Best Practices für Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000 mit CatOS-Konfiguration und -Verwaltung

Inhalt

Zugehörige Informationen

Einführung

In diesem Dokument wird die Implementierung von Switches der Cisco Catalyst-Serie in Ihrem Netzwerk beschrieben, insbesondere die Plattformen Catalyst 4500/4000, 5500/5000 und 6500/6000. Konfigurationen und Befehle werden unter der Annahme erörtert, dass Sie die Catalyst OS (CatOS) General Deployment Software 6.4(3) oder höher ausführen. Obwohl einige Design-Überlegungen vorgestellt werden, wird in diesem Dokument nicht das allgemeine Campus-Design behandelt.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass Sie mit der Catalyst 6500 Series Command Reference, 7.6 vertraut sind.

Auch wenn im gesamten Dokument Verweise auf öffentliches Online-Material für eine weitere Lektüre enthalten sind, handelt es sich um andere grundlegende und informative Verweise:

- Cisco ISP Essentials: Grundlegende IOS-Funktionen, die jeder ISP berücksichtigen sollte.
- Cisco Richtlinien zur Netzwerküberwachung und Ereigniskorrelation
- Gigabit Campus-Netzwerkdesign - Prinzipien und Architektur
- Cisco SAFE: Ein Sicherheitskonzept für Enterprise Networks

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Diese Lösungen verfügen über jahrelange Erfahrung von Cisco Technikern, die mit vielen unserer größten Kunden und komplexen Netzwerken zusammenarbeiten. Daher werden in diesem Dokument reale Konfigurationen hervorgehoben, die Netzwerke erfolgreich machen. In diesem Whitepaper werden folgende Lösungen vorgestellt:

- Lösungen, die statistisch die größte Feldexposition und damit das geringste Risiko aufweisen.
- Einfache Lösungen, die gewisse Flexibilität einbringen, um deterministische Ergebnisse zu erzielen.
- Einfache Verwaltung und Konfiguration von Lösungen durch Netzwerkbetriebsteams
- Lösungen, die hohe Verfügbarkeit und Stabilität fördern.

Dieses Dokument ist in vier Abschnitte unterteilt:

- Basiskonfiguration - Funktionen, die von der Mehrzahl der Netzwerke wie Spanning Tree Protocol (STP) und Trunking verwendet werden.
- Verwaltungskonfiguration - Designüberlegungen sowie System- und Ereignisüberwachung mithilfe von Simple Network Management Protocol (SNMP), Remote Monitoring (RMON), Syslog, Cisco Discovery Protocol (CDP) und Network Time Protocol (NTP).
- Sicherheitskonfiguration - Kennwörter, Port-Sicherheit, physische Sicherheit und Authentifizierung mit TACACS+.
- Konfigurations-Checkliste - Zusammenfassung der vorgeschlagenen Konfigurationsvorlagen

Basiskonfiguration

In diesem Abschnitt werden die Funktionen erläutert, die mit den meisten Catalyst-Netzwerken bereitgestellt werden.

Catalyst Control Plane-Protokolle

In diesem Abschnitt werden die Protokolle vorgestellt, die zwischen Switches im normalen Betrieb ausgeführt werden. Ein grundlegendes Verständnis dieser Protokolle ist hilfreich, um jeden Abschnitt anzugehen.

Supervisor-Datenverkehr

Die meisten in einem Catalyst-Netzwerk aktivierten Funktionen erfordern zwei oder mehr Switches zur Zusammenarbeit. Daher muss ein kontrollierter Austausch von Keepalive-Nachrichten, Konfigurationsparametern und Managementänderungen erfolgen. Unabhängig davon, ob es sich um proprietäre Cisco Protokolle wie CDP oder standardbasierte Protokolle wie IEEE 802.1d (STP) handelt, haben alle bei der Implementierung in der Catalyst-Serie bestimmte Elemente gemeinsam.

Bei der grundlegenden Frame-Weiterleitung stammen die Daten-Frames der Benutzer von den Endsystemen, und ihre Quell- und Zieladresse werden in Layer 2 (L2)-Switched-Domänen nicht geändert. Die Nachschlagetabellen für den Content Addressable Memory (CAM) auf jeder Switch Supervisor Engine werden durch einen Prozess zum Erlernen der Quelladresse aufgefüllt und geben an, welcher Ausgangsport jeden empfangenen Frame weiterleiten muss. Wenn der Adresserlernprozess unvollständig ist (das Ziel ist unbekannt oder der Frame ist für eine Broadcast- oder Multicast-Adresse bestimmt), wird er an alle Ports in diesem VLAN weitergeleitet (überflutet).

Der Switch muss auch erkennen, welche Frames durch das System geschaltet werden und welche an die Switch-CPU selbst (auch bekannt als Network Management Processor [NMP]) weitergeleitet werden müssen.

Die Catalyst-Kontrollebene wird mithilfe spezieller Einträge in der CAM-Tabelle erstellt, die als **Systemeinträge** bezeichnet werden, um Datenverkehr an den NMP auf einem internen Switch-Port zu empfangen und an diesen weiterzuleiten. Mithilfe von Protokollen mit bekannten Ziel-MAC-Adressen kann der Datenverkehr auf Kontrollebene vom Datenverkehr getrennt werden. Geben Sie den **Befehl** CAM-System auf einem Switch ein, um dies zu bestätigen, wie folgt:

```
>show cam system
```

```
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry
VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  -----------------    -----  ----------------------------------------
1     00-d0-ff-88-cb-ff  #          1/3
!--- NMP internal port. 1 01-00-0c-cc-cc-cc # 1/3 !--- CDP and so on. 1 01-00-0c-cc-cc-cd # 1/3
!--- Cisco STP. 1 01-80-c2-00-00-00 # 1/3 !--- IEEE STP. 1 01-80-c2-00-00-01 # 1/3 !--- IEEE
flow control. 1 00-03-6b-51-e1-82 R# 15/1 !--- Multilayer Switch Feature Card (MSFC) router. ...
```

Cisco verfügt, wie gezeigt, über einen reservierten Bereich von Ethernet-MAC- und Protokolladressen. Jeder dieser Punkte wird später in diesem Dokument behandelt. In dieser Tabelle wird jedoch eine Zusammenfassung angezeigt.

Funktion	SNAP HDLC-Protokolltyp	Ziel-Multicast-MAC
Port Aggregation Protocol (PAgP)	0 x 0104	01-00-0c-cc-cc-cc
Spanning Tree PVSTP+	0 x 010 b	01-00-0c-cc-cd
VLAN-Bridge	0 x 010 C	01-00-0c-cd-cd-ce
Unidirectional Link Detection (UDLD)	0 x 0111	01-00-0c-cc-cc-cc
Cisco Discovery Protocol	0 x 2000	01-00-0c-cc-cc-cc
Dynamisches Trunking (DTP)	0 x 2004	01-00-0c-cc-cc-cc
STP-Uplink Fast	0 x 200 a	01-00-0c-cd-cd-cd
IEEE Spanning Tree 802.1d	K/A - DSAP 42 SSAP 42	01-80-c2-00-00-00
Inter Switch Link (ISL)	K/A	01-00-0c-00-00-00-00
VLAN-Trunking (VTP)	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

Die meisten Cisco Steuerungsprotokolle verwenden eine IEEE 802.3-SNAP-Kapselung, einschließlich **LLC 0xAAAA03, OUI 0x0000C**, die in einer LAN-Analyzer-Ablaufverfolgung sichtbar ist. Weitere allgemeine Eigenschaften dieser Protokolle sind:

- Diese Protokolle setzen eine Punkt-zu-Punkt-Verbindung voraus. Beachten Sie, dass die bewusste Verwendung von Multicast-Zieladressen zwei Catalyst-Analysten die transparente Kommunikation über Switches von Drittanbietern ermöglicht, da Geräte, die die Frames nicht

verstehen und abfangen, diese einfach überfluten. Point-to-Multipoint-Verbindungen in Umgebungen mit Geräten verschiedener Anbieter können jedoch zu inkonsistentem Verhalten führen und müssen im Allgemeinen vermieden werden.
- Diese Protokolle enden an Layer-3-Routern (L3). sie funktionieren nur innerhalb einer Switch-Domäne.
- Diese Protokolle erhalten eine Priorisierung gegenüber Benutzerdaten, indem sie ASIC-Verarbeitung (Application-Specific Integrated Circuit) und -zeitplanung eingeben.

Nach der Einführung der Zieladressen des Steuerungsprotokolls muss die Quelladresse ebenfalls aus Gründen der Vollständigkeit beschrieben werden. Switch-Protokolle verwenden eine MAC-Adresse, die aus einer Bank von verfügbaren Adressen stammt, die von einem EPROM im Chassis bereitgestellt werden. Geben Sie den Befehl **show module** ein, um die Adressbereiche anzuzeigen, die für jedes Modul verfügbar sind, wenn es Datenverkehr wie STP Bridge Protocol Data Units (BPDUs) oder ISL-Frames sendet.

```
>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
!--- MACs for sourcing traffic. ... VLAN 1
```

VLAN 1

VLAN 1 hat in Catalyst-Netzwerken eine besondere Bedeutung.

Die Catalyst Supervisor Engine verwendet immer das Standard-VLAN VLAN 1, um eine Reihe von Steuerungs- und Verwaltungsprotokollen beim Trunking zu kennzeichnen, z. B. CDP, VTP und PAgP. Alle Ports, einschließlich der internen Schnittstelle sc0, sind standardmäßig als Mitglieder von VLAN 1 konfiguriert. Alle Trunks enthalten standardmäßig VLAN 1. In den CatOS-Softwareversionen vor Version 5.4 war es nicht möglich, Benutzerdaten in VLAN 1 zu blockieren.

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

- Das Management-VLAN ist der Standort von sc0. Dieses VLAN kann geändert werden.
- Das native VLAN wird als das VLAN definiert, zu dem ein Port zurückkehrt, wenn er kein Trunking vornimmt, und ist das nicht gekennzeichnete VLAN auf einem 802.1Q-Trunk. Standardmäßig ist VLAN 1 das native VLAN.
- Führen Sie zum Ändern des nativen VLAN den Befehl **set vlan** vlan-id mod/port aus.**Hinweis:** Erstellen Sie das VLAN, bevor Sie es als natives VLAN des Trunks festlegen.

Dies sind einige gute Gründe, um 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 STP-Sicht), muss er zurückgezogen werden. Dies wird im Abschnitt In-Band-Management dieses Dokuments ausführlicher beschrieben.
- Die Daten der Kontrollebene in VLAN 1 müssen von den Benutzerdaten getrennt gehalten werden, um die Fehlerbehebung zu vereinfachen und die verfügbaren CPU-Zyklen zu

maximieren.
- L2-Schleifen in VLAN 1 müssen vermieden werden, wenn Multilayer-Campus-Netzwerke ohne STP entworfen werden. Wenn es mehrere VLANs und IP-Subnetze gibt, ist weiterhin Trunking zum Access Layer erforderlich. Deaktivieren Sie dazu VLAN 1 manuell von den Trunk-Ports.

Beachten Sie in der Zusammenfassung die folgenden Informationen zu Trunks:

- **CDP-, VTP- und PAgP-**Aktualisierungen werden immer auf Trunks mit einem VLAN 1-Tag weitergeleitet. Dies ist auch der Fall, wenn VLAN 1 aus den Trunks entfernt wird und nicht das native VLAN ist. Wenn VLAN 1 für Benutzerdaten gelöscht wird, hat dies keine Auswirkungen auf den Steuerungsebenen-Datenverkehr, der weiterhin über 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 wird 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 wird.
- In PVST+ werden die **802.1Q IEEE-BPDUs** im allgemeinen Spanning Tree VLAN 1 nicht getaggt weitergeleitet, um mit anderen Anbietern kompatibel zu sein, es sei denn, VLAN 1 wird 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 in diesem Dokument.
- 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 wird.
- 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 verhindern können, dass die MST-Bridge ihre Begrenzungsports in den Root-Inkonsistent-Zustand versetzt. Weitere Informationen finden Sie unter Understanding Multiple Spanning Tree Protocol (802.1s).

Empfehlungen

Um ein VLAN **betriebsbereit** zu halten, ohne dass in diesem VLAN Clients oder Hosts verbunden sind, muss mindestens ein physisches Gerät in diesem VLAN verbunden sein. Andernfalls hat das VLAN den Status **auf/ab**. Derzeit gibt es keinen Befehl zum **Hochfahren/Hochfahren** einer VLAN-Schnittstelle, wenn der Switch für dieses VLAN keine aktiven Ports enthält.

Wenn Sie kein Gerät anschließen möchten, schließen Sie einen Loopback-Stecker an einen beliebigen Port für dieses VLAN an. Alternativ können Sie ein Crossover-Kabel verwenden, das zwei Ports in diesem VLAN am gleichen Switch miteinander verbindet. Diese Methode erzwingt den Anschluss. Weitere Informationen finden Sie im Abschnitt Loopback-Plug-Tests für T1/56K-Leitungen im Abschnitt Loopback-Tests.

Wenn ein Netzwerk für Service Provider Multihomed ist, fungiert es als Transit-Netzwerk zwischen zwei Service Providern. Wenn die in einem Paket empfangene VLAN-Nummer übersetzt oder geändert werden muss, wenn sie von einem Service Provider an einen anderen Service Provider übergeben wird, empfiehlt es sich, die QinQ-Funktion zu verwenden, um die VLAN-Nummer zu übersetzen.

VLAN Trunking Protocol

Bevor Sie VLANs erstellen, bestimmen Sie den im Netzwerk zu verwendenden VTP-Modus. VTP ermöglicht die zentrale Durchführung von VLAN-Konfigurationsänderungen auf einem oder mehreren Switches. Diese Änderungen werden automatisch an alle anderen Switches in der Domäne weitergeleitet.

Überblick

VTP ist ein L2-Messaging-Protokoll, das die Konsistenz der VLAN-Konfiguration aufrecht erhält. VTP verwaltet das Hinzufügen, Löschen und Umbenennen von VLANs auf netzwerkweiter Basis. VTP minimiert Fehlkonfigurationen und Konfigurationsinkonsistenzen, die eine Reihe von Problemen verursachen können, z. B. doppelte VLAN-Namen, falsche VLAN-Typspezifikationen und Sicherheitsverletzungen. Die VLAN-Datenbank ist eine Binärdatei und wird auf VTP-Servern separat von der Konfigurationsdatei im NVRAM gespeichert.

Das VTP-Protokoll kommuniziert zwischen Switches mithilfe einer Ethernet-Ziel-Multicast-MAC-Adresse (**01-00-0c-cc-cc**) und des SNAP-HDLC-Protokolltyps Ox2003. Es funktioniert nicht über Nicht-Trunk-Ports (VTP ist eine Nutzlast von ISL oder 802.1Q), daher können Nachrichten erst gesendet werden, wenn der DTP-Trunk online gestellt wurde.

Zu den Meldungstypen gehören zusammenfassende Anzeigen alle fünf Minuten, untergeordnete Anzeigen und Anforderungsanzeigen bei Änderungen sowie Verknüpfungen, wenn VTP-Bereinigung aktiviert ist. Die Revisionsnummer der VTP-Konfiguration wird mit jeder Änderung auf einem Server um eine erhöht, wodurch die neue Tabelle über die Domäne verteilt wird.

Wenn ein VLAN gelöscht wird, werden Ports, die einst Mitglied dieses VLANs waren, in einen inaktiven Zustand versetzt. Wenn ein Switch im Client-Modus beim Hochfahren die VTP VLAN-Tabelle nicht empfangen kann (entweder von einem VTP-Server oder einem anderen VTP-Client), werden alle Ports in anderen VLANs als dem Standard-VLAN 1 deaktiviert.

Diese Tabelle enthält eine Zusammenfassung des Funktionsvergleichs für verschiedene VTP-Modi:

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

Im VTP-`transparenten` Modus werden VTP-Updates ignoriert (die 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 ein Switch im transparenten Modus (oder ein Switch eines anderen Anbieters) einfach den Frame zu anderen Cisco Switches in der Domäne.

[1] Die CatOS-Softwareversion 7.1 bietet die Möglichkeit, VTP mit dem `Aus`-Modus zu deaktivieren. Im VTP-`Aus`-Modus verhält sich der Switch sehr ähnlich wie der VTP-`transparente` Modus, mit der Ausnahme, dass der `Aus`-Modus auch die Weiterleitung von VTP-Updates unterdrückt.

Diese Tabelle enthält eine Zusammenfassung der Erstkonfiguration:

Funktion	Standardwert
VTP-Domänenname	Null
VTP-Modus	Server
VTP-Version	Version 1 ist aktiviert.
VTP-Kennwort	Keine
VTP-Bereinigung	Deaktiviert

VTP Version 2 (VTPv2) bietet diese funktionale Flexibilität. Es ist jedoch nicht mit VTP Version 1 (VTPv1) kompatibel:

- Unterstützung für Token-Ring
- Unterstützung nicht erkannter VTP-Informationen; Switches geben jetzt Werte weiter, die nicht analysiert werden 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 durch die Konfiguration eines einzelnen Switches aktiviert werden.

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

VTP-Version 3

CatOS Software Version 8.1 bietet Unterstützung für VTP Version 3 (VTPv3). VTPv3 bietet Erweiterungen gegenüber den vorhandenen Versionen. Diese Erweiterungen ermöglichen:

- Unterstützung erweiterter VLANs
- Unterstützung für die Erstellung und Anzeige privater VLANs
- Unterstützung für VLAN-Instanzen und MST-Mapping-Weiterleitungsinstanzen (die in CatOS 8.3 unterstützt werden)
- Verbesserte Serverauthentifizierung
- Schutz vor versehentlicher Einfügung der "falschen" Datenbank in eine VTP-Domäne
- Interaktion mit VTPv1 und VTPv2
- Konfiguration pro Port

Einer der Hauptunterschiede zwischen der VTPv3-Implementierung und der früheren Version besteht in der Einführung eines primären VTP-Servers. Im Idealfall darf sich nur ein primärer Server in einer VTPv3-Domäne befinden, wenn die Domäne nicht partitioniert ist. Alle Änderungen, die Sie an der VTP-Domäne vornehmen, müssen auf dem primären VTP-Server ausgeführt werden, damit sie an die VTP-Domäne weitergeleitet werden können. Innerhalb einer

VTPv3-Domäne können mehrere Server vorhanden sein, die auch als sekundäre Server bezeichnet werden. Wenn ein Switch als Server konfiguriert ist, wird er standardmäßig zum Sekundärserver. Der sekundäre Server kann die Konfiguration der Domäne speichern, die Konfiguration jedoch nicht ändern. Ein sekundärer Server kann sich zum primären Server mit erfolgreicher Übernahme vom Switch entwickeln.

Switches, die VTPv3 ausführen, akzeptieren nur eine VTP-Datenbank mit einer höheren Revisionsnummer als der aktuelle Primärserver. Dieser Prozess unterscheidet sich erheblich von VTPv1 und VTPv2, bei denen ein Switch immer eine übergeordnete Konfiguration von einem Nachbarn in derselben Domäne akzeptiert. Diese Änderung mit VTPv3 bietet Schutz. Ein neuer Switch, der mit einer höheren VTP-Revisionsnummer in das Netzwerk eingeführt wird, kann die VLAN-Konfiguration der gesamten Domäne nicht überschreiben.

VTPv3 bietet darüber hinaus eine Erweiterung der VTP-Behandlung von Passwörtern. Wenn Sie die Option für die Konfiguration eines ausgeblendeten Kennworts verwenden, um ein Kennwort als "ausgeblendet" zu konfigurieren, geschieht Folgendes:

- Das Kennwort wird in der Konfiguration nicht im Klartext angezeigt. Das geheime Hexadezimalformat des Kennworts wird in der Konfiguration gespeichert.
- Wenn Sie versuchen, den Switch als Primärserver zu konfigurieren, werden Sie zur Eingabe des Kennworts aufgefordert. Wenn Ihr Kennwort mit dem geheimen Kennwort übereinstimmt, wird der Switch zum primären Server, der Ihnen die Konfiguration der Domäne ermöglicht.

Hinweis: Beachten Sie, dass der primäre Server nur erforderlich ist, wenn Sie die VTP-Konfiguration für eine beliebige Instanz ändern müssen. Eine VTP-Domäne kann ohne aktiven primären Server betrieben werden, da die sekundären Server die Persistenz der Konfiguration über Neuladungen sicherstellen. Der Status des primären Servers wird aus folgenden Gründen beendet:

- Neuladen eines Switches
- Hochverfügbares Switchover zwischen den aktiven und redundanten Supervisor Engines
- Übernahme von einem anderen Server
- Änderung der Moduskonfiguration
- Alle Konfigurationsänderungen der VTP-Domäne, z. B. eine Änderung in:VersionDomänennameDomänenkennwort

VTPv3 ermöglicht den Switches auch die Teilnahme an mehreren VTP-Instanzen. In diesem Fall kann derselbe Switch der VTP-Server für eine Instanz und ein Client für eine andere Instanz sein, da die VTP-Modi für verschiedene VTP-Instanzen spezifisch sind. Beispielsweise kann ein Switch im `transparenten` Modus für eine MST-Instanz betrieben werden, während der Switch im `Servermodus` für eine VLAN-Instanz konfiguriert ist.

In Bezug auf die Interaktion mit VTPv1 und VTPv2 bestand das Standardverhalten in allen VTP-Versionen darin, dass bei den früheren VTP-Versionen die Updates für die neue Version einfach verloren gingen. Wenn sich die VTPv1- und VTPv2-Switches nicht im `transparenten` Modus befinden, werden alle VTPv3-Updates verworfen. Nachdem VTPv3-Switches einen Legacy-VTPv1- oder VTPv2-Frame auf einem Trunk empfangen haben, übergeben die Switches andererseits eine verkleinerte Version ihres Datenbankupdates an die VTPv1- und VTPv2-Switches. Dieser Informationsaustausch ist jedoch einseitig, da von den VTPv3-Switches keine Updates von VTPv1- und VTPv2-Switches akzeptiert werden. Bei Trunk-Verbindungen senden VTPv3-Switches weiterhin verkleinerte Updates sowie komplette VTPv3-Updates, um VTPv2- und VTPv3-Nachbarn an den Trunk-Ports zu unterstützen.

Um VTPv3 für erweiterte VLANs zu unterstützen, wird das Format der VLAN-Datenbank, in der das VTP 70 Byte pro VLAN zuweist, geändert. Die Änderung ermöglicht die Kodierung von nicht standardmäßigen Werten, anstatt unmodifizierte Felder für die Legacy-Protokolle zu übernehmen. Aufgrund dieser Änderung entspricht die 4K-VLAN-Unterstützung der Größe der resultierenden VLAN-Datenbank.

Empfehlung

Es gibt keine spezifische Empfehlung, ob der VTP-`Client/Server`-Modus oder der VTP-`transparente` Modus verwendet werden soll. Einige Kunden ziehen die einfache Verwaltung des VTP-`Client/Server`-Modus vor, obwohl später einige Überlegungen angestellt wurden. Aus Redundanzgründen sollten in jeder Domäne zwei `Server`-Mode-Switches vorhanden sein, in der Regel die beiden Distribution-Layer-Switches. Für die übrigen Switches in der Domäne muss der `Client`-Modus festgelegt werden. Wenn Sie den `Client/Server`-Modus unter Verwendung von VTPv2 implementieren, achten Sie darauf, dass immer eine höhere Revisionsnummer in derselben VTP-Domäne akzeptiert wird. Wenn ein Switch, der entweder im VTP-`Client-` oder `Server`-Modus 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 die Überschrift einen schwerwiegenden Ausfall im Netzwerk verursachen. Um sicherzustellen, dass die `Client-` oder `Server`-Switches immer eine Konfigurationsrevisionsnummer haben, die niedriger ist als die des Servers, ändern Sie den Client-VTP-Domänennamen in einen anderen als den Standardnamen. Kehren Sie 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 den vorsichtigen Ansatz des VTP-`transparenten` Modus aus folgenden Gründen:

- Es fördert eine bewährte Änderungskontrollpraxis, da die Anforderung, ein VLAN auf einem Switch oder Trunk-Port zu ändern, jeweils als ein Switch betrachtet werden muss.
- Es begrenzt das Risiko eines Administratorfehlers, der sich auf die gesamte Domäne auswirkt, wie etwa das versehentliche Löschen eines VLAN.
- Es besteht kein Risiko, dass ein neuer Switch, der mit einer höheren VTP-Revisionsnummer in das Netzwerk eingeführt wurde, die gesamte Domänen-VLAN-Konfiguration überschreiben kann.
- Es empfiehlt, VLANs von Trunks zu trennen, die zu Switches ausgeführt werden, die keine Ports in diesem VLAN haben. Dadurch wird die Frame-Flutung bandbreiteneffizienter. Manuelles Beschneiden ist ebenfalls von Vorteil, da es den Spanning-Tree-Durchmesser verringert (siehe DTP-Abschnitt dieses Dokuments). Stellen Sie vor der Beschneidung nicht verwendeter VLANs auf Port-Channel-Trunks sicher, dass alle mit IP-Telefonen verbundenen Ports als Zugriffsports mit Sprach-VLAN konfiguriert sind.
- Der erweiterte VLAN-Bereich in CatOS 6.x und CatOS 7.x, Ziffern 1025 bis 4094, kann nur auf diese Weise konfiguriert werden. Weitere Informationen finden Sie im Abschnitt Erweiterte VLAN- und MAC-Adressenreduzierung in diesem Dokument.
- Der `transparente` VTP-Modus wird in Campus Manager 3.1, Teil von Cisco Works 2000, unterstützt. Die alte Einschränkung, die mindestens einen Server in einer VTP-Domäne erfordert, wurde entfernt.

VTP-Beispielbef	Kommentare

ehle	
vtp domain ***name*** **password** ***x***	CDP überprüft Namen, um bei der Suche nach Fehlverkabelungen zwischen Domänen zu helfen. Ein einfaches Passwort ist eine hilfreiche Vorsichtsmaßnahme gegen unbeabsichtigte Änderungen. Achten Sie beim Einfügen auf Groß- und Kleinschreibung.
Set vtp mode transparen t	
Name der VLAN- ***VLAN-Nummer*** **festlegen**	Pro Switch mit Ports im VLAN
Trunk- ***Modus/Por t-VLAN-Bereich*** **festlegen**	Ermöglicht Trunks, VLANs bei Bedarf zu übertragen - standardmäßig sind alle VLANs aktiviert.
Clear Trunk ***Mod/Port VLAN-Bereich***	Begrenzt den STP-Durchmesser durch manuelles Beschneiden, z. B. auf Trunks vom Distribution Layer zum Access Layer, wo das VLAN nicht vorhanden ist.

Hinweis: Durch die Angabe von VLANs mit dem **Befehl set** werden nur VLANs hinzugefügt, diese werden jedoch nicht gelöscht. Der **Befehl** set trunk x/y 1-10 setzt die zulässige Liste beispielsweise nicht auf die VLANs 1-10. Geben Sie den **Befehl** clear trunk x/y 11-1005 **ein,** um das gewünschte Ergebnis zu erzielen.

Obwohl das Switching von Token-Klingeltönen nicht in den Geltungsbereich dieses Dokuments fällt, wird der VTP-`transparente` Modus für TR-ISL-Netzwerke nicht empfohlen. Die Grundlage für Token Ring Switching besteht darin, dass die gesamte Domäne eine verteilte Multi-Port-Bridge bildet, sodass jeder Switch über dieselben VLAN-Informationen verfügen muss.

Weitere Optionen

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

VTPv3 bietet die Möglichkeit, eine strengere Authentifizierung und Konfigurationsrevisionskontrolle zu implementieren. VTPv3 bietet im Wesentlichen die gleiche Funktionalität, bietet aber eine höhere Sicherheit, wie VTPv1/VTPv2 `transparenter` Modus bietet. Darüber hinaus ist VTPv3 teilweise mit den älteren VTP-Versionen kompatibel.

In diesem Dokument werden die Vorteile einer Beschneidung von VLANs zur Reduzierung von unnötigem Frame-Flooding empfohlen. Der **Befehl** set vtp pruning enable löst VLANs automatisch aus, wodurch das ineffiziente Flooding von Frames, die nicht benötigt werden, verhindert wird.

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

Ab CatOS 5.1 können die Catalyst Switches 802.1Q-VLAN-Nummern größer als 1000 ISL-VLAN-Nummern zuordnen. In CatOS 6.x unterstützen Catalyst 6500/6000-Switches 4096 VLANs gemäß IEEE 802.1Q-Standard. Diese VLANs sind in diese drei Bereiche eingeteilt, von denen nur einige mit VTP auf andere Switches im Netzwerk verteilt werden:

- normale VLANs: 1-1001
- VLANs mit erweiterter Reichweite: 1025-4094 (kann nur von VTPv3 propagiert werden)
- VLANs mit reserviertem Bereich: 0, 1002-1024, 4095

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

Hinweis: CatOS 7.x bietet die Möglichkeit, VTP auf den `Aus`-Modus zu setzen, ein Modus, der dem `transparenten Modus` sehr ähnlich ist. Der Switch leitet jedoch keine VTP-Frames weiter. Dies kann in einigen Designs nützlich sein, wenn Sie mit Switches außerhalb Ihrer Verwaltungskontrolle verbunden sind.

Erweiterte VLAN- und MAC-Adressreduzierung

Die Funktion zur Reduzierung von MAC-Adressen ermöglicht die Identifizierung von VLANs mit erweiterten Bereichen. Durch die Aktivierung der Reduzierung von MAC-Adressen wird der Pool der MAC-Adressen deaktiviert, die für den VLAN-Spanning Tree verwendet werden, und es wird eine einzige MAC-Adresse beibehalten. Diese MAC-Adresse identifiziert den Switch. Die CatOS-Softwareversion 6.1(1) bietet Unterstützung für die MAC-Adressreduzierung für Catalyst 6500/6000- und Catalyst 4500/4000-Switches zur Unterstützung von 4096 VLANs gemäß IEEE 802.1Q-Standard.

Übersicht über Vorgänge

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

Catalyst Switches mit 1024 MAC-Adressen ermöglichen standardmäßig keine Reduzierung der MAC-Adressen. MAC-Adressen werden nacheinander zugewiesen. Die erste MAC-Adresse im Bereich ist VLAN 1 zugewiesen. Die zweite MAC-Adresse im Bereich ist VLAN 2 zugewiesen usw. Dadurch können die Switches 1024 VLANs mit jedem VLAN mithilfe einer eindeutigen Bridge-ID unterstützen.

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, WS-C6506-E, WS-C6506, WS-C6009, WS-	1024

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] Die Reduzierung von MAC-Adressen ist standardmäßig für Switches mit 64 MAC-Adressen aktiviert, und die Funktion kann nicht deaktiviert werden.

Bei Switches der Catalyst-Serie mit 1024 MAC-Adressen ermöglicht die Aktivierung der Reduzierung von MAC-Adressen die Unterstützung von 4096 VLANs, die unter PVST+ ausgeführt werden, oder von 16 MISTP-Instanzen (Multiple Instance STP), ohne dass die Anzahl der für den Switch erforderlichen MAC-Adressen erhöht werden muss. Durch die Reduzierung der MAC-Adresse wird die Anzahl der für das STP erforderlichen MAC-Adressen von einer pro VLAN- oder MISTP-Instanz auf eine pro Switch reduziert.

Diese Abbildung zeigt, dass die Reduzierung der MAC-Adresse für die Bridge-ID nicht aktiviert ist. Die Bridge-ID besteht aus einer 2-Byte-Bridge-Priorität und einer 6-Byte-MAC-Adresse:

Durch die Reduzierung der MAC-Adresse wird der STP Bridge Identifier-Teil der BPDU geändert. Das ursprüngliche 2-Byte-Prioritätsfeld ist in zwei Felder unterteilt. Diese Aufteilung führt zu einem 4-Bit-Bridge-Prioritätsfeld und einer 12-Bit-System-ID-Erweiterung, die eine VLAN-Nummerierung von 0 bis 4095 ermöglicht.

Wenn die Reduzierung der MAC-Adressen auf Catalyst Switches aktiviert ist, um VLANs mit erweitertem Bereich zu nutzen, ermöglichen Sie die Reduzierung der MAC-Adressen auf allen Switches innerhalb derselben STP-Domäne. Dieser Schritt ist erforderlich, um die STP-Root-Berechnungen auf allen Switches konsistent zu halten. Nachdem Sie die MAC-Adressreduzierung aktiviert haben, wird die Root Bridge-Priorität zu einem Vielfaches von 4096 plus der VLAN-ID. Die Switches ohne MAC-Adressenreduktion können unbeabsichtigt Root beanspruchen, da diese Switches eine feinere Präzision bei der Auswahl der Bridge-ID aufweisen.

Konfigurationsrichtlinien

Wenn Sie einen erweiterten VLAN-Bereich konfigurieren, müssen Sie bestimmte Richtlinien befolgen. Der Switch kann einen VLAN-Block aus dem erweiterten Bereich für interne Zwecke zuweisen. Beispielsweise kann der Switch die VLANs für die gerouteten Ports oder Flex WAN-Module zuweisen. Die Zuweisung des VLAN-Blocks beginnt immer von VLAN 1006 und geht hoch. Wenn Sie VLANs im Bereich haben, den das Flex WAN-Modul benötigt, werden nicht alle erforderlichen VLANs zugewiesen, da die VLANs nie vom Benutzer-VLAN-Bereich zugewiesen werden. Geben Sie den Befehl **show vlan** oder den Befehl **show vlan summary** auf einem Switch ein, um sowohl die vom Benutzer zugewiesenen als auch die internen VLANs anzuzeigen.

```
>show vlan summary

Current Internal Vlan Allocation Policy - Ascending

Vlan status    Count  Vlans
-------------  -----  -----------------------------------------
VTP Active         7   1,17,174,1002-1005

Internal           7   1006-1011,1016
!--- These are internal VLANs. >show vlan
---- -------------------------------- --------- ------- --------

1    default                          active    7       4/1-48


!--- Output suppressed. 1006 Online Diagnostic Vlan1 active 0 internal 1007 Online Diagnostic
Vlan2 active 0 internal 1008 Online Diagnostic Vlan3 active 0 internal 1009 Voice Internal Vlan
active 0 internal 1010 Dtp Vlan active 0 internal 1011 Private Vlan Internal Vlan suspend 0
internal 1016 Online SP-RP Ping Vlan active 0 internal !--- These are internal VLANs.
```

Darüber hinaus müssen Sie vor der Verwendung der VLANs mit erweitertem Bereich alle vorhandenen 802.1Q-to-ISL-Zuordnungen löschen. Darüber hinaus müssen Sie in Versionen vor VTPv3 statisch das erweiterte VLAN auf jedem Switch mithilfe des VTP-`transparenten` Modus konfigurieren. Weitere Informationen finden Sie im Abschnitt *Konfigurationsrichtlinien für VLANs mit* erweitertem *Bereich* unter Konfigurieren von VLANs.

Hinweis: In einer Software, die älter als die Softwareversion 8.1(1) ist, können Sie den VLAN-Namen für VLANs mit erweitertem Bereich nicht konfigurieren. Diese Funktion ist unabhängig von jeder VTP-Version oder jedem VTP-Modus.

Empfehlung

Versuchen Sie, eine konsistente Konfiguration zur Reduzierung von MAC-Adressen in derselben STP-Domäne beizubehalten. Die Durchsetzung einer Reduzierung der MAC-Adressen auf allen Netzwerkgeräten kann jedoch nicht praktikabel sein, wenn neue Chassis mit 64 MAC-Adressen in die STP-Domäne eingeführt werden. Die Reduzierung von MAC-Adressen ist standardmäßig für Switches mit 64 MAC-Adressen aktiviert, und diese Funktion kann nicht deaktiviert werden. Wenn zwei Systeme mit derselben Spanning-Tree-Priorität konfiguriert werden, hat das System ohne MAC-Adressenreduktion eine bessere Spanning-Tree-Priorität. Geben Sie diesen Befehl ein, um die MAC-Adressreduzierung zu aktivieren oder zu deaktivieren:

```
set spantree macreduction enable | disable
```

Die Zuweisung der internen VLANs erfolgt in aufsteigender Reihenfolge und beginnt bei VLAN 1006. Weisen Sie die Benutzer-VLANs so nahe wie möglich an VLAN 4094 zu, um Konflikte zwischen den Benutzer-VLANs und den internen VLANs zu vermeiden. Mit Catalyst 6500-Switches, auf denen die Cisco IOS®-Systemsoftware ausgeführt wird, können Sie die interne VLAN-Zuweisung in absteigender Reihenfolge konfigurieren. Die CLI-Entsprechung (Command Line Interface) für CatOS-Software wird nicht offiziell unterstützt.

