Dell™ PowerConnect™ 34XX- Systeme Benutzerhandbuch

Hinweise, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, die Ihnen die Arbeit mit dem Computer erleichtern.

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

VORSICHT: VORSICHT zeigt eine potenziell gefährliche Situation an, die zu Sachschäden, Verletzungen oder zum Tod führen könnte.

März 2005

Zurück zum Inhalt

Einführung

Dell™ PowerConnect™ 34XX- Systeme Benutzerhandbuch

Bei den Geräten PowerConnect 3424/3448 und PowerConnect 3424P/3448P handelt es sich um hoch entwickelte Multi-Layer-Switches, die im Stack eingesetzt werden können. Die PowerConnect-Einheiten können wahlweise als eigenständige Multi-Layer-Switches oder in Stacks mit bis zu sechs Komponenten eingesetzt werden.

Das vorliegende *Benutzerhandbuch* enthält die erforderlichen Informationen zur Geräteinstallation, -konfiguration und -wartung.

Systembeschreibung

Die Modelle PowerConnect 3424/3448 und PowerConnect 3424P/3448P zeichnen sich durch Vielseitigkeit und minimalen Verwaltungsaufwand aus. Die Reihen PowerConnect 3424 und 3448 umfassen die folgenden Gerätetypen:

- PowerConnect 3424
- PowerConnect 3424P
- PowerConnect 3448
- PowerConnect 3448P

PowerConnect 3424

Der PowerConnect 3424 bietet 24 10/100-Mbit/s-Ports plus zwei SFP-Ports sowie zwei Kupfer-Ports, die für die Weiterleitung des Datenverkehrs in einem Standalone-Gerät bzw. als Stack-Ports bei gestapelten Geräten zur Verfügung stehen. Das Gerät verfügt außerdem über einen RS-232-Anschluss für eine (externe) Konsole. Der PowerConnect 3424 ist eine stapelbare Geräteeinheit, die jedoch auch als eigenständiges Gerät eingesetzt werden kann (= Standalone-Modus).

PowerConnect 3424P

Der PowerConnect 3424P bietet 24 10/100-Mbit/s-Ports plus zwei SFP-Ports sowie zwei Kupfer-Ports, die für die Weiterleitung des Datenverkehrs in einem Standalone-Gerät bzw. als Stack-Ports bei gestapelten Geräten zur Verfügung stehen. Das Gerät verfügt außerdem über einen RS-232-Anschluss für eine (externe) Konsole. Der PowerConnect 3424P ist eine stapelbare Geräteeinheit, die jedoch auch als eigenständiges Gerät eingesetzt werden kann (= Standalone-Modus). Darüber hinaus unterstützt der PowerConnect 3424P Power over Ethernet (PoE).

Abbildung 1-1. PowerConnect 3424 und PowerConnect 3424P

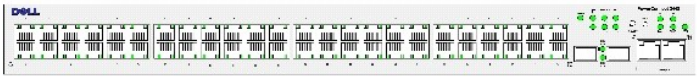
PowerConnect 3448

Der PowerConnect 3448 bietet 48 10/100-Mbit/s-Ports plus zwei SFP-Ports sowie zwei Kupfer-Ports, die für die Weiterleitung des Datenverkehrs in einem Standalone-Gerät bzw. als Stack-Ports bei gestapelten Geräten zur Verfügung stehen. Das Gerät verfügt außerdem über einen RS-232-Anschluss für eine (externe) Konsole. Der PowerConnect 3448 ist eine stapelbare Geräteeinheit, die jedoch auch als eigenständiges Gerät eingesetzt werden kann (= Standalone-Modus).

PowerConnect 3448P

Der PowerConnect 3448P bietet 48 10/100-Mbit/s-Ports, zwei SFP-Ports sowie zwei Kupfer-Ports, die für die Weiterleitung des Datenverkehrs im Standalone-Modus bzw. als Stack-Ports bei gestapelten Geräten zur Verfügung stehen. Das Gerät verfügt außerdem über einen RS-232-Anschluss für eine (externe) Konsole. Darüber hinaus bietet der PowerConnect 3448P PoE-Unterstützung.

Abbildung 1-2. PowerConnect 3448 und PowerConnect 3448P



Übersicht über die Stack-Montage

Der Einsatz der Switches PowerConnect 3424/P und PowerConnect 3448/P im Stack ermöglicht die Verwaltung mehrerer Geräte von einem zentralen Punkt aus, so als bildeten sämtliche Stack-Komponenten eine Einheit. Der Zugriff auf sämtliche Stack-Komponenten erfolgt über eine zentrale IP-Adresse, die eine Verwaltung des gesamten Stacks ermöglicht. Die Stack-Verwaltung erfolgt über:

- eine webbasierte Schnittstelle
- eine SNMP-Management-Station
- eine Befehlszeilenschnittstelle (Command Line Interface, CLI)

Die Modelle PowerConnect 3424/P und PowerConnect 3448/P unterstützen Stacks mit bis zu sechs Geräteeinheiten sowie einen eigenständigen Gerätebetrieb (Standalone-Modus).

Während des Stack-Setups wird ein Gerät als Mastereinheit (Stack-Master) ausgewählt; eine weitere Stack-Komponente kann als Mastersicherungseinheit (Backup-Master) vereinbart werden. Alle übrigen Geräte werden zu Stack-Komponenten und erhalten eine eindeutige Geräte-ID.

Die Switch-Software wird für jede Stack-Komponente separat heruntergeladen. Allerdings muss auf allen Geräteeinheiten eines Stacks dieselbe Softwareversion installiert werden.

Das Stacking und die Konfiguration der Switches erfolgt über den Stack-Master. Der Stack-Master erkennt und rekonfiguriert die Ports in folgenden Fällen mit minimalen Auswirkungen auf den Stack-Betrieb:

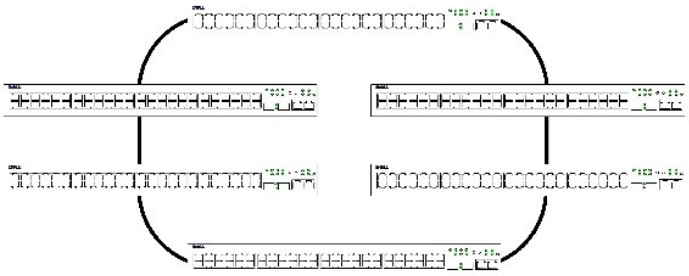
- Ausfall einer Einheit
- Verbindungsausfall zwischen Stack-Einheiten
- Einsetzen einer Einheit
- Entfernen einer Stack-Einheit

Aufbau der Stack-Topologie

Die Geräte der PowerConnect 3400-Reihe werden in einer Ringtopologie betrieben. Eine gestapelte Ringtopologie liegt vor, wenn alle Geräte des Stacks ringförmig miteinander verbunden sind. Jedes Gerät im Stack nimmt Daten entgegen und übermittelt diese an das Gerät, an das es selbst angeschlossen ist. Das Datenpaket wird anschließend durch den gesamten Stack durchgereicht, bis es zur vorgesehenen Zielstelle gelangt. Das System erkennt hierbei den optimalen Pfad für die Weiterleitung des Datenverkehrs.

Abbildung 1-3. Stacking in Ringtopologie

Ringtopologie



Schwierigkeiten treten in Ringtopologien meist auf, wenn eine Ringkomponente ausfällt oder die Funktionalität bzw. Qualität einer Verbindung beeinträchtigt ist. Bei einem PowerConnect 3424/P- oder PowerConnect 3448/P-Stack schaltet das System in diesem Fall automatisch und ohne Stillstandszeit auf eine Stacking Failover-Topologie um. Gleichzeitig wird eine SNMP-Meldung generiert; weitere Maßnahmen zur Stack-Verwaltung sind jedoch nicht erforderlich. Allerdings muss die Stack-Verbindung oder die Stack-Komponente repariert werden, um die Integrität des Stacks sicherzustellen.

Sobald alle Stack-Probleme behoben worden sind, kann das Gerät umgehend wieder den Stack integriert werden, um die Ringtopologie wiederherzustellen.

Stacking Failover-Topologie

Bei einem Fehler bzw. Ausfall der Stack-Topologie fällt der Stack automatisch auf die Stacking Failover-Topologie zurück. In der Stacking Failover-Topologie werden die Geräte in Kettenformation betrieben. Der Stack-Master bestimmt hierbei, an welche Geräteeinheit die Datenpakete übermittelt werden. Jede Einheit, mit Ausnahme der oberen und unteren Einheiten, ist mit zwei benachbarten Geräten verbunden.

Stack-Komponenten und Geräte-ID

Die Geräte-ID ist eine wesentliche Voraussetzung für die Stack-Konfiguration. Der Stack-Betrieb wird während des Startvorgangs festgelegt. Der Betriebsmodus ergibt sich aus der Geräte-ID, die während des Initialisierungsprozesses ausgewählt wird. Entscheidet sich der Benutzer beispielsweise für den Standalone-Modus, wird das Gerät während des Startvorgangs als eigenständiges Gerät gestartet.

Die Geräteeinheiten sind werkseitig mit einer Standard-Geräte-ID für den Einsatz als Standalone-Einheit vorkonfiguriert. Wird ein Gerät im Standalone-Modus betrieben, leuchtet keine der Stack-LEDs.

Wählt der Benutzer eine andere Geräte-ID aus, wird diese ID nicht gelöscht, sondern bleibt auch dann gültig, wenn die Einheit zurückgesetzt wird.

Die Geräte-IDs 1 und 2 sind für Mastergeräte reserviert. Die Geräte-IDs 3 bis 6 können Stack-Komponenten zugewiesen werden.

Wird die Mastereinheit gestartet bzw. eine Stack-Komponente eingesetzt oder entfernt, wird von der Mastereinheit ein Stack-Erkennungsvorgang initiiert.

ANMERKUNG: Selbst wenn festgestellt wird, dass zwei Komponenten dieselbe Geräte-ID aufweisen, ist der Stack weiterhin funktionstüchtig; allerdings wird nur die Einheit mit dem früheren Eintrittszeitpunkt in den Stack aufgenommen. Gleichzeitig wird eine Meldung ausgegeben, die darauf hinweist, dass eine Einheit nicht in den Stack integriert werden konnte.

Entfernen und Austauschen von Stack-Komponenten

Die Einheiten 1 und 2 fungieren als Mastergeräte. Einheit 1 und Einheit 2 sind als Mastereinheit oder Mastersicherungseinheit gekennzeichnet. Die Zuweisung des Stack-Masters erfolgt im Rahmen des Konfigurationsprozesses. Eine masterfähige Stack-Komponente wird als Mastereinheit, die jeweils andere masterfähige Komponente als Mastersicherungseinheit eingesetzt. Der Entscheidungsprozess ist hierbei wie folgt:

- Ist nur eine masterfähige Geräteeinheit verfügbar, wird diese automatisch zum Stack-Master.
- Sind zwei masterfähige Stack-Komponenten verfügbar, von denen eine manuell als Stack-Master konfiguriert wurde, übernimmt diese manuell konfigurierte Komponente die Rolle des Stack-Masters.
- Sind zwei masterfähige Geräteeinheiten verfügbar und wurde keine dieser Einheiten manuell als Mastereinheit konfiguriert, wird die Einheit mit der längeren Betriebszeit zum Stack-Master.

- Sind zwei masterfähige Geräteeinheiten verfügbar und wurden beide Einheiten manuell als Mastereinheit konfiguriert, wird die Einheit mit der längeren Betriebszeit zum Stack-Master.
- Sind die beiden masterfähigen Stack-Komponenten gleich lange aktiv, wird Einheit 1 zum Stack-Master.

ANMERKUNG: Zwei Stack-Komponenten gelten als Geräte mit identischer Betriebszeit, wenn sie innerhalb desselben 10 Minuten-Intervalls eingesetzt wurden.

Wurde Einheit 2 beispielsweise in der ersten Minute eines 10-Minuten-Intervalls eingesetzt und Einheit 1 in der fünften Minute desselben Intervalls, haben beide Einheiten per definitionem dieselbe Betriebszeit. Gibt es zwei masterfähige Stack-Komponenten, die gleich lange aktiv sind, wird Einheit 1 zur Mastereinheit.

Die Mastereinheit und die Mastersicherungseinheit unterstützen ein so genanntes Warm Standby. Die Warm Standby-Funktion stellt sicher, dass die Mastersicherungseinheit bei einem eventuellen Ausfall die Aufgaben des Stack-Masters übernimmt. Auf diese Weise ist gewährleistet, dass der Stack jederzeit funktionstüchtig bleibt.

Während der Warm Standby-Phase werden Mastereinheit und Mastersicherungseinheit nur mit der statischen Konfiguration synchronisiert. Bei Konfiguration der Mastereinheit muss der Stack-Master auch die Mastersicherungseinheit synchronisieren. Die dynamische Konfiguration wird nicht gespeichert; so werden beispielsweise dynamisch erkannte MAC-Adressen nicht gespeichert.

Jeder Port im Stack verfügt über eine spezifische Geräte-ID sowie über einen eigenen Port-Typ und eine Port-Nummer, die sowohl Teil der Konfigurationsbefehle als auch der Konfigurationsdateien sind. Konfigurationsdateien werden ausschließlich vom Stack-Master verwaltet. Die Verwaltung umfasst:

- Speichern im FLASH
- Hochladen von Konfigurationsdateien auf einen externen TFTP-Server
- Herunterladen von Konfigurationsdateien von einem externen TFTP-Server

ANMERKUNG: Selbst wenn der Stack zurückgesetzt wird und/oder die Ports nicht mehr vorhanden sind, wird die Stack-Konfiguration für alle konfigurierten Ports gespeichert.

Bei jedem Neustart erfolgt eine Topologie-Erkennung, und der Master stellt fest, welche Einheiten der Stack umfasst. Geräte-IDs werden in der jeweiligen Einheit gespeichert und im Rahmen der Topologie-Erkennung abgerufen. Eine Einheit, die nicht im Standalone-Modus betrieben wird, kann nicht gestartet werden, ohne zuvor einen Master zu vereinbaren.

Konfigurationsdateien können nur explizit durch einen Benutzer geändert werden. Die Konfigurationsdateien werden in folgenden Fällen nicht automatisch geändert:

- Hinzufügen von Einheiten
- Entfernen von Einheiten
- Neuzuweisung von Geräte-IDs
- Umschalten zwischen Stack-Modus und Standalone-Modus einer Einheit

Bei jedem Systemneustart wird der Stack anhand der Startkonfigurationsdatei in der Mastereinheit konfiguriert.

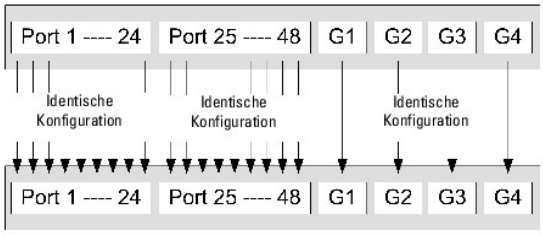
Wenn eine Stack-Komponente aus dem Stack entfernt und anschließend durch ein Gerät mit derselben Geräte-ID ersetzt wird, wird die Stack-Komponente mit den ursprünglichen Geräteeinstellungen konfiguriert. Auf der Startseite von PowerConnect OpenManage Switch Administrator werden lediglich physisch vorhandene Anschlüsse angezeigt; sie können mit Hilfe des Webverwaltungssystems konfiguriert werden. Nicht vorhandene Anschlüsse werden über die CLI- bzw. SNMP-Schnittstellen konfiguriert.

Austauschen von Stack-Komponenten

Wird eine vorhandene Stack-Komponente durch eine Geräteeinheit mit derselben Geräte-ID ersetzt, so wird die bisherige Gerätekonfiguration für die neue Stack-Komponente übernommen. Verfügt das neu hinzugefügte Gerät über mehr oder weniger Ports als das vorherige Gerät, wird die entsprechende Port-Konfiguration auf die neue Stack-Komponente angewendet. Beispiel:

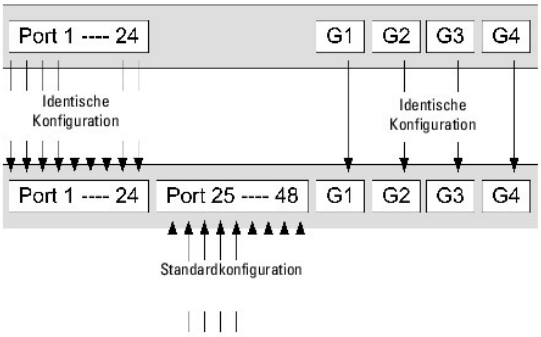
- Ersetzt ein PowerConnect 3424/P einen PowerConnect 3424/P, werden alle Port-Konfigurationen unverändert übernommen.
- Ersetzt ein PowerConnect 3448/P den PowerConnect 3448/P, werden alle Port-Konfigurationen unverändert übernommen.

Abbildung 1-4. PowerConnect 3448/P ersetzt PowerConnect 3448/P



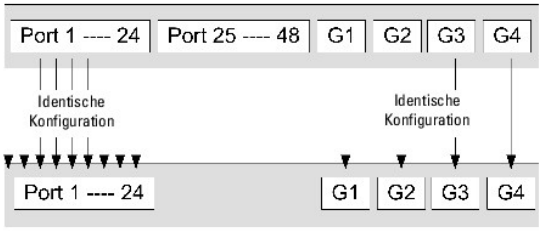
- Wenn ein PowerConnect 3448/P einen PowerConnect 3424/P ersetzt, wird die FE-Port-Konfiguration des 3424/P für die ersten 24 FE-Ports des 3448/P übernommen. Die GE-Port-Konfigurationen werden unverändert beibehalten. Für die übrigen Ports wird die Standard-Port-Konfiguration vereinbart.

Abbildung 1-5. PowerConnect 3424/P-Port ersetzt PowerConnect 3448/P-Port



- Wenn ein PowerConnect 3424/P einen PowerConnect 3448/P ersetzt, wird die Konfiguration der ersten 24 FE-Ports des PowerConnect 3448/P für die 24 FE-Ports des PowerConnect 3424/P übernommen. Die GE-Port-Konfigurationen werden unverändert beibehalten.

Abbildung 1-6. PowerConnect 3448/P-Port ersetzt PowerConnect 3424/P-Port



Wechsel von Mastereinheit zu Mastersicherungseinheit

In folgenden Fällen wird die Mastereinheit durch die Mastersicherungseinheit ersetzt:

- Der Stack-Master fällt aus oder wird aus dem Stack entfernt.
- Eine Verbindung zwischen dem Stack-Master und den Stack-Komponenten fällt aus.
- Bei einer Soft-Umschaltung über die Weboberfläche oder die CLI.

Die Umschaltung zwischen Mastereinheit und Mastersicherungseinheit hat einen begrenzten Dienstausfall zur Folge. Dynamische Tabellen werden im Fehlerfall neu abgerufen. Die momentan aktive Konfigurationsdatei wird zwischen Mastereinheit und Mastersicherungseinheit synchronisiert und bleibt auch auf der Mastersicherungseinheit weiterhin aktiv.

Funktionsübersicht

Dieser Abschnitt beschreibt die verschiedenen Gerätefunktionen. Eine umfassende Liste aller aktualisierten Gerätefunktionen finden Sie in den **Versionshinweisen** zur neuesten Software-Version.

Power over Ethernet

Power over Ethernet (PoE) ermöglicht eine Stromversorgung der angeschlossenen Geräte über die vorhandene LAN-Verkabelung, d. h. ohne Aktualisierung oder Modifikation der bestehenden Netzwerkinfrastruktur. Dank PoE entfällt die Notwendigkeit, Netzwerkgeräte in der Nähe einer Stromquelle zu installieren. Mögliche Anwendungsbereiche für PoE:

- IP-Telefone
- Wireless Access Points
- IP-Gateways
- PDAs
- Audio/Video-Fernüberwachung

Weitere Informationen zu Power over Ethernet finden Sie unter Power-Over-Ethernet.

Head-of-Line-Blocking

Head-of-Line-Blocking (HOL-Blocking) führt zu Verzögerungen und Frame-Verlusten durch Datenströme, die um die gleichen Egress-Port-Ressourcen konkurrieren. Beim HOL-Blocking befinden sich die Pakete in einer Warteschlange, wobei die Pakete am Anfang der Warteschlange vor den weiter hinten liegenden Paketen weitergeleitet werden.

Flusskontrolle (IEEE 802.3X)

Durch Flusskontrolle kann ein langsameres Gerät mit einem schnelleren Gerät kommunizieren, indem es das schnellere Gerät dazu auffordert, keine Pakete zu senden. Die Übertragung wird zeitweise angehalten, um einen Pufferüberlauf zu verhindern.

Informationen zur Konfiguration der Flusskontrolle für Ports oder LAGs finden Sie unter Festlegen der Port-Konfiguration bzw. Definieren von LAG-Parametern.

Backpressure

Bei Halbduplexverbindungen verhindert der empfangende Port Pufferüberläufe, indem er die Verbindung belegt, so dass diese für weitere Daten nicht verfügbar ist.

Informationen zur Konfiguration der Flusskontrolle für Ports oder LAGs finden Sie unter Festlegen der Port-Konfiguration bzw. Definieren von LAG-Parametern.

Virtuelle Kabelprüfung (VCT)

VCT erkennt und meldet Probleme mit der Verkabelung bei Kupferverbindungen (z. B. Kabelunterbrechungen und -kurzschlüsse). Weitere Informationen zum Austesten von Kabelverbindungen finden Sie unter Ausführen der Kabeldiagnose.

MDI/MDIX-Unterstützung

Wenn die Funktion Auto-Negotiation aktiviert ist, erkennt der Switch automatisch, ob das an einem RJ-45-Anschluss angeschlossene Kabel gekreuzt oder durchgehend ist.

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

Informationen zur MDI/MDIX-Konfiguration für Ports oder LAGs finden Sie unter Festlegen der Port-Konfiguration bzw. Definieren von LAG-Parametern.

Auto-Negotiation

Bei Auto-Negotiation kann das Gerät Betriebsarten "verhandeln". Die Funktion Auto-Negotiation ist ein Mittel zum Informationsaustausch zwischen zwei Geräten mit gemeinsamem Punkt-zu-Punkt-Verbindungssegment und ermöglicht die automatische Konfiguration beider Geräte, um deren Übertragungsfähigkeiten optimal zu nutzen.

Bei den Geräten der PowerConnect 3400-Reihe wird diese automatische Abstimmung durch Port-Anzeige optimiert. Anhand der Port-Anzeige kann der Systemadministrator die angezeigten Port-Geschwindigkeiten konfigurieren.

Weitere Informationen zur Funktion Auto-Negotiation finden Sie unter Festlegen der Port-Konfiguration bzw. Definieren von LAG-Parametern.

Unterstützte MAC-Adress-Funktionen

MAC-Adress-Unterstützung

Das Gerät unterstützt bis zu 8.000 MAC-Adressen. Bestimmte MAC-Adressen sind für den Systembetrieb reserviert.

Statische MAC-Einträge

MAC-Einträge können manuell in die Bridging-Tabelle eingetragen werden; dies stellt eine Alternative zum Auslesen der Informationen aus den eingehenden Frames dar. Benutzerdefinierte Einträge unterliegen keinem Alterungsprozess (Aging) und bleiben auch nach einem Reset oder Neustart erhalten.

Weitere Informationen finden Sie unter Definieren von statischen Adressen.

Selbstlernende MAC-Adressen

Der Switch kann MAC-Adressen aus eingehenden Paketen automatisch auslesen und erfassen. Die MAC-Adressen werden in der Bridging-Tabelle gespeichert.

Automatisches Altern von MAC-Adressen

MAC-Adressen, für die über einen bestimmten Zeitraum kein Datenverkehr stattfindet, veralten. Dadurch wird ein Überlauf der Bridging-Tabelle verhindert.

Weitere Informationen zur Konfiguration des Parameters MAC Address Age Out Time (Alterungszeit für MAC-Adressen) finden Sie unter Anzeigen von dynamischen Adressen.

VLAN-fähiges MAC-basiertes Switching

Das Bridging des Gerätes ist stets VLAN-fähig. Klassisches Bridging (IEEE802.1D), bei dem Frames nur nach ihrer MAC-Zieladresse weitergeleitet werden, findet nicht statt. Eine ähnliche Funktionalität lässt sich jedoch für Frames ohne Kennung konfigurieren. Frames, die an eine MAC-Zieladresse adressiert sind, die mit keinem Anschluss verknüpft ist, werden an alle Anschlüsse des relevanten VLANs weitergeleitet.

MAC Multicast

Der Multicastdienst ist ein eingeschränkter Broadcastdienst, über den sich Eins-zu-Viele- und Viele-zu-Viele-Verbindungen für die Informationsverteilung einrichten lassen. Man spricht von einem Layer 2-Multicastdienst, wenn ein Einzelframe an eine bestimmte Multicastadresse adressiert wird und von dort Kopien dieses Frames an alle relevanten Ports übermittelt werden.

Weitere Informationen finden Sie unter Zuweisen von Parametern für das Multitaskingmerkmal Alle weiterleiten.

Layer 2-Funktionen

IGMP-Snooping

Beim IGMP-Snooping wird der Inhalt von IGMP-Frames geprüft, bevor diese geräteseitig von Workstations an einen Upstream-Multicastrouter weitergeleitet werden. Anhand des Frames kann das Gerät erkennen, welche Workstations für Multicastsitzungen konfiguriert sind und welche Multicastrouter gerade Multicastframes übermitteln.

Weitere Informationen finden Sie unter IGMP-Snooping.

Port-Spiegelung

Bei der Port-Spiegelung wird der Netzwerkdatenverkehr überwacht und gespiegelt, indem Kopien eingehender und ausgehender Pakete von einem überwachten Port an einen überwachenden Port weitergeleitet werden. Der Benutzer kann hierbei festlegen, welcher Ziel-Port Kopien des gesamten Datenverkehrs von einem bestimmten Quell-Port erhält.

Weitere Informationen finden Sie unter Festlegen von Portspiegelungs-Sitzungen.

Broadcaststurmkontrolle

Mit der Broadcaststurmkontrolle lässt sich die Menge der vom Gerät angenommenen und weitergeleiteten Multicast- und Broadcastframes begrenzen.

Beim Weiterleiten von Layer-2-Frames werden Broadcast- und Multicastframes an alle Ports des relevanten VLANs gesendet. Dies belegt Bandbreite und bewirkt, dass sämtliche Knoten an allen Ports geladen werden.

Weitere Informationen finden Sie unter Aktivieren der Broadcaststurm-Kontrolle.

VLAN-Funktionen

VLAN-Unterstützung

VLANs sind Gruppen von Switching-Ports mit gemeinsamer Broadcastdomäne. Pakete werden VLANs entweder aufgrund der VLAN-Kennung oder einer Kombination von Ingress-Port und Paketinhalt zugeordnet. Pakete mit gemeinsamen Attributen können im gleichen VLAN gruppiert werden.

Weitere Informationen finden Sie unter Konfigurieren von VLANs.

Portbasierte virtuelle LANs (VLANs)

Portbasierte VLANs ordnen eingehende Pakete VLANs aufgrund des Ingress-Ports zu.

Weitere Informationen finden Sie unter Definieren von VLAN-Einstellungen für Ports.

Umfassende VLAN-Tagging-Konformität gemäß IEEE 802.1Q

IEEE 802.1Q definiert eine Architektur für virtuelle Bridge-LANs, die in VLANs bereitgestellten Dienste sowie die Protokolle und Algorithmen für die Dienstebereitstellung.

GVRP-Unterstützung

Das GARP-VLAN-Registrierungsprotokoll (GVRP) ermöglicht ein IEEE 802.1Q-konformes VLAN-Pruning sowie eine dynamische VLAN-Generierung an 802.1Q Trunk-Ports. Ist GVRP aktiviert, registriert und verbreitet das Gerät die VLAN-Mitgliedschaft an allen Ports, die zur aktiven Basistopologie gehören (siehe auch Funktionen des Spanning Tree-Protokolls).

Weitere Informationen finden Sie unter Konfigurieren von GVRP-Parametern.

Private VLANs

Private VLAN-Ports, eine Layer 2-Sicherheitsfunktion, ermöglichen die Port-Trennung innerhalb derselben Broadcastdomäne.

Weitere Informationen zu privaten VLANs finden Sie unter Konfigurieren von privaten VLANs.

Funktionen des Spanning Tree-Protokolls

Spanning Tree-Protokoll (STP)

802.1d Spanning Tree ist eine Standardanforderung an Layer 2-Switches, die es Bridges ermöglicht, L2-Weiterleitungsschleifen automatisch zu vermeiden bzw. aufzuheben. Switches tauschen über speziell formatierte Frames Konfigurationsinformationen untereinander aus, wodurch sich die Weiterleitung an den Ports selektiv aktivieren bzw. deaktivieren lässt.

Weitere Informationen finden Sie unter Konfigurieren des Spanning-Tree-Protokolls.

Fast Link

Die Konvergierung kann bei STP 30 bis 60 Sekunden dauern. Während dieser Zeit erkennt STP mögliche Schleifen, wobei der Zeitaufwand für die Verbreitung von Statuswechseln sowie für Reaktion aller relevanten Geräte eingeplant wird. Für viele Anwendungen ist eine Reaktionszeit von 30 bis 60 Sekunden zu lang. Die Fast Link-Option umgeht diese Verzögerung und kann daher in Netzwerktopologien eingesetzt werden, in denen keine Weiterleitungsschleifen auftreten.

Weitere Informationen zur Aktivierung von Fast Link für Ports und LAGs finden Sie unter Definieren von STP-Porteinstellungen und Definieren von statischen Adressen.

IEEE 802.1w Rapid Spanning Tree

Bei Spanning Tree kann es 30 bis 60 Sekunden dauern, bis jeder Host entschieden hat, ob die Host-Ports den Datenverkehr aktiv weiterleiten oder nicht. Rapid Spanning Tree (RSTP) erkennt, wie Netzwerktopologien genutzt werden, und ermöglicht daher eine schnellere Konvergenz – und dies ohne Generierung

von Weiterleitungsschleifen.

Weitere Informationen finden Sie unter Definieren von Rapid Spanning Tree.

IEEE 802.1s Multiple Spanning Tree

Im Multiple Spanning Tree-Betrieb (MSTP) werden VLANs bestimmten STP-Instanzen zugewiesen. MSTP unterstützt verschiedene Lastausgleichskonfigurationen. Pakete, die verschiedenen VLANs zugewiesen sind, werden auf unterschiedlichen Pfaden der MSTP-Regionen (MST Regions) übermittelt. Bei diesen Regionen handelt es sich um eine oder mehrere MSTP-Bridges, die für die Frame-Übermittlung zur Verfügung stehen. Standardmäßig können Administratoren den VLAN-Verkehr über bestimmte Pfade leiten.

Weitere Informationen finden Sie unter Konfigurieren des Spanning-Tree-Protokolls.

Link-Aggregation

Link-Aggregation

Es lassen sich maximal acht aggregierte Leitungen definieren, die wiederum mit bis zu acht Mitglied-Ports zu einer Link Aggregated Group (LAG) zusammengefasst werden können. Hierdurch ergeben sich folgende Möglichkeiten:

- Fehlertoleranz hinsichtlich physischer Verbindungsunterbrechung
- Verbindungen mit höherer Bandbreite
- Verbesserte Bandbreitengranularität
- Hohe Server-Verbindungsbandbreite

Eine LAG besteht aus Ports mit der gleichen Geschwindigkeit im Vollduplexbetrieb.

Weitere Informationen finden Sie unter Definieren von LAG-Parametern.

Link-Aggregation und LACP

Durch verbindungsübergreifenden Peer-Austausch überwacht LACP permanent die Aggregationsfähigkeit der verschiedenen Verbindungen und gewährleistet auf diese Weise eine maximale Aggregationsfähigkeit zwischen den einzelnen Gerätepaaren. LACP bestimmt, konfiguriert, bindet und überwacht automatisch die Port-Verknüpfungen innerhalb des Systems.

Weitere Informationen finden Sie unter Aggregieren von Ports.

BootP- und DHCP-Clients

Mit DHCP können beim Systemstart zusätzliche Setup-Parameter von einem Netzwerkserver empfangen werden. Der DHCP-Dienst ist ein laufender Prozess. DHCP ist eine Erweiterung von BootP.

Weitere Informationen zu DHCP finden Sie unter Definieren von DHCP IP-Schnittstellenparametern.

QoS-Funktionen (Quality of Service)

Class-of-Service 802.1p

Bei der IEEE 802.1p-Signalisierungstechnik handelt es sich um einen OSI Layer-2-Standard zur Markierung und Prioritätseinteilung von Netzwerkdatenverkehr in der Sicherungs-/MAC-Schicht. 802.1p-Datenverkehr wird klassifiziert und zum Ziel gesendet. Es werden keine Bandbreitenreservierungen oder -begrenzungen eingerichtet oder erzwungen. 802.1p ist ein Nebenprodukt des 802.1Q-Standards (VLANs). 802.1p vereinbart, ähnlich wie das IP Precedence IP Header Bit-Feld, acht Prioritätsebenen.

Weitere Informationen finden Sie unter Konfigurieren von Quality of Service (QoS).

Geräteverwaltungsfunktionen

SNMP-Alarme und Trap-Protokolle

Das System protokolliert alle Ereignisse mit Schweregrad und Zeitangabe. Ereignisse werden als SNMP-Traps an eine Trap-Empfängerliste übermittelt.

Weitere Informationen zu SNMP-Alarmen und Traps finden Sie unter Definieren von SNMP-Parametern.

SNMP-Versionen 1, 2 und 3

Das Simple Network Management Protocol (SNMP) kontrolliert über das UDP/IP-Protokoll sämtliche Systemzugriffe. Hierfür ist eine Liste mit Community-Einträgen definiert, die jeweils aus einer Community-Zeichenfolge und den zugehörigen Zugriffsrechten bestehen. Es gibt 3 SNMP-Sicherheitsebenen: Nur-Lese-Zugriff, Schreib-Lese-Zugriff und Superuser. Nur ein Superuser hat Zugang zur Community-Tabelle.

Weitere Informationen finden Sie unter Definieren von SNMP-Parametern.

Webbasierte Verwaltung

Über die webbasierte Verwaltung lässt sich das System von jedem Webbrowser aus verwalten. Das System ist mit einem Embedded Web Server (EWS) ausgestattet, der HTML-Seiten erzeugt, über die das System überwacht und konfiguriert werden kann. Systemintern werden webbasierte Eingaben in Konfigurationsbefehle, MIB-Variableneinstellungen sowie andere verwaltungsbezogene Einstellungen konvertiert.

Herunterladen und Hochladen von Konfigurationsdateien

Die Gerätekonfiguration ist in einer Konfigurationsdatei gespeichert. Die Konfigurationsdatei enthält sowohl systemweite als auch portspezifische Gerätekonfigurationsdaten. Das System kann Konfigurationsdateien als Sammlung von CLI-Befehlen anzeigen, die sich speichern und als Textdateien bearbeiten lassen.

Weitere Informationen finden Sie unter Verwalten von Dateien.

TFTP (Trivial File Transfer Protocol)

Das Gerät unterstützt Boot Images sowie das Hoch- und Herunterladen von Software- bzw. Konfigurationsdateien über TFTP.

Fernüberwachung

Die Fernüberwachung (Remote Monitoring, RMON) ist eine SNMP-Erweiterung, die umfassende Möglichkeiten zur Überwachung des Netzwerkverkehrs bereitstellt (im Gegensatz zum SNMP-Protokoll, das eine Verwaltung und Überwachung von Netzwerkgeräten ermöglicht). RMON ist eine Standard-MIB, die aktuelle und frühere MAC-Layer-Statistiken und -Kontrollobjekte definiert, wodurch sich im gesamten Netzwerk Echtzeitinformationen erfassen lassen.

Weitere Informationen finden Sie unter Anzeigen von Statistiken.

Befehlszeilenschnittstelle (CLI)

Die Befehlszeilenschnittstelle (Command Line Interface, CLI) entspricht unter syntaktischen und semantischen Gesichtspunkten weitgehend der gängigen Branchenpraxis. Die CLI setzt sich aus obligatorischen und optionalen Elementen zusammen. Die automatische Vervollständigung von Befehlen und Schlüsselwörtern macht den CLI-Interpreter besonders benutzerfreundlich und beschleunigt Eingaben.

Syslog

Das Syslog-Protokoll ermöglicht die Übermittlung von Ereignisbenachrichtigungen an mehrere Remote-Server, wo sich diese speichern und prüfen lassen, um entsprechend reagieren zu können. Das System gibt Benachrichtigungen zu signifikanten Ereignissen in Echtzeit aus und führt Buch über diese Ereignisse für eine eventuelle Nachbereitung.

Weitere Informationen zu Syslog finden Sie unter Verwalten von Protokollen.

SNTP

Das einfache Netzwerkzeit-Protokoll (Simple Network Time Protocol, SNTP) gewährleistet eine präzise, bis auf die Millisekunde genaue Zeitsynchronisierung der Ethernet-Switch-Uhr im Netzwerk. Die Zeitsynchronisierung erfolgt über einen SNTP-Server des Netzwerks. Die Zeitquellen werden über entsprechende Strata realisiert. Strata definieren den Abstand zur Referenzuhr. Je höher das Stratum (wobei Null den höchsten Wert darstellt), desto genauer arbeitet die Uhr.

Weitere Informationen finden Sie unter Konfigurieren von SNTP-Einstellungen.

Domain Name System (DNS)

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

Weitere Informationen finden Sie unter "Konfigurieren von Domänennamensystemen".

Traceroute

Traceroute erkennt, über welche IP-Routen die Datenpakete im Rahmen des Weiterleitungsprozesses übermittelt werden. Das Dienstprogramm CLI Traceroute kann wahlweise im User EXEC- oder Privileged EXEC-Modus ausgeführt werden.

Sicherheitsfunktionen

SSL

Secure Socket Layer (SSL) ist ein Protokoll, das auf Anwendungsebene arbeitet und durch Schutz-, Authentifizierungs- und Datenintegritätsmaßnahmen sichere Datentransaktionen ermöglicht. Das Protokoll greift hierfür auf Zertifikate und öffentliche sowie private Schlüssel zurück.

Portbasierte Authentifizierung (802.1x)

Bei Systemen mit portbasierter Authentifizierung erfolgt die Identitätsprüfung der Systembenutzer für jeden einzelnen Port über einen externen Server. Nur

überprüfte und zugelassene Systembenutzer dürfen Daten senden und empfangen. Die Port-Authentifizierung erfolgt über einen RADIUS-Server (Remote Authentication Dial In User Service) unter Verwendung des EAP-Protokolls (Extensible Authentication Protocol).

Weitere Informationen finden Sie unter Konfigurieren der portbasierten Authentifizierung.

Port-Sperre

Die Port-Sperre (Locked Port) erhöht die Netzwerksicherheit, indem jeder Port nur für Benutzer mit bestimmten MAC-Adressen freigegeben werden kann. Diese Adressen werden manuell definiert oder vom jeweiligen Port automatisch erkannt. Liegt ein Frame an einem gesperrten Port an und ist die MAC-Quelladresse dieses Rahmens nicht an diesen Port gekoppelt, wird der Schutzmechanismus automatisch aktiviert.

Weitere Informationen finden Sie unter Konfigurieren von Port-Sicherheit.

RADIUS-Client

RADIUS ist ein Client/Server-basiertes Protokoll. Ein RADIUS-Server pflegt eine Benutzerdatenbank mit benutzerbezogenen Authentifizierungsinformationen wie Benutzername, Kennwort und Accounting-Daten.

Weitere Informationen finden Sie unter Konfigurieren von RADIUS-Einstellungen.

SSH

Secure Shell (SSH) ist ein Protokoll, über das eine geschützte Remote-Verbindung zu einem anderen Gerät hergestellt werden kann. Derzeit wird SSH-Version 2 unterstützt. Die SSH-Server-Funktion ermöglicht es SSH-Clients, eine sichere, verschlüsselte Verbindung zu anderen Geräten herzustellen. Über diese Verbindung wird eine Funktionalität bereitgestellt, die mit einer eingehenden Telnet-Verbindung vergleichbar ist. SSH nutzt die RSA- und DSA Public Key-Verschlüsselung für Geräteverbindungen sowie Authentifizierung.

TACACS+

TACACS+ bietet eine zentrale Sicherheitsfunktionalität für die Validierung von Benutzer(zugriffe)n. TACACS+ stellt ein zentrales Benutzerverwaltungssystem bereit, das jedoch die Konsistenz zu RADIUS und anderen Authentifizierungsprozessen wahrt.

Weitere Informationen finden Sie unter Definieren von TACACS+-Einstellungen.

Kennwortverwaltung

Die Kennwortverwaltung sorgt für mehr Netzwerksicherheit sowie eine verbesserte Kennwortkontrolle. Bei den Kennwörtern für den SSH-, Telnet-, HTTP-, HTTPS- und SNMP-Zugang handelt es sich um zugewiesene Sicherheitsfunktionen. Weitere Informationen zur Kennwortverwaltung finden Sie unter Verwalten von Kennwörtern.

Zusätzliche CLI-Dokumentation

Das auf der Dokumentations-CD vorliegende CLI-Referenzhandbuch enthält Informationen zu den CLI-Befehlen für die Gerätekonfiguration. Sie finden hier neben einer Beschreibung der einzelnen Befehle Hinweise zu Syntax, Standardwerten und Richtlinien sowie entsprechende Beispiele.

Zurück zum Inhalt

Zurück zum Inhalt

Hardwarebeschreibung

Dell™ PowerConnect™ 34XX- Systeme Benutzerhandbuch

Port-Beschreibung

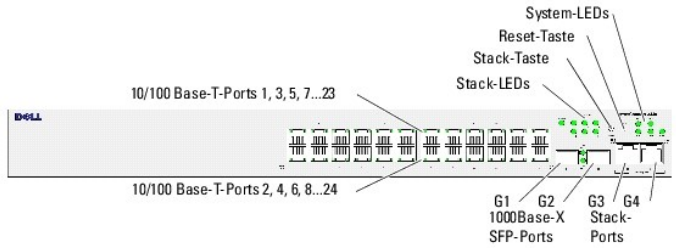
Beschreibung der PowerConnect 3424-Ports

Der PowerConnect 3424 verfügt über die folgenden Ports:

- **24 Fast Ethernet-Ports** — Als 10/100Base-T-Ports gekennzeichnete RJ-45-Anschlüsse
- **2 Fiber-Ports** – Als 1000Base-X SFP-Ports gekennzeichnet
- **2 Gigabit-Ports** – Als 1000Base-T-Ports gekennzeichnet
- **Konsolenport** – RS-232-Anschluss

Die folgende Abbildung zeigt die Vorderseite des PowerConnect 3424.

Abbildung 2-1. Vorderseite des PowerConnect 3424



An der Gerätevorderseite befinden sich 24 RJ-45-Anschlüsse (Port 1-24). Die obere Anschlussreihe enthält die ungeraden Nummern 1-23, die untere Reihe die geraden Nummern 2-24. Darüber hinaus befinden sich hier zwei Glasfaseranschlüsse (Port G1 und Port G2) sowie zwei Kupferanschlüsse (Port G3 und Port G4). Die Ports G3 und G4 können wahlweise als Stack-Ports oder zur Weiterleitung des Netzwerkverkehrs in einem Standalone-Modus genutzt werden.

An der Gerätevorderseite befinden sich zwei Tasten. Über die Taste Stack ID wird die Nummer der Geräteeinheit eingestellt. Die zweite Taste ist die Reset-Taste, über die sich das Gerät manuell zurücksetzen lässt. Um eine versehentliche Betätigung dieser Taste zu vermeiden, ist die Reset-Taste so angebracht, dass sie nicht über die Frontblende des Gerätes hinausragt. Sämtliche LEDs befinden sich an der Gerätevorderseite.

Die folgende Abbildung zeigt die Rückseite des PowerConnect 3424:

Abbildung 2-2. Rückseite des PowerConnect 3424

An der Geräterückseite befinden sich ein RPS-Anschluss, ein Anschluss für eine Konsole sowie ein Stromanschluss.

Beschreibung der PowerConnect 3448-Ports

Der PowerConnect 3448 Gerät verfügt über die folgenden Ports:

- **48 FE-Ports** – Als 10/100Base-T-Ports gekennzeichnete RJ-45-Anschlüsse
- **2 Fiber-Ports** – Als 1000Base-X SFP-Ports gekennzeichnet
- **2 Gigabit-Ports** – Als 1000Base-T-Ports gekennzeichnet
- **Konsolenport** – RS-232-Anschluss für Konsole

Die folgende Abbildung zeigt die Vorderseite des PowerConnect 3448.

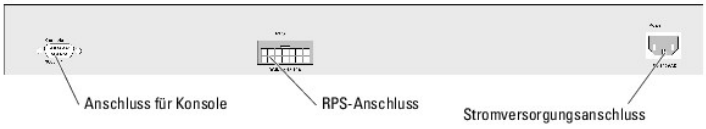
Abbildung 2-3. Vorderseite des PowerConnect 3448

An der Gerätevorderseite befinden sich 48 RJ-45-Anschlüsse (Port 1-48). Die obere Anschlussreihe enthält die ungeraden Nummern 1-47, die untere Reihe die geraden Nummern 2-48. Darüber hinaus befinden sich hier zwei Glasfaseranschlüsse (Port G1 und Port G2) sowie zwei Kupferanschlüsse (Port G3 und Port G4). Die Ports G3 und G4 können wahlweise als Stack-Ports oder zur Weiterleitung des Netzwerkverkehrs in einem Standalone-Gerät genutzt werden.

An der Gerätevorderseite befinden sich zwei Tasten. Über die Taste Stack ID wird die Nummer der Geräteeinheit eingestellt. Die zweite Taste ist die Reset-Taste, über die sich das Gerät manuell zurücksetzen lässt. Um eine versehentliche Betätigung dieser Taste zu vermeiden, ist die Reset-Taste so angebracht, dass sie nicht über die Frontblende des Gerätes hinausragt. Sämtliche LEDs befinden sich an der Gerätevorderseite.

Die folgende Abbildung zeigt die Rückseite des PowerConnect 3448.

Abbildung 2-4. Rückseite des PowerConnect 3448



An der Geräterückseite befinden sich ein RPS-Anschluss, ein Anschluss für eine (externe) Konsole sowie ein Stromanschluss.

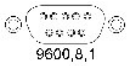
SFP-Ports

Bei den SFP-Ports (Small Form-Factor Pluggable) handelt es sich um eine als 1000Base-SX oder LX gekennzeichnete serielle 2-Draht-Schnittstelle (Two-Wire Serial Interface, TWSI) für die Kommunikation über ein CPLD-Gerät (Complex Programmable Logic Device).

RS-232-Anschluss für Konsole

DB-9-Anschluss für Terminalverbindungen. Dient zur Fehlersuche und ermöglicht Softwaredownloads etc. Die Standardbaudrate beträgt 9.600 Bit/s. Die Baudrate kann von 2.400 bis 115.200 Bit/s frei konfiguriert werden.

Abbildung 2-5. Anschluss für Konsole



Abmessungen

Die Abmessungen der Geräte PowerConnect 3424/P und PowerConnect 3448/P sind wie folgt:

PoE-Modell:

- **Breite** – 440 mm
- **Tiefe** – 387 mm
- **Höhe** – 43,2 mm

Sonstige Modelle (nicht PoE):

- **Breite** – 440 mm
- **Tiefe** – 257 mm
- **Höhe**: 43,2 mm

LED-Definitionen

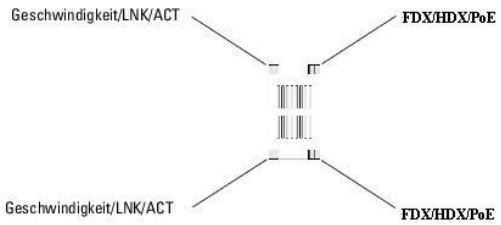
An der Vorderseite befinden sich mehrere Leuchtdioden (LEDs), die den aktuellen Gerätestatus signalisieren (Verbindung, Netzteile, Lüfter und Systemdiagnose).

Port-LEDs

Jeder 10/100/1000 Base-T- und 10/100 Base-T-Port verfügt über zwei LEDs. Die Geschwindigkeitsanzeige befindet sich an der linken, die LED für Verbindung/Duplex/Aktivität an der rechten Seite des zugehörigen Ports.

Die folgende Abbildung zeigt die 10/100 Base-T-Port-LEDs der Switches PowerConnect 3424 /P und PowerConnect 3448/P:

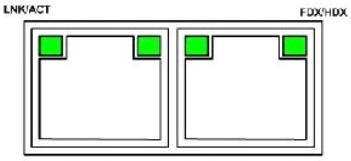
Abbildung 2-6. LEDs des 10/100 BaseT-Ports (RJ-45, Kupfer)



Die als RJ-45-Anschlüsse ausgeführten 100 Base-T-Ports der Modelle PowerConnect 3424 /P und PowerConnect 3448/P verfügen über zwei LEDs, die mit LNK/ACT beschriftet sind.

Die folgende Abbildung zeigt die LEDs des 100 Base-T-Ports.

Abbildung 2-7. LEDs des 1000 BaseT-Ports (RJ-45)



Die folgende Tabelle bietet einen Überblick über die RJ-45-LEDs der Modelle PowerConnect 3424 und PowerConnect 3448:

Tabelle 2-1. RJ-45-LEDs (100BaseT) der Modelle PowerConnect 3424 und PowerConnect 3448

LED	Farbe	Beschreibung
LNK/ACT/Geschwindigkeit	Grün (konstant)	Der Port arbeitet mit 100 Mbit/s.
	Grün (blinkend)	Der Port sendet bzw. empfängt Daten mit 100 Mbit/s.
	Gelb (konstant)	Der Port arbeitet mit 10 Mbit/s.
	Gelb (blinkend)	Der Port sendet bzw. empfängt Daten mit 10 Mbit/s.
	Aus	Der Port ist derzeit nicht in Betrieb.
FDX	Grün (konstant)	Der Port arbeitet derzeit im Vollduplexmodus.
	Aus	Der Port arbeitet derzeit im Halbduplexmodus.

Die folgende Tabelle bietet einen Überblick über die RJ-45-LEDs der Modelle PowerConnect 3424P und PowerConnect 3448P:

Tabelle 2-2. RJ-45-LEDs der Modelle PowerConnect 3424P und PowerConnect 3448P (100BaseT, Kupfer)

LED	Farbe	Beschreibung
Geschwindigkeit/LNK/ACT	Grün (konstant)	Der Port ist derzeit mit 100 Mbit/s verbunden.
	Grün (blinkend)	Die Ports arbeiten derzeit mit 100 Mbit/s.
	Aus	Der Port arbeitet mit 10 Mbit/s oder ist nicht verbunden.
PoE	Grün (konstant)	Das PD (Powered Device) wurde erkannt und arbeitet bei normaler Last. Weitere Informationen zu PDs finden Sie unter Power-Over-Ethernet.
	Gelb (konstant)	Am PD ist eine Überlastung bzw. ein Kurzschluss aufgetreten. Weitere Informationen zu PoE-Fehlern finden Sie unter Power-Over-Ethernet.
	Gelb (blinkend)	Das PD-Stromversorgungskonzept überschreitet die vorgegebene Stromzuweisung. Weitere Informationen zur PoE-Stromzuweisung finden Sie unter Power-Over-Ethernet.
	Aus	Es wurde kein PD erkannt.

Gigabit-Port-LEDs

Die folgende Tabelle bietet einen Überblick über die LEDs des Gigabit-Ports (Stack-Port):

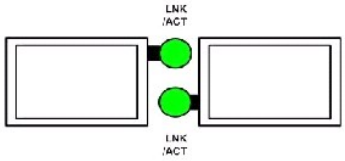
Tabelle 2-3. RJ-45-LEDs der Modelle PowerConnect 3424 und PowerConnect 3448 (100BaseT, Kupfer)

LED	Farbe	Beschreibung
LNK/ACT/Geschwindigkeit	Grün (konstant)	Der Port arbeitet mit 1000 Mbit/s.
	Grün (blinkend)	Der Port sendet bzw. empfängt Daten mit 1000 Mbit/s.
	Gelb (konstant)	Der Port arbeitet mit 10 Mbit/s oder 100 Mbit/s.
	Gelb (blinkend)	Der Port sendet bzw. empfängt Daten mit 10 oder 100 Mbit/s.
	Aus	Der Port ist derzeit nicht in Betrieb.
FDX	Grün (konstant)	Der Port arbeitet derzeit im Vollduplexmodus.
	Aus	Der Port arbeitet derzeit im Halbduplexmodus.

SFP-LEDs

Jeder SFP-Port verfügt über eine LED, die mit LNK/ACT beschriftet ist. Bei den Modellen PowerConnect 3424/P und PowerConnect 3448/P befinden sich diese runden LEDs genau zwischen den Ports. Die folgenden Abbildungen zeigen die LEDs der einzelnen Geräte.

Abbildung 2-8. SFP-Port-LEDs



Die Bedeutung der SFP-Port-LEDs sind in der folgenden Tabelle beschrieben:

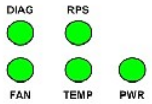
Tabelle 2-4. SFP-Port-LEDs

LED	Farbe	Beschreibung
LNK/ACT	Grün (konstant)	Es besteht eine Verbindung.
	Grün (blinkend)	Der Port sendet bzw. empfängt gerade Daten.
	Aus	Der Port ist derzeit nicht verbunden.

System-LEDs

Die System-LEDs der Modelle PowerConnect 3424 /P und PowerConnect 3448/P liefern Informationen zu den Netzteilen, Lüftern und Temperaturbedingungen sowie dem aktuellen Diagnosestatus der Geräte. Die folgende Abbildung zeigt die System-LEDs:

Abbildung 2-9. System-LEDs



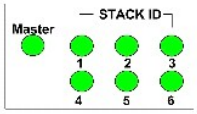
Die folgende Tabelle enthält die Anzeigemöglichkeiten der System-LEDs.

Tabelle 2-5. System-LEDs

LED	Farbe	Beschreibung
Netzteil (PWR)	Grün (konstant)	Der Switch ist eingeschaltet.
	Aus	Der Switch ist ausgeschaltet.
Redundantes Netzteil (RPS) (Modelle: 3424 und 3448)	Grün (konstant)	Das RPS ist derzeit in Betrieb.
	Rot (konstant)	Das RPS ist ausgefallen.
	Aus	Das redundante Netzteil ist nicht angeschlossen.
Redundantes Netzteil (RPS) (Modelle: 3424P und 3448P)	Grün (konstant)	Das RPS ist derzeit in Betrieb.
	Aus	Das redundante Netzteil ist ausgefallen oder nicht angeschlossen.
Diagnose (DIAG)	Grün (blinkend)	Der Systemdiagnosetest wird derzeit durchgeführt.
	Grün (konstant)	Der Systemdiagnosetest wurde erfolgreich abgeschlossen.
	Rot (konstant)	Der Systemdiagnosetest ist fehlgeschlagen.
	Aus	Das System arbeitet ordnungsgemäß.
Temperatur (TEMP)	Rot (konstant)	Die Gerätetemperatur liegt außerhalb des zulässigen Bereichs.
	Aus	Die Betriebstemperatur des Gerätes liegt im zulässigen Bereich.
Lüfter (FAN)	Grün (konstant)	Alle Gerätelüfter arbeiten normal.
	Rot (konstant)	Ein oder mehrere Gerätelüfter sind nicht in Betrieb.

Die Stack-LEDs geben die Position der Einheit im Stack an. Die folgende Abbildung zeigt die LEDs an der Gerätevorderseite.

Abbildung 2-10. Stack-LEDs



Die Stack-LEDs sind von 1 bis 6 durchnummeriert. Jede Stack-Einheit verfügt über eine leuchtende Stack-LED, die die Nummer der jeweiligen Einheit angibt. Leuchtet Stack-LED 1 oder 2, fungiert das Gerät als Mastereinheit bzw. als Mastersicherungseinheit.

Tabelle 2-6. Stack-LEDs

LED	Farbe	Beschreibung
Alle Stack-LEDs	Aus	Der Switch arbeitet derzeit als Standalone-Gerät.
Stack-LED 1-6 (S1-S6)	Grün (konstant)	Das Gerät ist als Stack-Einheit N gekennzeichnet.
	Aus	Das Gerät ist nicht als Stack-Einheit N gekennzeichnet.
Stack-Master-LED	Grün (konstant)	Das Gerät fungiert als Mastereinheit
	Aus	Das Gerät fungiert nicht als Mastereinheit

Netzteile

Das Gerät verfügt über ein internes Netzteil (Wechselstromeinheit) sowie einen Anschluss, über den man Geräte des Typs PowerConnect 3424/P oder PowerConnect 3448/P mit einer PowerConnect EPS-470-Einheit bzw. Geräte des Typs PowerConnect 3424 oder PowerConnect 3448 mit einer PowerConnect

RPS-600-Einheit verbinden kann. Die Modelle PowerConnect 3424/P und PowerConnect 3448/P verfügen über eine interne Stromversorgung (12 Volt).

Der Betrieb mit beiden Netzteilen wird durch Lastteilung geregelt. Die Netzteil-LEDs signalisieren hierbei den Netzteilstatus.

Die Modelle PowerConnect 3424/P und PowerConnect 3448/P verfügen über ein internes Netzteil mit 470 W (12 V/-48 V) und einer Gesamtleistung von 370 W für das PoE-Gerät mit 24 Ports.

Wechselstromnetzteil

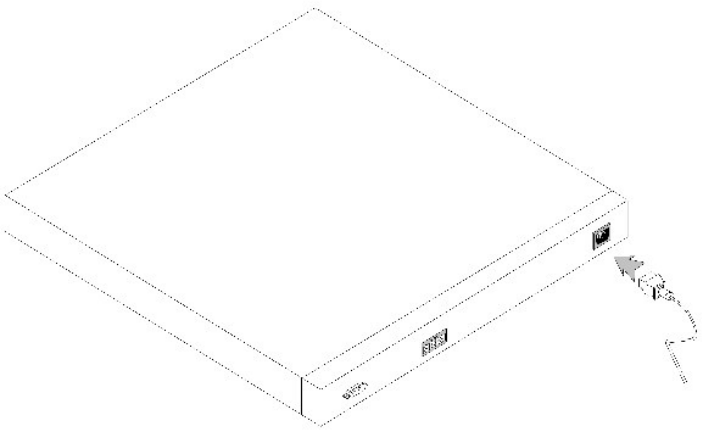
Das Wechselstromnetzteil unterstützt Netzspannungen von 90 bis 264 VAC sowie Netzfrequenzen von 47 bis 63 Hz. Das Wechselstromnetzteil ist mit einem Standardanschluss ausgestattet. Die LED-Anzeige an der Vorderseite signalisiert, ob die Wechselstromeinheit angeschlossen ist oder nicht.

Gleichstromnetzteil

Die Switches PowerConnect 3424 und PowerConnect 3448 lassen sich an einer externen RPS-600-Einheit anschließen, um eine redundante Stromversorgung zur Verfügung zu haben. Hierfür ist keine Konfiguration erforderlich. Die RPS-LED auf der Vorderseite zeigt an, ob die externe RPS-600-Einheit angeschlossen ist. Die Definition für die RPS-Anzeige finden Sie in Tabelle 2-5.

Die Switches PowerConnect 3424/P und PowerConnect 3448/P lassen sich an einer externen EPS-470-Einheit anschließen, um eine redundante Stromversorgung zur Verfügung zu haben. Hierfür ist keine Konfiguration erforderlich. Die RPS-LED auf der Vorderseite zeigt an, ob die externe EPS-470-Einheit angeschlossen ist. Die Definition für die RPS-Anzeige finden Sie in Tabelle 2-5.

Abbildung 2-11. Stromanschluss



Wird das Gerät an eine andere Stromquelle angeschlossen, reduziert sich die Ausfallwahrscheinlichkeit bei einem Stromausfall.

Taste Stack ID

An der Gerätevorderseite befindet sich die Taste Stack ID, die eine manuelle Auswahl der Geräte-ID für die Mastereinheit sowie andere Stack-Komponenten ermöglicht.

Der Stack-Master und die Stack-Komponenten müssen innerhalb von 15 Sekunden nach dem Gerätestart ausgewählt werden. Erfolgt die Auswahl des Stack-Masters nicht innerhalb von 15 Sekunden, wird das Gerät im Standalone-Modus gestartet. Um eine Geräte-ID für das Gerät vereinbaren zu können, ist ein erneuter Gerätestart erforderlich.

Der Stack-Master erhält die Geräte-ID 1 oder 2. Sind Geräteeinheit 1 und Geräteeinheit 2 verfügbar, fungiert die nicht gewählte Einheit als Mastersicherungseinheit. Stack-Komponenten erhalten eine separate Geräte-ID (3-6). Enthält ein Stack beispielsweise vier Geräteeinheiten, hat die Mastereinheit den Wert 1 oder 2 und die Mastersicherungseinheit (je nach Geräte-ID der Mastereinheit) den Wert 1 oder 2. Die dritte Stack-Komponente hat

den Wert 3 und die vierte Komponente den Wert 4.

ANMERKUNG: Eine Standalone-Einheit wird vom Gerät nicht automatisch erkannt. Wurde bereits eine Geräte-ID ausgewählt, die Taste Stack ID mehrmals betätigen, bis keine Stack-LED mehr leuchtet.

Reset-Taste

Die Switches PowerConnect 3424/P und PowerConnect 3448/P verfügen über eine Reset-Taste, die sich an der Vorderseite der Geräteeinheiten befindet und ein manuelles Zurücksetzen dieser Geräte ermöglicht. Ein Zurücksetzen der Mastereinheit hat zur Folge, dass der gesamte Stack zurückgesetzt wird. Wird nur eine Stack-Komponente zurückgesetzt, so hat dies keine Auswirkungen auf den Betrieb der übrigen Stack-Komponenten.

Die zentrale Reset-Schaltung des Switches wird während des Einschaltvorgangs sowie bei einem eventuellen Spannungsabfall aktiviert.

Belüftungssystem

Die Switches PowerConnect 3424/P und PowerConnect 3448/P mit PoE-Funktion verfügen über fünf integrierte Lüfter. Die Modelle PowerConnect 3424 und PowerConnect 3448 (ohne PoE-Unterstützung) sind mit zwei integrierten Lüftern ausgestattet. Der jeweilige Betriebsstatus kann anhand einer LED überprüft werden, die gegebenenfalls signalisiert, ob einer oder beide Lüfter defekt sind.

Zurück zum Inhalt

Zurück zum Inhalt

Installieren der PowerConnect-Switches 3424/P und 3448/P

Dell™ PowerConnect™ 34XX- Systeme Benutzerhandbuch

Standortvorbereitung

Die Modelle PowerConnect 3424 /P und PowerConnect 3448/P sind für die Montage in einem 19-Zoll-Standard-Rack sowie für die Tisch- bzw. Wandinstallation ausgelegt. Stellen Sie vor der Montage sicher, dass der ausgewählte Standort die unten beschriebenen Voraussetzungen erfüllt:

- **Stromversorgung** – Das Gerät sollte in der Nähe einer leicht zugänglichen Steckdose mit 100-240 V Wechselspannung und einer Netzfrequenz von 50-60 Hz installiert werden.
- **Allgemein** – Das redundante Netzteil (RPS) ist korrekt installiert, wenn die LEDs an der Gerätevorderseite leuchten.
- **PoE-Modelle** – Das redundante Netzteil (RPS) ist installiert, wenn die PoE-LEDs an Gerätevorderseite leuchten
- **Zugang** – Der Bediener sollte an der Vorderseite des Gerätes ausreichend Bewegungsfreiheit haben. Auch Verkabelung, Stromanschlüsse und Belüftungsöffnungen sollten problemlos zugänglich sein.
- **Verkabelung:** Die Kabel sollten so verlegt sein, dass elektrisches Rauschen durch Funksender, Funkverstärker, Stromleitungen sowie fluoreszierende Beleuchtungskörper vermieden werden.
- **Umgebungsbedingungen** – Die Betriebstemperatur des Gerätes sollte zwischen 0 und 50 ºC liegen, bei einer relativen Luftfeuchtigkeit von bis zu 95 %, nicht kondensierend.

Auspacken

Inhalt der Verpackung

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

- Gerät/Switch
- Netzkabel
- Gekreuztes RS-232-Kabel
- Selbsthaftende Gummiunterlagen
- Rack-Montagekit zur Installation im Rack oder Wandmontagekit
- Dokumentations-CD
- Produktinformationshandbuch

Auspacken des Gerätes

ANMERKUNG: Überprüfen Sie vor dem Auspacken des Gerätes die Verpackung, und melden Sie etwaige Beschädigungen unverzüglich.

1. Stellen Sie die Verpackung auf einen sauberen, ebenen Untergrund.
2. Öffnen Sie die Verpackung bzw. entfernen Sie den Deckel.
3. Entnehmen Sie das Gerät vorsichtig der Verpackung, und legen Sie es auf eine stabile und saubere Fläche.
4. Entfernen Sie das gesamte Verpackungsmaterial.
5. Untersuchen Sie das Gerät und Zubehör auf Beschädigungen. Schäden sollten unverzüglich gemeldet werden.

Montieren des Gerätes

Die folgenden Montageanweisungen gelten für die Modelle PowerConnect 3424/P und PowerConnect 3448/P. Der Anschluss für die Konsole befindet sich auf der Rückseite. Die Stromversorgungsanschlüsse befinden sich auf der Rückseite. Die Verbindung zu einer redundanten Stromversorgung (RPS) wird empfohlen, ist aber nicht erforderlich. Der RPS-Anschluss befindet sich auf der Rückseite der Geräte.

Montage in einem Rack

⚠ **VORSICHT: Lesen Sie die Sicherheitsinformationen im Produktinformationshandbuch. Sie finden hier Sicherheitshinweise zu Geräten, die mit dem Switch verbunden werden oder diesen unterstützen.**

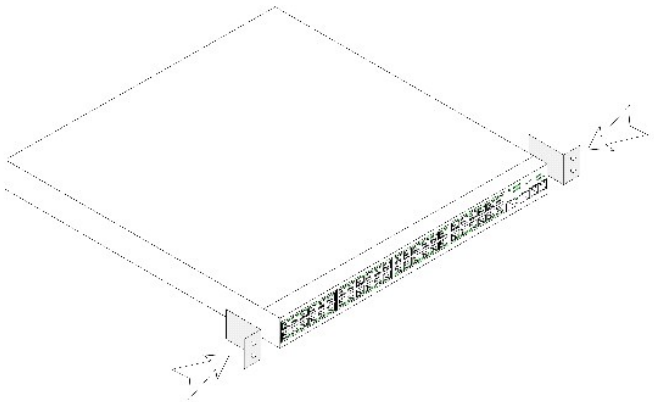
⚠ **VORSICHT: Trennen Sie alle Kabel von der Einheit, bevor Sie das PowerConnect-Gerät in einem Rack oder einem Schrank montieren.**

⚠ **VORSICHT: Wenn Sie mehrere Geräte in einem Rack einbauen, sollten Sie diese von unten nach oben montieren.**

1. Platzieren Sie das mitgelieferte Rackmontageblech auf einer Seite des Switches, wobei sich die Montagebohrungen am Switch mit den Montagebohrungen am Rackmontageblech decken müssen.

   Die folgende Abbildung zeigt an welchen Stellen die Halterungen montiert werden sollen.

Abbildung 3-1. Halterungen für die Rack-Montage anbringen



2. Führen Sie die mitgelieferten Schrauben in die Rack-Montagebohrungen ein, und ziehen Sie sie mit einem Schraubendreher fest.
3. Wiederholen Sie die Schritte für die Rack-Montagehalterung auf der anderen Seite des Gerätes.
4. Setzen Sie die Einheit in das 19-Zoll-Rack ein, und stellen Sie sicher, dass die Montagebohrungen am Gerät mit den Montagebohrungen am Rack übereinstimmen.
5. Befestigen Sie die Einheit mit den Rackschrauben (nicht im Lieferumfang enthalten) am Rack. Ziehen Sie zuerst die unteren und dann die oberen Schrauben an. Die Belüftungsöffnungen dürfen nicht versperrt sein.

Installieren auf einer ebenen Fläche

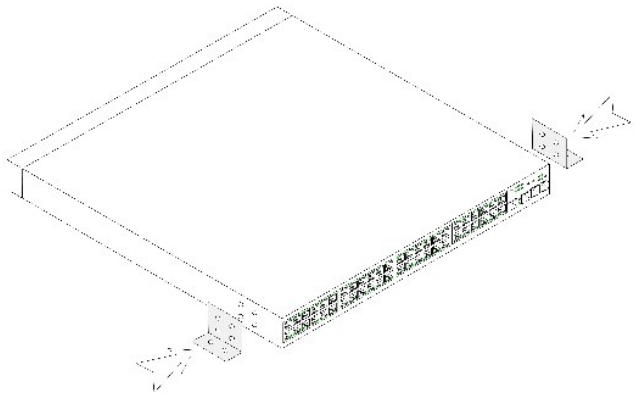
Falls kein Rack verwendet wird, muss das Gerät auf einer ebenen Fläche montiert werden. Die Tragfähigkeit der Fläche muss für das Gerät und die Gerätekabel ausreichen.

1. Befestigen Sie die Gummiunterlagen an den markierten Stellen auf der Unterseite des Gehäuses.
2. Stellen Sie das Gerät auf eine ebene Fläche, und lassen Sie an den Seiten mind. 5 cm und auf der Rückseite ca. 13 cm Platz.
3. Es muss eine ausreichende Belüftung gewährleistet sein.

Montieren des Gerätes an der Wand

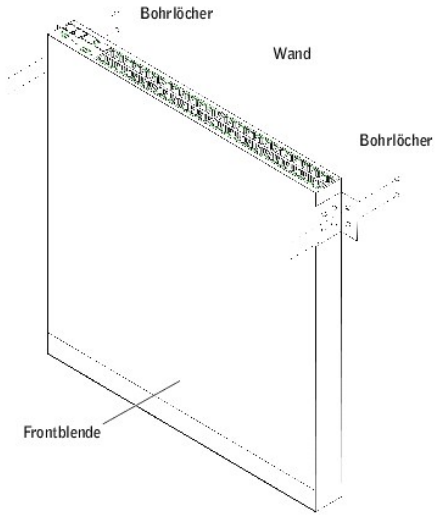
1. Halten Sie die mitgelieferte Wandmontagehalterung an eine Seite des Gerätes, wobei sich die Montagebohrungen am Gerät mit den Montagebohrungen an der Halterung decken müssen. Die folgende Abbildung zeigt an welchen Stellen die Halterungen montiert werden sollen.

Abbildung 3-2. Halterungen für die Wandmontage anbringen



2. Führen Sie die mitgelieferten Schrauben in die Rack-Montagebohrungen ein, und ziehen Sie sie mit einem Schraubendreher fest.
3. Wiederholen Sie die Schritte für die Wandmontagehalterung auf der anderen Seite des Gerätes.
4. Halten Sie das Gerät am Montagestandort gegen die Wand.
5. Markieren Sie an der Wand die Stellen, wo die Halteschrauben sitzen werden.
6. Bohren Sie an den markierten Stellen Löcher und setzen Sie entsprechende Dübel ein (nicht im Lieferumfang enthalten).
7. Befestigen Sie das Gerät mit Schrauben (nicht im Lieferumfang enthalten) an der Wand. Die Belüftungsöffnungen dürfen nicht versperrt sein.

Abbildung 3-3. Wandmontage eines Gerätes



Verbinden des Gerätes mit einem Terminal

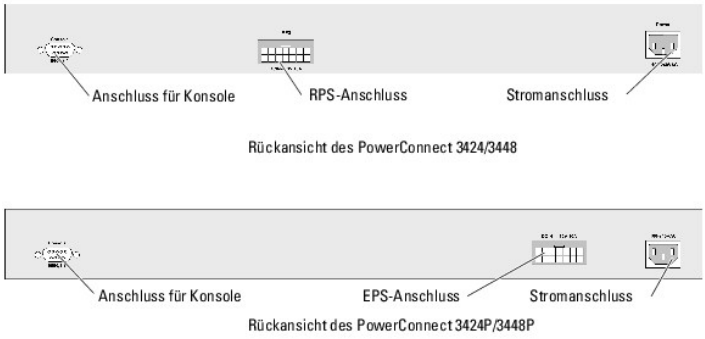
1. Verbinden Sie das andere Ende des gekreuzten Kabels RS-232 mit einem ASCII-Terminal oder dem seriellen Anschluss eines Desktop-Systems, auf dem eine Terminal- Emulationssoftware ausgeführt wird.
2. Verbinden Sie den DB-9-Anschluss am anderen Ende des Kabels mit der seriellen Schnittstelle des Gerätes.

Verbinden des Gerätes mit dem Netzteil

Verbinden Sie das mitgelieferte Netzkabel mit dem Stromanschluss auf der Rückseite.

ANMERKUNG: Schließen Sie noch nicht das Stromkabel an eine geerdete Netzsteckdose an. Verbinden Sie das Gerät mit einer Stromquelle. Siehe hierzu den Abschnitt Starten und Konfigurieren des Gerätes.

Abbildung 3-4. Stromanschluss an der Rückseite



Stellen Sie nach dem Anschließen des Gerätes an einer Stromquelle mit den Leuchtanzeigen auf der Vorderseite sicher, dass das Gerät korrekt verbunden ist und ordnungsgemäß funktioniert.

Installieren eines Stacks

Übersicht

Jedes Gerät kann als Standalone-Gerät oder als Stack-Komponente verwendet werden. Pro Stack werden sechs Geräte bzw. 192 Ports unterstützt.

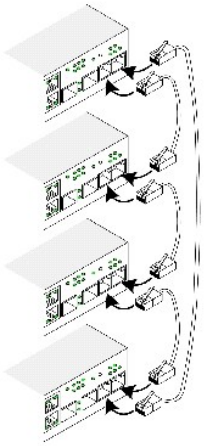
Für alle Stacks muss eine Mastereinheit und kann eine Mastersicherungseinheit vorhanden sein, und alle anderen mit dem Stack verbundenen Geräte sind abhängige Komponenten.

Stacking von Switches der Reihe PowerConnect 3400

Jeder Stack aus Switches der PowerConnect 3400-Reihe enthält eine einzelne Mastereinheit und kann eine Mastersicherungseinheit enthalten, während die übrigen Einheiten als abhängige Komponenten funktionieren.

Bei Switches der PowerConnect 3400-Reihe werden zum Stacking die als RJ-45-Anschlüsse ausgeführten Gigabit-Ethernet-Ports (G3 und G4) verwendet. Dadurch ergeben sich für die Geräte ohne weitere Zubehörteile erweiterte Stacking-Fähigkeiten. Verbinden Sie zum Stacking der Geräte den Port G3 am obersten Stack-Gerät und den Port G4 am Gerät direkt darunter mit einem Standardkabel der Kategorie 5. Wiederholen Sie diesen Vorgang, bis alle Geräte verbunden sind. Verbinden Sie den Port G3 des untersten Stack-Gerätes mit dem Port G4 des obersten Geräts im Stack.

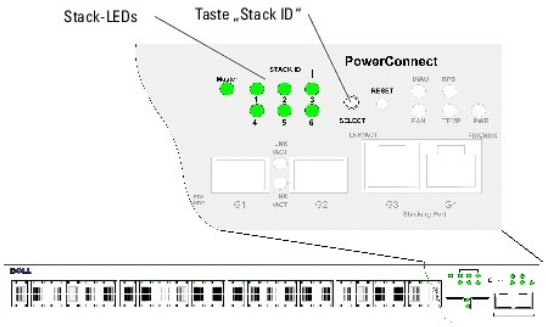
Abbildung 3-5. Abbildung der Stacking-Kabel



ANMERKUNG: Im Stack-Modus werden die als G3 und G4 gekennzeichneten Ports nicht im EWS angezeigt. Dies hat zur Folge, dass die Ports geräteseitig nicht verfügbar sind. Der Grund besteht darin, dass die Ports einen anderen Indexwert für das Stacking erhalten.

Die Stack-Einheiten können an der Vorderseite des Gerätes identifiziert werden, indem Sie die Taste Stack ID verwenden.

Abbildung 3-6. Stacking-Konfiguration und Anzeigen zur Identifizierung



Jede Stack-Komponente verfügt über eine identifizierende Geräte-ID, von der die Position und Funktion der Einheit innerhalb des Stacks definiert wird. Wenn es sich um eine Standalone-Einheit handelt, leuchtet die Stack-LED nicht auf. Der Standard ist auf Standalone-Gerät eingestellt.

Sie können die Geräte-ID über die Taste Stack ID-Taste manuell konfigurieren. Die Geräte-ID wird von den Stack-ID-LEDs angezeigt. Die Geräte-IDs 1 und 2 sind für die Mastereinheit und die Mastersicherungseinheit reserviert, IDs 3 bis 6 für die abhängigen Komponenten.

Auswählen der Geräte-ID

Die Geräte-IDs werden wie folgt ausgewählt:

1. Stellen Sie sicher, dass das Standalone-Gerät bzw. die Mastereinheit über ein gekreuztes RS- 232-Kabel mit einem VT100-Terminal oder einem VT100-Emulationsprogramm verbunden ist.
2. Suchen Sie einen Netzstromanschluss.
3. Deaktivieren Sie den Netzanschluss.
4. Verbinden Sie das Gerät mit dem Netzstromanschluss.
5. Aktivieren Sie den Netzanschluss.

Beim Einschaltvorgang beginnt die konfigurierte LED-Nummer (entspricht der zuvor gespeicherten Geräte-ID) zu blinken. Die LED blinkt für 15 Sekunden. Wählen Sie während dieser Zeit eine spezifische Stack-ID aus, indem Sie auf die Taste Stack ID drücken, bis die gewünschte Stack-ID-LED aufleuchtet.

6. Auswahlverfahren – Halten Sie die Taste Stack ID gedrückt, um zur nächsten Stack-ID-LED zu gelangen. Wenn die LED 6 blinkt, wird das Gerät beim Drücken der Taste Stack ID als Standalone-Gerät konfiguriert. Erneutes Drücken der Taste Stack ID rückt die Stack-ID auf 1 vor. Die Geräte 1 und 2 lassen sich als Mastergeräte definieren. Informationen zur Auswahl von Mastergeräten finden Sie unter Übersicht über die Stack-Montage.
7. Auswahl beenden: Die Auswahl der Geräte-ID ist beendet, wenn die LED nach 15 Sekunden aufhört zu blinken. Die Taste Stack ID reagiert nicht mehr, und die Geräte-ID wird der LED zugeordnet, die am Ende dieses Zeitraums blinkt.

ANMERKUNG: Diese Schritte sollten für jede Einheit einzeln durchgeführt werden, bis alle Stack- Komponenten eingeschaltet sind und die jeweiligen Stack-IDs ausgewählt wurden. Wenn Sie die Einheiten einzeln konfigurieren, haben Sie ausreichend Zeit eine Stack-ID für jede Einheit auszuwählen. Der gesamte Stack muss jedoch vor dem Einschalten der Geräte ordnungsgemäß verkabelt werden (siehe Abbildung der Stacking-Kabel).

Starten und Konfigurieren des Gerätes

Nachdem Sie alle externen Verbindungen vorgenommen haben, schließen Sie das Gerät an ein Terminal an, um es zu konfigurieren. Wie die zusätzlichen Erweiterungsfunktionen auszuführen sind, wird im Abschnitt Fortgeschrittene Konfigurationen beschrieben.

ANMERKUNG: Lesen Sie die Versionshinweise für dieses Produkt, bevor Sie fortfahren. Sie können diese Hinweise von der Dell Support-Website unter **support.dell.com** herunterladen.

ANMERKUNG: Es wird empfohlen, die aktuellste Version der Benutzerdokumentation auf der Dell Support-Website **support.dell.com** herunterzuladen.

Herstellen einer Geräteverbindung

Um das Gerät konfigurieren zu können, muss es an einer Konsole angeschlossen sein. Wenn das Gerät Teil eines Stacks ist, muss allerdings nur eine Komponente, nämlich die Mastereinheit, an das Terminal angeschlossen werden. Da der Stack wie ein einziges Gerät arbeitet, wird nur die Mastereinheit konfiguriert.

Verbinden eines Terminals mit dem Gerät

Das Gerät ermöglicht über einen Konsolenport eine Verbindung zu einem Desktop-System, auf dem eine Terminal-Emulationssoftware zur Überwachung und Konfiguration ausgeführt wird. Bei dem Konsolenport handelt es sich um einen DB-9-Anschluss, der als Data Terminal Equipment (DTE; Datenendeinrichtung) implementiert wird.

Um den Konsolenport nutzen zu können, wird Folgendes benötigt:

- Ein VT100-kompatibles Terminal oder ein Desktop- bzw. tragbares System mit einem seriellen Anschluss, auf dem die VT100-Terminal-Emulationssoftware ausgeführt wird
- Ein gekreuztes RS-232-Kabel mit DB-9-Buchse für den Konsolenport und dem geeigneten Anschluss für das Terminal

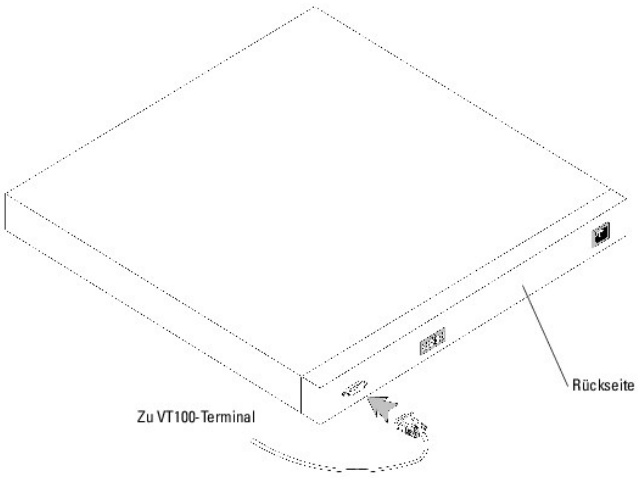
So wird das Terminal mit dem Anschluss für die Konsole verbunden:

1. Verbinden Sie das mitgelieferte, gekreuzte RS-232-Kabel mit dem Terminal, auf dem die VT100-Terminal-Emulationssoftware ausgeführt wird.
2. Wählen Sie einen geeigneten seriellen Anschluss (seriellen Anschluss 1 oder 2) zur Verbindung mit der Konsole aus.
3. Die Datenrate auf 9600 Baud festlegen.
4. Das Datenformat auf 8 Datenbits, 1 Stoppbit und keine Parität festlegen.
5. Setzen Sie die Flusskontrolle auf none (Keine).
6. Wählen Sie bei den Eigenschaften die Betriebsart VT100 für Emulation.
7. Wählen Sie für die Belegung der Funktions-, Pfeil und Strg-Tasten die Option Terminal. Stellen Sie sicher, dass die Einstellung Terminal lautet (*nicht* Windows).

HINWEIS: Wenn Sie HyperTerminal mit Microsoft® Windows® 2000 verwenden, stellen Sie sicher, dass Windows 2000 Service Pack 2 oder höher installiert ist. Mit Windows 2000 Service Pack 2 funktionieren die Pfeiltasten in der VT100-Emulierung von HyperTerminal ordnungsgemäß. Informationen zu den Service Packs von Windows 2000 finden Sie unter www.microsoft.com.

8. Verbinden Sie die Buchse des gekreuzten RS-232-Kabels direkt mit dem Anschluss für die Konsole am Mastergerät bzw. am Standalone-Gerät, und ziehen Sie die Halteschrauben fest. Der Anschluss für die Konsole befindet sich bei der PowerConnect 3400-Reihe auf der Geräterückseite.

Abbildung 3-7. Anschließen der Konsole (PowerConnect 3400)



ANMERKUNG: Sie können jeden Konsolenport im Stack mit einer Konsole verbinden; der Stack wird jedoch ausschließlich über die Mastereinheit (Geräte-ID 1 oder 2) verwaltet.

Zurück zum Inhalt

Zurück zum Inhalt

Konfigurieren der PowerConnect-Switches 3424/P und 3448/P

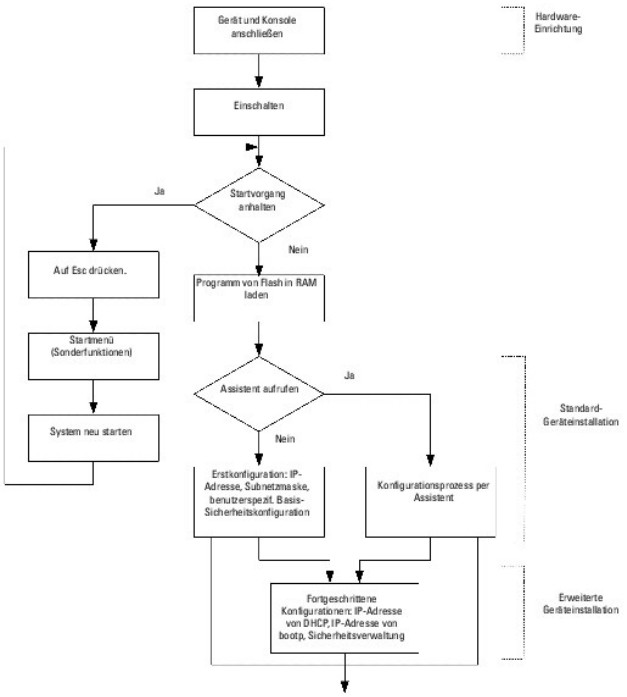
Dell™ PowerConnect™ 34XX- Systeme Benutzerhandbuch

Konfigurationsverfahren

Sobald alle externen Geräteverbindungen hergestellt sind, wird ein Terminal angeschlossen, um den Startvorgang sowie andere Maßnahmen überwachen zu können. Die Reihenfolge der Installations- und Konfigurationsmaßnahmen ist in der folgenden Abbildung dargestellt:

ANMERKUNG: Lesen Sie die Versionshinweise für dieses Produkt, bevor Sie fortfahren. Sie können diese Hinweise unter **support.dell.com** herunterladen.

Abbildung 4-1. Installation- und Konfigurationsverlauf



Den Switch starten

Wenn das Gerät mit dem lokalen Terminal verbunden ist und der Strom eingeschaltet wird, durchläuft der Switch den POST (Power On Self Test – Einschaltselbsttest). POST wird immer bei der Initialisierung des Gerätes ausgeführt und überprüft die Hardware-Komponenten, um zu ermitteln, ob das Gerät bereits vor Abschluss des Startvorgangs vollständig betriebsbereit ist. Wenn ein kritischer Fehler festgestellt wird, wird der Programmablauf unterbrochen. Bei erfolgreicher Ausführung von POST wird ein gültiges, ausführbares Bild in das RAM geladen. Die Fehler- bzw. Erfolgsmeldungen des Einschaltselbsttests werden terminalseitig angezeigt.

Der Startvorgang dauert ungefähr 30 Sekunden.

Erstkonfiguration

ANMERKUNG: Lesen Sie die Versionshinweise für dieses Produkt, bevor Sie fortfahren. Sie können diese Hinweise von der Dell Support-Website unter **support.dell.com** herunterladen.

ANMERKUNG: Für die Erstkonfiguration wird Folgendes vorausgesetzt:

- Das PowerConnect-Gerät wird zum ersten Mal konfiguriert und befindet sich in dem gleichen Zustand, in dem Sie es erhalten haben.
- Das PowerConnect-Gerät wurde erfolgreich gestartet.
- Es besteht eine Konsolenverbindung, und die Konsolenbefehlszeile wird auf dem Bildschirm eines VT100-Terminals angezeigt.

Die Erstkonfiguration des Gerätes wird über den Konsolenport vorgenommen. Nach der Erstkonfiguration kann das Gerät entweder über die bereits bestehende Verbindung zum Konsolenport oder über eine Schnittstelle verwaltet werden, die während der Erstkonfiguration definiert wird.

Wenn das Gerät erstmalig gestartet wird oder die Konfigurationsdatei keine Einträge enthält, weil das Gerät noch nicht konfiguriert wurde, wird der Benutzer aufgefordert, den Setup-Assistenten aufzurufen. Der Setup-Assistent führt Sie durch die Erstkonfiguration und macht das Gerät auf schnellstem Weg einsatzbereit.

ANMERKUNG: Erfragen Sie vor dem Konfigurieren des Gerätes die folgenden Informationen vom Netzwerkadministrator:

- IP-Adresse für die VLAN-1-Schnittstelle, über die das Gerät verwaltet werden soll (standardmäßig gehört jeder Port zu VLAN 1)
- IP Subnetzmaske für das Netzwerk
- IP-Adresse des Standard-Gateways (nächster Hop-Router) zur Konfiguration des Standardpfads
- SNMP-Community-String und SNMP-Management-System-IP-Adresse (optional)
- Benutzername und Kennwort

Der Setup-Assistent führt Sie durch die Erstkonfiguration des Switches und macht das System auf schnellstem Weg einsatzbereit. Sie können den Setup-Assistenten auch überspringen und das Gerät manuell über CLI-Befehle konfigurieren.

Mit dem Setup-Assistenten werden die folgenden Felder konfiguriert.

- SNMP-Community-String und SNMP-Management-System-IP-Adresse (optional)
- Benutzername und Kennwort
- IP-Adresse des Gerätes
- Standard-Gateway-IP-Adresse

Folgendes wird angezeigt (leicht abweichende Formulierungen möglich):

```
Welcome to Dell Easy Setup Wizard


The Setup Wizard guides you through the initial switch configuration, and gets you up and running as quickly as possible. You can skip
the setup wizard, and enter CLI mode to manually configure the switch.
The system will prompt you with a default answer; by pressing enter, you accept the default.
You must respond to the next question to run the setup wizard within 60 seconds, otherwise the system will continue with normal operation
using the default system configuration.


Would you like to enter the Setup Wizard (you must answer this question within 60 seconds? (Y/N)[Y]Y
You can exit the Setup Wizard at any time by entering [ctrl+Z].
```

Wenn Sie hier [N] eingeben, wird der Setup-Assistent beendet. Erfolgt innerhalb von 60 Sekunden keine Reaktion, wird der Setup-Assistent automatisch beendet, und die Eingabeaufforderung der CLI-Konsole erscheint.

Wenn Sie [J] eingeben, werden Sie vom Setup-Assistenten interaktiv durch die Erstkonfiguration des Gerätes geführt.

ANMERKUNG: Erfolgt innerhalb von 60 Sekunden keine Reaktion und ist netzwerkseitig ein BootP- Server verfügbar, wird eine Adresse von diesem Server abgerufen.

ANMERKUNG: Der Setup-Assistent lässt sich jederzeit durch Drücken von [STRG+Z] beenden.

Schritt 1 des Assistenten

Die folgende Meldung wird angezeigt:

```
The system is not setup for SNMP management by default.
To manage the switch using SNMP (required for Dell Network Manager) you can

   l  Setup the initial SNMP version 2 account now.

   l  Return later and setup additional SNMP v1/v3 accounts.


For more information on setting up SNMP accounts, please see the user documentation.


Would you like to setup the SNMP management interface now? (Y/N)[Y]Y
```

Geben Sie [N] ein, um mit Schritt 2 fortzufahren.

Geben Sie [J] ein, um den Setup-Assistenten fortzusetzen. Die folgende Meldung wird angezeigt:

```
To setup the SNMP management account you must specify the management system IP address and the "community string" or password that the
particular management system uses to access the switch. The wizard automatically assigns the highest access level [Privilege Level 15] to
this account.
You can use Dell Network Manager or CLI to change this setting, and to add additional management systems. For more information on adding
management systems, see the user documentation.
To add a management station:
Please enter the SNMP community string to be used: [Dell_Network_Manager]
Please enter the IP address of the Management System (A.B.C.D) or wildcard (0.0.0.0) to manage from any Management Station: [0.0.0.0]
```

Geben Sie folgende Informationen ein:

- SNMP-Community-Zeichenfolge, z. B. Dell_Network_Manager.
- IP-Adresse des Verwaltungssystems (A.B.C.D) oder Platzhalter (0.0.0.0), um die Verwaltung von jeder Verwaltungsstation aus vorzunehmen.

ANMERKUNG: Mit Null beginnende IP-Adressen und Masken können nicht verwendet werden.

Drücken Sie die **Eingabetaste**.

Schritt 2 des Assistenten

Die folgende Meldung wird angezeigt:

```
Now we need to setup your initial privilege (Level 15) user account.
This account is used to login to the CLI and Web interface.
You may setup other accounts and change privilege levels later.
For more information on setting up user accounts and changing privilege levels, see the user documentation.
To setup a user account:
Enter the user name<1-20>:[admin]
Please enter the user password:*
Please reenter the user password:*
```

Geben Sie folgende Informationen ein:

- Benutzername, z. B. admin
- Kennwort und Kennwortbestätigung

ANMERKUNG: Stimmen die erste und die zweite Kennworteingabe nicht überein, muss die Eingabe wiederholt werden, bis beide Einträge identisch sind.

