Best Practices für Catalyst Switches der Serien 6500/6000 und 4500/4000 mit Cisco IOS Software

Inhalt

Einführung

Dieses Dokument enthält Best Practices für Catalyst Switches der Serien 6500/6000 und 4500/4000, auf denen die Cisco IOS® Software auf der Supervisor Engine ausgeführt wird.

Die Catalyst Switches der Serien 6500/6000 und 4500/4000 unterstützen eines der beiden folgenden Betriebssysteme, die auf der Supervisor Engine ausgeführt werden:

- Catalyst OS (CatOS)
- Cisco IOS-Software

CatOS bietet die Möglichkeit, die Cisco IOS Software auf Router-Tochterkarten oder -Modulen auszuführen, z. B.:

- Die Multilayer Switch Feature Card (MSFC) im Catalyst 6500/6000
- Das 4232 Layer 3 (L3)-Modul im Catalyst 4500/4000

In diesem Modus stehen zwei Befehlszeilen für die Konfiguration zur Verfügung:

- Die CatOS-Befehlszeile für das Switching
- Die Cisco IOS Software-Befehlszeile für das Routing

CatOS ist die Systemsoftware, die auf der Supervisor Engine ausgeführt wird. Cisco IOS Software, die auf dem Routing-Modul ausgeführt wird, ist eine Option, die CatOS-Systemsoftware erfordert.

Für die Cisco IOS Software steht nur eine Befehlszeile zur Konfiguration zur Verfügung. In diesem Modus wurde die CatOS-Funktionalität in die Cisco IOS-Software integriert. Die Integration führt zu einer einzigen Befehlszeile für die Switching- und Routing-Konfiguration. In diesem Modus ist die Cisco IOS Software die Systemsoftware und ersetzt CatOS.

Sowohl CatOS- als auch Cisco IOS Software-Betriebssysteme werden in kritischen Netzwerken bereitgestellt. CatOS wird mit der Cisco IOS Software-Option für Router-Tochterkarten und -Module in dieser Switch-Serie unterstützt:

- Catalyst 6500/6000
- Catalyst 5500/5000
- Catalyst 4500/4000

Die Cisco IOS-Systemsoftware wird von den folgenden Switches unterstützt:

- Catalyst 6500/6000
- Catalyst 4500/4000

Informationen zu CatOS finden Sie im Dokument Best Practices für Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000 mit CatOS-Konfiguration und -Management, da dieses Dokument die Cisco IOS-Systemsoftware abdeckt.

Die Cisco IOS-Systemsoftware bietet Benutzern folgende Vorteile:

- Eine einzige Benutzeroberfläche
- Eine einheitliche Netzwerkverwaltungsplattform
- Erweiterte QoS-Funktionen
- Unterstützung von verteilten Switches

Dieses Dokument enthält Anleitungen zur modularen Konfiguration. Daher können Sie jeden Abschnitt einzeln lesen und Änderungen in einem stufenweisen Ansatz vornehmen. In diesem Dokument wird davon ausgegangen, dass die Benutzeroberfläche der Cisco IOS Software allgemein verständlich und bekannt ist. Das Dokument behandelt nicht das gesamte Campus-Netzwerkdesign.

Bevor Sie beginnen

Hintergrund

Die Lösungen, die dieses Dokument bietet, beinhalten eine jahrelange Erfahrung von Cisco Technikern, die mit komplexen Netzwerken arbeiten, sowie von vielen der größten Kunden. Daher werden in diesem Dokument reale Konfigurationen hervorgehoben, die Netzwerke erfolgreich machen. Dieses Dokument bietet folgende Lösungen:

- Lösungen, die statistisch die größte Feldexposition und damit das niedrigste Risiko aufweisen
- Einfache Lösungen, die gewisse Flexibilität für deterministische Ergebnisse eintauschen
- Einfache Verwaltung und Konfiguration durch Netzwerkbetriebsteams
- Lösungen zur Förderung von Hochverfügbarkeit und hoher Stabilität

Referenzen

Auf Cisco.com finden Sie zahlreiche Referenzseiten für die Produktlinien Catalyst 6500/6000 und Catalyst 4500/4000. Die in diesem Abschnitt aufgeführten Verweise bieten zusätzliche Informationen zu den Themen, die in diesem Dokument behandelt werden.

Weitere Informationen zu den Themen dieses Dokuments finden Sie im LAN Switching Technology Support. Auf der Support-Seite finden Sie Produktdokumentationen sowie Problembehebungs- und Konfigurationsdokumente.

Dieses Dokument enthält Verweise auf öffentliches Online-Material, damit Sie weiter lesen können. Weitere gute grundlegende und informative Referenzen sind jedoch:

- Grundlagen von Cisco ISP
- Vergleich der Cisco Catalyst-Betriebssysteme mit Cisco IOS-Betriebssystemen für Switches der Serie Cisco Catalyst 6500
- Cisco LAN Switching (CCIE Professional Development Series)
- Aufbau von Cisco Multilayer Switched Networks
- Leistungs- und Fehlermanagement
- SAFE: Ein Sicherheitskonzept für Enterprise Networks
- Cisco Außenhandbuch: Catalyst Switch-Konfiguration

Basiskonfiguration

In diesem Abschnitt werden die Funktionen erläutert, die bei der Verwendung der meisten Catalyst-Netzwerke bereitgestellt werden.

Catalyst Control Plane-Protokolle

In diesem Abschnitt werden die Protokolle vorgestellt, die zwischen Switches im normalen Betrieb ausgeführt werden. Ein grundlegendes Verständnis der Protokolle ist hilfreich, wenn Sie jeden Abschnitt angehen.

Supervisor Engine-Datenverkehr

Die meisten Funktionen, die in einem Catalyst-Netzwerk aktiviert sind, erfordern zwei oder mehr Switches, um zusammenzuarbeiten. Aus diesem Grund muss ein kontrollierter Austausch von Keepalive-Meldungen, Konfigurationsparametern und Verwaltungsänderungen erfolgen. Unabhängig davon, ob es sich um proprietäre Cisco Protokolle wie Cisco Discovery Protocol (CDP) oder standardbasierte Protokolle wie IEEE 802.1D (Spanning Tree Protocol [STP]) handelt, haben alle bestimmte Elemente gemeinsam, wenn die Protokolle in der Catalyst-Serie implementiert werden.

Bei der grundlegenden Frame-Weiterleitung stammen die Daten-Frames der Benutzer von den Endsystemen. Die Quelladresse (SA) und die Zieladresse (DA) der Datenframes werden nicht in allen L2-Switched-Domänen von Layer 2 geändert. Die CAM-Nachschlagetabellen (Content-Addressable Memory) auf jeder Switch Supervisor Engine werden durch einen SA-Lernprozess aufgefüllt. Die Tabellen geben an, welcher Ausgangsport jeden empfangenen Frame weiterleitet. Wenn das Ziel unbekannt ist oder der Frame für eine Broadcast- oder Multicast-Adresse bestimmt ist, ist der Prozess zum Erlernen von Adressen unvollständig. Wenn der Prozess unvollständig ist, wird der Frame an alle Ports in diesem VLAN weitergeleitet (geflutet). Der Switch muss auch erkennen, welche Frames durch das System geschaltet werden sollen und welche Frames an die Switch-CPU selbst weitergeleitet werden sollen. Die Switch-CPU wird auch als Network Management Processor (NMP) bezeichnet.

Sondereinträge in der CAM-Tabelle werden zur Erstellung der Catalyst-Kontrollebene verwendet. Diese Sondereinträge werden Systemeinträge genannt. Die Steuerungsebene empfängt und leitet den Datenverkehr an den NMP über einen internen Switch-Port weiter. Durch die Verwendung von Protokollen mit bekannten Ziel-MAC-Adressen kann der Datenverkehr auf Kontrollebene vom Datenverkehr getrennt werden.

Cisco verfügt über einen reservierten Bereich von Ethernet-MAC- und Protokolladressen, wie die Tabelle in diesem Abschnitt zeigt. Dieses Dokument behandelt jede reservierte Adresse im Detail, aber diese Tabelle bietet eine Zusammenfassung, um die folgenden Vorteile zu nutzen:

Funktion	SNAP[1] HDLC[2]-Protokolltyp	Ziel-Multicast-MAC
PAgP[3]	0 x 0104	01-00-0c-cc-cc-cc
PVST+, RPVST+[4]	0 x 010 b	01-00-0c-cc-cd
VLAN-Bridge	0 x 010 C	01-00-0c-cd-cd-ce
UDLD[5]	0 x 0111	01-00-0c-cc-cc-cc
CDP	0 x 2000	01-00-0c-cc-cc-cc
DTP[6]	0 x 2004	01-00-0c-cc-cc-cc
STP-UplinkFast	0 x 200 a	01-00-0c-cd-cd-cd
IEEE Spanning Tree 802.1D	K/A - DSAP[7] 42 SSAP[8] 42	01-80-c2-00-00-00

ISL[9]	K/A	01-00-0c-00-00-00-00
VTP[10]	0 x 2003	01-00-0c-cc-cc-cc
IEEE-Pause 802.3x	K/A - DSAP 81 SSAP 80	01-80-C2-00-00-00>0F

[1] SNAP = Subnetzwerk Access Protocol

[2] HDLC = High Level Data Link Control.

[3] PAgP = Port Aggregation Protocol

[4] PVST+ = Per VLAN Spanning Tree+ und RPVST+ = Rapid PVST+

[5] UDLD = UniDirectional Link Detection.

[6] DTP = Dynamic Trunking Protocol

[7] DSAP = Ziel Service Access Point.

[8] SSAP = Source Service Access Point

[9] ISL = Inter-Switch Link.

[10] VTP = VLAN Trunk Protocol

Die meisten Cisco Steuerungsprotokolle verwenden eine IEEE 802.3-SNAP-Kapselung, die Logical Link Control (LLC) 0xAAAA03 und Organizational Unique Identifier (OUI) 0x0000C umfasst. Sie können dies in einer LAN-Analyzer-Ablaufverfolgung sehen.

Diese Protokolle setzen eine Punkt-zu-Punkt-Verbindung voraus. Beachten Sie, dass die absichtliche Verwendung von Multicast-Zieladressen es zwei Catalyst-Switches ermöglicht, transparent über Switches zu kommunizieren, die nicht von Cisco stammen. Geräte, die die Frames nicht verstehen und abfangen, überfluten sie einfach. Point-to-Multipoint-Verbindungen in Umgebungen mit Geräten verschiedener Anbieter können jedoch zu inkonsistentem Verhalten führen. Vermeiden Sie im Allgemeinen Point-to-Multipoint-Verbindungen in Umgebungen mit Geräten verschiedener Anbieter. Diese Protokolle enden an Layer-3-Routern und funktionieren nur innerhalb einer Switch-Domäne. Diese Protokolle erhalten eine Priorisierung gegenüber Benutzerdaten, indem sie ASIC-Verarbeitung (Application-Specific Integrated Circuit) und -zeitplanung eingeben.

Nun wenden wir uns der SA zu. Switch-Protokolle verwenden eine MAC-Adresse, die einer Bank mit verfügbaren Adressen entnommen wird. Ein EPROM auf dem Chassis stellt die Bank der verfügbaren Adressen bereit. Geben Sie den Befehl **show module** ein, um die Adressbereiche anzuzeigen, die jedem Modul für die Sourcing von Datenverkehr zur Verfügung stehen, z. B. STP Bridge Protocol Data Units (BPDUs) oder ISL Frames. Dies ist eine Beispielbefehlsausgabe:

```
>show module
…

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------  -----------------
1   00-01-c9-da-0c-1e to 00-01-c9-da-0c-1f 2.2    6.1(3)      6.1(1d)
```

```
    00-01-c9-da-0c-1c to 00-01-c9-da-0c-1
    00-d0-ff-88-c8-00 to 00-d0-ff-88-cb-ff
!--- These are the MACs for sourcing traffic.
```

VLAN 1

VLAN 1 hat in Catalyst-Netzwerken eine besondere Bedeutung.

Beim Trunking verwendet die Catalyst Supervisor Engine immer das Standard-VLAN VLAN 1, um eine Reihe von Steuerungs- und Verwaltungsprotokollen zu kennzeichnen. Zu diesen Protokollen gehören CDP, VTP und PAgP. Alle Switch-Ports, einschließlich der internen Schnittstelle sc0, sind standardmäßig als Mitglieder von VLAN 1 konfiguriert. Alle Trunks übertragen standardmäßig VLAN 1.

Diese Definitionen sind erforderlich, um einige häufig verwendete Begriffe in Catalyst-Netzwerken zu klären:

- Das Management-VLAN ist der Standort sc0 für CatOS- und Low-End-Switches. Sie können dieses VLAN ändern. Berücksichtigen Sie dies beim Zusammenspiel von CatOS- und Cisco IOS-Switches.
- Das native VLAN ist das VLAN, zu dem ein Port zurückgegeben wird, wenn er kein Trunking ist. Darüber hinaus ist das native VLAN das nicht gekennzeichnete VLAN auf einem IEEE 802.1Q-Trunk.

Es gibt mehrere gute Gründe, ein Netzwerk zu optimieren und das Verhalten von Ports in VLAN 1 zu ändern:

- Wenn der Durchmesser von VLAN 1, wie jedes andere VLAN, groß genug ist, um ein Stabilitätsrisiko zu darstellen, insbesondere aus der Perspektive eines STP, müssen Sie das VLAN zurückschneiden. Weitere Informationen finden Sie im Abschnitt "Switch-Management-Schnittstelle und natives VLAN".
- Um die Fehlerbehebung zu vereinfachen und die verfügbaren CPU-Zyklen zu maximieren, müssen die Daten der Steuerungsebene in VLAN 1 von den Benutzerdaten getrennt gehalten werden. Vermeiden Sie Layer-2-Schleifen in VLAN 1, wenn Sie mehrschichtige Campus-Netzwerke ohne STP entwerfen. Um Layer-2-Schleifen zu vermeiden, müssen Sie VLAN 1 manuell von den Trunk-Ports löschen.

Beachten Sie in der Zusammenfassung die folgenden Informationen zu Trunks:

- CDP-, VTP- und PAgP-Updates werden immer auf Trunks mit einem VLAN 1-Tag weitergeleitet. Dies ist auch der Fall, wenn VLAN 1 aus den Trunks entfernt wurde und nicht das native VLAN ist. Wenn Sie VLAN 1 für Benutzerdaten löschen, hat die Aktion keine Auswirkungen auf den Steuerungsebenen-Datenverkehr, der noch unter Verwendung von VLAN 1 gesendet wird.
- Auf einem ISL-Trunk werden DTP-Pakete über VLAN1 gesendet. Dies ist auch der Fall, wenn VLAN 1 vom Trunk gelöscht wurde und nicht mehr das native VLAN ist. Auf einem 802.1Q-Trunk werden DTP-Pakete über das native VLAN gesendet. Dies ist auch dann der Fall, wenn das native VLAN vom Trunk gelöscht wurde.
- In PVST+ werden die 802.1Q IEEE-BPDUs nicht getaggt im allgemeinen Spanning Tree VLAN 1 weitergeleitet, um die Interoperabilität mit anderen Anbietern zu gewährleisten, es sei denn, VLAN 1 wurde aus dem Trunk entfernt. Dies ist unabhängig von der nativen VLAN-Konfiguration der Fall. Cisco PVST+ BPDUs werden für alle anderen VLANs gesendet und

getaggt. Weitere Informationen finden Sie im Abschnitt Spanning Tree Protocol.
- 802.1s MST-BPDUs (Multiple Spanning Tree) werden immer in VLAN 1 auf ISL- und 802.1Q-Trunks gesendet. Dies gilt auch dann, wenn VLAN 1 aus den Trunks entfernt wurde.
- Deaktivieren Sie VLAN 1 auf Trunks zwischen MST-Bridges und PVST+-Bridges nicht. Wenn VLAN 1 deaktiviert ist, muss die MST-Bridge jedoch als Root-Bridge fungieren, damit alle VLANs die MST-Bridge-Platzierung der Begrenzungsports im Root-Inkonsistent-Status vermeiden. Weitere Informationen finden Sie unter Understanding Multiple Spanning Tree Protocol (802.1s).

Standardfunktionen

Dieser Abschnitt des Dokuments konzentriert sich auf grundlegende Switching-Funktionen, die in jeder Umgebung zum Einsatz kommen. Konfigurieren Sie diese Funktionen auf allen Cisco IOS Software Catalyst Switching-Geräten im Kundennetzwerk.

VLAN-Trunk-Protokoll

Zweck

Eine VTP-Domäne, die auch als VLAN-Management-Domäne bezeichnet wird, besteht aus einem oder mehreren verbundenen Switches über einen Trunk, der denselben VTP-Domänennamen verwendet. VTP wurde entwickelt, um Benutzern die zentrale Durchführung von VLAN-Konfigurationsänderungen auf einem oder mehreren Switches zu ermöglichen. VTP kommuniziert die Änderungen automatisch mit allen anderen Switches in der VTP-Domäne (Netzwerk). Sie können einen Switch so konfigurieren, dass er sich nur in einer VTP-Domäne befindet. Bevor Sie VLANs erstellen, bestimmen Sie den VTP-Modus, der im Netzwerk verwendet werden soll.

Überblick

VTP ist ein Layer-2-Messaging-Protokoll. VTP verwaltet das Hinzufügen, Löschen und Umbenennen von VLANs auf netzwerkweiter Basis, um eine konsistente VLAN-Konfiguration zu gewährleisten. VTP minimiert Fehlkonfigurationen und Inkonsistenzen in der Konfiguration, die zu einer Reihe von Problemen führen können. Zu den Problemen gehören doppelte VLAN-Namen, falsche VLAN-Typspezifikationen und Sicherheitsverletzungen.

Standardmäßig befindet sich der Switch im VTP-Servermodus und befindet sich im Zustand "no management domain". Diese Standardeinstellungen ändern sich, wenn der Switch eine Anzeige für eine Domäne über einen Trunk-Link empfängt oder wenn eine Management-Domäne konfiguriert ist.

Das VTP-Protokoll kommuniziert zwischen Switches mithilfe eines bekannten Ethernet-Ziel-Multicast-MAC (01-00-0c-cc-cc) und des SNAP-HDLC-Protokolltyps 0x2003. Ähnlich wie andere systeminterne Protokolle verwendet VTP auch eine IEEE 802.3-SNAP-Kapselung, die LLC 0xAAAA03 und OUI 0x0000C umfasst. Sie können dies in einer LAN-Analyzer-Ablaufverfolgung sehen. VTP funktioniert nicht über Nicht-Trunk-Ports. Daher können Nachrichten erst gesendet werden, wenn der DTP-Trunk aktiviert wurde. Mit anderen Worten: VTP ist eine Nutzlast von ISL oder 802.1Q.

Zu den Meldungstypen gehören:

- Zusammenfassende Anzeigen alle 300 Sekunden (Sek.)
- Teilanzeigen und Anfordern von Anzeigen, wenn Änderungen vorgenommen werden
- Joins, wenn VTP Pruning aktiviert ist

Die Revisionsnummer der VTP-Konfiguration wird bei jeder Änderung auf einem Server um eine erhöht, und diese Tabelle wird über die Domäne verteilt.

Beim Löschen eines VLANs geben Ports, die einst Mitglied des VLANs waren, einen `inaktiven` Status ein. Wenn ein Switch im Client-Modus beim Start die VTP VLAN-Tabelle nicht entweder von einem VTP-Server oder einem anderen VTP-Client empfangen kann, werden alle Ports in VLANs außer dem Standard-VLAN 1 deaktiviert.

Sie können die meisten Catalyst Switches für den Betrieb in einem der folgenden VTP-Modi konfigurieren:

- Server - Im VTP-Servermodus können Sie:Erstellen von VLANsÄndern von VLANsVLANs löschenAngeben weiterer Konfigurationsparameter, z. B. VTP-Version und VTP-Bereinigung, für die gesamte VTP-DomäneVTP-Server geben ihre VLAN-Konfiguration an andere Switches in derselben VTP-Domäne weiter. VTP-Server synchronisieren ihre VLAN-Konfiguration auch mit anderen Switches auf der Grundlage von Meldungen, die über Trunk-Links empfangen werden. Der VTP-Server ist der Standardmodus.
- Client - VTP-Clients verhalten sich wie VTP-Server. Sie können VLANs auf einem VTP-Client jedoch nicht erstellen, ändern oder löschen. Darüber hinaus speichert der Client das VLAN nach einem Neustart nicht, da keine VLAN-Informationen im NVRAM geschrieben wurden.
- Transparent - VTP-transparente Switches sind nicht am VTP beteiligt. Ein VTP-transparenter Switch meldet seine VLAN-Konfiguration nicht an und synchronisiert seine VLAN-Konfiguration nicht auf der Grundlage empfangener Meldungen. In VTP-Version 2 leiten transparente Switches jedoch VTP-Meldungen weiter, dass die Switches ihre Trunk-Schnittstellen empfangen.

Funktion	Server	Client	Transparent	Aus [1]
Quell-VTP-Nachrichten	Ja	Ja	Nein	—
Abhören von VTP-Nachrichten	Ja	Ja	Nein	—
Erstellen von VLANs	Ja	Nein	Ja (nur lokal von Bedeutung)	—
VLANs speichern	Ja	Nein	Ja (nur lokal von Bedeutung)	—

[1] Die Cisco IOS Software kann VTP nicht mit dem `Aus`-Modus deaktivieren.

Diese Tabelle enthält eine Zusammenfassung der Erstkonfiguration:

Funktion	Standardwert
VTP-Domänenname	Null
VTP-Modus	Server
VTP-Version	Version 1 ist aktiviert.

VTP-Bereinigung	Deaktiviert

Im VTP-Modus werden VTP-Updates einfach ignoriert. Die bekannte VTP-Multicast-MAC-Adresse wird vom System-CAM entfernt, der normalerweise zum Erfassen von Steuerungs-Frames und zum Weiterleiten an die Supervisor Engine verwendet wird. Da das Protokoll eine Multicast-Adresse verwendet, überflutet der Switch im transparenten Modus oder ein Switch eines anderen Anbieters den Frame einfach mit anderen Cisco Switches in der Domäne.

VTP Version 2 (VTPv2) bietet die in dieser Liste beschriebene funktionale Flexibilität. VTPv2 ist jedoch nicht mit VTP Version 1 (VTPv1) kompatibel:

- Unterstützung für Token-Ring
- Unterstützung nicht erkannter VTP-Informationen - Switches geben jetzt Werte weiter, die sie nicht analysieren können.
- Versionsabhängiger transparenter Modus - Der transparente Modus überprüft den Domänennamen nicht mehr. Dies ermöglicht die Unterstützung von mehr als einer Domäne in einer transparenten Domäne.
- Weitergabe von Versionsnummern - Wenn VTPv2 auf allen Switches möglich ist, können alle Switches mit der Konfiguration eines einzelnen Switches aktiviert werden.

Weitere Informationen finden Sie unter VTP (VLAN Trunk Protocol).

VTP-Betrieb der Cisco IOS-Software

Konfigurationsänderungen in CatOS werden unmittelbar nach einer Änderung in den NVRAM geschrieben. Im Gegensatz dazu speichert die Cisco IOS-Software Konfigurationsänderungen im NVRAM nur, wenn Sie den Befehl **copy run start** ausführen. VTP-Client- und -Serversysteme erfordern VTP-Updates von anderen VTP-Servern, damit diese ohne Benutzereingriff sofort im NVRAM gespeichert werden können. Die VTP-Aktualisierungsanforderungen werden vom CatOS-Standardbetrieb erfüllt, für das Update-Modell der Cisco IOS-Software ist jedoch ein alternativer Aktualisierungsvorgang erforderlich.

Für diese Änderung wurde in der Cisco IOS-Software für den Catalyst 6500 eine VLAN-Datenbank eingeführt, um VTP-Updates für VTP-Clients und -Server sofort zu speichern. In einigen Softwareversionen besteht diese VLAN-Datenbank in Form einer separaten Datei im NVRAM, der Datei "vlan.dat". Überprüfen Sie Ihre Softwareversion, um festzustellen, ob eine Sicherung der VLAN-Datenbank erforderlich ist. Wenn Sie den Befehl **show vtp status** ausführen, können Sie VTP/VLAN-Informationen anzeigen, die in der Datei "vlan.dat" für den VTP-Client oder den VTP-Server gespeichert sind.

Die gesamte VTP/VLAN-Konfiguration wird nicht in der Startkonfigurationsdatei im NVRAM gespeichert, wenn Sie den Befehl **copy run start** auf diesen Systemen ausführen. Dies gilt nicht für Systeme, die als VTP-transparent ausgeführt werden. Bei VTP-transparenten Systemen wird die gesamte VTP/VLAN-Konfiguration in der Startkonfigurationsdatei im NVRAM gespeichert, wenn Sie den Befehl **copy run start** ausführen.

In Cisco IOS Software-Versionen, die älter sind als die Cisco IOS-Softwareversion 12.1(11b)E, können Sie VTP und VLANs nur über den VLAN-Datenbankmodus konfigurieren. Der VLAN-Datenbankmodus ist ein separater Modus vom globalen Konfigurationsmodus. Der Grund für diese Konfigurationsanforderung ist, dass VTP-Nachbarn bei der Konfiguration des Geräts im VTP-Modus-Server oder VTP-Modus-Client die VLAN-Datenbank dynamisch über VTP-Meldungen aktualisieren können. Diese Updates sollen nicht automatisch an die Konfiguration

weitergeleitet werden. Daher werden die VLAN-Datenbank und die VTP-Informationen nicht in der Hauptkonfiguration gespeichert, sondern im NVRAM in einer Datei mit dem Namen vlan.dat.

Dieses Beispiel zeigt, wie ein Ethernet-VLAN im VLAN-Datenbankmodus erstellt wird:

```
Switch#vlan database
Switch(vlan)#vlan 3
VLAN 3 added:
Name: VLAN0003
Switch(vlan)#exit
APPLY completed.
Exiting....
```

In der Cisco IOS Software Version 12.1(11b)E und höher können Sie VTP und VLANs über den VLAN-Datenbankmodus oder den globalen Konfigurationsmodus konfigurieren. Im VTP-Modus-Server oder im transparenten VTP-Modus aktualisiert die Konfiguration der VLANs die Datei "vlan.dat" im NVRAM. Diese Befehle werden jedoch nicht in der Konfiguration gespeichert. Daher werden die Befehle in der aktuellen Konfiguration nicht angezeigt.

Weitere Informationen finden Sie im Abschnitt *VLAN-Konfiguration im globalen Konfigurationsmodus* im Dokument Konfigurieren von VLANs.

Dieses Beispiel zeigt, wie Sie ein Ethernet-VLAN im globalen Konfigurationsmodus erstellen und die Konfiguration überprüfen:

```
Switch#configure terminal
Switch(config#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config#vlan 3
Switch(config-vlan)#end
Switch#
OR
Switch#vlan database
Switch(vlan#vtp server
Switch device to VTP SERVER mode.
Switch(vlan#vlan 3
Switch(vlan#exit
APPLY completed.
Exiting....
Switch#
```

Hinweis: Die VLAN-Konfiguration wird in der Datei "vlan.dat" gespeichert, die im nichtflüchtigen Speicher gespeichert ist. Um eine vollständige Sicherung Ihrer Konfiguration durchzuführen, fügen Sie die Datei "vlan.dat" zusammen mit der Konfiguration in die Sicherung ein. Wenn dann der gesamte Switch oder das Supervisor Engine-Modul ersetzt werden muss, muss der Netzwerkadministrator beide Dateien hochladen, um die vollständige Konfiguration wiederherzustellen:

- Die Datei "vlan.dat"
- Die Konfigurationsdatei

VTP und erweiterte VLANs

Die Funktion Extended System ID (Erweiterte System-ID) wird verwendet, um die VLAN-Identifizierung mit erweitertem Bereich zu ermöglichen. Wenn die Extended System ID aktiviert ist, wird der Pool der für den VLAN Spanning Tree verwendeten MAC-Adressen deaktiviert und eine

einzige MAC-Adresse hinterlassen, die den Switch identifiziert. Die Catalyst IOS Software-Version 12.1(11b)EX und 12.1(13)E bieten erweiterte System-ID-Unterstützung für Catalyst 6000/6500, um 4096 VLANs gemäß IEEE 802.1Q-Standard zu unterstützen. Diese Funktion wurde in der Cisco IOS Software Release 12.1(12c)EW für Catalyst 4000-/4500-Switches eingeführt. Diese VLANs sind in mehrere Bereiche eingeteilt, die jeweils unterschiedlich verwendet werden können. Einige dieser VLANs werden bei Verwendung des VTP auf andere Switches im Netzwerk verteilt. Die VLANs mit erweitertem Bereich werden nicht propagiert, daher müssen Sie VLANs mit erweitertem Bereich manuell auf jedem Netzwerkgerät konfigurieren. Diese erweiterte System-ID-Funktion entspricht der MAC-Adressenreduzierungsfunktion in Catalyst OS.

In dieser Tabelle werden die VLAN-Bereiche beschrieben:

VLANs	Bereich	Verwendung	Wird durch VTP weitergeleitet?
0.4095	Reserviert	Nur zur Verwendung im System. Sie können diese VLANs nicht sehen oder verwenden.	—
1	Normal	Cisco Standard. Sie können dieses VLAN verwenden, aber nicht löschen.	Ja
2-1001	Normal	Für Ethernet-VLANs. Sie können diese VLANs erstellen, verwenden und löschen.	Ja
1002-1005	Normal	Cisco legt die Standardwerte für FDDI und Token Ring fest. Sie können die VLANs 1002-1005 nicht löschen.	Ja
1006-4094	Reserviert	Nur für Ethernet-VLANs.	Nein

Switch-Protokolle verwenden eine MAC-Adresse, die von einer Bank der verfügbaren Adressen übernommen wurde, die ein EPROM im Chassis als Teil von Bridge-IDs für VLANs bereitstellt, die unter PVST+ und RPVST+ ausgeführt werden. Die Catalyst 6000/6500- und Catalyst 4000/4500-Switches unterstützen entweder 1024- oder 64-MAC-Adressen, die vom Chassis-Typ abhängen.

Catalyst Switches mit 1024 MAC-Adressen aktivieren standardmäßig keine Extended System ID. MAC-Adressen werden sequenziell zugewiesen, wobei die erste MAC-Adresse im Bereich, der VLAN 1 zugewiesen ist, die zweite MAC-Adresse im Bereich, der VLAN 2 zugewiesen ist usw. Dadurch können die Switches 1024 VLANs unterstützen, und jedes VLAN verwendet eine eindeutige Bridge-ID.

Chassis-Typ	Chassis-Adresse
WS-C4003-S1, WS-C4006-S2	1024
WS-C4503, WS-C4506	64[1]
WS-C6509-E, WS-C6509, WS-C6509-NEB,	1024

WS-C6506-E, WS-C6506, WS-C6009, WS-C6006, OSR-760 9-AC, OSR-7609-DC	
WS-C6513, WS-C6509-NEB-A, WS-C6504-E, WS-C6503-E, WS-C6503, CISCO7603, CISCO7606, CISCO76 09, CISCO7613	64[1]

[1] Chassis mit 64 MAC-Adressen aktiviert standardmäßig die erweiterte System-ID, die jedoch nicht deaktiviert werden kann.

Weitere Informationen finden Sie im Abschnitt *Understanding the Bridge ID* (*Die Bridge-ID*) unter Konfigurieren von STP und IEEE 802.1s MST.

Für Switches der Catalyst-Serie mit 1024 MAC-Adressen ermöglicht die Aktivierung der Extended System ID die Unterstützung von 4096 VLANs, die unter PVST+ ausgeführt werden, oder von 16 MISTP-Instanzen, eindeutige IDs zu besitzen, ohne dass die Anzahl der für den Switch erforderlichen MAC-Adressen erhöht werden muss. Die erweiterte System-ID reduziert die Anzahl der für das STP erforderlichen MAC-Adressen von einer pro VLAN- oder MISTP-Instanz auf eine pro Switch.

Diese Abbildung zeigt die Bridge-ID, wenn die Extended System ID nicht aktiviert ist. Die Bridge-ID besteht aus einer 2-Byte-Bridge-Priorität und einer 6-Byte-MAC-Adresse.

Die erweiterte System-ID ändert die Spanning Tree Protocol (STP) Bridge Identifier-Komponente der Bridge Protocol Data Units (BPDU). Das ursprüngliche 2-Byte-Prioritätsfeld ist in 2 Felder unterteilt. Ein 4-Bit-Bridge-Prioritätsfeld und eine 12-Bit-System-ID-Erweiterung, die die VLAN-Nummerierung von 0-4095 ermöglicht.

Wenn die Extended System ID auf Catalyst Switches aktiviert ist, um VLANs mit erweitertem Bereich zu nutzen, muss sie auf allen Switches innerhalb derselben STP-Domäne aktiviert werden. Dies ist erforderlich, um die STP-Root-Berechnungen auf allen Switches konsistent zu halten. Wenn die Extended System ID aktiviert ist, wird die Root Bridge-Priorität zu einem Vielfachen von 4096 plus der VLAN-ID. Die Switches ohne Extended System ID können möglicherweise unbeabsichtigt Root beanspruchen, da sie bei der Auswahl ihrer Bridge-ID eine feinere Präzision aufweisen.

Es wird zwar empfohlen, eine konsistente Konfiguration der Extended System ID innerhalb derselben STP-Domäne beizubehalten, es ist jedoch nicht sinnvoll, die Extended System ID für alle Netzwerkgeräte durchzusetzen, wenn Sie neue Chassis mit 64 MAC-Adressen in die STP-Domäne einführen. Wenn zwei Systeme mit derselben Spanning-Tree-Priorität konfiguriert sind, ist es jedoch wichtig zu verstehen, dass das System ohne Extended System ID über eine bessere Spanning-Tree-Priorität verfügt. Führen Sie diesen Befehl aus, um die Konfiguration der erweiterten System-ID zu aktivieren:

Spanning-Tree Extended System-ID

Die internen VLANs werden in aufsteigender Reihenfolge zugewiesen, beginnend mit VLAN 1006. Es wird empfohlen, die Benutzer-VLANs möglichst nahe am VLAN 4094 zuzuweisen, um Konflikte zwischen den Benutzer-VLANs und den internen VLANs zu vermeiden. Geben Sie den Befehl **show vlan internal use** on a switch ein, um die intern zugewiesenen VLANs anzuzeigen.

```
Switch#show vlan internal usage

VLAN Usage
---- --------------------
1006 online diag vlan0
1007 online diag vlan1
1008 online diag vlan2
1009 online diag vlan3
1010 online diag vlan4
1011 online diag vlan5
1012 PM vlan process (trunk tagging)
1013 Port-channel100
1014 Control Plane Protection
1015 L3 multicast partial shortcuts for VPN 0
1016 vrf_0_vlan0
1017 Egress internal vlan
1018 Multicast VPN 0 QOS vlan
1019 IPv6 Multicast Egress multicast
1020 GigabitEthernet5/1
1021 ATM7/0/0
1022 ATM7/0/0.1
1023 FastEthernet3/1
1024 FastEthernet3/2
------deleted------
```

In nativem IOS kann die **absteigende VLAN-Zuweisungsrichtlinie** so konfiguriert werden, dass die internen VLANs in absteigender Reihenfolge zugewiesen werden. Das CLI-Äquivalent für CatOS-Software wird nicht offiziell unterstützt.

VLAN-interne Zuweisungsrichtlinie absteigend

[Cisco Konfigurationsempfehlung]

VLANs können erstellt werden, wenn sich ein Catalyst 6500/6000 im VTP-Servermodus befindet, selbst wenn der VTP-Domänenname fehlt. Konfigurieren Sie zuerst den VTP-Domänennamen, bevor Sie VLANs auf Catalyst 6500/6000-Switches konfigurieren, auf denen die Cisco IOS-Systemsoftware ausgeführt wird. Die Konfiguration in dieser Reihenfolge gewährleistet Konsistenz mit anderen Catalyst Switches, auf denen CatOS ausgeführt wird.

Es gibt keine spezifische Empfehlung, ob der VTP-Client/Server-Modus oder der VTP-`transparente` Modus verwendet werden sollen. Einige Kunden bevorzugen trotz einiger Überlegungen, die in diesem Abschnitt angeführt werden, die einfache Verwaltung des VTP-Client/Server-Modus. Aus Redundanzgründen sollten in jeder Domäne zwei Switches im Servermodus vorhanden sein, in der Regel die beiden Switches auf dem Distribution Layer. Legen Sie für die übrigen Switches in der Domäne den Client-Modus fest. Wenn Sie den Client/Server-Modus unter Verwendung von VTPv2 implementieren, sollten Sie bedenken, dass eine höhere Revisionsnummer immer in derselben VTP-Domäne akzeptiert wird. Wenn ein Switch, der entweder im VTP-Client- oder Servermodus konfiguriert ist, in die VTP-Domäne eingeführt wird und eine höhere Revisionsnummer hat als die vorhandenen VTP-Server, wird die VLAN-Datenbank in der VTP-

Domäne überschrieben. Wenn die Konfigurationsänderung nicht beabsichtigt ist und VLANs gelöscht werden, kann diese Überschrift zu einem schwerwiegenden Netzwerkausfall führen. Um sicherzustellen, dass die Client- oder Server-Switches immer über eine Konfigurationsrevisionsnummer verfügen, die niedriger ist als die des Servers, ändern Sie den Client-VTP-Domänennamen in einen anderen als den Standardnamen, und kehren dann zum Standard zurück. Mit dieser Aktion wird die Konfigurationsversion auf dem Client auf 0 gesetzt.

Die VTP-Fähigkeit bietet Vor- und Nachteile, um problemlos Änderungen in einem Netzwerk durchzuführen. Viele Unternehmen bevorzugen einen vorsichtigen Ansatz und verwenden den VTP-`transparenten` Modus aus folgenden Gründen:

- Diese Vorgehensweise fördert eine gute Änderungskontrolle, da die Notwendigkeit, ein VLAN auf einem Switch oder Trunk-Port zu ändern, jeweils als ein Switch betrachtet werden muss.
- Der transparente VTP-Modus schränkt das Risiko eines Administratorfehlers ein, z. B. das versehentliche Löschen eines VLAN. Solche Fehler können sich auf die gesamte Domäne auswirken.
- VLANs können von Trunks nach unten zu Switches ohne Ports im VLAN abgeschnitten werden. Dies führt zu einer höheren Bandbreiteneffizienz bei Frame-Flooding. Die manuelle Beschneidung hat auch einen reduzierten Spanning-Tree-Durchmesser. Weitere Informationen finden Sie im Abschnitt Dynamic Trunking Protocol. Eine Switch-basierte VLAN-Konfiguration unterstützt diese Vorgehensweise ebenfalls.
- Es besteht kein Risiko, dass ein neuer Switch mit einer höheren VTP-Revisionsnummer in das Netzwerk eingeführt wird, der die gesamte Domänen-VLAN-Konfiguration überschreibt.
- Der transparente VTP-Modus der Cisco IOS Software wird in Campus Manager 3.2 unterstützt, der Teil von CiscoWorks2000 ist. Die frühere Einschränkung, dass mindestens ein Server in einer VTP-Domäne erforderlich ist, wurde entfernt.

VTP-Befehle	Kommentare
VTP-*Domänenname*	CDP überprüft den Namen, um eine fehlerhafte Verkabelung zwischen den Domänen zu verhindern. Bei Domänennamen wird Groß- und Kleinschreibung unterschieden.
VTP-Modus {Server | Kunde | transparent}	VTP wird in einem der drei Modi betrieben.
vlan *vlan_number*	Dadurch wird ein VLAN mit der angegebenen ID erstellt.
switchport trunk allowed *vlan_range*	Dies ist ein Schnittstellenbefehl, mit dem Trunks VLANs bei Bedarf übertragen können. Der Standardwert ist "alle VLANs".
switchport trunk pruning	Dies ist ein Schnittstellenbefehl, der den STP-Durchmesser durch manuelles Bereinigen begrenzt, z. B. auf Trunks vom Distribution

vlan_range	Layer zum Access Layer, wo das VLAN nicht vorhanden ist. In der Standardeinstellung sind alle VLANs für die Bereinigung zulässig.

Weitere Optionen

VTPv2 ist eine Anforderung in Token Ring-Umgebungen, in denen der Client/Server-Modus dringend empfohlen wird.

Im Abschnitt Cisco Konfigurationsempfehlungen dieses Dokuments werden die Vorteile der Beschneidung von VLANs empfohlen, um unnötiges Frame-Flooding zu vermeiden. Der Befehl **vtp pruning** löscht VLANs automatisch, wodurch das ineffiziente Flooding von Frames, die nicht benötigt werden, verhindert wird.

Hinweis: Anders als bei manueller VLAN-Bereinigung wird der Spanning-Tree-Durchmesser durch automatisches Beschneiden nicht begrenzt.

Die IEEE hat eine standardbasierte Architektur entwickelt, um VTP-ähnliche Ergebnisse zu erzielen. Als Mitglied des 802.1Q Generic Attribute Registration Protocol (GARP) ermöglicht das Generic VLAN Registration Protocol (GVRP) die Interoperabilität der VLAN-Verwaltung zwischen Anbietern. GVRP ist jedoch nicht Bestandteil dieses Dokuments.

Hinweis: Die Cisco IOS Software bietet keine Funktion für den VTP-Aus-Modus und unterstützt nur VTPv1 und VTPv2 mit Bereinigung.

Fast Ethernet-Autonegotiation

Zweck

Die Autonegotiation ist eine optionale Funktion des IEEE 802.3u Fast Ethernet (FE) Standards. Die Autonegotiation ermöglicht Geräten den automatischen Austausch von Informationen über Geschwindigkeit und Duplexfunktionen über eine Verbindung. Die Autonegotiation wird auf Layer 1 (L1) ausgeführt. Die Funktion ist auf Ports ausgerichtet, die Bereichen zugewiesen sind, in denen transiente Benutzer oder Geräte mit einem Netzwerk verbunden sind. Beispiele sind Access-Layer-Switches und -Hubs.

Überblick

Bei der Autonegotiation wird eine modifizierte Version des Link-Integritätstests für 10BASE-T-Geräte verwendet, um die Geschwindigkeit auszuhandeln und andere Autonegotiationsparameter auszutauschen. Der ursprüngliche 10BASE-T-Verbindungstest wird als Normal Link Pulse (NLP) bezeichnet. Die geänderte Version des Verbindungstests für die automatische Aushandlung mit 10/100 Mbit/s wird als Fast Link Pulse (FLP) bezeichnet. Die 10BASE-T-Geräte erwarten im Rahmen des Verbindungstests einen Burst-Puls alle 16 (+/-8) Millisekunden (ms). Bei der 10/100-Mbit/s-Autoübertragung sendet FLP diese Bursts alle 16 (+/-8) ms mit den zusätzlichen Impulsen alle 62,5 (+/-7) Mikrosekunden. Die Impulse innerhalb der Burst-Sequenz generieren Codewörter, die für den Kompatibilitätsaustausch zwischen Link-Partnern verwendet werden.

Bei 10BASE-T wird bei jedem Start einer Station ein Link Puls gesendet. Dies ist ein einzelner Impuls, der alle 16 ms gesendet wird. Die 10BASE-T-Geräte senden auch bei Inaktivität der Verbindung alle 16 ms einen Verbindungsimpuls. Diese Verbindungsimpulse werden auch als

Heartbeat oder NLP bezeichnet.

Ein 100BASE-T-Gerät sendet FLP. Dieser Puls wird als Burst anstatt als Impuls gesendet. Der Burst ist innerhalb von 2 ms abgeschlossen und wird alle 16 ms wiederholt. Nach der Initialisierung überträgt das Gerät dem Verbindungspartner eine 16-Bit-FLP-Nachricht für die Aushandlung von Geschwindigkeit, Duplex und Flusssteuerung. Diese 16-Bit-Nachricht wird wiederholt gesendet, bis die Nachricht vom Partner bestätigt wurde.

Hinweis: Gemäß der IEEE 802.3u-Spezifikation können Sie einen Verbindungspartner nicht manuell für 100-Mbit/s-Vollduplex konfigurieren und trotzdem mit dem anderen Verbindungspartner eine Vollduplex-Verhandlung durchführen. Wenn Sie versuchen, einen Verbindungspartner für 100-Mbit/s-Vollduplex zu konfigurieren, und der andere Verbindungspartner für die Autonegotiation, führt dies zu einer Duplexungleichheit. Duplex-Inkongruenzen werden erzielt, da ein Verbindungspartner automatisch verhandelt und keine Autonegotiationsparameter vom anderen Verbindungspartner angezeigt werden. Der erste Verbindungspartner verwendet dann standardmäßig Halbduplex.

Alle Catalyst 6500 Ethernet-Switching-Module unterstützen 10/100 Mbit/s und Halbduplex oder Vollduplex. Geben Sie den Befehl **show interface functions** (Schnittstellenfunktionen anzeigen) ein, um diese Funktionalität auf anderen Catalyst Switches zu überprüfen.

Eine der häufigsten Ursachen für Leistungsprobleme bei 10/100-Mbit/s-Ethernet-Verbindungen tritt auf, wenn ein Port an der Verbindung mit Halbduplex betrieben wird, während der andere Port mit Vollduplex betrieben wird. Diese Situation tritt gelegentlich ein, wenn Sie einen oder beide Ports auf eine Verbindung zurücksetzen, und der Verhandlungsprozess führt nicht zu derselben Konfiguration für beide Verbindungspartner. Die Situation tritt auch ein, wenn Sie die eine Seite einer Verbindung neu konfigurieren und vergessen, die andere Seite neu zu konfigurieren. Sie können es vermeiden, leistungsbezogene Support-Anrufe zu tätigen, wenn Sie:

- Erstellen einer Richtlinie, die die Konfiguration von Ports für das erforderliche Verhalten aller nicht-transienten Geräte erfordert
- Durchsetzung der Politik durch angemessene Maßnahmen zur Änderungskontrolle

Typische Symptome des Leistungsproblems sind eine Erhöhung der Frame-Check-Sequenz (FCS), eine zyklische Redundanzprüfung (CRC), eine Ausrichtung oder laufende Zähler am Switch.

Im Halbduplex-Modus verfügen Sie über ein Paar Empfangsdrähte und ein Paar Übertragungsdrähte. Beide Drähte können nicht gleichzeitig verwendet werden. Das Gerät kann keine Übertragung durchführen, wenn ein Paket auf der Empfangsseite vorhanden ist.

Im Vollduplex-Modus verfügen Sie über das gleiche Empfangs- und Übertragungskabel. Beide können jedoch gleichzeitig verwendet werden, da die Funktionen Carrier Sense und Collision Detect deaktiviert wurden. Das Gerät kann gleichzeitig senden und empfangen.

Aus diesem Grund funktioniert eine Halb-Duplex-Vollduplex-Verbindung, aber es gibt eine große Anzahl von Kollisionen auf der Halb-Duplex-Seite, die zu einer schlechten Leistung führen. Die Kollisionen treten auf, weil das als Vollduplex konfigurierte Gerät Daten gleichzeitig übertragen kann.