Autonegotiation

Ethernet/Fast Ethernet

Die Autonegotiation ist eine optionale Funktion des IEEE Fast Ethernet (FE)-Standards (802.3u), der es Geräten ermöglicht, automatisch Informationen über **Geschwindigkeit** und **Duplex-**Funktionen über eine Verbindung auszutauschen. Die Autonegotiation wird auf Layer 1 (L1) ausgeführt und bezieht sich auf Access-Layer-Ports, an denen **transiente Benutzer** wie PCs mit dem Netzwerk verbunden sind.

Überblick

Die häufigste Ursache für Leistungsprobleme bei 10/100-Mbit/s-Ethernet-Verbindungen tritt auf, wenn ein Port an der Verbindung mit Halbduplex betrieben wird, der andere mit Vollduplex. Dies geschieht gelegentlich, wenn ein oder beide Ports einer Verbindung zurückgesetzt werden und der Verhandlungsprozess nicht dazu führt, dass beide Verbindungspartner dieselbe Konfiguration haben. Dies geschieht auch, wenn Administratoren eine Seite einer Verbindung neu konfigurieren und vergessen, die andere Seite neu zu konfigurieren. Die typischen Symptome hierfür sind eine Erhöhung der Frame Check Sequence (FCS), eine zyklische Redundanzprüfung (CRC), eine Ausrichtung oder laufende Zähler am Switch.

Die Autonegotiation wird in diesen Dokumenten ausführlich behandelt. Diese Dokumente enthalten Erklärungen zur Funktionsweise der Autoübertragung und Konfigurationsoptionen.

- Konfiguration und Fehlerbehebung für Ethernet 10/100 MB 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 ist eine Folge der automatischen Verhandlung eines Verbindungspartners, der keine Auto-Negotiation-Parameter des anderen Verbindungspartners erkennt und auf Halbduplex zurückgesetzt wird.

Die meisten Catalyst Ethernet-Module unterstützen 10/100 Mbit/s und Halbduplex/Vollduplex. Der Befehl **show port functions *mod/port*** bestätigt dies **jedoch**.

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 **Ausfall am anderen Ende** ist ein Verbindungsfehler, den eine Station erkennen kann, während die andere nicht erkennen kann, z. B. ein nicht verbundener TX-Draht. In diesem Beispiel könnte die Sendestation noch gültige Daten empfangen und feststellen, dass die Verbindung durch den Link-Integrität-Monitor gut ist. Sie erkennt nicht, dass die Übertragung nicht von der anderen Station empfangen wird. Eine 100BASE-FX-Station, die einen solchen Remote-Fehler erkennt, kann seinen übertragenen IDLE-Stream so modifizieren, dass er ein spezielles Bitmuster (das FEFI IDLE-Muster) sendet, um den Nachbarn über den Remote-Fehler zu informieren. Das FEFI-IDLE-Muster löst anschließend ein Herunterfahren des Remote-Ports (errdisable) aus. Weitere Informationen zum Fehlerschutz finden Sie im UDLD-Abschnitt dieses Dokuments.

FEFI wird von dieser Hardware und den folgenden Modulen unterstützt:

- Catalyst 5500/5000: WS-X5201R, WS-X5305, WS-X5236, WS-X5237, WS-U5538 und WS-

U5539
- Catalyst 6500/6000 und 4500/4000: Alle 100BASE-FX-Module und GE-Module

Empfehlung

Ob die Autoübertragung für 10/100-Verbindungen oder für Geschwindigkeit und Duplex von Code konfiguriert werden soll, hängt letztendlich vom Verbindungspartner oder 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. Probleme können jedoch auftreten, wenn NIC- oder Anbieter-Switches nicht genau konform sind. Hardwarekompatibilität und andere Probleme können auch auf anbieterspezifische erweiterte Funktionen wie automatische Polarität oder Kabelintegrität zurückzuführen sein, die in der IEEE 802.3u-Spezifikation für die 10/100-Mbit/s-Autoübertragung nicht beschrieben sind. Siehe Problemhinweis: Leistungsprobleme bei Intel Pro/1000T NICs, die mit CAT4K/6K verbunden sind, z. B.

Es ist zu erwarten, dass in einigen Situationen Host, Port-Geschwindigkeit und Duplex eingestellt werden müssen. Befolgen Sie im Allgemeinen die folgenden grundlegenden Schritte zur Fehlerbehebung:

- Stellen Sie sicher, dass entweder die Autoübertragung auf beiden Seiten der Verbindung konfiguriert ist, oder dass die feste Codierung auf beiden Seiten konfiguriert ist.
- In den Versionshinweisen von CatOS finden Sie allgemeine Hinweise.
- Überprüfen Sie die Version des Netzwerkkartentreibers oder Betriebssystems, die Sie ausführen, da häufig der neueste Treiber oder Patch erforderlich ist.

Versuchen Sie in der Regel, zunächst die Autonegotiation für jeden Verbindungspartner zu verwenden. Die Konfiguration der automatischen Verhandlung für transiente Geräte wie Laptops bietet eindeutige Vorteile. Im Idealfall funktioniert die automatische Verhandlung auch bei nicht-transienten Geräten wie Servern und festen Workstations oder von Switch zu Switch und Switch zu Router. Aus einigen der genannten Gründe können sich Verhandlungsfragen ergeben. Befolgen Sie in diesen Fällen die grundlegenden Fehlerbehebungsschritte, die in den bereitgestellten TAC-Links beschrieben sind.

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

```
set port speed port range auto
!--- This is the default.
```

Wenn Sie den Port fest kodieren, geben Sie folgende Konfigurationsbefehle an:

```
set port speed port range 10 | 100 set port duplex port range full | half
```

In CatOS 8.3 und höher hat Cisco das optionale **auto-10-100**-Schlüsselwort eingeführt. Verwenden Sie das Schlüsselwort **auto-100** für Ports, die Geschwindigkeiten von 10/100/1000 Mbit/s unterstützen, bei denen jedoch eine Autonegotiation auf 1000 Mbit/s nicht wünschenswert ist. Durch die Verwendung des **Schlüsselworts auto-10-100** verhält sich der Port genau wie ein 10/100-Mbit/s-Port, dessen Geschwindigkeit auf **Auto** eingestellt ist. Geschwindigkeit und Duplex

werden nur für 10/100-Mbit/s-Ports ausgehandelt, und die Geschwindigkeit von 1000 Mbit/s nimmt nicht an der Aushandlung teil.

```
set port speed port_range auto-10-100
```

Weitere Optionen

Wenn zwischen Switches keine automatische Verhandlung erfolgt, kann bei bestimmten Problemen auch die L1-Fehleranzeige verloren gehen. Es ist hilfreich, L2-Protokolle zu verwenden, um die Fehlererkennung zu verbessern, z. B. aggressives UDLD.

Gigabit-Ethernet

Gigabit Ethernet (GE) verfügt über ein umfassenderes als das für 10/100-Mbit/s-Ethernet (IEEE 802.3z) und wird zum Austausch von Flusssteuerungsparametern, Remote-Fehlerinformationen und Duplexinformationen verwendet (obwohl die GE-Ports der Catalyst-Serie nur Vollduplex-Modus unterstützen).

Hinweis: 802.3z wurde durch die Spezifikationen IEEE 802.3:2000 ersetzt. Weitere Informationen finden Sie im IEEE Standards On Line LAN/MAN Standards Subscription: Archiv für weitere Informationen.

Überblick

Die GE-Port-Aushandlung ist standardmäßig aktiviert, und die Ports an beiden Enden einer GE-Verbindung müssen die gleiche Einstellung haben. Im Gegensatz zu FE wird die GE-Verbindung nicht angezeigt, wenn die Einstellung für die automatische Aushandlung von den Ports an den einzelnen Enden der Verbindung abweicht. Die einzige Bedingung, die für die Verbindung eines Ports mit deaktivierter Autoübertragung erforderlich ist, ist ein gültiges Gigabit-Signal vom anderen Ende. Dieses Verhalten ist unabhängig von der Auto-Negotiation-Konfiguration des Gegenstandes. Beispiel: Es gibt zwei Geräte, A und B. Auf jedem Gerät kann die automatische Verhandlung aktiviert oder deaktiviert sein. Diese Tabelle enthält eine Liste möglicher Konfigurationen und der 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 besteht, wird eine Bedingung für "Synchronisierung fehlgeschlagen" geltend gemacht, und die Verbindung 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 an einem Port deaktiviert ist, ist die "Autoübertragung"-Phase 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 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 set port sync-restart-delay hat nur dann eine Wirkung, wenn die Option Autoübertragung auf** `Aktivieren` eingestellt ist.

Empfehlung

In einer GE-Umgebung ist die Aktivierung der Autoverhandlungen wesentlich wichtiger als in einer 10/100-Umgebung. Die automatische Verhandlung darf nur bei Switch-Ports deaktiviert werden, die an Geräte angeschlossen sind, die keine Verhandlung unterstützen können, oder wenn Verbindungsprobleme aufgrund von Interoperabilitätsproblemen auftreten. Cisco empfiehlt, die Gigabit-Aushandlung (Standard) auf allen Switch-to-Switch-Verbindungen und generell auf allen GE-Geräten zu aktivieren. Geben Sie diesen Befehl ein, um die Autonegotiation zu aktivieren:

```
set port negotiation port range enable
!--- This is the default.
```

Eine bekannte Ausnahme ist, wenn eine Verbindung zu einem Gigabit Switch Router (GSR) besteht, auf dem die Cisco IOS Software vor Version 12.0(10)S ausgeführt wird, der Version, die die Flusskontrolle und Autoübertragung hinzugefügt hat. Schalten Sie in diesem Fall diese beiden Funktionen aus, oder die Switch-Port-Berichte `sind nicht verbunden`, und die GSR meldet Fehler. Dies ist eine Beispielbefehlssequenz:

```
set port flowcontrol receive port range off set port flowcontrol send port range off set port
negotiation port range disable
```

Switch-to-Server-Verbindungen müssen von Fall zu Fall untersucht werden. Bei Cisco Kunden traten Gigabit-Aushandlung auf Sun-, HP- und IBM-Servern Probleme auf.

Weitere Optionen

Die Flusssteuerung ist ein optionaler Teil der 802.3x-Spezifikation und muss bei Verwendung ausgehandelt werden. Geräte können oder können nicht auf PAUSE-Frames (**bekannte MAC 01-80-C2-00-00-00-0F**) senden und/oder antworten. Sie können auch der Flusskontrollanfrage des Nachbarn am anderen Ende nicht zustimmen. Ein Port mit einem ausgefüllten Eingangspuffer sendet einen PAUSE-Frame an seinen Verbindungspartner, der die Übertragung stoppt und weitere Frames in den Ausgabepuffern des Verbindungspartners speichert. Dies löst kein Problem mit der Überbelegung im Steady-State-Bereich, sondern macht den Eingangspuffer während eines Bursts im Endeffekt um einen Bruchteil des Partner-Ausgabepuffers größer.

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

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

```
set port flowcontrol mod/port 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, WS-X4306) senden niemals PAUSE-Frames, auch wenn sie dies aushandeln, da sie nicht blockieren.

Dynamisches Trunking Protocol

Kapselungstyp

Trunks erweitern VLANs zwischen Geräten, indem sie die ursprünglichen Ethernet-Frames vorübergehend identifizieren und markieren (link-local). Auf diese Weise können sie über eine einzelne Verbindung im Multiplexing verwendet werden. Dadurch wird auch sichergestellt, dass die separaten VLAN-Broadcast- und Sicherheitsdomänen zwischen den Switches aufrechterhalten werden. In den CAM-Tabellen wird die Frame-to-VLAN-Zuordnung in den Switches beibehalten.

Trunking wird auf mehreren L2-Medientypen unterstützt, darunter ATM LANE, FDDI 802.10 und Ethernet. Es wird jedoch nur letzteres angezeigt.

ISL-Übersicht

Das proprietäre Identifizierungs- oder Tagging-Schema von Cisco, ISL, wird seit vielen Jahren eingesetzt. Der 802.1Q IEEE-Standard ist ebenfalls verfügbar.

Durch die vollständige Kapselung des ursprünglichen Frames in ein zweistufiges Tagging-Schema ist ISL praktisch ein Tunneling-Protokoll und hat den zusätzlichen Vorteil, dass Frames ohne Ethernet transportiert werden können. Er fügt dem Standard-Ethernet-Frame einen 26-Byte-Header und einen 4-Byte-FCS hinzu - die größeren Ethernet-Frames werden erwartet und von Ports verarbeitet, die als Trunks konfiguriert sind. ISL unterstützt 1024 VLANs.

ISL Frame-Format

40 Bit	4 Bit	4 Bit	48 Bit	16 Bit	24 Bit	24 Bit	15 Bit	Bit	16 Bit	16 Bit	Variable Länge	32 Bit
Ziel. Adresse	Typ	BENUTZER	SA	LEN	SNAP LLC	HSA	VLAN	BPDU	INDEX	Reserve	Kapselter Rahmen	FCS
01-00-0c-00-00					AAA03	000000C						

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

802.1Q - Betriebsübersicht

Der IEEE 802.1Q-Standard gibt viel mehr an als Kapselungstypen, einschließlich Spanning Tree-Erweiterungen, GARP (siehe VTP-Abschnitt dieses Dokuments) und 802.1p Quality of Service (QoS)-Tagging.

Das 802.1Q-Frame-Format behält die ursprüngliche Ethernet-Quell- und Zieladresse bei, aber Switches müssen jetzt erwarten, dass Baby-Riant-Frames empfangen werden, auch auf Access-Ports, wo Hosts Tagging verwenden können, um die 802.1p-Benutzerpriorität für die QoS-Signalisierung auszudrücken. Das Tag ist 4 Byte, sodass 802.1Q Ethernet v2-Frames 1522 Byte enthalten, eine Leistung der IEEE 802.3ac-Arbeitsgruppe. 802.1Q unterstützt außerdem Platz für Nummern für 4096 VLANs.

Alle übertragenen und empfangenen Datenframes sind mit 802.1Q-Tags versehen, mit Ausnahme derjenigen im nativen VLAN (es gibt ein implizites Tag, das auf der Konfiguration des Eingangs-Switch-Ports basiert). Frames im nativen VLAN werden immer unmarkiert übertragen und normalerweise unmarkiert empfangen. Sie können jedoch auch getaggt empfangen werden.

Weitere Informationen finden Sie unter VLAN Standardization via IEEE 802.10 und Get IEEE 802 .

802.1Q/801.1p Frame-Format

		Tag-Header						
		TPID	TCI					
48 Bit	48 Bit	16 Bit	3 Bit	1 Bit	12 Bit	16 Bit	Variable Länge	32 Bit
DA	SA	TPID	Priorität	CFI	VLAN-ID	Länge/Typ	Daten mit PAD	FCS
		0 x 8100	0-7	0-1	0-4095			

Empfehlung

Da alle neueren Hardwarekomponenten 802.1Q unterstützen (und einige nur 802.1Q unterstützen, z. B. die Catalyst Serien 4500/4000 und CSS 11000), empfiehlt Cisco, dass alle neuen Implementierungen dem IEEE 802.1Q-Standard folgen und ältere Netzwerke schrittweise von ISL migrieren.

Der IEEE-Standard ermöglicht Anbieterinteroperabilität. Dies ist in allen Cisco Umgebungen von Vorteil, da neue 802.1p-fähige Host-NICs und -Geräte verfügbar werden. Obwohl sowohl die ISL- als auch die 802.1Q-Implementierungen ausgereift sind, wird der IEEE-Standard letztendlich eine größere Außendienstbelastung und eine größere Unterstützung durch Drittanbieter wie die Unterstützung von Netzwerkanalysen aufweisen. Der niedrigere Kapselungsaufwand von 802.1Q im Vergleich zu ISL ist ebenfalls ein kleiner Punkt zugunsten von 802.1Q.

Da der Kapselungstyp zwischen Switches über DTP ausgehandelt wird, wobei ISL standardmäßig als Gewinner ausgewählt wird, wenn beide Enden diese unterstützen, muss dieser Befehl zur Angabe von dot1q ausgeführt werden:

```
set trunk mod/port mode dot1q
```

Wenn VLAN 1 wie im Abschnitt In-Band-Management dieses Dokuments beschrieben aus einem Trunk gelöscht wird, obwohl keine Benutzerdaten übertragen oder empfangen werden, besteht der NMP weiterhin Steuerungsprotokolle wie CDP und VTP in VLAN 1.

Wie im VLAN 1-Abschnitt dieses Dokuments beschrieben, werden CDP-, VTP- und PAgP-Pakete beim Trunking immer in VLAN 1 gesendet. Wenn dot1q-Kapselung verwendet wird, werden diese Steuerungs-Frames mit VLAN 1 gekennzeichnet, wenn das native VLAN des Switches geändert wird. Wenn das dot1q-Trunking zu einem Router aktiviert ist und das native VLAN auf dem Switch geändert wird, wird eine Subschnittstelle in VLAN 1 benötigt, um die getaggten CDP-Frames zu empfangen und CDP-Nachbartransparenz auf dem Router bereitzustellen.

Hinweis: Die implizite Kennzeichnung des nativen VLANs mit dot1q bietet ein potenzielles Sicherheitsrisiko, da Frames von einem VLAN zu einem anderen ohne Router gesendet werden können. Weitere Informationen finden Sie unter Gibt es Schwachstellen in VLAN-Implementierungen? für weitere Informationen. Die Lösung besteht darin, eine VLAN-ID für das native VLAN des Trunks zu verwenden, das nicht für den Endbenutzerzugriff verwendet wird. Die meisten Cisco Kunden verlassen VLAN 1 als natives VLAN auf einem Trunk und weisen anderen VLANs als VLAN 1 Access Ports zu, um dies einfach zu erreichen.

Trunking-Modus

DTP ist die zweite Generation von Dynamic ISL (DISL) und wird implementiert, um sicherzustellen, dass die verschiedenen Parameter, die beim Senden von ISL- oder 802.1Q-Frames involviert sind, wie der konfigurierte Kapselungstyp, natives VLAN und Hardwarefunktionen, von den Switches an beiden Enden eines Trunks vereinbart werden. Dies trägt auch zum Schutz vor nicht-Trunk-Ports bei, die getaggte Frames überfluten, ein potenziell schwerwiegendes Sicherheitsrisiko, da sichergestellt wird, dass sich die Ports und ihre Nachbarn in konsistenten Zuständen befinden.

Überblick

DTP ist ein L2-Protokoll, das Konfigurationsparameter zwischen einem Switch-Port und seinem Nachbarn aushandelt. Es wird eine andere Multicast-MAC-Adresse (**01-00-0c-cc-cc**) und ein SNAP-Protokolltyp von 0x2004 verwendet. Diese Tabelle enthält eine Zusammenfassung der Konfigurationsmodi:

Modus	**Funktion**	**Übertragung von DTP-Frames**	**Endzustand (Lokaler Port)**
`Auto (Standard)`	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
`Ein`	Versetzt den Port in den permanenten Trunking-Modus und versucht über Aushandlungen, den Link in einen Trunk umzuwandeln. Der Port wird zu einem Trunk-Port, selbst wenn der benachbarte Port mit der Änderung nicht einverstanden ist.	Ja, regelmäßig.	Trunking, **bedingungslos**.
`unverh`	Versetzt den Port in	Nein	Trunking,

andeln	den permanenten Trunking-Modus, verhindert jedoch, dass der Port DTP-Frames generiert. Sie müssen den Nachbarport manuell als Trunk-Port konfigurieren, um eine Trunk-Verbindung herzustellen. Dies ist nützlich für Geräte, die kein DTP unterstützen.		**bedingungslos**.
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.
Aus	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 mit der Änderung nicht einverstanden ist.	Nein, im Steady-State, sondern übermittelt Informationen, um die Remote-Enderkennung nach dem Wechsel von On zu beschleunigen.	Nicht-Trunking

Dies sind einige Highlights des Protokolls:

- DTP geht von einer Punkt-zu-Punkt-Verbindung aus, und Cisco Geräte unterstützen nur 802.1Q-Trunk-Ports, die Punkt-zu-Punkt sind.
- Während der DTP-Aushandlung nehmen die Ports nicht am STP teil. Erst nachdem der Port zu einem der drei DTP-Typen (Access, ISL oder 802.1Q) wird, wird der Port dem STP hinzugefügt. Andernfalls wird PAgP, sofern konfiguriert, als nächster Prozess ausgeführt, bevor der Port an STP teilnimmt.
- Wenn der Port im ISL-Modus Trunking durchführt, werden DTP-Pakete in VLAN 1 gesendet.

Andernfalls (für 802.1Q-Trunking- oder Nicht-Trunking-Ports) werden sie im nativen VLAN ausgesendet.
- Im `wünschenswerten` Modus übertragen DTP-Pakete **den VTP-Domänennamen** (der für den Start eines ausgehandelten Trunks übereinstimmen muss) sowie die Trunk-Konfiguration und den **Admin-Status**.
- Nachrichten werden während der Aushandlung alle zwei Sekunden und danach alle 30 Sekunden gesendet.
- Vergewissern Sie sich, dass die Modi `ein`, `nicht verhandeln` und `aus` explizit angeben, in welchem Zustand der Port endet. Eine fehlerhafte Konfiguration kann zu einem gefährlichen/inkonsistenten Zustand führen, bei dem eine Seite Trunking (Trunking) und die andere Seite nicht verwendet.
- Ein Port im `Auto`- oder `im` Modus sendet regelmäßig DTP-Frames. Wenn ein Port im `automatischen` oder `wünschenswerten` Modus in fünf Minuten kein DTP-Paket sieht, wird er auf Non-Trunk festgelegt.

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.

Empfehlung

Cisco empfiehlt eine explizite Trunk-Konfiguration von `wünschenswert` an beiden Enden. In diesem Modus können Netzwerkbetreiber Syslog- und Befehlszeilenstatusmeldungen vertrauen, dass ein Port aktiv ist und Trunking, im Gegensatz `zum` Modus `im` Modus, wodurch ein Port angezeigt wird, auch wenn der Nachbar falsch konfiguriert ist. Darüber hinaus bietet der `wünschenswerte` Modus-Trunk Stabilität in Situationen, in denen eine Seite der Verbindung nicht zu einem Trunk werden kann oder den Trunk-Zustand verwirft. Geben Sie diesen Befehl ein, um den `wünschenswerten` Modus festzulegen:

```
set trunk mod/port desirable ISL | dot1q
```

Hinweis: Legen Sie für alle Nicht-Trunk-Ports `den` Trunk-Modus fest. Dies trägt dazu bei, die vergeudete Verhandlungszeit beim Hochladen der Host-Ports zu vermeiden. Dieser Befehl wird auch ausgeführt, wenn der **Befehl set port host** verwendet wird. Weitere Informationen finden Sie im STP-Abschnitt. Geben Sie diesen Befehl ein, um einen Trunk auf einer Reihe von Ports zu deaktivieren:

```
set trunk port range off
!--- Ports are not trunking; part of the set port host command.
```

Weitere Optionen

Eine andere gängige Kundenkonfiguration verwendet den `erwünschten` Modus nur auf dem Distribution Layer und die einfachste Standardkonfiguration (`automatischer` Modus) auf dem Access Layer.

Einige Switches, wie z. B. Catalyst 2900XL, Cisco IOS-Router oder Geräte anderer Anbieter, unterstützen derzeit keine Trunk-Aushandlung über DTP. Sie können den `UnNegotiate`-Modus für Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000 verwenden, um einen Port für Trunks mit diesen Geräten bedingungslos einzurichten. Dies kann dazu beitragen, eine einheitliche Einstellung im gesamten Campus zu erreichen. Außerdem können Sie den `Nicht-Verhandlung`-Modus implementieren, um die Initialisierungszeit der Verbindung insgesamt zu verkürzen.

Hinweis: Faktoren wie der Kanalmodus und die STP-Konfiguration können sich ebenfalls auf die Initialisierungszeit auswirken.

Geben Sie diesen Befehl ein, um den `nicht`-verhandelnden Modus festzulegen:

```
set trunk mod/port nonegotiate ISL | dot1q
```

Cisco empfiehlt, `nicht zu verhandeln`, wenn eine Verbindung zu einem Cisco IOS-Router besteht, da bei der Bridging-Funktion einige DTP-Frames, die im Modus empfangen werden, wieder in den Trunk-Port zurückkehren können. Beim Empfang des DTP-Frames versucht der Switch-Port, unnötigerweise neu zu verhandeln (oder den Trunk nach unten und nach oben zu bringen). Wenn `Non-Negotiate` aktiviert ist, sendet der Switch keine DTP-Frames.

Spanning Tree Protocol

Grundlegende Überlegungen

Das Spanning Tree Protocol (STP) gewährleistet eine schleifenfreie L2-Umgebung in redundanten Switching- und Bridge-Netzwerken. Ohne STP werden Frames auf unbestimmte Zeit schleifen und/oder multipliziert, was zu einer Netzwerkschmelze führt, da alle Geräte in der Broadcast-Domäne fortlaufend durch hohen Datenverkehr unterbrochen werden.

Obwohl STP in mancher Hinsicht ein ausgereiftes Protokoll ist, das ursprünglich für langsame, softwarebasierte Bridge-Spezifikationen (IEEE 802.1d) entwickelt wurde, kann es komplex sein, große Switch-Netzwerke mit vielen VLANs, vielen Switches in einer Domäne, Unterstützung mehrerer Anbieter und neuere IEEE-Erweiterungen gut zu implementieren.

Für die Zukunft übernimmt CatOS 6.x weiterhin die neue STP-Entwicklung, z. B. MISTP, Loop Guard, Root Guards und BPDU-Erkennung mit schiefer Ankunftszeit. Darüber hinaus sind in CatOS 7.x weitere standardisierte Protokolle verfügbar, wie IEEE 802.1s Shared Spanning Tree und IEEE 802.1w Rapid Convergence Spanning Tree.

Überblick

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.

Anfänglich werden BPDUs von allen Switches gesendet, die die BID jedes Switches und die Pfadkosten für die Verbindung mit diesem Switch enthalten. Dadurch können die Root-Bridge und der kostengünstigste Pfad zum Root bestimmt werden. Zusätzliche Konfigurationsparameter, die in BPDUs vom Root übertragen werden, überschreiben die lokal konfigurierten Parameter, sodass das gesamte Netzwerk konsistente Timer verwendet.

Die Topologie konvergiert dann über die folgenden Schritte:

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

Weitere Informationen finden Sie unter Konfigurieren von Spanning Tree.

Standard-Timer-Standardwerte (Sekunden)	Name	Funktion
2	`Hallo`	Steuert das Senden von BPDUs.
15	`Vorwärtsverzögerung (Fwddelay)`	Steuert die Zeit, die ein Port für das Abhören und Lernen verbringt, und beeinflusst den Prozess der Topologieänderung (siehe nächster Abschnitt).
20	`Max.`	Steuert, wie lange der Switch die aktuelle Topologie aufrechterhält, bevor er nach einem alternativen Pfad sucht. Nach der Maxage-Sekunden gilt eine BPDU als veraltet und der Switch sucht einen neuen Root-Port aus dem Pool blockierter Ports. Wenn kein blockierter Port verfügbar ist, wird behauptet, der Root selbst auf den designierten Ports zu sein.

Hafenstaaten	Bedeutung	Standard-Timing für den nächsten Status
`Deaktiviert`	Administrativ deaktiviert.	K/A
`Sperren`	Empfangen von BPDUs und Stoppen von Benutzerdaten.	Überwachen des Empfangs von BPDUs Warten Sie 20 Sekunden, bis die Max.-Zertifizierung abgelaufen ist oder die Änderung sofort erfolgt, wenn eine direkte/lokale Verbindung ausfällt.
`Zuhöre`	Senden oder	Fwddelay timer (Warten Sie

n	Empfangen von BPDUs, um zu prüfen, ob eine Rückkehr zur Blockierung erforderlich ist.	15 Sekunden)
Lernen	Erstellung der Topologie/CAM-Tabelle.	Fwddelay timer (Warten Sie 15 Sekunden)
Weiterleitung	Senden/Empfangen von Daten.	
	Grundlegende Topologieänderungen gesamt:	**20 + 2 (15) = 50 Sekunden, wenn auf Ablauf des Maxage-Zeitraums gewartet wird, oder 30 Sekunden für Fehler bei Direktverbindungen**

Die beiden BPDU-Typen in STP sind Konfigurations-BPDUs und Topology Change Notification (TCN)-BPDUs.

Konfigurations-BPDU-Fluss

Konfigurations-BPDUs werden jedes Hello-Intervall von jedem Port auf der Root-Bridge bezogen und anschließend an alle Leaf-Switches weitergeleitet, um den Zustand des Spanning Tree aufrechtzuerhalten. Im stationären Zustand ist der BPDU-Fluss unidirektional: Root-Ports und blockierende Ports empfangen nur Konfigurations-BPDUs, während designierte Ports nur Konfigurations-BPDUs senden.

Für jede BPDU, die ein Switch vom Root empfängt, wird ein neuer BPDU vom zentralen Catalyst-NMP verarbeitet und mit den Root-Informationen gesendet. Mit anderen Worten: Wenn die Root-Bridge verloren geht oder alle Pfade zur Root-Bridge verloren gehen, werden BPDUs nicht mehr empfangen (bis der Maxage-Timer mit der Wiederwahl beginnt).

TCN BPDU-Fluss

TCN-BPDUs werden von Leaf-Switches bezogen und fließen zur Root-Bridge, wenn eine Topologieänderung im Spanning Tree erkannt wird. Root-Ports senden nur TCNs, designierte Ports nur TCNs.

Die TCN-BPDU verläuft zum Root-Gradge und wird bei jedem Schritt bestätigt. Dies ist ein zuverlässiger Mechanismus. Wenn die Root Bridge an der Root Bridge ankommt, benachrichtigt die Root Bridge die gesamte Domäne, dass eine Änderung aufgetreten ist, indem sie Konfigurations-BPDUs mit dem TCN-Flag für die **Zeitdauer** **`maxage + fwddelay`** **(**standardmäßig 35 Sekunden) ausgibt. Dies bewirkt, dass alle Switches ihre normale CAM-Alterungszeit von fünf Minuten (standardmäßig) in das durch **fwddelay** festgelegte Intervall ändern **(**standardmäßig 15 Sekunden). Weitere Informationen finden Sie unter Änderungen der Spanning Tree Protocol-Topologie.

Spanning Tree-Modi

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

- Ein einzelner Spanning Tree für alle VLANs oder ein Mono Spanning Tree Protocol wie IEEE 802.1Q
- Spanning Tree pro VLAN oder Shared Spanning Tree wie Cisco PVST
- Spanning Tree pro Set von VLANs oder mehrere Spanning Tree wie Cisco MISTP und IEEE 802.1s

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 ermöglicht den Lastenausgleich, erfordert jedoch mehr BPDU-CPU-Verarbeitung, wenn die Anzahl der VLANs zunimmt. Die CatOS-Versionshinweise enthalten Anleitungen zur Anzahl der für den Spanning Tree pro Switch empfohlenen logischen Ports. Beispielsweise lautet die Catalyst 6500/6000 Supervisor Engine 1-Formel wie folgt:

Anzahl der Ports + (Anzahl der Trunks * Anzahl der VLANs auf Trunks) < 4000

Cisco MISTP und der neue 802.1s-Standard ermöglichen die Definition von nur zwei aktiven STP-Instanzen/-Topologien sowie die Zuordnung aller VLANs zu beiden Strukturen. Mit dieser Technik kann STP auf Tausende von VLANs skaliert werden, während der Lastenausgleich aktiviert ist.

BPDU-Formate

Um den IEEE 802.1Q-Standard zu unterstützen, wurde die bestehende Cisco STP-Implementierung um PVST+ erweitert, indem Tunneling in einer IEEE 802.1Q-Mono-Spanning-Tree-Region unterstützt wurde. PVST+ ist daher mit den Protokollen IEEE 802.1Q MST und Cisco PVST kompatibel und erfordert keine zusätzlichen Befehle oder Konfigurationen. Darüber hinaus bietet PVST+ Überprüfungsmechanismen, um sicherzustellen, dass Port-Trunking und VLAN-IDs nicht in der Konfiguration inkonsistent sind.

Dies sind einige betriebliche Highlights des PVST+-Protokolls:

- PVST+ ist mit 802.1Q-Mono-Spanning-Tree über den so genannten Common Spanning Tree (CST) über einen 802.1Q-Trunk kompatibel. Der CST befindet sich immer im VLAN 1, daher muss dieses VLAN auf dem Trunk aktiviert werden, um mit anderen Anbietern zusammenzuarbeiten. CST-BPDUs werden immer unmarkiert an die IEEE Standard Bridge-Group (MAC-Adresse 01-80-c2-00-00-00, DSAP 42, SSAP 42) übertragen. Um eine vollständige Beschreibung zu erhalten, wird ein paralleler Satz von BPDUs auch an die gemeinsame Spanning Tree-MAC-Adresse von Cisco für VLAN 1 übertragen.
- PVST+ tunnelt PVST-BPDUs in 802.1Q-VLAN-Regionen als Multicast-Daten. Cisco Shared Spanning Tree BPDUs werden an die MAC-Adresse 01-00-0c-cc-cd (SNAP HDLC-Protokolltyp 0x010b) für jedes VLAN auf einem Trunk übertragen. BPDUs sind im nativen VLAN nicht markiert und für alle anderen VLANs gekennzeichnet.
- PVST+ überprüft Port- und VLAN-Inkonsistenzen. PVST+ blockiert Ports, die inkonsistente BPDUs empfangen, um Weiterleitungsschleifen zu verhindern. Außerdem werden Benutzer über Syslog-Meldungen über Konfigurationsfehler benachrichtigt.
- PVST+ ist abwärtskompatibel mit vorhandenen Cisco Switches, auf denen PVST auf ISL-Trunks ausgeführt wird. ISL-gekapselte BPDUs werden weiterhin mithilfe der IEEE MAC-Adresse übertragen oder empfangen. Mit anderen Worten: Jeder BPDU-Typ ist "link-local". Es gibt keine Übersetzungsprobleme.

Empfehlung

Bei allen Catalyst-Switches ist STP standardmäßig aktiviert. Dies wird empfohlen, auch wenn ein Design gewählt wird, das keine L2-Schleifen enthält, sodass STP nicht aktiviert ist, da es aktiv einen blockierten Port aufrechterhält.