Drücken Sie die **Eingabetaste**.

Schritt 3 des Assistenten

Die folgende Meldung wird angezeigt:

```
Next, an IP address is setup.

    The IP address is defined on the default VLAN (VLAN #1), of which all ports are members. This is the IP address you use to access the
    CLI, Web interface, or SNMP interface for the switch.To setup an IP address:

    Please enter the IP address of the device (A.B.C.D):[1.1.1.1]

    Please enter the IP subnet mask (A.B.C.D or nn): [255.255.255.0]

    Geben Sie die IP-Subnetzmaske ein (A.B.C.D oder nn): [255.255.255.0]
```

Geben Sie die IP-Adresse und IP-Subnetzmaske ein, zum Beispiel 1.1.1.1 als IP-Adresse und 255.255.255.0 als IP-Subnetzmaske.

Drücken Sie die **Eingabetaste**.

Schritt 4 des Assistenten

Die folgende Meldung wird angezeigt:

```
    Finally, setup the default gateway.
    Please enter the IP address of the gateway from which this network is reachable (e.g. 192.168.1.1).Default gateway (A.B.C.D):[0.0.0.0]
```

Geben Sie das Standard-Gateway ein.

Drücken Sie die Eingabetaste. Folgendes wird angezeigt (mit den beschriebenen Beispielparametern):

```
    This is the configuration information that has been collected:

    ============================================================

    SNMP Interface = Dell_Network_Manager@0.0.0.0
    User Account setup = admin
    Password = *
    Management IP address = 1.1.1.1 255.255.255.0
    Default Gateway = 1.1.1.2s
```

```
============================================================
```

Schritt 5 des Assistenten

Die folgende Meldung wird angezeigt:

```
If the information is correct, please select (Y) to save the configuration, and copy to the start-up configuration file. If the
information is incorrect, select (N) to discard configuration and restart the wizard: (Y/N)[Y]Y
```

Geben Sie [N] ein, um den Assistenten neu zu starten.

Geben Sie [J] ein, um den Setup-Assistenten abzuschließen. Folgendes wird angezeigt (leicht abweichende Formulierungen möglich):

```
Configuring SNMP management interface
Configuring user account......
Configuring IP and subnet......
```

```
Thank you for using Dell Easy Setup Wizard. You will now enter CLI mode.
```

Schritt 6 des Assistenten

Die CLI-Eingabeaufforderung wird angezeigt.

Fortgeschrittene Konfigurationen

Dieser Abschnitt enthält Informationen zurr dynamischen Zuweisung von IP-Adressen sowie den AAA-Mechanismen im Rahmen der Sicherheitsverwaltung (Authentifizierung, Autorisierung und Accounting). Außerdem werden hier die folgenden Themen behandelt:

- Konfigurieren von IP-Adressen über DHCP
- Konfigurieren von IP-Adressen über BOOTP
- Sicherheitsverwaltung und Kennwortkonfiguration

Werden IP-Adressen über DHCP und BOOTP konfiguriert bzw. empfangen, umfasst die von diesen Servern eingehende Konfiguration neben den IP-Adressen gegebenenfalls auch eine Subnetzmaske sowie ein Standard-Gateway.

Abrufen einer IP-Adresse von einem DHCP-Server

Wenn eine IP-Adresse über das DHCP-Protokoll abgerufen wird, fungiert das Gerät als DHCP-Client. Beim Zurücksetzen des Gerätes wird der DHCP-Befehl in der Konfigurationsdatei gespeichert, die IP-Adresse jedoch nicht. Gehen Sie wie folgt vor, um eine IP-Adresse von einem DHCP-Server abzurufen:

1. Wählen Sie einen beliebigen Port und verbinden Sie diesen mit einem DHCP Server oder einem Subnetz, das über einen DHCP-Server verfügt, um die IP-Adresse abzurufen.
2. Geben Sie die nachfolgenden Befehle ein, um den gewählten Port für den Empfang der IP- Adressen zu nutzen. Die Befehle im nach folgenden Beispiel sind vom Port-Typ abhängig, der für die Konfiguration verwendet wird.
    - Zuweisen von dynamischen IP-Adressen:

```
console# configure
```

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


console(config-if)# ip address dhcp hostname powerconnect


console(config-if)# exit


console(config)#
```

- Zuweisen von dynamischen IP-Adressen (in einem VLAN):

```
console# configure


console(config)# interface ethernet vlan 1


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


console(config-if)# exit


console(config)#
```

Die IP-Adresse wird über die Schnittstelle automatisch empfangen.

3. Geben Sie an der Systemeingabeaufforderung den Befehl **show ip interface** wie im nachfolgenden Beispiel gezeigt ein, um die IP-Adresse zu überprüfen.

```
console# show ip interface


IP Address I/F Type




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


100.1.1.1/24 vlan 1 dynamic
```

ANMERKUNG: Die Gerätekonfiguration braucht nicht gelöscht zu werden, um eine IP-Adresse für den DHCP -Server abrufen zu können.

ANMERKUNG: Verwenden Sie beim Kopieren einer Konfigurationsdatei möglichst keine Datei, die eine Anweisung zur DHCP-Aktivierung an einer Schnittstelle für eine Verbindung zu demselben DHCP-Server enthält bzw. zu einem anderen Server mit identischer Konfiguration. In diesem Fall ruft das Gerät die neue Konfigurationsdatei ab und verwendet diese für den Startvorgang. Das Gerät aktiviert DHCP dann gemäß der Anweisung in der neuen Konfigurationsdatei, und der DHCP-Server weist das Gerät an, dieselbe Datei erneut zu laden.

ANMERKUNG: Wenn Sie eine DHCP-IP-Adresse konfigurieren, wird diese Adresse dynamisch abgerufen, und der Befehl `ip address dhcp` wird in der Konfigurationsdatei gespeichert. Bei einem Ausfall der Mastereinheit wird die Mastersicherungseinheit erneut versuchen, eine DHCP-Adresse abzurufen. Dies könnte die folgenden Auswirkungen haben:

- Eine identische IP-Adresse wird zugewiesen.
- Eine andere IP-Adresse wird zugewiesen, was eine Unterbrechung der Verbindung zur Verwaltungsstation zur Folge haben könnte.
- Der DHCP-Server fällt aus, was wiederum zur Folge hätte, dass keine IP-Adressen abgerufen werden können; auch die Verbindung zur Verwaltungsstation könnte unterbrochen werden.

Empfangen einer IP-Adresse von einem BOOTP-Server

Da das Standard-BOOTP-Protokoll unterstützt wird, kann das Gerät die geräteeigene IP-Host-Konfiguration von jedem Standard-BOOTP-Server im Netzwerk automatisch herunterladen. In diesem Fall fungiert das Gerät als BOOTP-Client.

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

1. Wählen Sie einen beliebigen Port und verbinden Sie diesen mit einem BOOTP-Server bzw. einem Subnetz, in dem sich ein solcher Server befindet, um die IP-Adresse abzurufen.
2. Geben Sie an der Systemeingabeaufforderung den Befehl **delete startup configuration** ein, um die Startkonfiguration aus dem Flash zu löschen.

   Das Gerät führt einen Neustart ohne Konfiguration durch und beginnt innerhalb von 60 Sekunden mit der Übermittlung von BOOTP-Anforderungen. Die IP-Adresse wird vom Gerät automatisch empfangen.

ANMERKUNG: Bei Beginn des Geräteneustarts hat jede Eingabe per ASCII-Terminal oder Tastatur automatisch zur Folge, dass der BOOTP-Prozess vorzeitig abgebrochen wird und das Gerät keine IP- Adresse vom BOOTP-Server empfangen kann.

Das folgende Beispiel veranschaulicht diesen Prozess:

```
console> enable

console# delete startup-config

Startup file was deleted

console# reload

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

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

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

/* the device reboots */
```

Geben Sie den Befehl **show ip interface** ein, um die IP-Adresse zu überprüfen.

Das Gerät besitzt jetzt eine gültige IP-Adresse.

Sicherheitsverwaltung und Kennwortkonfiguration

Die Systemsicherheit wird über den so genannten AAA-Mechanismus (Authentifizierung, Autorisierung und Accounting) realisiert, der eine Verwaltung der benutzerspezifischen Zugriffsrechte, Privilegien und Verwaltungsmethoden ermöglicht. AAA greift hierbei auf lokale und dezentral installierte Benutzerdatenbanken zurück. Die Datenverschlüsselung erfolgt über den SSH-Mechanismus.

Das System wird ohne vorkonfiguriertes Standard-Kennwort ausgeliefert; sämtliche Kennwörter sind benutzerseitig definiert. Falls ein benutzerdefiniertes Kennwort verloren geht, kann über das **Startmenü** eine Prozedur zur Kennwortwiederherstellung aufgerufen werden. Diese Prozedur, die am lokalen Terminal verfügbar ist, bietet die Möglichkeit, von diesem Terminal aus einmalig ohne Kennworteingabe auf das Gerät zuzugreifen.

Konfigurieren von Sicherheitskennwörtern

Für folgende Dienste können Sicherheitskennwörter konfiguriert werden:

- Terminal
- Telnet
- SSH
- HTTP
- HTTPS

ANMERKUNG: Kennwörter sind benutzerdefiniert.

ANMERKUNG: Bei der Einrichtung eines Benutzernamens wird standardmäßig die Priorität 1 vereinbart (d. h. einfacher Zugang ohne Konfigurationsrechte). Um Gerätzugriffe mit Konfigurationsrechten zu ermöglichen, muss ausdrücklich die Priorität 15 festgelegt werden. Es ist zwar grundsätzlich möglich, einem Benutzer die Berechtigungsstufe 15 zuzuweisen, ohne ein Kennwort zu vereinbaren; die Kennwortvergabe wird aber empfohlen. Existiert kein bestimmtes Kennwort, können Benutzer mit entsprechenden Privilegien die Weboberfläche ohne Kennworteingabe aufrufen.

ANMERKUNG: Kennwörter können mit Hilfe von speziellen Kennwort-Verwaltungsbefehlen geschützt werden, die den Gültigkeitszeitraum der Kennwörter befristen. Weitere Informationen hierzu finden Sie unter Sicherheitsverwaltung und Kennwortkonfiguration.

Konfigurieren eines ersten Terminal-Kennworts

Geben Sie die folgenden Befehle ein, um ein erstes Terminal-Kennwort zu konfigurieren:

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

console(config)# aaa authentication enable default line

console(config)# line console

console(config-line)# login authentication default

console(config-line)# enable authentication default

console(config-line)# password george
```

- Wenn Sie sich erstmalig über eine Terminalsitzung bei einem Gerät anmelden, geben Sie an der Kennwort-Eingabeaufforderung george ein.
- Wenn Sie einen Gerätemodus erstmalig von deaktiviert in aktiviert ändern, geben Sie an der Kennwort-Eingabeaufforderung george ein.

Konfigurieren eines ersten Telnet-Kennworts

Geben Sie die folgenden Befehle ein, um ein erstes Telnet-Kennwort zu konfigurieren:

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

console(config)# aaa authentication enable default line

console(config)# line telnet
```

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

console(config-line)# enable authentication default

console(config-line)# password bob
```

- Wenn Sie sich erstmalig über eine Telnet-Sitzung bei einem Gerät anmelden, geben Sie an der Kennwort-Eingabeaufforderung `bob` ein.
- Wenn Sie einen Gerätemodus erstmalig von deaktiviert in aktiviert ändern, geben Sie `bob` ein.

Konfigurieren eines ersten SSH-Passworts

Geben Sie die folgenden Befehle ein, um ein erstes SSH-Kennwort zu konfigurieren:

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

console(config)# aaa authentication enable default line

console(config)# line ssh

console(config-line)# login authentication default

console(config-line)# enable authentication default

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

- Wenn Sie sich erstmalig über eine SSH-Sitzung bei einem Gerät anmelden, geben Sie an der Kennwort-Eingabeaufforderung `jones` ein.
- Wenn Sie einen Gerätemodus erstmalig von deaktiviert in aktiviert ändern, geben Sie `jones` ein.

Konfigurieren eines ersten HTTP-Kennworts

Geben Sie die folgenden Befehle ein, um ein erstes HTTP-Kennwort zu konfigurieren:

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

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

Konfigurieren eines ersten HTTPS-Kennworts:

Geben Sie die folgenden Befehle ein, um ein erstes HTTPS-Kennwort zu konfigurieren:

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

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

Geben Sie die nachfolgenden Befehle einmalig ein, wenn Sie eine Terminal-, Telnet- oder SSH-Sitzung für eine HTTPS-Sitzung konfigurieren möchten.

ANMERKUNG: Aktivieren Sie im Webbrowser SSL 2.0 (oder höher) für den anzuzeigenden Seiteninhalt.

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

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

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

ANMERKUNG: Eine Nutzung der Dienste HTTP und HTTPS ist nur auf Zugriffsebene 15 sowie bei direkter Anbindung an den Konfigurationszugang möglich.

Startprozeduren

Startmenü-Prozeduren

Über das Startmenü lassen sich verschiedene Prozeduren für Softwaredownloads, die Flash-Handhabung sowie die Wiederherstellung von Kennwörtern aufrufen. Die Diagnoseprozeduren sind nur für die Mitarbeiter des Technischen Supports vorgesehen und werden im vorliegenden Dokument daher nicht näher beschrieben.

Sie können das Startmenü während des Gerätestarts aufrufen. Die Benutzereingabe muss unmittelbar nach dem POST-Test erfolgen.

Um das Startmenü aufzurufen:

1. Schalten Sie das Gerät ein und achten Sie auf die Selbststartmeldung.

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

```
**************** SYSTEM RESET *****************
```

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

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

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

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

```
BOOT Software Version 1.0.0.05 Built 06-Jan-2005 14:46:49
```

```
Carrier board, based on PPC8247
```

```
128 MByte SDRAM. I-Cache 16 KB. I-Cache 16 KB. Cache Enabled.
```

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

2. Drücken Sie bei Erscheinen der Meldung "auto-boot" die <Eingabetaste>, um das Startmenü aufzurufen. Die Startmenü-Prozeduren können über das ASCII-Terminal oder Windows HyperTerminal ausgeführt werden.

```
[1] Download Software


[2] Erase Flash File


[3] Password Recovery Procedure


[4] Enter Diagnostic Mode


[5] Set Terminal Baud-Rate


[6] Back
```

In den folgenden Abschnitten werden die verfügbaren Startmenü-Optionen beschrieben.

ANMERKUNG: Beachten Sie bei der Auswahl einer Option im Startmenü folgende Zeitbeschränkung: Erfolgt die Optionsauswahl nicht innerhalb von 35 Sekunden (Standard), läuft das Gerätezeitlimit ab. Dieser Standardwert kann über die CLI-Schnittstelle geändert werden.

ANMERKUNG: Der Diagnosemodus (Option[4]) kann nur von Mitarbeitern des Technischen Supports aktivieren werden. Der Diagnosemodus wird daher in diesem Handbuch nicht näher beschrieben.

Download Software - Option[1]

Die Softwaredownload-Prozedur wird ausgeführt, wenn eine neue Version heruntergeladen muss, um defekte Dateien zu ersetzen oder die Systemsoftware zu aktualisieren bzw. zu erweitern. Um die Software über das Startmenü herunterzuladen:

1. Drücken Sie im Startmenü auf [1]. Die folgende Meldung erscheint:

```
Downloading code using XMODEM


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


*** Running SW Ver. 1.0.0.30 Date 09-Jan-2005 Time 14:30:02


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


HW version is


Base Mac address is  : 00:00:b0:45:54:00


Dram size is : 128M bytes


Dram first block size is : 36864K bytes


Dram first PTR is : 0x1C00000
```

```
Flash size is: 16M

Loading running configuration.

Number of configuration items loaded: 5

Loading startup configuration.

Number of configuration items loaded: 5

Device configuration:

Slot 1 - PowerConnect 3424 HW Rev. 0.0

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

-- Unit Number 1 Standalone --

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

BOXP_high_appl_init: dpssIpcInitStandAlone

Tapi Version: v1.3.1.6P_01_03

Core Version: v1.3.1.6P_01_02

01-Jan-2000 01:01:19 %INIT-I-InitCompleted: Initialization task is completed

01-Jan-2000 01:01:19 %Box-I-FAN-STAT-CHNG: FAN# 1 status changed - operational.

01-Jan-2000 01:01:19 %Entity-I-SEND-ENT-CONF-CHANGE-TRAP: entity configuration change trap.

01-Jan-2000 01:01:19 %Box-I-FAN-STAT-CHNG: FAN# 2 status changed - operational.

01-Jan-2000 01:01:19 %Box-I-PS-STAT-CHNG: PS# 1 status changed - operational.
```

2. Klicken Sie bei Einsatz von HyperTerminal in der HyperTerminal-Menüleiste auf Übertragung.
3. Geben Sie Im Feld Dateiname den Dateipfad für die herunterzuladende Datei ein.
4. Vergewissern Sie sich, dass im Feld Protokoll das Xmodem-Protokoll markiert ist.
5. Klicken Sie auf Senden. Die Software wird heruntergeladen.

ANMERKUNG: Nach dem Softwaredownload wird das Gerät automatisch neu gestartet.

Erase FLASH File - Option[2]

In einigen Fällen muss die Gerätekonfiguration gelöscht werden. Nach dem Löschen der Konfiguration müssen alle über CLI, EWS oder SNMP konfigurierten Parameter neu konfiguriert werden.

So löschen Sie die Gerätekonfiguration:

1. Drücken Sie im Startmenü innerhalb von zwei Sekunden auf [2], um die Flash-Datei zu löschen. Die folgende Meldung wird angezeigt:

```
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. Vereinbaren Sie config als Namen für die Flash-Datei. Die Konfiguration wird gelöscht, und das Gerät wird neu gestartet.
4. Wiederholen Sie die Geräteerstkonfiguration.

Password Recovery - Option[3]

Falls ein Kennwort verloren geht, können Sie diese Prozedur zur Kennwortwiederherstellung über das Startmenü aufrufen. Die Prozedur ermöglicht einen einmaligen Gerätezugriff ohne vorherige Kennworteingabe.

Um ein verloren gegangenes Kennwort wiederherzustellen (nur bei Zugriff auf das lokale Terminal):

1. Geben Sie im Startmenü [3] ein und drücken Sie die <Eingabetaste>. Das Kennwort wird gelöscht.

   Wählen Sie eine Menüoption oder drücken Sie auf ESC, um das Menü zu verlassen:

```
Current password will be ignored!
```

ANMERKUNG: Um die Gerätesicherheit sicherzustellen, müssen die Kennwörter für alle relevanten Verwaltungsmethoden neu konfiguriert werden.

Enter Diagnostic Mode - Option[4]

Nur für den Technischen Support.

Set Terminal Baud-Rate - Option[5]

Geben Sie [5] ein und drücken Sie die <Eingabetaste>, um die Baudrate des Terminals einzustellen.

Wählen Sie eine Menüoption oder drücken Sie auf ESC, um das Menü zu verlassen:

```
Set new device baud-rate: 38,400
```

Softwaredownload über einen TFTP-Server

Dieser Abschnitt enthält Anweisungen zum Herunterladen der Gerätesoftware (System- und Boot-Images) über einen TFTP-Server. Vor dem Herunterladen der Software muss der TFTP-Server konfiguriert werden.

Herunterladen des System-Image

Beim Gerätstart wird das System-Image aus dem Flash-Speicherbereich, wo eine Kopie des System-Image gespeichert ist, dekomprimiert. Beim Herunterladen eines neuen Image wird dieses in einem Bereich gespeichert, der für eine weitere Kopie des System-Image vorgesehen ist.

Beim nächsten Startvorgang dekomprimiert und startet das Gerät vom derzeit aktiven System-Image, falls nicht anders festgelegt.

So laden Sie ein System-Image vom TFTP-Server herunter:

1. Stellen Sie sicher, dass an einem der Gerätports eine IP-Adresse konfiguriert ist und Ping- Befehle an einen TFTP-Server gesendet werden können.
2. Die herunterzuladende Datei muss auf dem TFTP-Server gespeichert sein (die Datei arc).
3. Geben Sie den Befehl **show version** ein, um die derzeitige Versionsnummer der Gerätesoftware zu überprüfen. Es werden beispielsweise folgende Informationen angezeigt:

```
console# show version

SW version 1.0.0.30 (date 27-Jan-2005 time 13:42:41)

Boot version 1.0.0.05 (date 27-Jan-2005 time 15:12:20)

HW version
```

4. Geben Sie den Befehl **show bootvar** ein, um festzustellen, welches System-Image derzeit aktiv ist. Es werden beispielsweise folgende Informationen angezeigt:

```
console# show bootvar

Images currently available on the Flash

Image-1 active (selected for next boot)

Image-2 not active

console#
```

5. Geben Sie den Befehl **copy tftp:**//{tftp-Adresse}/{Dateiname} **image** ein, um ein neues System-Image auf das Gerät zu kopieren. Nach dem Herunterladen des neuen Image wird es in dem Bereich gespeichert, der für die andere Kopie des System-Image vorgesehen ist (im Beispiel image-2). Es werden beispielsweise folgende Informationen angezeigt:

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

Accessing file `file1' on 176.215.31.3Ö
```

```
Loading file1 from 176.215.31.3:


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


Copy took 00:01:11 [hh:mm:ss]
```

Ausrufezeichen zeigen den Fortschritt des Kopiervorgangs an. Jedes Ausrufezeichen (!) entspricht 512 Byte übertragener Daten. Ein Punkt zeigt an, dass das Zeitlimit für den Kopiervorgang überschritten wurde. Viele Punkte in einer Reihe zeigen an, dass der Kopiervorgang fehlgeschlagen ist.

6. Wählen Sie das Image für den nächsten Start aus, indem Sie den Befehl boot system eingeben. Geben Sie danach den Befehl **show bootvar** ein, um zu überprüfen, dass die im Befehl **boot system** als Parameter eingegebene Kopie für den nächsten Start ausgewählt ist.

Es werden beispielsweise folgende Informationen angezeigt:

```
console# boot system image-2


console# show bootvar


Images currently available on the Flash


Image-1 active


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

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

7. Geben Sie den Befehl **reload** ein. Die folgende Meldung wird angezeigt:

```
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. Das Gerät wird neu gestartet.

Herunterladen des Boot-Image

Zum Update des Boot-Images wird ein neues Boot-Image vom TFTP-Server geladen und in den Flash-Speicher programmiert. Das Boot-Image wird bei eingeschaltetem Gerät geladen. Benutzer haben keine Kontrolle über die Boot-Image-Kopien. So laden Sie ein Boot-Image vom TFTP-Server herunter:

1. Stellen Sie sicher, dass an einem der Gerätports eine IP-Adresse konfiguriert ist und Ping- Befehle an einen TFTP-Server gesendet werden können.
2. Die herunterzuladende Datei muss auf dem TFTP-Server gespeichert sein (die Datei rfb).
3. Geben Sie den Befehl show version ein, um die derzeitige Versionsnummer der Gerätesoftware zu überprüfen. Es werden beispielsweise folgende Informationen angezeigt:

```
console# show version


SW version 1.0.0.30 (date 27-Jan-2005 time 13:42:41)
```

```
Boot version 1.0.0.05 (date 27-Jan-2005 time 15:12:20)


HW version
```

4. Geben Sie den Befehl **copy tftp:**//{tftp-Adresse}/{Dateiname} **boot** ein, um ein neues System-Image auf das Gerät zu kopieren. Es werden beispielsweise folgende Informationen angezeigt:

```
console# copy tftp://176.215.31.3/332448-10018.rfb boot


Erasing file..done.


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


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

5. Geben Sie den Befehl **reload** ein. Die folgende Meldung wird angezeigt:

```
console# reload


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

6. Geben Sie y ein. Das Gerät wird neu gestartet.

Port-Standardeinstellungen

Die allgemeinen Informationen für die Konfiguration der Geräteports umfassen eine Kurzbeschreibung der Funktion Auto-Negotiation sowie die Standardeinstellungen für die Switching-Ports.

Auto-Negotiation

Die Funktion Auto-Negotiation ermöglicht eine automatische Erkennung der Parameter Geschwindigkeit, Duplexmodus und Flusskontrolle für alle 10/100/1000BaseT-Switching-Ports. Auto-Negotiation wird standardmäßig auf Portbasis aktiviert.

Auto-Negotiation bezeichnet einen Mechanismus zwischen zwei Verbindungspartnern, der bewirkt, dass ein Port dem zugehörigen Partnerpart die eigenen Einstellungen für Übertragungsrate, Duplexmodus und Flusskontrollverhalten (standardmäßig deaktiviert) mitteilt. In diesem Fall werden beide Anschlüsse unter Zugrundelegung des größten gemeinsamen Nenners betrieben.

Bei Anschluss einer NIC, die keine Auto-Negotiation unterstützt oder die nicht für die Auto-Negotiation konfiguriert ist, müssen sowohl der Switching-Port des Gerätes als auch die NSC manuell für dieselbe Geschwindigkeit und denselben Duplexmodus konfiguriert werden.

Falls die Station am anderen Ende der Verbindung versucht, eine Auto-Negotiation mit einem geräteseitigen 100Base-T-Port durchzuführen, der für Vollduplexbetrieb konfiguriert ist, bewirkt die Auto-Negotiation, dass die Station versucht, im Halbduplexmodus zu arbeiten.

MDI/MDIX

Das Gerät erkennt automatisch, ob an den 10/100/1000BaseT-Switching-Ports durchgehende oder gekreuzte Kabel angeschlossen sind. Diese Funktion ist Teil der Auto-Negotiation und wird bei Aktivierung der Funktion Auto-Negotiation ebenfalls aktiviert.

Die Aktivierung der Funktion MDI/MDIX (Media Dependent Interface with Crossover) ermöglicht eine automatische Korrektur von Fehlern bei der Kabelauswahl

und macht somit eine Unterscheidung zwischen durchgehenden und gekreuzten Kabeln überflüssig. (Die Standardverkabelung für Endstationen ist MDI (Media Dependent Interface), die Standardverkabelung für Hubs und Switches wird als MDIX bezeichnet.

Flow Control (Flusskontrolle)

Das Gerät unterstützt eine Flusskontrolle gemäß 802.3x an allen Ports, die für den Vollduplexmodus konfiguriert sind. Standardmäßig ist diese Funktion deaktiviert. Eine Aktivierung ist auf Portbasis möglich. Dank der Flusskontrolle kann die Empfängerseite dem Sender signalisieren, dass die Übertragung vorübergehend angehalten werden muss, um einen Pufferüberlaufe zu vermeiden.

Backpressure (Zurückweisung)

Das Gerät unterstützt die Backpressure-Funktion für alle Ports, die für den Halbduplexmodus konfiguriert sind. Standardmäßig ist diese Funktion deaktiviert. Eine Aktivierung ist auf Portbasis möglich. Der Backpressure-Mechanismus verhindert vorübergehend die Übermittlung weiterer Daten durch die Sendeseite. Der Empfänger kann eine Verbindung belegen, so dass sie für weitere Daten nicht verfügbar ist.

Standardeinstellungen der Switching-Ports

Die nachfolgende Tabelle bietet einen Überblick über die Standardeinstellungen der einzelnen Ports.

Tabelle 4-7. Port-Standardeinstellungen

Funktion	***Standardeinstellung***
Geschwindigkeit und Betriebsart	10/100BaseT (Kupfer): Auto-Negotiation 100 Mbit/s Vollduplex
	10/100/1000BaseT (Kupfer / SFP): Auto-Negotiation 1000 Mbit/s Vollduplex
Weiterleitungsstatus der Ports	Aktiviert
Port-Tagging (Kennzeichnung)	Keine Kennzeichnung
Flow Control (Flusskontrolle)	Aus (deaktiviert bei Ingress)
Backpressure (Zurückweisung)	Aus (deaktiviert bei Ingress)

Zurück zum Inhalt

Zurück zum Inhalt

Verwenden von Dell OpenManage Switch Administrator

Dell™ PowerConnect™ 34XX- Systeme Benutzerhandbuch

Dieser Abschnitt enthält eine Einführung in die Benutzerschnittstelle von Dell OpenManage Switch Administrator.

Starten der Anwendung

ANMERKUNG: Vor dem Start der Anwendung muss die IP-Adresse definiert werden. Weitere Informationen finden Sie unter Erstkonfiguration.

1. Öffnen Sie einen Webbrowser.
2. Geben Sie in der Adressleiste die IP-Adresse des Gerätes ein drücken Sie die <Eingabetaste>.
3. Wenn das Fenster **Log In** (Anmeldung) erscheint, geben Sie einen Benutzernamen und das Kennwort ein.

ANMERKUNG: Kennwörter sind alphanumerisch, und es wird zwischen Groß- und Kleinschreibung unterschieden.

4. Klicken Sie auf **OK**.

Die Startseite von **Dell OpenManage™ Switch Administrator** wird angezeigt.

Aufbau der Benutzeroberfläche

Die Startseite enthält folgende Felder:

- Strukturansicht – Sie befindet sich links auf der Startseite und bietet eine erweiterbare Ansicht der Merkmale und ihrer Komponenten.
- Geräteansicht– Sie befindet sich rechts auf der Startseite und enthält eine Ansicht des Gerätes, einen Informations- oder Tabellenbereich sowie Konfigurationsanweisungen.

Abbildung 5-1. Komponenten von Switch Administrator

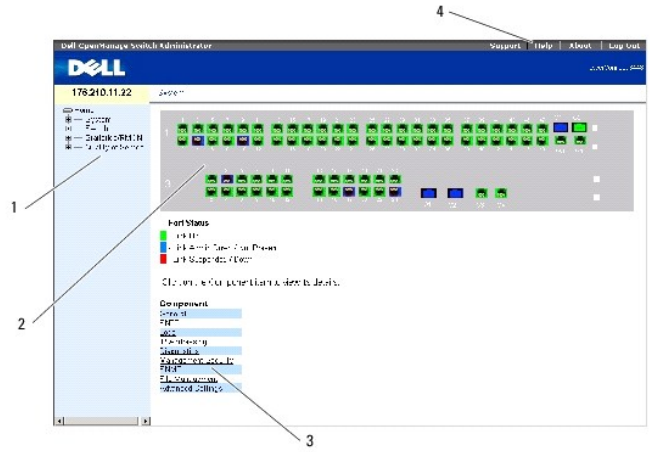


Tabelle 5-8 enthält die Schnittstellenkomponenten mit den entsprechenden Nummern.

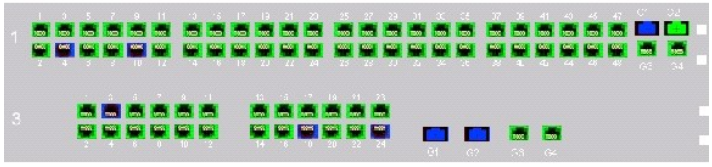
Tabelle 5-8. Schnittstellenkomponenten

Komponente	Beschreibung
1	Die Strukturansicht enthält eine Liste der verschiedenen Gerätefunktionen. Die Verzweigungen der Strukturansicht können eingeblendet werden, um alle Komponenten unterhalb einer bestimmten Funktion anzuzeigen, bzw. ausgeblendet werden, um die Funktionskomponenten zu verbergen. Durch Ziehen des vertikalen Balkens nach rechts kann die Strukturansicht erweitert werden, damit der vollständige Name einer Komponente angezeigt wird.
2	Die Geräteansicht enthält Informationen zu den Geräteports, die aktuelle Konfiguration sowie den Status, Tabelleninformationen und Funktionskomponenten. Je nach ausgewählter Option erscheinen im unteren Bereich der Geräteansicht andere Geräteinformationen und/oder Dialogfelder zum Konfigurieren von Parametern.
3	Die Komponentenliste enthält eine Liste mit Funktionskomponenten. Komponenten können auch durch Erweiterung einer Funktion in der Strukturansicht eingesehen werden.
4	Über die Informationsschaltflächen kann man Informationen zum Gerät abrufen und auf den Dell Support zugreifen. Weitere Informationen finden Sie unter Informationsschaltflächen.

Gerätedarstellung

Die Startseite enthält eine grafische Darstellung der Gerätevorderseite.

Abbildung 5-2. Port-Anzeigen des PowerConnect-Gerätes



An der Farbgebung der Ports ist erkennbar, ob ein bestimmter Port derzeit aktiv ist. Folgende Port-Farben sind möglich:

Tabelle 5-9. PowerConnect-Port und Stack-Anzeigen

Komponente	Beschreibung
Port-Anzeigen	
Grün	Der Port ist derzeit aktiviert.
Rot	Ein Port-Fehler ist aufgetreten.
Blau	Der Port ist derzeit deaktiviert.

Rot	Das Gerät ist derzeit nicht in einen Stack eingebunden.

ANMERKUNG: Die Port-LEDs sind in der Darstellung der PowerConnect-Vorderseite in OpenManage Switch Administrator nicht zu sehen. Der LED-Status kann somit nur am Gerät selbst festgestellt werden. Die Stack-LEDs spiegeln jedoch sehr wohl den Stack-Port-Status wieder. Weitere Informationen zu den LEDs finden Sie unter **LED-Definitionen**.

Verwenden der Schaltflächen in Switch Administrator

In diesem Abschnitt werden die Schaltflächen der OpenManage Switch Administrator-Schnittstelle beschrieben. Die Schnittstellenschaltflächen lassen sich in folgende Kategorien unterteilen:

Informationsschaltflächen

Die Informationsschaltflächen ermöglichen den Zugriff auf Online-Support und -Hilfe, und es lassen sich Informationen über die OpenManage Switch Administrator-Schnittstelle anzeigen.

Tabelle 5-10. Informationsschaltflächen

Schaltfläche	Beschreibung
Support (Support)	Öffnet die Dell Support-Website **support.dell.com.**
Help (Hilfe)	Onlinehilfe mit Informationen zum Konfigurieren und Verwalten des Gerätes. Die Seiten der Onlinehilfe sind kontextsensitiv. Ist beispielsweise die Seite **IP Addressing** (IP-Adressierung) geöffnet, wird das entsprechende Hilfethema angezeigt, sobald man auf **Hilfe klickt**.
About (Info)	Enthält die Versions- und Build-Nummer sowie Informationen zum Dell Copyright.
Log Out (Abmelden)	Öffnet das Fenster Log Out (Abmelden).

Schaltflächen für die Geräteverwaltung

Über die Geräteverwaltungsschaltflächen lassen sich die Geräteinformationen auf einfache Weise konfigurieren. Folgende Schaltflächen sind verfügbar :

Tabelle 5-11. Schaltflächen für die Geräteverwaltung

Schaltfläche	Beschreibung
Apply Changes (Änderungen übernehmen)	Übernimmt die festgelegten Änderungen für das Gerät.
Add (Hinzufügen)	Ermöglicht die Eingabe von Information in Tabellen oder Dialogen.
Telnet (Telnet)	Startet eine Telnetsitzung.
Query (Abfrage)	Führt Tabellenabfragen durch.
Show All (Alle zeigen)	Zeigt die Gerätetabellen an.
Linkspfeil/Rechtspfeil	Verschiebt Informationen zwischen Listen.
Refresh (Aktualisieren)	Aktualisiert Geräteinformationen.
Reset All Counters (Alle Zähler zurücksetzen)	Setzt die Statistikzähler zurück.
Print (Drucken)	Druckt die Seite **Network Management System** oder Tabelleninformationen.
Draw (Zeichnen)	Erstellt Ad-hoc-Statistiken in Diagrammform.

Felddefinitionen

Benutzerdefinierte Felder können – soweit auf der Webseite OpenManage Switch Administrator nichts anderes angegeben ist – 1 bis 159 Zeichen enthalten. Nahezu alle Buchstaben oder Zeichen können verwendet werden. Ausnahmen:

1 \

- /
- :
- *
- ?
- <
- >
- |

Gerätezugriffe über die CLI

Sie können das Gerät über eine Direktverbindung zum Terminalport oder über eine Telnet-Verbindung verwalten. Beim Zugriff über eine Telnet-Verbindung sollten Sie sicherstellen, dass eine IP-Adresse für das Gerät definiert wurde und dass die für den Gerätezugriff verwendete Workstation bereits vor Verwendung der CLI-Befehle mit dem Gerät verbunden ist.

Informationen zur Konfiguration einer ersten IP-Adresse finden Sie unter Erstkonfiguration.

ANMERKUNG: Stellen Sie sicher, dass die Software geräteseitig geladen wurde, bevor Sie CLI- Fernzugriffe auf das Gerät durchführen.

Terminalverbindung

1. Schalten Sie das Gerät ein und warten Sie, bis der Startvorgang abgeschlossen ist.
2. Geben Sie bei Erscheinen der Eingabeaufforderung Console> (Konsole) enable (aktivieren) ein und drücken Sie die <Eingabetaste>.
3. Konfigurieren Sie das Gerät und geben Sie die erforderlichen Befehle ein, um die gewünschten Vorgänge auszuführen.
4. Geben Sie abschließend den Befehl **exit** (Beenden) ein, um den Privileged EXEC-Modus zu verlassen.

   Die Sitzung wird beendet.

ANMERKUNG: Wenn sich ein anderer Benutzer im Privileged EXEC-Befehlsmodus beim System anmeldet, wird der aktuelle Benutzer automatisch abgemeldet, und der neue Benutzer wird angemeldet.

Telnet-Verbindung

Telnet ist ein TCP/IP-Protokoll für die Terminal-Emulation. RS-232-Terminals können über ein Netzwerk mit TCP/IP-Protokoll virtuell mit dem lokalen Gerät verbunden werden. Telnet stellt eine Alternative zur Anmeldung am lokalen Terminal dar, wenn eine Remote-Anmeldung erforderlich ist.

Das Gerät unterstützt maximal vier gleichzeitige Telnet-Sitzungen zur Geräteverwaltung. In einer Telnet-Sitzung können sämtliche CLI-Befehle verwendet werden.

So starten Sie eine Telnet-Sitzung:

1. Wählen Sie Start > Ausführen.

   Das Fenster Ausführen wird geöffnet.
2. Geben Sie im Fenster **Ausführen** Telnet *<IP-Adresse>* im Feld **Öffnen** ein.
3. Klicken Sie auf **OK.**

   Die Telnet-Sitzung beginnt.

Verwenden der CLI

Dieser Abschnitt enthält Informationen zum Einsatz der Befehlszeilenschnittstelle (Command Line Interface, CLI).

Befehlsmodus – Übersicht

Die CLI ist in verschiedene Befehlsmodi unterteilt. Jeder Befehlsmodus verfügt über einen spezifischen Befehlssatz. Durch Eingabe eines Fragezeichens (?) an der Terminal-Eingabeaufforderung wird eine Liste der für diesen spezifischen Befehlsmodus verfügbaren Befehle angezeigt.

In jedem Modus wird ein spezifischer Befehl verwendet, um von einem Befehlsmodus zum anderen zu wechseln.

Während der Initialisierung der CLI-Sitzung wird der User EXEC-Modus als CLI-Modus verwendet. Im User EXEC-Modus ist nur eine Teilmenge der Befehle verfügbar. Diese Ebene ist für Vorgänge reserviert, die keinen Einfluss auf die Terminalkonfiguration haben; sie wird zum Zugriff auf Konfigurationsteilsysteme, wie das CLI-Programm, genutzt. Für den Zugriff auf die nächste Ebene, den Privileged EXEC-Modus, ist ein Kennwort erforderlich.

Der Privileged EXEC-Modus bietet Zugriff auf die globale Gerätekonfiguration. Für bestimmte globale Konfigurationen innerhalb des Gerätes wechseln Sie zur nächsten Ebene, dem Global Configuration-Modus. Es ist kein Passwort erforderlich.

Im Global Configuration-Modus wird die Gerätekonfiguration auf globaler Ebene verwaltet.

Im Interface Configuration-Modus wird das Gerät auf der physischen Schnittstellenebene konfiguriert. Schnittstellenbefehle, die Unterbefehle erfordern, sind einer anderen Ebene zugeordnet, dem so genannten Subinterface Configuration-Modus. Es ist kein Passwort erforderlich.

User EXEC-Modus

Nach der Anmeldung beim Gerät ist standardmäßig der EXEC-Befehlsmodus aktiviert. Die Eingabeaufforderung auf Benutzerebene besteht aus dem Hostnamen, gefolgt von einer spitzen Klammer (>). Beispiel:

```
console>
```

ANMERKUNG: Sofern er bei der Erstkonfiguration nicht geändert wurde, lautet der Standardhostname console.

Mit Hilfe der User EXEC-Befehle werden Verbindungen zu Remote-Geräten hergestellt, Terminaleinstellungen temporär geändert, grundlegende Tests durchgeführt und Systeminformationen aufgelistet.

Um die User EXEC-Befehle aufzulisten, geben Sie ein Fragezeichen in der Befehlszeile ein.

Privileged EXEC-Modus

Der privilegierte Zugang kann durch ein Kennwort geschützt werden, um unbefugte Zugriffe zu verhindern und sicherzustellen, dass alle Betriebsparameter funktionstüchtig sind. Bei der Anzeige der Passwörter wird zwischen Groß- und Kleinschreibung unterschieden.

So können Sie auf die Befehle im Privileged EXEC Mode zugreifen und diese auflisten:

1. Geben Sie an der Eingabeaufforderung enable ein und drücken Sie die <Eingabetaste>.
2. Falls eine Kennwort-Eingabeaufforderung erscheint, geben Sie das Kennwort ein und betätigen die <Eingabetaste>.

Die Eingabeaufforderung für den Privileged EXEC-Modus besteht aus dem Hostnamen des Gerätes, gefolgt von einem Rautenzeichen (#). Beispiel:

```
console#
```

Um die Privileged EXEC-Befehle aufzulisten, geben Sie ein Fragezeichen in der Befehlszeile ein.

Um vom Privileged EXEC-Modus in den User EXEC-Modus zurückzukehren, müssen Sie `disable` eingeben und <Enter> drücken.

Das folgende Beispiel veranschaulicht, wie Sie den Privileged EXEC-Modus aufrufen und zum User EXEC-Modus zurückkehren:

```
console> enable

Enter Password: ******

console#

console# disable

console>
```

Mit dem Befehl **exit** können Sie zu einem vorherigen Modus zurückkehren. So ist beispielsweise eine Rückkehr vom Interface Configuration-Modus zum Global Configuration-Modus und vom Global Configuration-Modus zum Privileged EXEC-Modus möglich.

Global Configuration-Modus

Die Global Configuration-Befehle werden für Systemfunktionen und nicht für ein bestimmtes Protokoll bzw. eine Schnittstelle verwendet.

Um den Global Configuration-Modus aufzurufen, geben Sie an der Eingabeaufforderung für den Privileged EXEC-Modus den Befehl **configure** ein und drücken dann die <Eingabetaste>. Die Eingabeaufforderung für den Global Configuration-Modus erscheint als Host-Name des Gerätes, gefolgt von (config) und einem Rautenzeichen (#).

```
console(config)#
```

Um die Global Configuration-Befehle aufzulisten, geben Sie ein Fragezeichen in der Befehlszeile ein.

Über den Befehl **exit** oder die Tastenkombination <Strg>+<Z> können Sie vom Global Configuration-Modus zum Privileged EXEC-Modus zurückzukehren.

Das folgende Beispiel veranschaulicht, wie Sie den Global Configuration-Modus aufrufen und wider zum Privileged EXEC-Modus zurückkehren:

```
console#

console# configure

console(config)# exit
```

```
console#
```

Eine vollständige Liste der CLI-Modi finden Sie im Dokument **Dell™ PowerConnect™3424/P and PowerConnect 3448/P CLI Guide**.

Zurück zum Inhalt

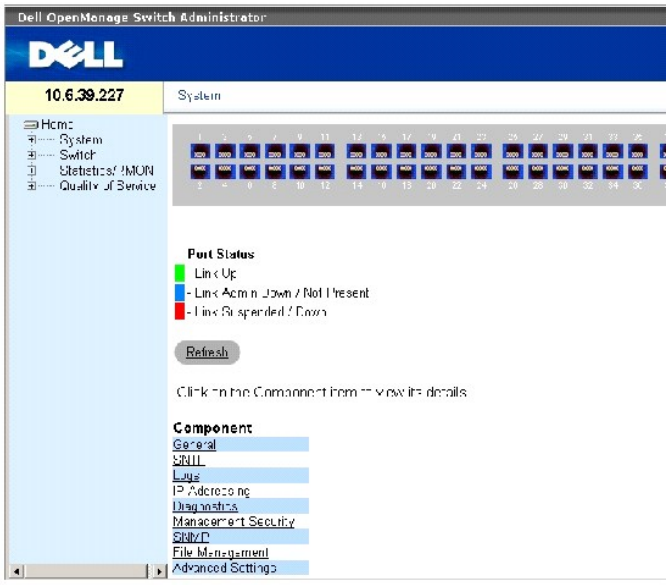
Zurück zum Inhalt

Konfigurieren von Systeminformationen

Dell™ PowerConnect™ 34XX- Systeme Benutzerhandbuch

Dieser Abschnitt enthält Informationen zum Definieren von Systemparametern, einschließlich Sicherheitsfunktionen, zum Herunterladen von Switch-Software sowie zum Zurücksetzen des Switches. Klicken Sie zum Öffnen der Seite **System** in der Strukturansicht auf **System**.

Abbildung 6-1. System



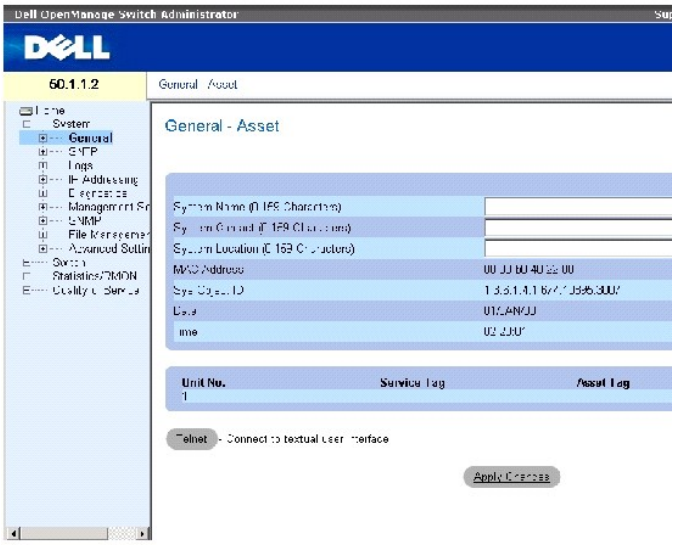
Definieren allgemeiner Switch-Informationen

Die Seite **General (Allgemein)** enthält Links zu Seiten, über die Netzwerkverwalter Switch-Parameter konfigurieren können.

Anzeigen von Switch-Geräteinformationen

Die Seite **Asset (Bestand)** enthält Parameter für die Konfiguration und Anzeige allgemeiner Geräteinformationen, einschließlich Systemname, -standort und -kontaktperson, MAC-Adresse und Objekt-ID des Systems sowie Datum, Uhrzeit und Systembetriebszeit. Klicken Sie zum Öffnen der Seite **Asset (Bestand)** in der Strukturansicht auf System→ General→ Asset.

Abbildung 6-2. Asset (Bestand)



Die Seite Asset (Bestand) enthält folgende Felder:

System Name (0-159 Characters) (Systemname (0-159 Zeichen)) – Gibt den benutzerdefinierten Gerätenamen an.

System Contact (0-159 Characters) (Systemkontakt (0-159 Zeichen)) – Gibt den Namen der Kontaktperson an.

System Location (0-159 Characters) (Systemstandort (0-159 Zeichen)) – Der Name des Standorts, an dem das System derzeit betrieben wird.

MAC Address – Gibt die MAC-Adresse des Gerätes an.

Sys Object ID – Gibt die maßgebende ID des Herstellers des Netzwerkverwaltungs-Subsystems an, das in der Einheit enthalten ist.

Date (DD/MMM//YY) – Das aktuelle Datum. Es wird im Format Tag, Monat, Jahr angezeigt. 10/OCT/03 entspricht beispielsweise dem 10. Oktober 2003.

Time (HH:MM:SS) – Gibt die Uhrzeit an. Sie wird im Format Stunde, Minute, Sekunde angezeigt. 20:12:21 entspricht beispielsweise zwanzig Uhr, zwölf Minuten und einundzwanzig Sekunden.

Unit No. (Einheit-Nr.) – Gibt die Nummer der Einheit an, für die Geräteinformationen angezeigt werden.

Service Tag (Service-Kennnummer) – Die bei der Wartung des Gerätes verwendete Wartungsreferenznummer.

Asset Tag (0-16 Characters) (Systemkennnummer (0-16 Zeichen)) – Die benutzerdefinierte Gerätereferenz.

Serial No. (Seriennummer) – Die Seriennummer des Gerätes.

Definieren von Systeminformationen

1. Öffnen Sie die Seite **Asset (Bestand)**.
2. Definieren Sie die relevanten 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 Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **Asset (Bestand)** äquivalenten CLI-Befehle zur Anzeige und Festlegung von Feldern zusammengefasst.

Tabelle 6-1. CLI-Befehle für Geräteinformationen

CLI-Befehl	Beschreibung
hostname Name	Gibt den Hostnamen des Gerätes an oder ändert ihn.
snmp-server contact Text	Richtet eine Kontaktperson für das System ein.
snmp-server location Text	Fügt Informationen zum Gerätestandort ein.
clock set hh:mm:ss Tag Monat Jahr	Legt Systemuhrzeit und -datum manuell fest.
show clock [detail]	Zeigt Uhrzeit und Datum der Systemuhr an.
show system id	Zeigt Informationen zur Service-Kennnummer an.
show system	Zeigt Systeminformationen an.
asset-tag Text	Legt die System-Kennnummer fest.
show stack <1-6>	Zeigt Informationen zum System-Stack an.
show system [unit *Einheit*]	Zeigt Systeminformationen an.
show system id [unit *Einheit*]	Zeigt Informationen zur Systemkennung an.

Das folgende Beispiel zeigt, wie Sie mit Hilfe von CLI-Befehlen den Hostnamen des Gerätes, den Systemkontakt und den Standort des Gerätes sowie das Datum und die Uhrzeit der Systemuhr festlegen:

```
console(config)# hostname dell

dell (config)# snmp-server contact Dell_Tech_Supp

dell (config)# snmp-server location New_York

dell (config)# exit

Console(config)# snmp-server host 10.1.1.1 management 2

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

Console# show clock
```

```
15:29:03 Jun 17 2002
```

Das folgende Beispiel zeigt, wie Sie mit Hilfe von CLI-Befehlen Systeminformationen für ein freistehendes Gerät anzeigen:

console# **show system id**	
Service tag :	
Serial number : 51	
Asset tag :	
console# **show system**	
System Description:	Ethernet Switch
System Up Time (days,hour:min:sec):	0,00:00:57
System Contact:	
System Name:	CARRIER-1
System Location:	
System MAC Address:	00:00:00:08:12:51
System Object ID:	1.3.6.1.4.1.674.10895.3006
Type:	PowerConnect 3424
Main Power Supply Status:	OK
Fan 1 Status:	NOT OPERATIONAL
Fan 2 Status:	NOT OPERATIONAL
Temperature (Celsius):	30
Temperature Sensor Status:	OK

Das folgende Beispiel zeigt, wie Sie mit Hilfe von CLI-Befehlen Systeminformationen für Stack-Geräte anzeigen:

```
console# show system id
```

Unit	Serial number	Asset tag	Service tag
1	893658972	mkt-1	89788978
2	893658973	mkt-2	89788979
3	893658974	mkt-3	89788980
4	893658975	mkt-4	89788981
5	893658976	mkt-5	89788982
6	893658977	mkt-6	89788983

```
console# show system
```

Unit	Type
1	PowerConnect 3424
2	PowerConnect 3424
3	PowerConnect 3428
4	PowerConnect 3424P
5	PowerConnect 3424P
6	PowerConnect 3424P

Unit	Main Power Supply	Redundant Power Supply
1	OK	

2	OK				
3	OK				
4	OK		OK		
5	OK		OK		
6	OK		OK		
Unit	Fan1	Fan2	Fan3	Fan4	Fan5
----	----	----	----	----	----
1	OK	OK			
2	OK	OK			
3	OK	OK			
4	OK	OK	OK	OK	OK
5	OK	OK	OK	OK	OK
6	OK	OK	OK	OK	OK
Unit	Temperature (Celsius)		Temperature Sensor Status		
----	----------		----------		
1	30		OK		
2	30		OK		
3	30		OK		
4	30		OK		
5	30		OK		
6	30		OK		

Festlegen von Systemzeiteinstellungen

Die Seite **Time Synchronization (Zeitsynchronisierung)** enthält Felder für die Festlegung von Systemzeitparametern für die lokale Hardware-Uhr und die externe SNTP-Uhr. Wenn die Systemzeit von einer externen SNTP-Uhr bezogen wird und die externe SNTP-Uhr ausfällt, werden für die Systemzeit wieder die Datums- und Uhrzeiteinstellungen der lokalen Hardware-Uhr verwendet. Für das Gerät kann die Umstellung auf Sommerzeit aktiviert werden. Die folgende Liste enthält den Beginn und das Ende der Sommerzeit in verschiedenen Ländern:

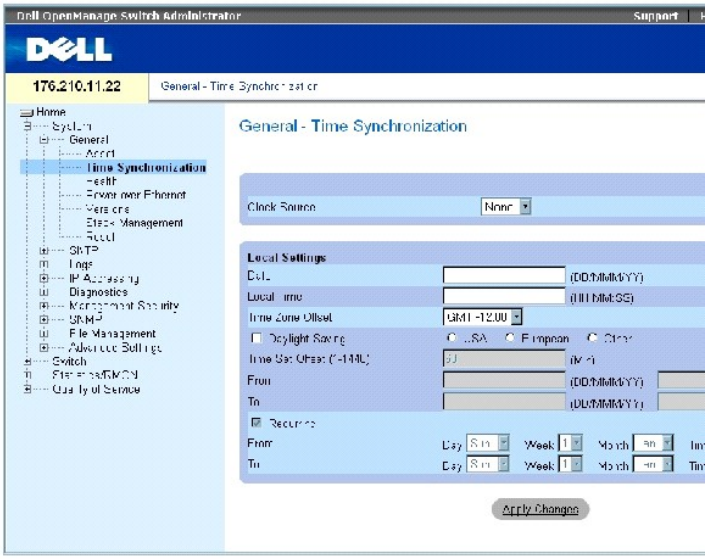
- Albanien – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Australien – Ende Oktober bis Ende März.
- Australien - Tasmanien – Anfang Oktober bis Ende März.
- Armenien – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Österreich – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Bahamas – Von April bis Oktober, entsprechend der Umstellung auf Sommerzeit in den USA.
- Weißrussland – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Belgien – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Brasilien – Dritter Sonntag im Oktober bis dritter Samstag im März. Während der Sommerzeit werden die Uhren im größten Teil des Südostens von Brasilien um eine Stunde vorgestellt.
- Chile – Osterinsel 9. März bis 12. Oktober. Erster Sonntag im März oder nach dem 9. März.
- China – In China gibt es keine Sommerzeit.
- Kanada – Erster Sonntag im April bis letzter Sonntag im Oktober. Die Sommerzeit wird normalerweise von den Regierungen der einzelnen Provinzen und Territorien festgelegt. In manchen Gemeinden können Ausnahmeregelungen bestehen.
- Kuba – Letzter Sonntag im März bis letzter Sonntag im Oktober.
- Zypern – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Dänemark – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Ägypten – Letzter Freitag im April bis letzter Donnerstag im September.
- Estland – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Finnland – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Frankreich – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Deutschland – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Griechenland – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Ungarn – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Indien – In Indien gibt es keine Sommerzeit.
- Iran – 1. Farvardin bis 1. Mehr.
- Irak – 1. April bis 1. Oktober.
- Irland – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Israel – Von Jahr zu Jahr verschieden.
- Italien – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Japan – In Japan gibt es keine Sommerzeit.
- Jordanien – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Lettland – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Libanon – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Litauen – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Luxemburg – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Mazedonien – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Mexiko – Erster Sonntag im April um 2.00 Uhr bis letzter Sonntag im Oktober um 2.00 Uhr.
- Moldawien – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Montenegro – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Niederlande – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Neuseeland – Erster Sonntag im Oktober bis erster Sonntag am oder nach dem 15. März.
- Norwegen – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Paraguay – 6. April bis 7. September.
- Polen – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Portugal – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Rumänien – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Russland – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Serbien – Letztes Wochenende im März bis letztes Wochenende im Oktober.

- Slowakei – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Südafrika – In Südafrika gibt es keine Sommerzeit.
- Spanien – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Schweden – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Schweiz – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Syrien – 31. März bis 30. Oktober.
- Taiwan – In Taiwan gibt es keine Sommerzeit.
- Türkei – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- Großbritannien – Letztes Wochenende im März bis letztes Wochenende im Oktober.
- USA – Erster Sonntag im April um 2.00 Uhr bis letzter Sonntag im Oktober um 2.00 Uhr.

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

Klicken Sie zum Öffnen der Seite **Time Synchronization (Zeitsynchronisierung)** in der *Strukturansicht* auf **System**→ **General**→ **Time Synchronization**.

Abbildung 6-3. Time Synchronization (Zeitsynchronisierung)



Die Seite Time Synchronization (Zeitsynchronisierung) enthält folgende Felder:

Clock Source (Zeitquelle)

Clock Source (Zeitquelle) – Die der Systemzeit zugrunde liegende Zeitquelle. Die möglichen Feldwerte lauten:

SNTP – Gibt an, dass die Systemzeit über einen SNTP-Server eingestellt wird. Weitere Informationen hierzu finden Sie unter **Konfigurieren von SNTP-Einstellungen**.

None (Keine) – Gibt an, dass die Systemzeit nicht über eine externe Zeitquelle eingestellt wird.

Local Settings (Lokale Einstellungen)

Date (Datum) – Legt das Systemdatum fest. Es wird im Format TT/MMM/JJ angegeben, beispielsweise 04/May/05.

Local Time (Ortszeit) – Legt die Systemuhrzeit fest. Sie wird im Format HH/MM/SS angegeben, beispielsweise 21/15/03.

Time Zone Offset (Zeitzonendifferenz) – Der Unterschied zwischen Greenwich Mean Time (GMT; mittlere Greenwich-Zeit) und der Ortszeit. Der Zeitunterschied beträgt beispielsweise für Paris GMT +1 Stunde, während die Ortszeit in New York GMT –5 Stunden ist.

Sie können die Sommerzeit auf zwei verschiedene Weisen festlegen. Sie können entweder die betreffenden Daten für ein bestimmtes Jahr oder periodisch wiederkehrende Einstellungen unabhängig vom Jahr eingeben. Um die Daten für ein bestimmtes Jahr festzulegen, geben Sie die entsprechenden Werte im Bereich **Daylight Savings** (Sommerzeit) ein. Für eine periodische Einstellung geben Sie die entsprechenden Werte im Bereich **Recurring** (Wiederkehrend) ein.

Daylight Saving (Sommerzeit) – Aktiviert die Sommerzeit für das Gerät entsprechend dem Standort des Gerätes. Die möglichen Feldwerte lauten:

USA – Die Umstellung auf Sommerzeit durch das Gerät erfolgt am ersten Sonntag im April um 2.00 Uhr. Die Umstellung auf Normalzeit erfolgt am letzten Sonntag im Oktober um 2.00 Uhr.

European (Europa) – Die Umstellung auf Sommerzeit durch das Gerät erfolgt am letzten Sonntag im März um 1.00 Uhr. Die Umstellung auf Normalzeit erfolgt am letzten Sonntag im Oktober um 1.00 Uhr. Die Option European gilt für Mitgliedsländer der EU und andere europäische Länder, die die EU-Regelung verwenden.

Other (Andere) – Die Festlegung der Sommerzeit erfolgt benutzerdefiniert in Abhängigkeit vom Gerätestandort. Bei Auswahl von **Other** müssen Werte in die Felder **From** (Von) und **To** (Bis) eingegeben werden.

Time Set Offset (1-1440) (Zeitunterschied) – Für Länder außerhalb der USA und Europas kann der Unterschied zwischen der Sommerzeit und der Normalzeit in Minuten angegeben werden. Der Standardwert ist 60 Minuten.

From (Von) – Legt den Zeitpunkt des Beginns der Sommerzeit in Ländern außerhalb der USA oder Europas fest. Das Datum wird im Format TT/MMM/JJ im ersten Feld angegeben; die Uhrzeit im zweiten Feld. Beginnt die Sommerzeit beispielsweise am 25. Oktober 2007 um 5.00 Uhr, werden in die beiden Felder die Werte 25/Oct/07 und 05:00 eingegeben. Die möglichen Feldwerte lauten:

Date (Datum) – Der Tag, an dem die Sommerzeit beginnt. Als Feldwerte können die Werte 1 bis 31 festgelegt werden.

Month (Monat) – Der Monat, in dem die Sommerzeit beginnt. Als Feldwerte können die Werte Jan bis Dec festgelegt werden.

Year (Jahr) – Das Jahr, in dem die konfigurierte Sommerzeit beginnt.

Time (Uhrzeit) – Die Uhrzeit, zu der die Sommerzeit beginnt. Sie wird im Format Stunde: Minute angegeben, beispielsweise 05:30.

To (Bis) – Legt den Zeitpunkt des Endes der Sommerzeit in Ländern außerhalb der USA oder Europas fest. Das Datum wird im Format TT/MMM/JJ im ersten Feld angegeben; die Uhrzeit im zweiten Feld. Endet die Sommerzeit beispielsweise am 23. März 2008 um 12.00 Uhr, werden in die beiden Felder die Werte 23/Mar/08 und 12:00 eingegeben. Die möglichen Feldwerte lauten:

Date (Datum) – Der Tag, an dem die Sommerzeit endet. Als Feldwerte können die Werte 1 bis 31 festgelegt werden.

Month (Monat) – Der Monat, in dem die Sommerzeit endet. Als Feldwerte können die Werte Jan bis Dec festgelegt werden.

Year (Jahr) – Das Jahr, in dem die konfigurierte Sommerzeit endet.

Time (Uhrzeit) – Die Uhrzeit, zu der die Sommerzeit endet. Sie wird im Format Stunde:Minute angegeben, beispielsweise 05:30.

Recurring (Wiederkehrend) – Legt den Zeitpunkt des Beginns und des Endes der Sommerzeit in Ländern außerhalb der USA oder Europas fest, in denen die Sommerzeit in jedem Jahr an demselben Termin beginnt bzw. endet. Die möglichen Feldwerte lauten:

From (Von) – Legt den Zeitpunkt fest, an dem die Sommerzeit jedes Jahr beginnt. Beispiel: Die Sommerzeit beginnt an dem betreffenden Ort immer am zweiten Sonntag im April um 5.00 Uhr. Die möglichen Feldwerte lauten:

Day (Tag) – Der Wochentag, an dem die Sommerzeit jedes Jahr beginnt. Als Feldwerte können die Werte Sunday bis Saturday festgelegt werden.

Week (Woche) – Die Woche des Monats, in dem die Sommerzeit jedes Jahr beginnt. Als Feldwerte können die Werte 1 bis 5 festgelegt werden.

Month (Monat) – Der Monat, in dem die Sommerzeit jedes Jahr beginnt. Als Feldwerte können die Werte Jan bis Dec festgelegt werden.

Time (Uhrzeit) – Die Uhrzeit, zu der die Sommerzeit jedes Jahr beginnt. Sie wird im Format Stunde: Minute angegeben, beispielsweise 02:10.

To (Bis) – Legt den Zeitpunkt fest, an dem die Sommerzeit jedes Jahr endet. Beispiel: Die Sommerzeit endet an dem betreffenden Ort immer am vierten Freitag im Oktober um 5.00 Uhr. Die möglichen Feldwerte lauten:

Day (Tag) – Der Wochentag, an dem die Sommerzeit jedes Jahr endet. Als Feldwerte können die Werte Sunday bis Saturday festgelegt werden.

Week (Woche) – Die Woche des Monats, in dem die Sommerzeit jedes Jahr endet. Als Feldwerte können die Werte 1 bis 5 festgelegt werden.

Month (Monat) – Der Monat, in dem die Sommerzeit jedes Jahr endet. Als Feldwerte können die Werte Jan bis Dec festgelegt werden.

Time (Uhrzeit) – Die Uhrzeit, zu der die Sommerzeit jedes Jahr endet. Sie wird im Format Stunde:Minute angegeben, beispielsweise 05:30.

Auswählen einer Zeitquelle

1. Öffnen Sie die Seite **Time Synchronization (Zeitsynchronisierung)**.
2. Wählen Sie im Feld **Clock Source** (Zeitquelle) den gewünschten Eintrag aus.
3. Klicken Sie auf Apply Changes (Änderungen übernehmen).

Die Zeitquelle wird ausgewählt und das Gerät aktualisiert.

Festlegen von lokalen Zeiteinstellungen

1. Öffnen Sie die Seite **Time Synchronization (Zeitsynchronisierung)**.
2. Definieren Sie die Felder.
3. Klicken Sie auf Apply Changes (Änderungen übernehmen).

Die lokalen Zeiteinstellungen werden angewendet.

Festlegen von Zeiteinstellungen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **Time Synchronization (Zeitsynchronisierung)** äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

ANMERKUNG: Vor dem Festlegen der Einstellungen für die Sommerzeit müssen die folgenden Schritte ausgeführt werden:

1. Konfigurieren Sie die Sommerzeit.
2. Legen Sie die Zeitzone fest.
3. Stellen Sie die Uhr.

Beispiel:

```
console(config)# clock summer-time recurring usa
console(config)# clock time zone 2 zone TMZ2
console(config)# clock set 10:00:00 apr 15 2004
```

Tabelle 6-2. CLI-Befehle zum Festlegen von Zeiteinstellungen

CLI	Beschreibung
clock source sntp	Konfiguriert eine externe Zeitquelle für die Systemuhr.
clock time zone *Unterschied in Stunden* [**minutes** *Unterschied in Minuten*][**zone** *Akronym*]	Legt die Zeitzone für die Anzeige fest.
clock summer-time	Aktiviert die automatische Umstellung des Systems auf Sommerzeit.
clock summer-time recurring {**usa** | **eu** | *Woche Tag Monat hh:mm Woche Tag Monat hh:mm}* [**offset** *Unterschied*] [**zone** *Akronym*]	Aktiviert die automatische Umstellung des Systems auf Sommerzeit (gemäß den Regelungen in den USA bzw. in Europa).
clock summer-time date *Tag Monat Jahr hh:mm Tag Monat Jahr hh:mm* **[offset** *Unterschied***] [zone** *Akronym***]**	Aktiviert die automatische Umstellung des Systems auf Sommerzeit für einen bestimmten Zeitraum, der im Format Tag/Monat/Jahr angegeben wird.

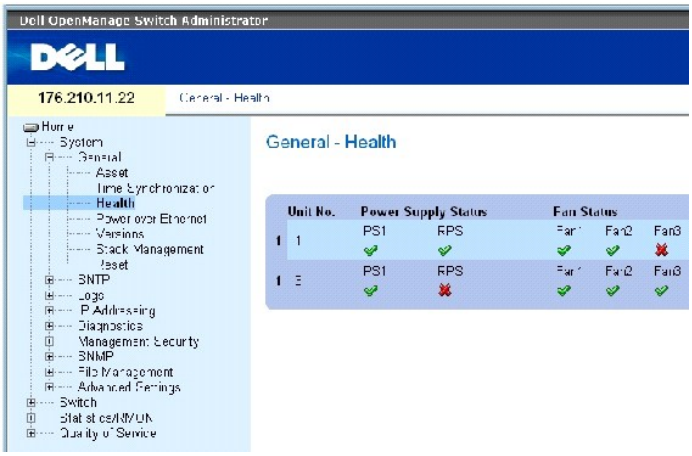
Im Folgenden ein Beispiel für die CLI-Befehle:

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

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

console(config)# clock
source sntp

console(config)# interface
ethernet e14

console(config-if)# sntp
client enable

console(config-if)# exit

console(config)# sntp
broadcast client enable
```

Anzeigen von Informationen zum Systemzustand

Die Seite System Health (Systemzustand) enthält Informationen zu physischen Komponenten des Gerätes, beispielsweise den Netzteilen und Lüftern. Klicken Sie zum Öffnen der Seite System Health (Systemzustand) in der Strukturansicht auf **System**→ **General**→ **Health**.

Abbildung 6-4. System Health (Systemzustand)



Die Seite System Health (Systemzustand) enthält folgende Felder:

Unit No. (Einheit-Nr.) – Gibt die Nummer der Einheit an, für die die Geräte-Systeminformationen angezeigt werden.

Power Supply Status (Status der Netzteile) – Das Gerät verfügt über zwei Netzteile. Für das erste Netzteil wird an der Oberfläche die Bezeichnung PS1 angezeigt, für das redundante Netzteil die Bezeichnung RPS. Die möglichen Feldwerte lauten:

– Das Netzteil funktioniert ordnungsgemäß.

– Das Netzteil funktioniert nicht ordnungsgemäß.

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

Fan Status (Lüfterstatus) – Geräte ohne Power-Over-Ethernet verfügen über zwei Lüfter, PoE-Geräte besitzen fünf Lüfter. Bei den einzelnen Lüftern ist die jeweilige Lüfternummer angegeben, die an der Oberfläche angezeigt wird. Die möglichen Feldwerte lauten:

– Der Lüfter funktioniert ordnungsgemäß.

– Der Lüfter funktioniert nicht ordnungsgemäß.

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

Temperature – Die aktuelle Gerätetemperatur. Die Gerätetemperatur wird in Grad Celsius angezeigt. Der zulässige Temperaturbereich für das Gerät beträgt 0 bis 40 °C (32 bis 104 °F). Die folgende Tabelle zeigt Temperaturwerte in Schritten von 5 Grad und die entsprechenden Temperaturwerte in Grad Fahrenheit an.

Tabelle 6-3. Tabelle für die Umrechnung von Grad Celsius in Grad Fahrenheit

Celsius	Fahrenheit
0	32
5	41
10	50
15	59
20	68

25	77
30	86
35	95
40	104

Anzeigen von Informationen zum Systemzustand mit Hilfe der CLI-Befehle

In der folgenden Tabelle wird der der Seite System Health (Systemzustand) äquivalente CLI-Befehl zur Anzeige von Feldern zusammengefasst.

Tabelle 6-4. CLI-Befehl zum Anzeigen des Systemzustands

CLI-Befehl	Beschreibung
show system [**unit** *Einheit*]	Zeigt Systeminformationen an.

Im Folgenden ein Beispiel für den CLI-Befehl zum Anzeigen des Systemzustands:

```
Console> show system

System Description: Ethernet switch

System Up Time (days,hour:min:sec): 1,22:38:21

System Contact:

System Name: RS1

System location:

System MAC Address: 00.10.B5.F4.00.01

Sys Object ID: 1.3.6.1.4.1.674.10895.3004

Type: PowerConnect 3424

Temperature Sensors:

Unit   Sensor                 Temperature (Celsius)          Status
----   ------                 ---------------------          ------
1      1                                  41                 OK
1      2                                  41                 OK
2      1                                  42                 OK
```

2	2		42	OK
Unit	Power Supply	Source	Status	
----	----------	------	------	
1	Main	AC	OK	
2	Secondary	AC	OK	
Unit	Fan	Status		
----	---	------		
1	CPU	OK		
2	CPU	OK		

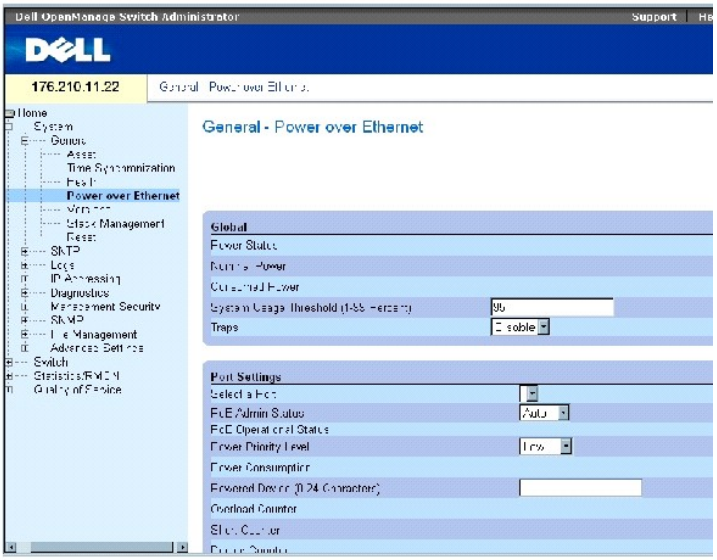
Power-Over-Ethernet

Power-Over-Ethernet (PoE) ermöglicht die Stromversorgung von Endgeräten über vorhandene LAN-Kabel ohne Aufrüstung oder Änderung der Netzwerkinfrastruktur. Der Vorteil von Power-Over-Ethernet besteht darin, dass Netzwerkgeräte nicht mehr in der Nähe von Steckdosen aufgestellt werden müssen.

Powered Devices sind Endgeräte, die über die Netzteile des PowerConnect-Switches mit Strom versorgt werden, beispielsweise IP-Telefone. Der Anschluss von Powered Devices an das PowerConnect-Gerät erfolgt über Ethernet-Ports. Powered Devices werden entweder über alle 24 FE-Ports von PowerConnect 3424P-Geräten oder über alle 48 FE-Ports von PowerConnect 3448P-Geräten angeschlossen.

Klicken Sie zum Öffnen der Seite Power Over Ethernet in der Strukturansicht auf **System**→ **General**→ **Power over Ethernet**.

Abbildung 6-5. Power Over Ethernet



Die Seite Power Over Ethernet enthält folgende Bereiche:

- Global (Globale Einstellungen)
- Port Settings (Port-Einstellungen)

Global (Globale Einstellungen)

Der Bereich für die globalen Power-Over-Ethernet-Einstellungen enthält folgende Felder:

Power Status (Stromversorgungsstatus) – Gibt den Status der PoE-Stromversorgung an.

On (Ein) – Zeigt an, dass das Netzteil funktioniert.

Off (Aus) – Zeigt an, dass das Netzteil nicht funktioniert.

Faulty (Störung) – Zeigt an, dass das Netzteil funktioniert, aber ein Fehler aufgetreten ist; beispielsweise eine Überlastung oder ein Kurzschluss.

Nominal Power (Nennleistung) – Gibt die Nennleistung des Gerätes an. Der Feldwert wird in Watt angezeigt.

Consumed Power (Aufgenommene Leistung) – Gibt die vom Gerät aufgenommene Leistung an. Der Feldwert wird in Watt angezeigt.

System Usage Threshold (1-99 Percent) (Schwellenwert für die Systemauslastung (1-99 Prozent)) – Gibt den Prozentsatz der Leistungsaufnahme des Systems an, ab dem ein Alarm ausgegeben wird. Der Feldwert kann im Bereich 1 bis 99 Prozent festgelegt werden. Der Standardwert ist 95 Prozent.

Traps – Aktiviert bzw. deaktiviert den Empfang von PoE-Geräte-Traps. Die Standardeinstellung lautet Disable (Deaktiviert).

Port Settings (Port-Einstellungen)

Select a Port (Port auswählen) – Gibt die betreffende Schnittstelle an, für die PoE-Parameter definiert werden. Die definierten Parameter werden der PoE-

Schnittstelle zugewiesen, die mit dem ausgewählten Port verbunden ist.

PoE Admin Status (PoE-Verwaltungsstatus) – Gibt den PoE-Modus des Gerätes an. Die möglichen Feldwerte lauten:

Auto (Automatisch) – Aktiviert das Geräteerkennungsprotokoll und versorgt das Gerät über das PoE-Modul mit Strom. Mit Hilfe des Geräteerkennungsprotokolls kann das Gerät Powered Devices erkennen, die an die Geräteschnittstellen angeschlossen sind, und ihre jeweilige Klasse ermitteln. Dies ist die Standardeinstellung.

Never (Nie) – Deaktiviert das Geräteerkennungsprotokoll und beendet die Stromversorgung des Gerätes über das PoE-Modul.

PoE Operational Status (PoE-Betriebsstatus) – Gibt an, ob der Port für die PoE-Stromversorgung aktiviert ist. Die möglichen Feldwerte lauten:

On (Ein) – Gibt an, dass die Schnittstelle vom Gerät mit Strom versorgt wird.

Off (Aus) – Gibt an, dass die Schnittstelle vom Gerät nicht mit Strom versorgt wird.

Test Fail (Test fehlgeschlagen) – Gibt an, dass der Test des Powered Device fehlgeschlagen ist. Beispiel: Ein Port konnte nicht aktiviert werden und steht somit nicht für die Stromversorgung des Powered Device zur Verfügung.

Testing (Gerät wird getestet) – Gibt an, dass das Powered Device derzeit getestet wird. Durch den Test wird beispielsweise bestätigt, dass das Powered Device über das Netzteil mit Strom versorgt wird.

Searching (Suchen) – Gibt an, dass das PowerConnect-Gerät derzeit nach einem Powered Device sucht. Searching ist die Standardeinstellung für den PoE-Betriebsstatus.

Fault (Störung) – Gibt an, dass das PowerConnect-Gerät einen Fehler am Powered Device festgestellt hat. Beispiel: Der Speicher des Powered Device konnte nicht gelesen werden.

Power Priority Level (Stromversorgungspriorität) – Legt die Port-Priorität bei niedriger Versorgungsspannung fest. Die Einstellungen für die Port-Priorität werden verwendet, wenn die Versorgungsspannung niedrig ist. Die Standardeinstellung des Felds lautet Low (Niedrig). Beispiel: Wenn für Port 1 die Priorität High (Hoch) und für Port 3 die Priorität Low festgelegt ist und die Auslastung des Netzteils 99 % beträgt, besitzt die Stromversorgung von Port 1 Priorität; die Stromversorgung von Port 3 wird unter Umständen deaktiviert.

Critical (Kritisch) – Weist die höchste Prioritätsstufe für die Stromversorgung zu.

High (Hoch) – Weist die zweithöchste Prioritätsstufe für die Stromversorgung zu.

Low (Niedrig) – Weist die niedrigste Prioritätsstufe für die Stromversorgung zu.

Power Consumption (Leistungsaufnahme) – Gibt die Leistungsaufnahme an, die dem an die ausgewählte Schnittstelle angeschlossenen Powered Device zugewiesen ist. Powered Devices sind in verschiedene Klassen eingeteilt; diese Klassifizierungsinformationen werden von den PowerConnect-Geräten verwendet. Die Feldwerte werden in Watt angezeigt. Die möglichen Feldwerte lauten:

0.44 – 12.95 – Gibt an, dass dem Port eine Leistungsaufnahme zwischen 0,44 und 12,95 Watt zugewiesen ist.

0.44 – 3.8 – Gibt an, dass dem Port eine Leistungsaufnahme zwischen 0,44 und 3,8 Watt zugewiesen ist.

3.84 – 6.49 – Gibt an, dass dem Port eine Leistungsaufnahme zwischen 3,84 und 6,49 Watt zugewiesen ist.

6.49 – 12.95 – Gibt an, dass dem Port eine Leistungsaufnahme zwischen 6,49 und 12,95 Watt zugewiesen ist.

Power Device (0-24 characters) (Powered Device (0-24 Zeichen)) – Enthält eine benutzerdefinierte Beschreibung des Powered Device. Das Feld darf bis zu 24 Zeichen enthalten.

Overload Counter (Überlastzähler) – Gibt die Gesamtzahl der während der Stromversorgung aufgetretenen Überlastungen an.

Short Counter (Zähler für Stromausfälle) – Gibt die Gesamtzahl der während der Stromversorgung aufgetretenen Stromausfälle an.

Denied Counter (Zähler für abgelehnte Stromversorgung) – Gibt an, wie oft die Stromversorgung des Powered Device abgelehnt wurde.

Absent Counter (Zähler für Geräte-Nichterkennung) – Gibt an, wie oft die Stromversorgung des Powered Device beendet wurde, weil das Powered Device nicht mehr erkannt wurde.

Invalid Signature Counter (Zähler für ungültige Signaturen) – Gibt an, wie oft eine ungültige Signatur empfangen wurde. Powered Devices identifizieren sich anhand von Signaturen gegenüber dem PSE. Signaturen werden während der Erkennung, Klassifizierung oder Wartung von Powered Devices erzeugt.

Definieren von PoE-Einstellungen

1. Öffnen Sie die Seite Power Over Ethernet.
2. Definieren Sie die Felder.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die PoE-Einstellungen werden definiert und das Gerät aktualisiert.

Verwalten von PoE-Einstellungen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite Power Over Ethernet äquivalenten CLI-Befehle zur Anzeige von Feldern zusammengefasst.

Tabelle 6-5. CLI-Befehle für PoE-Einstellungen

CLI-Befehl	Beschreibung
power inline {auto | never}	Konfiguriert den Verwaltungsmodus für die PoE-Speisung einer Schnittstelle.
power inline powered-device *PD-Typ*	Fügt eine Beschreibung des Powered Device-Typs hinzu.
power inline priority {critical | high | low}	Konfiguriert die Priorität der Schnittstelle hinsichtlich der PoE-Stromversorgung.
power inline usage-threshold	Konfiguriert den Schwellenwert für die Auslösung von Alarmen.
power inline traps enable	Aktiviert den Empfang von PoE-Geräte-Traps.
show power inline [Ethernet- Schnittstelle]	Zeigt PoE-Konfigurationsinformationen an.

Im Folgenden ein Beispiel für die PoE-CLI-Befehle:

```
Console# show power inline
```

Power: On

Nominal Power: 150 Watts

Consumed Power: 120 Watts (80%)

Usage Threshold: 95%

Traps: Enabled

Port	Powered Device	State	Priority	Status	Classification [W]
1/e1	IP Phone Model A	Auto	High	On	0.44 – 12.95
2/e1	Wireless AP Model	Auto	Low	On	0.44 – 3.84
3/e1		Auto	Low	Off	N/A

Console# **show power inline ethernet** 1/e1

Port	Powered Device	State	Priority	Status	Classification [W]
1/1e	IP Phone Model A	Auto	High	On	0.44 – 12.95

Overload Counter: 1

Short Counter: 0

Denied Counter: 0

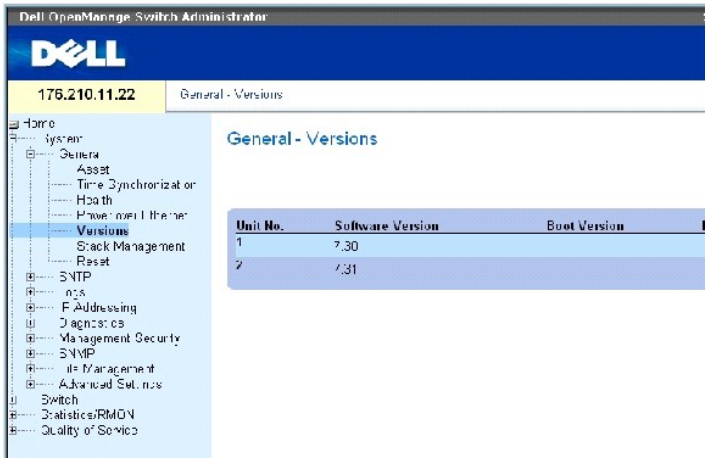
Absent Counter: 0

Invalid Signature Counter: 0

Anzeigen von Versionsinformationen

Die Seite **Versions (Versionen)** enthält Informationen zu den Versionen der derzeit ausgeführten Hardware und Software. Klicken Sie zum Öffnen der Seite **Versions (Versionen)** in der Strukturansicht auf System→ General→ Versions.

Abbildung 6-6. Versions (Versionen)



Die Seite **Versions (Versionen)** enthält folgende Felder:

Unit No. (Einheit-Nr.) – Gibt die Nummer der Einheit an, für die die Geräteversionen angezeigt werden.

Software Version (Softwareversion) – Die Version der derzeit auf dem Gerät ausgeführten Software.

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

Hardware Version (Hardwareversion) – Die aktuelle Hardwareversion des Gerätes.

Anzeigen von Geräteversionen mit Hilfe der CLI-Befehle

In der folgenden Tabelle wird der der Seite Versions (Versionen) äquivalente CLI-Befehl zur Anzeige von Feldern zusammengefasst.

Tabelle 6-6. CLI-Befehl für die Anzeige von Versionen

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

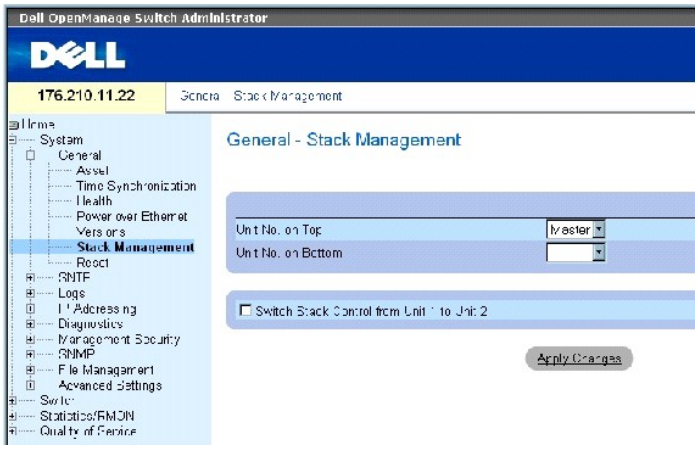
Im Folgenden ein Beispiel für die CLI-Befehle:

```
console> show version

SW version 1.0.0.0 (date 23-Jan-2005 time 17:34:19)

Boot version 1.0.0.0 (date 11-Jan-2005 time 11:48:21)

HW version 1.0.0
```

Verwalten von Stack-Komponenten

Über die Seite **Stack Management (Stack-Verwaltung)** können Netzwerkverwalter den gesamten Stack oder ein bestimmtes Gerät zurücksetzen. Klicken Sie zum Öffnen der Seite **Stack Management (Stack-Verwaltung)** in der Strukturansicht auf **System→ General→ Stack Management**.

Abbildung 6-7. Stack Management (Stack-Verwaltung)



ANMERKUNG: Speichern Sie vor dem Zurücksetzen des Gerätes alle Änderungen an der Datei Running Configuration (Aktive Konfiguration). Hierdurch wird verhindert, dass die aktuelle Gerätekonfiguration verloren geht. Weitere Informationen zum Speichern von Konfigurationsdateien finden Sie unter Verwalten von Dateien.

Unit No. on Top (Nummer der oberen Einheit) – Die Nummer der ersten Stack-Komponente. Mögliche Werte sind Master und 1 bis 6.

Unit No. on Bottom (Nummer der unteren Einheit) – Die Nummer der zweiten Stack-Komponente. Mögliche Werte sind Master und 1 bis 6.

Switch Stack Control from Unit 1 to Unit 2 (Stack-Steuerung von Einheit 1 auf Einheit 2 umschalten) – Aktiviert die Umschaltung der Stack-Steuerung von der aktuellen Stack-Mastereinheit auf die Mastersicherungseinheit.

ANMERKUNG: Durch das Zurücksetzen der Mastereinheit wird der gesamte Stack zurückgesetzt.

Umschalten zwischen Stack-Mastereinheiten

1. Öffnen Sie die Seite **Stack Management (Stack-Verwaltung)**.
2. Aktivieren Sie das Kontrollkästchen Switch Stack Control from Unit 1 to Unit 2 (Stack- Steuerung von Einheit 1 auf Einheit 2 umschalten).
3. Klicken Sie auf Apply Changes (Änderungen übernehmen).

   Eine Bestätigungsmeldung wird angezeigt.
4. Klicken Sie auf OK.

   Das Gerät wird zurückgesetzt. Nach dem Zurücksetzen des Gerätes wird eine Aufforderung zur Eingabe eines Benutzernamens und Kennworts angezeigt.

Konfigurieren der Anzeigereihenfolge von Stack-Einheiten

1. Öffnen Sie die Seite **Stack Management (Stack-Verwaltung)**.
2. Legen Sie die Stack-Topologie durch Auswählen der oberen Einheit (Unit No. on Top) und unteren Einheit (Unit No. on Bottom) fest. Bei diesen Einheiten sollte es sich um benachbarte Komponenten handeln.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Anzeigereihenfolge auf der Seite **System** wird aktualisiert.

Verwalten von Stacks mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **Stack Management (Stack-Verwaltung)** äquivalenten CLI-Befehle zur Anzeige von Feldern zusammengefasst.

Tabelle 6-7. CLI-Befehle für die Stack-Verwaltung

CLI-Befehl	Beschreibung
reload	Lädt das Betriebssystem neu.
stack reload	Lädt Stack-Komponenten neu.
stack master	Erzwingt die Auswahl des Stack-Masters.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console# reload


Are you sure you want to erase running configuration (y/n) [n]
```

Zurücksetzen des Gerätes

Auf der Seite Reset (Zurücksetzen) kann das Gerät von einem Remote-Standort aus zurückgesetzt werden. Klicken Sie zum Öffnen der Seite Reset in der Strukturansicht auf System→ General→ Reset.

Die Seite Reset (Zurücksetzen) enthält das folgende Feld:

Reset Unit No. (Einheit-Nr. zurücksetzen) – Setzt die ausgewählte Stack-Komponente zurück.

ANMERKUNG: Speichern Sie vor dem Zurücksetzen des Gerätes alle Änderungen an der Datei Startup Configuration (Startkonfiguration). Hierdurch wird verhindert, dass die aktuelle Gerätekonfiguration verloren geht. Weitere Informationen zum Speichern von Konfigurationsdateien finden Sie unter Verwalten von Dateien.

Zurücksetzen des Gerätes

1. Öffnen Sie die Seite Reset (Zurücksetzen).
2. Wählen Sie im Feld **Reset Unit Number** (Einheit-Nr. zurücksetzen) eine Einheit aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Eine Bestätigungsmeldung wird angezeigt.
4. Klicken Sie auf **OK**.

   Das Gerät wird zurückgesetzt. Nach dem Zurücksetzen des Gerätes wird eine Aufforderung zur Eingabe eines Benutzernamens und Kennworts angezeigt.
5. Geben Sie einen Benutzernamen und ein Kennwort ein, um sich erneut bei der Weboberfläche anzumelden.

Zurücksetzen des Gerätes mit Hilfe der CLI-Befehle

In der folgenden Tabelle wird der äquivalente CLI-Befehl zum Zurücksetzen des Gerätes über die CLI zusammengefasst:

Tabelle 6-8. CLI-Befehl zum Zurücksetzen des Gerätes

CLI-Befehl	Beschreibung
reload	Lädt das Betriebssystem neu.

