable

console# config

console (config)# rmon event 1 log

Console(config)# exit

Console# show rmon events

```

Index	Beschreibung	Typ	Community	Owner	Last time sent
----	-----	-----	-----	-----	-----
1	Errors	Log		CLI	Jan 18 2002 23:58:17



2	High Broadcast	Log-Trap	router	Manager	Jan 18 2002 23:59:48
---	----------------	----------	--------	---------	----------------------

## Anzeigen des RMON-Ereignisprotokolls

Die Seite [RMON Events Log](#) enthält eine Liste von RMON-Ereignissen. Öffnen Sie die Seite [RMON Events Log](#), indem Sie auf **Statistics/RMON→ RMON→ Events** in der Strukturansicht klicken.

Abb. 8-125. RMON-Ereignisprotokoll



**Event** Die Eintragsnummer im RMON-Ereignisprotokoll.

**Log Nr.** Die Protokollnummer.

**Log Time** Die Uhrzeit, zu welcher der Protokolleintrag erfasst wurde.

**Description** Beschreibt den Protokolleintrag.

## Definieren von Geräteereignissen mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Definition von Geräteereignissen.

Tabelle 8-88. CLI-Befehle für die Definition von Geräteereignissen

CLI-Befehl	Beschreibung
<code>show rmon log [event]</code>	Zeigt die RMON-Protokolltabelle an.

Das folgende Beispiel illustriert die CLI-Befehle:

```
console> enable

console# config

console (config)# rmon event 1 log
```

Console(config)# exit

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

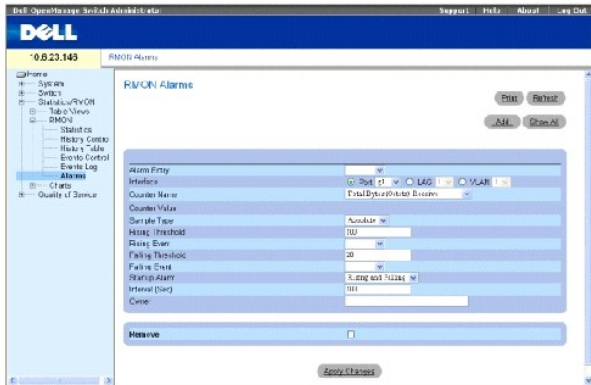
Maximum table size: 500 (800 after reset)

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 RMON-Gerätealarmen

Die Seite [RMON Alarms](#) enthält Felder zur Einstellung von Netzwerkalarmen. Ein Netzwerkalarm wird ausgegeben, wenn ein Netzwerkproblem oder ein Ereignis auftritt. Beim Über- oder Unterschreiten eines Schwellenwerts wird ein Alarm ausgegeben. Öffnen Sie die Seite [RMON Alarms](#), indem Sie auf **Statistics/RMON → RMON → Alarms** in der Strukturansicht klicken.

Abb. 8-126. RMON-Alarme



**Alarm Entry** Zeigt einen spezifischen Alarm an.

**Interface** Gibt die Schnittstelle an, für die RMON-Statistiken angezeigt werden.

**Counter Name** Gibt die ausgewählte MIB-Variante an.

**Counter Value** Der Wert der ausgewählten MIB-Variablen.

**Sample Type** Gibt das Stichprobenverfahren für die ausgewählte Variable an und vergleicht den Wert mit den Schwellenwerten. 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. Der obere Schwellenwert wird oben auf den Diagrammbalken grafisch dargestellt. Jeder überwachten Variablen wird eine eigene Farbe zugewiesen.

**Rising /Falling Event** Der Mechanismus, durch den ein Alarm gemeldet wird LOG, TRAP oder eine Kombination aus beiden. 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. Der untere Schwellenwert wird unten 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.

**Interval (sec)** Die Intervallzeit für den Alarm.

**Owner** Das Gerät bzw. der Benutzer, von dem der Alarm definiert wurde.

**Remove** Entfernt, wenn aktiviert, einen RMON-Alarm.

## Hinzufügen eines Eintrags in die Alarmtabelle

1. Öffnen Sie die Seite [RMON Alarms](#).
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite **Add an Alarm Entry** wird geöffnet:

**Abb. 8-127. Hinzufügen eines Alarmeintrags**

Alarm Entry	1
Interface	<input type="radio"/> Port <input type="radio"/> LAG <input type="radio"/> VLAN
Counter Name	Total Bytes (C/Usr) Perceive
Sample Type	Absolute
Rising Threshold	100
Rising Event	
Falling Threshold	20
Falling Event	
Startup Alarm	Rising and Falling
Interval	100
Overcr	

3. Wählen Sie eine Schnittstelle.
4. Geben Sie die Informationen in den Feldern des Dialogfeldes ein.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der RMON-Alarm wird hinzugefügt und das Gerät wird aktualisiert.

## Ändern eines Eintrags in der Alarmtabelle:

1. Öffnen Sie die Seite [RMON Alarms](#).
2. Wählen Sie einen Eintrag im **Alarm Entry** Drop-Down-Menü.
3. Ändern Sie die Felder im Dialogfeld wie gewünscht.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag wird geändert und das Gerät wird aktualisiert.

## Anzeigen der Alarmtabelle:

1. Öffnen Sie die Seite [RMON Alarms](#).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die Seite **Alarms Table** wird geöffnet.

## Löschen eines Eintrags aus der Alarmtabelle

1. Öffnen Sie die Seite [RMON Alarms](#).
2. Wählen Sie einen Eintrag im Drop-Down-Menü **Alarm Entry**.
3. Wählen Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der ausgewählte Eintrag wird gelöscht und das Gerät wird aktualisiert.

## Definieren von Gerätealarmen mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Definition der Gerätealarme.

Tabelle 8-89. CLI-Befehle für Gerätealarm

CLI-Befehl	Beschreibung
<code>rmon alarm index variable interval rthreshold fthreshold revent fevent [type type] [startup direction] [owner name]</code>	Konfiguriert die RMON-Alarmbedingungen.
<code>show rmon alarm-table</code>	Zeigt eine Übersicht der Alarmtabelle an.
<code>show rmon alarm</code>	Zeigt die RMON-Alarmkonfiguration an.

Das folgende Beispiel illustriert die CLI-Befehle:

```

console> enable

console# config

Console (config)# rmon alarm 1000 dell 360000 1000000 1000000 10 20

Console# show rmon alarm-table

```

Index	OID	Owner
1	1.3.6.1.2.1.2.2.1.1 0.1	CLI
2	1.3.6.1.2.1.2.2.1.1 0.1	Manager
3	1.3.6.1.2.1.2.2.1.1 0.9	CLI

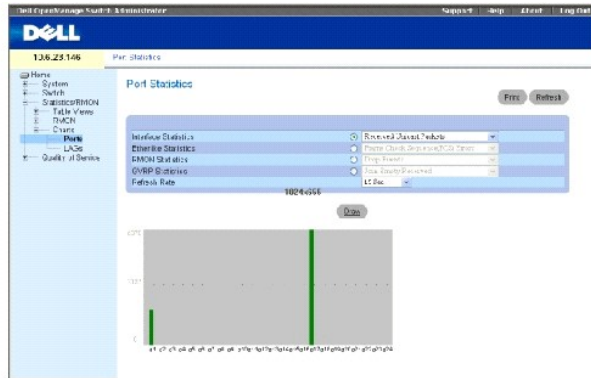
## Anzeigen von Diagrammen

Die Seite [Chart](#) enthält Links zur Anzeige von Statistiken in Diagrammform. Um die Seite zu öffnen, klicken Sie auf [Statistics](#)→[Charts](#) in der Strukturansicht.

## Anzeigen der Port-Statistiken

Die Seite [Port Statistics](#) enthält Felder zur Öffnung von Statistiken in Diagrammform für Portelemente. Öffnen Sie die Seite [Port Statistics](#), indem Sie auf [Statistics](#)→[Charts](#)→[Ports](#) in der Strukturansicht klicken.

Abb. 8-128. Portstatistiken



**Interface Statistics** Wählt die Art der zu öffnenden Schnittstellenstatistik aus.

**Etherlike Statistics** Wählt die Art der zu öffnenden Etherlike-Statistik aus.

**RMON Statistics** Wählt die Art der zu öffnenden RMON-Statistik aus.

**GVRP Statistics** Wählt die Art der zu öffnenden GVRP-Statistik aus.

**Refresh Rate** Die Zeitspanne, die vergeht, bevor die Statistiken aktualisiert werden.

### Anzeigen der Port-Statistiken

1. Öffnen Sie die Seite [Port Statistics](#).
2. Wählen Sie die Art der zu öffnenden Statistik aus.
3. Wählen Sie die gewünschte Aktualisierungsrate aus dem Drop-Down-Menü **Refresh Rate** aus.
4. Klicken Sie auf **Draw**

Die Grafik für die ausgewählte Statistik wird angezeigt.

### Anzeigen der Port-Statistiken mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Anzeige der Port-Statistiken.

**Tabelle 8-90. CLI-Befehle für Port-Statistiken**

CLI-Befehl	Beschreibung
<code>show interfaces counters {ethernet interface   port-channel port-channel-number}</code>	Zeigt den an der physikalischen Schnittstelle abgewickelten Datenverkehr an.
<code>show rmon statistics {ethernet interface   port-channel port-channel-number}</code>	Zeigt die RMON-Ethernet-Statistiken an.
<code>show gvrp statistics {ethernet interface   port-channel port-channel-number}</code>	Zeigt die GVRP-Statistiken an.
<code>show gvrp error-statistics {ethernet interface   port-channel port-channel-number}</code>	Zeigt die GVRP-Fehlerstatistiken an.