```
set spantree enable all
!--- This is the default.
```

Cisco empfiehlt, STP aus folgenden Gründen weiterhin zu aktivieren:

- Wenn eine Schleife (verursacht durch falsche Patches, fehlerhafte Kabel usw.) vorhanden ist, verhindert STP schädliche Auswirkungen auf das Netzwerk, die durch Multicast- und Broadcast-Daten verursacht werden.
- Schutz vor Ausfall eines EtherChannels.
- Die meisten Netzwerke sind mit STP konfiguriert, wodurch eine maximale Feldbelegung erreicht wird. Eine höhere Exposition entspricht im Allgemeinen einem stabilen Code.
- Schutz vor doppelten NIC-Fehlverhalten (oder Bridging aktiviert auf Servern).
- Die Software für viele Protokolle (wie PAgP, IGMP-Snooping und Trunking) ist eng mit STP verknüpft. Wenn Sie ohne STP arbeiten, kann dies zu unerwünschten Ergebnissen führen.

Ändern Sie keine Timer, 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-interval und Maxage), bestehen selbst aus einem komplexen Satz von anderen angenommenen und systeminternen Timern. Daher ist es schwierig, Timer zu optimieren und alle Auswirkungen zu berücksichtigen. Darüber hinaus besteht die Gefahr, den UDLD-Schutz zu untergraben.

Im Idealfall sollten Sie den Benutzerdatenverkehr vom Management-VLAN fernhalten. Insbesondere bei älteren Catalyst Switch-Prozessoren ist es am besten, STP-Probleme zu vermeiden, indem das Management-VLAN von den Benutzerdaten getrennt bleibt. Eine fehlerhafte Endstation könnte den Supervisor Engine-Prozessor so stark mit Broadcast-Paketen belasten, dass eine oder mehrere BPDUs übersehen werden können. Neuere Switches mit leistungsfähigeren CPUs und Drosselungssteuerungen entlasten diese Überlegungen. Weitere Informationen finden Sie im Abschnitt In-Band-Management dieses Dokuments.

Vermeiden Sie übermäßige Redundanz. Dies kann zu einem Albtraum bei der Fehlerbehebung führen - zu viele blockierende Ports wirken sich negativ auf die langfristige Stabilität aus. **Den gesamten SPT-Durchmesser unter sieben Hops halten**. Versuchen Sie, das Cisco Multilayer-Modell mit kleineren Switched-Domänen, STP-Dreiecken und deterministischen blockierten Ports (wie in Gigabit Campus Network Design - Prinzipien und Architektur) erklärt zu entwerfen.

Beeinflussung und Ermitteln von Root-Funktionen und blockierten Ports und Dokumentieren dieser Funktionen im Topologiediagramm. An den blockierten Ports beginnt die STP-Fehlerbehebung. Was sie von der Blockierung zur Weiterleitung veranlasst hat, ist häufig der zentrale Bestandteil der Ursachenanalyse. **Wählen Sie die Distribution-Layer und die Core-Layer als Speicherort für Root/sekundäre Root**, da diese als die stabilsten Teile des Netzwerks gelten. Überprüfen Sie, ob das L3- und HSRP-Overlay mit L2-Datenweiterleitungspfaden optimal ist. Dieser Befehl ist ein Makro, das die Bridge-Priorität konfiguriert. root setzt es viel niedriger als der Standardwert (32768), während root sekundär deutlich niedriger als der Standardwert ist:

```
set spantree root secondary vlan range
```

Hinweis: Dieses Makro legt die Root-Priorität entweder auf 8192 (standardmäßig), auf die aktuelle Root-Priorität minus 1 (wenn eine andere Root-Bridge bekannt ist) oder auf die aktuelle Root-Priorität fest (wenn ihre MAC-Adresse niedriger ist als der aktuelle Root).

Vermeidung unnötiger VLANs von Trunk-Ports (bidirektionale Übung) 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. Weitere Informationen finden Sie im VTP-Abschnitt dieses Dokuments. Das Standard-VLAN 1 kann auch mit CatOS 5.4 und höher aus Trunks entfernt werden.

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

Weitere Optionen

Cisco verfügt über ein weiteres STP, das **als VLAN-Bridge** bezeichnet wird. Dieses Protokoll verwendet die MAC-Zieladresse **01-00-0c-cd-cd-ce** und den Protokolltyp 0x010c.

Dies ist besonders nützlich, wenn nicht routbare oder veraltete Protokolle zwischen VLANs überbrückt werden müssen, ohne dass die auf diesen VLANs ausgeführte(n) IEEE Spanning Tree-Instanz(n) beeinträchtigt wird. Wenn VLAN-Schnittstellen für nicht überbrückten Datenverkehr für L2-Datenverkehr blockiert werden (und dies könnte problemlos passieren, wenn sie am selben STP wie IP-VLANs beteiligt sind), wird auch der überlagerte L3-Datenverkehr versehentlich abgeschnitten - ein unerwünschter Nebeneffekt. VLAN-Bridge ist daher eine separate STP-Instanz für überbrückte Protokolle, die eine separate Topologie bereitstellt, die ohne Beeinträchtigung des IP-Datenverkehrs bearbeitet werden kann.

Cisco empfiehlt, VLAN-Bridge auszuführen, wenn eine Bridging-Funktion zwischen VLANs auf Cisco Routern wie der MSFC erforderlich ist.

PortFast

PortFast wird verwendet, um den normalen Spanning Tree-Vorgang an Zugriffsports zu umgehen, um die Verbindungen zwischen Endstationen und den Diensten, mit denen sie nach der Verbindungsinitialisierung eine Verbindung herstellen müssen, zu beschleunigen. Bei einigen Protokollen wie IPX/SPX ist es wichtig, den Access-Port unmittelbar nach dem Verbindungsstatus im Weiterleitungsmodus zu sehen, um GNS-Probleme zu vermeiden.

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

Überblick

PortFast überspringt die normalen `Überwachungs`- und `Lernstatus` von STP, indem ein Port direkt von der `Blockierung` in den `Weiterleitungsmodus` verschoben wird, nachdem die Verbindung bekanntermaßen ausgeführt wird. Wenn diese Funktion nicht aktiviert ist, verwirft STP alle Benutzerdaten, bis er entscheidet, dass der Port in den `Weiterleitungsmodus` verschoben werden

kann. Dies kann die doppelte `ForwardDelay`-Zeit dauern (standardmäßig insgesamt 30 Sekunden).

Der PortFast-Modus verhindert außerdem, dass eine STP-TCN jedes Mal generiert wird, wenn ein Portstatus von `Lernen` zu `Weiterleitung` wechselt. TCNs sind an sich kein Problem, aber wenn eine Welle von TCNs die Root Bridge erreicht (in der Regel morgens, wenn die Benutzer ihre PCs einschalten), kann dies die Konvergenzzeit unnötigerweise verlängern.

STP PortFast ist sowohl in Multicast-CGMP- als auch in Catalyst 5500/5000-MLS-Netzwerken besonders wichtig. TCNs in diesen Umgebungen können dazu führen, dass die Einträge der statischen CGMP-CAM-Tabelle veraltet werden. Dies führt zum Verlust von Multicast-Paketen bis zum nächsten IGMP-Bericht und/oder zum Löschen von MLS-Cache-Einträgen, die dann neu erstellt werden müssen und je nach Cache-Größe zu einer CPU-Spitze des Routers führen können. (Catalyst 6500/6000 MLS-Implementierungen und Multicast-Einträge, die aus IGMP-Snooping gelernt wurden, sind davon nicht betroffen.)

Empfehlung

Cisco empfiehlt, STP PortFast für alle aktiven Host-Ports zu aktivieren und für Switch-Switch-Verbindungen und nicht verwendete Ports zu deaktivieren.

Trunking und Channeling müssen auch für alle Host-Ports deaktiviert werden. Jeder Access-Port ist standardmäßig für Trunking und Channeling aktiviert, jedoch werden Switch-Nachbarn für Host-Ports nicht erwartet. Werden diese Protokolle ausgehandelt, kann die spätere Verzögerung bei der Port-Aktivierung zu unerwünschten Situationen führen, in denen die ursprünglichen Pakete von Workstations, z. B. DHCP-Anfragen, nicht weitergeleitet werden.

CatOS 5.2 führte einen Makrobefehl ein, der den **Port-Host-*Portbereich* festlegt**, der diese Konfiguration für Access-Ports implementiert und die Automatisierung und Verbindungsleistung erheblich unterstützt:

```
set port host port range
!--- Macro command for these commands: set spantree portfast port range enable set trunk port
range off set port channel port range mode off
```

Hinweis: PortFast bedeutet nicht, dass Spanning Tree auf diesen Ports überhaupt nicht ausgeführt wird. BPDUs werden weiterhin gesendet, empfangen und verarbeitet.

Weitere Optionen

PortFast BPDU-Guard bietet eine Möglichkeit, Schleifen zu verhindern, indem ein Nicht-Trunking-Port in einen `errdisable`-Zustand verschoben wird, wenn an diesem Port eine BPDU empfangen wird.

Ein BPDU-Paket darf nie an einem für PortFast konfigurierten Zugriffsport empfangen werden, da Host-Ports nicht an Switches angeschlossen werden dürfen. Wenn eine BPDU beobachtet wird, weist dies auf eine ungültige und möglicherweise gefährliche Konfiguration hin, die administrative Maßnahmen erfordert. Wenn die BPDU-Guard-Funktion aktiviert ist, deaktiviert Spanning Tree für PortFast konfigurierte Schnittstellen, die BPDUs empfangen, statt sie in den STP-`Blockierungsstatus` zu versetzen.

Der Befehl funktioniert auf Switch-Basis, nicht auf Port-Basis, wie gezeigt:

```
set spantree portfast bpdu-guard enable
```

Der Netzwerkmanager wird über ein SNMP-Trap oder eine Syslog-Meldung benachrichtigt, wenn der Port ausfällt. Es ist auch möglich, eine automatische Wiederherstellungszeit für deaktivierte Ports zu konfigurieren. Weitere Informationen finden Sie im Abschnitt UDLD dieses Dokuments. Weitere Informationen finden Sie unter Spanning Tree Portfast BPDU Guard Enhancement.

Hinweis: PortFast für Trunk-Ports wurde in CatOS 7.x eingeführt und hat in früheren Versionen keine Auswirkungen auf Trunk-Ports. PortFast für Trunk-Ports wurde zur Erhöhung der Konvergenzzeiten für L3-Netzwerke entwickelt. Ergänzend zu dieser Funktion hat CatOS 7.x auch die Möglichkeit eingeführt, PortFast BPDU-Guard auf Port-Basis zu konfigurieren.

UplinkFast

UplinkFast bietet schnelle STP-Konvergenz nach einem direkten Verbindungsausfall auf der Netzwerkzugriffs-Ebene. STP wird nicht geändert, und der Zweck besteht darin, die Konvergenzzeit in einem bestimmten Fall auf weniger als drei Sekunden zu beschleunigen, anstatt auf die typische Verzögerung von 30 Sekunden. Weitere Informationen finden Sie unter Understanding and Configuring the Cisco Uplink Fast Feature for more information.

Überblick

Wenn der Forwarding-Uplink über das Cisco Multilayer-Designmodell auf dem Access Layer verloren geht, wird der blockierende Uplink sofort in einen `Weiterleitungsstatus` verschoben, ohne auf `Zuhören` und `Lernstatus` zu warten.

Eine Uplink-Gruppe besteht aus einer Reihe von Ports pro VLAN, die als Root-Port und Backup-Root-Port angesehen werden 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 eine typische Konvergenzverzögerung von 30 Sekunden durchlaufen werden muss.

Da dadurch der normale Prozess zur Handhabung von STP-Topologieänderungen (`Abhören` und `Lernen`) effektiv umgangen wird, ist ein alternativer Mechanismus zur Topologiekorrektur erforderlich, um Switches in der Domäne zu aktualisieren, die lokale Endstationen über einen alternativen Pfad erreichen können. Der Access-Layer-Switch, auf dem UplinkFast ausgeführt wird, generiert auch Frames für jede MAC-Adresse im CAM zu einer Multicast-MAC-Adresse (01-00-0c-cd-cd-cd, HDLC-Protokoll 0x200a), um die CAM-Tabelle in allen Switches in der Domäne mit der neuen Topologie zu aktualisieren.

Empfehlung

Cisco empfiehlt, UplinkFast für Switches mit blockierten Ports, in der Regel auf dem Access Layer, zu aktivieren. Nicht auf Switches verwenden, ohne über die implizierte Topologie eines Backup-Root-Links zu verfügen - in der Regel Distribution-Switches und Core-Switches im Cisco Multilayer-Design. Sie kann ohne Unterbrechung zu einem Produktionsnetzwerk hinzugefügt werden. Geben Sie diesen Befehl ein, um UplinkFast zu aktivieren:

```
set spantree uplinkfast enable
```

Mit diesem Befehl wird auch die **Bridge-Priorität** hoch gesetzt, um das Risiko zu minimieren, dass diese zu einer Root-Bridge wird und die **Port-Priorität** hoch ist, um zu einem designierten Port zu werden, der die Funktionalität beeinträchtigt. Wenn Sie einen Switch wiederherstellen, der UplinkFast aktiviert hat, muss die Funktion deaktiviert, die Uplink-Datenbank mit "clear uplink" gelöscht und die Bridge-Prioritäten manuell wiederhergestellt werden.

Hinweis: Das Schlüsselwort **aller Protokolle** für den UplinkFast-Befehl wird benötigt, wenn die Protokollfilterfunktion aktiviert ist. Wenn der CAM den Protokolltyp sowie MAC- und VLAN-Informationen aufzeichnet, wenn die Protokollfilterung aktiviert ist, muss für jedes Protokoll an jeder MAC-Adresse ein UplinkFast-Frame generiert werden. Das **rate**-Schlüsselwort gibt die Pakete pro Sekunde der Uplinkfast Topology Update Frames an. Die Standardeinstellung wird empfohlen. BackboneFast muss nicht mit Rapid STP (RSTP) oder IEEE 802.1w konfiguriert werden, da der Mechanismus nativ enthalten ist und automatisch im RSTP aktiviert wird.

BackboneFast

BackboneFast ermöglicht eine schnelle Konvergenz bei indirekten Verbindungsausfällen. Dank der zusätzlichen Funktionen für STP können Konvergenzzeiten in der Regel von der Standardeinstellung von 50 Sekunden auf 30 Sekunden reduziert werden.

Überblick

Der Mechanismus wird initiiert, wenn ein Root-Port oder ein blockierter Port eines Switches unterlegene BPDUs von seiner designierten Bridge empfängt. Dies kann auftreten, wenn ein Downstream-Switch seine Verbindung zum Root verloren hat und beginnt, eigene BPDUs zu senden, 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 standardmäßig unterlegene BPDUs für die konfigurierte maximale Alterungszeit, 20 Sekunden. Bei BackboneFast sieht der Switch die untergeordnete BPDU jedoch als Signal, dass sich die Topologie hätte ändern können, und versucht, mithilfe von RLQ-BPDUs (Root Link Query) zu ermitteln, ob ein alternativer Pfad zur Root-Bridge vorhanden ist. Durch diese Protokollerweiterung kann ein Switch überprüfen, ob der Root noch verfügbar ist, einen `blockierten` Port in kürzerer Zeit an die `Weiterleitung` verschieben und den isolierten Switch, der die untergeordnete BPDU gesendet hat, darüber informieren, dass der Root noch vorhanden ist.

Dies sind einige Highlights der Protokolloperation:

- Ein Switch überträgt das RLQ-Paket nur über den Root-Port (d. h. zur Root-Bridge).
- Ein Switch, der einen RLQ empfängt, kann entweder antworten, wenn er der Root-Switch ist, oder wenn er weiß, dass er die Verbindung zum Root verloren hat. Wenn er diese Fakten nicht kennt, muss er die Abfrage über den Root-Port weiterleiten.
- Wenn ein Switch die Verbindung zum Root verloren hat, muss er 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, wird sie verworfen.

Die STP-Konvergenzzeiten können daher um bis zu 20 Sekunden reduziert werden, da die Max. nicht ablaufen muss.

Weitere Informationen finden Sie unter Understanding and Configuring Backbone Fast on Catalyst Switches.

Empfehlung

Cisco empfiehlt, BackboneFast auf allen Switches zu aktivieren, auf denen STP ausgeführt wird. Sie kann ohne Unterbrechung zu einem Produktionsnetzwerk hinzugefügt werden. Geben Sie diesen Befehl ein, um BackboneFast zu aktivieren:

```
set spantree backbonefast enable
```

Hinweis: Dieser globale Befehl muss auf allen Switches in einer Domäne konfiguriert werden, da er dem STP-Protokoll Funktionen hinzufügt, die alle Switches verstehen müssen.

Weitere Optionen

BackboneFast wird auf 2900XLs und 3500s nicht unterstützt. Sie darf nicht aktiviert werden, wenn die Switch-Domäne neben den Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000 diese Switches enthält.

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

Spanning Tree Loop Guard

Loop Guard ist eine proprietäre STP-Optimierung von Cisco. Loop Guard schützt L2-Netzwerke vor Schleifen, die durch Folgendes verursacht werden:

- Netzwerkschnittstellen, die fehlerhaft sind
- Besetzt-CPUs
- Alles, was die normale Weiterleitung von BPDUs verhindert

Eine STP-Schleife tritt ein, wenn ein blockierender Port in einer redundanten Topologie irrtümlicherweise in den Weiterleitungsstatus wechselt. Dieser Übergang erfolgt in der Regel, weil einer der Ports in einer physisch redundanten Topologie (nicht notwendigerweise der blockierende Port) keine BPDUs mehr empfängt.

Loop Guard ist nur in Switched Networks nützlich, wo Switches über Point-to-Point-Verbindungen verbunden werden. Die meisten modernen Campus- und Rechenzentrumsnetzwerke sind solche Netzwerke. Auf einer Punkt-zu-Punkt-Verbindung kann eine designierte Bridge nur dann verschwinden, wenn sie eine unterlegene BPDU sendet oder die Verbindung herunterfährt. Die STP-Loop Guard-Funktion wurde in CatOS 6.2(1) für Catalyst 4000- und Catalyst 5000-Plattformen und in Version 6.2(2) für die Catalyst 6000-Plattform 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 der Port 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 das STP bestimmt den Port-Status, da eine solche Wiederherstellung automatisch erfolgt.

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 wenn die STP-Timer eingestellt werden. Aus diesen Gründen implementieren Sie Loop Guard in Verbindung mit UDLD in Topologien, die auf STP basieren und in denen die Software die Funktionen unterstützt.

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

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated
in VLAN 77. Moved to root-inconsistent state.
```

Wenn die BPDU an einem Port in einem schleifeninkonsistenten STP-Status empfangen wird, wechselt der Port in einen anderen STP-Status. Entsprechend der empfangenen BPDU erfolgt die Wiederherstellung automatisch, ohne dass ein Eingreifen erforderlich ist. Nach der Wiederherstellung wird diese Meldung protokolliert.

```
SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```

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 der Root-Port oder ein alternativer Port ist. Diese Funktionen schließen sich gegenseitig aus. Loop Guard und Root Guard können 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, setzt 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. Der Empfang einer unterlegenen BPDU, die von einer designierten Bridge stammt, löst BackboneFast aus. Da BPDUs von dieser Verbindung empfangen werden, wird Loop Guard nicht aktiviert, sodass BackboneFast und Loop Guard kompatibel sind.
- **PortFast**PortFast wechselt einen Port unmittelbar nach der Verbindung in den designierten Weiterleitungsstatus. Da ein PortFast-fähiger Port kein Root- oder Alternativport sein kann, 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, kompatible Konfigurationen aufweisen. PAgP erzwingt die einheitliche Konfiguration von Loop Guard auf

allen physischen Ports, um einen Kanal zu bilden.**Hinweis:** Dies sind Vorbehalte, wenn Sie Loop Guard 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 Ports, die bereits von Loop Guard blockiert wurden, gruppiert werden, um einen Kanal zu bilden, verliert STP alle Statusinformationen für diese Ports. Der neue Channel-Port kann 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 der festgelegten Rolle erreichen, selbst wenn eine oder mehrere der Verbindungen, aus denen der Kanal besteht, unidirektional sind.In den letzten beiden Fällen in dieser Liste besteht die Möglichkeit einer Schleife, bis UDLD den Ausfall erkennt. Aber Loop Guard ist nicht in der Lage, die Schleife zu erkennen.

Loop Guard- und UDLD-Funktionen im Vergleich

Die Loop Guard-Funktionalität und die UDLD-Funktionalität überschneiden sich teilweise. Beide schützen vor STP-Ausfällen, die durch unidirektionale Links verursacht werden. Diese beiden Merkmale unterscheiden sich jedoch sowohl im Problemlösungsansatz als auch im Hinblick auf die Funktionalität. Insbesondere gibt es bestimmte 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. Falls die Verbindung seit der Verbindung unidirektional erfolgt, empfängt der Port niemals BPDUs und wird designiert. Dieses Verhalten kann normal sein, sodass Loop Guard diesen speziellen Fall nicht abdeckt. UDLD bietet Schutz vor einem solchen Szenario.

Aktivieren Sie UDLD und Loop Guard, um ein Höchstmaß an Schutz zu gewährleisten. Erweiterungen des Spanning Tree Protocol unter Verwendung von Loop Guard- und BPDU Skew-Erkennungsfunktionen für einen Loop Guard- und UDLD-Funktionsvergleich finden Sie im Abschnitt "Loop Guard vs. Unidirectional Link Detection" (*Loop-Guard- und Unidirectional Link Detection)*.

Empfehlung

Cisco empfiehlt die globale Aktivierung von Loop Guard in einem Switch-Netzwerk mit physischen Schleifen. In Version 7.1(1) der Catalyst-Software und höher können Sie Loop Guard global auf allen Ports aktivieren. Tatsächlich ist diese Funktion für alle Point-to-Point-Verbindungen aktiviert. Der Duplexstatus der Verbindung erkennt die Point-to-Point-Verbindung. Wenn die Duplexeinheit voll ist, wird die Verbindung als Punkt-zu-Punkt betrachtet. Geben Sie diesen Befehl ein, um Global Loop Guard zu aktivieren:

```
set spantree global-default loopguard enable
```

Weitere Optionen

Bei Switches, die keine globale Loop Guard-Konfiguration unterstützen, aktivieren Sie die Funktion auf allen einzelnen Ports, einschließlich Port-Channel-Ports. Obwohl die Aktivierung von Loop Guard auf einem designierten Port keine Vorteile bringt, stellt diese Aktivierung kein Problem dar. 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. Geben Sie diesen Befehl ein, um Loop Guard zu aktivieren:

```
set spantree guard loop mod/port
```

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. Um schleifenfreie Topologien zu erstellen und Probleme mit der Netzwerkisolierung zu vermeiden, müssen Sie mit diesen Befehlen Loop Guard global oder einzeln deaktivieren. Aktivieren Sie kein Loop Guard für gemeinsam genutzte Links.

- ```
  set spantree global-default loopguard disable
  !--- This is the global default.
  ```
  oder
- ```
  set spantree guard none mod/port
  !--- This is the default port 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 Root Guard die Position der Root-Bridge. Root Guard ist in CatOS für Catalyst 29xx, 4500/4000, 5500/5000 und 6500/6000 in Software-Version 6.1.1 und höher verfügbar.

Überblick

Root Guard ist ein integrierter STP-Mechanismus. Root Guard hat keinen eigenen Timer und verlässt sich nur auf den Empfang von BPDU. Wenn Root Guard auf einen Port angewendet wird, lässt Root Guard nicht zu, dass ein Port ein Root-Port wird. 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 Root-Inkonsistent-Status versetzt. Diese Syslog-Meldung zeigt die Aktion an:

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated
in VLAN 77. Moved to root-inconsistent state
```

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 schließlich zum Status

"Forwarding" (Weiterleitung). Die Wiederherstellung erfolgt automatisch, und es ist kein menschliches Eingreifen erforderlich. Diese Syslog-Meldung enthält ein Beispiel:

```
%SPANTREE-2-ROOTGUARDUNBLOCK: Port 1/1 restored in VLAN 77
```

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

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

Empfehlung

Cisco empfiehlt, die Root Guard-Funktion an Ports zu aktivieren, die mit Netzwerkgeräten verbunden sind, die nicht direkt von der Verwaltung kontrolliert werden. Führen Sie folgenden Befehl aus, um Root Guard zu konfigurieren:

```
set spantree guard root mod/port
```

EtherChannel

EtherChannel-Technologien ermöglichen das umgekehrte Multiplexing mehrerer Kanäle (bis zu acht auf Catalyst 6500/6000) in einer einzigen logischen Verbindung. Obwohl sich die einzelnen Plattformen bei der Implementierung von der nächsten unterscheiden, ist es wichtig, die allgemeinen Anforderungen zu verstehen:

- Ein Algorithmus, um Frames statistisch über mehrere Kanäle zu multiplizieren
- Erstellung eines logischen Ports, sodass eine einzelne STP-Instanz ausgeführt werden kann
- Ein Channel-Managementprotokoll wie PAgP oder Link Aggregation Control Protocol (LACP)

Frame-Multiplexing

Der EtherChannel umfasst einen Algorithmus zur Frame-Verteilung, der Frames effizient über die Komponenten 10/100- oder Gigabit-Verbindungen hinweg multipliziert. 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 Channel-Steuerungsprotokolle. 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.

Hinweis: Diese Informationen müssen berücksichtigt werden:

- Der Catalyst 6500/600 verfügt über eine neuere Switching-Hardware als der Catalyst 5500/5000 und kann IP-Layer-4 (L4)-Informationen mit Leitungsgeschwindigkeit lesen, um eine intelligentere Multiplexing-Entscheidung zu treffen als einfache MAC-L2-Informationen.

- Die Funktionen des Catalyst 5500/5000 hängen vom Vorhandensein eines Ethernet Bundling Chip (EBC) auf dem Modul ab. Der Befehl **show port functions *mod/port*** command bestätigt, was für jeden Port möglich ist.

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

Plattform	Channel Load Balancing-Algorithmus
Catalyst Serie 5500/5000	Mit einem Catalyst 5500/500 mit den erforderlichen Modulen können pro FEC[1] zwei bis vier Links vorhanden sein, die sich jedoch im gleichen Modul befinden müssen. Die Quell- und Ziel-MAC-Adresspaare bestimmen den für die Frame-Weiterleitung gewählten Link. Ein X-OR-Vorgang wird für die mindestens zwei Bits der Quell-MAC-Adresse und der Ziel-MAC-Adresse durchgeführt. Dieser Vorgang führt zu einem von vier Ergebnissen: (0 0), (0 1), (1 0) oder (1 1). Jeder dieser Werte verweist auf einen Link im FEC-Paket. Bei einem Fast EtherChannel mit zwei Ports wird bei der X-OR-Operation nur ein Bit verwendet. Es kann vorkommen, dass eine Adresse im Quell-/Zielpaar eine Konstante ist. Das Ziel kann beispielsweise ein Server oder, noch wahrscheinlicher, ein Router sein. In diesem Fall wird ein statistischer Lastenausgleich gesehen, da die Quelladresse immer unterschiedlich ist.
Catalyst Serie 4500/4000	Der Catalyst 4500/4000 EtherChannel verteilt Frames über die Verbindungen in einem Kanal (auf einem einzelnen Modul), basierend auf den Bits der Quell- und Ziel-MAC-Adressen der einzelnen Frames in niedriger Reihenfolge. Im Vergleich zum Catalyst 5500/5000 ist der Algorithmus stärker beteiligt und verwendet einen deterministischen Hash dieser Felder der MAC DA (Bytes 3, 5, 6), SA (Bytes 3, 5, 6), Eingangsport und VLAN-ID. Die Frame-Verteilungsmethode ist nicht konfigurierbar.
Catalyst Serie 6500/6000	Je nach Supervisor Engine-Hardware gibt es zwei mögliche Hash-Algorithmen. Bei dem Hash handelt es sich um ein in der Hardware implementiertes Polynom mit siebzehnter Stufe, das in allen Fällen die MAC-Adresse, die IP-Adresse oder die IP-TCP/UDP[2]-Portnummer verwendet und den Algorithmus zur Generierung eines Drei-Bit-Werts anwendet. Dies wird für Quell- und Zieladressen separat durchgeführt. Die Ergebnisse sind dann XORd, um einen weiteren 3-Bit-Wert zu generieren, der verwendet wird, um zu bestimmen, welcher Port im Channel für die Weiterleitung des Pakets verwendet wird. Die Kanäle des Catalyst 6500/6000 können zwischen den Ports eines beliebigen Moduls gebildet werden und können bis

	zu 8 Ports umfassen.

[1] FEC = Fast EtherChannel

[2] UDP = User Datagram Protocol

Diese Tabelle zeigt die von den verschiedenen Catalyst 6500/6000 Supervisor Engine-Modellen unterstützten Verteilungsmethoden und deren Standardverhalten.

Hardware	Beschreibung	Verteilungsmethoden
WS-F6020 (L2-Modul)	Frühzeitige Supervisor Engine 1	L2-MAC: SA; DA; SA und DA
WS-F6020A (L2-Engine) WS-F6K-PFC (L3-Engine)	Später Supervisor Engine 1 und Supervisor Engine 1A/PFC1	L2-MAC: SA; DA; SA & DA L3 IP: SA; DA; SA und DA (Standard)
WS-F6K-PFC2	Supervisor Engine 2/PFC2 (benötigt CatOS 6.x)	L2-MAC: SA; DA; SA & DA L3 IP: SA; DA; SA & DA (Standard) L4-Sitzung: S-Hafen; D-Port; S & D-Port (Standard)
WS-F6K-PFC3BXL WS-F6K-PFC3B WS-F6K-PFC3A	Supervisor Engine 720/PFC3A (benötigt CatOS 8.1.x) Supervisor Engine 720/Supervisor Engine 32/PFC3B (benötigt CatOS 8.4.x) Supervisor Engine 720/PFC3BXL (benötigt CatOS 8.3.x)	L2-MAC: SA; DA; SA & DA L3 IP: SA; DA; SA & DA (Standard) L4-Sitzung: S-Hafen; D-Port; IP-VLAN-L4-Sitzung mit S- und D-Port: SA- und VLAN- und S-Port; DA- & VLAN- & D-Port; SA- und DA- und VLAN- sowie S-Port und D-Port

Hinweis: Bei der L4-Distribution verwendet das erste fragmentierte Paket die L4-Distribution. Alle nachfolgenden Pakete verwenden die L3-Distribution.

Weitere Informationen zur Unterstützung von EtherChannel auf anderen Plattformen sowie zur Konfiguration und Fehlerbehebung finden Sie in den folgenden Dokumenten:

- Grundlegendes zum EtherChannel-Lastenausgleich und zur Redundanz auf Catalyst-Switches

- Konfigurieren Sie den EtherChannel zwischen Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000, die CatOS-Systemsoftware ausführen
- Konfigurieren von LACP (802.3ad) zwischen einem Catalyst 6500/6000 und einem Catalyst 4500/4000
- Konfigurieren von Layer-3- und Layer-2-EtherChannel

Empfehlung

Catalyst Switches der Serien 6500/6000 führen standardmäßig einen Lastenausgleich über IP-Adressen durch. Dies wird in CatOS 5.5 empfohlen, unter der Annahme, dass IP das vorherrschende Protokoll ist. Geben Sie diesen Befehl ein, um den Lastenausgleich festzulegen:

```
set port channel all distribution ip both
!--- This is the default.
```

Die Frame-Verteilung der Catalyst Serien 4500/4000 und 5500/5000 über eine L2-MAC-Adresse ist in den meisten Netzwerken akzeptabel. Dieselbe Verbindung wird jedoch für den gesamten Datenverkehr verwendet, wenn nur zwei Hauptgeräte über einen Kanal kommunizieren (da SMAC und DMAC konstant sind). Dies kann in der Regel ein Problem bei der Serversicherung und anderen großen Dateiübertragungen oder bei der Übertragung eines Segments zwischen zwei Routern sein.

Obwohl der logische Aggregation Port (Agent) als separate Instanz von SNMP verwaltet werden kann und aggregierte Durchsatzstatistiken erfasst werden, empfiehlt Cisco weiterhin, jede physische Schnittstelle separat zu verwalten, um zu überprüfen, wie die Frame-Verteilungsmechanismen funktionieren und ob ein statistischer Lastenausgleich erreicht wird.

Mit dem Befehl show channel traffic kann in CatOS 6.x die prozentuale Verteilungsstatistik einfacher angezeigt werden, als wenn Sie einzelne Port-Zähler mit dem Befehl show counter mod/port oder dem Befehl show mac *mod/port* in CatOS 5.x überprüfen. Mit einem anderen neuen Befehl, dem Befehl show channel hash (Hash anzeigen) **in CatOS 6.x können Sie anhand des Verteilungsmodus überprüfen, welcher Port als ausgehender Port für bestimmte Adressen und/oder Portnummern ausgewählt wird.** Entsprechende Befehle für LACP-Kanäle sind der **Befehl** show lacp-channel traffic und der **Befehl** show lacp-channel hash.

Weitere Optionen

Dies sind mögliche Schritte, wenn die relativen Einschränkungen von MAC-basierten Algorithmen auf Catalyst 4500/4000- oder Catalyst 5500/5000-MAC-Systemen ein Problem darstellen und kein guter statistischer Lastenausgleich erreicht wird:

- Catalyst Switches der Serien 6500/6000 mit Point-Bereitstellung
- Erhöhen Sie die Bandbreite ohne Kanalisierung, indem Sie beispielsweise von mehreren FE-Ports auf einen GE-Port oder von mehreren GE-Ports auf einen 10 GE-Port umschalten.
- Adressieren von Paaren von Endstationen mit großen Datenflüssen
- Bereitstellung dedizierter Links/VLANs für Geräte mit hoher Bandbreite

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. Befolgen Sie die Richtlinien, um Probleme bei der Bündelung zu vermeiden. Wenn z. B. QoS aktiviert ist, bilden EtherChannels bei der Bündelung von Switching-Modulen der Catalyst 6500-/6000-Serie mit unterschiedlichen QoS-Funktionen keine Form. In der Cisco IOS-Software können Sie die QoS-Port-Attributprüfung bei der EtherChannel-Bündelung mit dem **Schnittstellenbefehl** no mls qos channel-consistency**-port-channel** deaktivieren. Ein entsprechender Befehl zum Deaktivieren der QoS-Port-Attributprüfung ist in CatOS nicht verfügbar. Um die QoS-Portfunktion anzuzeigen und festzustellen, ob die Ports kompatibel sind, können Sie den Befehl show port feature *mod/port* ausführen.

Befolgen Sie diese Richtlinien für verschiedene Plattformen, um Konfigurationsprobleme zu vermeiden:

- Der Abschnitt *"EtherChannel-Konfigurationsrichtlinien"* zur Konfiguration des EtherChannels (Catalyst 6500/6000)
- Der Abschnitt *"EtherChannel-Konfigurationsrichtlinien und -einschränkungen"* zur Konfiguration von Fast EtherChannel und Gigabit EtherChannel (Catalyst 4500/4000)
- Der Abschnitt *"EtherChannel-Konfigurationsrichtlinien und -einschränkungen"* zur Konfiguration von Fast EtherChannel und Gigabit EtherChannel (Catalyst 5000)

Hinweis: Die maximale Anzahl der vom Catalyst 4000 unterstützten Port-Channels beträgt 126. Mit den Software-Versionen 6.2(1) und früher unterstützen die Catalyst Switches der Serie 6500 mit sechs oder neun Steckplätzen maximal 128 EtherChannels. In der Softwareversion 6.2(2) und höheren Versionen wird die Port-ID von der Spanning Tree-Funktion behandelt. Daher ist die maximale Anzahl unterstützter EtherChannels 126 für ein Chassis mit sechs oder neun Steckplätzen und 63 für ein Chassis mit 13 Steckplätzen.

Port Aggregation Protocol

PAgP ist ein Verwaltungsprotokoll, das die Parameterkonsistenz an beiden Enden der Verbindung überprüft und den Kanal bei der Anpassung an Verbindungsausfälle oder das Hinzufügen unterstützt. Beachten Sie die folgenden Fakten zu PAgP:

- 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 sie nicht Teil der EtherChannel-Teilnahme.)
- Wenn bereits ein Paket vorhanden ist und die Konfiguration eines Ports geändert wird (z. B. Ändern des VLAN- oder Trunking-Modus), werden alle Ports im Paket entsprechend dieser Konfiguration geändert.
- 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. PAgP-Pakete werden über dieselbe Multicast-Gruppen-MAC-Adresse gesendet, die für CDP-Pakete verwendet wird: **01-00-0c-cc-cc**. Der Protokollwert ist 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.
- Das Protokoll überwacht PAgP-Pakete, die belegen, dass der physische Port eine bidirektionale Verbindung zu einem anderen PAgP-fähigen Gerät aufweist.
- Wenn Datenpakete, aber keine PAgP-Pakete empfangen werden, wird davon ausgegangen, dass der Port mit einem nicht PAgP-fähigen Gerät verbunden ist.
- Sobald zwei PAgP-Pakete auf einer Gruppe physischer Ports empfangen wurden, versucht das Gerät, einen aggregierten Port zu bilden.
- Wenn PAgP-Pakete für einen bestimmten Zeitraum anhalten, wird der PAgP-Status `abgebrochen`.

Normale Verarbeitung

Diese Konzepte müssen definiert werden, um das Verständnis des Protokollverhaltens zu erleichtern:

- **Agport**: Ein logischer Port, der aus allen physischen Ports in derselben Aggregation besteht, kann durch einen eigenen SNMP ifIndex identifiziert werden. Daher enthält ein Port keine nicht betriebsbereiten Ports.
- **Channel**: eine Aggregation, die die Formationskriterien erfüllt; Es kann daher nicht betriebsbereite Ports enthalten (Agenten sind eine Teilmenge von Kanälen). Protokolle wie STP und VTP, jedoch mit Ausnahme von CDP und DTP, werden über PAgP über den Aggregaten ausgeführt. Keines dieser Protokolle kann Pakete senden oder empfangen, bis PAgP ihre Ports an einen oder mehrere physische Ports anbindet.
- **Gruppenfähigkeit** - Jeder physische Port und jeder Port verfügt über einen Konfigurationsparameter, der als Gruppenfunktion bezeichnet wird. Ein physischer Port kann nur dann mit einem anderen physischen Port aggregiert werden, wenn er über die gleiche Gruppenfunktion verfügt.
- **Aggregationsverfahren** - Wenn ein physischer Port die `UpData-` oder `UpPAgP-`Zustände erreicht, wird er an einen geeigneten Port angeschlossen. Wenn einer dieser Staaten einen anderen Staat verlässt, wird er von dem Port getrennt.

Die Definitionen der Zustände und der Erstellungsverfahren finden Sie in der folgenden Tabelle:

Staat	Bedeutung
`UpData`	Es wurden keine PAgP-Pakete empfangen. PAgP-Pakete werden gesendet. Der physische Port ist der einzige, der mit dem Port verbunden ist. Nicht-PAgP-Pakete werden zwischen dem physischen Port und dem Port an- 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 an- und ausgeleitet.

Beide Enden beider Verbindungen müssen sich darauf einigen, wie die Gruppe aussehen soll. Diese Gruppe wird als die größte Port-Gruppe im Port definiert, die von beiden Enden der Verbindung zugelassen wird.

Wenn ein physischer Port den `UpPAgP-`Status erreicht, wird er dem Port zugewiesen, der über physische Mitglieds-Ports verfügt, die mit der Gruppenfunktion des neuen physischen Ports übereinstimmen und sich in den `BiDir-` oder `UpPAgP-`Zuständen befinden. (Alle BiDir-Ports werden gleichzeitig in den `UpPAgP-`Status verschoben.) Wenn kein Port vorhanden ist, dessen physische Port-Parameter mit dem neu fertig gestellten physischen Port kompatibel sind, wird er einem Port mit geeigneten Parametern zugewiesen, die keine zugehörigen physischen Ports aufweisen.

Ein PAgP-Timeout kann beim letzten Nachbarn auftreten, der am physischen Port bekannt ist. Die Port-Zeitüberschreitung wird aus dem Port entfernt. Gleichzeitig werden alle physischen Ports auf dem gleichen Port, deren Timer ebenfalls abgelaufen sind, entfernt. Dadurch kann ein Agent, dessen anderes Ende verendet ist, gleichzeitig und nicht mehr jeweils ein physischer Port beendet werden.

Verhalten im Fehlerfall

Wenn eine Verbindung in einem vorhandenen Kanal fehlschlägt (z. B. Port getrennt, Gigabit Interface Converter [GBIC] entfernt oder Glasfaser kaputt gemacht), 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 (Datenverkehr, der weiterhin über dieselbe Verbindung gesendet wird), geht nicht verloren. Durch die Wiederherstellung der ausgefallenen Verbindung wird eine weitere Aktualisierung des Agenten ausgelöst, und der Datenverkehr wird erneut gehasht.

Hinweis: Das Verhalten kann variieren, wenn eine Verbindung in einem Kanal aufgrund einer Deaktivierung oder des Entfernens eines Moduls ausfällt. Definitionsgemäß müssen zwei physische Ports für einen Kanal vorhanden sein. Wenn ein Port in einem Kanal mit zwei Ports vom System verloren geht, wird der logische Port beendet und der ursprüngliche physische Port mit Bezug auf Spanning Tree neu initialisiert. Das bedeutet, dass Datenverkehr verworfen werden kann, bis STP es dem Port ermöglicht, wieder für Daten verfügbar zu sein.

Für den Catalyst 6500/6000 gilt eine Ausnahme von dieser Regel. In Versionen vor CatOS 6.3 wird ein Agent beim Entfernen `von` Modulen nicht `heruntergefahren`, wenn der Kanal nur aus Ports auf den Modulen 1 und 2 besteht.

Dieser Unterschied in den beiden Fehlermodi ist wichtig, wenn die Wartung eines Netzwerks geplant ist, da bei der Online-Entfernung oder -Einfügung eines Moduls eine STP-TCN berücksichtigt werden kann. Wie bereits erwähnt, ist es wichtig, jede physische Verbindung im Kanal mit dem NMS zu verwalten, da der Port bei einem Ausfall ungestört bleiben kann.

Es werden folgende Schritte empfohlen, um unerwünschte Topologieänderungen auf dem Catalyst 6500/600 zu vermeiden:

- Wenn pro Modul ein einzelner Port zur Bildung eines Kanals verwendet wird, müssen drei oder mehr Module verwendet werden (insgesamt drei oder mehr Ports).

- Wenn der Kanal zwei Module umfasst, müssen zwei Ports auf jedem Modul verwendet werden (insgesamt vier Ports).
- Wenn ein Zweiport-Kanal für zwei Karten erforderlich ist, verwenden Sie nur die Supervisor Engine-Ports.
- Führen Sie ein Upgrade auf CatOS 6.3 durch, das das Entfernen von Modulen ohne STP-Neuberechnung für auf Module aufgeteilte Kanäle behandelt.

Konfigurationsoptionen

EtherChannels können in verschiedenen Modi konfiguriert werden, wie in der folgenden Tabelle zusammengefasst:

Modus	Konfigurierbare Optionen
`Ein`	PAgP nicht in Betrieb. Der Port leitet den Datenverkehr unabhängig von der Konfiguration des Nachbarports weiter. Wenn der Port-Modus des Nachbarn aktiviert ist, wird ein Kanal gebildet.
`Aus`	Der Port leitet keine Kanäle weiter, unabhängig davon, wie der Nachbar konfiguriert wurde.
`Auto (Standard)`	Die Aggregation erfolgt über das PAgP-Protokoll. Setzt einen Port in einen passiven `Verhandlungs`-Zustand, und auf der Schnittstelle werden keine PAgP-Pakete gesendet, bis mindestens ein PAgP-Paket empfangen wird, das anzeigt, dass der Sender im `wünschenswerten` Modus arbeitet.
`wünschenswert`	Die Aggregation erfolgt über das PAgP-Protokoll. Setzt einen Port in einen aktiven `Verhandlungsstatus`, in dem der Port Verhandlungen mit anderen Ports durch das Senden von PAgP-Paketen aufnimmt. Ein Kanal wird mit einer anderen Portgruppe entweder im wünschenswerten oder im automatischen Modus gebildet.
`Nicht stumm` (Standard 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 Bidirektionalitätsprüfung wurde für bestimmte Catalyst 5500/5000-Hardware durchgeführt, da bei einigen Verbindungsausfällen der Kanal

	auseinandergebrochen wird. Da der `Nicht-Silent-`Modus aktiviert ist, darf ein wiedergewinnender 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` (Standard für alle Catalyst 6500/6000- und 4500/4000-Ports und 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 automatisch an einen Agenten angeschlossen und kann daher 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, oder die Art, wie sie Failover durchführen. Wenn ein Port nicht übertragen werden kann (z. B. aufgrund einer fehlerhaften physischen Subschicht [PHY] oder einer defekten Glasfaser oder eines defekten Kabels), kann der Nachbarport weiterhin betriebsbereit sein. Der Partner überträgt weiterhin Daten, aber Daten gehen verloren, da kein Datenrückverkehr empfangen werden kann. Spanning Tree-Schleifen können sich auch aufgrund der unidirektionalen Natur der Verbindung bilden.

Einige Glasfaserports haben die gewünschte Funktion, den Port in einen nicht betriebsbereiten Zustand zu versetzen, wenn das Empfangssignal (FEFI) verloren geht. Dies führt dazu, dass der Partner-Port nicht betriebsbereit ist und die Ports an beiden Enden der Verbindung effektiv ausfallen.

Bei der Verwendung von Geräten, die Daten übertragen (z. B. BPDUs) und unidirektionale Bedingungen nicht erkennen können, muss der `Nicht-Silent-`Modus verwendet werden, damit die Ports nicht betriebsbereit bleiben, bis Empfangsdaten vorhanden sind und die Verbindung als bidirektional verifiziert wird. Die Zeit, die PAgP benötigt, um eine unidirektionale Verbindung zu erkennen, beträgt etwa 3,5 * 30 Sekunden = 105 Sekunden, wobei 30 Sekunden die Zeit zwischen zwei aufeinander folgenden PAgP-Nachrichten sind. UDLD wird als schnellerer Detektor für unidirektionale Verbindungen empfohlen.

Bei der Verwendung von Geräten, die keine Daten übertragen, muss `der` Silent-Mode verwendet werden. Dadurch wird der Port unabhängig davon, ob empfangene Daten vorhanden sind oder nicht, verbunden und betriebsbereit. Zusätzlich wird für Ports, die unidirektionale Bedingungen erkennen können, z. B. neuere Plattformen, die L1 FEFI und UDLD verwenden, standardmäßig der Silent-Mode verwendet.

Überprüfung

ist eine Tabelle, die eine Zusammenfassung aller möglichen PAgP-Channeling-Szenarien

zwischen zwei direkt verbundenen Switches (Switch-A und Switch-B) darstellt. Einige dieser Kombinationen können dazu führen, dass STP die Ports auf der Channeling-Seite in den `errdisable`-Zustand versetzt (d. h., dass einige der Kombinationen die Ports auf der Channeling-Seite herunterfahren).

Switch-A-Channel-Modus	Switch-B-Kanalmodus	Channel-Staat
Ein	Ein	Channel (nicht PAgP)
Ein	Aus	Kein Kanal (errdisable)
Ein	Automatisch	Kein Kanal (errdisable)
Ein	wünschenswert	Kein Kanal (errdisable)
Aus	Ein	Kein Kanal (errdisable)
Aus	Aus	Kein Channel
Aus	Automatisch	Kein Channel
Aus	wünschenswert	Kein Channel
Automatisch	Ein	Kein Kanal (errdisable)
Automatisch	Aus	Kein Channel
Automatisch	Automatisch	Kein Channel
Automatisch	wünschenswert	PAgP-Kanal
wünschenswert	Ein	Kein Kanal (errdisable)
wünschenswert	Aus	Kein Channel
wünschenswert	Automatisch	PAgP-Kanal
wünschenswert	wünschenswert	PAgP-Kanal

Empfehlung

Cisco empfiehlt, PAgP auf allen Kanalverbindungen zwischen Switches zu aktivieren, um den `Ein`-Modus zu vermeiden. Die bevorzugte Methode besteht darin, den `wünschenswerten` Modus an beiden Enden einer Verbindung festzulegen. Die zusätzliche Empfehlung besteht darin, das `Silent/Non-Silent`-Schlüsselwort auf Catalyst 6500/6000- und 4500/4000-Switches standardmäßig stumm zu lassen, `nicht` auf Catalyst 5500/5000-Glasfaserports.

Wie in diesem Dokument erläutert, ist die explizite Konfiguration der Kanalisierung auf allen anderen Ports hilfreich für eine schnelle Datenweiterleitung. Es ist zu vermeiden, dass PAgP bis zu 15 Sekunden auf ein Timeout auf einem Port wartet, der nicht für die Weiterleitung verwendet werden soll, zumal der Port dann an STP übergeben wird, was wiederum 30 Sekunden dauern kann, um die Weiterleitung von Daten zu ermöglichen, plus potenziell 5 Sekunden für DTP für insgesamt 50 Sekunden. Der **Befehl** set port host wird im STP-Abschnitt dieses Dokuments ausführlicher erläutert.

```
set port channel port range mode desirable

set port channel port range mode off
!--- Ports not channeled; part of the set port hostcommand.
```

Dieser Befehl weist den Kanälen **eine Admin-Gruppennummer zu**, die mit einem **Befehl** show channel group **(Kanalgruppe anzeigen)** angezeigt wird. Das Hinzufügen und Entfernen von Channeling-Ports zum selben Port kann dann nach Wunsch mithilfe der Admin-Nummer verwaltet werden.

Weitere Optionen

Eine weitere gängige Konfiguration für Kunden mit minimalem Administrationsaufwand auf dem Access-Layer besteht darin, den Modus auf der Distribution-Layer und der Core-Ebene `festzulegen` und die Access-Layer-Switches in der `automatischen` Standardkonfiguration zu belassen.

Wenn der Kanal an Geräte geleitet wird, die PAgP nicht unterstützen, muss der Kanal `fest` kodiert werden. Dies gilt für Geräte wie Server, Local Director, Content Switches, Router, Switches mit älterer Software, Catalyst XL-Switches und Catalyst 8540-Switches. Geben Sie den folgenden Befehl ein:

```
set port channel port range mode on
```

Der neue, in CatOS 7.x verfügbare 802.3ad-IEEE-LACP-Standard ersetzt wahrscheinlich langfristig PAgP, da er plattformübergreifende und anbieterübergreifende Interoperabilität bietet.

Link Aggregation Control Protocol

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 nur auf Cisco Switches und Switches ausgeführt werden kann, die von lizenzierten Anbietern erhältlich sind. 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. Mit den CatOS 7.x-Softwareversionen wurde die LACP-Unterstützung eingeführt.

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 der Erstellung des Pakets überprüft. Zu diesen Porteigenschaften gehören:

- Geschwindigkeit
- Duplex
- Natives VLAN
- Trunking-Typ

Die wesentlichen Unterschiede zwischen LACP und PAgP sind:

- LACP kann nur auf Vollduplex-Ports ausgeführt werden, und LACP unterstützt keine Halbduplex-Ports.
- LACP unterstützt Hot-Standby-Ports. LACP versucht immer, die maximale Anzahl kompatibler Ports in einem Kanal zu konfigurieren, bis zur maximalen Anzahl, die die Hardware zulässt (acht Ports). Wenn LACP nicht in der Lage ist, alle kompatiblen Ports zusammenzufassen, werden alle Ports, die nicht aktiv in den Kanal eingeschlossen werden können, in den Hot-

Standby-Zustand versetzt und nur verwendet, wenn einer der verwendeten Ports ausfällt. Ein Beispiel für eine Situation, in der LACP nicht alle kompatiblen Ports aggregieren kann, ist, dass das Remote-System eingeschränktere Hardware-Beschränkungen aufweist.

Hinweis: In CatOS kann derselbe administrative Schlüssel maximal acht Ports zugewiesen werden. In der Cisco IOS-Software versucht LACP, die maximale Anzahl kompatibler Ports in einem EtherChannel zu konfigurieren, bis zur maximalen Anzahl, die 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. Im Folgenden finden Sie 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 hören die Informationen zu, die im Protokoll gesendet werden, und entscheiden, welche Maßnahmen ergriffen werden sollen.
- Kompatible Ports werden in einem Kanal konfiguriert, bis zur maximalen Anzahl, die 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 entsprechende Maßnahmen ergriffen.
- Zusätzlich zu periodischen LACP-Dateneinheiten (LACPDU)-Übertragungen überträgt das Protokoll eine ereignisgesteuerte LACPDU an den Partner, wenn die Statusinformationen geändert werden. Die Protokollpartner ergreifen die geeigneten Maßnahmen auf der Grundlage des neuen Status des Systems.

LACP-Parameter

Damit LACP feststellen kann, ob eine Reihe von Verbindungen mit demselben System verbunden sind und ob diese Verbindungen aus Sicht der Aggregation kompatibel sind, müssen folgende Parameter festgelegt werden:

- Eine global eindeutige Kennung für jedes System, das an der Link-Aggregation beteiligt istJedem System, das LACP ausführt, muss eine Priorität zugewiesen werden, die entweder automatisch oder vom Administrator ausgewählt werden kann. Die Standardsystempriorität ist 32768. Die Systempriorität wird hauptsächlich in Verbindung mit der MAC-Adresse des Systems verwendet, um die System-ID zu bilden.
- Eine Möglichkeit zur Identifizierung der Funktionen, die jedem Port und jedem Aggregator zugeordnet sind, je nachdem, welches System sie verstehtJedem Port im System muss entweder automatisch oder vom Administrator eine Priorität zugewiesen werden. Der

Standardwert ist 128. Die Priorität wird zusammen mit der Portnummer verwendet, um die Port-ID zu bilden.
- Eine Möglichkeit zur Identifizierung einer Link-Aggregation-Gruppe und des zugehörigen AggregatorsDie Möglichkeit, dass ein Port mit einem anderen aggregiert, wird durch einen einfachen 16-Bit-Integer-Parameter zusammengefasst, der absolut größer als Null ist. Dieser Parameter wird als "Schlüssel" bezeichnet. Jeder Schlüssel wird durch unterschiedliche Faktoren bestimmt, z. B.:Die physischen Merkmale des Ports, darunter:DatenrateDuplexitätPoint-to-Point oder gemeinsam genutztes MediumKonfigurationsbeschränkungen, die der Netzwerkadministrator festlegtJedem Port sind zwei Schlüssel zugeordnet:Ein administrativer Schlüssel - Dieser Schlüssel ermöglicht die Manipulation von Schlüsselwerten durch das Management. Ein Benutzer kann diesen Schlüssel auswählen.Ein Betriebsschlüssel - Das System verwendet diesen Schlüssel, um Aggregationen zu bilden. Ein Benutzer kann diesen Schlüssel nicht auswählen oder direkt ändern.Es wird davon ausgegangen, dass der Port-Satz in einem System, das denselben betrieblichen Schlüsselwert hat, zur gleichen Schlüsselgruppe gehört.

Wenn Sie über zwei Systeme und eine Reihe von Ports mit demselben Administratorschlüssel verfügen, versucht jedes System, die Ports zu aggregieren. Jedes System beginnt am Port mit der höchsten Priorität im System mit der höchsten Priorität. Dieses Verhalten ist möglich, da jedes System seine eigene Priorität kennt, die entweder dem Benutzer oder dem System zugewiesen wurde, sowie seine Partnerpriorität, die durch LACP-Pakete erkannt wurde.

Verhalten im Fehlerfall

Das Fehlerverhalten für LACP entspricht dem für PAgP. Wenn eine Verbindung in einem vorhandenen Kanal fehlschlägt, wird der Port aktualisiert, und der Datenverkehr wird innerhalb einer Sekunde über die verbleibenden Links gehasht. Ein Link kann aus folgenden und anderen Gründen fehlschlagen:

- Ein Port ist nicht angeschlossen.
- Ein GBIC wird entfernt.
- Eine Glasfaser ist defekt.
- Hardwarefehler (Schnittstelle oder Modul)

Datenverkehr, der nach dem Ausfall nicht neu gestartet werden muss (Datenverkehr, der weiterhin über dieselbe Verbindung gesendet wird), geht nicht verloren. Durch die Wiederherstellung der ausgefallenen Verbindung wird eine weitere Aktualisierung des Agenten ausgelöst, und der Datenverkehr wird erneut gehasht.

Konfigurationsoptionen

LACP EtherChannels können in verschiedenen Modi konfiguriert werden, wie in der folgenden 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 Nachbarport-Modus `aktiviert` ist, wird ein Kanal gebildet.

Aus	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, indem er ein LACP-Paket sendet. Der Switch empfängt und antwortet auf das Paket und bildet schließlich den Aggregationskanal mit dem Peer.
Aktiv	Dies ähnelt dem wünschenswerten Modus in PAgP. Der Switch initiiert die Aushandlung, um einen Aglink zu bilden. Das Link-Aggregat wird gebildet, wenn das andere Ende im aktiven oder passiven LACP-Modus ausgeführt wird.

Verifizierung (LACP und LACP)

Die Tabelle in diesem Abschnitt zeigt eine Zusammenfassung aller möglichen LACP-Channeling-Mode-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 errdisable-Zustand versetzt. Dies bedeutet, dass einige der Kombinationen die Ports auf der Channeling-Seite herunterfahren.

Switch-A-Channel-Modus	Switch-B-Kanalmodus	Switch-A-Kanalzustand	Switch-B-Kanalstatus
Ein	Ein	Channel (nicht LACP)	Channel (nicht LACP)
Ein	Aus	Kein Kanal (errdisable)	Kein Channel
Ein	Passiv	Kein Kanal (errdisable)	Kein Channel
Ein	Aktiv	Kein Kanal (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

Verifizierung (LACP und PAgP)

Die Tabelle in diesem Abschnitt zeigt eine Zusammenfassung aller möglichen LACP-zu-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 `errdisable`-Zustand versetzt. Dies bedeutet, dass einige der Kombinationen die Ports auf der Channeling-Seite herunterfahren.

Switch-A-Channel-Modus	Switch-B-Kanalmodus	Switch-A-Kanalzustand	Switch-B-Kanalstatus
Ein	Ein	Channel (nicht LACP)	Channel (nicht PAgP)
Ein	Aus	Kein Kanal (errdisable)	Kein Channel
Ein	Automatisch	Kein Kanal (errdisable)	Kein Channel
Ein	wünschenswert	Kein Kanal (errdisable)	Kein Channel
Aus	Ein	Kein Channel	Kein Kanal (errdisable)
Aus	Aus	Kein Channel	Kein Channel
Aus	Automatisch	Kein Channel	Kein Channel
Aus	wünschenswert	Kein Channel	Kein Channel
Passiv	Ein	Kein Channel	Kein Kanal (errdisable)
Passiv	Aus	Kein Channel	Kein Channel
Passiv	Automatisch	Kein Channel	Kein Channel
Passiv	wünschenswert	Kein Channel	Kein Channel
Aktiv	Ein	Kein Channel	Kein Kanal (errdisable)
Aktiv	Aus	Kein Channel	Kein Channel
Aktiv	Automatisch	Kein Channel	Kein Channel
Aktiv	wünschenswert	Kein Channel	Kein Channel

Empfehlung

Cisco empfiehlt, PAgP für Channel-Verbindungen zwischen Cisco Switches zu aktivieren. Wenn Sie zu Geräten kanalisieren, die PAgP nicht unterstützen, aber LACP unterstützen, aktivieren Sie LACP durch die Konfiguration von LACP, das auf beiden Enden der Geräte `aktiv ist`. Wenn ein Ende der Geräte kein LACP oder PAgP unterstützt, müssen Sie den Kanal fest `einschalten`.

- **`set channelprotocol lacp`** *`module`*

  Auf Switches, die CatOS ausführen, verwenden alle Ports auf einem Catalyst 4500/4000 und einem Catalyst 6500/6000 standardmäßig das Channel-Protokoll PAgP und führen als solches kein LACP aus. 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.
-

set port lacp-channel *port_range admin-key*

Ein **admin key**-Parameter (administrativer Schlüssel) wird im LACP-Paket ausgetauscht. Ein Kanal wird nur zwischen Ports erstellt, die über denselben Administratorschlüssel verfügen. Der Befehl **set port lacp-channel *port_rangeadmin-key*** weist den Kanälen eine admin-Schlüsselnummer zu. Der **Befehl show lacp-channel group** gibt die Zahl an. Der Befehl **set port lacp-channel *port_range admin-key* weist allen Ports im Port-Bereich den gleichen Admin-Schlüssel zu**. Der Admin-Schlüssel wird zufällig zugewiesen, wenn kein bestimmter Schlüssel konfiguriert wurde. Anschließend können Sie, falls gewünscht, den Admin-Schlüssel verwenden, um das Hinzufügen und Entfernen von Channeling-Ports zum gleichen Port zu verwalten.

- **set port lacp-channel** *port_range* **mode active**

  Der Befehl **set port lacp-channel *port_range* mode active** ändert den Kanalmodus `für` eine Reihe von Ports, denen zuvor derselbe Administrator-Schlüssel zugewiesen wurde.

Darüber hinaus verwendet LACP nach der Einrichtung der LACP-EtherChannels einen 30-Sekunden-Intervalltimer (Slow_Periodic_Time). Die Anzahl der Sekunden vor der Invalidierung der empfangenen LACPDU-Informationen bei Verwendung von Long Timeouts (3 x Slow_Periodic_Time) beträgt 90. Verwenden Sie UDLD, ein schnellerer Detektor unidirektionaler Verbindungen. Sie können die LACP-Timer nicht anpassen, und heute können Sie die Switches nicht so konfigurieren, dass sie die schnelle PDU-Übertragung (jede Sekunde) verwenden, um den Kanal nach der Kanalbildung aufrechtzuerhalten.

Weitere Optionen

Wenn Sie ein Modell mit minimaler Verwaltung auf dem Access Layer haben, besteht eine gängige Konfiguration darin, den Modus auf `aktive` Distribution- und Core-Layer festzulegen. Lassen Sie die Access-Layer-Switches in der `passiven` Standardkonfiguration konfiguriert.

Unidirectional Link Detection

UDLD ist ein proprietäres Lightweight-Protokoll von Cisco, das entwickelt wurde, um Instanzen der unidirektionalen Kommunikation zwischen Geräten zu erkennen. Obwohl es andere Methoden zum Erkennen des bidirektionalen Zustands von Übertragungsmedien gibt, z. B. FEFI, gibt es Fälle, in denen die L1-Erkennungsmechanismen nicht ausreichen. Diese Szenarien können zu einem der folgenden Ereignisse führen:

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

Die UDLD-Funktion ist für die Behebung dieser Fehlerzustände an Glasfaser- und Kupfer-Ethernet-Schnittstellen vorgesehen:

- Überwachen Sie physische Verkabelungskonfigurationen, und deaktivieren Sie alle falsch verdrahteten Ports als `errdisable`.
- Schutz vor unidirektionalen Links. Wenn aufgrund einer Medien- oder Port-/Schnittstellenfehlfunktion eine unidirektionale Verbindung erkannt wird, wird der betroffene

Port bei `errdisable` geschlossen und eine entsprechende Syslog-Meldung generiert.
- Darüber hinaus überprüft der aggressive UDLD-Modus, ob eine Verbindung, die zuvor als bidirektional eingestuft wurde, während einer Überlastung keine Verbindung verliert und unbrauchbar wird. UDLD 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.

Spanning Tree mit seinem unidirektionalen BPDU-Fluss im stationären Zustand war akut an diesen Ausfällen beteiligt. Es ist leicht zu erkennen, wie ein Port plötzlich nicht in der Lage sein kann, BPDUs zu übertragen. Dies führt dazu, dass sich der STP-Status von der `Blockierung` auf die `Weiterleitung` auf dem Nachbarn ändert. Diese Änderung erzeugt eine Schleife, da der Port immer noch empfangen werden kann.

Überblick

UDLD ist ein L2-Protokoll, das über der LLC-Schicht arbeitet (Ziel-MAC 01-00-0c-cc-cc, SNAP HDLC-Protokolltyp 0x0111). Wenn UDLD in Kombination mit FEFI- und Auto-Negotiation-L1-Mechanismen ausgeführt wird, kann die physische (L1) und logische (L2) Integrität einer Verbindung überprüft werden.

UDLD verfügt über Funktionen und Schutzvorkehrungen, die FEFI und Autoübertragung nicht durchführen können. Dazu gehören die Erkennung und Zwischenspeicherung von Nachbarinformationen, die Möglichkeit, falsch verbundene Ports herunterzufahren und Fehler bei logischen Schnittstellen/Ports oder bei Verbindungen zu erkennen, die nicht Point-to-Point sind (Verbindungen, die Medien-Konverter oder Hubs passieren).

UDLD verwendet zwei grundlegende Mechanismen: Er erfährt Informationen über die Nachbarn und hält die Informationen in einem lokalen Cache auf dem neuesten Stand und sendet einen Zug von UDLD-Sonde-/Echo-(hello-)Nachrichten, wenn er einen neuen Nachbarn erkennt oder ein Nachbar eine erneute Synchronisierung des Cache anfordert.

UDLD sendet kontinuierlich Testnachrichten an allen Ports, an denen UDLD aktiviert ist. Wenn eine bestimmte "Triggering"-UDLD-Nachricht an einem Port empfangen wird, werden eine Erkennungsphase und ein Validierungsprozess gestartet. Wenn am Ende dieses Prozesses alle gültigen Bedingungen erfüllt sind, wird der Portstatus nicht geändert. Um die Bedingungen zu erfüllen, muss der Port bidirektional und korrekt verkabelt sein. Andernfalls ist der Port `errdisable`, und es wird eine Syslog-Meldung angezeigt. Die Syslog-Meldung ähnelt den folgenden Meldungen:

- `UDLD-3-DISABLE: Unidirectional Link detected on port [dec]/[dec] (auf Port [dec]/[dec] erkannte unidirektionale Verbindung). Port deaktiviert`
- `UDLD-4-ONEWAYPATH: Eine unidirektionale Verbindung von Port [dec]/[dec] zu Port [dec]/[dec] des Geräts [chars] wurde erkannt`

Eine vollständige Liste der Systemmeldungen nach Einrichtung, die auch UDLD-Ereignisse enthält, finden Sie unter Messages and Recovery Procedures (Catalyst Series Switches, 7.6).

Nachdem eine Verbindung hergestellt und als bidirektional klassifiziert wurde, kündigt UDLD in einem Standardintervall von 15 Sekunden weiterhin Sonde-/Echonachrichten an. Diese Tabelle stellt gültige UDLD-Verbindungsstatus dar, wie in der Ausgabe des Befehls **show udld port** angegeben:

Port-Status	Kommentar

Unbestimmt	Die Erkennung wird durchgeführt, oder eine benachbarte UDLD-Einheit wurde deaktiviert oder die Übertragung wurde blockiert.
Nicht zutreffend	UDLD wurde deaktiviert.
Herunterfahren	Eine unidirektionale Verbindung wurde erkannt und der Port deaktiviert.
Bidirektional	Es wurde eine bidirektionale Verbindung erkannt.

- **Neighbor Cache Maintenance**: UDLD sendet regelmäßig Hello-Sonde-/Echo-Pakete an jede aktive Schnittstelle, um die Integrität des UDLD-Nachbarcache zu wahren. Wenn eine Hello-Nachricht empfangen wird, wird sie zwischengespeichert und für einen als Haltezeit definierten Zeitraum im Speicher aufbewahrt. 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.
- Um die Integrität des UDLD-Cache zu wahren, werden bei jeder Deaktivierung einer UDLD-fähigen Schnittstelle oder beim Zurücksetzen eines Geräts alle vorhandenen Cache-Einträge für die von der Konfigurationsänderung betroffenen Schnittstellen gelöscht, und UDLD überträgt mindestens eine Nachricht, um die entsprechenden Nachbarn zu informieren, die entsprechenden Cache-Einträge zu leeren.
- **Echorkennungsmechanismus**: Der Echomechanismus bildet die Grundlage des Erkennungsalgorithmus. Wenn ein UDLD-Gerät von einem neuen Nachbarn erfährt oder eine Resynchronisierungsanfrage von einem Out-of-Synch-Nachbarn empfängt, startet/startet es 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 zurücksendet. Wenn das Erkennungsfenster beendet wird und keine gültige Antwortnachricht eingegangen ist, wird die Verbindung als unidirektional angesehen, und ein Vorgang zum Wiederherstellen oder Herunterfahren der Verbindung kann ausgelöst werden.

Konvergenzzeit

Um STP-Schleifen zu verhindern, reduzierte CatOS 5.4(3) das UDLD-Standardmeldungsintervall von 60 Sekunden auf 15 Sekunden, um eine unidirektionale Verbindung zu schließen, bevor ein blockierter Port in der Lage war, in einen Weiterleitungsstatus umzuschalten.

Hinweis: 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 gesendet, und das Zeitüberschreitungsintervall für diesen Peer wird berechnet als (3 * message_interval). Aus diesem Grund wird eine Peer-Beziehung nach drei aufeinander folgenden Hellos (oder Probes) abgebrochen. Da sich die Nachrichtenintervalle auf jeder Seite unterscheiden, ist dieser Timeout-Wert auf jeder Seite unterschiedlich.

Die ungefähre Zeit, die UDLD zum Erkennen eines unidirektionalen Fehlers benötigt, ist ungefähr (2,5 * message_interval + 4 Sekunden) oder etwa 41 Sekunden bei Verwendung des Standard-

Nachrichtenintervalls von 15 Sekunden. Dieser Wert liegt deutlich unter den 50 Sekunden, die normalerweise für die Neukonvergierung von STP erforderlich sind. Wenn die NMP-CPU über einige Ersatzzyklen verfügt und Sie den Auslastungsgrad genau überwachen, können Sie das Nachrichtenintervall (sogar) auf mindestens 7 Sekunden reduzieren. Dieses Nachrichtenintervall beschleunigt die Erkennung um einen signifikanten Faktor.

Daher wird von UDLD von Standard-Spanning-Tree-Timern ausgegangen. Wenn Sie STP so einstellen, dass es schneller konvergiert als UDLD, sollten Sie einen alternativen Mechanismus in Betracht ziehen, z. B. die CatOS 6.2 Loop Guard-Funktion. Berücksichtigen Sie auch einen alternativen Mechanismus, wenn Sie RSTP (IEEE 802.1w) implementieren, da RSTP in Millisekunden Konvergenzmerkmale aufweist, die von der Topologie abhängen. Verwenden Sie für diese Instanzen Loop Guard in Verbindung mit UDLD, das den meisten Schutz bietet. Loop Guard verhindert STP-Schleifen mit der Geschwindigkeit der verwendeten STP-Version, und UDLD erkennt unidirektionale Verbindungen auf einzelnen EtherChannel-Verbindungen oder in Fällen, in denen BPDUs nicht in die unterbrochene Richtung fließen.

Hinweis: UDLD erfasst nicht jede STP-Fehlersituation, z. B. Fehler, die von einer CPU verursacht werden, die keine BPDUs für einen Zeitraum von mehr als (2 * FwdDelay + Maxage) sendet. Aus diesem Grund empfiehlt Cisco die Implementierung von UDLD in Verbindung mit Loop Guard (eingeführt in CatOS 6.2) in Topologien, die auf STP basieren.

Vorsicht: Achten Sie auf frühere Versionen von UDLD, die ein nicht konfigurierbares Standard-Nachrichtenintervall von 60 Sekunden verwenden. Diese Versionen sind anfällig für Spanning-Tree-Schleifenbedingungen.

Aggressive UDLD-Modus

Aggressive UDLD wurde erstellt, um speziell auf die (wenigen) Fälle einzugehen, 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, wird kein Port deaktiviert.
- Eine Seite einer Verbindung hat einen Port-Stock (sowohl Transmit [Tx] als auch Rx).
- Eine Seite einer Verbindung bleibt aktiv, während die andere Seite der Verbindung ausfällt.
- Die Autonegotiation oder ein anderer L1-Fehlererkennungsmechanismus ist deaktiviert.
- Eine Verringerung der Abhängigkeit von L1-FEFI-Mechanismen ist wünschenswert.
- Es ist ein maximaler Schutz gegen unidirektionale Verbindungsausfälle auf FE/GE-Point-to-Point-Verbindungen erforderlich. Insbesondere, wenn ein Ausfall zwischen zwei Nachbarn nicht zulässig ist, können UDLD-aggressive Sonden als "Herzschlag" angesehen werden, dessen Vorhandensein die Integrität der Verbindung garantiert.

Der häufigste Fall für eine Implementierung von aggressivem UDLD besteht darin, die Verbindungsprüfung für ein Mitglied eines Pakets durchzuführen, wenn die automatische Aushandlung oder ein anderer L1-Fehlererkennungsmechanismus deaktiviert oder unbrauchbar ist. Dies gilt insbesondere für EtherChannel-Verbindungen, da PAgP/LACP selbst bei Aktivierung keine sehr niedrigen Hello-Timer im Steady-State verwendet. In diesem Fall bietet aggressives UDLD den zusätzlichen Vorteil, dass mögliche Spanning-Tree-Schleifen vermieden werden.

Die Umstände, die zum symmetrischen Verlust von UDLD-Sondepaketen beitragen, sind schwieriger zu beschreiben. Sie müssen sich darüber im Klaren sein, dass das normale UDLD

selbst dann eine unidirektionale Verbindungsbedingung prüft, wenn eine Verbindung den bidirektionalen Status erreicht. UDLD soll L2-Probleme erkennen, die STP-Schleifen verursachen. Diese Probleme sind in der Regel unidirektional, da BPDUs im Steady-State nur in eine Richtung fließen. Daher ist die Verwendung von normalem UDLD in Verbindung mit Autoübertragung und Loop Guard (für Netzwerke, die auf STP basieren) fast immer ausreichend. Der aggressive UDLD-Modus ist jedoch in Situationen nützlich, in denen Überlastungen in beide Richtungen gleichermaßen betroffen sind, was den Verlust von UDLD-Sonden in beide Richtungen verursacht. Dieser Verlust von UDLD-Tests kann beispielsweise auftreten, wenn die CPU-Auslastung an jedem Ende der Verbindung erhöht ist. Weitere Beispiele für bidirektionale Verbindungsverluste sind die Fehler eines dieser Geräte:

- DWDM-Transponder (Dense Wavelength Division Multiplexing)
- Ein Medienkonverter
- Ein Hub
- Weiteres L1-Gerät**Hinweis:** Der Fehler kann durch automatische Aushandlung nicht erkannt werden.

Der aggressive UDLD-Fehler deaktiviert den Port in diesen Fehlersituationen. Berücksichtigen Sie die Auswirkungen sorgfältig, wenn Sie den aggressiven UDLD-Modus für Links aktivieren, die nicht Point-to-Point-Links sind. Links zu Medienkonvertern, Hubs oder ähnlichen Geräten sind keine Point-to-Point-Links. Zwischengeräte können die Weiterleitung von UDLD-Paketen verhindern und das unnötige Herunterfahren einer Verbindung erzwingen.

Nachdem alle Nachbarn eines Ports ausgefallen sind, startet der aggressive UDLD-Modus (wenn er aktiviert ist) die Verbindungssequenz neu, um eine Resynchronisierung mit anderen potenziell nicht synchronisierten Nachbarn durchzuführen. Dieser Aufwand erfolgt entweder in der Werbe- oder in der Erkennungsphase. Wenn die Verbindung nach einem schnellen Nachrichtenzug (acht fehlgeschlagene Wiederholungen) immer noch als "unbestimmt" gilt, wird der Port in den Status `errdisable` gesetzt.

Hinweis: Einige Switches sind nicht aggressiv UDLD-fähig. Derzeit verfügen der Catalyst 2900XL und der Catalyst 3500XL über hartcodierte Nachrichtenintervalle von 60 Sekunden. Dieses Intervall gilt nicht als ausreichend schnell, um sich vor potenziellen STP-Schleifen zu schützen (unter Verwendung der Standard-STP-Parameter).

UDLD auf Routed Links

Für diese Diskussion ist eine geroutete Verbindung einer von zwei Verbindungstypen:

- Point-to-Point zwischen zwei Router-KnotenDiese Verbindung wird mit einer 30-Bit-Subnetzmaske konfiguriert.
- Ein VLAN mit mehreren Ports, aber nur geroutete Verbindungen unterstütztEin Beispiel ist eine Split-L2-Core-Topologie.

Jedes Interior Gateway Routing Protocol (IGRP) weist einzigartige Merkmale auf, wie es Nachbarbeziehungen und Routenkonvergenz handhabt. Die in diesem Abschnitt behandelten Merkmale sind relevant, wenn Sie zwei der heute verwendeten Routingprotokolle, das Open Shortest Path First (OSPF)-Protokoll und das Enhanced IGRP (EIGRP), gegenüberstellen.

Beachten Sie zunächst, dass ein L1- oder L2-Ausfall in einem gerouteten Point-to-Point-Netzwerk zu einer nahezu sofortigen Beendigung der L3-Verbindung führt. Da der einzige Switch-Port in diesem VLAN bei einem L1/L2-Ausfall in einen nicht verbundenen Zustand wechselt, werden die L2- und L3-Portstatus mit der MSFC-Funktion in etwa zwei Sekunden synchronisiert. Bei dieser

Synchronisierung befindet sich die L3-VLAN-Schnittstelle im Ein-/Ausschaltzustand (bei deaktiviertem Leitungsprotokoll).

Nehmen Sie die Standardwerte für den Timer an. OSPF sendet 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 im schlimmsten Fall 40 Sekunden. Dieser Failover ist auch dann der Fall, wenn der L1/L2-Ausfall nicht nur bei einer Punkt-zu-Punkt-Verbindung auftritt. Somit bleibt ein Halbbetrieb-Szenario bestehen, mit dem das L3-Protokoll umgehen muss. Da die Erkennungszeit von UDLD der Zeit eines OSPF-Dead Timers sehr ähnlich ist, der abläuft (etwa 40 Sekunden), sind die Vorteile der Konfiguration des UDLD-Normalmodus auf einer OSPF-L3-Point-to-Point-Verbindung begrenzt.

In vielen Fällen konvergiert EIGRP schneller als OSPF. Beachten Sie jedoch, dass keine bidirektionale Kommunikation erforderlich ist, damit Nachbarn Routing-Informationen austauschen können. In sehr spezifischen Szenarien mit Halbbetrieb-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 die in diesem Abschnitt beschriebenen Umstände lindern. Der normale UDLD-Modus erkennt den Ausfall einer unidirektionalen Verbindung, und der Fehler deaktiviert den Port.

Bei L3-gerouteten Verbindungen, die ein beliebiges Routing-Protokoll verwenden, bietet UDLD normal nach wie vor Schutz vor Problemen bei der ersten Aktivierung der Verbindung. Zu diesen Problemen gehören fehlerhafte Verkabelung oder fehlerhafte Hardware. Zusätzlich bietet der aggressive UDLD-Modus bei L3-gerouteten Verbindungen die folgenden Vorteile:

- Verhindert das unnötige Blackholing von Datenverkehr**Hinweis:** In einigen Fällen sind Timer mit minimalem Timer erforderlich.
- Fügt einen Flapping-Link in den Status `errdisable ein`
- Schützt vor Schleifen, die durch L3-EtherChannel-Konfigurationen entstehen

Standardverhalten von UDLD

UDLD ist global deaktiviert und standardmäßig für Glasfaserports einsatzbereit aktiviert. Da UDLD ein Infrastrukturprotokoll ist, das nur zwischen Switches erforderlich ist, wird UDLD auf Kupferports standardmäßig deaktiviert. Kupferports werden in der Regel für den Host-Zugriff verwendet.

Hinweis: UDLD muss global und auf Schnittstellenebene aktiviert werden, bevor Nachbarn bidirektionalen Status erreichen können. In CatOS 5.4(3) und höher beträgt das Standard-Nachrichtenintervall 15 Sekunden und kann zwischen 7 und 90 Sekunden konfiguriert werden.

Die Wiederherstellung von Errdisable ist standardmäßig global deaktiviert. Wenn ein Port global aktiviert ist und in den `errdisable-`Zustand 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. Sie können eine erneute Aktivierung eines Ports manuell verhindern, wenn Sie die Zeitüberschreitung bei errdisable für diesen Port `deaktivieren`. Geben Sie den Befehl set port errdisable-timeout *mod/port* ***disable*** ein.

Hinweis: Die Verwendung dieses Befehls hängt von Ihrer Softwareversion ab.

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.

Unter Konfiguration von Ethernet, Fast Ethernet, Gigabit Ethernet und 10-Gigabit Ethernet Switching finden Sie weitere Informationen zum Konfigurieren einer Zeitüberschreitungsfrist für Ports, die sich im `errdisable`-Status befinden.

Empfehlung

UDLD im normalen Modus ist in den meisten Fällen ausreichend, wenn Sie es ordnungsgemäß und in Verbindung mit den entsprechenden Funktionen und Protokollen verwenden. Zu diesen Funktionen und Protokollen gehören:

- FEFI
- Autonegotiation
- Loop Guard

Bei der Bereitstellung von UDLD sollten Sie in Betracht ziehen, ob ein kontinuierlicher Test der bidirektionalen Konnektivität (aggressiver Modus) erforderlich ist. Wenn die Autoübertragung aktiviert ist, ist normalerweise der aggressive Modus nicht erforderlich, da die automatische Aushandlung die Fehlererkennung bei L1 kompensiert.

Cisco empfiehlt die Aktivierung des normalen UDLD-Modus für alle FE/GE-Point-to-Point-Verbindungen zwischen Cisco Switches, bei denen das UDLD-Nachrichtenintervall auf den 15-Sekunden-Standard festgelegt ist. Bei dieser Konfiguration wird von den standardmäßigen 802.1d Spanning Tree-Timern ausgegangen. Darüber hinaus sollte UDLD in Verbindung mit Loop Guard in Netzwerken verwendet werden, die für Redundanz und Konvergenz auf STP angewiesen sind. Diese Empfehlung gilt für Netzwerke, in denen sich ein oder mehrere Ports im STP-Blockierungsstatus in der Topologie befinden.

Führen Sie die folgenden Befehle aus, um UDLD zu aktivieren:

```
set udld enable
!--- After global enablement, all FE and GE fiber !--- ports have UDLD enabled by default. set
udld enable port range
!--- This is for additional specific ports and copper media, if needed.
```

Sie müssen Ports manuell aktivieren, die aufgrund eines Fehlers aufgrund von Symptomen für unidirektionale Verbindungen deaktiviert wurden. Geben Sie den Befehl **set port enable ein**.

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

Weitere Optionen

Um einen maximalen Schutz gegen Symptome zu gewährleisten, die durch unidirektionale Links entstehen, konfigurieren Sie UDLD im aggressiven Modus:

```
set udld aggressive-mode enable port_range
```

Darüber hinaus können Sie den Wert für das UDLD-Nachrichtenintervall zwischen 7 und 90 Sekunden an jedem Ende einstellen, sofern dies unterstützt wird, um eine schnellere Konvergenz zu erreichen:

```
set udld interval time
```

Erwägen Sie die Verwendung der errdisable-Zeitüberschreitungsfunktion auf jedem Gerät, das im Falle einer errdisable-Situation vom Netzwerk isoliert werden kann. Diese Situation trifft in der Regel auf den Access-Layer zu, und wenn Sie den aggressiven UDLD-Modus ohne Out-of-Band-Netzwerkmanagementfunktionen implementieren.

Wenn ein Port in den Status `errdisable` gesetzt wird, bleibt der Port standardmäßig inaktiv. Sie können diesen Befehl ausführen, mit dem Ports nach einem Zeitüberschreitungsintervall erneut aktiviert werden:

Hinweis: Das Zeitüberschreitungsintervall beträgt standardmäßig 300 Sekunden.

```
>set errdisable-timeout enable ?
bpdu-guard
!--- This is BPDU port-guard. channel-misconfig !--- This is a channel misconfiguration. duplex-
mismatch udld other !--- These are other reasons. all !--- Apply errdisable timeout to all
reasons.
```

Wenn das Partnergerät nicht UDLD-fähig ist (z. B. ein End-Host oder -Router), führen Sie das Protokoll nicht aus. Geben Sie den folgenden Befehl ein:

```
set udld disable port_range
```

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 z. B. einen einfachen Test durchführen und einen Glasfaserstrang trennen, um den gewünschten `errdisable`-Status anzuzeigen, müssen Sie die L1-Autonegotiation deaktiviert haben. Andernfalls wird der physische Port deaktiviert, wodurch die UDLD-Nachrichtenkommunikation zurückgesetzt wird. Das Remote-Ende wird im normalen UDLD in den unbestimmten Zustand verschoben. Wenn Sie den aggressiven UDLD-Modus verwenden, wechselt das Remote-Ende in den Status `errdisable`.

Es gibt eine zusätzliche Testmethode, um den PDU-Verlust des Nachbarn für UDLD zu simulieren. Verwenden Sie MAC-Layer-Filter, um die UDLD-/CDP-Hardwareadresse zu blockieren, aber die Weiterleitung anderer Adressen zu ermöglichen.

Führen Sie folgende Befehle aus, um UDLD zu überwachen:

```
>show udld
```

```
UDLD              : enabled
Message Interval  : 15 seconds
```

```
>show udld port 3/1

UDLD              : enabled
Message Interval  : 15 seconds
Port      Admin Status  Aggressive Mode  Link State
--------  ------------  ---------------  ----------------
3/1      enabled       disabled         bidirectional
```

Auch im `Aktivierungsmodus` können Sie den Befehl **ausgeblendetes udld-Nachbarn anzeigen**, um den Inhalt des UDLD-Cache zu überprüfen (wie dies bei CDP der Fall ist). Oft ist ein Vergleich des UDLD-Cache mit dem CDP-Cache hilfreich, um zu überprüfen, ob eine protokollspezifische Anomalie vorliegt. Wenn CDP ebenfalls betroffen ist, sind in der Regel alle PDUs/BPDUs betroffen. Aktivieren Sie daher auch STP. Überprüfen Sie beispielsweise, ob die Root-Identitätsänderungen oder Änderungen an der Root/Designated-Portplatzierung vorgenommen wurden.

```
>show udld neighbor 3/1

Port  Device Name            Device ID    Port-ID OperState
----- --------------------  ------------ ------- ----------
3/1   TSC07117119M(Switch)   000c86a50433 3/1     bidirectional
```

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

Jumbo-Frame

Die standardmäßige MTU-Frame-Größe (Maximum Transmission Unit) beträgt 1.518 Byte für alle Ethernet-Ports, einschließlich GE und 10 GE. Die Jumbo Frame-Funktion ermöglicht Schnittstellen zum Umschalten von Frames, die größer als die standardmäßige Ethernet-Frame-Größe sind. Diese Funktion ist nützlich, um die Server-zu-Server-Leistung zu optimieren und Anwendungen wie Multi-Protocol Label Switching (MPLS), 802.1Q Tunneling und L2 Tunneling Protocol Version 3 (L2TPv3) zu unterstützen, die die Größe der ursprünglichen Frames erhöhen.

Überblick

Die IEEE 802.3-Standardspezifikation definiert eine maximale Ethernet-Frame-Größe von 1518 Byte für reguläre Frames und 1522 Byte für 802.1Q-gekapselte Frames. Die 802.1Q-gekapselten Frames werden manchmal auch als "Babygiganten" bezeichnet. Im Allgemeinen werden Pakete als gigantische Frames klassifiziert, wenn die Pakete die angegebene Ethernet-Höchstlänge für eine bestimmte Ethernet-Verbindung überschreiten. Riesenpakete werden auch als Jumbo Frames bezeichnet.

Es gibt verschiedene Gründe, warum die MTU-Größe bestimmter Frames 1518 Byte überschreiten kann. Hier einige Beispiele:

- Herstellerspezifische Anforderungen - Anwendungen und bestimmte NICs können eine MTU-Größe außerhalb der Standard-1500-Byte angeben. Die Tendenz zur Angabe solcher MTU-Größen beruht auf durchgeführten Studien, die belegen, dass eine Vergrößerung des Ethernet-Frames den durchschnittlichen Durchsatz erhöhen kann.
- Trunking - Um VLAN-ID-Informationen zwischen Switches oder anderen Netzwerkgeräten zu

übertragen, wurde Trunking verwendet, um den standardmäßigen Ethernet-Frame zu erweitern. Heute sind die beiden gängigsten Formen des Trunking die proprietäre ISL-Kapselung von Cisco und IEEE 802.1Q.
- MPLS - Nachdem MPLS auf einer Schnittstelle aktiviert wurde, kann die Frame-Größe eines Pakets erhöht werden. Diese Erweiterung hängt von der Anzahl der Labels im Label-Stack für ein mit MPLS gekennzeichnetes Paket ab. Die Gesamtgröße eines Labels beträgt 4 Byte. Die Gesamtgröße eines Label-Stacks beträgt x 4 Byte. 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 ein Tag für die Hardware sichtbar ist. Daher fügt das interne Tag dem MTU-Wert (Payload-Größe) 4 Byte hinzu.
- Universal Transport Interface (UTI)/L2TPv3 - UTI/L2TPv3 kapselt L2-Daten, die über das IP-Netzwerk weitergeleitet werden sollen. Die Kapselung kann die ursprüngliche Frame-Größe um bis zu 50 Byte erhöhen. Der neue Frame enthält einen neuen IP-Header (20 Byte), einen L2TPv3-Header (12 Byte) und einen neuen L2-Header. Die L2TPv3-Nutzlast besteht aus dem gesamten L2-Frame, der den L2-Header enthält.

Die Unterstützung verschiedener Frame-Größen durch die verschiedenen Catalyst Switches hängt von zahlreichen Faktoren ab, darunter Hardware und Software. Bestimmte Module können größere Frame-Größen unterstützen, selbst innerhalb derselben Plattform.

- Die Catalyst 5500/5000-Switches unterstützen Jumbo-Frames in der CatOS 6.1-Version. Wenn die Funktion für Jumbo-Frames auf einem Port aktiviert ist, erhöht sich die MTU-Größe auf 9216 Byte. Auf UTP-basierten Line Cards mit 10/100 Mbit/s und ungeschirmtem Twisted Pair (Unshielded Twisted Pair) wird eine maximale Frame-Größe von nur 8.092 Byte unterstützt. Diese Einschränkung ist eine ASIC-Einschränkung. Die Aktivierung der Funktion für die Jumbo-Frame-Größe unterliegt in der Regel keinen Einschränkungen. Sie können diese Funktion für Trunking/Nicht-Trunking und Channeling/Nonchannel verwenden.
- Die Catalyst 4000-Switches (Supervisor Engine 1 [WS-X4012] und Supervisor Engine 2 [WS-X4013]) unterstützen aufgrund einer ASIC-Einschränkung keine Jumbo-Frames. Eine Ausnahme bildet jedoch das 802.1Q-Trunking.
- Die Plattform der Catalyst 6500-Serie unterstützt Jumbo-Frames in CatOS 6.1(1) und höher. Diese Unterstützung hängt jedoch von der Art der Linecards ab, die Sie verwenden. Die Aktivierung der Funktion für die Jumbo-Frame-Größe unterliegt in der Regel keinen Einschränkungen. Sie können diese Funktion für Trunking/Nicht-Trunking und Channeling/Nonchannel verwenden. Die MTU-Standardgröße beträgt 9.216 Byte, nachdem die Unterstützung für Jumbo-Frames auf dem einzelnen Port aktiviert wurde. Die Standard-MTU kann mit CatOS nicht konfiguriert werden. In der Cisco IOS Software-Version 12.1(13)E wurde jedoch der **Befehl** **system jumbomtu** **(Jumbomtu)** eingeführt, um die Standard-MTU zu überschreiben.

Weitere Informationen finden Sie im Konfigurationsbeispiel für Jumbo/Riant Frame Support für Catalyst Switches.

In dieser Tabelle werden die MTU-Größen beschrieben, die von verschiedenen Linecards für Catalyst Switches der Serien 6500 und 6000 unterstützt werden:

Hinweis: Die MTU-Größe oder Paketgröße bezieht sich nur auf die Ethernet-Nutzlast.

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(V), WS-X6348 RJ-21(V)	8092 Byte (begrenzt durch den PHY-Chip)
WS-X6148-RJ-45(V), WS-X6148-RJ-21(V) WS-X6148-45AF, WS-X6148-21AF	9.100 Byte (@ 100 Mbit/s) 9.216 Byte (@ 10 Mbit/s)
WS-X6148A-RJ-45, WS-X6148A-45AF, WS-X6148-FE-SFP	9216 Byte
WS-X6324-100FX-MM, -SM, WS-X6024-10FL-MT	9216 Byte
WS-X6548-RJ-45, WS-X6548-RJ-21, WS-X6524-100FX-MM WS-X6148X2-RJ-45, WS-X6148X2-45WS X6196-RJ-21, WS-X6196-21AF WS-X6408-GBIC, WS-X6316-GE-TX, WS-X6416-GBIC WS-X6516-GBIC, WS-X 6516A-GBIC-, WS-X6816-GBIC-Uplinks der Supervisor Engine 1, 2, 32 und 720	9216 Byte
WS-X6516-GE-TX	8.092 Byte (@ 100 Mbit/s) 9.216 Byte (@ 10 oder 1.000 Mbit/s)
WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6148-GE-45AF, WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6548 GE-45AF	1.500 Byte (Jumbo-Frame wird nicht unterstützt)
WS-X6148A-GE-TX, WS-X6148A-GE-45AF, WS-X6502-10GE, WS-X67xx-Serie	9216 Byte
OSM ATM (OC12c)	9180 Byte
OSM CHOC3, CHOC12, CHOC48, CT3	9216

	Byte (OCx und DS3) 7673 Byte (T1/E1)
Flex-WAN	7673 Byte (CT3 T1/DS0) 9216 Byte (OC3c POS) 7673 Byte (T1)
CSM (WS-X6066-SLB-APC)	9.216 Byte (als CSM 3.1(5) und 3.2(1))
OSM POS OC3c, OC12c, OC48c; OSM DPT OC48c, OSM GE WAN	9216 Byte

Layer-3-Jumbo Frame-Unterstützung

Mit CatOS, das auf der Supervisor Engine und der Cisco IOS Software ausgeführt wird, die auf der MSFC ausgeführt wird, bieten die Catalyst 6500/6000-Switches auch L3-Jumbo Frame-Unterstützung in der Cisco IOS® Softwareversion 12.1(2)E und höher, wobei PFC/MSFC2, PFC2/MSFC2 oder neuere Hardware verwendet wird. Wenn sowohl Eingangs- als auch Ausgangs-VLANs für Jumbo Frames konfiguriert sind, werden alle Pakete mit Leitungsgeschwindigkeit von der PFC auf Hardware umgeschaltet. Wenn das Eingangs-VLAN für Jumbo-Frames konfiguriert ist und das Ausgangs-VLAN nicht konfiguriert ist, gibt es zwei Szenarien:

- Ein Jumbo-Frame, der vom End-Host mit festgelegtem Don't Fragment (DF)-Bit gesendet wird (für die MTU-Pfaderkennung) - Das Paket wird verworfen, und ein nicht erreichbares Internet Control Message Protocol (ICMP) wird an den End-Host gesendet, wobei das `erforderliche` Nachrichtencodefragment `und das DF-`Protokoll `festgelegt werden`.
- Ein Jumbo Frame, der vom End-Host ohne festgelegtes DF-Bit gesendet wird - Pakete werden auf MSFC2/MSFC3 gestrafft, um fragmentiert und in der Software umgeschaltet zu werden.

In dieser Tabelle ist die L3-Jumbo-Unterstützung für verschiedene Plattformen zusammengefasst:

L3-Switch oder -Modul	Maximale L3-MTU-Größe
Catalyst Serie 2948G-L3/4908G-L3	Jumbo Frames werden nicht unterstützt.

Catalyst 5000 RSM[1]/RSFC[2]	Jumbo Frames werden nicht unterstützt.
Catalyst 6500 MSFC1	Jumbo Frames werden nicht unterstützt.
Catalyst 6500 MSFC2 und höher	Cisco IOS Software Release 12.1(2)E: 9216 Byte

[1] RSM = Route Switch Module

[2] RSFC = Route Switch Feature Card

Überlegungen zur Netzwerkleistung

Die Leistung von TCP over WANs (Internet) wurde umfassend untersucht. Diese Gleichung erklärt, wie der TCP-Durchsatz eine Obergrenze aufweist, die auf folgenden Faktoren basiert:

- 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. Bei konstantem RTT und Paketverlust können Sie den TCP-Durchsatz verdoppeln, 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.

Zweitens erfordern die stetig wachsenden Leistungsanforderungen von Serverfarmen ein effizienteres Mittel, um höhere Datenraten mit NFS-UDP-Datagrammen (Network File System) sicherzustellen. NFS ist der am häufigsten eingesetzte Datenspeicherungsmechanismus für die Dateiübertragung zwischen UNIX-basierten Servern und verfügt über 8400-Byte-Datagramme. Aufgrund der erweiterten Ethernet-MTU-Größe von 9 KB ist ein einzelner Jumbo Frame groß genug, um ein Anwendungsdatagramm von 8 KB (z. B. NFS) plus den Overhead für den Paket-Header zu übertragen. Diese Funktion ermöglicht im Übrigen effizientere DMA-Übertragungen (Direct Memory Access) auf den Hosts, da die Software nicht mehr benötigt, um NFS-Blöcke in separate UDP-Datagramme zu fragmentieren.

Empfehlung

Wenn Sie Unterstützung für Jumbo Frames benötigen, beschränken Sie die Verwendung von Jumbo Frames auf Bereiche des Netzwerks, in denen alle Switch-Module (L2) und Schnittstellen (L3) Jumbo Frames unterstützen. Diese Konfiguration verhindert die Fragmentierung an einer beliebigen Stelle im Pfad. Die Konfiguration von Jumbo Frames, die größer als die unterstützte Frame-Länge im Pfad sind, eliminiert alle Vorteile, die durch die Verwendung der Funktion erzielt werden, da eine Fragmentierung erforderlich ist. Wie die Tabellen in diesem Jumbo Frame-Abschnitt zeigen, können unterschiedliche Plattformen und Linecards in Bezug auf die maximal unterstützten Paketgrößen variieren.

Konfigurieren Sie Jumbo Frame-fähige Hostgeräte mit einer MTU-Größe, die der von der Netzwerkhardware unterstützte gemeinsame Mindestnenner für das gesamte L2-VLAN ist, in dem sich das Hostgerät befindet. Führen Sie folgenden Befehl aus, um die Unterstützung von Jumbo Frames für Module mit Jumbo Frame-Unterstützung zu aktivieren:

```
set port jumbo mod/port enable
```

Wenn Sie eine Unterstützung für Jumbo-Frames über L3-Grenzen hinweg wünschen, müssen Sie außerdem den größten verfügbaren MTU-Wert von 9216 Byte für alle relevanten VLAN-Schnittstellen konfigurieren. Geben Sie den Befehl **mtu** unter den VLAN-Schnittstellen aus:

```
interface vlan vlan# mtu 9216
```

Diese Konfiguration stellt sicher, dass die von den Modulen unterstützte L2-Jumbo-Frame-MTU immer kleiner oder gleich dem Wert ist, der für die L3-Schnittstellen konfiguriert ist, die der Datenverkehr durchläuft. Dadurch wird eine Fragmentierung verhindert, wenn der Datenverkehr vom VLAN über die L3-Schnittstelle weitergeleitet wird.

Verwaltungskonfiguration

Überlegungen zur Steuerung, Bereitstellung und Fehlerbehebung eines Catalyst-Netzwerks werden in diesem Abschnitt behandelt.

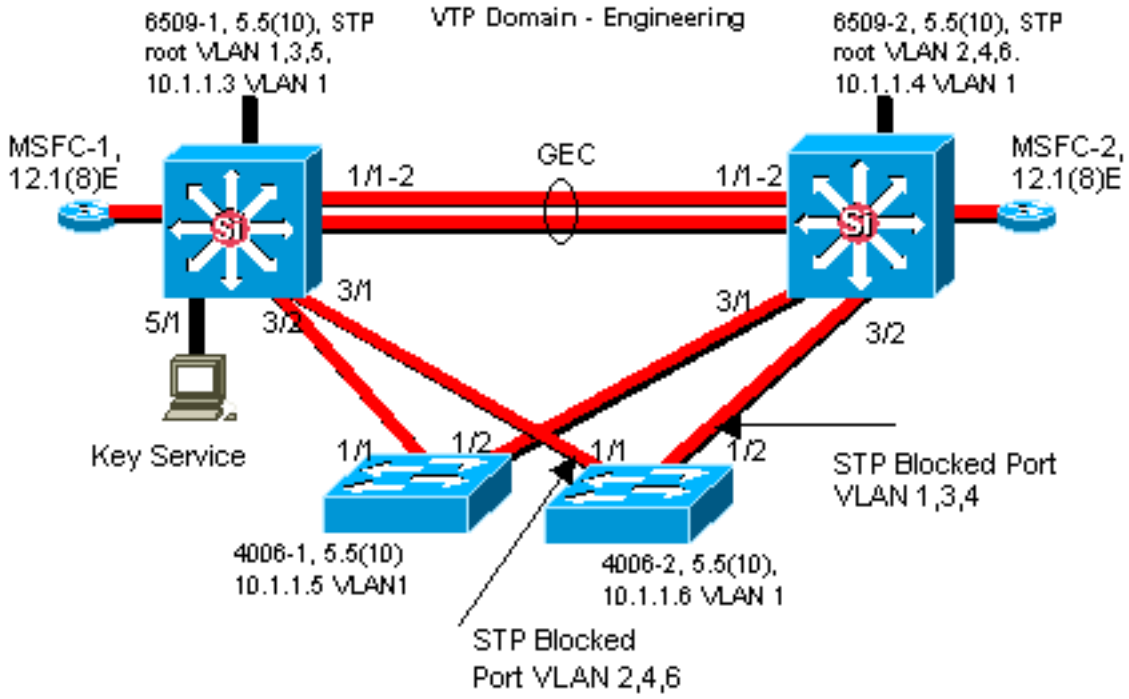
Netzwerkdiagramme

Klare Netzwerkdiagramme sind ein wesentlicher Bestandteil des Netzwerkbetriebs. Sie werden bei der Fehlerbehebung entscheidend und sind das wichtigste Medium für die Informationsweitergabe, wenn diese bei einem Ausfall an Anbieter und Partner eskaliert wird. Ihre Vorbereitung, Bereitschaft und Zugänglichkeit dürfen nicht unterschätzt werden.

Empfehlung

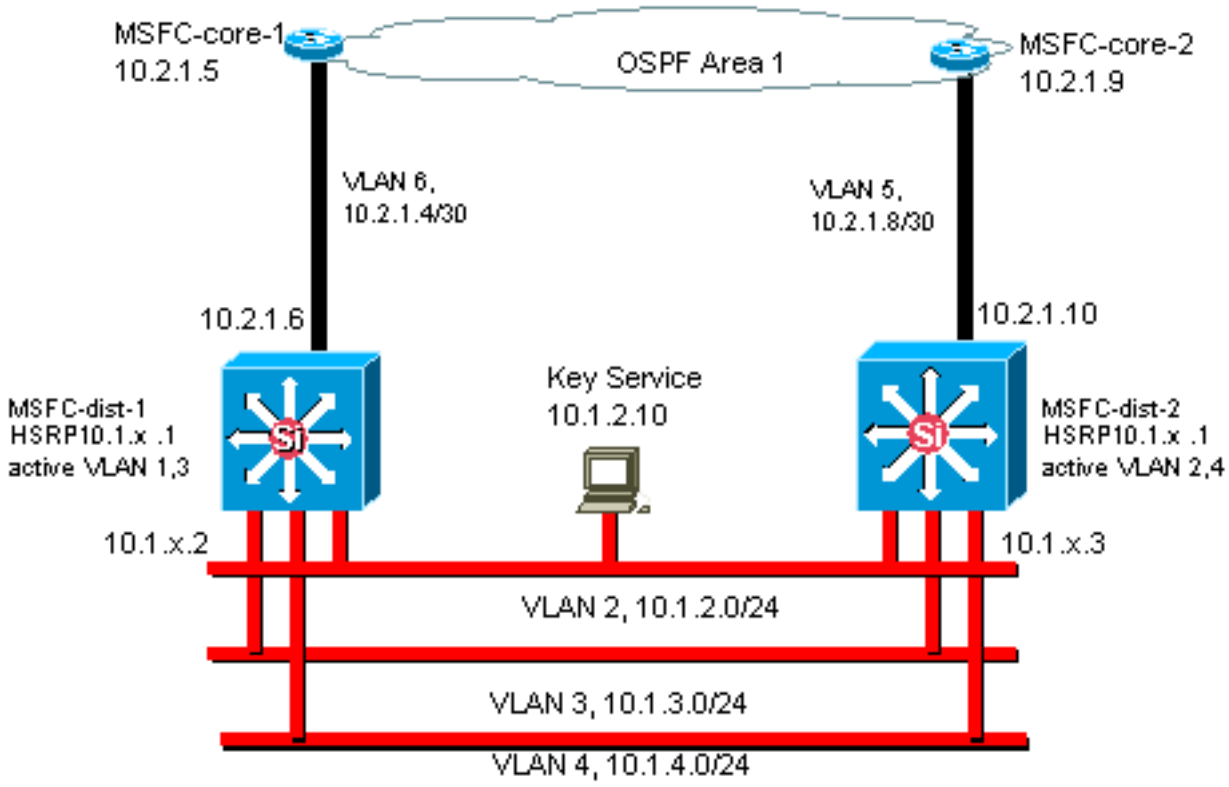
Cisco empfiehlt, die folgenden drei Diagramme zu erstellen:

- **Gesamtdiagramm** - selbst für die größten Netzwerke ist ein Diagramm wichtig, das die End-to-End-physische und logische Konnektivität zeigt. Unternehmen, die ein hierarchisches Design implementiert haben, können die einzelnen Ebenen häufig separat dokumentieren. Bei der Planung und Problemlösung ist es jedoch oft ein gutes Wissen darüber, wie die Domänen miteinander verknüpft sind.
- **Physisches Diagramm** - Zeigt alle Switch- und Router-Hardware und -Kabel an. Trunks, Links, Geschwindigkeiten, Channel-Gruppen, Portnummern, Steckplätze, Chassis-Typen, Software, VTP-Domänen, Root Bridge, Backup Root Bridge-Priorität, MAC-Adresse und blockierte Ports pro VLAN müssen gekennzeichnet werden. Häufig ist es klarer, interne Geräte wie die Catalyst 6500/6000 MSFC als Router auf einem über einen Trunk verbundenen Stick



darzustellen.

- **Logisches Diagramm** - Zeigt nur L3-Funktionen an (Router als Objekte, VLANs als Ethernet-Segmente). IP-Adressen, Subnetze, sekundäre Adressierung, HSRP Aktiv und Standby, Distribution Layer für den Access-Core und Routing-Informationen müssen gekennzeichnet werden.



In-Band-Management

Je nach Konfiguration muss die interne Switch-Verwaltungsschnittstelle (sc0) diese Daten verarbeiten:

- Switch-Management-Protokolle wie SNMP, Telnet, Secure Shell Protocol (SSH) und Syslog
- Benutzerdaten wie Broadcasts und Multicasts

- Switch-Steuerungsprotokolle wie STP BPDUs, VTP, DTP, CDP usw.

Im Multilayer-Design von Cisco ist es üblich, ein Verwaltungs-VLAN zu konfigurieren, das eine geschaltete Domäne umfasst und alle sc0-Schnittstellen enthält. Dadurch wird der Management-Datenverkehr vom Benutzerdatenverkehr getrennt und die Sicherheit der Switch-Management-Schnittstellen erhöht. In diesem Abschnitt werden die Bedeutung und die potenziellen Probleme beschrieben, die bei der Verwendung des Standard-VLAN 1 und bei der Ausführung des Verwaltungsdatenverkehrs zum Switch im selben VLAN wie beim Benutzerdatenverkehr auftreten können.

Überblick

Das Hauptproblem bei der Verwendung von VLAN 1 für Benutzerdaten besteht darin, dass der NMP der Supervisor Engine im Allgemeinen nicht durch einen Großteil des Multicast- und Broadcast-Datenverkehrs unterbrochen werden muss, der von Endstationen generiert wird. Ältere Catalyst 5500/500-Hardware, insbesondere die Supervisor Engine I und die Supervisor Engine II, verfügt nur über begrenzte Ressourcen, um mit diesem Datenverkehr umzugehen. Das Prinzip gilt jedoch für alle Supervisor Engines. Wenn die Supervisor Engine-CPU, der Puffer oder der In-Band-Kanal zur Backplane vollständig belegt sind und unnötigen Datenverkehr überwacht wird, können Kontrollrahmen möglicherweise verpasst werden. Im schlimmsten Fall kann dies zu einer Spanning Tree-Schleife oder einem EtherChannel-Ausfall führen.

Wenn die Befehle show interface und **show ip stats** auf dem Catalyst ausgegeben werden, können sie einen gewissen Hinweis auf den Anteil des Broadcast-Datenverkehrs an Unicast-Datenverkehr und den Anteil des IP-Datenverkehrs an Nicht-IP-Datenverkehr geben (wird in der Regel in Management-VLANs nicht angezeigt).

Eine weitere Integritätsprüfung für ältere Catalyst 5500/5000-Hardware besteht in der Untersuchung der Ausgabe von **show *inband*** | *biga* (ausgeblendeter Befehl) für Ressourcenfehler (RscrcErrors), ähnlich wie Pufferverluste in einem Router. Wenn diese Ressourcenfehler kontinuierlich ansteigen, steht Speicher nicht für den Empfang von Systempaketen zur Verfügung, möglicherweise wegen eines erheblichen Datenverkehrs im Management-VLAN. Ein einziger Ressourcenfehler kann bedeuten, dass die Supervisor Engine ein Paket wie BPDUs nicht verarbeiten kann, was schnell zu einem Problem werden könnte, da Protokolle wie Spanning Tree keine verpassten BPDUs erneut senden.

Empfehlung

Wie im Abschnitt Cat Control dieses Dokuments hervorgehoben, ist VLAN 1 ein spezielles VLAN, das den Großteil des Kontrollebenen-Datenverkehrs markiert und verarbeitet. VLAN 1 ist auf allen Trunks standardmäßig aktiviert. Bei größeren Campus-Netzwerken muss der Durchmesser der VLAN 1-**STP-Domäne** berücksichtigt werden. Instabilitäten in einem Teil des Netzwerks können VLAN 1 beeinträchtigen und somit die Stabilität der Kontrollebene und somit die STP-Stabilität für alle anderen VLANs beeinflussen. In CatOS 5.4 und höheren Versionen war es möglich, VLAN 1 so zu beschränken, dass es Benutzerdaten überträgt und STP mit dem folgenden Befehl ausführt:

```
clear trunk mod/port vlan 1
```

Dies verhindert jedoch nicht, dass vom Switch zum Switch in VLAN 1 gesendete Steuerungspakete gesendet werden, wie dies bei einem Netzwerkanalyst der Fall ist. Es werden jedoch keine Daten weitergeleitet, und STP wird nicht über diesen Link ausgeführt. Aus diesem

Grund kann mit dieser Technik VLAN 1 in kleinere Failure-Domains unterteilt werden.

Hinweis: Derzeit ist es nicht möglich, VLAN 1-Trunks auf 3500- und 2900XLs zu löschen.

Auch wenn beim Campus-Design darauf geachtet wurde, die Benutzer-VLANs auf relativ kleine Switch-Domänen und entsprechend kleine Ausfälle/L3-Grenzen zu beschränken, sind einige Kunden immer noch versucht, das Management-VLAN anders zu behandeln und versuchen, das gesamte Netzwerk mit einem einzigen Management-Subnetz abzudecken. Es gibt keinen technischen Grund, warum eine zentrale NMS-Anwendung an die verwalteten Geräte L2-angrenzt. Dies ist auch kein qualifiziertes Sicherheitsargument. Cisco empfiehlt, den Durchmesser der Management-VLANs auf dieselbe geroutete Domänenstruktur wie die Benutzer-VLANs zu beschränken und die Out-of-Band-Verwaltung und/oder CatOS 6.x SSH-Unterstützung als Möglichkeit zur Erhöhung der Sicherheit des Netzwerkmanagements in Betracht zu ziehen.

Weitere Optionen

Allerdings gibt es bei einigen Topologien Designüberlegungen für diese Cisco Empfehlungen. So ist z. B. ein wünschenswertes und gemeinsames Cisco Multilayer-Design geeignet, um die Verwendung eines aktiven Spanning Tree zu vermeiden. Dazu müssen Sie jedes IP-Subnetz/VLAN auf einen einzelnen Access-Layer-Switch oder ein Switch-Cluster beschränken. In diesen Designs konnte kein Trunking bis zum Access Layer konfiguriert werden.

Es gibt keine einfache Antwort auf die Frage, ob ein separates Management-VLAN erstellt und Trunking aktiviert wird, um es zwischen den L2-Access- und L3-Distribution-Layern zu übertragen. Es gibt zwei Optionen zur Überprüfung des Designs bei Ihrem Cisco Techniker:

- **Option 1:** zwei oder drei eindeutige VLANs vom Distribution Layer bis hin zu jedem Access-Layer-Switch miteinander verbinden. Dies ermöglicht beispielsweise ein Daten-VLAN, ein Sprach-VLAN und ein Management-VLAN und hat weiterhin den Vorteil, dass STP inaktiv ist. (Wenn VLAN 1 aus den Trunks entfernt wird, gibt es einen zusätzlichen Konfigurationsschritt.) Bei dieser Lösung sind außerdem Designaspekte zu berücksichtigen, um das vorübergehende Blackholing von geroutetem Datenverkehr bei der Wiederherstellung nach Ausfällen zu vermeiden: STP PortFast für Trunks (CatOS 7.x und höher) oder VLAN Autostate-Synchronisierung mit STP-Weiterleitung (später als CatOS 5.5[9]).
- **Option 2:** Ein einzelnes VLAN für Daten und Management könnte akzeptabel sein. Bei neuerer Switch-Hardware, wie z. B. leistungsstärkere CPUs und Kontrollen zur Ratenbegrenzung auf Kontrollebene, sowie einem Design mit relativ kleinen Broadcast-Domänen, wie es vom Multilayer-Design empfohlen wird, ist es für viele Kunden in der Realität so, dass die sc0-Schnittstelle von den Benutzerdaten getrennt zu halten weniger problematisch ist als früher. Eine endgültige Entscheidung treffen Sie wahrscheinlich am besten, wenn Sie das Broadcast-Datenverkehrsprofil für dieses VLAN prüfen und mit Ihrem Cisco Techniker über die Funktionen der Switch-Hardware sprechen. Wenn das Management-VLAN tatsächlich alle Benutzer auf diesem Access-Layer-Switch enthält, wird die Verwendung von IP-Eingabefeldern dringend empfohlen, um den Switch vor den Benutzern zu schützen, wie im Abschnitt Sicherheitskonfiguration dieses Dokuments beschrieben.

Out-of-Band-Management

Unter Berücksichtigung der Argumente des vorherigen Abschnitts kann die Netzwerkverwaltung

durch den Aufbau einer separaten Management-Infrastruktur im Produktionsnetzwerk erweitert werden, sodass Geräte unabhängig von Ereignissen auf Datenverkehrs- oder Kontrollebene immer remote erreichbar sind. Diese beiden Ansätze sind typisch:

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

Überblick

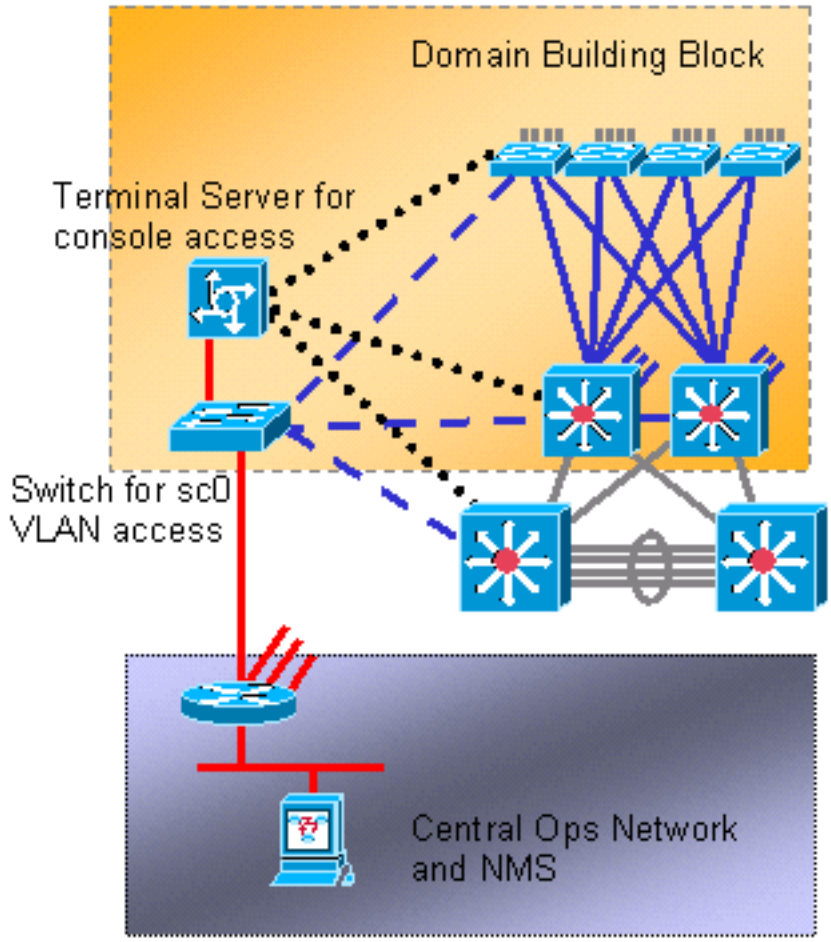
Jeder Router und Switch im Netzwerk kann über eine Out-of-Band-Ethernet-Managementschnittstelle in einem Management-VLAN bereitgestellt werden. Ein Ethernet-Port auf jedem Gerät wird im Management-VLAN konfiguriert und außerhalb des Produktionsnetzwerks über die sc0-Schnittstelle mit einem separaten Switch-Management-Netzwerk verkabelt. Beachten Sie, dass die Catalyst 4500/4000-Switches über eine spezielle Me1-Schnittstelle auf der Supervisor Engine verfügen, die nur für das Out-of-Band-Management, nicht als Switch-Port, verwendet wird.

Darüber hinaus kann die Terminalserver-Konnektivität durch die Konfiguration eines Cisco 2600 oder 3600 mit RJ-45-zu-Serial-Kabeln erreicht werden, um auf den Konsolenport jedes Routers und Switches im Layout zuzugreifen. Ein Terminalserver vermeidet auch die Notwendigkeit der Konfiguration von Backup-Szenarien, wie Modems an AUX-Ports für jedes Gerät. Ein Modem kann auf dem AUX-Port des Terminalservers konfiguriert werden, um bei einem Ausfall der Netzwerkverbindung Einwahldienst für die anderen Geräte bereitzustellen.

Empfehlung

Bei dieser Anordnung sind neben zahlreichen In-Band-Pfaden zwei Out-of-Band-Pfade zu jedem Switch und Router möglich, um ein hochverfügbares Netzwerkmanagement zu ermöglichen. Out-of-Band ist verantwortlich für:

- Out-of-Band trennt den Verwaltungsdatenverkehr von den Benutzerdaten.
- Out-of-Band verfügt über die Management-IP-Adresse in einem separaten Subnetz, VLAN und Switch für eine höhere Sicherheit.
- Out-of-Band bietet eine höhere Sicherheit für die Bereitstellung von Managementdaten bei Netzwerkausfällen.
- Out-of-Band hat kein aktives Spanning Tree im Management-VLAN. Redundanz ist nicht entscheidend.



Systemtests

Startdiagnose

Beim Systemstart werden mehrere Prozesse durchgeführt, um sicherzustellen, dass eine zuverlässige und betriebsbereite Plattform verfügbar ist, sodass fehlerhafte Hardware das Netzwerk nicht stört. Die Catalyst-Startdiagnose ist in den Einschalt-Selbsttest (POST) und die Online-Diagnose aufgeteilt.

Überblick

Je nach Plattform- und Hardwarekonfiguration werden beim Hochfahren und beim Hot-Swap einer Karte unterschiedliche Diagnosen durchgeführt. Eine höhere Diagnosestufe führt zu einer größeren Anzahl von erkannten Problemen, jedoch zu einem längeren Bootzyklus. Diese drei Stufen der POST-Diagnose können ausgewählt werden (alle Tests überprüfen DRAM, RAM und Cache-Präsenz und -Größe und initialisieren diese):

Überblick			
Umgehen	K/A	1	Nicht verfügbar für Serie 4500/4000 mit CatOS 5.5 oder früher.
Minimal	Musterschreibtests nur auf der ersten MB des DRAM.	30	Standard für die Serien 5500/5000 und 6500/6000; nicht verfügbar für Serie

			4500/4000.
Abgeschlossen	Musterschreibtests für alle Speicher.	60	Standard für die Serie 4500/4000.

Online-Diagnose

Diese Tests überprüfen die Paketpfade intern im Switch. Hierbei ist zu beachten, dass Online-Diagnosen daher systemweite Tests sind und nicht nur Port-Tests. Bei Catalyst Switches der Serien 5500/500 und 6500/6000 werden die Tests zuerst von der Standby-Supervisor Engine und wieder von der primären Supervisor Engine durchgeführt. Die Länge der Diagnose hängt von der Systemkonfiguration ab (Anzahl der Steckplätze, Module, Ports). Es gibt drei Testkategorien:

- Loopback-Test - Pakete vom Supervisor Engine NMP werden an jeden Port gesendet, dann an den NMP zurückgesendet und auf Fehler überprüft.
- Pakettest - Es werden Kanäle von bis zu acht Ports erstellt und Loopback-Tests für den Port durchgeführt, um das Hashing für bestimmte Verbindungen zu überprüfen (weitere Informationen finden Sie im EtherChannel-Abschnitt dieses Dokuments).
- Enhanced Address Recognition Logic (EARL)-Test - Sowohl die zentrale Supervisor Engine als auch die In-Line Ethernet-Modul L3-Rewrite-Engines werden getestet. Vor dem Versenden von Beispielpaketen (für jeden Protokollkapselungstyp) vom NMP über die Switching-Hardware der einzelnen Module und zurück an den NMP werden Einträge für die Hardware-Weiterleitung und geroutete Ports erstellt. Dies gilt für Catalyst 6500/6000 PFC-Module und neuere Versionen.

Die vollständige Online-Diagnose kann etwa zwei Minuten in Anspruch nehmen. Die Minimaldiagnose führt keine Paketprüfung durch oder schreibt die Tests für andere Module als die Supervisor Engine neu. Sie kann ungefähr 90 Sekunden dauern.

Wenn während eines Speichertests beim Zurücklesen des Musters im Vergleich zum geschriebenen Muster ein Unterschied festgestellt wird, wird der Portstatus auf `defekt` geändert. Die Ergebnisse dieser Tests sind sichtbar, wenn der Befehl **show test** ausgeführt wird, gefolgt von der zu prüfenden Modulnummer:

```
>show test 9

Diagnostic mode: complete (mode at next reset: complete)
!--- Configuration setting. Module 9 : 4-port Multilayer Switch Line Card Status for Module 9 :
PASS Port Status : Ports 1 2 3 4 ---------------- . . . . Line Card Diag Status for Module 9 (.
= Pass, F = Fail, N = N/A) Loopback Status [Reported by Module 1] : Ports 1 2 3 4 -------------
--- . . F . !--- Faulty. Channel Status : Ports 1 2 3 4 ---------------- . . . .
```

Empfehlung

Cisco empfiehlt, dass alle Switches so konfiguriert werden, dass sie eine vollständige Diagnose ausführen, um eine maximale Fehlererkennung zu ermöglichen und Ausfälle während des normalen Betriebs zu verhindern.

Hinweis: Diese Änderung wird erst beim nächsten Booten des Geräts wirksam. Führen Sie diesen Befehl aus, um die vollständige Diagnose festzulegen:

```
set test diaglevel complete
```

Weitere Optionen

In manchen Fällen ist eine schnelle Systemstartzeit vorzuziehen, wenn auf die Ausführung einer vollständigen Diagnose gewartet wird. Es gibt noch weitere Faktoren und Zeitpunkte, die bei der Einrichtung eines Systems eine Rolle spielen. Insgesamt ergeben der POST-Test und die Online-Diagnose jedoch ein Drittel mehr. Bei Tests mit einem vollständig bestückten Einzel-Supervisor Engine-Chassis mit neun Steckplätzen und einem Catalyst 6509 betrug die Gesamtstartzeit bei vollständiger Diagnose etwa 380 Sekunden, bei minimaler Diagnose etwa 300 Sekunden und bei überholter Diagnose nur 250 Sekunden. Geben Sie diesen Befehl ein, um die Umgehung zu konfigurieren:

```
set test diaglevel bypass
```

Hinweis: Der Catalyst 4500/4000 akzeptiert die Konfiguration einer Minimaldiagnose, obwohl dies dennoch zu einem vollständigen Test führt. Der Minimalmodus könnte in Zukunft auf dieser Plattform unterstützt werden.

Zeitdiagnose ausführen

Sobald das System betriebsbereit ist, überwacht die Switch Supervisor Engine die anderen Module. Wenn ein Modul nicht über die Managementnachrichten (Serial Control Protocol [SCP], die über den Out-of-Band-Managementbus ausgeführt werden) erreichbar ist, versucht die Supervisor Engine, die Karte neu zu starten oder gegebenenfalls andere Maßnahmen zu ergreifen.

Überblick

Die Supervisor Engine führt automatisch verschiedene Überwachungsfunktionen aus. Dies erfordert keine Konfiguration. Für Catalyst 5500/5000 und 6500/6000 werden diese Komponenten des Switches überwacht:

- NMP durch einen Watchdog
- Erweiterte EARL-Chip-Fehler
- In-Band-Kanal von der Supervisor Engine zur Backplane
- Module über Keepalives über Out-of-Band-Kanal (Catalyst 6500/6000)
- Die aktive Supervisor Engine wird von der Standby-Supervisor Engine hinsichtlich des Status überwacht (Catalyst 6500/6000).

System- und Hardwarefehlererkennung

Überblick

In CatOS 6.2 und höher wurden weitere Funktionen hinzugefügt, um kritische Komponenten auf System- und Hardware-Ebene zu überwachen. Diese drei Hardwarekomponenten werden unterstützt:

- Inband
- Port-Zähler
- Arbeitsspeicher

Wenn die Funktion aktiviert ist und ein Fehlerzustand erkannt wird, generiert der Switch eine Syslog-Meldung. Die Meldung informiert den Administrator, dass ein Problem vorliegt, bevor eine spürbare Leistungsminderung auftritt. In CatOS-Versionen 6.4(16), 7.6(12), 8.4(2) und höher wurde der Standardmodus für alle drei Komponenten von "Deaktiviert" in "Aktiviert" geändert.

Inband

Wenn ein In-Band-Fehler erkannt wird, werden Sie durch eine Syslog-Meldung darüber informiert, dass ein Problem vorliegt, bevor eine spürbare Leistungsminderung auftritt. Der Fehler zeigt die Art des Inband-Fehlers an. Beispiele:

- In-Band fixiert
- Ressourcenfehler
- Die Inband schlägt beim Hochfahren fehl.

Bei der Erkennung eines Inband-Ping-Fehlers meldet die Funktion außerdem eine zusätzliche Syslog-Meldung mit einem Snapshot der aktuellen Tx- und Rx-Rate für die Inband-Verbindung, CPU und die Backplane-Last des Switches. Mit dieser Meldung können Sie feststellen, ob das In-Band feststeckt (kein Tx/Rx) oder überladen (übermäßiges Tx/Rx). Diese zusätzlichen Informationen können Ihnen dabei helfen, die Ursache von Inband-Ping-Fehlern zu ermitteln.

Port-Zähler

Wenn Sie dieses Feature aktivieren, wird ein Prozess zum Debuggen von Port-Zählern erstellt und gestartet. Der Port-Zähler überwacht regelmäßig ausgewählte interne Port-Fehlerzähler. Die Architektur der Linecard und insbesondere die ASICs auf dem Modul bestimmen, welche Zähler die Feature-Abfragen auslösen. Der technische Support oder die Entwicklungsabteilung von Cisco können diese Informationen dann zur Fehlerbehebung verwenden. Diese Funktion fragt keine Fehlerzähler wie FCS, CRC, Alignment und Runts ab, die direkt mit der Link-Partner-Verbindung verknüpft sind. Informationen zum Einbinden dieser Funktion finden Sie im Abschnitt EtherChannel/Link Errors Handling dieses Dokuments.

Das Polling wird alle 30 Minuten ausgeführt und im Hintergrund ausgewählter Fehlerindikatoren ausgeführt. Wenn die Anzahl zwischen zwei nachfolgenden Umfragen auf demselben Port ansteigt, meldet eine Syslog-Meldung den Vorfall und gibt Details zu Modul/Port und Fehlerzähler an.

Die Port-Zähleroption wird auf der Catalyst 4500/4000-Plattform nicht unterstützt.

Arbeitsspeicher

Durch die Aktivierung dieser Funktion werden Hintergrundüberwachung und die Erkennung von DRAM-Korruptionsbedingungen durchgeführt. Zu diesen Speicherbeschädigungsbedingungen gehören:

- Zuweisung
- Freistellung
- Außerhalb des Bereichs

- Fehlerhafte Ausrichtung

Empfehlung

Aktivieren Sie alle Fehlererkennungsfunktionen, z. B. In-Band, Port-Zähler und Speicher, wo diese unterstützt werden. Durch die Aktivierung dieser Funktionen wird eine verbesserte proaktive Diagnose von System- und Hardwarewarnungen für die Catalyst Switch-Plattform ermöglicht. Führen Sie die folgenden Befehle aus, um alle drei Fehlererkennungsfunktionen zu aktivieren:

```
set errordetection inband enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection
portcounters enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection memory
enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later.
```

Führen Sie diesen Befehl aus, um zu bestätigen, dass die Fehlererkennung aktiviert ist:

```
>show errordetection

Inband error detection:                  enabled
Memory error detection:                  enabled
Packet buffer error detection:           errdisable
Port counter error detection:            enabled
Port link-errors detection:              disabled
Port link-errors action:                 port-failover
Port link-errors interval:               30 seconds
```

Behandeln von EtherChannel-/Link-Fehlern

Überblick

In CatOS 8.4 und höher wurde eine neue Funktion eingeführt, um ein automatisches Failover des Datenverkehrs von einem Port in einem EtherChannel zu einem anderen Port im gleichen EtherChannel zu ermöglichen. Der Port-Failover tritt auf, wenn einer der Ports im Kanal innerhalb des angegebenen Intervalls einen konfigurierbaren Fehlergrenzwert überschreitet. Der Port-Failover tritt nur dann auf, wenn ein betrieblicher Port im EtherChannel übrig ist. Wenn der ausgefallene Port der letzte Port im EtherChannel ist, wechselt der Port nicht in den `Port-Failover-` Status. Dieser Port leitet den Datenverkehr weiter, unabhängig von der Art der Fehler, die empfangen werden. Einzelne Ports ohne Kanalfunktion wechseln nicht in den `Port-Failover-` Zustand. Diese Ports gelangen in den `errdisable-`Status, wenn die Fehlerschwelle innerhalb des angegebenen Intervalls überschritten wird.

Diese Funktion ist nur dann wirksam, wenn Sie **Fehlererkennungsindikatoren festlegen**. Die zu überwachenden Verbindungsfehler basieren auf drei Zählern:

- InErrors
- RxCRCs (CRCAlignErrors)
- TxCRCs

Geben Sie den Befehl show counter auf einem Switch aus, um die Anzahl der Fehlerzähler anzuzeigen. Dies ist ein Beispiel:

```
>show counters 4/48

.......

32 bit counters

0  rxCRCAlignErrors           =          0
.......

6  ifInErrors                 =          0
.......

12 txCRC                      =          0
```

Diese Tabelle enthält eine Liste möglicher Konfigurationsparameter und der entsprechenden Standardkonfiguration:

Parameter	Standard
global	Deaktiviert
Port-Monitor für RxCRC	Deaktiviert
Port-Monitor für InErrors	Deaktiviert
Port-Monitor für TxCRC	Deaktiviert
Aktion	Port-Failover
Intervall	30 Sekunden
Anzahl der Stichproben	3 aufeinander folgend
Niedriger Grenzwert	1000
Hoher Grenzwert	1001

Wenn die Funktion aktiviert ist und die Fehleranzahl eines Ports den hohen Wert des konfigurierbaren Grenzwerts innerhalb der festgelegten Abtastrate erreicht, ist die konfigurierbare Aktion entweder "error disable" oder "port failover". Durch die Aktion "Error disable" wird der Port in den `errdisable-`Status versetzt. Wenn Sie die Port-Failover-Aktion konfigurieren, wird der Port-Channel-Status berücksichtigt. Der Port ist nur dann fehlerhaft, wenn sich der Port in einem Kanal befindet, dieser Port jedoch nicht der letzte betriebliche Port im Kanal ist. Wenn die konfigurierte Aktion ein Port-Failover ist und der Port ein einzelner oder nicht-kanalisierter Port ist, wird der Port im `errdisable-`Status platziert, wenn die Anzahl der Port-Fehler den hohen Wert des Schwellenwerts erreicht.

Das Intervall ist eine Timer-Konstante für das Lesen der Port-Fehlerzähler. Der Standardwert des Intervalls für Verbindungsfehler beträgt 30 Sekunden. Der zulässige Bereich liegt zwischen 30 und 1800 Sekunden.

Ein Port kann aufgrund eines unerwarteten einmaligen Ereignisses versehentlich aufgrund eines Fehlers deaktiviert werden. Um dieses Risiko zu minimieren, werden Aktionen für einen Port nur dann durchgeführt, wenn der Zustand in dieser Folge mehrere Male andauert. Der Standardwert für die Probenahme ist 3 und der zulässige Bereich liegt zwischen 1 und 255.

Der Schwellenwert ist eine absolute Zahl, die auf Basis des Intervalls für Verbindungsfehler überprüft werden muss. Der niedrige Standardwert für Verbindungsfehler ist 1000 und der zulässige Bereich ist 1 bis 65.535. Der Standard-Schwellenwert für Verbindungsfehler ist 1001. Wenn die Anzahl der ununterbrochenen Probenahmezeiten den unteren Grenzwert erreicht, wird ein Syslog gesendet. Wenn die aufeinander folgenden Probenahmezeiten den hohen Grenzwert

erreichen, wird ein Syslog gesendet, und es wird ein Fehler deaktiviert oder eine Port-Failover-Aktion ausgelöst.

Hinweis: Verwenden Sie für alle Ports in einem Kanal dieselbe Konfiguration zur Erkennung von Port-Fehlern. Weitere Informationen finden Sie in den folgenden Abschnitten des Software-Konfigurationsleitfadens für die Catalyst 6500-Serie:

- Der Abschnitt *Konfigurieren der Fehlerbehandlung bei EtherChannel-/Link-Fehlern* überprüft Status und Konnektivität.
- Der Abschnitt *zur* Konfiguration der Erkennung von *Portfehlern* enthält die Konfiguration von Ethernet-, Fast Ethernet-, Gigabit Ethernet- und 10-Gigabit Ethernet-Switching.

Empfehlungen

Da die Funktion SCP-Nachrichten zum Aufzeichnen und Vergleichen der Daten verwendet, kann eine große Anzahl aktiver Ports CPU-intensiv sein. Dieses Szenario ist noch CPU-intensiver, wenn das Grenzwertintervall auf einen sehr kleinen Wert festgelegt wird. Aktivieren Sie diese Funktion nach eigenem Ermessen für Ports, die als kritische Verbindungen festgelegt sind, und übertragen Sie Datenverkehr für vertrauliche Anwendungen. Führen Sie diesen Befehl aus, um die Erkennung von Verbindungsfehlern global zu aktivieren:

```
set errordetection link-errors enable
```

Beginnen Sie außerdem mit dem Standardgrenzwert, dem Standardintervall und den Sampling-Parametern. Verwenden Sie die Standardaktion "Port Failover".

Führen Sie die folgenden Befehle aus, um die globalen Link-Error-Parameter auf einzelne Ports anzuwenden:

```
set port errordetection mod/port inerrors enable

set port errordetection mod/port rxcrc enable

set port errordetection mod/port txcrc enable
```

Sie können die folgenden Befehle ausgeben, um die Konfiguration für Verbindungsfehler zu überprüfen:

```
show errordetection

show port errordetection {mod | mod/port}
```

Catalyst 6500/6000 Paketpuffer-Diagnose

In CatOS 6.4(7), 7.6(5) und 8.2(1) wurde die Paketpufferdiagnose für Catalyst 6500/6000 eingeführt. Die standardmäßig aktivierten Paketpufferdiagnosen erkennen Paketpufferausfälle, die durch vorübergehende SRAM-Ausfälle (Static RAM) verursacht werden. Die Erkennung erfolgt bei

diesen 10/100-Mbit/s-Leitungsmodulen mit 48 Ports:

- WS-X6248-RJ45
- WS-X6248-RJ21
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6148-RJ45
- WS-X6148-RJ21

Bei einem Ausfall bleiben 12 von 48 10/100-Mbit/s-Ports weiterhin verbunden und können zufällige Verbindungsprobleme aufweisen. Die einzige Möglichkeit zur Wiederherstellung nach diesem Zustand besteht darin, das Leitungsmodul aus- und wieder einzuschalten.

Überblick

Die Paketpufferdiagnose überprüft die Daten, die in einem bestimmten Abschnitt des Paketpuffers gespeichert sind, um festzustellen, ob sie durch vorübergehende SRAM-Ausfälle beschädigt sind. Wenn der Prozess etwas Anderes liest als das, was er geschrieben hat, führt er zwei mögliche konfigurierbare Wiederherstellungsoptionen durch:

1. Die Standardaktion besteht darin, die Line Card-Ports zu deaktivieren, die vom Pufferfehler betroffen sind.
2. Die zweite Option besteht darin, die Linecard aus- und wieder einzuschalten.

Zwei Syslog-Meldungen wurden hinzugefügt. Die Meldungen geben eine Warnung vor der fehlerhaften Deaktivierung der Ports oder dem Aus- und Wiedereinschalten des Moduls aufgrund von Paketpufferfehlern aus:

```
%SYS-3-PKTBUFFERFAIL_ERRDIS:Packet buffer failure detected.
Err-disabling port 5/1.
%SYS-3-PKTBUFFERFAIL_PWRCYCLE: Packet buffer failure detected.
Power cycling module 5.
```

In CatOS-Versionen, die älter als 8.3 und 8.4 sind, beträgt die Power-Cycle-Zeit der Linecards zwischen 30 und 40 Sekunden. In CatOS 8.3 und 8.4 wurde eine Rapid Boot-Funktion eingeführt. Die Funktion lädt die Firmware während des Startvorgangs automatisch auf die installierten Linecards herunter, um die Startzeit zu minimieren. Die Rapid Boot-Funktion verkürzt den Ein- und Ausschaltvorgang auf ca. 10 Sekunden.

Empfehlung

Cisco empfiehlt die Standardoption *errdisable*. Diese Aktion hat während der Produktionszeiten die geringsten Auswirkungen auf den Netzwerkservice. Wenn möglich, verschieben Sie die Verbindung, die von den fehlerhaft deaktivierten Ports betroffen ist, auf andere verfügbare Switch-Ports, um den Dienst wiederherzustellen. Planen Sie während des Wartungsfensters ein manuelles Ein- und Ausschalten der Linecard. Geben Sie den Befehl **reset module *mod*** ein, um die beschädigte Paketpufferbedingung vollständig zu beheben.

Hinweis: Wenn die Fehler nach dem Zurücksetzen des Moduls weiter bestehen, versuchen Sie, das Modul wieder einzusetzen.

Geben Sie diesen Befehl ein, um die *errdisable*-Option zu aktivieren:

```
set errordetection packet-buffer errdisable
!--- This is the default.
```

Andere Option

Da ein Aus- und Wiedereinschalten der Linecard erforderlich ist, um alle Ports, bei denen ein SRAM-Ausfall aufgetreten ist, vollständig wiederherzustellen, besteht eine Alternative zur Wiederherstellung in der Konfiguration der Aus- und Wiedereinschaltoption. Diese Option ist nützlich, wenn ein Ausfall von Netzwerkservices zwischen 30 und 40 Sekunden akzeptabel ist. Diese Zeitdauer ist die Zeit, die ein Line-Modul benötigt, um ohne die Rapid Boot-Funktion vollständig ein- und auszuschalten und wieder in Betrieb zu nehmen. Mit der Option zum Ein- und Ausschalten kann die Rapid Boot-Funktion die Ausfallzeit der Netzwerkdienste auf 10 Sekunden reduzieren. Geben Sie diesen Befehl ein, um die Option zum Ein- und Ausschalten zu aktivieren:

```
set errordetection packet-buffer power-cycle
```

Paketpufferdiagnose

Dieser Test ist nur für Catalyst 5500/5000-Switches vorgesehen. Dieser Test wurde entwickelt, um fehlerhafte Hardware auf Catalyst 5500/500-Switches zu finden, die Ethernet-Module mit spezieller Hardware verwenden, die 10/100-Mbit/s-Verbindungen zwischen Benutzerports und der Switch-Backplane bereitstellen. Da sie keine CRC-Prüfung auf gebündelte Frames durchführen können, können Pakete beschädigt werden und CRC-Fehler verursachen, wenn während der Laufzeit ein Port-Paket-Puffer fehlerhaft ist. Unglücklicherweise kann dies dazu führen, dass fehlerhafte Frames weiter in das ISL-Netzwerk des Catalyst 5500/500 weitergeleitet werden, was im schlimmsten Fall zu Unterbrechungen der Kontrollebene und Broadcast-Stürmen führen kann.

Neuere Catalyst 5500/500-Module und andere Plattformen verfügen über aktualisierte integrierte Hardwarefehlerüberprüfung und benötigen die Paketpuffertests nicht, daher gibt es keine Konfigurationsoption.

Die Leitungsmodule, die die Paketpufferdiagnose benötigen, sind WS-X5010, WS-X5011, WS-X5013, WS-X5020, WS-X5111, WS-X5113, WS-X5114, WS-X5. WS-X5203, WS-X5213/a, WS-X5223, WS-X5224, WS-X5506, WS-X5509, WS-U5531, WS-U55 33 und WS-U5535.

Überblick

Diese Diagnose überprüft, ob die in einem bestimmten Abschnitt des Paketpuffers gespeicherten Daten nicht versehentlich durch fehlerhafte Hardware beschädigt werden. Wenn der Prozess etwas Anderes liest, als er geschrieben hat, wird der Port im `ausgefallenen` Modus deaktiviert, da dieser Port Daten beschädigen kann. Es ist kein Schwellenwert für Fehler erforderlich. Ausgefallene Ports können erst wieder aktiviert werden, wenn das Modul zurückgesetzt (oder ersetzt) wurde.

Für Paketpuffertests gibt es zwei Modi: geplant und nach Bedarf. Wenn ein Test beginnt, werden Syslog-Meldungen generiert, um die erwartete Testdauer (aufgerundet auf die nächste Minute) und die Tatsache anzugeben, dass der Test begonnen hat. Die genaue Länge des Tests variiert je nach Port-Typ, Größe des Puffers und Art des Testlaufs.

On-Demand-Tests sind aggressiv, um innerhalb weniger Minuten abgeschlossen zu sein. Da diese Tests den Paketspeicher aktiv stören, müssen die Ports vor dem Testen vom Administrator geschlossen werden. Geben Sie diesen Befehl ein, um die Ports herunterzufahren:

```
> (enable) test packetbuffer 4/1
Warning: only disabled ports may be tested on demand - 4/1 will be skipped.
> (enable) set port disable 4/1
> (enable) test packetbuffer 4/1
Packet buffer test started. Estimated test time: 1 minute.
%SYS-5-PKTTESTSTART:Packet buffer test started
%SYS-5-PKTTESTDONE:Packet buffer test done. Use 'show test' to see test results
```

Geplante Tests sind weitaus weniger aggressiv als On-Demand-Tests und werden im Hintergrund ausgeführt. Die Tests werden parallel über mehrere Module hinweg, jedoch jeweils an einem Port pro Modul durchgeführt. Der Test behält, schreibt und liest kleine Abschnitte des Paketpufferspeichers, bevor die Daten des Benutzerpaketpuffers wiederhergestellt werden, und generiert somit keine Fehler. Da der Test jedoch in Pufferspeicher geschrieben wird, blockiert er eingehende Pakete für einige Millisekunden und verursacht einen gewissen Verlust bei ausgelasteten Verbindungen. Standardmäßig gibt es zwischen jedem Pufferschreibtest eine Pause von acht Sekunden, um Paketverluste zu minimieren. Dies bedeutet jedoch, dass ein System mit vielen Modulen, die den Paketpuffertest benötigen, mehr als 24 Stunden dauern kann, bis der Test abgeschlossen ist. Dieser geplante Test ist standardmäßig aktiviert, damit er an Sonntagen ab CatOS 5.4 wöchentlich um 03:30 Uhr ausgeführt werden kann. Der Teststatus kann mit dem folgenden Befehl bestätigt werden:

```
>show test packetbuffer status

!--- When test is running, the command returns !--- this information: Current packet buffer test
details Test Type : scheduled Test Started : 03:30:08 Jul 20 2001 Test Status : 26% of ports
tested Ports under test : 10/5,11/2 Estimated time left : 11 minutes !--- When test is not
running, !--- the command returns this information: Last packet buffer test details Test Type :
scheduled Test Started : 03:30:08 Jul 20 2001 Test Finished : 06:48:57 Jul 21 2001
```

Empfehlung

Cisco empfiehlt die Verwendung der Funktion zum Testen des geplanten Paketpuffers für Catalyst 5500/5000-Systeme, da der Vorteil der Erkennung von Modulproblemen das Risiko eines geringen Paketverlusts überwiegt.

Anschließend muss eine standardisierte wöchentliche Zeit im gesamten Netzwerk geplant werden, sodass der Kunde ggf. Links von fehlerhaften Ports oder RMA-Modulen ändern kann. Da dieser Test, abhängig von der Netzwerkauslastung, einen gewissen Paketverlust verursachen kann, muss er für ruhigere Netzwerkzeiten geplant werden, z. B. für die Standardeinstellung von 3:30 Uhr an einem Sonntagmorgen. Geben Sie diesen Befehl ein, um die Testzeit festzulegen:

```
set test packetbuffer Sunday 3:30
!--- This is the default.
```

Wenn diese Option aktiviert ist (z. B. wenn CatOS zum ersten Mal auf 5.4 und höher aktualisiert wird), besteht die Möglichkeit, dass ein zuvor verborgenes Speicher-/Hardwareproblem verfügbar gemacht wird und ein Port automatisch heruntergefahren wird. Sie können diese Meldung sehen:

```
%SYS-3-PKTBUFBAD:Port 1/1 failed packet buffer test
```

Weitere Optionen

Wenn es nicht akzeptabel ist, wöchentlich einen geringen Paketverlust pro Port zu riskieren, wird empfohlen, die On-Demand-Funktion bei geplanten Ausfällen zu verwenden. Geben Sie diesen Befehl ein, um diese Funktion manuell für jeden Bereich zu starten (obwohl der Port zuerst vom Administrator deaktiviert werden muss):