Im Folgenden ein Beispiel für den CLI-Befehl:

```
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

Der Switch unterstützt das Simple Network Time Protocol (SNTP). SNTP gewährleistet eine auf die Millisekunde genaue Synchronisierung der Zeiteinstellungen von Netzwerk-Switches. Die Zeitsynchronisierung erfolgt durch einen Netzwerk-SNTP-Server. Das Gerät wird nur als SNTP-Client betrieben; es kann keine Zeitdienste für andere Systeme bereitstellen.

Der Switch kann die Serverzeit von den folgenden Servertypen abfragen:

- Unicast-Server
- Anycast-Server
- Broadcast-Server

Zeitquellen sind durch Stratum-Werte (Schichten) gekennzeichnet. Die Stratum-Werte legen die Genauigkeit der Referenzuhr fest. Je höher das Stratum ist (null steht für das höchste Stratum), desto genauer ist die Uhr. Der Switch empfängt die Zeit von Stratum 1 und höher. Im Folgenden ist ein Beispiel für Stratum-Werte gezeigt:

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

Die von SNTP-Servern empfangenen Informationen werden auf der Grundlage der Zeitebene und des Servertyps ausgewertet. SNTP-Zeitdefinitionen werden anhand der folgenden Zeitebenen beurteilt und ermittelt:

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

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

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

Die Abfrage von Anycast-Informationen wird verwendet, wenn die IP-Adresse des Servers unbekannt ist. Wenn dieses Verfahren ausgewählt ist, können alle SNTP-Server im Netzwerk Synchronisierungsinformationen senden. Das Gerät wird synchronisiert, wenn es proaktiv Synchronisierungsinformationen anfordert.

Die beste Antwort (niedrigstes Stratum) der ersten 3 SNTP-Server, die auf die Abfrage von Synchronisierungsinformationen antworten, wird zur Festlegung des Zeitwertes verwendet. Die Serverzeit wird anhand der Zeitebenen T3 und T4 ermittelt.

Anycast-Abfragen für den Abruf von Informationen zur Synchronisierung der Gerätezeit werden Broadcast-Abfragen vorgezogen. Dieses Verfahren bietet jedoch weniger Sicherheit als die Verwendung von Unicast-Abfragen, da SNTP-Pakete von SNTP-Servern akzeptiert werden, die nicht für das Gerät konfiguriert wurden.

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

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

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

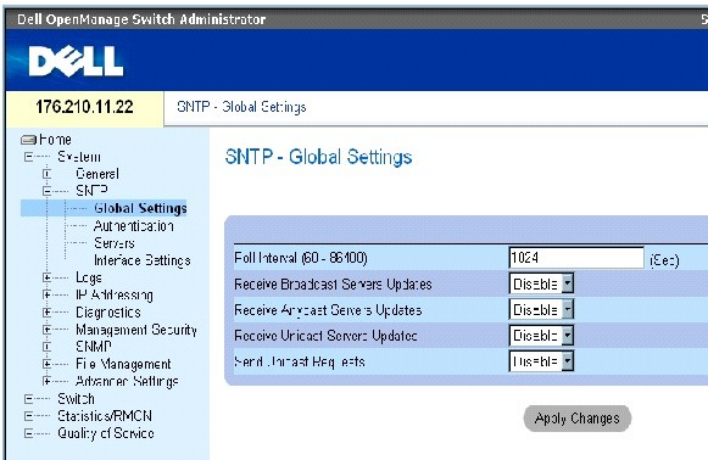
Pfade zu SNTP-Servern, über die eine Gerätesynchronisierung erfolgt, sind durch MD5-Authentifizierung (Message Digest 5) geschützt. MD5 ist ein Algorithmus, der einen 128 Bit langen Hash-Wert erzeugt. MD5 ist eine Variante von MD4, die höhere Sicherheit als MD4 bietet. MD5 prüft die Integrität der Kommunikation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

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

Definieren globaler SNTP-Parameter

Die Seite **SNTP Global Settings (Globale SNTP-Einstellungen)** enthält Felder für die globale Festlegung von SNTP-Parametern. Klicken Sie zum Öffnen der Seite **SNTP Global Settings (Globale SNTP-Einstellungen)** in der Strukturansicht auf **System**→ **SNTP**→ **Global Settings**.

Abbildung 6-8. SNTP Global Settings (Globale SNTP-Einstellungen)



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

Poll Interval (60-86400) (Abfrageintervall (60-86400)) – Definiert das Intervall (in Sekunden) für die Abfrage von Unicast-Informationen des SNTP-Servers. Das Abfrageintervall ist standardmäßig auf 1024 Sekunden gesetzt.

Receive Broadcast Servers Updates (Aktualisierungen von Broadcast-Servern empfangen) – Wenn diese Option aktiviert ist (Einstellung Enable), prüfen die

ausgewählten Schnittstellen, ob Broadcast-Server-Zeitinformationen von den SNTP-Servern gesendet werden.

Receive Anycast Servers Updates (Aktualisierungen von Anycast-Servern empfangen) – Wenn diese Option aktiviert ist (Einstellung Enable), werden Anycast-Server-Zeitinformationen vom SNTP-Server abgerufen. Wenn sowohl die Option **Receive Anycast Servers Update** als auch die Option **Receive Broadcast Servers Update** aktiviert ist, werden für die Festlegung der Systemzeit Anycast-Server-Zeitinformationen verwendet.

Receive Unicast Servers Updates (Aktualisierungen von Unicast-Servern empfangen) – Wenn diese Option aktiviert ist (Einstellung Enable), werden Unicast-Server-Zeitinformationen vom SNTP-Server abgerufen. Sind die Optionen **Receive Broadcast Servers Updates**, **Receive Anycast Servers Updates** und **Receive Unicast Servers Updates** gleichzeitig aktiviert, werden für die Festlegung der Systemzeit Unicast-Server-Zeitinformationen verwendet.

Send Unicast Requests (Unicast-Anforderungen senden) – Wenn diese Option aktiviert ist (Einstellung Enable), werden an den SNTP-Server Anforderungen zum Senden von Unicast-Server-Zeitinformationen gesendet.

Auswählen einer Zeitquelle

1. Öffnen Sie die Seite **Time Synchronization (Zeitsynchronisierung)**.
2. Wählen Sie im Feld **Clock Source** (Zeitquelle) den gewünschten Eintrag aus.
3. Klicken Sie auf Apply Changes (Änderungen übernehmen).

Die Zeitquelle wird ausgewählt und das Gerät aktualisiert.

Festlegen von lokalen Zeiteinstellungen

1. Öffnen Sie die Seite **Time Synchronization (Zeitsynchronisierung)**.
2. Definieren Sie die Felder.
3. Klicken Sie auf Apply Changes (Änderungen übernehmen).

Die lokalen Zeiteinstellungen werden angewendet.

Definieren globaler SNTP-Parameter mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **SNTP Global Settings (Globale SNTP-Einstellungen)** äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-9. CLI-Befehle für globale SNTP-Parameter

CLI-Befehl	Beschreibung
sntp broadcast client enable	Aktiviert SNTP-Broadcast-Clients.
sntp anycast client enable	Aktiviert SNTP-Anycast-Clients.
sntp unicast client enable	Aktiviert vordefinierte SNTP-Unicast-Clients.

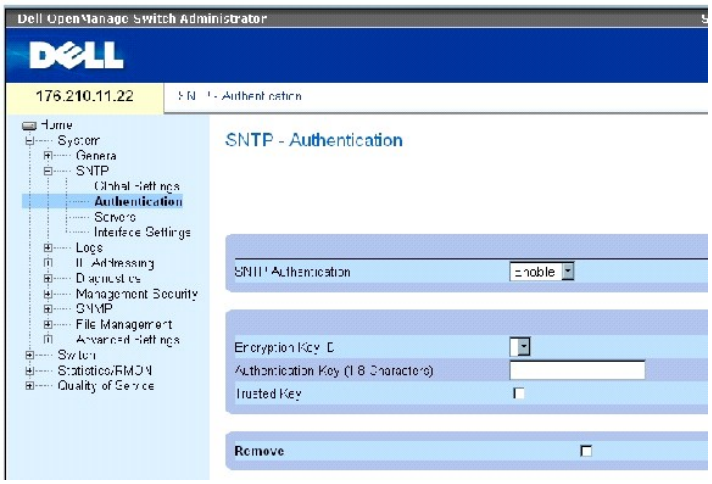
Im Folgenden ein Beispiel für die CLI-Befehle:

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

Definieren von SNTP-Authentifizierungsmethoden

Auf der Seite SNTP Authentication (SNTP-Authentifizierung) können Sie die SNTP-Authentifizierung zwischen dem Gerät und einem SNTP-Server aktivieren. Auch die Methode für die Authentifizierung des SNTP-Servers wird auf der Seite SNTP Authentication (SNTP-Authentifizierung) ausgewählt. Klicken Sie zum Öffnen der Seite SNTP Authentication (SNTP-Authentifizierung) in der Strukturansicht auf **System→ SNTP→ Authentication**.

Abbildung 6-9. SNTP Authentication (SNTP-Authentifizierung)



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

SNTP Authentication (SNTP-Authentifizierung) – Wenn diese Option aktiviert ist (Einstellung Enable), wird bei einer SNTP-Sitzung zwischen dem Gerät und einem SNTP-Server eine Authentifizierung durchgeführt.

Encryption Key ID (Verschlüsselungs-ID) – Legt die Schlüssel-ID für die Authentifizierung des SNTP-Servers und des Gerätes fest. Der Feldwert kann bis zu 4294967295 Zeichen umfassen.

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

Trusted Key (Vertrauenswürdiger Schlüssel) – Gibt den für die Authentifizierung des SNTP-Servers verwendeten Verschlüsselungsschlüssel (Unicast) an.

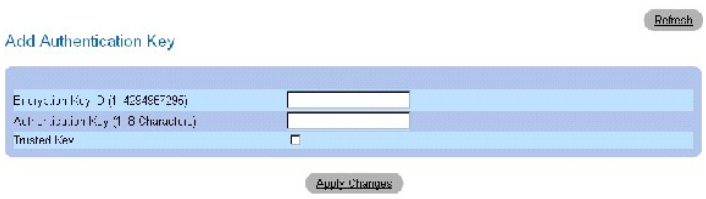
Remove (Entfernen) – Wenn dieses Kontrollkästchen aktiviert ist, werden die ausgewählten Authentifizierungsschlüssel entfernt.

Hinzufügen eines SNTP-Authentifizierungsschlüssels

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

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

Abbildung 6-10. Add Authentication Key (Authentifizierungsschlüssel hinzufügen)



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

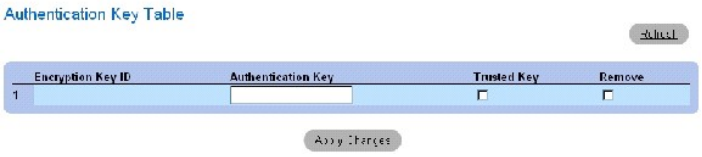
Der SNMP-Authentifizierungsschlüssel wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der Seite Authentication Key Table (Tabelle der Authentifizierungsschlüssel)

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

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

Abbildung 6-11. Authentication Key Table (Tabelle der Authentifizierungsschlüssel)



Löschen des Authentifizierungsschlüssels

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

Die Seite **Authentication Key Table (Tabelle der Authentifizierungsschlüssel)** wird geöffnet.

3. Wählen Sie einen Eintrag in der **Authentication Key Table** aus.
4. Aktivieren Sie das Kontrollkästchen Remove (Entfernen).
5. Klicken Sie auf Apply Changes (Änderungen übernehmen).

Der Eintrag wird entfernt und das Gerät aktualisiert.

Definieren von SNTP-Authentifizierungseinstellungen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **SNTP Authentication (SNTP-Authentifizierung)** äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-10. CLI-Befehle für die SNTP-Authentifizierung

CLI-Befehl	Beschreibung
sntp authenticate	Aktiviert die Authentifizierung des von Servern eingehenden SNTP-Datenverkehrs (Simple Network Time Protocol).
sntp trusted key	Authentifiziert die Identität eines Systems, mit dem eine Synchronisierung über SNTP erfolgen soll.
sntp authentication-key *Nummer* **md5** *Wert*	Definiert einen Authentifizierungsschlüssel für SNTP.

Im Folgenden ein Beispiel für die CLI-Befehle:

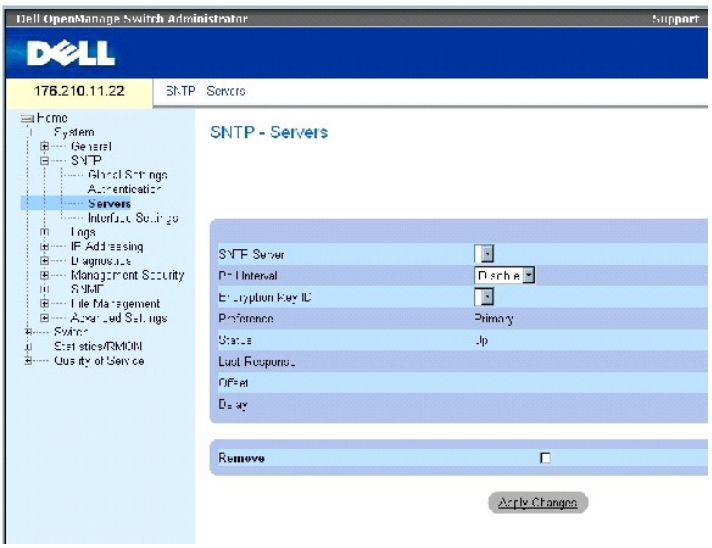
```
console(config)# sntp
authentication-key 8 md5
Calked


console(config)# sntp
```

```
trusted-key 8


Console(config)# sntp
authenticate
```

Definieren von SNTP-Servern

Sie können über die Seite **SNTP Servers (SNTP-Server)** sowohl SNTP-Server aktivieren als auch neue SNTP-Server hinzufügen. *Klicken Sie zum Öffnen der Seite* **SNTP Servers (SNTP-Server)** in der Strukturansicht auf **System→ SNTP→ Servers**.

Abbildung 6-12. SNTP Servers (SNTP-Server)



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

SNTP Server – Wählen Sie die IP-Adresse eines benutzerdefinierten SNTP-Servers aus. Bis zu acht SNTP-Server können definiert werden.

Poll Interval (Abfrageintervall) – Wenn diese Option aktiviert ist, werden Systemzeitinformationen vom ausgewählten SNTP-Server abgerufen.

Encryption Key ID (Verschlüsselungs-ID) – Gibt die für die Kommunikation zwischen dem SNTP-Server und dem Gerät verwendete Schlüssel-ID an. Bereich: 1 - 4294967295.

Preference (Vorrang) – Der SNTP-Server, der SNTP-Systemzeitinformationen bereitstellt. Die möglichen Feldwerte lauten:

Primary (Primär) – Die SNTP-Informationen werden von dem primären Server bereitgestellt.

Secondary (Sekundär) – Die SNTP-Informationen werden von dem sekundären Server bereitgestellt.

Status – Der Betriebsstatus des SNTP-Servers. Die möglichen Feldwerte lauten:

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

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

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

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

Last Response (Letzte Antwort) – Der letzte Zeitpunkt, zu dem eine Antwort vom SNTP-Server empfangen wurde.

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

Delay (Verzögerung) – Die zum Erreichen des SNTP-Servers benötigte Zeit.

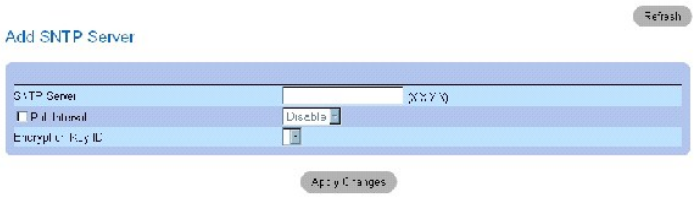
Remove (Entfernen) – Wenn dieses Kontrollkästchen aktiviert ist, wird der betreffende SNTP-Server aus der Liste **SNTP Server** entfernt.

Hinzufügen eines SNTP-Servers

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

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

Abbildung 6-13. Add SNTP Server (SNTP-Server hinzufügen)



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

Der SNTP-Server wird hinzugefügt und das Gerät aktualisiert.

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

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

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

Abbildung 6-14. SNTP Servers Table (Tabelle der SNTP-Server)

Ändern eines SNTP-Servers

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

   Die Seite **SNTP Servers Table (Tabelle der SNTP-Server)** wird geöffnet.
3. Wählen Sie den Eintrag eines SNTP-Servers aus.
4. Ändern Sie die relevanten Felder.
5. Klicken Sie auf Apply Changes (Änderungen übernehmen).

   Die Informationen zum SNTP-Server werden aktualisiert.

Löschen eines SNTP-Servers

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

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

   Der Eintrag wird entfernt und das Gerät aktualisiert.

Definieren von SNTP-Servereinstellungen mit Hilfe der CLI-Befehle

In der folgenden Tabelle wird der der Seite **SNTP Servers (SNTP-Server)** äquivalente CLI-Befehl zur Festlegung von Feldern zusammengefasst.

Tabelle 6-11. CLI-Befehl für SNTP-Server

CLI-Befehl	Beschreibung
sntp server IP-Adresse|Hostname [poll] [key Schlüssel-ID]	Konfiguriert das Gerät zur Verwendung von SNTP für die Abfrage und den Empfang von SNTP-Datenverkehr von einem Server.

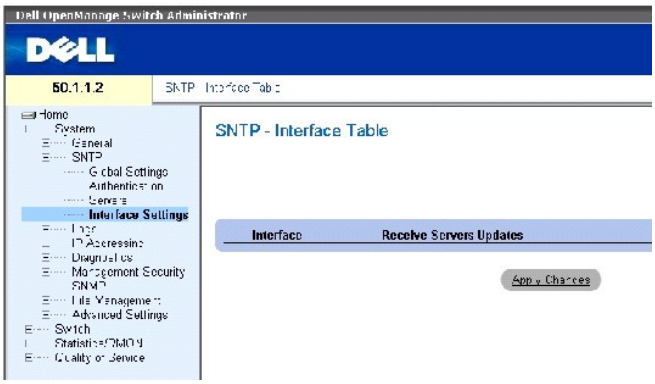
Im Folgenden ein Beispiel für die CLI-Befehle:

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

Definieren von SNTP-Schnittstellen

Die Seite **SNTP Interface Settings (SNTP-Schnittstelleneinstellungen)** enthält Informationen zu SNTP-Schnittstellen. Klicken Sie zum Öffnen der Seite **SNTP Interface Settings (SNTP-Schnittstelleneinstellungen)** in der Strukturansicht auf System→ SNTP→Interface Settings.

Abbildung 6-15. SNTP Interface Settings (SNTP-Schnittstelleneinstellungen)



Die Seite **SNTP Interface Settings (SNTP-Schnittstelleneinstellungen)** enthält folgende Felder:

Unit No. (Einheit-Nr.) – Gibt die Stack-Komponente an, auf der die SNTP-Schnittstelle aktiviert ist.

Interface (Schnittstelle) – Enthält eine Liste der Schnittstellen, für die SNTP aktiviert werden kann.

Receive Servers Updates (Server-Aktualisierungen annehmen) – Aktiviert bzw. deaktiviert SNTP für die betreffende Schnittstelle.

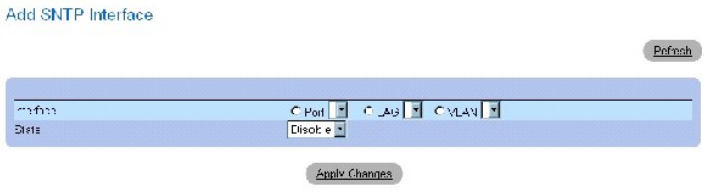
Remove (Entfernen) – Wenn diese Option aktiviert ist, wird SNTP für die betreffende Schnittstelle entfernt.

Hinzufügen einer SNTP-Schnittstelle

1. Öffnen Sie die Seite **SNTP Interface Settings (SNTP-Schnittstelleneinstellungen)**.
2. Klicken Sie auf Add (Hinzufügen).

   Die Seite **Add SNTP Interface (SNTP-Schnittstelle hinzufügen)** wird geöffnet.

Abbildung 6-16. Add SNTP Interface (SNTP-Schnittstelle hinzufügen)



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

   Die SNTP-Schnittstelle wird hinzugefügt und das Gerät aktualisiert.

Definieren von SNTP-Schnittstelleneinstellungen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **SNTP Interface Settings (SNTP-Schnittstelleneinstellungen)** äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

ANMERKUNG: Für eine Schnittstelle, die als Anycast- oder Broadcast-Schnittstelle konfiguriert werden soll, muss eine IP-Adresse definiert worden sein.

Tabelle 6-12. CLI-Befehle für SNTP-Schnittstelleneinstellungen

CLI-Befehl	Beschreibung
sntp client enable	Aktiviert den SNTP-Client (Simple Network Time Protocol) für eine Schnittstelle.
show sntp configuration	Zeigt die Konfiguration des Simple Network Time Protocol (SNTP) an.

Im Folgenden ein Beispiel für die CLI-Befehle zum Anzeigen von SNTP-Schnittstellen:

```
console# show sntp configuration

Polling interval: 7200 seconds.

MD5 Authentication keys: 8, 9

Authentication is required for synchronization.

Trusted Keys: 8,9

Unicast Clients Polling: Enabled.

Server                  Polling     Encryption Key
----------              --------    --------------
176.1.1.8               Enabled     9
176.1.8.179             Disabled    Disabled

Broadcast Clients: Enabled

Broadcast Clients Poll: Enabled

Broadcast Interfaces:1/e1, 1/e3
```

Verwalten von Protokollen

Die Seite **Logs (Protokolle)** enthält Links zu verschiedenen Protokollseiten. Klicken Sie zum Öffnen der Seite **Logs** in der Strukturansicht auf System→ Logs.

Definieren globaler Protokollparameter

Mit Hilfe von Systemprotokollen können Sie Geräteereignisse in Echtzeit anzeigen und diese Ereignisse zur späteren Verwendung aufzeichnen. Systemprotokolle dienen zur Aufzeichnung und Verwaltung von Ereignissen und enthalten Fehler- oder Informationsmeldungen.

Ereignismeldungen verfügen gemäß dem empfohlenen Syslog-Protokoll über ein eindeutiges Meldungsformat für die gesamte Fehlerberichterstellung. Beispielsweise wird Syslog- und lokalen Geräteberichtsmeldungen ein Schweregrad-Code sowie ein mnemonisches Zeichen zugewiesen, durch das die Quellanwendung identifiziert wird, von der die Meldung ausgegeben wurde. Hierdurch können Meldungen in Abhängigkeit von ihrer Dringlichkeit bzw. Wichtigkeit gefiltert werden. Der Versand von Protokollmeldungen an die verschiedenen Empfänger, beispielsweise den Protokollpufferspeicher, die Protokolldatei oder den Syslog-Server, wird durch die Syslog-Konfigurationsparameter gesteuert. Benutzer können bis zu acht Syslog-Server definieren.

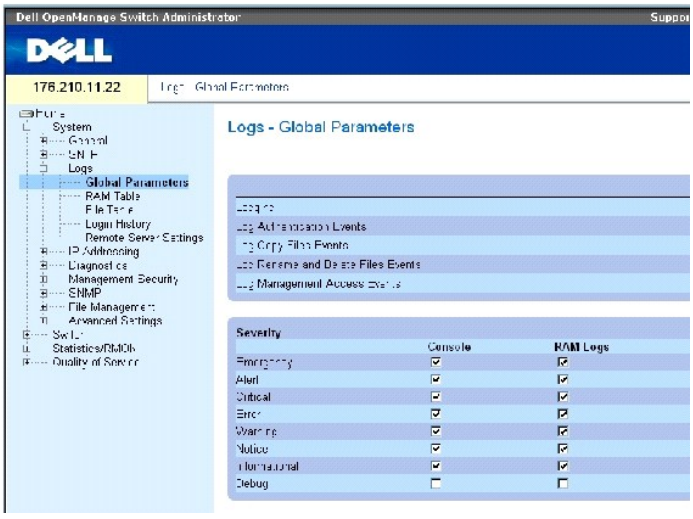
In der folgenden Tabelle sind die Schweregrade von Protokollmeldungen aufgeführt:

Tabelle 6-13. Schweregrade von Protokollmeldungen

Art des Schweregrads	Schweregrad	Beschreibung
Emergency (Notfall)	0	Das System ist nicht funktionsfähig.
Alert (Alarm)	1	Das System muss umgehend gewartet werden.
Critical (Kritisch)	2	Das System befindet sich in einem kritischen Zustand.
Error (Fehler)	3	Ein Systemfehler ist aufgetreten.
Warning (Warnung)	4	Eine Systemwarnung wurde ausgegeben.
Notice (Hinweis)	5	Das System arbeitet ordnungsgemäß, es wurde jedoch eine Systemmeldung ausgegeben.
Informational (Information)	6	Zeigt Geräteinformationen an.
Debug (Fehlerbehebung)	7	Zeigt ausführliche Informationen zum Protokoll an. Wenden Sie sich bei Auftreten eines Debug-Fehlers an den technischen Online-Support von Dell.

Die Seite Global Log Parameters (Globale Protokollparameter) enthält Felder, über die Sie festlegen können, welche Ereignisse in welchen Protokollen aufgezeichnet werden. Sie enthält Felder, mit denen Protokolle global aktiviert werden können, sowie Felder für die Definition von Protokollparametern. Die unter dem Schweregrad aufgeführten Protokollmeldungen sind vom höchsten bis zum niedrigsten Schweregrad angeordnet. Klicken Sie zum Öffnen der Seite Global Log Parameters (Globale Protokollparameter) in der Strukturansicht auf System→ Logs→ Global Parameters.

Abbildung 6-17. Global Log Parameters (Globale Protokollparameter)



Die Seite Global Log Parameters (Globale Protokollparameter) enthält folgende Parameter:

Logging (Protokolle aufzeichnen) – Ermöglicht die Erstellung globaler Geräteprotokolle in Form von Cache-, Datei- und Serverprotokollen. Konsolenprotokolle sind standardmäßig aktiviert.

Log Authentication Events (Authentifizierungsereignisse protokollieren) – Ermöglicht die Erstellung von Protokollen bei der Authentifizierung von Benutzern.

Log Copy Files Events (Dateikopiervorgänge protokollieren) – Ermöglicht die Erstellung von Protokollen beim Kopieren von Dateien.

Log Rename and Delete Files Events (Dateiumbenennungs- und -löschvorgänge protokollieren) – Ermöglicht die Erstellung von Protokollen beim Umbenennen oder Löschen von Sicherungskopien von Konfigurationsdateien.

Log Management Access Events (Verwaltungszugriffe protokollieren) – Ermöglicht die Erstellung von Protokollen, wenn ein Zugriff auf das Gerät mit Hilfe einer Verwaltungsmethode erfolgt. Beispielweise wird bei jedem Gerätezugriff über SSH ein Geräteprotokoll erstellt.

Severity (Schweregrad) – Die folgenden Schweregrade sind für Protokolle verfügbar:

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

Alert (Alarm) – Die zweithöchste Warnstufe. Ein Warnprotokoll wird bei einer schwerwiegenden Gerätefehlfunktion gespeichert, beispielsweise wenn versucht wurde, eine nicht vorhandene Konfigurationsdatei herunterzuladen.

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

Error (Fehler) – Ein Gerätefehler ist aufgetreten; beispielsweise ist ein Kopiervorgang fehlgeschlagen.

Warning (Warnung) – Die niedrigste Gerätewarnstufe. Das Gerät funktioniert zwar, doch ist beispielsweise eine Port-Verbindung derzeit nicht betriebsbereit.

Notice (Hinweis) – Zeigt wichtige Geräteinformationen an.

Informational (Information) – Zeigt Geräteinformationen an. Beispielsweise, dass an einem Port derzeit eine Verbindung besteht.

Debug (Fehlerbehebung) – Zeigt Debuggingmeldungen an.

ANMERKUNG: Bei Auswahl eines Schweregrades werden alle über dieser Auswahl befindlichen Schweregrade automatisch ebenfalls aktiviert.

Die Seite **Global Log Parameters (Globale Protokollparameter)** enthält zusätzlich Kontrollkästchen, die jeweils einem bestimmten Protokollierungssystem entsprechen:

Console (Konsole) – Der geringste Schweregrad, bei dessen Auftreten Protokolle an die Konsole gesendet werden.

RAM Logs (RAM-Protokolle) – Der geringste Schweregrad, bei dessen Auftreten Protokolle an die im RAM (Cache) enthaltene Protokolldatei gesendet werden.

Log File (Protokolldatei) – Der geringste Schweregrad, 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 in der Dropdown-Liste **Logging** (Protokolle aufzeichnen) die Option **Enable** (Aktivieren) aus.

3. Wählen Sie mit Hilfe der Kontrollkästchen auf der Seite **Global Log Parameters** den Protokolltyp und den Protokollschweregrad aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Protokolleinstellungen werden gespeichert und das Gerät aktualisiert.

Aktivieren von Protokollen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **Global Log Parameters (Globale Protokollparameter)** äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-14. CLI-Befehle für globale Protokollparameter

CLI-Befehl	Beschreibung
logging on	Aktiviert die Protokollierung von Fehlermeldungen.
logging {IP-Adresse | Hostname} [port Port] [severity Schweregrad] [facility Anlage] [description Text]	Protokolliert Meldungen auf einem Syslog-Server. Eine Liste der Schweregrade finden Sie unter **Schweregrade von Protokollmeldungen**.
logging console Schweregrad	Beschränkt die Protokollierung auf der Konsole auf Fehlermeldungen des angegebenen Schweregrads.
logging buffered Schweregrad	Beschränkt die Anzeige von Syslog-Meldungen aus einem internen Pufferspeicher (RAM) auf Meldungen des angegebenen Schweregrads.
logging file Schweregrad	Beschränkt das Senden von Syslog-Meldungen an die Protokolldatei auf Meldungen des angegebenen Schweregrads.
clear logging	Löscht den Protokollinhalt.
clear logging file	Löscht Meldungen aus der Protokolldatei.

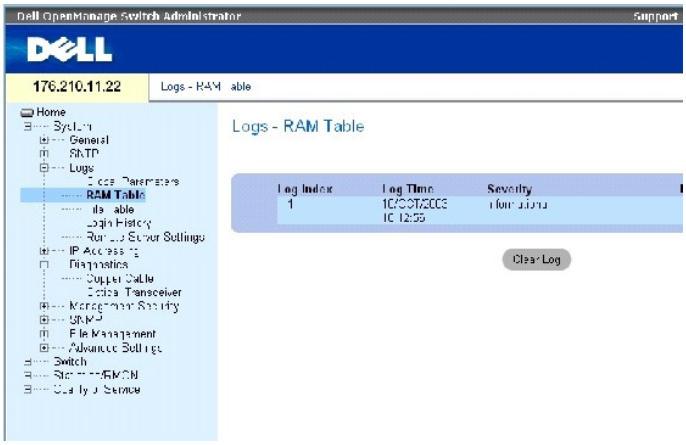
Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# logging
on

console(config)# logging
console errors

console(config)# logging
buffered debugging

console(config)# logging
file alerts

console(config)# end

console# clear logging
file

Clear Logging File [y/n]y
```

Anzeigen der Seite RAM Log Table (Tabelle der RAM-Protokolleinträge)

Die Seite **RAM Log Table (Tabelle der RAM-Protokolleinträge)** enthält Informationen zu Protokolleinträgen im RAM, einschließlich der Uhrzeit, zu der das Protokoll aufgezeichnet wurde, des Protokollschweregrads und einer Beschreibung des Protokolls. Klicken Sie zum Öffnen der Seite **RAM Log Table (Tabelle der RAM-Protokolleinträge)** in der Strukturansicht auf System→ Logs→ RAM Table.

Abbildung 6-18. RAM Log Table (Tabelle der RAM-Protokolleinträge)



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

Log Index (Protokollverzeichnis) – Die Protokollnummer in der **RAM Log Table**.

Log Time (Protokollzeit) – Gibt die Uhrzeit an, zu der das Protokoll in die **RAM Log Table** eingefügt wurde.

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

Description (Beschreibung) – Eine Beschreibung des Protokolleintrags.

Entfernen von Protokollinformationen:

1. Öffnen Sie die Seite **RAM Log Table (Tabelle der RAM-Protokolleinträge)**.
2. Klicken Sie auf Clear Log (Protokoll löschen).

Die Protokollinformationen werden aus der Seite **RAM Log Table** entfernt und das Gerät aktualisiert.

Anzeigen und Löschen der RAM Log Table mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **RAM Log Table (Tabelle der RAM-Protokolleinträge)** äquivalenten CLI-Befehle zum Anzeigen und Löschen von Feldern zusammengefasst.

Tabelle 6-15. CLI-Befehle für die RAM Log Table

CLI-Befehl	Beschreibung
show logging	Zeigt den Protokollierungsstatus und die im internen Pufferspeicher enthaltenen Syslog-Meldungen an.
clear logging	Löscht den Protokollinhalt.

Im Folgenden ein Beispiel für die CLI-Befehle:

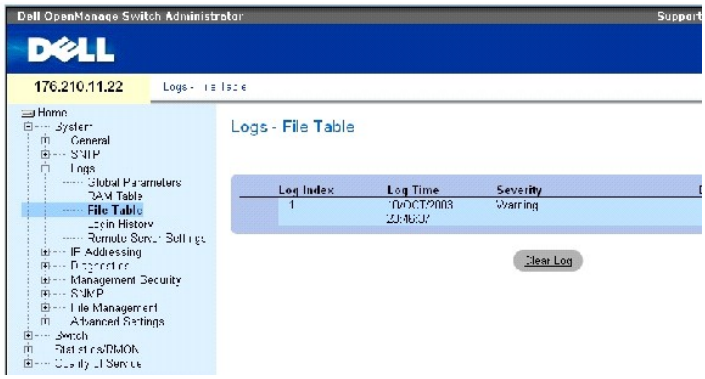
```
console# show logging
```

```
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: 1/e14



01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e13



01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e12



01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e15



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




console# clear logging



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

Anzeigen der Seite Log File Table (Tabelle der Protokolldateieinträge)

Die Seite Log File Table (Tabelle der Protokolldateieinträge) enthält Informationen zu Protokolleinträgen, die in der Protokolldatei im FLASH-Speicher abgelegt wurden, einschließlich der Uhrzeit, zu der das Protokoll aufgezeichnet wurde, des Protokollschweregrads und einer Beschreibung der Protokollmeldung. Klicken Sie zum Öffnen der Seite Log File Table (Tabelle der Protokolldateieinträge) in der Strukturansicht auf System→ Logs→ File Table.

Abbildung 6-19. Log File Table (Tabelle der Protokolldateieinträge)



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

Log Index (Protokollverzeichnis) – Die Protokollnummer in der **Log File Table**.

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) – Der Text der Protokollmeldung.

Anzeigen der Log File Table mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite Log File Table (Tabelle der Protokolldateieinträge) äquivalenten CLI-Befehle zur Anzeige und Festlegung von Feldern zusammengefasst.

Tabelle 6-16. CLI-Befehle für die 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 Meldungen aus der Protokolldatei.

Im Folgenden ein Beispiel für 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.
```

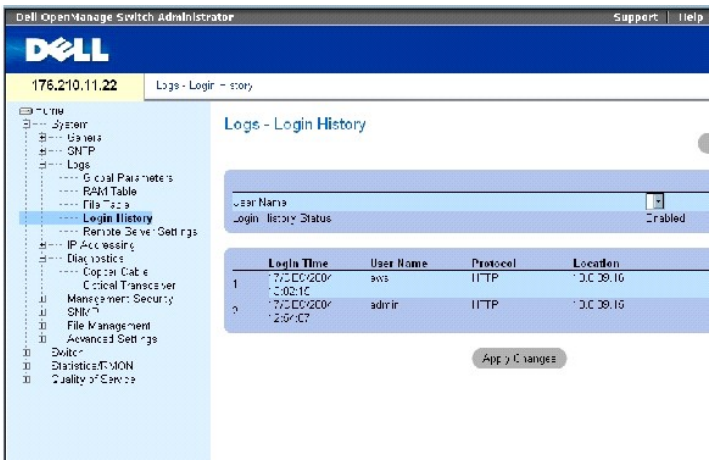
```
File Logging: Level
debug. File Messages:
11 Logged, 51
Dropped.



SysLog server
12.1.1.2 Logging:
warning. Messages: 14
Dropped.



SysLog server 1.1.1.1
Logging: info.
Messages: 0 Dropped.



01-Jan-2000
01:12:01 :%COPY-W-
TRAP: The copy
operation was
completed
successfully



01-Jan-2000
01:11:49 :%LINK-I-Up:
1/e11



01-Jan-2000
01:11:46 :%LINK-I-Up:
1/e12



01-Jan-2000
01:11:42 :%LINK-W-
Down: 1/e13



01-Jan-2000
01:11:35 :%LINK-I-Up:
1/e14
```

Anzeigen des Verlaufs von Geräteanmeldungen

Die Seite **Login History (Anmeldungsverlauf)** enthält Informationen zum Anzeigen und Überwachen der Gerätenutzung, einschließlich der Uhrzeit, zu der sich ein Benutzer angemeldet hat, und des für die Anmeldung am Gerät verwendeten Protokolls.

Klicken Sie zum Öffnen der Seite **Login History (Anmeldungsverlauf)** in der Strukturansicht auf System→ Logs→ Login History.

Abbildung 6-20. Login History (Anmeldungsverlauf)



Die Seite **Login History (Anmeldungsverlauf)** enthält folgende Felder:

User Name (Benutzername) – Enthält eine benutzerdefinierte Liste der Namen von Gerätebenutzern.

Login History Status (Status des Anmeldungsverlaufs) – Gibt an, ob Kennwort-Verlaufsprotokolle für das Gerät aktiviert sind.

Login Time (Anmeldezeit) – Gibt den Zeitpunkt an, zu dem sich der ausgewählte Benutzer bei dem Gerät angemeldet hat.

User Name (Benutzername) – Gibt den Benutzer an, der sich bei dem Gerät angemeldet hat.

Protocol (Protokoll) – Gibt an, über welches Protokoll sich der Benutzer bei dem Gerät angemeldet hat.

Location (Standort) – Gibt die IP-Adresse der Station an, von der auf das Gerät zugegriffen wurde.

Anzeigen des Anmeldungsverlaufs

1. Öffnen Sie die Seite **Login History (Anmeldungsverlauf)**.
2. Wählen Sie im Feld **User Name** (Benutzername) einen Benutzer aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Anmeldeinformationen für den ausgewählten Benutzer werden angezeigt.

Anzeigen des Verlaufs von Geräteanmeldungen mit Hilfe der CLI-Befehle

In der folgenden Tabelle wird der der Seite **Login History (Anmeldungsverlauf)** äquivalente CLI-Befehl zur Anzeige und Festlegung von Feldern zusammengefasst.

Tabelle 6-17. CLI-Befehle zum Anzeigen des Verlaufs von Geräteanmeldungen

CLI-Befehl	Beschreibung
show users login-history	Zeigt Verlaufsinformationen für die Kennwortverwaltung an.

Im Folgenden ein Beispiel für die CLI-Befehle:

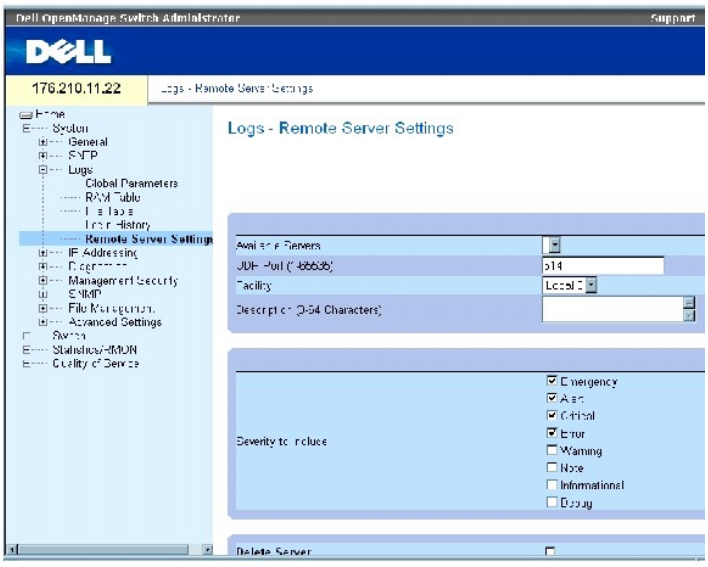
console# **show users login-history**

Login Time	Username	Protocol	Location
----------	--------	--------	----------
Jan 1. 2005 23:58:17	Anna	HTTP	172.16.1.8
Jan 1. 2005 07:59:23	Errol	HTTP	172.16.0.8
Jan 1. 2005 08:23:48	Amy	Serial	
Jan 1. 2005 08:29:29	Alan	SSH	172.16.0.8
Jan 1. 2005 08:42:31	Bob	HTTP	172.16.0.1
Jan 1. 2005 08:49:52	Cindy	Telnet	172.16.1.7

Ändern der Einstellungen von Remote-Protokollservern

Die Seite **Remote Log Server Settings (Einstellungen von Remote-Protokollservern)** enthält Felder zum Anzeigen und Konfigurieren der verfügbaren Protokollserver. Darüber hinaus können auf dieser Seite neue Protokollserver und der an die einzelnen Server gesendete Protokollschweregrad definiert werden. Klicken Sie zum Öffnen der Seite **Remote Log Server Settings (Einstellungen von Remote-Protokollservern)** in der Strukturansicht auf System→ Logs→ Remote Server Settings.

Abbildung 6-21. Remote Log Server Settings (Einstellungen von Remote-Protokollservern)



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

Available Servers (Verfügbare Server) – Enthält eine Liste der Server, an die Protokolle gesendet werden können.

UDP Port (1-65535) – Der UDP-Port, an den die Protokolle für den jeweiligen Server gesendet werden. Der zulässige Bereich liegt zwischen 1 und 65535. Der Standardwert lautet 514.

Facility (Anlage) – Legt eine benutzerdefinierte Anwendung fest, aus der Systemprotokolle an den Remote-Server gesendet werden. Jedem Server kann nur eine Anlage zugewiesen werden. Wird eine zweite Anlagenebene zugewiesen, wird die erste Anlagenebene aufgehoben. Alle für ein Gerät definierten Anwendungen verwenden dieselbe Anlage auf einem Server. Der Standardwert lautet Local 7. Die möglichen Feldwerte sind:

Local 0 - Local 7.

Description (0-64 Characters) (Beschreibung (0-64 Zeichen)) – Die benutzerdefinierte Serverbeschreibung.

Delete Server (Server löschen) – Wenn dieses Kontrollkästchen aktiviert ist, wird der aktuell ausgewählte Server aus der Liste **Available Servers** gelöscht.

Die Seite **Remote Log Server Settings (Einstellungen von Remote-Protokollservern)** enthält ebenfalls 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 (Einstellungen von Remote- Protokollservern)**.
2. Wählen Sie aus der Dropdown-Liste **Available Servers** (Verfügbare Server) einen Server aus.
3. Definieren Sie die Felder.
4. Wählen Sie mit Hilfe der Kontrollkästchen neben **Severity to Include** (Einzubeziehender Schweregrad) den Protokollschweregrad aus.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

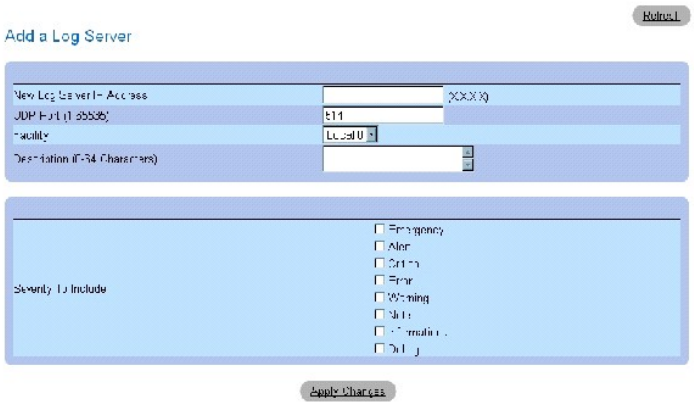
Die Protokolleinstellungen werden gespeichert und das Gerät aktualisiert.

Definieren eines neuen Servers:

1. Öffnen Sie die Seite **Remote Log Server Settings (Einstellungen von Remote- Protokollservern)**.
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite **Add a Log Server (Protokollserver hinzufügen)** wird geöffnet:

Abbildung 6-22. Add a Log Server (Protokollserver hinzufügen)



Die Seite **Add a Log Server (Protokollserver hinzufügen)** enthält ein zusätzliches Feld:

New Log Server IP Address (IP-Adresse des neuen Protokollservers) – Legt die IP-Adresse des neuen Protokollservers fest.

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

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

Anzeigen der Seite Log Server Table (Tabelle der Protokollserver):

1. Öffnen Sie die Seite **Remote Log Server Settings (Einstellungen von Remote- Protokollservern)**.
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die Seite **Log Server Table (Tabelle der Protokollserver)** wird geöffnet:

Abbildung 6-23. Log Server Table (Tabelle der Protokollserver)

Entfernen eines Protokollservers aus der Seite Log Server Table (Tabelle der Protokollserver):

1. Öffnen Sie die Seite **Remote Log Server Settings (Einstellungen von Remote- Protokollservern)**.
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die Seite **Log Server Table (Tabelle der Protokollserver)** wird geöffnet.

3. Wählen Sie einen Eintrag in der **Log Server Table (Tabelle der Protokollserver)** aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen), um den bzw. die Server zu entfernen.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag wird aus der Tabelle **Log Server Table (Tabelle der Protokollserver)** entfernt und das Gerät aktualisiert.

Festlegen von Einstellungen für Remote-Protokollserver mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die äquivalenten CLI-Befehle zur Protokollierung von Meldungen auf Remote-Servern zusammengefasst.

Tabelle 6-18. CLI-Befehle für Remote-Protokollserver

CLI-Befehl	Beschreibung
logging *{IP-Adresse* **|** *Hostname}* [**port** *Port*] [**severity** *Schweregrad*] [**facility** *Anlage*] [**description** *Text*]	Protokolliert Meldungen auf einem Remote-Server.
no logging	Löscht einen Syslog-Server.
show logging	Zeigt den Protokollierungsstatus und die Syslog-Meldungen an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console> enable

console# configure

console(config) # logging
10.1.1.1 severity critical

console(config)# end

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: 1/e11

03-Mar-2004 12:02:01 :%
LINK-W-Down: 1/e12

03-Mar-2004 12:02:01 :%
```

```
LINK-I-Up: 1/e13
```

Festlegen von IP-Adressen

Die Seite IP Addressing (IP-Adressierung) enthält Links, über die Schnittstellen- und Standardgateway-IP-Adressen zugewiesen sowie ARP- und DHCP-Parameter für die Schnittstellen definiert werden können. Klicken Sie zum Öffnen der Seite IP Addressing (IP-Adressierung) in der Strukturansicht auf System→ IP Addressing.

Definieren von Standard-Gateways

Die Seite **Default Gateway (Standard-Gateway)** enthält Felder zum Zuweisen eines Gateways zu Geräten. Beim Senden von Paketen an ein Remote-Netzwerk werden diese an die IP-Standardadresse weitergeleitet. Die konfigurierte IP-Adresse muss dem IP-Adressen-Subnetz einer der IP-Schnittstellen angehören. Klicken Sie zum Öffnen der Seite **Default Gateway (Standard-Gateway)** in der Strukturansicht auf System→ IP Addressing→ Default Gateway.

Die Seite **Default Gateway (Standard-Gateway)** enthält folgende Felder:

User Defined (Benutzerdefiniert) – Die Gateway-IP-Adresse des Gerätes.

Active (Aktiv) – Gibt an, ob das Gateway aktiv ist.

Remove User Defined (Benutzerdefiniertes Gateway entfernen) – Wenn diese Option aktiviert ist, wird das Gateway des Gerätes aus der Dropdown-Liste **Default Gateway** (Standard-Gateway) entfernt.

Auswählen eines Gateways für ein Gerät:

1. Öffnen Sie die Seite **Default Gateway (Standard-Gateway)**.
2. Wählen Sie in der Dropdown-Liste **Default Gateway** (Standard-Gateway) eine IP-Adresse aus.
3. Aktivieren Sie das Kontrollkästchen Active (Aktiv).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das Standard-Gateway des Gerätes wird ausgewählt und das Gerät aktualisiert.

Entfernen des Standard-Gateways eines Gerätes:

1. Öffnen Sie die Seite **Default Gateway (Standard-Gateway)**.
2. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen), um Standard-Gateways zu entfernen.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag des Standard-Gateways wird entfernt und das Gerät aktualisiert.

Definieren des Gateways für ein Gerät mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **Default Gateway (Standard-Gateway)** äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

.

Tabelle 6-19. CLI-Befehle für Standard-Gateways

CLI-Befehl	Beschreibung
ip default-gateway IP-Adresse	Definiert ein Standard-Gateway.
no ip default-gateway	Entfernt ein Standard-Gateway.

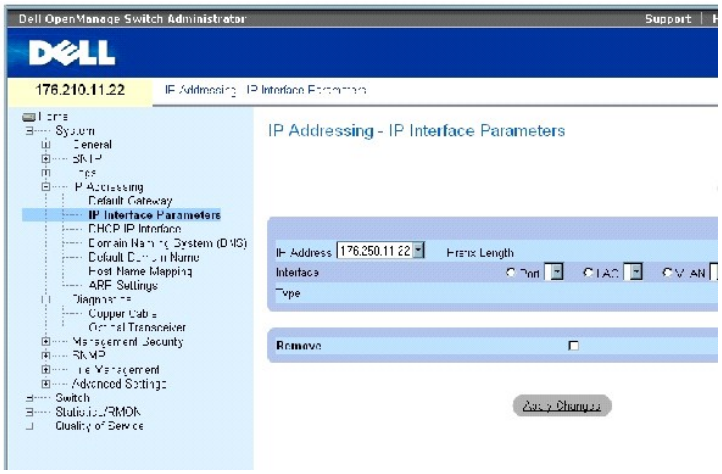
Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# ip
default-gateway
196.210.10.1



console(config)# no ip
default-gateway
```

Definieren von IP-Schnittstellen

Die Seite IP Interfaces Parameters (IP-Schnittstellenparameter) enthält Felder zum Zuweisen von IP-Parametern zu Schnittstellen. Klicken Sie zum Öffnen der Seite IP Interfaces Parameters (IP-Schnittstellenparameter) in der Strukturansicht auf **System→ IP Addressing→ IP Interface Parameters**.

Abbildung 6-24. IP Interfaces Parameters (IP-Schnittstellenparameter)



Die Seite IP Interfaces Parameters (IP-Schnittstellenparameter) enthält folgende Felder:

IP Address – Die IP-Adresse der Schnittstelle.

Prefix Length (Präfixlänge) – Die Anzahl der Bits, aus denen das Präfix der IP-Quelladresse oder der Netzwerkmaske der IP-Quelladresse besteht.

Source Interface (Quellenschnittstelle) – Der Schnittstellentyp, für den die IP-Adresse definiert ist. Wählen Sie **Port**, **LAG** oder **VLAN** aus.

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

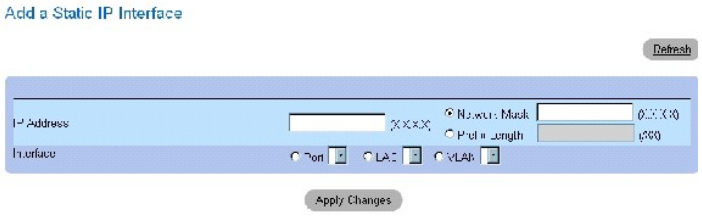
Remove (Entfernen) – Wenn dieses Kontrollkästchen aktiviert ist, wird die Schnittstelle aus dem Dropdown-Menü **IP Address** entfernt.

Hinzufügen einer IP-Schnittstelle

1. Öffnen Sie die Seite IP Interfaces Parameters (IP-Schnittstellenparameter).
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite Add a Static IP Interface (Statische IP-Adresse hinzufügen) wird geöffnet:

Abbildung 6-25. Add a Static IP Interface (Statische IP-Adresse hinzufügen)



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

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

Die neue IP-Adresse wird zur Schnittstelle hinzugefügt und das Gerät aktualisiert.

Ändern von IP-Adressparametern

1. Öffnen Sie die Seite IP Interfaces Parameters (IP-Schnittstellenparameter).
2. Wählen Sie im Dropdown-Menü **IP Address** eine IP-Adresse aus.
3. Ändern Sie den Schnittstellentyp.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

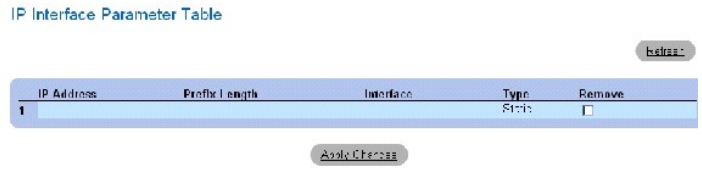
Die Parameter werden geändert und das Gerät aktualisiert.

Löschen von IP-Adressen

1. Öffnen Sie die Seite IP Interfaces Parameters (IP-Schnittstellenparameter).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die Seite **IP Interface Parameter Table (Tabelle der IP-Schnittstellenparameter)** wird geöffnet:

Abbildung 6-26. IP Interface Parameter Table (Tabelle der IP-Schnittstellenparameter)



3. Wählen Sie eine IP-Adresse aus und aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die ausgewählte IP-Adresse wird gelöscht und das Gerät aktualisiert.

Definieren von IP-Schnittstellen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite IP Interfaces Parameters (IP-Schnittstellenparameter) äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-20. CLI-Befehle für IP-Schnittstellenparameter

CLI-Befehl	Beschreibung
ip address IP-Adresse {Maske | Präfixlänge}	Legt eine IP-Adresse fest.
no ip address [IP-Adresse]	Entfernt eine IP-Adresse.
show ip interface [ethernet Schnittstellennummer | vlan VLAN-ID | port-channel Nummer]	Zeigt den Verwendungsstatus der für IP konfigurierten Schnittstellen an.

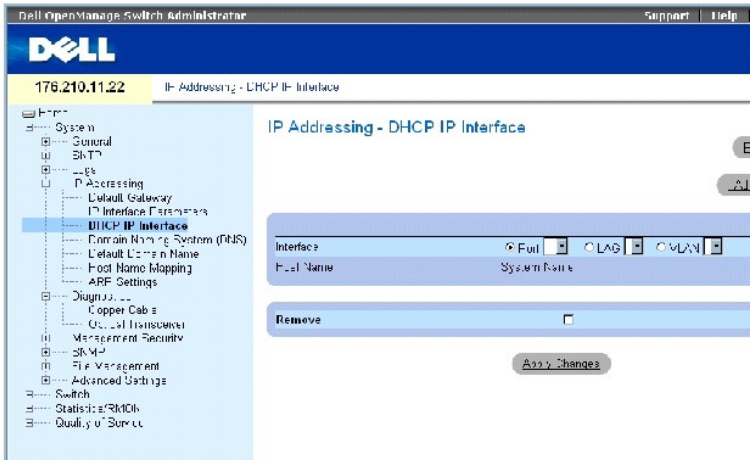
Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# interface
vlan 1

console(config-if)# ip
address 92.168.1.123
255.255.255.0

console(config-if)# no ip
address 92.168.1.123

console(config-if)# end

console# show ip interface
vlan 1

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

Die Seite **DHCP IP Interface (DHCP IP-Schnittstelle)** enthält Parameter zum Definieren von DHCP-Clients, die mit dem Gerät verbunden sind. Klicken Sie zum Öffnen der Seite **DHCP IP Interface (DHCP IP-Schnittstelle) in der Strukturansicht** auf **System→ IP Addressing→ DHCP IP Interface**.

Abbildung 6-27. DHCP IP Interface (DHCP IP-Schnittstelle)



Die Seite **DHCP IP Interface (DHCP IP-Schnittstelle)** enthält folgende Felder:

Interface (Schnittstelle) – Die Schnittstelle, die an das Gerät angeschlossen ist. Klicken Sie auf das Optionsfeld neben **Port**, **LAG** oder **VLAN** und wählen Sie die an das Gerät angeschlossene Schnittstelle aus.

Host Name – Der Hostname.

Remove (Entfernen) – Wenn dieses Kontrollkästchen aktiviert ist, werden DHCP-Clients entfernt.

Hinzufügen von DHCP-Clients

1. Öffnen Sie die Seite DHCP IP Interface (DHCP IP-Schnittstelle).
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add DHCP IP Interface (DHCP IP-Schnittstelle hinzufügen)** wird geöffnet.
3. Füllen Sie die Felder auf der Seite aus.
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 gewünschten Felder.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Eintrag wird geändert und das Gerät aktualisiert.

Löschen einer DHCP IP-Schnittstelle

1. Öffnen Sie die Seite DHCP IP Interface (DHCP IP-Schnittstelle).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **DHCP Client Table (Tabelle der DHCP-Clients)** wird geöffnet.
3. Wählen Sie einen DHCP-Clienteintrag aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der ausgewählte Eintrag wird gelöscht und das Gerät aktualisiert.

Definieren von DHCP IP-Schnittstellen mit Hilfe der CLI-Befehle

In der folgenden Tabelle wird der äquivalente CLI-Befehl zum Definieren von DHCP-Clients zusammengefasst.

Tabelle 6-21. CLI-Befehl für die DHCP IP-Schnittstelle

CLI-Befehl	Beschreibung
ip address dhcp [**hostname** *Hostname*]	Dient zum Bezug einer IP-Adresse an einer Ethernet-Schnittstelle über das Dynamic Host Configuration Protocol (DHCP, Dynamisches Hostkonfigurationsprotokoll).

Im Folgenden ein Beispiel für den CLI-Befehl:

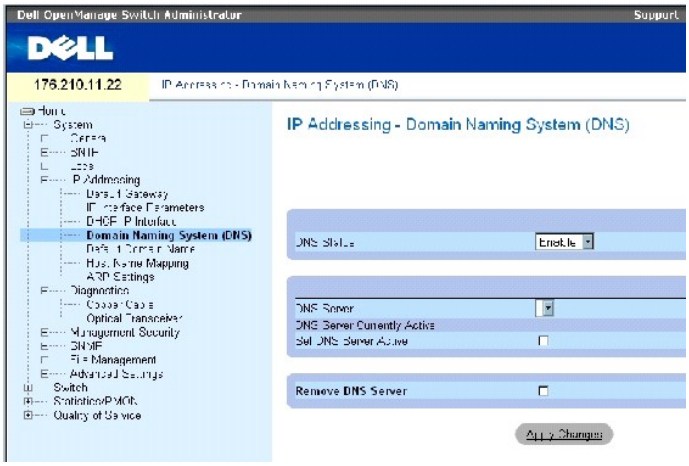
```
console(config)# interface
ethernet 1/e11

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

Konfigurieren von Domänennamensystemen

Das Domänennamensystem (Domain Name System, DNS) wandelt benutzerdefinierte Domänennamen in IP-Adressen um. Bei jeder Zuweisung eines Domänennamens übersetzt der DNS-Dienst den Namen in eine numerische IP-Adresse. Beispielsweise wird der Name www.ipbeispiel.com in die Adresse 192.87.56.2 übersetzt. DNS-Server verfügen über Datenbanken mit Domänennamen und den entsprechenden IP-Adressen.

Die Seite **Domain Naming System (DNS) (Domänennamensystem (DNS))** enthält Felder zum Aktivieren des DNS-Dienstes und Aktivieren bestimmter DNS-Server. Klicken Sie zum Öffnen der Seite **Domain Naming System (DNS) (Domänennamensystem (DNS))** in der Strukturansicht auf **System→ IP Addressing→ Domain Naming System (DNS)**.

Abbildung 6-28. Domain Naming System (DNS) (Domänennamensystem (DNS))



Die Seite **Domain Naming System (DNS) (Domänennamensystem (DNS))** enthält folgende Felder:

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

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

DNS Server Currently Active (Gegenwärtig aktiver DNS-Server) – Der derzeit aktive DNS-Server.

Set DNS Server Active (DNS-Server aktivieren) – Aktiviert den ausgewählten DNS-Server.

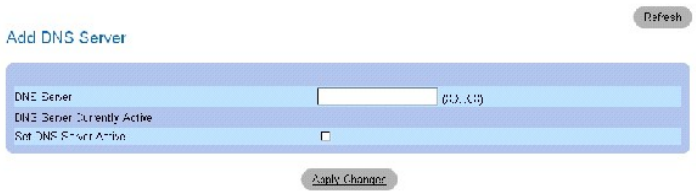
Remove DNS Server (DNS-Server entfernen) – Wenn dieses Kontrollkästchen aktiviert ist, wird der ausgewählte DNS-Server entfernt.

Hinzufügen eines DNS-Servers

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

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

Abbildung 6-29. Add DNS Server (DNS-Server hinzufügen)



DNS Server – Die IP-Adresse des DNS-Servers.

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

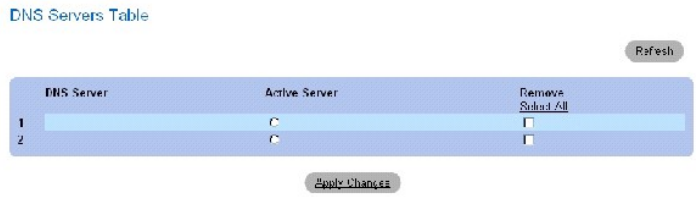
Der neue DNS-Server wird definiert und das Gerät aktualisiert.

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

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

Die Seite **DNS Servers Table (Tabelle der DNS-Server)** wird geöffnet:

Abbildung 6-30. DNS Servers Table (Tabelle der DNS-Server)



Entfernen von DNS-Servern

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

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

3. Wählen Sie einen Eintrag in der **DNS Servers Table** aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

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

Konfigurieren von DNS-Servern mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die CLI-Befehle zum Konfigurieren von DNS-Servern zusammengefasst.

Tabelle 6-22. CLI-Befehle für DNS-Server

CLI-Befehl	Beschreibung
ip name-server *Serveradresse*	Legt die verfügbaren DNS-Namenserver fest. Bis zu acht Namenserver können festgelegt werden.
no ip name-server *Serveradresse*	Entfernt einen Namenserver.
ip domain-name *Name*	Definiert einen Standard-Domänennamen, der von der Software zum Vervollständigen unvollständiger Hostnamen verwendet wird.
clear host {Name | *}	Löscht Einträge aus dem Cache, in dem die Zuordnung von Hostnamen zu Adressen gespeichert ist.
show hosts [*Name*]	Zeigt den Standard-Domänennamen, eine Liste von Namenserver-Hosts, die statische sowie die im Cache gespeicherte Liste der Hostnamen und Adressen an.
ip domain-lookup	Aktiviert die Übersetzung von Hostnamen in IP-Adressen durch das DNS-System.

Im Folgenden ein Beispiel für die CLI-Befehle:

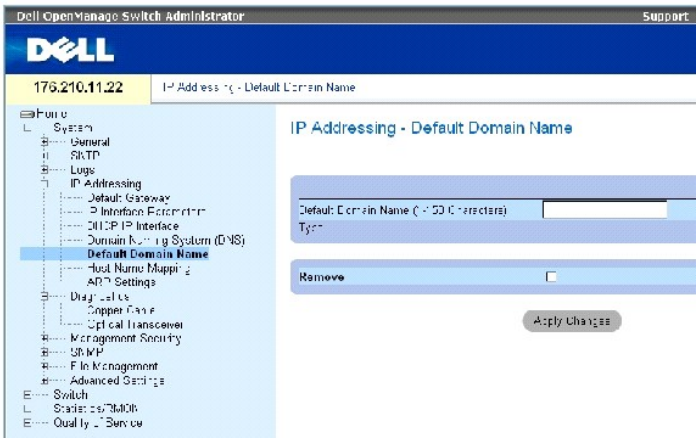
```
console(config)# ip name-
```

```
server 176.16.1.18
```

Definieren von Standarddomänen

Die Seite **Default Domain Name (Standard-Domänenname)** enthält Felder zum Definieren von Standard-DNS-Domänennamen. Klicken Sie zum Öffnen der Seite **Default Domain Name (Standard-Domänenname)** in der Strukturansicht auf **System→ IP Addressing→ Default Domain Name**.

Abbildung 6-31. Default Domain Name (Standard-Domänenname)



Die Seite **Default Domain Name (Standard-Domänenname)** enthält folgende Felder:

Default Domain Name (1-158 characters) (Standard-Domänenname (1-158 Zeichen)) – Enthält einen benutzerdefinierten Standard-Domänennamen. Wenn ein Standard-Domänenname festgelegt ist, wird dieser für alle unvollständigen Hostnamen übernommen.

Type – Der IP-Adresstyp. Die möglichen Feldwerte lauten:

Dynamic (Dynamisch) – Die IP-Adresse wird dynamisch erstellt.

Static (Statisch) – Die IP-Adresse ist eine statische IP-Adresse.

Remove (Entfernen) – Wenn dieses Kontrollkästchen aktiviert ist, wird der Standard-Domänenname entfernt.

Definieren von DNS-Domänennamen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die CLI-Befehle zum Konfigurieren von DNS-Domänennamen zusammengefasst:

Tabelle 6-23. CLI-Befehle für DNS-Domänennamen

CLI-Befehl	Beschreibung
ip domain-name *Name*	Definiert einen Standard-Domänennamen, der von der Software zum Vervollständigen unvollständiger Hostnamen verwendet wird.
no ip domain-name	Deaktiviert die Verwendung des Domänennamensystems (DNS).
show hosts [*Name***]**	Zeigt den Standard-Domänennamen, eine Liste von Namenserver-Hosts, die statische sowie die im Cache gespeicherte Liste der Hostnamen und Adressen an.

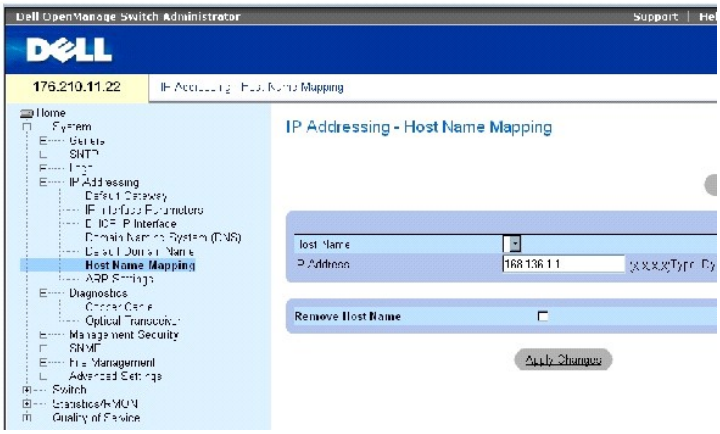
Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# ip
domain-name dell.com
```

Zuweisen des Domänen-Hosts

Die Seite Host Name Mapping (Zuweisung von Hostnamen) enthält Parameter für die Zuweisung von IP-Adressen zu statischen Hostnamen. Auf dieser Seite kann pro Host eine IP-Adresse zugewiesen werden. Klicken Sie zum Öffnen der Seite **Host Name Mapping** in der Strukturansicht *auf* **System→ IP Addressing→ Host Name Mapping.**

Abbildung 6-32. Host Name Mapping (Zuweisung von Hostnamen)



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

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

IP Address (X.X.X.X) – Enthält die IP-Adresse, die dem betreffenden Hostnamen zugewiesen ist.

Type – Der IP-Adresstyp. Die möglichen Feldwerte lauten:

Dynamic (Dynamisch) – Die IP-Adresse wird dynamisch erstellt.

Static (Statisch) – Die IP-Adresse ist eine statische IP-Adresse.

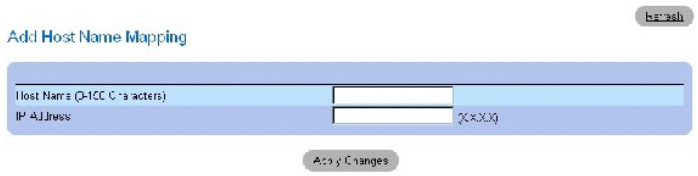
Remove Host Name (Hostname entfernen) – Wenn dieses Kontrollkästchen aktiviert ist, wird die DNS-Host-Zuweisung entfernt.

Hinzufügen von Host-Domänennamen

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

Die Seite **Add Host Name Mapping (Hostnamen-Zuweisung hinzufügen)** wird geöffnet:

Abbildung 6-33. Add Host Name Mapping (Hostnamen-Zuweisung hinzufügen)



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

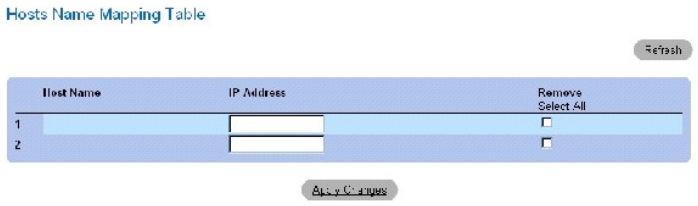
Die IP-Adresse wird dem Hostnamen zugeordnet und das Gerät aktualisiert.

Anzeigen der Seite Hosts Name Mapping Table (Zuweisungstabelle für Hostnamen)

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

Die Seite **Hosts Name Mapping Table (Zuweisungstabelle für Hostnamen)** wird geöffnet:

Abbildung 6-34. Hosts Name Mapping Table (Zuweisungstabelle für Hostnamen)



Entfernen der Zuweisung eines Hostnamens zu einer IP-Adresse

1. Öffnen Sie die Seite Host Name Mapping (Zuweisung von Hostnamen).
2. Klicken Sie auf **Show All** (Alle anzeigen).
3. Die Seite **Hosts Name Mapping Table (Zuweisungstabelle für Hostnamen)** wird geöffnet.
4. **Wählen Sie in der Seite Hosts Name Mapping Table einen Eintrag aus.**
5. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag wird aus der Seite **Hosts Name Mapping Table (Zuweisungstabelle für Hostnamen)** gelöscht und das Gerät aktualisiert.

Zuweisen von IP-Adressen zu Domänen-Hostnamen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die äquivalenten CLI-Befehle zur Zuweisung von Domänen-Hostnamen zu IP-Adressen zusammengefasst.

Tabelle 6-24. CLI-Befehle für Domänen-Hostnamen

CLI-Befehl	Beschreibung
ip host *Name*	Definiert die statische Zuweisung eines Hostnamens zu einer Adresse im Cache des Hosts.

Adresse	
no ip host Name	Entfernt die Zuweisung eines Namens zu einer Adresse.
clear host {Name | *}	Löscht Einträge aus dem Cache, in dem die Zuordnung von Hostnamen zu Adressen gespeichert ist.
show hosts [Name]	Zeigt den Standard-Domänennamen, eine Liste von Namenserver-Hosts, die statische sowie die im Cache gespeicherte Liste der Hostnamen und Adressen an.

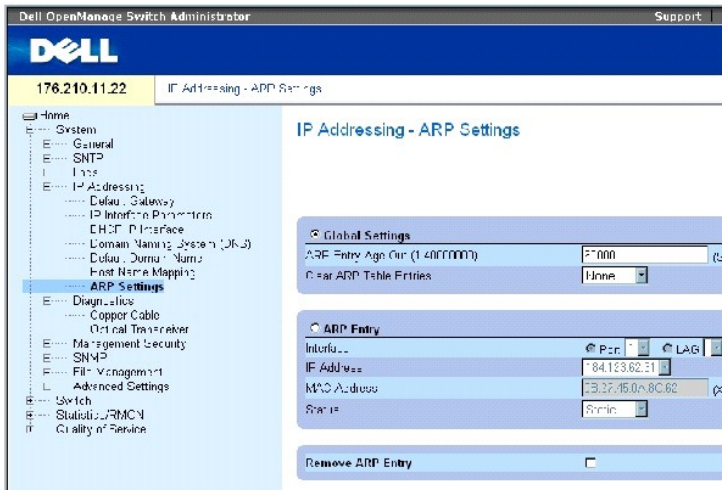
Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# ip host
accounting.abc.com
176.10.23.1
```

Definieren von ARP-Einstellungen

Das Address Resolution Protocol (ARP) wandelt IP-Adressen in physische Adressen um und ordnet der IP-Adresse eine MAC-Adresse zu. ARP ermöglicht nur dann die Kommunikation zwischen einem Host und anderen Hosts, wenn die IP-Adresse der benachbarten Hosts bekannt ist. Klicken Sie zum Öffnen der Seite **ARP Settings (ARP-Einstellungen)** **in** der Strukturansicht auf System→ IP Addressing→ ARP.

Abbildung 6-35. ARP Settings (ARP-Einstellungen)



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

Global Settings (Globale Einstellungen) – Wählen Sie diese Option aus, um die Felder für globale ARP-Einstellungen zu aktivieren.

ARP Entry Age Out (1-40000000) (Alterungszeit von ARP-Einträgen) – Gibt für alle Geräte an, wie viel Zeit (in Sekunden) zwischen zwei ARP-Anfragen zu einem Eintrag in der ARP-Tabelle vergeht. Nach diesem Zeitraum wird der Eintrag aus der Tabelle gelöscht. Bereich: 1 - 40000000. Der Standardwert lautet 60000 Sekunden.

Clear ARP Table Entries (ARP-Tabelleneinträge löschen) – Die Art der auf allen Geräten zu löschenden ARP-Einträge. Die möglichen Werte lauten:

None (Keine) – Es werden keine ARP-Einträge gelöscht.

All (Alle) – Es werden alle ARP-Einträge gelöscht.

Dynamic (Dynamisch) – Es werden lediglich dynamische ARP-Einträge gelöscht.

Static (Statisch) – Es werden lediglich statische ARP-Einträge gelöscht.

ARP Entry (ARP-Eintrag) – Wählen Sie diese Option aus, um die Felder für ARP-Einstellungen eines einzelnen Ethernet-Gerätes zu aktivieren.

Interface (Schnittstelle) – Die Schnittstellenummer des an das Gerät angeschlossenen Ports, LAGs oder VLANs.

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

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

Status – Der Status des ARP-Tabelleneintrags. Die möglichen Feldwerte lauten:

Dynamic – Der ARP-Eintrag wird dynamisch ermittelt.

Static – Bei dem ARP-Eintrag handelt es sich um einen statischen Eintrag.

Remove ARP Entry (ARP-Eintrag entfernen) – Wenn dieses Kontrollkästchen aktiviert ist, wird der betreffende ARP-Eintrag entfernt.

Hinzufügen eines statischen ARP-Eintrags zur 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.
3. Wählen Sie eine Schnittstelle aus.
4. Definieren Sie die Felder.
5. Klicken Sie auf Apply Changes (Änderungen übernehmen).

   Der Eintrag wird zur Seite **ARP Table (ARP-Tabelle)** hinzugefügt und das Gerät aktualisiert.

Anzeigen der Seite ARP Table (ARP-Tabelle)

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

   Die Seite **ARP Table (ARP-Tabelle)** wird geöffnet.

Löschen eines Eintrags aus der Seite ARP Table (ARP-Tabelle)

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

   Die Seite **ARP Table (ARP-Tabelle)** wird geöffnet.
3. Wählen Sie einen Tabelleneintrag aus.

4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf Apply Changes (Änderungen übernehmen).

Der in der **ARP Table** ausgewählte Eintrag wird gelöscht und das Gerät aktualisiert.

Konfigurieren von ARP-Einstellungen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **ARP Settings (ARP-Einstellungen)** äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-25. CLI-Befehle für ARP-Einstellungen

CLI-Befehl	Beschreibung
arp IP-Adr. HW-Adr. {ethernet Schnittstellennummer | vlan VLAN-ID | port-channel Nummer}	Fügt einen permanenten Eintrag zum ARP-Cache hinzu.
arp timeout Sekunden	Legt fest, wie lange ein Eintrag im ARP-Cache verbleibt.
clear arp-cache	Löscht alle dynamischen Einträge im ARP-Cache.
show arp	Zeigt die Einträge der ARP-Tabelle an.
no arp	Entfernt einen ARP-Eintrag aus der ARP-Tabelle.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# arp 198.133.219.232 00-00-0c-40-0f-bc

console(config)# arp timeout 12000

console(config)# exit

console# show arp

ARP timeout: 12000 Seconds
```

Interface	IP address	HW address	Status
---------	----------	----------	------
1/e11	10.7.1.102	00:10:B5:04:DB:4B	Dynamic
1/e12	10.7.1.135	00:50:22:00:2A:A4	Static

Ausführen der Kabeldiagnose

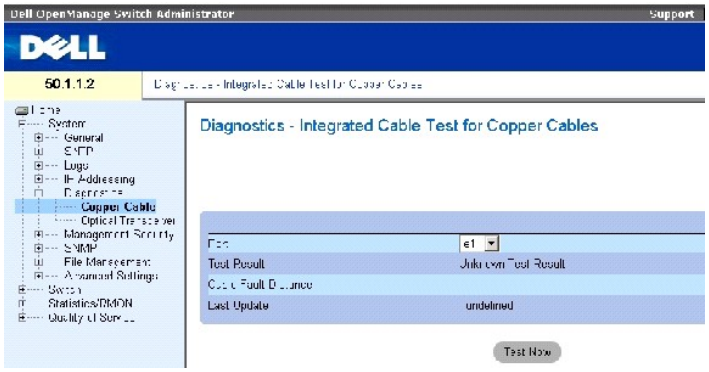
Die Seite **Diagnostics (Diagnose)** enthält Links zu Seiten, auf denen Kupferkabel virtuell geprüft werden können. Klicken Sie zum Öffnen der Seite **Diagnostics** in der Strukturansicht auf **System→ Diagnostics**.

Anzeigen der Kupferkabel-Diagnose

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

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

Abbildung 6-36. Integrated Cable Test for Copper Cables (Integrierter Kabeltest für Kupferkabel)



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

Port – Der Port, an den das Kabel angeschlossen ist.

Test Result (Testergebnis) – Die Ergebnisse der Kabelprüfung. Die möglichen Feldwerte lauten:

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

Open Cable (Offenes Kabel) – Das Kabel ist nur auf einer Seite angeschlossen.

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

OK – Die Kabelprüfung wurde erfolgreich abgeschlossen.

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

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

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

Durchführen einer Kabelprüfung

1. Stellen Sie sicher, dass beide Enden des Kupferkabels an ein Gerät angeschlossen sind.
2. Öffnen Sie die Seite **Integrated Cable Test for Copper Cables (Integrierter Kabeltest für Kupferkabel)**.
3. Wählen Sie die zu prüfende Schnittstelle aus.
4. Klicken Sie auf **Test Now** (Jetzt prüfen).

Das Kupferkabel wird geprüft und die Ergebnisse werden auf der Seite **Integrated Cable Test for Copper Cables (Integrierter Kabeltest für Kupferkabel)** angezeigt.

Anzeigen der Ergebnistabelle für die virtuelle Kabelprüfung

1. Öffnen Sie die Seite **Integrated Cable Test for Copper Cables (Integrierter Kabeltest für Kupferkabel)**.
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die Seite **Integrated Cable Test Results Table (Ergebnistabelle für integrierte Kabelprüfung)** wird geöffnet.

ANMERKUNG: In diesem Bildschirm werden lediglich die Ergebnisse von bereits durchgeführten Tests angezeigt; -es findet keine aktuelle Prüfung aller Ports statt.

Zusätzlich zu den Feldern auf der Seite **Integrated Cable Test for Copper Cables (Integrierter Kabeltest für Kupferkabel)** enthält die Seite **Integrated Cable Test Results Table** folgendes Feld:

Unit No. (Einheit-Nr.) – Die Nummer der Einheit, an die das angezeigte Kabel angeschlossen ist.

Prüfen von Kupferkabeln mit Hilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für die Prüfung von Kupferkabeln.

Tabelle 6-26. CLI-Befehle für die Prüfung von Kupferkabeln

CLI-Befehl	Beschreibung
test copper-port tdr *Schnittstelle*	Führt eine virtuelle Kabelprüfung durch.
show copper-port tdr *Schnittstelle*	Zeigt die Ergebnisse der zuletzt an Ports durchgeführten virtuellen Kabelprüfungen an.
show copper-port cable-length *Schnittstelle*	Zeigt die geschätzte Länge des an einen Port angeschlossenen Kupferkabels an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console> enable

Console# test copper-port tdr 1/e3

Cable is open at 100 meters.