```

Console# show interfaces
description ethernet g1

```

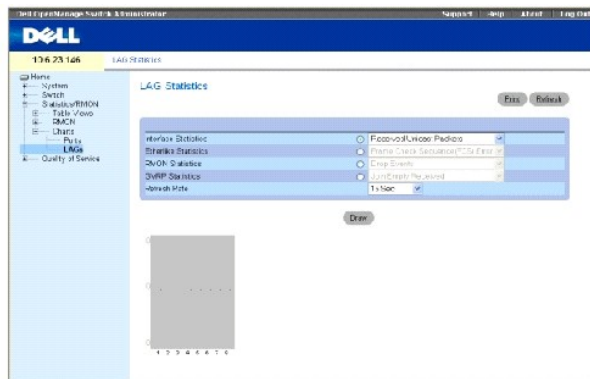
Port	Description

g1	Management_port
g2	R&D_port
g3	Finance_port
Ch	Description
1	Output

## Anzeigen der LAG-Statistiken

Die Seite [LAG Statistics](#) enthält Felder zum Öffnen von Statistiken als Diagramme für LAGs. Öffnen Sie die Seite [LAG Statistics](#), indem Sie auf **Statistics**→**Charts**→**LAGs** in der Strukturansicht klicken.

Abb. 8-129. LAG-Statistiken



**Interface Statistics** Wählt die Art der zu öffnenden Schnittstellenstatistik aus.

**Etherlike Statistics** Wählt die Art der zu öffnenden Etherlike-Statistik aus.

**RMON Statistics** Wählt die Art der zu öffnenden RMON-Statistik aus.

**GVRP Statistics** Wählt die Art der zu öffnenden GVRP-Statistik aus.

**Refresh Rate** Die Zeitspanne, die vergeht, bevor die Statistiken aktualisiert werden.

## Anzeigen der LAG-Statistiken

1. Öffnen Sie die Seite [LAG Statistics](#).

2. Wählen Sie den Typ der zu öffnenden Statistik.
3. Wählen Sie die gewünschte Aktualisierungsrate aus dem Drop-Down-Menü **Refresh Rate** aus.
4. Klicken Sie auf **Draw**.

Die Grafik für die ausgewählte Statistik wird angezeigt.

## Anzeigen der LAG-Statistiken mit den CLI-Befehlen

Die folgende Tabelle bietet eine Übersicht über die entsprechenden CLI-Befehle zur Anzeige der LAG-Statistiken.

**Tabelle 8-91. CLI-Befehle für LAG-Statistiken**

CLI-Befehl	Beschreibung
<code>show interfaces counters {ethernet interface   port-channel port-channel-number}</code>	Zeigt den an der physikalischen Schnittstelle abgewickelten Datenverkehr an.
<code>show rmon statistics {ethernet interface   port-channel port-channel-number}</code>	Zeigt die RMON-Ethernet-Statistiken an.
<code>show gvrp statistics {ethernet interface   port-channel port-channel-number}</code>	Zeigt die GVRP-Statistiken an.
<code>show gvrp error-statistics {ethernet interface   port-channel port-channel-number}</code>	Zeigt die GVRP-Fehlerstatistiken an.

```

Console# show gvrp statistics

GVRP statistics:
-----
rJE : Join Empty Received      rJIn : Join In Received
rEmp : Empty Received          rLIn : Leave In Received
rLE : Leave Empty Received     rLA : Leave All Received
sJE : Join Empty Sent          sJIn : Join In Sent
sEmp : Empty Sent              sLIn : Leave In Sent
sLE : Leave Empty Sent         sLA : Leave All Sent
-----
Port  rJE  rJIn  rEmp  rLIn  rLE  rLA  sJE  sJIn  sEmp  sLIn  sLE  sLA
-----
g1   0   0   0   0   0   0   0   0   0   0   0   0
g2   0   0   0   0   0   0   0   0   0   0   0   0

```



g3	0	0	0	0	0	0	0	0	0	0	0	0	0
g4	0	0	0	0	0	0	0	0	0	0	0	0	0
g5	0	0	0	0	0	0	0	0	0	0	0	0	0
g6	0	0	0	0	0	0	0	0	0	0	0	0	0
g7	0	0	0	0	0	0	0	0	0	0	0	0	0
g8	0	0	0	0	0	0	0	0	0	0	0	0	0

---

[Zurück zum Inhaltsverzeichnis](#)