```
test packetbuffer port range
```

Systemprotokollierung

Syslog-Meldungen sind für Cisco spezifisch und stellen eine wichtige Komponente des proaktiven Fehlermanagements dar. Ein breiteres Spektrum an Netzwerk- und Protokollbedingungen wird mithilfe von Syslog gemeldet, als durch standardisiertes SNMP möglich ist. Verwaltungsplattformen wie Cisco Resource Manager Essentials (RMEs) und das Network Analysis Toolkit (NATkit) nutzen Syslog-Informationen sehr gut, da sie diese Aufgaben ausführen:

- Analyse nach Schweregrad, Meldung, Gerät usw.
- Filtern von eingehenden Nachrichten zur Analyse aktivieren
- Auslösen von Warnmeldungen wie Pagern oder On-Demand-Erfassung von Bestands- und Konfigurationsänderungen

Empfehlung

Ein wichtiger Punkt ist, welche Protokollierungsinformationen lokal generiert und im Switch-Puffer gespeichert werden sollen, im Gegensatz zu dem, der an einen Syslog-Server gesendet wird (unter Verwendung des Befehls zum *Schweregrad des Protokollierungsservers*). Einige Unternehmen protokollieren ein hohes Maß an Informationen zentral, während andere den Switch selbst aufsuchen, um detailliertere Protokolle für ein Ereignis anzuzeigen oder eine höhere Ebene der Syslog-Erfassung nur bei der Fehlerbehebung zu ermöglichen.

Das Debuggen ist auf CatOS-Plattformen anders als bei der Cisco IOS-Software. Die detaillierte Systemprotokollierung kann jedoch pro Sitzung aktiviert werden, wobei die Standardprotokollierungssitzung aktiviert ist, ohne dass die Standardprotokollierung geändert wird.

Cisco empfiehlt in der Regel, die spanischen Baum- und System-Syslog-Anlagen auf die Ebene 6 zu bringen, da dies wichtige Stabilitätsfunktionen sind. Darüber hinaus wird für Multicast-Umgebungen empfohlen, die Protokollierungsebene der Mcast-Einrichtung auf bis zu 4 zu erhöhen, sodass Syslog-Meldungen generiert werden, wenn Router-Ports gelöscht werden. Leider kann dies vor CatOS 5.5(5) dazu führen, dass Syslog-Meldungen für IGMP-Joins und -Blätter aufgezeichnet werden, was zu laut ist, um sie zu überwachen. Wenn IP-Eingabelisten verwendet werden, wird eine Protokollierungsebene von mindestens 4 empfohlen, um nicht autorisierte Anmeldeversuche zu erfassen. Geben Sie die folgenden Befehle ein, um folgende Optionen festzulegen:

```
set logging buffer 500
!--- This is the default. set logging server syslog server IP address set logging server enable
!--- This is the default. set logging timestamp enable
```

```
set logging level spantree 6 default
!--- Increase default STP syslog level. set logging level sys 6 default
!--- Increase default system syslog level. set logging server severity 4
!--- This is the default; !--- it limits messages exported to syslog server. set logging console
disable
```

Schalten Sie die Konsolenmeldungen aus, um sich vor dem Risiko zu schützen, dass der Switch beim Warten auf eine Antwort eines langsamen oder nicht vorhandenen Terminals hängt, wenn das Nachrichtenvolumen hoch ist. Die Konsolenprotokollierung ist eine hohe Priorität unter CatOS und wird hauptsächlich verwendet, um die letzten Meldungen lokal bei der Fehlerbehebung oder bei einem Switch-Absturz zu erfassen.

Diese Tabelle enthält die einzelnen Protokollierungsfunktionen, die Standardwerte und die empfohlenen Änderungen für Catalyst 6500/6000. Jede Plattform verfügt je nach unterstützten Funktionen über leicht unterschiedliche Einrichtungen.

Einrichtung	Standardstufe	Empfohlene Aktion
ACL	5	Lass dich in Ruhe!
CDP	4	Lass dich in Ruhe!
Bullen	1	Lass dich in Ruhe!
TCP	8	Lass dich in Ruhe!
Ohrfeige	2	Lass dich in Ruhe!
Ethisch[1]	5	Lass dich in Ruhe!
Dateien	2	Lass dich in Ruhe!
GVRP	2	Lass dich in Ruhe!
IP	2	**Bei Verwendung von IP-Eingabelisten in 4 ändern.**
Kernel	2	Lass dich in Ruhe!
1 d	1	Lass dich in Ruhe!
Mast	2	**Bei Verwendung von Multicast (CatOS 5.5[5] und höher) in 4 ändern.**
Mgmt	5	Lass dich in Ruhe!
Säugetiere	5	Lass dich in Ruhe!
Pagsschlag	5	Lass dich in Ruhe!
Profilin	2	Lass dich in Ruhe!
Beschneiden	2	Lass dich in Ruhe!
Privates	1	Lass dich in Ruhe!
QoS	1	Lass dich in Ruhe!
Radius	2	Lass dich in Ruhe!
rsvp	1	Lass dich in Ruhe!
Sicherheit	2	Lass dich in Ruhe!
Schnappschuss	2	Lass dich in Ruhe!
Span	2	**In 6 ändern.**
sys	5	**In 6 ändern.**

Tac	2	Lass dich in Ruhe!
TCP	2	Lass dich in Ruhe!
Telnet	2	Lass dich in Ruhe!
TFTP	2	Lass dich in Ruhe!
UDLD	4	Lass dich in Ruhe!
VMPS	2	Lass dich in Ruhe!
VTP	2	Lass dich in Ruhe!

[1] In CatOS 7.x und höher ersetzt der Ethc Facility Code den Pagp Facility-Code, um die LACP-Unterstützung wiederzugeben.

Hinweis: Derzeit protokollieren die Catalyst Switches eine Syslog-Konfigurationsänderungsmeldung der Ebene 6 für jeden **set-** oder **clear-**Befehl, der ausgeführt wird, im Gegensatz zur Cisco IOS-Software, die die Meldung erst nach dem Beenden des Konfigurationsmodus auslöst. Wenn Sie bei diesem Trigger RMEs benötigen, um Konfigurationen in Echtzeit zu sichern, müssen diese Meldungen auch an den Syslog-Server des RME gesendet werden. Für die meisten Kunden sind regelmäßige Konfigurations-Backups für Catalyst Switches ausreichend, und der Standardserverprotokollierungsschweregrad muss nicht geändert werden.

Wenn Sie Ihre NMS-Warnungen abstimmen, lesen Sie im System Message Guide nach.

Einfaches Netzwerkmanagement-Protokoll

SNMP wird zum Abrufen von Statistiken, Zählern und Tabellen verwendet, die in MIBs (Network Device Management Information Bases) gespeichert sind. Die gesammelten Informationen können von NMSs (z. B. HP OpenView) verwendet werden, um Warnmeldungen in Echtzeit zu generieren, die Verfügbarkeit zu messen und Informationen zur Kapazitätsplanung zu generieren sowie Konfigurations- und Fehlerbehebungsprüfungen durchzuführen.

Überblick

Mit einigen Sicherheitsmechanismen kann eine Netzwerkmanagementstation Informationen in den MIBs abrufen, die SNMP-Protokolle abrufen und die nächsten Anforderungen abrufen, und die Parameter mit dem **set-**Befehl ändern. Darüber hinaus kann ein Netzwerkgerät so konfiguriert werden, dass es eine Trap-Meldung für das NMS für Echtzeit-Warnmeldungen generiert. Beim SNMP Polling wird der IP-UDP-Port 161 verwendet, und SNMP-Traps verwenden den Port 162.

Cisco unterstützt folgende SNMP-Versionen:

- SNMPv1: RFC 1157 Internet Standard mit Clear Text Community String Security Eine Zugriffsliste für IP-Adressen und ein Kennwort definieren die Community von Managern, die auf die Agent-MIB zugreifen können.
- SNMPv2C: eine Kombination aus SNMPv2, einem in den RFCs 1902 bis 1907 definierten Draft-Internetstandard, und SNMPv2C, einem Community-basierten Verwaltungsframework für SNMPv2, das ein in RFC 1901 definierter experimenteller Entwurf ist. Zu den Vorteilen gehört ein Massenabruf-Mechanismus, der das Abrufen von Tabellen und große Informationsmengen unterstützt, die Anzahl erforderlicher Rundreisen minimiert und die Fehlerbehandlung verbessert.
- SNMPv3: Der vorgeschlagene RFC 2570-Entwurf bietet sicheren Zugriff auf Geräte durch die

Kombination von Authentifizierung und Verschlüsselung von Paketen über das Netzwerk. Die in SNMPv3 bereitgestellten Sicherheitsfunktionen sind:Nachrichtenintegrität: stellt sicher, dass ein Paket nicht manipuliert wurde, wenn es bei der ÜbertragungAuthentifizierung: stellt fest, dass die Nachricht von einer gültigen Quelle stammt.Verschlüsselung: den Inhalt eines Pakets verwirft, um zu verhindern, dass es von einer nicht autorisierten Quelle einfach angezeigt wird

In dieser Tabelle werden die Kombinationen von Sicherheitsmodellen aufgelistet:

Modellebene	Authentifizierung	Verschlüsselung	Ergebnis
V1	noAuthNoPriv, Community-Zeichenfolge	Nein	Verwendet einen Community-String-Abgleich für die Authentifizierung.
v2c	noAuthNoPriv, Community-Zeichenfolge	Nein	Verwendet einen Community-String-Abgleich für die Authentifizierung.
V3	noAuthNoPriv, Benutzername	Nein	Verwendet einen Benutzernamen-Abgleich für die Authentifizierung.
V3	authNoPriv, MD5 oder SHA	NP	Bietet Authentifizierung auf der Basis von HMAC-MD5- oder HMAC-SHA-Algorithmen.
V3	authPriv, MD5 oder SHA	DES	Bietet Authentifizierung auf der Basis von HMAC-MD5- oder HMAC-SHA-Algorithmen. DES 56-Bit-Verschlüsselung sowie Authentifizierung nach dem DES-56-Standard (CBC-DES)

Hinweis: Beachten Sie diese Informationen zu SNMPv3-Objekten:

- Jeder Benutzer gehört zu einer Gruppe.
- Eine Gruppe definiert die Zugriffsrichtlinie für eine Gruppe von Benutzern.
- Eine Zugriffsrichtlinie definiert, auf welche SNMP-Objekte zugegriffen werden kann, um sie zu lesen, zu schreiben und zu erstellen.
- Eine Gruppe bestimmt die Liste der Benachrichtigungen, die ihre Benutzer erhalten können.
- Eine Gruppe definiert außerdem das Sicherheitsmodell und die Sicherheitsstufe für ihre Benutzer.

SNMP-Trap-Empfehlung

SNMP ist die Grundlage für das gesamte Netzwerkmanagement und wird in allen Netzwerken aktiviert und verwendet. Der SNMP-Agent auf dem Switch muss so konfiguriert werden, dass er die von der Managementstation unterstützte SNMP-Version verwendet. Da ein Agent mit mehreren Managern kommunizieren kann, ist es möglich, die Software so zu konfigurieren, dass sie beispielsweise die Kommunikation mit einer Managementkonsole über das SNMPv1-Protokoll und mit einem anderen über das SNMPv2-Protokoll unterstützt.

Die meisten NMS-Stationen verwenden heute SNMPv2C unter dieser Konfiguration:

```
set snmp community read-only string
!--- Allow viewing of variables only. set snmp community read-write string
!--- Allow setting of variables. set snmp community read-write-all string
!--- Include setting of SNMP strings.
```

Cisco empfiehlt, SNMP-Traps für alle verwendeten Funktionen zu aktivieren (Funktionen, die nicht verwendet werden, können bei Bedarf deaktiviert werden). Wenn ein Trap aktiviert ist, kann es mit dem **Befehl test snmp** getestet werden und die entsprechende Behandlung auf dem NMS für den Fehler eingerichtet werden (z. B. eine Pager-Warnung oder ein Popup-Fenster).

Alle Traps sind standardmäßig deaktiviert und müssen der Konfiguration entweder einzeln oder mithilfe des **all-**Parameters hinzugefügt werden, wie folgt:

```
set snmp trap enable all
set snmp trap server address read-only community string
```

Zu den verfügbaren Traps in CatOS 5.5 gehören:

Trap	Beschreibung
Eier	Authentifizierung
Brücke	Brücke
Gehäuse	Gehäuse
Konfiguration	Konfiguration
Einheit	Einheit
vertreiben	IP-Genehmigung
Modul	Modul
Repeater	Repeater
stpx	Spanning Tree-Erweiterung
Syslog	Syslog-Benachrichtigung
VMPS	Richtlinienserver für VLAN-Mitgliedschaft
VTP	VLAN-Trunk-Protokoll

Hinweis: Die Syslog-Trap sendet alle vom Switch generierten Syslog-Meldungen ebenfalls als SNMP-Trap an das NMS. Wenn Syslog-Alerting bereits von einem Analyzer wie Cisco Works 2000 RMEs durchgeführt wird, ist es nicht unbedingt sinnvoll, diese Informationen zweimal zu erhalten.

Im Gegensatz zur Cisco IOS Software sind SNMP-Traps auf Portebene standardmäßig deaktiviert, da Switches Hunderte von aktiven Schnittstellen haben können. Cisco empfiehlt daher, dass SNMP-Traps auf Portebene für Schlüsselports wie Infrastrukturverbindungen zu Routern, Switches und Hauptservern aktiviert sind. Andere Ports, wie z. B. Benutzer-Host-Ports, sind nicht erforderlich, was die Netzwerkverwaltung vereinfacht.

```
set port trap port range enable
!--- Enable on key ports only.
```

SNMP Polling-Empfehlung

Es wird eine Überprüfung des Netzwerkmanagements empfohlen, um spezifische Anforderungen detailliert zu besprechen. Einige grundlegende Philosophien von Cisco für die Verwaltung großer Netzwerke sind jedoch aufgelistet:

- Tun Sie etwas Einfaches und machen Sie es gut.
- Verringerung der Mitarbeiterüberlastung durch exzessive Abfrage von Daten, Erfassung, Tools und manuelle Analysen
- Das Netzwerkmanagement ist mit wenigen Tools möglich, z. B. HP OpenView als NMS, Cisco RMEs als Konfigurations-, Syslog-, Bestands- und Software-Manager, Microsoft Excel als NMS-Datenanalysator und CGI als Möglichkeit zur Veröffentlichung im Internet.
- Durch die Veröffentlichung von Berichten im Internet können sich Benutzer, z. B. leitende Angestellte und Analysten, auf Informationen konzentrieren, ohne dass die Mitarbeiter des Betriebs mit vielen speziellen Anfragen beschäftigt werden müssen.
- Finden Sie heraus, was im Netzwerk gut funktioniert, und lassen Sie es in Ruhe. Konzentrieren Sie sich auf das, was nicht funktioniert.

Die erste Phase der NMS-Implementierung muss auf der Basis der Netzwerk-Hardware erfolgen. Die Geräte- und Protokollintegrität kann durch die einfache CPU-, Speicher- und Puffer-Auslastung auf Routern sowie die Auslastung von NMP CPU, Speicher und Backplane auf Switches erheblich beeinflusst werden. Erst nach einer Hardware-Baseline können L2- und L3-Datenverkehrslast, Peak und durchschnittliche Baselines ihre volle Wirkung entfalten. Baselines werden in der Regel über mehrere Monate eingerichtet, um die täglichen, wöchentlichen und vierteljährlichen Trends - je nach Geschäftszyklus des Unternehmens - transparent zu machen.

In vielen Netzwerken treten durch Überfrachtung Probleme mit der Leistung und Kapazität des NMS auf. Es wird daher empfohlen, nach der Festlegung der Basislinie RMON-Schwellenwerte für Alarme und Ereignisse auf den Geräten selbst festzulegen, um das NMS auf anormale Änderungen hinzuweisen und so Polling zu entfernen. So kann das Netzwerk den Netzbetreibern sagen, wann etwas nicht normal ist, und nicht fortlaufend abfragen, ob alles normal ist. Grenzwerte können auf der Grundlage verschiedener Regeln festgelegt werden, z. B. Höchstwert plus ein Prozentsatz oder Standardabweichung vom Mittelwert. Sie fallen nicht in den Anwendungsbereich dieses Dokuments.

In der zweiten Phase der NMS-Implementierung werden bestimmte Netzwerkbereiche mit SNMP genauer abgefragt. Dazu gehören Zweifelsbereiche, Bereiche vor einer Änderung oder Bereiche, die als gut charakterisiert sind. Verwenden Sie die NMS-Systeme als Suchfunktion, um das Netzwerk detailliert zu scannen und Hotspots zu beleuchten (versuchen Sie nicht, das gesamte Netzwerk zu beleuchten).

Die Cisco Network Management Consulting-Gruppe schlägt vor, diese zentralen Fehler-MIBs in

Campus-Netzwerken zu analysieren oder zu überwachen. Weitere Informationen finden Sie in den Cisco Richtlinien für Netzwerküberwachung und Ereigniskorrelation (z. B. zu Leistungs-MIBs, die abgefragt werden müssen).

Objektname	Objektbeschreibung	OID	Umfrageintervall	Grenzwert
MIB-II				
sysUpTime	Systemverfügbarkeit in 1/100 Sekunden	1.3.6.1.2.1.1.3	5 Min.	< 30.000

Objektname	Objektbeschreibung	OID	Umfrageintervall	Grenzwert
CISCO-PROCESS-MIB				
cpmCPUTotal5min	Der prozentuale Gesamtanteil der CPU-Auslastung in den letzten 5 Minuten	1.3.6.1.4.1.9.9.109.1.1.1.1.5	10 Min.	Ausgangswert

Objektname	Objektbeschreibung	OID	Umfrageintervall	Grenzwert
CISCO STACK-MIB				
sysEnableChassisTraps	Gibt an, ob ChassisAlarmOn- und ChassisAlarmOff-Traps in dieser MIB generiert werden müssen.	1.3.6.1.4.1.9.5.1.1.24	24 Std.	1
sysEnableModuleTraps	Gibt an, ob ModulUp- und ModulDown-Traps in dieser MIB generiert werden müssen.	1.3.6.1.4.1.9.5.1.1.25	24 Std.	1
sysEnableBridgeTraps	Gibt an, ob neue Root- und TopologyChange-Traps in der BRIDGE-MIB (RFC 1493) generiert werden müssen.	1.3.6.1.4.1.9.5.1.1.26	24 Std.	1
sysEnableR	Gibt an, ob die	1.3.6.1.4.1.	24 Std.	1

epeaterTraps	Traps in der REPEATER-MIB (RFC1516) generiert werden müssen.	9.5.1.1.29		
sysEnableIpPermitTraps	Gibt an, ob die IP-Genehmigungsfallen in dieser MIB generiert werden müssen.	1.3.6.1.4.1.9.5.1.1.31	24 Std.	1
sysEnableVmpsTraps	Gibt an, ob der in CISCO-VLAN-MEMBERSHIP-MIB definierte vmVmpsChange-Trap generiert werden muss.	1.3.6.1.4.1.9.5.1.1.31	24 Std.	1
sysEnableConfigTraps	Gibt an, ob in dieser MIB sysConfigChange-Trap generiert werden muss.	1.3.6.1.4.1.9.5.1.1.35	24 Std.	1
sysEnableStpxTrap	Gibt an, ob stpxInconsistencyUpdate-Trap in der CISCO-STP-EXTENSIONS-MIB generiert werden muss.	1.3.6.1.4.1.9.5.1.1.40	24 Std.	1
ChassisPs1Status	Status des Netzteils 1.	1.3.6.1.4.1.9.5.1.2.4	10 Min.	2
ChassisPs1TestResult	Detaillierte Informationen zum Status des Netzteils 1.	1.3.6.1.4.1.9.5.1.2.5	Nach Bedarf.	
ChassisPs2Status	Status des Netzteils 2.	1.3.6.1.4.1.9.5.1.2.7	10 Min.	2
ChassisPs2TestResult	Detaillierte Informationen zum Status des Netzteils 2	1.3.6.1.4.1.9.5.1.2.8	Nach Bedarf.	
ChassisLüfterstatus	Status des Gehäuselüfters	1.3.6.1.4.1.9.5.1.2.9	10 Min.	2
ChassisFanTestResult	Detaillierte Informationen zum Status des	1.3.6.1.4.1.9.5.1.2.10	Nach Bedarf.	

	Gehäuselüfters.			
ChassisMinorAlarm	Geringfügiger Alarmstatus für Chassis.	1.3.6.1.4.1.9.5.1.2.11	10 Min.	1
ChassisMajorAlarm	Hauptalarmstatus des Chassis	1.3.6.1.4.1.9.5.1.2.12	10 Min.	1
ChassisTempAlarm	Alarmstatus Chassis-Temperatur	1.3.6.1.4.1.9.5.1.2.13	10 Min.	1
ModulStatus	Betriebsstatus des Moduls.	1.3.6.1.4.1.9.5.1.3.1.1.10	30 Min.	2
moduleTestResult	Detaillierte Informationen zum Modulzustand.	1.3.6.1.4.1.9.5.7.3.1.1.11	Nach Bedarf.	
moduleStandbyStatus	Status eines redundanten Moduls.	1.3.6.1.4.1.9.5.7.3.1.1.21	30 Min.	=1 oder =4

Objektname	Objektbeschreibung	OID	Umfrageintervall	Grenzwert
CISCO-MEMORY-POOL-MIB				
dot1dStpTimeSinceTopologyChange	Die Zeit (in 1/100 Sekunden) seit der letzten von der Entität erkannten Topologieänderung.	1.3.6.1.2.1.17.2.3	5 Min.	< 30.000
dot1dStpTopChanges	Die Gesamtzahl der von dieser Bridge erkannten Topologieänderungen seit dem letzten Zurücksetzen oder Initialisieren der Verwaltungseinheit.	1.3.6.1.2.1.17.2.4	Nach Bedarf.	

dot1dStpPortState [1]	Der aktuelle Status des Ports gemäß der Anwendung des Spanning Tree Protocol. Der Rückgabewert kann einer der folgenden Werte sein: deaktiviert (1), Blockierung (2), Zuhören (3), Lernen (4), Weiterleitung (5) oder unterbrochen (6).	1.3.6.1.2.1.17.2.15.1.3	Nach Bedarf.	

Objektname	Objektbeschreibung	OID	Umfrageintervall	Grenzwert
CISCO-MEMORY-POOL-MIB				
ciscoMemoryPoolVerwendet	Gibt die Anzahl der Byte aus dem Speicherpool an, die derzeit von Anwendungen auf dem verwalteten Gerät verwendet werden.	1.3.6.1.4.1.9.9.48.1.1.1.5	30 Min.	Ausgangswert
ciscoMemoryPoolFree	Gibt die Anzahl der Byte aus dem Speicherp	1.3.6.1.4.1.9.9.48.1.1.1.6	30 Min.	Ausgangswert

	ool an, die auf dem verwaltete n Gerät derzeit nicht verwendet werden. **Hinweis:** Die Summe aus ciscoMem oryPoolUs ed und ciscoMem oryPoolFre e entspricht der gesamten Speicherk apazität im Pool.			
ciscoMemory PoolLargestFr ee	Gibt die größte Anzahl zusammen hängender Bytes aus dem Speicherp ool an, die auf dem verwaltete n Gerät derzeit nicht verwendet werden.	1.3.6.1.4.1. 9.9.48.1.1.1 .7	30 Min.	Ausga ngswe rt

Weitere Informationen zur Unterstützung von Cisco MIBs finden Sie im Cisco Network Management Toolkit - MIBs.

Hinweis: Einige Standard-MIBs gehen davon aus, dass eine bestimmte SNMP-Einheit nur eine Instanz der MIB enthält. Daher verfügt die Standard-MIB über keinen Index, der Benutzern den direkten Zugriff auf eine bestimmte Instanz der MIB ermöglicht. In diesen Fällen wird eine Community String-Indexierung bereitgestellt, um auf jede Instanz der Standard-MIB zuzugreifen. Die Syntax lautet [Community String]@[Instance number], wobei die Instanz in der Regel eine VLAN-Nummer ist.

Weitere Optionen

Die Sicherheitsaspekte von SNMPv3 bedeuten, dass SNMPv2 durch die Verwendung dieses Tools rechtzeitig überholt wird. Cisco empfiehlt Kunden, sich im Rahmen ihrer NMS-Strategie auf dieses neue Protokoll vorzubereiten. Der Vorteil besteht darin, dass Daten sicher von SNMP-Geräten gesammelt werden können, ohne dass Manipulationen oder Beschädigungen entstehen. Vertrauliche Informationen wie SNMP-**set-**Befehlspakete, die eine Switch-Konfiguration ändern, können verschlüsselt werden, um zu verhindern, dass ihr Inhalt im Netzwerk verfügbar gemacht wird. Darüber hinaus können verschiedene Benutzergruppen unterschiedliche Berechtigungen haben.

Hinweis: Die Konfiguration von SNMPv3 unterscheidet sich erheblich von der SNMPv2-Befehlszeile, und es ist eine erhöhte CPU-Last für die Supervisor Engine zu erwarten.

Remote-Überwachung

RMON ermöglicht die Vorverarbeitung von MIB-Daten durch das Netzwerkgerät selbst, um diese für allgemeine Verwendungszwecke oder zur Anwendung durch den Netzwerkmanager vorzubereiten, z. B. für die Durchführung von Verlaufsanalysen zu Baseline und Schwellenwertanalysen.

Die Ergebnisse der RMON-Verarbeitung werden in RMON-MIBs gespeichert, um anschließend von einem NMS, wie in RFC 1757 definiert, erfasst zu werden.

Überblick

Catalyst Switches unterstützen Mini-RMON in der Hardware an jedem Port, der aus vier einfachen RMON-1-Gruppen besteht: Statistiken (Gruppe 1), Verlauf (Gruppe 2), Alarme (Gruppe 3) und Ereignisse (Gruppe 9).

Der leistungsstärkste Teil von RMON-1 ist der **Grenzwertmechanismus**, der von den **Alarm- und** Ereignisgruppen bereitgestellt wird. Wie bereits erwähnt, ermöglicht die Konfiguration von RMON-Schwellenwerten dem Switch, ein SNMP-Trap zu senden, wenn ein ungewöhnlicher Zustand auftritt. Nachdem die Schlüsselports identifiziert wurden, kann SNMP verwendet werden, um Zähler oder RMON-Verlaufsgruppen abzufragen und Baselines für die Aufzeichnung der normalen Datenverkehrsaktivität für diese Ports zu erstellen. Als Nächstes können Grenzwerte für steigende und fallende RMON festgelegt und Alarme konfiguriert werden, wenn eine Abweichung von der Basislinie besteht.

Die Konfiguration von Schwellenwerten wird am besten mit einem RMON-Managementpaket durchgeführt, da die erfolgreiche Erstellung der Parameterreihen in Alarm- und Ereignistabellen mühsam ist. Kommerzielle RMON NMS-Pakete, z. B. Cisco Traffic Director, Teil von Cisco Works 2000, enthalten GUIs, die die Einstellung von RMON-Schwellenwerten deutlich vereinfachen.

Zu Ausgangszwecken stellt die EtherStats-Gruppe einen nützlichen Bereich von L2-Datenverkehrsstatistiken bereit. Die Objekte in dieser Tabelle können verwendet werden, um Statistiken über Unicast-, Multicast- und Broadcast-Datenverkehr sowie eine Reihe von L2-Fehlern abzurufen. Der RMON-Agent auf dem Switch kann auch so konfiguriert werden, dass diese Sampling-Werte in der Verlaufsgruppe gespeichert werden. Dieser Mechanismus ermöglicht eine Verringerung der Polling-Menge, ohne die Abtastrate zu reduzieren. Die RMON-Historien können präzise Baselines liefern, ohne dass ein erheblicher Umfrageaufwand entsteht. Je mehr Historien gesammelt werden, desto mehr Switch-Ressourcen werden verwendet.

Während Switches nur vier grundlegende RMON-1-Gruppen bereitstellen, ist es wichtig, den Rest

von RMON-1 und RMON-2 nicht zu vergessen. Alle Gruppen sind in RFC 2021 definiert, einschließlich des Benutzerverlaufs (Gruppe 18) und der ProbeConfig (Gruppe 19). L3- und höhere Informationen können von Switches mit SPAN-Port- oder VLAN-ACL-Umleitungsfunktionen abgerufen werden, mit denen der Datenverkehr auf eine externe RMON SwitchProbe oder ein internes Network Analysis Module (NAM) kopiert werden kann.

NAMs unterstützen alle RMON-Gruppen und können sogar **Daten auf Anwendungsebene** überprüfen, einschließlich der von Catalyst exportierten NetFlow-Daten, wenn MLS aktiviert ist. Das Ausführen von MLS bedeutet, dass der Router nicht alle Pakete in einem Datenfluss umschaltet, sodass nur der NetFlow-Datenexport und nicht die Schnittstellenzähler eine zuverlässige VLAN-Abrechnung ermöglichen.

Sie können einen SPAN-Port und eine Switch-Abfrage verwenden, um einen Paket-Stream für einen bestimmten Port, Trunk oder VLAN zu erfassen und die Pakete hochzuladen, um sie mit einem RMON-Managementpaket zu decodieren. Der SPAN-Port kann über die SPAN-Gruppe in der CISCO-STACK-MIB SNMP-gesteuert werden, sodass dieser Prozess einfach zu automatisieren ist. Der Traffic Director nutzt diese Funktionen mit seiner Roving Agent-Funktion.

Ein gesamtes VLAN kann nicht abgedeckt werden. Selbst wenn Sie eine 1-Gbit/s-Abfrage verwenden, kann der gesamte Paketstream eines VLAN oder sogar eines 1-Gbit/s-Vollduplex-Ports die Bandbreite des SPAN-Ports überschreiten. Wenn der SPAN-Port ständig mit voller Bandbreite läuft, besteht die Gefahr, dass Daten verloren gehen. Weitere Informationen finden Sie unter Konfigurieren der SPAN-Funktion (Catalyst Switched Port Analyzer).

Empfehlung

Cisco empfiehlt die Bereitstellung von RMON-Schwellenwerten und Warnhinweisen, um die Netzwerkverwaltung intelligenter zu gestalten als das SNMP Polling. Dadurch wird der Datenverkehrsaufwand für das Netzwerkmanagement reduziert, und das Netzwerk kann intelligent auf Änderungen reagieren. RMON muss von einem externen Agenten wie Traffic Director gesteuert werden. Es gibt keine CLI-Unterstützung. Führen Sie die folgenden Befehle aus, um RMON zu aktivieren:

```
set snmp rmon enable
set snmp extendedrmon netflow enable mod
!--- For use with NAM module only.
```

Es ist wichtig zu beachten, dass die primäre Funktion eines Switches darin besteht, Frames weiterzuleiten, nicht als große RMON-Abfrage mit mehreren Ports zu fungieren. Wenn Sie also Verlaufsberichte und Schwellenwerte für mehrere Ports für mehrere Bedingungen einrichten, sollten Sie bedenken, dass Ressourcen verbraucht werden. Erwägen Sie ein NAM-Modul, wenn Sie RMON hochfahren. Beachten Sie auch die kritische Port-Regel: nur die Ports abfragen und Schwellenwerte festlegen, die in der Planungsphase als wichtig identifiziert wurden.

Speicheranforderungen

Die RMON-Speichernutzung ist auf allen Switch-Plattformen hinsichtlich Statistiken, Verlaufsdaten, Alarmen und Ereignissen konstant. RMON verwendet einen Eimer, um Verlaufshistorien und Statistiken auf dem RMON-Agenten (in diesem Fall dem Switch) zu speichern. Die Größe der Eimer wird auf der RMON-Sonde (Switch Probe) oder der RMON-Anwendung (Traffic Director) definiert und zur Einstellung an den Switch gesendet. In der Regel

sind Speichereinschränkungen nur bei älteren Supervisor Engines mit weniger als 32 MB DRAM zu berücksichtigen. Beachten Sie diese Richtlinien:

- Um Mini-RMON zu unterstützen (vier RMON-Gruppen), werden dem NMP-Image etwa 450 K Codespeicher hinzugefügt. Dies sind vier Gruppen von RMON: Statistiken, Verlauf, Alarme und Ereignisse). Die Anforderungen an den dynamischen Arbeitsspeicher für RMON variieren, da sie von der Laufzeitkonfiguration abhängen. Die Informationen zur RMON-Speichernutzung zur Laufzeit für jede Mini-RMON-Gruppe finden Sie hier:Ethernet Statistics Group (Ethernet-Statistik-Gruppe): benötigt 800 Byte für jede Switch-Ethernet-/FE-Schnittstelle.Verlaufsgruppe - Für die Ethernet-Schnittstelle benötigt jeder konfigurierte Verlaufssteuerungseintrag mit 50 Buckets ca. 3,6 KB Arbeitsspeicher und 56 Byte pro zusätzlichem Bucket.Alarme and Events groups (Alarme und Ereignisse): benötigt 2,6 KB für jeden konfigurierten Alarm und die zugehörigen Ereigniseinträge.
- Zum Speichern der RMON-bezogenen Konfiguration benötigen Sie etwa 20.000 NVRAM, wenn die NVRAM-Gesamtgröße des Systems 256.000 oder mehr beträgt, und 10.000 NVRAM, wenn die NVRAM-Gesamtgröße 128.000 beträgt.

Netzwerkzeitprotokoll

Das NTP, RFC 1305 synchronisiert die Zeiterfassung für eine Reihe von verteilten Zeitservern und Clients und ermöglicht die Korrelation von Ereignissen, wenn Systemprotokolle erstellt werden oder andere zeitspezifische Ereignisse auftreten.

NTP bietet genaue Client-Zeitangaben, in LANs in der Regel innerhalb einer Millisekunde und in WANs in einigen Zehntel Millisekunden, im Vergleich zu einem Primärserver, der mit koordinierter Universal Time (UTC) synchronisiert ist. 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.

Überblick

NTP wurde erstmals in RFC 958 dokumentiert, wurde aber durch RFC 119 (NTP-Version 2) weiterentwickelt und befindet sich jetzt in der dritten Version, wie in RFC 1305 definiert. Er wird über den UDP-Port 123 ausgeführt. Alle NTP-Kommunikation verwendet UTC, was der Greenwich Mean Time entspricht.

Zugreifen 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 sind und über 100.000 Clients und Server im Internet synchronisieren. Die aktuellen Listen werden auf der Seite Liste der öffentlichen NTP-Server verwaltet, die regelmäßig aktualisiert wird. Es gibt zahlreiche private primäre und sekundäre Server, die normalerweise nicht für die Öffentlichkeit verfügbar sind. Eine Liste der öffentlichen NTP-Server und Informationen zur Verwendung finden Sie auf der Website University of Delaware Time Synchronization Server .

Da es keine Garantie dafür gibt, dass diese öffentlichen Internet-NTP-Server verfügbar sind oder

die richtige Zeit liefern, wird dringend empfohlen, andere Optionen in Betracht zu ziehen. Dies kann die Verwendung verschiedener Standalone Global Positioning Service (GPS)-Geräte umfassen, die direkt mit einer Reihe von Routern verbunden sind.

Eine weitere mögliche Option ist die Verwendung verschiedener Router, die als Stratum 1-Master konfiguriert sind. Dies wird jedoch nicht empfohlen.

Stratum

Jeder NTP-Server verwendet eine Schicht, die angibt, wie weit von einer externen Zeitquelle der Server entfernt ist. Stratum 1-Server haben Zugriff auf eine externe Zeitquelle, z. B. eine Funkuhr. Stratum-2-Server erhalten Zeitdetails von einer benannten Gruppe von Stratum-1-Servern, während Stratum-3-Server Zeitdetails von Stratum-2-Servern abrufen usw.

Server-Peer-Beziehung

- Ein Server ist ein Server, der auf Clientanforderungen reagiert, aber nicht versucht, Datumsinformationen aus einer Clientzeitquelle zu integrieren.
- Ein Peer reagiert auf Client-Anfragen, versucht aber, die Client-Anfragen als potenziellen Kandidaten für eine bessere Zeitquelle zu nutzen und hilft bei der Stabilisierung seiner Taktfrequenz.
- Um ein echter Peer zu sein, müssen beide Seiten der Verbindung eine Peer-Beziehung aufbauen, anstatt einen Peer und den anderen Benutzer einen Server zu haben. Es wird außerdem empfohlen, dass Peers Schlüssel austauschen, sodass nur vertrauenswürdige Hosts als Peers miteinander kommunizieren.
- Bei einer Client-Anfrage an einen Server antwortet der Server dem Client und vergisst, dass der Client je eine Frage gestellt hat. In einer Clientanforderung an einen Peer antwortet der Server auf den Client und speichert Statusinformationen über den Client, um zu verfolgen, wie gut er sich in der Zeiterfassung verhält und welcher Stratum-Server ausgeführt wird.**Hinweis:** CatOS kann nur als NTP-Client fungieren.

Ein NTP-Server kann Tausende von Clients verarbeiten. Die Verarbeitung von Hunderten von Peers hat jedoch Auswirkungen auf den Arbeitsspeicher, und die Statuswartung verbraucht mehr CPU-Ressourcen auf dem Gerät sowie Bandbreite.

Umfragen

Das NTP-Protokoll ermöglicht es einem Client, jederzeit einen Server abzufragen. Wenn NTP zum ersten Mal auf einem Cisco Gerät konfiguriert wird, sendet es acht Abfragen in schneller Folge in NTP_MINPOLL-Intervallen (24 = 16 Sekunden). NTP_MAXPOLL beträgt 214 Sekunden (das sind 16.384 Sekunden oder 4 Stunden, 33 Minuten, 4 Sekunden). Dies ist die maximale Zeit, die es dauert, bis NTP erneut eine Abfrage für eine Antwort durchführt. Derzeit verfügt Cisco nicht über eine Methode, um die Einstellung der POLL-Zeit durch den Benutzer manuell zu erzwingen.

Der NTP-Abfragezähler beginnt mit 2^6 (64) Sekunden und wird um zwei Kräfte erhöht (wenn die beiden Server sich synchronisieren), auf 2^{10}. Das heißt, Sie können erwarten, dass die Synchronisierungsmeldungen im Intervall von 64, 128, 256, 512 oder 1024 Sekunden pro konfiguriertem Server oder Peer gesendet werden. Die Zeit variiert zwischen 64 und 1024 Sekunden als Leistung von zwei Sekunden, basierend auf der Phase-Loop, die Pakete sendet und empfängt. Wenn es zu der Zeit viel Jitter gibt, wird häufiger abgefragt. Wenn die Referenzuhr korrekt ist und die Netzwerkverbindung konsistent ist, sehen Sie, dass die Polling-Zeiten zwischen

den einzelnen Umfragen in 1024 Sekunden konvergieren.

In der Praxis bedeutet dies, dass sich das NTP-Umfrageintervall ändert, wenn sich die Verbindung zwischen Client und Server ändert. Je besser die Verbindung, desto länger das Polling-Intervall, d. h. der NTP-Client hat acht Antworten für seine letzten acht Anfragen erhalten (das Polling-Intervall wird verdoppelt). Bei einer einmaligen versäumten Antwort wird das Polling-Intervall halbiert. Das Abfrageintervall beginnt mit 64 Sekunden und erreicht maximal 1024 Sekunden. Im besten Fall dauert es etwas mehr als zwei Stunden, bis das Umfrageintervall von 64 Sekunden auf 1024 Sekunden ansteigt.

Broadcasts

NTP-Broadcasts werden niemals weitergeleitet. Der Befehl **ntp broadcast** bewirkt, dass der Router NTP-Broadcasts auf der Schnittstelle ausgibt, auf der er konfiguriert ist. Der **Befehl** ntp-Broadcast-Client veranlasst den Router oder Switch, NTP-Broadcasts auf der Schnittstelle abzurufen, auf der er konfiguriert ist.

NTP-Datenverkehrsstufen

Die vom NTP genutzte Bandbreite ist minimal, da das Intervall zwischen den Polling-Nachrichten, die zwischen Peers ausgetauscht werden, in der Regel alle 17 Minuten (1024 Sekunden) auf maximal eine Nachricht zurückgeht. Bei sorgfältiger Planung kann dies in Routernetzwerken über die WAN-Verbindungen aufrechterhalten werden. Die NTP-Clients müssen eine Peer-Verbindung zu lokalen NTP-Servern herstellen, nicht über das gesamte WAN hinweg zu den Core-Routern des zentralen Standorts, die die Layer-2-Server sind.

Ein konvergenter NTP-Client benötigt ca. 0,6 Bit/s pro Server.

Empfehlung

Viele Kunden haben NTP heute auf ihren CatOS-Plattformen im Client-Modus konfiguriert, der von mehreren zuverlässigen Feeds aus dem Internet oder einer Funkuhr synchronisiert wird. Eine einfachere Alternative zum Servermodus beim Betrieb einer großen Anzahl von Switches ist jedoch die Aktivierung von NTP im Broadcast-Client-Modus im Management-VLAN in einer Switch-Domäne. Dieser Mechanismus ermöglicht es einer ganzen Domäne von Catalyst, eine Uhr aus einer einzigen Broadcast-Nachricht 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:

- Serveraktualisierungen filtern
- Authentifizierung

Die zeitliche Korrelation von Ereignissen ist in zwei Fällen äußerst wertvoll: Fehlerbehebung und Sicherheitsprüfungen. Es ist darauf zu achten, dass die Zeitquellen und Daten geschützt werden, und eine Verschlüsselung wird empfohlen, damit wichtige Ereignisse nicht absichtlich oder unabsichtlich gelöscht werden.

Cisco empfiehlt folgende Konfigurationen:

Catalyst-Konfiguration