Console# show copper-port cable-length

Port    Length (meters)
----    ---------------
```

1/e3	110-140
1/e4	Fiber

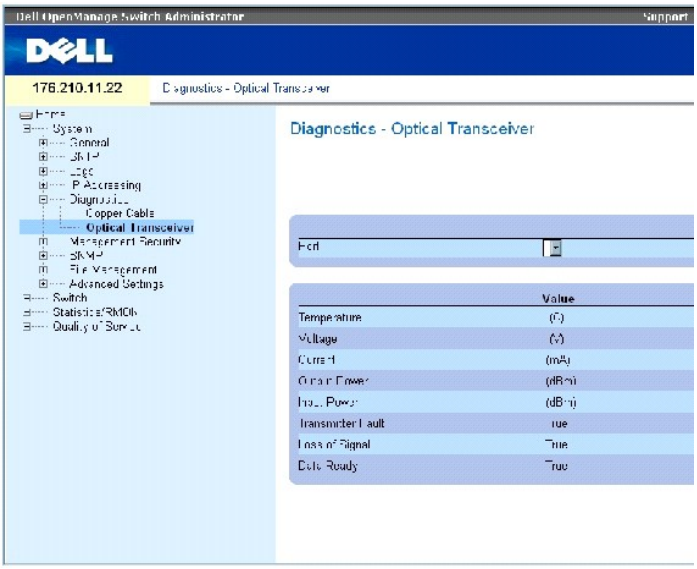
ANMERKUNG: Die durch den integrierten Kabelprüfer (Integrated Cable Tester, ICT) ermittelte Kabellänge ist ein ungefährer Wert, der einem der folgenden Bereiche zugeordnet wird: bis 50 Meter, 50 - 80 m, 80 - 110 m, 110 - 120 m oder mehr als 120 m. Die Abweichung kann bis zu 20 Meter betragen; bei 10- Mbit/s-Verbindungen kann keine Messung der Kabellänge durchgeführt werden.

Anzeigen der Diagnose für optische Transceiver

Über die Seite Optical Transceiver (Optischer Transceiver) können Sie Prüfungen an Glasfaserkabeln vornehmen. Klicken Sie zum Öffnen der Seite Optical Transceiver (Optischer Transceiver) in der Strukturansicht auf **System→ Diagnostics→ Optical Transceiver**.

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

Abbildung 6-37. Optical Transceiver (Optischer Transceiver)



Die Seite Optical Transceiver (Optischer Transceiver) enthält folgende Felder:

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

Temperature – Die Betriebstemperatur (°C) des Kabels.

Voltage (Spannung) – Die Betriebsspannung des Kabels.

Current (Strom) – Der Betriebsstrom des Kabels.

Output Power (Ausgangsleistung) – Der Übertragungspegel der Ausgangsleistung.

Input Power (Eingangsleistung) – Der Übertragungspegel der Eingangsleistung.

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

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

Data Ready (Daten bereit) – Der Transceiver ist betriebsbereit und es stehen Daten bereit.

Anzeigen der Ergebnistabelle für die Prüfung optischer Transceiver

1. Öffnen Sie die Seite Optical Transceiver (Optischer Transceiver).
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Prüfung wird durchgeführt und die Seite **Optical Transceiver Diagnostics Table** (Ergebnistabelle für die Prüfung optischer Transceiver) wird geöffnet.

Zusätzlich zu den Feldern auf der Seite **Optical Transceiver (Optischer Transceiver)** enthält die Seite **Optical Transceiver Diagnostics Table** folgendes Feld:

Unit No. (Einheit-Nr.) – Die Nummer der Einheit, an die das angezeigte Kabel angeschlossen ist.

- **N/A** – Not Available (Keine Angabe), N/S – Not Supported (Nicht unterstützt), W – Warning (Warnung), E – Error (Fehler).

ANMERKUNG: Finisar-Transceiver unterstützen den Senderfehler-Diagnosetest nicht.

ANMERKUNG: Eine Analyse von Glasfaserkabeln kann nur bei SFPs durchgeführt werden, die den Standard SFF--872 für digitale Diagnosen unterstützen.

Prüfen von Glasfaserkabeln mit Hilfe der CLI-Befehle

Die folgende Tabelle enthält den CLI-Befehl für die Prüfung von Glasfaserkabeln.

Tabelle 6-27. CLI-Befehl für die Prüfung von Glasfaserkabeln

CLI-Befehl	Beschreibung
show fiber-ports optical- transceiver [*Schnittstelle*] [*detailed*]	Zeigt die Diagnose für optische Transceiver an.

Im Folgenden ein Beispiel für den CLI-Befehl:

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

Port	Temp [C]	Voltage	Current [Volt]	Output [mA]	Input [mWatt]	POWER TX [mWatt]	LOS Fault
----	----	------	-----	------	------	------	-----
1/e1	48	5.15	50	1.789	1.789	No	No
1/e2	43	5.15	10	1.789	1.789	No	No

Verwalten der Switch-Sicherheit

Die Seite **Management Security (Verwalten der Gerätesicherheit)** bietet Zugriff auf Sicherheitsseiten, die Felder zur Festlegung von Sicherheitsparametern für Ports, Geräteverwaltungsmethoden sowie die Benutzer- und Serversicherheit enthalten. Klicken Sie zum Öffnen der Seite **Management Security** in der Strukturansicht auf System→ Management Security.

Definieren von Zugriffsprofilen

Die Seite **Access Profiles (Zugriffsprofile)** enthält Felder für die Festlegung von Profilen und Regeln für den Gerätezugriff. Der Zugriff auf Verwaltungsfunktionen kann auf bestimmte Benutzergruppen beschränkt werden, die durch Ingress-Schnittstellen und die IP-Quelladresse oder IP-Quellsubnetze definiert werden.

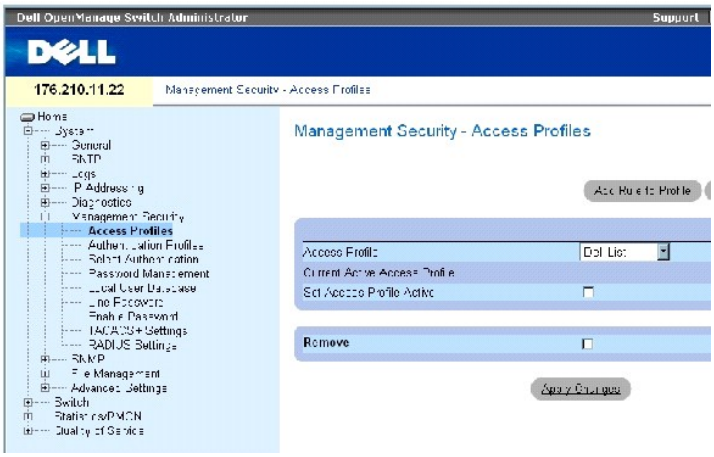
Verwaltungszugriffe können für jede der folgenden Zugriffsmethoden getrennt definiert werden: Webzugriff (HTTP), Sicherer Webzugriff (HTTPS), Telnet und Secure Telnet.

Der Zugriff auf die verschiedenen Verwaltungsmethoden kann je nach Benutzergruppe variieren. Beispielsweise kann festgelegt werden, dass Gerätezugriffe durch Benutzergruppe 1 nur über eine HTTPS-Sitzung erfolgen können, während Benutzergruppe 2 sowohl über HTTPS- als auch über Telnet-Sitzungen auf das Gerät zugreifen kann.

Die Verwaltungszugriffslisten enthalten bis zu 256 Regeln, über die festgelegt wird, welche Benutzer zur Verwaltung des Gerätes berechtigt sind und welche Methoden hierbei verwendet werden dürfen. Es ist auch möglich, den Gerätezugriff für Benutzer zu sperren.

Die Seite **Access Profiles (Zugriffsprofile)** enthält Felder für die Konfigurierung von Verwaltungslisten und ihre Anwendung auf bestimmte Schnittstellen. Klicken Sie zum Öffnen der Seite **Access Profiles** in der Strukturansicht auf **System→ Management Security→ Access Profiles**.

Abbildung 6-38. Access Profiles (Zugriffsprofile)



Die Seite **Access Profiles** enthält folgende Felder:

Access Profile (Zugriffsprofil) – Listen von benutzerdefinierten Zugriffsprofilen. Die Liste **Access Profile** enthält den Standardeintrag **Console Only** (Nur Konsole). Bei Auswahl dieses Zugriffsprofils kann die aktive Verwaltung des Gerätes nur über die Konsolenverbindung erfolgen.

Current Active Access Profile (Derzeit aktives Zugriffsprofil) – Das derzeit aktive Zugriffsprofil.

Set Access Profile Active (Zugriffsprofil aktivieren) – Aktiviert ein Zugriffsprofil.

Remove (Entfernen) – Wenn dieses Kontrollkästchen aktiviert ist, wird das Zugriffsprofil aus der Liste **Access Profile Name** (Zugriffsprofilname) entfernt.

Aktivieren eines Profils

1. Öffnen Sie die Seite **Access Profiles (Zugriffsprofile)**.
2. Wählen Sie im Feld **Access Profile** ein Zugriffsprofil aus.
3. Aktivieren Sie das Kontrollkästchen **Set Access Profile Active** (Zugriffsprofil aktivieren).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das Zugriffsprofil wird aktiviert.

Hinzufügen eines Zugriffsprofils

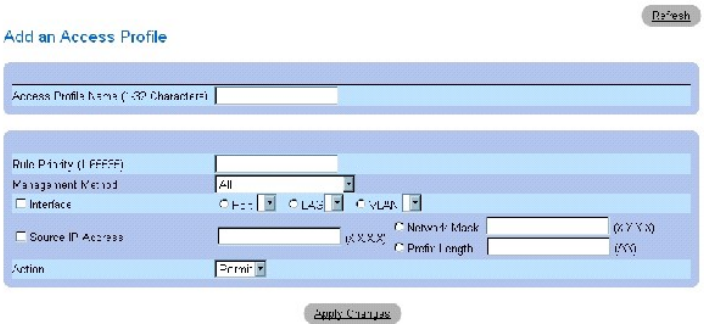
Bei der Bestimmung der Priorität von Regeln, der Geräteverwaltungsmethode, des Schnittstellentyps, der IP-Quelladresse sowie der Netzwerkmaske und des Zugriffs auf die Geräteverwaltung haben Regeln die Funktion von Filtern. Benutzern kann der Verwaltungszugriff gewährt oder verwehrt werden. Die Reihenfolge, in der die Regeln angewendet werden, hängt von der Priorität der Regeln ab.

Definieren von Regeln für ein Zugriffsprofil:

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

Die Seite **Add an Access Profile (Zugriffsprofil hinzufügen)** wird geöffnet:

Abbildung 6-39. Add an Access Profile (Zugriffsprofil hinzufügen)



Die Seite Add an Access Profile (Zugriffsprofil hinzufügen) enthält die folgenden zusätzlichen Felder:

Access Profile Name (1-32 Characters) (Zugriffsprofilname) – Der benutzerdefinierte Name des Zugriffsprofils. Der Name des Zugriffsprofils darf bis zu 32 Zeichen umfassen.

Rule Priority (1-65535) (Regelpriorität) – Die Priorität der Regeln. Bei dem Abgleich des Pakets mit einer Regel wird Benutzergruppen der Verwaltungszugriff auf das Gerät entweder gewährt oder verwehrt. Die Reihenfolge der Regeln wird durch Eingeben einer Regelpriorität in diesem Feld festgelegt. Die Regelnummer spielt eine wichtige Rolle für den Abgleich von Paketen mit Regeln, da Pakete nach dem First-Fit-Verfahren (erste passende Regel) abgeglichen werden. Die Priorität der Regeln kann der Seite **Profile Rules Table (Tabelle der Profilregeln)** entnommen werden.

Management Method (Verwaltungsmethode) – Die Verwaltungsmethode, für die das Zugriffsprofil definiert wurde. Benutzern mit diesem Zugriffsprofil wird der Zugriff auf das Gerät über die ausgewählte Verwaltungsmethode (Leitung) gewährt oder verwehrt.

Interface (Schnittstelle) – Der Schnittstellentyp, auf den die Regel angewendet wird. Dieses Feld ist optional. Diese Regel kann auf einen Port, eine LAG oder ein VLAN angewendet werden. Aktivieren Sie zunächst das Kontrollkästchen und wählen Sie dann das gewünschte Optionsfeld und die betreffende

Schnittstelle aus.

ANMERKUNG: Durch die Zuweisung eines Zugriffsprofils zu einer Schnittstelle wird der Zugriff über andere Schnittstellen gesperrt. Wenn keiner Schnittstelle ein Zugriffsprofil zugewiesen ist, kann über alle Schnittstellen auf das Gerät zugegriffen werden.

Source IP Address (X.X.X.X) (IP-Quelladresse (X.X.X.X)) – Die IP-Quelladresse der Schnittstelle, auf die die Regel angewendet wird. Dieses Feld ist optional und gibt an, dass die Regel für ein Subnetz gilt.

Network Mask (X.X.X.X) (Netzwerkmaske (X.X.X.X)) – Die IP-Subnetzmaske.

Prefix Length (/XX) (Präfixlänge (/XX)) – Die Anzahl der Bits, aus denen das Präfix der IP-Quelladresse oder der Netzwerkmaske der IP-Quelladresse besteht.

Action (Maßnahme) – Legt fest, ob der Verwaltungszugriff auf die definierte Schnittstelle gewährt oder verwehrt ist.

3. Definieren Sie das Feld **Access Profile Name** (Zugriffsprofilname).
4. Definieren Sie die relevanten Felder.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das neue Zugriffsprofil wird hinzugefügt und das Gerät aktualisiert.

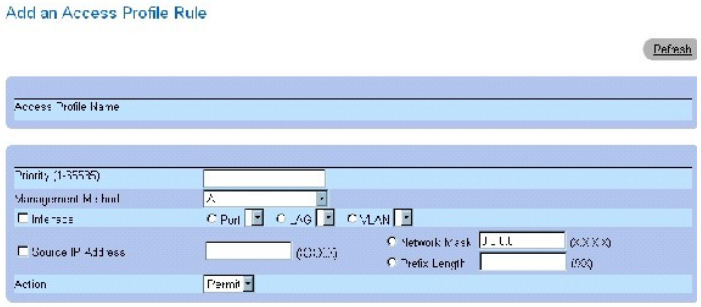
Hinzufügen von Regeln zu einem Zugriffsprofil

ANMERKUNG: Die erste Regel muss definiert werden, damit der Datenverkehr mit Zugriffsprofilen verglichen werden kann.

1. Öffnen Sie die Seite **Access Profiles (Zugriffsprofile)**.
2. Klicken Sie auf **Add Rule to Profile** (Regel zu Profil hinzufügen).

Die Seite **Add an Access Profile Rule** (Zugriffsprofilregel hinzufügen) wird geöffnet:

Abbildung 6-40. Add an Access Profile Rule (Zugriffsprofilregel hinzufügen)



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

Die Regel wird zum Zugriffsprofil hinzugefügt und das Gerät aktualisiert.

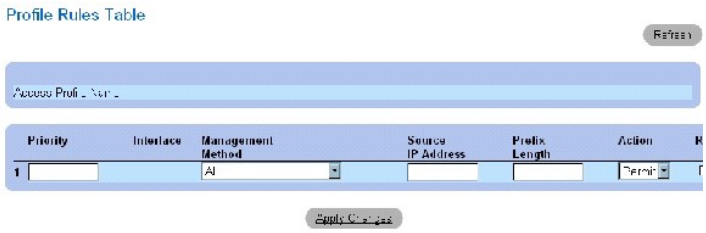
Anzeigen der Seite Profile Rules Table (Tabelle der Profilregeln)

ANMERKUNG: Die Reihenfolge, in der Regeln in der Seite Profile Rules Table angezeigt werden, ist von Bedeutung. Pakete werden mit der ersten Regel abgeglichen, die die für die Regel festgelegten Kriterien erfüllt.

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

Die Seite **Profile Rules Table (Tabelle der Profilregeln)** wird geöffnet:

Abbildung 6-41. Profile Rules Table (Tabelle der Profilregeln)



Entfernen einer Regel

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

Die Seite **Profile Rules Table (Tabelle der Profilregeln)** wird geöffnet.

3. Wählen Sie eine Regel aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die ausgewählte Regel wird gelöscht und das Gerät aktualisiert.

Definieren von Zugriffsprofilen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite Access Profiles (Zugriffsprofile) äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-28. CLI-Befehle für Zugriffsprofile

CLI-Befehl	Beschreibung
management access-list Name	Definiert eine Verwaltungszugriffsliste und erfasst den Zugriffslistenkontext zu Konfigurationszwecken.
permit [ethernet Schnittstellennummer | vlan VLAN-ID | port-channel Nummer] [service Dienst]	Legt Port-Zugriffsbedingungen für die Verwaltungszugriffsliste fest.
permit ip-source IP-Adresse [mask Maske | Präfixlänge] [ethernet Schnittstellennummer | vlan VLAN-ID | port-channel Nummer] [service Dienst]	Legt Port-Zugriffsbedingungen für die Verwaltungszugriffsliste sowie die ausgewählte Verwaltungsmethode fest.
deny [ethernet Schnittstellennummer | vlan VLAN-ID | port-channel Nummer] [service Dienst]	Legt Port-Sperrbedingungen für die Verwaltungszugriffsliste sowie die ausgewählte Verwaltungsmethode fest.
deny ip-source IP-Adresse [mask Maske | Präfixlänge] [ethernet Schnittstellennummer | vlan VLAN-ID | port-channel Nummer] [service Dienst]	Legt 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 zur Verwaltungszugriffsklasse an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)#
management access-list
```

```
mlist



console(config-macl)#
permit ethernet 1/e1



console(config-macl)#
permit ethernet 1/e2



console(config-macl)# deny
ethernet 1/e3



console(config-macl)# deny
ethernet 1/e4



console(config-macl)# exit



console(config)#
management access-class
mlist



console(config)# exit



console# show management
access-list



mlist



-----



permit ethernet 1/e1



permit ethernet 1/e2



deny ethernet 1/e3



deny ethernet 1/e4



! (Note: all other access
implicitly denied)



Console# show management
access-class



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

Definieren von Authentifizierungsprofilen

Die Seite Authentication Profiles (Authentifizierungsprofile) enthält Felder für die Auswahl der Benutzerauthentifizierungsmethode für das Gerät. Die Benutzerauthentifizierung erfolgt:

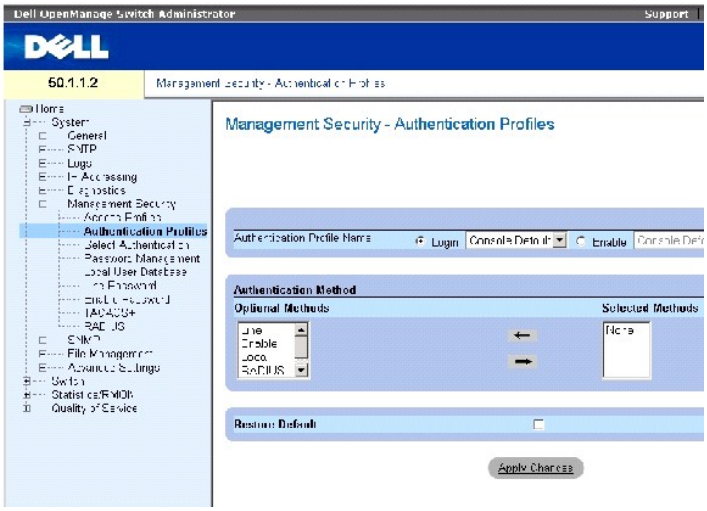
- lokal
- über einen externen Server

Außerdem kann die Benutzerauthentifizierung auf None (Keine) gesetzt werden.

Die Benutzerauthentifizierung erfolgt in der Reihenfolge, in der die Methoden ausgewählt werden. Wird beispielsweise sowohl die Option Local als auch die Option RADIUS ausgewählt, wird der Benutzer zuerst lokal authentifiziert. Wenn die lokale Benutzerdatenbank keine Datensätze enthält, wird der Benutzer über den RADIUS-Server authentifiziert. Wenn die Authentifizierung mit Hilfe der ersten Methode fehlschlägt, wird keine weitere Authentifizierung durchgeführt.

Falls während der Authentifizierung ein Fehler auftritt, wird die nächste ausgewählte Methode verwendet. Klicken Sie zum Öffnen der Seite Authentication Profiles (Authentifizierungsprofile) in der Strukturansicht auf System→ Management Security→ Authentication Profiles.

Abbildung 6-42. Authentication Profiles (Authentifizierungsprofile)



Die Seite Authentication Profiles (Authentifizierungsprofile) enthält folgende Felder:

Authentication Profile Name (Authentifizierungsprofilname) – Listen mit benutzerdefinierten Authentifizierungsprofilen, zu denen benutzerdefinierte Authentifizierungsprofile hinzugefügt werden. Die Standardwerte lauten **Network Default** (Netzwerk) und **Console Default** (Konsole).

- Login (Anmeldung) – Legt die Liste benutzerdefinierter Authentifizierungsprofile für Anmeldekennwörter fest.
- Enable (Aktivierung) – Legt die Liste benutzerdefinierter Authentifizierungsprofile für Aktivierungskennwörter fest.

Optional Methods (Optionale Methoden) – Benutzerauthentifizierungsmethoden. Die möglichen Optionen lauten:

None (Keine) – Es erfolgt keine Benutzerauthentifizierung.

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

RADIUS – Die Benutzerauthentifizierung erfolgt auf dem RADIUS-Server. Weitere Informationen hierzu finden Sie unter Konfigurieren von RADIUS-Einstellungen.

Line (Leitung) – Für die Benutzerauthentifizierung wird das Leitungskennwort verwendet.

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

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

Restore Default (Standardeinstellungen wiederherstellen) – Stellt die Standardmethode zur Benutzerauthentifizierung auf dem Gerät wieder her. Diese Option ist nur für Standardprofile verfügbar.

Remove (Entfernen) – Wenn dieses Kontrollkästchen aktiviert ist, wird das ausgewählte Profil entfernt. Aktive Profile können nicht gelöscht werden. Diese Option ist nur für benutzerdefinierte Profile verfügbar.

Auswählen eines Authentifizierungsprofils:

1. Öffnen Sie die Seite **Authentication Profiles (Authentifizierungsprofile)**.
2. Wählen Sie im Feld **Authentication Profile Name** (Authentifizierungsprofilname) ein Profil aus.
3. Wählen Sie mit den Pfeilschaltflächen eine Authentifizierungsmethode aus. Die Authentifizierung erfolgt in der Reihenfolge, in der die Authentifizierungsmethoden aufgeführt sind.
4. Klicken Sie auf Apply Changes (Änderungen übernehmen).

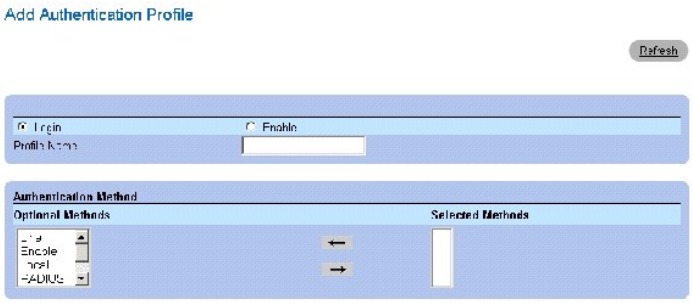
Das Benutzerauthentifizierungsprofil für das Gerät wird aktualisiert.

Hinzufügen eines Authentifizierungsprofils:

1. Öffnen Sie die Seite **Authentication Profiles (Authentifizierungsprofile)**.
2. Klicken Sie auf Add (Hinzufügen).

Die Seite **Add Authentication Profile** (Authentifizierungsprofil hinzufügen) wird geöffnet:

Abbildung 6-43. Add Authentication Profile (Authentifizierungsprofil hinzufügen)



3. Konfigurieren Sie das Profil.

ANMERKUNG: Verwenden Sie im Namen des neuen Profils keine Leerzeichen.

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

Das Authentifizierungsprofil für das Gerät wird aktualisiert.

Anzeigen der Seite Authentication Profiles Table (Tabelle der Authentifizierungsprofile):

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

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

   Die Seite **Authentication Profiles Table** (Tabelle der Authentifizierungsprofile) wird geöffnet.

Löschen eines Authentifizierungsprofils:

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

   Die Seite **Authentication Profiles Table** (Tabelle der Authentifizierungsprofile) wird geöffnet.
3. Wählen Sie ein Authentifizierungsprofil aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Das ausgewählte Authentifizierungsprofil wird gelöscht.

Konfigurieren eines Authentifizierungsprofils mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **Authentication Profiles (Authentifizierungsprofile)** äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-29. CLI-Befehle für Authentifizierungsprofile

CLI-Befehl	Beschreibung
aaa authentication login {default | Listenname} Methode1 [Methode2]	Konfiguriert die Anmeldungsauthentifizierung.
no aaa authentication login {default | Listenname}	Entfernt ein Anmeldungsauthentifizierungsprofil.

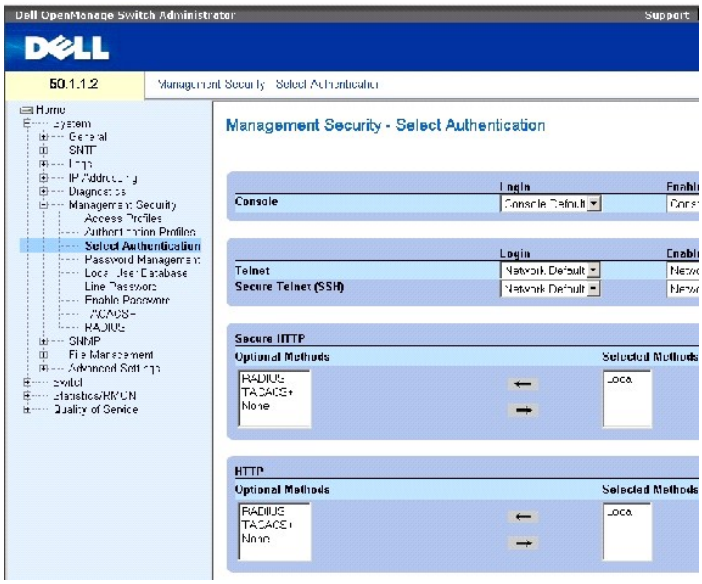
Im Folgenden ein Beispiel für die CLI-Befehle:

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



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

Auswählen von Authentifizierungsprofilen

Nach dem Konfigurieren von Authentifizierungsprofilen können diese auf Verwaltungszugriffsmethoden angewendet werden. Beispielsweise können Konsolenbenutzer anhand der Authentifizierungsmethodenliste 1 und Telnet-Benutzer anhand der Authentifizierungsmethodenliste 2 authentifiziert werden. Klicken Sie zum Öffnen der Seite **Select Authentication (Authentifizierung auswählen)** in der Strukturansicht auf System→ Management Security→ Select Authentication.

Abbildung 6-44. Select Authentication (Authentifizierung auswählen)



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

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

Login (Anmeldung) – Legt Authentifizierungsprofile für Benutzer fest, die sich bei der Konsolenschnittstelle anmelden.

Enable (Aktivierung) – Legt Authentifizierungsprofile für Benutzer fest, die an der Konsolenschnittstelle den Privileged EXEC Mode aktivieren.

Telnet – Authentifizierungsprofile für die Authentifizierung von Telnet-Benutzern.

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

HTTP und **Secure HTTP** – Authentifizierungsmethoden für den HTTP-Zugriff bzw. Secure HTTP-Zugriff. Die möglichen Feldwerte lauten:

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

Local (Lokal) – Die Authentifizierung erfolgt lokal.

RADIUS – Die Authentifizierung erfolgt auf dem RADIUS-Server.

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

Zuweisen einer Authentifizierungsliste zu Konsolensitzungen

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

Konsolensitzungen wird eine Authentifizierungsliste zugewiesen.

Zuweisen eines Authentifizierungsprofils zu Telnet-Sitzungen

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

Telnet-Sitzungen wird eine Authentifizierungsliste zugewiesen.

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

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

Secure Telnet-(SSH-)Sitzungen wird ein Authentifizierungsprofil zugewiesen.

Zuweisen einer Authentifizierungssequenz zu HTTP-Sitzungen

1. Öffnen Sie die Seite **Select Authentication (Authentifizierung auswählen)**.
2. Wählen Sie im Feld **HTTP** eine Authentifizierungssequenz aus.
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 im Feld **Secure HTTP** eine Authentifizierungssequenz aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Secure HTTP-Sitzungen wird eine Authentifizierungssequenz zugewiesen.

Zuweisen von Zugriffsauthentifizierungsprofilen oder -sequenzen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **Select Authentication (Authentifizierung auswählen)** äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-30. CLI-Befehle für die Auswahl von Authentifizierungsprofilen

CLI-Befehl	Beschreibung
enable authentication [default | Listenname]	Gibt die Authentifizierungsmethodenliste für Zugriffe auf eine höhere Berechtigungsebene über eine Remote-Telnet-, Konsolen- oder SSH-Sitzung an.
login authentication [default | Listenname]	Gibt die Liste der Anmeldungsauthentifizierungsmethoden für eine Remote-Telnet-, Konsolen- oder SSH-Sitzung an.
ip http authentication Methode1 [Methode2]	Gibt Authentifizierungsmethoden für HTTP-Server an.
ip https authentication Methode1 [Methode2]	Gibt Authentifizierungsmethoden für HTTPS-Server an.
show authentication methods	Zeigt Informationen zu den Authentifizierungsmethoden an.

Im Folgenden ein Beispiel für die CLI-Befehle:

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

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

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

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

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

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

```

```

```
console# show authentication methods
```

```
Login Authentication Method Lists


---------------------------------
```

Console_Default	: None	
Network_Default	: Local	

```
Enable Authentication Method Lists


---------------------------------
```

Console_Default	: Enable None	
Network_Default	: Enable	
Line	Login Method List	Enable Method List
----	---------- ----	------- ------- ----
Console	Default	Default
Telnet	Default	Default
SSH	Default	Default

http	: Local	
https	: Local	
dot1x	:	

Verwalten von Kennwörtern

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

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

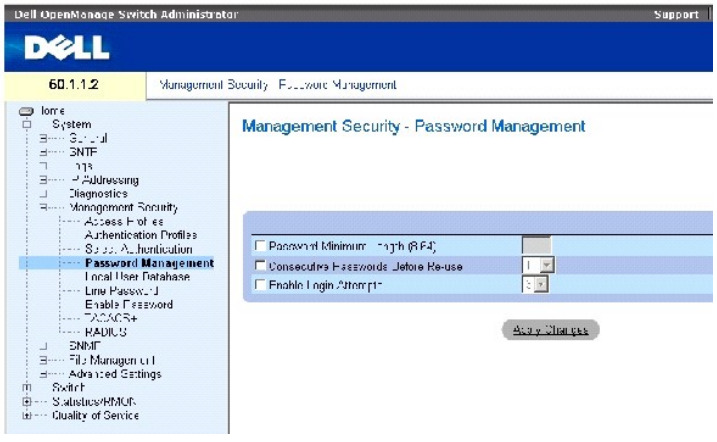
Die Kennwortalterung beginnt unmittelbar nach der Aktivierung der Kennwortverwaltung. Wann ein Kennwort abläuft, wird durch benutzerdefinierte Einstellungen für Ablauftag/-uhrzeit festgelegt. Zehn Tage vor dem Ablauf eines Kennworts zeigt das Gerät eine Warnmeldung an, dass das Kennwort in Kürze abläuft.

Nach dem Ablauf des Kennworts können sich Benutzer noch dreimal anmelden. Während dieser drei verbleibenden Anmeldungen wird eine zusätzliche Warnmeldung angezeigt, die den Benutzer darauf hinweist, dass das Kennwort umgehend geändert werden muss. Wird das Kennwort nicht geändert, wird Benutzern der Zugriff auf das System verwehrt. Sie können sich dann nur noch über die Konsole anmelden. Kennwortwarnmeldungen werden in der Syslog-Datei protokolliert.

Wenn eine Berechtigungsebene neu definiert wird, muss auch der Benutzer neu definiert werden. Die Kennwortalterung beginnt jedoch wieder ab dem Zeitpunkt, zu dem der Benutzer erstmalig eingerichtet wurde.

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

Abbildung 6-45. Password Management (Kennwortverwaltung)



Die Seite **Password Management (Kennwortverwaltung)** enthält folgende Felder:

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

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

ANMERKUNG: Der Benutzer wird vor dem Ablaufen des Kennworts informiert und darauf hingewiesen, dass es geändert werden muss. Webbenutzern wird diese Meldung jedoch nicht angezeigt.

Enable Login Attempts (Zulässige Anmeldeversuche) – Wenn dieses Kontrollkästchen aktiviert ist, wird dem Benutzer der Gerätezugriff verwehrt, sobald die Anzahl fehlerhafter Kennworteingaben die hier festgelegte benutzerdefinierte Anzahl übersteigt. Beispiel: Ist das Kontrollkästchen aktiviert und ist für die Anzahl der Anmeldeversuche der Wert 5 festgelegt, kann ein Benutzer fünf Mal versuchen, sich mit einem falschen Kennwort anzumelden. Beim sechsten Mal wird der Benutzer durch das Gerät gesperrt. Die möglichen Feldwerte lauten 1 bis 5.

Definieren der Kennwortverwaltung

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

Die Kennwortverwaltung wird definiert und das Gerät aktualisiert.

Verwalten von Kennwörtern mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **Password Management (Kennwortverwaltung)** äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-31. Verwalten von Kennwörtern mit Hilfe der CLI-Befehle

CLI-Befehl	Beschreibung
password min-length *Länge*	Legt die Mindestlänge von Kennwörtern fest.
password history Anzahl	Legt fest, wie oft das Kennwort geändert werden muss, bevor das ursprüngliche Kennwert erneut verwendet werden kann.
password lock-out *Anzahl*	Legt fest, wie oft ein falsches Kennwort eingegeben werden darf, bevor der Gerätezugriff für den Benutzer gesperrt wird.
show password configuration	Zeigt Informationen zur Kennwortverwaltung an.

Im Folgenden ein Beispiel für die CLI-Befehle:

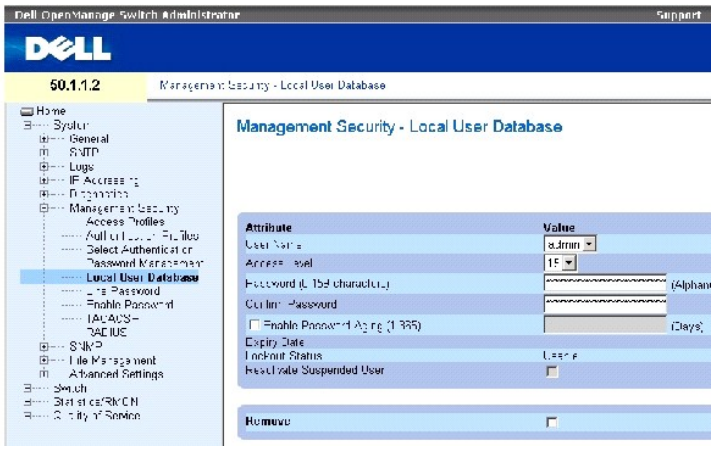
```
console # show passwords configuration

Minimal length: 0

History: Disabled

History hold time: no limit

Lockout control: disabled

Enable Passwords
```

Level	Password Aging	Password Expiry date	Lockout	
-----	--------	----------	-------	
1	-	-	-	
15	-	-	-	
Line Passwords				
Line	Password Aging	Password Expiry date	Lockout	
-------	--------	----------	-------	
Telnet	-	-	-	
SSH	-	-	-	
Console	-	-	-	
console # **show users accounts**				
Username	Privilege	Password Aging	Password Expiry Date	Lockout
--------	---------	--------	----------	-------
nim	15	39	18-Feb-2005	

Definieren der lokalen Benutzerdatenbanken

Die Seite **Local User Database (Lokale Benutzerdatenbank)** enthält Felder zum Festlegen von Benutzern, Kennwörtern und Berechtigungsstufen. Klicken Sie zum Öffnen der Seite **Local User Database (Lokale Benutzerdatenbank)** in der Strukturansicht auf System→ Management Security→ Local User Database.

Abbildung 6-46. Local User Database (Lokale Benutzerdatenbank)



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

User Name (Benutzername) – Die Liste der Benutzer.

Access Level (Berechtigungsstufe) – Die Berechtigungsstufe von Benutzern. Die niedrigste Berechtigungsstufe von Benutzern ist **1**, die höchste Berechtigungsstufe ist **15**. Benutzer der Berechtigungsstufe 15 besitzen Privileged Exec-Zugriff; nur sie können auf OpenManage Switch Administrator zugreifen und die Oberfläche verwenden.

Password (0-159 Characters) (Kennwort (0-159 Zeichen)) – Das benutzerdefinierte Kennwort.

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

Enable Password Aging (1-365) (Kennwortalterung aktivieren (1-365)) – Gibt bei Aktivierung des Kontrollkästchens an, nach wie vielen Tagen ein Kennwort abläuft.

Expiry Date (Ablaufdatum) – Gibt das Ablaufdatum des benutzerdefinierten Kennworts an.

Lockout Status (Gesperrt-Status) – Gibt die Anzahl der fehlgeschlagenen Authentifizierungsversuche seit der letzten erfolgreichen Anmeldung des Benutzers an, wenn auf der Seite **Password Management (Kennwortverwaltung)** das Kontrollkästchen **Enable Login Attempts** (Zulässige Anmeldeversuche) aktiviert ist. Wenn das Benutzerkonto gesperrt ist, wird hier der Eintrag **LOCKOUT** (GESPERRT) angezeigt.

Reactivate Suspended User (Gesperrten Benutzer reaktivieren) – Ist das Kontrollkästchen aktiviert, werden die Zugriffsrechte des betreffenden Benutzers reaktiviert. Zugriffsrechte können nach einem fehlgeschlagenen Anmeldeversuch vorübergehend außer Kraft gesetzt werden.

Remove (Entfernen) – Ist das Kontrollkästchen aktiviert, werden Benutzer aus der Liste **User Name** (Benutzername) entfernt.

Zuweisen von Zugriffsrechten zu einem Benutzer:

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

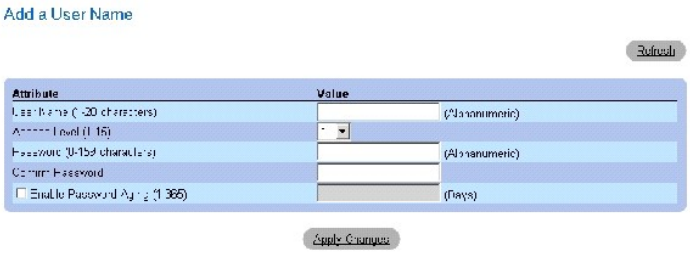
Die Benutzerzugriffsrechte und Kennwörter werden definiert und das Gerät aktualisiert.

Definieren eines neuen Benutzers:

1. Öffnen Sie die Seite **Local User Database (Lokale Benutzerdatenbank)**.
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite **Add a User Name** (Benutzername hinzufügen) wird geöffnet:

Abbildung 6-47. Add a User Name (Benutzername hinzufügen)



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

Der neue Benutzer wird definiert und das Gerät aktualisiert.

Anzeigen der Seite Local User Table (Lokale Benutzertabelle):

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

Die Seite Local User Table (Lokale Benutzertabelle) wird geöffnet:

Abbildung 6-48. Local User Table (Lokale Benutzertabelle)

Reaktivieren eines gesperrten Benutzers:

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

Die Seite Local User Table (Lokale Benutzertabelle) wird geöffnet.

3. Wählen Sie unter **User Name** (Benutzername) einen Eintrag aus.
4. Aktivieren Sie das Kontrollkästchen **Reactivate Suspended User** (Gesperrten Benutzer reaktivieren).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Zugriffsrechte des Benutzers werden reaktiviert und das Gerät aktualisiert.

Löschen von Benutzern:

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

   Die Seite **Local User Table (Lokale Benutzertabelle)** wird geöffnet.
3. Wählen Sie unter **User Name** (Benutzername) einen Eintrag aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der ausgewählte Benutzer wird gelöscht und das Gerät aktualisiert.

Zuweisen von Benutzern mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **Local User Database (Lokale Benutzerdatenbank)** äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-32. CLI-Befehle für die lokale Benutzerdatenbank

CLI-Befehl	Beschreibung
username Name [password Kennwort] [level Stufe] [encrypted]	Richtet ein auf Benutzernamen basierendes Authentifizierungssystem ein.
set username Name **active**	Reaktiviert die Zugriffsrechte eines gesperrten Benutzers.

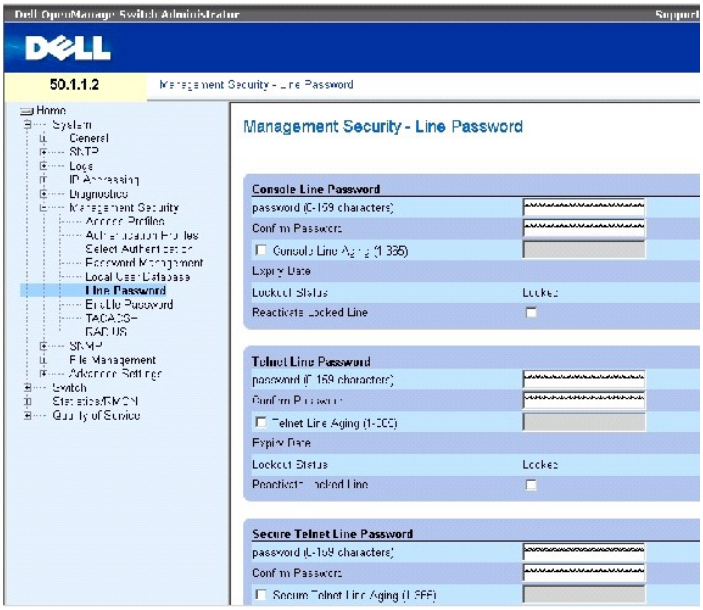
Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# username
bob password lee level 15


console# set username bob
active
```

Definieren von Leitungskennwörtern

Die Seite Line Password (Leitungskennwort) enthält Felder zur Festlegung von Leitungskennwörtern für Verwaltungsmethoden. Klicken Sie zum Öffnen der Seite Line Password (Leitungskennwort) in der Strukturansicht auf System→ Management Security→ Line Passwords.

Abbildung 6-49. Line Password (Leitungskennwort)



Die Seite Line Password (Leitungskennwort) enthält folgende Felder:

Line Password (Leitungskennwort für Konsole/Telnet/Secure Telnet) – Das Leitungskennwort für den Gerätezugriff über eine Konsolen-, Telnet- oder Secure Telnet-Sitzung.

Confirm Password (Kennwort bestätigen für Konsole/Telnet/Secure Telnet) – Bestätigt das neue Leitungskennwort. Anstelle des Kennworts werden Sternchen (*****) angezeigt.

Line Aging (1-365) (Kennwortablauf für Konsole/Telnet/Secure Telnet (1-365)) – Gibt an, nach wie vielen Tagen ein Leitungskennwort bei Aktivierung des Kontrollkästchens abläuft.

Expiry Date (Ablaufdatum für Konsole/Telnet/Secure Telnet) – Gibt das Ablaufdatum des Leitungskennworts an.

Lockout Status (Gesperrt-Status für Konsole/Telnet/Secure Telnet) – Gibt die Anzahl der fehlgeschlagenen Authentifizierungsversuche seit der letzten erfolgreichen Anmeldung des Benutzers an, wenn auf der Seite **Password Management (Kennwortverwaltung)** das Kontrollkästchen **Enable Login Attempts** (Zulässige Anmeldeversuche) aktiviert ist. Wenn das Benutzerkonto gesperrt ist, wird hier der Eintrag **LOCKOUT** (GESPERRT) angezeigt.

Reactivate Locked Line (Gesperrtes Leitungskennwort für Konsole/Telnet/Secure Telnet reaktivieren) – Ist das Kontrollkästchen aktiviert, wird das Leitungskennwort für die Konsolen-, Telnet- bzw. Secure Telnet-Sitzung reaktiviert. Zugriffsrechte können nach einem fehlgeschlagenen Anmeldeversuch vorübergehend außer Kraft gesetzt werden.

Definieren von Leitungskennwörtern für Konsolensitzungen

1. Öffnen Sie die Seite **Line Password (Leitungskennwort)**.
2. Definieren Sie das Feld **Console Line Password** (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 Telnet Line Password (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 **Secure Telnet Line Password** (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 Hilfe der CLI-Befehle

In der folgenden Tabelle wird der der Seite **Line Password (Leitungskennwort)** äquivalente CLI-Befehl zur Festlegung von Feldern zusammengefasst.

Tabelle 6-33. CLI-Befehl für Leitungskennwörter

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

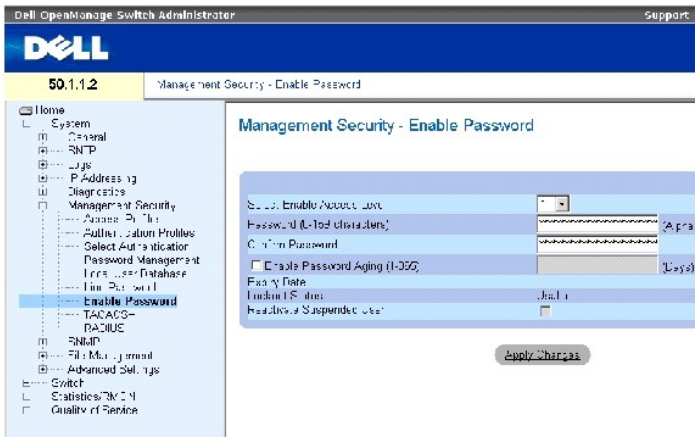
Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config-line)#
password dell
```

Definieren von Aktivierungskennwörtern

Auf der Seite **Enable Password (Aktivierungskennwort)** wird ein lokales Kennwort festgelegt, das den Zugriff auf normale und privilegierte Berechtigungsstufen steuert. Klicken Sie zum Öffnen der Seite **Enable Password (Aktivierungskennwort)** in der Strukturansicht auf System→ Management Security→ Enable Passwords.

Abbildung 6-50. Enable Password (Aktivierungskennwort)



Die Seite **Enable Password (Aktivierungskennwort)** enthält folgende Felder:

Select Enable Access Level (Berechtigungsstufe für Aktivierungskennwort auswählen) – Die dem Aktivierungskennwort zugeordnete Berechtigungsstufe. Die möglichen Feldwerte lauten 1 bis 15.

Password (0-159 Characters) (Kennwort (0-159 Zeichen)) – Das aktuelle Aktivierungskennwort.

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

Enable Password Aging (1-365) (Kennwortalterung aktivieren (1-365)) – Gibt bei Aktivierung des Kontrollkästchens an, nach wie vielen Tagen ein Kennwort abläuft.

Expiry Date (Ablaufdatum) – Gibt das Ablaufdatum des Aktivierungskennworts an.

Lockout Status (Gesperrt-Status) – Gibt die Anzahl der fehlgeschlagenen Authentifizierungsversuche seit der letzten erfolgreichen Anmeldung des Benutzers an, wenn auf der Seite **Password Management (Kennwortverwaltung)** das Kontrollkästchen **Enable Login Attempts** (Zulässige Anmeldeversuche) aktiviert ist. Wenn das Benutzerkonto gesperrt ist, wird hier der Eintrag **LOCKOUT** (GESPERRT) angezeigt.

Reactivate Suspended User (Gesperrten Benutzer reaktivieren) – Ist das Kontrollkästchen aktiviert, werden die Zugriffsrechte des betreffenden Benutzers reaktiviert. Zugriffsrechte können nach einem fehlgeschlagenen Anmeldeversuch vorübergehend außer Kraft gesetzt werden.

Definieren eines neuen Aktivierungskennworts:

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

Das neue Aktivierungskennwort wird definiert und das Gerät aktualisiert.

Zuweisen von Aktivierungskennwörtern mit Hilfe der CLI-Befehle

In der folgenden Tabelle wird der der Seite **Enable Password (Aktivierungskennwort)** äquivalente CLI-Befehl zur Festlegung von Feldern zusammengefasst.

Tabelle 6-34. CLI-Befehl zum Ändern von Aktivierungskennwörtern

CLI-Befehl	Beschreibung
enable password [level Stufe] Kennwort [encrypted]	Legt ein lokales Kennwort fest, um den Zugriff auf die Benutzer- und Berechtigungsstufen zu steuern.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# enable
password level 15 secret
```

Definieren von TACACS+-Einstellungen

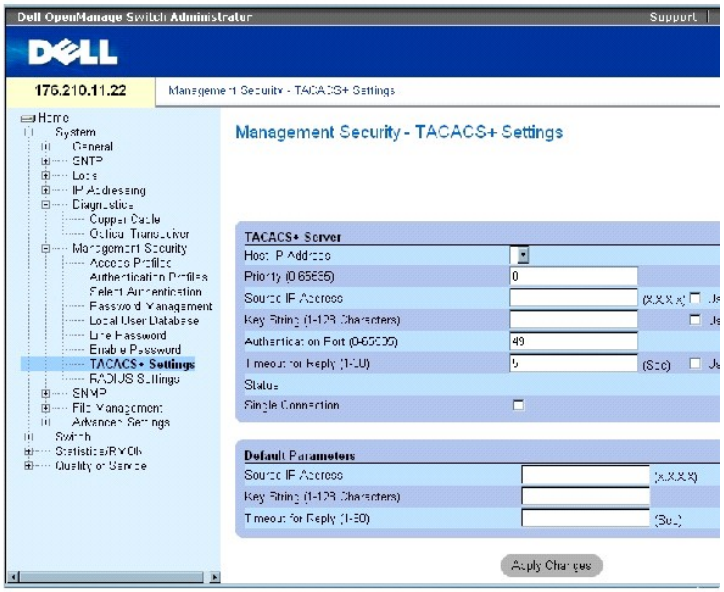
Die Geräte verfügen über Client-Unterstützung für das Terminal Access Controller Access Control System (TACACS+). TACACS+ stellt eine zentrale Sicherheitsfunktion für die Authentifizierung von Benutzern bereit, die auf das Gerät zugreifen.

TACACS+ implementiert ein zentralisiertes Benutzerverwaltungssystem, das jedoch mit RADIUS- und anderen Authentifizierungsverfahren kompatibel ist. TACACS+ stellt die folgenden Dienste bereit:

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

Das TACACS+-Protokoll gewährleistet die Netzwerkintegrität durch verschlüsselte Protokollaustausche zwischen dem Gerät und dem TACACS+-Server. Klicken Sie zum Öffnen der Seite **TACACS+ Settings (TACACS+-Einstellungen)** in der Strukturansicht auf **System→ Management Security→ TACACS+**.

Abbildung 6-51. TACACS+ Settings (TACACS+-Einstellungen)



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

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

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

Source IP Address (IP-Quelladresse) – Die IP-Quelladresse des Gerätes, die für die TACACS+-Sitzung zwischen dem Gerät und dem TACACS+-Server verwendet wird.

Key String (0-128 Characters) (Schlüsselzeichenfolge (0-128 Zeichen)) – Definiert den Schlüssel für die Authentifizierung und Verschlüsselung der TACACS+-Kommunikation zwischen dem Gerät und dem TACACS+-Server. Dieser Schlüssel muss mit dem auf dem TACACS+-Server verwendeten Verschlüsselungsschlüssel übereinstimmen. Dieser Schlüssel ist verschlüsselt.

Authentication Port (0-65535) (Authentifizierungs-Port) – Die Nummer des Ports, über den die TACACS+-Sitzung erfolgt. Die Standardeinstellung ist Port 49.

Timeout for Reply (1-30) (Zeitlimit für Antwort (1-30)) – Der Zeitraum bis zum Ablauf des Zeitlimits für die Verbindung zwischen dem Gerät und dem TACACS+-Server. Für das Feld können die Werte 1 bis 30 Sekunden festgelegt werden.

Status – Der Status der Verbindung zwischen dem Gerät und dem TACACS+-Server. Die möglichen Feldwerte lauten:

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

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

Single Connection (Einzelne Verbindung) – Wenn dieses Kontrollkästchen aktiviert ist, wird zwischen dem Gerät und dem TACACS+-Server eine einzelne offene Verbindung aufrechterhalten.

Bei den im Bereich Default Parameters (Standardparameter) angegebenen TACACS+-Parametern handelt es sich um benutzerdefinierte Standardeinstellungen. Die Standardeinstellungen werden auf neu definierte TACACS+-Server angewendet. Wenn keine Standardwerte definiert sind, werden auf neue TACACS+-Server die Standardeinstellungen des Systems angewendet.

Die TACACS+-Standardeinstellungen lauten:

Source IP Address (IP-Quelladresse) – Die Standard-IP-Quelladresse des Gerätes, die für die TACACS+-Sitzung zwischen dem Gerät und dem TACACS+-Server verwendet wird. Die Standard-IP-Quelladresse lautet 0.0.0.0.

Key String (0-128 Characters) (Schlüsselzeichenfolge (0-128 Zeichen)) – Die Standardschlüsselzeichenfolge, die für die Authentifizierung und Verschlüsselung der gesamten Kommunikation zwischen dem Gerät und dem TACACS+-Server verwendet wird. Dieser Schlüssel ist verschlüsselt.

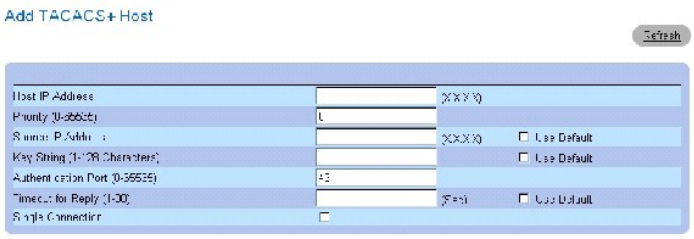
Timeout for Reply (1-30) (Zeitlimit für Antwort (1-30)) – Der Standardzeitraum bis zum Ablauf des Zeitlimits für die Verbindung zwischen dem Gerät und dem TACACS+-Server. Der Standardwert beträgt 5 Sekunden.

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**:

Abbildung 6-52. Add TACACS+ Host (TACACS+-Host hinzufügen)



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

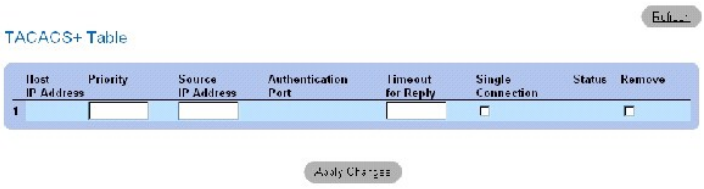
Der TACACS+-Server wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der Seite TACACS+ Table (TACACS+-Tabelle)

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

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

Abbildung 6-53. TACACS+ Table (TACACS+-Tabelle)



Entfernen eines TACACS+-Servers

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

   Die Seite **TACACS+ Table (TACACS+-Tabelle)** wird geöffnet:
3. Wählen Sie einen Eintrag in der Seite **TACACS+ Table (TACACS+-Tabelle)** aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf Apply Changes (Änderungen übernehmen).

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

Definieren von TACACS+-Einstellungen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **TACACS+ Settings (TACACS+-Einstellungen)** äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-35. CLI-Befehle für TACACS+-Einstellungen

CLI-Befehl	Beschreibung
tacacs-server host {*IP-Adresse* | *Hostname*} [**single-connection**] [**port** *Port-Nummer*] [**timeout** *Zeitlimit*] [**key** *Schlüsselzeichenfolge*] [**source** *Quelle*] [**priority** *Priorität*]	Gibt einen TACACS+-Host an.
tacacs-server key Schlüsselzeichenfolge	Gibt den Schlüssel für die Authentifizierung und Verschlüsselung der gesamten TACACS+-Kommunikation zwischen dem Gerät und dem TACACS+-Server an. Dieser Schlüssel muss mit der vom TACACS+-Daemon verwendeten Verschlüsselung übereinstimmen. (Bereich: 0-128 Zeichen.)
tacacs-server timeout Zeitlimit	Gibt das Zeitlimit in Sekunden an. (Bereich: 1 - 30.)
tacacs-server source-ip Quelle	Gibt die IP-Quelladresse an. (Bereich: gültige IP-Adressen.)
show tacacs [*IP-Adresse*]	Zeigt Konfigurationsinformationen und Statistiken für einen TACACS+-Server an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console# show tacacs

Device Configuration

IP address      Status      Port  Single Connection  TimeOut  Source IP  Priority
--------------  ----------  ----  -----------------  -------  ---------  --------
12.1.1.2        Not         49    Yes                1        12.1.1.1   1
```

	Connected					
Global values						

TimeOut : 5						
Device Configuration ----------						
Source IP : 0.0.0.0						
console#						

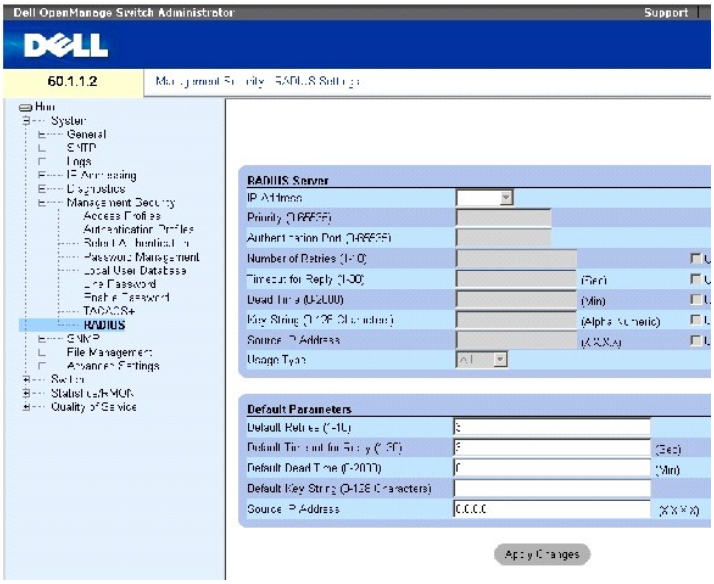
Konfigurieren von RADIUS-Einstellungen

RADIUS-Server (Remote Authorization Dial-In User Service) bieten zusätzliche Sicherheit für Netzwerke. Bis zu vier RADIUS-Server können definiert werden. RADIUS-Server stellen eine zentralisierte Authentifizierungsmethode für folgende Zugriffsarten bereit:

- Telnet-Zugriff
- Secure Shell-Zugriff
- Webzugriff
- Konsolenzugriff

Klicken Sie zum Öffnen der Seite RADIUS Settings (RADIUS-Einstellungen) in der Strukturansicht auf System→ Management Security→ RADIUS.

Abbildung 6-54. RADIUS Settings (RADIUS-Einstellungen)



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

IP Address (IP-Adresse) – Die Liste der IP-Adressen von Authentifizierungsservern.

Priority (0-65535) (Priorität (0-65535)) – Die Priorität des Servers. Die möglichen Werte liegen im Bereich von 0 bis 65535, wobei 0 den höchsten Wert darstellt. Dieser Wert wird zum Festlegen der Abfragereihenfolge der Server verwendet.

Authentication Port (Authentifizierungs-Port) – Gibt den Authentifizierungs-Port an. Der Authentifizierungs-Port wird für die Prüfung der RADIUS-Serverauthentifizierung verwendet.

Number of Retries (1-10) (Anzahl der Wiederholungsversuche (1-10)) – Gibt die Anzahl der Anforderungen an, die an den RADIUS-Server gesendet werden können, bevor ein Fehler auftritt. Die möglichen Feldwerte lauten 1 bis 10.

Timeout for Reply (1-30) (Zeitlimit für Antwort (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 lauten 1 bis 30.

Dead Time (0-2000) (Totzeit (0-2000)) – Gibt die Zeit (in Minuten) an, während der ein RADIUS-Server für Dienstanforderungen umgangen wird. Bereich: 0-2000.

Key String (1-128 Characters) (Schlüsselzeichenfolge (1-128 Zeichen)) – Die Schlüsselzeichenfolge, die für die Authentifizierung und Verschlüsselung der gesamten RADIUS-Kommunikation zwischen dem Gerät und dem RADIUS-Server verwendet wird. Dieser Schlüssel ist verschlüsselt.

Source IP Address (IP-Quelladresse) – Gibt die IP-Quelladresse an, die für die Kommunikation mit RADIUS-Servern verwendet wird.

Usage Type (Verwendungsart) – Gibt die Verwendungsart des Servers an. Mögliche Werte für die Verwendungsart sind: login (Anmeldung), 802.1x oder All (Alle). Ist kein Wert festgelegt, wird standardmäßig die Einstellung All verwendet.

Durch die folgenden Felder werden die RADIUS-Standardwerte festgelegt:

ANMERKUNG: Falls für Timeout (Zeitlimit), Retries (Wiederholungsversuche) oder Dead Time (Totzeit) keine hostspezifischen Werte angegeben sind, werden den einzelnen Hosts die globalen Werte (Standardeinstellungen) zugewiesen.

Default Retries (1-10) (Standardanzahl der Wiederholungsversuche (1-10)) – Gibt die Standardanzahl der Anforderungen an, die an den RADIUS-Server

gesendet werden können, bevor ein Fehler auftritt.

Default Timeout for Reply (1-30) (Standard-Zeitlimit für Antwort (1-30)) – Gibt das Standardzeitintervall (in Sekunden) an, das ein Gerät auf eine Antwort vom RADIUS-Server wartet, bevor eine Zeitüberschreitung auftritt. Der Standardwert beträgt 5 Sekunden.

Default Dead Time (0-2000) (Standard-Totzeit (0-2000)) – Gibt die Standardzeit (in Minuten) an, während der ein RADIUS-Server für Dienstanforderungen umgangen wird. Bereich: 0-2000.

Default Key String (1-128 Characters) (Standardschlüsselzeichenfolge (1-128 Zeichen)) – Die Standardschlüsselzeichenfolge, die für die Authentifizierung und Verschlüsselung der gesamten RADIUS-Kommunikation zwischen dem Gerät und dem RADIUS-Server verwendet wird. Dieser Schlüssel ist verschlüsselt.

Source IP Address (IP-Quelladresse) – Gibt die Standard-IP-Quelladresse an, die für die Kommunikation mit RADIUS-Servern verwendet wird. Die Standard-IP-Quelladresse lautet 0.0.0.0.

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).

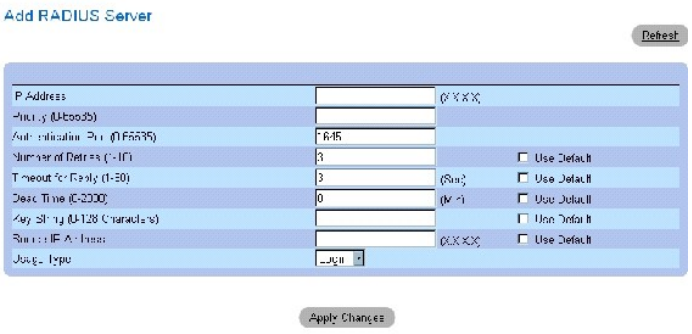
Die RADIUS-Einstellungen für das Gerät werden aktualisiert.

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:

Abbildung 6-55. Add RADIUS Server (RADIUS-Server hinzufügen)



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

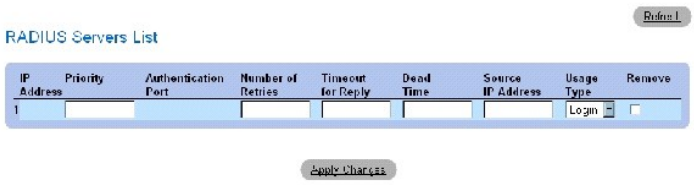
Der neue RADIUS-Server wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der Seite RADIUS Servers List (Liste der RADIUS-Server):

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

Die Seite RADIUS Servers List (Liste der RADIUS-Server) wird geöffnet:

Abbildung 6-56. RADIUS Servers List (Liste der RADIUS-Server)



Entfernen eines RADIUS-Servers

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

   Die Seite RADIUS Servers List (Liste der RADIUS-Server) wird geöffnet.
3. Wählen Sie einen Eintrag in der Seite RADIUS Servers List (Liste der RADIUS-Server) aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf Apply Changes (Änderungen übernehmen).

   Der RADIUS-Server wird entfernt und das Gerät aktualisiert.

Definieren von RADIUS-Servern mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite RADIUS Settings (RADIUS-Einstellungen) äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-36. CLI-Befehle für RADIUS-Server

CLI-Befehl	Beschreibung
radius-server timeout *Zeitlimit*	Legt das Intervall fest, während dem ein Router auf die Antwort eines Server-Hosts wartet.
radius-server retransmit *Wiederholungsversuche*	Legt fest, wie oft die Liste der RADIUS-Server-Hosts von der Software durchsucht wird.
radius-server deadtime Totzeit	Legt fest, dass nicht verfügbare Server übersprungen werden.
radius-server key *Schüsselzeichenfolge*	Legt den Schlüssel für die Authentifizierung und Verschlüsselung der gesamten RADIUS-Kommunikation zwischen dem Router und der RADIUS-Umgebung fest.
radius-server host *IP- Adresse* [**auth-port** *Auth.-Port-Nummer*] [**timeout** Zeitlimit] [**retransmit** *Wiederholungsversuche*] [**deadtime** *Totzeit*] [**key** *Schlüsselzeichenfolge*] [**source** *Quelle*] [**priority** *Priorität*]	Legt einen RADIUS-Server-Host fest.
show radius-servers	Zeigt die Einstellungen der RADIUS-Server an.

Im Folgenden ein Beispiel für die CLI-Befehle:

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

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


Console(config)# radius-
server deadtime 10


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


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


Console# show radius-
servers


IP address Auth Acct
TimeOut Retransmit
Deadtime Source IP
Priority


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


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

Definieren von SNMP-Parametern

SNMP (Simple Network Management Protocol) bietet eine Methode zur Verwaltung von Netzwerkgeräten. Der Switch unterstützt die folgenden SNMP-Versionen:

- SNMPv1 (Version 1)
- SNMPv2 (Version 2)
- SNMPv3 (Version 3)

SNMPv1 und SNMPv2

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

SNMPv1 und SNMPv2 sind standardmäßig aktiviert.

SNMPv3

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

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

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

- Sicherheit
- Kontrolle des Zugriffs auf Funktionen
- Traps

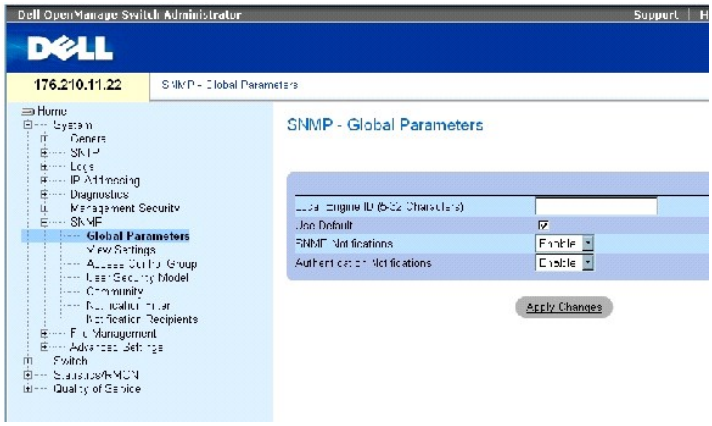
Authentifizierungs- und Datenschutzschlüssel werden auf der Seite User Security Model (Benutzersicherheitsmodell) geändert.

SNMPv3 kann nur aktiviert werden, wenn für die Option Local Engine ID (ID der lokalen Engine) ein Wert definiert ist.

Definieren globaler SNMP-Parameter

Auf der Seite **SNMP Global Parameters (Globale SNMP-Parameter)** können sowohl SNMP- als auch Authentifizierungsbenachrichtigungen aktiviert werden. Klicken Sie zum Öffnen der Seite **SNMP Global Parameters (Globale SNMP-Parameter)** in der Strukturansicht auf System→ SNMP→ Global Parameters.

Abbildung 6-57. SNMP Global Parameters (Globale SNMP-Parameter)



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

Local Engine ID (ID der lokalen Engine) – Gibt die Engine-ID des lokalen Gerätes an. Der Feldwert ist eine hexadezimale Zeichenkette. Jedes Byte einer hexadezimalen Zeichenkette entspricht zwei Hexadezimalziffern. Die einzelnen Bytes können durch einen Punkt oder einen Doppelpunkt getrennt werden. Vor der Aktivierung von SNMPv3 muss die Engine-ID definiert werden.

Legen Sie für freistehende Geräte eine Standard-Engine-ID fest, die aus der Enterprise Number (Unternehmensnummer) und der MAC-Standardadresse besteht.

Vergewissern Sie sich bei der Konfigurierung der Engine-ID von Stack-Systemen, dass die Engine-ID in der Verwaltungsdomäne eindeutig ist. Hierdurch wird verhindert, dass zwei Geräte in einem Netzwerk dieselbe Engine-ID besitzen.

Use Defaults (Standardeinstellungen verwenden) – Verwendet die vom Gerät generierte Engine-ID. Die Standard-Engine-ID basiert auf der MAC-Adresse des Gerätes und ist standardmäßig folgendermaßen definiert:

Erste 4 Oktetts – erstes Bit = 1, für die übrigen Werte wird die IANA Enterprise Number verwendet (= 674).

Fünftes Oktett – Ist auf 3 gesetzt, um darauf hinzuweisen, dass die MAC-Adresse folgt.

Letzte 6 Oktetts – Die MAC-Adresse des Gerätes.

SNMP Notifications (SNMP-Benachrichtigungen) – Aktiviert bzw. deaktiviert den Versand von SNMP-Benachrichtigungen durch den Router.

Authentication Notifications (Authentifizierungsbenachrichtigungen) – Aktiviert bzw. deaktiviert den Versand von SNMP-Traps durch den Router, wenn die Authentifizierung fehlschlägt.

Aktivieren von SNMP-Benachrichtigungen

1. Öffnen Sie die Seite **SNMP Global Parameters (Globale SNMP-Parameter)**.
2. Wählen Sie in der Liste neben dem Feld **SNMP Notifications** (SNMP-Benachrichtigungen) den Eintrag **Enable** (Aktivieren) aus.
3. Klicken Sie auf Apply Changes (Änderungen übernehmen).

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

Aktivieren von Authentifizierungsbenachrichtigungen

1. Öffnen Sie die Seite **SNMP Global Parameters (Globale SNMP-Parameter)**.
2. Wählen Sie in der Liste neben dem Feld **Authentication Notifications** (Authentifizierungsbenachrichtigungen) den Eintrag **Enable** (Aktivieren) aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Aktivieren von SNMP-Benachrichtigungen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **SNMP Global Parameters (Globale SNMP-Parameter)** äquivalenten CLI-Befehle zur Anzeige von Feldern zusammengefasst.

Tabelle 6-37. CLI-Befehle für den Versand von SNMP-Benachrichtigungen

CLI-Befehl	Beschreibung
snmp-server enable traps	Aktiviert den Versand von SNMP-Traps (Simple Network Management Protocol) durch den Router.
snmp-server trap authentication	Aktiviert den Versand von SNMP-Traps (Simple Network Management Protocol) durch den Router, wenn die Authentifizierung fehlschlägt.
show snmp	Überprüft den Status der SNMP-Kommunikation.
snmp-server engine ID local {*Engine-ID-Zeichenkette* | **default**}	Gibt die Engine-ID des lokalen Gerätes an. Der Feldwert ist eine hexadezimale Zeichenkette. Jedes Byte einer hexadezimalen Zeichenkette entspricht zwei Hexadezimalziffern. Die einzelnen Bytes können durch einen Punkt oder einen Doppelpunkt getrennt werden. Vor der Aktivierung von SNMPv3 muss die Engine-ID definiert werden.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console(config)# snmp-server enable traps

Console(config)# snmp-server trap authentication
```

```
Console# show snmp

Community-String                Community-Access        View name       IP address
------------------------------  ----------------------  --------------  ----------
public                          read only               view-1          All

Community-String                Group name              IP address      Type
------------------------------  ----------------------  --------------  ----

Traps are enabled.
Authentication-failure trap is enabled.

Version 1,2 notifications

Target Address  Type  Community  Version  Udp Port  Filter name  To Sec  Retries
--------------  ----  ---------  -------  --------  -----------  ------  -------

Version 3 notifications

Target Address  Type  Username  Security Level  Udp Port  Filter name  To Sec  Retries
--------------  ----  --------  --------------  --------  -----------  ------  -------

System Contact: Robert
System Location: Marketing
```

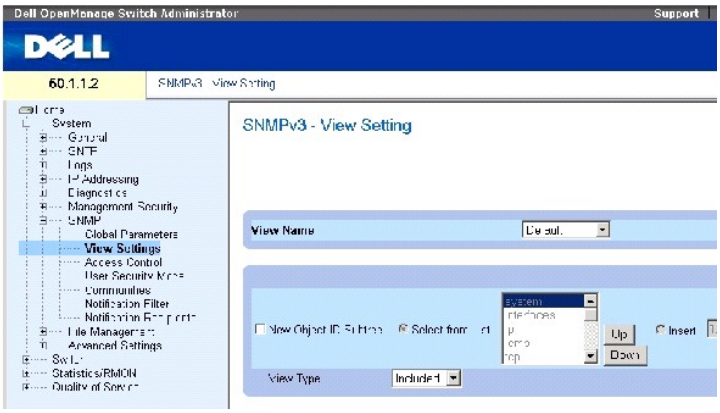
Definieren von Einstellungen für SNMP-Ansichten

Mit Hilfe von SNMP-Ansichten kann der Zugriff auf Gerätefunktionen oder -teilfunktionen gewährt oder verwehrt werden. Beispielweise können Sie eine Ansicht definieren, in der für den Zugriff auf Multicast-Gruppen festgelegt ist, dass SNMP-Gruppe A Nur-Lese-Zugriff (R/O) und SNMP-Gruppe B Lese-/Schreibzugriff (R/W) besitzt. Der Zugriff auf Funktionen wird über den MIB-Namen bzw. die MIB-Objekt-ID gewährt.

Mit Hilfe der Schaltflächen Up (Nach oben) bzw. Down (Nach unten) können Sie durch die MIB-Struktur und die MIB-Teilstrukturen navigieren.

Klicken Sie zum Öffnen der Seite **SNMPv3 View Settings (Einstellungen für SNMPv3-Ansichten)** in der Strukturansicht auf **System→ SNMP→ View Settings**.

Abbildung 6-58. SNMPv3 View Settings (Einstellungen für SNMPv3-Ansichten)



Die Seite **SNMPv3 View Settings (Einstellungen für SNMPv3-Ansichten)** enthält folgende Felder:

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

New Object ID Subtree (Neue Objekt-ID-Teilstruktur) – Gibt die Gerätefunktions-OID an, die in die ausgewählte SNMP-Ansicht einbezogen bzw. aus ihr ausgeschlossen ist.

Select from List (Aus Liste auswählen) – Wählen Sie die Gerätefunktions-OID aus der Liste aus. Mit den Schaltflächen **Up** (Nach oben) und **Down** (Nach unten) können Sie durch eine Liste aller Geräte-OIDs blättern.

Insert (Einfügen) – Geben Sie die Gerätefunktions-OID an.

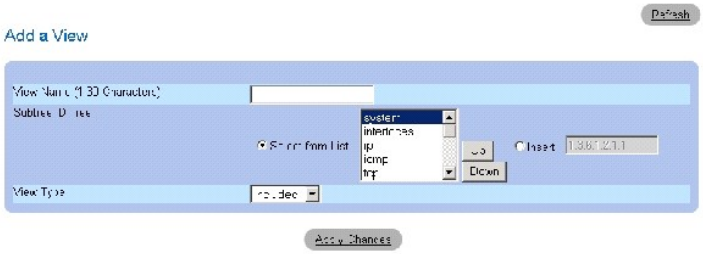
View Type (Ansichtstyp) – Gibt an, ob die definierte OID-Teilstruktur in die ausgewählte SNMP-Ansicht einbezogen (Included) oder aus ihr ausgeschlossen (Excluded) wird.

Hinzufügen einer Ansicht

1. Öffnen Sie die Seite **SNMPv3 View Settings (Einstellungen für SNMPv3-Ansichten)**.
2. Klicken Sie auf Add (Hinzufügen).

Die Seite **Add a View (Ansicht hinzufügen)** wird geöffnet:

Abbildung 6-59. Add a View (Ansicht hinzufügen)



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

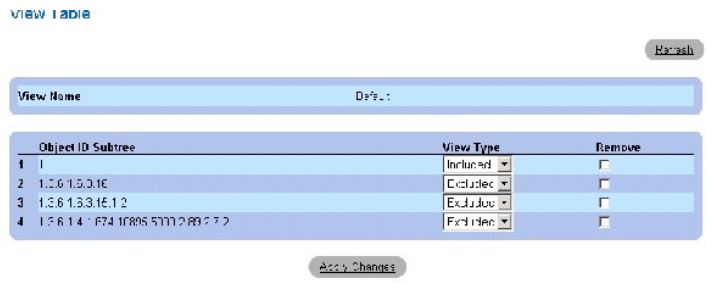
Die SNMP-Ansicht wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der Seite View Table (Tabelle der Ansichten)

1. Öffnen Sie die Seite **SNMPv3 View Settings (Einstellungen für SNMPv3-Ansichten)**.
2. Klicken Sie auf Show All (Alle anzeigen).

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

Abbildung 6-60. View Table (Tabelle der Ansichten)



Definieren von SNMPv3-Ansichten mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **SNMPv3 View Settings (Einstellungen für SNMPv3-Ansichten)** äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-38. CLI-Befehle für SNMP-Ansichten

CLI-Befehl	Beschreibung
snmp-server view *Ansichtsname OID- Struktur* {**included** | **excluded**}	Erstellt oder aktualisiert einen Ansichtseintrag.
show snmp views [*Ansichtsname*]	Zeigt die Konfiguration von Ansichten an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console(config)# snmp-server view user1
1 included
```

```
Console(config)# end

Console# show snmp views
```

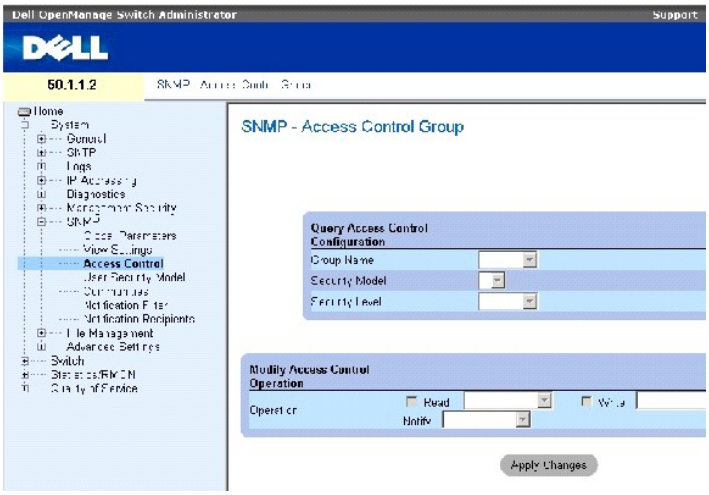
Name	OID Tree	Type
----------	----------	----------
user1	iso	included
Default	iso	included
Default	snmpVacmMIB	excluded
Default	usmUser	excluded
Default	rndCommunityTable	excluded
DefaultSuper	iso	included

Definieren von SNMP-Zugriffsrechten

Die Seite Access Control Group (Zugriffsberechtigungs-Gruppe) enthält Informationen zum Erstellen von SNMP-Gruppen und zum Zuweisen von SNMP-Zugriffsrechten zu SNMP-Gruppen. Mit Hilfe von Gruppen können Netzwerkverwalter Berechtigungen für den Zugriff auf bestimmte Gerätefunktionen oder -teilfunktionen festlegen.

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

Abbildung 6-61. Access Control Group (Zugriffsberechtigungs-Gruppe)



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

Group Name (Gruppenname) – Die benutzerdefinierte Gruppe, für die die Zugriffsregeln gelten. Das Feld darf bis zu 30 Zeichen enthalten.

SNMP Version (SNMP-Version) – Legt die SNMP-Version fest, die der Gruppe zugeordnet ist. Die möglichen Feldwerte lauten:

SNMPv1 – Für die Gruppe ist SNMPv1 festgelegt.

SNMPv2 – Für die Gruppe ist SNMPv2 festgelegt.

SNMPv3 – Für die Gruppe ist SNMPv3 festgelegt.

Security Level (Sicherheitsstufe) – Die der Gruppe zugeordnete Sicherheitsstufe. Sicherheitsstufen können nur bei SNMPv3 zugeordnet werden. Die möglichen Feldwerte lauten:

No Authentication (Keine Authentifizierung) – Der Gruppe ist weder die Sicherheitsstufe Authentication (Authentifizierung) noch die Sicherheitsstufe Privacy (Datenschutz) zugeordnet.

Authentication (Authentifizierung) – Authentifiziert SNMP-Nachrichten und gewährleistet, dass der Ursprung von SNMP-Nachrichten authentifiziert wird.

Privacy (Datenschutz) – Verschlüsselt SNMP-Nachrichten.

Operation (Zugriffsmodus) – Legt die Zugriffsrechte der Gruppe fest. Die möglichen Feldwerte lauten:

Read (Lesezugriff) – Der Verwaltungszugriff ist auf Lesezugriffe beschränkt und es können keine Änderungen an der zugeordneten SNMP-Ansicht vorgenommen werden.

Write (Schreibzugriff) – Verwaltungszugriffe in Form von Lese- und Schreibzugriffen sind zulässig und es können Änderungen an der zugeordneten SNMP-Ansicht vorgenommen werden.

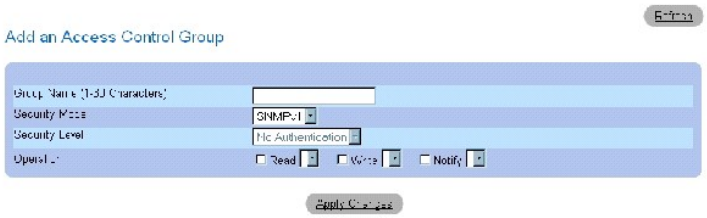
Notify (Benachrichtigen) – Für die zugeordnete SNMP-Ansicht werden Traps versendet.

Definieren von SNMP-Gruppen

1. Öffnen Sie die Seite Access Control Group (Zugriffsberechtigungs-Gruppe).
2. Klicken Sie auf Add (Hinzufügen).

Die Seite **Add an Access Control Group** (Zugriffsberechtigungs-Gruppe hinzufügen) wird geöffnet:

Abbildung 6-62. Add an Access Control Group (Zugriffsberechtigungs-Gruppe hinzufügen)



3. Definieren Sie die Felder der Seite Add an Access Control Group (Zugriffsberechtigungs- Gruppe hinzufügen).
4. Klicken Sie auf Apply Changes (Änderungen übernehmen).

Die Gruppe wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der Seite Access Table (Zugriffstabelle)

1. Öffnen Sie die Seite Access Control Group (Zugriffsberechtigungs-Gruppe).
2. Klicken Sie auf Show All (Alle anzeigen).

Die Seite Access Table (Zugriffstabelle) wird geöffnet:

Abbildung 6-63. Access Table (Zugriffstabelle)

Entfernen von SNMP-Gruppen

1. Öffnen Sie die Seite Access Control Group (Zugriffsberechtigungs-Gruppe).
2. Klicken Sie auf Show All (Alle anzeigen).

Die Seite Access Table (Zugriffstabelle) wird geöffnet.

3. Wählen Sie eine SNMP-Gruppe aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf Apply Changes (Änderungen übernehmen).

Die SNMP-Gruppe wird gelöscht und das Gerät aktualisiert.

Definieren von SNMP-Zugriffsrechten mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite Access Control Group (Zugriffsberechtigungs-Gruppe) äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-39. CLI-Befehle für die SNMP-Zugriffssteuerung

CLI-Befehl	Beschreibung
	Konfiguriert eine neue SNMP-Gruppe (Simple Network Management

snmp-server group *Gruppenname* {**v1	v2	v3** {**noauth**	**auth**	**priv**}} [**read** *Ansicht mit Lesezugriff*] [**write** *Ansicht mit Schreibzugriff*] [**notify** *Ansicht mit Benachrichtigung*]	Protocol) bzw. eine Tabelle für die Zuordnung von SNMP-Benutzern zu SNMP-Ansichten.
show snmp groups [*Gruppenname*]	Zeigt die Konfiguration von Gruppen an.

Im Folgenden ein Beispiel für die CLI-Befehle:

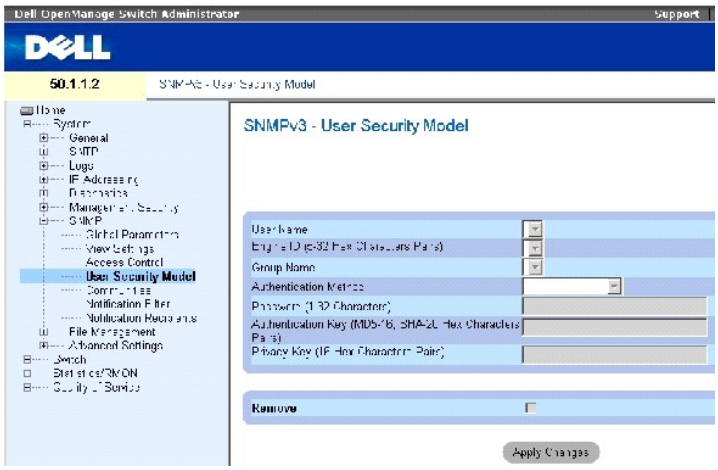
```
console (config)# snmp-
server group user-group v3
priv read user- view
```

Zuweisen der SNMP-Benutzersicherheit

Auf der Seite **SNMPv3 User Security Model (SNMPv3-Benutzersicherheitsmodell)** können Systembenutzer zu SNMP-Gruppen zugewiesen und die Methode für die Benutzerauthentifizierung festlegt werden.

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

Abbildung 6-64. SNMPv3 User Security Model (SNMPv3-Benutzersicherheitsmodell)



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

User Name (Benutzername) – Enthält eine Liste benutzerdefinierter Benutzernamen. Das Feld darf bis zu 30 alphanumerische Zeichen enthalten.

Engine ID – Gibt die lokale oder die Remote-SNMP-Entität an, mit der der Benutzer verbunden ist. Durch das Ändern oder Entfernen der lokalen SNMP-Engine-ID wird die SNMPv3-Benutzerdatenbank gelöscht.

Local (Lokal) – Gibt an, dass der Benutzer mit einer lokalen SNMP-Entität verbunden ist.

Remote – Gibt an, dass der Benutzer mit einer Remote-SNMP-Entität verbunden ist. Wenn die Engine-ID definiert ist, werden Informationsmeldungen an Remote-Geräte gesendet.

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

Authentication Method (Authentifizierungsmethode) – Die für die Authentifizierung von Benutzern verwendete Methode. Die möglichen Feldwerte lauten:

MD5 Key (MD5-Schlüssel) – Die Authentifizierung von Benutzern erfolgt mit Hilfe des Algorithmus HMAC-MD5.

SHA Key (SHA-Schlüssel) – Die Authentifizierung von Benutzern erfolgt mit Hilfe der Authentifizierungsebene HMAC-SHA-96.

MD5 Password (MD5-Kennwort) – Gibt an, dass für die Authentifizierung ein HMAC-MD5-96-Kennwort verwendet wird. Der Benutzer muss ein Kennwort eingeben.

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

None (Keine) – Es erfolgt keine Benutzerauthentifizierung.

Password (0-32 Characters) (Kennwort (0-32 Zeichen)) – Ändert das benutzerdefinierte Kennwort für eine Gruppe. Kennwörter dürfen aus maximal 32 alphanumerischen Zeichen bestehen.

Authentication Key (MD5-16; SHA-20 hexa chars) (Authentifizierungsschlüssel (MD5-16; SHA-20 Hexadezimalzeichenpaare)) – Definiert die Authentifizierungsebene HMAC-MD5-96 bzw. HMAC-SHA-96. Für die Festlegung des Authentifizierungsschlüssels werden der Authentifizierungs- und der Datenschutzschlüssel eingegeben. Wenn nur eine Authentifizierung erforderlich ist, werden für MD5 16 Bytes definiert. Wenn sowohl Datenschutz als auch eine Authentifizierung erforderlich ist, werden für MD5 32 Bytes definiert. Jedes Byte einer hexadezimalen Zeichenkette entspricht zwei Hexadezimalziffern. Die einzelnen Bytes können durch einen Punkt oder einen Doppelpunkt getrennt werden.

Privacy Key (16 hexa characters) (Datenschutzschlüssel (16 Hexadezimalzeichenpaare)) – Wenn nur eine Authentifizierung erforderlich ist, werden 20 Bytes definiert. Wenn sowohl Datenschutz als auch eine Authentifizierung erforderlich ist, werden 16 Bytes definiert. Jedes Byte einer hexadezimalen Zeichenkette entspricht zwei Hexadezimalziffern. Die einzelnen Bytes können durch einen Punkt oder einen Doppelpunkt getrennt werden.

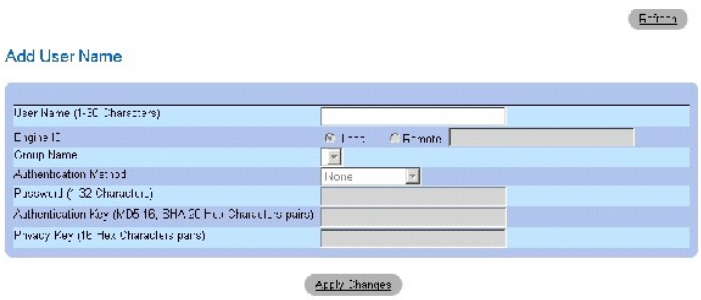
Remove (Entfernen) – Wenn dieses Kontrollkästchen aktiviert ist, werden Benutzer aus der betreffenden Gruppe entfernt.

Hinzufügen von Benutzern zu einer Gruppe

1. Öffnen Sie die Seite SNMPv3 User Security Model (SNMPv3-Benutzersicherheitsmodell).
2. Klicken Sie auf Add (Hinzufügen).

Die Seite Add SNMPv3 User Name (SNMPv3-Benutzername hinzufügen) wird geöffnet:

Abbildung 6-65. Add SNMPv3 User Name (SNMPv3-Benutzername hinzufügen)



3. Definieren Sie die relevanten Felder.

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

Der Benutzer wird zur Gruppe hinzugefügt und das Gerät aktualisiert.

Anzeigen der Seite User Security Model Table (Benutzersicherheitsmodell-Tabelle)

1. Öffnen Sie die Seite **SNMPv3 User Security Model (SNMPv3-Benutzersicherheitsmodell)**.
2. Klicken Sie auf Show All (Alle anzeigen).

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

Abbildung 6-66. User Security Model Table (Benutzersicherheitsmodell-Tabelle)

Löschen eines Eintrags aus der Seite User Security Model Table (Benutzersicherheitsmodell-Tabelle)

1. Öffnen Sie die Seite **SNMPv3 User Security Model (SNMPv3-Benutzersicherheitsmodell)**.
2. Klicken Sie auf Show All (Alle anzeigen).

Die Seite **User Security Model Table (Benutzersicherheitsmodell-Tabelle)** wird geöffnet.

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

Der Eintrag wird aus der Seite **User Security Model Table (Benutzersicherheitsmodell-Tabelle)** gelöscht und das Gerät aktualisiert.

Definieren von SNMPv3-Benutzern mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **SNMPv3 User Security Model (SNMPv3-Benutzersicherheitsmodell)** äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-40. CLI-Befehle für SNMPv3-Benutzer

CLI-Befehl	Beschreibung
snmp-server user *Benutzername Gruppenname* [**remote** Engine-ID- Zeichenkette][**auth-md5** Kennwort | **auth-sha Kennwort** | **auth-md5-key** *MD5-DES-Schlüssel* | **auth- sha-key** *SHA-DES-Schlüssel*]	Konfiguriert einen neuen SNMPv3-Benutzer.
show snmp users [*Benutzername*]	Zeigt die Konfiguration von Benutzern an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console (config)# snmp-
server user John user-
group auth-md5 1234
```

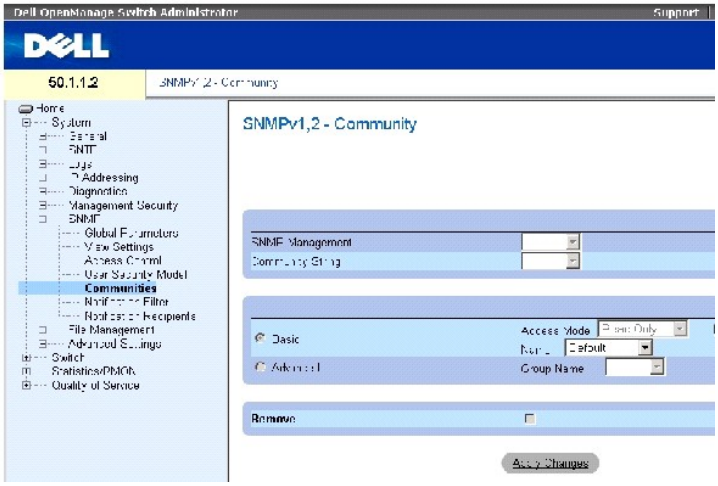
```
console (config)# end

console# show snmp users
```

Name	Group Name	Auth Method	Remote
----------	----------	----------	----------
John	user-group	md5	

Definieren von SNMP-Communitys

Die Verwaltung von Zugriffsrechten erfolgt durch die Festlegung von Communitys auf der Seite **SNMPv1,2 Community**. Sobald der Name einer Community geändert wird, ändern sich auch die Zugriffsrechte. SNMP-Communitys werden nur für SNMPv1 und SNMPv2 definiert. Klicken Sie zum Öffnen der Seite **SNMPv1,2 Community** in der Strukturansicht auf **System→ SNMP→ Communities**.

Abbildung 6-67. SNMPv1,2 Community



Die Seite **SNMPv1,2 Community**enthält folgende Felder:

SNMP Management Station – Die IP-Adresse der Management-Station, für die die SNMP-Community definiert ist.

Community String (Communityzeichenfolge) – Diese Zeichenfolge besitzt die Funktion eines Kennworts und wird zur Authentifizierung der Management-Station gegenüber dem Gerät verwendet.

Basic (Standard) – Aktiviert den SNMP-Modus Basic (Standard) für die ausgewählte Community. Die möglichen Feldwerte lauten:

Access Mode (Zugriffsmodus) – Definiert die Zugriffsrechte der Community. Die möglichen Feldwerte lauten:

Read Only (Nur Lesezugriff) – Der Verwaltungszugriff ist auf Lesezugriffe beschränkt und es können keine Änderungen an der Community vorgenommen werden.

Read-Write (Lese- und Schreibzugriff) – Verwaltungszugriffe in Form von Lese- und Schreibzugriffen sind möglich und es können Änderungen an der Gerätekonfiguration, nicht jedoch an der Community vorgenommen werden.

SNMP-Admin (SNMP-Verwaltung) – Der Benutzer kann auf sämtliche Gerätekonfigurationsoptionen zugreifen und ist berechtigt, die Community zu ändern.

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

Name – Legt den Namen der für SNMPv1,v2 verwendeten Community fest.

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

Group Name (Gruppenname) – Legt den Namen der Gruppe bei Zugriffen im SNMP-Modus Advanced fest.

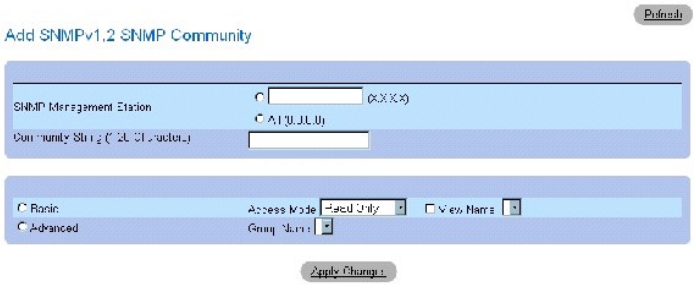
Remove (Entfernen) – Ist dieses Kontrollkästchen aktiviert, wird die betreffende Community entfernt.

Definieren einer neuen Community

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

Die Seite **Add SNMP Community** (SNMP-Community hinzufügen) wird geöffnet:

Abbildung 6-68. Add SNMP Community (SNMP-Community hinzufügen)



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

Die neue Community wird gespeichert und das Gerät aktualisiert.

Löschen von Communitys

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

Die Seite **Community Table (Community-Tabelle)** wird geöffnet.

3. Wählen Sie eine Community aus und aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Community-Eintrag wird gelöscht und das Gerät aktualisiert.

Konfigurieren von Communitys mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **SNMPv1,2 Community** äquivalenten CLI-Befehle zur Anzeige von Feldern zusammengefasst.

Tabelle 6-41. CLI-Befehle für SNMP-Communitys

CLI-Befehl	Beschreibung
snmp-server community *Community* [**ro** | **rw** | **su**] [*IP-Adresse*][**view** *Ansichtsname*]	Konfiguriert die Community-Zugriffszeichenfolge so, dass Zugriffe auf das SNMP-Protokoll zulässig sind.
snmp-server community-group *Community Gruppenname* [*IP-Adresse*]	Konfiguriert die Community-Zugriffszeichenfolge so, dass eingeschränkte Zugriffe auf das SNMP-Protokoll gemäß den Gruppenzugriffsrechten möglich sind.
show snmp	Zeigt die aktuelle SNMP-Gerätekonfiguration an.

Im Folgenden ein Beispiel für die CLI-Befehle:

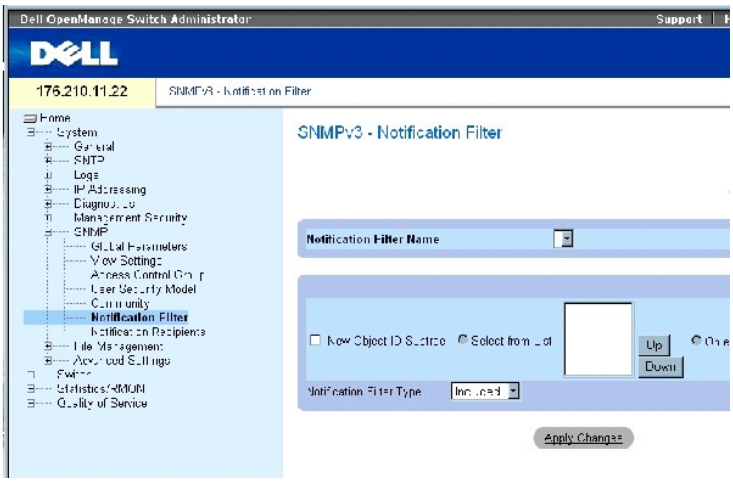
```
Console (config)# snmp-server community dell ro 10.1.1.1
```

Definieren von SNMP-Benachrichtigungsfiltern

Über die Seite **Notification Filter (Benachrichtigungsfilter)** können Traps auf der Grundlage von OIDs gefiltert werden. Jede OID ist mit einer Gerätefunktion oder -teilfunktion verknüpft. Netzwerkverwalter können auf der Seite **Notification Filter (Benachrichtigungsfilter)** außerdem Benachrichtigungen filtern.

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

Abbildung 6-69. Notification Filter (Benachrichtigungsfilter)



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

Notification Filter Name (Name des Benachrichtigungsfilters) – Der benutzerdefinierte Benachrichtigungsfilter.

New Object Identifier Tree (Neue Objekt-ID-Struktur) – Die OID, für die Benachrichtigungen gesendet oder blockiert werden. Wenn ein Filter mit einer OID verknüpft ist, werden Traps oder Informationsmeldungen erzeugt und an die Trap-Empfänger gesendet. Objekt-IDs werden entweder über die Liste *Select from List* (Aus Liste auswählen) oder die Liste *Object ID* (Objekt-ID) ausgewählt.

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

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

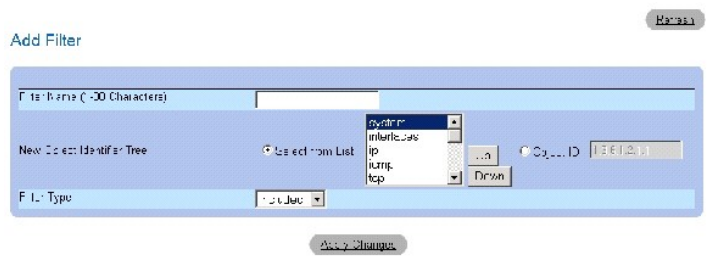
Included (Eingeschlossen) – Aktiviert den Versand von OID-Informationsmeldungen oder -Traps.

Hinzufügen von SNMP-Filtern

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

   Die Seite Add Filter (Filter hinzufügen) wird geöffnet:

Abbildung 6-70. Add Filter (Filter hinzufügen)



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

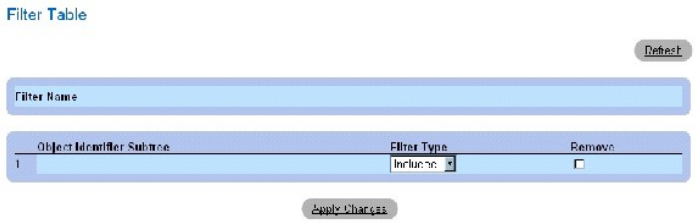
Der neue Filter wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der Seite Filter Table (Filtertabelle)

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

Die Seite **Filter Table (Filtertabelle)** wird geöffnet:

Abbildung 6-71. Filter Table (Filtertabelle)



Entfernen eines Filters

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

Die Seite **Filter Table (Filtertabelle)** wird geöffnet.

3. Wählen Sie einen Eintrag in der Seite **Filter Table (Filtertabelle)** aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).

Der Filtereintrag wird gelöscht und das Gerät aktualisiert.

Konfigurieren von Benachrichtigungsfiltern mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **Notification Filter (Benachrichtigungsfilter)** äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-42. CLI-Befehle für SNMP-Benachrichtigungsfilter

CLI-Befehl	Beschreibung
snmp-server filter Filtername OID- Struktur {**included** | **excluded**}	Erstellt oder aktualisiert einen SNMP-Benachrichtigungsfilter.
show snmp filters [Filtername]	Zeigt die Konfiguration von SNMP-Benachrichtigungsfiltern an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# snmp-server filter user1 iso included
Console(config)# end
```

```
Console # show snmp filters

Name        OID Tree      Type
----------  ------------  --------
user1       iso           Included
```

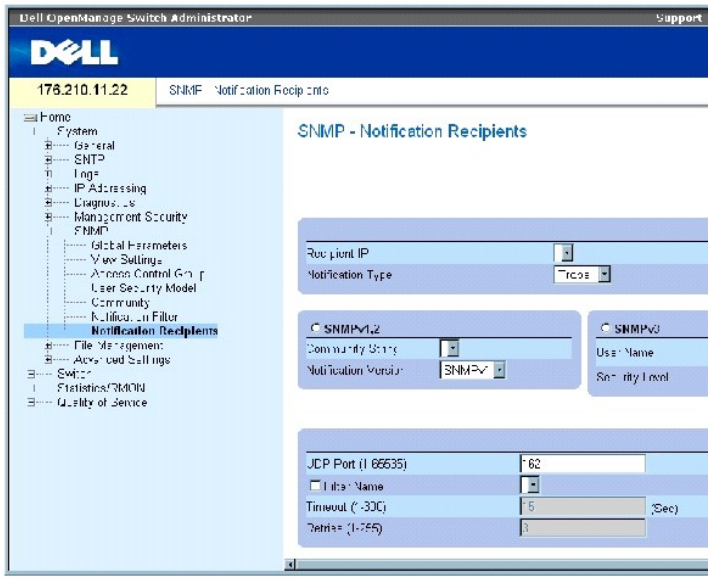
Definieren von SNMP-Benachrichtigungsempfängern

Die Seite **Notification Recipients (Benachrichtigungsempfänger)** enthält Informationen zum Definieren von Filtern. Die Filter legen fest, ob Traps an bestimmte Benutzer gesendet werden und welcher Trap-Typ gesendet wird. SNMP-Benachrichtigungsfilter stellen folgende Funktionen bereit:

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

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

Abbildung 6-72. Notification Recipients (Benachrichtigungsempfänger)



Die Seite **Notification Recipients (Benachrichtigungsempfänger)** enthält folgende Felder:

Recipient IP (Empfänger-IP) – Gibt die IP-Adresse des Empfängers an, an den die Traps gesendet werden.

Notification Type (Benachrichtigungstyp) – Der Typ der zu sendenden Benachrichtigung. Die möglichen Feldwerte lauten:

Trap – Es werden Traps gesendet.

Inform – Es werden Informationsmeldungen gesendet.

SNMPv1,2 – Für den ausgewählten Empfänger sind die SNMP-Versionen 1 und 2 aktiviert. Definieren Sie die folgenden Felder für SNMPv1 und SNMPv2:

Community String (1-20 Characters) (Communityzeichenfolge (1-20 Zeichen)) – Gibt die Communityzeichenfolge des Trap Managers an.

Notification Version (Benachrichtigungsversion) – Legt den Trap-Typ fest. Die möglichen Feldwerte lauten:

SNMP V1 – Es werden Traps der SNMP-Version 1 gesendet.

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

SNMPv3 – Für den Versand und Empfang von Traps wird SNMPv3 verwendet. Definieren Sie die folgenden Felder für SNMPv3:

User Name (Benutzername) – Der Benutzer, an den SNMP-Benachrichtigungen gesendet werden.

Security Level (Sicherheitsstufe) – Legt die Methode für die Authentifizierung des Pakets fest. Die möglichen Feldwerte lauten:

No Authentication (Keine Authentifizierung) – Das Paket wird weder authentifiziert noch verschlüsselt.

Authentication (Authentifizierung) – Das Paket wird authentifiziert.

Privacy (Datenschutz) – Das Paket wird sowohl authentifiziert als auch verschlüsselt.

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

Filter Name (Filtername) – Dient zum Einbeziehen oder Ausschließen von SNMP-Filtern.

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

Retries (1-255) (Wiederholungsversuche (1-255)) – Gibt an, wie oft das Gerät eine Anforderung zum Senden einer Informationsmeldung wiederholt. Der Standardwert lautet 3.

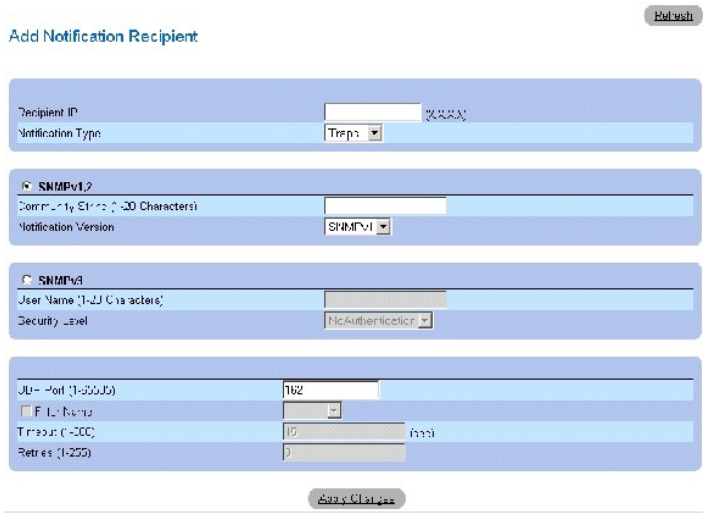
Remove Notification Recipient (Benachrichtigungsempfänger entfernen) – Ist dieses Kontrollkästchen aktiviert, werden die ausgewählten Benachrichtigungsempfänger entfernt.

Hinzufügen eines neuen Trap-Empfängers

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

Die Seite **Add Notification Recipients (Benachrichtigungsempfänger hinzufügen)** wird geöffnet:

Abbildung 6-73. Add Notification Recipients (Benachrichtigungsempfänger hinzufügen)



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

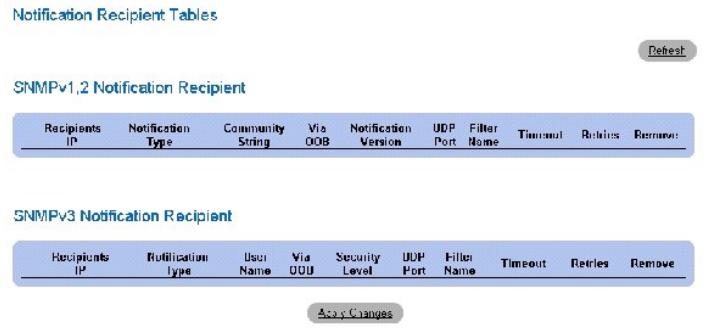
Der Benachrichtigungsempfänger wird hinzugefügt und das Gerät aktualisiert.

Anzeigen der Seite Notification Recipients Tables (Benachrichtigungsempfänger-Tabellen)

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

Die Seite **Notification Recipients Tables (Benachrichtigungsempfänger-Tabellen)** wird **geöffnet:**

Abbildung 6-74. Notification Recipients Tables (Benachrichtigungsempfänger-Tabellen)



Löschen von Benachrichtigungsempfängern

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

Die Seite **Notification Recipients Tables (Benachrichtigungsempfänger-Tabellen)** wird geöffnet.

3. Wählen Sie in der Tabelle **SNMPv1,2 Notification Recipient** oder in der Tabelle **SNMPv3 Notification Recipient** einen Benachrichtigungsempfänger aus.
4. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
5. Klicken Sie auf Apply Changes (Änderungen übernehmen).

Der Empfänger wird gelöscht und das Gerät aktualisiert.

Konfigurieren von SNMP-Benachrichtigungsempfängern mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **Notification Recipients (Benachrichtigungsempfänger)** äquivalenten CLI-Befehle zur Anzeige von Feldern zusammengefasst.

Tabelle 6-43. CLI-Befehle für SNMP-Benachrichtigungsempfänger

CLI-Befehl	Beschreibung
snmp-server host {IP-Adresse | Hostname} *Communityzeichenfolge* [**traps** | **informs**] [**1** | **2**] [**udp-port** Port] [**filter** Filtername] [**timeout** Sekunden] [**retries** Wiederholungsversuche]	Erstellt oder aktualisiert einen Benachrichtigungsempfänger, an den Benachrichtigungen der SNMP-Versionen 1 oder 2 gesendet werden.
snmp-server v3-host {IP-Adresse | Hostname} *Benutzername* [**traps** | **informs**] {**noauth** | **auth** | **priv**} [**udp-port** *Port*] [**filter** Filtername] [**timeout** Sekunden] [**retries** Wiederholungsversuche]	Erstellt oder aktualisiert einen Benachrichtigungsempfänger, an den Benachrichtigungen der SNMP-Version 3 gesendet werden.
show snmp	Zeigt die aktuelle SNMP-Konfiguration an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# snmp-server host 172.16.1.1
private

console(config)# end

console# show snmp
```

Community-String	Community-Access	View name	IP address
---	---	---	---
public	read only	user-view	All
private	read write	default	172.16.1.1
private	su	DefaultSuper	172.17.1.1

Verwalten von Dateien

Über die Seite **File Management (Dateiverwaltung)** können Sie Gerätesoftware, die Image-Dateien und die Konfigurationsdateien verwalten. Die Dateien können über einen TFTP-Server herunter- oder hochgeladen werden.