Die Dokumente in dieser Liste besprechen die Autonegotiation im Detail. In diesen Dokumenten wird erklärt, wie die Autonegotiation funktioniert, und es werden verschiedene Konfigurationsoptionen erörtert:

- Konfiguration und Fehlerbehebung für Ethernet 10/100/1000MB Half/Vollduplex Auto-Negotiation
- Beheben von Problemen mit der NIC-Kompatibilität bei Cisco Catalyst Switches

Ein häufiges Missverständnis bei der Autoübertragung besteht darin, dass es möglich ist, einen Verbindungspartner für 100-Mbit/s-Vollduplex manuell zu konfigurieren und mit dem anderen Verbindungspartner automatisch Vollduplex auszuhandeln. Tatsächlich führt ein Versuch, dies zu einer Duplexungleichheit. Dies hat zur Folge, dass ein Verbindungspartner automatisch verhandelt, keine Auto-Negotiation-Parameter des anderen Verbindungspartners sieht und standardmäßig Halbduplex verwendet.

Die meisten Catalyst Ethernet-Module unterstützen 10/100 Mbit/s und Halbduplex/Vollduplex. Sie können dies jedoch bestätigen, wenn Sie den Befehl **show interface mod *[/port]* functions (Schnittstellenmodus*/Port*-Funktionen anzeigen**) ausführen.

FEFI

Far End Failure Indications (FEFI) schützt 100BASE-FX (Glasfaser)- und Gigabit-Schnittstellen, während die Autoübertragung 100BASE-TX (Kupfer) gegen physische Layer-/Signalisierungsfehler schützt.

Ein Fehler am anderen Ende ist ein Fehler in der Verbindung, die eine Station erkennen kann, die andere Station nicht. Ein nicht verbundenes Übertragungskabel ist ein Beispiel. In diesem Beispiel erhält die Sendestation noch gültige Daten und stellt fest, dass die Verbindung über den Link-Integritätsmonitor gut funktioniert. Die Sendestation kann jedoch nicht feststellen, dass die andere Station die Übertragung nicht empfängt. Eine 100BASE-FX-Station, die einen solchen Remote-Fehler erkennt, kann den übertragenen `IDLE`-Stream ändern, um ein spezielles Bitmuster zu senden, um den Nachbarn über den Remote-Fehler zu informieren. Das spezielle Bitmuster wird als `FEFI-IDLE`-Muster bezeichnet. Das `FEFI-IDLE`-Muster löst anschließend ein Herunterfahren des Remote-Ports (`errDisable`) aus. Weitere Informationen zum Schutz vor Fehlern finden Sie im Abschnitt UniDirectional Link Detection dieses Dokuments.

Diese Module/Hardware unterstützen FEFI:

- Catalyst 6500/6000 und 4500/4000:Alle 100BASE-FX-Module und GE-Module

Cisco Infrastruktur-Port-Empfehlung

Ob die Autoübertragung auf 10/100-Mbit/s-Verbindungen oder auf Geschwindigkeit und Duplex des Codes konfiguriert werden soll, hängt letztendlich vom Verbindungspartner oder vom Endgerät ab, das Sie mit einem Catalyst Switch-Port verbunden haben. Die Autonegotiation zwischen Endgeräten und Catalyst Switches funktioniert im Allgemeinen gut, und Catalyst Switches sind mit der IEEE 802.3u-Spezifikation konform. Wenn jedoch die Switches der Netzwerkschnittstellenkarte (NIC) oder des Anbieters nicht genau übereinstimmen, können Probleme auftreten. Darüber hinaus können anbieterspezifische erweiterte Funktionen, die nicht in der IEEE 802.3u-Spezifikation für die 10/100-Mbit/s-Autoübertragung beschrieben sind, zu Hardwarekompatibilität und anderen Problemen führen. Zu diesen erweiterten Funktionen gehören die Autopolarität und die Kabelintegrität. Dieses Dokument enthält ein Beispiel:

- Feldwarnung: Leistungsproblem bei Intel Pro/1000T NICs, die mit CAT4K/6K verbunden sind

In einigen Situationen müssen Sie Host, Portgeschwindigkeit und Duplex einstellen. Führen Sie im Allgemeinen die folgenden grundlegenden Schritte zur Fehlerbehebung aus:

- Stellen Sie sicher, dass die Autonegotiation auf beiden Seiten der Verbindung konfiguriert ist oder dass die feste Kodierung auf beiden Seiten konfiguriert ist.
- In den Versionshinweisen finden Sie allgemeine Hinweise.
- Überprüfen Sie die Version des Netzwerkkartentreibers oder -betriebssystems, die Sie ausführen. Oft ist der aktuelle Treiber oder Patch erforderlich.

Verwenden Sie in der Regel zunächst die Autonegotiation für jeden Verbindungspartner. Die Konfiguration der automatischen Verhandlung für transiente Geräte wie Laptops bietet eindeutige Vorteile. Die Autonegotiation funktioniert auch mit anderen Geräten gut, z. B.:

- Mit nicht-transienten Geräten wie Servern und festen Workstations
- Vom Switch zum Switch
- Vom Switch zum Router

Aber aus einigen der in diesem Abschnitt erwähnten Gründe können Verhandlungsthemen entstehen. Unter Konfiguration und Fehlerbehebung von Ethernet 10/100/1000MB Half/Full Duplex Auto-Negotiation finden Sie grundlegende Schritte zur Fehlerbehebung in diesen Fällen.

Autonegotiation für deaktivieren:

- Ports, die Netzwerkinfrastrukturgeräte wie Switches und Router unterstützen
- Andere nicht-transiente Endsysteme wie Server und Drucker

Stets die Geschwindigkeit und die Duplexeinstellungen für diese Ports festschreiben.

Konfigurieren Sie diese 10/100-Mbit/s-Verbindungskonfigurationen manuell für Geschwindigkeit und Duplex, bei denen es sich in der Regel um Vollduplex mit 100 Mbit/s handelt:

- Switch-to-Switch
- Switch-to-Server
- Switch-to-Router

Wenn die Portgeschwindigkeit auf Auto für einen 10/100-Mbit/s-Ethernet-Port eingestellt ist, werden Geschwindigkeit und Duplex automatisch verhandelt. Geben Sie diesen Schnittstellenbefehl ein, um den Port auf Auto (Automatisch) festzulegen:

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed auto
!--- This is the default.
```

Führen Sie die folgenden Schnittstellenbefehle aus, um Geschwindigkeit und Duplex zu konfigurieren:

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed {10 | 100 | auto}
Switch(config-if)#duplex {full | half}
```

Empfehlungen für Cisco Access Ports

Endbenutzer, mobile Mitarbeiter und transiente Hosts müssen autonome Verhandlungen führen, um das Management dieser Hosts auf ein Minimum zu reduzieren. Sie können die Autonegotiation auch mit Catalyst Switches durchführen. Häufig werden die neuesten NIC-Treiber benötigt.

Führen Sie diese globalen Befehle aus, um die automatische Verhandlung der Geschwindigkeit

für den Port zu ermöglichen:

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed auto
```

Hinweis: Wenn Sie die Portgeschwindigkeit auf Auto für einen 10/100-Mbit/s-Ethernet-Port festlegen, werden sowohl Geschwindigkeit als auch Duplex automatisch verhandelt. Sie können den Duplexmodus von Auto-Negotiation-Ports nicht ändern.

Wenn NICs oder anbieterspezifische Switches nicht genau der IEEE-Spezifikation 802.3u entsprechen, können Probleme auftreten. Darüber hinaus können anbieterspezifische erweiterte Funktionen, die nicht in der IEEE 802.3u-Spezifikation für die 10/100-Mbit/s-Autoübertragung beschrieben sind, zu Hardwarekompatibilität und anderen Problemen führen. Zu diesen erweiterten Funktionen gehören die Autopolarität und die Kabelintegrität.

Weitere Optionen

Wenn die automatische Verhandlung zwischen Switches deaktiviert ist, kann bei bestimmten Problemen auch die Layer-1-Fehleranzeige verloren gehen. Verwenden Sie Layer-2-Protokolle, um die Fehlererkennung zu verbessern, z. B. aggressive UDLD.

Die Autonegotiation erkennt diese Situationen nicht, auch wenn die Autoübertragung aktiviert ist:

- Die Ports bleiben hängen und empfangen oder übertragen sie nicht.
- Eine Seite der Linie ist oben, die andere Seite jedoch nicht mehr.
- Glasfaserkabel sind verdrahtet

Bei der Autonegotiation werden diese Probleme nicht erkannt, da sie sich nicht auf der physischen Ebene befinden. Die Probleme können zu STP-Schleifen oder Datenverkehrslöchern führen.

UDLD kann all diese Fälle erkennen und beide Ports auf der Verbindung errdisable, wenn UDLD auf beiden Seiten konfiguriert ist. Auf diese Weise verhindert UDLD STP-Schleifen und schwarze Datenverkehrslöcher.

Gigabit Ethernet-Autonegotiation

Zweck

Gigabit Ethernet (GE) verfügt über ein umfassenderes Verfahren als das Verfahren für 10/100-Mbit/s-Ethernet (IEEE 802.3z). Bei GE-Ports wird die Autonegotiation für den Austausch von folgenden Elementen verwendet:

- Flusssteuerungsparameter
- Remote-Fehlerinformationen
- Duplex-Informationen**Hinweis:** GE-Ports der Catalyst-Serie unterstützen nur den Vollduplex-Modus.

IEEE 802.3z wurde durch die Spezifikationen IEEE 802.3:2000 ersetzt. Weitere Informationen finden Sie im Local and Metropolitan Area Networks + Drafts (LAN/MAN 802s) Standards Subscription .

Überblick

Im Gegensatz zur Autoübertragung mit 10/100-Mbit/s-FE beinhaltet die GE-Autonegotiation keine Verhandlung der Portgeschwindigkeit. Außerdem können Sie den Befehl **set port speed (Portgeschwindigkeit festlegen)** nicht ausführen, um die Autonegotiation zu deaktivieren. Die GE-Port-Aushandlung ist standardmäßig aktiviert, und die Ports an beiden Enden einer GE-Verbindung müssen die gleiche Einstellung haben. Die Verbindung wird nicht angezeigt, wenn die Ports an den einzelnen Enden der Verbindung inkonsistent eingestellt sind, was bedeutet, dass die ausgetauschten Parameter unterschiedlich sind.

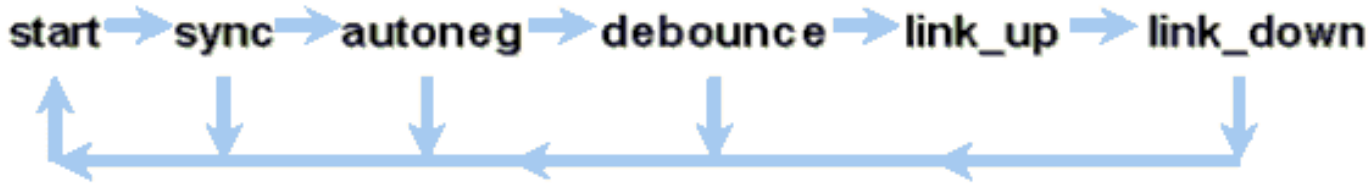
Beispiel: Es gibt zwei Geräte, A und B. Auf jedem Gerät kann die automatische Verhandlung aktiviert oder deaktiviert sein. Diese Tabelle enthält mögliche Konfigurationen mit den jeweiligen Verbindungsstatus:

Verhandlung	B Aktiviert	B Deaktiviert
A Aktiviert	`nach oben` auf beiden Seiten	A `Down`, B `Up`
Eine Deaktivierung	A `up`, B `down`	`nach oben` auf beiden Seiten

In GE werden Synchronisierung und Autonegotiation (sofern aktiviert) beim Start der Verbindung mithilfe einer speziellen Sequenz reservierter Link-Code-Wörter ausgeführt.

Hinweis: Es gibt ein Wörterbuch gültiger Wörter, und nicht alle möglichen Wörter sind in GE gültig.

Die Lebensdauer einer GE-Verbindung kann folgendermaßen charakterisiert werden:



Ein Synchronisierungsverlust bedeutet, dass die MAC eine Verbindung nicht erkennt. Der Synchronisierungsverlust gilt unabhängig davon, ob die Autoübertragung aktiviert oder deaktiviert ist. Die Synchronisierung geht unter bestimmten Fehlern verloren, z. B. beim Empfang von drei ungültigen Wörtern in Folge. Wenn diese Bedingung 10 ms lang andauert, wird eine Bedingung für den Synchronisierungsfehler geltend gemacht, und der Link wird in den Status `link_down` geändert. Nach der Synchronisierung sind drei weitere gültige Inaktivitäten erforderlich, um neu synchronisiert zu werden. Andere Katastrophen, wie z. B. ein Verlust des Empfangssignals (Rx), verursachen ein Link-Down-Ereignis.

Die Autonegotiation ist Teil des Verbindungsprozesses. Wenn die Verbindung aktiv ist, ist die Autoverhandlungen beendet. Der Switch überwacht jedoch weiterhin den Verbindungsstatus. Wenn die Autoübertragung auf einem Port deaktiviert ist, ist die Autoübertragung nicht mehr möglich.

Die GE-Kupferspezifikation (1000BASE-T) unterstützt die Autonegotiation über einen Next Page Exchange. Next Page Exchange ermöglicht die automatische Verhandlung für Geschwindigkeiten von 10/100/1000 Mbit/s an Kupferports.

Hinweis: Die GE-Glasfaserspezifikation enthält jedoch nur Bestimmungen für die Aushandlung

von Duplex, Flusssteuerung und Remote-Fehlererkennung. GE-Glasfaserports handeln die Portgeschwindigkeit nicht aus. Weitere Informationen zur Autonegotiation finden Sie in den Abschnitten 28 und 37 der Spezifikation IEEE 802.3-2002 .

Die Verzögerung des Synchronisierungsneustarts ist eine Softwarefunktion, die die gesamte Autonegotiationszeit steuert. Wenn die Autoübertragung innerhalb dieser Zeit nicht erfolgreich ist, startet die Firmware die Autonegotiation neu, falls ein Deadlock auftritt. Der Befehl **sync-restart-delay** hat nur Auswirkungen, wenn die Option Autoübertragung aktiviert ist.

Cisco Infrastruktur-Port-Empfehlung

Die Konfiguration der Autoübertragung ist in einer GE-Umgebung wesentlich wichtiger als in einer 10/100-Mbit/s-Umgebung. Deaktivieren Sie die automatische Verhandlung nur in folgenden Situationen:

- An Switch-Ports, die an Geräte angeschlossen sind, die die Aushandlung nicht unterstützen können
- Wenn Verbindungsprobleme aufgrund von Interoperabilitätsproblemen auftreten

Aktivieren Sie die Gigabit-Aushandlung auf allen Switch-to-Switch-Verbindungen und generell auf allen GE-Geräten. Der Standardwert für Gigabit-Schnittstellen ist Autoübertragung. Führen Sie diesen Befehl dennoch aus, um sicherzustellen, dass die Autonegotiation aktiviert ist:

```
switch(config)#interface type slot/port
switch(config-If)#no speed
!--- This command sets the port to autonegotiate Gigabit parameters.
```

Eine bekannte Ausnahme ist die Verbindung mit einem Gigabit Switch Router (GSR), der Cisco IOS Software ausführt, die älter ist als die Cisco IOS Software Release 12.0(10)S, die Flusssteuerung und Autoübertragung hinzugefügt hat. Schalten Sie in diesem Fall diese beiden Funktionen aus. Wenn Sie diese Funktionen nicht ausschalten, meldet der Switch-Port keine Verbindung, und der GSR meldet Fehler. Dies ist eine Beispielbefehlsfolge für die Benutzeroberfläche:

```
flowcontrol receive off
flowcontrol send off
speed nonegotiate
```

Empfehlungen für Cisco Access Ports

Da FLPs von Anbieter zu Anbieter unterschiedlich sein können, müssen Sie die Switch-to-Server-Verbindungen von Fall zu Fall betrachten. Bei Cisco Kunden traten bei Gigabit-Aushandlung für Sun-, HP- und IBM-Server einige Probleme auf. Lassen Sie alle Geräte die Gigabit-Autoübertragung verhandeln, es sei denn, der NIC-Anbieter gibt ausdrücklich etwas Anderes an.

Weitere Optionen

Die Flusssteuerung ist ein optionaler Teil der 802.3x-Spezifikation. Flusskontrolle muss ausgehandelt werden, wenn Sie sie verwenden. Geräte können oder können möglicherweise einen PAUSE-Frame senden und/oder darauf reagieren (bekannte MAC 01-80-C2-00-00-00 0F). Und die Geräte können der Flusskontrollanforderung des Nachbarn am anderen Ende

möglicherweise nicht zustimmen. Ein Port mit einem zu füllenden Eingangspuffer sendet einen PAUSE-Frame an den Verbindungspartner. Der Verbindungspartner beendet die Übertragung und hält alle zusätzlichen Frames in den Ausgabepuffern des Verbindungspartners. Diese Funktion löst kein Problem mit Überbelegung im Dauerzustand. Die Funktion macht den Eingangspuffer jedoch effektiv um einen Bruchteil des Partner-Ausgabepuffers während des Bursts größer.

Die PAUSE-Funktion soll verhindern, dass eingehende Frames von Geräten (Switches, Routern oder Endstationen) aufgrund von Pufferüberlaufbedingungen, die eine kurzfristige Überlastung des vorübergehenden Datenverkehrs verursachen, unnötig verworfen werden. Ein Gerät mit Datenverkehrsüberlastung verhindert einen internen Pufferüberlauf, wenn das Gerät einen PAUSE-Frame sendet. Der PAUSE-Frame enthält einen Parameter, der angibt, wie lange der Vollduplex-Partner warten muss, bevor der Partner weitere Daten-Frames sendet. Der Partner, der den PAUSE-Frame empfängt, sendet für den angegebenen Zeitraum keine Daten mehr. Wenn dieser Timer abläuft, beginnt die Station erneut, Datenframes zu senden, von wo aus die Station abgeschaltet wurde.

Eine Station, die eine PAUSE ausgibt, kann einen anderen PAUSE-Frame ausgeben, der einen Parameter von null Zeit enthält. Durch diese Aktion wird der restliche Pausenzeitraum abgebrochen. Ein neu empfangener PAUSE-Frame überschreibt also alle derzeit laufenden PAUSE-Operationen. Die Station, die den PAUSE-Frame ausgibt, kann außerdem die PAUSE-Zeit verlängern. Die Station gibt einen weiteren PAUSE-Frame aus, der einen Nicht-Nullzeitparameter vor Ablauf der ersten PAUSE-Periode enthält.

Dieser PAUSE-Vorgang ist keine datenflussbasierte Flusskontrolle. Der Vorgang ist ein einfacher Start-Stopp-Mechanismus, der dem Gerät, das den PAUSE-Frame gesendet hat, die Möglichkeit gibt, die Pufferüberlastung zu reduzieren.

Diese Funktion wird am besten für Verbindungen zwischen Access-Ports und End-Hosts verwendet, bei denen der Host-Ausgabepuffer potenziell so groß ist wie der virtuelle Speicher. Switch-to-Switch bietet nur begrenzte Vorteile.

Führen Sie folgende Schnittstellenbefehle aus, um dies an den Switch-Ports zu steuern:

```
flowcontrol {receive | send} {off | on | desired}
```

```
>show port flowcontrol

 Port  Send FlowControl    Receive FlowControl   RxPause TxPause
       admin    oper       admin    oper
-----  -------- --------   -------- --------     ------- -------
 6/1   off      off        on       on           0       0
 6/2   off      off        on       on           0       0
 6/3   off      off        on       on           0       0
```

Hinweis: Alle Catalyst-Module reagieren auf PAUSE-Frames, wenn sie ausgehandelt werden. Einige Module (z. B. WS-X5410 und WS-X4306) senden niemals Pausen-Frames, selbst wenn sie dies aushandeln, da sie nicht blockieren.

Dynamisches Trunking Protocol

Zweck

Um VLANs zwischen Geräten zu erweitern, identifizieren Trunks vorübergehend die ursprünglichen Ethernet-Frames und markieren (lokal anschließen) sie. Auf diese Weise können die Frames über eine einzelne Verbindung Multiplex-Modus betrieben werden. Außerdem wird sichergestellt, dass zwischen Switches separate VLAN-Broadcast- und Sicherheitsdomänen beibehalten werden. In den CAM-Tabellen wird die Zuordnung zwischen Frame und VLAN innerhalb der Switches beibehalten.

Überblick

DTP ist die zweite Generation von Dynamic ISL (DISL). DISL wird nur von ISL unterstützt. DTP unterstützt sowohl ISL als auch 802.1Q. Diese Unterstützung stellt sicher, dass die Switches an beiden Enden eines Trunks die verschiedenen Parameter von Trunking-Frames vereinbaren. Zu diesen Parametern gehören:

- Konfigurierter Kapselungstyp
- Natives VLAN
- Hardware-Funktionalität

Die DTP-Unterstützung trägt außerdem zum Schutz vor der Flutung getaggter Frames durch Nicht-Trunk-Ports bei, was ein potenziell schwerwiegendes Sicherheitsrisiko darstellt. DTP schützt vor solchen Überflutungen, da gewährleistet wird, dass sich die Ports und ihre Nachbarn in einem konsistenten Zustand befinden.

Trunking-Modus

DTP ist ein Layer-2-Protokoll, das Konfigurationsparameter zwischen einem Switch-Port und seinem Nachbarn aushandelt. DTP verwendet eine weitere bekannte Multicast-MAC-Adresse von 01-00-0c-cc-cc und einen SNAP-Protokolltyp von 0x2004. In dieser Tabelle werden die Funktionen für die einzelnen DTP-Verhandlungsmodi beschrieben:

Modus	Funktion	Übertragen von DTP-Frames?	Endzustand (Lokaler Port)
`Dynamisches Auto` (entspricht dem Modus `Auto` in CatOS)	Stellt den Port bereit, den Link in einen Trunk zu konvertieren. Der Port wird zu einem Trunk-Port, wenn der benachbarte Port `in den` bzw. den `wünschenswerten` Modus eingestellt ist.	Ja, regelmäßig	`Trunking`
`Trunk` (entspricht dem Modus `ON` in CatOS)	Versetzt den Port in den permanenten `Trunking`-Modus und versucht über Aushandlungen, den Link in einen Trunk umzuwandeln. Der Port wird zu einem	Ja, regelmäßig	`Trunking`, bedingungslos

	Trunk-Port, selbst wenn der benachbarte Port mit der Änderung nicht einverstanden ist.		
`unverhandeln`	Versetzt den Port in den permanenten `Trunking-`Modus, erlaubt dem Port jedoch nicht, DTP-Frames zu generieren. Sie müssen den benachbarten Port manuell als Trunk-Port konfigurieren, um eine Trunk-Verbindung herzustellen. Dies ist nützlich für Geräte, die kein DTP unterstützen.	Nein	`Trunking`, bedingungslos
`Dynamisch wünschenswert` (CatOS-ähnlicher Befehl ist `wünschenswert`)	Der Port versucht aktiv, den Link in einen Trunk-Link umzuwandeln. Der Port wird zu einem Trunk-Port, wenn der benachbarte Port `eingeschaltet` ist, `wünschenswert ist` oder `automatisch` aktiviert ist.	Ja, regelmäßig	Sie endet nur dann im `Trunking-`Zustand, wenn der Remote-Modus `eingeschaltet`, `automatisch` oder `wünschenswert` ist.
`Zugriff`	Versetzt den Port in den permanenten `Nicht-Trunking-`Modus und versucht über Aushandlungen, den Link in einen Nicht-Trunk-Link umzuwandeln. Der Port wird zu einem Nicht-Trunk-Port, selbst wenn der benachbarte Port der Änderung nicht zustimmt.	Nein, im Steady-State, sondern sendet Informationen, um die Fernerkennung nach einer Änderung von `On` zu beschleunigen.	`Nicht-Trunking`

Hinweis: Der ISL- und 802.1Q-Kapselungstyp kann eingestellt oder ausgehandelt werden.

In der Standardkonfiguration setzt DTP folgende Eigenschaften für die Verbindung voraus:

- Point-to-Point-Verbindungen und Cisco Geräte unterstützen 802.1Q-Trunk-Ports, die nur Punkt-zu-Punkt-Ports sind.
- Während der DTP-Aushandlung nehmen die Ports nicht am STP teil. Der Port wird dem STP erst hinzugefügt, nachdem der Port-Typ zu einem der folgenden drei Typen geworden ist:ZugriffISL802.1QPAgP ist der nächste Prozess, der ausgeführt wird, bevor der Port an STP teilnimmt. PAgP wird für die EtherChannel-Automatisierung verwendet.
- VLAN 1 ist immer auf dem Trunk-Port vorhanden. Wenn der Port im ISL-Modus als Trunking fungiert, werden DTP-Pakete in VLAN 1 gesendet. Wenn der Port im ISL-Modus kein Trunking durchführt, werden die DTP-Pakete im nativen VLAN gesendet (für 802.1Q-Trunking- oder Nicht-Trunking-Ports).
- DTP-Pakete übertragen den VTP-Domänennamen sowie die Trunk-Konfiguration und den Admin-Status. Der VTP-Domänenname muss übereinstimmen, damit ein ausgehandelter Trunk aktiviert werden kann. Diese Pakete werden während der Aushandlung alle zwei Sekunden und nach der Aushandlung alle 30 Sekunden gesendet. Wenn ein Port im `automatischen` oder `wünschenswerten` Modus ein DTP-Paket nicht innerhalb von 5 Minuten (min) erkennt, wird der Port als Nicht-Trunk festgelegt.

Achtung: Sie müssen verstehen, dass die Modi `Trunk`, `Unegotiate` und `Zugriff` explizit angeben, in welchem Zustand der Port endet. Eine fehlerhafte Konfiguration kann zu einem gefährlichen/inkonsistenten Zustand führen, in dem eine Seite Trunking und die andere keine Trunking-Komponente ist.

Weitere Informationen zu ISL finden Sie unter Konfigurieren von ISL-Trunking auf Catalyst Switches der Serien 5500/5000 und 6500/6000. Weitere Informationen zu 802.1Q-Kapselung mit Cisco CatOS-Systemsoftware finden Sie unter Trunking zwischen Catalyst Switches der Serien 4500/400, 5500/5000 und 6500/600.

Kapselungstyp

ISL-Übersicht

ISL ist ein proprietäres Trunking Protocol (VLAN Tagging Schema) von Cisco. ISL wird seit vielen Jahren eingesetzt. Im Gegensatz dazu ist 802.1Q viel neuer, aber 802.1Q ist der IEEE-Standard.

ISL kapselt den ursprünglichen Frame vollständig in ein zweistufiges Tagging-Schema ein. Auf diese Weise ist ISL praktisch ein Tunneling-Protokoll und überträgt als zusätzlichen Vorteil Frames, die nicht Ethernet-orientiert sind. ISL fügt dem standardmäßigen Ethernet-Frame einen 26-Byte-Header und einen 4-Byte-FCS hinzu. Ports, die als Trunks konfiguriert sind, erwarten und behandeln die größeren Ethernet-Frames. ISL unterstützt 1024 VLANs.

Frame-Format - ISL-Tag ist schattiert

40 Bits	4 Bits	4 Bits	48 Bits	16 Bits	24 Bits	24 Bits	15 Bits	1 Bit	16 Bits	16 Bits
DA	Type	USER	SA	LEN	SNAP LLC	HSA	VLAN	BPDU	INDEX	Reserve
01-00-0c-00-00					AAAA03	00000C				

Encapsulated Frame	FCS
Variable length	32 bits

Weitere Informationen finden Sie unter InterSwitch Link und IEEE 802.1Q Frame Format.

802.1Q - Betriebsübersicht

Obwohl der IEEE 802.1Q-Standard nur Ethernet betrifft, gibt der Standard viel mehr an als Kapselungstypen. 802.1Q umfasst neben anderen GARPs (Generic Attribute Registration Protocols) auch Spanning-Tree-Erweiterungen und 802.1p QoS-Tagging. Weitere Informationen finden Sie unter IEEE Standards Online .

Das 802.1Q-Frame-Format behält die ursprüngliche Ethernet SA und DA bei. Allerdings müssen Switches jetzt erwarten, dass sie selbst auf Zugriffsports mit großen Babyframes empfangen, wo Hosts Tagging verwenden können, um die 802.1p-Benutzerpriorität für die QoS-Signalisierung auszudrücken. Das Tag ist 4 Byte. Die 802.1Q Ethernet v2-Frames haben eine Größe von 1522 Byte. Dies ist eine Leistung der IEEE 802.3ac-Arbeitsgruppe. 802.1Q unterstützt außerdem Platz für 4096 VLANs.

Alle übertragenen und empfangenen Datenframes sind mit 802.1Q gekennzeichnet, mit Ausnahme der Datenframes, die sich im nativen VLAN befinden. In diesem Fall gibt es ein implizites Tag, das auf der Konfiguration des Eingangs-Switch-Ports basiert. Frames im nativen VLAN werden immer unmarkiert übertragen und werden normalerweise unmarkiert empfangen. Diese Frames können jedoch auch getaggt empfangen werden.

Weitere Informationen finden Sie in diesen Dokumenten:

- VLAN-Interoperabilität
- Trunking zwischen Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000 unter Verwendung von 802.1q-Kapselung mit Cisco CatOS-Systemsoftware

802.1Q/802.1p Frame-Format

		Tag Header						
		TPID	TCI					
48 bits	48 bits	16 bits	3 bits	1 bit	12 bits	16 bits	Variable length	32 bits
DA	SA	TPID	Priority	CFI	VLAN ID	Length/ Type	Data with PAD	FCS
		0x8100	0 – 7	0-1	0-4095			

Cisco Konfigurationsempfehlung

Ein Hauptziel des Cisco Designs ist die Konsistenz im Netzwerk, wo Konsistenz möglich ist. Alle neueren Catalyst-Produkte unterstützen 802.1Q und einige nur 802.1Q, z. B. ältere Module der Catalyst 4500/4000- und Catalyst 6500-Serien. Daher müssen alle neuen Implementierungen diesem IEEE 802.1Q-Standard entsprechen, und ältere Netzwerke müssen schrittweise von der ISL migrieren.

Führen Sie diese Schnittstellenbefehle aus, um das 802.1Q-Trunking an einem bestimmten Port zu aktivieren:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#switchport
!--- Configure the interface as a Layer 2 port. Switch(config-if)#switchport trunk encapsulation
dot1q
```

Der IEEE-Standard ermöglicht Anbieterinteroperabilität. Mit der Verfügbarkeit neuer 802.1p-fähiger Netzwerkkarten und Geräte ist die Interoperabilität mit Anbietern in allen Cisco Umgebungen von Vorteil. Obwohl sowohl die ISL- als auch die 802.1Q-Implementierung stabil sind, weist der IEEE-Standard letztendlich eine größere Außendienstbelastung auf und unterstützt einen größeren Drittanbieter-Support, der auch die Unterstützung von Netzwerkanalysen umfasst. Ein kleinerer Aspekt ist, dass der 802.1Q-Standard auch einen geringeren Kapselungsaufwand als ISL aufweist.

Aus Gründen der Vollständigkeit werden bei der impliziten Kennzeichnung nativer VLANs Sicherheitsaspekte berücksichtigt. Die Übertragung von Frames von einem VLAN, VLAN X, zu einem anderen VLAN, VLAN Y, ohne Router ist möglich. Die Übertragung kann ohne Router erfolgen, wenn sich der Quellport (VLAN X) im gleichen VLAN wie das native VLAN eines 802.1Q-Trunks auf demselben Switch befindet. Die Problemumgehung besteht darin, ein Dummy-VLAN für das native VLAN des Trunks zu verwenden.

Führen Sie diese Schnittstellenbefehle aus, um ein VLAN als nativ (Standard) für 802.1Q-Trunking an einem bestimmten Port einzurichten:

```
Switch(config)#interface type slot#/port#
Switch(config-If)#switchport trunk native vlan 999
```

Da alle neueren Hardwarekomponenten 802.1Q unterstützen, müssen alle neuen Implementierungen dem IEEE 802.1Q-Standard entsprechen und ältere Netzwerke schrittweise von ISL migrieren. Bis vor kurzem unterstützten viele Catalyst 4500/4000-Module ISL nicht. Daher ist 802.1Q die einzige Option für Ethernet-Trunking. Weitere Informationen finden Sie in der Ausgabe des Befehls **show interface functions** oder im Befehl **show port abilities** für CatOS. Da die Trunking-Unterstützung die entsprechende Hardware erfordert, kann ein Modul, das 802.1Q nicht unterstützt, 802.1Q niemals unterstützen. Ein Software-Upgrade bietet keine Unterstützung für 802.1Q. Die meisten neuen Hardwarekomponenten für die Catalyst Switches der Serien 6500/6000 und 4500/4000 unterstützen sowohl ISL als auch 802.1Q.

Wenn VLAN 1 aus einem Trunk gelöscht wird, wie im Abschnitt Switch Management Interface und Native VLAN beschrieben wird, werden zwar keine Benutzerdaten übertragen oder empfangen, aber der NMP besteht weiterhin die Steuerungsprotokolle für VLAN 1. Beispiele für Steuerungsprotokolle sind CDP und VTP.

Wie im VLAN 1-Abschnitt erläutert wird, werden CDP-, VTP- und PAgP-Pakete beim Trunking immer in VLAN 1 gesendet. Bei Verwendung der 802.1q-Kapselung (dot1q) werden diese Steuerungs-Frames mit VLAN 1 markiert, wenn das native VLAN des Switches geändert wird. Wenn das dot1q-Trunking zu einem Router und das native VLAN auf dem Switch geändert wird, ist eine Subschnittstelle in VLAN 1 erforderlich, um die getaggten CDP-Frames zu empfangen und die CDP-Nachbartransparenz auf dem Router bereitzustellen.

Hinweis: Bei dot1q besteht ein potenzieller Sicherheitsbezug, den das implizite Tagging des nativen VLANs verursacht. Die Übertragung von Frames von einem VLAN zu einem anderen ohne Router kann möglich sein. Weitere Informationen finden Sie in den Häufig gestellten Fragen zur Angriffserkennung. Die Lösung besteht darin, eine VLAN-ID für das native VLAN des Trunks zu verwenden, das nicht für den Endbenutzerzugriff verwendet wird. Um dies zu erreichen, verlassen die meisten Kunden von Cisco VLAN 1 einfach als natives VLAN auf einem Trunk und weisen Access Ports anderen VLANs als VLAN 1 zu.

Cisco empfiehlt eine explizite Trunk-Modus-Konfiguration der `dynamisch wünschenswert` an beiden Enden. Dieser Modus ist der Standardmodus. In diesem Modus können Netzwerkbetreiber Syslog- und Befehlszeilenstatusmeldungen darauf vertrauen, dass ein Port `aktiv` und Trunking ist. Dieser Modus unterscheidet sich vom `On`-Modus, wodurch ein Port angezeigt werden kann, auch wenn der Nachbar falsch konfiguriert ist. Darüber hinaus bieten `wünschenswerte` Modus-Trunks Stabilität in Situationen, in denen eine Seite der Verbindung nicht zu einem Trunk werden kann oder den `Trunk`-Zustand verwirft.

Wenn der Kapselungstyp zwischen Switches unter Verwendung von DTP ausgehandelt wird und ISL standardmäßig als Sieger ausgewählt wird, wenn beide Enden ihn unterstützen, müssen Sie diesen Schnittstellenbefehl ausführen, um dot1q[1] anzugeben:

```
switchport trunk encapsulation dot1q
```

[1] Bestimmte Module wie WS-X6548-GE-TX und WS-X6148-GE-TX unterstützen kein ISL-Trunking. Diese Module akzeptieren die **Trunk-Kapselung über** den Befehl **switchport *dot1q*** nicht.

Hinweis: Geben Sie den Befehl **switchport mode access** ein, um Trunks an einem Port zu deaktivieren. Diese Deaktivierung trägt dazu bei, verschwendete Verhandlungszeit beim Hochfahren von Host-Ports zu vermeiden.

```
Switch(config-if)#switchport host
```

Weitere Optionen

Eine weitere gängige Kundenkonfiguration verwendet den `dynamischen` Erwünschungsmodus auf dem Distribution Layer und die einfachste Standardkonfiguration (`dynamischer automatischer` Modus) auf dem Access Layer. Einige Switches wie der Catalyst 2900XL, Cisco IOS-Router oder andere Geräte anderer Anbieter unterstützen derzeit keine Trunk-Aushandlung über DTP. Sie können den `nicht verhandelbaren` Modus verwenden, um einen Port bedingungslos für einen Trunk mit diesen Geräten festzulegen. Dieser Modus ermöglicht die Standardisierung in einer gemeinsamen Umgebung auf dem gesamten Campus.

Cisco empfiehlt, `bei` der Verbindung mit einem Cisco IOS-Router keine Verhandlungen aufzunehmen. Während des Bridging können einige DTP-Frames, die von einem Port empfangen werden, der mit einem **Switch-Port-Modus-Trunk** konfiguriert ist, zum Trunk-Port zurückkehren. Beim Empfang des DTP-Frames versucht der Switch-Port, unnötigerweise neu zu verhandeln. Zur Neuverhandlung führt der Switch-Port den Trunk `herunter` und dann `hoch`. Wenn `Non-Negotiate` aktiviert ist, sendet der Switch keine DTP-Frames.

```
switch(config)#interface type slot#/port#
switch(config-if)#switchport mode dynamic desirable
!--- Configure the interface as trunking in desirable !--- mode for switch-to-switch links with
multiple VLANs. !--- And... switch(config-if)#switchport mode trunk
!--- Force the interface into trunk mode without negotiation of the trunk connection. !--- Or...
switch(config-if)#switchport nonegotiate
!--- Set trunking mode to not send DTP negotiation packets !--- for trunks to routers.
switch(config-if)#switchport access vlan vlan_number
!--- Configure a fallback VLAN for the interface. switch(config-if)#switchport trunk native vlan
999
!--- Set the native VLAN. switch(config-if)#switchport trunk allowed vlan vlan_number_or_range
!--- Configure the VLANs that are allowed on the trunk.
```

Spanning Tree Protocol

Zweck

Spanning Tree erhält eine schleifenfreie Layer-2-Umgebung in redundanten Switching- und Bridges-Netzwerken aufrecht. Ohne STP werden Frames auf unbestimmte Zeit schleifen und/oder multipliziert. Dieses Vorkommen verursacht einen Zusammenbruch des Netzwerks, da der hohe Datenverkehr alle Geräte in der Broadcast-Domäne unterbricht.

In mancher Hinsicht ist STP ein früheres Protokoll, das ursprünglich für langsame, softwarebasierte Bridge-Spezifikationen (IEEE 802.1D) entwickelt wurde. STP kann jedoch kompliziert sein, um es erfolgreich in großen Switch-Netzwerken zu implementieren, die über folgende Merkmale verfügen:

- Viele VLANs
- Viele Switches in einer Domäne
- Unterstützung mehrerer Anbieter
- Neuere IEEE-Erweiterungen

Die Cisco IOS-Systemsoftware hat neue STP-Entwicklungen übernommen. Neue IEEE-Standards wie 802.1w Rapid STP und 802.1s Multiple Spanning Tree-Protokolle ermöglichen schnelle Konvergenz, Lastverteilung und Skalierung auf Kontrollebene. Darüber hinaus bieten STP-Optimierungsfunktionen wie RootGuard, BPDU-Filterung, Portfast BPDU Guard und Loopguard zusätzlichen Schutz vor Layer-2-Weiterleitungsschleifen.

PVST+ - Übersicht über den Betrieb

Die Root-Bridge-Auswahl pro VLAN wird vom Switch mit der niedrigsten Root Bridge Identifier (BID) übernommen. Die BID ist die Bridge-Priorität in Kombination mit der Switch-MAC-Adresse.

Zunächst werden BPDUs von allen Switches gesendet und enthalten die BID jedes Switches sowie die Pfadkosten für die Verbindung mit diesem Switch. Dies ermöglicht die Bestimmung der Root-Bridge und des kostengünstigsten Pfads zum Root. Zusätzliche Konfigurationsparameter, die in BPDUs vom Root übertragen werden, überschreiben diese Parameter, die lokal konfiguriert sind, sodass das gesamte Netzwerk konsistente Timer verwendet. Für jede BPDU, die ein Switch vom Root empfängt, verarbeitet der Catalyst Central NMP eine neue BPDU und sendet sie mit den Root-Informationen heraus.

Die Topologie konvergiert dann über die folgenden Schritte:

1. Eine einzelne Root Bridge wird für die gesamte Spanning Tree-Domäne ausgewählt.
2. Auf jeder Non-Root-Bridge wird ein Root-Port (der zur Root-Bridge führt) ausgewählt.
3. Ein designierter Port wird für die BPDU-Weiterleitung auf jedem Segment ausgewählt.
4. Nicht designierte Ports werden blockiert.

Weitere Informationen finden Sie in diesen Dokumenten:

- Konfigurieren von STP und IEEE 802.1s MST
- Rapid Spanning Tree Protocol (802.1w)

Standard-Timer	Name	Funktion
2 Sek.	Hallo	Steuert die Abfahrt von BPDUs.
15 Sek.	Forward Delay (Fwd delay)	Steuert die Zeitdauer, die ein Port im `Überwachungs-` und `Lernstatus` verbringt, und beeinflusst den Topologieänderungsprozess.
20 Sek.	Maxime	Steuert die Zeitdauer, die der Switch die aktuelle Topologie aufrechterhält, bevor der Switch einen alternativen Pfad sucht. Nach der maximalen Alterungszeit (Maximal) gilt eine BPDU als veraltet und der Switch sucht einen neuen Root-Port aus dem Pool der blockierenden Ports.

		Wenn kein blockierter Port verfügbar ist, behauptet der Switch, der Root selbst an den designierten Ports zu sein.

Cisco empfiehlt, Timer nicht zu ändern, da dies die Stabilität beeinträchtigen kann. Die Mehrzahl der bereitgestellten Netzwerke ist nicht abgestimmt. Die einfachen STP-Timer, auf die über die Befehlszeile zugegriffen werden kann (z. B. Hello-Intervall, Maxage usw.), bestehen selbst aus einem komplexen Satz von anderen angenommenen und systeminternen Timern. Daher ist es schwierig, Timer einzustellen und alle Auswirkungen zu berücksichtigen. Darüber hinaus können Sie den UDLD-Schutz untergraben. Weitere Informationen finden Sie im Abschnitt UniDirectional Link Detection (UniDirectional Link Detection).

Hinweis zu STP-Timern:

Die standardmäßigen STP-Timer-Werte basieren auf einer Berechnung, die einen Netzwerkdurchmesser von sieben Switches (sieben Switch-Hops vom Root zum Netzwerk-Edge) berücksichtigt, sowie auf der Zeit, die eine BPDU für die Fahrt von der Root-Bridge zu den Edge-Switches im Netzwerk, die sieben Hops entfernt sind, benötigt. Diese Annahme berechnet Timer-Werte, die für die meisten Netzwerke akzeptabel sind. Sie können diese Timer jedoch in optimale Werte ändern, um Konvergenzzeiten bei Änderungen der Netzwerktopologie zu beschleunigen.

Sie können die Root Bridge mit dem Netzwerkdurchmesser für ein bestimmtes VLAN konfigurieren, und die Timer-Werte werden entsprechend berechnet. Wenn Sie Änderungen vornehmen müssen, empfiehlt Cisco, nur den Durchmesser und die optionalen Hello-Zeitparameter auf der Root-Bridge für das VLAN zu konfigurieren.

```
spanning-tree vlan vlan-id [root {primary | secondary}] [diameter diameter-value [hello hello-time]]
!--- This command needs to be on one line.
```

Dieses Makro macht den Switch-Root für das angegebene VLAN, berechnet neue Timer-Werte basierend auf dem angegebenen Durchmesser und der festgelegten Hello-Zeit und leitet diese Informationen in Konfigurations-BPDUs an alle anderen Switches in der Topologie weiter.

Der Abschnitt Neue Portstatus- und Portrollen beschreibt 802.1D STP und vergleicht und vergleicht 802.1D STP mit Rapid STP (RSTP). Weitere Informationen zum RSTP finden Sie unter Understanding Rapid Spanning Tree Protocol (802.1w).

Neue Hafenstaaten- und Hafenrollen

802.1D ist in vier verschiedenen Portzuständen definiert:

- Zuhören
- Lernen
- Sperren
- Weiterleitung

Weitere Informationen finden Sie in der Tabelle im Abschnitt Portstatus. Der Status des Ports ist gemischt (ob er den Datenverkehr blockiert oder weiterleitet), ebenso wie die Rolle, die der Port in der aktiven Topologie spielt (Root-Port, designierter Port usw.). Aus betrieblicher Sicht besteht beispielsweise kein Unterschied zwischen einem Port im Blockierungsstatus und einem Port im Überwachungsstatus. Sie verwerfen Frames und lernen keine MAC-Adressen. Der eigentliche

Unterschied liegt in der Rolle, die der Spanning Tree dem Port zuweist. Sie können sicher davon ausgehen, dass ein Überwachungsport entweder designiert oder als Root festgelegt ist und sich auf dem Weg zum Weiterleitungsstatus befindet. Wenn sich der Port im Weiterleitungsstatus befindet, kann leider nicht vom Port-Status abgeleitet werden, ob der Port Root oder designiert ist. Dies zeigt das Versagen dieser zustandsbasierten Terminologie. RSTP behebt diesen Fehler, da RSTP die Rolle und den Status eines Ports entkoppelt.

Hafenstaaten

Portstatus in STP 802.1D

Ports	Mittel	Standardzeiten für den nächsten Status
`Deaktiviert`	Administrativ deaktiviert.	
`Sperren`	Empfängt BPDUs und stoppt Benutzerdaten.	Überwacht den Empfang von BPDUs. 20 Sekunden warten, bis die maximale Dauer abgelaufen ist oder eine sofortige Änderung erfolgt, wenn eine direkte/lokale Verbindung ausfällt.
`Zuhören`	Sendet oder empfängt BPDUs, um zu überprüfen, ob eine Rückkehr zur Blockierung erforderlich ist.	Warten Sie 15 Sekunden Verzögerung.
`Lernen`	Erstellung der Topologie/CAM-Tabelle	Warten Sie 15 Sekunden Verzögerung.
`Weiterleitung`	Sendet/empfängt Daten.	

Die grundlegende Änderung der Topologie insgesamt ist:

- 20 + 2 (15) = 50 Sek., wenn das Maximum bis zum Ablauf der Nutzungsdauer wartet
- 30 Sekunden bei Ausfall einer Direktverbindung

Im RSTP verbleiben nur drei Portzustände, die den drei möglichen Betriebszuständen entsprechen. Die 802.1D-Zustände "Deaktiviert", "Blockieren" und "Abhören" wurden in einem einzigartigen 802.1w-Status zusammengeführt, der verworfen wird.