Übersicht über die Dateiverwaltung

Die Verwaltungsdateistruktur umfasst die folgenden Dateien:

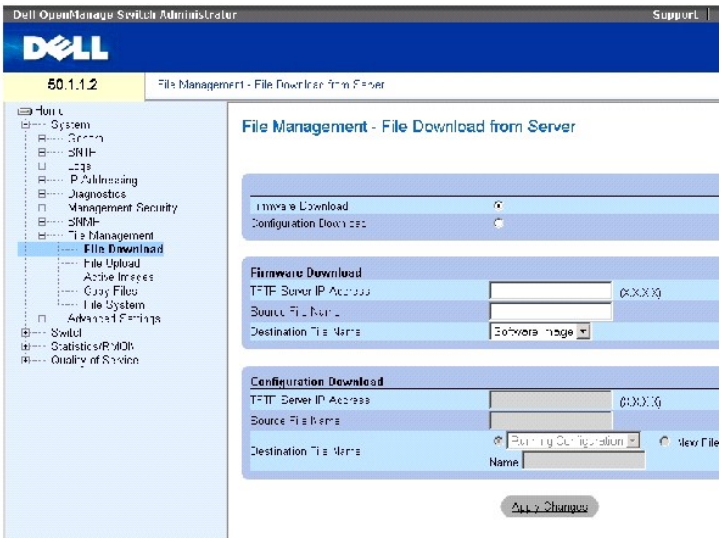
- Datei Startup Configuration (Startkonfiguration) – Enthält die erforderlichen Befehle zum Konfigurieren des Gerätes während des Starts oder nach einem Neustart. Die Datei Startup Configuration wird erstellt, indem die Konfigurationsbefehle aus der Datei Running Configuration (Aktive Konfiguration) oder der Datei Backup Configuration (Sicherungskopie der Konfiguration) in die Datei Startup Configuration kopiert werden.
- Datei Running Configuration (Aktive Konfiguration) – Enthält alle Befehle aus der Datei Startup Configuration sowie alle während der aktuellen Sitzung eingegebenen Befehle. Nach dem Ausschalten oder Neustart des Gerätes werden alle in der Datei Running Configuration gespeicherten Befehle gelöscht. Während des Startvorgangs werden alle Befehle aus der Datei Startup Configuration in die Datei Running Configuration kopiert und auf das Gerät angewendet. Während der Sitzung werden alle neuen Befehle zu den bereits in der Datei Running Configuration enthaltenen Befehlen hinzugefügt. Um die Datei Startup Configuration zu aktualisieren, muss die Datei Running Configuration vor dem Ausschalten des Gerätes in die Datei Startup Configuration kopiert werden.
- Datei Backup Configuration (Sicherungskopie der Konfiguration) – Enthält eine Sicherungskopie der Gerätekonfiguration. Es können bis zu fünf Sicherungskopien von Gerätekonfigurationen unter benutzerdefinierten Namen auf dem Gerät gespeichert werden. Diese Dateien werden erstellt, wenn der Benutzer die Datei Running Configuration oder Startup Configuration in eine Datei mit einem benutzerdefinierten Namen kopiert. Der Inhalt von Sicherungskopien der Gerätekonfiguration kann sowohl in die Datei Running Configuration als auch in die Datei Startup Configuration kopiert werden.
- Image-Dateien – Systemdatei-Images werden in zwei Flash-Dateien mit den Namen Image 1 und Image 2 gespeichert. Im aktiven Image ist 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.

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

Herunterladen von Dateien

Die Seite **File Download from Server (Dateien vom Server herunterladen)** enthält Felder zum Herunterladen von System-Image- und Konfigurationsdateien vom TFTP-Server auf das Gerät. Klicken Sie zum Öffnen der Seite **File Download from Server (Dateien vom Server herunterladen)** in der Strukturansicht auf System→ File Management→ File Download.

Abbildung 6-75. File Download from Server (Dateien vom Server herunterladen)



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

Firmware Download (Firmware herunterladen) – Die Firmware-Datei wird heruntergeladen. Bei Auswahl von **Firmware Download** werden die Felder unter **Configuration Download** (Konfiguration herunterladen) grau dargestellt.

Configuration Download (Konfiguration herunterladen) – Die Konfigurationsdatei wird heruntergeladen. Bei Auswahl von **Configuration Download** werden die Felder unter **Firmware Download** (Firmware herunterladen) grau dargestellt.

Firmware Download (Firmware herunterladen)

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

Source File Name (Name der Quelldatei) – Gibt die herunterzuladende Datei an.

Destination File Name (Name der Zieldatei) – Der Typ der Zieldatei, in die die Datei heruntergeladen wird. Die möglichen Feldwerte lauten:

Software Image (Software-Image) – Lädt die Image-Datei herunter.

Boot Code (Startcode) – Lädt die Startdatei herunter.

Configuration Download (Konfiguration herunterladen)

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

Source File Name (Name der Quelldatei) – Gibt die herunterzuladenden Konfigurationsdateien an.

Destination File Name (Name der Zieldatei) – Die Zieldatei, in die die Konfigurationsdatei heruntergeladen wird. Die möglichen Feldwerte lauten:

Running Configuration (Aktive Konfiguration) – Lädt Befehle in die Datei Running Configuration herunter.

Startup Configuration (Startkonfiguration) – Lädt die Datei Startup Configuration herunter und überschreibt die alte Datei.

User Defined Backup Configuration (Benutzerdefinierte Sicherung der Konfiguration) – Lädt die benutzerdefinierte Datei Backup Configuration herunter und überschreibt die alte Datei.

New File Name (Neuer Dateiname) – Lädt eine neue Sicherungskopie der Konfiguration herunter, die als Zieldatei angegeben werden kann.

ANMERKUNG: Die Image-Datei überschreibt das nicht aktive Image. Es wird empfohlen, für das nicht aktive Image festzulegen, dass es nach einem Zurücksetzen des Gerätes als aktives Image verwendet wird. Nach dem Herunterladen der Datei sollte dann das Gerät zurückgesetzt werden.

Während des Herunterladens der Image-Datei wird in einem Dialogfeld der Fortschritt beim Herunterladen angezeigt. Nach dem Herunterladen der Datei wird das Fenster automatisch geschlossen.

Herunterladen von Dateien

1. Öffnen Sie die Seite **File Download from Server (Dateien vom Server herunterladen)**.
2. Wählen Sie den Typ der herunterzuladenden Datei aus.
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 **Umschalten zwischen Stack- Mastereinheiten**.

Herunterladen von Dateien mit Hilfe der CLI-Befehle

In der folgenden Tabelle wird der der Seite **File Download from Server (Dateien vom Server herunterladen)** äquivalente CLI-Befehl zur Festlegung von Feldern zusammengefasst.

Tabelle 6-44. CLI-Befehl zum Herunterladen von Dateien

CLI-Befehl	Beschreibung
copy Quell-URL Ziel-URL	Kopiert eine beliebige Datei von einem Quellort an einen Zielort.

Im Folgenden ein Beispiel für die CLI-Befehle:

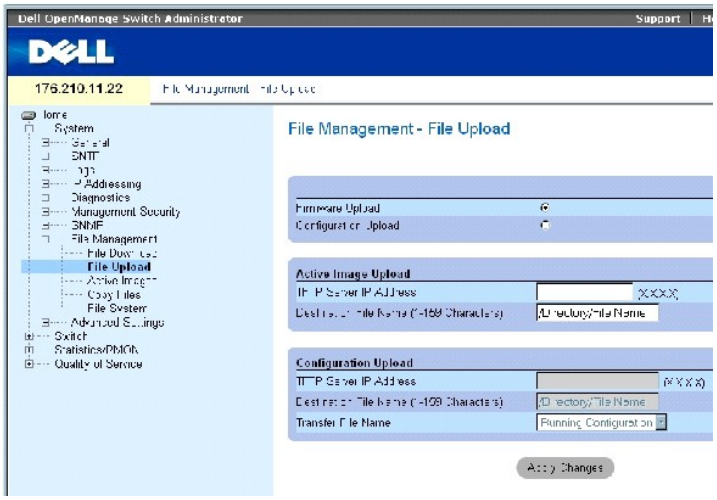
```
console# copy
tftp://10.6.6.64/pp.txt
startup-config



....!



Copy: 575 bytes copied in
00:00:06 [hh:mm:ss]



01-Jan-2000 06:41:55 %
COPY-W-TRAP: The copy
operation was completed
successfully
```

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

Hochladen von Dateien

Die Seite **File Upload to Server (Dateien auf den Server hochladen)** enthält Felder zum Hochladen der Software vom Gerät auf den TFTP-Server. Auch die Image-Datei kann über die Seite **File Upload to Server (Dateien auf den Server hochladen)** hochgeladen werden. Klicken Sie zum Öffnen der Seite **File Upload to Server (Dateien auf den Server hochladen)** in der Strukturansicht auf System→ File Management→ File Upload.

Abbildung 6-76. File Upload to Server (Dateien auf den Server hochladen)



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

Firmware Upload (Firmware hochladen) – Die Firmware-Datei wird hochgeladen. Bei Auswahl von **Firmware Upload** sind die Felder unter **Configuration Upload** (Konfiguration hochladen) nicht verfügbar.

Configuration Upload (Konfiguration hochladen) – Die Konfigurationsdatei wird hochgeladen. Bei Auswahl von **Configuration Upload** sind die Felder unter **Active Image Upload** (Aktives Image hochladen) nicht verfügbar.

Active Image Upload (Aktives Image hochladen)

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

Destination File Name (1-159 Characters) (Name der Zieldatei (1-159 Zeichen)) – Gibt den Dateipfad an, auf den das Software-Image hochgeladen wird.

Configuration Upload (Konfiguration hochladen)

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

Destination File Name (1-159 Characters) (Name der Zieldatei (1-159 Zeichen)) – Gibt den Dateipfad an, auf den die Konfigurationsdatei hochgeladen wird.

Transfer File Name (Name der zu übertragenden Datei) – Die Softwaredatei, in die die Konfiguration hochgeladen wird. Die möglichen Feldwerte lauten:

Running Configuration (Aktive Konfiguration) – Lädt die Datei Running Configuration hoch.

Startup Configuration (Startkonfiguration) – Lädt die Datei Startup Configuration hoch.

List of User Defined Configuration Files (Liste benutzerdefinierter Konfigurationsdateien) – Lädt eine benutzerdefinierte Konfigurationsdatei hoch.

ANMERKUNG: Die Liste der benutzerdefinierten Konfigurationsdateien erscheint nur, wenn vom Benutzer zuvor Sicherungskopien von Konfigurationsdateien erstellt wurden. Wenn beispielsweise die Datei Running Configuration vom Benutzer in eine benutzerdefinierte Konfigurationsdatei mit dem Namen BACKUP-STANDORT-1 kopiert wurde, erscheint die Liste auf der Seite **File Upload to Server (Dateien auf den Server hochladen)** und die Konfigurationsdatei BACKUP-STANDORT-1 ist in der Liste enthalten.

Hochladen von Dateien

1. Öffnen Sie die Seite **File Upload to Server (Dateien auf den Server hochladen)**.
2. Wählen Sie den Typ der hochzuladenden Datei aus.
3. Definieren Sie die Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Software wird auf den TFTP-Server hochgeladen.

Hochladen von Dateien mit Hilfe der CLI-Befehle

In der folgenden Tabelle wird der der Seite **File Upload to Server (Dateien auf den Server hochladen)** äquivalente CLI-Befehl zur Festlegung von Feldern zusammengefasst.

Tabelle 6-45. CLI-Befehl zum Hochladen von Dateien

CLI-Befehl	Beschreibung
copy Quell-URL Ziel-URL	Kopiert eine beliebige Datei von einem Quellort an einen Zielort.

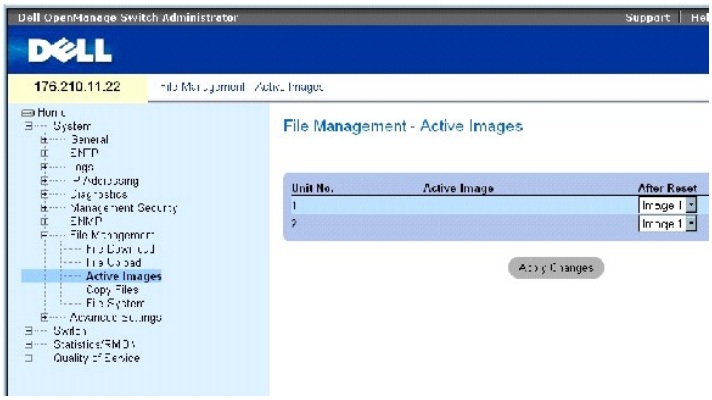
Im Folgenden ein Beispiel für die CLI-Befehle:

```
console# copy image tftp://10.6.6.64/uploaded.ros

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

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

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

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

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

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

Copy: 4234656 bytes copied in 00:00:33 [hh:mm:ss]

01-Jan-2000 07:30:42 %COPY-W-TRAP: The copy operation was
completed successfully
```

Aktivieren von Image-Dateien

Auf der Seite **Active Images (Aktive Image-Dateien)** können Netzwerkverwalter Image-Dateien auswählen und zurücksetzen. Für jede Einheit in einer Stack-Konfiguration kann die aktive Image-Datei individuell ausgewählt werden. Klicken Sie zum Öffnen der Seite **Active Images (Aktive Image-Dateien)** in der Strukturansicht auf System→ File Management→ Active Images.

Abbildung 6-77. Active Images (Aktive Image-Dateien)



Die Seite **Active Images (Aktive Image-Dateien)** enthält folgende Felder:

Unit No. (Einheit-Nr.) – Die Nummer der Einheit, für die die Image-Datei ausgewählt wird.

Active Image (Aktives Image) – Die derzeit auf der Einheit aktive Image-Datei.

After Reset (Nach Zurücksetzen) – Die Image-Datei, die nach dem Zurücksetzen des Gerätes auf der Einheit aktiv sein wird. Die möglichen Feldwerte lauten:

Image 1 – Aktiviert nach dem Zurücksetzen des Gerätes die Image-Datei 1.

Image 2 – Aktiviert nach dem Zurücksetzen des Gerätes die Image-Datei 2.

Auswählen einer Image-Datei

1. Öffnen Sie die Seite **Active Images (Aktive Image-Dateien)**.
2. Wählen Sie für die betreffende Einheit im Feld **After Reset** (Nach Zurücksetzen) eine Image-Datei aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Image-Datei wird ausgewählt. Die Image-Datei wird erst nach dem nächsten Zurücksetzen neu geladen. Die derzeit ausgewählte Image-Datei wird so lange ausgeführt, bis das Gerät das nächste Mal zurückgesetzt wird.

Verwalten der aktiven Image-Datei mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **Active Images (Aktive Image-Dateien)** äquivalenten CLI-Befehle zur Anzeige von Feldern zusammengefasst.

Tabelle 6-46. CLI-Befehle zum Hochladen von Dateien

CLI-Befehl	Beschreibung
boot system [**unit** | *Einheit*] {**image-1** | **image-2**}	Gibt das System-Image an, das beim Start vom Gerät geladen wird.
show version [**unit** *Einheit*]	Zeigt Versionsinformationen zum System an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console# boot system
image-1
```

Kopieren von Dateien

Dateien können über die Seite **Copy Files (Dateien kopieren)** kopiert und gelöscht werden. Klicken Sie zum Öffnen der Seite **Copy Files (Dateien kopieren)** in der Strukturansicht auf System→ File Management→ Copy Files.

Abbildung 6-78. Copy Files (Dateien kopieren)

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

Copy Configuration (Konfiguration kopieren) – Wenn diese Option aktiviert ist, wird die Datei Running Configuration, Startup Configuration oder Backup Configuration der Mastereinheit in die Zieldatei kopiert.

Source (Quelldatei) – Gibt den Typ der Datei an, die in die Zieldatei kopiert werden soll. Wählen Sie die Datei Running Configuration, Startup Configuration oder eine der benutzerdefinierten Sicherungskopien von Konfigurationsdateien (Backup Configuration) aus.

Destination (Zieldatei) – Gibt die Zielkonfigurationsdatei an, in die die Quelldatei kopiert wird. Dateien können nicht in die Sicherungskopie der Mastersicherungseinheit kopiert werden. Im Feld **Destination Unit** (Zieleinheit) werden nur dann Sicherungskopien angezeigt, wenn diese zuvor definiert wurden. Aktivieren Sie das Kontrollkästchen New File Name (Neuer Dateiname) und geben Sie den Namen einer neuen Datei an, um die Quelldatei in eine neue Sicherungskopie der Konfigurationsdatei zu kopieren.

New File Name (Neuer Dateiname) – Gibt den Namen der neu erstellten Sicherungskopie der Konfigurationsdatei an.

Restore Configuration Factory Defaults (Werkseitige Konfigurationseinstellungen wiederherstellen) – Die Aktivierung dieses Kontrollkästchens gibt an, dass die aktuellen Konfigurationseinstellungen auf die werkseitigen Standard-Konfigurationseinstellungen zurückgesetzt werden sollen. Ist das Kontrollkästchen deaktiviert, werden die aktuellen Konfigurationseinstellungen beibehalten.

Kopieren von Dateien

1. Öffnen Sie die Seite **Copy Files (Dateien kopieren)**.
2. Definieren Sie die Felder **Source** (Quelldatei) und **Destination** (Zieldatei).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Datei wird kopiert und das Gerät aktualisiert.

Wiederherstellen der werkseitigen Standardeinstellungen

1. Öffnen Sie die Seite **Copy Files (Dateien kopieren)**.
2. Klicken Sie auf **Restore Configuration Factory Defaults** (Werkseitige Konfigurationseinstellungen wiederherstellen).
3. Klicken Sie auf Apply Changes (Änderungen übernehmen).

Die werkseitigen Standardeinstellungen werden wiederhergestellt und das Gerät aktualisiert.

Kopieren und Löschen von Dateien mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **Copy Files (Dateien kopieren)** äquivalenten CLI-Befehle zur Festlegung von Feldern zusammengefasst.

Tabelle 6-47. CLI-Befehle zum Kopieren und Löschen von Dateien

CLI-Befehl	Beschreibung
copy *Quell-URL Ziel-URL*	Kopiert eine beliebige Datei von einem Quellort an einen Zielort.
delete startup-config	Löscht die Datei Startup Configuration (Startkonfiguration).

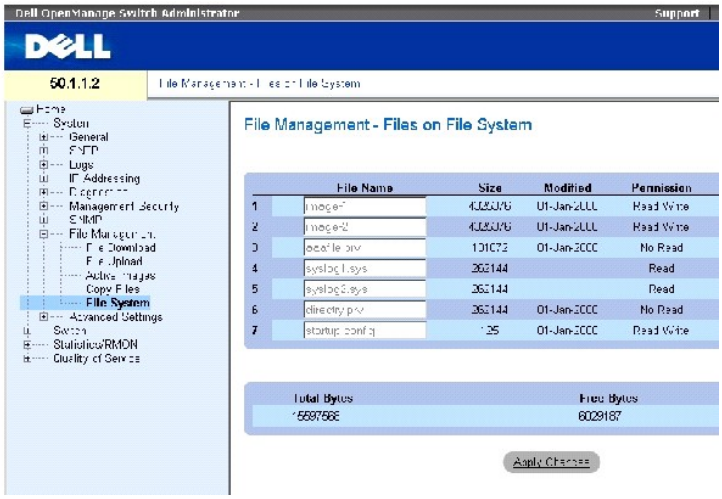
Im Folgenden ein Beispiel für die CLI-Befehle:

```
console# delete startup-
config


Startup file was deleted


console#


console# copy running-
config startup-config


01-Jan-2000 06:55:32 %
COPY-W-TRAP: The copy
operation was completed
successfully


Copy succeeded


console#
```

Verwalten von Gerätedateien

Die Seite Files on File System (Dateien im Dateisystem) enthält Informationen über aktuell auf dem System gespeicherte Dateien, einschließlich Name und Größe der Dateien, Datum der letzten Änderung und Dateiberechtigungen. Das Dateisystem unterstützt die Verwaltung von bis zu fünf Dateien und einer Gesamtdateigröße von 3 MB. Klicken Sie zum Öffnen der Seite Files on File System (Dateien im Dateisystem) in der Strukturansicht auf System→ File Management→ File System.

Abbildung 6-79. Files on File System (Dateien im Dateisystem)



Die Seite Files on File System (Dateien im Dateisystem) enthält folgende Felder:

File Name (Dateiname) – Gibt den Namen einer aktuell im Dateiverwaltungssystem gespeicherten Datei an.

Size (Größe) – Gibt die Dateigröße an.

Modified (Geändert) – Gibt das Datum der letzten Änderung der Datei an.

Permission (Berechtigung) – Gibt den der Datei zugewiesenen Berechtigungstyp an. Die möglichen Feldwerte lauten:

Read Only (Schreibgeschützt) – Die Datei ist schreibgeschützt.

Read Write (Lese-/Schreibzugriff) – Für die Datei ist Lese-/Schreibberechtigung festgelegt.

Remove (Entfernen) – Ist diese Option aktiviert, wird die Datei gelöscht.

Rename (Umbenennen) – Ermöglicht die Umbenennung der Datei. Die Umbenennung der Datei erfolgt im Feld **File Name** (Dateiname).

Total Bytes (Bytes insgesamt) – Gibt den gesamten aktuell belegten Speicherplatz an.

Free Bytes (Bytes frei) – Gibt den aktuell verbleibenden freien Speicherplatz an.

Verwalten von Dateien mit Hilfe der CLI-Befehle

In der folgenden Tabelle wird der äquivalente CLI-Befehl zum Verwalten von Systemdateien zusammengefasst.

Tabelle 6-48. CLI-Befehl zum Kopieren von Dateien

CLI-Befehl	Beschreibung
dir	Zeigt eine Liste der Dateien in einem Flash-Dateisystem an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console# dir

Directory of flash:

File Name        Permis-  Flash   Data    Modified
                 sion     Size    Size
---------------  ------   ------  ------  ------------------
3.txt            rw       524288  523776  22-Feb-2005 18:49:27
setup            rw       524288  95      22-Feb-2005 15:58:19
setup2           rw       524288  95      22-Feb-2005 15:58:35
image-1          rw       4325376 4325376 06-Feb-2005 17:55:32
image-2          rw       4325376 4325376 06-Feb-2005 17:55:31
test.txt         rw       524288  95      22-Feb-2005 12:16:44
aaafile.prv      --       131072  --      06-Feb-2005 19:09:02
syslog1.sys      r-       262144  --      22-Feb-2005 18:49:27
syslog2.sys      r-       262144  --      22-Feb-2005 18:49:27
directory.prv    --       262144  --      06-Feb-2005 17:55:31
startup-config   rw       524288  347     22-Feb-2005 11:56:03
```

```
Total size of flash: 16646144 bytes

Free size of flash: 4456448 bytes
```

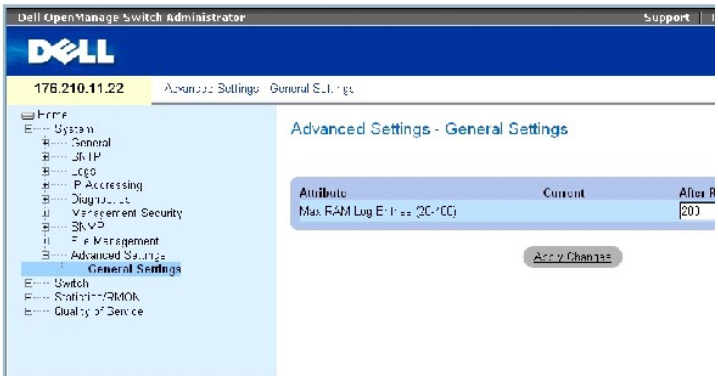
Konfigurieren allgemeiner Einstellungen

Auf der Seite **Advanced Settings (Erweiterte Einstellungen)** können Sie verschiedene globale Attribute für den Switch festlegen. Änderungen an diesen Attributen werden erst nach dem Zurücksetzen des Switches wirksam. Klicken Sie zum Öffnen der Seite **Advanced Settings** in der Strukturansicht auf **System→ Advanced Settings**.

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

Die Seite **General Settings (Allgemeine Einstellungen)** enthält Informationen zum Definieren allgemeiner Geräteparameter. Klicken Sie zum Öffnen der Seite **General Settings (Allgemeine Einstellungen)** in der Strukturansicht auf System→ Advanced Settings→ General Settings.

Abbildung 6-80. General Settings (Allgemeine Einstellungen)



Die Seite **General Settings (Allgemeine Einstellungen)** enthält folgende Informationen:

Attribute (Attribut) – Das Attribut der allgemeinen Einstellung.

Current (Aktuell) – Der aktuell konfigurierte Wert.

After Reset (Nach Zurücksetzen) – Der künftige Wert (nach dem Zurücksetzen). Durch Eingabe eines Wertes in die Spalte After Reset wird der Feldtabelle Arbeitsspeicher zugewiesen.

Max RAM Log Entries (20-400) (Maximale Anzahl von RAM-Protokolleinträgen (20-400)) – Die maximale Anzahl von RAM-Protokolleinträgen. Sobald die maximale Anzahl von Protokolleinträgen erreicht ist, wird der Protokollinhalt gelöscht und die Erfassung neu gestartet.

Anzeigen des Zählers für RAM-Protokolleinträge mit Hilfe der CLI-Befehle

In der folgenden Tabelle wird der der Seite **General Settings (Allgemeine Einstellungen)** äquivalente CLI-Befehl zur Festlegung von Feldern zusammengefasst.

Tabelle 6-49. CLI-Befehl für allgemeine Einstellungen

CLI-Befehl	Beschreibung
logging buffered size Anzahl	Legt die Anzahl der im internen Pufferspeicher (RAM) gespeicherten Syslog-Meldungen fest.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# logging
buffered size 300
```

Zurück zum Inhalt

Zurück zum Inhalt

Konfigurieren von Switch-Informationen

Dell™ PowerConnect™ 34XX- Systeme Benutzerhandbuch

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

Konfigurieren der Netzwerksicherheit

Verwenden Sie die Seite **Network Security**, um über ACLs und Locked Ports (gesperrte Ports) die Netzwerksicherheit einzurichten. So öffnen Sie die Seite **Network Security**: Wählen Sie: **Switch** → **Network Security**.

Portbasierte Authentifizierung

Bei der portbasierten Authentifizierung können Systembenutzer auf Basis einzelner Ports über einen externen Server authentifiziert werden. Nur authentifizierte und zugelassene Systembenutzer können Daten senden und empfangen. Zur Authentifizierung von Ports über den RADIUS-Server kommt das erweiterbare Authentifizierungsprotokoll (EAP) zum Einsatz. An der portbasierten Authentifizierung sind beteiligt:

- **Authentifizierer** – Bezeichnet den Geräteport, der authentifiziert wird, bevor der Zugriff auf das System zugelassen wird.
- **Bittsteller** – Bezeichnet den Host, der an den authentifizierten Port angeschlossen ist und den Zugriff auf die Dienste des Systems anfordert.
- **Authentifizierungsserver** – Bezeichnet den externen Server, beispielsweise einen RADIUS-Server, der im Namen des Authentifizierers die Authentifizierung durchführt und anzeigt, ob der Bittsteller zum Zugriff auf die Dienste des Systems berechtigt ist.

Bei portbasierter Authentifizierung existieren zwei Zugriffszustände:

- **Controlled Access** (Kontrollierter Zugriff) – Lässt die Kommunikation zwischen Bittsteller und System nur dann zu, wenn der Bittsteller autorisiert ist.
- **Uncontrolled Access** (Unkontrollierter Zugriff) – Unabhängig vom Portzustand wird unkontrollierte Kommunikation zugelassen.

Derzeit unterstützt das Gerät die portbasierte Authentifizierung über RADIUS-Server.

Erweiterte portbasierte Authentifizierung

Bei der erweiterten portbasierten Authentifizierung:

- können mehrere Hosts an einen einzelnen Port angeschlossen werden,
- muss lediglich ein Host autorisiert werden, um allen Hosts Zugriff auf das System zu verschaffen, und wenn der Port nicht autorisiert ist, wird allen angeschlossenen Hosts der Zugriff auf das Netzwerk verweigert,
- kann die Authentifizierung auf Benutzerbasis erfolgen. Bestimmte VLANs des Geräts sind immer verfügbar, selbst wenn bestimmte, dem VLAN zugeordnete Ports nicht autorisiert sind.
    - Zum Beispiel erfordert Voice-over-IP keine Authentifizierung, während Datenverkehr eine Authentifizierung erfordert. Es können VLANs definiert werden, für die keine Auto-ri-sie-rung erforderlich ist. VLANs ohne Authentifizierung stehen den Benutzern selbst dann zur Verfügung, wenn die dem VLAN zugeordneten Ports als autorisierte Ports definiert sind.

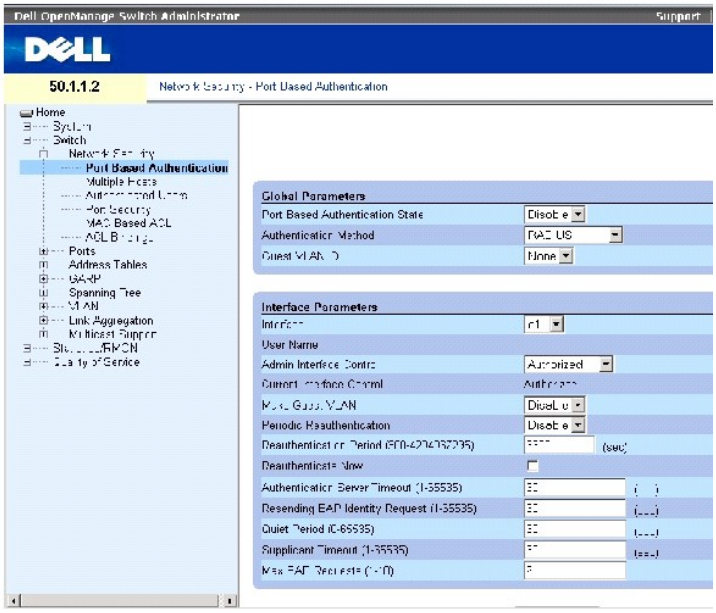
Die erweiterte portbasierte Authentifizierung ist in folgenden Modi implementiert:

- **Single Host Mode** (Einzelhostmodus) – Nur der autorisierte Host kann auf den Port zugreifen.
- **Multiple Host Mode** (Multihostmodus) – An einen einzelnen Port können mehrere Hosts angeschlossen werden. Lediglich ein Host muss autorisiert werden, um allen Hosts Zugriff auf das Netzwerk zu gewähren. Wenn die Authentifizierung des Hosts fehlschlägt oder eine EAPOL-Abmeldenachricht empfangen wird, wird allen angeschlossenen Clients der Zugriff auf das Netzwerk verweigert.
- **Guest VLANs** (Gast-VLAN-Modus) – Gewährt Ports den eingeschränkten autorisierten Zugriff auf das Netzwerk. Wenn einem Port bei der portbasierten Autorisierung der Netzwerkzugriff verweigert wird, jedoch das Gast-VLAN aktiviert ist, so erhält der Port eingeschränkten Zugriff auf das Netzwerk. Ein Netzwerkadministrator kann Gast-VLANs z. B. verwenden, um nicht autorisierten Benutzern über portbasierte Authentifizierung den Zugriff auf das Netzwerk zu verweigern, ihnen jedoch Zugriff aufs Internet zu gewähren.

Konfigurieren der portbasierten Authentifizierung

Auf der Seite Port Based Authentication (Portbasierte Authentifizierung) können Netzwerkverwalter die portbasierte Authentifizierung konfigurieren. So öffnen Sie die Seite Port Based Authentication (Portbasierte Authentifizierung): Klicken Sie auf **Switch** → **Network Security** → **Port Based Authentication**.

Abbildung 7-1. Port Based Authentication (Portbasierte Authentifizierung)



Die Seite Port Based Authentication (Portbasierte Authentifizierung) enthält folgende Felder:

Port Based Authentication State (Zustand der portbasierten Authentifizierung) – Lässt die portbasierte Authentifizierung auf dem Gerät zu. Folgende Feldwerte können ausgewählt werden:

Enable (Aktivieren) – Aktiviert die portbasierte Authentifizierung auf dem Gerät.

Disable (Deaktivieren) – Deaktiviert die portbasierte Authentifizierung auf dem Gerät.

Authentication Method (Authentifizierungsmethode) – Gibt die verwendete Authentifizierungs-methode an. Folgende Feldwerte können ausgewählt werden:

None (Keine) – Gibt an, dass keine Authentifizierungsmethode zur Authentifizierung des Ports zum Einsatz kommt.

RADIUS – Gibt an, dass die Authentifizierung des Ports über einen RADIUS-Server vorgenommen wird.

RADIUS, None (RADIUS, Keine) – Gibt an, dass die Authentifizierung des Ports zunächst über einen RADIUS-Server durchgeführt wird. Wenn der Port hierbei nicht authentifiziert wird, wird keine Authentifizierungsmethode benutzt, und die Sitzung wird zugelassen.

Guest VLAN (Gast-VLAN) – Aktiviert die Verwendung eines Gast-VLANs für nicht autorisierte Ports. Wenn ein Gast-VLAN aktiviert ist, nimmt der nicht autorisierte Port automatisch an dem im Feld **VLAN List** (VLAN-Liste) ausgewählten VLAN teil. Der Vorgabewert für dieses Feld lautet disabled (deaktiviert).

Interface (Schnittstelle) – Enthält eine Liste mit Schnittstellen, für die die portbasierte Authenti-fizie-rung aktiviert ist.

User Name (Benutzername) – Gibt den Benutzernamen des Bittstellers an.

Admin Interface Control (Administrierte Schnittstellensteuerung) – Legt den Autorisierungs-zustand des Ports fest. Folgende Feldwerte können ausgewählt werden:

Auto (Automatisch) – Aktiviert die portbasierte Authentifizierung auf dem Gerät. Auf Basis des Authentifizierungsaustauschs zwischen Gerät und Client wechselt die Schnittstelle entweder in einen autorisierten oder in einen nicht autorisierten Zustand.

Authorized (Autorisiert) – Versetzt die Schnittstelle ohne Authentifizierung in einen autori-sierten Zustand. Die Schnittstelle leitet normalen Verkehr weiter, ohne eine portbasierte Authenti-fizie-rung des Clients vorzunehmen.

Unauthorized (Nicht autorisiert) – Verweigert der ausgewählten Schnittstelle den Zugang zum System, indem die Schnittstelle in den nicht autorisierten Zustand versetzt wird. Das Gerät kann dem Client durch die Schnittstelle keine Authentifizierungsdienste zur Verfügung stellen.

Current Interface Control (Aktuelle Schnittstellensteuerung) – Gibt den aktuellen Autori-sierungs-zustand des Ports an.

Make Guest VLAN (Gast-VLAN herstellen) – Wenn dieser Punkt aktiviert ist, können nicht autorisierte Benutzer, die nicht an diese Schnittstelle angeschlossen sind, auf das Gast-VLAN zugreifen.

Periodic Reauthentication (Periodische Reauthentifizierung) – Erlaubt die unmittelbare Reauthentifizierung von Ports.

Reauthentication Period (300-4294967295) (Reauthentifizierungsperiode) – Gibt die Zeitspanne an, innerhalb derer der ausgewählte Port reauthentifiziert wird. Der Wert des Feldes wird in Sekunden angegeben. Der Standardwert des Feldes beträgt 3600 Sekunden.

Reauthenticate Now (Jetzt reauthentifizieren) – Erlaubt, wenn aktiviert, die umgehende Reauthentifizierung des Ports.

Authentication Server Timeout (1-65535) (Zeitüberschreitung für Authentifizierungsserver) – Legt fest, wie viel Zeit verstreichen muss, bevor das Gerät eine Anfrage an den Authentifizierungsserver erneut versendet. Der Wert des Feldes wird in Sekunden angegeben. Der Standardwert des Feldes beträgt 30 Sekunden.

Resending EAP Identity Request (1-65535) (Erneutes Senden der EAP-Identitätsanforderung) – Legt fest, wie viel Zeit verstreichen muss, bevor EAP-Identitätsanforderungen erneut versendet werden. Der Standardwert des Feldes beträgt 30 Sekunden.

Quiet Period (0-65535) (Ruheperiode) – Gibt die Anzahl an Sekunden an, die das Gerät nach einem fehlgeschlagenen Authentifizierungsaustausch im Ruhezustand wartet. Der Wertebereich umfasst die Werte 0 bis 65535. Der Standardwert lautet 60 Sekunden.

Supplicant Timeout (1-65535) (Zeitüberschreitung für Bittsteller) – Gibt an, wie viel Zeit verstreichen muss, bevor EAP-Anfragen erneut an den Bittsteller versendet werden. Der Wert des Feldes wird in Sekunden angegeben. Der Standardwert des Feldes beträgt 30 Sekunden.

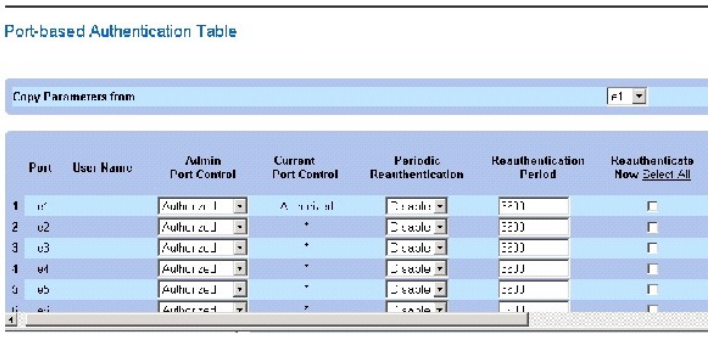
Max EAP Requests (1-10) (Max. EAP-Anfragen) – Gibt die Gesamtzahl der EAP-Anfragen an, die gesendet werden. Wenn nach der angegebenen Anzahl von Anfragen keine Antwort empfangen wurde, wird der Authentifizierungsprozess neu gestartet. Der Standardwert des Feldes beträgt 2 Wieder-holungs-versuche.

Anzeigen der Port Based Authentication Table (portbasierte Authentifizierungstabelle)

1. Öffnen Sie die Seite Port Based Authentication (Portbasierte Authentifizierung).
2. Klicken Sie auf Show All (Alle anzeigen).

Die Port Based Authentication Table (portbasierte Authentifizierungstabelle) wird geöffnet:

Abbildung 7-2. Port Based Authentication Table (Portbasierte Authentifizierungstabelle)



Zusätzlich zu den Feldern auf der Port Based Authentication (Portbasierte Authentifizierung) Seite werden in der Port Based Authentication Table (Portbasierte Authentifizierungstabelle) außerdem folgende Felder angezeigt:

Unit No. (Einheit Nr.) – Auswahl einer Stack-Komponente.

Copy Parameters from Port No. (Kopiere Parameter von Port Nr.) – Kopiert Parameter von dem ausgewählten Port.

Kopieren von Parametern in der Port Based Authentication Table (Portbasierte Authentifizierungstabelle)

1. Öffnen Sie die Seite Port Based Authentication (Portbasierte Authentifizierung).
2. Klicken Sie auf Show All (Alle anzeigen).

Die Port Based Authentication Table (Portbasierte Authentifizierungstabelle) wird geöffnet.

3. Wählen Sie im Feld **Copy Parameters from Port No.** (Kopiere Parameter von Port Nr.) die Schnittstelle aus.
4. Wählen Sie in der Port Based Authentication Table (Portbasierte Authentifizierungstabelle) eine Schnittstelle aus.
5. Aktivieren Sie das Kontrollkästchen **Copy to** (Kopieren nach), um die Schnittstellen festzulegen, zu denen die portbasierten Authentifizierungsparameter kopiert werden.
6. Klicken Sie auf Apply Changes (Änderungen übernehmen).

Aktivieren der portbasierten Authentifizierung mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Port Based Authentication Table (Portbasierte Authentifizierungstabelle) äquivalenten CLI-Befehle zur Aktivierung der portbasierten Authentifizierung zusammengefasst.

Tabelle 7-1. CLI-Befehle für portbasierte Authentifizierung

CLI-Befehl	Beschreibung
aaa authentication dot1x default *Methode1* [*Methode2*.]	Gibt zur Verwendung auf Schnittstellen, die IEEE 802.1X ausführen, eine oder mehrere Methoden für Authentifizierung, Autorisierung und Abrechnung (AAA) an.

dot1x max-req *Anzahl*	Legt fest wie oft das Gerät eine EAP an den Client sendet, bevor der Authentifizierungsvorgang neu gestartet wird.
dot1x re-authenticate [**ethernet** *Schnittstelle*]	Löst manuell eine Reauthentifizierung aller Ports mit aktiviertem 802.1X bzw. des angegebenen Ports mit aktiviertem 802.1X aus.
dot1x re-authentication	Aktiviert die periodische Reauthentifizierung des Clients.
dot1x timeout quiet-period Sekunden	Legt die Anzahl der Sekunden fest, die das Gerät nach einem fehlgeschlagenen Authenti-fi-zie-rungs-austausch im Ruhezustand wartet.
dot1x timeout re-authperiod *Sekunden*	Legt die Anzahl von Sekunden zwischen Reauthentifizierungsversuchen fest.
dot1x timeout server-timeout *Sekunden*	Legt die Zeit fest, nach deren Überschreitung Pakete erneut an den Authentifizierungsserver übertragen werden.
dot1x timeout supp-timeout *Sekunden*	Legt die Zeit fest, nach deren Überschreitung ein EAP-Anfrageframe erneut an den Client übertragen wird.
dot1x timeout tx-period *Sekunden*	Legt fest, wie viele Sekunden das Gerät auf eine Antwort auf einen EAP-Anforderungs-/Iden-ti-täts-frame vom Client wartet, bevor es die Anforderung erneut sendet.
show dot1x [ethernet *Schnittstelle*]	Zeigt den 802.1X-Status für das Gerät oder für die angegebene Schnittstelle an.
show dot1x users [username Benutzername]	Zeigt 802.1X-Benutzer des Geräts an.
dot1x guest-vlan enable	Aktiviert die Verwendung eines Gast-VLANs für nicht autorisierte Ports. Wenn ein Gast-VLAN aktiviert ist, nimmt der nicht autorisierte Port automatisch an dem im Feld **VLAN List** (VLAN-Liste) ausgewählten VLAN teil. Der Vorgabewert für dieses Feld lautet disabled (deaktiviert).
dot1x guest-vlan	Enthält eine Liste mit VLANs. Das Gast-VLAN wird aus der **VLAN List** (VLAN-Liste) ausgewählt.

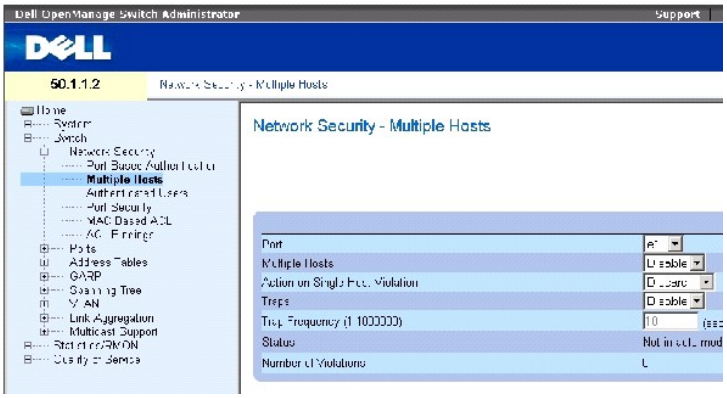
Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console# show dot1x

Interface  Admin Mode  Oper Mode     Reauth Control  Reauth Period  Username
---------  ----------  ----------    --------------  -------------  --------
1/e1       Auto        Authorized    Ena             3600           Bob
1/e2       Auto        Authorized    Ena             3600           John
1/e3       Auto        Unauthorized  Ena             3600           Clark
1/e4       Force-auth  Authorized    Dis             3600           n/a
```

Konfigurieren der erweiterten portbasierten Authentifizierung

Die Seite **Multiple Hosts (Mehrere Hosts)** enthält Angaben zur Definition von erweiterten portbasierten Authentifizierungseinstellungen für bestimmte Ports und VLANs. Weitere Informationen zur erweiterten portbasierten Authentifizierung finden Sie unter **Erweiterte portbasierte Authentifizierung**. So öffnen Sie die Seite **Multiple Hosts (Mehrere Hosts)**: Klicken Sie auf Switch →Network Security → Multiple Hosts.

Abbildung 7-3. Multiple Hosts (Mehrere Hosts)



Die Seite **Multiple Hosts (Mehrere Hosts)** enthält folgende Felder:

Port (Port) – Die Nummer des Ports, für den die erweiterte portbasierte Authentifizierung aktiviert wird.

Multiple Hosts (Mehrere Hosts) – Lässt zu oder verhindert, dass ein einzelner Host mehrere Hosts für den Systemzugriff autorisieren kann. Diese Einstellung muss aktiviert sein, damit auf dem ausgewählten Port entweder der Ingress-Filter deaktiviert oder Sicherheit durch Portsperren verwendet werden kann.

Action on Single Host Violation (Aktion bei Verletzung durch einzelnen Host) – Legt fest, wie verfahren wird, wenn im Einzelhostmodus Pakete von einem Host empfangen werden, dessen MAC-Adresse nicht die MAC-Adresse des Clients (Bittstellers) ist. Folgende Feldwerte können ausgewählt werden:

Forward (Weiterleiten) – Leitet die aus einer unbekannten Quelle stammenden Pakete weiter, die MAC-Adresse wird jedoch nicht erfasst.

Discard (Verwerfen) – Verwirft die aus einer unbekannten Quelle stammenden Pakete. Dies ist der Standardwert.

Shutdown (Herunterfahren) – Verwirft das aus einer nicht erfassten Quelle stammende Paket und fährt den Port herunter. Ports bleiben heruntergefahren, bis sie aktiviert werden oder der Switch zurückgesetzt wird.

Traps (Traps) – Aktiviert oder deaktiviert das Senden von Traps an den Host im Falle einer Sicherheitsverletzung.

Trap Frequency (1-1000000) (Sec) (Traphäufigkeit) – Legt das Zeitintervall in Sekunden fest, mit dem Traps an den Host gesendet werden. Im Feld **Trap Frequency (1-1000000)** kann nur dann eine Traphäufigkeit festgelegt werden, wenn das Feld **Multiple Hosts** (mehrere Hosts) auf **Disable** (Deaktivieren) gestellt ist. Der Standardwert beträgt 10 Sekunden.

Status (Status) – Der Hoststatus. Folgende Feldwerte können ausgewählt werden:

Unauthorized (Nicht autorisiert) – Gibt an, dass die Portsteuerung auf *Force Unauthorized* (Nicht autorisierten Betrieb erzwingen) steht, keine Verbindung am Port besteht oder die Portsteuerung auf *Auto* steht, aber ein Client über den Port nicht authentifiziert wurde.

Not in Auto Mode – Gibt an, dass die Portsteuerung auf *Forced Authorized* (Autorisierten Betrieb erzwingen) steht und Clients vollen Zugriff auf den Port haben.

Single-host Lock (Sperre auf einzelnen Host) – Gibt an, dass die Portsteuerung auf *Auto* (Automatisch) steht und über den Port ein einzelner Client authentifiziert wurde.

No Single Host (Kein Einzelhostbetrieb) – Gibt an, dass der Multihostmodus aktiviert ist.

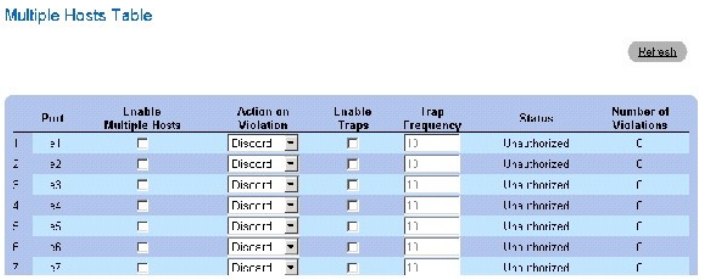
Number of Violations (Anzahl von Verletzungen) – Die Anzahl der Pakete, die im Einzelhostmodus an der Schnittstelle eingegangen sind und von einem Host stammen, dessen MAC-Adresse nicht die MAC-Adresse des Clients (Bittstellers) ist.

Anzeigen der Multiple Hosts Table (Multihosttabelle)

1. Öffnen Sie die Seite **Multiple Hosts (Mehrere Hosts)** .
2. Klicken Sie auf Show All (Alle anzeigen).

Die **Multiple Hosts Table (Multihosttabelle)** wird geöffnet.

Abbildung 7-4. Multiple Hosts Table (Multihosttabelle)



Aktivieren des Multihostmodus mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite **Multiple Hosts (Mehrere Hosts)** äquivalenten CLI-Befehle zur Aktivierung der erweiterten portbasierten Authentifizierung zusammengefasst.

Tabelle 7-2. CLI-Befehle für Multihostmodus

CLI-Befehl	Beschreibung
dot1x multiple-hosts	Erlaubt mehrere Hosts (Clients) auf einem 802.1X-autorisierten Port, dessen dot1x port-control-Schnittstellenkonfigurationskommando auf Auto eingestellt ist.
dot1x single-host-violation {forward |discard |discard-shutdown}[trap Sekunden]	Konfiguriert, wie vorgegangen wird, wenn eine Station auf die Schnittstelle zuzugreifen versucht, deren MAC-Adresse nicht die MAC-Adresse des Clients (Bittstellers) ist.

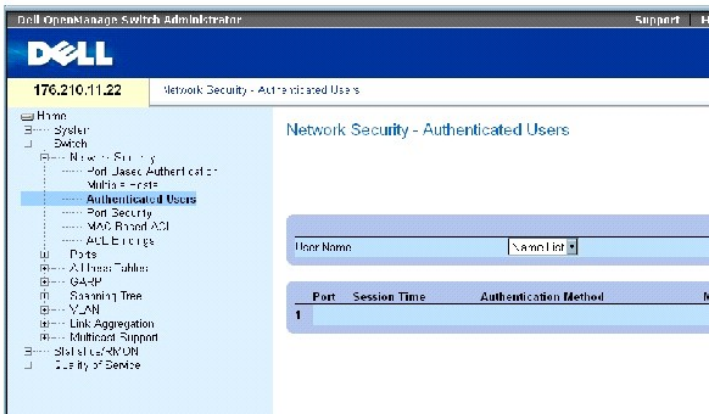
Im Folgenden ein Beispiel für den CLI-Befehl:

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


Console(config-if)# dot1x
multiple-hosts
```

Authentifizieren von Benutzern

Die Seite Authenticated Users (Authentifizierte Benutzer) zeigt nach Ports aufgeschlüsselte Benutzerzugriffslisten. Die Zugriffslisten werden auf der Seite Add User Name (Benutzername hinzufügen) definiert. So öffnen Sie die Seite Authenticated Users (Authentifizierte Benutzer): Klicken Sie auf Switch → Network Security → Authenticated Users.

Abbildung 7-5. Authenticated Users (Authentifizierte Benutzer)



Die Seite Authenticated Users (Authentifizierte Benutzer) enthält folgende Felder:

User Name (Benutzername) – Liste von über den RADIUS-Server autorisierten Benutzern.

Port (Port) – Die je Benutzername zur Authentifizierung benutzte(n) Portnummer(n).

Session Time (Sitzungsdauer) – Wie lange der Benutzer an dem Gerät angemeldet war. Das Feld-format lautet: Tag:Stunde:Minute:Sekunden, z. B.: 3 Tage: 2 Stunden: 4 Minuten: 39 Sekunden.

Authentication Method (Authentifizierungsmethode) – Die Methode, mit der die letzte Sitzung authentifiziert wurde. Folgende Feldwerte sind möglich:

Remote (Entfernt) – Der Benutzer wurde von einem entfernten Server aus authentifiziert.

None (Keine) – Der Benutzer wurde nicht authentifiziert.

MAC Address (MAC-Adresse) – Die MAC-Adresse des Bittstellers.

Anzeigen der Tabelle authentifizierter Benutzer

1. Öffnen Sie die Seite Authenticated Users (Authentifizierte Benutzer).
2. Klicken Sie auf Show All (Alle anzeigen).

Die **Authenticated Users Table** (Tabelle authentifizierter Benutzer) wird geöffnet.

Abbildung 7-6. Authenticated Users Table (Tabelle authentifizierter Benutzer)

Authentifizieren von Benutzern mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite Authenticated Users (Authentifizierte Benutzer) äquivalenten CLI-Befehle zum Authentifizieren von Benutzern zusammengefasst.

Tabelle 7-63. CLI-Befehle zum Hinzufügen von Benutzernamen

CLI-Befehl	Beschreibung
show dot1x users [username Benutzername]	Zeigt 802.1X-Benutzer des Geräts an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console# show dot1x users

Port Username Session Time Auth Method MAC Address

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

1/e11 gili 00:09:27 Remote 00:80:c8:b9:dc:1d
```

Konfigurieren von Port-Sicherheit

Die Netzwerksicherheit lässt sich verbessern, indem der Zugriff auf einen bestimmten Port auf Benutzer mit bestimmten MAC-Adressen beschränkt wird. Die MAC-Adressen können zuvor dynamisch erfasst oder statisch konfiguriert werden. Bei der auf Portsperren basierenden Port-Sicherheitsfunktion werden sowohl empfangene als auch erfasste Pakete überwacht, die auf bestimmten Ports empfangen werden. Der Zugriff auf den gesperrten Port wird auf Benutzer mit bestimmten MAC-Adressen beschränkt. Die Adressen werden entweder manuell für den Port festgelegt, oder sie werden von dem Port vor Aktivierung der Portsperre erfasst. Wenn ein gesperrter Port ein Paket empfangt, dessen MAC-Adresse nicht an diesen Port gebunden ist (d. h., sie wurde entweder auf einem anderen Port erfasst oder ist dem System unbekannt), wird ein Schutz-mechanismus aktiviert, der verschiedene Optionen anbietet. An einem gesperrten Port ankommende, nicht autorisierte Pakete werden entweder:

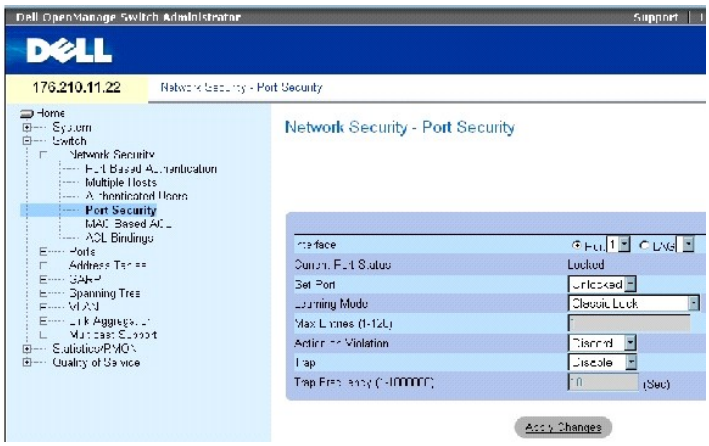
- weitergeleitet,
- ohne Trap verworfen,
- mit einem Trap verworfen,
- oder der Port wird heruntergefahren.

Die auf Portsperren basierende Port-Sicherheitsfunktion aktiviert außerdem die Speicherung einer Liste mit MAC-Adressen in der Konfigurationsdatei. So kann die MAC-Adressliste nach dem Zurücksetzen des Gerätes wiederhergestellt werden.

ANMERKUNG: Vor Aktivieren der Port-Sicherheit muss auf den entsprechenden Ports das Merkmal Multiple Hosts (Mehrere Hosts) aktiviert werden.

Deaktivierte Ports werden über die Seite Port Security (Port-Sicherheit) aktiviert. Die Seite **Ports** enthält Links zur Konfiguration von Portfunktionen, darunter auch erweiterte Merkmale wie z. B. Broadcaststurm-Kontrolle und Portspiegelung, und zum Durchführen von Tests virtueller Ports. So öffnen Sie die Seite Port Security (Port-Sicherheit): Klicken Sie auf Switch→ Network Security→ Port Security.

Abbildung 7-7. Port Security (Port-Sicherheit)



Die Seite Port Security (Port-Sicherheit) enthält folgende Felder:

Interface (Schnittstelle) – Gibt den ausgewählten Schnittstellentyp an, auf dem die Portsperre aktiviert ist.

Port – Der ausgewählte Schnittstellentyp ist ein Port.

LAG – Der ausgewählte Schnittstellentyp ist eine LAG.

Current Port Status (Aktueller Portstatus) – Der derzeit konfigurierte Portstatus.

Set Port (Port setzen auf) – Der Port wird entweder gesperrt oder freigegeben. Folgende Feldwerte können ausgewählt werden:

Unlocked (Nicht gesperrt) – Gibt den Port frei. Dies ist der Standardwert.

Locked (Gesperrt) – Sperrt den Port.

Learning Mode (Erfassungsmodus) – Legt den Typ der Portsperre fest. Das Feld **Learning Mode** ist nur dann aktiviert, wenn im Feld **Set Port** die Einstellung **Locked** ausgewählt ist. Die folgenden Feldwerte können ausgewählt werden:

Classic Lock (Klassische Sperre) – Sperrt den Port mit dem klassischen Portsperrmechanismus. Der Port wird unabhängig von der Anzahl der bereits erfassten Adressen umgehend gesperrt.

Limited Dynamic Lock (Eingeschränkte dynamische Sperre) – Sperrt den Port, indem die aktuell mit dem Port verknüpften dynamischen MAC-Adressen gelöscht werden. Der Port erfasst daraufhin MAC-Adressen bis zu dem auf dem Port erlaubten Maximum. Sowohl die Neuerfassung als auch das Aging (zeitgesteuertes Löschen) von MAC-Adressen werden aktiviert.

Max Entries (Max. Einträge) – Legt die Anzahl der MAC-Adressen fest, die auf dem Port erfasst werden können. Das Feld **Max Entries** (Max. Einträge) ist nur dann aktiviert, wenn im Feld **Set Port** (Port setzen auf) die Einstellung **Locked** (Gesperrt) ausgewählt wurde. Außerdem wird der Modus Limited Dynamic Lock (Eingeschränkte dynamische Sperre) ausgewählt. Der Standardwert lautet 1.

Action on Violation (Aktion bei Verletzung) – Gibt an, wie verfahren wird, wenn Pakete auf einem gesperrten Port eingehen. Folgende Feldwerte können ausgewählt werden:

Forward (Weiterleiten) – Leitet die aus einer unbekannten Quelle stammenden Pakete weiter, die MAC-Adresse wird jedoch nicht erfasst.

Discard (Verwerfen) – Verwirft die aus einer unbekannten Quelle stammenden Pakete. Dies ist der Standardwert.

Shutdown (Herunterfahren) – Verwirft das aus einer beliebigen unbekannten Quelle stammende Paket und fährt den Port herunter. Der Port bleibt heruntergefahren, bis er erneut aktiviert oder das Gerät zurückgesetzt wird.

Trap (Trap) – Aktiviert das Senden von Traps, wenn ein Paket auf einem gesperrten Port empfangen wird.

Trap Frequency (1-1000000) (Traphäufigkeit) – Das zwischen Traps liegende Zeitintervall (in Sekunden). Der Standardwert lautet 10 Sekunden.

Festlegen einer Portsperre

1. Öffnen Sie die Seite **Port Security (Port-Sicherheit)** .
2. Wählen Sie den Typ und die Nummer einer Schnittstelle aus.
3. Legen Sie die Felder fest.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der gesperrte Port wird der **Port Security Table (Portsicherheitstabelle)** hinzugefügt und das Gerät aktualisiert.

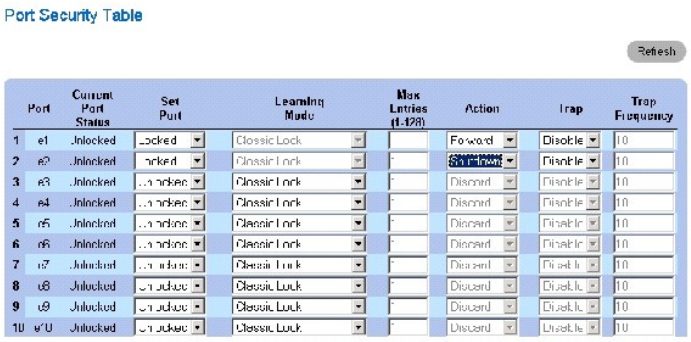
Anzeigen der Port Security Table (Portsicherheitstabelle)

1. Öffnen Sie die Seite **Port Security (Port-Sicherheit)** .
2. Klicken Sie auf **Show All**.

Die **Port Security Table (Portsicherheitstabelle)** wird geöffnet:

ANMERKUNG: Portsperren werden in der **Port Security Table (Portsicherheitstabelle)** festgelegt.

Abbildung 7-8. Port Security Table (Portsicherheitstabelle)



Die **Port Security Table (Portsicherheitstabelle)** enthält folgende zusätzliche Felder:

Unit No. (Einheitennr.) – Gibt die Nummer der Stack-Einheit an, für die Informationen zur Portsperre angezeigt werden.

Copy Parameters from (Kopiere Parameter von Port Nr.) – Kopiert Parameter an die ausgewählte Einheitennummer.

Konfigurieren von Portsperren mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite Port Security (Portsicherheit) äquivalenten CLI-Befehle zur Konfiguration von Portsperren zusammengefasst.

Tabelle 7-3. CLI-Befehle für Portsicherheit

CLI-Befehl	Beschreibung
shutdown	Deaktiviert Schnittstellen.
set interface active {ethernet Schnittstelle| port-channel Portkanalnummer}	Reaktiviert eine Schnittstelle, die aus Gründen der Portsicherheit deaktiviert wurde.
port security learning {disabled | dynamic}	Legt den Typ der Portsperre fest.
port security max Maximalzahl	Legt die maximale Anzahl der MAC-Adressen fest, die auf dem Port gelernt werden können.
port security [forward | discard | discard-shutdown] [trap Sekunden]	Sperrt die Erfassung neuer Adressen auf einer Schnittstelle.
show ports security {ethernetSchnittstelle| port-channel Portkanalnummer}	Zeigt den Sperrstatus des Ports an.

Im Folgenden ein Beispiel für die CLI-Befehle:

console # **show ports security**

Port	Status	Action	Trap	Frequency	Counter
1/e1	locked	Discard	Enable	100	88
1/e2	locked	Discard, Shutdown	Disable		
1/e3	Unlocked	-	-	-	-

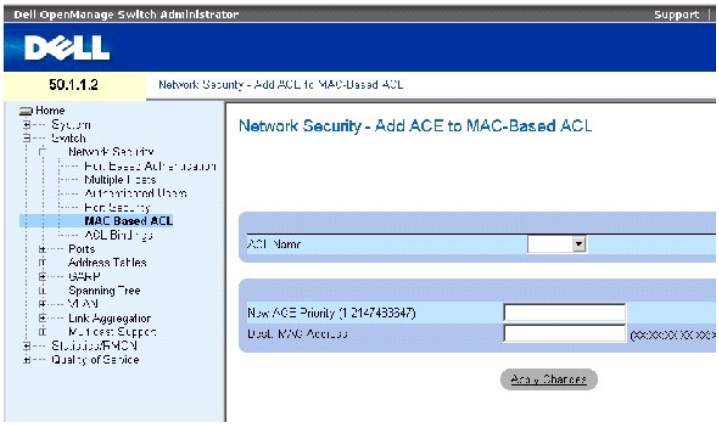
Definieren MAC-basierter ACLs

Über Zugriffskontrolllisten (Access Control Lists, ACL) können Netzwerkverwalter Klassifikationsaktionen und -regeln für spezifische Ingress-Ports festlegen. Eine ACL enthält mehrere Klassifikationsregeln und -aktionen. Die einzelnen Klassifikationsregeln und –aktionen werden Zugriffskontrolleinträge (Access Control Elements, ACE) genannt. ACEs fungieren als Filter, die den Datenverkehr klassifizieren. MAC-basierte ACLs werden auf alle Pakete angewendet, insbesondere auch auf Nicht-IP-Pakete. Klassifizierungsfelder basieren ausschließlich auf L2-Feldern.

MAC-basierte ACLs können auf der Seite MAC Based ACL (MAC-basierte ACL) definiert werden. Eine Erläuterung zu ACLs finden Sie unter Definieren MAC-basierter ACLs.

So öffnen Sie die Seite MAC Based ACL (MAC-basierte ACL): Wählen Sie **Switch→ Network Security→ MAC based ACL**.

Abbildung 7-9. MAC Based ACL (MAC-basierte ACL)



Die Seite MAC Based ACL (MAC-basierte ACL) enthält folgende Felder:

ACL Name (ACL-Name) – Benutzerdefinierte ACL.

New ACE Priority (1-2147483647) (Neue ACE-Priorität) – Eintragsnummer der ACE-Regel im ACL-Feld.

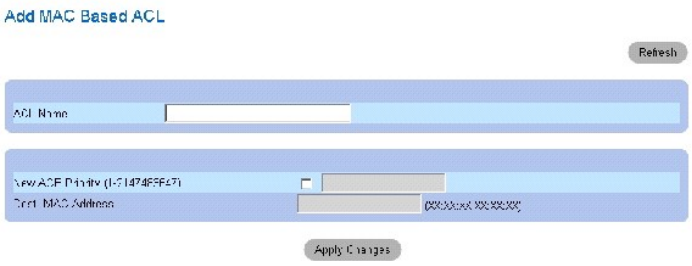
Destination MAC Address (MAC-Zieladresse) – Weist dem ACE die MAC-Zieladresse zu, an die Pakete sind, auf die der ACE zutrifft.

Hinzufügen einer MAC-basierten ACL:

1. Öffnen Sie die Seite MAC Based ACL (MAC-basierte ACL).
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite Add MAC Based ACLs (Hinzufügen MAC-basierter ACLs) wird geöffnet.

Abbildung 7-10. Add MAC Based ACLs (Hinzufügen MAC-basierter ACLs)



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

Die MAC-basierte ACL wird definiert und das Gerät aktualisiert.

Anzeigen ACL-spezifischer ACEs:

1. Öffnen Sie die Seite MAC Based ACL (MAC-basierte ACL).
2. Wählen Sie eine ACL aus.
3. Klicken Sie auf **Show All** (Alle anzeigen).

Die Seite **ACEs Associated with MAC ACL** (Mit der MAC-ACL assoziierte ACEs) wird geöffnet.

Entfernen von ACLs

1. Öffnen Sie die Seite MAC Based ACL (MAC-basierte ACL).

ANMERKUNG: ACLs können nur dann entfernt werden, wenn sie nicht an eine Schnittstelle gebunden sind.

2. Wählen Sie eine ACL aus.
3. Klicken Sie auf **Show All** (Alle anzeigen).

Die Seite **ACEs Associated with MAC ACL** (Mit der MAC-ACL assoziierte ACEs) wird geöffnet.

4. Markieren Sie das Kontrollkästchen **Remove ACL** (ACL entfernen).

Zuweisen MAC-basierter ACEs an ACLs mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite MAC Based ACL (MAC-basierte ACL) äquivalenten CLI-Befehle zum Zuweisen von MAC-basierten ACEs an ACLs zusammengefasst.

Tabelle 7-4. CLI-Befehle für MAC-basierte ACEs

CLI-Befehl	Beschreibung
`mac access-list Name`	Erstellt Layer-2-MAC-ACLs und wechselt in den Konfigurationsmodus für MAC-ACLs.
`deny` *`Ziel`*	Lehnt Datenverkehr ab, wenn die in der MAC-basierten ACL definierten Bedingungen erfüllt sind.
`show access-lists [`*`Name`*`]`	Zeigt die auf dem Gerät konfigurierten ACLs an.

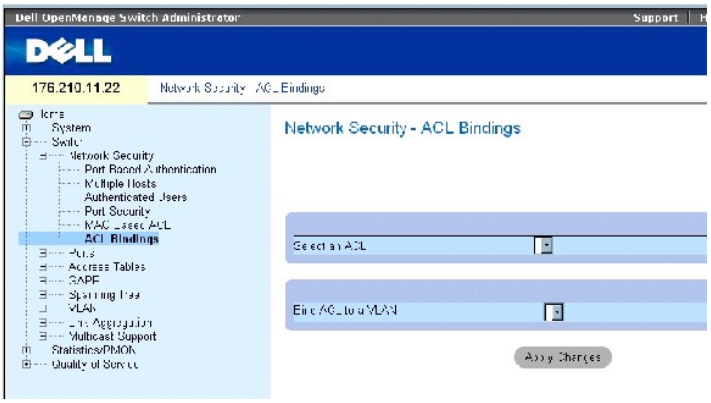
Im Folgenden ein Beispiel für die CLI-Befehle:

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

console (config-mac-al)# deny 00-10-B5-F4-00-01
```

Konfigurieren von ACL-Bindungen

Wenn eine ACL auf eine Schnittstelle gebunden ist, wird die ACL auf die ausgewählte Schnittstelle angewendet. Verwenden Sie die Seite ACL Bindings (ACL-Bindungen), um ACL-Listen an Klassifikationsmethoden und Schnittstellen zuzuweisen. So öffnen Sie die Seite ACL Bindings (ACL-Bindungen): Wählen Sie **Switch→ Network Security→ ACL Binding**.

Abbildung 7-11. ACL Bindings (ACL-Bindungen)



Die Seite ACL Bindings (ACL-Bindungen) enthält folgende Felder:

Select an ACL (ACL auswählen) – Der Typ der ACL, gegen die eingehende Pakete abgeglichen werden.

Bind ACL to VLAN (ACL an VLAN binden) – Das VLAN, mit dem die ACL verknüpft ist.

Zuweisen einer ACL an eine Schnittstelle

1. Öffnen Sie die Seite ACL Bindings (ACL-Bindungen).
2. Wählen Sie im Feld **Select an ACL** (ACL auswählen) den ACL-Typ aus.
3. Wählen Sie im Feld **Bind ACL to an VLAN** (ACL an VLAN binden) das VLAN aus, mit dem die ACL verknüpft wird.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die ACL wird mit der Schnittstelle verknüpft.

Entfernen eines Eintrags aus der ACL-Bindungstabelle

1. Öffnen Sie die Seite ACL Bindings (ACL-Bindungen).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die **ACL Bindings Table** (ACL-Bindungstabelle) wird geöffnet.

3. Aktivieren Sie das mit **Remove** (Entfernen) bezeichnete Kontrollkästchen neben dem zu entfernenden Eintrag.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der gewählte Eintrag wird aus der Tabelle entfernt, und das Gerät wird aktualisiert.

Anzeigen der ACL-Bindungstabelle

1. Öffnen Sie die Seite ACL Bindings (ACL-Bindungen).
2. Klicken Sie auf **Show All** (Alle anzeigen), um die **ACL Bindings Table** (ACL- Bindungstabelle) zu öffnen.

Die Felder in der **ACL Bindings Table** (ACL-Bindungstabelle) sind die gleichen wie auf der Seite **ACL Bindings** (ACL-Bindungen).

Kopieren von Parametern in der ACL-Bindungstabelle

1. Öffnen Sie die Seite ACL Bindings (ACL-Bindungen).

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

   Die Seite **ACL Bindings Table** (ACL-Bindungstabelle) wird geöffnet.

3. Wählen Sie im Feld **Copy Parameters from** (Parameter kopieren von) eine Schnittstelle aus.
4. Wählen Sie im Dropdown-Menü **VLAN** ein VLAN aus.

   Die Definitionen dieser Schnittstelle werden an die gewählten Zielports bzw. -trunks kopiert.

5. Aktivieren Sie das Kontrollkästchen **Copy to** (Kopieren nach) für den zu bearbeitenden Eintrag, oder kopieren Sie die Definitionen an alle verfügbaren Ports/Trunks.
6. Klicken Sie auf **Select All** (Alle auswählen).
7. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die Parameter werden an die Zielports bzw. -trunks in der *ACL Bindings Table* (ACL-Bindungstabelle) kopiert, und das Gerät wird aktualisiert.

Zuweisen von ACL-Mitgliedschaften mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite **ACL Binding** (ACL-Bindung) äquivalenten CLI-Befehle zur Zuweisung von ACL-Mitgliedschaften zusammengefasst.

Tabelle 7-5. CLI-Befehle für die ACL-Bindung

CLI-Befehl	Beschreibung
service-acl {**input** *ACL-Name*}	Wendet eine Zugriffsliste auf den Schnittstelleneingang an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# interface vlan 123

console(config-if)# service-acl input dell
```

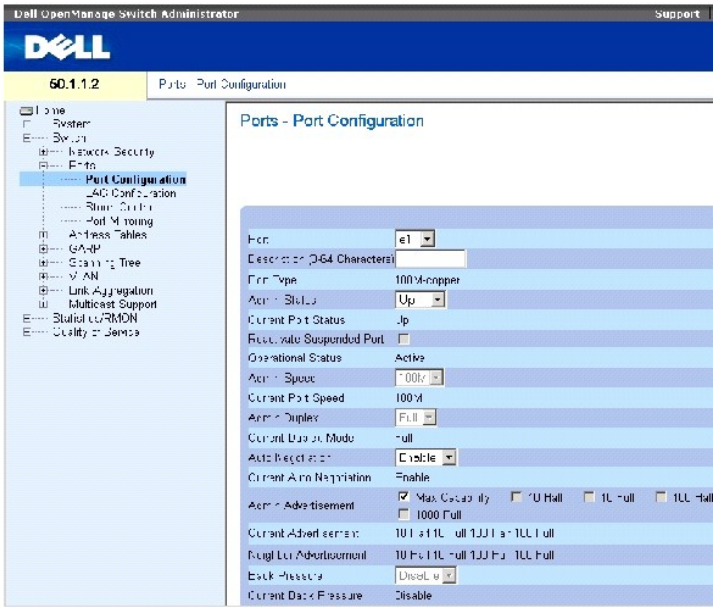
Konfigurieren von Ports

Die Seite **Ports** enthält Links zur Konfiguration von Portfunktionen, darunter auch erweiterte Merkmale wie z. B. Broadcaststurm-Kontrolle und Portspiegelung, und zum Durchführen von Tests virtueller Ports. So öffnen Sie die Seite **Ports**: Wählen Sie **Switch**→ **Ports**.

Festlegen der Port-Konfiguration

Verwenden Sie die Seite **Port Configuration (Port-Konfiguration)**, um Portparameter festzulegen. Wenn die Portkonfiguration geändert wird, während der Port einer LAG angehört, werden die Konfigurationsänderungen erst wirksam, nachdem der Port aus der LAG entfernt wurde. So öffnen Sie die Seite **Port Configuration (Port-Konfiguration)**: Klicken Sie in der Strukturansicht auf **Switch**→ **Ports**→ **Port Configuration** .

Abbildung 7-12. Port Configuration (Port-Konfiguration)



Die Seite **Port Configuration (Port-Konfiguration)** enthält folgende Felder:

Port (Port) – Die Nummer des Ports, für den Parameter festgelegt werden.

Description (0 - 64 Characters) (Beschreibung, 0-64 Zeichen) – Eine kurze Beschreibung der Schnittstelle, z. B. Ethernet.

Port Type (Port-Typ) – Der Typ des Ports.

Admin Status (Administrierter Status) – Aktiviert oder deaktiviert die Weiterleitung von Daten durch den Port.

Current Port Status (Aktueller Portstatus) – Zeigt an, ob der Port derzeit in Betrieb oder außer Betrieb ist.

Re-Activate Suspended Port (Ausgesetzten Port reaktivieren) – Reaktiviert einen Port, nachdem er über die Portsperre-Sicherheitsoption deaktiviert wurde.

Operational Status (Betriebsstatus) – Zeigt den Betriebsstatus des Ports an. Folgende Feldwerte sind möglich:

Suspended (Ausgesetzt) – Der Port ist derzeit aktiv und empfängt oder sendet keine Daten.

Active (Aktiv) – Der Port ist derzeit aktiv und empfängt oder sendet Daten.

Disable (Inaktiv) – Der Port ist derzeit deaktiviert und empfängt oder sendet keine Daten.

Admin Speed (Administrierte Geschwindigkeit) – Die für den Port konfigurierte Übertragungsrate. Der Port-Typ bestimmt, welche Optionen für die Geschwindigkeitseinstellung verfügbar sind. Die administrierte Geschwindigkeit kann nur festgelegt werden, wenn der Port deaktiviert ist.

Current Port Speed (Aktuelle Portgeschwindigkeit) – Gibt die derzeit synchronisierte Geschwindigkeit des Ports in Bit/s an.

Admin Duplex (Administrierte Duplexeinstellung) – Der Duplexmodus des Ports in Bit/s. **Full** (Vollduplex) bedeutet, dass die Schnittstelle die gleichzeitige Übertragung in beide Richtungen zwischen Gerät und Client unterstützt. **Half** (Halbduplex) bedeutet, dass die Schnittstelle die Übertragung zwischen Gerät und Client nur in jeweils eine Richtung gleichzeitig unterstützt.

Current Duplex Mode (Aktueller Duplexmodus) – Der tatsächlich synchronisierte Duplexmodus des Ports.

Auto Negotiation (Autom. Aushandeln) – Aktiviert Auto-Negotiation auf dem Port. Auto-Negotiation bezeichnet ein Protokoll zwischen zwei Verbindungspartnern, mit dessen Hilfe ein Port dem jeweils anderen Port seine Fähigkeiten bezüglich Datenübertragungsrate, Duplexmodus und Flusskontrolle bekannt machen kann.

Current Auto Negotiation (Aktuelle Auto-Negotiation) – Gibt die aktuelle Einstellung für die Auto-Negotiation an.

Admin Advertisement (Administrierte Bekanntmachung) – Legt die Auto-Negotiation-Einstellung fest, die der Port bekannt macht. Folgende Feldwerte sind möglich:

Max Capability (Max. Fähigkeit) – Gibt an, dass alle Portgeschwindigkeiten und Duplexmodi akzeptiert werden.

10 Half (10 Halbduplex) – Gibt an, dass der Port eine Portgeschwindigkeit von 10 MBit/s im Halbduplexmodus bekannt macht.

10 Full (10 Vollduplex) – Gibt an, dass der Port eine Portgeschwindigkeit von 10 MBit/s im Vollduplexmodus bekannt macht.

100 Half (100 Halbduplex) – Gibt an, dass der Port eine Portgeschwindigkeit von 100 MBit/s im Halbduplexmodus bekannt macht.

100 Full (100 Vollduplex) – Gibt an, dass der Port eine Portgeschwindigkeit von 100 MBit/s im Vollduplexmodus bekannt macht.

1000 Full (1000 Vollduplex) – Gibt an, dass der Port eine Portgeschwindigkeit von 1000 MBit/s im Vollduplexmodus bekannt macht.

Current Advertisement (Aktuelle Bekanntmachung) – Der Port macht seine Geschwindigkeit seinem Nachbarport bekannt, um das Aushandeln zu beginnen. Die möglichen Feldwerte sind die im Feld Admin Advertisement angegebenen.

Neighbor Advertisement (Bekanntmachung des Nachbarn) – Zeigt die Porteinstellungen, die der Nachbarport bekannt gibt. Die möglichen Feldwerte sind mit den Werten des Felds Admin Advertisement identisch.

Back Pressure (Backpressure) – Aktiviert auf dem Port den Backpressure-Modus. Der Backpressure-Modus wird im Halbduplexmodus verwendet, um auf Ports den Empfang von Nachrichten zu unterbinden. Bei OOB-Ports wird Backpressure nicht unterstützt.

Current Back Pressure (Aktuelle Backpressure) – Die aktuelle Backpressure-Einstellung.

Flow Control (Flusskontrolle) – Aktiviert bzw. deaktiviert die Flusskontrolle oder aktiviert das automatische Aushandeln der Flusskontrolle auf dem Port.

Current Flow Control (Aktuelle Flusskontrolle) – Die aktuelle Einstellung der Flusskontrolle.

MDI/MDIX (MDI/MDIX) – Ermöglicht dem Gerät die Erkennung gekreuzter und nicht gekreuzter Kabel. Die Ports von Hubs und Switches sind im Vergleich zu den Ports von Endstationen absichtlich umgekehrt belegt, so dass zum Anschluss eines Hubs oder Switches an eine Endstation ein ungekreuztes 1:1-Kabel verwendet werden kann und die Adernpaare dabei richtig miteinander verbunden werden. Wenn zwei Hubs/Switches bzw. zwei Endstationen miteinander verbunden werden, wird ein gekreuztes Kabel verwendet, um sicherzustellen, dass die Adernpaare richtig miteinander verbunden werden. Die automatische MDIX-Unterstützung funktioniert bei FE-Ports nicht, wenn Auto-Negotiation (automatisches Aushandeln) deaktiviert ist. Folgende Feldwerte sind möglich:

Auto (automatisch) – Benutzen Sie diese Einstellung, um den Kabeltyp automatisch erkennen zu lassen.

MDIX – Benutzen Sie diese Einstellung für Hubs und Switches.

MDI – Benutzen Sie diese Einstellung für Endstationen.

Current MDI/MDIX (Aktuelle MDI/MDIX) – Gibt die aktuelle MDIX-Einstellung des Geräts an. Folgende Feldwerte sind möglich:

MDI – Die aktuelle MDI-Einstellung ist MDI.

MDIX – Die aktuelle MDI-Einstellung ist MDIX.

LAG – Gibt an, ob der Port einer LAG angehört.

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.

Definieren von Portparametern

1. Öffnen Sie die Seite **Port Configuration (Port-Konfiguration)**.
2. Wählen Sie im Feld **Port** einen Port aus.
3. Legen Sie die im Dialogfeld verfügbaren Einstellungen fest.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

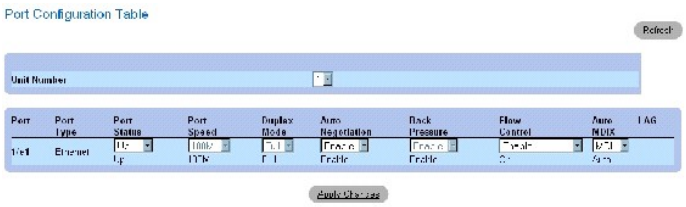
Die Portparameter werden auf dem Gerät gespeichert.

Anzeigen der Porttabelle

1. Öffnen Sie die Seite **Port Configuration (Port-Konfiguration)**.
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die **Port Configuration Table** (Port-Konfigurationstabelle) wird geöffnet.

Abbildung 7-13. Port Configuration Table (Portkonfigurationstabelle)



Konfigurieren von Ports mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite Port Configuration (Port-Konfiguration) äquivalenten CLI-Befehle zum Konfigurieren von Ports zusammengefasst.

Tabelle 7-6. CLI-Befehle zur Portkonfiguration

CLI-Befehl	Beschreibung
interface ethernet *Schnittstelle*	Aktiviert den Schnittstellenkonfigurationsmodus, um eine Ethernet-Schnittstelle zu konfigurieren.
description *Zeichenkette*	Fügt einer Schnittstellenkonfiguration eine Beschreibung hinzu.
shutdown	Deaktiviert Schnittstellen, die Teil des derzeit festgelegten Kontexts sind.
set interface active {**ethernet** *Schnittstelle* | **port-channel** *Port-Kanalnummer*}	Reaktiviert eine Schnittstelle, die aus Sicherheitsgründen heruntergefahren wurde.
speed *MBit/s*	Konfiguriert die Geschwindigkeit einer bestimmten Ethernet-Schnittstelle, wenn keine Auto-Negotiation verwendet wird.
duplex {half | full}	Konfiguriert den Voll-/Halbduplexbetrieb einer bestimmten Ethernet-Schnittstelle, wenn keine Auto-Negotiation verwendet wird.
negotiation [Fähigkeit1 [Fähigkeit2 ...Fähigkeit5]	Aktiviert das automatische Aushandeln (Auto-Negotiation) von Geschwindigkeit und Duplexparametern einer gegebenen Schnittstelle.
back-pressure	Aktiviert Backpressure auf einer gegebenen Schnittstelle.
flowcontrol {auto | on | off | rx | tx}	Konfiguriert die Flusskontrolle auf einer gegebenen Schnittstelle.
mdix {on | auto}	Aktiviert auf einer gegebenen Schnittstelle/einem gegebenen Portkanal die automatische Erkennung von Crossover-Kabeln.
show interfaces configuration [**ethernet** *Schnittstelle* |**port-channel** *Port-Kanalnummer*]	Zeigt die Konfiguration aller konfigurierten Schnittstellen an.
show interface advertise	Zeigt an, welche Fähigkeiten die Schnittstelle beim Aushandeln der Einstellungen bekannt macht.
show interfaces status [**ethernet** *Schnittstelle* | **port-channel** *Port-Kanal-Nummer*]	Zeigt den Status aller konfigurierten Schnittstellen an.
show interfaces description [**ethernet** *Schnittstelle* | **port-channel** *Port-Kanalnummer*]	Zeigt die Beschreibung aller konfigurierten Schnittstellen an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# interface ethernet 1/e3

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)# end

console# show interfaces configuration ethernet 1/e3
```

Port	Type	Duplex	Speed	Neg	Flow Control	Admin State	Back Pressure	Mdix Mode
----	----	------	-----	----	------	-----	------	----
1/e3	100	Full	100	Enabled	On	Up	Enable	Auto

Console# **show interfaces status**

Port	Type	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	Mdix Mode
----	----	------	-----	----	------	-----	------	----
1/e3	100	Full	100	Auto	On	Up	Enable	On
1/e4	100	Full	1000	Off	Off	Up	Disable	On

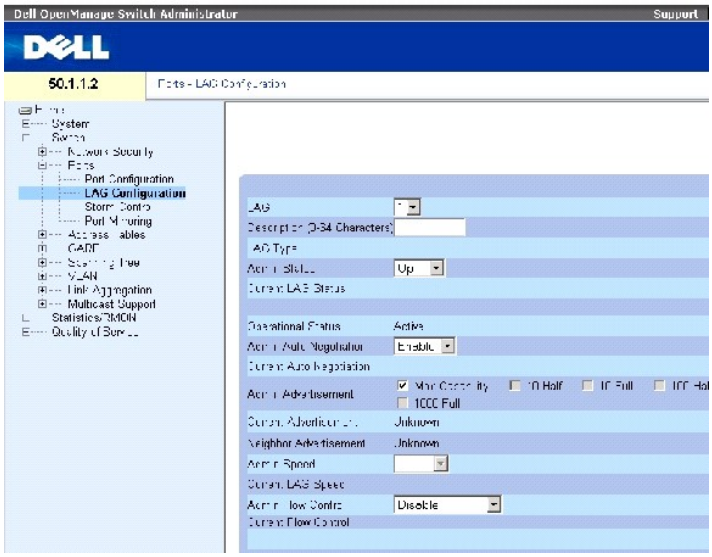
Ch	Type	Duplex	Speed	Neg	Flow Control	Back Pressure	Link State	
---	----	------	-----	-----	-------	--------	------	
1	1000	Full	1000	Off	Off	Disable	Up	

Definieren von LAG-Parametern

Die Seite **LAG Configuration (LAG-Konfiguration)** enthält Felder zur Konfiguration von Parametern für konfigurierte LAGs. Das Gerät unterstützt bis zu acht Ports pro LAG und acht LAGs pro System. Weitere Informationen zu Link Aggregated Groups (LAG) und zum Zuweisen von Ports an LAGs finden Sie unter **Aggregieren von Ports**.

So öffnen Sie die Seite **Port Configuration (Port-Konfiguration)**: Klicken Sie in der Strukturansicht auf Switch→ Ports→ LAG Configuration.

Abbildung 7-14. LAG Configuration (LAG-Konfiguration)



Die Seite **LAG Configuration (LAG-Konfiguration)** enthält folgende Felder:

LAG (LAG) – Die LAG-Nummer.

Description (0 - 64 Characters) (Beschreibung, 0 bis 64 Zeichen) – Bietet eine benutzerdefinierte Beschreibung der konfigurierten LAG.

LAG Type (LAG-Typ) – Die Porttypen, aus denen die LAG besteht.

Admin Status (Administrierter Status) – Aktiviert oder deaktiviert die ausgewählte LAG.

Current LAG Status (Aktueller LAG-Status) – Gibt an, ob die LAG derzeit in Betrieb ist.

Operational Status (Betriebsstatus) – Aktiviert oder deaktiviert die Weiterleitung von Datenverkehr durch die ausgewählte LAG.

Admin Auto Negotiation (Administrierte Auto-Negotiation) – Aktiviert oder deaktiviert die Auto-Negotiation (automatisches Aushandeln) auf der LAG. Auto-Negotiation bezeichnet ein Protokoll zwischen zwei Verbindungspartnern, mit dessen Hilfe eine LAG der jeweils anderen LAG ihre Fähigkeiten bezüglich Datenübertragungsrate, Duplexmodus und Flusskontrolle bekannt machen kann.

Current Auto Negotiation (Aktuelle Auto-Negotiation) – Gibt die aktuell konfigurierte Einstellung für die Auto-Negotiation an.

Admin Advertisement (Administrierte Bekanntmachung) – Legt die Auto-Negotiation-Einstellung fest, die die LAG bekannt macht. Folgende Feldwerte sind möglich:

Max Capability (Max. Fähigkeit) – Gibt an, dass alle LAG-Geschwindigkeiten und Duplexmodi akzeptiert werden.

10 Half (10 Halbduplex) – Gibt an, dass die LAG eine LAG-Geschwindigkeit von 10 MBit/s im Halbduplexmodus bekannt macht.

10 Full (10 Vollduplex) – Gibt an, dass die LAG eine LAG-Geschwindigkeit von 10 MBit/s im Vollduplexmodus bekannt macht.

100 Half (100 Halbduplex) – Gibt an, dass die LAG eine LAG-Geschwindigkeit von 100 MBit/s im Halbduplexmodus bekannt macht.

100 Full (100 Vollduplex) – Gibt an, dass die LAG eine LAG-Geschwindigkeit von 100 MBit/s im Vollduplexmodus bekannt macht.

1000 Full (1000 Vollduplex) – Gibt an, dass die LAG eine LAG-Geschwindigkeit von 1000 MBit/s im Vollduplexmodus bekannt macht.

Current Advertisement (Aktuelle Bekanntmachung) – Die LAG macht ihre Geschwindigkeit ihrer Nachbar-LAG bekannt, um das Aushandeln zu beginnen. Die möglichen Feldwerte sind die im Feld Admin Advertisement (Administrierte Bekanntmachung) angegebenen.

Neighbor Advertisement (Bekanntmachung des Nachbarn) – Zeigt die LAG-Einstellungen an, die der Nachbarport bekannt gibt. Die möglichen Feldwerte sind mit den Werten des Felds Admin Advertisement (Administrierte Bekanntmachung) identisch.

Admin Speed (Administrierte Geschwindigkeit) – Die Geschwindigkeit, mit der die LAG arbeitet.

Current LAG Speed (aktuelle LAG-Geschwindigkeit) – Die aktuelle Geschwindigkeit, mit der die LAG arbeitet.

Admin Flow Control (Administrierte Flusskontrolle) – Aktiviert bzw. deaktiviert Flusskontrolle oder aktiviert das automatische Aushandeln der Flusskontrolle auf der LAG. Die Flusskontrolle wirkt sich auf diejenigen Ports in der LAG aus, die im Vollduplexbetrieb arbeiten.

Current Flow Control (Aktuelle Flusskontrolle) – Die vom Benutzer festgelegte Einstellung für die Flusskontrolle.

Definieren von LAG-Parametern

1. Öffnen Sie die Seite **LAG Configuration (LAG-Konfiguration)**.
2. Wählen Sie im Feld **LAG** eine LAG aus.
3. Legen Sie die Felder fest.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die LAG-Parameter werden auf dem Gerät gespeichert.

Modifizieren von LAG-Parametern

1. Öffnen Sie die Seite **LAG Configuration (LAG-Konfiguration)**.
2. Wählen Sie im Feld **LAG** eine LAG aus.
3. Modifizieren Sie die Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

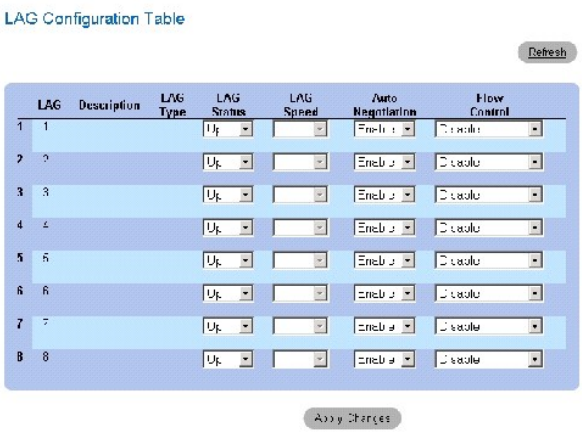
Die LAG-Parameter werden auf dem Gerät gespeichert.

Anzeigen der LAG-Konfigurationstabelle:

1. Öffnen Sie die Seite **LAG Configuration (LAG-Konfiguration)**.
2. Klicken Sie auf **Show All**.

Die **LAG Configuration Table (LAG-Konfigurationstabelle)** wird geöffnet:

Abbildung 7-15. LAG Configuration Table (LAG-Konfigurationstabelle)



Konfigurieren von LAGs mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite **LAG Configuration (LAG-Konfiguration)** äquivalenten CLI-Befehle zum Konfigurieren von LAGs zusammengefasst.

Tabelle 7-68. CLI-Befehle zur LAG-Konfiguration

CLI-Befehl	Beschreibung
interface port-channel *Port-Kanalnummer*	Aktiviert den Schnittstellen-konfigurations-modus eines bestimmten Port-Kanals.
description *Zeichenkette*	Fügt einer Schnittstellenkonfiguration eine Beschreibung hinzu.
shutdown	Deaktiviert Schnittstellen, die Teil des derzeit festgelegten Kontexts sind.
speed *Bit/s*	Konfiguriert die Geschwindigkeit einer gegebenen Ethernet-Schnittstelle, wenn keine Auto-Negotiation verwendet wird.
negotiation [Fähigkeit1 [Fähigkeit2 ...Fähigkeit5]	Aktiviert das automatische Aushandeln der Schnittstellengeschwindigkeit.
back-pressure	Aktiviert Backpressure auf einer gegebenen Schnittstelle.
flowcontrol \{auto | on | off | rx | tx\}	Konfiguriert die Flusskontrolle auf einer gegebenen Schnittstelle.
show interfaces configuration [**ethernet** *Schnittstelle* | **port-channel** *Port-Kanalnummer*]	Zeigt die Konfiguration aller konfigurierten Schnittstellen an.
show interfaces status [**ethernet** *Schnittstelle* | **port-channel** *Port-Kanalnummer*]	Zeigt den Status aller konfigurierten Schnittstellen an.
show interfaces description [**ethernet** *Schnittstelle* |**port-channel** *Port-Kanalnummer*]	Zeigt die Beschreibung aller konfigurierten Schnittstellen an.
show interfaces port-channel [*Port-Kanalnummer*]	Zeigt Port-Kanalinformationen an (welche Ports einem Port-Kanal angehören, und ob sie derzeit aktiv sind oder nicht).

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# interface port-channel 2

console(config-if)# no negotiation

console(config-if)# speed 100

console(config-if)# flowcontrol on

console(config-if)# exit
```

```
console(config)# interface port-channel 3

console(config-if)# shutdown

console(config-if)# exit

console(config)# interface port-channel 4

console(config-if)# back-pressure

console(config-if)# description p4

console(config-if)# end

console# show interfaces port-channel
```

Channel	Ports
---------	---------
ch1	Inactive: 1/e(11-13)
ch2	Active: 1/e14

Aktivieren der Broadcaststurm-Kontrolle

Ein Broadcaststurm resultiert aus einer übermäßig hohen Anzahl von Broadcast-Nachrichten, die von einem einzelnen Port gleichzeitig über ein Netzwerk übertragen werden. Die Antworten auf diese weitergeleiteten Nachrichten stapeln sich im Netzwerk auf, was zu Überlastung der Netzwerkressourcen oder Zeitüberschreitungen im Netzwerk führt.

Die Broadcaststurm-Kontrolle wird für jeden Port individuell aktiviert, indem der Pakettyp und die Übertragungsrate der Pakete definiert wird.

Das System misst separat auf jedem Port die Framerate der eingehenden Broadcast-, Unicast- und Multicastframes und verwirft Frames, sobald die gemessene Rate eine benutzerdefinierte Rate überschreitet.

Die Seite **Storm Control (Broadcaststurm-Kontrolle)** enthält Felder, mit denen die Broadcaststurm-Kontrolle aktiviert und konfiguriert werden kann. So öffnen Sie die Seite **Storm Control (Broadcaststurm-Kontrolle)**: Klicken Sie in der Strukturansicht auf Switch→ Ports→ Storm Control .

Abbildung 7-16. Storm Control (Broadcaststurm-Kontrolle)

Die Seite **Storm Control (Broadcaststurm-Kontrolle)** enthält folgende Felder:

Port (Port) – Der Port, für den die Broadcaststurm-Kontrolle aktiviert wird.

Broadcast Control (Broadcast-Kontrolle) – Aktiviert oder deaktiviert das Weiterleiten von Broadcast-Paketen auf der angegebenen Schnittstelle.

Broadcast Mode (Broadcast-Modus) – Gibt den derzeit auf dem Gerät oder Stack aktivierten Broadcast-Modus an. Folgende Feldwerte sind möglich:

Unknown Unicast, Multicast & Broadcast – Zählt Unicast-, Multicast- und Broadcastverkehr.

Multicast & Broadcast – Zählt Broadcast- und Multicastverkehr zusammen.

Broadcast Only – Zählt nur Broadcast-Verkehr.

Broadcast Rate Threshold (70-285000) (Schwellwert für Broadcastrate, 70-285000) – Die maximale Rate (Kilobyte pro Sekunde), mit der unbekannte Pakete weitergeleitet werden. Der Wertebereich des Felds reicht von 70 bis 285000 Kilobyte pro Sekunde.

Aktivieren der Broadcaststurm-Kontrolle

1. Öffnen Sie die Seite **Storm Control (Broadcaststurm-Kontrolle)**.
2. Wählen Sie eine Schnittstelle aus, für die die Broadcaststurm-Kontrolle implementiert wird.
3. Legen Sie die Felder fest.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Broadcaststurm-Kontrolle wird aktiviert.

Modifizieren der Port-Parameter für die Broadcaststurm-Kontrolle

1. Öffnen Sie die Seite **Storm Control (Broadcaststurm-Kontrolle)**.
2. Modifizieren Sie die Felder.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

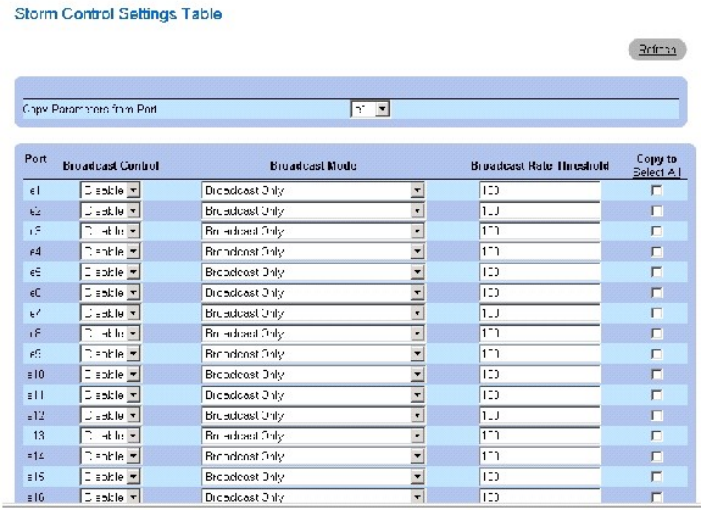
Die Port-Parameter für die Broadcaststurm-Kontrolle werden auf dem Gerät gespeichert.

Anzeigen der Portparameter-Tabelle

1. Öffnen Sie die Seite **Storm Control (Broadcaststurm-Kontrolle)**.
2. Klicken Sie auf **Show All** (Alle anzeigen)..

Die **Storm Control Settings Table (Tabelle mit Einstellungen für die Broadcaststurm-Kontrolle)** wird geöffnet.

Abbildung 7-17. Storm Control Settings Table (Tabelle mit Einstellungen für die Broadcaststurm-Kontrolle)



Über die auf der Seite Storm Control (Broadcaststurm-Kontrolle) angezeigten Felder hinaus enthält die Storm Control Settings Table (Tabelle mit Einstellungen für die Broadcaststurm-Kontrolle) folgende zusätzlichen Felder:

Copy Parameters from Port (Kopiere Parameter von Port) – Gibt den Port an, von dem die Parameter für die Broadcaststurm-Kontrolle kopiert werden.

Kopieren von Parametern in der Tabelle mit Einstellungen für die Broadcaststurm-Kontrolle

1. Öffnen Sie die Seite Storm Control (Broadcaststurm-Kontrolle).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die Storm Control Settings Table (Tabelle mit Einstellungen für die Broadcaststurm-Kontrolle) wird geöffnet.

3. Wählen Sie im Feld **Copy Parameters from Port** (Kopiere Parameter von Port) den Port, von dem die Einstellungen kopiert werden sollen.
4. Aktivieren Sie das Kontrollkästchen **Copy to** (Kopieren nach), um die Schnittstellen auszuwählen, an die die Definitionen für die Broadcaststurmkontrolle kopiert werden sollen, oder klicken Sie auf **Select All** (Alle auswählen), um die Definitionen an alle Ports zu kopieren.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Parameter werden an die ausgewählten Ports in der **Strom Control Settings Table** (Tabelle mit Einstellungen für die Broadcaststurm-Kontrolle) kopiert, und das Gerät wird aktualisiert.

Konfigurieren der Broadcaststurm-Kontrolle mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite Storm Control (Broadcaststurm-Kontrolle) äquivalenten CLI-Befehle zum Konfigurieren der Broadcaststurm-Kontrolle zusammengefasst.

Tabelle 7-7. CLI-Befehle für die Broadcaststurm-Kontrolle

CLI-Befehl	Beschreibung

`port storm-control include-multicast`	Aktiviert die gemeinsame Zählung von Multicast-, Unicast- und Broadcast-Paketen durch das Gerät.
`port storm-control broadcast enable`	Aktiviert die Broadcaststurm-Kontrolle.
`port storm-control broadcast rate`	Konfiguriert die maximale Broadcastrate.
`show ports storm-control` *Port*	Zeigt die Konfiguration der Broadcaststurm-Kontrolle an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# port storm-control include-multicast

console(config)# interface ethernet 1/e1

console(config-if)# port storm-control broadcast enable

console(config-if)# port storm-control broadcast rate 100000

console(config-if)# end

console# show ports storm-control
```

Port	Broadcast Storm control [kbyes/sec]
----	----------
1/e1	8000
2/e1	Disabled
3/e2	Disabled

Festlegen von Portspiegelungs-Sitzungen

Portspiegelung:

- überwacht und spiegelt den Netzwerkdatenverkehr, indem Kopien eingehender und ausgehender Pakete von einem Port an einen Überwachungsport weitergeleitet werden,
- kann als Diagnosetool und/oder zur Fehlersuche verwendet werden,

- ermöglicht die Leistungsüberwachung des Geräts.

Die Port-Spiegelung wird konfiguriert, indem ein bestimmter Port ausgewählt wird, an den alle Pakete kopiert werden, und andere Ports festgelegt werden, von denen die Pakete kopiert werden.

Vor dem Konfigurieren der Portspiegelung sollten Sie Folgendes beachten:

- Bei der Port-Spiegelung wird der Netzwerkdatenverkehr überwacht und gespiegelt, indem Kopien eingehender und ausgehender Pakete von einem überwachten Port an einen überwachenden Port weitergeleitet werden.
- Überwachte Ports können keine höhere Leistung erzielen als der überwachende Port.
- Alle RX/TX-Pakete sollten auf demselben Port überwacht werden.

Die folgenden Beschränkungen gelten für Ports, die als Zielports konfiguriert werden:

- Die Ports dürfen nicht als Quellports konfiguriert werden.
- Die Ports dürfen kein Mitglied einer LAG sein.
- Auf dem Port dürfen keine IP-Schnittstellen konfiguriert sein.
- GVRP darf nicht auf dem Port aktiviert sein.
- Der Port darf nicht Mitglied eines VLANs sein.
- Es kann nur ein Zielport definiert werden.

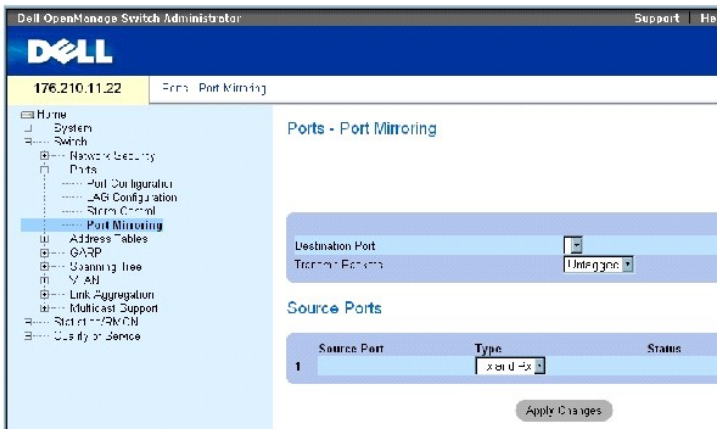
Die folgenden Beschränkungen gelten für Ports, die als Quellports konfiguriert werden:

- Quellports dürfen keine Mitglieder von LAGs sein.
- Die Ports dürfen nicht als Zielports konfiguriert werden.
- Es werden bis zu 8 Quellports unterstützt.

So öffnen Sie die Seite **Port Mirroring (Portspiegelung)**: Klicken Sie in der Strukturansicht auf **Switch→ Ports→ Port Mirroring**.

ANMERKUNG: Wenn ein Port als Zielport für eine Portspiegelungs-Sitzung festgelegt wird, werden alle normalen Operationen auf diesem Port ausgesetzt, insbesondere auch Spanning-Tree und LACP.

Abbildung 7-18. Port Mirroring (Portspiegelung)



Die Seite **Port Mirroring (Portspiegelung) enthält folgende Felder:**

Destination Port (Zielport) – Die Nummer des Ports, auf den der Datenverkehr kopiert wird.

Transmit Packets (Pakete übertragen) – Legt fest, wie die Pakete gespiegelt werden. Folgende Feldwerte sind möglich:

Untagged (Ohne Kennung) – Spiegelt die Pakete als VLAN-Pakete ohne Kennung. Dies ist der Standardwert.

Tagged (Mit Kennung) – Spiegelt die Pakete als VLAN-Pakete mit Kennung.

Type (Typ) – Gibt an, ob die gespiegelten Pakete RX-, TX- oder sowohl RX- als auch TX-Pakete sind.

Status (Status) – Zeigt an, ob der Port derzeit überwacht (**Active**) oder nicht überwacht wird (**Ready**).

Remove (Entfernen) – Wenn markiert, wird die Portspiegelungs-Sitzung entfernt.

Hinzufügen einer Portspiegelungs-Sitzung:

1. Öffnen Sie die Seite Port Mirroring (Portspiegelung) .
2. Klicken Sie auf **Add** (hinzufügen).

Die Seite **Add Source Port** (Quellport hinzufügen) wird geöffnet.

3. Definieren Sie die Felder **Source Port** (Quellport) and **Type** (Typ).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).
5. Wählen Sie im Dropdown-Menü **Destination Port** den Zielport aus.
6. Klicken Sie den **Refresh** (Aktualisieren) auf der Seite Port Mirroring (Portspiegelung).
7. Definieren Sie das Feld **Tagged Packets** (Pakete mit Kennung).
8. Definieren Sie das Feld **Type** (Typ).
9. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der neue Quellport wird definiert und das Gerät aktualisiert.

Löschen eines Copy-Ports aus einer Portspiegelungs-Sitzung

1. Öffnen Sie die Seite Port Mirroring (Portspiegelung) .
2. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die ausgewählte Portspiegelungs-Sitzung wird gelöscht und das Gerät aktualisiert.

Konfigurieren einer Portspiegelungs-Sitzung mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite Port Mirroring (Portspiegelung) äquivalenten CLI-Befehle für die Konfiguration einer Portspiegelungs-Sitzung zusammengefasst.

Tabelle 7-8. CLI-Befehle für die Portspiegelung

CLI-Befehl	Beschreibung
port monitor *Quell*-Schnittstelle [**rx** | **tx**]	Startet eine Portspiegelungs-Sitzung.

Im Folgenden ein Beispiel für die CLI-Befehle:

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


console(config-if)# port monitor 1/e2


console (config-if)# end


console# show ports monitor
```

Source Port	Destination Port	Type	Status	VLAN Tagging
----------	----------	----------	----------	----------
1/e2	1/e1	RX, TX	Active	No

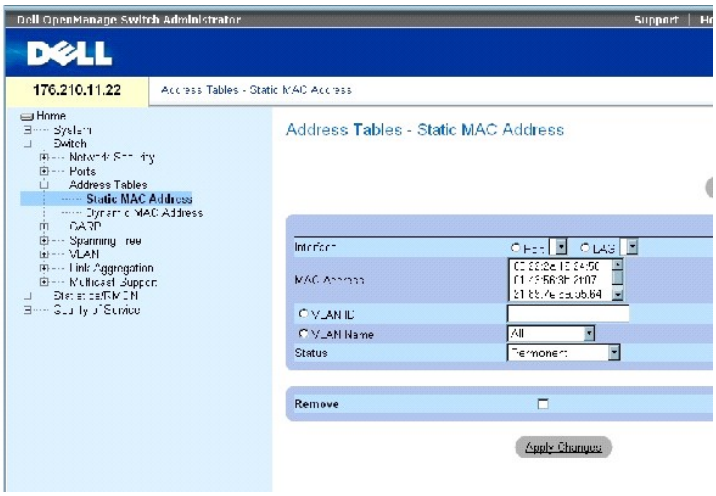
Konfigurieren von Adresstabellen

MAC-Adressen werden entweder in der Datenbank mit statischen oder der Datenbank mit dynamischen Adressen gespeichert. Ein Paket, das an eine Zieladresse adressiert ist, die in einer der Datenbanken gespeichert ist, wird sofort an den jeweiligen Port weitergeleitet. Die Einträge in der dynamischen Adresstabelle können nach Schnittstelle, VLAN oder MAC-Adresse sortiert werden. MAC-Adressen werden dynamisch erfasst, sobald Pakete von einer Quelle am Gerät eingehen. Adressen werden mit Ports verknüpft, indem die Ports aus der Quelladresse des Frames erfasst werden. Frames, die an eine MAC-Zieladresse adressiert sind, welche mit keinem Port verknüpft ist, werden an alle Ports des relevanten VLANs geflutet. Statische Adressen werden manuell konfiguriert. Damit in der Bridging-Tabelle kein Überlauf auftritt, werden dynamische MAC-Adressen gelöscht, von denen über einen gewissen Zeitraum hinweg kein Datenverkehr ausgegangen ist. So öffnen Sie die Seite Address Tables (Adresstabellen): Klicken Sie in der Strukturansicht auf Switch → Address Tables.

Definieren von statischen Adressen

Die Seite Static MAC Address Table (Statische MAC-Adressentabelle) enthält eine Liste statischer MAC-Adressen. Statische Adressen können über die Seite Static MAC Address Table (Statische MAC-Adressentabelle) hinzugefügt und entfernt werden. Außerdem können für einen einzelnen Port mehrere MAC-Adressen definiert werden. So öffnen Sie die Seite Static MAC Address Table (Statische MAC-Adressentabelle): Klicken Sie in der Strukturansicht auf Switch →Address Tables →Static Address Table.

Abbildung 7-19. Static MAC Address Table (Statische MAC-Adressentabelle)



Die Seite Static MAC Address Table (Statische MAC-Adressentabelle) enthält folgende Felder:

Interface (Schnittstelle) – Der spezifische Port bzw. die spezifische LAG, auf die die statische MAC-Adresse angewendet wird.

MAC Address (MAC-Adresse) – Die MAC-Adressen, die in der aktuellen Liste statischer Adressen aufgeführt sind.

VLAN ID (VLAN-ID) – Die mit der MAC-Adresse verknüpfte VLAN-ID.

VLAN Name (VLAN-Name) – Benutzerdefiniertes VLAN.

Status (Status) – Der Status der MAC-Adresse. Folgende Werte sind möglich:

Secure (Sicher) – Wird zur Definition von statischen MAC-Adressen für gesperrte Ports verwendet.

Permanent (Permanent) – Es handelt sich um eine permanente MAC-Adresse.

Delete on Reset (Bei Rücksetzen löschen) – Die MAC-Adresse wird gelöscht, wenn das Gerät zurückgesetzt wird.

Delete on Timeout (Bei Zeitüberschreitung löschen) – Die MAC-Adresse wird bei Auftreten einer Zeitüberschreitung gelöscht.

ANMERKUNG: Stellen Sie sicher, dass der einer statischen MAC-Adresse zugeordnete Port gesperrt ist, um zu verhindern, dass die statische MAC-Adresse bei Rücksetzen des Ethernet- Geräts gelöscht wird.

Remove (Entfernen) – Wenn markiert, wird die gewählte MAC-Adresse aus der MAC-Adresstabelle entfernt.

Hinzufügen einer statischen MAC-Adresse

1. Öffnen Sie die Seite Static MAC Address Table (Statische MAC-Adressentabelle) .
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add Static MAC Address** (Statische MAC-Adresse hinzufügen) wird geöffnet.
3. Füllen Sie die Felder aus.

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

Die neue statische Adresse wird der **Static MAC Address Table** (statische MAC-Adressentabelle) hinzugefügt, und das Gerät wird aktualisiert.

Modifizieren einer statischen Adresseinstellung in der statischen MAC-Adressentabelle

1. Öffnen Sie die Seite Static MAC Address Table (Statische MAC-Adressentabelle).
2. Wählen Sie eine Schnittstelle.
3. Modifizieren Sie die Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die statische MAC-Adresse wird modifiziert und das Gerät aktualisiert.

Entfernen einer statischen Adresse aus der statischen Adresstabelle

1. Öffnen Sie die Seite Static MAC Address Table (Statische MAC-Adressentabelle).
2. Wählen Sie eine Schnittstelle.
3. Klicken Sie auf **Show All** (Alle anzeigen).

Die **Static MAC Address Table** (Statische MAC-Adressentabelle) wird geöffnet.

4. Wählen Sie einen Tabelleneintrag aus.
5. Aktivieren Sie das Kontrollkästchen **Remove** (Entfernen).
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die ausgewählte statische Adresse wird gelöscht und das Gerät aktualisiert.

Konfigurieren von Parametern im Zusammenhang mit statischen Adressen mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite Static MAC Address Table (Statische MAC-Adressentabelle) äquivalenten CLI-Befehle zum Konfigurieren von Parametern im Zusammenhang mit statischen Adressen zusammengefasst.

Tabelle 7-9. CLI-Befehle für statische Adressen

CLI-Befehl	Beschreibung
bridge address *MAC-Adresse* [permanent | delete-on-reset | delete-on-timeout | secure] {ethernet Schnittstelle | port-channel *Port-Kanalnummer*}	Fügt der Bridge-Tabelle eine statische Quelladresse einer MAC-Layer-Station hinzu.
show bridge address-table [**vlan** *VLAN*] [**ethernet** *Schnittstelle* | **port-channel** *Port-Kanalnummer*]	Zeigt Einträge in der Bridge-Weiter-leitungs-daten-bank an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config-if)#bridge address 00:60:70:4C:73:FF permanent ethernet g8

console# show bridge address-table

Aging time is 300 sec
```

vlan	mac address	port	type

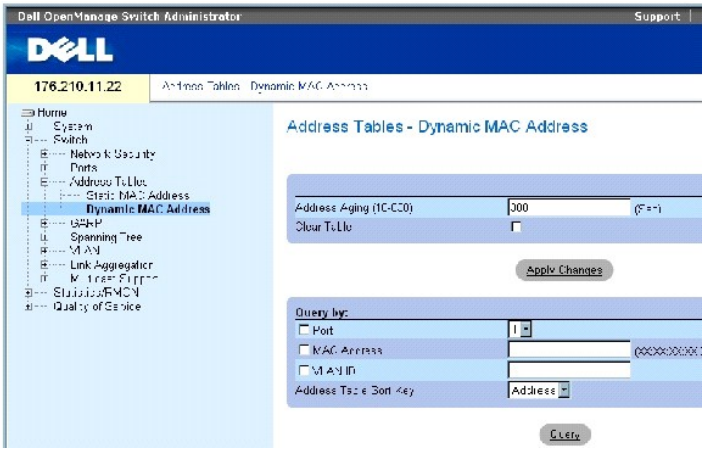
----	----------	----	--------
1	00:60:70:4C:73:FF	1/e8	dynamic
1	00:60:70:8C:73:FF	1/e8	dynamic
200	00:10:0D:48:37:FF	1/e9	static

Anzeigen von dynamischen Adressen

Die Seite**Dynamic MAC Address (Dynamische MAC-Adresse)** enthält Angaben für die Abfrage von Informationen in der dynamischen Adresstabelle, darunter Schnittstellentyp, MAC-Adresse, VLAN und Tabellensortierung. Pakete, die an eine in der Adresstabelle gespeicherte Adresse gerichtet sind, werden direkt an die entsprechenden Ports weitergeleitet. Die Seite **Dynamic MAC Address (Dynamische MAC-Adresse)** enthält außerdem Informationen über die Alterungszeit (Aging Time), nach deren Ablauf eine dynamische MAC-Adresse gelöscht wird, sowie Parameter zum Abfragen und Anzeigen der Liste dynamischer Adressen. Die **Current Address Table** (Aktuelle Adresstabelle) enthält dynamische Adressparameter, anhand derer Pakete direkt an die Ports weitergeleitet werden.

So öffnen Sie die Seite **Dynamic MAC Address (Dynamische MAC-Adresse)**: Klicken Sie in der Strukturansicht auf Switch →Address Tables → Dynamic **MAC Address** .

Abbildung 7-20. Dynamic MAC Address (Dynamische MAC-Adresse)



Die Seite **Dynamic MAC Address (Dynamische MAC-Adresse)** enthält folgende Felder:

Address Aging (10-630) (Zeitgesteuertes Löschen, 10-630) – Legt die Zeitdauer fest, die die MAC-Adresse in der Tabelle Dynamic MAC Address (Dynamische MAC-Adresse) verbleibt, bevor Sie abläuft (d. h. gelöscht wird), sofern während dieser Zeitdauer keine Daten von der Quelle erfasst wurden. Der Standardwert lautet 300 Sekunden.

Clear Table (Tabelle löschen) – Ist dieses Kontrollkästchen markiert, wird die dynamische Adresstabelle gelöscht.

Port (Port) – Gibt die Schnittstelle an, nach der die Tabelle abgefragt wird. Es kann unter zwei Schnittstellentypen ausgewählt werden:

MAC Address (MAC-Adresse) – Legt die MAC-Adresse fest, nach der die Tabelle abgefragt wird.

VLAN ID (VLAN-ID) – Die VLAN-ID, nach der die Tabelle abgefragt wird.

Address Table Sort Key (Sortierschlüssel für Adresstabelle) – Legt die Methode fest, nach der die dynamische Adresstabelle sortiert wird. Die Tabelle kann nach Adresse, VLAN oder Schnittstelle sortiert werden.

Neudefinieren der Alterungszeit

1. Öffnen Sie die Seite **Dynamic MAC Address (Dynamische MAC-Adresse)**.
2. Definieren Sie das Feld **Aging Time** (Alterungszeit).
3. Klicken Sie auf Apply Changes (Änderungen übernehmen).

Die Alterungszeit wird geändert und das Gerät aktualisiert.

Abfragen der dynamischen Adressentabelle

1. Öffnen Sie die Seite **Dynamic MAC Address (Dynamische MAC-Adresse)**.
2. Definieren Sie die Parameter, nach denen die **Dynamic Address Table** (Dynamische Adressentabelle) abgefragt werden soll.

Einträge können nach **Port** (Port), **MAC Address** (MAC-Adresse) oder **VLAN ID** (VLAN-ID) abgefragt werden.

3. Klicken Sie auf **Query** (Abfragen).

Die Dynamic MAC Address (Dynamische MAC-Adresse) (dynamische Adresstabelle) wird abgefragt.

Sortieren der dynamischen Adressentabelle

1. Öffnen Sie die Seite **Dynamic MAC Address (Dynamische MAC-Adresse)**.
2. Wählen Sie im Dropdown-Menü **Address Table Sort Key** (Sortierschlüssel für Adresstabelle) aus, ob die Adressen nach Adresse, VLAN-ID oder Schnittstelle sortiert werden sollen.
3. Klicken Sie auf **Query** (abfragen).

Die Dynamic MAC Address (Dynamische MAC-Adresse) wird sortiert.

Abfragen und Sortieren von dynamischen Adressen mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite Dynamic MAC Address (Dynamische MAC-Adresse) äquivalenten CLI-Befehle zum zeitgesteuerten Löschen sowie zum Abfragen und Sortieren dynamischer Adressen zusammengefasst.

Tabelle 7-10. CLI-Befehle zum Abfragen und Löschen

CLI-Befehl	Beschreibung
bridge aging-time *Sekunden*	Stellt die Alterungsdauer der Adresstabelle ein.
show bridge address-table [**vlan** *VLAN*] [**ethernet** *Schnittstelle* | **port-channel** *Port-Kanalnummer*]	Zeigt Klassen von Einträgen an, die in der Datenbank für die Bridge-Weiterleitung dynamisch erstellt wurden.

Im Folgenden ein Beispiel für die CLI-Befehle:

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

console (config)# end

console# show bridge address-table
```

Aging time is 250 sec

vlan	mac address	port	type
----	----------	----	----
1	00:60:70:4C:73:FF	1/e8	dynamic
1	00:60:70:8C:73:FF	1/e8	dynamic
200	00:10:0D:48:37:FF	1/e8	static

Konfigurieren von GARP

Das Generic Attribute Registration Protocol (GARP) ist ein universell einsetzbares Protokoll, das beliebige Informationen zur Netzwerkkonnektivität oder über Mitgliedschaften registriert. GARP definiert eine Gruppe von Geräten, die an einem bestimmten Netzwerkattribut interessiert sind, beispielsweise an einer VLAN- oder Multicastadresse.

Folgendes ist bei der Konfiguration von GARP zu beachten:

- Die Leave-Zeit muss größer oder gleich der dreimaligen Join-Zeit sein.
- Die Leave-all-Zeit muss größer als die Leave-Zeit sein.
- Stellen Sie auf allen über Layer 2 miteinander verbundenen Geräten die gleichen GARP-Timerwerte ein. Wenn auf über Layer 2 miteinander verbundenen Geräten unterschiedliche GARP-Timer eingestellt sind, funktioniert die GARP-Anwendung nicht wie gewünscht.

So öffnen Sie die Seite GARP: Klicken Sie in der Strukturansicht auf Switch→GARP.

Definieren von GARP-Timern

Die Seite GARP Timers (GARP-Zeitgeber) enthält Felder zum Aktivieren von GARP auf dem Gerät. So öffnen Sie die Seite GARP Timers (GARP-Zeitgeber): Klicken Sie in der Strukturansicht auf Switch → GARP → GARP Timers.

Abbildung 7-21. GARP Timers (GARP-Zeitgeber)

Die Seite GARP Timers (GARP-Zeitgeber) enthält folgende Felder:

Interface (Schnittstelle) – Auswahl eines Ports oder einer LAG für die Bearbeitung der GARP-Timer.

GARP Join Timer (10 - 2147483640) Zeit (in Millisekunden), in der PDUs übertragen werden. Der Standardwert lautet 200 Millisekunden.

GARP Leave Timer (10 - 2147483640) – Gibt die Zeit in Millisekunden an, die ein Gerät vor Verlassen seines GARP-Zustands wartet. Die Leave-Zeit wird durch eine gesendete/empfangene Leave-all-Zeit-Nachricht aktiviert und durch die empfangene Join-Nachricht beendet. Die Leave-Zeit muss größer oder gleich dem Dreifachen der Join-Zeit sein. Der Standardwert lautet 600 Millisekunden.

GARP Leave All Timer (10 - 2147483640) – Gibt die Zeit in Millisekunden an, die alle Geräte vor Verlassen des GARP-Zustands warten. Die Leave-all-Zeit muss größer als die Leave-Zeit sein. Der Standardwert lautet 10000 Millisekunden.

Definieren von GARP-Timern

1. Öffnen Sie die Seite GARP Timers (GARP-Zeitgeber).
2. Wählen Sie eine Schnittstelle.
3. Füllen Sie die Felder aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die GARP-Parameter werden auf dem Gerät gespeichert.

Kopieren von Parametern in der GARP Timers Table (GARP-Zeitgeber-Tabelle)

1. Öffnen Sie die Seite GARP Timers (GARP-Zeitgeber).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die **GARP Timers Table** (GARP-Zeitgeber-Tabelle) wird geöffnet.

3. Wählen Sie im Feld **Copy Parameters from** (Parameter kopieren von) den Schnittstellentyp aus.
4. Wählen Sie entweder im **Port**- oder **LAG**-Dropdown-Menü eine Schnittstelle aus.

Die Definitionen dieser Schnittstelle werden an die gewählten Schnittstellen kopiert. Siehe Schritt 6.

5. Aktivieren Sie das Kontrollkästchen **Copy to** (Kopieren nach), um die Schnittstellen auszuwählen, an die die Definitionen für die GARP-Timer kopiert werden sollen, oder klicken Sie auf **Select All** (Alle auswählen), um die Definitionen an alle Ports oder LAGs zu kopieren.
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Parameter werden an die ausgewählten Ports oder LAGs in der **GARP Timers Table** (GARP-Timer-Tabelle) kopiert, und das Gerät wird aktualisiert.

Definieren von GARP-Timern mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite GARP Timers (GARP-Zeitgeber) äquivalenten CLI-Befehle zum Definieren von GARP-Timern zusammengefasst.

Tabelle 7-11. CLI-Befehle für GARP-Timer

CLI-Befehl	Beschreibung
garp timer {join | leave | leaveall} *Timer-Wert*	Stellt die Join-, Leave- und Leaveall-GARP-Zeitgeberwerte der GARP-Anwendung ein.

Im Folgenden ein Beispiel für die CLI-Befehle:

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

console(config-if)# garp timer leave 900

console(config-if)# end

console# show gvrp configuration ethernet 1/e11


GVRP Feature is currently Disabled on the device.

Maximum VLANs: 223
```

Port (s)	GVRP-Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
1/e11	Disabled	Normal	Enabled	200	900	10000

Konfigurieren des Spanning-Tree-Protokolls

Das Spanning-Tree-Protokoll (STP) sorgt bei beliebigen Bridge-Anordnungen für eine Baumtopologie. STP stellt zwischen zwei beliebigen Endstationen genau einen Pfad bereit und vermeidet so Netzwerkschleifen.

Schleifen treten auf, wenn zwischen Hosts alternative Leitwege existieren. Schleifen in einem erweiterten Netzwerk können dazu führen, dass die Bridges Datenverkehr unbegrenzt weiterleiten. Dies führt zu erhöhtem Datenaufkommen und einer Minderung der Netzwerkeffizienz.

Das Gerät unterstützt folgende Versionen des Spanning-Tree-Protokolls:

- Classic STP – Stellt zwischen zwei beliebigen Endstationen jeweils genau einen Pfad bereit und vermeidet bzw. eliminiert so Netzwerkschleifen. Weitere Informationen zur Konfiguration von klassischem STP finden Sie unter **Festlegen von globalen STP-Einstellungen**.
- Rapid STP – Erkennt und verwendet diejenigen Netzwerktopologien, bei denen der aufgespannte Baum schneller konvergiert, ohne dass dabei Weiterleitungsschleifen erzeugt werden. Wenn auf dem Gerät RSTP aktiviert ist, auf dem Nachbargerät aber STP aktiviert ist, benutzt das lokale Gerät STP.

  Weitere Informationen zur Konfiguration von RSTP finden Sie unter **Definieren von Rapid Spanning Tree**.

- Multiple STP – Stellt volle Konnektivität für Pakete zur Verfügung, die beliebigen VLANs zugeordnet sein können. Multiple STP basiert auf RSTP. Zusätzlich überträgt Multiple STP Pakete, die verschiedenen VLANs zugeordnet sind, durch verschiedene MST-Regionen. Wenn auf dem Gerät MSTP aktiviert ist, fungieren die MST-Regionen als einzelne Brücke. Wenn jedoch auf dem Nachbar-gerät RSTP aktiviert ist und das lokale Gerät STP, RSTP und MSTP benutzt, sind beide Geräte interoperabel.

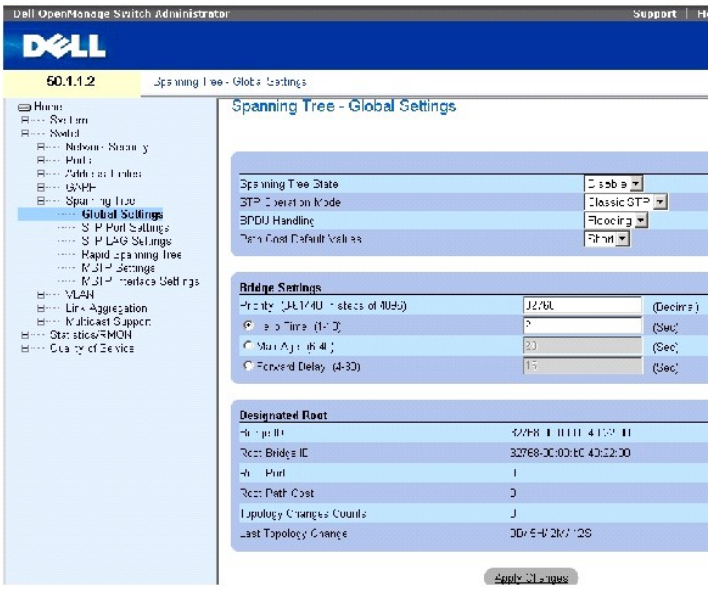
Weitere Informationen zur Konfiguration von Multiple STP finden Sie unter **Konfigurieren von Multiple Spanning Tree**.

So öffnen Sie die Seite **Spanning Tree**: Klicken Sie in der Strukturansicht auf **Switch→ Spanning Tree** .

Festlegen von globalen STP-Einstellungen

Die Seite Spanning Tree Global Settings (Globale Spanning-Tree-Einstellungen) enthält Parameter zum Aktivieren von STP auf dem Gerät. So öffnen Sie die Seite Spanning Tree Global Settings (Globale Spanning-Tree-Einstellungen): Klicken Sie in der Strukturansicht auf **Switch→ Spanning Tree→ Global Settings**.

Abbildung 7-22. Spanning Tree Global Settings (Globale Spanning-Tree-Einstellungen)



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

Spanning Tree State (Spanning-Tree-Zustand) – Aktiviert oder deaktiviert auf dem Gerät STP, Rapid STP oder MSTP.

STP Operation Mode (STP-Betriebsmodus) – Gibt den STP-Modus an, gemäß dem STP auf dem Gerät aktiviert wird. Folgende Feldwerte sind möglich:

Classic STP — Aktiviert auf dem Gerät Classic STP. Dies ist der Standardwert.

Rapid STP — Aktiviert auf dem Gerät Rapid STP.

Multiple STP — Aktiviert auf dem Gerät Multiple STP.

BPDU Handling (BPDU-Behandlung) – Legt fest, wie BPDU-Pakete behandelt werden, wenn auf dem Port/Gerät STP deaktiviert ist. BPDUs werden verwendet, um Spanning-Tree-Informationen zu übermitteln. Folgende Feldwerte sind möglich:

Filtering (Filtern) – Wenn auf einer Schnittstelle Spanning-Tree deaktiviert ist, werden BPDU-Pakete ausgefiltert. Dies ist der Standardwert.

Flooding (Fluten) – Wenn auf einer Schnittstelle Spanning-Tree deaktiviert ist, werden BPDU-Pakete geflutet.

Path Cost Default Values (Pfadkosten-Standardwerte) – Gibt die Methode an, nach der Standardwerte für die Pfadkosten an STP-Ports zugewiesen werden. Folgende Feldwerte sind möglich:

Short (Kurz) – Legt für die an die Ports zugewiesenen Pfadkosten einen Wertebereich von 1 bis 65535 fest. Dies ist der Standardwert.

Long (lang) – Legt für die an die Ports zugewiesenen Pfadkosten einen Wertebereich von 1 bis 200000000 fest.

Die einer Schnittstelle zugewiesenen Standard-Pfadkosten hängen von der ausgewählten Methode ab:

Schnittstelle	Lang	Kurz
LAG	20000	4
1000 MBit/s	20000	4
100 MBit/s	200000	19
10 MBit/s	2000000	100

Priority (0-65535) (Priorität, 0 bis 65535) – Legt den Wert für die Bridge-Priorität fest. Wenn auf Switches oder Bridges STP ausgeführt wird, wird jedem Switch und jeder Bridge eine Priorität zugewiesen. Nach dem Austausch der BPDUs wird das Gerät mit dem niedrigsten Prioritätswert zur Root-Bridge. Der Standardwert lautet 32768. Der Wert für die Port-Priorität wird in Schritten von 4096 angegeben, beispielsweise 4096, 8192, 12288 usw.

Hello Time (1-10) (Hello-Zeit, 1 bis 10) – Legt die Hello-Zeit des Geräts fest. Die Hello-Zeit gibt die Zeitdauer in Sekunden an, die eine Root-Bridge zwischen Konfigurationsnachrichten abwartet. Der Standardwert beträgt zwei Sekunden.

Max Age (6-40) (Max. Alter, 6 bis 40) – Legt die maximale Alterungszeit für das Gerät fest. Die maximale Alterungszeit entspricht der Zeit in Sekunden, die eine Bridge wartet, bevor sie Konfigurationsnachrichten sendet. Der Standardwert für die maximale Alterungszeit beträgt 20 Sekunden.

Forward Delay (4-30) (Weiterleitungsverzögerung, 4 bis 30) – Legt die Weiterleitungsverzögerung für das Gerät fest. Die Weiterleitungsverzögerung gibt die Zeitdauer in Sekunden an, die eine Bridge in einem Lausch- und Erfassungszustand verbleibt, bevor Sie mit der Weiterleitung von Paketen beginnt. Der Standardwert lautet 10 Sekunden.

Bridge ID (Bridge-ID) – Bezeichnet Priorität und MAC-Adresse der Bridge.

Root Bridge ID (Root-Bridge-ID) – Bezeichnet Priorität und MAC-Adresse der Root-Bridge.

Root Port (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.

Root Path Cost (Root-Pfadkosten) – Die Kosten des Pfads von dieser Bridge bis zum Root-Gerät.

Topology Changes Counts (Zähler für Topologieänderungen) – Gibt die Gesamtanzahl der aufgetretenen STP-Zustandsänderungen an.

Last Topology Change (Letzte Topologieänderung) – Gibt die Zeit an, die verstrichen ist, seit die Bridge zuletzt initialisiert oder zurückgesetzt wurde und die letzte Topologieänderung aufgetreten ist. Die Zeit wird im Format Tag/Stunde/Minute/Sekunde angezeigt, z.B. 2D/5H/10M/4S (2 Tage, 5 Stunden, 10 Minuten, 4 Sekunden).

Festlegen von globalen STP-Parametern

1. Öffnen Sie die Seite Spanning Tree Global Settings (Globale Spanning-Tree- Einstellungen).
2. Wählen Sie im Feld **Spanning Tree State** (Spanning-Tree-Zustand) **Enable** (Aktivieren) aus.
3. Wählen Sie im Feld **STP Operation Mode** (STP-Betriebsmodus) den **STP**-Modus aus, und definieren Sie die Bridge-Einstellungen.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

STP wird auf dem Gerät aktiviert.

Modifizieren globaler STP-Parameter

1. Öffnen Sie die Seite Spanning Tree Global Settings (Globale Spanning-Tree- Einstellungen).
2. Legen Sie die im Dialogfeld verfügbaren Einstellungen fest.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die STP-Parameter werden modifiziert und das Gerät aktualisiert.

Festlegen globaler STP-Parameter mit Hilfe von CLI-Befehlen.

In der folgenden Tabelle werden die der Seite **Spanning Tree Global Settings** (Globale Spanning-Tree-Einstellungen) äquivalenten CLI-Befehle zum Festlegen von globalen STP-Parametern zusammengefasst.

Tabelle 7-12. CLI-Befehle für globale STP-Parameter

CLI-Befehl	Beschreibung
spanning-tree	Aktiviert die Spanning-Tree-Funktion.
spanning-tree mode {**stp** | **rstp** | **mstp**}	Konfiguriert den Modus des Spanning-Tree-Protokolls.
spanning-tree priority Priorität	Konfiguriert die Spanning-Tree-Priorität.
spanning-tree hello-time *Sekunden*	Konfiguriert die Hello-Zeit der Spanning-Tree-Bridge, die angibt, wie häufig das Gerät Hello-Nachrichten an andere Geräte sendet.
spanning-tree max-age *Sekunden*	Konfiguriert die maximale Alterungszeit der Spanning-Tree-Bridge.
spanning-tree forward- time Sekunden	Konfiguriert die Weiterleitungszeit für die Spanning Tree-Bridge. Diese gibt die Zeitdauer an, die ein Port im Lausch- und Erfassungszustand verbleibt, bevor er in den Weiterleitungszustand übergeht.
show spanning-tree [**ethernet** *Schnittstelle* | **port-channel** *Port- Kanalnummer*] [**instance** *Instanz-ID*]	Zeigt die Spanning-Tree-Konfiguration an.
show spanning-tree [**detail**] [**active** | **blockedports**] [**instance** *Instanz-ID*]	Zeigt detaillierte Spanning-Tree-Informationen über aktive oder blockierte Ports an.
show spanning-tree mst- configuration	Zeigt die Spanning-Tree-MST-Konfigurations-ID an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# spanning-tree

console(config)# spanning-tree mode rstp

console(config)# spanning-tree priority 12288

console(config)# spanning-tree hello-time 5
```

```
console(config)# spanning-tree max-age 12

console(config)# spanning-tree forward-time 25

console(config)# exit

console# show spanning-tree

Spanning tree enabled mode MSTP

Default port cost method: short

Gathering information .........

###### MST 0 Vlans Mapped:                16-4094

CST Root ID Priority 20480

         Address                         00:30:ab:00:00:08

         Path Cost                       4

         Root Port                       ch2

         This switch is the IST master

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

Bridge ID Priority                       32768

         Address                         00:00:00:16:00:64

         Max hops                        20

Name   State    Prio.Nbr  Cost  Sts   Role  PortFast  Type
----   -----    -------   ----  ---   ----  -------   ----
1/e2   enabled  128.2     100   DSBL  Dsbl  No        P2p Intr
1/e3   enabled  128.3     100   DSBL  Dsbl  No        P2p Intr
1/e4   enabled  128.4     100   DSBL  Dsbl  No        P2p Intr
```

1/e5	enabled	128.5	19	FRW	Desg	Yes	P2p Intr
1/e6	enabled	128.6	100	DSBL	Dsbl	No	P2p Intr
1/e7	enabled	128.7	100	DSBL	Dsbl	No	P2p Intr
1/e8	enabled	128.8	100	DSBL	Dsbl	No	P2p Intr
1/e9	enabled	128.9	100	DSBL	Dsbl	No	P2p Intr
1/e10	enabled	128.10	100	DSBL	Dsbl	No	P2p Intr
1/e11	enabled	128.11	19	DSBL	Desg	Yes	P2p Intr

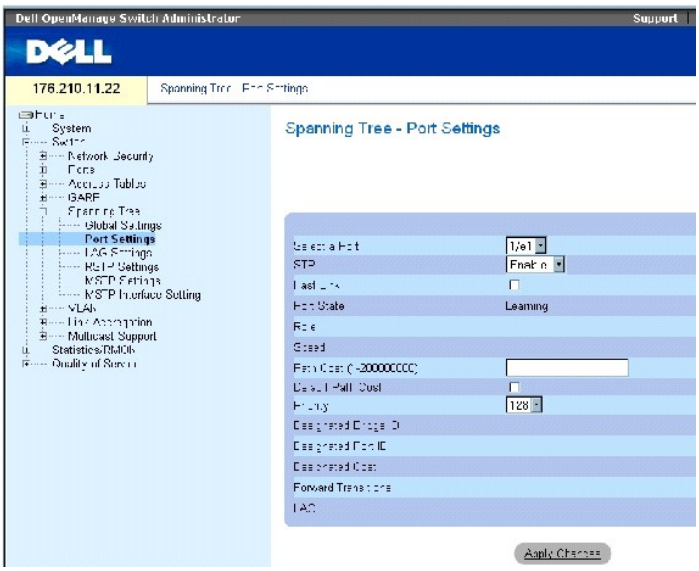
```
console# show spanning-tree active

Spanning tree enabled mode MSTP

Default port cost method: short

Gathering information .........

###### MST 0 Vlans Mapped: 16-4094

CST Root ID Priority 20480
    Address                   00:30:ab:00:00:08
    Path Cost                 4
    Root Port                 ch2
    This switch is the IST master
    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority            32768
    Address                   00:00:00:16:00:64
    Max hops                  20

Name    State    Prio.Nbr    Cost    Sts    Role    PortFast    Type
----    -----    -------     ----    ---    ----    -------     ----
```

1/e5	enabled	128.2	19	FRW	Desg	Yes	P2p Intr
1/e7	enabled	128.7	19	DSCR	Altn	No	P2p Bound (STP)
1/e11	enabled	128.11	19	FRW	Desg	Yes	P2p Intr
1/e15	enabled	128.15	19	FRW	Desg	No	P2p Intr
1/e22	enabled	128.22	19	FRW	Desg	Yes	P2p Intr

Definieren von STP-Porteinstellungen

Benutzen Sie die Seite **Spanning Tree Port Settings** (Spanning-Tree-Porteinstellungen), um einzelnen Ports STP-Eigenschaften zuzuweisen. So öffnen Sie die Seite Spanning Tree Port Settings (Spanning-Tree-Porteinstellungen): Klicken Sie in der Strukturansicht auf **Switch**→ **Spanning Tree**→ **Port Settings**.

Abbildung 7-23. Spanning Tree Port Settings (Spanning-Tree-Porteinstellungen)



Die Seite **Spanning Tree Global Settings** (Spanning-Tree-Porteinstellungen) enthält folgende Felder:

Select a Port (Portauswahl) – Bezeichnet die Nummer des Ports, dessen STP-Einstellungen modifiziert werden.

STP (STP) – Aktiviert oder deaktiviert STP auf dem Port.

Fast Link (Schnelle Verbindung) – Ist dieses Kontrollkästchen markiert, wird der Fast-Link-Modus für den Port aktiviert. Falls der Fast-Link-Modus für einen Port aktiviert ist, wird der **Port State** (Portzustand) automatisch in den Zustand **Forwarding** (Weiterleitung) versetzt, sobald auf dem Port eine Verbindung besteht. Der Fast-Link-Modus optimiert die Zeit, die benötigt wird, bis das STP-Protokoll konvergiert. Bis zum Konvergieren des STP können in großen Netzwerken zwischen 30 und 60 Sekunden verstreichen.

Port State (Portzustand) – Gibt den aktuellen STP-Zustand eines Ports an. Falls aktiviert, legt der Portzustand fest, wie der Port mit Datenverkehr umgeht. Folgende Portzustände sind möglich:

Disabled (Deaktiviert) – STP ist derzeit auf dem Port deaktiviert. Der Port leitet Datenverkehr weiter und erfasst dabei MAC-Adressen.

Blocking (Blockieren) – Der Port ist derzeit blockiert und kann nicht für die Weiterleitung von Datenverkehr oder die Erfassung von MAC-Adressen verwendet werden. Wird angezeigt, wenn Classic STP aktiviert ist.

Listening (Lauschen) – Der Port befindet sich derzeit im Lauschmodus. Der Port kann weder Datenverkehr weiterleiten noch MAC-Adressen erfassen.

Learning (Erfassen) – Der Port befindet sich derzeit im Erfassungsmodus. Der Port kann keinen Datenverkehr weiterleiten, er kann jedoch neue MAC-Adressen erfassen.

Forwarding (Weiterleiten) – Der Port befindet sich derzeit im Weiterleitungsmodus. Der Port kann Datenverkehr weiterleiten und neue MAC-Adressen erfassen.

Role (Funktion) – Gibt die Portfunktion an, die der STP-Algorithmus dem Port zugewiesen hat, um STP-Pfade bereitstellen. Folgende Feldwerte sind möglich:

Root (Wurzel) – Stellt den kostengünstigsten Pfad für die Weiterleitung von Paketen an den Root-Switch bereit.

Designated (Designiert) – Gibt den Port an, über den der designierte Switch an das LAN angeschlossen ist.

Alternate (Alternativ) – Stellt für die Weiterleitung von Paketen zum Root-Switch einen zur Weiterleitung über die Root-Schnittstelle alternativen Pfad bereit.

Backup (Reserve) – Stellt einen Reservepfad zu den Endgeräten (Blättern) des Spanning-Tree als Alternative zu dem designierten Portpfad bereit. Reserveports treten nur auf, wenn zwei Ports durch eine Punkt-zu-Punkt-Verbindung in einer Schleife miteinander verbunden sind. Reserveports treten auch auf, wenn ein LAN zwei oder mehr Verbindungen zu einem gemeinsamen Segment aufweist.

Disabled (Deaktiviert) Gibt an, dass der Port nicht an dem von Spanning-Tree aufgespannten Baum teilnimmt.

Speed (Geschwindigkeit) – Die Geschwindigkeit, mit der der Port betrieben wird.

Path Cost (1-200000000) (Pfadkosten) – Der Anteil dieses Ports an den Root-Pfadkosten. Wenn der Leitweg eines Pfads geändert wird, werden die Kosten für den Pfad auf einen höheren oder niedrigen Wert gesetzt und entsprechend zur Weiterleitung von Datenverkehr herangezogen.

Default Path Cost (Standardpfadkosten) – Die standardmäßig vorgegebenen Kosten für den Pfad. Die Standardwerte für Pfadkosten im Langformat lauten:

Ethernet – 2000000

Fast Ethernet – 200000

Gigabit Ethernet – 20000

Die Standardwerte für Pfadkosten im Kurzformat lauten:

Ethernet – 100

Fast Ethernet – 19

Gigabit Ethernet – 4

Priority (0-240, in steps of 16) (Priorität, von 0 bis 240, in 16er-Schritten) – Prioritätswert des Ports. Der Prioritätswert beeinflusst die Portwahl, wenn eine Brücke zwei Ports in einer Schleifenkonfiguration aufweist. Der Prioritätswert liegt zwischen 0 und 240 und wird in 16er-Schritten angegeben.

Designated Bridge ID (ID der designierten Bridge) – Bridge-Priorität und MAC-Adresse der designierten Bridge.

Designated Port ID (ID des designierten Ports) – Priorität und Schnittstelle des designierten Ports.

Designated Cost (Designierte Kosten) – Kosten des an der STP-Topologie teilnehmenden Ports. Wenn STP eine Schleifenkonfiguration entdeckt, werden Ports mit niedrigeren Kosten mit geringerer Wahrscheinlichkeit blockiert.

Forward Transitions (Weiterleitungsübergänge) – Gibt an, wie oft der Port vom Zustand **Forwarding** (Weiterleiten) in den Zustand **Blocking** (Blockieren) gewechselt ist.

LAG – Die LAG, mit der der Port verknüpft ist.

Aktivieren von STP auf einem Port

1. Öffnen Sie die Seite **Spanning Tree Port Settings** (Spanning-Tree-Porteinstellungen).
2. Wählen Sie den Port aus.
3. Wählen Sie im Feld **STP** den Eintrag **Enabled** (Aktiviert) aus.
4. Definieren Sie die Felder **Fast Link** (schnelle Verbindung), **Path Cost** (Pfadkosten) und **Priority** (Priorität).
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

STP wird auf dem Port aktiviert.

Modifizieren von STP-Porteigenschaften

1. Öffnen Sie die Seite **Spanning Tree Port Settings** (Spanning-Tree-Porteinstellungen).
2. Wählen Sie den Port aus.
3. Modifizieren Sie die relevanten Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die STP-Portparameter werden geändert und das Gerät aktualisiert.

Anzeigen der STP Port Table (STP-Porttabelle)

1. Öffnen Sie die Seite **Spanning Tree Port Settings** (Spanning-Tree-Porteinstellungen).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die **STP Port Table** (STP-Porttabelle) wird geöffnet.

Festlegen von STP-Porteinstellungen mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite **Spanning Tree Global Settings** (globale Spanning-Tree-Einstellungen) äquivalenten CLI-Befehle zum Festlegen von STP-Portparametern zusammengefasst.

Tabelle 7-13. CLI-Befehle für STP-Porteinstellungen

CLI-Befehl	Beschreibung
spanning-tree disable	Deaktiviert Spanning-Tree auf einem spezifischen Port.
spanning-tree cost cost	Konfiguriert die Kostenbeitrag eines Ports zum Spanning-Tree.
spanning-tree port-priority Priorität	Konfiguriert die Portpriorität.
show **spanning-tree** [**ethernet** Schnittstelle | **port-channel** Port-Kanalnummer] [**instance** *Instanz-ID*]	Zeigt die Spanning-Tree-Konfiguration an.
spanning-tree portfast	Aktiviert den PortFast-Modus.
show spanning-tree [detail] [**active** | **blockedports**] [**instance** *Instanz-ID*]	Zeigt detaillierte Spanning-Tree-Informationen über aktive oder blockierte Ports an.
show spanning-tree mst- configuration	Zeigt die Spanning-Tree-MST-Konfigurations-ID an.

Im Folgenden ein Beispiel für die CLI-Befehle:

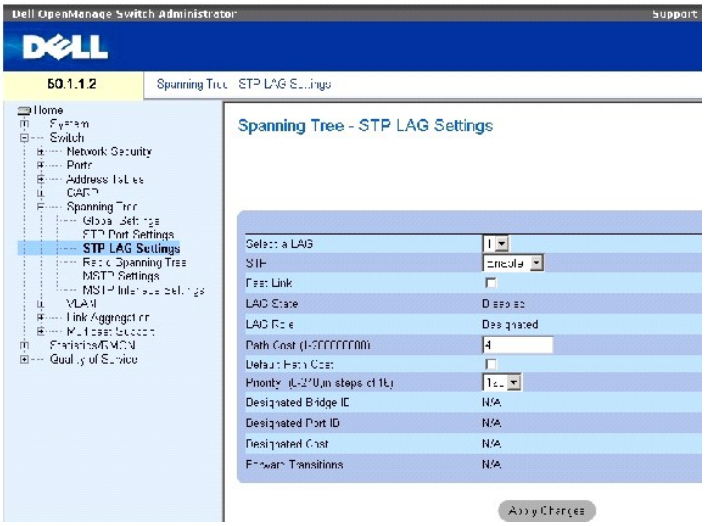
```
console> enable

console# configure

Console(config)# interface ethernet 1/e1

Console(config-if)# spanning-tree disable

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

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

Console(config-if)# spanning-tree portfast

Console(config-if)# exit

Console(config)# exit

Console# show spanning-tree ethernet 1/e15

Port 1/e15 enabled
```

State: forwarding			Role: designated	
Port id: 128.15			Port cost: 19	
Type: P2p (configured: Auto) Internal Port Fast: No (configured: No)				
Designated bridge Priority : 32768			Address: 00:00:00:16:00:64	
Designated port id: 128.15			Designated path cost: 4	
Guard root: Disabled				
Number of transitions to forwarding state: 2				
BPDU: sent 483, received 1037				
console# **show spanning-tree ethernet** 1/e15 **instance** 12				
Port 1/e15 enabled				
State: discarding			Role: alternate	
Port id: 128.15			Port cost: 19	
Type: P2p (configured: Auto) Internal Port Fast: No (configured: No)				
Designated bridge Priority : 32768			Address: 00:00:b0:07:07:49	
Designated port id: 128.11			Designated path cost: 0	
Guard root: Disabled				
Number of transitions to forwarding state: 3				
BPDU: sent 482, received 1035				

Definieren von STP-LAG-Einstellungen

Verwenden Sie die Seite **Spanning Tree LAG Settings** (Spanning-Tree-LAG-Einstellungen), um STP-Parameter für aggregierte Ports zuzuweisen. So öffnen Sie die Seite LAG Settings: Klicken Sie in der Strukturansicht auf **Switch**→ **Spanning Tree**→ **LAG Settings**.

Abbildung 7-24. Spanning Tree LAG Settings (Spanning-Tree-LAG-Einstellungen)



Die Seite **Spanning Tree LAG Settings** (Spanning-Tree-LAG-Einstellungen) enthält folgende Felder:

Select a LAG (LAG auswählen) – Die LAG-Nummer, deren STP-Einstellungen Sie modifizieren möchten.

STP (STP) – Aktiviert oder deaktiviert STP auf der LAG.

Fast Link (schnelle Verbindung) – Aktiviert den Fast-Link-Modus auf der LAG. Falls der Fast-Link-Modus für eine LAG aktiviert ist, wird der **LAG State** (LAG-Zustand) automatisch in den Zustand **Forwarding** (Weiterleitung) versetzt, sobald auf der LAG eine Verbindung besteht. Der Fast-Link-Modus optimiert die Zeit, die benötigt wird, bis das STP-Protokoll konvergiert. Bis zum Konvergieren des STP können in großen Netzwerken zwischen 30 und 60 Sekunden verstreichen.

LAG State (LAG-Zustand) – Der aktuelle STP-Zustand einer LAG. Falls aktiviert, legt der LAG-Zustand fest, wie die LAG mit Datenverkehr umgeht. Wenn die Bridge eine fehlerhaft arbeitende LAG entdeckt, wird diese in den Zustand **Broken** (Defekt) versetzt. Folgende LAG-Zustände sind möglich:

Disabled (Deaktiviert) – STP ist derzeit auf der LAG deaktiviert. Die LAG leitet Datenverkehr weiter und erfasst dabei MAC-Adressen.

Blocking (Blockieren) – Die LAG ist blockiert und kann nicht für die Weiterleitung von Datenverkehr oder die Erfassung von MAC-Adressen verwendet werden.

RSTP Discarding State (RSTP-Zustand Verwerfen) – In diesem Zustand lernt der Port keine MAC-Adressen und leitet keine Frames weiter.

Dieser Zustand vereint in sich die Zustände Blocking (Blockieren) und Listening (Lauschen), die in STP (802.1.D) eingeführt wurden.

Listening (Lauschen) – Die LAG ist im Lauschmodus und kann weder Datenverkehr weiterleiten noch MAC-Adressen erfassen.

Learning (erfassen) – Die LAG ist im Erfassungsmodus und kann keinen Datenverkehr weiterleiten, jedoch kann sie neue MAC-Adressen erfassen.

Forwarding (Weiterleiten) – Die LAG ist derzeit im Weiterleitungsmodus und kann Datenverkehr weiterleiten und neue MAC-Adressen erfassen.

Broken (Defekt) – Die LAG funktioniert derzeit nicht korrekt und kann nicht zur Weiterleitung von Datenverkehr verwendet werden.

LAG Role (Funktion) – Gibt die Funktion an, die der STP-Algorithmus der LAG zugewiesen hat, um STP-Pfade bereitstellen. Folgende Feldwerte können ausgewählt werden:

Root (Wurzel) – Stellt den kostengünstigsten Pfad für die Weiterleitung von Paketen an den Root-Switch bereit.

Designated (designiert) – Gibt die LAG an, über die der designierte Switch an das LAN angeschlossen ist.

Alternate (Alternativ) – Stellt für die Weiterleitung von Paketen zum Root-Switch eine zur Weiterleitung über die Root-Schnittstelle alternative LAG bereit.

Backup (Reserve) – Stellt einen Reservepfad zu den Endgeräten (Blättern) des Spanning-Tree als Alternative zu dem designierten Portpfad bereit. Reserveports treten nur auf, wenn zwei Ports durch eine Punkt-zu-Punkt-Verbindung in einer Schleife miteinander verbunden sind. Reserveports treten auch auf, wenn ein LAN zwei oder mehr Verbindungen zu einem gemeinsamen Segment aufweist.

Disabled (Deaktiviert) – Gibt an, dass die LAG nicht an dem von Spanning-Tree aufgespannten Baum teilnimmt.

Path Cost (1-200000000) (Pfadkosten) – Der Anteil dieser LAG an den Root-Pfadkosten. Wenn der Leitweg eines Pfads geändert wird, werden die Kosten für den Pfad auf einen höheren oder niedrigen Wert gesetzt und entsprechend zur Weiterleitung von Datenverkehr herangezogen. Die Pfadkosten können einen Wert zwischen 1 und 200000000 haben.

Default Path Cost (Standardpfadkosten) – Zeigt an, ob die Standardpfadkosten benutzt werden. Die möglichen Standardwerte für LAG-Pfadkosten sind:

Langformat für LAG – 20000

Kurzformat für LAG – 4

Priority (0-240, in steps of 16) (Priorität, von 0 bis 240, in 16er-Schritten) – Prioritätswert der LAG. Der Prioritätswert beeinflusst die LAG-Wahl, wenn eine Brücke Ports in einer Schleifenkonfiguration aufweist. Der Prioritätswert liegt zwischen 0 und 240 und wird in 16er-Schritten angegeben.

Designated Bridge ID (ID der designierten Bridge) – Priorität und MAC-Adresse der designierten Bridge.

Designated Port ID (ID des designierten Ports) – Die ID der ausgewählten Schnittstelle.

Designated Cost (designierte Kosten) – Kosten des an der STP-Topologie teilnehmenden Ports. Wenn STP eine Schleifenkonfiguration entdeckt, werden Ports mit niedrigeren Kosten mit geringerer Wahrscheinlichkeit blockiert.

Forward Transitions (Weiterleitungsübergänge) – Gibt an, wie oft der **LAG-Zustand** vom Zustand **Forwarding** (Weiterleiten) in den Zustand **Blocking** (Blockieren) gewechselt ist.

Modifizieren der STP-Parameter für die LAG

1. Öffnen Sie die Seite **Spanning Tree LAG Settings** (Spanning-Tree-LAG-Einstellungen).
2. Wählen Sie im Dropdown-Menü **Select a LAG** (LAG auswählen) eine LAG aus.
3. Modifizieren Sie die Felder nach Wunsch.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die STP-Parameter für die LAG werden geändert und das Gerät aktualisiert.

Definieren von STP-LAG-Einstellungen mit Hilfe von CLI-Befehlen

Die folgende Tabelle enthält die CLI-Befehle zum Definieren von STP-LAG-Einstellungen.

Tabelle 7-14. CLI-Befehle für STP-LAG-Einstellungen

CLI-Befehl	Beschreibung
`spanning-tree`	Aktiviert Spanning-Tree.
`spanning-tree disable`	Deaktiviert Spanning-Tree auf einer spezifischen LAG.
`spanning-tree cost` *`Kosten`*	Konfiguiert die Kostenbeitrag einer LAG zum Spanning-Tree.
`spanning-tree port-priority` *`Priorität`*	Konfiguriert die Portpriorität.
`show spanning-tree [`**`ethernet`** `Schnittstelle | `**`port-channel`** *`Port-Kanalnummer`*`] [`**`instance`** *`Instanz-ID`*`]`	Zeigt die Spanning-Tree-Konfiguration an.
`show spanning-tree [detail] [active | blockedports] [`**`instance`** *`Instanz-ID`*`]`	Zeigt detaillierte Spanning-Tree-Informationen über aktive oder blockierte Ports an.

Im Folgenden ein Beispiel für die CLI-Befehle:

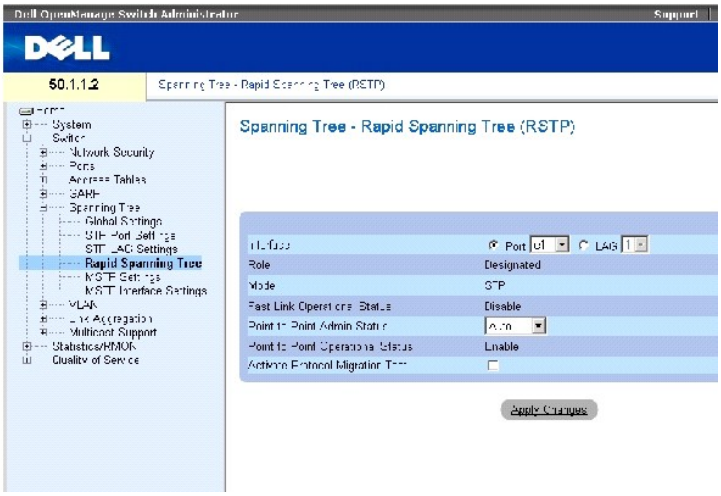
```
console(config)# interface
port-channel 1

console(config-if)#
spanning-tree disable

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

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

console(config-if)#
spanning-tree portfast
```

Definieren von Rapid Spanning Tree

Zwar verhindert das klassische Spanning-Tree-Protokoll in allgemeinen Netzwerktopologien Schleifenkonfigurationen, jedoch können ca. 30 bis 60 Sekunden verstreichen, bis das Protokoll konvergiert. Diese Verzögerungszeit wird benötigt, um mögliche Schleifen zu erkennen und Statusänderungen zu verbreiten.

Das Rapid Spanning Tree Protocol (RSTP) erkennt und benutzt Netzwerktopologien, die ein schnelleres Konvergieren des Spanning-Tree ermöglichen, ohne dabei Weiterleitungsschleifen zuzulassen. So öffnen Sie die Seite Rapid Spanning Tree Settings (RSTP-Einstellungen): Klicken Sie in der Strukturansicht auf **Switch→ Spanning Tree→ Rapid Spanning Tree**.

Abbildung 7-25. Rapid Spanning Tree Settings (RSTP-Einstellungen)



Die Seite RSTP-Einstellungsseite enthält folgende Felder:

Interface (Schnittstelle) – Port oder LAG, deren RSTP-Einstellungen angezeigt und bearbeitet werden können.

State(Zustand) – Deaktiviert den RSTP-Zustand der ausgewählten Schnittstelle.

Role (Funktion) – Gibt die Funktion an, die der STP-Algorithmus dem Port zugewiesen hat, um STP-Pfade bereitstellen. Folgende Feldwerte sind möglich:

Root (Wurzel) – Stellt den kostengünstigsten Pfad für die Weiterleitung von Paketen an den Root-Switch bereit.

Designated (Designiert) – Gibt den Port bzw. die LAG an, über den/die der designierte Switch an das LAN angeschlossen ist.

Alternate (Alternativ) – Stellt für die Weiterleitung von Paketen zum Root-Switch einen zur Weiterleitung über die Root-Schnittstelle alternativen Pfad bereit.

Backup (Reserve) – Stellt einen Reservepfad zu den Endgeräten (Blättern) des Spanning-Tree als Alternative zu dem designierten Portpfad bereit. Reserveports treten nur auf, wenn zwei Ports durch eine Punkt-zu-Punkt-Verbindung in einer Schleife miteinander verbunden sind. Reserveports treten auch auf, wenn ein LAN zwei oder mehr Verbindungen zu einem gemeinsamen Segment aufweist.

Disabled (deaktiviert) – Gibt an, dass der Port nicht an dem von Spanning-Tree aufgespannten Baum teilnimmt.

Mode (Modus) – Bezeichnet den aktuellen Spanning-Tree-Modus. Der Spanning-Tree-Modus kann auf der Seite Spanning Tree Global Settings (Globale Spanning-Tree-Einstellungen) ausgewählt werden. Folgende Feldwerte sind möglich:

Classic STP – Zeigt an, dass auf dem Gerät Classic STP aktiviert ist.

Rapid STP – Zeigt an, dass auf dem Gerät Rapid STP aktiviert ist.

Multiple STP – Zeigt an, dass auf dem Gerät Multiple STP aktiviert ist.

Fast Link Operational Status (Fast-Link-Betriebsstatus) – Zeigt an, ob der Fast-Link-Modus auf dem Port bzw. der LAG aktiviert oder deaktiviert ist. Falls Fast-Link für eine Schnittstelle aktiviert ist, wird die Schnittstelle automatisch in den Weiterleitungszustand versetzt.

Point-to-Point Admin Status (Aministrierter Punkt-zu-Punkt-Status) – Aktiviert oder deaktiviert die Herstellung einer Punkt-zu-Punkt-Verbindung durch das Gerät, oder legt fest, dass das Gerät automatisch eine Punkt-zu-Punkt-Verbindung herstellt.

Um die Datenübertragung über eine Punkt-zu-Punkt-Verbindung herzustellen, sendet das Ursprungs-PPP zunächst LCP-Pakete (Link Control Protocol), um die Datenverbindung zu konfigurieren und zu testen. Nachdem die Verbindung hergestellt ist und optionale Merkmale, wie von dem LCP benötigt, ausgehandelt wurden, sendet das Ursprungs-PPP NCP-Pakete (Network Control Protocols), um ein oder mehrere Schicht-3-Protokolle auszuwählen und zu konfigurieren. Nachdem die einzelnen gewählten Schicht-3-Protokolle konfiguriert wurden, können Pakete der einzelnen Schicht-3-Protokolle über die Verbindung gesendet werden. Die Verbindung verbleibt für die Datenübertragung konfiguriert, bis sie explizit durch LCP- oder NCP-Pakete geschlossen wird, oder bis ein externes Ereignis auftritt. Dies ist der tatsächliche Verbindungstyp des Switch-Ports. Er kann vom administrierten Zustand abweichen.

Point-to-Point Operational Status (Punkt-zu-Punkt-Betriebsstatus) – Der Betriebszustand der Punkt-zu-Punkt-Verbindung.

Activate Protocol Migrational (Protokollmigrationstest aktivieren) – Wenn dieses Kontrollkästchen markiert ist, sendet PPP LCP-Pakete (Link Control Protocol), um die Datenverbindung zu konfigurieren und zu testen.

Definieren von RSTP-Parametern

1. Öffnen Sie die RSTP-Einstellungsseite.
2. Wählen Sie eine Schnittstelle aus.
3. Definieren Sie die Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die RSTP-Parameter werden definiert und das Gerät aktualisiert.

Anzeigen der Rapid Spanning Tree Table (RSTP-Tabelle)

1. Öffnen Sie die Seite Rapid Spanning Tree (RSTP).
2. Klicken Sie auf **Show All** (Alle anzeigen)

Die **Rapid Spanning Tree Table** (RSTP-Tabelle) wird geöffnet.

Definieren von RSTP-Parametern mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite Rapid Spanning Tree (RSTP) äquivalenten CLI-Befehle zum Definieren der Rapid-STP-Parameter zusammengefasst.

Tabelle 7-15. CLI-Befehle für RSTP-Einstellungen

CLI-Befehl	Beschreibung
`spanning-tree link-type {point-to-point | shared}`	Setzt die Vorgabeeinstellung für den Verbindungstyp außer Kraft.
`spanning tree mode {stp | rstp | mstp}`	Konfiguriert das derzeit ausgeführte Spanning-Tree-Protokoll.
`clear spanning-tree detected-protocols [ethernet Schnittstelle | port-channel Port-Kanalnummer]`	Startet den Protokollmigrationsprozess neu.
`show spanning-tree [ethernet Schnittstelle | port-channel Port- Kanalnummer]`	Zeigt die Spanning-Tree-Konfiguration an.

Im Folgenden ein Beispiel für die CLI-Befehle:

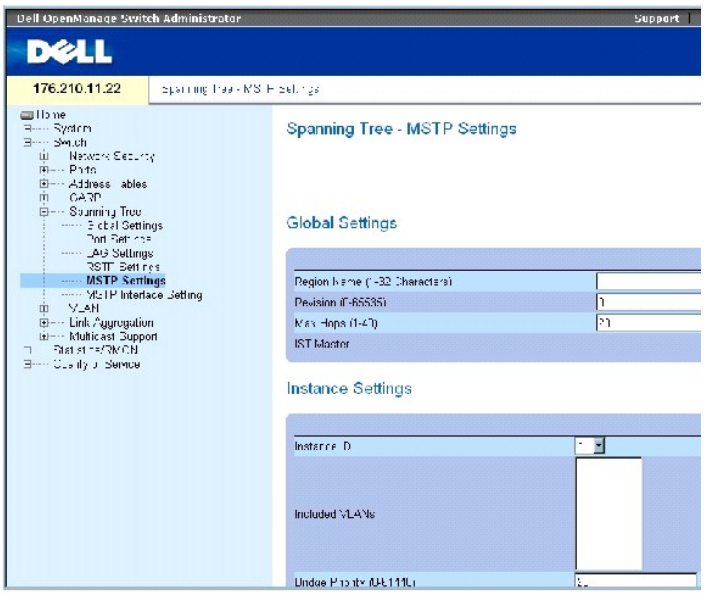
```
console(config)# interface ethernet 1/e5

console(config-if)# spanning-tree link-type shared

console(config-if)# spanning tree mode rstp
```

Konfigurieren von Multiple Spanning Tree

MSTP (Multiple Spanning Tree) bildet VLANs auf STP-Instanzen ab. Außerdem ist das Lastausgleichszenario bei MSTP ein anderes. Während zum Beispiel Port A in einer STP-Instanz blockiert ist, befindet sich derselbe Port in einer anderen STP-Instanz im Zustand Forwarding (Weiterleiten).

Außerdem werden Pakete, die unterschiedlichen VLANs zugeordnet sind, innerhalb sogenannter Multiple Spanning Tree Regions (MST-Regionen) entlang verschiedener Pfade übertragen. Bei diesen Regionen handelt es sich um eine oder mehrere MST-Brücken, von denen Frames übertragen werden können. So öffnen Sie die Seite MSTP Settings (MSTP-Einstellungen): Klicken Sie in der Strukturansicht auf Switch → Spanning Tree → MSTP Settings .

Abbildung 7-26. MSTP Settings (MSTP-Einstellungen)



Die Seite MSTP Settings (MSTP-Einstellungen) enthält folgende Felder:

Region Name (1-32 Characters) (Regionsname, 1 bis 32 Zeichen) – Gibt den benutzerdefinierten Namen der MSTP-Region an.

Revision (0-65535) – Legt eine nicht vorzeichenbehaftete 16-Bit-Zahl fest, die die aktuelle MST-Konfigurationsrevision bezeichnet. Die Revisionsnummer ist ein erforderlicher Bestandteil der MST-Konfiguration. Der mögliche Wertebereich reicht von 0 bis 65535.

Max Hops (1-40) (Max. Sprünge, 1 bis 40) – Definiert die Gesamtzahl von in einer spezifischen Region zulässigen Hops (Sprüngen), bevor die BPDU verworfen wird. Die Portinformationen verfallen, sobald die BPDU verworfen wird. Der mögliche Wertebereich für das Feld erstreckt sich von 1 bis 40. Der Standardwert lautet 20 Sprünge.

IST Master (IST-Master) – Bezeichnet die ID des Internal Spanning Tree Master (IST-Master). Der IST-Master ist Root der Instanz 0.

Instance ID (Instanz-ID) – Definiert die MSTP-Instanz. Der Feldbereich erstreckt sich von 1 bis 15.

Included VLANs (Eingeschlossene VLANs) – Zeigt die VLANs an, die auf die ausgewählte Schnittstelle abgebildet werden. Jedes VLAN gehört zu einer Instanz.

Bridge Priority (0-61440) (Bridge-Priorität, 0 bis 61440) – Spezifiziert die Gerätepriorität der ausgewählten Spanning-Tree-Instanz. Der Wertebereich des Felds erstreckt sich in Schritten von 4096 von 0 bis 61140.

Designated Root Bridge ID (ID der designierten Root-Bridge) – Bezeichnet die ID der Bridge, die Root der ausgewählten Instanz ist.

Root Port (Root-Port) – Bezeichnet den Root-Port der ausgewählten Instanz.

Root Path Cost (Root-Pfadkosten) – Gibt die Pfadkosten der ausgewählten Instanz an.

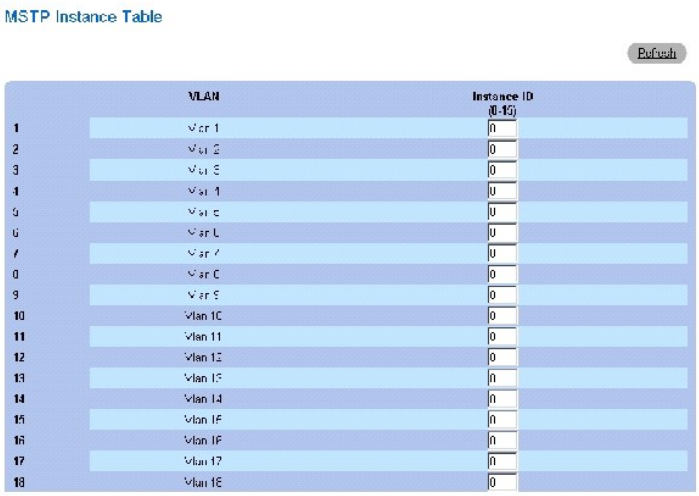
Bridge ID (Bridge-ID) – Gibt die Bridge-ID der ausgewählten Instanz an.

Remaining Hops (Verbleibende Sprünge) – Gibt die Anzahl der bis zum nächsten Ziel verbleibenden Sprünge an.

Anzeigen der MSTP Instance Table (MSTP-Instanzentabelle)

1. Öffnen Sie die Seite **Spanning Tree** MSTP Settings (MSTP-Einstellungen).
2. Klicken Sie auf **Show All** (alle anzeigen), um die MSTP Instance Table (MSTP- Instanzentabelle) zu öffnen.

Abbildung 7-27. MSTP Instance Table (MSTP-Instanzentabelle)



Definieren von MST-Instanzen mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite **Spanning Tree** MSTP Settings (MSTP-Einstellungen) äquivalenten CLI-Befehle zum Definieren der Rapid-STP-Parameter zusammengefasst.

Tabelle 7-16. CLI-Befehle für MSTP-Instanzen

CLI-Befehl	Beschreibung
`spanning-tree mst configuration`	Aktiviert den MST-Konfigurationsmodus.

instance Instanz-ID {add | remove} vlan VLAN- Bereich	Bildet VLANs auf die MST-Instanz ab.
name Zeichenkette	Stellt den Namen der Konfiguration ein.
revision Wert	Stellt die Konfigurationsrevisionsnummer ein.
spanning-tree **mst** Instanz-ID port-priority Priorität	Stellt die Priorität eines Ports ein.
spanning-tree mst Instanz-ID priority Priorität	Stellt die Gerätepriorität für die angegebene Spanning-Tree-Instanz ein.
spanning-tree mst max- hops Hop-Anzahl	Stellt die Anzahl der in einer MST-Region zulässigen Hops (Sprüngen) ein, bevor die BPDU verworfen wird und die verfügbaren Informationen über einen Port verfallen.
spanning-tree mst Instanz-ID **cost** Kosten	Stellt die Pfadkosten des Ports für MST-Berechnungen ein.
exit	Verlässt den MST-Regionskonfigurationsmodus und übernimmt die Änderungen an der Konfiguration.
abort	Verlässt den MST-Regionskonfigurationsmodus, ohne die Änderungen an der Konfiguration zu übernehmen.
show {current | pending}	Zeigt die aktuelle oder die anstehende MST-Regionskonfiguration an.

Im Folgenden ein Beispiel für die CLI-Befehle:

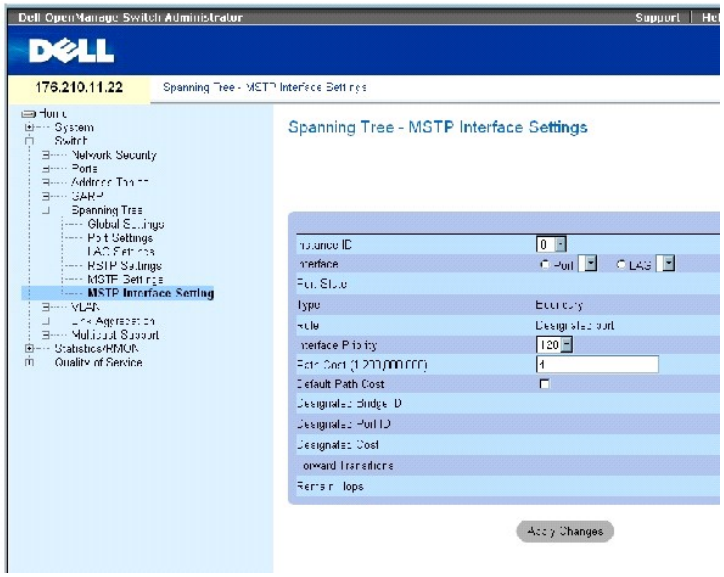
```
console(config)# spanning-tree mst configuration

console(config-mst)# instance 1 add vlan 10-20

console(config-mst)# name region1

console(config-mst)# revision 1

console(config)# spanning-tree mst configuration

console(config-mst)# instance 2 add vlan 21-30

console(config-mst)# name region1

console(config-mst)# revision 1

console(config-mst)# show pending

Pending MST configuration
```

```
Name: Region1

Revision: 1

Instance Vlans Mapped

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

0 1-9,31-4094

1 10-20

2 21-30
```

Definieren von MSTP-Schnittstelleneinstellungen

Die Seite MSTP Interface Settings (MSTP-Schnittstelleneinstellungen) enthält Parameter zum Zuweisen von MSTP-Einstellungen an spezifische Schnittstellen. So öffnen Sie die Seite MSTP Interface Settings (MSTP-Schnittstelleneinstellungen): Klicken Sie in der Strukturansicht auf Switch → Spanning Tree → MSTP Interface Settings.

Abbildung 7-28. MSTP Interface Settings (MSTP-Schnittstelleneinstellungen)



Die Seite MSTP Interface Settings (MSTP-Schnittstelleneinstellungen) enthält folgende Felder:

Instance ID (Instanz-ID) – Listet die auf dem Gerät konfigurierten MSTP-Instanzen auf. Der Wertebereich des Feldes erstreckt sich von 1 bis 15.

Interface (Schnittstelle) – Weist der ausgewählten MSTP-Instanz entweder Ports oder LAGs zu.

Port State (Port-Zustand) – Gibt an, ob der Port in der gegebenen Instanz aktiviert oder deaktiviert ist.

Type (Typ) – Gibt an, ob MSTP den Port als Punkt-zu-Punkt-Port oder als einen an einen Hub angeschlossenen Port behandelt, und ob es sich um einen internen Port der MST-Region oder um einen Port an der Grenze handelt. Ein Master-Port stellt die Verbindung von einer MSTP-Region zu einem außerhalb dieser befindlichen CIST-Root her. Ein Boundary-Port (Grenz-Port) verbindet MST-Bridges mit LANs in einer anderen Region. Falls es sich bei dem Port um einen Boundary-Port handelt, wird auch angegeben, ob das Gerät am anderen Ende der Verbindung im RSTP- oder im STP-Modus arbeitet.

Role (Funktion) – Gibt die Funktion an, die der STP-Algorithmus dem Port zugewiesen hat, um STP-Pfade bereitstellen. Folgende Feldwerte sind möglich:

Root (Wurzel) – Stellt den kostengünstigsten Pfad für die Weiterleitung von Paketen an das Root-Gerät bereit.

Designated (Designiert) – Gibt den Port bzw. die LAG an, über den/die das designierte Gerät an das LAN angeschlossen ist.

Alternate (Alternativ) – Stellt für die Weiterleitung von Paketen zum Root-Gerät einen zur Weiterleitung über die Root-Schnittstelle alternativen Pfad bereit.

Backup (Reserve) – Stellt einen Reservepfad zu den Endgeräten (Blättern) des Spanning-Tree als Alternative zu dem designierten Portpfad bereit. Reserveports treten nur auf, wenn zwei Ports durch eine Punkt-zu-Punkt-Verbindung in einer Schleife miteinander verbunden sind. Reserveports treten auch auf, wenn ein LAN zwei oder mehr Verbindungen zu einem gemeinsamen Segment aufweist.

Disabled (Deaktiviert) – Gibt an, dass der Port nicht an dem Spanning-Tree teilnimmt.

Interface Priority (0-240, in steps of 16) (Schnittstellenpriorität, von 0 bis 240 in 16er-Schritten) – Legt die Schnittstellenpriorität für die angegebene Instanz fest. Der Standardwert lautet 128.

Path Cost- (Pfadkosten) – Der Beitrag des Ports zu der Spanning-Tree-Instanz. Der Wert sollte stets zwischen 1 und 200000000 liegen.

Default Path Cost (Standard-Pfadkosten) – Gibt an, dass die Standardpfadkosten gemäß der auf der Seite Spanning Tree Global Settings (Globale Spanning-Tree-Einstellungen) ausgewählten Methode zugewiesen werden.