STP (802.1D) Portstatus	RSTP (802.1w) Portstatus	Ist Port in der aktiven Topologie enthalten?	Handelt es sich um MAC-Adressen für Portlernen?
Deaktiviert	Verwerfen	Nein	Nein
Sperren	Verwerfen	Nein	Nein

Zuhören	Verwerfen	Ja	Nein
Lernen	Lernen	Ja	Ja
Weiterleitung	Weiterleitung	Ja	Ja

Portrollen

Die Rolle ist nun eine Variable, die einem bestimmten Port zugewiesen ist. Die Root-Port- und die designierten Port-Rollen bleiben erhalten, aber die Blockierungsportrolle ist nun in die Backup- und die alternativen Port-Rollen aufgeteilt. Der Spanning-Tree-Algorithmus (STA) bestimmt die Rolle eines Ports auf der Grundlage von BPDUs. Denken Sie daran, dass es sich bei BPDUs um einfache Dinge handelt: Es gibt immer eine Möglichkeit, zwei BPDUs zu vergleichen und zu entscheiden, ob eine nützlicher ist als die andere. Grundlage der Entscheidung ist der Wert, der in der BPDU gespeichert wird, und gelegentlich auch der Port, an dem die BPDU empfangen wird. Im verbleibenden Teil dieses Abschnitts werden sehr praktische Ansätze für Portrollen erläutert.

Root-Port-Rolle

Der Port, der die beste BPDU auf einer Bridge empfängt, ist der Root-Port. Dies ist der Port, der hinsichtlich der Pfadkosten der Root-Bridge am nächsten liegt. Der STA wählt eine einzelne Root Bridge im gesamten Bridge-Netzwerk (pro VLAN) aus. Die Root Bridge sendet BPDUs, die nützlicher sind als die, die andere Bridges senden können. Die Root-Bridge ist die einzige Bridge im Netzwerk, die über keinen Root-Port verfügt. Alle anderen Bridges empfangen BPDUs auf mindestens einem Port.

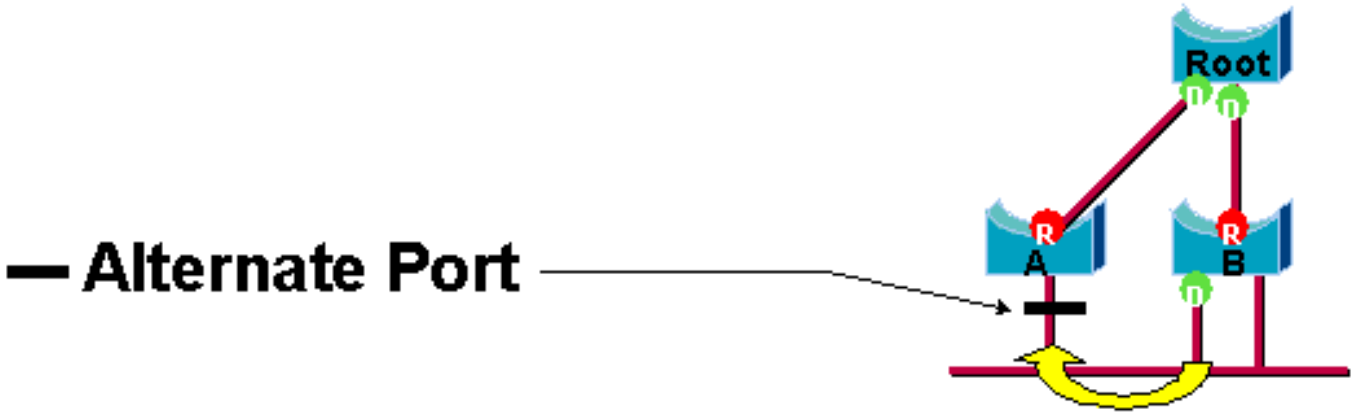
Festgelegte Portrolle

Ein Port wird festgelegt, wenn er die beste BPDU für das Segment senden kann, mit dem der Port verbunden ist. 802.1D-Bridges verbinden verschiedene Segmente (z. B. Ethernet-Segmente), um eine überbrückte Domäne zu erstellen. Auf einem bestimmten Segment kann es nur einen Pfad zur Root Bridge geben. Wenn es zwei Pfade gibt, gibt es eine Bridging-Schleife im Netzwerk. Alle Bridges, die mit einem bestimmten Segment verbunden sind, überwachen die BPDUs der anderen und vereinbaren die Bridge, die die beste BPDU als designierte Bridge für das Segment sendet. Der entsprechende Port auf dieser Bridge ist benannt.

Alternative und Backup-Port-Rollen

Diese beiden Portrollen entsprechen dem Blockierungsstatus von 802.1D. Die Definition eines blockierten Ports ist ein Port, der nicht der designierte oder der Root-Port ist. Ein blockierter Port empfängt eine nützlichere BPDU als die BPDU, die er auf seinem Segment aussendet. Denken Sie daran, dass ein Port unbedingt BPDUs empfangen muss, um blockiert zu bleiben. RSTP führt diese beiden Rollen zu diesem Zweck ein.

Ein alternativer Port ist ein Port, der blockiert wird, indem nützlichere BPDUs von einer anderen Bridge empfangen werden. Dieses Diagramm veranschaulicht:



Ein Backup-Port ist ein Port, der blockiert wird, indem er nützlichere BPDUs von der gleichen Bridge empfängt, auf der sich der Port befindet. Dieses Diagramm veranschaulicht:

Diese Unterscheidung wurde bereits intern in 802.1D vorgenommen. So funktioniert Cisco UplinkFast. Der Grund dafür ist, dass ein alternativer Port einen alternativen Pfad zur Root Bridge bereitstellt. Daher kann dieser Port den Root-Port ersetzen, wenn er ausfällt. Natürlich bietet ein

Backup-Port eine redundante Verbindung mit demselben Segment und kann keine alternative Verbindung zur Root Bridge garantieren. Daher wurde der Backup-Port von der Uplink-Gruppe ausgeschlossen.

Das Ergebnis ist, dass RSTP die endgültige Topologie für den Spanning Tree berechnet, wobei die gleichen Kriterien wie 802.1D verwendet werden. Die Verwendung der verschiedenen Bridge- und Port-Prioritäten ändert sich nicht. Die Namensblockierung wird für den verworfenen Zustand in der Cisco Implementierung verwendet. CatOS Release 7.1 und höher zeigt noch immer den Status "Listening and Learning" (Zuhören und Lernen) an, der noch mehr Informationen über einen Port liefert, als der IEEE-Standard erfordert. Die neue Funktion besteht jedoch darin, dass es nun einen Unterschied zwischen der Rolle gibt, die das Protokoll für einen Port festgelegt hat, und seinem aktuellen Status. Beispielsweise ist es jetzt vollkommen gültig, dass ein Port gleichzeitig designiert und blockiert wird. Dies geschieht in der Regel über sehr kurze Zeiträume, aber es bedeutet einfach, dass dieser Port sich in einem Übergangszustand zur designierten Weiterleitung befindet.

STP-Interaktionen mit VLANs

Es gibt drei Möglichkeiten, VLANs mit Spanning Tree zu korrelieren:

- Ein einzelner Spanning Tree für alle VLANs oder Common Spanning Tree Protocol (CST) wie IEEE 802.1D
- Spanning Tree pro VLAN oder Shared Spanning Tree wie Cisco PVST
- Spanning Tree pro Set von VLANs oder Multiple Spanning Tree (MST) wie IEEE 802.1s

Aus Konfigurationssicht können diese drei Typen von Spanning Tree-Modi, die sich auf die Interaktion mit VLANs beziehen, in einem von drei Modi konfiguriert werden:

- **pvst**: Per-VLAN Spanning Tree (Spanning Tree pro VLAN) Dies implementiert tatsächlich PVST+, wird jedoch in der Cisco IOS-Software lediglich als PVST bezeichnet.
- **rapid-pvst** - Die Weiterentwicklung des 802.1D-Standards verbessert Konvergenzzeiten und umfasst die standardbasierten (802.1w) Eigenschaften von UplinkFast und BackboneFast.
- **mst** - Dies ist der 802.1s-Standard für einen Spanning Tree pro Set von VLANs oder MSTs. Dies umfasst auch die 802.1w Rapid-Komponente innerhalb des Standards.

Ein Mono Spanning Tree für alle VLANs ermöglicht nur eine aktive Topologie und somit keinen Lastenausgleich. Ein durch STP blockierter Port blockiert alle VLANs und enthält keine Daten.

Ein Spanning Tree pro VLAN oder PVST+ ermöglicht den Lastenausgleich, erfordert jedoch bei zunehmender Anzahl von VLANs mehr BPDU-CPU-Verarbeitung.

Der neue 802.1s-Standard (MST) ermöglicht die Definition von bis zu 16 aktiven STP-Instanzen/-Topologien und die Zuordnung aller VLANs zu diesen Instanzen. In einer typischen Campus-Umgebung müssen nur zwei Instanzen definiert werden. Diese Technik ermöglicht die STP-Skalierung auf Tausende von VLANs und ermöglicht den Lastenausgleich.

Rapid-PVST und Pre-Standard MST werden in der Cisco IOS Software Version 12.1(11b)EX und 12.1(13)E für Catalyst 6500 unterstützt. Catalyst 4500 mit Cisco IOS Software Release 12.1(12c)EW und höheren Versionen unterstützen eine Pre-Standard MST. Die Cisco IOS Software Release 12.1(19)EW für die Catalyst 4500-Plattform bietet Rapid PVST-Unterstützung. Das standardkonforme MST wird von der Cisco IOS Software Release 12.2(18)SXF für Catalyst 6500 und der Cisco IOS Software Release 12.2(25)SG für Catalyst Switches der Serie 4500 unterstützt.

Weitere Informationen finden Sie unter Understanding Rapid Spanning Tree Protocol (802.1w) und Understanding Multiple Spanning Tree Protocol (802.1s).

Logische Spanning Tree-Ports

Die Versionshinweise für Catalyst 4500 und 6500 enthalten Anleitungen zur Anzahl der logischen Ports in Spanning Tree pro Switch. Die Summe aller logischen Ports entspricht der Anzahl der Trunks auf dem Switch-mal der Anzahl der aktiven VLANs auf den Trunks plus der Anzahl der Nicht-Trunking-Schnittstellen auf dem Switch. Die Cisco IOS-Software generiert eine Systemprotokollmeldung, wenn die maximale Anzahl logischer Schnittstellen die Beschränkung überschreitet. Es wird empfohlen, die empfohlene Empfehlung nicht zu überschreiten.

In dieser Tabelle wird die Anzahl der unterstützten logischen Ports mit verschiedenen STP-Modi und Supervisor-Typen verglichen:

Supervisor	PVST+	RPVST+	MST
Catalyst 6500 Supervisor 1	6.000[1] insgesamt 1.200 pro Switching-Modul	6.000 insgesamt 1.200 pro Switching-Modul	25.000 insgesamt 3.000[2] pro Switching-Modul
Catalyst 6500 Supervisor 2	13.000[1] insgesamt 1.800[2] pro Switching-Modul	10.000 insgesamt 1.800[2] pro Switching-Modul	50.000 insgesamt 6.000[2] pro Switching-Modul
Catalyst 6500 Supervisor 720	13.000 insgesamt 1.800[2] pro Switching-Modul	10.000 insgesamt 1.800[2] pro Switching-Modul	50.0003 insgesamt 6.000[2] pro Switching-Modul
Catalyst 4500 Supervisor II plus	Insgesamt 1.500	Insgesamt 1.500	Insgesamt 25.000
Catalyst 4500 Supervisor II plus 10GE	Insgesamt 1.500	Insgesamt 1.500	Insgesamt 25.000
Catalyst 4500 Supervisor IV	Insgesamt 3.000	Insgesamt 3.000	Insgesamt 50.000
Catalyst 4500 Supervisor V	Insgesamt 3.000	Insgesamt 3.000	Insgesamt 50.000
Catalyst 4500	Insgesamt 3.000	Insgesamt 3.000	Insgesamt 80.000

Supervisor V 10GE			

[1] Die maximale Anzahl der in PVST+ unterstützten logischen Ports vor der Cisco IOS Software Release 12.1(13)E beträgt 4.500.

[Zwei] Switching-Module mit 10 Mbit/s, 10/100 Mbit/s und 100 Mbit/s unterstützen maximal 1.200 logische Schnittstellen pro Modul.

[3] Die maximale Anzahl der logischen Ports, die im MST vor der Cisco IOS Software-Version 12.2(17b)SXA unterstützt werden, beträgt 30.000.

Empfehlung

Es ist schwierig, eine Spanning-Tree-Modusempfehlung ohne detaillierte Informationen wie Hardware, Software, Anzahl der Geräte und Anzahl der VLANs bereitzustellen. Wenn die Anzahl der logischen Ports die empfohlene Richtlinie nicht überschreitet, wird für die neue Netzwerkbereitstellung der Rapid PVST-Modus empfohlen. Der Rapid PVST-Modus ermöglicht eine schnelle Netzwerkkonvergenz, ohne dass zusätzliche Konfigurationen wie Backbone Fast oder Uplink Fast erforderlich sind. Führen Sie den folgenden Befehl aus, um den Spanning-Tree im Rapid-PVST-Modus einzustellen:

```
spanning-tree mode rapid-pvst
```

Weitere Optionen

In einem Netzwerk mit einer Kombination aus älterer Hardware und älterer Software wird der PVST+-Modus empfohlen. Geben Sie diesen Befehl ein, um den Spanning-Tree im PVST+-Modus festzulegen:

```
spanning-tree mode pvst
----This is default and it shows in the configuration.
```

Der MST-Modus wird für VLANs mit einer großen Anzahl von VLANs in allen Netzwerkdesigns empfohlen. Für dieses Netzwerk kann die Summe der logischen Ports die Richtlinien für PVST und Rapid-PVST überschreiten. Geben Sie diesen Befehl ein, um das Spanning-Tree im MST-Modus festzulegen:

```
spanning-tree mode mst
```

BPDU-Formate

Um den IEEE 802.1Q-Standard zu unterstützen, erweiterte Cisco das vorhandene PVST-Protokoll, um das PVST+-Protokoll bereitzustellen. PVST+ bietet Unterstützung für Verbindungen in der IEEE 802.1Q-Mono-Spanning-Tree-Region. PVST+ ist sowohl mit IEEE 802.1Q-Mono-Spanning-Tree als auch mit den vorhandenen Cisco PVST-Protokollen kompatibel. Darüber hinaus bietet PVST+ Überprüfungsmechanismen, um sicherzustellen, dass Port-Trunking und VLAN-IDs zwischen Switches nicht durch eine inkonsistente Konfiguration voneinander getrennt

werden. PVST+ ist Plug-and-Play-kompatibel mit PVST, ohne dass ein neuer CLI-Befehl oder eine neue CLI-Konfiguration erforderlich sind.

Hier einige Highlights der Betriebstheorie des PVST+-Protokolls:

- PVST+ ist mit einem 802.1Q-Mono-Spanning-Tree kompatibel. PVST+ ist mit 802.1Q-konformen Switches auf gängigen STP- bis 802.1Q-Trunking-Systemen kompatibel. Ein gemeinsamer Spanning Tree befindet sich standardmäßig im VLAN 1, dem nativen VLAN. Eine gemeinsame Spanning-Tree-BPDU wird über 802.1Q-Verbindungen mit der IEEE-Standard-Bridge-Group-MAC-Adresse (01-80-c2-00-00-00, Protokolltyp 0x010c) übertragen oder empfangen. Ein gemeinsamer Spanning Tree kann in der PVST- oder Mono Spanning Tree-Region verwurzelt sein.
- PVST+ tunnelt die PVST-BPDUs in der 802.1Q-VLAN-Region als Multicast-Daten. Für jedes VLAN auf einem Trunk werden BPDUs mit der MAC-Adresse (01-00-0c-cc-cd) des Cisco Shared STP (SSTP) übertragen oder empfangen. Bei VLANs, die der PVID (Port VLAN Identifier) entsprechen, ist BPDU nicht markiert. Für alle anderen VLANs werden BPDUs mit einem Tag versehen.
- PVST+ ist abwärtskompatibel mit dem vorhandenen Cisco Switch auf PVST über ISL-Trunking. ISL-gekapselte BPDUs werden über ISL-Trunks übertragen oder empfangen. Dies entspricht dem vorherigen Cisco PVST.
- PVST+ überprüft den Port und die VLAN-Inkonsistenzen. PVST+ blockiert Ports, die inkonsistente BPDUs empfangen, um das Auftreten von Weiterleitungsschleifen zu verhindern. PVST+ benachrichtigt Benutzer auch über Syslog-Meldungen über Inkonsistenzen.

Hinweis: In ISL-Netzwerken werden alle BPDUs unter Verwendung der IEEE MAC-Adresse gesendet.

Cisco Konfigurationsempfehlungen

Bei allen Catalyst-Switches ist STP standardmäßig aktiviert. Auch wenn Sie ein Design auswählen, das keine Layer-2-Schleifen enthält und STP nicht aktiviert ist, um einen blockierten Port aktiv zu erhalten, lassen Sie die Funktion aus folgenden Gründen aktiviert:

- Wenn eine Schleife vorhanden ist, verhindert STP Probleme, die durch Multicast- und Broadcast-Daten noch verschlimmert werden können. Häufig führen Patches, fehlerhafte Kabel oder andere Ursachen zu einer Schleife.
- STP schützt vor einem EtherChannel-Ausfall.
- Die meisten Netzwerke sind mit STP konfiguriert, sodass ein Höchstmaß an Außendienst gewährleistet ist. Eine höhere Exposition entspricht im Allgemeinen einem stabileren Code.
- STP schützt vor Fehlverhalten von zwei angeschlossenen NICs (oder Bridging aktiviert auf Servern).
- Viele Protokolle sind im Code eng mit STP verknüpft. Beispiele:PAgPIGMP-Snooping (Internet Group Message Protocol)TrunkingWenn Sie ohne STP arbeiten, können unerwünschte Ergebnisse erzielt werden.
- Bei einer Netzwerkstörung legen die Techniker von Cisco normalerweise nahe, dass die Nichtnutzung von STP im Fehlerzentrum liegt, wenn überhaupt möglich.

Führen Sie folgende globale Befehle aus, um Spanning Tree auf allen VLANs zu aktivieren:

```
Switch(config)#spanning-tree vlan vlan_id
!--- Specify the VLAN that you want to modify. Switch(config)#default spanning-tree vlan vlan_id
!--- Set spanning-tree parameters to default values.
```

Ändern Sie keine Timer, die die Stabilität beeinträchtigen können. Die Mehrzahl der bereitgestellten Netzwerke ist nicht abgestimmt. Die einfachen STP-Timer, auf die über die Befehlszeile zugegriffen werden kann, z. B. Hello-Intervall und Maxage, verfügen über einen komplexen Satz von anderen angenommenen und systeminternen Timern. Daher können Sie Schwierigkeiten haben, wenn Sie versuchen, Timer zu optimieren und alle Auswirkungen zu berücksichtigen. Darüber hinaus können Sie den UDLD-Schutz untergraben.

Im Idealfall sollten Sie den Benutzerdatenverkehr vom Management-VLAN fernhalten. Dies gilt nicht für den Catalyst 6500/6000 Cisco IOS-Switch. Dennoch müssen Sie diese Empfehlung für die kleineren Cisco IOS-Switches und CatOS-Switches einhalten, die über eine separate Verwaltungsschnittstelle verfügen und in Cisco IOS-Switches integriert werden müssen. Insbesondere bei älteren Catalyst Switch-Prozessoren sollte das Management-VLAN von den Benutzerdaten getrennt bleiben, um Probleme mit STP zu vermeiden. Eine fehlerhafte Endstation kann den Supervisor Engine-Prozessor möglicherweise so stark mit Broadcast-Paketen belasten, dass der Prozessor eine oder mehrere BPDUs übersehen kann. Neuere Switches mit leistungsfähigeren CPUs und Drosselungssteuerungen entlasten diese Überlegungen. Weitere Informationen finden Sie im Abschnitt Switch-Management-Schnittstelle und natives VLAN in diesem Dokument.

Vermeiden Sie eine Übergestaltung der Redundanz. Dies kann zu vielen blockierenden Ports führen und die langfristige Stabilität beeinträchtigen. Behalten Sie den gesamten STP-Durchmesser unter sieben Hops bei. Versuchen Sie, das Design an allen Standorten, an denen dieses Design möglich ist, auf das Cisco Multilayer-Modell anzuwenden. Das Modell bietet folgende Funktionen:

- Kleinere Switched-Domänen
- STP-Dreiecke
- Deterministische blockierte Ports

Beeinflussen und wissen, wo sich Root-Funktionen und blockierte Ports befinden. Dokumentieren Sie diese Informationen im Topologiediagramm. Machen Sie sich mit der Spanning Tree-Topologie vertraut, die für die Fehlerbehebung unerlässlich ist. An den blockierten Ports beginnt die STP-Fehlerbehebung. Die Ursache für den Wechsel von der Blockierung zur Weiterleitung ist häufig der Hauptbestandteil der Ursachenanalyse. Wählen Sie die Distribution-Layer und die Core-Layer als Speicherort des Root/sekundären Roots aus, da diese Layer als die stabilsten Teile des Netzwerks gelten. Prüfen Sie, ob ein optimales Layer 3- und Hot Standby Router Protocol (HSRP)-Overlay mit Layer 2-Pfaden für die Datenweiterleitung verwendet wird.

Dieser Befehl ist ein Makro, das die Bridge-Priorität konfiguriert. Der Root legt fest, dass die Priorität viel niedriger als der Standardwert (32.768) ist, und der sekundäre Wert legt die Priorität auf einen deutlich niedrigeren Wert als der Standardwert fest:

```
Switch(config)#interface type slot/port
Switch(config)#spanning-tree vlan vlan_id root primary
!--- Configure a switch as root for a particular VLAN.
```

Hinweis: Dieses Makro legt die Root-Priorität entweder folgendermaßen fest:

- Standardmäßig 8192

- Die aktuelle Root-Priorität minus 1, wenn eine andere Root-Bridge bekannt ist
- Die aktuelle Root-Priorität, wenn die MAC-Adresse niedriger als die aktuelle Root-Adresse ist

Deaktivieren Sie nicht benötigte VLANs von den Trunk-Ports, was eine bidirektionale Übung ist. Dadurch wird der Durchmesser des Overhead für die STP- und NMP-Verarbeitung in Teilen des Netzwerks, in denen bestimmte VLANs nicht erforderlich sind, begrenzt. Durch die automatische VTP-Bereinigung wird STP nicht aus einem Trunk entfernt. Sie können auch das Standard-VLAN 1 aus Trunks entfernen.

Weitere Informationen finden Sie unter Spanning Tree Protocol-Probleme und zugehörige Entwurfsüberlegungen.

Weitere Optionen

Cisco verfügt über ein weiteres STP-Protokoll, **VLAN-Bridge**, das mit einer bekannten Ziel-MAC-Adresse von **01-00-0c-cd-cd-ce** und dem Protokolltyp 0x010c betrieben wird.

Dieses Protokoll ist besonders nützlich, wenn nicht routbare oder veraltete Protokolle zwischen VLANs ohne Interferenz mit den IEEE Spanning Tree-Instanzen überbrückt werden müssen, die auf diesen VLANs ausgeführt werden. Wenn VLAN-Schnittstellen für nicht überbrückten Datenverkehr für Layer-2-Datenverkehr blockiert werden, wird auch der überlagerte Layer-3-Datenverkehr versehentlich abgeschnitten, was eine unerwünschte Nebenwirkung darstellt. Diese Layer-2-Blockierung kann problemlos auftreten, wenn die VLAN-Schnittstellen für nicht überbrückten Datenverkehr im selben STP wie IP-VLANs vorhanden sind. VLAN-Bridge ist eine separate Instanz von STP für überbrückte Protokolle. Das Protokoll stellt eine separate Topologie bereit, die ohne Auswirkungen auf den IP-Datenverkehr bearbeitet werden kann.

Führen Sie das VLAN-Bridge-Protokoll aus, wenn zwischen VLANs auf Cisco Routern wie der MSFC Bridging erforderlich ist.

STP PortFast-Funktion

Sie können PortFast verwenden, um den normalen Spanning Tree-Betrieb an den Access-Ports zu umgehen. PortFast beschleunigt die Verbindung zwischen Endstationen und den Diensten, mit denen Endstationen nach der Initialisierung der Verbindung verbunden werden müssen. Bei der Microsoft DHCP-Implementierung muss der Access-Port unmittelbar nach dem `Hochfahren` des Verbindungsstatus im `Weiterleitungsmodus` angezeigt werden, um eine IP-Adresse anzufordern und zu empfangen. Einige Protokolle, wie Internetwork Packet Exchange (IPX)/Sequected Packet Exchange (SPX), müssen den Access-Port unmittelbar nach dem `Hochfahren` des Verbindungsstatus im `Weiterleitungsmodus` sehen, um GNS-Probleme (Get Nearest Server) zu vermeiden.

Weitere Informationen finden Sie unter Verwenden von PortFast und anderen Befehlen zum Beheben von Workstation-Startverbindungsverzögerungen.

Übersicht über PortFast-Betrieb

PortFast überspringt die normalen `Zustände` für `Zuhören`, `Lernen` und `Weiterleiten` von STP. Die Funktion verschiebt einen Port direkt von der `Blockierung` in den `Weiterleitungsmodus`, nachdem die Verbindung als `aktiv` angesehen wird. Wenn diese Funktion nicht aktiviert ist, verwirft STP alle Benutzerdaten, bis er entscheidet, dass der Port in den `Weiterleitungsmodus` verschoben werden kann. Dieser Prozess kann die (2 x ForwardDelay)-Zeit in Anspruch nehmen, die standardmäßig

30 Sekunden beträgt.

`Der Portfast-`Modus verhindert die Generierung einer STP-Topologieänderungsbenachrichtigung (TCN), wenn sich ein Portstatus vom `Lernen` zur `Weiterleitung` ändert. TCNs sind normal. Aber eine Welle von TCNs, die auf die Root Bridge trifft, kann die Konvergenzzeit unnötigerweise verlängern. Eine Welle von TCNs tritt häufig morgens auf, wenn die Benutzer ihre PCs einschalten.

Empfehlung zur Konfiguration von Cisco Access Ports

Stellen Sie STP PortFast für alle aktivierten Host-Ports `ein`. Legen Sie außerdem STP PortFast explizit auf `Aus` für Switch-Switch-Verbindungen und nicht verwendete Ports fest.

Führen Sie den **Befehl switchport host** als Makro im Schnittstellenkonfigurationsmodus aus, um die empfohlene Konfiguration für Zugriffsports zu implementieren. Die Konfiguration trägt außerdem erheblich zur Autoübertragung und Verbindungsleistung bei:

```
switch(config)#interface type slot#/port#

switch(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
!--- This macro command modifies these functions.
```

Hinweis: PortFast bedeutet nicht, dass Spanning Tree auf den Ports überhaupt nicht ausgeführt wird. BPDUs werden weiterhin gesendet, empfangen und verarbeitet. Spanning Tree ist für ein voll funktionsfähiges LAN unerlässlich. Ohne Loop-Erkennung und -Blockierung kann eine Schleife unbeabsichtigt das gesamte LAN schnell zum Erliegen bringen.

Deaktivieren Sie außerdem das Trunking und Channeling für alle Host-Ports. Jeder Access-Port ist standardmäßig für Trunking und Channeling aktiviert, jedoch werden Switch-Nachbarn für Host-Ports nicht erwartet. Wenn Sie diese Protokolle aushandeln lassen, kann die spätere Verzögerung bei der Port-Aktivierung zu unerwünschten Situationen führen. Erste Pakete von Workstations, wie DHCP- und IPX-Anfragen, werden nicht weitergeleitet.

Eine bessere Option besteht darin, PortFast standardmäßig im globalen Konfigurationsmodus mithilfe des folgenden Befehls zu konfigurieren:

```
Switch(config)#spanning-tree portfast enable
```

Deaktivieren Sie dann auf jedem Zugriffsport, der über einen Hub oder einen Switch in nur einem VLAN verfügt, die PortFast-Funktion auf jeder Schnittstelle mit dem Befehl **interface**:

```
Switch(config)#interface type slot_num/port_num
Switch(config-if)#spanning-tree portfast disable
```

Weitere Optionen

PortFast BPDU Guard bietet eine Methode, um Schleifen zu verhindern. BPDU Guard verschiebt einen Nicht-Trunking-Port beim Empfang einer BPDU an diesem Port in den `errDisable`-Zustand.

Unter normalen Bedingungen dürfen Sie niemals BPDU-Pakete an einem Zugriffsport empfangen, der für PortFast konfiguriert ist. Eine eingehende BPDU weist auf eine ungültige Konfiguration hin. Die beste Aktion ist, den Access-Port herunterzufahren.

Die Cisco IOS-Systemsoftware bietet einen nützlichen globalen Befehl, der automatisch `BPDU-ROOT-GUARD` auf jedem für UplinkFast aktivierten Port aktiviert. Verwenden *Sie immer* diesen Befehl. Der Befehl funktioniert auf Switch-Basis und nicht auf Port-Basis.

Geben Sie diesen globalen Befehl ein, um `BPDU-ROOT-GUARD` zu aktivieren:

```
Switch(config)#spanning-tree portfast bpduguard default
```

Ein Simple Network Management Protocol (SNMP)-Trap oder eine Syslog-Meldung benachrichtigt den Netzwerkmanager, wenn der Port ausfällt. Sie können auch eine automatische Wiederherstellungszeit für `fehlerhafte` Ports konfigurieren. Weitere Informationen finden Sie im Abschnitt UniDirectional Link Detection (UniDirectional Link Detection) dieses Dokuments.

Weitere Informationen finden Sie unter Spanning Tree PortFast BPDU Guard Enhancement.

Hinweis: PortFast für Trunk-Ports wurde in Version 12.1(11b)E der Cisco IOS-Software eingeführt. PortFast für Trunk-Ports wurde entwickelt, um die Konvergenzzeiten für Layer-3-Netzwerke zu erhöhen. Wenn Sie diese Funktion verwenden, stellen Sie sicher, dass Sie den BPDU Guard- und BPDU-Filter auf Schnittstellenbasis deaktivieren.

UplinkFast

Zweck

UplinkFast bietet schnelle STP-Konvergenz nach einem direkten Verbindungsausfall auf der Netzwerkzugriffs-Ebene. UplinkFast arbeitet ohne Änderung von STP. Der Zweck besteht darin, die Konvergenzzeit in einem bestimmten Fall auf weniger als drei Sekunden zu beschleunigen, anstatt auf eine typische Verzögerung von 30 Sekunden. Weitere Informationen finden Sie unter Informationen zur Konfiguration der Cisco UplinkFast-Funktion.

Überblick

Beim Cisco Multilayer-Designmodell auf dem Access Layer wird der blockierende Uplink sofort in den `Weiterleitungsstatus` verschoben, wenn der Weiterleitungs-Uplink verloren geht. Die Funktion wartet nicht auf die `Zustände` zum `Hören` und `Lernen`.

Eine Uplink-Gruppe besteht aus einer Reihe von Ports pro VLAN, die Sie sich als Root-Port und Backup-Root-Port vorstellen können. Unter normalen Bedingungen stellen die Root-Ports die Verbindung vom Zugriff zum Root sicher. Wenn diese primäre Root-Verbindung aus irgendeinem Grund ausfällt, wird die Backup-Root-Verbindung sofort aktiviert, ohne dass die typische Konvergenzverzögerung von 30 Sekunden durchlaufen werden muss.

Da UplinkFast den normalen STP-Topologieänderungsprozess (`Abhören` und `Lernen`) effektiv umgeht, ist ein alternativer Mechanismus zur Topologiekorrektur erforderlich. Der Mechanismus muss die Switches in der Domäne mit den Informationen aktualisieren, dass lokale Endgeräte über einen alternativen Pfad erreichbar sind. Der Access-Layer-Switch, der UplinkFast ausführt, erzeugt daher auch Frames für jede MAC-Adresse in der CAM-Tabelle zu einer bekannten

Multicast-MAC-Adresse (01-00-0c-cd-cd-HDLC-Protokoll 0x200a). Dieser Prozess aktualisiert die CAM-Tabelle in allen Switches der Domäne mit der neuen Topologie.

Empfehlung von Cisco

Cisco empfiehlt, UplinkFast für Access Switches mit blockierten Ports zu aktivieren, wenn Sie 802.1D Spanning Tree ausführen. Verwenden Sie UplinkFast nicht auf Switches ohne implizite Topologiekenntnisse einer Backup-Root-Verbindung. In der Regel sind Distribution- und Core-Switches im Cisco Multilayer-Design vorhanden. Im Allgemeinen sollten Sie UplinkFast nicht auf einem Switch mit mehr als zwei Ausgängen aus einem Netzwerk aktivieren. Wenn sich der Switch in einer komplexen Zugriffsumgebung befindet und Sie mehrere Verbindungs- und Weiterleitungsfunktionen blockieren, vermeiden Sie die Verwendung dieser Funktion auf dem Switch, oder wenden Sie sich an Ihren Advanced Services-Techniker.

Geben Sie diesen globalen Befehl ein, um UplinkFast zu aktivieren:

```
Switch(config)#spanning-tree uplinkfast
```

Mit diesem Befehl in der Cisco IOS Software werden nicht automatisch alle Bridge-Prioritätswerte auf einen hohen Wert eingestellt. Stattdessen ändert der Befehl nur die VLANs mit einer Bridge-Priorität, die nicht manuell in einen anderen Wert geändert wurde. Im Gegensatz zu CatOS werden bei der Wiederherstellung eines Switches mit aktivierter UplinkFast-Funktion alle geänderten Werte durch die No-Form dieses Befehls (**kein Spanning-Tree-Uplinkfast**) auf ihre Standardwerte zurückgesetzt. Wenn Sie diesen Befehl verwenden, *müssen* Sie daher vor und nach dem aktuellen Status der Bridge-Prioritäten überprüfen, um sicherzustellen, dass das gewünschte Ergebnis erreicht wird.

Hinweis: Sie benötigen das Schlüsselwort **alle Protokolle** für den UplinkFast-Befehl, wenn die Protokollfilterfunktion aktiviert ist. Da der CAM bei aktivierter Protokollfilterung den Protokolltyp sowie MAC- und VLAN-Informationen aufzeichnet, muss für jedes Protokoll an jeder MAC-Adresse ein UplinkFast-Frame generiert werden. Das **rate**-Schlüsselwort gibt die Pakete pro Sekunde der UplinkFast-Topologie-Update-Frames an. Die Standardeinstellung wird empfohlen. UplinkFast muss nicht mit RSTP konfiguriert werden, da der Mechanismus nativ integriert und automatisch im RSTP aktiviert ist.

BackboneFast

Zweck

BackboneFast ermöglicht eine schnelle Konvergenz bei indirekten Verbindungsausfällen. BackboneFast reduziert die Konvergenzzeiten von der Standardeinstellung von 50 Sekunden auf normalerweise 30 Sekunden und fügt so STP Funktionen hinzu. Auch diese Funktion ist nur verfügbar, wenn Sie 802.1D ausführen. Konfigurieren Sie die Funktion nicht, wenn Sie Rapid PVST oder MST ausführen (dies schließt die Rapid-Komponente ein).

Überblick

BackboneFast wird initiiert, wenn ein Root-Port oder ein blockierter Port an einem Switch unterlegene BPDUs von der designierten Bridge empfängt. Der Port empfängt in der Regel untergeordnete BPDUs, wenn ein Downstream-Switch die Verbindung zum Root verliert und BPDUs sendet, um einen neuen Root auszuwählen. Eine untergeordnete BPDU identifiziert einen

Switch sowohl als Root Bridge als auch als designierte Bridge.

Unter normalen Spanning Tree-Regeln ignoriert der empfangende Switch unterlegene BPDUs für die konfigurierte Maxage-Zeit. Standardmäßig beträgt die maximale Dauer 20 Sekunden. Mit BackboneFast sieht der Switch die unterlegene BPDU jedoch als Signal für eine mögliche Änderung der Topologie. Der Switch verwendet Root Link Query (RLQ) BPDUs, um festzustellen, ob ein alternativer Pfad zur Root Bridge vorhanden ist. Durch diese RLQ-Protokollerweiterung kann ein Switch überprüfen, ob der Root noch verfügbar ist. RLQ verschiebt einen blockierten Port zu einem früheren Zeitpunkt zur `Weiterleitung` und benachrichtigt den isolierten Switch, der die untergeordnete BPDU gesendet hat, dass der Root noch vorhanden ist.

Hier einige Highlights der Protokolloperation:

- Ein Switch überträgt das RLQ-Paket nur über den Root-Port (d. h. das Paket geht zum Root).
- Ein Switch, der einen RLQ empfängt, kann antworten, wenn er der Root-Switch ist oder wenn dieser Switch weiß, dass er die Verbindung zum Root verloren hat. Wenn der Switch diese Fakten nicht kennt, muss er die Abfrage über den Root-Port weiterleiten.
- Wenn ein Switch die Verbindung zum Root verloren hat, muss der Switch diese Abfrage negativ beantworten.
- Die Antwort darf nur an den Port gesendet werden, von dem die Abfrage stammt.
- Der Root-Switch muss auf diese Abfrage immer mit einer positiven Antwort antworten.
- Wenn die Antwort auf einem Nicht-Root-Port eingeht, verwerfen Sie die Antwort.

Der Vorgang kann die STP-Konvergenzzeiten um bis zu 20 Sekunden reduzieren, da die Maxage nicht ablaufen muss. Weitere Informationen finden Sie unter Understanding and Configuring Backbone Fast on Catalyst Switches.

Empfehlung von Cisco

Aktivieren Sie BackboneFast auf allen Switches, auf denen STP ausgeführt wird, nur, wenn die gesamte Spanning-Tree-Domäne diese Funktion unterstützen kann. Sie können die Funktion ohne Unterbrechung zu einem Produktionsnetzwerk hinzufügen.

Geben Sie diesen globalen Befehl ein, um BackboneFast zu aktivieren:

```
Switch(config)#spanning-tree backbonefast
```

Hinweis: Sie müssen diesen globalen Befehl auf allen Switches in einer Domäne konfigurieren. Der Befehl fügt STP Funktionen hinzu, die alle Switches verstehen müssen.

Weitere Optionen

BackboneFast wird auf Catalyst Switches der Serien 2900XL und 3500XL nicht unterstützt. Im Allgemeinen müssen Sie BackboneFast aktivieren, wenn die Switch-Domäne zusätzlich zu den Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000 diese Switches enthält. Wenn Sie BackboneFast in Umgebungen mit XL-Switches implementieren, können Sie unter strengen Topologien die Funktion aktivieren, bei der der XL-Switch der letzte Line-Switch ist und nur an zwei Stellen mit dem Kern verbunden ist. Implementieren Sie diese Funktion nicht, wenn sich die Architektur der XL-Switches in Reihenschaltung befindet.

BackboneFast muss nicht mit RSTP oder 802.1w konfiguriert werden, da der Mechanismus nativ integriert und automatisch im RSTP aktiviert ist.

Spanning Tree Loop Guard

Loop Guard ist eine proprietäre STP-Optimierung von Cisco. Loop Guard schützt Layer-2-Netzwerke vor Schleifen, die aufgrund einer Netzwerkschnittstellen-Fehlfunktion, einer ausgelasteten CPU oder anderen Ereignissen auftreten, die die normale Weiterleitung von BPDUs verhindern. Eine STP-Schleife wird erstellt, wenn ein blockierender Port in einer redundanten Topologie irrtümlicherweise in den Weiterleitungsstatus wechselt. Dies geschieht in der Regel, weil einer der Ports in einer physisch redundanten Topologie (nicht unbedingt der blockierende Port) keine BPDUs mehr empfängt.

Loop Guard ist nur in Switched Networks nützlich, wo Switches über Point-to-Point-Verbindungen verbunden sind, wie dies in den meisten modernen Campus- und Rechenzentrumsnetzwerken der Fall ist. Die Idee dahinter ist, dass eine designierte Bridge auf einer Punkt-zu-Punkt-Verbindung nicht verschwinden kann, ohne eine unterlegene BPDU zu senden oder die Verbindung herunterzufahren. Die STP-Loop Guard-Funktion wurde in der Cisco IOS Software Version 12.1(13)E der Catalyst Cisco IOS Software für Catalyst 6500 und der Cisco IOS Software Version 12.1(9)EA1 für Catalyst 4500 Switches eingeführt.

Weitere Informationen zu Loop Guard und BPDU Skew Detection Features finden Sie unter Spanning Tree Protocol Enhancements.

Überblick

Loop Guard überprüft, ob ein Root-Port oder ein alternativer/Backup-Root-Port BPDUs empfängt. Wenn der Port keine BPDUs empfängt, setzt Loop Guard den Port in einen inkonsistenten Zustand (Blockierung), bis er wieder BPDUs empfängt. Ein Port im inkonsistenten Zustand überträgt keine BPDUs. Wenn ein solcher Port erneut BPDUs empfängt, wird der Port (und die Verbindung) erneut als funktionsfähig erachtet. Die schleifeninkonsistente Bedingung wird aus dem Port entfernt, und STP bestimmt den Port-Status. Auf diese Weise erfolgt die Wiederherstellung automatisch.

Loop Guard isoliert den Ausfall und ermöglicht die Konvergenz von Spanning Tree in einer stabilen Topologie ohne fehlerhafte Verbindung oder Bridge. Loop Guard verhindert STP-Schleifen mit der Geschwindigkeit der verwendeten STP-Version. Es besteht keine Abhängigkeit von STP selbst (802.1D oder 802.1w) oder bei der Einstellung der STP-Timer. Aus diesen Gründen empfiehlt Cisco die Implementierung von Loop Guard in Verbindung mit UDLD in Topologien, die auf STP basieren und von denen die Software die Funktionen unterstützt.

Wenn Loop Guard einen inkonsistenten Port blockiert, wird diese Meldung protokolliert:

```
%SPANTREE-SP-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet2/1 on VLAN0010
```

Nachdem die BPDU an einem Port in einem schleifeninkonsistenten STP-Status empfangen wurde, wechselt der Port in einen anderen STP-Status. Laut BPDU bedeutet dies, dass die Wiederherstellung automatisch erfolgt und keine Intervention erforderlich ist. Nach der Wiederherstellung wird diese Meldung protokolliert:

```
%SPANTREE-SP-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet2/1 on
VLAN0010
```

Interaktion mit anderen STP-Funktionen

Root Guard

Root Guard erzwingt, dass ein Port immer benannt wird. Loop Guard ist nur dann wirksam, wenn der Port ein Root-Port oder ein alternativer Port ist, was bedeutet, dass sich deren Funktionen gegenseitig ausschließen. Aus diesem Grund können Loop Guard und Root Guard nicht gleichzeitig auf einem Port aktiviert werden.

UplinkFast

Loop Guard ist mit UplinkFast kompatibel. Wenn ein Loop Guard einen Root-Port in einen Blockierungsstatus versetzt, versetzt UplinkFast einen neuen Root-Port in den Weiterleitungsstatus. UplinkFast wählt auch keinen *schleifeninkonsistenten Port* als Root-Port aus.

BackboneFast

Loop Guard ist kompatibel mit BackboneFast. BackboneFast wird durch den Empfang einer unterlegenen BPDU ausgelöst, die von einer designierten Bridge stammt. Da BPDUs von dieser Verbindung empfangen werden, wird kein Schleifenschutz aktiviert. Daher sind BackboneFast und Loop Guard kompatibel.

PortFast

PortFast wechselt einen Port unmittelbar nach der Verbindung in den designierten Weiterleitungsstatus. Da ein PortFast-fähiger Port kein Root-/Alternativport ist, schließen Loop Guard und PortFast sich gegenseitig aus.

PAgP

Loop Guard verwendet die Ports, die STP bekannt sind. Daher kann Loop Guard die Abstraktion der logischen Ports nutzen, die PAgP bereitstellt. Um jedoch einen Kanal zu bilden, müssen alle physischen Ports, die im Channel gruppiert sind, über kompatible Konfigurationen verfügen. PAgP erzwingt die einheitliche Konfiguration von Loop Guard an allen physischen Ports, um einen Kanal zu bilden. Beachten Sie diese Vorbehalte, wenn Sie Schleifenschutz auf einem EtherChannel konfigurieren:

- STP wählt immer den ersten betrieblichen Port im Kanal aus, um die BPDUs zu senden. Wenn diese Verbindung unidirektional wird, blockiert der Loop Guard den Kanal, selbst wenn andere Links im Channel ordnungsgemäß funktionieren.
- Wenn eine Reihe von Ports, die bereits durch Loop Guard blockiert sind, gruppiert werden, um einen Kanal zu bilden, verliert STP alle Statusinformationen für diese Ports, und der neue Channel-Port kann möglicherweise den Weiterleitungsstatus mit einer festgelegten Rolle erreichen.
- Wenn ein Kanal von Loop Guard blockiert wird und der Kanal ausfällt, verliert STP alle Statusinformationen. Die einzelnen physischen Ports können den Weiterleitungsstatus mit einer festgelegten Rolle erreichen, selbst wenn eine oder mehrere der Verbindungen, aus denen der Kanal besteht, unidirektional sind.

In diesen beiden letzten Fällen besteht die Möglichkeit einer Schleife, bis UDLD den Ausfall erkennt. Aber Loop Guard kann es nicht erkennen.

Loop Guard- und UDLD-Funktionen im Vergleich

Schleifenschutz- und UDLD-Funktionen überschneiden sich teilweise, teilweise in dem Sinne, dass beide vor STP-Ausfällen schützen, die durch unidirektionale Links verursacht werden. Diese

beiden Funktionen unterscheiden sich sowohl hinsichtlich des Problemlösungsansatzes als auch hinsichtlich der Funktionalität. Insbesondere gibt es spezifische unidirektionale Ausfälle, die UDLD nicht erkennen kann, z. B. Ausfälle, die von einer CPU verursacht werden, die keine BPDUs sendet. Darüber hinaus kann die Verwendung aggressiver STP-Timer und des RSTP-Modus zu Schleifen führen, bevor UDLD die Fehler erkennen kann.

Loop Guard funktioniert nicht auf gemeinsam genutzten Links oder in Situationen, in denen die Verbindung seit der Verbindung unidirektional ist. Bei einer Verbindung, die seit der Verbindung unidirektional ist, empfängt der Port niemals BPDUs und wird designiert. Dies kann ein normales Verhalten sein, deshalb wird dieser Fall von Loop Guard nicht behandelt. UDLD bietet Schutz vor einem solchen Szenario.