Designated Bridge ID (ID der designierten Bridge) – Die ID-Nummer der Bridge, die die Verbindung oder das gemeinsame LAN mit dem Root-Gerät verbindet.

Designated Port ID (ID des designierten Ports) – Die ID-Nummer des Ports auf der designierten Bridge, die die Verbindung oder das gemeinsame LAN mit dem Root-Gerät verbindet.

Designated Cost (designierte Kosten) – Kosten des Pfads von der Verbindung oder dem gemeinsamen LAN zum Root-Gerät.

Forward Transitions (Weiterleitungsübergänge) – Gibt an, wie oft der Port in den Zustand **Forwarding** (Weiterleiten) gewechselt ist.

Remain Hops (Verbleibende Sprünge) – Gibt die Anzahl der bis zum nächsten Ziel verbleibenden Hops (Sprünge) an.

Definieren von MSTP-Schnittstelleneinstellungen

1. Öffnen Sie die Seite MSTP Interface Settings (MSTP-Schnittstelleneinstellungen).
2. Wählen Sie eine Schnittstelle aus.
3. Definieren Sie die Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

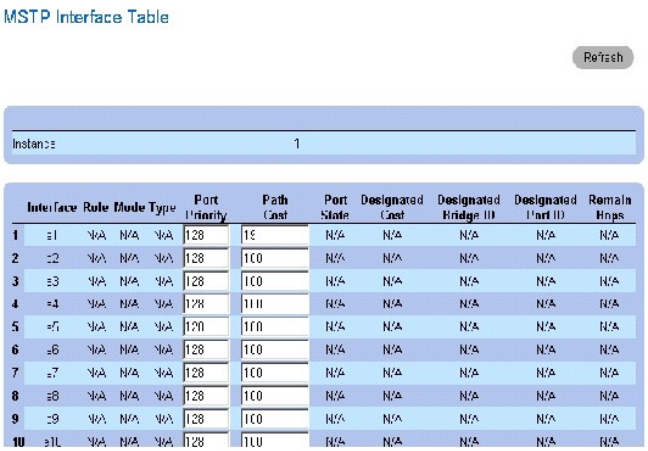
Die MSTP-Parameter werden definiert und das Gerät aktualisiert.

Anzeigen der MSTP Interface Table (MSTP-Schnittstellentabelle).

1. Öffnen Sie die Seite MSTP Interface Settings (MSTP-Schnittstelleneinstellungen).
2. Klicken Sie auf Show All (Alle anzeigen).

Die Seite MSTP Interface Table (MSTP-Schnittstellentabelle) wird geöffnet:

Abbildung 7-29. MSTP Interface Table (MSTP-Schnittstellentabelle)



Definieren von MSTP-Schnittstellen mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite **Spanning Tree** MSTP Interface Settings (MSTP-Schnittstelleneinstellungen) äquivalenten CLI-Befehle zum Definieren von MSTP-Schnittstellen zusammengefasst.

Tabelle 7-17. CLI-Befehle für MSTP-Schnittstellen

CLI-Befehl	Beschreibung
`spanning-tree mst Instanz-ID cost Kosten`	Stellt die Pfadkosten des Ports für MST-Berechnungen ein.
`spanning-tree mst Instanz-ID priority Priorität`	Stellt die Gerätepriorität für die angegebene Spanning-Tree-Instanz ein.
`show spanning-tree mst- configuration`	Zeigt die MST-Konfiguration an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console# show spanning-tree mst-configuration

Gathering information .....

Current MST configuration

Name: Gili

Revision: 65000
```

Instance	Vlans Mapped	State
---------	------------------------	----------
0	16-4094	enabled
1	1	enabled
2	2	enabled
3	3	enabled
4	4	enabled
5	5	enabled
6	6	enabled
7	7	enabled
8	8	enabled
9	9	enabled
10	10	enabled
11	11	enabled
12	12	enabled
13	13	enabled
14	14	enabled
15	15	enabled

Konfigurieren von VLANs

VLANs sind logische Untergruppen innerhalb eines LANs, die softwarebasiert und nicht durch eine Hardwarelösung erstellt werden. VLANs fassen Benutzerstationen und Netzwerkgeräte in einer einzigen Einheit zusammen, und zwar unabhängig von dem physischen LAN-Segment, mit dem die jeweiligen Geräte verbunden sind. VLANs schaffen die Voraussetzung für einen effizienteren Netzwerk-daten-verkehrs-fluss innerhalb der Untergruppen. Mittels Software verwaltete VLANs verkürzen die Zeit für die Implementierung von Änderungen an, Erweiterungen von und Umstellungen in Netzwerken.

VLANs haben keine minimale Portzahl und können pro Einheit, pro Gerät, pro Stack bzw. einer anderen logischen Verbindungskombination erstellt werden, da VLANs softwarebasiert sind und nicht durch physische Attribute festgelegt werden.

VLANs arbeiten auf der Ebene von 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 desjenigen VLANs übertragen, in dem der Verkehr

generiert wird.

VLAN-Kennungen bieten eine Methode, um VLAN-Informationen zwischen VLAN-Gruppen zu übertragen. Für eine VLAN-Kennung wird eine aus vier Bytes bestehende Datenkennung an den Paketheader angehängt. Die VLAN-Kennung gibt das VLAN an, dem das Paket angehört. VLAN-Kennungen werden entweder von der Endstation oder von dem Netzwerkgerät an das VLAN angehängt. VLAN-Kennungen enthalten darüber hinaus Informationen zur Priorität von VLAN-Netzwerken.

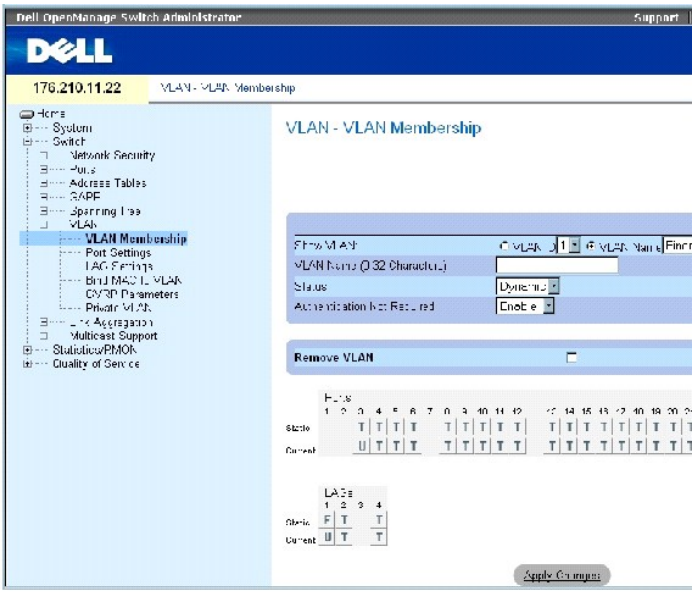
Die Kombination von VLANs und GVRP ermöglicht es Netzwerkverwaltern, Netzwerknoten in Broadcast-Domänen anzuordnen. Broadcast- und Multicast-Datenverkehr wird auf die Gruppe beschränkt, von der die jeweiligen Daten ausgehen.

So öffnen Sie die Seite **VLAN**: Klicken Sie in der Strukturansicht auf **Switch** → **VLAN**.

Definieren der VLAN-Mitgliedschaft

Die Seite **VLAN Membership (VLAN-Mitgliedschaft)** enthält Felder zum Definieren von VLAN-Gruppen. Das Gerät unterstützt die Abbildung von 4094 VLAN-IDs auf 256 VLANs. Für alle Ports muss eine PVID definiert werden. Falls kein anderer Wert konfiguriert ist, wird die Standard-PVID des VLANs verwendet. VLAN-ID Nr. 1 ist das Standard-VLAN, das nicht aus dem System gelöscht werden kann. So öffnen Sie die Seite **VLAN Membership (VLAN-Mitgliedschaft)**: Klicken Sie in der Strukturansicht auf **Switch**→ **VLAN**→ **VLAN Membership**.

Abbildung 7-30. VLAN Membership (VLAN-Mitgliedschaft)



Die Seite **VLAN Membership (VLAN-Mitgliedschaft)** enthält folgende Felder:

Show VLAN (VLAN anzeigen) – Listet entsprechend der VLAN-ID bzw. dem VLAN-Namen spezifische VLAN-Informationen auf.

VLAN Name (VLAN-Name, 0 bis 32 Zeichen) – Der benutzerdefinierte VLAN-Name.

Status (Status) – Der VLAN-Typ. Folgende Werte sind möglich:

Dynamic (Dynamisch) – Das VLAN wurde dynamisch über GVRP erstellt.

Static (Statisch) – Es handelt sich um ein benutzerdefiniertes VLAN.

Default (Standard) – Es handelt sich um das Standard-VLAN.

Authentication Not Required (Authentifizierung nicht erforderlich) – Aktiviert oder deaktiviert den Zugriff auf das VLAN für nicht autorisierte Benutzer.

Remove VLAN (VLAN entfernen) – Wenn dieses Kontrollkästchen ausgewählt ist, wird das VLAN aus der **VLAN Membership Table** (VLAN-Mitgliedschaftstabelle) entfernt.

Hinzufügen neuer VLANs

1. Öffnen Sie die Seite **VLAN Membership (VLAN-Mitgliedschaft)**.
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Create New VLAN** (Neues VLAN erstellen) wird geöffnet.
3. Geben Sie ID und Namen des VLANs ein.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Das neue VLAN wird hinzugefügt und das Gerät aktualisiert.

Modifizieren von VLAN-Mitgliedschaftsgruppen

1. Öffnen Sie die Seite **VLAN Membership (VLAN-Mitgliedschaft)**.
2. Wählen Sie im Dropdown-Menü **Show VLAN** (VLAN anzeigen) ein VLAN aus.
3. Modifizieren Sie die Felder nach Wunsch.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Die VLAN-Mitgliedschaftsinformationen werden modifiziert, und das Gerät wird aktualisiert.

Löschen von VLANs

1. Öffnen Sie die Seite **VLAN Membership (VLAN-Mitgliedschaft)**.
2. Wählen Sie im Feld **Show VLAN** (zeige VLAN:) ein VLAN aus.
3. Aktivieren 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-Mitgliedschaftsgruppen mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite VLAN Membership (VLAN-Mitgliedschaft) äquivalenten CLI-Befehle zum Definieren von VLAN-Mitgliedschaftsgruppen zusammengefasst.

Tabelle 7-18. CLI-Befehle für VLAN-Mitgliedschaftsgruppen

CLI-Befehl	Beschreibung
vlan database	Aktiviert den VLAN-Konfigurationsmodus.
vlan {*VLAN-Bereich*}	Erstellt ein VLAN.
name *Zeichenkette*	Fügt einem VLAN einen Namen hinzu.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# vlan
database

console(config-vlan)# vlan
1972

console(config-vlan)# end

console(config)# interface
vlan 1972

console(config-if)# name
Marketing

console(config-if)# end
```

VLAN Port Membership Table (VLAN-Portmitgliedschaftstabelle)

Die **VLAN Port Membership Table** (VLAN-Portmitgliedschaftstabelle) enthält eine **Port Table** (Porttabelle) für das Zuweisen von Ports an VLANs. Ports lassen sich mit der **Port Control** (Port-Steuerung) an VLANs zuweisen. Die Ports können die folgenden Werte aufweisen:

Tabelle 7-81. VLAN Port Membership Table (VLAN-Portmitgliedschaftstabelle)

Port Control	Definition
T	Die Schnittstelle gehört einem VLAN an. Alle über die Schnittstelle weitergeleiteten Pakete verfügen über eine Kennung. Die Pakete enthalten VLAN-Informationen.
U	Die Schnittstelle gehört einem VLAN an. Über die Schnittstelle weitergeleitete Pakete besitzen keine Kennung.
F	Der Schnittstelle wird die Mitgliedschaft in einem VLAN verweigert.
Leer	Die Schnittstelle gehört keinem VLAN an. Mit der Schnittstelle verknüpfte Pakete werden nicht weitergeleitet.

Die **VLAN Port Membership Table** (VLAN-Portmitgliedschaftstabelle) zeigt Ports samt Portzuständen und LAGs an.

Zuweisen von Ports zu einer VLAN-Gruppe

1. Öffnen Sie die Seite VLAN Membership (VLAN-Mitgliedschaft).
2. Markieren Sie eines der Optionsfelder **VLAN ID** oder **VLAN Name**, und wählen Sie ein VLAN aus dem Dropdown-Menü aus.
3. Wählen Sie in der **Port Membership Table** (Portmitgliedschaftstabelle) einen Port aus, 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 aktualisiert.

Löschen eines VLANs

1. Öffnen Sie die Seite VLAN Membership (VLAN-Mitgliedschaft).
2. Markieren Sie eines der Optionsfelder **VLAN ID** oder **VLAN Name**, und wählen Sie ein VLAN aus dem Dropdown-Menü aus.

3. Aktivieren Sie das Kontrollkästchen **Remove VLAN** (VLAN entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Das ausgewählte VLAN wird gelöscht und das Gerät aktualisiert.

Zuweisen von Ports zu VLAN-Gruppen mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zum Zuweisen von Ports zu VLAN-Gruppen zusammengefasst.

Tabelle 7-19. CLI-Befehle zum Zuweisen von Ports zu VLAN-Gruppen

CLI-Befehl	Beschreibung
switchport general acceptable-frame-types tagged-only	Lehnt Frames ohne Kennung bei der Ingress-Filterung ab.
switchport forbidden vlan {add *VLAN-Liste* | remove *VLAN-Liste*}	Verbietet das Hinzufügen spezifischer VLANs zum Port.
switchport mode {access | trunk | general}	Konfiguriert den VLAN-Mitgliedschaftsmodus eines Ports.
switchport access vlan vlan-id	Konfiguriert die VLAN-ID, wenn sich die Schnittstelle im Zugriffsmodus befindet.
switchport trunk allowed vlan {add VLAN-Liste | remove VLAN-Liste}	Fügt einem Trunk-Port VLANs hinzu, oder entfernt VLANs von einem Trunk-Port.
switchport trunk native vlan VLAN-ID	Definiert den Port als Mitglied des angegebenen VLANs und die VLAN-ID als Standard-VLAN-ID des Ports (PVID).
switchport general allowed vlan add VLAN-Liste [tagged | untagged]	Fügt einem Port im allgemeinen Modus VLANs hinzu, oder entfernt VLANs von einem solchen Port.
switchport general pvid VLAN-ID	Konfiguriert die PVID, wenn sich die Schnittstelle im allgemeinen Modus befindet.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# vlan
database

console(config-vlan)# vlan
23-25

console(config-vlan)# end

console(config)# interface
vlan 23

console(config-if)# name
Marketing

console(config-if)# end

console(config)# interface
ethernet 1/e8

console(config-if)#
switchport mode access

console(config-if)#
```

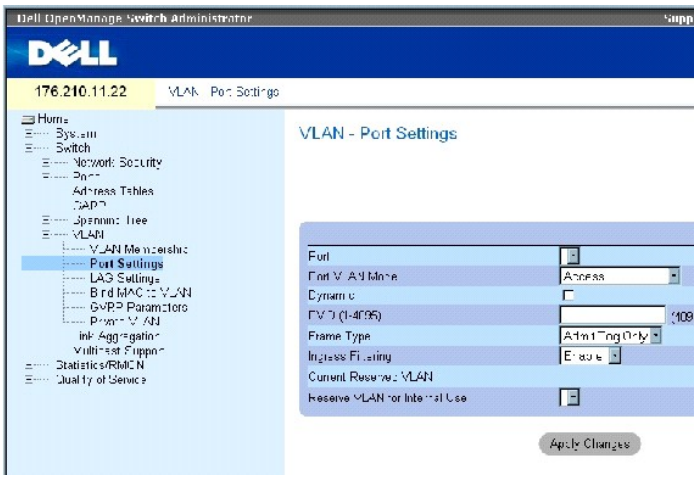
```
switchport access vlan 23



console(config-if)# end



console(config)# interface
ethernet 1/e9



console(config-if)#
switchport mode trunk



console(config-if)#
switchport mode trunk
allowed vlan add 23-25



console(config-if)# end



console(config)# interface
ethernet 1/e11



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 (VLAN-Porteinstellungen) enthält Felder zur Verwaltung von Ports, die einem VLAN angehören. Die Standard-VLAN-ID der Ports (PVID) wird auf der Seite VLAN Port Settings (VLAN-Porteinstellungen) konfiguriert. Alle über das Gerät eingehenden Pakete ohne Kennung erhalten als Kennung die PVID des Ports.

So öffnen Sie die Seite VLAN Port Settings (VLAN-Porteinstellungen): Klicken Sie in der Strukturansicht auf **Switch→ VLAN→ Port Settings**.

Abbildung 7-31. VLAN Port Settings (VLAN-Porteinstellungen)



Die Seite VLAN Port Settings (VLAN-Porteinstellungen) enthält folgende Felder:

Port (Port) – Die Nummer des im VLAN enthaltenen Ports.

Port VLAN Mode (Port-VLAN-Modus) – Der Portmodus. Folgende Werte sind möglich:

General (Allgemeiner Modus) – Der Port gehört einem oder mehreren VLANs an, und jedes einzelne VLAN wurde vom Benutzer als VLAN mit oder als VLAN ohne Kennung definiert (voller 802.1Q-Modus).

Access (Zugriffsmodus) – Der Port gehört einem einzigen VLAN ohne Kennung an. Wenn sich ein Port im Zugriffsmodus befindet, ist es nicht möglich, die Typen von Paketen anzugeben, die auf dem Port akzeptiert werden. Die Ingress-Filterung lässt sich auf einem Port im Zugriffsmodus nicht aktivieren/deaktivieren.

Trunk – Der Port gehört einem VLAN an, in dem alle Ports über eine Kennung verfügen (mit Ausnahme eines Ports, der nicht über eine Kennung verfügen muss).

PVE Promiscuous – Der Port gehört einem PVE Promiscuous VLAN an.

PVE Community – Der Port gehört einem PVE Community VLAN an.

PVE Isolated – Der Port gehört einem PVE Isolated VLAN an.

Dynamic (Dynamisch) – **Weist einen Port basierend auf der MAC-Adresse des an den Port angeschlossenen Hosts einem VLAN zu.**

PVID – Weist allen Paketen ohne Kennung eine VLAN-ID zu. Die möglichen Werte liegen im Bereich von 1 bis 4095. Das VLAN Nr. 4095 ist, wie in der Branche üblich, als Discard-VLAN (Wegwerf-VLAN) definiert. Ordnet die Klassifikation eines Pakets dieses dem Discard-VLAN zu, so wird das Paket verworfen.

Frame Type (Frame-Typ) – Auf dem Port akzeptierter Pakettyp. Folgende Werte sind möglich:

Admit Tag Only (Nur mit Kennung zulassen) – Auf dem Port werden nur Pakete mit Kennung akzeptiert.

Admit All (alle zulassen) – Auf dem Port werden sowohl Pakete mit als auch Pakete ohne Kennung akzeptiert.

Ingress Filtering (Ingress-Filterung) – Aktiviert oder deaktiviert die Ingress-Filterung auf dem Port. Die Ingress-Filterung verwirft Pakete, die an VLANs adressiert sind, denen der jeweilige Port nicht angehört.

Current Reserved VLAN (Aktuell reserviertes VLAN) – Das derzeit vom System als reserviertes VLAN ausgewiesene VLAN.

Reserve VLAN for Internal Use (VLAN für interne Verwendung reservieren) – Das vom Benutzer als reserviertes VLAN ausgewählte VLAN, sofern nicht vom System unter Verwendung.

Zuweisen von Porteinstellungen

1. Öffnen Sie die Seite VLAN Port Settings (VLAN-Porteinstellungen).
2. Wählen Sie im Dropdown-Menü **Port** den Port aus, dem Einstellungen zugewiesen werden sollen.
3. Füllen Sie die verbleibenden Felder auf der Seite aus.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die VLAN-Porteinstellungen werden definiert und das Gerät aktualisiert.

Anzeigen der VLAN Port Table (VLAN-Porttabelle):

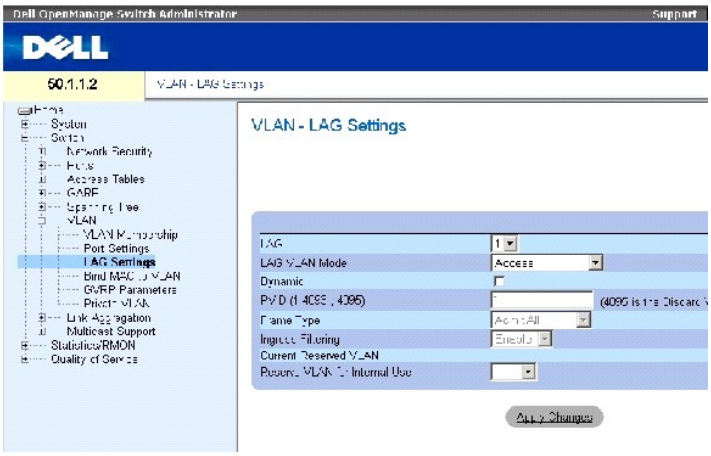
1. Öffnen Sie die Seite VLAN Port Settings (VLAN-Porteinstellungen).
2. Klicken Sie auf **Show All** (Alle anzeigen)..

Die **VLAN Port Table** (VLAN-Porttabelle) wird geöffnet.

Definieren von VLAN-Einstellungen für LAGs

Die Seite VLAN LAG Settings (VLAN-LAG-Einstellungen) bietet Parameter zur Verwaltung von LAGs, die einem VLAN angehören. VLANs können entweder aus einzelnen Ports oder aus LAGs bestehen. Am Gerät eingehende Pakete ohne Kennung erhalten als Kennung die durch die PVID angegebene LAG-ID. So öffnen Sie die Seite VLAN LAG Settings (VLAN-LAG-Einstellungen): Klicken Sie in der Strukturansicht auf **Switch→ VLAN→ LAG Settings**.

Abbildung 7-32. VLAN LAG Settings (VLAN-LAG-Einstellungen)



Die Seite VLAN LAG Settings (VLAN-LAG-Einstellungen) enthält folgende Felder:

LAG (LAG) – Die Nummer der im VLAN enthaltenen LAG.

LAG VLAN Mode (LAG-VLAN-Modus) – Der LAG-VLAN-Modus. Folgende Werte sind möglich:

General (Allgemeiner Modus) – Die LAG gehört einem oder mehreren VLANs an, und die einzelnen VLANs wurden vom Benutzer jeweils als VLAN mit oder als VLAN ohne Kennung definiert (voller 802.1Q-Modus).

Access (Zugriffsmodus) – Die LAG gehört einem einzigen VLAN ohne Kennung an.

Trunk – Die LAG gehört einem VLAN an, in dem alle Ports über eine Kennung verfügen (mit Ausnahme eines Ports, der nicht über eine Kennung verfügen muss).

PVE Promiscuous – Die LAG gehört einem PVE Promiscuous VLAN an.

PVE Community — Die LAG gehört einem PVE Community VLAN an.

PVE Isolated — Die LAG gehört einem PVE Isolated VLAN an.

Dynamic (Dynamisch) – Weist eine LAG einem VLAN zu, basierend auf der MAC-Adresse des an die LAG angeschlossenen Hosts.

PVID (1-4093, 4095) – Weist Paketen ohne Kennung eine VLAN-ID zu. Die möglichen Feldwerte liegen im Bereich von 1 bis 4095. Das VLAN Nr. 4095 ist, wie in der Branche üblich, als Discard-VLAN (Wegwerf-VLAN) definiert. Wenn die Klassifikation eines Pakets das Paket dem Discard-VLAN zuordnet, wird das Paket fallen gelassen.

Frame Type (Frame-Typ) – Von der LAG akzeptierter Pakettyp. Folgende Werte sind möglich:

Admit Tag Only (Nur mit Kennung zulassen) – Die LAG akzeptiert nur Pakete mit Kennung.

Admit All (Alle zulassen) – Die LAG akzeptiert sowohl Pakete mit als auch Pakete ohne Kennung.

Ingress Filtering (Ingress-Filterung) – Aktiviert oder deaktiviert die Ingress-Filterung durch die LAG. Die Ingress-Filterung verwirft Pakete, die an VLANs adressiert sind, denen die betreffende LAG nicht angehört.

Current Reserve VLAN (Aktuelles Reserve-VLAN) – Das derzeit als reserviertes VLAN ausgewiesene VLAN.

Reserve VLAN for Internal Use (VLAN für interne Verwendung reservieren) – Das VLAN, das nach Rücksetzen des Geräts als reserviertes VLAN ausgewiesen ist.

Zuweisen von VLAN-Einstellungen für LAGs:

1. Öffnen Sie die Seite VLAN LAG Settings (VLAN-LAG-Einstellungen).
2. Wählen Sie aus dem Dropdown-Menü **LAG** eine Lag aus, und füllen Sie die Felder auf der Seite aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die VLAN-Parameter für die LAG werden definiert und das Gerät aktualisiert.

Anzeigen der VLAN LAG Table (VLAN-LAG-Tabelle)

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

Die **VLAN LAG Table** (VLAN-LAG-Tabelle) wird geöffnet.

Zuweisen von LAGs an VLAN-Gruppen mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite VLAN LAG Settings (VLAN-LAG-Einstellungen) äquivalenten CLI-Befehle zum Zuweisen von LAGs an VLAN-Gruppen zusammengefasst.

Tabelle 7-20. CLI-Befehle zum Zuweisen von LAGs an VLAN-Gruppen

CLI-Befehl	Beschreibung
switchport mode {access | trunk | general}	Konfiguriert den VLAN-Mitgliedschaftsmodus für eine LAG.
switchport trunk native vlan *VLAN-ID*	Definiert die LAG als Mitglied des angegebenen VLANs und die VLAN-ID als Standard-VLAN-ID der LAG (PVID).
switchport general pvid *VLAN-ID*	Konfiguriert die PVID (VLAN-ID der LAG), während sich die Schnittstelle im allgemeinen Modus befindet.
switchport general allowed vlan add *VLAN-Liste* [**tagged** | **untagged**]	Fügt einer allgemeinen LAG VLANs hinzu, oder entfernt VLANs von einer solchen LAG.
switchport general acceptable-frame-type tagged-only	Lehnt Pakete ohne Kennung bei der Ingress-Filterung ab.
switchport access vlan dynamic	Bindet die MAC-Adresse an das VLAN.
switchport general ingress-filtering disable	Deaktiviert die Ingress-Filterung für eine LAG.

Im Folgenden ein Beispiel für 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
```

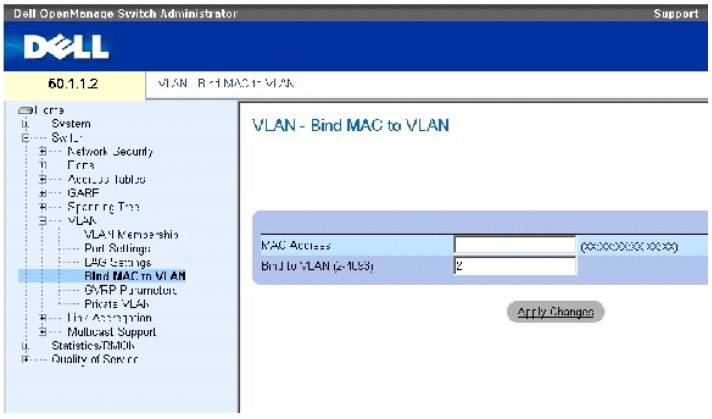
Binden von MAC-Adressen an VLANs

Das Binden von MAC-Adressen an VLANs ermöglicht die Zuweisung an VLANs auf der Basis von MAC-Adressen. Sobald eine einem VLAN zugewiesene MAC-Adresse auf einem Port erfasst wurde, tritt der Port dem VLAN bei, an das die MAC-Adresse gebunden ist. Wenn die MAC-Adresse zeitgesteuert gelöscht wird, verlässt der Port das VLAN. Nur dynamische VLANs können an MAC-Adressen gebunden werden.

Stellen Sie zum Binden von MAC-Adressen an einen VLAN sicher, dass die VLAN-Ports dynamisch hinzugefügt wurden und keine statischen VLAN-Ports sind.

So öffnen Sie die Seite **Bind MAC to VLAN (MAC an VLAN binden)**: Klicken Sie auf **Switch→ VLAN→ Bind MAC to VLAN**.

Abbildung 7-33. Bind MAC to VLAN (MAC an VLAN binden)



Die Seite Bind MAC to VLAN (MAC an VLAN binden) enthält folgende Felder:

MAC Address (MAC-Adresse) – Bezeichnet die MAC-Adresse, die an das VLAN gebunden wird.

Bind to VLAN (2-4093) (An VLAN binden) – Gibt das VLAN an, an das die MAC-Adresse gebunden wird.

Anzeigen der MAC to VLAN Table (MAC-VLAN-Zuordnungstabelle):

1. Öffnen Sie die Seite Bind MAC to VLAN (MAC an VLAN binden).
2. Klicken Sie auf **Show All**.

Die **MAC to VLAN Table** (MAC-VLAN-Zuordnungstabelle) erscheint.

Binden von MAC-Adressen an VLANs mit Hilfe von CLI-Befehlen:

In der folgenden Tabellen werden die entsprechenden CLI-Befehle zum Binden von MAC-Adressen an VLANs zusammengefasst.

Tabelle 7-21. CLI-Befehle zum Binden von MAC-Adressen an VLANs

CLI-Befehl	Beschreibung
mac-to-vlan MAC-Adresse VLAN-ID	Bindet die MAC-Adresse an das VLAN.
switchport access vlan dynamic	Konfiguriert private VLANs.
show mac-to-vlan	Zeigt die MAC-VLAN-Zuordnungsdatenbank.
no mac-to-vlan MAC-Adresse	Löst die Bindung zwischen MAC-Adresse und VLAN.

Im Folgenden ein Beispiel für die CLI-Befehle:

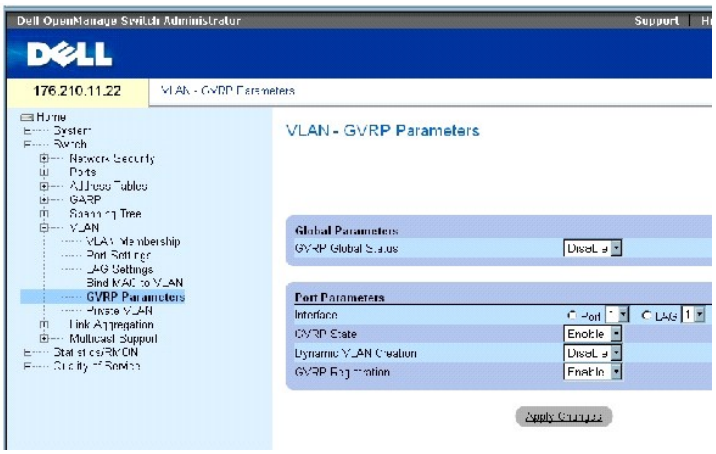
```
console(config-vlan)# mac-to-vlan 0060.704c.73ff 123

console(config-vlan)# exit

console(config)# exit

console# show vlan mac-to-vlan

MAC Address VLAN

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

0060.704c.73ff 123
```

Konfigurieren von GVRP-Parametern

Das GARP VLAN Registration Protocol (GVRP) dient insbesondere der automatischen Verteilung von VLAN-Mitgliedschaftsinformationen zwischen Bridges mit VLAN-Funktionalität. Mittels GVRP können Bridges mit VLAN-Funktionalität automatisch die Zuordnung zwischen VLANs und Bridge-Ports erfassen, ohne dass jede Brücke einzeln konfiguriert und jede VLAN-Mitgliedschaft einzeln registriert werden muss.

Auf der Seite **GVRP Parameters (GVRP-Parameter)** wird GVRP global aktiviert. GVRP kann auch für einzelne Schnittstellen aktiviert werden. So öffnen Sie die Seite GVRP Parameters (GVRP-Parameter): Klicken Sie in der Strukturansicht auf **Switch→ VLAN→ GVRP Parameters**.

Abbildung 7-34. GVRP Parameters (GVRP-Parameter)



Die Seite GVRP Parameters (GVRP-Parameter) enthält folgende Felder:

GVRP Global Status (Globaler GVRP-Status) – Aktiviert oder deaktiviert GVRP auf dem Gerät. GVRP ist standardmäßig deaktiviert.

Interface (Schnittstelle) – Gibt zur Bearbeitung von GVRP-Einstellungen einen Port oder eine LAG an.

GVRP State (GVRP-Zustand) – Aktiviert oder deaktiviert GVRP auf einer Schnittstelle.

Dynamic VLAN Creation (Erstellung dynamischer VLANs) – Aktiviert oder deaktiviert auf einer Schnittstelle das Erstellen von VLANs durch GVRP.

GVRP Registration (GVRP-Registrierung) – Aktiviert oder deaktiviert auf einer Schnittstelle die Registrierung von VLANs durch GVRP.

Aktivieren von GVRP auf dem Gerät

1. Öffnen Sie die Seite GVRP Global Parameters (Globale GVRP-Parameter).
2. Wählen im Feld **GVRP Global Status** (Globaler GVRP-Status) den Eintrag **Enable** (Aktivieren) aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

GVRP wird auf dem Gerät aktiviert.

Aktivieren der VLAN-Registrierung durch GVRP

1. Öffnen Sie die Seite GVRP Global Parameters (Globale GVRP-Parameter).
2. Wählen im Feld **GVRP Global Status** (Globaler GVRP-Status) den Eintrag **Enable** (Aktivieren) aus.
3. Wählen Sie im Feld **GVRP State** (GVRP-Zustand) für das gewünschte Gerät den Eintrag **Enable** (Aktivieren) aus.
4. Wählen im Feld **GVRP Registration** (GVRP-Registrierung) den Eintrag **Enable** (Aktivieren) aus.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die GVRP-VLAN-Registrierung wird auf dem Port aktiviert, und das Gerät wird aktualisiert.

Konfigurieren von GVRP mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite GVRP Global Parameters (Globale GVRP-Parameter) äquivalenten CLI-Befehle zum Konfigurieren von GVRP zusammengefasst.

Tabelle 7-22. CLI-Befehle für globale GVRP-Parameter

CLI-Befehl	Beschreibung
gvrp enable (global**)**	Aktiviert GVRP global.
gvrp enable (interface)	Aktiviert GVRP auf einer Schnittstelle
gvrp vlan-creation-forbid	Aktiviert oder deaktiviert die Erstellung von dynamischen VLANs.
gvrp registration-forbid	Hebt alle dynamischen VLAN-Registrierungen auf und verhindert die dynamische VLAN-Registrierung auf dem Port.
show gvrp configuration [**ethernet** *Schnittstelle*| **port-channel** *Port-Kanalnummer*]	Zeigt GVRP-Konfigurationsinformationen an, darunter Zeitgeberwerte, ob GVRP und die dynamische VLAN-Erstellung aktiviert ist und auf welchen Ports GVRP ausgeführt wird.
show gvrp error-statistics [**ethernet** *Schnittstelle*| **port-channel** *Port-Kanalnummer*]	Zeigt GVRP-Fehlerstatistiken an.
show gvrp statistics [**ethernet** *Schnittstelle*| **port-channel** *Port-Kanalnummer*]	Zeigt GVRP-Statistiken an.
clear gvrp statistics [**ethernet** *Schnittstelle*| **port-channel** *Port-Kanalnummer*]	Löscht die gesamten GVRP-Statistikdaten.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# gvrp enable

console(config)# interface ethernet 1/e1

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
1/e11	Enabled	Forbidden	Disabled	200	900	10000
1/e12	Disabled	Normal	Enabled	200	600	10000

Konfigurieren von privaten VLANs

Private VLANs (PVLAN) schränken innerhalb eines VLANs die Kommunikation zwischen den Ports ein und erhöhen dadurch die Sicherheit im Netzwerk. Private VLANs schränken den Netzwerkverkehr auf der Ebene von Layer 2 ein. Netzwerkadministratoren legen ein primäres VLAN fest. Innerhalb des primären VLANs existieren isolierte (Isolated VLANs) und gemeinschaftliche VLANs (Community VLANs). Die Ports eines privaten VLANs können folgende Zustände einnehmen:

- **Promiscuous** (Unbeschränkt) – Ein Promiscuous-Port kann mit allen Ports innerhalb eines PVLANs kommunizieren. Alle Promiscuous-Pakete werden automatisch sowohl dem Isolated-VLAN als auch dem Community-VLAN zugeordnet.
- **Isolated** (Isoliert) – Isolated-Ports werden von anderen Ports in demselben PVLAN vollständig isoliert. Isolierte Ports können jedoch mit Promiscuous-Ports kommunizieren. Ansonsten wird aller Datenverkehr von und zu isolierten Ports blockiert. Ausgenommen ist allein Verkehr von Promiscuous-Ports. Alle isolierten Ports werden automatisch dem Isolated-VLAN zugewiesen.
- **Community** (Gemeinschaftlich) – Community-Ports kommunizieren mit anderen Community-Ports und mit Promiscuous-Ports. Community-Ports sind von allen anderen Schnittstellen in anderen Communitys und von isolierten Ports in demselben PVLAN getrennt. Alle Community-Ports werden automatisch dem Community-VLAN und dem Private-VLAN zugewiesen.

ANMERKUNG: Ports, bei denen es sich um bestehende VLAN-Mitglieder handelt, können nicht als Promiscuous-Ports oder Isolated-Ports definiert werden.

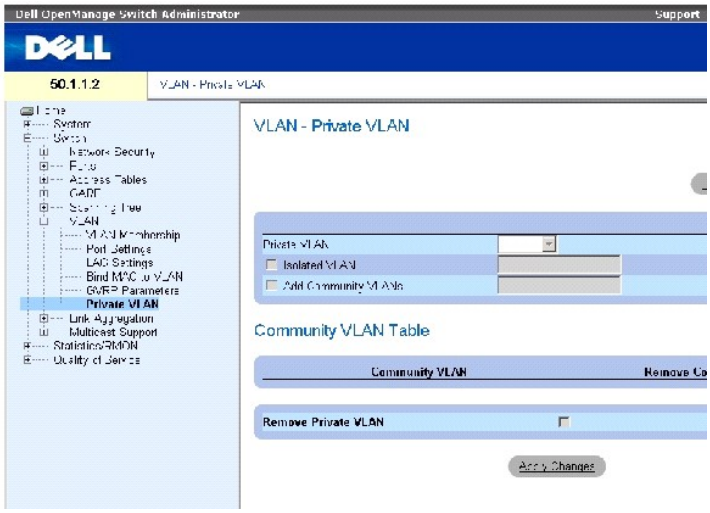
ANMERKUNG: Zuvor erstellte VLANs können nicht als Isolated-VLANs oder Community-VLANs konfiguriert werden.

ANMERKUNG: Isolated-VLANs und Community-VLANs werden bei der Ermittlung der Gesamtzahl der VLANs mitgezählt.

Wird das primäre VLAN gelöscht, so werden auch das Isolated-VLAN und das Community-VLAN gelöscht. Außerdem leiten das Isolated-VLAN und das Community-VLAN nur Datenverkehr ohne Kennung weiter.

So öffnen Sie die Seite Private VLAN (Privates VLAN): Klicken Sie in der Strukturansicht auf Switch → VLAN →Private VLAN.

Abbildung 7-35. Private VLAN (Privates VLAN)



Die Seite Private VLAN (Privates VLAN) enthält folgende Felder:

Private VLAN (Privates VLAN) – Enthält eine Liste benutzerdefinierter privater VLANs. Die privaten VLANs werden auf der Seite **Add Private VLAN (Privates VLAN hinzufügen)** definiert.

Isolated VLAN (Isoliertes VLAN) – Bezeichnet das VLAN, dem isolierte Ports zugewiesen werden.

Add Community VLANs (Community-VLANs hinzufügen) – Fügt ein Community-VLAN hinzu, dem Community-Ports zugewiesen werden.

Community VLAN (Community-VLAN) – Zeigt eine Liste der Community-VLANs an.

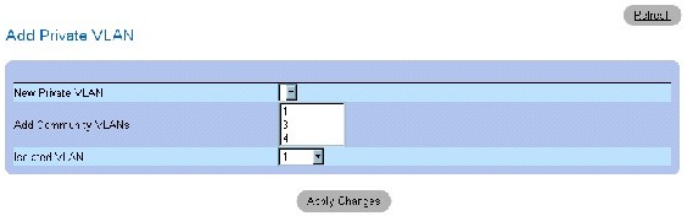
Remove Community (Community entfernen) – Wenn dieses Kontrollkästchen markiert ist, wird ein Community-VLAN entfernt.

Remove Private VLAN (Privates VLAN entfernen) – Wenn dieses Kontrollkästchen markiert ist, wird ein privates VLAN entfernt.

Hinzufügen von privaten VLANs

1. Öffnen Sie die Seite Private VLAN (Privates VLAN).
2. Klicken Sie auf **Add** (Hinzufügen). Die Seite **Add Private VLAN (Privates VLAN hinzufügen)** wird geöffnet:

Abbildung 7-36. Add Private VLAN (Privates VLAN hinzufügen)



Die Seite Add Private VLAN (Privates VLAN hinzufügen) enthält folgende Felder:

New Private VLAN (Neues privates VLAN) – Enthält eine Liste mit privaten VLANs. Community-VLANs werden dem privaten VLAN hinzugefügt.

Add Community VLANs (Community-VLANs hinzufügen) – Fügt dem privaten VLAN ein Community-VLAN hinzu.

Isolated VLAN (Isoliertes VLAN) – Fügt dem privaten VLAN ein Isolated-VLAN hinzu.

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

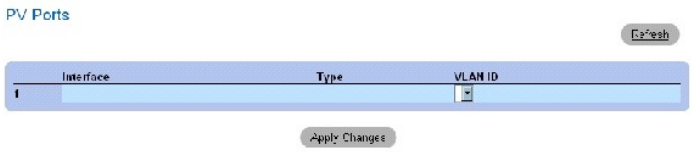
Das private VLAN wird definiert und das Gerät aktualisiert.

Anzeigen der PV Ports Table (PV-Porttabelle)

1. Öffnen Sie die Seite Private VLAN (Privates VLAN).
2. Klicken Sie auf **Show PV Ports** (PV-Ports anzeigen).

Die **PV Ports Table (PV-Porttabelle)** wird geöffnet:

Abbildung 7-37. PV Ports Table (PV-Porttabelle)



Konfigurieren von PVLANs mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite **Private VLAN (Privates VLAN)** äquivalenten CLI-Befehle zum Konfigurieren von PVLANs zusammengefasst.

Tabelle 7-23. CLI-Befehle für private VLANs

CLI-Befehl	Beschreibung
switchport mode private vlan promiscuous	**Fügt einem Promiscuous-VLAN einen Promiscuous-Port hinzu.**
switchport mode private vlan community	**Fügt einem Community-VLAN einen Community-Port hinzu.**
switchport mode private vlan isolated	**Fügt einem isolierten VLAN einen isolierten Port hinzu.**
private-vlan primary	Definiert ein primäres VLAN.
private-vlan community {add Community-VLAN-Liste | remove Community-VLAN-Liste }	Definiert oder entfernt ein Community-VLAN des primären VLANs.
private-vlan isolated	Definiert ein Isolated-VLAN des primären VLANs.
switchport private-vlan *PVLAN* **[community** *CVLAN***]**	Definiert private VLAN-Ports**.**
show vlan private-vlan [primary vlan-id]	Zeigt das private primäre VLAN.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# vlan
database

console(config-vlan)#vlan
2

console(config-vlan)#exit

console(config)#interface
vlan 2

console(config-if)#
private-vlan primary

console(config)#interface
vlan 2

console(config-if)#
private-vlan isolated 10

console(config-if)#
private-vlan community add
20
```

```
console# show vlan
private-vlan



console(config-if)# end
```

Aggregieren von Ports

Bei der Link-Aggregation wird zur Optimierung der Portnutzung eine Gruppe aus mehreren Ports zu einer LAG (Link Aggregated Group) zusammengeschaltet. Die Portaggregation vervielfacht die zwischen den Geräten verfügbare Bandbreite, steigert die Flexibilität der Ports und ermöglicht redundante Verbindungen.

Das Gerät unterstützt sowohl statische LAGs als auch LAGs gemäß dem Link Aggregation Control Protocol (LACP).LACP-LAGs handeln die Verbindungen der aggregierten Ports mit anderen LACP-Ports aus, die sich an einem anderen Gerät befinden. Wenn es sich bei den Ports des anderen Gerätes ebenfalls um LACP-Ports handelt, richten die Geräte eine LAG für diese Ports ein.

Beim Aggregieren von Ports ist Folgendes zu berücksichtigen:

- Alle Ports innerhalb einer LAG müssen denselben Medientyp aufweisen.
- Auf dem Port darf kein VLAN konfiguriert sein.
- Der Port darf keiner anderen LAG zugewiesen sein.
- Auto-Negotiation darf auf dem Port nicht konfiguriert sein.
- Der Port muss sich im Vollduplexmodus befinden.
- Alle Ports in der LAG müssen sich in den gleichen Ingress-Filter- und Kennungsmodi befinden.
- Alle Ports in der LAG müssen sich in den gleichen Backpressure- und Flusskontrollmodi befinden.
- Alle Ports in der LAG müssen die gleiche Priorität haben.
- Alle Ports in der LAG müssen den gleichen Transceiver-Typ haben.
- Das Gerät unterstützt bis zu acht LAGs sowie acht Ports in jeder LAG.
- Ports können nur als LACP-Ports konfiguriert werden, wenn sie keiner zuvor konfigurierten LAG angehören.

Beim Hinzufügen zu einer LAG verlieren die Ports ihre individuelle Portkonfiguration. Wenn Ports aus der LAG entfernt werden, wird wieder die ursprüngliche Port-Konfiguration auf sie angewendet.

Das Gerät legt über eine Hash-Funktion fest, welche Pakete über welche Komponente der aggregierten Verbindung übertragen werden. Die Hash-Funktion sorgt für den statistischen Lastenausgleich zwischen den aggregierten Verbindungskomponenten. Das Gerät betrachtet eine aggregierte Verbindung als einen einzigen logischen Port.

Definieren von LACP-Parametern

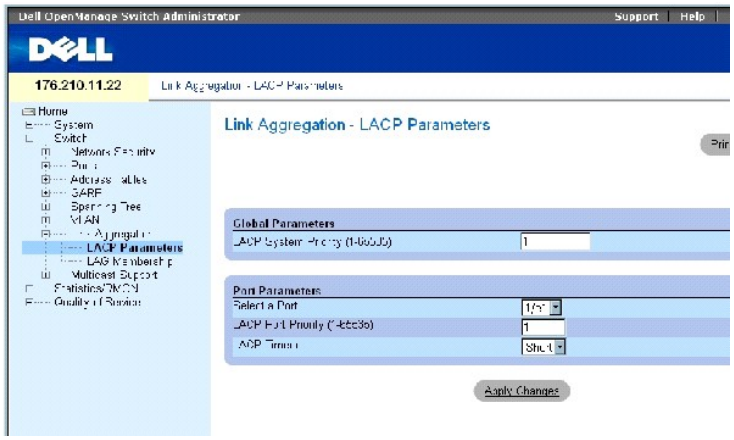
Aggregierte Ports können in Link-Aggregation-Gruppen (LAGs) zusammengefasst werden. Innerhalb einer einzelnen Gruppe sind alle Ports auf dieselbe Geschwindigkeit und auf Vollduplexbetrieb eingestellt.

Ports in einer LAG können unterschiedliche Medientypen aufweisen, wenn die Ports mit derselben Geschwindigkeit arbeiten. Aggregierte Verbindungen können manuell oder automatisch konfiguriert werden, indem auf den relevanten Verbindungen das Link Aggregation Control Protocol (LACP) aktiviert wird.

Definieren von LACP-Parametern

Die Seite **LACP Parameters** (LACP-Parameter) enthält Felder zur Konfiguration von LACP-LAGs. Aggregierte Ports können in Link-Aggregation-Gruppen (LAGs) 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. So öffnen Sie die Seite LACP Parameters (LACP-Parameter): Klicken Sie in der Strukturansicht auf **Switch→ Link Aggregation→ LACP Parameters**.

Abbildung 7-38. LACP Parameters (LACP-Parameter)



Die Seite LACP Parameters (LACP-Parameter) enthält folgende Felder:

LACP System Priority (LACP-Systempriorität, 1-65535) – Der LACP-Prioritätswert für globale Einstellungen. Der Wertebereich umfasst die Werte 1 bis 65535. Der Standardwert lautet 1.

Select a Port (Port auswählen) – Die Portnummer, der Zeitüberschreitungs- und Prioritätswerte zugewiesen werden.

LACP Port Priority (LACP-Portpriorität, 1-65535) – LACP-Prioritätswert für den Port.

LACP Timeout (LACP-Zeitüberschreitung) – Administrierte LACP-Zeitüberschreitung. Folgende Feldwerte sind möglich:

Short (Kurz) – Legt eine kurze Zeitüberschreitung fest.

Long (Lang) – Legt eine lange Zeitüberschreitung fest.

Definieren von globalen Link-Aggregation-Parametern

1. Öffnen Sie die Seite LACP Parameters (LACP-Parameter).
2. Füllen Sie das Feld **LACP System Priority** (LACP-Systempriorität) aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Parameter werden definiert und das Gerät aktualisiert.

Definieren von Link-Aggregation-Portparametern

1. Öffnen Sie die Seite LACP Parameters (LACP-Parameter).
2. Füllen Sie die Felder im Bereich **Port Parameters** (Portparameter) aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Parameter werden definiert und das Gerät aktualisiert.

Anzeigen der LACP Parameters Table (LACP-Parametertabelle)

1. Öffnen Sie die Seite LACP Parameters (LACP-Parameter).
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die **LACP Parameters Table** (LACP-Parametertabelle) wird geöffnet.

Konfigurieren von LACP-Parametern mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite LACP Parameters (LACP-Parameter) äquivalenten CLI-Befehle zum Konfigurieren der LACP-Parameter zusammengefasst.

Tabelle 7-87. CLI-Befehle für LACP-Parameter

CLI-Befehl	Beschreibung
lacp system-priority *Wert*	Konfiguriert die Systempriorität.
lacp port-priority *Wert*	Konfiguriert den Prioritätswert für physische Ports.
lacp timeout {**long** | **short**}	Weist einen administrativen Wert für die LACP-Zeitüberschreitung zu.
show lacp ethernet *Schnittstelle* [**parameters** | **statistics** | **protocol-state**]	Zeigt LACP-Informationen für Ethernet-Ports an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console (config)# lacp
system-priority 120

Console (config)#
interface ethernet 1/e11

Console (config-if)# lacp
port-priority 247

Console (config-if)# lacp
timeout long

Console (config-if)# end

Console# show lacp
ethernet 1/e11 statistics

Port 1/e11 LACP
Statistics:

LACP PDUs sent:2

LACP PDUs received:2
```

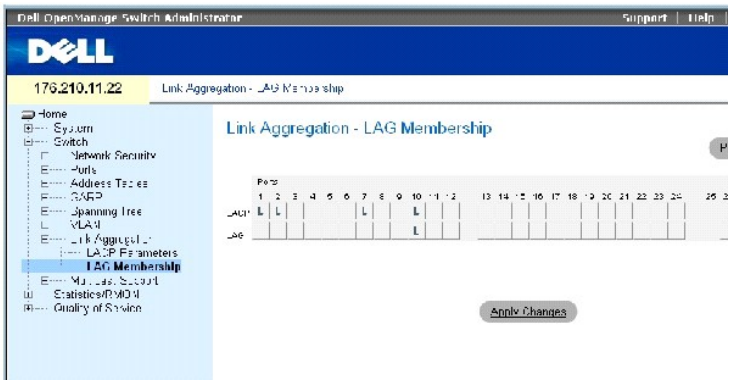
Definieren von LAG-Mitgliedschaften

Das Gerät unterstützt bis zu acht LAGs pro System sowie acht Ports in jeder LAG, unabhängig davon, ob das Gerät eigenständig oder in einem Stack betrieben wird.

Wenn ein Port einer LAG hinzugefügt wird, übernimmt er die Eigenschaften der LAG. Wenn es nicht möglich ist, den Port mit den Eigenschaften der LAG zu konfigurieren, wird er der LAG nicht hinzugefügt, und es wird eine Fehlermeldung generiert. Wenn jedoch der erste Port, der der LAG beitritt, nicht mit den LAG-Einstellungen konfiguriert werden kann, wird er dennoch der LAG hinzugefügt, wobei die Standard-Porteinstellungen verwendet werden, und es wird eine Fehlermeldung generiert. Da es sich jedoch um den einzigen Port in der LAG handelt, arbeitet die gesamte LAG mit den Einstellungen des Ports anstelle der für die LAG definierten Einstellungen.

Verwenden Sie die Seite **LAG Membership (LAG-Mitgliedschaft)**, um Ports zu LAGs zuzuweisen. So öffnen Sie die Seite **LAG Membership (LAG-Mitgliedschaft)**: Klicken Sie in der Strukturansicht auf **Switch** → **Link Aggregation**→ **LAG Membership**.

Abbildung 7-39. LAG Membership (LAG-Mitgliedschaft)



Die Seite **LAG Membership (LAG-Mitgliedschaft)** enthält folgende Felder:

LACP – Aggregiert den Port unter Verwendung von LACP zu einer LAG.

LAG – Fügt den Port einer LAG hinzu und gibt die spezifische LAG an, zu der der Port gehören soll.

Hinzufügen von Ports zu einer LAG oder LACP

1. Öffnen Sie die Seite **LAG Membership (LAG-Mitgliedschaft)**.
2. Schalten Sie die Schaltfläche in der LAG-Zeile (die zweite Zeile) auf eine Nummer um, um den Port zu der LAG mit dieser Nummer hinzuzufügen bzw. aus ihr zu entfernen.
3. Schalten Sie in der LACP-Zeile (die erste Zeile) die Schaltfläche unter der Portnummer um, um entweder die LACP oder die statische LAG zuzuweisen.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Port wird der LAG bzw. LACP hinzugefügt, und das Gerät wird aktualisiert.

Hinzufügen von Ports zu LAGs mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite **LAG Membership (LAG-Mitgliedschaft)** äquivalenten CLI-Befehle zum Zuweisen von Ports an LAGs zusammengefasst.

Tabelle 7-24. CLI-Befehle für LAG-Mitgliedschaft

CLI-Befehl	Beschreibung
channel-group *Port-Kanalnummer* **mode** {**on** | **auto**}	Ordnet einen Port einem Port-Kanal zu. Mit der no-Form dieses Befehls wird die Kanalgruppen-Konfiguration von der Schnittstelle entfernt.
show interfaces port-channel [*Port-Kanalnummer*]	Zeigt Port-Kanalinformationen an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# interface
ethernet 1/e11

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

Unterstützung für Multicast-Weiterleitung

Bei der Multicast-Weiterleitung können einzelne Pakete an mehrere Ziele weitergeleitet werden. Der Multicastdienst auf Layer 2 beruht darauf, dass ein Layer-2-Gerät ein einzelnes Paket empfängt, das an eine bestimmte Multicastadresse adressiert ist. Die Multicast-Weiterleitung erstellt Kopien der Pakete und überträgt die Pakete an die relevanten Ports.

Registered Multicast traffic (Registrierter Multicastverkehr) – Wenn Daten empfangen werden, die an eine registrierte Multicastgruppe adressiert sind, werden diese von einem Eintrag in der Multicast-Filterdatenbank behandelt und nur an die registrierten Ports weitergeleitet.

Unregistered Multicast traffic (Unregistrierter Multicastverkehr) – Wenn Daten empfangen werden, die an eine nicht registrierte Multicastgruppe adressiert sind, werden sie von einem speziellen Eintrag in der Multicast-Filterdatenbank behandelt. Die Standardeinstellung lautet, jeglichen solchen Datenverkehr (d. h. Datenverkehr an nicht registrierte Multicastgruppen) zu fluten.

Das Gerät unterstützt folgende Optionen:

- **Forwarding L2 Multicast Packets** (Weiterleiten von L2-Multicastpaketen) – Layer-2-Multicastpakete werden weitergeleitet. Die Layer-2-Multicastfilterung wird aktiviert und kann nicht vom Benutzer konfiguriert werden.

ANMERKUNG: Das System unterstützt die Multicastfilterung für 256 Multicastgruppen.

- **Filtering L2 Multicast Packets** (Filtern von L2-Multicastpaketen) – Leitet Layer-2-Pakete an Schnittstellen weiter. Wenn die Multicastfilterung deaktiviert ist, werden Multicastpakete an alle relevanten Ports geflutet.

So öffnen Sie die Seite **Multicast Support** (Multicast-Unterstützung): Klicken Sie in der Strukturansicht auf **Switch** → **Multicast Support**.

Definieren von Globalen Multicast-Parametern

Das Layer-2-Switching leitet Multicastpakete standardmäßig an alle relevanten VLAN-Ports weiter, wobei das Paket als eine einzige Multicast-Übertragung behandelt wird. Die Weiterleitung von Multi-cast-verkehr ist effektiv, jedoch nicht optimal, da die Multicastpakete auch von nicht beabsich-tig-ten Ports empfangen werden. Diese überschüssigen Pakete bedeuten ein unnötig hohes Daten-aufkommen auf dem Netzwerk. Mit Multicast-Weiterleitungsfiltern werden Layer-2-Paketen nur an Port-Untergruppen weitergeleitet.

Wenn IGMP-Snooping global aktiviert ist, werden alle IGMP-Pakete an die CPU weitergeleitet. Die CPU analysiert die eingehenden Pakete und bestimmt

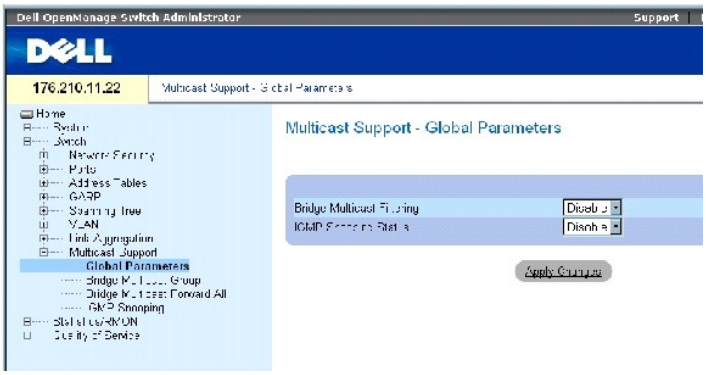
- welche Ports welchen Multicastgruppen beitreten möchten,
- welche Ports Multicastrouter aufweisen, die IGMP-Anfragen generieren und
- welche Routingprotokolle Pakete und Multicastverkehr weiterleiten.

Ports fordern die Teilnahme an einer bestimmten Multicastgruppe an, indem sie einen IGMP-Bericht ausgeben, der die Mitglieder aufnehmende Multicastgruppe bezeichnet. Dies führt dazu, dass die Multicast-Filterdatenbank erstellt wird.

So öffnen Sie die Seite **Multicast Support** (Multicast-Unterstützung): Klicken Sie in der Strukturansicht auf **Switch** → **Multicast Support**.

Die Seite **GlobaleParametes (Globale Parameter)** enthält Felder zum Aktivieren von IGMP-Snooping auf dem Gerät. So öffnen Sie die Seite **GlobaleParametes (Globale Parameter)**: Klicken Sie in der Strukturansicht auf **Switch→ Multicast Support→ Global Parameters**.

Abbildung 7-40. GlobaleParametes (Globale Parameter)



Die Seite **GlobaleParametes (Globale Parameter)** enthält folgende Felder:

Bridge Multicast Filtering (Bridge-Multicastfilterung) – Aktiviert oder deaktiviert die Bridge-Multicastfilterung. Der Standardwert lautet disabled (deaktiviert).

IGMP Snooping Status (IGMP-Snooping-Status) – aktiviert oder deaktiviert IGMP-Snooping auf dem Gerät. Der Standardwert lautet disabled (deaktiviert). IGMP-Snooping kann nur aktiviert werden, wenn **GlobaleParametes (Globale Parameter)** aktiviert ist.

Aktivieren von Bridge-Multicastfilterung auf dem Gerät

1. Öffnen Sie die Seite **GlobaleParametes (Globale Parameter)**.
2. Wählen Sie im Feld **Bridge Multicast Filtering** (Bridge-Multicastfilterung) den Eintrag **Enable** (Aktivieren) aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Bridge-Multicastfilterung *wird* auf dem Gerät aktiviert.

Aktivieren von IGMP-Snooping auf dem Gerät

1. Öffnen Sie die Seite **GlobaleParametes (Globale Parameter)**.
2. Wählen im Feld **IGMP Snooping Status** (IGMP-Snoopingstatus) den Eintrag **Enable** (Aktivieren) aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

IGMP-Snooping wird auf dem Gerät aktiviert.

Aktivieren von Multicastfilterung und IGMP-Snooping mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite **GlobaleParametes (Globale Parameter)** äquivalenten CLI-Befehle zum Aktivieren von Multicastfilterung und IGMP-Snooping zusammengefasst.

Tabelle 7-25. CLI-Befehle für Multicastfilterung und IGMP-Snooping

CLI-Befehl	Beschreibung
bridge multicast filtering	Aktiviert die Filterung von Multicastadressen.
ip igmp snooping	Aktiviert das Snooping des Internet Group Membership Protocol (IGMP).

Im Folgenden ein Beispiel für die CLI-Befehle:

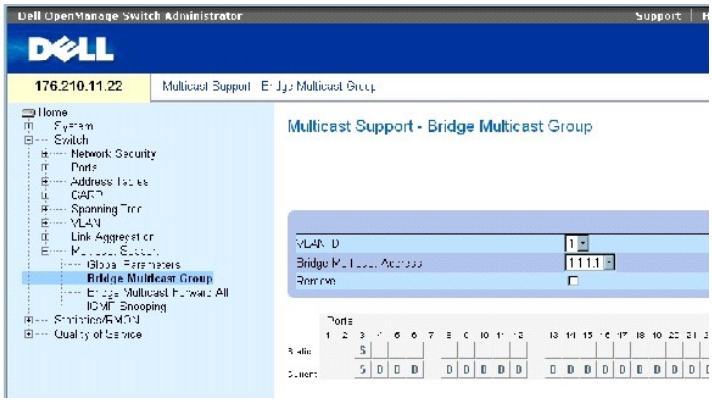
```
console(config)# bridge
multicast filtering

console(config)# ip igmp
snooping
```

Hinzufügen von Mitgliedern zu einer Bridge-Multicastgruppe

Die Seite **Bridge Multicast Group (Bridge-Multicastgruppe)** zeigt in den Tabellen **Ports** und **LAGs** die mit der Multicast-Servicegruppe verbundenen Ports und LAGs an. In den Port- und LAG-Tabellen wird auch angegeben, auf welche Weise der Port oder die LAG der Multicastgruppe hinzugefügt wurde. Ports können entweder vorhandenen Gruppen oder einer neuen Multicast-Servicegruppe hinzugefügt werden. Die Seite **Bridge Multicast Group (Bridge-Multicastgruppe)** erlaubt die Erstellung neuer Multicast-Servicegruppen. Die Seite **Bridge Multicast Group (Bridge-Multicastgruppe)** dient außerdem der Zuweisung von Ports an eine bestimmte Multicast-Serviceadressgruppe.

So öffnen Sie die Seite **Bridge Multicast Group (Bridge-Multicastgruppe)**: Klicken Sie in der Strukturansicht auf **Switch→ Multicast Support→ Bridge Multicast Group**.

Abbildung 7-41. Bridge Multicast Group (Bridge-Multicastgruppe)



Die Seite **Bridge Multicast Group (Bridge-Multicastgruppe)** enthält folgende Felder:

VLAN ID (VLAN-ID) – Bezeichnet ein VLAN und enthält Informationen zur Adresse der Multicastgruppe.

Bridge Multicast Address (Bridge-Multicastadresse) – Bezeichnet die MAC-/IP-Adresse der Multicastgruppe.

Remove (Entfernen) – Wenn dieses Kontrollkästchen markiert ist, wird eine Bridge-Multicastadresse entfernt.

Ports (Ports) – Ports, die zu einem Multicastservice hinzugefügt werden können.

LAGs (LAGs) – LAGs, die zu einem Multicastservice hinzugefügt werden können.

Die folgende Tabelle enthält die Verwaltungseinstellungen für IGMP-Port- und LAG-Mitglieder.

Tabelle 7-26. Tabelle: Steuereinstellungen in der IGMP-Port- /LAG-Mitgliedertabelle

Portsteuerung	Definition

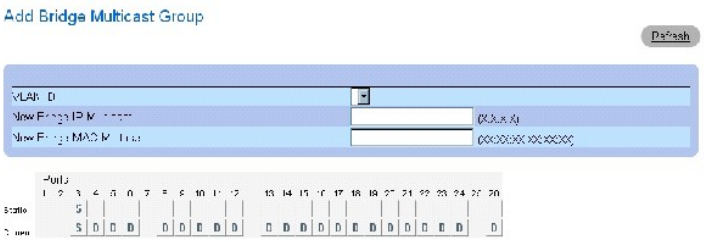
D	Gibt in der Zeile *Current* (Aktuell) an, dass der Port/die LAG der Multicastgruppe dynamisch beigetreten ist.
S	Verknüpft den Port in der Zeile *Static* (Statisch) als statisches Mitglied mit der Multicastgruppe. Gibt in der Zeile *Current* (Aktuell) an, dass der Port/die LAG der Multicastgruppe statisch beigetreten ist.
F	Verboten.
Leer	Der Port ist mit keiner Multicastgruppe verknüpft.

Hinzufügen von Bridge-Multicastadressen

1. Öffnen Sie die Seite **Bridge Multicast Group (Bridge-Multicastgruppe)**.
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite **Add Bridge Multicast Group (Bridge-Multicastgruppe hinzufügen)** wird geöffnet:

Abbildung 7-42. Add Bridge Multicast Group (Bridge-Multicastgruppe hinzufügen)



3. Definieren Sie die Felder **VLAN ID** (VLAN-ID) und **New Bridge Multicast Address** (Neue Bridge-Multicastadresse).
4. Schalten Sie einen Port auf **S** um, um ihn der ausgewählten Multicastgruppe hinzuzufügen.
5. Schalten Sie einen Port auf **F** um, um das Hinzufügen bestimmter Multicast-Adressen an diesen Port zu verbieten.
6. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die Bridge-Multicastadresse wird der Multicast-Gruppe zugewiesen und das Gerät aktualisiert.

Definieren von Ports für den Empfang von Multicastservice

1. Öffnen Sie die Seite **Bridge Multicast Group (Bridge-Multicastgruppe)**.
2. Definieren Sie die Felder **VLAN ID** (VLAN-ID) und **Bridge Multicast Address** (Bridge- Multicastadresse).
3. Schalten Sie einen Port auf **S** um, um ihn der ausgewählten Multicastgruppe hinzuzufügen.
4. Schalten Sie einen Port auf **F** um, um das Hinzufügen bestimmter Multicast-Adressen an diesen Port zu verbieten.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Port wird der Multicastgruppe zugewiesen und das Gerät aktualisiert.

Zuweisen von LAGs für den Empfang von Multicastservice

1. Öffnen Sie die Seite **Bridge Multicast Group (Bridge-Multicastgruppe)**.
2. Definieren Sie die Felder **VLAN ID** (VLAN-ID) und **Bridge Multicast Address** (Bridge- Multicastadresse).
3. Schalten Sie die LAG auf **S** um, um sie der ausgewählten Multicastgruppe hinzuzufügen.
4. Schalten Sie die LAG auf **F** um, um das Hinzufügen bestimmter Multicast-Adressen zu dieser LAG zu verbieten.
5. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die LAG wird der Multicastgruppe zugewiesen und das Gerät aktualisiert.

Verwalten von Multicastservice-Mitgliedern mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die der Seite **Bridge Multicast Group (Bridge-Multicastgruppe)** äquivalenten CLI-Befehle zum Verwalten von Multicastservice-Mitgliedern zusammengefasst.

Tabelle 7-27. CLI-Befehle für Multicastservice-Mitglieder

CLI-Befehl	Beschreibung
bridge multicast address {*MAC-Multicastadresse* | *IP-Multicastadresse*}	Registriert Multicastadressen des MAC-Layers in der Bridge-Tabelle und fügt der Gruppe statische Ports hinzu.
bridge multicast forbidden address {*MAC-Multicastadresse* | *IP-Multicastadresse*}[**add** | **remove**] {**ethernet** *Schnittstellenliste* | **port-channel** *Port-Kanalnummernliste*}	Verbietet das Hinzufügen einer spezifischen Multicastadresse an spezifische Ports. Mit der no-Form dieses Befehls können Sie den Standardzustand wieder herstellen.
show bridge multicast address-table [**vlan** *VLAN-ID*] [**address** {*MAC-Multicastadresse* | *IP-Multicastadresse*}] [**format ip** | **mac**]	Zeigt Informationen der MAC-Multicastadresstabelle an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console(config-if)# bridge multicast address 0100.5e02.0203

add ethernet 1/e11,1/e12

console(config-if)# end

console # show bridge multicast address-table
```

Vlan	MAC Address	Type	Ports
----	-----------	-----	----------
1	0100.5e02.0203	static	1/e11, 1/e12
19	0100.5e02.0208	static	1/e11-16
19	0100.5e02.0208	dynamic	1/e11-12

```
Forbidden ports for multicast addresses:
```

Vlan	MAC Address	Ports	
----	-----------	----------	
1	0100.5e02.0203	1/e8	
19	0100.5e02.0208	1/e8	

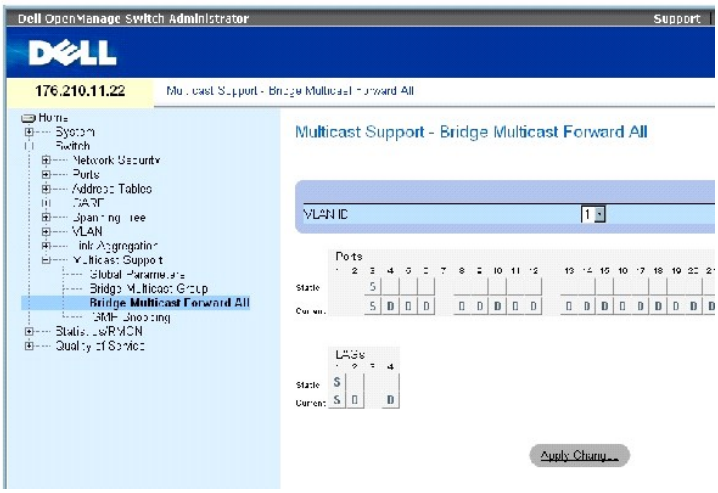
console # **show bridge multicast address-table format ip**			
Vlan	IP Address	Type	Ports
----	----------	-----	----------
1	224-239.130|2.2.3	static	1/e11, 1/e12
19	224-239.130|2.2.8	static	1/e11-16
19	224-239.130|2.2.8	dynamic	1/e11-12
Forbidden ports for multicast addresses:			
Vlan	IP Address	Ports	
----	----------	----------	
1	224-239.130|2.2.3	1/e8	
19	224-239.130|2.2.8	1/e8	

Zuweisen von Parametern für das Multitaskingmerkmal Alle weiterleiten

Die Seite **Bridge Multicast Forward All (Bridge-Multicastmerkmal alle weiterleite)** enthält Felder, mit denen Ports oder LAGs mit einem Gerät verbunden werden können, das mit einem benachbarten Multicast-Router/-Switch verbunden ist. Sobald IGMP-Snooping aktiviert wird, werden die Multicast-Pakete an den entsprechenden Port bzw. das entsprechende VLAN weitergeleitet.

So öffnen Sie die Seite **Bridge Multicast Forward All (Bridge-Multicastmerkmal alle weiterleite)**: Klicken Sie in der Strukturansicht auf **Switch→ Multicast Support→ Bridge Multicast Forward All (Bridge-Multicastmerkmal alle weiterleite)**.

Abbildung 7-43. Bridge Multicast Forward All (Bridge-Multicastmerkmal alle weiterleite)



Die Seite Bridge Multicast Forward All (Bridge-Multicastmerkmal alle weiterleite) enthält folgende Felder:

VLAN ID (VLAN-ID) – Bezeichnet ein VLAN.

Ports (Ports) – Ports, die einem Multicastservice hinzugefügt werden können.

LAGs (LAGs) – LAGs, die einem Multicastservice hinzugefügt werden können.

Die **Switch-/Port-Steuerungseinstellungstabelle für das Bridge-Multicastingmerkmal Alle weiterleiten** enthält die Einstellungen für die Verwaltung von Router- und Porteinstellungen.

Verwalten der Switch-/Port-Steuerungseinstellungstabelle für das Bridge-Multicastmerkmal Alle weiterleiten

Die folgende Tabelle beschreibt die Einstellungen für die Portsteuerung.

Tabelle 7-28. Switch-/Port-Steuerungseinstellungstabelle für das Bridge-Multicastingmerkmal Alle weiterleiten

Portsteuerung	Definition
D	Verbindet den Port als dynamischen Port mit dem Multicast-Router oder -Switch.
S	Verbindet den Port als statischen Port mit dem Multicast-Router oder -Switch.
F	Verboten.
Leer	Der Port ist mit keinem Multicast-Router oder -Switch verbunden.

Verbinden eines Ports mit einem Multicast-Router oder -Switch

1. Öffnen Sie die Seite **Bridge Multicast Forward All (Bridge-Multicastmerkmal alle weiterleite)**.
2. Definieren Sie das Feld **VLAN ID** (VLAN-ID).
3. Wählen Sie in der **Ports**-Tabelle einen Port aus, und weisen Sie ihm einen Wert zu.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Port wird mit dem Multicast-Router oder -Switch verbunden.

Verbinden einer LAG mit einem Multicast-Router oder -Switch

1. Öffnen Sie die Seite **Bridge Multicast Forward All (Bridge-Multicastmerkmal alle weiterleite)**.
2. Definieren Sie das Feld **VLAN ID** (VLAN-ID).
3. Wählen Sie in der **LAGs**-Tabelle eine LAG aus, und weisen Sie ihr einen Wert zu.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die LAG wird mit dem Multicast-Router oder -Switch verbunden.

Verwalten von mit Multicast-Routern verbundenen LAGs und Ports mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **Bridge Multicast Forward All (Bridge-Multicastmerkmal alle weiterleite)** äquivalenten CLI-Befehle zum Verwalten von mit Multicast-Routern verbundenen LAGs und Ports zusammengefasst.

Tabelle 7-29. CLI-Befehle zum Verwalten von mit Multicast-Routern verbundenen LAGs und Ports

CLI-Befehl	Beschreibung
show bridge multicast filtering *VLAN-ID*	Zeigt die Multicast-Filterkonfiguration an.
bridge multicast forward-all {**add** | **remove**} {**ethernet** *Schnittstellenliste* | **port-channel** *Port-Kanalnummernliste*}	Aktiviert auf einem Port die Weiterleitung aller Multicastpakete. Mit der no-Form dieses Befehls können Sie den Standardzustand wieder herstellen.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
Console(config)# interface vlan 1

Console(config-if)# bridge multicast forward-all add ethernet 1/e3

Console(config-if)# end

Console# show bridge multicast filtering 1
```

```
Filtering: Enabled
```

VLAN:	Forward-All	
Port	Static	Status
-------	----------	----------
1/e11	Forbidden	Filter
1/e12	Forward	Forward(s)
1/e13	-	Forward(d)

IGMP-Snooping

Die Seite **IGMP Snooping** enthält Felder zum Aktivieren von IGMP-Snooping für einzelne VLANs und zum Definieren der Aging-Zeit (Speicherdauer) für Pakete. So öffnen Sie die Seite **IGMP Snooping (IGMP-Snooping)**: Klicken Sie in der Strukturansicht auf **Switch**→ **Multicast Support**→ **IGMP Snooping**.

Abbildung 7-44. IGMP Snooping (IGMP-Snooping)

VLAN ID (VLAN-ID) – Gibt die VLAN-ID an.

IGMP Snooping Status (IGMP-Snoopingstatus) – Aktiviert oder deaktiviert IGMP-Snooping auf dem VLAN.

Auto Learn (Autom. Erfassen) – Aktiviert oder deaktiviert das automatische Erfassen auf dem Ethernetgerät.

Host Timeout (1-2147483647) (Host-Zeitüberschreitung) – Zeit, nach der die Speicherdauer eines IGMP-Snooping-Eintrags abläuft. Der Standardwert lautet 260 Sekunden.

Multicast Router Timeout (1-2147483647) (Multicast-Router-Zeitüberschreitung) – Zeit, nach der ein Multicast-Routereintrag abläuft. Der Standardwert lautet 300 Sekunden.

Leave Timeout (0-2147483647) (Leave-Zeitüberschreitung) – Zeit (in Sekunden), bevor nach Empfang einer Leave-Nachricht für einen Port der entsprechende Eintrag abläuft. Der Standardwert lautet 10 Sekunden.

Aktivieren von IGMP-Snooping auf dem Gerät

1. Öffnen Sie die Seite **IGMP Snooping (IGMP-Snooping)**.
2. Wählen Sie die VLAN-ID für das Gerät, auf dem IGMP-Snooping aktiviert werden soll.
3. Wählen Sie im Feld **IGMP Snooping Status** (IGMP-Snoopingstatus) den Eintrag **Enable** (Aktivieren) aus.
4. Füllen Sie die Felder auf der Seite aus.
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 (IGMP-Snooping)**.
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die **IGMP Snooping Table** (IGMP-Snooping-Tabelle) wird geöffnet.

Konfigurieren von IGMP-Snooping mit Hilfe von CLI-Befehlen

In der folgenden Tabelle werden die entsprechenden CLI-Befehle zum Konfigurieren von IGMP Snooping (IGMP-Snooping) auf dem Gerät zusammengefasst:

Tabelle 7-30. CLI-Befehle für IGMP-Snooping

CLI-Befehl	Beschreibung
ip igmp snooping	Aktiviert das Snooping des Internet Group Membership Protocol (IGMP).
ip igmp snooping mrouter learn-pim-dvmrp	Aktiviert die automatische Erfassung von Multicastrouter-Ports im Kontext eines spezifischen VLANs.
ip igmp snooping host-time-out Timeout	Konfiguriert den Wert host-time-out (Host-Zeitüberschreitung).
ip igmp snooping mrouter-time-out *Timeout*	Konfiguriert den Wert mrouter-time-out (Multicastrouter-Zeitüberschreitung).
ip igmp snooping leave-time-out {*Timeout* | **immediate-leave**}	Konfiguriert den Wert leave-time-out (Leave-Zeitüberschreitung).
show ip igmp snooping groups [**vlan** *VLAN-ID*] [**address** *IP-Multicastadresse*]	Zeigt die durch IGMP-Snooping erfassten Multicastgruppen an.
show ip igmp snooping interface *VLAN-ID*	Zeigt die IGMP-Snooping-Konfiguration an.
show ip igmp snooping mrouter [Schnittstelle VLAN-ID]	Zeigt Informationen zu dynamisch erfassten Multicastrouter-Schnittstellen an.

Im Folgenden ein Beispiel für 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)# ip igmp
snooping leave-time-out 60

console(config-if)# end

console# show ip igmp snooping
groups
```

Vlan	IP Address	Querier	Ports
----	----------	------	------
1	224-239.130|2.2.3	Yes	1/e11, 1/e12

19	224-239.130|2.2.8	Yes	1/e11-13

```
console# show ip igmp snooping interface 1/e1


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	1/e11		

Zurück zum Inhalt

Zurück zum Inhalt

Anzeigen von Statistiken

Dell™ PowerConnect™ 34XX- Systeme Benutzerhandbuch

Die Statistikseiten enthalten Geräteinformationen zu Schnittstellen, GVRP, Etherlike, RMON sowie zur Gerätenutzung. Klicken Sie zum Öffnen der Statistikseiten in der Strukturansicht auf **Statistics**.

ANMERKUNG: Für die Statistikseiten sind keine CLI-Befehle verfügbar.

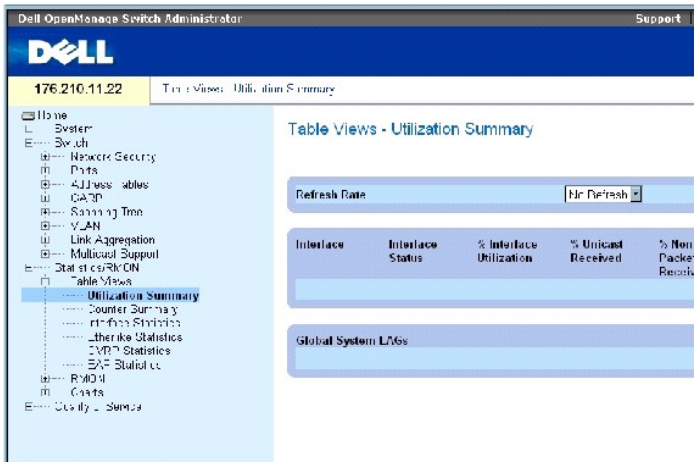
Anzeigen von Tabellen

Die Seite **Table Views** (Tabellenansichten) enthält Links zur Anzeige von Statistiken in Tabellenform. Klicken Sie zum Öffnen der Statistikseiten in der Strukturansicht auf **Statistics→ Table**.

Anzeigen der Nutzungsübersicht

Die Seite Utilization Summary (Nutzungsübersicht) enthält Statistiken zur Schnittstellennutzung. Klicken Sie zum Öffnen der Seite in der Strukturansichtauf **Statistics→ Table Views→ Utilization Summary**.

Abbildung 8-1. Utilization Summary (Nutzungsübersicht)



ANMERKUNG: Dieser Bildschirm wird in bestimmten Zeitabständen aktualisiert, um Computer mit geringerer Speicherkapazität nicht übermäßig zu belasten. In dieser Phase wird die Anzeige eventuell kurzfristig unterbrochen.

Die Seite Utilization Summary (Nutzungsübersicht) enthält folgende Felder:

Refresh Rate – Gibt den Zeitraum bis zur Aktualisierung der Schnittstellenstatistiken an.

Interface – Die Schnittstellennummer.

Interface Status – Status der Schnittstelle.

% Interface Utilization – Prozentuale Auslastung der Netzwerkschnittstelle im Duplexmodus Der hier angezeigte Wert kann zwischen 0 und 200 % liegen. Der maximale Anzeigewert für eine Vollduplexverbindung (200 %) signalisiert, dass die gesamte Bandbreite von ein- und ausgehenden Verbindungen für den Datenverkehr über diese Schnittstelle belegt ist. Der maximale Anzeigewert für eine Halbduplexverbindung ist 100 %.

% Unicast Received – Prozentualer Anteil der schnittstellenseitig empfangenen Unicastpakete.

% Non Unicast Packets Received – Prozentualer Anteil der schnittstellenseitig empfangenen sonstigen Datenpakete (nicht Unicast).

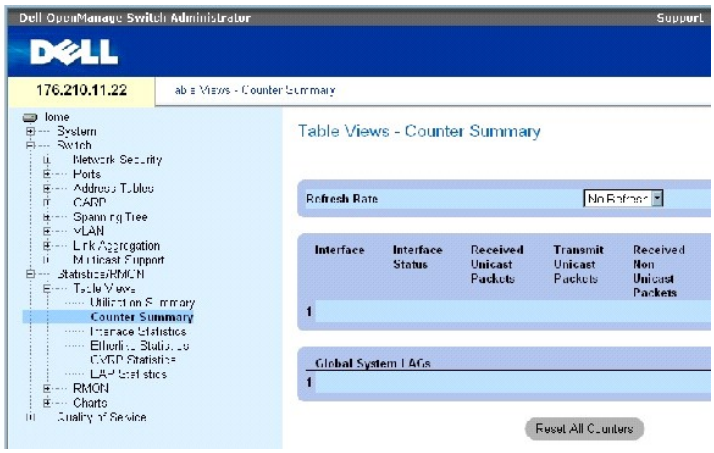
% Error Packets Received – Prozentualer Anteil der schnittstellenseitig empfangenen fehlerhaften Datenpakete.

Global System LAGs – Gibt die aktuelle globale LAG-Nutzung an.

Anzeigen der Zählerübersicht

Die auf der Seite **Counter Summary (Zählerübersicht)** enthaltenen Statistiken geben die Port-Nutzung in absoluten Zahlen und nicht in Prozentwerten wieder. Klicken Sie zum Öffnen der Seite **Counter Summary (Zählerübersicht)** in der Strukturansicht auf **Statistics/RMON→ Table Views→ Counter Summary**.

Abbildung 8-2. Counter Summary (Zählerübersicht)



Die Seite Counter Summary (Zählerübersicht) enthält folgende Felder:

Refresh Rate – Gibt den Zeitraum bis zur Aktualisierung der Schnittstellenstatistiken an.

Interface – Die Schnittstellennummer.

Interface Status – Status der Schnittstelle.

Received Unicast Packets – Die Anzahl der schnittstellenseitig empfangenen Unicastpakete.

Transmit Unicast Packets – Die Anzahl der über die Schnittstelle gesendeten Unicastpakete.

Received Non Unicast Packets – Die Anzahl der schnittstellenseitig empfangenen sonstigen Pakete (nicht Unicast).

Transmit Non Unicast Packets – Die Anzahl der über die Schnittstelle gesendeten sonstigen Pakete (nicht Unicast).

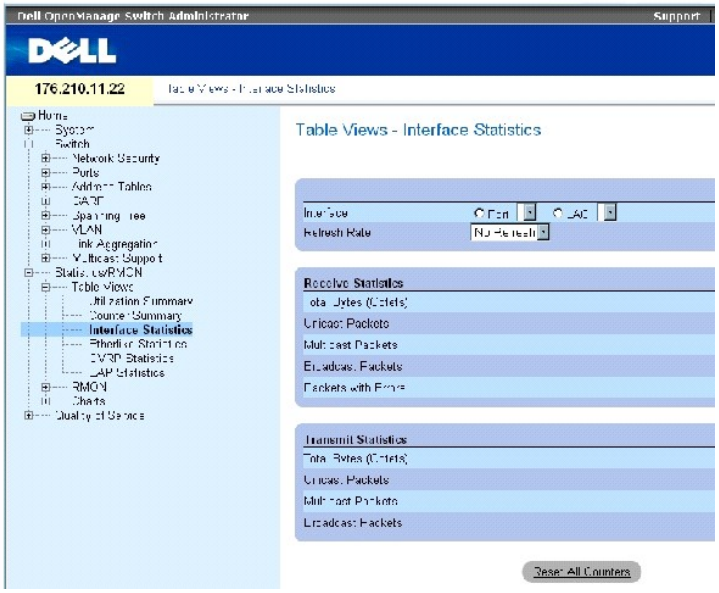
Received Errors – Die Anzahl der schnittstellenseitig empfangenen fehlerhaften Datenpakete.

Global System LAGs – Bietet eine Zählerübersicht für globale System-LAGs.

Anzeigen von Schnittstellenstatistiken

Die Seite **Interface Statistics (Schnittstellenstatistiken)** enthält Statistiken zu empfangenen und gesendeten Datenpaketen. Die Felder für empfangene und gesendete Datenpakete sind identisch. Klicken Sie zum Öffnen der Seite **Interface Statistics (Schnittstellenstatistiken)** in der Strukturansicht auf **Statistics/RMON→ Table Views→ Interface Statistics**.

Abbildung 8-3. Interface Statistics (Schnittstellenstatistiken)



Die Seite **Interface Statistics (Schnittstellenstatistiken)** enthält folgende Felder:

Interface – Gibt an, ob Port- oder LAG-Statistiken angezeigt werden sollen.

Refresh Rate – Zeitraum bis zur Aktualisierung der Schnittstellenstatistiken.

Receive Statistics (Empfangsstatistiken)

Total Bytes (Octets) – Anzahl der über die ausgewählte Schnittstelle empfangenen Oktette.

Unicast Packets – Anzahl der über die ausgewählte Schnittstelle empfangenen Unicastpakete.

Multicast Packets – Anzahl der über die ausgewählte Schnittstelle empfangenen Multicastpakete.

Broadcast Packets – Anzahl der über die ausgewählte Schnittstelle empfangenen Broadcastpakete.

Transmit Statistics (Sendestatistiken)

Total Bytes (Octets) – Anzahl der über die ausgewählte Schnittstelle gesendeten Oktette.

Unicast Packets – Anzahl der über die ausgewählte Schnittstelle gesendeten Unicastpakete.

Multicast Packets – Anzahl der über die ausgewählte Schnittstelle gesendeten Multicastpakete.

Broadcast Packets – Anzahl der über die ausgewählte Schnittstelle empfangenen Broadcastpakete.

Anzeigen von Schnittstellenstatistiken

1. Öffnen Sie die Seite **Interface Statistics (Schnittstellenstatistiken)**.
2. Wählen Sie im Feld **Interface** eine Schnittstelle aus.

Die **Statistiken für die ausgewählte Schnittstelle werden angezeigt.**

Zurücksetzen der Zähler für Schnittstellenstatistiken

1. Öffnen Sie die Seite **Interface Statistics (Schnittstellenstatistiken)**.
2. Klicken Sie auf **Reset All Counters** (Alle Zähler zurücksetzen).

Die Zähler für die Schnittstellenstatistiken werden zurückgesetzt.

Anzeigen von Schnittstellenstatistiken mit Hilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für die Anzeige von Schnittstellenstatistiken.

Tabelle 8-1. CLI-Befehle für Schnittstellenstatistiken

CLI-Befehl	Beschreibung
show interfaces counters [**ethernet** *Schnittstelle* | **port-channel** *Port-Kanalnummer*]	Zeigt den über die physische Schnittstelle abgewickelten Datenverkehr an.

Im Folgenden ein Beispiel für die CLI-Befehle.

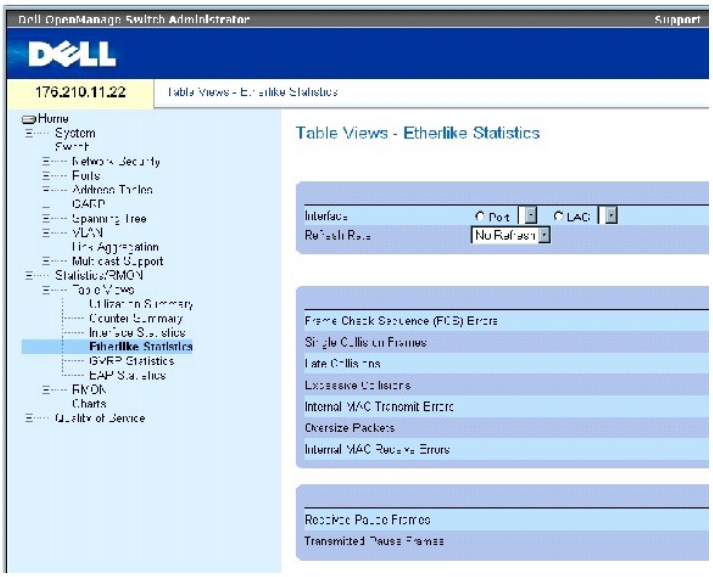
```
console> enable
```

```
console# show interfaces counters

Port InOctets InUcastPkts InMcastPkts InBcastPkts

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

1/e1 0 0 0 0

1/e2 0 0 0 0

1/e3 0 0 0 0

1/e4 0 0 0 0

1/e5 0 0 0 0

1/ e6 0 0 0 0

1/e7 0 0 0 0

1/e8 0 0 0 0

1/e9 0 0 0 0

1/e10 0 0 0 0
```

Anzeigen von Etherlike-Statistiken

Die Seite **Etherlike Statistics (Etherlike-Statistiken)** enthält Statistiken zu Schnittstellenfehlern. Klicken Sie zum Öffnen der Seite **Etherlike Statistics (Etherlike-Statistiken)** in der Strukturansicht auf **Statistics/RMON→ Table Views→ Etherlike Statistics**.

Abbildung 8-4. Etherlike Statistics (Etherlike-Statistiken)



Die Seite **Etherlike Statistics (Etherlike-Statistiken)** enthält folgende Felder:

Interface – Gibt an, ob Port- oder LAG-Statistiken angezeigt werden sollen.

Refresh Rate – Zeitraum bis zur Aktualisierung der Schnittstellenstatistiken.

Frame Check Sequence (FCS) Errors – Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen FCS-Fehler.

Single Collision Frames – Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen einfachen Frame-Kollisionsfehler.

Late Collisions – Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen verspäteten Kollisionen.

Oversize Packets – Anzahl der über die ausgewählte Schnittstelle empfangenen überlangen Datenpakete.

Internal MAC Transmit Errors – Anzahl interner MAC-Übertragungsfehler an der ausgewählten Schnittstelle.

Received Pause Frames – Anzahl der beim Empfang über die ausgewählte Schnittstelle aufgetretenen Pause-Fehler.

Transmitted Pause Frames – Anzahl der beim Senden über die ausgewählte Schnittstelle aufgetretenen Pause-Fehler.

Anzeigen von Etherlike-Statistiken für eine Schnittstelle

1. Öffnen Sie die Seite **Etherlike Statistics (Etherlike-Statistiken)**.
2. Wählen Sie im Feld **Interface** eine Schnittstelle aus.

Zurücksetzen der Etherlike-Statistiken

1. Öffnen Sie die Seite **Etherlike Statistics (Etherlike-Statistiken)**.
2. Klicken Sie auf **Reset All Counters** (Alle Zähler zurücksetzen).

Die Zähler für Etherlike Statistics (Etherlike-Statistiken) werden zurückgesetzt.

Anzeigen von Etherlike-Statistiken mit Hilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für die Anzeige von Etherlike-Statistiken.

Tabelle 8-2. CLI-Befehle für Etherlike-Statistiken

CLI-Befehl	Beschreibung
show interfaces counters [**ethernet** *Schnittstelle* | **port-channel** Port-Kanalnummer]	Zeigt den über die physische Schnittstelle abgewickelten Datenverkehr an.

Im Folgenden ein Beispiel für die CLI-Befehle.

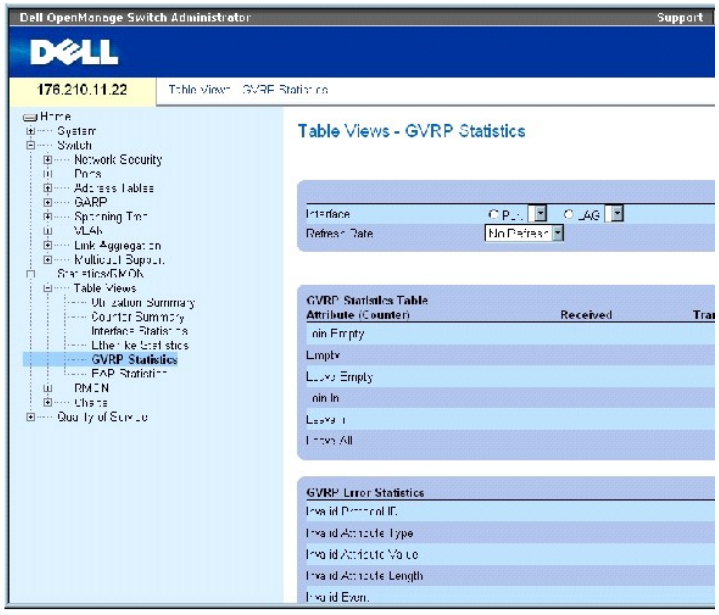
```
Console# show interfaces counters ethernet 1/1

Port    IN Octets   InUcastPkts  InMcastPkts  InBcastPkts
----    ---------   -----------  -----------  -----------
1/e1    183892      1289         987          8

Port    OUT Octets  OutUcastPkts OutMcastPkts OutBcastPkts
----    ----------  ------------ ------------ ------------
1/e1    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 von GVRP-Statistiken

Die Seite **GVRP Statistics (GVRP-Statistiken)** enthält Gerätestatistiken für GVRP. Klicken Sie zum Öffnen der Seite in der Strukturansicht auf **Statistics/RMON→ Table Views→ GVRP Statistics**.