Die Aktivierung von UDLD und Loop Guard bietet ein Höchstmaß an Schutz. Weitere Informationen zum Funktionsvergleich zwischen Loop Guard und UDLD finden Sie unter:

- *Loop Guard und Unidirectional Link Detection* im Abschnitt der Spanning Tree Protocol-Erweiterungen unter Verwendung von Loop Guard- und BPDU Skew Detection-Funktionen
- Abschnitt UDLD dieses Dokuments

Empfehlung von Cisco

Cisco empfiehlt die globale Aktivierung von Loop Guard in einem Switch-Netzwerk mit physischen Schleifen. Sie können Loop Guard global auf allen Ports aktivieren. Tatsächlich ist diese Funktion für alle Point-to-Point-Verbindungen aktiviert. Die Point-to-Point-Verbindung wird durch den Duplexstatus der Verbindung erkannt. Wenn die Duplexeinheit voll ist, wird die Verbindung als Punkt-zu-Punkt betrachtet.

```
Switch(config)#spanning-tree loopguard default
```

Weitere Optionen

Für Switches, die keine globale Loop Guard-Konfiguration unterstützen, wird empfohlen, die Funktion auf allen einzelnen Ports zu aktivieren, die Port-Channel-Ports umfasst. Obwohl es keine Vorteile gibt, wenn Sie Loop Guard auf einem designierten Port aktivieren, sollten Sie die Aktivierung nicht als Problem betrachten. Darüber hinaus kann eine gültige Spanning Tree Rekonvergenz einen designierten Port tatsächlich in einen Root-Port umwandeln, was die Funktion für diesen Port nützlich macht.

```
Switch(config)#interface type slot#/port#
Switch(config-if)#spanning-tree guard loop
```

Für Netzwerke mit schleifenfreien Topologien kann bei versehentlicher Schleifenschaltung weiterhin ein Loop Guard eingesetzt werden. Die Aktivierung von Loop Guard in dieser Topologie kann jedoch zu Problemen bei der Netzwerkisolierung führen. Wenn Sie eine schleifenfreie Topologie erstellen und Probleme mit der Netzwerkisolierung vermeiden möchten, können Sie Loop Guard global oder einzeln deaktivieren. Aktivieren Sie kein Loop Guard für gemeinsam genutzte Links.

```
Switch(config)#no spanning-tree loopguard default
!--- This is the global configuration.
```

oder

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no spanning-tree guard loop
!--- This is the interface configuration.
```

Spanning Tree Root Guard

Die Root Guard-Funktion bietet eine Möglichkeit, die Root Bridge-Platzierung im Netzwerk durchzusetzen. Root Guard stellt sicher, dass der Port, auf dem Root Guard aktiviert ist, der designierte Port ist. Normalerweise sind Root Bridge-Ports alle designierten Ports, es sei denn, zwei oder mehr Ports der Root Bridge sind miteinander verbunden. Wenn die Bridge überlegene STP-BPDUs auf einem Port mit aktiviertem Root Guard empfängt, verschiebt sie diesen Port in einen Root-inkonsistenten STP-Status. Dieser Status ist inkonsistent und entspricht im Prinzip einem Listening-Zustand. Über diesen Port wird kein Datenverkehr weitergeleitet. Auf diese Weise erzwingt der Root Guard die Position der Root-Bridge. Root Guard ist bereits ab Version 12.1E der Cisco IOS Software verfügbar.

Überblick

Root Guard ist ein integrierter STP-Mechanismus. Root Guard hat keinen eigenen Timer und verlässt sich nur auf den Empfang von BPDUs. Wenn Root Guard auf einen Port angewendet wird, wird diesem Port die Möglichkeit verweigert, ein Root-Port zu werden. Wenn der Empfang einer BPDU eine Spanning Tree-Konvergenz auslöst, durch die ein designierter Port zu einem Root-Port wird, wird der Port in einen inkonsistenten Root-Status versetzt. Diese Syslog-Meldung veranschaulicht:

```
%SPANTREE-SP-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet2/1 on VLAN0010
```

Wenn der Port keine überlegenen BPDUs mehr sendet, wird der Port wieder entsperrt. Über STP wechselt der Port vom Status "Listening" zum Status "Learning" und wechselt schließlich zum Status "Forwarding" (Weiterleitung). Diese Syslog-Meldung zeigt den Übergang an:

```
%SPANTREE-SP-2-ROOTGUARD_UNBLOCK: Root guard unblocking port GigabitEthernet2/1
on VLAN0010
```

Die Wiederherstellung erfolgt automatisch. Es ist kein menschliches Eingreifen erforderlich.

Da die Root Guard erzwingt, dass ein Port designiert wird und Loop Guard nur dann wirksam ist, wenn der Port ein Root-Port oder ein alternativer Port ist, schließen sich die Funktionen gegenseitig aus. Daher können Loop Guard und Root Guard nicht gleichzeitig auf einem Port aktiviert werden.

Weitere Informationen finden Sie unter Spanning Tree Protocol Root Guard Enhancement.

Empfehlung von Cisco

Cisco empfiehlt, die Root Guard-Funktion an Ports zu aktivieren, die mit Netzwerkgeräten verbunden sind, die nicht direkt von der Verwaltung kontrolliert werden. Um Root Guard zu konfigurieren, verwenden Sie die folgenden Befehle, wenn Sie sich im Schnittstellenkonfigurationsmodus befinden:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#spanning-tree guard root
```

EtherChannel

Zweck

Der EtherChannel umfasst einen Algorithmus zur Frame-Verteilung, der Frames effizient über die 10/100-Mbit/s- oder Gigabit-Verbindungen der Komponente Multiplex-Verbindungen verteilt. Der Frame-Distribution-Algorithmus ermöglicht das inverse Multiplexing mehrerer Kanäle in einer einzigen logischen Verbindung. Obwohl sich jede Plattform von der nächsten Plattform bei der Implementierung unterscheidet, müssen Sie die folgenden allgemeinen Eigenschaften verstehen:

- Es muss ein Algorithmus geben, um Frames statistisch über mehrere Kanäle zu multiplizieren. Bei Catalyst Switches ist dies hardwarebezogen. Hier einige Beispiele:Catalyst 5500/5000s: Vorhandensein oder Fehlen eines Ethernet Bundling Chip (EBC) auf dem ModulCatalyst 6500/6000 - Ein Algorithmus, der weiter in den Frame eingelesen und durch die IP-Adresse multipliziert werden kann
- Es wird ein logischer Kanal erstellt, sodass eine einzelne STP-Instanz ausgeführt oder ein einziges Routing-Peering verwendet werden kann. Dies hängt davon ab, ob es sich um einen Layer-2- oder Layer-3-EtherChannel handelt.
- Es gibt ein Verwaltungsprotokoll, das die Parameterkonsistenz an beiden Enden der Verbindung überprüft und die gebündelte Wiederherstellung nach Verbindungsausfall oder Hinzufügen unterstützt. Bei diesem Protokoll kann es sich um PAgP oder Link Aggregation Control Protocol (LACP) handeln.

Überblick

Der EtherChannel umfasst einen Algorithmus zur Frame-Verteilung, der Frames effizient über die Komponenten 10/100-Mbit/s-, Gigabit- oder 10-Gigabit-Verbindungen Multiplexing-Verbindungen verteilt. Unterschiede bei Algorithmen pro Plattform ergeben sich aus der Fähigkeit der einzelnen Hardware-Typen, Frame-Header-Informationen zu extrahieren, um die Distributionsentscheidung zu treffen.

Der Lastverteilungsalgorithmus ist eine globale Option für beide Kanalsteuerungsprotokolle. PAgP und LACP verwenden den Frame-Verteilungsalgorithmus, da der IEEE-Standard keine bestimmten Verteilungsalgorithmen zulässt. Jeder Verteilungsalgorithmus stellt jedoch sicher, dass beim Empfang von Frames der Algorithmus nicht die Fehlordnung von Frames verursacht, die Teil einer bestimmten Konversation sind, oder die Vervielfältigung von Frames.

In dieser Tabelle wird detailliert der Frame-Verteilungsalgorithmus für jede aufgelistete Plattform veranschaulicht:

Plattform	Channel Load Balancing-Algorithmus
Catalyst Serie 3750	Catalyst 3750, der einen Lastenausgleich-Algorithmus der Cisco IOS Software ausführt, der MAC-Adressen oder IP-Adressen sowie die Quelle oder das Ziel der Nachrichten oder beides verwendet.
Cata	Catalyst 4500, der einen Lastenausgleich-

lyst Serie 4500	Algorithmus der Cisco IOS Software ausführt, der MAC-Adressen, IP-Adressen oder Layer-4-Portnummern (L4) und entweder die Nachrichtenquelle oder das Nachrichtenziel oder beides verwendet.
Catalyst Serie 6500/6000	Es können zwei Hashing-Algorithmen verwendet werden, die von der Supervisor Engine-Hardware abhängen. Der Hash ist ein polynomisches Siebzehnter Grad, das in der Hardware implementiert wird. In allen Fällen übernimmt der Hash die MAC-, IP- oder IP-TCP/UDP-Portnummer und wendet den Algorithmus an, um einen 3-Bit-Wert zu generieren. Dieser Prozess wird für die SAs und DAs separat durchgeführt. Der XOR-Vorgang wird dann mit den Ergebnissen verwendet, um einen weiteren 3-Bit-Wert zu generieren. Der Wert legt fest, welcher Port im Kanal zum Weiterleiten des Pakets verwendet wird. Die Kanäle des Catalyst 6500/6000 können zwischen den Ports eines Moduls gebildet werden und können bis zu acht Ports umfassen.

Diese Tabelle zeigt die Verteilungsmethoden, die von den verschiedenen Catalyst 6500/6000 Supervisor Engine-Modellen unterstützt werden. Die Tabelle zeigt auch das Standardverhalten:

Hardware	Beschreibung	Verteilungsmethoden
WS-F6020A (Layer-2-Engine) WS-F6K-PFC (Layer-3-Engine)	Spätere Supervisor Engine I und Supervisor Engine IA Supervisor Engine IA/Policy Feature Card 1 (PFC1)	Layer-2-MAC: SA; DA; SA- und DA Layer 3-IP: SA; DA; SA und DA (Standard)
WS-F6K-PFC 2	Supervisor Engine II/PFC2	Layer-2-MAC: SA; DA; SA- und DA Layer 3-IP: SA; DA; SA- und DA-Sitzung (Standard) Layer 4: S-Hafen; D-Port; S- und D-Port
WS-F6K-PFC3A WS-F6K-PFC3B WS-F6K-PFC3BXL	Supervisor Engine 720/PFC3A Supervisor Engine 720/Supervisor Engine 32/PFC3B Supervisor Engine 720/PFC3BXL	Layer-2-MAC: SA; DA; SA- und DA Layer 3-IP: SA; DA; SA- und DA-Sitzung (Standard) Layer 4: S-Hafen; D-Port; S- und D-Port

Hinweis: Bei der Layer-4-Distribution verwendet das erste fragmentierte Paket die Layer-4-Distribution. Alle nachfolgenden Pakete verwenden die Layer-3-Distribution.

Hinweis: Weitere Informationen zur EtherChannel-Unterstützung auf anderen Plattformen und zur Konfiguration und Fehlerbehebung für EtherChannel finden Sie in diesen Dokumenten:

- Grundlegendes zum EtherChannel-Lastenausgleich und zur Redundanz auf Catalyst-Switches
- Konfigurieren von Layer 3 und Layer 2 EtherChannel (Cisco IOS Software Configuration Guide Catalyst 6500, 12.2SX)
- Konfigurieren von Layer 3 und Layer 2 EtherChannel (Cisco IOS Software Configuration Guide Catalyst 6500 Series, 12.1E)
- Konfigurieren von EtherChannel (Catalyst Switch der Serie 4500, Cisco IOS Software Configuration Guide, 12.2(31)SG)
- Konfigurieren von EtherChannels (Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE)
- Konfigurieren Sie den EtherChannel zwischen Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000, die CatOS-Systemsoftware ausführen

Empfehlung von Cisco

Die Switches der Serien Catalyst 3750, Catalyst 4500 und Catalyst 6500/6000 führen Load Balancing durch, indem sie standardmäßig sowohl die Quell- als auch die Ziel-IP-Adressen hashen. Dies wird unter der Annahme empfohlen, dass IP das vorherrschende Protokoll ist. Geben Sie diesen Befehl ein, um den Lastenausgleich festzulegen:

```
port-channel load-balance src-dst-ip
!--- This is the default.
```

Weitere Optionen

Je nach Datenverkehrsfluss können Sie die Layer-4-Verteilung verwenden, um den Lastenausgleich zu verbessern, wenn der Großteil des Datenverkehrs zwischen derselben Quell- und Ziel-IP-Adresse verläuft. Wenn die Layer-4-Distribution konfiguriert ist, muss klar sein, dass das Hashing nur Quell- und Zielports für Layer 4 umfasst. Es werden keine Layer-3-IP-Adressen in den Hashing-Algorithmus kombiniert. Geben Sie diesen Befehl ein, um den Lastenausgleich festzulegen:

```
port-channel load-balance src-dst-port
```

Hinweis: Die Layer-4-Distribution kann auf Catalyst Switches der Serie 3750 nicht konfiguriert werden.

Geben Sie den Befehl **show etherchannel load-balance** ein, um die Frame-Verteilungsrichtlinie zu überprüfen.

Abhängig von den Hardwareplattformen können Sie CLI-Befehle verwenden, um zu bestimmen, welche Schnittstelle im EtherChannel den bestimmten Datenverkehrsfluss weiterleitet, wobei die Frame-Verteilungsrichtlinie als Grundlage dient.

Geben Sie für Catalyst 6500-Switches den Befehl **remote login switch** ein, um sich remote bei der Switch Processor (SP)-Konsole anzumelden. Geben Sie dann die *Port-Channel-Nummer* ***{ip} für den Test-Etherchannel-Lastenausgleich ein.*** **| l4port | mac} [***source_ip_add* | *source_mac_add* |

source_l4_port] [*dest_ip_add* | *dest_mac_add* | *dest_l4_port*]-Befehl.

Geben Sie für Catalyst 3750-Switches die **Test-Ethernet-Lastenausgleich-Schnittstelle *Port-Channel-Nummer* {ip | mac} [*source_ip_add* | *source_mac_add*] [*dest_ip_add* Befehl | *dest_mac_add*]**.

Für Catalyst 4500 ist der entsprechende Befehl noch nicht verfügbar.

EtherChannel-Konfigurationsrichtlinien und -beschränkungen

EtherChannel überprüft die Porteigenschaften aller physischen Ports, bevor er kompatible Ports zu einem einzelnen logischen Port aggregiert. Konfigurationsrichtlinien und -beschränkungen variieren je nach Switch-Plattform. Vervollständigen Sie diese Richtlinien und Einschränkungen, um Probleme bei der Bündelung zu vermeiden. Wenn beispielsweise QoS aktiviert ist, werden bei der Bündelung von Switching-Modulen der Catalyst 6500-/6000-Serie mit unterschiedlichen QoS-Funktionen keine EtherChannels gebildet. Für Catalyst 6500-Switches, auf denen die Cisco IOS Software ausgeführt wird, können Sie die QoS-Port-Attributprüfung für die EtherChannel-Bündelung mit dem Schnittstellenbefehl **no mls qos channel-consistency**-port-channel deaktivieren. Der Befehl **show interface fähigkeit *mod/port* zeigt die QoS-Portfunktion an und stellt fest, ob die Ports kompatibel sind.**

Beachten Sie die folgenden Richtlinien für verschiedene Plattformen, um Konfigurationsprobleme zu vermeiden:

- Konfigurieren von Layer 3 und Layer 2 EtherChannel (Cisco IOS Software Configuration Guide Catalyst 6500, 12.2SX)
- Konfigurieren von Layer 3 und Layer 2 EtherChannel (Cisco IOS Software Configuration Guide Catalyst 6500 Series, 12.1E)
- Konfigurieren von EtherChannel (Catalyst Switch der Serie 4500, Cisco IOS Software Configuration Guide, 12.2(31)SG)
- Konfigurieren von EtherChannels (Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE)

Die maximale Anzahl unterstützter EtherChannels hängt auch von der Hardwareplattform und den Softwareversionen ab. Catalyst Switches der Serie 6500 mit Cisco IOS Software, Version 12.2(18)SXE, unterstützen bis zu 128 Port-Channel-Schnittstellen. Softwareversionen, die älter sind als die Cisco IOS Software, Version 12.2(18)SXE, unterstützen maximal 64 Port-Channel-Schnittstellen. Die konfigurierbare Gruppennummer kann unabhängig von der Softwareversion zwischen 1 und 256 liegen. Die Catalyst Switches der Serie 4500 unterstützen maximal 64 EtherChannels. Für Catalyst 3750-Switches wird empfohlen, nicht mehr als 48 EtherChannels auf dem Switch-Stack zu konfigurieren.

Berechnung der Spanning Tree-Port-Kosten

Sie müssen die Spanning-Tree-Port-Kostenberechnung für EtherChannels verstehen. Sie können die Spanning-Tree-Port-Kosten für EtherChannels entweder mit der kurzen oder der langen Methode berechnen. Die Port-Kosten werden standardmäßig im Kurzmodus berechnet.

In dieser Tabelle werden die Spanning-Tree-Port-Kosten für einen Layer-2-EtherChannel anhand der Bandbreite veranschaulicht:

Bandbreite	Alter STP-Wert	Neuer Long STP-Wert

10 Mbit/s	100	2.000.000
100 Mbit/s	19	200.000
1 Gbit/s	4	20.000
N x 1 Gbit/s	1	660
10 Gbit/s	2	2.000
100 Gbit/s	K/A	200
1 Tbit/s	K/A	20
10 Tbit/s	K/A	2

Hinweis: In CatOS bleiben die Spanning-Tree-Port-Kosten für einen EtherChannel unverändert, nachdem die Verbindung der Port-Channel-Mitglieder ausfällt. In der Cisco IOS-Software werden die Port-Kosten für den EtherChannel sofort aktualisiert, um die neue verfügbare Bandbreite wiederzugeben. Wenn das gewünschte Verhalten darin besteht, unnötige Änderungen der Spanning-Tree-Topologie zu vermeiden, können Sie die Kosten für den Spanning-Tree-Port statisch mithilfe des **Spanning-Tree-*Kostenbefehls*** konfigurieren.

Port Aggregation Protocol (PAgP)

Zweck

PAgP ist ein Verwaltungsprotokoll, das die Parameterkonsistenz an beiden Enden der Verbindung überprüft. PAgP unterstützt den Kanal auch bei der Anpassung an Verbindungsausfälle oder -additionen. PAgP zeichnet sich durch folgende Merkmale aus:

- PAgP erfordert, dass alle Ports im Kanal demselben VLAN angehören oder als Trunk-Ports konfiguriert sind. Da dynamische VLANs den Wechsel eines Ports in ein anderes VLAN erzwingen können, sind dynamische VLANs nicht in die EtherChannel-Teilnahme einbezogen.
- Wenn bereits ein Paket vorhanden ist und die Konfiguration eines Ports geändert wird, werden alle Ports im Paket entsprechend dieser Konfiguration geändert. Ein Beispiel für eine solche Änderung ist eine Änderung des VLAN- oder `Trunking`-Modus.
- PAgP gruppiert keine Ports, die mit unterschiedlichen Geschwindigkeiten oder Port-Duplex betrieben werden. Wenn Geschwindigkeit und Duplex geändert werden, wenn ein Paket vorhanden ist, ändert PAgP die Portgeschwindigkeit und die Duplexfunktion für alle Ports im Paket.

Überblick

Der PAgP-Port steuert jeden einzelnen physischen (oder logischen) Port, der gruppiert werden soll. Zum Senden von PAgP-Paketen wird dieselbe Multicast-Gruppen-MAC-Adresse verwendet, die auch für CDP-Pakete verwendet wird. Die MAC-Adresse lautet 01-00-0c-cc-cc-cc. Der Protokollwert ist jedoch 0x0104. Dies ist eine Zusammenfassung der Protokolloperation:

- Solange der physische Port aktiv ist, werden PAgP-Pakete während der Erkennung jede Sekunde und im Steady-State alle 30 Sekunden übertragen.
- Wenn Datenpakete empfangen werden, aber keine PAgP-Pakete empfangen werden, wird davon ausgegangen, dass der Port mit einem Gerät verbunden ist, das nicht PAgP-fähig ist.
- Achten Sie auf PAgP-Pakete, die belegen, dass der physische Port eine bidirektionale Verbindung zu einem anderen PAgP-fähigen Gerät aufweist.
- Sobald zwei dieser Pakete auf einer Gruppe physischer Ports empfangen werden, versuchen

Sie, einen aggregierten Port zu bilden.
- Wenn PAgP-Pakete für einen bestimmten Zeitraum anhalten, wird der `PAgP-`Status beendet.

Normale Verarbeitung

Diese Konzepte helfen, das Verhalten des Protokolls zu veranschaulichen:

- Agport - Ein logischer Port, der aus allen physischen Ports in derselben Aggregation besteht und durch einen eigenen SNMP ifIndex identifiziert werden kann. Ein Port enthält keine nicht betriebsbereiten Ports.
- Channel (Kanal): Eine Aggregation, die die Formationskriterien erfüllt. Ein Kanal kann nicht betriebsbereite Ports enthalten und ist eine übergeordnete Gruppe von Ports. Protokolle, zu denen STP und VTP gehören, jedoch CDP und DTP nicht gehören, werden über PAgP über die Ports ausgeführt. Keines dieser Protokolle kann Pakete senden oder empfangen, bis PAgP die Ports an einen oder mehrere physische Ports anbindet.
- Gruppenfunktion - Jeder physische Port und jeder Port verfügt über einen Konfigurationsparameter, der als `Gruppenfunktion` bezeichnet wird. Ein physischer Port kann mit jedem anderen physischen Port, der die gleiche `Gruppenfunktion` hat, und nur mit einem solchen physischen Port aggregiert werden.
- Aggregationsverfahren - Wenn ein physischer Port den `UpData`- oder `UpPAgP-`Status erreicht, wird der Port an einen geeigneten Port angeschlossen. Wenn der Port einen dieser Status für einen anderen Status verlässt, wird der Port vom Port getrennt.

Diese Tabelle enthält weitere Details zu den Zuständen:

Staat	Bedeutung
`UpData`	Es wurden keine PAgP-Pakete empfangen. PAgP-Pakete werden gesendet. Der physische Port ist der einzige Port, der mit dem Port verbunden ist. Nicht-PAgP-Pakete werden zwischen dem physischen Port und dem Port ein- und ausgeleitet.
`BiDir`	Genau ein PAgP-Paket wurde empfangen, das eine bidirektionale Verbindung mit genau einem Nachbarn nachweist. Der physische Port ist mit keinem Port verbunden. PAgP-Pakete werden gesendet und können empfangen werden.
`UpPAgP`	Dieser physische Port ist möglicherweise in Verbindung mit anderen physischen Ports mit einem Port verbunden. PAgP-Pakete werden auf dem physischen Port gesendet und empfangen. Nicht-PAgP-Pakete werden zwischen dem physischen Port und dem Port ein- und ausgeleitet.

Beide Enden beider Verbindungen müssen sich auf die Gruppierung einigen. Die Gruppierung wird als die größte Gruppe von Ports im Port definiert, die beide Enden der Verbindungsgenehmigung haben.

Wenn ein physischer Port den `UpPAgP-`Status erreicht, wird der Port dem Port zugewiesen, der über physische Mitglieds-Ports verfügt, die mit der `Gruppenfunktion` des neuen physischen Ports übereinstimmen und sich im `BiDir-` oder `UpPAgP-`Zustand befinden. Alle `BiDir-`Ports werden

gleichzeitig in den `UpPAgP`-Status verschoben. Wenn kein Port über physische Port-Parameter verfügt, die mit dem neu fertig gestellten physischen Port kompatibel sind, wird der Port einem Port mit geeigneten Parametern zugewiesen, die keine zugehörigen physischen Ports haben.

Ein PAgP-Timeout kann beim letzten Nachbarn auftreten, der auf dem physischen Port bekannt ist. Der Port, der das Zeitlimit überschreitet, wird aus dem Port entfernt. Gleichzeitig werden alle physischen Ports auf dem gleichen Port, die Timer aufweisen, die auch das Timeout erreicht haben, entfernt. Dadurch kann ein Agent, dessen anderes Ende verendet ist, gleichzeitig und nicht mehr jeweils ein physischer Port beendet werden.

Verhalten im Fehlerfall

Wenn ein Link in einem vorhandenen Kanal fehlschlägt, wird der Port aktualisiert, und der Datenverkehr wird über die Links gehasht, die unverändert bleiben. Beispiele für solche Fehler:

- Port ist nicht angeschlossen
- Gigabit Interface Converter (GBIC) wird entfernt
- Glasfaser ist defekt

Hinweis: Wenn ein Link in einem Kanal bei ausgeschaltetem oder abgenommenem Modul ausfällt, kann sich das Verhalten ändern. Ein Kanal benötigt definitionsgemäß zwei physische Ports. Wenn ein Port in einem Kanal mit zwei Ports vom System verloren geht, wird der logische Port abgebrochen und der ursprüngliche physische Port mit Bezug auf Spanning Tree neu initialisiert. Datenverkehr kann verworfen werden, bis STP es ermöglicht, dass der Port wieder für Daten verfügbar ist.

Dieser Unterschied in den beiden Fehlermodi ist wichtig, wenn Sie die Wartung eines Netzwerks planen. Es kann eine Änderung der STP-Topologie geben, die Sie berücksichtigen müssen, wenn Sie ein Modul online entfernen oder einfügen. Sie müssen jede physische Verbindung im Kanal mit dem Netzwerkmanagementsystem (NMS) verwalten, da der Port bei einem Ausfall ungestört bleiben kann.

Vervollständigen Sie eine dieser Empfehlungen, um unerwünschte Topologieänderungen beim Catalyst 6500/600 zu vermeiden:

- Wenn pro Modul ein einzelner Port verwendet wird, um einen Kanal zu bilden, sollten Sie drei oder mehr Module verwenden (insgesamt drei).
- Wenn der Kanal zwei Module umfasst, verwenden Sie zwei Ports für jedes Modul (insgesamt vier).
- Wenn ein Zweiport-Kanal für zwei Karten erforderlich ist, verwenden Sie nur die Supervisor Engine-Ports.

Konfigurationsoptionen

Sie können EtherChannels in verschiedenen Modi konfigurieren, wie in dieser Tabelle zusammengefasst:

Modus	Konfigurierbare Optionen
`Ein`	PAgP ist nicht in Betrieb. Die Port-Channels, unabhängig von der Konfiguration des Nachbarports. Wenn der Nachbarport-Modus `aktiviert` ist, wird ein Kanal gebildet.

Automatisch	Die Aggregation wird von PAgP gesteuert. Ein Hafen wird in einen passiven Verhandlungszustand versetzt. PAgP-Pakete werden erst an die Schnittstelle gesendet, wenn mindestens ein PAgP-Paket empfangen wurde, das anzeigt, dass der Sender im wünschenswerten Modus arbeitet.
wünschenswert	Die Aggregation wird von PAgP gesteuert. Ein Port wird in einen aktiven Verhandlungsstatus versetzt, in dem der Port Verhandlungen mit anderen Ports über die Übertragung von PAgP-Paketen einleitet. Ein Kanal wird mit einer anderen Portgruppe im wünschenswerten oder automatischen Modus gebildet.
Non-Silent Dies ist die Standardeinstellung für Catalyst 5500/500 FE- und GE-Glasfaser-Ports.	Ein auto- oder wish mode-Schlüsselwort. Wenn auf der Schnittstelle keine Datenpakete empfangen werden, wird die Schnittstelle nie an einen Port angeschlossen und kann nicht für Daten verwendet werden. Diese Bidirectional Check (Bidirektionalitätsprüfung) wurde für bestimmte Catalyst 5500/500-Hardware durchgeführt, da bei einigen Verbindungsausfällen ein Kanalabbruch stattfand. Wenn Sie den Nicht-Silent-Modus aktivieren, darf ein sich erholender Nachbar-Port nie wieder hochfahren und den Kanal unnötigerweise auseinanderbrechen. Die Hardware der Catalyst Serien 4500/4000 und 6500/6000 bietet standardmäßig flexiblere Pakete und verbesserte Prüfungen der Bidirektionalität.
Silent Dies ist der Standardwert für alle Catalyst 6500/6000- und 4500/4000-Ports sowie für 5500/5000-Kupfer-Ports.	Ein auto- oder wish mode-Schlüsselwort. Wenn auf der Schnittstelle keine Datenpakete empfangen werden, wird die Schnittstelle nach einer Zeitüberschreitungszeit von 15 Sekunden allein an einen Port angeschlossen. So kann die Schnittstelle für die Datenübertragung verwendet werden. Der Silent Mode ermöglicht auch den Kanalbetrieb, wenn der Partner Analyzer oder Server sein kann, der PAgP nie sendet.

Die Standby-/Nicht-Stummschaltung-Einstellungen beeinflussen die Reaktion von Ports auf Situationen, die unidirektionalen Datenverkehr verursachen. Wenn ein Port aufgrund einer ausgefallenen physischen Schnittstelle oder einer defekten Glasfaser oder eines defekten Kabels nicht übertragen werden kann, kann der Nachbarport weiterhin betriebsbereit bleiben. Der Partner

übermittelt weiterhin Daten. Daten gehen jedoch verloren, da kein Rückgabeverkehr empfangen werden kann. Spanning-Tree-Schleifen können sich auch aufgrund der unidirektionalen Natur der Verbindung bilden.

Einige Glasfaser-Ports haben die gewünschte Funktion, den Port in einen nicht betriebsbereiten Zustand zu versetzen, wenn der Port sein Empfangssignal (FEFI) verliert. Diese Aktion führt dazu, dass der Partner-Port nicht mehr betriebsbereit ist und die Ports an beiden Enden der Verbindung tatsächlich ausfallen.

Wenn Sie Geräte verwenden, die Daten übertragen (BPDUs), und unidirektionale Bedingungen nicht erkennen können, verwenden Sie den `nicht-stummen` Modus, damit die Ports nicht betriebsbereit bleiben, bis Empfangsdaten vorhanden sind und die Verbindung als bidirektional verifiziert wird. PAgP benötigt zum Erkennen einer unidirektionalen Verbindung etwa 3,5 * 30 Sekunden = 105 Sekunden. Dreißig Sekunden ist die Zeit zwischen zwei aufeinander folgenden PAgP-Nachrichten. Verwenden Sie UDLD, ein schnellerer Detektor für unidirektionale Verbindungen.

Wenn Sie Geräte verwenden, die keine Daten übertragen, verwenden Sie den `Stummmodus`. Die Verwendung des `Silent`-Modus bewirkt, dass der Port angeschlossen und betriebsbereit ist, unabhängig davon, ob empfangene Daten vorhanden sind oder nicht. Darüber hinaus wird für Ports, die das Vorhandensein einer unidirektionalen Bedingung erkennen können, standardmäßig der `Silent-`Modus verwendet. Beispiele für diese Ports sind neuere Plattformen, die Layer-1-FEFI und UDLD verwenden.

Geben Sie den Befehl **no channel-group** *number* (**keine Kanalgruppennummer**) an, um das Channeling auf einer Schnittstelle zu deaktivieren:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no channel-group 1
```

Überprüfung

Die Tabelle in diesem Abschnitt bietet eine Zusammenfassung aller möglichen PAgP-Channeling-Szenarien zwischen zwei direkt verbundenen Switches, Switch A und Switch B. Einige dieser Kombinationen können dazu führen, dass STP die Ports auf der Channeling-Seite in den `fehlerhaften` Zustand versetzt, was bedeutet, dass diese Kombinationen die Ports auf der Channeling-Seite herunterfahren. Die Funktion "EtherChannel Misconfiguration Guard" ist standardmäßig aktiviert.

Channel-Modus wechseln	Switch B Channel-Modus	Kanal-Status wechseln	Switch B Channel-Staat
Ein	Ein	Kanal (nicht PAgP)	Kanal (nicht PAgP)
Ein	Nicht konfiguriert	Not Channel (ErrDisable)	Kein Channel
Ein	Automatisch	Not Channel (ErrDisable	Kein Channel

		)	
Ein	wünschenswert	Not Channel (ErrDisable)	Kein Channel
Nicht konfiguriert	Ein	Kein Channel	Not Channel (ErrDisable)
Nicht konfiguriert	Nicht konfiguriert	Kein Channel	Kein Channel
Nicht konfiguriert	Automatisch	Kein Channel	Kein Channel
Nicht konfiguriert	wünschenswert	Kein Channel	Kein Channel
Automatisch	Ein	Kein Channel	Not Channel (ErrDisable)
Automatisch	Nicht konfiguriert	Kein Channel	Kein Channel
Automatisch	Automatisch	Kein Channel	Kein Channel
Automatisch	wünschenswert	PAgP-Kanal	PAgP-Kanal
wünschenswert	Ein	Kein Channel	Kein Channel
wünschenswert	Nicht konfiguriert	Kein Channel	Kein Channel
wünschenswert	Automatisch	PAgP-Kanal	PAgP-Kanal
wünschenswert	wünschenswert	PAgP-Kanal	PAgP-Kanal

Cisco Konfigurationsempfehlung für L2-Kanäle

Aktivieren Sie PAgP, und verwenden Sie eine Einstellung für `wünschenswert` für alle EtherChannel-Verbindungen. Weitere Informationen finden Sie in dieser Ausgabe:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no ip address
!--- This ensures that there is no IP !--- address that is assigned to the LAN port.
Switch(config-if)#channel-group number mode desirable
!--- Specify the channel number and the PAgP mode.
```

Überprüfen Sie die Konfiguration folgendermaßen:

```
Switch#show run interface port-channel number
Switch#show running-config interface type slot#/port#
Switch#show interfaces type slot#/port# etherchannel
Switch#show etherchannel number port-channel
```

Verhindern von Fehlern bei der EtherChannel-Konfiguration

Sie können einen EtherChannel falsch konfigurieren und eine Spanning-Tree-Schleife erstellen. Diese Fehlkonfiguration kann den Switch-Prozess überfordern. Die Cisco IOS-Systemsoftware umfasst die **Spanning-Tree-Etherchannel-Guard-**Funktion zur **fehlerhaften Konfiguration**, um dieses Problem zu vermeiden.

Führen Sie diesen Konfigurationsbefehl auf allen Catalyst Switches aus, auf denen die Cisco IOS Software als Systemsoftware ausgeführt wird:

```
Switch(config)#spanning-tree etherchannel guard misconfig
```

Weitere Optionen

Wenn zwei Geräte kanalisiert werden, die PAgP nicht unterstützen, aber LACP unterstützen, wird empfohlen, LACP mit der Konfiguration von LACP zu aktivieren, das an beiden Enden der Geräte aktiv ist. Weitere Informationen finden Sie im Abschnitt Link Aggregation Control Protocol (LACP) dieses Dokuments.

Wenn Sie den Kanal an Geräte weiterleiten, die PAgP oder LACP nicht unterstützen, müssen Sie den Kanal `einschalten`. Diese Anforderung gilt für die folgenden Geräte:

- Server
- Lokaler Leiter
- Content-Switches
- Router
- Switches mit früherer Software
- Catalyst Switches der Serie 2900XL/3500XL
- Catalyst 8540

Geben Sie folgende Befehle ein:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#channel-group number mode on
```

Link Aggregation Control Protocol (LACP)

LACP ist ein Protokoll, mit dem Ports mit ähnlichen Merkmalen durch dynamische Aushandlung mit benachbarten Switches einen Kanal bilden können. PAgP ist ein proprietäres Protokoll von Cisco, das Sie nur auf Cisco Switches und Switches ausführen können, für die Lizenzgeber eine Lizenz erwerben. LACP, das in IEEE 802.3ad definiert ist, ermöglicht Cisco Switches jedoch die Verwaltung von Ethernet-Channeling mit Geräten, die der 802.3ad-Spezifikation entsprechen.

LACP wird von den folgenden Plattformen und Versionen unterstützt:

- Catalyst 6500/6000-Serie mit Cisco IOS Software Release 12.1(11b)EX und höher
- Catalyst Serie 4500 mit Cisco IOS Software, Version 12.1(13)EW und höher
- Catalyst Serie 3750 mit Cisco IOS Software Version 12.1(14)EA1 und höher

In Bezug auf die Funktion gibt es kaum Unterschiede zwischen LACP und PAgP. Beide Protokolle unterstützen maximal acht Ports in jedem Kanal, und die gleichen Porteigenschaften werden vor dem Bündeln überprüft. Zu diesen Porteigenschaften gehören:

- Geschwindigkeit
- Duplex
- Natives VLAN und Trunking-Typ

Die wesentlichen Unterschiede zwischen LACP und PAgP sind:

- Das LACP-Protokoll kann nur auf Vollduplex-Ports ausgeführt werden und unterstützt keine Halbduplex-Ports.
- Das LACP-Protokoll unterstützt Hot-Standby-Ports. LACP versucht immer, die maximale Anzahl kompatibler Ports in einem Kanal zu konfigurieren, bis zu dem Maximum, das die Hardware zulässt (acht Ports). Wenn LACP nicht in der Lage ist, alle kompatiblen Ports zusammenzufassen (z. B. wenn das Remote-System restriktivere Hardware-Beschränkungen aufweist), werden alle Ports, die nicht aktiv in den Kanal eingeschlossen werden können, im Hot-Standby-Zustand versetzt und nur verwendet, wenn einer der verwendeten Ports ausfällt.

Hinweis: Für Catalyst Switches der Serie 4500 beträgt die maximale Anzahl von Ports, für die Sie denselben Administratorschlüssel zuweisen können, acht. Bei Catalyst Switches der Serien 6500 und 3750, auf denen die Cisco IOS Software ausgeführt wird, versucht LACP, die maximale Anzahl kompatibler Ports in einem EtherChannel zu konfigurieren, bis zu dem Maximum, das die Hardware zulässt (acht Ports). Weitere acht Ports können als Hot-Standby-Ports konfiguriert werden.

Überblick

Das LACP steuert jeden einzelnen physischen (oder logischen) Port, der gebündelt werden soll. LACP-Pakete werden unter Verwendung der MAC-Adresse der Multicast-Gruppe **01-80-c2-00-00-02** gesendet. Der Typ/Feldwert ist 0x8809 mit dem Subtyp 0x01. Dies ist eine Zusammenfassung der Protokolloperation:

- Das Protokoll verwendet die Geräte, um ihre Aggregationsfunktionen und Zustandsinformationen anzugeben. Die Übertragungen werden regelmäßig auf jeder aggregierbaren Verbindung gesendet.
- Solange der physische Port aktiv ist, werden während der Erkennung alle zwei Sekunden und im Steady-State alle 30 Sekunden LACP-Pakete übertragen.
- Die Partner auf einem aggregierbaren Link überwachen die im Protokoll gesendeten Informationen und legen fest, welche Aktionen oder Aktionen sie durchführen sollen.
- Kompatible Ports werden in einem Kanal konfiguriert, bis zu dem Maximum, das die Hardware zulässt (acht Ports).
- Die Aggregationen werden durch den regelmäßigen, zeitnahen Austausch aktueller Statusinformationen zwischen den Verbindungspartnern verwaltet. Wenn sich die Konfiguration ändert (z. B. aufgrund eines Verbindungsausfalls), wird von den Protokollpartnern eine Zeitüberschreitung verzeichnet, und es werden entsprechend des neuen Systemstatus die entsprechenden Maßnahmen ergriffen.
- Zusätzlich zu periodischen LACP-Dateneinheiten (LACPDU)-Übertragungen überträgt das Protokoll bei Änderungen der Statusinformationen eine ereignisgesteuerte LACPDU an die Partner. Die Protokollpartner ergreifen je nach dem neuen Status des Systems die entsprechenden Maßnahmen.

LACP-Parameter

Damit LACP ermitteln kann, ob eine Reihe von Verbindungen mit demselben System verbunden sind und ob diese Verbindungen aus Sicht der Aggregation kompatibel sind, muss Folgendes

festgelegt werden können:

- Eine global eindeutige Kennung für jedes System, das an der Link-Aggregation beteiligt ist.Jedes System, das LACP ausführt, muss eine Priorität zugewiesen werden, die entweder automatisch (mit der Standardpriorität von 32768) oder vom Administrator ausgewählt werden kann. Die Systempriorität wird hauptsächlich in Verbindung mit der MAC-Adresse des Systems verwendet, um die System-ID zu bilden.
- Eine Methode zur Identifizierung der Funktionen, die jedem Port und jedem Aggregator zugeordnet sind, wie von einem bestimmten System verstanden.Jeder Port im System muss entweder automatisch (mit der Standardpriorität von 128) oder vom Administrator eine Priorität zugewiesen werden. Die Priorität wird zusammen mit der Portnummer verwendet, um die Port-ID zu bilden.
- Eine Methode zur Identifizierung einer Link-Aggregation-Gruppe und des zugehörigen Aggregators.Die Möglichkeit, dass ein Port mit einem anderen aggregiert, wird durch einen einfachen 16-Bit-Integer-Parameter zusammengefasst, der strikt größer als Null ist, der als Schlüssel bezeichnet wird. Jeder Schlüssel wird anhand verschiedener Faktoren bestimmt, z. B.:Die physischen Merkmale des Ports, z. B. Datenrate, Duplexität und Point-to-Point- oder gemeinsam genutztes MediumKonfigurationseinschränkungen, die vom Netzwerkadministrator festgelegt wurdenJedem Port sind zwei Schlüssel zugeordnet:Ein AdministrationsschlüsselEin BetriebsschlüsselDer administrative Schlüssel ermöglicht die Manipulation von Schlüsselwerten durch die Verwaltung und der Benutzer kann daher diesen Schlüssel auswählen. Der Betriebsschlüssel wird vom System zum Erstellen von Aggregationen verwendet. Der Benutzer kann diesen Schlüssel nicht direkt auswählen oder ändern. Die Port-Gruppe eines bestimmten Systems, die den gleichen betrieblichen Schlüsselwert haben, wird als Mitglieder derselben Schlüsselgruppe angesehen.

Daher versucht jedes System bei zwei Systemen und einer Reihe von Ports mit demselben administrativen Schlüssel, die Ports zu aggregieren, beginnend mit dem Port mit der höchsten Priorität im System mit der höchsten Priorität. Dieses Verhalten ist möglich, da jedes System die folgenden Prioritäten kennt:

- Ihre eigene Priorität, die entweder dem Benutzer oder der Software zugewiesen wurde
- Partnerpriorität, die durch LACP-Pakete erkannt wurde

Verhalten im Fehlerfall

Das Fehlerverhalten für LACP entspricht dem Fehlerverhalten für PAgP. Wenn eine Verbindung in einem vorhandenen Kanal fehlschlägt (z. B. wenn ein Port getrennt, ein GBIC entfernt oder eine Glasfaser beschädigt wird), wird der Port aktualisiert, und der Datenverkehr wird innerhalb einer Sekunde über die verbleibenden Verbindungen gehasht. Datenverkehr, der nach dem Ausfall nicht neu gestartet werden muss (d. h. Datenverkehr, der weiterhin über dieselbe Verbindung gesendet wird), geht nicht verloren. Durch die Wiederherstellung der ausgefallenen Verbindung wird ein weiteres Update des Agenten ausgelöst, und der Datenverkehr wird erneut gehasht.

Konfigurationsoptionen

Sie können LACP EtherChannels in verschiedenen Modi konfigurieren, wie in dieser Tabelle zusammengefasst:

Modus	Konfigurierbare Optionen

Ein	Die Link-Aggregation muss ohne LACP-Aushandlung gebildet werden. Der Switch sendet das LACP-Paket nicht und verarbeitet auch kein eingehendes LACP-Paket. Wenn der Port-Modus des Nachbarn aktiviert ist, wird ein Kanal gebildet.
Aus (oder) nicht konfiguriert	Der Port leitet keine Kanäle weiter, unabhängig davon, wie der Nachbar konfiguriert wurde.
Passiv (Standard)	Dies ähnelt dem **automatischen** Modus in PAgP. Der Switch initiiert den Kanal nicht, erkennt jedoch eingehende LACP-Pakete. Der Peer (im aktiven Zustand) initiiert die Aushandlung (durch das Senden eines LACP-Pakets), das der Switch empfängt und an den der Switch antwortet, und bildet schließlich den Aggregationskanal mit dem Peer.
Aktiv	Dies ähnelt dem **wünschenswerten** Modus in PAgP. Der Switch initiiert die Aushandlung, um eine aggregierte Verbindung zu bilden. Das Link-Aggregat wird gebildet, wenn das andere Ende im aktiven oder passiven LACP-Modus ausgeführt wird.

Das LACP verwendet einen 30-Sekunden-Intervall-Timer (Slow_Periodic_Time), nachdem die LACP-EtherChannels erstellt wurden. Die Anzahl der Sekunden vor der Invalidierung der empfangenen LACPDU-Informationen bei Verwendung von Long Timeouts (3fache Slow_Periodic_Time) beträgt 90. UDLD wird als schnellerer Detektor unidirektionaler Verbindungen empfohlen. Sie können die LACP-Timer nicht anpassen, und zu diesem Zeitpunkt können Sie die Switches nicht so konfigurieren, dass sie die schnelle PDU-Übertragung (Fast Protocol Data Unit) (jede Sekunde) verwenden, um den Kanal nach der Kanalbildung aufrechtzuerhalten.

Überprüfung

Die Tabelle in diesem Abschnitt bietet eine Zusammenfassung aller möglichen LACP-Channeling-Modus-Szenarien zwischen zwei direkt verbundenen Switches (Switch A und Switch B). Einige dieser Kombinationen können dazu führen, dass EtherChannel Guard die Ports auf der Channeling-Seite in den errdisable-Status versetzt. Die Funktion "EtherChannel Misconfiguration Guard" ist standardmäßig aktiviert.

Channel-Modus wechseln	Switch B Channel-Modus	Kanal-Status wechseln	Switch B Channel-Staat
Ein	Ein	Kanal (nicht LACP)	Kanal (nicht LACP)
Ein	Aus	Not Channel (ErrDisable)	Kein Channel

Ein	Passiv	Not Channel (ErrDisable)	Kein Channel
Ein	Aktiv	Not Channel (ErrDisable)	Kein Channel
Aus	Aus	Kein Channel	Kein Channel
Aus	Passiv	Kein Channel	Kein Channel
Aus	Aktiv	Kein Channel	Kein Channel
Passiv	Passiv	Kein Channel	Kein Channel
Passiv	Aktiv	LACP-Channel	LACP-Channel
Aktiv	Aktiv	LACP-Channel	LACP-Channel

Empfehlungen von Cisco

Cisco empfiehlt, PAgP für Channel-Verbindungen zwischen Cisco Switches zu aktivieren. Wenn zwei Geräte kanalisiert werden, die PAgP nicht unterstützen, aber LACP unterstützen, wird empfohlen, LACP mit der Konfiguration von LACP zu aktivieren, das an beiden Enden der Geräte aktiv ist.

Auf Switches, die CatOS ausführen, verwenden alle Ports eines Catalyst 4500/4000 und eines Catalyst 6500/6000 standardmäßig das PAgP-Kanalprotokoll. Um Ports für die Verwendung von LACP zu konfigurieren, müssen Sie das Channel-Protokoll der Module auf LACP festlegen. LACP und PAgP können nicht auf Switches ausgeführt werden, auf denen CatOS ausgeführt wird. Diese Einschränkung gilt nicht für Switches, auf denen die Cisco IOS Software ausgeführt wird. Die Switches, auf denen die Cisco IOS-Software ausgeführt wird, können PAgP und LACP auf demselben Modul unterstützen. Führen Sie diese Befehle aus, um den LACP-Kanalmodus auf "active" festzulegen und eine administrative Schlüsselnummer zuzuweisen:

```
Switch(config)#interface range type slot#/port#
Switch(config-if)#channel-group admin_key mode active
```

Der Befehl **show etherchannel summary** zeigt eine einzeilige Zusammenfassung pro Kanalgruppe an, die folgende Informationen enthält:

- Gruppennummern
- Port-Channel-Nummern
- Status der Ports
- Die Ports, die Teil des Kanals sind

Der Befehl **show etherchannel port-channel** zeigt detaillierte Informationen zu Port-Channels für alle Kanalgruppen an. Die Ausgabe enthält folgende Informationen:

- Status des Kanals
- Verwendetes Protokoll
- Die Zeit seit der Bündelung der Ports

Um detaillierte Informationen für eine bestimmte Kanalgruppe anzuzeigen, wobei die Details für jeden Port separat angezeigt werden, verwenden Sie den Befehl **show etherchannel *channel_number* detail**. Die Befehlsausgabe enthält die Details zum Partner und zum Port-Channel. Weitere Informationen finden Sie unter Konfigurieren von LACP (802.3ad) zwischen einem Catalyst 6500/6000 und einem Catalyst 4500/4000.

Weitere Optionen

Bei Kanalgeräten, die PAgP oder LACP nicht unterstützen, muss der Kanal `eingeschaltet` werden. Diese Anforderung gilt für folgende Geräte:

- Server
- Lokaler Leiter
- Content-Switches
- Router
- Switches mit älterer Software
- Catalyst Switches der Serie 2900XL/3500XL
- Catalyst 8540

Geben Sie folgende Befehle ein:

```
Switch(config)#interface range type slot#/port#
Switch(config-if)#channel-group admin_key mode on
```

UniDirectional Link Detection

Zweck

UDLD ist ein proprietäres Lightweight-Protokoll von Cisco, das entwickelt wurde, um Instanzen der unidirektionalen Kommunikation zwischen Geräten zu erkennen. Es gibt andere Methoden zum Erkennen des bidirektionalen Zustands von Übertragungsmedien, z. B. FEFI. Es gibt jedoch Fälle, in denen die Erkennungsmechanismen für Layer 1 nicht ausreichen. Diese Szenarien können Folgendes bewirken:

- Der unvorhersehbare Betrieb von STP
- Falsche oder übermäßige Überflutung von Paketen
- Blackholing von Datenverkehr

Die UDLD-Funktion behandelt die folgenden Fehlerzustände an Glasfaser- und Kupfer-Ethernet-Schnittstellen:

- Überwachung physischer Verkabelungskonfigurationen - Herunterfahren bei `fehlerhaften` Ports, `die` falsch verdrahtet sind.
- Schützt vor unidirektionalen Verbindungen - Bei der Erkennung einer unidirektionalen Verbindung, die aufgrund einer Medien- oder Port-/Schnittstellenfehlfunktion auftritt, wird der betroffene Port bei `errDisabled` geschlossen. Eine entsprechende Syslog-Meldung wird generiert.
- Darüber hinaus überprüft der aggressive UDLD-Modus, ob eine zuvor als bidirektional eingestufte Verbindung die Verbindung nicht verliert, falls die Verbindung aufgrund einer Überlastung unbrauchbar wird. Der aggressive UDLD-Modus führt fortlaufende Verbindungstests für die gesamte Verbindung durch. Der Hauptzweck des aggressiven

UDLD-Modus besteht darin, das Blackholing von Datenverkehr unter bestimmten ausgefallenen Bedingungen zu vermeiden, die nicht durch UDLD im normalen Modus behandelt werden.

Weitere Informationen finden Sie unter Verstehen und Konfigurieren der Unidirectional Link Detection Protocol (UDLD)-Funktion.

Spanning Tree weist einen unidirektionalen Steady-State-BPDU-Fluss auf und kann die in diesem Abschnitt aufgeführten Fehler aufweisen. Ein Port kann BPDUs plötzlich nicht übertragen, was dazu führt, dass sich der STP-Status von der `Blockierung` auf die `Weiterleitung` am Nachbarn ändert. Dennoch existiert eine Schleife, weil der Port immer noch empfangen werden kann.

Überblick

UDLD ist ein Layer-2-Protokoll, das oberhalb der LLC-Schicht arbeitet (MAC 01-00-0c-cc-cc, SNAP HDLC-Protokolltyp 0x011). Wenn Sie UDLD in Kombination mit FEFI- und Auto-Negotiation-Layer-1-Mechanismen ausführen, können Sie die physische (L1) und logische (L2) Integrität einer Verbindung validieren.

UDLD verfügt über Bestimmungen für Funktionen und Schutz, die FEFI und Autoverhandlungen nicht leisten können. Zu diesen Funktionen gehören:

- Erkennung und Zwischenspeicherung von Nachbarinformationen
- Herunterfahren falsch verbundener Ports
- Erkennung von Fehlfunktionen oder Fehlern logischer Schnittstellen/Ports bei Verbindungen, die nicht Point-to-Point sind**Hinweis:** Wenn Links keine Point-to-Point-Verbindungen sind, durchlaufen sie Medienkonverter oder Hubs.

UDLD verwendet diese beiden grundlegenden Mechanismen.

1. UDLD lernt über die Nachbarn und hält die Informationen in einem lokalen Cache auf dem neuesten Stand.
2. UDLD sendet bei der Erkennung eines neuen Nachbarn oder bei jeder Anforderung einer Resynchronisierung des Cache eine Reihe von UDLD-Tests/Echo (Hello)-Nachrichten.

UDLD sendet kontinuierlich Tests/Echo-Meldungen an allen Ports. Beim Empfang einer entsprechenden UDLD-Nachricht an einem Port werden eine Erkennungsphase und ein Validierungsprozess ausgelöst. Der Port wird aktiviert, wenn alle gültigen Bedingungen erfüllt sind. Die Bedingungen sind erfüllt, wenn der Port bidirektional und korrekt verkabelt ist. Wenn die Bedingungen nicht erfüllt werden, ist der Port `errDisabled`, was diese Syslog-Meldung auslöst:

```
UDLD-3-AGGRDISABLE: Neighbor(s) of port disappeared on bidirectional link.
   Port disabled
UDLD-3-AGGRDISABLEFAIL: Neighbor(s) of port disappeared on bidirectional link.
   Failed to disable port
UDLD-3-DISABLE: Unidirectional link detected on port disabled.
UDLD-3-DISABLEFAIL: Unidirectional link detected on port, failed to disable port.
UDLD-3-SENDFAIL: Transmit failure on port.
UDLD-4-ONEWAYPATH: A unidirectional link from port to port of device [chars]
   was detected.
```

Eine vollständige Liste der Systemmeldungen nach Einrichtung, die UDLD-Ereignisse enthalten, finden Sie unter UDLD-Meldungen (Cisco IOS-Systemmeldungen, Band 2 von 2).

Nach der Einrichtung einer Verbindung und ihrer Klassifizierung als bidirektional kündigt UDLD

weiterhin in einem Standardintervall von 15 Sekunden Probes/Echo-Nachrichten an.

Diese Tabelle enthält Informationen zu den Portstatus:

Port-Status	Kommentar
Unbestimmt	Die Erkennung in Verarbeitung/benachbartes UDLD wurde deaktiviert.
Nicht zutreffend	UDLD wurde deaktiviert.
Herunterfahren	Eine unidirektionale Verbindung wurde erkannt und der Port wurde deaktiviert.
Bidirektional	Es wurde eine bidirektionale Verbindung erkannt.

Wartung des Nachbarcaches

UDLD sendet regelmäßig Hello-Sonde-/Echo-Pakete an jede aktive Schnittstelle, um die Integrität des UDLD-Nachbarcache zu wahren. Beim Empfang einer Hello-Nachricht wird die Nachricht zwischengespeichert und für einen Zeitraum im Speicher aufbewahrt, der als Haltezeit definiert ist. Wenn die Haltezeit abläuft, wird der entsprechende Cache-Eintrag veraltet. Wenn innerhalb der Haltezeit eine neue Hello-Nachricht eingeht, ersetzt die neue den älteren Eintrag, und der entsprechende Time-to-Live-Timer wird zurückgesetzt.

Wenn eine UDLD-aktivierte Schnittstelle deaktiviert wird oder ein Gerät zurückgesetzt wird, werden alle vorhandenen Cache-Einträge für die Schnittstellen gelöscht, die von der Konfigurationsänderung betroffen sind. Diese Freigabe erhält die Integrität des UDLD-Cache aufrecht. UDLD sendet mindestens eine Nachricht, um die entsprechenden Nachbarn darüber zu informieren, dass die entsprechenden Cache-Einträge gelöscht werden müssen.

Echoerkennungsmechanismus

Der Echomechanismus bildet die Grundlage des Erkennungsalgorithmus. Wenn ein UDLD-Gerät von einem neuen Nachbarn erfährt oder eine Resynchronisierungsanforderung von einem nicht synchronisierten Nachbarn empfängt, startet oder startet das Gerät das Erkennungsfenster auf seiner Seite der Verbindung neu und sendet eine Anhäufung von Echo-Meldungen als Antwort. Da dieses Verhalten bei allen Nachbarn gleich sein muss, erwartet der Echosender, dass er als Antwort Echos erhält. Wenn das Erkennungsfenster ohne den Empfang gültiger Antwortnachrichten endet, wird der Link als unidirektional betrachtet. Ab diesem Zeitpunkt kann ein Prozess zur Wiederherstellung von Verbindungen oder zum Herunterfahren des Ports ausgelöst werden. Andere, seltene ungewöhnliche Bedingungen, für die das Gerät überprüft:

- Looped-Back-Transmit-Glasfasern (Tx) an den Rx-Anschluss desselben Ports
- Fehlende Verbindungen im Fall einer gemeinsam genutzten Medienverbindung (z. B. ein Hub oder ein ähnliches Gerät)

Konvergenzzeit

Um STP-Schleifen zu vermeiden, wurde das UDLD-Standard-Nachrichtenintervall in der Cisco IOS Software, Version 12.1 und höher, von 60 auf 15 Sekunden reduziert. Dieses Intervall wurde geändert, um eine unidirektionale Verbindung zu schließen, bevor ein zuvor blockierter Port in

802.1D Spanning Tree in der Lage ist, in einen Weiterleitungsstatus zu wechseln. Der Nachrichtenintervallwert bestimmt die Geschwindigkeit, mit der ein Nachbar UDLD-Tests nach der Verbindungs- oder Erkennungsphase sendet. Das Nachrichtenintervall muss an beiden Enden einer Verbindung nicht übereinstimmen, obwohl eine konsistente Konfiguration nach Möglichkeit wünschenswert ist. Wenn UDLD-Nachbarn eingerichtet sind, wird das konfigurierte Nachrichtenintervall an den Nachbarn gesendet, und das Zeitüberschreitungsintervall für diesen Peer wird wie folgt berechnet:

```
3 * (message interval)
```

Daher wird eine Peer-Beziehung nach drei aufeinander folgenden Hellos (oder Sonden) zeitlich unterbrochen. Da sich die Nachrichtenintervalle auf jeder Seite unterscheiden, ist dieser Timeout-Wert auf jeder Seite einfach unterschiedlich, und eine Seite erkennt einen Fehler schneller.

Die ungefähre Zeit, die UDLD benötigt, um einen unidirektionalen Ausfall einer zuvor stabilen Verbindung zu erkennen, beträgt ungefähr:

```
2.5 * (message interval) + 4 seconds
```

Dies ist etwa 41 Sekunden bei einem Standard-Nachrichtenintervall von 15 Sekunden. Diese Zeitspanne ist deutlich kürzer als die 50 Sekunden, die normalerweise für die Neukonvergierung von STP erforderlich sind. Wenn die NMP-CPU über einige Ersatzzyklen verfügt und der Benutzer den Auslastungsgrad sorgfältig überwacht (eine bewährte Vorgehensweise), ist eine Reduzierung des Nachrichtenintervalls (gerade) auf mindestens 7 Sekunden akzeptabel. Diese Verringerung des Nachrichtenintervalls beschleunigt zudem die Erkennung um einen signifikanten Faktor.

Hinweis: Cisco IOS Software Release 12.2(25)SEC enthält mindestens 1 Sekunde.

Daher wird von UDLD von Standard-Spanning-Tree-Timern ausgegangen. Wenn STP so konfiguriert ist, dass es schneller konvergiert als UDLD, sollten Sie einen alternativen Mechanismus in Betracht ziehen, z. B. die Funktion für STP-Loop Guard. Wenn Sie RSTP (802.1w) implementieren, sollten Sie in diesem Fall einen alternativen Mechanismus in Betracht ziehen, da RSTP, abhängig von der Topologie, Konvergenzmerkmale in ms aufweist. Verwenden Sie für diese Instanzen Loop Guard in Verbindung mit UDLD, um den meisten Schutz zu bieten. Loop Guard verhindert STP-Schleifen mit der Geschwindigkeit der verwendeten STP-Version. UDLD übernimmt die Erkennung unidirektionaler Verbindungen auf einzelnen EtherChannel-Verbindungen oder in Fällen, in denen BPDUs nicht entlang der unterbrochenen Richtung fließen.

Hinweis: UDLD ist unabhängig von STP. UDLD erfasst nicht jede STP-Fehlersituation, z. B. Fehler, die von einer CPU verursacht werden, die keine BPDUs für einen Zeitraum sendet, der größer ist als (2 * Fwddelay + Max). Aus diesem Grund empfiehlt Cisco die Implementierung von UDLD in Verbindung mit Loop Guard in Topologien, die auf STP basieren.

Vorsicht: Achten Sie auf frühere Versionen von UDLD in den 2900XL/3500XL-Switches, die ein nicht konfigurierbares Standard-Nachrichtenintervall von 60 Sekunden verwenden. Sie sind anfällig für Spanning-Tree-Schleifenbedingungen.

Aggressive UDLD-Modus

Aggressive UDLD wurde erstellt, um speziell die wenigen Fälle zu behandeln, in denen ein fortlaufender Test der bidirektionalen Konnektivität erforderlich ist. Daher bietet die Funktion für den aggressiven Modus in folgenden Situationen besseren Schutz vor gefährlichen

unidirektionalen Verbindungsbedingungen:

- Wenn der Verlust von UDLD-PDUs symmetrisch ist und beide das Zeitlimit überschreiten. In diesem Fall wird kein Port deaktiviert.
- Eine Seite einer Verbindung hat einen Port stecken (sowohl Tx als auch Rx).
- Eine Seite einer Verbindung bleibt aktiv, während die andere Seite der Verbindung ausfällt.
- Die Autonegotiation oder ein anderer Layer-1-Fehlererkennungsmechanismus ist deaktiviert.
- Eine Verringerung der Abhängigkeit von Layer-1-FEFI-Mechanismen ist wünschenswert.
- Sie benötigen maximalen Schutz vor Ausfällen unidirektionaler Verbindungen auf FE/GE-Point-to-Point-Verbindungen. Insbesondere wenn ein Ausfall zwischen zwei Nachbarn nicht zulässig ist, können UDLD-aggressive Tests als Herzschlag betrachtet werden, dessen Vorhandensein die Integrität der Verbindung garantiert.

Der häufigste Fall für eine aggressive UDLD-Implementierung besteht darin, die Verbindungsprüfung für ein Mitglied eines Pakets durchzuführen, wenn die Autoübertragung oder ein anderer Layer-1-Fehlererkennungsmechanismus deaktiviert oder unbrauchbar ist. Dies ist besonders bei EtherChannel-Verbindungen nützlich, da PAgP und LACP selbst bei Aktivierung keine sehr niedrigen Hello-Timer im Steady-State verwenden. In diesem Fall bietet UDLD Aggressive den zusätzlichen Vorteil, dass mögliche Spanning-Tree-Schleifen verhindert werden.

Es ist wichtig zu verstehen, dass der normale UDLD-Modus selbst dann eine unidirektionale Verbindungsbedingung überprüft, wenn eine Verbindung den bidirektionalen Status erreicht. UDLD ist für die Erkennung von Layer-2-Problemen vorgesehen, die STP-Schleifen verursachen. Diese Probleme sind in der Regel unidirektional (da BPDUs nur in eine Richtung im Steady-State fließen). Daher ist die Verwendung von UDLD normal in Verbindung mit Autoübertragung und Loop Guard (für Netzwerke, die auf STP basieren) fast immer ausreichend. Wenn der aggressive UDLD-Modus aktiviert ist, startet der aggressive UDLD-Modus die Verbindungssequenz neu, nachdem alle Nachbarn eines Ports entweder in der Werbe- oder in der Erkennungsphase ausgefallen sind, um eine Resynchronisierung mit allen potenziell nicht synchronisierten Nachbarn durchzuführen. Wenn die Verbindung nach einem schnellen Nachrichtenzug (acht fehlgeschlagene Wiederholungen) immer noch als nicht erkannt gilt, wird der Port in den errdisable-Status gesetzt.

Hinweis: Einige Switches sind nicht aggressiv UDLD-fähig. Derzeit verfügen die Catalyst Switches der Serien 2900XL und 3500XL über hartcodierte Nachrichtenintervalle von 60 Sekunden. Dies gilt nicht als ausreichend schnell, um den Schutz vor potenziellen STP-Schleifen zu gewährleisten (wobei von den Standard-STP-Parametern ausgegangen wird).

Automatische Wiederherstellung von UDLD-Links

Die Wiederherstellung von Errdisable ist standardmäßig global deaktiviert. Wenn ein Port global aktiviert ist und in den errdisable-Status wechselt, wird er nach einem ausgewählten Zeitintervall automatisch wieder aktiviert. Die Standardzeit beträgt 300 Sekunden. Dies ist ein globaler Timer, der für alle Ports eines Switches beibehalten wird. Abhängig von der Softwareversion können Sie eine erneute Aktivierung eines Ports manuell verhindern, wenn Sie das errdisable-Timeout für diesen Port so festlegen, dass er mithilfe des errdisable-Timeout-Wiederherstellungsmechanismus für UDLD deaktiviert wird:

```
Switch(config)#errdisable recovery cause udld
```

Verwenden Sie die Zeitüberschreitungsfunktion "errdisable", wenn Sie den aggressiven UDLD-Modus ohne Out-of-Band-Netzwerkmanagementfunktionen implementieren, insbesondere im

Access Layer oder auf jedem Gerät, das im Falle einer Erdisable-Situation vom Netzwerk isoliert werden kann.

Weitere Informationen zum Konfigurieren einer Zeitüberschreitungsfrist für Ports im errdisable-Status finden Sie unter errdisable-Wiederherstellung (Catalyst 6500 Series Cisco IOS Command Reference, 12.1 E).

Die Wiederherstellung mit Erdisable kann für UDLD im Access Layer besonders wichtig sein, wenn die Access Switches über eine Campus-Umgebung verteilt sind und der manuelle Besuch jedes Switches eine beträchtliche Zeit in Anspruch nimmt, um beide Uplinks wieder zu aktivieren.

Cisco rät davon ab, die Fehlerbehebung im Netzwerkkern zu deaktivieren, da in der Regel mehrere Einstiegspunkte in einen Kern vorhanden sind und eine automatische Wiederherstellung im Core zu wiederkehrenden Problemen führen kann. Daher müssen Sie einen Port im Core manuell erneut aktivieren, wenn UDLD den Port deaktiviert.

UDLD auf Routed Links

Für diese Diskussion ist eine geroutete Verbindung entweder einer der beiden folgenden Verbindungstypen:

- Point-to-Point zwischen zwei Routerknoten (konfiguriert mit einer 30-Bit-Subnetzmaske)
- Ein VLAN mit mehreren Ports, das jedoch nur geroutete Verbindungen unterstützt, z. B. in einer Split-Layer-2-Core-Topologie

Jedes Interior Gateway Routing Protocol (IGRP) weist einzigartige Merkmale auf, wie es Nachbarbeziehungen und Routenkonvergenz handhabt. In diesem Abschnitt werden die für diese Diskussion relevanten Merkmale beschrieben, die im Gegensatz zu zwei der heute verwendeten Routingprotokolle stehen: Open Shortest Path First (OSPF) Protocol und Enhanced IGRP (EIGRP).

Hinweis: Ein Layer-1- oder Layer-2-Ausfall in einem gerouteten Point-to-Point-Netzwerk führt zur beinahe sofortigen Beendigung der Layer-3-Verbindung. Da der einzige Switch-Port in diesem VLAN beim Ausfall von Layer 1/Layer 2 in einen nicht verbundenen Zustand wechselt, werden die Layer 2- und Layer 3-Port-Zustände mit der Funktion "Auto-State" der Schnittstelle in ca. zwei Sekunden synchronisiert und die Layer 3-VLAN-Schnittstelle in einen Ein-/Ausschaltzustand versetzt (das Leitungsprotokoll wird deaktiviert).

Wenn Sie von den Standardwerten für den Timer ausgehen, sendet OSPF alle 10 Sekunden Hello-Nachrichten und hat ein Dead-Intervall von 40 Sekunden (4 * Hello). Diese Timer sind konsistent für OSPF-Point-to-Point- und Broadcast-Netzwerke. Da OSPF eine bidirektionale Kommunikation erfordert, um eine Adjacency zu bilden, beträgt die Ausfallsicherungszeit 40 Sekunden. Dies gilt auch dann, wenn der Layer-1-/Layer-2-Ausfall nicht ausschließlich auf einer Punkt-zu-Punkt-Verbindung auftritt und ein halb-Backup-Szenario bleibt, mit dem das Layer-3-Protokoll umgehen muss. Da die Erkennungszeit von UDLD der Erkennungszeit eines OSPF-Dead-Timers sehr ähnlich ist (ca. 40 Sekunden), sind die Vorteile der Konfiguration des normalen UDLD-Modus auf einer Point-to-Point-OSPF-Layer-3-Verbindung begrenzt.

In vielen Fällen konvergiert EIGRP schneller als OSPF. Dabei ist jedoch zu beachten, dass die bidirektionale Kommunikation keine Anforderung für Nachbarn ist, Routing-Informationen auszutauschen. In sehr spezifischen Szenarien mit Halbbacken-Ausfällen ist EIGRP anfällig für das Blackholing von Datenverkehr, der anhält, bis ein anderes Ereignis die Routen über diesen Nachbarn aktiv macht. Der normale UDLD-Modus kann diese Umstände mindern, da er den

Ausfall einer unidirektionalen Verbindung erkennt und den Port aufgrund eines Fehlers deaktiviert.

Bei Layer-3-gerouteten Verbindungen, die ein beliebiges Routing-Protokoll verwenden, bietet UDLD normal weiterhin Schutz vor Problemen, die bei der anfänglichen Aktivierung der Verbindung auftreten, z. B. fehlerhafte Verkabelung oder Hardware. Zusätzlich bietet der aggressive UDLD-Modus bei gerouteten Layer-3-Verbindungen die folgenden Vorteile:

- Verhindert unnötiges Blackholing von Datenverkehr (in einigen Fällen mit minimalem Timer erforderlich)
- Fügt einen Flapping-Link in den errdisable-Status ein
- Schützt vor Schleifen, die aus Layer-3-EtherChannel-Konfigurationen resultieren

Standardverhalten von UDLD

UDLD ist global deaktiviert und standardmäßig für Glasfaserports einsatzbereit aktiviert. Da UDLD ein Infrastrukturprotokoll ist, das nur zwischen Switches benötigt wird, ist UDLD standardmäßig auf Kupferports deaktiviert, die in der Regel für den Host-Zugriff verwendet werden. Beachten Sie, dass Sie UDLD global und auf Schnittstellenebene aktivieren müssen, bevor Nachbarn bidirektionalen Status erreichen können. Das Standard-Nachrichtenintervall beträgt 15 Sekunden. Das Standard-Nachrichtenintervall kann jedoch in einigen Fällen als sieben Sekunden angezeigt werden. Weitere Informationen finden Sie unter Cisco Bug ID CSCea70679 (nur registrierte Kunden). Das Standard-Nachrichtenintervall kann zwischen sieben und 90 Sekunden konfiguriert werden, und der aggressive UDLD-Modus ist deaktiviert. Die Cisco IOS Software-Version 12.2(25)SEC reduziert diesen Timer zusätzlich auf eine Sekunde.

Cisco Konfigurationsempfehlung

In den meisten Fällen empfiehlt Cisco, den UDLD-Normalmodus für alle FE/GE-Point-to-Point-Verbindungen zwischen Cisco Switches zu aktivieren und das UDLD-Nachrichtenintervall auf 15 Sekunden festzulegen, wenn Sie Standard-802.1D-Spanning-Tree-Timer verwenden. Wenn Netzwerke aus Gründen der Redundanz und Konvergenz auf STP angewiesen sind (was bedeutet, dass es in der Topologie einen oder mehrere Ports im STP-Blockierungsstatus gibt), sollten Sie außerdem UDLD in Verbindung mit den entsprechenden Funktionen und Protokollen verwenden. Zu diesen Funktionen gehören FEFI, Autoübertragung, Loop Guard usw. Wenn die Autoübertragung aktiviert ist, ist normalerweise der aggressive Modus nicht erforderlich, da die automatische Aushandlung die Fehlererkennung auf Layer 1 kompensiert.

Führen Sie eine der beiden folgenden Befehlsoptionen aus, um UDLD zu aktivieren:

Hinweis: Die Syntax hat sich über verschiedene Plattformen/Versionen hinweg geändert.

-
```
udld enable
!--- Once globally enabled, all FE and GE fiber !--- ports have UDLD enabled by default.
udld port
```

  oder

-
```
udld enable
!--- The copper ports of some earlier Cisco IOS Software !--- releases can have UDLD enabled
by individual port command.
```

Sie müssen Ports manuell aktivieren, die aufgrund von Symptomen für unidirektionale

Verbindungen geschlossen werden. Verwenden Sie eine der folgenden Methoden:

```
udld reset
!--- Globally reset all interfaces that UDLD shut down. no udld port
udld port [aggressive]
!--- Per interface, reset and reenable interfaces that UDLD shut down.
```

Die **Befehle errdisable restore restore udld** and **errdisable-intervall *für* die globale Konfiguration können verwendet werden, um automatisch den** Status UDLD-Fehler-Deaktivierung wiederherzustellen.

Cisco empfiehlt, den Wiederherstellungsmechanismus errdisable nur im Access Layer des Netzwerks mit Wiederherstellungszeiträumen von 20 Minuten oder mehr zu verwenden, wenn der physische Zugriff auf den Switch schwierig ist. Die beste Situation besteht darin, Zeit für die Netzwerkstabilisierung und Fehlerbehebung zu lassen, bevor der Port wieder in Betrieb genommen wird und die Instabilität des Netzwerks verursacht.

Cisco empfiehlt, *keine* Wiederherstellungsmechanismen im Netzwerkkern zu verwenden, da dies zu Instabilitäten führen kann, die sich auf Konvergenzereignisse beziehen, wenn eine fehlerhafte Verbindung wiederhergestellt wird. Das redundante Design eines Core-Netzwerks stellt einen Backup-Pfad für eine ausgefallene Verbindung bereit und bietet genügend Zeit für eine Analyse der Ursachen für einen UDLD-Ausfall.

UDLD ohne STP-Loop-Guard verwenden

Für Layer-3-Point-to-Point- oder Layer-2-Verbindungen, bei denen eine schleifenfreie STP-Topologie vorhanden ist (keine Port-Blockierung), empfiehlt Cisco die Aktivierung von aggressivem UDLD auf Point-to-Point-FE/GE-Verbindungen zwischen Cisco Switches. In diesem Fall wird das Nachrichtenintervall auf sieben Sekunden festgelegt, und 802.1D STP verwendet Standard-Timer.

UDLD auf EtherChannels

Unabhängig davon, ob STP-Loop Guard bereitgestellt wird oder nicht, wird für alle EtherChannel-Konfigurationen in Verbindung mit dem wünschenswerten Channel-Modus der UDLD-aggressive Modus empfohlen. Bei EtherChannel-Konfigurationen kann ein Ausfall der Verbindung des Kanals, der die Spanning-Tree-BPDUs und den PAgP-Kontrollverkehr überträgt, sofortige Schleifen zwischen den Channel-Partnern verursachen, wenn die Channel-Verbindungen entbündelt werden. Im aggressiven UDLD-Modus wird ein ausgefallener Port heruntergefahren. PAgP (automatischer/wünschenswerter Kanalmodus) kann dann eine neue Steuerungsverbindung aushandeln und eine ausgefallene Verbindung effektiv vom Kanal entfernen.

UDLD mit 802.1w Spanning Tree

Um Schleifen zu vermeiden, wenn Sie neuere Spanning Tree-Versionen verwenden, sollten Sie den normalen UDLD-Modus und STP-Loop Guard mit RSTPs wie 802.1w verwenden. UDLD kann während einer Verbindungsphase Schutz vor unidirektionalen Verbindungen bieten, und STP-Loop Guard kann STP-Schleifen verhindern, falls die Verbindungen unidirektional werden, *nachdem* UDLD die Verbindungen als bidirektional eingerichtet hat. Da Sie UDLD nicht so konfigurieren können, dass es kleiner als die Standard-802.1w-Timer ist, ist STP Loop Guard erforderlich, um Loops in redundanten Topologien vollständig zu verhindern.

Weitere Informationen finden Sie unter Verstehen und Konfigurieren der Unidirectional Link Detection Protocol (UDLD)-Funktion.

UDLD testen und überwachen

UDLD lässt sich ohne eine wirklich fehlerhafte/unidirektionale Komponente im Labor, z. B. ein defektes GBIC, nicht leicht testen. Das Protokoll wurde entwickelt, um weniger häufig auftretende Fehlerszenarien zu erkennen, als die Szenarien, die normalerweise in einem Labor verwendet werden. Wenn Sie beispielsweise einen einfachen Test durchführen, z. B. das Trennen eines Faserstrands, um den gewünschten `errdisable`-Status anzuzeigen, müssen Sie zuerst die Layer-1-Autonegotiation deaktivieren. Andernfalls wird der physische Port `ausgeschaltet`, wodurch die UDLD-Nachrichtenkommunikation zurückgesetzt wird. Das Remote-Ende wechselt im normalen UDLD-Modus in den `unbestimmten` Zustand und wechselt nur im aggressiven UDLD-Modus in den errdisable-Status.

Eine zusätzliche Testmethode simuliert den PDU-Verlust des Nachbarn für UDLD. Die Methode besteht in der Verwendung von MAC-Layer-Filtern, um die UDLD/CDP-Hardwareadresse zu blockieren, während Sie die Weiterleitung anderer Adressen zulassen. Einige Switches senden keine UDLD-Frames, wenn der Port als SPAN-Ziel (Switched Port Analyzer) konfiguriert ist, was einen nicht reagierenden UDLD-Nachbarn simuliert.

Verwenden Sie den folgenden Befehl, um UDLD zu überwachen:

```
show udld gigabitethernet1/1
Interface Gi1/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 7
Time out interval: 5
```

Darüber hinaus können Sie über den Aktivierungsmodus in Switches der Cisco IOS Software, Version 12.2(18)SXD oder höher, den Befehl **show udld neighbor** ausgeben, um den Inhalt des UDLD-Cache (wie CDP) zu überprüfen. Oft ist es sehr nützlich, den UDLD-Cache mit dem CDP-Cache zu vergleichen, um zu überprüfen, ob eine protokollspezifische Anomalie vorliegt. Wenn CDP ebenfalls betroffen ist, bedeutet dies in der Regel, dass alle BPDUs/PDUs betroffen sind. Aktivieren Sie daher auch STP. Überprüfen Sie beispielsweise, ob die Root-Identitätsänderungen oder Änderungen an der Root/Designated-Portplatzierung vorgenommen wurden.

Sie können den UDLD-Status und die Konfigurationskonsistenz mithilfe der Cisco UDLD SNMP MIB-Variablen überwachen.

Multilayer-Switching

Übersicht

In der Cisco IOS-Systemsoftware wird Multilayer Switching (MLS) von der Catalyst 6500/6000-Serie und nur intern unterstützt. Das bedeutet, dass der Router im Switch installiert werden muss. Die neueren Catalyst 6500/600 Supervisor Engines unterstützen MLS CEF, bei dem die Routing-Tabelle auf jede Karte heruntergeladen wird. Hierfür ist zusätzliche Hardware erforderlich,

darunter eine Distributed Forwarding Card (DFC). DFCs werden in der CatOS-Software nicht unterstützt, selbst wenn Sie sich für die Verwendung der Cisco IOS-Software auf der Routerkarte entscheiden. DFCs werden nur in der Cisco IOS-Systemsoftware unterstützt.

Der MLS-Cache, der zur Aktivierung von NetFlow-Statistiken auf Catalyst-Switches verwendet wird, ist der Flow-basierte Cache, den die Supervisor Engine I-Karte und Legacy-Catalyst-Switches zur Aktivierung von Layer-3-Switching verwenden. MLS ist auf der Supervisor Engine 1 (oder Supervisor Engine 1A) mit MSFC oder MSFC2 standardmäßig aktiviert. Für die Standard-MLS-Funktionalität ist keine zusätzliche MLS-Konfiguration erforderlich. Sie können den MLS-Cache in einem von drei Modi konfigurieren:

- Ziel
- Quelle-Ziel
- Quell-Ziel-Port

Die Maske des Datenflusses dient zur Bestimmung des MLS-Modus des Switches. Diese Daten werden anschließend verwendet, um Layer-3-Datenflüsse in den von der Supervisor Engine IA bereitgestellten Catalyst-Switches zu ermöglichen. Die Blades der Supervisor Engine II nutzen den MLS-Cache nicht, um Pakete zu verteilen, da diese Karte Hardware-CEF-fähig ist, eine wesentlich skalierbarere Technologie. Der MLS-Cache wird auf der Supervisor Engine II-Karte verwaltet, um nur den statistischen NetFlow-Export zu ermöglichen. Aus diesem Grund kann die Supervisor Engine II bei Bedarf für vollständigen Datenfluss ohne negative Auswirkungen auf den Switch aktiviert werden.

Konfiguration

Die MLS-Alterungszeit wird auf alle MLS-Cacheeinträge angewendet. Der Wert für die Alterungszeit wird direkt auf das Alternieren im Zielmodus angewendet. Sie teilen den Wert für die MLS-Alterungszeit durch zwei auf, um die Alterungszeit zwischen Quelle und Ziel abzuleiten. Teilen Sie den Wert für die MLS-Alterungszeit durch acht auf, um die vollständige Alterungszeit zu ermitteln. Der Standardwert für die MLS-Alterungszeit ist 256 Sekunden.

Sie können die normale Alterungszeit zwischen 32 und 4092 Sekunden in acht Sekunden-Schritten konfigurieren. Jeder Wert für die Alterungszeit, der nicht ein Vielfaches von acht Sekunden ist, wird auf das nächste Vielfaches von 8 Sekunden eingestellt. Beispielsweise wird ein Wert von 65 auf 64 und ein Wert von 127 auf 128 angepasst.

Andere Ereignisse können zum Löschen von MLS-Einträgen führen. Zu diesen Ereignissen gehören:

- Routingänderungen
- Änderung des LinkstatusZum Beispiel ist die PFC-Verbindung ausgefallen.

Um die Größe des MLS-Cache unter 32.000 Einträge zu halten, aktivieren Sie diese Parameter, nachdem Sie den Befehl **mls aging** ausgegeben haben:

```
Normal: configures the wait before aging out and deleting shortcut entries in
the L3 table.

Fast aging: configures an efficient process to age out entries created for flows that
only switch a few packets and then are never used again. The fast aging parameter uses
the time keyword value to check if at least the threshold keyword value of packets has
been switched for each flow. If a flow has not switched the threshold number of packets
during the time interval, then the entry in the L3 table is aged out.
```

```
Long: configures entries for deletion that have been up for the specified value even if
the L3 entry is in use. Long aging is used to prevent counter wraparound, which could
cause inaccurate statistics.
```

Konfiguration

Ein typischer Cache-Eintrag, der entfernt wird, ist der Eintrag für Flows zu und von einem Domain Name Server (DNS) oder TFTP-Server, der nach dem Erstellen des Eintrags möglicherweise nie wieder verwendet werden kann. Durch die Erkennung und das Abmelden dieser Einträge wird Platz im MLS-Cache für anderen Datenverkehr gespart.

Wenn Sie MLS Fast-aging Time aktivieren müssen, legen Sie den Anfangswert auf 128 Sek. fest. Wenn die Größe des MLS-Cache weiter über 32.000 Einträge ansteigt, reduzieren Sie die Einstellung, bis die Cache-Größe unter 32.000 bleibt. Wenn der Cache weiter um mehr als 32.000 Einträge wächst, reduzieren Sie die normale MLS-Alterungszeit.

Von Cisco empfohlene MLS-Konfiguration

Behalten Sie MLS bei dem Standardwert, nur Ziel, es sei denn, ein NetFlow-Export ist erforderlich. Wenn NetFlow erforderlich ist, aktivieren Sie MLS Full Flow nur auf Supervisor Engine II-Systemen.

Geben Sie diesen Befehl ein, um das MLS-Flussziel zu aktivieren:

```
Switch(config)#mls flow ip destination
```

Jumbo-Frames

Maximale Übertragungseinheit

Die Maximum Transmission Unit (MTU) ist die größte Datagramm- oder Paketgröße in Byte, die eine Schnittstelle senden oder empfangen kann, ohne das Paket zu fragmentieren.

Laut IEEE 802.3-Standard ist die maximale Ethernet-Frame-Größe:

- **1.518 Byte** für reguläre Frames (1.500 Byte plus 18 zusätzliche Byte Ethernet-Header und CRC-Trailer)
- **1522 Byte** für 802.1Q-gekapselte Frames (1518 plus 4 Byte Tagging)

Babygiganten: Mit der Funktion "Babygiganten" kann der Switch Pakete, die etwas größer als die IEEE Ethernet-MTU sind, passieren/weiterleiten, anstatt die Frames als übergroß anzugeben und zu verwerfen.

Jumbo: Die Definition der Frame-Größe ist herstellerabhängig, da die Frame-Größen nicht zum IEEE-Standard gehören. Jumbo Frames sind Frames, die größer sind als die standardmäßige Ethernet-Frame-Größe (1518 Byte, einschließlich der Layer-2-Header- und Frame-Check-Sequenz [FCS]).

Die MTU-Standardgröße beträgt 9.216 Byte, nachdem die Unterstützung für Jumbo-Frames auf dem einzelnen Port aktiviert wurde.

Wann sind Pakete mit einem Volumen von mehr als 1518 Byte zu erwarten?

Um den Datenverkehr zwischen Switched Networks zu übertragen, stellen Sie sicher, dass die MTU des übertragenen Datenverkehrs die MTU nicht überschreitet, die von den Switchplattformen unterstützt wird. Die MTU-Größe bestimmter Frames kann aus verschiedenen Gründen abgeschnitten werden:

- **Herstellerspezifische Anforderungen**: Anwendungen und bestimmte NICs können eine MTU-Größe angeben, die über die standardmäßigen 1500 Byte hinausgeht. Diese Änderung wurde durch Studien erzielt, die belegen, dass eine Vergrößerung eines Ethernet-Frames den durchschnittlichen Durchsatz erhöhen kann.
- **Trunking** - Zur Übertragung von VLAN-ID-Informationen zwischen Switches oder anderen Netzwerkgeräten wurde Trunking verwendet, um den standardmäßigen Ethernet-Frame zu erweitern. Die zwei gängigsten Formen von Trunking sind heute:Cisco proprietäre ISL-Kapselung802.1Q
- **Multiprotocol Label Switching (MPLS)** - Nachdem Sie MPLS auf einer Schnittstelle aktiviert haben, kann MPLS die Frame-Größe eines Pakets erhöhen. Dies hängt von der Anzahl der Labels im Label-Stack für ein MPLS-getaggtes Paket ab. Die Gesamtgröße eines Labels beträgt 4 Byte. Die Gesamtgröße eines Label-Stacks beträgt:
  ```
  n * 4 bytes
  ```
  Wenn ein Label-Stack gebildet wird, können die Frames die MTU überschreiten.
- **802.1Q-Tunneling** - 802.1Q-Tunneling-Pakete enthalten zwei 802.1Q-Tags, von denen in der Regel nur jeweils einer für die Hardware sichtbar ist. Daher fügt das interne Tag dem MTU-Wert (Payload-Größe) 4 Byte hinzu.
- **Universal Transport Interface (UTI)/Layer 2 Tunneling Protocol Version 3 (Layer 2TPv3)** - UTI/Layer 2TPv3 kapselt Layer-2-Daten, die über das IP-Netzwerk weitergeleitet werden sollen. UTI/Layer 2TPv3 kann die ursprüngliche Frame-Größe um bis zu 50 Byte erhöhen. Der neue Frame enthält einen neuen IP-Header (20 Byte), einen Layer-2TPv3-Header (12 Byte) und einen neuen Layer-2-Header. Die Layer-2TPv3-Nutzlast besteht aus dem gesamten Layer-2-Frame, der den Layer-2-Header enthält.

Zweck

Hardware-basiertes Hochgeschwindigkeits-Switching (1 Gbit/s und 10 Gbit/s) hat Jumbo Frames zu einer sehr konkreten Lösung für Probleme mit dem suboptimalen Durchsatz gemacht. Obwohl es keinen offiziellen Standard für die Jumbo-Frame-Größe gibt, liegt ein ziemlich allgemeiner Wert, der häufig in diesem Feld verwendet wird, bei 9.216 Byte (9 KB).

Überlegungen zur Netzwerkeffizienz

Sie können die Netzwerkeffizienz für eine Paketweiterleitung berechnen, wenn Sie die Nutzlastgröße durch die Summe des Overhead-Werts und der Nutzlastgröße dividieren.

Selbst wenn die Netzwerkeffizienz mit Jumbo Frames nur geringfügig ansteigt und von 94,9 Prozent (1.500 Byte) auf 99,1 Prozent (9.216 Byte) steigt, sinken der Verarbeitungsaufwand (CPU-Auslastung) der Netzwerkgeräte und der Endhosts proportional zur Paketgröße. Aus diesem Grund tendieren Hochleistungs-LAN- und WAN-Netzwerktechnologien dazu, eher große maximale Frame-Größen zu bevorzugen.

Eine Leistungsverbesserung ist nur möglich, wenn lange Datentransfers durchgeführt werden.

Beispiele für Anwendungen:

- Back-to-Back-Kommunikation zwischen Servern (z. B. NFS-Transaktionen)
- Server-Clustering
- Hochgeschwindigkeits-Datensicherungen
- Hochgeschwindigkeits-Supercomputer-Verbindung
- Datentransfers für grafische Anwendungen

Überlegungen zur Netzwerkleistung

Die Leistung von TCP over WANs (Internet) wurde umfassend untersucht. Diese Gleichung erklärt, wie der TCP-Durchsatz eine Obergrenze hat, basierend auf:

- Die maximale Segmentgröße (MSS), d. h. die MTU-Länge abzüglich der Länge der TCP/IP-Header
- Round Trip Time (RTT)
- Paketverlust

$$Throughput \leq\sim 0.7 \times MSS / \left(RTT \times \sqrt{packet\_loss}\right)$$

Laut dieser Formel ist der maximal erreichbare TCP-Durchsatz direkt proportional zur MSS. Das bedeutet, dass Sie bei konstantem RTT- und Paketverlust den TCP-Durchsatz verdoppeln können, wenn Sie die Paketgröße verdoppeln. Wenn Sie statt 1518-Byte-Frames Jumbo-Frames verwenden, kann eine sechsfache Vergrößerung des TCP-Durchsatzes einer Ethernet-Verbindung zu einer sechsfachen Verbesserung führen.

Überblick

Die IEEE 802.3-Standardspezifikation definiert eine maximale Ethernet-Frame-Größe von **1518**. Die 802.1Q-gekapselten Frames mit einer Länge zwischen 1519 und 1522 Byte wurden zu einem späteren Zeitpunkt durch das IEEE Std 802.3ac-1998-Addendum zur Spezifikation 802.3 hinzugefügt. Sie werden manchmal in der Literatur als **Babygiganten** bezeichnet.

Im Allgemeinen werden Pakete als **gigantische Frames** klassifiziert, wenn sie die angegebene Ethernet-Höchstlänge für eine bestimmte Ethernet-Verbindung überschreiten. Riesenpakete werden auch als **Jumbo-Frames** bezeichnet.

Der Hauptpunkt für die Verwirrung bei Jumbo Frames ist die Konfiguration: unterschiedliche Schnittstellen unterstützen unterschiedliche maximale Paketgrößen und behandeln große Pakete manchmal auf etwas unterschiedliche Weise.

Catalyst Serie 6500

In dieser Tabelle werden die MTU-Größen zusammengefasst, die derzeit von verschiedenen Karten auf der Catalyst 6500-Plattform unterstützt werden:

Line Card	MTU-Größe
Standard	9216 Byte
WS-X6248-RJ-45, WS-X6248A-RJ-45, WS-X6248-TEL, WS-X6248A-TEL, WS-X6348-RJ-45, WS-X6348-RJ J45V,	8092 Byte (begrenzt durch den PHY-Chip)

WS-X6348-RJ-21 und WX-X6348-RJ21V	
WS-X6148-RJ-45(V), WS-X6148-RJ-21(V), WS-X6148-45AF und WS-X6148-21AF	9.100 Byte (bei 100 Mbit/s) 9.216 Byte (bei 10 Mbit/s)
WS-X6516-GE-TX	8.092 Byte (bei 100 Mbit/s) 9.216 Byte (bei 10 oder 1.000 Mbit/s)
WS-X6148(V)-GE-TX, WS-X6148-GE-45AF, WS-X6548(V)-GE-TX und WS-X6548-GE-45AF	1500 Byte
OSM ATM (OC12c)	9180 Byte
OSM CHOC3, CHOC12, CHOC48 und CT3	9216 Byte (OCx und DS3) 7673 Byte (T1/E1)
FlexWAN	7673 Byte (CT3 T1/DS0) 9216 Byte (OC3c POS) 7673 Byte (T1)
WS-X6148-GE-TX und WS-X6548-GE-TX	Keine Unterstützung

Weitere Informationen finden Sie unter Konfiguration von Ethernet, Fast Ethernet, Gigabit Ethernet und 10-Gigabit Ethernet Switching.

Layer-2- und Layer-3-Jumbo-Unterstützung in der Cisco IOS Software Catalyst 6500/6000

Auf allen GE-Ports, die als physische Layer-2- und Layer-3-Schnittstellen konfiguriert sind, wird Layer-2- und Layer-3-Jumbo-Unterstützung mit PFC/MSFC1, PFC/MSFC2 und PFC2/MSFC2 unterstützt. Die Unterstützung existiert unabhängig davon, ob diese Ports Trunking oder Channeling sind. Diese Funktion ist ab Cisco IOS Software Release 12.1.1E verfügbar.

- Die MTU-Größen aller Jumbo-fähigen physischen Ports sind miteinander verknüpft. Eine Änderung in einem von ihnen ändert alle. Nach Aktivierung behalten sie immer die gleiche MTU-Größe für Jumbo-Frames bei.
- Aktivieren Sie während der Konfiguration entweder alle Ports im gleichen VLAN, die Jumbo-fähig sind, oder aktivieren Sie keine der Ports, die Jumbo-fähig sind.
- Die MTU-Größe der Switched Virtual Interface (SVI) (VLAN-Schnittstelle) wird getrennt von der MTU der physischen Ports festgelegt. Eine Änderung der MTU der physischen Ports ändert nicht die MTU-Größe der SVI. Eine Änderung der SVI-MTU hat keine Auswirkungen auf die MTU der physischen Ports.
- Die Unterstützung von Layer-2- und Layer-3-Jumbo-Frames an FE-Schnittstellen begann mit der Cisco IOS Software, Version 12.1(8a) EX01. Der Befehl **mtu 1500** deaktiviert Jumbo auf FE, und der Befehl **mtu 9216** aktiviert Jumbo auf FE. Weitere Informationen finden Sie unter Cisco Bug ID CSCdv90450 (nur registrierte Kunden).

- Layer-3-Jumbo Frames an VLAN-Schnittstellen werden nur auf folgenden Geräten unterstützt:PFC/MSFC2 (Cisco IOS Software Release 12.1(7a)E und höher)PFC2/MSFC2 (Cisco IOS Software Release 12.1(8a)E4 und höher)
- Es wird nicht empfohlen, Jumbo Frames mit PFC/MSFC1 für VLAN-Schnittstellen (SVIs) zu verwenden, da MSFC1 die Fragmentierung möglicherweise nicht wie gewünscht verarbeiten kann.
- Für Pakete im gleichen VLAN (Layer-2-Jumbo) wird keine Fragmentierung unterstützt.
- Pakete, die über VLANs/Subnetze (Layer-3-Jumbo) fragmentiert werden müssen, werden zur Fragmentierung an die Software gesendet.

Jumbo Frame-Unterstützung in der Cisco IOS Software Catalyst 6500/6000

Ein Jumbo Frame ist ein Frame, der größer als die standardmäßige Ethernet-Frame-Größe ist. Um die Unterstützung von Jumbo-Frames zu aktivieren, konfigurieren Sie eine MTU-Größe, die größer als die Standardgröße ist, auf einem Port oder einer VLAN-Schnittstelle und konfigurieren Sie mit der Cisco IOS Software Version 12.1(13)E und höher die MTU-Größe des globalen LAN-Ports.

Prüfung der Größe des Bridge- und Routed-Datenverkehrs in der Cisco IOS-Software

Line Card	Eingang	Ausgehend
10-, 10/100-, 100-Mbit/s-Ports	Die MTU-Größe wird überprüft. Bei der Jumbo-Frame-Unterstützung wird die Größe des eingehenden Datenverkehrs mit der globalen MTU-Größe des LAN-Ports bei 10-, 10/100- und 100-Mbit/s-Ethernet- und 10-GE-LAN-Ports verglichen, für die eine nicht standardmäßige MTU-Größe konfiguriert wurde. Der Port verwirft überdimensionierten Datenverkehr.	Die MTU-Größenüberprüfung wird nicht durchgeführt. Ports, die mit einer nicht standardmäßigen MTU-Größe konfiguriert sind, übertragen Frames, die Pakete einer beliebigen Größe von mehr als 64 Byte enthalten. Bei konfigurierter, nicht standardmäßiger MTU-Größe überprüfen 10-, 10/100- und 100-Mbit/s-Ethernet-LAN-Ports keine übergroßen Ausgangs-Frames.
GE-Ports	Die MTU-Größenüberprüfung wird nicht durchgeführt. Ports, die mit einer nicht standardmäßigen MTU-Größe konfiguriert sind,	Die MTU-Größe wird überprüft. Bei der Jumbo-Frame-Unterstützung wird die Größe des Ausgangs-

	akzeptieren Frames, die Pakete jeder Größe von mehr als 64 Byte enthalten, und überprüfen nicht, ob übergroße Eingangs-Frames vorhanden sind.	Datenverkehrs mit der globalen MTU-Größe des Ausgangs-LAN-Ports bei GE- und 10-GE-LAN-Ports verglichen, für die eine nicht standardmäßige MTU-Größe konfiguriert wurde. Der Port verwirft überdimensionierten Datenverkehr.
10-GE-Ports	Die MTU-Größe wird überprüft. Der Port verwirft überdimensionierten Datenverkehr.	Die MTU-Größe wird überprüft. Der Port verwirft überdimensionierten Datenverkehr.
SVI	Die MTU-Größenüberprüfung wird nicht durchgeführt. Die SVI überprüft nicht die Frame-Größe auf der Eingangsseite.	Die MTU-Größe wird überprüft. Die MTU-Größe wird auf der Egress-Seite der SVI überprüft.
	PFC	
Gesamter gerouteter Datenverkehr	Bei Datenverkehr, der geroutet werden muss, vergleicht die Jumbo-Frame-Unterstützung auf der PFC die Datenverkehrsgrößen mit der konfigurierten MTU-Größe und bietet Layer-3-Switching für Jumbo-Datenverkehr zwischen Schnittstellen, die mit MTU-Größen konfiguriert sind, die groß genug sind, um den Datenverkehr aufzunehmen. Zwischen Schnittstellen, die nicht mit ausreichend großen MTU-Größen konfiguriert sind: • Wenn das DF-Bit (Don't Fragment) nicht festgelegt ist, sendet die PFC den Datenverkehr an die MSFC, um fragmentiert und in der Software geroutet zu werden. • Wenn das DF-Bit festgelegt ist, verwirft der PFC den Datenverkehr.	

Empfehlungen von Cisco

Bei ordnungsgemäßer Implementierung können Jumbo Frames den TCP-Durchsatz einer Ethernet-Verbindung um das Sechsfache verbessern und den Fragmentierungs-Overhead (plus geringerer CPU-Overhead auf Endgeräten) reduzieren.

Sie müssen sicherstellen, dass dazwischen kein Gerät liegt, das die angegebene MTU-Größe

nicht verarbeiten kann. Wenn dieses Gerät die Pakete fragmentiert und weiterleitet, wird der gesamte Prozess deaktiviert. Dies kann zu einem zusätzlichen Overhead auf diesem Gerät für die Fragmentierung und Reassemblierung von Paketen führen.

In solchen Fällen hilft die MTU-Erkennung des IP-Pfads dem Absender, die für die Übertragung des Datenverkehrs entlang der einzelnen Pfade geeignete gemeinsame Mindestpaketlänge zu ermitteln. Alternativ können Sie Jumbo Frame-fähige Hostgeräte mit einer MTU-Größe konfigurieren, die der Mindestgröße aller im Netzwerk unterstützten Geräte entspricht.

Sie müssen jedes Gerät sorgfältig prüfen, um sicherzustellen, dass es die MTU-Größe unterstützen kann. Siehe die Tabelle zur Unterstützung der MTU-Größe in diesem Abschnitt.

Die Unterstützung von Jumbo Frames kann für folgende Schnittstellentypen aktiviert werden:

- Port-Channel-Schnittstelle
- SVI
- Physische Schnittstelle (Layer 2/Layer 3)

Sie können Jumbo Frames auf dem Port-Channel oder den physischen Schnittstellen aktivieren, die am Port-Channel beteiligt sind. Es ist sehr wichtig sicherzustellen, dass die MTU auf allen physischen Schnittstellen gleich ist. Andernfalls kann eine ausgesetzte Schnittstelle entstehen. Sie müssen die MTU einer Port-Channel-Schnittstelle ändern, da sie die MTU aller Mitglieds-Ports ändert.

Hinweis: Wenn die MTU eines Mitglieds-Ports nicht auf den neuen Wert geändert werden kann, da der Mitglieds-Port der blockierende Port ist, wird der Port-Channel ausgesetzt.

Stellen Sie sicher, dass alle physischen Schnittstellen in einem VLAN für Jumbo Frames konfiguriert sind, bevor Sie die Unterstützung von Jumbo Frames in einer SVI konfigurieren. Die MTU eines Pakets wird nicht auf der Eingangsseite einer SVI überprüft. Sie wird jedoch auf der Egress-Seite einer SVI überprüft. Wenn die Paket-MTU größer als die Ausgangs-SVI-MTU ist, wird das Paket durch Software fragmentiert (wenn das DF-Bit nicht festgelegt ist), was zu einer schlechten Leistung führt. Die Softwarefragmentierung erfolgt nur für Layer-3-Switching. Wenn ein Paket an einen Layer-3-Port oder eine SVI mit einer kleineren MTU weitergeleitet wird, tritt eine Softwarefragmentierung auf.

Die MTU einer SVI muss immer kleiner als die kleinste MTU aller Switch-Ports im VLAN sein.

Catalyst Serie 4500

Jumbo Frames werden hauptsächlich auf den blockierungsfreien Ports der Catalyst 4500 Line Cards unterstützt. Diese blockierungsfreien GE-Ports verfügen über direkte Verbindungen zur Supervisor Engine Switching Fabric und unterstützen Jumbo Frames:

- Supervisor EnginesWS-X4515, WS-X4516 - Zwei Uplink-GBIC-Ports auf der Supervisor Engine IV oder VWS-X4516-10GE - Zwei 10-GE-Uplinks und die vier 1-GE SFP-Uplinks (Small Form Factor Pluggable)WS-X4013+ - Zwei 1-GE-UplinksWS-X4013+10GE - Zwei 10-GE-Uplinks und die vier 1-GE-SFP-UplinksWS-X4013+TS - 20 1-GE-Ports
- Line CardsWS-X4306-GB - 1000BASE-X (GBIC)-GE-Modul mit sechs PortsWS-X4506-GB-T - Sechs-Port-10/100/1000-Mbit/s und sechs-Port-SFPWS-X4302-GB - 1000BASE-X (GBIC)-GE-Modul mit zwei PortsDie ersten beiden GBIC-Ports eines 18-Port-Server-Switching-GE-Moduls (WS-X4418-GB) und der GBIC-Ports des WS-X4232-GB-RJ-Moduls

- Festkonfigurierte SwitchesWS-C4948 - Alle 48 1-GE-PortsWS-C4948-10GE - Alle 48 1-GE-Ports und zwei 10-GE-Ports

Sie können diese blockierungsfreien GE-Ports verwenden, um Jumbo Frames mit 9 KB oder Hardware-Broadcast-Unterdrückung zu unterstützen (nur Supervisor Engine IV). Alle anderen Linecards unterstützen Baby Riant Frames. Sie können Babygiganten für das Bridging von MPLS oder für Q in Q-Passthrough mit einer maximalen Nutzlast von 1552 Byte verwenden.

Hinweis: Die Frame-Größe wird mit ISL/802.1Q-Tags erhöht.

Babygiganten und Jumbo-Frames sind für andere Cisco IOS-Funktionen mit Supervisor Engines IV und V transparent.

Sicherheitsfunktionen der Cisco IOS Software

Grundlegende Sicherheitsfunktionen

Früher wurde die Sicherheit in Campus-Designs oft außer Acht gelassen. Sicherheit ist heute jedoch ein wesentlicher Bestandteil jedes Unternehmensnetzwerks. Normalerweise hat der Client bereits eine Sicherheitsrichtlinie erstellt, um zu definieren, welche Tools und Technologien von Cisco anwendbar sind.

Grundlegender Kennwortschutz

Die meisten Cisco IOS Software-Geräte sind mit zwei Kennwortstufen konfiguriert. Die erste Stufe betrifft den Telnet-Zugriff auf das Gerät, das auch als vty-Access bezeichnet wird. Nachdem der vty-Zugriff gewährt wurde, müssen Sie auf den Aktivierungsmodus oder den privilegierten exec-Modus zugreifen.

Sichern des Aktivierungsmodus des Switches

Das enable-Kennwort ermöglicht Benutzern den vollständigen Zugriff auf ein Gerät. Geben Sie das enable-Kennwort nur vertrauenswürdigen Personen zu.

```
Switch(config)#enable secret password
```

Achten Sie darauf, dass das Kennwort die folgenden Regeln befolgt:

- Das Passwort muss zwischen einem und 25 alphanumerischen Kleinbuchstaben enthalten.
- Das Kennwort darf nicht als erstes Zeichen eine Zahl enthalten.
- Sie können Leerzeichen verwenden, die jedoch ignoriert werden. Zwischen- und nachfolgende Leerzeichen werden erkannt.
- Bei der Passwortprüfung wird die Groß- und Kleinschreibung beachtet. Beispielsweise unterscheidet sich das Passwort Secret von dem Passwort secret.

Hinweis: Der Befehl **enable secret** verwendet eine unidirektionale kryptografische Message Digest 5 (MD5)-Hashing-Funktion. Wenn Sie den Befehl **show running-config** ausführen, wird dieses verschlüsselte Kennwort angezeigt. Die Verwendung des Befehls **enable password** ist eine weitere Möglichkeit zum Festlegen des enable-Kennworts. Der mit dem Befehl **enable password** verwendete Verschlüsselungsalgorithmus ist jedoch schwach und kann leicht umgekehrt werden,

um das Kennwort zu erhalten. Verwenden Sie daher nicht den Befehl **enable password**. Verwenden Sie den Befehl **enable secret**, um die Sicherheit zu erhöhen. Weitere Informationen finden Sie unter Cisco IOS Password Encryption Facts.

Sicherer Telnet-/VTY-Zugriff auf den Switch

Standardmäßig unterstützt die Cisco IOS Software fünf aktive Telnet-Sitzungen. Diese Sitzungen werden als VTY 0 bis 4 bezeichnet. Sie können diese Leitungen für den Zugriff aktivieren. Um die Anmeldung zu aktivieren, müssen Sie jedoch auch das Kennwort für diese Posten festlegen.

```
Switch(config)#line vty 0 4
Switch(config-line)#login
Switch(config-line)#password password
```

Mit dem Befehl **login** werden diese Leitungen für den Telnet-Zugriff konfiguriert. Der Befehl **password** konfiguriert ein Kennwort. Achten Sie darauf, dass das Kennwort die folgenden Regeln befolgt:

- Beim ersten Zeichen darf es sich nicht um eine Zahl handeln.
- Die Zeichenfolge kann aus bis zu 80 alphanumerischen Zeichen bestehen. Die Zeichen enthalten Leerzeichen.
- Sie können das Kennwort nicht im Format numerischer Leerzeichen angeben. Das Leerzeichen nach der Nummer verursacht Probleme. Beispiel: hello 21 ist ein legales Kennwort, 21 hello ist jedoch kein legales Kennwort.
- Bei der Passwortprüfung wird die Groß- und Kleinschreibung beachtet. Beispielsweise unterscheidet sich das Passwort Secret von dem Passwort secret.

Hinweis: Bei dieser VTY-Leitungskonfiguration speichert der Switch das Kennwort im Klartext. Wenn jemand den Befehl **show running-config** ausgibt, wird dieses Kennwort angezeigt. Um dies zu vermeiden, verwenden Sie den Befehl **service password-encryption**. Der Befehl verschlüsselt das Kennwort lose. Der Befehl verschlüsselt nur das vty-Line-Kennwort und das enable-Kennwort, das mit dem Befehl **enable password** konfiguriert wurde. Das mit dem Befehl **enable secret** konfigurierte enable-Kennwort verwendet eine stärkere Verschlüsselung. Die empfohlene Methode ist die Konfiguration mit dem Befehl **enable secret**.

Hinweis: Um ein flexibleres Sicherheitsmanagement zu gewährleisten, sollten alle Cisco IOS Software-Geräte das Sicherheitsmodell AAA (Authentication, Authorization, Accounting) implementieren. AAA kann lokale, RADIUS- und TACACS+-Datenbanken verwenden. Weitere Informationen finden Sie im Abschnitt TACACS+ Authentication Configuration (Konfiguration der TACACS+-Authentifizierung).

AAA-Sicherheitsdienste

AAA - Übersicht über den Betrieb

Zugriffskontrollkontrollen, die über Zugriffsberechtigungen für den Switch verfügen und welche Services diese Benutzer verwenden können. Die AAA-Netzwerksicherheitsservices bilden das primäre Framework für die Einrichtung der Zugriffskontrolle auf Ihrem Switch.

In diesem Abschnitt werden die verschiedenen Aspekte von AAA ausführlich beschrieben:

- Authentication (Authentifizierung) - Dieser Prozess überprüft die angegebene Identität eines Endbenutzers oder eines Geräts. Zunächst werden die verschiedenen Methoden angegeben, mit denen der Benutzer authentifiziert werden kann. Diese Methoden definieren den Authentifizierungstyp (z. B. TACACS+ oder RADIUS). Die Reihenfolge, in der diese Authentifizierungsmethoden angewendet werden sollen, ist ebenfalls definiert. Die Methoden werden dann auf die entsprechenden Schnittstellen angewendet, die die Authentifizierung aktivieren.
- Authorization (Autorisierung): Dieser Prozess gewährt einem Benutzer, einer Gruppe von Benutzern, einem System oder einem Prozess Zugriffsrechte. Der AAA-Prozess kann eine einmalige Autorisierung oder Autorisierung auf Aufgabenbasis durchführen. Der Prozess definiert Attribute (auf dem AAA-Server) für die Ausführung durch den Benutzer. Wenn der Benutzer versucht, einen Dienst zu initiieren, fragt der Switch den AAA-Server ab und fordert die Berechtigung zur Autorisierung des Benutzers an. Wenn der AAA-Server die Genehmigung erteilt, ist der Benutzer autorisiert. Wenn der AAA-Server nicht genehmigt wird, erhält der Benutzer keine Berechtigung zur Ausführung dieses Dienstes. Sie können diesen Prozess verwenden, um anzugeben, dass einige Benutzer nur bestimmte Befehle ausführen können.
- Buchhaltung - Mit diesem Prozess können Sie verfolgen, auf welche Dienste Benutzer zugreifen und wie viele Netzwerkressourcen die Benutzer nutzen. Wenn Accounting aktiviert ist, meldet der Switch Benutzeraktivitäten in Form von Accounting-Datensätzen an den AAA-Server. Beispiele für Benutzeraktivitäten, die gemeldet werden, sind die Sitzungszeit sowie die Start- und Stoppzeit. Anschließend kann eine Analyse dieser Aktivität zu Verwaltungs- oder Abrechnungszwecken durchgeführt werden.

Obwohl AAA die primäre und empfohlene Methode für die Zugriffskontrolle ist, bietet die Cisco IOS-Software zusätzliche Funktionen für eine einfache Zugriffskontrolle, die außerhalb des AAA-Bereichs liegen. Zu diesen zusätzlichen Funktionen gehören:

- Lokale Benutzername-Authentifizierung
- Line Password-Authentifizierung
- Kennwortauthentifizierung aktivieren

Diese Funktionen bieten jedoch nicht die gleiche Zugriffskontrolle wie AAA.

Um AAA besser zu verstehen, lesen Sie die folgenden Dokumente:

- Authentifizierung, Autorisierung und Abrechnung (AAA)
- Konfigurieren des grundlegenden AAA auf einem Zugriffsserver
- TACACS+- und RADIUS-Vergleich

In diesen Dokumenten wird nicht unbedingt auf Switches verwiesen. Die in den Dokumenten beschriebenen AAA-Konzepte gelten jedoch auch für Switches.

TACACS+

Zweck

Kennwörter für nicht privilegierten und privilegierten Modus sind standardmäßig global. Diese Kennwörter gelten für alle Benutzer, die entweder über den Konsolen-Port oder über eine Telnet-Sitzung im Netzwerk auf den Switch oder Router zugreifen. Die Implementierung dieser Kennwörter auf Netzwerkgeräten ist zeitaufwendig und nicht zentralisiert. Außerdem können Sie

bei der Implementierung von Zugriffsbeschränkungen Schwierigkeiten haben, wenn Zugriffskontrolllisten (ACLs) verwendet werden, die anfällig für Konfigurationsfehler sein können. Um diese Probleme zu beheben, sollten Sie beim Konfigurieren von Benutzernamen, Kennwörtern und Zugriffsrichtlinien auf einem zentralen Server einen zentralisierten Ansatz verwenden. Dieser Server kann der Cisco Secure Access Control Server (ACS) oder ein Drittanbieter-Server sein. Die Geräte sind so konfiguriert, dass sie diese zentralisierten Datenbanken für AAA-Funktionen verwenden. In diesem Fall handelt es sich bei den Geräten um Cisco IOS Software-Switches. Das Protokoll, das zwischen den Geräten und dem zentralen Server verwendet wird, kann folgendermaßen lauten:

- TACACS+
- RADIUS
- Kerberos

TACACS+ ist eine allgemeine Bereitstellung in Cisco Netzwerken und steht im Mittelpunkt dieses Abschnitts. TACACS+ bietet folgende Funktionen:

- Authentication (Authentifizierung) - Der Prozess zur Identifizierung und Überprüfung eines Benutzers. Zur Authentifizierung eines Benutzers können mehrere Methoden verwendet werden. Die gängigste Methode ist jedoch eine Kombination aus Benutzername und Kennwort.
- Authorization (Autorisierung): Wenn der Benutzer versucht, einen Befehl auszuführen, kann der Switch mit dem TACACS+-Server nachfragen, ob dem Benutzer die Berechtigung zur Verwendung dieses Befehls erteilt wurde.
- Accounting - Dieser Prozess zeichnet auf dem Gerät auf, was ein Benutzer tut oder getan hat.

Im TACACS+- und RADIUS-Vergleich finden Sie einen Vergleich zwischen TACACS+ und RADIUS.

Überblick

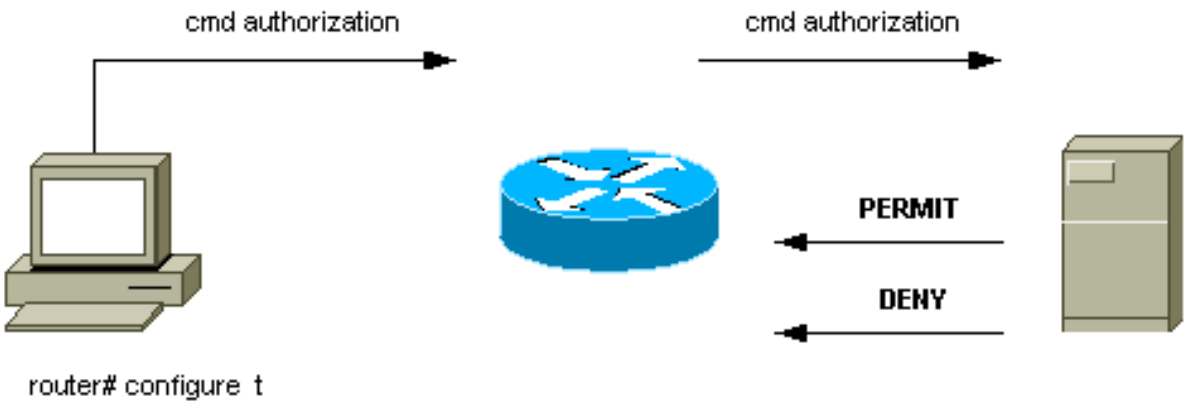
Das TACACS+-Protokoll leitet Benutzernamen und Kennwörter an den zentralisierten Server weiter. Die Informationen werden mit MD5-Einweg-Hashing über das Netzwerk verschlüsselt. Weitere Informationen finden Sie in RFC 1321 . TACACS+ verwendet TCP-Port 49 als Transportprotokoll, was gegenüber UDP folgende Vorteile bietet:

Hinweis: RADIUS verwendet UDP.

- Verbindungsorientierter Transport
- Separate Bestätigung, dass eine Anfrage eingegangen ist (TCP-Bestätigung [ACK]), unabhängig davon, wie geladen der Backend-Authentifizierungsmechanismus ist
- Sofortige Anzeige eines Serverabsturzes (Zurücksetzen von [RST]-Paketen)

Wenn während einer Sitzung eine zusätzliche Autorisierungsüberprüfung erforderlich ist, überprüft der Switch mit TACACS+, um festzustellen, ob dem Benutzer die Berechtigung zur Verwendung eines bestimmten Befehls erteilt wurde. Dieser Schritt bietet eine bessere Kontrolle über die Befehle, die auf dem Switch ausgeführt werden können, und ermöglicht eine Entkopplung vom Authentifizierungsmechanismus. Mithilfe der Befehlsabrechnung können Sie die Befehle überwachen, die ein bestimmter Benutzer ausgegeben hat, während der Benutzer an ein bestimmtes Netzwerkgerät angeschlossen ist.

Dieses Diagramm zeigt den beteiligten Autorisierungsprozess:



Wenn sich ein Benutzer bei einem Netzwerkgerät mithilfe von TACACS+ bei einem einfachen ASCII-Anmeldeversuch authentifiziert, findet dieser Vorgang in der Regel statt:

- Wenn die Verbindung hergestellt ist, kontaktiert der Switch den TACACS+-Daemon, um eine Eingabeaufforderung für den Benutzernamen abzurufen. Der Switch zeigt dann die Eingabeaufforderung für den Benutzer an. Der Benutzer gibt einen Benutzernamen ein, und der Switch kontaktiert den TACACS+-Daemon, um eine Kennwortaufforderung zu erhalten. Der Switch zeigt die Kennwortaufforderung für den Benutzer an, der ein Kennwort eingibt, das auch an den TACACS+-Daemon gesendet wird.
- Das Netzwerkgerät erhält schließlich eine dieser Antworten vom TACACS+-Daemon:ACCEPT - Der Benutzer wird authentifiziert, und der Dienst kann beginnen. Wenn das Netzwerkgerät so konfiguriert ist, dass eine Autorisierung erforderlich ist, beginnt die Autorisierung zu diesem Zeitpunkt.REJECT (ABLEHNEN): Der Benutzer konnte sich nicht authentifizieren. Dem Benutzer wird entweder der Zugriff verweigert oder er wird aufgefordert, die Anmeldesequenz erneut auszuführen. Das Ergebnis hängt vom TACACS+-Daemon ab.FEHLER - Während der Authentifizierung ist ein Fehler aufgetreten. Der Fehler kann sich entweder am Daemon oder in der Netzwerkverbindung zwischen dem Daemon und dem Switch befinden. Wenn eine FEHLER-Antwort empfangen wird, versucht das Netzwerkgerät in der Regel, eine alternative Methode zur Authentifizierung des Benutzers zu verwenden.FORTFAHREN - Der Benutzer wird zur Eingabe zusätzlicher Authentifizierungsinformationen aufgefordert.
- Benutzer müssen zuerst erfolgreich die TACACS+-Authentifizierung abschließen, bevor sie mit der TACACS+-Autorisierung fortfahren können.
- Wenn eine TACACS+-Autorisierung erforderlich ist, wird der TACACS+-Daemon erneut kontaktiert. Der TACACS+-Daemon gibt eine ACCEPT-Autorisierungsantwort oder eine REJECT-Autorisierungsantwort zurück. Wenn eine ACCEPT-Antwort zurückgegeben wird, enthält die Antwort Daten in Form von Attributen, die für die Leitung der EXEC- oder NETWORK-Sitzung für diesen Benutzer verwendet werden. Dadurch wird festgelegt, auf welche Befehle der Benutzer zugreifen kann.

Grundlegende AAA-Konfigurationsschritte

Die Konfiguration von AAA ist relativ einfach, wenn Sie den grundlegenden Prozess verstanden haben. So konfigurieren Sie die Sicherheit auf einem Cisco Router oder Zugriffsserver mithilfe von AAA:

1. Um AAA zu aktivieren, geben Sie den globalen Konfigurationsbefehl **aaa new-model** aus.
   ```
   Switch(config)#aaa new-model
   ```

   Tipp: Speichern Sie die Konfiguration, bevor Sie die AAA-Befehle konfigurieren. Speichern Sie die Konfiguration nur erneut, wenn Sie alle AAA-Konfigurationen abgeschlossen haben und die Konfiguration richtig funktioniert. Anschließend können Sie den Switch neu laden, um bei Bedarf von unvorhergesehenen Sperren wiederherzustellen (bevor Sie die Konfiguration speichern).
2. Wenn Sie sich für die Verwendung eines separaten Sicherheitsservers entscheiden, konfigurieren Sie Sicherheitsprotokollparameter wie RADIUS, TACACS+ oder Kerberos.
3. Verwenden Sie den Befehl **aaa authentication**, um die Methodenlisten für die Authentifizierung zu definieren.
4. Verwenden Sie den Befehl **login authentication**, um die Methodenlisten auf eine bestimmte Schnittstelle oder Leitung anzuwenden.
5. Geben Sie den optionalen **AAA-Autorisierungsbefehl** aus, um die Autorisierung zu konfigurieren.
6. Geben Sie den optionalen Befehl **aaa accounting** aus, um die Rechnungslegung zu konfigurieren.
7. Konfigurieren Sie den externen AAA-Server so, dass die Authentifizierungs- und Autorisierungsanfragen vom Switch verarbeitet werden.**Hinweis:** Weitere Informationen finden Sie in der Dokumentation Ihres AAA-Servers.

TACACS+-Authentifizierungskonfiguration

Führen Sie die folgenden Schritte aus, um die TACACS+-Authentifizierung zu konfigurieren:

1. Geben Sie den Befehl **aaa new-model** im globalen Konfigurationsmodus aus, um AAA auf dem Switch zu aktivieren.
2. Definieren Sie den TACACS+-Server und den zugehörigen Schlüssel.Dieser Schlüssel wird zur Verschlüsselung des Datenverkehrs zwischen dem TACACS+-Server und dem Switch verwendet. Im Befehl **tacacs-server host 1.1.1.1 key mysekrekey** lautet der TACACS+-Server unter der IP-Adresse 1.1.1.1, und der Verschlüsselungsschlüssel lautet myseckey. Um zu überprüfen, ob der Switch den TACACS+-Server erreichen kann, starten Sie vom Switch einen ICMP-Ping (Internet Control Message Protocol).
3. Definieren einer Methodenliste.Eine Methodenliste definiert die Sequenz von Authentifizierungsmechanismen, die für verschiedene Dienste versucht werden sollen. Die verschiedenen Services können z. B.:AktivierenAnmeldung (für VTY/Telnet-Zugriff)**Hinweis:** Weitere Informationen zum vty/Telnet-Zugriff finden Sie im Abschnitt Basic Security Features dieses Dokuments.KonsoleIn diesem Beispiel wird nur **Anmeldung** berücksichtigt. Sie müssen die Methodenliste auf die Schnittstellen/Posten anwenden:
   ```
   Switch(config)#aaa authentication login METHOD-LIST-LOGIN group tacacs+ line
   Switch(config)#line vty 0 4
   Switch(config-line)#login authentication METHOD-LIST-LOGIN
   Switch(config-line)#password hard_to_guess
   ```

   In dieser Konfiguration verwendet der Befehl **aaa authentication login** den generierten Listennamen METHOD-LIST-LOGIN und die Methode tacacs+, bevor die Methodenzeile verwendet wird. Benutzer werden mithilfe des TACACS+-Servers als erste Methode authentifiziert. Wenn der TACACS+-Server nicht antwortet oder keine FEHLER-Meldung

sendet, wird das Kennwort, das für die Leitung konfiguriert ist, als zweite Methode verwendet. Wenn der TACACS+-Server den Benutzer jedoch ablehnt und mit einer REJECT-Nachricht antwortet, betrachtet AAA die Transaktion als erfolgreich und verwendet nicht die zweite Methode.**Hinweis:** Die Konfiguration ist erst abgeschlossen, wenn Sie die Liste (METHODE-LIST-LOGIN) auf die vty-Zeile anwenden. Geben Sie den Befehl **login authentication-LIST-LOGIN** im Leitungskonfigurationsmodus aus, wie das Beispiel zeigt.**Hinweis:** Im Beispiel wird eine Backdoor erstellt, wenn der TACACS+-Server nicht verfügbar ist. Sicherheitsadministratoren können oder können die Implementierung einer Backdoor nicht akzeptieren. Stellen Sie sicher, dass die Entscheidung, solche Backdoors zu implementieren, den Sicherheitsrichtlinien der Website entspricht.

RADIUS-Authentifizierungskonfiguration

Die RADIUS-Konfiguration ist nahezu identisch mit der TACACS+-Konfiguration. Ersetzen Sie in der Konfiguration einfach das Wort RADIUS durch TACACS. Dies ist eine Beispiel-RADIUS-Konfiguration für den COM-Port-Zugriff:

```
Switch(config)#aaa new-model
Switch(config)#radius-server host 1.1.1.1 key mysecretkey
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group radius line
Switch(config)#line con 0
Switch(config-line)#login authentication METHOD-LIST-LOGIN
Switch(config-line)#password hard_to_guess
```

Anmeldebanner

Erstellen Sie geeignete Gerätebanner, in denen die Aktionen angegeben werden, die bei nicht autorisiertem Zugriff ausgeführt werden. Werben Sie nicht für unbefugte Benutzer mit dem Namen der Website oder den Netzwerkinformationen. Die Banner bieten Rückgriff auf den Fall, dass ein Gerät kompromittiert wird und der Täter gefangen wird. Geben Sie diesen Befehl ein, um Anmeldebanner zu erstellen:

```
Switch(config)#banner motd ^C
*** Unauthorized Access Prohibited ***
^C
```

Physische Sicherheit

Stellen Sie sicher, dass eine ordnungsgemäße Autorisierung für den physischen Zugriff auf Geräte erforderlich ist. Halten Sie das Gerät in einem kontrollierten (gesperrten) Bereich. Um sicherzustellen, dass das Netzwerk betriebsbereit bleibt und nicht von schädlichen Manipulationen oder Umgebungsfaktoren beeinflusst wird, müssen alle Geräte über Folgendes verfügen:

- Eine geeignete unterbrechungsfreie Stromversorgung (USV) mit nach Möglichkeit redundanten Quellen
- Temperaturregelung (Klimaanlage)

Denken Sie daran, dass eine Person mit böswilliger Absicht den physischen Zugriff verletzt, eine Unterbrechung durch Kennwortwiederherstellung oder andere Mittel viel wahrscheinlicher ist.

Verwaltungskonfiguration

Netzwerkdiagramme

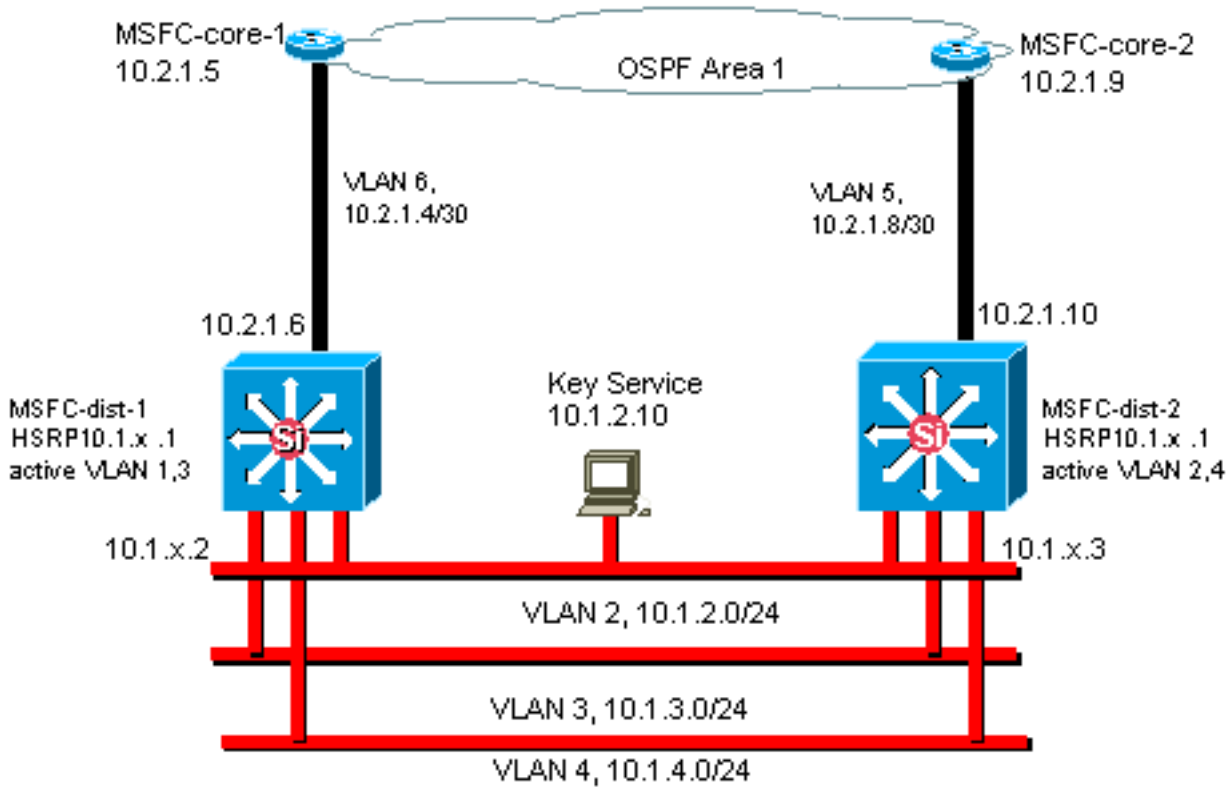
Zweck

Klare Netzwerkdiagramme sind ein wesentlicher Bestandteil des Netzwerkbetriebs. Die Diagramme werden bei der Fehlerbehebung kritisch und stellen das wichtigste Medium für die Kommunikation von Informationen während der Eskalation an Anbieter und Partner bei einem Ausfall dar. Unterschätzen Sie nicht die Vorbereitung, Bereitschaft und Zugänglichkeit, die Netzwerkdiagramme bieten.

Empfehlung

Diese drei Typen von Diagrammen sind erforderlich:

- **Gesamtdiagramm** - Selbst für die größten Netzwerke ist ein Diagramm, das die End-to-End-physische oder logische Konnektivität zeigt, wichtig. Häufig dokumentieren Unternehmen, die ein hierarchisches Design implementiert haben, jede Ebene separat. Bei der Planung und Problemlösung ist es wichtig, dass Sie wissen, wie die Domänen miteinander verknüpft sind.
- **Physisches Diagramm** - Dieses Diagramm zeigt die gesamte Switch- und Router-Hardware und -Verkabelung. Stellen Sie sicher, dass das Diagramm die folgenden Aspekte kennzeichnet:TrunksLinksGeschwindigkeitenChannel-GruppenPortnummernSteckplätzeChassis-TypenSoftwareVTP-DomänenRoot BridgeBackup-Root-Bridge-PrioritätMAC-AdresseBlockierte Ports pro VLANAus Gründen der Klarheit sollten interne Geräte wie der Catalyst 6500/6000 MSFC-Router als Router auf einem Stick dargestellt werden, der über einen Trunk verbunden ist.
- **Logisches Diagramm** - Dieses Diagramm zeigt nur die Layer-3-Funktionalität, d. h. Router werden als Objekte und VLANs als Ethernet-Segmente angezeigt. Stellen Sie sicher, dass das Diagramm die folgenden Aspekte beschreibt:IP-AdressenSubnetzeSekundäre AdressierungHSRP Aktiv und StandbyAccess Core Distribution LayerRouting-Informationen



Switch-Management-Schnittstelle und natives VLAN

Zweck

In diesem Abschnitt werden die Bedeutung und die potenziellen Probleme bei der Verwendung des Standard-VLAN 1 beschrieben. Dieser Abschnitt behandelt auch mögliche Probleme, wenn Sie Verwaltungsdatenverkehr zum Switch im selben VLAN wie Benutzerdatenverkehr auf Switches der Serien 6500 und 6000 ausführen.

Die Prozessoren der Supervisor Engines und MSFCs für die Catalyst 6500/6000-Serie verwenden VLAN 1 für eine Reihe von Steuerungs- und Verwaltungsprotokollen. Beispiele:

- Switch-Steuerungsprotokolle:STP-BPDUsVTPDTPCDP
- Verwaltungsprotokolle:SNMPTelnetSecure Shell Protocol (SSH)Syslog

Wenn das VLAN auf diese Weise verwendet wird, wird es als natives VLAN bezeichnet. In der Standard-Switch-Konfiguration wird VLAN 1 auf den Catalyst-Trunk-Ports als natives Standard-VLAN festgelegt. Sie können VLAN 1 als natives VLAN beibehalten. Beachten Sie jedoch, dass alle Switches, auf denen die Cisco IOS-Systemsoftware im Netzwerk ausgeführt wird, standardmäßig alle Schnittstellen festlegen, die als Layer-2-Switch-Ports konfiguriert sind, um auf Ports in VLAN 1 zuzugreifen. Höchstwahrscheinlich verwendet ein Switch im Netzwerk VLAN 1 als VLAN für Benutzerdatenverkehr.

Das Hauptproblem bei der Verwendung von VLAN 1 besteht darin, dass der NMP der Supervisor Engine im Allgemeinen nicht durch einen Großteil des Broadcast- und Multicast-Datenverkehrs unterbrochen werden muss, den Endstationen generieren. Insbesondere Multicast-Anwendungen senden tendenziell viele Daten zwischen Servern und Clients. Die Supervisor Engine muss diese Daten nicht sehen. Wenn die Ressourcen oder Puffer der Supervisor Engine vollständig belegt sind, während die Supervisor Engine unnötigen Datenverkehr überwacht, kann die Supervisor

Engine Managementpakete nicht anzeigen, die einen Spanning-Tree-Loop oder einen EtherChannel-Ausfall verursachen können (im schlimmsten Fall).

Der Befehl **show interfaces** *interface_type slot/port* **counter** und der Befehl **show ip traffic können Ihnen einige Hinweise auf Folgendes geben:**

- Der Anteil der Übertragung an Unicast-Datenverkehr
- Der Anteil des IP-Datenverkehrs an Nicht-IP-Datenverkehr (der in der Regel in Management-VLANs nicht sichtbar ist)

VLAN 1-Tags und verarbeitet den Großteil des Kontrollebenen-Datenverkehrs. VLAN 1 ist auf allen Trunks standardmäßig aktiviert. Bei größeren Campus-Netzwerken müssen Sie auf den Durchmesser der STP-Domäne von VLAN 1 achten. Instabilität in einem Teil des Netzwerks kann sich auf VLAN 1 auswirken und die Stabilität der Kontrollebene und die STP-Stabilität für alle anderen VLANs beeinflussen. Sie können die VLAN 1-Übertragung von Benutzerdaten und den Betrieb von STP auf einer Schnittstelle einschränken. Konfigurieren Sie einfach das VLAN nicht auf der Trunk-Schnittstelle.

Diese Konfiguration unterbindet nicht die Übertragung von Steuerungspaketen zwischen Switches in VLAN 1, wie bei einem Netzwerkanalyse. Es werden jedoch keine Daten weitergeleitet, und STP wird nicht über diesen Link ausgeführt. Daher können Sie mit dieser Technik VLAN 1 in kleinere Failure-Domains aufteilen.

Hinweis: Sie können VLAN 1 nicht von Trunks zu Catalyst 2900XL/3500XLs löschen.

Selbst wenn Sie darauf achten, die Benutzer-VLANs auf relativ kleine Switch-Domänen und entsprechend kleine Fehler-/Layer-3-Grenzen zu beschränken, sind einige Kunden immer noch versucht, das Management-VLAN anders zu behandeln. Diese Kunden versuchen, das gesamte Netzwerk über ein zentrales Management-Subnetz abzudecken. Es gibt keinen technischen Grund, warum eine zentrale NMS-Anwendung an die von der Anwendung verwalteten Geräte Layer 2 angebunden sein muss. Dies ist auch kein qualifiziertes Sicherheitsargument. Begrenzen Sie den Durchmesser der Management-VLANs auf die gleiche geroutete Domänenstruktur wie die der Benutzer-VLANs. Betrachten Sie Out-of-Band-Management und/oder SSH-Unterstützung als Möglichkeit, die Sicherheit des Netzwerkmanagements zu erhöhen.

Weitere Optionen

Für diese Cisco Empfehlungen gibt es in einigen Topologien Designüberlegungen. So ist z. B. ein wünschenswertes und gemeinsames Cisco Multilayer-Design geeignet, um die Verwendung eines aktiven Spanning Tree zu vermeiden. Auf diese Weise erfordert das Design die Einschränkung jedes IP-Subnetzes/VLAN auf einen einzelnen Access-Layer-Switch (oder Switch-Cluster). In diesen Designs kann kein Trunking bis zum Access Layer konfiguriert werden.

Erstellen Sie ein separates Management-VLAN, und aktivieren Sie Trunking, um es zwischen den Layer-2-Access- und Layer-3-Distribution-Layer zu übertragen? Auf diese Frage gibt es keine einfache Antwort. Lassen Sie sich von den folgenden beiden Optionen bei der Überprüfung des Designs mit Ihrem Cisco Techniker beraten:

- **Option 1**: Zwei oder drei eindeutige VLANs vom Distribution Layer bis hin zu jedem Access Layer-Switch miteinander verbinden. Diese Konfiguration ermöglicht ein Daten-VLAN, ein Sprach-VLAN und ein Management-VLAN und hat weiterhin den Vorteil, dass STP inaktiv ist. Zum Löschen von VLAN 1 aus Trunks ist ein zusätzlicher Konfigurationsschritt erforderlich. Bei dieser Lösung sind außerdem Designaspekte zu berücksichtigen, um zu verhindern, dass

bei der Wiederherstellung nach Ausfällen vorübergehend schwarzer Datenverkehr mit geroutetem Code verloren geht. Verwenden Sie STP PortFast für Trunks (in Zukunft) oder die automatische VLAN-Zustandssynchronisierung mit STP-Weiterleitung.

- **Option 2**: Ein einzelnes VLAN für Daten und Management kann akzeptabel sein. Wenn Sie die sc0-Schnittstelle von den Benutzerdaten trennen möchten, ist dieses Szenario mit neuerer Switch-Hardware weniger problematisch als früher. Die neuere Hardware bietet:Leistungsstärkere CPUs und Kontrollen zur Ratenbegrenzung auf KontrollebeneDesign mit relativ kleinen Broadcast-Domänen, wie vom Multilayer-Design empfohlenUm eine endgültige Entscheidung zu treffen, sollten Sie das Broadcast-Datenverkehrsprofil für das VLAN prüfen und mit Ihrem Cisco Techniker die Funktionen der Switch-Hardware besprechen. Wenn das Management-VLAN alle Benutzer auf diesem Access-Layer-Switch enthält, verwenden Sie IP-Eingabefelder, um den Switch gemäß dem Abschnitt Cisco IOS Software Security Features (Sicherheitsfunktionen der Cisco IOS-Software) vor den Benutzern zu schützen.

Cisco Management Interface und die Empfehlung nativer VLANs

Verwaltungsschnittstelle

Die Cisco IOS-Systemsoftware bietet die Möglichkeit, Schnittstellen als Layer-3-Schnittstellen oder als Layer-2-Switch-Ports in einem VLAN zu konfigurieren. Wenn Sie den Befehl **switchport** in der Cisco IOS-Software verwenden, sind alle Switch-Ports standardmäßig Zugriffsports in VLAN 1. Wenn Sie also nichts anderes konfigurieren, können Benutzerdaten standardmäßig auch in VLAN 1 vorhanden sein.

Verwandeln Sie das Management-VLAN in ein anderes VLAN als VLAN 1. Verwahren Sie alle Benutzerdaten aus dem Management-VLAN heraus. Konfigurieren Sie stattdessen eine loopback0-Schnittstelle als Management-Schnittstelle auf jedem Switch.

Hinweis: Wenn Sie das OSPF-Protokoll verwenden, wird dies auch zur OSPF-Router-ID.

Stellen Sie sicher, dass die Loopback-Schnittstelle eine 32-Bit-Subnetzmaske hat, und konfigurieren Sie die Loopback-Schnittstelle als reine Layer 3-Schnittstelle auf dem Switch. Dies ist ein Beispiel:

```
Switch(config)#interface loopback 0
Switch(config-if)#ip address 10.x.x.x 255.255.255.255
Switch(config-if)#end
Switch#
```

Natives VLAN

Konfigurieren Sie das native VLAN als offensichtliches Dummy-VLAN, das auf dem Router nicht aktiviert ist. Cisco hat in der Vergangenheit VLAN 999 empfohlen, die Auswahl ist jedoch rein willkürlich.

Führen Sie diese Schnittstellenbefehle aus, um ein VLAN als natives (Standard-)VLAN für 802.1Q-Trunking an einem bestimmten Port einzurichten:

```
Switch(config)#interface type slot/port
Switch(config-if)#switchport trunk native vlan 999
```

Weitere Empfehlungen zur Trunking-Konfiguration finden Sie im Abschnitt Dynamic Trunking Protocol in diesem Dokument.

Out-of-Band-Management

Zweck

Durch den Aufbau einer separaten Management-Infrastruktur im Produktionsnetzwerk können Sie das Netzwerkmanagement noch weiter optimieren. Diese Konfiguration ermöglicht die Remote-Erreichbarkeit von Geräten, auch wenn der Datenverkehr geleitet wird oder Ereignisse auf der Steuerungsebene auftreten. Diese beiden Ansätze sind typisch:

- Out-of-Band-Management mit einem exklusiven LAN
- Out-of-Band-Management mit Terminalservern

Überblick

Sie können jedem Router und Switch im Netzwerk eine Out-of-Band-Ethernet-Management-Schnittstelle in einem Management-VLAN bereitstellen. Sie konfigurieren für jedes Gerät im Management-VLAN einen Ethernet-Port und für die Verkabelung eines Ports außerhalb des Produktionsnetzwerks zu einem separaten Switched Management-Netzwerk.

Hinweis: Catalyst Switches der Serien 4500 und 4000 verfügen über eine spezielle Me1-Schnittstelle auf der Supervisor Engine, die nur für das Out-of-Band-Management und nicht als Switch-Port verwendet wird.

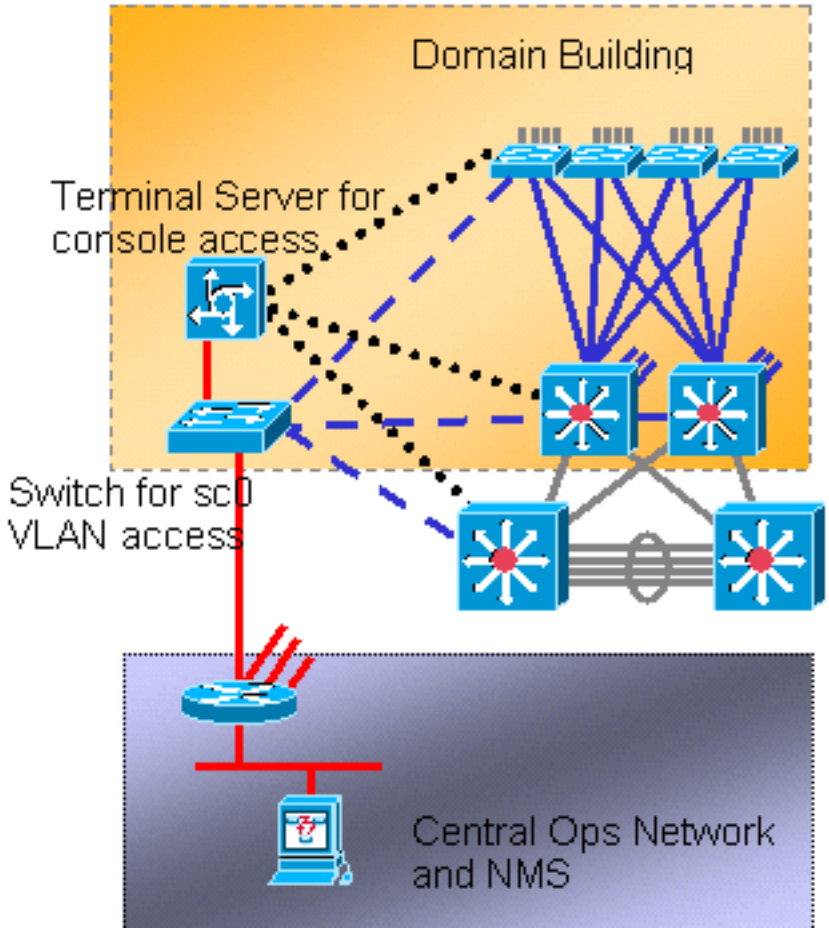
Darüber hinaus können Sie Terminalserververbindungen herstellen, wenn Sie einen Cisco 2600 oder 3600 Router mit seriellen RJ-45-Kabeln konfigurieren, um auf den Konsolenport jedes Routers und Switches im Layout zuzugreifen. Durch die Verwendung eines Terminalservers ist es zudem nicht erforderlich, Backup-Szenarien zu konfigurieren, z. B. Modems an AUX-Ports für jedes Gerät. Sie können ein einzelnes Modem auf dem AUX-Port des Terminalservers konfigurieren. Diese Konfiguration stellt bei einem Netzwerkverbindungsausfall einen Einwahldienst für die anderen Geräte bereit. Weitere Informationen finden Sie unter Verbinden eines Modems mit dem Konsolenport der Catalyst Switches.

Empfehlung

Bei dieser Anordnung sind neben zahlreichen In-Band-Pfaden zwei Out-of-Band-Pfade zu jedem Switch und Router möglich. Die Anordnung ermöglicht ein hochverfügbares Netzwerkmanagement. Die Vorteile sind:

- Die Anordnung trennt den Verwaltungsdatenverkehr von den Benutzerdaten.
- Die Management-IP-Adresse befindet sich aus Sicherheitsgründen in einem separaten Subnetz, VLAN und Switch.
- Die Gewährleistung für die Bereitstellung von Managementdaten bei Netzwerkausfällen ist höher.
- Im Management-VLAN ist kein aktiver Spanning Tree vorhanden. Redundanz ist hier nicht entscheidend.

Dieses Diagramm zeigt die Out-of-Band-Verwaltung:



Systemprotokollierung

Zweck

Syslog-Meldungen sind Cisco-spezifisch und können reaktionsfähigere und genauere Informationen liefern als das standardisierte SNMP. Verwaltungsplattformen wie Cisco Resource Manager Essentials (RME) und Network Analysis Toolkit (NATKit) nutzen beispielsweise Syslog-Informationen zur Erfassung von Bestands- und Konfigurationsänderungen.

Cisco Syslog-Konfigurationsempfehlung

Die Systemprotokollierung ist eine gängige und akzeptierte Praxis. Ein UNIX-Syslog kann Informationen/Ereignisse auf dem Router erfassen und analysieren, z. B.:

- Schnittstellenstatus
- Sicherheitswarnungen
- Umgebungsbedingungen
- CPU-Prozess-Hosting
- Weitere Veranstaltungen

Die Cisco IOS Software kann die UNIX-Protokollierung auf einem UNIX-Syslog-Server durchführen. Das Cisco UNIX-Syslog-Format ist kompatibel mit 4.3 Berkeley Standard Distribution (BSD) UNIX. Verwenden Sie die folgenden Protokolleinstellungen der Cisco IOS-Software:

- **no logging console** (**keine Protokollierungskonsole**): Standardmäßig werden alle Systemmeldungen an die Systemkonsole gesendet. Die Konsolenprotokollierung ist eine

vorrangige Aufgabe der Cisco IOS Software. Diese Funktion wurde hauptsächlich entwickelt, um dem Systembetreiber vor einem Systemausfall Fehlermeldungen zu senden. Deaktivieren Sie die Konsolenprotokollierung in allen Gerätekonfigurationen, um zu verhindern, dass der Router/Switch hängen bleibt, während das Gerät auf eine Antwort von einem Terminal wartet. Konsolenmeldungen können jedoch während der Problemisolierung nützlich sein. Aktivieren Sie in diesen Fällen die Konsolenprotokollierung. Geben Sie den Befehl für die Protokollierungskonsolenebene ein, um die gewünschte Stufe der Nachrichtenprotokollierung zu erhalten. Die Protokollierungsebenen reichen von 0 bis 7.

- **no logging monitor** - Mit diesem Befehl wird die Protokollierung für andere Terminalleitungen als die Systemkonsole deaktiviert. Die Protokollierung von Überwachen kann erforderlich sein (mit der Verwendung von **Protokollierung von Monitor-Debugging** oder einer anderen Befehlsoption). Aktivieren Sie in diesem Fall die Überwachungsprotokollierung auf der für die Aktivität erforderlichen Protokollierungsebene. Weitere Informationen über die Protokollierungsebenen finden Sie in der Menüoption "**no logging console**" in dieser Liste.
- **logging puffered 16384** - Der Befehl **logging puffered** muss hinzugefügt werden, um Systemmeldungen im internen Protokollpuffer zu protokollieren. Der Protokollierungspuffer ist kreisförmig. Sobald der Protokollierungspuffer gefüllt ist, werden ältere Einträge durch neuere Einträge überschrieben. Die Größe des Protokollierungspuffers kann vom Benutzer konfiguriert werden und wird in Byte angegeben. Die Größe des Systempuffers variiert je nach Plattform. 16384 ist ein guter Standard, der in den meisten Fällen eine angemessene Protokollierung ermöglicht.
- **logging trap notification** (**Trap-Benachrichtigungen**): Dieser Befehl stellt dem angegebenen Syslog-Server Nachrichten auf Benachrichtigungsebene (5) zur Verfügung. Die Standard-Protokollierungsebene für alle Geräte (Konsole, Monitor, Puffer und Traps) ist Debugging (Stufe 7). Wenn Sie die Trap-Protokollierungsebene bei 7 belassen, werden viele externe Nachrichten erstellt, die für den Zustand des Netzwerks wenig oder gar nicht relevant sind. Legen Sie die Standardprotokollierungsstufe für Traps auf 5 fest.
- **logging einrichtung local7**: Mit diesem Befehl wird die standardmäßige Protokollierungseinrichtung/-ebene für die UNIX-Syslogging-Protokollierung festgelegt. Konfigurieren Sie den Syslog-Server, der diese Meldungen empfängt, für die gleiche Einrichtung/Ebene.
- **logging host**: Dieser Befehl legt die IP-Adresse des UNIX-Protokollierungsservers fest.
- **logging source-interface loopback 0**: Mit diesem Befehl wird die Standard-IP-SA für die Syslog-Meldungen festgelegt. Hard Code die Protokollierung SA, um die Identifizierung des Hosts zu erleichtern, der die Nachricht gesendet hat.
- **service timestamps debug datetime localtime show-timezone msec** - Protokollmeldungen werden standardmäßig nicht mit einem Zeitstempel versehen. Mit diesem Befehl können Sie das Timestamping von Protokollmeldungen aktivieren und das Timestamping von Systemdebugmeldungen konfigurieren. Timestamping bietet die relative zeitliche Steuerung protokollierter Ereignisse und verbessert das Debuggen in Echtzeit. Diese Informationen sind besonders nützlich, wenn Kunden Fehlerbehebungsausgaben an die Mitarbeiter des technischen Supports senden. Verwenden Sie den Befehl im globalen Konfigurationsmodus, um das Timestamping von Systemdebugmeldungen zu aktivieren. Der Befehl hat nur Auswirkungen, wenn Debuggen aktiviert ist.

Hinweis: Aktivieren Sie außerdem die Protokollierung für den Verbindungsstatus und den Paketstatus auf allen Gigabit-Infrastrukturschnittstellen.

Die Cisco IOS Software bietet einen einzigen Mechanismus, um die Einrichtung und die

Protokollstufe für alle Systemmeldungen festzulegen, die für einen Syslog-Server bestimmt sind. Legen Sie für die Protokollierungsfalle die Benachrichtigung fest (Stufe 5). Wenn Sie die Trap-Nachrichtenebene auf Benachrichtigung festlegen, können Sie die Anzahl der an den Syslog-Server weitergeleiteten Informationsmeldungen minimieren. Diese Einstellung kann die Menge des Syslog-Datenverkehrs im Netzwerk erheblich reduzieren und die Auswirkungen auf die Syslog-Serverressourcen reduzieren.

Fügen Sie die folgenden Befehle zu jedem Router und Switch hinzu, der die Cisco IOS Software ausführt, um Syslog-Messaging zu aktivieren:

- Globale Syslog-Konfigurationsbefehle:

```
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging host-ip
logging source-interface loopback 0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
```

- Syslog-Schnittstellenkonfigurationsbefehle:

```
logging event link-status
logging event bundle-status
```

SNMP

Zweck

Sie können SNMP verwenden, um Statistiken, Zähler und Tabellen abzurufen, die in MIBs von Netzwerkgeräten gespeichert sind. NMSs wie HP OpenView können diese Informationen nutzen, um:

- Echtzeit-Warnmeldungen generieren
- Verfügbarkeitsmessung
- Erstellung von Informationen zur Kapazitätsplanung
- Unterstützung bei der Durchführung von Konfigurations- und Fehlerbehebungsprüfungen

SNMP-Management-Schnittstellenbetrieb

SNMP ist ein Protokoll auf Anwendungsebene, das ein Nachrichtenformat für die Kommunikation zwischen SNMP-Managern und -Agenten bereitstellt. SNMP bietet ein standardisiertes Framework und eine gemeinsame Sprache für die Überwachung und Verwaltung von Geräten in einem Netzwerk.

Das SNMP-Framework besteht aus den folgenden drei Komponenten:

- Ein SNMP-Manager
- Ein SNMP-Agent

- A MIB

Der SNMP-Manager ist das System, das SNMP verwendet, um die Aktivitäten der Netzwerk-Hosts zu steuern und zu überwachen. Das gängigste Managementsystem heißt NMS. Sie können den Begriff NMS entweder auf ein dediziertes Gerät anwenden, das für die Netzwerkverwaltung verwendet wird, oder auf die Anwendungen, die auf einem solchen Gerät verwendet werden. Für die Verwendung mit SNMP stehen verschiedene Netzwerkverwaltungsanwendungen zur Verfügung. Diese Anwendungen reichen von einfachen CLI-Anwendungen bis hin zu funktionsreichen GUIs wie der CiscoWorks-Produktreihe.

Der SNMP-Agent ist die Softwarekomponente im verwalteten Gerät, die die Daten für das Gerät verwaltet und diese Daten ggf. an das Management der Systeme meldet. Der Agent und die MIB befinden sich auf dem Routing-Gerät (Router, Zugriffsserver oder Switch). Um den SNMP-Agent auf einem Cisco Routing-Gerät zu aktivieren, müssen Sie die Beziehung zwischen dem Manager und dem Agenten definieren.

Die MIB ist ein virtueller Informationsspeicherbereich für Netzwerkmanagementinformationen. Die MIB besteht aus Auflistungen verwalteter Objekte. Innerhalb der MIB gibt es Auflistungen verwandter Objekte, die in MIB-Modulen definiert sind. MIB-Module werden in der Sprache des SNMP MIB-Moduls geschrieben, wie STD 58, RFC 2578 , RFC 2579 und RFC 2580 definieren.

Hinweis: Einzelne MIB-Module werden auch als MIBs bezeichnet. Beispielsweise ist die Schnittstellengruppe MIB (IF-MIB) ein MIB-Modul innerhalb der MIB auf Ihrem System.

Der SNMP-Agent enthält MIB-Variablen, deren Werte der SNMP-Manager anfordern oder ändern kann, indem er Abruf- oder Abrufvorgänge durchführt. Ein Manager kann einen Wert von einem Agenten erhalten oder einen Wert in diesem Agenten speichern. Der Agent sammelt Daten von der MIB, dem Repository für Informationen über Geräteparameter und Netzwerkdaten. Der Agent kann auch auf Manager-Anfragen reagieren, um Daten abzurufen oder festzulegen.

Ein Manager kann die Agentenanfragen senden, um MIB-Werte abzurufen und festzulegen. Der Mitarbeiter kann auf diese Anfragen antworten. Unabhängig von dieser Interaktion kann der Agent unaufgefordert Benachrichtigungen (Traps oder Informationen) an den Manager senden, um den Manager über die Netzwerkbedingungen zu informieren. Mit einigen Sicherheitsmechanismen kann ein NMS Informationen in den MIBs abrufen, indem es `nächste` Anforderungen `abruft` und `abruft` und den **set-**Befehl ausgeben kann, um Parameter zu ändern. Darüber hinaus können Sie ein Netzwerkgerät einrichten, um eine Trap-Nachricht für Echtzeit-Warnmeldungen an das NMS zu generieren. Für Traps werden die IP UDP-Ports 161 und 162 verwendet.

SNMP-Benachrichtigungen Operative Übersicht

Eine wichtige Funktion von SNMP ist die Möglichkeit, Benachrichtigungen von einem SNMP-Agent zu generieren. Für diese Benachrichtigungen müssen keine Anfragen vom SNMP-Manager gesendet werden. Unerwünschte (asynchrone) Benachrichtigungen können als Traps generiert oder als Instruktanforderungen generiert werden. Traps sind Meldungen, die den SNMP-Manager auf einen Zustand im Netzwerk hinweisen. Informationsanfragen (Informationen) sind Traps, die eine Anfrage zur Bestätigung des Empfangs durch den SNMP-Manager enthalten. Benachrichtigungen können auf wichtige Ereignisse hinweisen, z. B.:

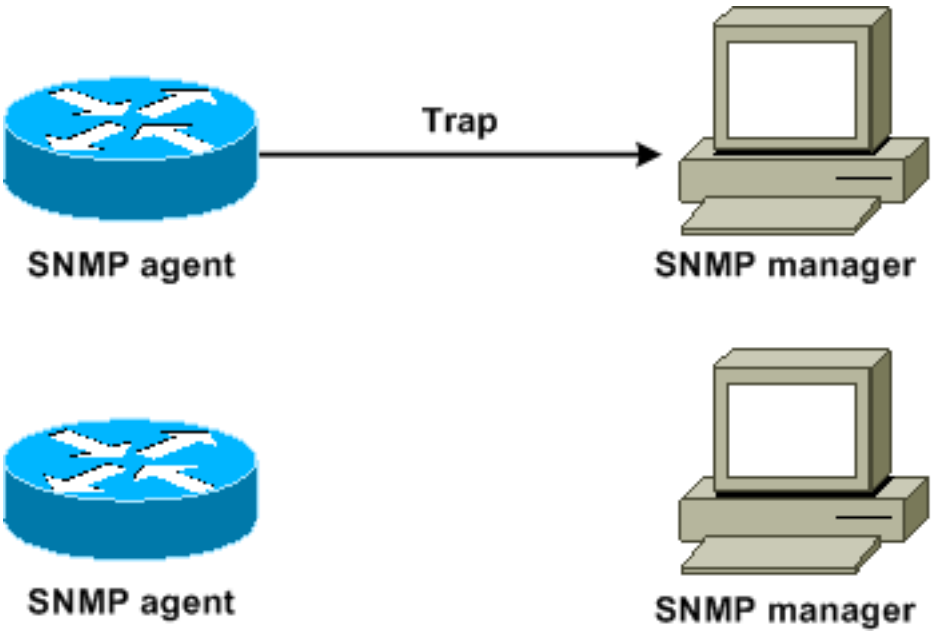
- Falsche Benutzerauthentifizierung
- Neustart
- Schließen einer Verbindung
- Verlust der Verbindung zu einem Nachbarrouter

- Weitere Veranstaltungen

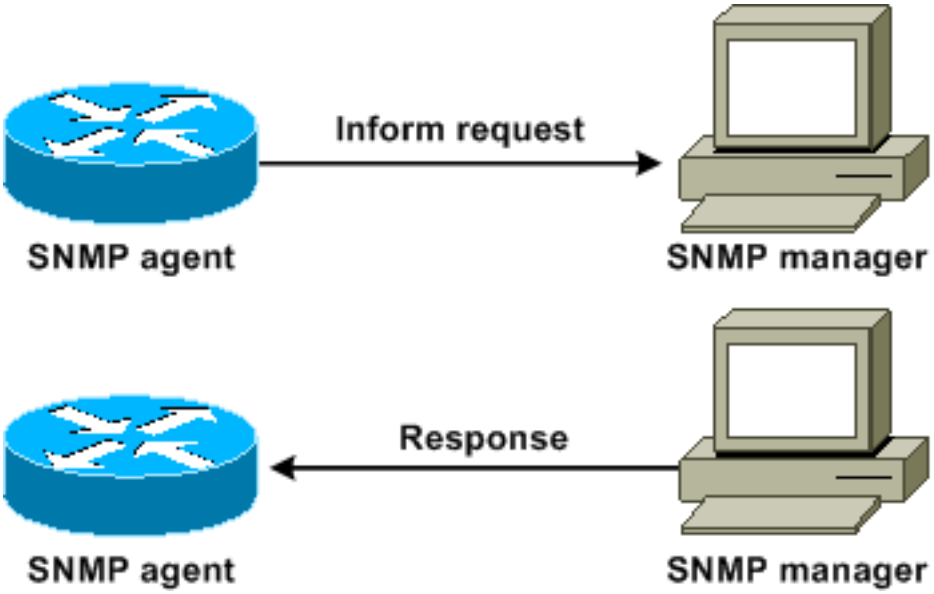
Traps sind weniger zuverlässig als Informationen, da der Empfänger keine Bestätigung sendet, wenn der Empfänger eine Falle empfängt. Der Absender kann nicht feststellen, ob das Trap empfangen wurde. Ein SNMP-Manager, der eine Insider-Anfrage empfängt, bestätigt die Nachricht mit einer SNMP-PDU (Response Protocol Data Unit). Wenn der Manager keine Instruktionsanfrage erhält, sendet er keine Antwort. Wenn der Absender nie eine Antwort erhält, kann der Absender die Anforderung erneut senden. Bei Informs ist es wahrscheinlicher, dass sie das beabsichtigte Ziel erreichen.

Traps sind jedoch häufig vorzuziehen, da Informationen mehr Ressourcen im Router und im Netzwerk beanspruchen. Eine Falle wird verworfen, sobald sie gesendet wird. Eine Insider-Anfrage muss jedoch im Gedächtnis gehalten werden, bis eine Antwort eingeht oder die Anfrage abstürzt. Traps werden auch nur einmal gesendet, während eine Information mehrfach versucht werden kann. Die erneuten Versuche erhöhen den Datenverkehr und tragen zu einem höheren Overhead im Netzwerk bei. Fallen und Informationsanfragen stellen somit einen Kompromiss zwischen Zuverlässigkeit und Ressourcen dar. Wenn Sie den SNMP-Manager benötigen, um jede Benachrichtigung zu erhalten, verwenden Sie Insider-Anfragen. Wenn Sie jedoch Bedenken hinsichtlich des Datenverkehrs im Netzwerk oder Speicher im Router haben und Sie nicht jede Benachrichtigung erhalten müssen, verwenden Sie Traps.

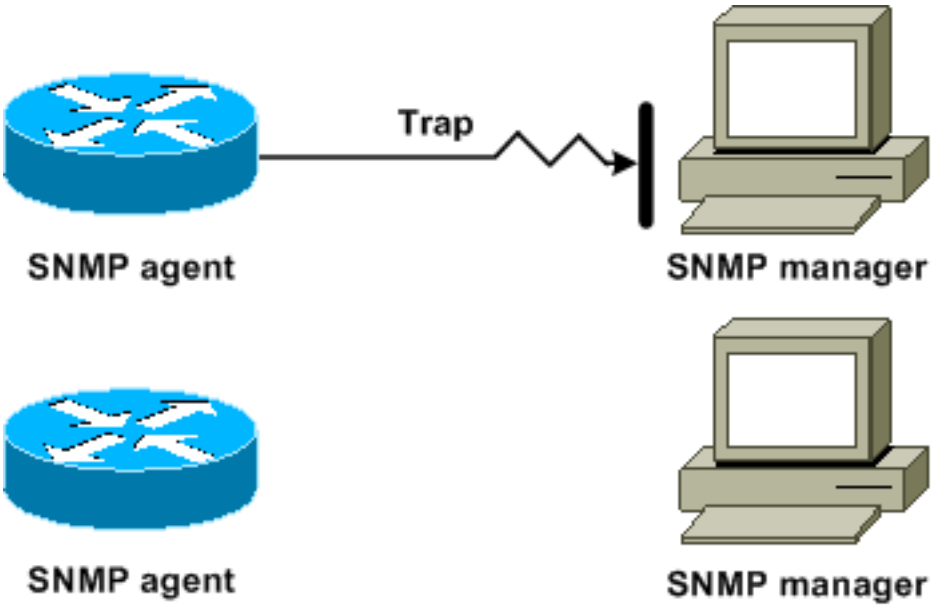
In diesen Diagrammen werden die Unterschiede zwischen Traps und Informationsanforderungen veranschaulicht:



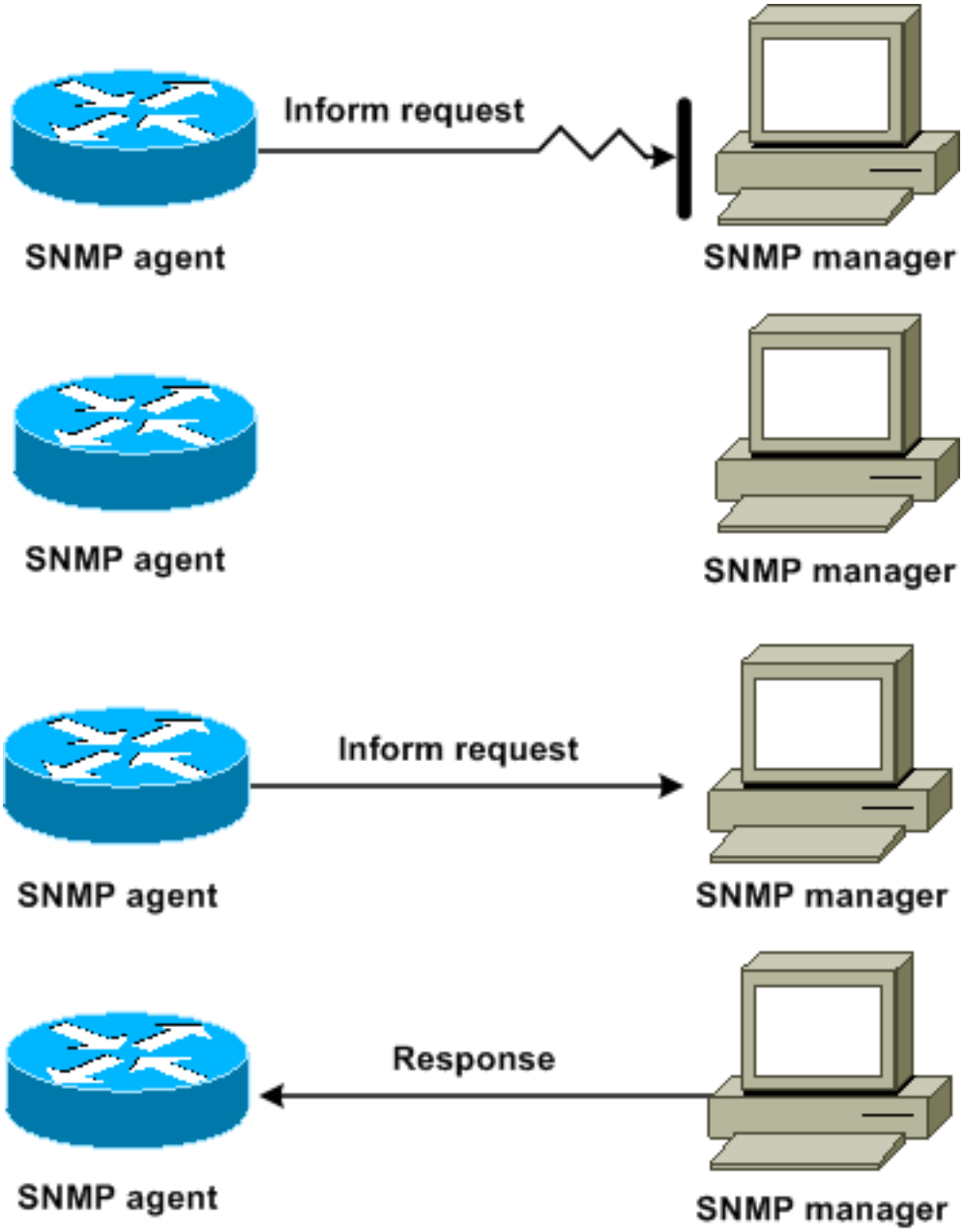
Dieses Diagramm zeigt, wie der Agent-Router erfolgreich ein Trap an den SNMP-Manager sendet. Obwohl der Manager das Trap empfängt, sendet der Manager keine Bestätigung an den Agenten. Der Agent kann nicht wissen, dass die Trap das Ziel erreicht hat.



In diesem Diagramm wird veranschaulicht, wie der Agent-Router erfolgreich eine Informationsanfrage an den Manager sendet. Wenn der Manager die Informationsanfrage erhält, sendet er eine Antwort an den Agenten. Auf diese Weise weiß der Support-Mitarbeiter, dass die Insider-Anfrage das Ziel erreicht hat. Beachten Sie, dass in diesem Beispiel doppelt so viel Datenverkehr vorhanden ist. Der Mitarbeiter weiß jedoch, dass der Manager die Benachrichtigung erhalten hat.



In diesem Diagramm sendet der Agent ein Trap an den Manager, aber das Trap erreicht den Manager nicht. Der Agent kann nicht wissen, dass die Trap nicht das Ziel erreicht hat, und so wird die Trap nicht erneut gesendet. Der Manager erhält nie die Falle.



In diesem Diagramm sendet der Agent eine Insider-Anfrage an den Manager, die Insider-Anfrage wird jedoch nicht an den Manager weitergeleitet. Da der Manager die Instruktionsanfrage nicht erhalten hat, gibt es keine Antwort. Nach einiger Zeit sendet der Support-Mitarbeiter die Anfrage erneut. Beim zweiten Mal erhält der Manager die Informationsanfrage und antwortet mit einer Antwort. In diesem Beispiel gibt es mehr Datenverkehr. Die Benachrichtigung wird jedoch an den SNMP-Manager gesendet.

Referenz zu Cisco MIBs und RFCs

RFC-Dokumente definieren in der Regel MIB-Module. RFC-Dokumente werden der Internet Engineering Task Force (IETF), einem internationalen Normungsgremium, übermittelt. Einzelpersonen oder Gruppen schreiben RFCs für die Internet Society (ISOC) und die Internet Community als Ganzes. Auf der Homepage der Internet Society finden Sie Informationen zum Standardisierungsprozess und zu den Aktivitäten der IETF. Auf der IETF -Startseite können Sie den vollständigen Text aller RFCs, Internet Drafts (I-Ds) und STDs lesen, auf die Cisco Dokumente verweisen.

Die Cisco-Implementierung von SNMP verwendet:

- Die Definitionen der MIB II-Variablen, die RFC 1213 beschreibt
- Die Definitionen von SNMP-Traps, die RFC 1215 beschreibt

Cisco stellt für jedes System eigene private MIB-Erweiterungen bereit. Cisco Enterprise MIBs erfüllen die Richtlinien, die die jeweiligen RFCs beschreiben, sofern die Dokumentation nichts anderes festlegt. Die MIB-Moduldefinitionsdateien und eine Liste der MIBs, die auf jeder Cisco Plattform unterstützt werden, finden Sie auf der Cisco MIB-Startseite.

SNMP-Versionen

Die Cisco IOS-Software unterstützt folgende SNMP-Versionen:

- SNMPv1 - Ein vollständiger Internetstandard, der von RFC 1157 definiert wird. RFC 1157 ersetzt die früheren Versionen, die als RFC 1067 und RFC 1098 veröffentlicht wurden. Sicherheit basiert auf Community-Strings.
- SNMPv2c - SNMPv2c ist das Community String-basierte Administrations-Framework für SNMPv2. SNMPv2c (der c steht für Community) ist ein experimentelles Internetprotokoll, das von RFC 1901 , RFC 1905 und RFC 1906 definiert wird. SNMPv2c ist eine Aktualisierung der Protokollvorgänge und Datentypen von SNMPv2p (SNMPv2 Classic). SNMPv2c verwendet das Community-basierte Sicherheitsmodell von SNMPv1.
- SNMPv3 - SNMPv3 ist ein interoperables, standardbasiertes Protokoll, das von RFC 2273 , RFC 2274 und RFC 2275 definiert wird. SNMPv3 bietet sicheren Zugriff auf Geräte mit einer Kombination aus Authentifizierung und Paketverschlüsselung über das Netzwerk.SNMPv3 bietet folgende Sicherheitsfunktionen:Nachrichtenintegrität - Stellt sicher, dass ein Paket bei der Übertragung nicht manipuliert wurde.Authentication (Authentifizierung): Bestimmt, dass die Nachricht von einer gültigen Quelle stammt.Verschlüsselung - Scrambles der Inhalte eines Pakets, wodurch die Erkennung durch eine nicht autorisierte Quelle verhindert wird.

SNMPv1 und SNMPv2c verwenden eine Community-basierte Form der Sicherheit. Eine IP-Adressen-ACL und ein Kennwort definieren die Community von Managern, die auf die Agent-MIB zugreifen können.

SNMPv2c-Unterstützung umfasst einen Mechanismus zum Sammelabruf und detailliertere Fehlermeldungen, die an Managementstationen gemeldet werden. Der Massenabruf-Mechanismus unterstützt das Abrufen von Tabellen und großen Informationsmengen, wodurch die Anzahl der erforderlichen Rundreisen minimiert wird. Die verbesserte SNMPv2c-Fehlerbehandlungsunterstützung umfasst erweiterte Fehlercodes, die verschiedene Arten von Fehlerzuständen unterscheiden. Diese Bedingungen werden in SNMPv1 durch einen einzigen Fehlercode gemeldet. Fehlerrückgabecodes geben jetzt den Fehlertyp an.

SNMPv3 bietet sowohl Sicherheitsmodelle als auch Sicherheitsstufen. Ein Sicherheitsmodell ist eine Authentifizierungsstrategie, die für einen Benutzer und die Gruppe, in der sich der Benutzer befindet, eingerichtet wird. Eine Sicherheitsstufe ist der zulässige Sicherheitsgrad innerhalb eines Sicherheitsmodells. Die Kombination aus Sicherheitsmodell und Sicherheitsstufe bestimmt, welcher Sicherheitsmechanismus beim Umgang mit einem SNMP-Paket verwendet wird.

Allgemeine SNMP-Konfiguration

Führen Sie diese Befehle auf allen Kundenswitches aus, um die SNMP-Verwaltung zu aktivieren:

- Befehl für SNMP-ACLs:
  ```
  Switch(config)#access-list 98 permit ip_address
  ```

```
!--- This is the SNMP device ACL.
```

- Globale SNMP-Befehle:

```
!--- These are sample SNMP community strings. Switch(config)#snmp-server community RO-
community ro 98
snmp-server community RW-community rw 98
snmp-server contact Glen Rahn (Home Number)
snmp-server location text
```

SNMP-Trap-Empfehlung

SNMP ist die Grundlage für das Netzwerkmanagement und wird in allen Netzwerken aktiviert und verwendet.

Ein SNMP-Agent kann mit mehreren Managern kommunizieren. Aus diesem Grund können Sie die Software so konfigurieren, dass die Kommunikation mit einer Managementkonsole über SNMPv1 und einer anderen Managementstation über SNMPv2 unterstützt wird. Die meisten Kunden und NMSs verwenden weiterhin SNMPv1 und SNMPv2c, da die Unterstützung von SNMPv3-Netzwerkgeräten auf NMS-Plattformen etwas zu gering ist.

Aktivieren Sie SNMP-Traps für alle verwendeten Funktionen. Sie können andere Funktionen deaktivieren, wenn Sie möchten. Nachdem Sie ein Trap aktiviert haben, können Sie den Befehl **test snmp** ausgeben und die entsprechende Behandlung auf dem NMS für den Fehler einrichten. Beispiele für solche Behandlungen sind eine Pager-Warnung oder ein Popup-Fenster.

Alle Traps sind standardmäßig deaktiviert. Aktivieren Sie alle Traps auf Core-Switches, wie im folgenden Beispiel gezeigt:

```
Switch(config)#snmp trap enable
Switch(config)#snmp-server trap-source loopback0
```

Aktivieren Sie außerdem Port-Traps für wichtige Ports, z. B. Infrastrukturverbindungen zu Routern und Switches sowie wichtige Server-Ports. Eine Aktivierung ist für andere Ports, z. B. Host-Ports, nicht erforderlich. Geben Sie diesen Befehl ein, um den Port zu konfigurieren und die Benachrichtigung zum Ein-/Ausschalten der Verbindung zu aktivieren:

```
Switch(config-if)#snmp trap link-status
```

Geben Sie als Nächstes die Geräte an, die die Traps empfangen sollen, und handeln Sie entsprechend auf den Traps. Sie können jetzt jedes Trap-Ziel als SNMPv1-, SNMPv2- oder SNMPv3-Empfänger konfigurieren. Für SNMPv3-Geräte können statt UDP-Traps zuverlässige Informationen gesendet werden. Dies ist die Konfiguration:

```
Switch(config)#snmp-server host ip_address [traps | informs] [version {1 | 2c | 3}] community-
string
!--- This command needs to be on one line. !--- These are sample host destinations for SNMP
traps and informs. snmp-server host 172.16.1.27 version 2c public
snmp-server host 172.16.1.111 version 1 public
snmp-server host 172.16.1.111 informs version 3 public
snmp-server host 172.16.1.33 public
```

SNMP Polling-Empfehlungen

Stellen Sie sicher, dass diese MIBs die wichtigsten MIBs sind, die in Campus-Netzwerken abgefragt oder überwacht werden:

Hinweis: Diese Empfehlung stammt von der Cisco Network Management Consulting Group.

Object Name	Object Description	OID	Period	Max
MIB-II				
SysUpTime	system uptime in 1/100ths of seconds	1.3.6.1.2.1.1.3	5 min	< 30000
CISCO-STACK-MIB				
ChassisPs1status	Status of power supply 1	1.3.6.1.4.1.9.5.1.2.4	10 min	≠ 2
ChassisPs2Status	Status of power supply 2	1.3.6.1.4.1.9.5.1.2.7	10 min	≠ 2
ChassisFanStatus	Status of Chassis Fan	1.3.6.1.4.1.9.5.1.2.9	10 min	≠ 2
ChassisMinorAlarm	Chassis Minor Alarm Status	1.3.6.1.4.1.9.5.1.2.11	10 min	≠ 1
chassis MajorAlarm	Chassis Major Alarm Status	1.3.6.1.4.1.9.5.1.2.12	10 min	≠ 1

Object Name	Object Description	OID	Period	Max
ChassisTempAlarm	Chassis Temperature Alarm status	1.3.6.1.4.1.9.5.1.2.13	10 min	≠ 1
ModuleStatus	Operational Status of the module	1.3.6.1.4.1.9.5.1.3.1.1.10	30 min	≠ 2
CISCO-PROCESS-MIB				
CpmCPUTotal5min	The overall CPU busy percentage in the last 5 minute period. This object deprecates the avgBusy5 object from the OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.5	5 min	
CISCO-STACK-MIB				
SysTraffic	% of bandwidth utilization for the previous polling interval	1.3.6.1.4.1.9.5.1.1.8	30 min	

Object Name	Object Description	OID	Period	Max
SysTrafficPeak	Peak traffic meter value since the last time the port counters were cleared or the system started	1.3.6.1.4.1.9.5.1.1.19	30 min	
BRIDGE-MIB				
CiscoEsStackSwitchBufferOverruns	Number of times the switch was out of buffers	1.3.6.1.4.1.9.5.14.2.1.1.17	30 min	

Netzwerkzeitprotokoll

Zweck

Das Network Time Protocol (NTP), RFC 1305 , synchronisiert die Zeiterfassung für eine Reihe von verteilten Zeitservern und Clients. NTP ermöglicht die Korrelation von Ereignissen bei der Erstellung von Systemprotokollen und wenn andere zeitspezifische Ereignisse auftreten.

Überblick

RFC 958 dokumentierte zunächst NTP. NTP wurde jedoch durch RFC 1119 (NTP-Version 2) weiterentwickelt. RFC 1305 definiert NTP jetzt in der dritten Version.

Das NTP synchronisiert die Zeit eines Computer-Clients oder -Servers mit einem anderen Server oder einer anderen Referenzzeitquelle, z. B. einem Funkmodul, Satellitenempfänger oder Modem. NTP bietet eine Clientgenauigkeit, die in der Regel innerhalb eines ms in LANs und bis zu einigen Dutzend ms in WANs im Vergleich zu einem synchronisierten Primärserver liegt. Beispielsweise können Sie NTP verwenden, um die koordinierte Weltzeit (Coordinated Universal Time, UTC) über einen GPS-Empfänger (Global Positioning Service) zu koordinieren.

Typische NTP-Konfigurationen verwenden mehrere redundante Server und unterschiedliche Netzwerkpfade, um eine hohe Genauigkeit und Zuverlässigkeit zu erreichen. Einige Konfigurationen beinhalten die kryptografische Authentifizierung, um versehentliche oder böswillige Protokoll-Angriffe zu verhindern.

NTP wird über das UDP ausgeführt, das wiederum über IP ausgeführt wird. Alle NTP-Kommunikation verwendet UTC, was der Greenwich Mean Time entspricht.

Derzeit sind Implementierungen für NTP Version 3 (NTPv3) und NTP Version 4 (NTPv4)

verfügbar. Die neueste Softwareversion, an der gearbeitet wird, ist NTPv4, aber der offizielle Internet-Standard ist noch NTPv3. Darüber hinaus passen einige Anbieter von Betriebssystemen die Implementierung des Protokolls an.

NTP-Schutzmechanismen

Die NTP-Implementierung versucht auch, die Synchronisierung mit einem Computer zu vermeiden, auf dem die Uhrzeit möglicherweise nicht genau ist. NTP bietet hierfür zwei Möglichkeiten:

- NTP wird nicht mit einem Computer synchronisiert, der selbst nicht synchronisiert ist.
- NTP vergleicht immer die Zeit, die von mehreren Computern gemeldet wird, und synchronisiert sie nicht mit einem Computer, auf dem die Zeit deutlich anders ist als die anderen, auch wenn dieser Computer eine niedrigere Schicht hat.

Assoziationen

Die Kommunikation zwischen Systemen, auf denen NTP ausgeführt wird, wird in der Regel statisch konfiguriert. Jeder Computer erhält die IP-Adressen aller Computer, mit denen er Verknüpfungen bilden muss. Eine präzise Zeiterfassung ist durch den Austausch von NTP-Nachrichten zwischen den beiden Systemen mit Zuordnung möglich. In einer LAN-Umgebung können Sie NTP jedoch so konfigurieren, dass es IP-Broadcast-Nachrichten verwendet. Mit dieser Alternative können Sie den Computer so konfigurieren, dass Broadcast-Nachrichten gesendet oder empfangen werden. Die Genauigkeit der Zeiterfassung wird jedoch geringfügig reduziert, da der Informationsfluss nur eine Richtung ist.

Wenn das Netzwerk vom Internet isoliert ist, können Sie mit der Cisco NTP-Implementierung einen Computer so konfigurieren, als ob er mit der Verwendung von NTP synchronisiert wäre, obwohl er die Zeit mit der Verwendung anderer Methoden bestimmt hat. Andere Computer synchronisieren mit diesem Computer, wenn NTP verwendet wird.

Eine NTP-Zuordnung kann sein:

- Eine Peer-ZuordnungDies bedeutet, dass dieses System entweder mit dem anderen System synchronisiert werden kann oder dass das andere System mit diesem synchronisiert werden kann.
- Eine ServerzuordnungDas bedeutet, dass nur dieses System mit dem anderen System synchronisiert wird. Das andere System führt keine Synchronisierung mit diesem System durch.

Wenn Sie eine NTP-Zuordnung zu einem anderen System erstellen möchten, verwenden Sie einen der folgenden Befehle im globalen Konfigurationsmodus:

Befehl	Zweck
ntp peer *ip-address* [normal-sync] [*Versionsnummer*] [key *key-id*] [source-*interface*] [ziehen]	Erstellt eine Peer-Zuordnung zu einem anderen System
ntp server *ip-address* [*Versionsnummer*] [Schlüssel-*Schlüssel-ID*] [Quellschnittstelle] [bevorzugen]	Erstellt eine Serverzuordnung mit einem anderen System

Hinweis: Es muss nur ein Ende einer Zuordnung konfiguriert werden. Das andere System stellt automatisch die Assoziation her.

Zugriff auf öffentliche Zeitserver

Das NTP-Subnetz umfasst derzeit mehr als 50 öffentliche Primärserver, die direkt über Funk, Satellit oder Modem mit UTC synchronisiert werden. In der Regel führen Client-Workstations und Server mit einer relativ kleinen Anzahl von Clients keine Synchronisierung mit Primärservern durch. Es gibt etwa 100 öffentliche sekundäre Server, die mit den primären Servern synchronisiert werden. Diese Server ermöglichen die Synchronisierung von insgesamt mehr als 100.000 Clients und Servern im Internet. Die Seite für öffentliche NTP-Server verwaltet die aktuellen Listen und wird regelmäßig aktualisiert.

Außerdem gibt es zahlreiche private primäre und sekundäre Server, die normalerweise nicht für die Öffentlichkeit verfügbar sind. Unter Network Time Protocol Project (University of Delaware) finden Sie eine Liste der öffentlichen NTP-Server und Informationen zur Verwendung dieser Server. Es gibt keine Garantie dafür, dass diese öffentlichen Internet-NTP-Server verfügbar sind und die richtige Zeit liefern. Aus diesem Grund müssen Sie andere Optionen in Betracht ziehen. Verwenden Sie beispielsweise verschiedene eigenständige GPS-Geräte, die direkt mit einer Reihe von Routern verbunden sind.

Eine weitere Option ist die Verwendung verschiedener Router, die als Master für Stratum 1 festgelegt wurden. Die Verwendung eines solchen Routers wird jedoch nicht empfohlen.

Stratum

NTP verwendet eine Schicht, um die Anzahl der NTP-Hops zu beschreiben, die ein System von einer maßgeblichen Zeitquelle entfernt ist. Ein Schicht-1-Zeitserver verfügt über eine Funk- oder Atomuhr, die direkt angeschlossen ist. Ein Schicht-2-Zeitserver erhält seine Zeit von einem Schicht-1-Zeitserver usw. Ein Computer, der NTP ausführt, wählt als Zeitquelle automatisch den Computer mit der niedrigsten Schicht-Nummer aus, mit der er für die Kommunikation über NTP konfiguriert ist. Mit dieser Strategie wird effektiv eine Struktur zur Selbstverwaltung von NTP-Lautsprechern erstellt.

Das NTP vermeidet die Synchronisierung mit einem Gerät, auf dem die Uhrzeit möglicherweise nicht korrekt ist. Weitere Informationen finden Sie im *NTP Safeguards*-Abschnitt des Network Time Protocol.

Server-Peer-Beziehung

- Ein Server reagiert auf Clientanforderungen, versucht jedoch nicht, Datumsinformationen aus einer Clientzeitquelle zu integrieren.
- Ein Peer reagiert auf Kundenanfragen und versucht, die Client-Anfrage als potenziellen Kandidaten für eine bessere Zeitquelle zu nutzen und bei der Stabilisierung der Taktfrequenz zu helfen.
- Um echte Peers zu sein, müssen beide Seiten der Verbindung eine Peer-Beziehung aufbauen und nicht eine Situation, in der ein Benutzer als Peer fungiert und der andere Benutzer als Server dient. Lassen Sie Peers Schlüssel austauschen, sodass nur vertrauenswürdige Hosts mit anderen als Peers sprechen können.
- In einer Clientanforderung an einen Server antwortet der Server dem Client und vergisst, dass der Client eine Frage gestellt hat.
- In einer Clientanforderung an einen Peer antwortet der Server auf den Client. Der Server

speichert Statusinformationen über den Client, um festzustellen, wie gut der Client zur Zeit arbeitet und welcher Schicht-Server der Client ausführt.

Ein NTP-Server kann viele Tausend Clients problemlos verwalten. Wenn ein NTP-Server jedoch mehr als einige wenige Clients (bis zu einige hundert) verarbeitet, wirkt sich dies auf die Speicherkapazität des Servers zur Speicherung von Statusinformationen aus. Wenn ein NTP-Server mehr als die empfohlene Menge verarbeiten muss, werden mehr CPU-Ressourcen und mehr Bandbreite im Gerät verbraucht.

Kommunikationsmodi mit dem NTP-Server

Es gibt zwei verschiedene Modi für die Kommunikation mit dem Server:

- Broadcast-Modus
- Client/Server-Modus

Im Broadcast-Modus hören die Clients zu. Im Client/Server-Modus wird der Server von den Clients abgefragt. Sie können NTP-Broadcast verwenden, wenn aufgrund der Geschwindigkeit keine WAN-Verbindung vorhanden ist. Um über eine WAN-Verbindung zu gehen, verwenden Sie den Client/Server-Modus (durch Abfrage). Der Broadcast-Modus ist für ein LAN konzipiert, in dem viele Clients möglicherweise den Server abfragen müssen. Ohne den Broadcast-Modus können solche Abfragen möglicherweise eine große Anzahl von Paketen im Netzwerk generieren. NTP-Multicast ist in NTPv3 noch nicht verfügbar, aber in NTPv4 verfügbar.

Die Cisco IOS Software kommuniziert standardmäßig mit der Verwendung von NTPv3. Die Software ist jedoch abwärtskompatibel mit früheren NTP-Versionen.

Umfragen

Das NTP-Protokoll ermöglicht es einem Client, jederzeit einen Server abzufragen.

Wenn Sie NTP zum ersten Mal in einer Cisco Box konfigurieren, sendet NTP acht Abfragen in schneller Folge in Intervallen von `NTP_MINPOLL` (2^4=16 Sek.). Das `NTP_MAXPOLL` ist 2^14 Sekunden (16.384 Sek. oder 4 Stunden, 33 Min., 4 Sek.). Dieser Zeitraum ist der längste Zeitraum, bevor NTP erneut eine Antwort abfragt. Derzeit verfügt Cisco nicht über eine Methode, mit der der Benutzer die `POLL`-Zeit manuell erzwingen kann.

Der NTP-Abfragezähler beginnt bei 2^6 (64) Sekunden oder 1 Minute, 4 Sekunden. Diese Zeit wird um die Kräfte von 2 erhöht, wenn die beiden Server sich synchronisieren, auf 2^10. Sie können erwarten, dass die Synchronisierungsmeldungen im Intervall von 64, 128, 256, 512 oder 1024 Sekunden gesendet werden, je nach Server- oder Peer-Konfiguration. Die längere Zeitspanne zwischen den Umfragen tritt auf, wenn die aktuelle Uhr aufgrund der phasensperrenden Schleifen stabiler wird. Die Phasenverriegelungen schneiden den lokalen Uhrkristall bis zu 1024 Sekunden (17 Min.) ab.

Die Zeit variiert zwischen 64 Sekunden und 1024 Sekunden als Leistung von 2 (das entspricht einmal alle 64, 128, 256, 512 oder 1024 Sekunden). Die Zeit basiert auf der Phase-Loop, die Pakete sendet und empfängt. Wenn die Zeit viel Jitter enthält, findet häufiger eine Umfrage statt. Wenn die Referenzuhr korrekt ist und die Netzwerkverbindung konsistent ist, werden die Polling-Zeiten zwischen den einzelnen Umfragen in 1024 Sekunden konvergiert.

Das NTP-Abfrageintervall ändert sich, wenn sich die Verbindung zwischen Client und Server ändert. Mit einer besseren Verbindung ist das Polling-Intervall länger. In diesem Fall bedeutet eine bessere Verbindung, dass der NTP-Client acht Antworten für die letzten acht Anfragen erhalten

hat. Das Abfrageintervall wird dann verdoppelt. Bei einer einmaligen versäumten Antwort wird das Umfrageintervall um die Hälfte reduziert. Das Abfrageintervall beginnt mit 64 Sekunden und erreicht eine maximale Dauer von 1024 Sekunden. Unter den besten Umständen beträgt die Zeit, die erforderlich ist, damit das Umfrageintervall von 64 Sekunden auf 1024 Sekunden verlängert werden kann, etwas mehr als 2 Stunden.

Broadcasts

NTP-Broadcasts werden niemals weitergeleitet. Wenn Sie den Befehl **ntp broadcast** ausführen, beginnt der Router, NTP-Broadcasts auf der Schnittstelle zu generieren, auf der er konfiguriert ist.

In der Regel geben Sie den Befehl **ntp broadcast** aus, um NTP-Broadcasts an ein LAN zu senden, um die Client-Endstationen und -Server zu bedienen.

Zeitsynchronisierung

Die Synchronisierung eines Clients mit einem Server besteht aus mehreren Paketaustauschvorgängen. Jeder Austausch ist ein Anfrage-/Antwortpaar. Wenn ein Client eine Anforderung sendet, speichert der Client seine lokale Zeit im gesendeten Paket. Wenn ein Server das Paket empfängt, speichert er seine eigene Schätzung der aktuellen Uhrzeit im Paket und das Paket wird zurückgegeben. Wenn die Antwort eingeht, protokolliert der Empfänger erneut seine eigene Empfangszeit, um die Reisezeit des Pakets zu schätzen.

Diese Zeitunterschiede können verwendet werden, um die Zeit zu schätzen, die für die Übertragung des Pakets vom Server an den Anforderer erforderlich war. Diese Round-Trip-Zeit wird bei der Schätzung der aktuellen Zeit berücksichtigt. Je kürzer die Round-Trip-Zeit ist, desto genauer ist die Schätzung der aktuellen Zeit.

Die Zeit wird erst akzeptiert, wenn mehrere Vereinbarungen über den Austausch von Paketen getroffen wurden. Einige essenzielle Werte werden in mehrstufige Filter eingesetzt, um die Qualität der Proben zu schätzen. Normalerweise sind etwa 5 Minuten erforderlich, damit ein NTP-Client mit einem Server synchronisiert werden kann. Interessanterweise gilt dies auch für lokale Referenzuhren, die per Definition keine Verzögerung aufweisen.

Darüber hinaus beeinflusst die Qualität der Netzwerkverbindung auch die Endgenauigkeit. Langsame und unvorhersehbare Netzwerke mit unterschiedlichen Verzögerungen haben negative Auswirkungen auf die Zeitsynchronisierung.

Für die Synchronisierung des NTP ist eine Zeitdifferenz von weniger als 128 ms erforderlich. Die Genauigkeit im Internet liegt in der Regel zwischen 5 ms und 100 ms, was bei Netzwerkverzögerungen unterschiedlich sein kann.

NTP-Datenverkehrsstufen

Die Bandbreite, die das NTP nutzt, ist minimal. Das Intervall zwischen den Polling-Nachrichten, die Peers austauschen, wird in der Regel alle 17 Minuten (1024 Sek.) auf maximal eine Nachricht zurückgesetzt. Bei sorgfältiger Planung können Sie dies in Routernetzwerken über die WAN-Verbindungen aufrechterhalten. Lassen Sie die NTP-Clients Peer zu lokalen NTP-Servern und nicht über das WAN zu den Core-Routern am zentralen Standort führen, bei denen es sich um die Stratum 2-Server handelt.

Ein konvergenter NTP-Client verwendet pro Server durchschnittlich etwa 0,6 Bit/s.

Cisco NTP-Empfehlung

- Cisco empfiehlt, mehrere Zeitserver und unterschiedliche Netzwerkpfade einzusetzen, um eine hohe Genauigkeit und Zuverlässigkeit zu erreichen. Einige Konfigurationen beinhalten die kryptografische Authentifizierung, um versehentliche oder böswillige Protokoll-Angriffe zu verhindern.
- Laut RFC ist NTP so konzipiert, dass Sie mehrere verschiedene Zeitserver abfragen und komplizierte statistische Analysen verwenden können, um eine gültige Zeit zu erhalten, selbst wenn Sie nicht sicher sind, ob alle Server, die Sie abfragen, autoritär sind. NTP schätzt die Fehler aller Uhren. Aus diesem Grund geben alle NTP-Server die Zeit zusammen mit einer Schätzung des aktuellen Fehlers zurück. Wenn Sie mehrere Zeitserver verwenden, möchte NTP auch, dass diese Server zu einem bestimmten Zeitpunkt übereinstimmen.
- Die Cisco Implementierung von NTP unterstützt keinen Schicht-1-Service. Sie können keine Verbindung zu einer Funk- oder Atomuhr herstellen. Cisco empfiehlt, den Zeitdienst für Ihr Netzwerk von den öffentlichen NTP-Servern abzuleiten, die im IP-Internet verfügbar sind.
- Ermöglichen Sie allen Client-Switches, regelmäßig Anfragen zur Tageszeit an einen NTP-Server zu senden. Sie können bis zu 10 Server-/Peer-Adressen pro Client konfigurieren, um eine schnelle Synchronisierung zu ermöglichen.
- Um den Protokoll-Overhead zu reduzieren, verteilen die sekundären Server die Zeit über NTP an die verbleibenden lokalen Netzwerk-Hosts. Im Interesse der Zuverlässigkeit können Sie ausgewählte Hosts mit weniger präzisen, aber kostengünstigeren Uhren ausstatten, die bei einem Ausfall des primären und/oder sekundären Servers oder der Kommunikationspfade zwischen diesen Servern als Backup verwendet werden können.
- **ntp update-calendar** - NTP ändert normalerweise nur die Systemuhr. Mit diesem Befehl kann NTP die Datums-/Uhrzeitinformationen im Kalender aktualisieren. Die Aktualisierung wird nur durchgeführt, wenn die NTP-Zeit synchronisiert ist. Andernfalls behält der Kalender seine eigene Zeit und wird nicht von der NTP-Zeit oder Systemuhr beeinflusst. Verwenden Sie dies immer auf den High-End-Routern.
- **clock kalender-valide** - Dieser Befehl erklärt, dass die Kalenderinformationen gültig und synchronisiert sind. Verwenden Sie diese Option auf dem NTP-Master. Wenn dies nicht konfiguriert ist, hält der High-End-Router, der über den Kalender verfügt, seine Zeit selbst dann für nicht autoritär, wenn er über die NTP-Master-Leitung verfügt.
- Jede Schicht-Nummer über 15 gilt als nicht synchronisiert. Aus diesem Grund sehen Sie Stratum 16 in der Ausgabe des Befehls **show ntp status** auf Routern, für die die Uhren nicht synchronisiert sind. Wenn der Master mit einem öffentlichen NTP-Server synchronisiert wird, stellen Sie sicher, dass die Stratumnummer auf der NTP-Master-Leitung eine oder zwei höher ist als die höchste Schicht-Nummer auf den öffentlichen Servern, die Sie abfragen.
- Viele Kunden haben NTP auf ihren Cisco IOS Software-Plattformen im Servermodus konfiguriert, der von mehreren zuverlässigen Feeds aus dem Internet oder einer Funkuhr synchronisiert wird. Eine einfachere Alternative zum Servermodus, wenn Sie eine große Anzahl von Switches betreiben, ist die Aktivierung von NTP im Broadcast-Modus im Management-VLAN in einer Switch-Domäne. Dieser Mechanismus ermöglicht es dem Catalyst, eine Uhr aus einzelnen Broadcast-Nachrichten zu empfangen. Die Genauigkeit der Zeiterfassung wird jedoch geringfügig reduziert, da der Informationsfluss in eine Richtung verläuft.
- Die Verwendung von Loopback-Adressen als Quelle für Updates kann ebenfalls zu Konsistenz beitragen. Sicherheitsbedenken lassen sich auf zwei Arten ausräumen:Cisco empfiehlt, Server-Updates unter Kontrolle zu halten.Durch Authentifizierung

Globale NTP-Konfigurationsbefehle

```
!--- For the client: clock timezone EST  -5  ????
ntp source loopback 0 ?????
ntp server ip_address key 1
ntp peer ip_address
!--- This is for a peer association. ntp authenticate
ntp authentication-key 1 md5 xxxx
ntp trusted-key 1

!--- For the server: clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ntp source loopback0
ntp update-calendar

!--- This is optional: interface vlan_id ntp broadcast
!--- This sends NTP broadcast packets. ntp broadcast client
!--- This receives NTP broadcast packets. ntp authenticate
ntp authentication-key 1 md5 xxxxx
ntp trusted-key 1
ntp access-group access-list
!--- This provides further security, if needed.
```

NTP-Statusbefehl

```
show ntp status

Clock is synchronized, stratum 8, reference is 127.127.7.1
nominal freq is 250.0000 Hz, actual freq is 249.9974 Hz, precision is 2**18
reference time is C6CF0C30.980CCA9D (01:34:00.593 IST Mon Sep 12 2005)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec
```

Dies ist die Referenztaktadresse für den Cisco Router, wenn der Router als NTP-Master fungiert. Wenn der Router nicht mit einem NTP-Server synchronisiert wurde, verwendet der Router diese Adresse als Referenz-ID. Weitere Informationen zur Konfiguration und zu den Befehlen finden Sie im Abschnitt *Konfigurieren* von *NTP* im Abschnitt Durchführen grundlegender Systemverwaltung.

Cisco Discovery Protocol

Zweck

CDP wird auf allen Cisco Routern, Bridges, Zugriffsservern und Switches über Layer 2 (Sicherungsschicht) ausgeführt. CDP ermöglicht Netzwerkmanagementanwendungen die Erkennung von Cisco Geräten, die Nachbarn bereits bekannter Geräte sind. Insbesondere Netzwerkmanagementanwendungen können Nachbarn erkennen, die transparente Protokolle der unteren Ebene ausführen. Mit CDP können Netzwerkverwaltungsanwendungen den Gerätetyp und die SNMP-Agentadresse benachbarter Geräte ermitteln. Mit dieser Funktion können Anwendungen SNMP-Abfragen an benachbarte Geräte senden.

Mit den **show**-Befehlen, die der CDP-Funktion zugeordnet sind, kann der Netzwerktechniker folgende Informationen ermitteln:

- Die Modul-/Portnummer anderer benachbarter CDP-fähiger Geräte

- Diese Adressen des benachbarten Geräts:MAC-AdresseIP-AdressePort-Channel-Adresse
- Die benachbarte Gerätesoftware-Version
- Diese Informationen zum benachbarten Gerät:GeschwindigkeitDuplexVTP-DomäneNative VLAN-Einstellung

Im Abschnitt Betriebsübersicht werden einige der Verbesserungen von CDP Version 2 (CDPv2) gegenüber CDP Version 1 (CDPv1) beschrieben.

Überblick

CDP wird auf allen LAN- und WAN-Medien ausgeführt, die SNAP unterstützen.

Jedes CDP-konfigurierte Gerät sendet regelmäßig Nachrichten an eine Multicast-Adresse. Jedes Gerät gibt mindestens eine Adresse an, an die das Gerät SNMP-Meldungen empfangen kann. Die Anzeigen enthalten auch die Zeit bis zur Veröffentlichung bzw. zum Halten von Daten. Diese Informationen geben an, wie lange ein empfangendes Gerät CDP-Informationen speichern muss, bevor diese verworfen werden.

CDP verwendet SNAP-Kapselung mit dem Typcode 2000. Auf Ethernet, ATM und FDDI wird die Ziel-Multicast-Adresse 01-00-0c-cc-cc-cc verwendet. Auf Token Rings wird die funktionale Adresse c000.0800.000 verwendet. CDP-Frames werden jede Minute regelmäßig gesendet.

CDP-Nachrichten enthalten eine oder mehrere Nachrichten, mit denen das Zielgerät Informationen über jedes benachbarte Gerät sammeln und speichern kann.

Diese Tabelle enthält die Parameter, die CDPv1 unterstützt:

Parameter	Typ	Beschreibung
1	Geräte-ID	Hostname des Geräts oder Seriennummer der Hardware in ASCII
2	Adresse	Die Layer-3-Adresse der Schnittstelle, die das Update sendet
1	Port-ID	Der Port, an den das CDP-Update gesendet wird
4	Funktionen	Beschreibt die Funktionsmerkmale des Geräts wie folgt: • Router: 0 x 01 • SR[1] Bridge: 0 x 04 • Switch: 0x08 (bietet Layer-2- und/oder Layer-3-Switching) • Host: 0 x 10 • IGMP-bedingte Filterung: 0 x 20 • Die Bridge oder der Switch leitet IGMP-Berichtspakete nicht an Router-Ports weiter.
5	Version	Eine Zeichenfolge, die die Softwareversion enthält.

		Hinweis: Die Ausgabe des Befehls **show version** enthält dieselben Informationen.
6	Plattform	Die Hardwareplattform, z. B. WS-C5000, WS-C6009 und Cisco RSP[2]

[1] SR = source-route

[2] RSP = Route Switch Processor.

In CDPv2 wurden zusätzliche Typen, Längen und Werte (TLVs) eingeführt. CDPv2 unterstützt alle TLVs. Diese Tabelle enthält jedoch die Parameter, die besonders in Umgebungen mit Switches nützlich sein können und die von der Catalyst-Software verwendet werden.

Wenn ein Switch CDPv1 ausführt, verwirft der Switch CDPv2-Frames. Wenn ein Switch CDPv2 ausführt und einen CDPv1-Frame auf einer Schnittstelle empfängt, sendet der Switch neben CDPv2-Frames auch CDPv1-Frames aus dieser Schnittstelle.

Parameter	Typ	Beschreibung
9	VTP-Domäne	Die VTP-Domäne, falls sie auf dem Gerät konfiguriert ist
10	Natives VLAN	In dot1q bleiben die Frames für das VLAN, in dem sich der Port befindet, wenn der Port nicht Trunking ist, nicht markiert. Dies wird in der Regel als natives VLAN bezeichnet.
11	Vollduplex/ Halbduplex	Diese TLV enthält die Duplexeinstellung des sendenden Ports.
14	Appliance-VLAN-ID	Ermöglicht die Differenzierung des VoIP-Datenverkehrs von anderem Datenverkehr über eine separate VLAN-ID (zusätzliches VLAN).
16	Stromverbrauch	Die maximale Strommenge, die das angeschlossene Gerät in mW voraussichtlich verbrauchen wird.
17	MTU	Die MTU der Schnittstelle, über die der CDP-Frame übertragen wird.
18	Erweiterte Vertrauenswürdigkeit	Gibt an, dass sich der Port im Modus "Extended Trust" befindet.
19	COS für nicht vertrauenswürdige Ports	Der Class of Service (CoS)-Wert, der verwendet wird, um alle Pakete zu kennzeichnen, die auf dem nicht vertrauenswürdigen Port eines angeschlossenen Switching-Geräts empfangen werden.
20	SysName	Vollqualifizierter Domänenname des

		Geräts (0, wenn unbekannt).
25	Stromversorgung angefordert	Übertragung über ein stromfähiges Gerät zur Aushandlung eines geeigneten Leistungsniveaus.
26	Stromversorgung verfügbar	Von einem Switch übertragen. Ermöglicht einem netzfähigen Gerät die Aushandlung und Auswahl einer geeigneten Energieeinstellung.

CDPv2/Power over Ethernet

Einige Switches, wie der Catalyst 6500/6000 und 4500/4000, können über UTP-Kabel (Unshielded Twisted Pair) mit Strom versorgt werden. Die über CDP empfangenen Informationen (Parameter 16, 25, 26) helfen bei der Optimierung der Stromverwaltung des Switches.

CDPv2/Cisco IP-Telefon-Interaktion

Cisco IP-Telefone bieten Konnektivität für ein extern angeschlossenes 10/100-Mbit/s-Ethernet-Gerät. Diese Anbindung wird durch die Integration eines internen Layer-2-Switches mit drei Ports in das IP-Telefon erreicht. Die internen Switch-Ports werden wie folgt bezeichnet:

- P0 (internes IP-Telefon-Gerät)
- P1 (externer 10/100-Mbit/s-Port)
- P2 (externer 10/100-Mbit/s-Port, der mit dem Switch verbunden ist)

Sie können Sprachdatenverkehr in einem separaten VLAN am Switch-Port übertragen, wenn Sie die Trunk-Ports für den dot1q-Zugriff konfigurieren. Dieses zusätzliche VLAN wird als zusätzliches (CatOS) oder Sprach-VLAN (Cisco IOS Software) bezeichnet. Der mit dot1q gekennzeichnete Datenverkehr vom IP-Telefon kann daher über das Hilfs-/Sprach-VLAN gesendet werden, und nicht markierter Datenverkehr kann über den externen 10/100-Mbit/s-Port des Telefons über das Zugriffs-VLAN gesendet werden.

Catalyst Switches können ein IP-Telefon über CDP über die Sprach-VLAN-ID informieren (Parameter-14: Appliance VLAN-ID TLV). Daher kennzeichnet das IP-Telefon alle VoIP-bezogenen Pakete mit der entsprechenden VLAN-ID und 802.1p-Priorität. Mit dieser CDP-TLV wird auch ermittelt, ob ein IP-Telefon über den Parameter "Appliance ID" (Geräte-ID) verbunden ist.

Dieses Konzept kann bei der Entwicklung einer QoS-Richtlinie genutzt werden. Sie können den Catalyst Switch für die Interaktion mit dem IP-Telefon auf drei Arten konfigurieren:

- Vertrauenswürdige Cisco IP-TelefoneCoS nur dann bedingt vertrauen, wenn ein IP-Telefon über CDP erkannt wird. Wenn ein IP-Telefon über den CDP-Parameter-14 erkannt wird, wird der Port-Vertrauensstatus auf Trust COS festgelegt. Wenn kein IP-Telefon erkannt wird, ist der Port nicht vertrauenswürdig.
- Erweiterte VertrauenswürdigkeitDer Switch kann das IP-Telefon über CDP (Parameter-18) darüber informieren, dass alle Frames vertrauenswürdig sind, die über seinen externen 10/100-Mbit/s-Geräteport empfangen werden.
- Umschreiben von COS für nicht vertrauenswürdige PortsDer Switch kann das IP-Telefon über CDP (Parameter-19) informieren, um die 802.1p-CoS-Werte, die an seinem externen 10/100-Mbit/s-Geräteport empfangen werden, umzuschreiben.**Hinweis:** Standardmäßig ist der

gesamte Datenverkehr, der auf den externen 10/100-Mbit/s-Ports des IP-Telefons empfangen wird, nicht vertrauenswürdig.

Hinweis: Dies ist eine Beispielkonfiguration für die Verbindung des IP-Telefons eines Drittanbieters mit einem Switch.

Hinweis: Beispiel:

```
Switch(config)#interface gigabitEthernet 2/1
Switch(config-if)#switchport mode trunk

!--- For example use VLAN 30 for voice VLAN, and VLAN 10 for access VLAN. Switch(config-
if)#switchport trunk native vlan 10
Switch(config-if)#switchport trunk allow vlan 10,30
Switch(config-if)#switchport voice vlan 30
Switch(config-if)#spanning-tree portfast trunk

!--- And besides that enable LLDP as Non Cisco IP Phone do not use CDP. Switch(config)#lldp run
```

Cisco Konfigurationsempfehlung

Die von CDP bereitgestellten Informationen können bei der Behebung von Layer-2-Verbindungsproblemen äußerst hilfreich sein. Aktivieren Sie CDP auf allen Geräten, die den Betrieb unterstützen. Geben Sie folgende Befehle ein:

- So aktivieren Sie CDP global auf dem Switch:
  ```
  Switch(config)#cdp run
  ```

- So aktivieren Sie CDP auf Port-Basis:
  ```
  Switch(config)#interface type slot#/port#
  Switch(config-if)#cdp enable
  ```

Konfigurations-Checkliste

Globale Befehle

Melden Sie sich an, aktivieren Sie den globalen Konfigurationsmodus, und wechseln Sie in den globalen Konfigurationsmodus, um mit dem Konfigurationsprozess des Switches zu beginnen.

```
Switch>enable
Switch#
Switch#configure terminal
Switch(Config)#
```

Allgemeine globale Befehle (unternehmensweit)

In diesem Abschnitt Global Commands sind die globalen Befehle aufgelistet, die auf alle Switches im Kundennetzwerk angewendet werden.

Diese Konfiguration enthält die empfohlenen globalen Befehle, die der Erstkonfiguration hinzugefügt werden sollen. Sie müssen die Werte in der Ausgabe ändern, bevor Sie den Text

kopieren und in die CLI einfügen. Führen Sie die folgenden Befehle aus, um die globale Konfiguration anzuwenden:

```
vtp domain domain_name
vtp mode transparent
spanning-tree portfast bpduguard
spanning-tree etherchannel guard misconfig
cdp run
no service pad
service password-encryption
enable secret password
clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ip subnet-zero
ip host tftpserver your_tftp_server
ip domain-name domain_name
ip name-server name_server_ip_address
ip name-server name_server_ip_address
ip classless
no ip domain-lookup
no ip http server
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging syslog_server_ip_address
logging syslog_server_ip_address
logging source-interface loopback0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
access-list 98 permit host_ip_address_of_primary_snmp_server
access-list 98 permit host_ip_address_of_secondary_snmp_server
snmp-server community public ro 98
snmp-server community laneng rw 98
snmp-server enable traps entity
snmp-server host host_address traps public
snmp-server host host_address traps public
banner motd ^CCCCC

This is a proprietary system, NOT for public or personal use.  All work products,
communications, files, data or information directly or indirectly created, input
or accessed on this system are and shall become the sole property of the company.
This system is actively monitored and accessed by the company.  By logging onto
this system, the user consents to such monitoring and access.

USE OF THIS SYSTEM WITHOUT OR IN EXCESS OF THE PROPER AUTHORIZATION MAY SUBJECT
THE USER TO DISCIPLINE AND/OR CIVIL AND CRIMINAL PENALTIES

^C
line console 0
exec-timeout 0 0
password cisco
login
transport input none
line vty 0 4
exec-timeout 0 0
password cisco
login
length 25
```

```
clock calendar-valid
ntp server ntp_server_ip_address
ntp server ntp_server_ip_address
ntp update-calendar
```

Globale Befehle, die für jedes Switch-Chassis spezifisch sind

Die globalen Befehle in diesem Abschnitt beziehen sich auf jedes Switch-Chassis, das im Netzwerk installiert ist.

Chassis-spezifische Konfigurationsvariablen

Geben Sie den folgenden Befehl ein, um Datum und Uhrzeit festzulegen:

```
Switch#clock set hh:mm:ss day month year
```

Führen Sie folgende Befehle aus, um den Geräte-Hostnamen festzulegen:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Cat6500
```

Führen Sie folgende Befehle aus, um die Loopback-Schnittstelle für die Verwaltung zu konfigurieren:

```
CbrCat6500(config)#interface loopback 0
Cat6500(config-if)#description Cat6000 - Loopback address and Router ID
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#exit
```

Führen Sie folgende Befehle aus, um die Cisco IOS Software-Version der Supervisor Engine anzuzeigen:

```
Cbrcat6500#show version | include IOS
IOS (tm) MSFC Software (C6MSFC-DSV-M), Version 12.1(13)E9, EARLY DEPLOYMENT RELE
ASE SOFTWARE (fc1)
cat6500#
```

Führen Sie folgenden Befehl aus, um die Version der MSFC-Startdatei anzuzeigen:

```
Cat6500#dir bootflash:
Directory of bootflash:/
 1 -rw- 1879040 Aug 19 2003 19:03:29 c6msfc-boot-mz.121-19.E1a

15990784 bytes total (14111616 bytes free
```

Geben Sie die folgenden Befehle ein, um die Kontaktinformationen und den Speicherort des SNMP-Servers anzugeben:

```
Cat6500(config)#snmp-server contact contact_information
```

```
Cat6500(config)#snmp-server location location_of_device
```

Um die Startkonfiguration von einer vorhandenen Supervisor Engine auf eine neue Supervisor Engine zu kopieren, kann es zu Konfigurationsverlusten kommen, z. B. bei der Konfiguration der Schnittstellen des vorhandenen Supervisors. Cisco empfiehlt, die Konfiguration in eine Textdatei zu kopieren und in Segmente in die Konsole einzufügen, um festzustellen, ob Konfigurationsprobleme auftreten.

Schnittstellenbefehle

Cisco Funktionelle Port-Typen

Switch-Ports in der Cisco IOS Software werden als Schnittstellen bezeichnet. In der Cisco IOS Software gibt es zwei Arten von Schnittstellenmodi:

- Layer-3-geroutete Schnittstelle
- Layer-2-Switch-Schnittstelle

Die Schnittstellenfunktion bezieht sich auf die Konfiguration des Ports. Die Portkonfiguration kann folgendermaßen lauten:

- Geroutete Schnittstelle
- Switched Virtual Interface (SVI)
- Zugriffsport
- Trunk
- EtherChannel
- Eine Kombination dieser

Schnittstellentyp bezieht sich auf einen Port-Typ. Der Port-Typ kann sein:

- FE
- GE
- Port-Channel

Diese Liste beschreibt kurz die verschiedenen Funktionen der Cisco IOS Software-Benutzeroberfläche:

- Geroutete physische Schnittstelle (Standard) - Jede Schnittstelle am Switch ist standardmäßig eine geroutete Layer-3-Schnittstelle, die mit jedem Cisco Router vergleichbar ist. Die geroutete Schnittstelle muss auf ein eindeutiges IP-Subnetz fallen.
- Access Switch Port Interface (Schnittstelle für Access-Switch-Port): Diese Funktion wird verwendet, um Schnittstellen im gleichen VLAN zu platzieren. Ports müssen von einer gerouteten Schnittstelle in eine geswitchte Schnittstelle umgewandelt werden.
- SVI - Eine SVI kann einem VLAN zugeordnet werden, das Access Switch-Ports für Inter-VLAN-Routing enthält. Konfigurieren Sie die SVI so, dass sie einem VLAN zugeordnet wird, wenn Sie eine Route oder Bridge zwischen Access Switch-Ports in verschiedenen VLANs wünschen.
- Trunk Switch Port Interface (Schnittstelle für Trunk-Switch-Ports) - Diese Funktion wird verwendet, um mehrere VLANs auf ein anderes Gerät zu übertragen. Ports müssen von einer gerouteten Schnittstelle in einen Trunk-Switch-Port umgewandelt werden.
- EtherChannel - Ein EtherChannel wird verwendet, um einzelne Ports für Redundanz und Lastenausgleich in einem einzigen logischen Port zu bündeln.

Empfehlungen zu Funktionstypen von Cisco

Mithilfe der Informationen in diesem Abschnitt können Sie die Parameter festlegen, die auf die Schnittstellen angewendet werden sollen.

Hinweis: Einige schnittstellenspezifische Befehle werden nach Möglichkeit integriert.

Autonegotiation

Verwenden Sie keine automatische Verhandlung in einer der folgenden Situationen:

- Für Ports, die Netzwerkinfrastrukturgeräte wie Switches und Router unterstützen
- Für andere nicht transiente Endsysteme wie Server und Drucker

Konfigurieren Sie diese 10/100-Mbit/s-Verbindungskonfigurationen manuell für Geschwindigkeit und Duplex. Die Konfigurationen sind in der Regel 100-Mbit/s-Vollduplex:

- 100 MB Link Switch-to-Switch
- 100 MB Link Switch-to-Server
- 100 MB Link Switch-to-Router

Sie können diese Einstellungen folgendermaßen konfigurieren:

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed 100
Cat6500(config-if)#duplex full
```

Cisco empfiehlt Verbindungskonfigurationen mit 10/100 Mbit/s für Endbenutzer. Mobile Mitarbeiter und transiente Hosts müssen automatisch verhandelt werden, wie das folgende Beispiel zeigt:

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed auto
```

Der Standardwert für Gigabit-Schnittstellen ist `automatische Aushandlung`. Stellen Sie jedoch diese Befehle aus, um sicherzustellen, dass die Autonegotiation aktiviert ist. Cisco empfiehlt die Aktivierung der Gigabit-Aushandlung:

```
Cat6500(config-if)#interface gigabitethernet mod#/port#
Cat6500(config-if)#no speed
```

Spanning Tree Root

Identifizieren Sie unter Berücksichtigung des Netzwerkdesigns den Switch, der am besten als Root für jedes VLAN geeignet ist. Wählen Sie im Allgemeinen einen leistungsstarken Switch in der Mitte des Netzwerks aus. Stellen Sie die Root Bridge in die Mitte des Netzwerks ein, und verbinden Sie die Root Bridge direkt mit den Servern und Routern. Diese Konfiguration reduziert in der Regel die durchschnittliche Entfernung zwischen den Clients und den Servern und Routern. Weitere Informationen finden Sie unter Spanning Tree Protocol-Probleme und zugehörige Entwurfsüberlegungen.

Führen Sie folgenden Befehl aus, um zu erzwingen, dass ein Switch der Root für ein designiertes VLAN ist:

```
Cat6500(config)#spanning-tree vlan vlan_id root primary
```

Spanning Tree PortFast

PortFast umgeht den normalen Spanning Tree-Betrieb an Access-Ports, um die anfänglichen Verbindungsverzögerungen zu beschleunigen, die beim Anschluss von Endstationen an einen Switch auftreten. Weitere Informationen zu PortFast finden Sie unter Verwenden von PortFast und anderen Befehlen zum Beheben von Workstation-Startverbindungsverzögerungen.

Legen Sie STP PortFast für alle aktivierten Zugriffsports, die mit einem einzigen Host verbunden sind, auf "on" fest. Dies ist ein Beispiel:

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on FastEthernet3/1 but will only have effect
when the interface is in a non-trunking mode.
```

UDLD

Aktivieren Sie UDLD nur auf mit Glasfaserverbindungen verbundenen Infrastruktur-Ports oder Kupfer-Ethernet-Kabeln, um die physische Konfiguration der Kabel zu überwachen. Führen Sie die folgenden Befehle aus, um UDLD zu aktivieren:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#udld enable
```

Informationen zur VLAN-Konfiguration

Konfigurieren Sie VLANs mithilfe der folgenden Befehle:

```
Cat6500(config)#vlan vlan_number
Cat6500(config-vlan)#name vlan_name
Cat6500(config-vlan)#exit
Cat6500(config)#spanning-tree vlan vlan_id
Cat6500(config)#default spanning-tree vlan vlan_id
```

Wiederholen Sie die Befehle für jedes VLAN, und beenden Sie das Programm. Geben Sie den folgenden Befehl ein:

```
Cat6500(config)#exit
```

Geben Sie diesen Befehl ein, um alle VLANs zu überprüfen:

```
Cat6500#show vlan
```

Geroutete SVIs

Konfigurieren der SVIs für Inter-VLAN-Routing Geben Sie folgende Befehle ein:

```
Cat6500(config)#interface vlan vlan_id
Cat6500(config-if)#ip address svi_ip_address subnet_mask
Cat6500(config-if)#description interface_description
Cat6500(config-if)#no shutdown
```

Wiederholen Sie diese Befehle für jede Schnittstellenfunktion, die eine geroutete SVI enthält, und schließen Sie dann das Dialogfeld. Geben Sie den folgenden Befehl ein:

```
Cat6500(config-if)#^Z
```

Geroutete zentrale physische Schnittstelle

Führen Sie die folgenden Befehle aus, um die standardmäßig geroutete Layer-3-Schnittstelle zu konfigurieren:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#description interface_description
```

Wiederholen Sie diese Befehle für jede Schnittstellenfunktion, die eine geroutete physische Schnittstelle enthält, und schließen Sie dann das Dialogfeld. Geben Sie den folgenden Befehl ein:

```
Cat6500(config-if)#^Z
```

Gerouteter EtherChannel (L3)

Führen Sie die Befehle in diesem Abschnitt aus, um den EtherChannel auf Layer-3-Schnittstellen zu konfigurieren.

Konfigurieren Sie auf diese Weise eine logische Port-Channel-Schnittstelle:

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#description port_channel_description
Cat6500(config-if)#ip address port_channel_ip_address subnet_mask
Cat6500(config-if)#no shutdown
```

Führen Sie die Schritte in diesem Abschnitt für die Ports aus, die diesen bestimmten Kanal bilden. Wenden Sie die verbleibenden Informationen auf den Port-Channel an, wie in diesem Beispiel gezeigt:

```
Cat6500(config)#interface range [type] mod/port_range
```

```
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#^Z
```

Hinweis: Nachdem Sie einen EtherChannel konfiguriert haben, wirkt sich die Konfiguration, die Sie auf die Port-Channel-Schnittstelle anwenden, auf den EtherChannel aus. Die Konfiguration, die Sie auf die LAN-Ports anwenden, wirkt sich nur auf den LAN-Port aus, auf den die Konfiguration angewendet wird.

EtherChannel (L2) mit Trunking

Konfigurieren Sie den Layer-2-EtherChannel für das Trunking wie folgt:

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport encapsulation encapsulation_type
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Führen Sie die Schritte in diesem Abschnitt nur für die Ports aus, die diesen bestimmten Kanal bilden.

```
Cat6500(config)#interface range [type] mod/port_range
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Hinweis: Nachdem Sie einen EtherChannel konfiguriert haben, wirkt sich die Konfiguration, die Sie auf die Port-Channel-Schnittstelle anwenden, auf den EtherChannel aus. Die Konfiguration, die Sie auf die LAN-Ports anwenden, wirkt sich nur auf den LAN-Port aus, auf den die Konfiguration angewendet wird.

Überprüfen Sie die Erstellung aller EtherChannels und Trunks. Dies ist ein Beispiel:

```
Cat6500#show etherchannel summary
Cat6500#show interface trunk
```

Access-Ports

Wenn es sich bei der Schnittstellenfunktion um einen Zugriffsport handelt, der als eine einzige Schnittstelle konfiguriert ist, führen Sie die folgenden Befehle aus:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport mode access
Cat6500(config-if)#switchport access vlan vlan_id
Cat6500(config-if)#exit
```

Wiederholen Sie diese Befehle für jede Schnittstelle, die als Layer-2-Switch-Port konfiguriert werden muss.

Wenn der Switch-Port mit Endstationen verbunden werden soll, führen Sie den folgenden Befehl aus:

```
Cat6500(config-if)#spanning-tree portfast
```

Trunk-Port (eine physische Schnittstelle)

Wenn es sich bei der Schnittstellenfunktion um einen Trunk-Port handelt, der als eine einzige Schnittstelle konfiguriert ist, führen Sie die folgenden Befehle aus:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport trunk encapsulation dot1q
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Wiederholen Sie diese Befehle für jede Schnittstellenfunktion, die als Trunk-Port konfiguriert werden muss.

Kennwortinformationen

Geben Sie folgende Befehle für Kennwortinformationen ein:

```
Cat6500(config)#service password-encryption
Cat6500(config)#enable secret password

CbrCat6500(config)#line con 0
Cat6500(config-line)#password password

CbrCat6500(config-line)#line vty 0 4
Cat6500(config-line)#password password
Cat6500(config-line)#^Z
```

Speichern der Konfiguration

Geben Sie den folgenden Befehl ein, um die Konfiguration zu speichern:

```
Cat6500#copy running-config startup-config
```

Neue Softwarefunktionen in Cisco IOS Software, Version 12.1(13)E

Weitere Informationen zur Unterstützung von IP-Telefonen finden Sie unter Konfigurieren des Cisco IP-Telefon-Supports.

Weitere Informationen zur Network-Based Application Recognition (NBAR) für LAN-Ports finden Sie unter Network-Based Application Recognition und Distributed Network-Based Application Recognition (NBAR).

Hinweise:

- NBAR für LAN-Ports wird in der MSFC2-Software unterstützt.
- PFC2 bietet Hardwareunterstützung für Eingabe-ACLs an LAN-Ports, an denen Sie NBAR konfigurieren.
- Wenn PFC QoS aktiviert ist, durchläuft der Datenverkehr über LAN-Ports, für die Sie NBAR konfigurieren, die Eingangs- und Ausgangswarteschlangen und die Drop-Schwellenwerte.
- Wenn PFC QoS aktiviert ist, legt MSFC2 die CoS (Egress Class of Service) auf die gleiche Ausgangs-IP-Rangfolge fest.
- Nachdem der Datenverkehr eine Eingangswarteschlange passiert hat, wird der gesamte Datenverkehr in Software auf den MSFC2 an LAN-Ports verarbeitet, auf denen Sie NBAR konfigurieren.
- Distributed NBAR ist auf FlexWAN-Schnittstellen mit der Cisco IOS Software, Version 12.1(6)E und höher, verfügbar.

Verbesserungen beim NetFlow Data Export (NDE):

- Zielquell- und Vollschnittstellen-Flussmasken
- NDE Version 5 von PFC2
- Sampled NetFlow
- Eine Option zum Ausfüllen dieser zusätzlichen Felder in NDE-Datensätzen:IP-Adresse des nächsten Hop-RoutersSNMP ifIndex für die EingangsschnittstelleSNMP ifIndex für die AusgangsschnittstelleQuellcode des autonomen Systems

Weitere Informationen zu diesen Erweiterungen finden Sie unter Konfigurieren von NDE.

Weitere Funktionsverbesserungen:

- Konfigurieren von UDLD
- Konfigurieren von VTP
- Konfigurieren von Webcache-Diensten mit WCCP

Diese Befehle sind neue Befehle:

- **Minimale Neubelastung bei Standby-Verzögerung**
- **Link auflösen**
- **VLAN-interne Zuweisungsrichtlinie {aufsteigend | absteigend}**
- **System-Jumbombe**
- **Clear Catalyst6000 - Datenverkehrsmeter**

Diese Befehle sind erweiterte Befehle:

- **show vlan internal Usage**: Dieser Befehl wurde um VLANs erweitert, die von WAN-Schnittstellen verwendet werden.
- **show vlan id**: Dieser Befehl wurde erweitert, um den Eintrag einer Reihe von VLANs zu unterstützen.
- **show l2protocol-tunnel**: Dieser Befehl wurde erweitert, um die Eingabe einer VLAN-ID zu unterstützen.

Die Cisco IOS Software-Version 12.1(13)E unterstützt diese Softwarefunktionen, die zuvor von den Cisco IOS Software-Versionen 12.1 EX unterstützt wurden:

- Konfiguration von Layer-2-EtherChannels mit Schnittstellen auf verschiedenen Switching-

Modulen, die mit DFC ausgestattet sindLesen Sie den Abschnitt Behoben von allgemeinen Bedenken in Version 12.1(13)E der Cisco Bug-ID CSCdt27074 (nur registrierte Kunden) .
- Route Processor Redundancy Plus (RPR+)-RedundanzWeitere Informationen finden Sie unter Konfigurieren der RPR- oder RPR+ Supervisor Engine-Redundanz.**Hinweis:** In der Cisco IOS Softwareversion 12.1(13)E und höher ersetzen die RPR- und RPR+-Redundanzfunktionen die erweiterte EHSA-Redundanz (High System Availability).
- 4.096 Layer-2-VLANsWeitere Informationen finden Sie unter Konfigurieren von VLANs.**Hinweis:** Cisco IOS Software Release 12.1(13)E und spätere Versionen unterstützen die Konfiguration von 4.096 Layer-3-VLAN-Schnittstellen. Konfigurieren Sie insgesamt maximal 2.000 Layer-3-VLAN-Schnittstellen und Layer-3-Ports auf einer MSFC2-Plattform entweder mit einer Supervisor Engine II oder einer Supervisor Engine I. Konfigurieren Sie insgesamt maximal 1.000 Layer-3-VLAN-Schnittstellen und Layer-3-Ports auf einer MSFC.
- IEEE 802.1Q-TunnelingWeitere Informationen finden Sie unter Konfigurieren von IEEE 802.1Q Tunneling und Layer 2 Protocol Tunneling.
- IEEE 802.1Q Protokoll-TunnelingWeitere Informationen finden Sie unter Konfigurieren von IEEE 802.1Q Tunneling und Layer 2 Protocol Tunneling.
- IEEE 802.1s Multiple Spanning Tree (MST)Weitere Informationen finden Sie unter Konfigurieren von STP und IEEE 802.1s MST.
- IEEE 802.1w Rapid STP (RSTP)Weitere Informationen finden Sie unter Konfigurieren von STP und IEEE 802.1s MST.
- IEEE 802.3ad LACPWeitere Informationen finden Sie unter Konfigurieren von Layer 3 und Layer 2-EtherChannel.
- PortFast BPDU-FilterungWeitere Informationen finden Sie unter Konfigurieren von STP-Funktionen.
- Automatische Erstellung von Layer-3-VLAN-Schnittstellen zur Unterstützung von VLAN-ACLs (VACLs)Weitere Informationen finden Sie unter Konfigurieren der Netzwerksicherheit.
- VACL-Erfassungsports können jeder Layer-2-Ethernet-Port in jedem VLAN seinWeitere Informationen finden Sie unter Konfigurieren der Netzwerksicherheit.
- Konfigurierbare MTU-Größe auf einzelnen physischen Layer-3-PortsWeitere Informationen finden Sie unter Übersicht über die Schnittstellenkonfiguration.
- Konfiguration der SPAN-Ziel-Ports als Trunks, sodass der gesamte SPAN-Datenverkehr mit Tags versehen wirdWeitere Informationen finden Sie unter Konfigurieren des lokalen und Remote-SPAN.

Zugehörige Informationen

- Tools und Ressourcen - Cisco Systems
- Produktsupport für Switches
- Unterstützung der LAN Switching-Technologie
- Technischer Support und Dokumentation - Cisco Systems