Abbildung 8-5. GVRP Statistics (GVRP-Statistiken)



Die Seite **GVRP Statistics (GVRP-Statistiken)** enthält folgende Felder:

Interface – Gibt an, ob Port- oder LAG-Statistiken angezeigt werden sollen.

Refresh Rate – Zeitraum bis zur Aktualisierung der Schnittstellenstatistiken.

Join Empty – Gerätespezifische GVRP Join Empty-Statistik.

Leave Empty – Gerätespezifische GVRP Leave Empty-Statistik.

Empty – Gibt die Anzahl der leeren GVRP-Statistiken an.

Join In – Gerätespezifische GVRP Join In-Statistik.

Leave In – Gerätespezifische GVRP Leave In-Statistik.

Leave All – Gerätespezifische GVRP Leave All-Statistik.

Invalid Protocol ID – GVRP-Gerätestatistik zu ungültigen Protokoll-IDs.

Invalid Attribute Type – GVRP-Gerätestatistik zu ungültigen Attribut-IDs.

Invalid Attribute Value – GVRP-Gerätestatistik zu ungültigen Attributwerten.

Invalid Attribute Length – GVRP-Gerätestatistik zu ungültigen Attributlängen.

Invalid Event – GVRP-Gerätestatistik zu ungültigen Ereignissen.

Anzeigen von GVRP-Statistiken für einen Port

1. Öffnen Sie die Seite **GVRP Statistics (GVRP-Statistiken)**.
2. Wählen Sie im Feld **Interface** eine Schnittstelle aus.

Die GVRP-Statistiken für die ausgewählte Schnittstelle werden angezeigt.

Zurücksetzen der GVRP-Statistiken

1. Öffnen Sie die Seite **GVRP Statistics (GVRP-Statistiken)**.
2. Klicken Sie auf **Reset All Counters** (Alle Zähler zurücksetzen).

Die Zähler für die GVRP-Statistiken werden zurückgesetzt.

Anzeigen von GVRP-Statistiken mit Hilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für die Anzeige von GVRP-Statistiken.

Tabelle 8-3. CLI-Befehle für GVRP-Statistiken

CLI-Befehl	Beschreibung
show gvrp statistics [**ethernet** *Schnittstelle* | **port-channel** *Port- Kanalnummer*]	Zeigt GVRP-Statistiken an.
show gvrp error- statistics [**ethernet** *Schnittstelle* | **port- channel** *Port-Kanalnummer*]	Zeigt GVRP-Fehlerstatistiken an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console# show gvrp statistics

GVRP statistics:

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

Legend:

rJE: Join Empty Received

rJIn : Join In Received

rEmp : Empty Received

rLIn : Leave In Received

rLE : Leave Empty Received

rLA : Leave All Received

sJE : Join Empty Sent

sJIn : Join In Sent

sEmp : Empty Sent

sLIn : Leave In Sent

sLE : Leave Empty Sent

sLA : Leave All Sent
```

```
Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE
sLA

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

1/e1 0 0 0 0 0 0 0 0 0 0 0 0
```

```
1/e2 0 0 0 0 0 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0 0 0 0 0 00 0
```

```
Console# show gvrp error-statistics

GVRP error statistics:

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

Legend:

INVPROT : Invalid Protocol Id

INVPLEN : Invalid PDU Length

INVATYP : Invalid Attribute Type

INVALEN : Invalid Attribute Length

INVAVAL : Invalid Attribute Value

INVEVENT : Invalid Event

Port INVPROT INVATYP INVAVAL INVPLEN INVALEN INVEVENT

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

1/e1 0 0 0 0 0 0 0

1/e2 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0

1/e4 0 0 0 0 0 0 0
```

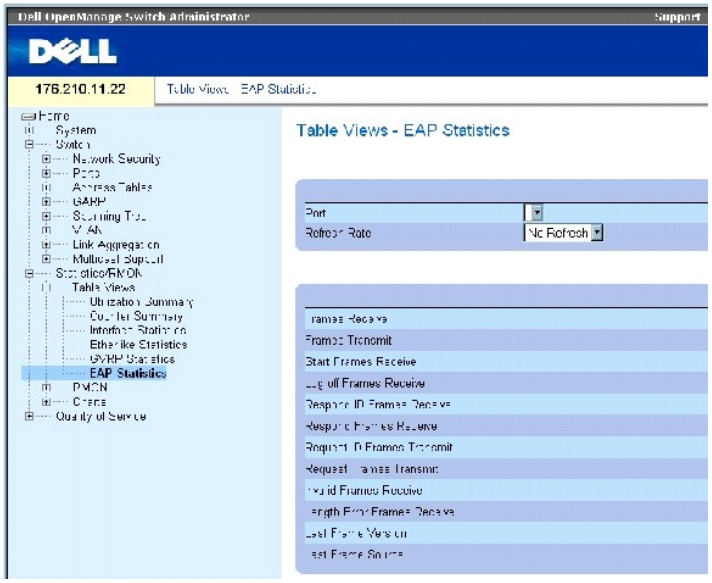
```
sLE : Leave Empty Sent

sLA : Leave All Sent
```

```
Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE
sLA


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


1/e1 0 0 0 0 0 0 0 0 0 0 0 0


1/e2 0 0 0 0 0 0 0 0 0 0 0 0


1/e3 0 0 0 0 0 0 0 0 0 0 0 0


1/e4 0 0 0 0 0 0 0 0 0 0 0 0


1/e5 0 0 0 0 0 0 0 0 0 0 0 0


1/e6 0 0 0 0 0 0 0 0 0 0 0 0


1/e7 0 0 0 0 0 0 0 0 0 0 0 0


1/e8 0 0 0 0 0 0 0 0 0 0 0 0
```

Anzeigen von EAP-Statistiken

Die Seite **EAP Statistics (EAP-Statistiken)** enthält Informationen zu den EAP-Paketen, die an einem bestimmten Port eingegangen sind. Weitere Informationen zu EAP finden Sie unter **Konfigurieren der portbasierten Authentifizierung**. Klicken Sie zum Öffnen der Seite **EAP Statistics (EAP-Statistiken)** in der Strukturansicht auf Statistics/RMON→ Table Views→ EAP Statistics.

Abbildung 8-6. EAP Statistics (EAP-Statistiken)



Die Seite **EAP Statistics (EAP-Statistiken)** enthält folgende Felder:

Port – Gibt an, von welchem Port Statistikdaten abgerufen werden.

Refresh Rate – Zeitraum bis zur Aktualisierung der Schnittstellenstatistiken.

Frames Receive – Gibt die Anzahl der portseitig empfangenen gültigen EAPOL-Frames an.

Frames Transmit – Gibt die Anzahl der über den Port übertragenen EAPOL-Frames an.

Start Frames Receive – Gibt die Anzahl der portseitig empfangenen EAPOL-Start-Frames an.

Log off Frames Receive – Gibt die Anzahl der portseitig empfangenen EAPOL-Abmeldeframes an.

Respond ID Frames Receive – Gibt die Anzahl der portseitig empfangenen EAP Resp/Id-Frames an.

Respond ID Frames Receive – Gibt die Anzahl der portseitig empfangenen gültigen EAP-Antwortframes an.

Request ID Frames Transmit – Gibt die Anzahl der über den Port übertragenen EAP Req/Id-Frames an.

Request Frames Transmit – Gibt die Anzahl der über den Port übertragenen EAP-Anforderungsframes an.

Invalid Frames Receive – Gibt die Anzahl der an diesem Port empfangenen nicht erkannten EAPOL-Frames an.

Length Error Frames Receive – Gibt die Anzahl der an diesem Port empfangenen EAPOL-Frames mit einer ungültigen Paketkörperlänge an.

Last Frame Version – Gibt die Protokollversionsnummer für den zuletzt empfangenen EAPOL-Frame an.

Last Frame Source – Gibt die MAC-Quelladresse für den zuletzt empfangenen EAPOL-Frame an.

Anzeigen von EAP-Statistiken für einen Port

1. Öffnen Sie die Seite **EAP Statistics (EAP-Statistiken)**.
2. Wählen Sie im Feld **Interface** eine Schnittstelle aus.

Die schnittstellenbezogenen EAP-Statistiken werden angezeigt.

Zurücksetzen der EAP-Statistiken

1. Öffnen Sie die Seite **EAP Statistics (EAP-Statistiken)**.
2. Klicken Sie auf Reset All Counters (Alle Zähler zurücksetzen).

Die Zähler für die EAP-Statistiken werden zurückgesetzt.

Anzeigen von EAP-Statistiken mit Hilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für die Anzeige von EAP-Statistiken.

Tabelle 8-4. CLI-Befehle für EAP-Statistiken

CLI-Befehl	Beschreibung
show dot1x statistics	Zeigt 802.1X-Statistiken für die angegebene Schnittstelle an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console# show dot1x statistics ethernet 1/e1

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
```

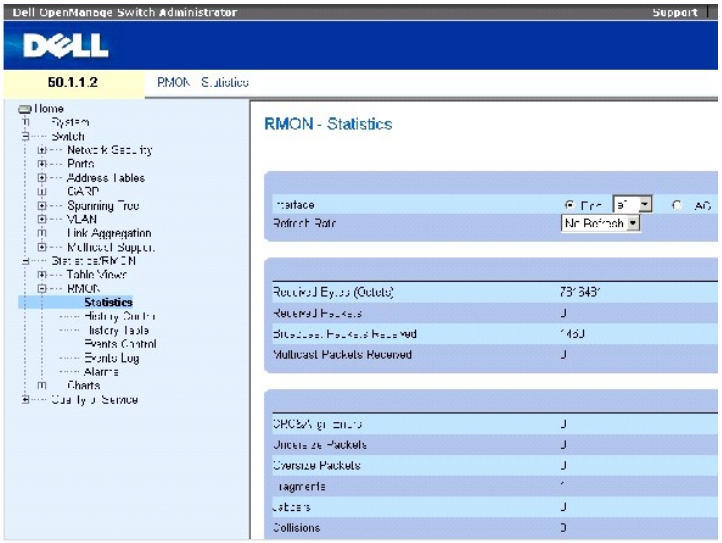
Anzeigen von RMON-Statistiken

Mit Hilfe von RMON (Remote Monitoring) können Netzwerkverwalter von einem Remote-Standort aus Informationen zum Netzwerkverkehr anzeigen lassen. Klicken Sie zum Öffnen der Seite **RMON** in der Strukturansicht auf **Statistics / RMON → RMON**.

Anzeigen der RMON-Statistikgruppe

Auf der Seite RMON Statistics (RMON-Statistiken) können Sie Informationen zur Gerätenutzung sowie zu Gerätefehlern abrufen. Klicken Sie zum Öffnen der Seite RMON Statistics (RMON-Statistiken) in der Strukturansicht auf **Statistics / RMON → RMON → Statistics**.

Abbildung 8-7. RMON Statistics (RMON-Statistiken)



Die Seite RMON Statistics (RMON-Statistiken) enthält folgende Felder:

Interface – Gibt den Port oder die LAG an, für die Statistikdaten angezeigt werden.

Refresh Rate – Zeitraum bis zur Aktualisierung der Statistiken.

Received Bytes (Octets) – Anzahl der über die ausgewählte Schnittstelle empfangene Bytes.

Received Packets – Anzahl der über die ausgewählte Schnittstelle empfangene Datenpakete.

Broadcast Packets Received – Anzahl der schnittstellenseitig empfangenen gültigen Broadcastpakete seit der letzten Aktualisierung des Gerätes. Diese Zahl beinhaltet keine Multicastpakete.

Multicast Packets Received – Anzahl der schnittstellenseitig empfangenen gültigen Multicastpakete seit der letzten Aktualisierung des Gerätes.

CRC & Align Errors – Anzahl der CRC- und Align-Fehler, die seit der letzten Aktualisierung des Gerätes an der Schnittstelle aufgetreten sind.

Undersize Packets – Anzahl der Pakete unter Normalgröße (weniger als 64 Oktette), die seit der letzten Aktualisierung des Gerätes an der Schnittstelle eingegangen sind.

Oversize Packets – Anzahl der Pakete über Normalgröße (mehr als 1518 Oktette), die seit der letzten Aktualisierung des Gerätes an der Schnittstelle eingegangen sind.

Fragments – Anzahl der Fragmente (Pakete mit weniger als 64 Oktetten, ohne Synchronisierbits, aber einschließlich FCS-Oktetten), die seit der letzten Aktualisierung des Gerätes an der Schnittstelle eingegangen sind.

Jabbers – Anzahl der Pakete mit mehr als 1518 Oktetten, die seit der letzten Aktualisierung des Gerätes an der Schnittstelle eingegangen sind.

Collisions – Anzahl der Kollisionen, die seit der letzten Aktualisierung des Gerätes an der Schnittstelle registriert wurden.

Frames of *xx* Bytes – Anzahl der *xx*-Byte-Frames, die seit der letzten Aktualisierung des Gerätes an der Schnittstelle eingegangen sind.

Anzeigen von Schnittstellenstatistiken

1. Öffnen Sie die Seite RMON Statistics (RMON-Statistiken).
2. Wählen Sie den Schnittstellentyp und eine Nummer im Feld **Interface** aus.

Die Schnittstellenstatistik wird angezeigt.

Anzeigen von RMON-Statistiken mit Hilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für die Anzeige von RMON-Statistiken.

Tabelle 8-5. CLI-Befehle für RMON-Statistiken

CLI-Befehl	Beschreibung
show rmon statistics {**ethernet** *Schnittstelle* | **port-channel** *Port- Kanalnummer*}	Zeigt RMON-Ethernet-Statistiken an.

Im Folgenden ein Beispiel für die CLI-Befehle:

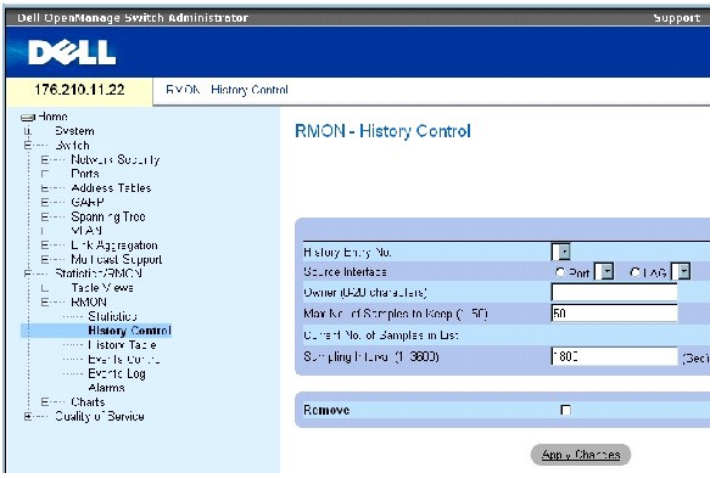
```
console# show rmon statistics ethernet 1/e1

Port 1/e1

Dropped: 8

Octets: 878128 Packets: 978

Broadcast: 7 Multicast: 1

CRC Align Errors: 0 Collisions: 0

Undersize Pkts: 0 Oversize Pkts: 0
```

```
Fragments: 0 Jabbers: 0


64 Octets: 98 65 to 127 Octets: 0


128 to 255 Octets: 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 (RMON-Verlaufssteuerung)** enthält Information zu Stichprobendaten, die an den Ports erfasst wurden. Diese Stichproben können beispielsweise Schnittstellendefinitionen oder Abrufzeiträume umfassen. Klicken Sie zum Öffnen der Seite **RMON History Control (RMON-Verlaufssteuerung)** in der Strukturansicht auf **Statistics / RMON → RMON → History Control**.

Abbildung 8-8. RMON History Control (RMON-Verlaufssteuerung)



Die Seite RMON History Control (RMON-Verlaufssteuerung) enthält folgende Felder:

History Entry No. – Eintragsnummer für die Seite **History Control** (Verlaufssteuerung).

Source Interface – Die Quelle, von der die Verlaufsstichproben erfasst wurden: Port oder LAG.

Owner (0-20 characters) – RMON-Station bzw. Benutzer, die/der die RMON-Informationen angefordert hat.

Max No. of Samples to Keep (1-50) – Anzahl der zu speichernden Stichproben. Der Standardwert ist 50.

Current No. of Samples in List – Gibt die Anzahl der derzeit erfassten Stichproben an.

Sampling Interval (1-3600) –Gibt das Zeitintervall (in Sekunden) an, in dem Stichproben von den Ports erfasst werden. Die möglichen Werte liegen zwischen 1 und 3.600 Sekunden. Der Standardwert lautet 1.800 Sekunden (30 Minuten).

Remove – Bei Aktivierung dieser Option wird der Eintrag aus der **History Control Table** (Verlaufssteuerungstabelle) entfernt.

Hinzufügen eines Verlaufssteuerungseintrags

1. Öffnen Sie die Seite **RMON History Control (RMON-Verlaufssteuerung)**.
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add History Entry** (Verlaufseintrag hinzufügen) wird geöffnet.
3. Nehmen Sie im Dialogfeld die entsprechenden Einstellungen vor.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Eintrag wird in die **History Control Table** (Verlaufssteuerungstabelle) aufgenommen.

Ändern eines Eintrags in der Verlaufssteuerungstabelle

1. Öffnen Sie die Seite **RMON History Control (RMON-Verlaufssteuerung)**.
2. Wählen Sie einen Verlaufseintrag im Feld **History Entry No.** aus.
3. Nehmen Sie gegebenenfalls Änderungen in den Feldern vor.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Tabelleneintrag wird geändert und das Gerät aktualisiert.

Löschen eines Eintrags aus der Verlaufssteuerungstabelle

1. Öffnen Sie die Seite **RMON History Control (RMON-Verlaufssteuerung)**.
2. Wählen Sie einen Verlaufseintrag im Feld **History Entry No.** aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Tabelleneintrag wird gelöscht und das Gerät aktualisiert.

Anzeigen der RMON-Verlaufssteuerung mit Hilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für die Anzeige der RMON-Verlaufssteuerung.

Tabelle 8-6. CLI-Befehle für den RMON-Verlauf

CLI-Befehl	Beschreibung
rmon collection history Index [**owner** *Besitzername* | **buckets** *Bucket-Nummer*] [**interval** *Sekunden*]	Aktiviert und konfiguriert RMON für eine Schnittstelle.
show rmon collection history [**ethernet** *Schnittstelle* | **port- channel** *Port-Kanalnummer*]	Zeigt Statistiken zum RMON-Erfassungsverlauf an.

Im Folgenden ein Beispiel für die CLI-Befehle:

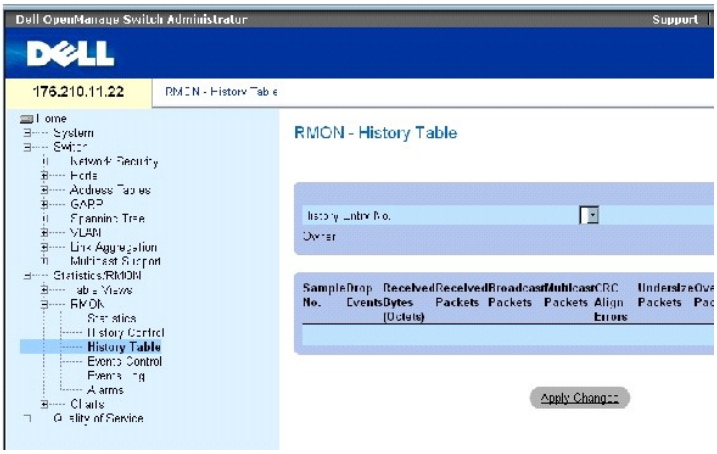
```
console(config)# interface ethernet 1/e8
```

```
console(config-if)# rmon collection history 1 interval
2400
```

Anzeigen der RMON-Verlaufstabelle

Die **RMON History Table (RMON-Verlaufstabelle)** (RMON-Verlaufstabelle) enthält schnittstellenspezifische, statistische Netzwerkstichproben. Jeder Tabelleneintrag repräsentiert alle während einer einzelnen Stichprobe erfassten Zählerwerte. Klicken Sie zum Öffnen von **RMON History Table (RMON-Verlaufstabelle)** in der Strukturansicht auf **Statistics / RMON→ RMON→ History Table**.

Abbildung 8-9. RMON History Table (RMON-Verlaufstabelle)



Die Seite **RMON History Table (RMON-Verlaufstabelle)** enthält folgende Felder:

ANMERKUNG: In der RMON-Verlaufstabelle werden nicht alle Felder angezeigt.

History Entry No. – Gibt die Eintragsnummer von der Seite **History Control** (Verlaufssteuerung) an.

Owner – Gibt die RMON-Station bzw. den Benutzer an, die/der die RMON-Informationen angefordert hat.

Sample No. – Gibt die Nummer einer bestimmten Stichprobe an, die die Informationen in der Tabelle darstellen.

Drop Events – Die Anzahl von Paketen, die aufgrund unzureichender Netzwerkressourcen während des Stichprobenintervalls abgewiesen wurden. Dieser Wert bezieht sich nicht unbedingt auf die genaue Anzahl abgewiesener Pakete, sondern auf die Häufigkeit, mit der abgewiesene Pakete identifiziert wurden.

Received Bytes (Octets)– 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 Broadcastpakete.

Multicast Packets – Die Anzahl der während des Stichprobenintervalls empfangenen gültigen Multicastpakete.

CRC Align Errors – Die Anzahl der während der Stichprobensitzung empfangenen Pakete mit einer Länge zwischen 64 und 1.518 Oktetten. Die Pakete weisen jedoch eine fehlerhafte Paketprüffolge (FCS) mit einer ganzzahligen oder einer nicht ganzzahligen Oktettanzahl auf.

Undersize Packets – Die Anzahl der während der Stichprobensitzung empfangenen Pakete mit einer Länge unter 64 Oktetten.

Oversize Packets – Die Anzahl der während der Stichprobensitzung empfangenen Pakete mit einer Länge über 1.518 Oktetten.

Fragments – Die Anzahl der empfangenen Pakete mit einer Länge unter 64 Oktetten, für die während der Stichprobensitzung eine Frame-Prüfsequenz generiert wurde.

Jabbers – Die Anzahl der empfangenen Pakete mit einer Länge über 1.518 Oktetten, für die während der Stichprobensitzung eine Frame-Prüfsequenz generiert wurde.

Collisions – Enthält einen Schätzwert zur Gesamtzahl der während der Stichprobensitzung aufgetretenen Paketkollisionen. Kollisionen treten auf, wenn von einem Zwischenverstärkerport festgestellt wird, dass mindestens zwei Stationen gleichzeitig Daten übertragen.

Utilization – Ein Schätzwert, der die Nutzung der primären Bitübertragungsschicht des Netzwerks an einer Schnittstelle während der Stichprobensitzung angibt. Der Wert wird in x-hundert Prozent angegeben.

Anzeigen von Statistiken für einen bestimmten Verlaufseintrag

1. Öffnen Sie die Seite **RMON History Table (RMON-Verlaufstabelle)**.
2. Wählen Sie einen Eintrag im Feld **History Entry No.** aus.

Die Eintragsstatistik wird in der RMON-Verlaufstabelle angezeigt.

Anzeigen der RMON-Verlaufssteuerung mit Hilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für die Anzeige des RMON-Verlaufs.

Tabelle 8-7. CLI-Befehle für die RMON-Verlaufssteuerung

CLI-Befehl	Beschreibung
show rmon history Index {throughput | errors | other} [period Sekunden]	Zeigt RMON-Ethernet-Verlaufsstatistiken an.

Das folgende Beispiel zeigt den Einsatz von CLI-Befehlen zur Anzeige der RMON-Ethernet-Statistiken für den Durchsatz an Index 1:

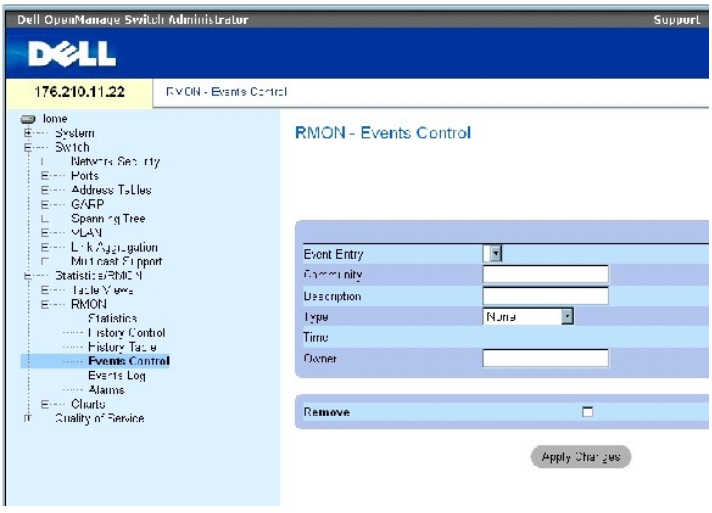
```
console> enable

console# show rmon history 1 throughput

Sample Set: 5 Owner: cli

Interface: 24 interval: 10

Requested samples: 50 Granted samples: 50

Maximum table size: 270
```

```
Time Octets Packets Broadcast Multicast %


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


09-Mar-2003 18:29:32 0 0 0 0 0


09-Mar-2003 18:29:42 0 0 0 0 0


09-Mar-2003 18:29:52 0 0 0 0 0


09-Mar-2003 18:30:02 0 0 0 0 0


09-Mar-2003 18:30:12 0 0 0 0 0


09-Mar-2003 18:30:22 0 0 0 0 0
```

Definieren von gerätespezifischen RMON-Ereignissen

Auf der Seite **RMON Events Control (RMON-Ereignissteuerung)** können Sie RMON-Ereignisse definieren. Klicken Sie zum Öffnen der Seite **RMON Events Control (RMON-Ereignissteuerung)** in der Strukturansicht auf **Statistics / RMON→ RMON→ Events Control**.

Abbildung 8-10. RMON Events Control (RMON-Ereignissteuerung)



Die Seite **RMON Events Control (RMON-Ereignissteuerung)** enthält folgende Felder:

Event Entry – Gibt das Ereignis an.

Community – Die Community, der das Ereignis angehört.

Description – Benutzerdefinierte Ereignisbeschreibung.

Type – Beschreibt den Ereignistyp. Mögliche Werte:

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 liegt kein Ereignis vor.

Time – Die Uhrzeit, zu der das Ereignis aufgetreten ist.

Owner – Das Gerät bzw. der Benutzer, von dem das Ereignis definiert wurde.

Remove – Bei Aktivierung dieser Option wird das Ereignis aus der RMON Events Table (RMON-Ereignistabelle) entfernt.

Hinzufügen eines RMON-Ereignisses

1. Öffnen Sie die Seite **RMON Events Control (RMON-Ereignissteuerung)**.
2. Klicken Sie auf **Add** (Hinzufügen).

   Die Seite **Add an Event Entry** (Ereigniseintrag hinzufügen) wird geöffnet.
3. Machen Sie die erforderlichen Angaben in dem Dialogfeld und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Eintrag wird in die **Event Table** (Ereignistabelle) aufgenommen und das Gerät aktualisiert.

Ändern eines RMON-Ereignisses

1. Öffnen Sie die Seite **RMON Events Control (RMON-Ereignissteuerung)**.
2. Wählen Sie einen Eintrag in der **Event Table** (Ereignistabelle).
3. Nehmen Sie die erforderlichen Änderungen im Dialogfeld vor und klicken Sie auf **Apply Changes** (Änderungen übernehmen).

   Der Eintrag in der **Event Table** wird geändert und das Gerät aktualisiert.

Löschen von RMON-Ereigniseinträgen

1. Öffnen Sie die Seite **RMON Events Control (RMON-Ereignissteuerung)**.
2. Klicken Sie auf **Show All** (Alle anzeigen).

   Die Seite **RMON Events Table** (RMON-Ereignistabelle) wird geöffnet.
3. Markieren Sie das Kontrollkästchen **Remove** (Entfernen) für alle zu löschenden Ereignisse und klicken auf **Apply Changes** (Änderungen übernehmen).

   Der Tabelleneintrag wird gelöscht und das Gerät aktualisiert.

ANMERKUNG: Ein einzelner Ereigniseintrag kann mit Hilfe des Kontrollkästchens **Remove** (Entfernen) von der Seite **RMON Events Control** (RMON-Ereignissteuerung) entfernt werden.

Definieren von Geräteereignissen mit Hilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für die Definition von Geräteereignissen.

Tabelle 8-8. CLI-Befehle für die Definition von Geräteereignissen

CLI-Befehl	Beschreibung
rmon event *Indextyp* [**community** *Text*] [**description** *Text*] [**ownerName**]	Konfiguriert RMON-Ereignisse.
show rmon events	Zeigt die RMON-Ereignistabelle an.

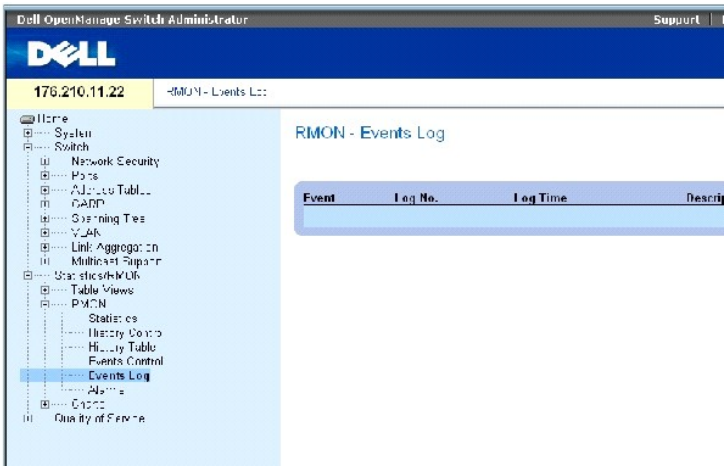
Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# rmon event 1 log

console(config)# exit

console# show rmon events

Index  Description  Type  Community  Owner  Last Time Sent
-----  -----------  ----  ---------  -------  ----------
1  Errors  Log  CLI  Jan 18 2002 23:58:17
2  High Broadcast  Log-Trap  router  Manager  Jan 18 2002 23:59:48
```

Anzeigen des RMON-Ereignisprotokolls

Die Seite **RMON Events Log (RMON-Ereignisprotokoll)** enthält eine Liste mit RMON-Ereignissen. Klicken Sie zum Öffnen der Seite **RMON Events Log (RMON-Ereignisprotokoll)** in der Strukturansicht auf **Statistics / RMON→ RMON→ Events Log**.

Abbildung 8-11. RMON Events Log (RMON-Ereignisprotokoll)



Die Seite **RMON Events Log (RMON-Ereignisprotokoll)** enthält folgende Felder:

Event – Die Nummer des Eintrags im RMON-Ereignisprotokoll.

Log No.– Die Protokollnummer.

Log Time – Die Uhrzeit, zu der der Protokolleintrag erfasst wurde.

Description – Eine Beschreibung des Protokolleintrags.

Definieren von Geräteereignissen mit Hilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für die Definition von Geräteereignissen.

Tabelle 8-9. CLI-Befehle für die Definition von Geräteereignissen

CLI-Befehl	Beschreibung
show rmon log [*Ereignis*]	Zeigt die RMON-Protokolltabelle an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# rmon event 1 log

Console> show rmon log

Maximum table size: 500

Event Description Time
```

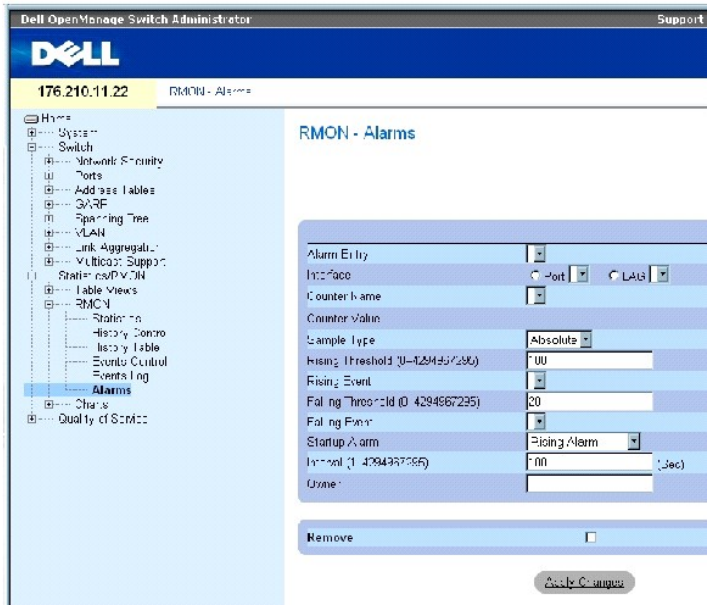
```
----- ---------- ----- --------------


1 Errors Jan 18 2002 23:58:17


2 High Broadcast Jan 18 2002 23:59:48
```

Definieren von RMON-Gerätealarmen

Auf der Seite **RMON Alarms (RMON-Alarme)** können Sie Netzwerkalarme einrichten. Ein Netzwerkalarm wird ausgegeben, wenn ein Netzwerkproblem, d. h. ein Ereignis, vorliegt. Beim Über- oder Unterschreiten eines Schwellenwertes wird ein Ereignis generiert. Weitere Informationen zu Ereignissen finden Sie unter Anzeigen des RMON-Ereignisprotokolls.

Klicken Sie zum Öffnen der Seite **RMON Alarms (RMON-Alarme)** in der Strukturansicht auf **Statistics/RMON→ RMON→ Alarms**.

Abbildung 8-12. RMON Alarms (RMON-Alarme)



Die Seite **RMON Alarms (RMON-Alarme)** enthält folgende Felder:

Alarm Entry – Weist auf einen spezifischen Alarm hin.

Interface – Gibt an, für welche Schnittstelle die RMON-Statistiken angezeigt werden.

Counter Name – Gibt die ausgewählte MIB-Variable an.

Counter Value – Der Wert der ausgewählten MIB-Variable.

Sample Type – Gibt das Stichprobenverfahren für die ausgewählte Variable an und vergleicht den Wert mit den Schwellenwerten. Die für dieses Feld möglichen Werte sind:

Delta – Subtrahiert den letzten Stichprobenwert vom aktuellen Wert. Die Differenz zwischen den Werten wird mit dem Schwellenwert verglichen.

Absolute – Vergleicht die Werte am Ende des Stichprobenintervalls direkt mit den Schwellenwerten.

Rising Threshold (0–4294967295) – Der obere Zählerwert, durch den der Alarm für die Überschreitung des oberen Schwellenwertes ausgelöst wird. Der obere Schwellenwert ist oben auf den Diagrammbalken dargestellt. Jeder überwachten Variablen ist eine eigene Farbe zugewiesen. Der Standardwert für dieses Feld beträgt 100 Sekunden.

Rising Event – Der Mechanismus für die Ausgabe der Alarme: Protokoll, Trap oder beides. Bei Auswahl eines Protokolls verfügen weder das Gerät noch das Verwaltungssystem über einen Speichermechanismus. Wird das Gerät jedoch nicht zurückgesetzt, verbleibt sein Eintrag in der gerätespezifischen Protokolltabelle. Bei Auswahl eines Traps wird ein SNMP-Trap generiert und über einen entsprechenden Trap-Mechanismus gemeldet. Der TRAP kann mit demselben Mechanismus gespeichert werden.

Falling Threshold (0–4294967295) – Der untere Zählerwert, durch den der Alarm für die Unterschreitung des unteren Schwellenwertes ausgelöst wird. Der untere Schwellenwert ist oben auf den Diagrammbalken grafisch dargestellt. Jeder überwachten Variablen ist eine eigene Farbe zugewiesen. Der Standardwert ist 20.

Startup Alarm – Der Auslöser, durch den die Alarmgenerierung aktiviert wird. Ein Anstieg wird wie folgt definiert: Das Überschreiten der Schwelle von einem niedrigeren zu einem höheren Schwellenwert.

Interval (1–4294967295) **(sec)** – Intervallzeit für den Alarm. Der Standardwert für dieses Feld beträgt 100 Sekunden.

Owner – Gerät oder Benutzer, von dem der Alarm definiert wurde.

Remove – Bei Aktivierung dieser Option wird ein RMON-Alarm entfernt.

Hinzufügen eines Eintrags in die Alarmtabelle

1. Öffnen Sie die Seite **RMON Alarms (RMON-Alarme)**.
2. Klicken Sie auf **Add** (Hinzufügen).

Die Seite **Add An Alarm Entry** (Alarmeintrag hinzufügen) wird geöffnet.

Abbildung 8-13. Seite Add an Alarm Entry Page (Alarmeintrag hinzufügen)

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

Der RMON-Alarm wird hinzugefügt und das Gerät aktualisiert.

Ändern eines Eintrags in der Alarmtabelle

1. Öffnen Sie die Seite **RMON Alarms (RMON-Alarme)**.
2. Wählen Sie einen Eintrag im Dropdown-Menü **Alarm Entry** (Alarmeintrag) aus.
3. Nehmen Sie die erforderlichen Änderungen in den Feldern vor.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag wird geändert und das Gerät aktualisiert.

Anzeigen der Alarmtabelle

1. Öffnen Sie die Seite **RMON Alarms (RMON-Alarme)**.
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die **Event Table** (Ereignistabelle) wird geöffnet.

Löschen eines Eintrags aus der Alarmtabelle

1. Öffnen Sie die Seite **RMON Alarms (RMON-Alarme)**.
2. Wählen Sie einen Eintrag im Dropdown-Menü **Alarm Entry** (Alarmeintrag) aus.
3. Markieren Sie das Kontrollkästchen **Remove** (Entfernen).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Eintrag wird gelöscht und das Gerät aktualisiert

Definieren von Gerätealarmen mit Hilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für die Definition von Gerätealarmen.

Tabelle 8-10. CLI-Befehle für Gerätealarme

CLI-Befehl	Beschreibung
rmon alarm *Index MIB_Objekt_ID Intervall oSchwelle uSchwelle oEreignis uEreignis* [**type** *Type*] [**startup** *Richtung*] [**owner** *Name*]	Konfiguriert RMON-Alarmbedingungen.
show rmon alarm-table	Zeigt eine Übersicht der Alarmtabelle an.
show rmon alarm	Zeigt die RMON-Alarmkonfiguration an.

Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1
360000 1000000 1000000 10 20
```

```
Console# show rmon alarm-table

Index OID Owner

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

1 1.3.6.1.2.1.2.2.1.10.1 CLI

2 1.3.6.1.2.1.2.2.1.10.1 Manager

3 1.3.6.1.2.1.2.2.1.10.9 CLI
```

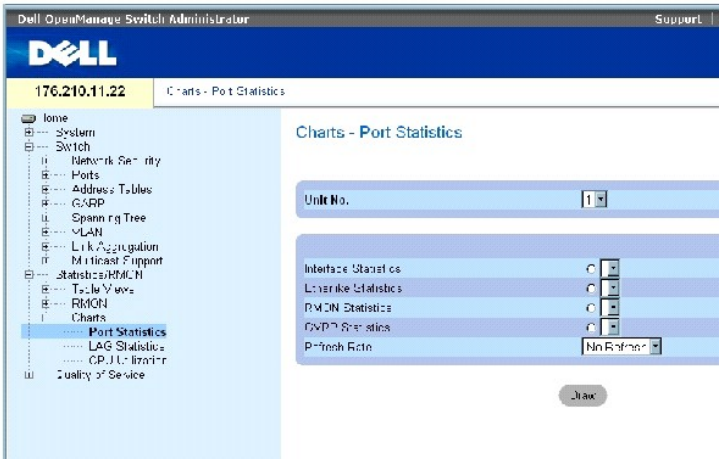
Anzeigen von Diagrammen

Die Seite **Chart** (Diagramm) enthält Links zur Anzeige von Statistiken in Diagrammform. Klicken Sie zum Öffnen der Seite in der Strukturansicht auf Statistics→ Charts.

Anzeigen von Port-Statistiken

Auf der Seite **Port Statistics (Port-Statistiken)** können Sie Statistiken zu Port-Elementen in Diagrammform abrufen. Klicken Sie zum Öffnen der Seite **Port Statistics (Port-Statistiken)** in der Strukturansicht auf **Statistics / RMON→ Charts→ Port Statistics**.

Abbildung 8-14. Port Statistics (Port-Statistiken)



Die Seite Port Statistics (Port-Statistiken) enthält folgende Felder:

Unit No. – Gibt die Stack-Einheit an, für die Statistikdaten angezeigt werden.

Interface Statistics – Vereinbart, welche Schnittstellenstatistiken angezeigt werden.

Etherlike Statistics – Vereinbart, welche Etherlike-Statistiken angezeigt werden.

RMON Statistics – Vereinbart, welche RMON-Statistiken angezeigt werden.

GVRP Statistics – Vereinbart, welche GVRP-Statistiken angezeigt werden.

Refresh Rate – Zeitraum bis zur Aktualisierung der Statistiken.

Anzeigen von Port-Statistiken

1. Öffnen Sie die Seite **Port Statistics (Port-Statistiken)**.
2. Wählen Sie den aufzurufenden Statistiktyp aus.
3. Wählen Sie im Dropdown-Menü **Refresh Rate** die gewünschte Aktualisierungsrate aus.
4. Klicken Sie auf **Draw** (Zeichnen).

Die Grafik für die ausgewählte Statistik wird angezeigt.

Anzeigen von Port-Statistiken mit Hilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für die Anzeige von Portstatistiken.

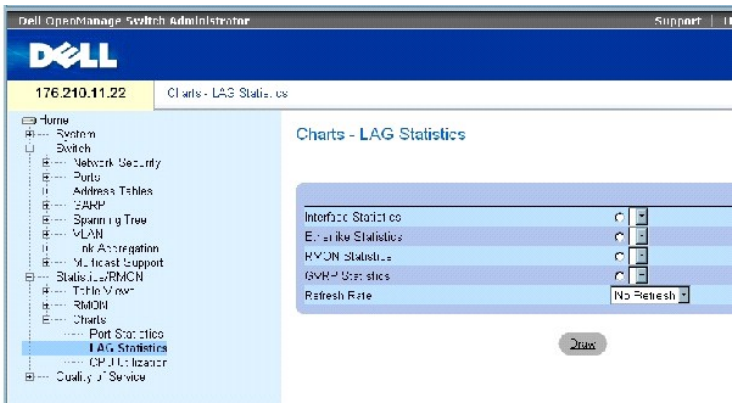
Tabelle 8-11. CLI-Befehle für Port-Statistiken

CLI-Befehl	Beschreibung
show interfaces counters [**ethernet** *Schnittstelle* | **port- channel** *Port-Kanalnummer*]	Zeigt den über die physische Schnittstelle abgewickelten Datenverkehr an.
show rmon statistics {**ethernet** *Schnittstelle* | **port-channel** *Port-Kanalnummer*}	Zeigt RMON-Ethernet-Statistiken an.
show gvrp statistics {**ethernet** *Schnittstelle* | **port-channel** *Port-Kanalnummer*}	Zeigt GVRP-Statistiken an.
show gvrp-error statistics {**ethernet** *Schnittstelle* | **port- channel** *Port-Kanalnummer*}	Zeigt GVRP-Fehlerstatistiken an.

Anzeigen von LAG-Statistiken

Auf der Seite **LAG Statistics (LAG-Statistiken)** können Sie LAG-Statistiken in Diagrammform abrufen. Klicken Sie zum Öffnen der Seite **LAG Statistics (LAG-Statistiken)** in der Strukturansicht auf **Statistics/RMON→ Charts→ LAG Statistics**.

Abbildung 8-15. LAG Statistics (LAG-Statistiken)



Die Seite LAG Statistics (LAG-Statistiken) enthält folgende Felder:

Interface Statistics – Vereinbart, welche Schnittstellenstatistiken angezeigt werden.

Etherlike Statistics – Vereinbart, welche Etherlike-Statistiken angezeigt werden.

RMON Statistics – Vereinbart, welche RMON-Statistiken angezeigt werden.

GVRP Statistics – Vereinbart, welche GVRP-Statistiken angezeigt werden.

Refresh Rate – Zeitraum bis zur Aktualisierung der Statistiken.

Anzeigen von LAG-Statistiken

1. Öffnen Sie die Seite **LAG Statistics (LAG-Statistiken)**.
2. Wählen Sie den aufzurufenden Statistiktyp aus.
3. Wählen Sie im Dropdown-Menü **Refresh Rate** die gewünschte Aktualisierungsrate aus.
4. Klicken Sie auf **Draw** (Zeichnen).

Die Grafik für die ausgewählte Statistik wird angezeigt.

Anzeigen von LAG-Statistiken mit Hilfe der CLI-Befehle

Die folgende Tabelle enthält die CLI-Befehle für die Anzeige von LAG-Statistiken.

Tabelle 8-12. CLI-Befehle für LAG-Statistiken

CLI-Befehl	Beschreibung
show interfaces counters [**ethernet** *Schnittstelle* | **port- channel** *Port-Kanalnummer*]	Zeigt den über die physische Schnittstelle abgewickelten Datenverkehr an.
show rmon statistics {**ethernet** *Schnittstelle* | **port-channel** *Port-Kanalnummer*}	Zeigt RMON-Ethernet-Statistiken an.
show gvrp statistics {**ethernet** *Schnittstelle* | **port-channel** *Port-Kanalnummer*}	Zeigt GVRP-Statistiken an.

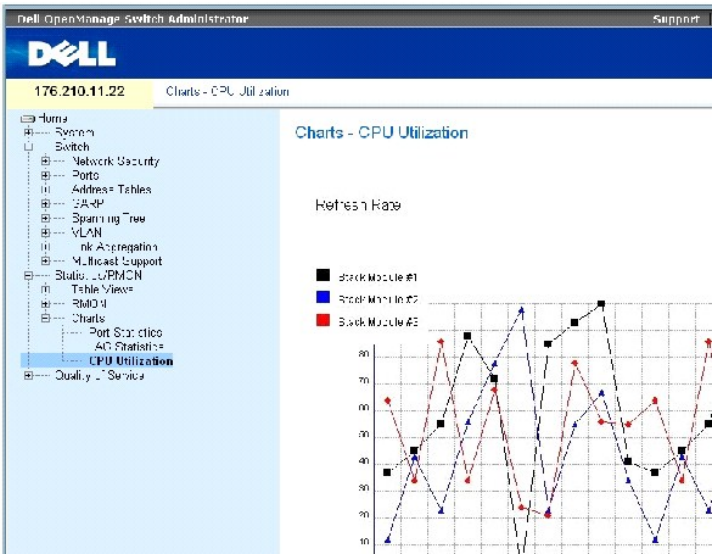
show gvrp-error statistics {**ethernet** *Schnittstelle* | **port- channel** *Port-Kanalnummer*}	Zeigt GVRP-Fehlerstatistiken an.

Anzeigen der CPU-Auslastung

Die Seite **CPU Utilization (CPU-Auslastung)** enthält Informationen zur CPU-Auslastung des Systems sowie dem prozentualen Anteil der CPU-Ressourcen, der von den einzelnen Stack-Komponenten belegt wird. Jeder Stack-Komponente ist in der Grafik eine bestimme Farbe zugewiesen.

Klicken Sie zum Öffnen der Seite **CPU Utilization (CPU-Auslastung)** in der Strukturansicht auf **Statistics / RMON → Charts → CPU Utilization**.

Abbildung 8-16. CPU Utilization (CPU-Auslastung)



Die Seite **CPU Utilization (CPU-Auslastung)** enthält folgende Informationen:

Refresh Rate – Zeitraum bis zur Aktualisierung der Statistiken.

Zurück zum Inhalt

Zurück zum Inhalt

Konfigurieren von Quality of Service (QoS)

Dell™ PowerConnect™ 34XX- Systeme Benutzerhandbuch

Dieser Abschnitt enthält Informationen zum Definieren und Konfigurieren von QoS-Parametern (Quality of Service). Klicken Sie zum Öffnen der Seite Quality of Service in der Strukturansicht auf Quality of Service.

Übersicht über Quality of Service (QoS)

Mittels Quality of Service (QoS) können innerhalb eines Netzwerks QoS- und Prioritätswarteschlangen implementiert werden.

Bei bestimmten Implementierungen mit Datenverkehr wie Voice, Video und Echtzeitdaten ist QoS erforderlich; dieser anspruchsvolle Datenverkehr kann einer Warteschlange mit hoher Priorität zugeordnet werden, während der übrige Verkehr in eine Warteschlange mit geringerer Priorität gelangt. Das Ergebnis ist ein optimierter Datenfluss für Netzwerkverkehr mit hohen Anforderungen.

QoS wird durch folgende Kriterien definiert:

- Klassifizierung – Legt fest, welchen Paketfeldern spezifische Werte zugewiesen werden. Alle mit den benutzerdefinierten Spezifikationen übereinstimmenden Pakete werden unter einer Kategorie zusammengefasst.
- Aktion – Definiert die Verwaltung des Datenverkehrs, wobei die Pakete auf Grundlage von Paketinformationen und Paketfeldwerten wie VLAN-Prioritätskennung (VPT) und DSCP (DiffServ Code Point) weitergeleitet werden.

VPT-Klassifizierungsinformationen

VLAN-Prioritätskennungen werden zum Klassifizieren von Paketen verwendet, indem Pakete einer der Egress-Warteschlangen zugeordnet werden. VLAN-Prioritätskennungen zum Zuweisen von Warteschlangen sind vom Benutzer definierbar. In der folgenden Tabelle sind die VPTs gegenüber den Warteschlangen-Standardeinstellungen aufgeführt:

Tabelle 9-1. Standardwerte der CoS to Queue Mapping Table

CoS-Wert	Werte der Weiterleitungswarteschlangen
0	q1 (Niedrigste Priorität)
1	q1 (Niedrigste Priorität)
2	q1 (Niedrigste Priorität)
3	q1 (Niedrigste Priorität)
4	q2
5	q2
6	q3
7	q3

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

Ankommenden Paketen ohne Kennung wird ein Standard-VPT-Wert zugewiesen, der nach Port festgelegt ist. Die zugewiesene VPT wird zum Zuordnen des Pakets in der Egress-Warteschlange verwendet.

DSCP-Werte können Prioritätswarteschlangen zugewiesen werden. Die folgende Tabelle enthält die Standard-DSCP-Zuordnung zu Egress-Warteschlangenwerten:

Tabelle 9-2. Standardwerte der DSCP to Queue Mapping Table

DSCP-Wert	Werte der Weiterleitungswarteschlangen
0-15	q1 (Niedrigste Priorität)
16-39	q2
40-63	q3

Die DSCP-Zuweisung wird auf Systembasis aktiviert.

CoS-Dienste

Nachdem Pakete einer bestimmten Egress-Warteschlange zugewiesen wurden, können den Warteschlangen CoS-Dienste zugewiesen werden. Egress-Warteschlangen werden gemäß einer der folgenden Methoden mit einem Zeitplanschema konfiguriert:

- Strict Priority — Stellt sicher, dass zeitkritische Anwendungsdaten immer beschleunigt weitergeleitet werden. Bei Strict Priority (SP) wird missions- und zeitkritischem Datenverkehr vor weniger zeitkritischen Anwendungen Priorität eingeräumt.
  SP ermöglicht beispielsweise eine Priorisierung des Voice-over-IP-Datenverkehrs, um sicherzustellen, dass IP-Daten vor FTP oder E-Mail (SMTP) weitergeleitet werden.
- Weighted Round Robin — Stellt sicher, dass einzelne Anwendungen nicht die Weiterleitungskapazität des Gerätes dominieren können. Bei Weighted Round Robin (WRR) werden ganze Warteschlangen in einer zyklischen Reihenfolge weitergeleitet. Alle Warteschlangen mit Ausnahme von SP-Warteschlangen können am WRR-Verfahren teilnehmen.
  SP-Warteschlangen werden vor WRR-Warteschlangen verarbeitet. Bei minimalem Datenfluss und wenn die SP-Warteschlangen nicht die gesamte Bandbreite eines Ports belegen, können die WRR-Warteschlangen die verfügbare Bandbreite gemeinsam mit den SP-Warteschlangen nutzen. Auf diese Weise ist sichergestellt, dass die verbleibende Bandbreite gemäß dem vorgesehenenGewichtungsverhältnis verteilt wird. Bei Auswahl von WRR werden den Warteschlangen folgende Gewichtungen zugewiesen: 1, 2, 4, 8.

Definieren globaler QoS-Parameter

Die Seite **QoS Parameters** enthält Links zu Seiten, auf denen globale Quality of Service-Parameter vereinbart werden können.

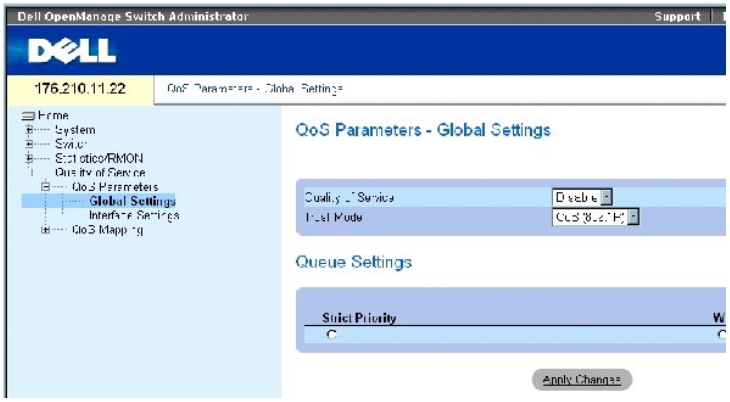
Konfigurieren globaler QoS-Einstellungen

Die Seite **Global Settings (Globale Einstellungen)** enthält ein Feld für das Aktivieren bzw. Deaktivieren von QoS. Über ein weiteres Feld dieser Seite können Sie den Trust-Modus auswählen. Der Trust-Modus beruht auf vordefinierten Feldern im Paket zum Bestimmen der Egress-Warteschlange.

Darüber hinaus stehen auf der Seite **Global Settings (Globale Einstellungen)** folgende Einstellungen für Warteschlangen zur Verfügung: Strict Priority (SP) oder Weighted Round Robin (WRR).

Klicken Sie zum Öffnen der Seite **Global Settings (Globale Einstellungen)** in der Strukturansicht auf Quality of Service→ QoS Parameters → Global Settings.

Abbildung 9-1. Global Settings (Globale Einstellungen)



Die Seite **Global Settings (Globale Einstellungen)** enthält folgende Bereiche:

- QoS Settings (QoS-Einstellungen)
- Queue Settings (Warteschlangeneinstellungen)

QoS Settings (QoS-Einstellungen)

Quality of Service – Aktiviert bzw. Deaktiviert die Verwaltung des Netzwerkdatenverkehrs mit Quality of Service.

Trust Mode – Legt fest, anhand welcher Paketfelder geräteseitig eingehende Pakete klassifiziert werden. Wenn keine Regeln definiert wurden, wird Datenverkehr mit dem vordefinierten CoS- oder DSCP-Paketfeld entsprechend dem ausgewählten Trust-Modus zugewiesen. Datenverkehr ohne vordefiniertes Paketfeld wird der Best-Effort-Warteschlange (q2) zugewiesen. Die möglichen Werte für Trust Mode lauten:

CoS (802.1p) — Die zugewiesene Egress-Warteschlange wird über die IEEE802.1p VLAN-Prioritätskennung (VPT) oder die einem Port zugewiesene Standard-VPT ermittelt. Die Standardeinstellung des Gerätes ist IEEE802.1p.

DSCP – Die zugewiesene Egress-Warteschlange wird über das DSCP-Feld ermittelt.

ANMERKUNG: Die Trust-Einstellungen der Schnittstellen überschreiben die globale Trust-Einstellung.

Queue Settings (Warteschlangeneinstellungen)

Strict Priority – Zeigt an, dass die Systemwarteschlangen bei Auswahl wie SP-Warteschlangen gehandhabt werden.

WRR – Zeigt an, dass die Systemwarteschlangen bei Auswahl wie WRR-Warteschlangen gehandhabt werden.

Aktivieren von Quality of Service:

1. Öffnen Sie die Seite **Global Settings (Globale Einstellungen)** .
2. Wählen Sie im Feld **Quality of Service** die Option **Enable** (Aktivieren) aus.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Class of Service wird für das Gerät aktiviert.

So konfigurieren Sie den Trust-Modus:

1. Öffnen Sie die Seite **Global Settings (Globale Einstellungen)** .
2. Definieren Sie das Feld **Trust Mode**.
3. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der Trust-Modus wird für das Gerät aktiviert.

Aktivieren des Trust-Modus' mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **Global Settings (Globale Einstellungen)** äquivalenten CLI-Befehle zur Feldkonfiguration zusammengefasst.

Tabelle 9-3. CLI-Befehle für die QoS-Einstellungen

CLI-Befehl	Beschreibung
qos trust [**cos** | **dscp**]	Konfiguriert den Trust-Modus des Systems.
no qos trust	Kehrt in den Nicht-Trust-Status zurück.

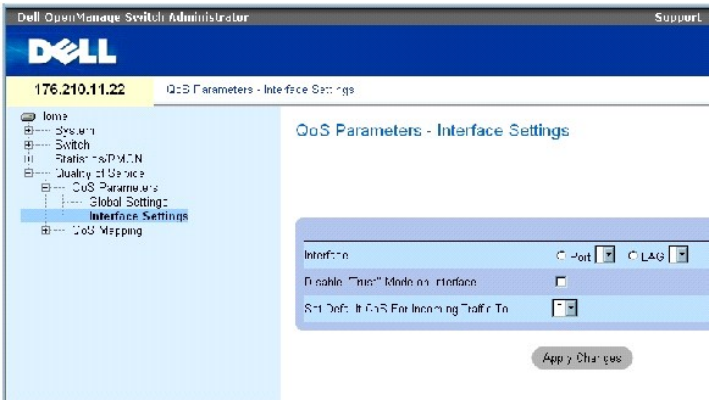
Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# qos trust
dscp
```

Definieren von QoS-Schnittstelleneinstellungen

Die Seite **Interface Settings (Schnittstelleneinstellungen)** enthält Felder, über die man den Trust-Modus deaktivieren und den Standard-CoS-Wert für eingehende Pakete ohne Kennung vereinbaren kann. Klicken Sie zum Öffnen der Seite **Interface Settings (Schnittstelleneinstellungen)** in der Strukturansicht auf Quality of Service→ QoS Parameters → Interface Settings.

Abbildung 9-2. Interface Settings (Schnittstelleneinstellungen)



Die Seite **Interface Settings (Schnittstelleneinstellungen)** enthält folgende Felder:

Interface – Der zu konfigurierende Port bzw. die LAG.

Disable Trust Mode on Interface – Deaktiviert den Trust-Modus für die angegebene Schnittstelle. Diese Einstellung setzt den global für das Gerät konfigurierten Trust-Modus außer Kraft.

Set Default CoS For Incoming Traffic To – Setzt den Wert der CoS-Standardkennung für Pakete ohne Kennung. Die Werte der CoS-Kennung gehen von 0 bis 7. Der Standardwert ist 0.

Zuweisen von QoS-Einstellungen für eine Schnittstelle:

1. Öffnen Sie die Seite **Interface Settings (Schnittstelleneinstellungen)**.
2. Wählen Sie im Feld **Interface** eine Schnittstelle aus.
3. Definieren Sie die Felder.
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Die CoS-Einstellungen werden der Schnittstelle zugewiesen.

Anzeigen der QoS/CoS-Einstellungen:

1. Öffnen Sie die Seite **Interface Settings (Schnittstelleneinstellungen)**.
2. Klicken Sie auf **Show All** (Alle anzeigen).

Die Interface Table (Schnittstellentabelle) wird angezeigt.

Zuweisen von QoS-Schnittstellen mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **Interface Settings (Schnittstelleneinstellungen)** äquivalenten CLI-Befehle zur Feldkonfiguration zusammengefasst.

Tabelle 9-4. CLI-Befehle für die QoS-Schnittstelle

CLI-Befehl	Beschreibung
qos trust	Aktiviert den Trust-Modus.
no qos trust	Deaktiviert den Trust-Status für die einzelnen Anschlüsse.

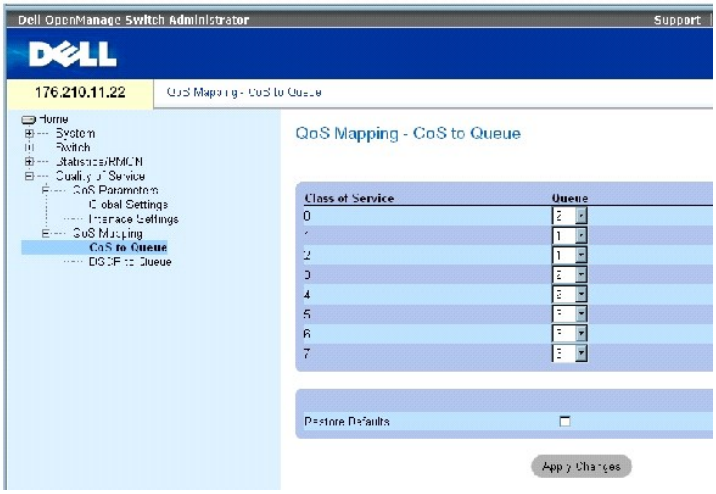
Im Folgenden ein Beispiel für die CLI-Befehle:

```
console(config)# interface
ethernet 1/e15


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

Zuweisen von CoS-Werten zu Warteschlangen

Die Seite **CoS to Queue (CoS-Warteschlangen-Zuordnung)** enthält Felder zum Klassifizieren von CoS-Einstellungen für Datenverkehrswarteschlangen. Klicken Sie zum Öffnen der Seite **CoS to Queue (CoS-Warteschlangen-Zuordnung)** in der Strukturansicht auf Quality of Service→ **QoS Mapping**→ CoS to Queue .

Abbildung 9-3. CoS to Queue (CoS-Warteschlangen-Zuordnung)



Die Seite **CoS to Queue (CoS-Warteschlangen-Zuordnung)** enthält folgende Felder:

Class of Service – Gibt die Werte der CoS-Prioritätskennung an, wobei 0 der niedrigsten und 7 der höchsten Priorität entspricht.

Queue – Die Warteschlange, der die CoS-Priorität zugewiesen wird. Vier Prioritätswarteschlangen werden unterstützt.

Restore Defaults – Stellt für die Zuweisung von CoS-Werten zu Egress-Warteschlangen die Standardwerte des Herstellers wieder her.

Zuweisen eines CoS-Wertes zu einer Warteschlange

1. Öffnen Sie die Seite **CoS to Queue (CoS-Warteschlangen-Zuordnung)**.
2. Wählen Sie einen CoS-Eintrag aus.
3. Definieren Sie die Warteschlangennummer im Feld **Queue** (Warteschlange).
4. **Klicken Sie auf** Apply Changes (Änderungen übernehmen).

Der CoS-Wert wird der gewünschten Warteschlange zugewiesen, und das Gerät wird aktualisiert.

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

In der folgenden Tabelle werden die der Seite **CoS to Queue (CoS-Warteschlangen-Zuordnung)** äquivalenten CLI-Befehle zur Feldkonfiguration zusammengefasst.

Tabelle 9-5. CLI-Befehle für die CoS to Queue-Einstellungen

CLI-Befehl	Beschreibung
wrr-queue cos-map Warteschlangen-ID cos0.cos7	Weist den Egress-Warteschlangen festgelegte CoS-Werte zu.

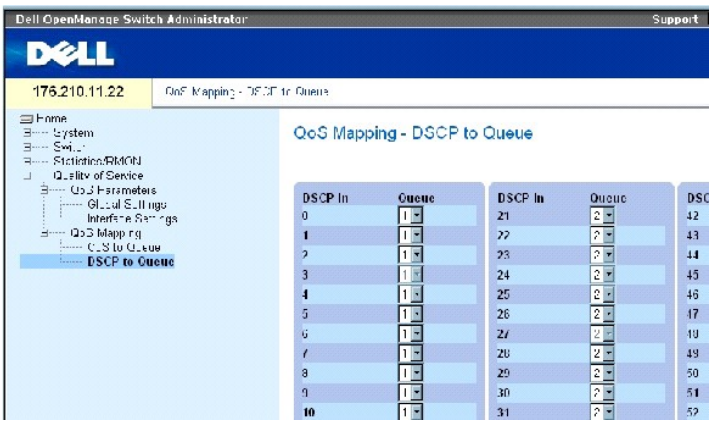
Im Folgenden ein Beispiel für die CLI-Befehle:

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

Zuweisen von DSCP-Werten zu Warteschlangen

Die Seite **DSCP to Queue (DSCP-Warteschlangen-Zuordnung)** enthält Felder zum Zuweisen von Egress-Warteschlangen zu bestimmten DSCP-Feldern. Klicken Sie zum Öffnen der Seite **DSCP to Queue (DSCP-Warteschlangen-Zuordnung)** in der Strukturansicht auf Quality of Service→ **QoS** Mapping→ DSCP to Queue .

Abbildung 9-4. DSCP to Queue (DSCP-Warteschlangen-Zuordnung)



Die Seite **DSCP to Queue (DSCP-Warteschlangen-Zuordnung)** enthält folgende Felder:

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

Queue – Die Warteschlange, der Pakete mit dem spezifischen DSCP-Wert zugewiesen werden. Die Werte gehen von 1 bis 4, wobei 1 der niedrigste und 4 der höchste Wert ist.

Zuweisen eines DSCP-Wertes und einer Prioritätswarteschlange

1. Öffnen Sie die Seite **DSCP to Queue (DSCP-Warteschlangen-Zuordnung)**.
2. Wählen Sie einen Wert in der Spalte **DSCP In** .
3. Definieren Sie das Feld **Queue** (Warteschlange).
4. Klicken Sie auf **Apply Changes** (Änderungen übernehmen).

Der DSCP-Wert wird überschrieben, und dem Wert wird eine Egress-Warteschlange zugewiesen.

Zuweisen von DSCP-Werten mit Hilfe der CLI-Befehle

In der folgenden Tabelle werden die der Seite **DSCP to Queue (DSCP-Warteschlangen-Zuordnung)** äquivalenten CLI-Befehle zur Feldkonfiguration zusammengefasst.

Tabelle 9-6. CLI-Befehle für DSCP to Queue-Einstellungen

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

Im Folgenden ein Beispiel für die CLI-Befehle:

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

Zurück zum Inhalt

Zurück zum Inhalt

Dell™ PowerConnect™ 34XX- Systeme Benutzerhandbuch

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, die Ihnen die Arbeit mit dem Computer erleichtern.

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

VORSICHT: VORSICHT zeigt eine potenziell gefährliche Situation an, die zu Sachschäden, Verletzungen oder zum Tod führen könnte.

März 2005

Zurück zum Inhalt

Zurück zum Inhalt

Wechselwirkungen der Gerätefunktionen

Dell™ PowerConnect™ 34XX- Systeme Benutzerhandbuch

Die nachfolgende Tabelle enthält Informationen zu den Wechselwirkungen der verschiedenen Gerätefunktionen (Feature Interaction).

Funktion	Funktionshinweise
802.1x Unauthenticated VLAN (802.1x-VLAN ohne Authentifizierung)	Für 802.1x-VLANs ohne Authentifizierung gibt es Funktionseinschränkungen in Verbindung mit: • 802.1X Guest VLAN • Private VLAN • Isolated VLAN • Community VLAN • Special VLAN
802.1x Unauthenticated VLAN Port (802.1x-VLAN-Port ohne Authentifizierung)	Bei 802.1x-VLAN-Ports ohne Authentifizierung gibt es Funktionseinschränkungen in Verbindung mit: • Isolated Ports • Community Ports • Promiscuous Ports • MAC based VLAN ports • Ingress Filtering
ACL	Die ACL-Funktionalität ist eingeschränkt in Verbindung mit: • MAC Based ACLs • Special VLANs
Auto-Negotiation	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
Backpressure	
Bridge Multicast Filtering (Bridge-Multicastfilterung)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
Cable Tests (Kabeltests)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
Community ports (Community-Ports)	Die Funktionalität der Community-Ports ist in Verbindung mit gesperrten Ports (Locked Ports) eingeschränkt.
Community-VLAN	Bei Community-VLANs gibt es Funktionseinschränkungen in Verbindung mit: • Static MAC addresses • ACLs • GVRP • IGMP Snooping • Special VLANs
DNS	Keine Einschränkungen.
Duplex Mode (Duplexmodus)	
Flow Control (Flusskontrolle)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
GARP	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
Guest VLANs (Gast-VLANs)	Gast-VLANs arbeiten nicht in Verbindung mit: • Private VLAN • Isolated VLAN • Community VLAN • MAC Based VLANs • Special VLANs
GVRP	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
IGMP Snooping (IGMP-Snooping)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
Ingress Filtering (Ingress-Filterung)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
Isolated Port (Isolierter Port)	Isolierte Ports arbeiten nicht in Verbindung mit: • Community Ports • Promiscuous Ports • Port Lock • GVRP • MAC based ACLs • Ingress Filtering
Isolated VLAN (Isoliertes VLAN)	Isolierte VLANs arbeiten nicht in Verbindung mit: • Community VLANs • Static MAC Addresses • ACLs • GVRP

	• IGMP Snooping • Special VLANs
LAG Statistics (LAG-Statistiken)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
Link Aggregation (Link-Aggregation)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung. Allerdings gelten bei Einsatz dieser Funktion bestimmte Richtlinien für die Konfiguration der Link-Aggregation. Sämtliche Funktionsrichtlinien finden Sie unter Definieren von LAG-Parametern.
Locked Ports (Gesperrte Ports)	Bei gesperrten Ports gibt es Funktionseinschränkungen in Verbindung mit: • MAC Based ACLs • Ingress Filtering
Logging (Protokolle)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
MAC Address Support (MAC-Adressen)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
MDI/MDIX Detection (MDI/MDIX-Erkennung)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
Multicast Filtering (Multicastfilterung)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
Multiple Hosts (Mehrere Hosts)	802.1x Standard (mehrere Hosts) arbeiten nicht in Verbindung mit: • Isolated Port • MAC Based VLAN Port
Multiple Spanning Tree	Multiple Spanning Tree arbeitet nicht in Verbindung mit: • Isolated Port • Ingress Filtering
Port Based Authentication (Portbasierte Authentifizierung)	Bei der portbasierten Authentifizierung gibt es Funktionseinschränkungen in Verbindung mit: • 802.1 Single • Isolated Port • Locked Ports • MAC Based VLANs • Ingress Ports
Port Mirroring (Port-Spiegelung)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung. Allerdings gelten bei Einsatz dieser Funktion bestimmte Richtlinien für die Konfiguration der Broadcaststurmkontrolle. Sämtliche Funktionsrichtlinien finden Sie unter Festlegen von Portspiegelungs-Sitzungen.
Port Statistics (Port-Statistiken)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
Private VLAN (Privates VLAN)	Private VLANs arbeiten nicht in Verbindung mit: • Isolated Ports • Community Ports • GVRP • IGMP Snooping • Special VLAN
Private VLAN (Privates VLAN)	Bei privaten VLANs gibt es Funktionseinschränkungen in Verbindung mit: • Isolated VLANs • GVRP • IGMP Snooping • Special VLAN
Promiscuous Ports	Promiscuous Ports arbeiten nicht in Verbindung mit: • Locked Ports • GVRP • MAC Based VLAN Ports
Quality of Service (Dienstgüte)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
RMON Statistics (RMON-Statistiken)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
SNMP Authentication Notifications (SNMP-Authentifizierungsbenachrichtigungen)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
SNMP Notifications (SNMP-Benachrichtigungen)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
SNTP Authentication (SNTP-Authentifizierung)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
Spanning Tree	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
Special VLAN (Spezial-VLANs)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
Static MAC (Statische MAC-Adresse)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
Storm Control (Broadcaststurmkontrolle)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
System Logs (Systemprotokolle)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
System Time Synchronization (Synchronisierung der Systemzeit)	Keine Einschränkungen hinsichtlich der Funktionswechselwirkung.
Unauthenticated VLAN Ports (VLAN-Ports ohne Authentifizierung)	Bei VLAN-Ports ohne Authentifizierung gibt es Funktionseinschränkungen in Verbindung mit: • Isolated Ports • Community Ports

	• Promiscuous Ports • GVRP • MAC Based VLAN ports • Ingress Filtering

Zurück zum Inhalt

Zurück zum Inhalt

Glossar

Dell™ PowerConnect™ 34XX- Systeme Benutzerhandbuch

In diesem Glossar sind die wichtigsten technischen Fachbegriffe verzeichnet.

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

A

Abfrage

Abruf von Information aus einer Datenbank und Darstellung der Informationen zur weiteren Nutzung.

Aggregiertes VLAN

Gruppiert 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 (Adressauflösungsprotokoll). Ein Protokoll, das IP-Adressen in physische Adressen konvertiert.

ASIC

Application-Specific Integrated Circuit (Anwendungsspezifische integrierte Schaltung). Ein für eine bestimmte Anwendung speziell entwickelter Chip.

Asset Tag (Systemkennnummer)

Gibt die benutzerdefinierte Gerätreferenz des Switch-Moduls an.

Authentifizierungsprofile

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

Auto-Negotiation

Ermöglicht bei Ethernet-Ports mit 10/100 Mbps oder 10/100/1000 Mbps das automatische Aushandeln der folgenden Funktionen:

- Duplex/Halbduplexmodus
- Flusskontrolle
- Geschwindigkeit

B

Backpressure

Ein Mechanismus mit dem ein Port im Halbduplexmodus Nachrichten abweisen kann.

Backup-Konfigurationsdateien

Enthalten eine Sicherungskopie der Switch-Modul-Konfiguration. Die Datei Backup Configuration ändert sich, sobald die Datei Running Configuration oder Startup Configuration in die Datei Backup Configuration kopiert werden.

Bandbreite

Die Brandbreite gibt die Datenmenge an, die in einem festlegten Zeitraum übertragen werden kann. Bei digitalen Switch-Modulen wird die Bandbreite in Bit pro Sekunde (bps) oder Byte pro Sekunde angegeben.

Bandbreitenzuweisung

Die Menge an Bandbreite, die einer spezifischen Anwendung, einem Benutzer oder einer Schnittstelle zugewiesen ist.

Bits pro Sekunde

Die Anzahl der Signalelemente, die pro Sekunde übertragen werden.

Best Effort

Der Datenverkehr wird der Warteschlange mit der niedrigsten Priorität zugewiesen, und die Zustellung von Paketen ist nicht garantiert.

Boot-Version

Die Boot-Version.

BootP

Bootstrap Protocol.Hiermit kann eine Workstation auf seine IP-Adresse, die IP-Adresse eines BootP-Servers auf einem Netzwerk oder eine Konfigurationsdatei im Boot-Bereich eines Switch-Moduls zugreifen.

BPDU

Bridge Protocol Data Unit (Dateneinheit des Brdige-Protokolls). Stellt Bridge-Informationen in Meldungsformat bereit. BPDUs werden über Switch-Modul-Informationen hinweg innerhalb von Spanning-Tree-Konfigurationen übertragen. BPDU-Pakete enthalten Informationen zu Ports, Adressen, Prioritäten und Weiterleitungskosten.

Bridge

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

Broadcastdomäne

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 Weiterleitung von Paketen an alle Ports eines Netzwerks.

Broadcaststurm

Eine übermäßig große Menge von Broadcastnachrichten, die gleichzeitig von einem einzelnen Port in einem Netzwerk gesendet werden. Rückmeldungen auf weitergeleitete Nachrichten belasten das Netzwerk, wodurch Netzwerkressourcen strapaziert bzw. Netzwerkausfälle verursacht werden.

Weitere Informationen zu Broadcaststürmen finden Sie unter "Definieren von LAG-Parametern".

C

CDB

Configuration Data Base (Konfigurationsdatenbank). Eine Datei mit Informationen zur Gerätekonfiguration.

Class of Service

Class of Service (CoS) (Berechtigungsklasse).Class of Service ist das 802.1p-Prioritätsschema. CoS ist eine Methode zum Kennzeichnen von Paketen mit Prioritätsinformationen. Ein CoS-Wert zwischen 0 und 7 wird dem Layer-II-Header von Paketen hinzufügt, wobei null die niedrigste und sieben die höchste Priorität darstellt.

Eine überlappende Übertragung von zwei oder mehr Paketen, die miteinander kollidieren. Die so übertragenen Daten können nicht genutzt werden, und die Sitzung wird neu gestartet.

CLI

Command Line Interface(Befehlszeilenschnittstelle). Ein Befehlszeilenssatz zur Konfiguration des Systems. Weitere Informationen zum Einsatz der CLI finden Sie unter Verwenden der CLI.

Communities

Gibt eine Gruppe von Benutzern mit den gleichen Systemzugriffsrechten an.

CPU

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

D

DHCP-Client

Ein Gerätehost, der DHCP zum Bereitstellen von Konfigurationsparametern verwendet, etwa einer Netzwerkadresse.

DSCP

DiffServe Code Point (DSCP). DSCP ist eine Methode zum Kennzeichnen von IP-Paketen mit QoS-Prioritätsinformationen.

Domäne

Eine Gruppe von Computern und Geräten in einem Netzwerk, die durch gemeinsame Regeln und Prozeduren zusammengefasst sind.

DRAC/MC

DRAC/MC. Bildet einen zentralen Punkt für die Steuerung der Komponenten des Dell Modular Server Systems.

Duplexmodus

Ermöglicht gleichzeitiges Senden und Empfangen von Daten. Es gibt zwei verschiedene Duplexmodi:

- **Vollduplexmodus** – Für bisynchrone Kommunikation, wie etwa beim Telefonieren. Beide Gegenstellen können gleichzeitig Informationen senden.
- **Halbduplexmodus** – Für asynchrone Kommunikation, wie etwa beim Walkie-Talkie. Nur eine Gegenstelle kann jeweils Daten senden.

E

Egress-Ports

Ports, von denen Netzwerkdatenverkehr ausgeht.

Endsystem

Ein Endbenutzergerät in einem Netzwerk.

Ethernet

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

EWS

Embedded Web Server (Integrierter Webserver). Stellt Geräteverwaltung über einen Standard-Web-Browser bereit. Embedded Web Servers werden zusätzlich zu oder an Stelle von CLI oder NMS eingesetzt.

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 aufgeführte 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 eingereihte Paket als erstes aus der Warteschlange herauskommt.

Flapping (ständiger Wechsel)

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

Flow Control (Flusskontrolle)

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

Fragment

Ethernet-Pakete mit weniger als 576 Bit.

Frame

Pakete mit Header und Trailer-Informationen, die vom physischen Übertragungsmedium benötigt werden.

G

GARP

General Attributes Registration Protocol (Allgemeines Attributregistrierungsprotokoll). Dient zur Registrierung von Client-Stations in einer Multicast-Domäne.

Gigabit Ethernet

Gigabit-Ethernet überträgt mit 1000 Mbps und ist kompatibel zu den bestehenden 10/100 Mbps-Ethernet-Standards

GVRP

GARP VLAN Registration Protocol (GARP-VLAN-Registrierungsprotokoll). Registriert Client-Stationen in VLANs.

H

HOL

Head of Line. Pakete werden Warteschlangen zugeordnet. Pakete an der Spitze einer Warteschlange werden vor den weiter hinten liegenden Paketen weitergeleitet.

Host

Ein Computer, der als Quelle von Daten oder Diensten für andere Computer dient.

HTTP

Hypertext Transfer Protocol.Dient zum Übertragen von HTML-Dokumenten 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 einem Gateway oder Ziel-Host die Kommunikation mit einem Quell-Host, etwa um einen Verarbeitungsfehler zu melden.

IEEE

Institute of Electrical and Electronics Engineers.Vereinigung von Elektrotechnikern, 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

Dient zum Zuordnen von Prioritäten für Netzwerkdatenverkehr in der Sicherungs-/MAC-Schicht.

IEEE 802.1Q

Definiert den Betrieb von VLAN-Bridges für die Verwaltung von VLANs in Bridged-LAN-Infrastrukturen.

Image-Datei

System-Images werden in zwei Flash-Sektoren 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.

Ingress-Port

Ports, an denen Netzwerkdatenverkehr empfangen wird.

IP

Internet Protocol (Internet-Protokoll). Legt das Format von Paketen und die Adressierungsmethode fest. Mit IP werden Pakete adressiert und zum korrekten Port weitergeleitet.

IP-Adresse

Internet-Protokoll-Adresse. Eine eindeutige Adresse, die einem Netzwerkgerät in zwei oder mehreren verbundenen LANs oder WANs zugewiesen ist.

J

Jumbo-Frames

Ermöglicht die Übertragung gleicher Datenmengen mit weniger Frames. Bei Verwendung von Jumbo-Frames werden Overhead und Rechenzeit verringert, und es treten weniger Unterbrechungen auf.

K

Knoten

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

- Prozessoren
- Controller
- Workstations

L

LAG

Link Aggregated Group. Fasst Ports oder VLANs zu einem einzigen virtuellen Port oder VLAN zusammen.

Weitere Informationen zu LAGs finden Sie im Abschnitt **Definieren von LAG-Mitgliedschaften**.

LAN

Local Area Networks (Lokale Netzwerke). Ein Netzwerk, das sich in einem einzelnen Raum, einem Gebäude, Campus oder einem anderen begrenzten geographischen Bereich befindet.

Layer 2

Sicherungsschicht oder MAC-Schicht. Enthält die physische Adresse eines Clients oder einer Serverstation. Die Verarbeitung mit Layer 2 ist schneller als mit Layer 3, da weniger Informationen anfallen.

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 hardwarespezifische Adresse, die die einzelnen Netzwerkknoten identifiziert.

MAC-Adresserfassung

Bei der MAC-Adresserfassung werden die Quell-MAC-Adressen von Paketen ausgelesen und erfasst. Pakete für diese Adresse werden nur zu der Bridge-Schnittstelle weitergeleitet, an der sich diese Adressse befindet. Pakete zu unbekannten Adressen werden an alle Bridge-Schnittstellen weitergeleitet. Durch MAC-Adresserfassung wird der Datenverkehr auf den verbundenen LANs minimiert.

MAC-Schicht

Eine Subschicht der Datenübertragungssteuerungsschicht (Data Link Control, DTL).

Maske

Ein Filter, mit dem bestimmte Werte einbezogen oder ausgeschlossen werden, etwa Teile einer IP-Adresse.

Beispielsweise wird die Einheit 2 in der ersten Minute eines Zehn-Minuten-Zyklus eingefügt, Einheit 1 in der fünften Minute desselben Zyklus. In diesem Fall werden beide Einheiten als gleich alt betrachtet.

MD5

Message Digest 5. Ein Algorithmus, der einen 128-Bit-Hash produziert. MMD5 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 für Endstationen verwendetes Kabel.

MDIX

Media Dependent Interface with Crossover (Gekreuzte medianabhängige Schnittstelle). Ein für Hubs und Switches verwendetes Kabel.

MIB

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

Multicast

Sendet Kopien eines einzelnen Pakets an mehrere Ports.

N

NMS

Network Management System (Netzverwaltungssystem). Eine Schnittstelle, die eine Methode zur Verwaltung eines System bereitstellt.

O

OID

Object Identifier (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

Pakete

Blöcke von Informationen zum Übertragen in Paket-Switch-Systemen.

PDU

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

PING

Packet Internet Groper.Hiermit lässt sich überprüfen, ob eine bestimmte IP-Adresse verfügbar ist. Ein Paket wird an eine andere IP-Adresse gesendet, und die Antwort wird abgewartet.

Port

Physische Schnittstellen zum Verbinden von Komponenten, damit Mikroprozessoren mit externen Geräten kommunizieren können.

Port-Spiegelung

Bei der Port-Spiegelung wird der Netzwerkdatenverkehr überwacht und gespiegelt, indem Kopien eingehender und ausgehender Pakete von ausgewählten Ports an einen Überwachungsport weitergeleitet werden.

Weitere Information zur Port-Spiegelung finden Sie unter **Defining Port Mirroring Sessions**.

Port-Geschwindigkeit

Gibt die Geschwindigkeit des Ports wieder. Folgendes sind gängige Port-Geschwindigkeiten:

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

Protokoll

Ein Satz von Regeln, der festlegt, wie Geräte Informationen in Netzwerken austauschen.

Q

QoS

Quality of Service (Dienstgüte). Mit QoS können Netzwerkverwalter bestimmen, welcher Netzwerkdatenverkehr entsprechend festgelegter Prioritäten, Anwendungstypen sowie Quell- und Zieladressen weitergeleitet wird und wie dies geschieht.

R

RADIUS

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

RMON

Remote Monitoring (Fernüberwachung). Hiermit lassen sich Netzwerkinformationen an einer einzelnen Workstation erfassen.

Router

Ein Gerät, dass mit separaten Netzwerken verbunden ist. Router leiten Pakete zwischen zwei oder mehreren Netzwerken weiter. Router funktionieren auf Layer-3-Ebene.

RSTP

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

Running Configuration

Enthält sämtliche Befehle aus der Datei Startup Configuration sowie alle während der aktuellen Sitzung eingegebenen Befehle. Nachdem das Switch-Modul

ausgeschaltet oder neu gestartet wurde, werden alle in der Datei Running Configuration gespeicherten Befehle verworfen.

Rückwandplatine

Der Haupt-BUS, der die Informationen im Switch-Modul transportiert.

S

Segmentierung

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

Server

Ein zentraler Computer, der für andere Computer auf einem Netzwerk Dienste zur Verfügung stellt. Bei den Diensten kann es sich um Datenspeicherung oder Zugang zu Anwendungen handeln.

SNMP

Simple Network Management Protocol (Einfaches Netzwerk-Verwaltungsprotokoll). Dient zum Verwalten von LANs. SNMP-basierte Software kommuniziert mit Netzwerkgeräten über integrierte SNMP-Agents. SNMP-Agents erfassen Netzwerkaktivität und Gerätestatusinformationen von Ethernet-Switches und senden die Informationen zurück zu einer Workstation.

SNTP

Simple Network Time Protocol (Einfaches Netzwerkzeit-Protokoll). SNTP stellt die genaue Zeitsynchronisierung des Netzwerk-Switch 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 Protocol

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

SSH

Secure Shell. Erlaubt, sich an einem Remote-Computer über ein Netzwerk anzumelden, Befehle auszuführen und Dateien von einem Computer zum anderen zu übertragen. Secure Shell stellt leistungsfähige Authentifizierungs- und sichere Kommunikationsverfahren über unsichere Kanäle bereit.

Startkonfiguration

Speichert die genaue Modulkonfiguration, wenn das Switch-Modul ausgeschaltet oder neu gestartet wird.

Subnetz

Sub-Netzwerk. Subnetze sind Teile eines Netzwerks, die eine gemeinsame Adresskomponente aufweisen. Bei TCP/IP-Netzwerken gehören Geräte mit einem gemeinsamen Präfix dem gleichen Subnetz an. Beispielsweise gehören alle Geräte mit dem Präfix 157.100.100.100 zum gleichen Subnetz.

Subnetzmaske

Dient zum Maskieren der IP-Adresse oder eines Teils davon für eine Subnetzadresse.

Switch

Dient zum Filtern und Weiterleiten von Paketen zwischen LAN-Segmenten. Switches unterstützen beliebige Paket-Protokolltypen.

T

TCP/IP

Transmissions Control Protocol (Übertragungssteuerungsprotokoll). Ermöglicht zwei Hosts zu kommunizieren und Datenströme auszutauschen. TCP sichert die Zustellung der Pakete und gewährleistet, dass die Pakete in der Reihenfolge des Sendens übertragen und empfangen werden.

Telnet

Terminal-Emulationsprotokoll. Ermöglicht den Systembenutzern, sich bei Remote-Netzwerken anzumelden und deren Ressourcen zu verwenden.

TFTP

Trivial File Transfer Protocol. Verwendet zum Übertragen von Dateien das User Data Protocol (UDP) ohne Sicherheitsfunktionen.

Trap (Ereignismeldung)

Eine vom SNMP versandte Meldung über das Auftreten eines Systemereignisses.

Trunking

Link-Aggregation.Optimiert die Port-Nutzung, indem eine Gruppe von Ports zu einem einzelnen Trunk (aggregierte Gruppen) zusammengefasst wird.

U

UDP

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

Unicast

Eine Art von Routing, bei dem ein Paket zu einem Benutzer gesendet wird.

V

VLAN

Virtual Local Area Networks (Virtuelle lokale Netzwerke). Logische Untergruppen eines LANs (Local Area Network), die softwarebasiert und nicht durch eine Hardwarelösung erstellt werden.

W

WAN

Wide Area Networks (Weitverkehrsnetze). Netzwerk, das sich über einen weiten geographischen Bereich erstreckt.

Platzhaltermaske

Legt fest, welche IP-Adressbits verwendet und welche ignoriert werden. Die Switch-Modul-Platzhaltermaske 255.255.255.255 gibt an, dass alle Bits ignoriert werden. Der Platzhalter 0.0.0.0 gibt an, dass alle Bits berücksichtigt werden.

Wenn die IP-Zieladresse beispielsweise 149.36.184.198 und die Platzhaltermaske 255.36.184.00 lautet, werden die ersten beiden Bits der IP-Adresse verwendet, während die letzten beiden Bits ignoriert werden.

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 Switch-Modul. Der Zugriff auf Verwaltungsfunktionen kann auf Benutzergruppen beschränkt werden, die nach den folgenden Kriterien definiert werden:

- Ingress-Schnittstellen
- Quell-IP-Adresse oder Quell-IP Subnetze

Zurück zum Inhalt