```
set ntp broadcastclient enable
set ntp authentication enable
set ntp key key
!--- This is a Message Digest 5 (MD5) hash. set ntp
timezone
```

Alternative Catalyst-Konfiguration

```
!--- This more traditional configuration creates !---
more configuration work and NTP peerings. set ntp client
enable
set ntp server IP address of time server set timezone
zone name set summertime date change details
```

Router-Konfiguration

```
!--- This is a sample router configuration to distribute
!--- NTP broadcast information to the Catalyst broadcast
clients. ntp source loopback0
ntp server IP address of time server ntp update-calendar
clock timezone zone name clock summer-time date change
details ntp authentication key key ntp access-group
access-list
!--- To filter updates to allow only trusted sources of
NTP information. Interface to campus/management VLAN
containing switch sc0 ntp broadcast
```

Cisco Discovery Protocol

CDP tauscht Informationen zwischen benachbarten Geräten über die Sicherungsschicht aus und ist äußerst hilfreich bei der Bestimmung der Netzwerktopologie und der physischen Konfiguration außerhalb der logischen oder IP-Schicht. Unterstützte Geräte sind hauptsächlich Switches, Router und IP-Telefone. In diesem Abschnitt werden einige der Verbesserungen von CDP Version 2 gegenüber Version 1 vorgestellt.

Überblick

CDP verwendet SNAP-Kapselung mit dem Typcode 2000. Auf Ethernet, ATM und FDDI, der Ziel-Multicast-Adresse **01-00-0c-cc-cc, wird der HDLC-Protokolltyp 0x2000** verwendet. Auf Token Rings wird die funktionale Adresse c000.0800.000 verwendet. CDP-Frames werden standardmäßig jede Minute gesendet.

CDP-Nachrichten enthalten eine oder mehrere Untermeldungen, mit denen die Zielgeräte Informationen über jedes benachbarte Gerät sammeln und speichern können.

CDP Version 1 unterstützt folgende Parameter:

Para	Typ	Beschreibung

meter		
1	Geräte-ID	Hostname des Geräts oder Seriennummer der Hardware in ASCII.
2	Adresse	Die L3-Adresse der Schnittstelle, die das Update gesendet hat.
1	Port-ID	Der Port, an den das CDP-Update gesendet wurde.
4	Funktionen	Beschreibt die Funktionsmerkmale des Geräts: Router: 0 x 01 TB Bridge: 0x02 SR Bridge: 0x04-Switch: 0x08 (bietet L2- und/oder L3-Switching) Host: 0x10 IGMP-bedingte Filterung: 0x20 Die Bridge oder der Switch leitet IGMP-Berichtspakete nicht an Router-Ports weiter. Repeater: 0 x 40
5	Version	Eine Zeichenkette, die die Softwareversion enthält (wie in der **Anzeigeversion**).
6	Plattform	Hardwareplattform, z. B. WS-C5000, WS-C6009 oder Cisco RSP.

In CDP, Version 2, wurden zusätzliche Protokollfelder eingeführt. CDP-Version 2 unterstützt alle Felder, aber die aufgeführten können besonders in Umgebungen mit Switches nützlich sein und werden in CatOS verwendet.

Hinweis: Wenn ein Switch CDPv1 ausführt, verwirft er v2-Frames. Wenn ein Switch mit CDPv2 einen CDPv1-Frame auf einer Schnittstelle empfängt, sendet er neben CDPv2-Frames auch CDPv1-Frames aus dieser Schnittstelle.

Parameter	Typ	Beschreibung
9	VTP-Domäne	Die VTP-Domäne, falls auf dem Gerät konfiguriert.
10	Natives VLAN	In dot1q ist dies das nicht gekennzeichnete VLAN.
11	Vollduplex/Halbduplex	Dieses Feld enthält die Duplexeinstellung des sendenden Ports.

Empfehlung

CDP ist standardmäßig aktiviert und ist für die Transparenz benachbarter Geräte und die Fehlerbehebung unerlässlich. Sie wird auch von Netzwerkmanagementanwendungen zum Erstellen von L2-Topologieübersichten verwendet. Führen Sie die folgenden Befehle aus, um CDP einzurichten:

```
set cdp enable
```

```
!--- This is the default. set cdp version v2
!--- This is the default.
```

In Teilen des Netzwerks, in denen ein hohes Maß an Sicherheit erforderlich ist (z. B. DMZs mit Internetanbindung), muss CDP als solches deaktiviert werden:

```
set cdp disable port range
```

Der **Befehl** show cdp neighbors zeigt die lokale CDP-Tabelle an. Mit einem Stern (*) gekennzeichnete Einträge weisen auf eine VLAN-Diskrepanz hin. mit # gekennzeichnete Einträge weisen auf eine Duplexungleichheit hin. Dies kann eine hilfreiche Hilfe bei der Fehlerbehebung sein.

```
>show cdp neighbors

* - indicates vlan mismatch.
# - indicates duplex mismatch.
Port  Device-ID          Port-ID Platform
----- ----------------- ------- ------------
 3/1  TBA04060103(swi-2) 3/1     WS-C6506
 3/8  TBA03300081(swi-3) 1/1     WS-C6506
15/1  rtr-1-msfc         VLAN 1  cisco    Cat6k-MSFC
16/1  MSFC1b             Vlan2   cisco    Cat6k-MSFC
```

Weitere Optionen

Einige Switches wie der Catalyst 6500/6000 können IP-Telefone über UTP-Kabel mit Strom versorgen. Die über CDP empfangenen Informationen unterstützen die Stromverwaltung am Switch.

Da IP-Telefone einen PC mit ihnen verbinden können und beide Geräte mit demselben Catalyst-Port verbunden sind, kann der Switch das VoIP-Telefon in einem separaten VLAN, dem AUX, platzieren. So kann der Switch problemlos eine andere Quality of Service (QoS) für den VoIP-Datenverkehr anwenden.

Wenn das zusätzliche VLAN geändert wird (z. B. um das Telefon zur Verwendung eines bestimmten VLAN oder einer bestimmten Tagging-Methode zu zwingen), werden diese Informationen über CDP an das Telefon gesendet.

Parameter	Typ	Beschreibung
14	Appliance-ID	Ermöglicht die Differenzierung des VoIP-Datenverkehrs vom anderen Datenverkehr, z. B. durch ein separates VLAN-ID (zusätzliches VLAN).
16	Stromverbrauch	Der Stromverbrauch eines VoIP-Telefons in Milliwatt.

Hinweis: Catalyst Switches der Serien 2900 und 3500XL unterstützen derzeit kein CDPv2.

Sicherheitskonfiguration

Im Idealfall hat der Kunde bereits eine Sicherheitsrichtlinie aufgestellt, um zu definieren, welche Tools und Technologien von Cisco qualifiziert sind.

Hinweis: Die Sicherheit der Cisco IOS-Software wird im Gegensatz zu CatOS in vielen Dokumenten, z. B. Cisco ISP Essentials, behandelt.

Grundlegende Sicherheitsfunktionen

Kennwörter

Konfigurieren Sie ein Kennwort auf Benutzerebene (Anmeldung). Bei Kennwörtern wird in CatOS 5.x und höher die Groß- und Kleinschreibung beachtet. Sie können zwischen 0 und 30 Zeichen lang sein, einschließlich Leerzeichen. Legen Sie das enable-Kennwort fest:

```
set password password set enablepass password
```

Alle Kennwörter müssen mindestens den Längenstandards entsprechen (z. B. mindestens sechs Zeichen, eine Kombination aus Buchstaben und Zahlen, Groß- und Kleinbuchstaben), um sich anzumelden und Kennwörter bei Verwendung zu aktivieren. Diese Kennwörter werden mit dem MD5-Hashing-Algorithmus verschlüsselt.

Um eine größere Flexibilität bei der Verwaltung von Kennwortsicherheit und Gerätezugriff zu ermöglichen, empfiehlt Cisco die Verwendung eines TACACS+-Servers. Weitere Informationen finden Sie im TACACS+-Abschnitt dieses Dokuments.

Secure Shell

Verwenden Sie die SSH-Verschlüsselung, um die Sicherheit für Telnet-Sitzungen und andere Remote-Verbindungen zum Switch zu gewährleisten. Die SSH-Verschlüsselung wird nur für Remote-Anmeldungen am Switch unterstützt. Sie können keine Telnet-Sitzungen verschlüsseln, die vom Switch aus initiiert werden. SSH-Version 1 wird von CatOS 6.1 unterstützt, und Version 2 wurde in CatOS 8.3 hinzugefügt. SSH-Version 1 unterstützt die Verschlüsselungsmethoden DES (Data Encryption Standard) und Triple-DES (3-DES), und SSH-Version 2 unterstützt die Verschlüsselungsverfahren 3-DES und AES (Advanced Encryption Standard). Sie können die SSH-Verschlüsselung mit RADIUS- und TACACS+-Authentifizierung verwenden. Diese Funktion wird von SSH-Images (k9) unterstützt. Weitere Informationen finden Sie unter So konfigurieren Sie SSH auf Catalyst-Switches mit CatOS.

```
set crypto key rsa 1024
```

Führen Sie folgenden Befehl aus, um die Fallback-Funktion in Version 1 zu deaktivieren und Verbindungen in Version 2 zu akzeptieren:

```
set ssh mode v2
```

IP-Berechtigungsfilter

Diese Filter schützen den Zugriff auf die sc0-Verwaltungsschnittstelle über Telnet und andere Protokolle. Diese sind besonders wichtig, wenn das für die Verwaltung verwendete VLAN auch Benutzer enthält. Geben Sie die folgenden Befehle ein, um die IP-Adresse und die Port-Filterung zu aktivieren:

```
set ip permit enable
set ip permit IP address mask Telnet|ssh|snmp|all
```

Wenn der Telnet-Zugriff jedoch mit diesem Befehl eingeschränkt wird, kann der Zugriff auf CatOS-Geräte nur über wenige vertrauenswürdige Endgeräte erfolgen. Diese Konfiguration kann die Fehlerbehebung behindern. Beachten Sie, dass es möglich ist, IP-Adressen zu täuschen und gefilterten Zugriff zu täuschen, sodass dies nur die erste Schutzschicht ist.

Port-Sicherheit

Erwägen Sie, die Port-Sicherheit zu verwenden, um nur einer oder mehreren bekannten MAC-Adressen die Weiterleitung von Daten an einen bestimmten Port zu ermöglichen (um beispielsweise zu verhindern, dass statische Endstationen für neue Stationen ohne Änderungskontrolle ausgetauscht werden). Möglich wird dies durch statische MAC-Adressen.

```
set port security mod/port enable MAC address
```

Dies ist auch möglich, wenn beschränkte MAC-Adressen dynamisch gelernt werden.

```
set port security port range enable
```

Diese Optionen können konfiguriert werden:

- set port security *mod/port* age *time value* (Zeitwert für Portsicherheit) - gibt die Dauer an, für die Adressen am Port gesichert werden, bevor eine neue Adresse abgerufen werden kann. Die Gültigkeitsdauer in Minuten beträgt 10-1440. Die Standardeinstellung ist nicht "aging".
- set port *securitymod/port* maximum *value* - Schlüsselwort, das die maximale Anzahl an MAC-Adressen angibt, die auf dem Port gesichert werden sollen. Gültige Werte sind 1 (Standard) - 1025.
- Port Security *Mod/Port*-Verletzung herunterfahren - Bei einer Verletzung wird der Port (Standard) heruntergefahren, Syslog-Meldung (Standard) gesendet und der Datenverkehr wird verworfen.
- Legen Sie den *Zeitwert für* Portsicherheit-*Modus/Port*-Shutdown fest - Dauer, für die ein Port deaktiviert bleibt. Gültige Werte sind 10-1440 Minuten. Die Standardeinstellung wird

permanent heruntergefahren.

Mit CatOS 6.x und höher hat Cisco die 802.1x-Authentifizierung eingeführt, mit der sich Clients auf einem zentralen Server authentifizieren können, bevor Ports für Daten aktiviert werden können. Diese Funktion befindet sich in der Anfangsphase der Unterstützung auf Plattformen wie Windows XP, kann aber von vielen Unternehmen als strategische Richtung angesehen werden. Weitere Informationen zur Konfiguration der Port-Sicherheit auf Switches, auf denen die Cisco IOS Software ausgeführt wird, finden Sie unter Konfigurieren der Port-Sicherheit.

Anmeldebanner

Erstellen Sie geeignete Gerätebanner, um speziell die für den unbefugten Zugriff ergriffenen Maßnahmen anzugeben. Werben Sie nicht mit dem Namen der Website oder den Netzwerkdaten, die nicht autorisierte Benutzer mit Informationen versorgen könnten. Diese Banner bieten Rückgriff, wenn ein Gerät kompromittiert wird und der Täter erwischt wird:.

```
# set banner motd ^C
*** Unauthorized Access Prohibited ***
***  All transactions are logged   ***
------------- Notice Board -------------
----Contact Joe Cisco at 1 800 go cisco for access problems----
^C
```

Physische Sicherheit

Die Geräte dürfen nicht physisch ohne entsprechende Autorisierung zugänglich sein, daher muss sich das Gerät in einem kontrollierten (verschließbaren) Raum befinden. Um sicherzustellen, dass das Netzwerk betriebsbereit bleibt und von schädlicher Manipulation von Umgebungsfaktoren nicht beeinträchtigt wird, müssen alle Geräte über eine geeignete USV (mit redundanten Quellen, wenn möglich) und eine Temperaturregelung (Klimaanlage) verfügen. Denken Sie daran, dass bei einer Verletzung des physischen Zugriffs durch eine Person mit böswilliger Absicht eine Unterbrechung durch Kennwortwiederherstellung oder andere Methoden viel wahrscheinlicher ist.

Terminal Access Controller Access Control System

Standardmäßig sind Kennwörter für nicht privilegierten und privilegierten Modus global und gelten für jeden Benutzer, der auf den Switch oder Router zugreift, entweder über den Konsolen-Port oder über eine Telnet-Sitzung im Netzwerk. Ihre Implementierung auf Netzwerkgeräten ist zeitaufwendig und nicht zentralisiert. Es ist außerdem schwierig, Zugriffsbeschränkungen mithilfe von Zugriffslisten zu implementieren, die anfällig für Konfigurationsfehler sein können.

Es stehen drei Sicherheitssysteme zur Verfügung, mit denen der Zugriff auf Netzwerkgeräte kontrolliert und überwacht werden kann. Diese verwenden Client/Server-Architekturen, um alle Sicherheitsinformationen in einer zentralen Datenbank zu speichern. Diese drei Sicherheitssysteme sind:

- TACACS+
- RADIUS
- Kerberos

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

- Authentication (Authentifizierung): Der Identifizierungs- und Verifizierungsprozess für einen Benutzer. Die Authentifizierung eines Benutzers kann auf verschiedene Weise erfolgen, am häufigsten jedoch eine Kombination aus Benutzername und Kennwort.
- Authorization (Autorisierung): Verschiedene Befehle können nach der Authentifizierung eines Benutzers erteilt werden.
- Accounting - Die Aufzeichnung, die festlegt, was ein Benutzer auf dem Gerät tut oder getan hat.

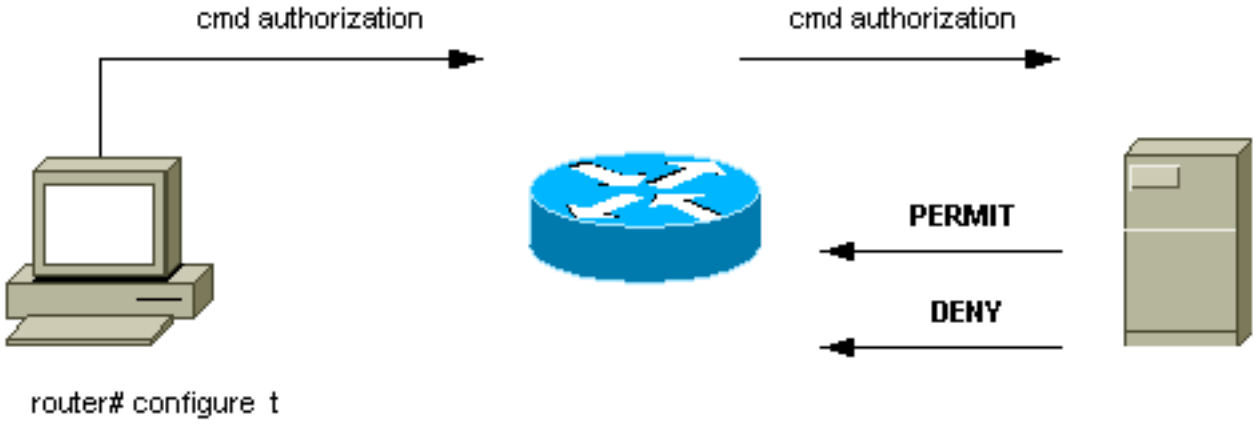
Weitere Informationen finden Sie unter Konfigurieren von TACACS+, RADIUS und Kerberos auf Cisco Catalyst-Switches.

Überblick

Das TACACS+-Protokoll leitet Benutzernamen und Kennwörter an den zentralisierten Server weiter, verschlüsselt über das Netzwerk mithilfe von **MD5-**Einweg-Hashing (RFC 1321). Es verwendet TCP-Port 49 als Transportprotokoll. Dies bietet gegenüber UDP (bei RADIUS verwendet) folgende Vorteile:

- Verbindungsorientierter Transport
- Separate Bestätigung, dass eine Anfrage empfangen wurde (TCP ACK), unabhängig davon, wie geladen der Backend-Authentifizierungsmechanismus derzeit ist
- Sofortige Anzeige eines Serverabsturzes (RST-Pakete)

Wenn während einer Sitzung eine zusätzliche Autorisierungsüberprüfung erforderlich ist, überprüft der Switch mit TACACS+, ob dem Benutzer die Berechtigung zur Verwendung eines bestimmten Befehls erteilt wurde. Dies bietet eine bessere Kontrolle über die Befehle, die auf dem Switch ausgeführt werden können, während sie vom Authentifizierungsmechanismus getrennt werden. Mithilfe der Befehlsabrechnung können die Befehle überprüft werden, die ein bestimmter Benutzer während der Verbindung mit einem bestimmten Netzwerkgerät ausgegeben hat.



Wenn ein Benutzer eine einfache ASCII-Anmeldung versucht, indem er sich bei einem Netzwerkgerät mit TACACS+ 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, die dann dem Benutzer angezeigt wird. Der Benutzer gibt einen Benutzernamen ein, und der Switch kontaktiert den TACACS+-Daemon, um eine Kennwortaufforderung zu erhalten. Der Switch zeigt die Kennwortaufforderung an den Benutzer an, der dann ein Kennwort eingibt, das auch an den TACACS+-Daemon gesendet wird.
- Das Netzwerkgerät erhält schließlich eine dieser Antworten vom TACACS+-Daemon:ACCEPT

(Akzeptieren): 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 hat sich nicht authentifiziert. Dem Benutzer kann je nach dem TACACS+-Daemon der weitere Zugriff verweigert oder er wird aufgefordert, die Anmeldesequenz erneut auszuführen.FEHLER - ein Fehler ist irgendwann während der Authentifizierung aufgetreten. Dies kann entweder am Daemon oder in der Netzwerkverbindung zwischen dem Daemon und dem Switch erfolgen. 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 und gibt eine ACCEPT- oder REJECT-Autorisierungsantwort zurück. Wenn eine ACCEPT-Antwort zurückgegeben wird, enthält die Antwort Daten in Form von Attributen, mit denen die EXEC- oder NETZWERKsitzung für diesen Benutzer gesteuert wird, und bestimmt die Befehle, auf die der Benutzer zugreifen kann.

Empfehlung

Cisco empfiehlt die Verwendung von TACACS+, da diese problemlos mithilfe von Cisco Secure ACS für NT, Unix oder anderer Software von Drittanbietern implementiert werden kann. Zu den TACACS+-Funktionen gehören eine detaillierte Abrechnung, um Statistiken über Befehlsverwendung und Systemnutzung, einen MD5-Verschlüsselungsalgorithmus und eine administrative Kontrolle der Authentifizierungs- und Autorisierungsprozesse bereitzustellen.

In diesem Beispiel verwenden die Anmelde- und Aktivierungsmodi den TACACS+-Server für die Authentifizierung und können auf die lokale Authentifizierung zurückgreifen, wenn der Server nicht verfügbar ist. In den meisten Netzwerken ist dies eine wichtige Hintertür. Führen Sie die folgenden Befehle aus, um TACACS+ einzurichten:

```
set tacacs server server IP primary set tacacs server server IP
!--- Redundant servers are possible. set tacacs attempts 3
!--- This is the default. set tacacs key key
!--- MD5 encryption key. set tacacs timeout 15
!--- Longer server timeout (5 is default). set authentication login tacacs enable
set authentication enable tacacs enable
set authentication login local enable
set authentication enable local enable
!--- The last two commands are the default; they allow fallback !--- to local if no TACACS+
server available.
```

Weitere Optionen

Es ist möglich, die Befehle, die jeder Benutzer oder jede Benutzergruppe auf dem Switch ausführen kann, mit der TACACS+-Autorisierung zu steuern. Es ist jedoch schwierig, eine Empfehlung abzugeben, da alle Kunden individuelle Anforderungen in diesem Bereich haben. Weitere Informationen finden Sie unter Steuern des Zugriffs auf den Switch mithilfe von Authentifizierung, Autorisierung und Abrechnung.

Schließlich bieten Accounting-Befehle einen Prüfpfad für die von jedem Benutzer eingegebenen

und konfigurierten Daten. Dies ist ein Beispiel für die Verwendung der gängigen Praxis, die Überwachungsinformationen am Ende des Befehls zu erhalten:

```
set accounting connect enable start-stop tacacs+
set accounting exec enable start-stop tacacs+
set accounting system enable start-stop tacacs+
set accounting commands enable all start-stop tacacs+
set accounting update periodic 1
```

Diese Konfiguration bietet folgende Funktionen:

- Mit dem Befehl "Connect" können ausgehende Verbindungsereignisse auf dem Switch wie Telnet erfasst werden.
- Der **exec**-Befehl ermöglicht die Abrechnung von Anmeldesitzungen auf dem Switch, z. B. von Betriebspersonal.
- Der Befehl **system** ermöglicht die Erfassung von Systemereignissen auf dem Switch, wie z. B. Neuladen oder Zurücksetzen.
- Der **Befehl Befehlen** ermöglicht die Abrechnung der auf dem Switch eingegebenen Befehle für **Anzeige**- und Konfigurationsbefehle.
- Regelmäßige *Updates* pro Minute zum Server sind hilfreich, um festzustellen, ob Benutzer noch angemeldet sind.

Konfigurations-Checkliste

Dieser Abschnitt enthält eine Zusammenfassung der empfohlenen Konfigurationen mit Ausnahme der Sicherheitsdetails.

Es ist äußerst hilfreich, alle Ports zu kennzeichnen. Geben Sie diesen Befehl ein, um die Ports zu kennzeichnen:

```
set port description descriptive name
```

Verwenden Sie diesen Schlüssel zusammen mit den aufgelisteten Befehlstabellen:

Schlüssel:
Fett formatierter Text - empfohlene Änderung
Normaler Text - Standardeinstellung, empfohlene Einstellung

Globale Konfigurationsbefehle

Befehl	**Kommentar**
VTP-*Domänenname*-*Passwort* festlegen	Schutz vor nicht autorisierten VTP-Updates von neuen Switches
Set vtp mode	Wählen Sie den in diesem

transparent	Dokument hochgestuften VTP-Modus aus. Weitere Informationen finden Sie im Abschnitt zum VLAN Trunking Protocol in diesem Dokument.
set spantree enable all	Stellen Sie sicher, dass STP in allen VLANs aktiviert ist.
set spantree root *vlan*	Empfohlen, Root-Bridges (und sekundäre Root-Bridges) pro VLAN zu positionieren.
set spantree backbonefast enable	Schnelle STP-Konvergenz bei indirekten Ausfällen (nur wenn alle Switches in der Domäne die Funktion unterstützen)
set spantree uplfast enable	Schnelle STP-Konvergenz bei direkten Ausfällen (nur für Access-Layer-Switches)
set spantree portfast bpduguard enable	Aktivieren Sie das automatische Herunterfahren des Ports, wenn eine nicht autorisierte Spanning Tree-Erweiterung vorhanden ist.
set udenable	Aktivieren Sie die unidirektionale Verbindungserkennung (auch Konfiguration auf Portebene erforderlich).
Prüfstufe abgeschlossen	Aktivieren Sie beim Hochfahren die vollständige Diagnose (Standardeinstellung bei Catalyst 4500/4000).
set test packetbuffer sun 3:30	Aktivieren Sie die Fehlerprüfung für den Port-Puffer (gilt nur für Catalyst 5500/5000).
Protokollierungspuffer 500	Beibehaltung des maximalen internen Syslog-Puffers
IP-Adresse ***des Protokollierungsservers festlegen***	Konfigurieren Sie den Ziel-Syslog-Server für die Protokollierung externer Systemmeldungen.
set logging server	Lassen Sie den externen Protokollierungsserver zu.
Festlegen des Zeitstempels für die Protokollierung	Aktivieren Sie Zeitstempel von Nachrichten im Protokoll.
voreingestellte Protokollierungsebene Span 6	Erhöhen Sie die Standard-STP-Syslog-Ebene.
Protokollierungsebene festlegen, Standard 6	Erhöhen Sie die Standard-System-Syslog-Ebene.
Protokollierungsserver	Exportieren des Syslog mit

-Schweregrad 4 festlegen	höherem Schweregrad zulassen.
Sperrkonsole einrichten	Deaktivieren Sie die Konsole, wenn Sie keine Fehlerbehebung durchführen.
set snmp community read-only *string*	Konfigurieren Sie das Kennwort, um die Remote-Datenerfassung zu ermöglichen.
set snmp community read-write *string*	Konfigurieren Sie das Kennwort, um eine Remote-Konfiguration zu ermöglichen.
set snmp community read-write-all *string*	Konfigurieren Sie das Kennwort, um eine Remote-Konfiguration einschließlich Kennwörtern zu ermöglichen.
set snmp trap aktiviert alle	Aktivieren Sie SNMP-Traps für Fehler- und Ereigniswarnungen beim NMS-Server.
set snmp trap *server address string*	Konfigurieren Sie die Adresse des NMS-Trap-Empfängers.
set snmp rmon aktivieren	Aktivieren Sie RMON für die lokale Statistikerfassung. Weitere Informationen finden Sie im Abschnitt Remote Monitoring dieses Dokuments.
Set ntp Broadcast Client aktivieren	Aktivieren Sie die genaue Empfang der Systemuhr von einem Upstream-Router.
NTP-Zeitzonenname *festlegen*	Legen Sie die lokale Zeitzone für das Gerät fest.
NTP *Sommerzeitumstellungsdetails* festlegen	Konfigurieren Sie ggf. die Sommerzeit für die Zeitzone.
Set ntp authentication enable	Konfigurieren Sie verschlüsselte Zeitinformationen zu Sicherheitszwecken.
NTP-*Schlüssel* festlegen	Konfigurieren Sie den Verschlüsselungsschlüssel.
set cdp enable	Stellen Sie sicher, dass die Erkennung von Nachbarn aktiviert ist (standardmäßig auch auf Ports aktiviert).
Festlegen der *IP-Adresse des* Takacs-Servers	Konfigurieren Sie die Adresse des AAA-Servers.
IP-Adresse des TACACS-Servers festlegen	Redundante AAA-Server, falls möglich.
Takacs-Versuche	3 Kennwortversuche für das

festlegen 3	AAA-Benutzerkonto zulassen.
Schlüssel ***für Takaks festlegen***	Legen Sie den AAA MD5-Verschlüsselungsschlüssel fest.
Takaks-Timeout festlegen 15	Verlängern Sie die Serverzeitüberschreitung (standardmäßig fünf Sekunden).
Authentifizierungs-Anmeldetaktiken aktivieren	Verwenden Sie AAA zur Authentifizierung für die Anmeldung.
set authentication enable tacacs aktivieren	Verwenden Sie AAA für die Authentifizierung für den Aktivierungsmodus.
Authentifizierungs-Login lokal aktivieren	Default; ermöglicht das Fallback auf lokal, wenn kein AAA-Server verfügbar ist.
set authentication enable local enable aktivieren	Default; ermöglicht das Fallback auf lokal, wenn kein AAA-Server verfügbar ist.

Konfigurationsbefehle für Host-Ports

Befehl	Kommentar
Port Host-*Port-Bereich* festlegen	Entfernen Sie unnötige Port-Verarbeitung. Dieses Makro setzt spantree PortFast enable, channel off, trunk off.
set udld deaktiviert *Port-Bereich*	Entfernen Sie unnötige Port-Verarbeitung (standardmäßig auf Kupferport deaktiviert).
Port-Geschwindigkeit *Port-Bereich* automatisch einstellen	Verwenden Sie die automatische Aushandlung mit aktuellen Host-NIC-Treibern.
Port-Trap-*Port-Bereich* deaktivieren	SNMP-Traps für allgemeine Benutzer sind nicht erforderlich. nur Tastaturanschlüsse verfolgen.

Serverkonfigurationsbefehle

Befehl	Kommentar
Port Host-*Port-Bereich* festlegen	Entfernen Sie unnötige Port-Verarbeitung. Dieses Makro setzt spantree PortFast enable, channel off, trunk off.
set udld deaktiviert *Port-Bereich*	Entfernen Sie unnötige Port-Verarbeitung (standardmäßig auf Kupferport deaktiviert).
Port-Geschwindigkeit *Portbereich 10*	In der Regel sind statische Ports/Server-Ports zu

festlegen	*100*	konfigurieren. Andernfalls automatisierte Verhandlung verwenden.
Port-Duplex-*Portbereich* ***vollständig*** **eingestellt**	***Hälfte***	In der Regel statische Server-Ports; Andernfalls automatisierte Verhandlung verwenden.
Port-Trap-*Port-Bereich* **aktivieren**	Die wichtigen Service-Ports müssen Trap an das NMS senden.

Konfigurationsbefehle für nicht verwendete Ports

Befehl	Kommentar
Festlegung des SpanTree Portfast-*Port-Bereichs* Deaktivieren	Aktivieren Sie die erforderliche Port-Verarbeitung und den erforderlichen Schutz für STP.
Port-Deaktivierung des ***Port-Bereichs festlegen***	Deaktivieren Sie nicht verwendete Ports.
Legen Sie VLAN ***nicht verwendete Dummy-VLAN-Port-Bereich fest.***	Leiten Sie nicht autorisierten Datenverkehr an nicht verwendete VLAN weiter, wenn der Port aktiviert ist.
Trunk-*Port-Bereich* **deaktiviert**	Port vom Trunking bis zur Administration deaktivieren
Port-Channel-*Port-Bereich***-Modus deaktiviert**	Deaktivieren Sie Port-Channeling bis zur Administration.

Infrastruktur-Ports (Switch-Switch, Switch-Router)

Befehl	Kommentar
set udld enable *Port-Bereich*	Aktivieren Sie die unidirektionale Verbindungserkennung (nicht die Standardeinstellung für Kupferports).
set udld Aggressive-Mode enable-*Port-Bereich*	Aktivieren Sie den aggressiven Modus (für Geräte, die diesen Modus unterstützen).
Port Negotiation *Port*-Bereich aktivieren	Zulassen der GE-Standardautomatisierung der Link-Parameter.
Port-Trap-*Port-Bereich* **aktivieren**	SNMP-Traps für diese Schlüsselports zulassen.
Trunk-*Port-Bereich* **deaktiviert**	Funktion deaktivieren, wenn keine Trunks verwendet werden.
Trunk-*Modus/Port* ***wünschenswerte ISL***	Bei Verwendung von Trunks wird dot1q bevorzugt.

festlegen | dot1q | verhandeln	
Clear Trunk *Mod/Port VLAN-Bereich*	Begrenzen Sie den STP-Durchmesser, indem Sie VLANs von Trunks entfernen, die nicht benötigt werden.
Port-Channel-*Port-Bereich*-Modus deaktiviert	Deaktivieren Sie Funktion, wenn Sie keine Kanäle verwenden.
Erwünschter Port-Channel-*Port-Bereich*-Modus festlegen	Bei Verwendung von Kanälen wird PAgP aktiviert.
Festlegen des Port-Channels für alle Distribution-IPs	Lassen Sie bei Verwendung von Kanälen den L3-Quell-/Ziel-Lastenausgleich zu (Standard bei Catalyst 6500/6000).
Trunk-*Modus/Port* ohne Aushandlung von *ISL* festlegen | *dot1q*	Deaktivieren Sie DTP, wenn Trunking zu Router, Catalyst 2900XL, 3500 oder einem anderen Anbieter erfolgt.
Port-Aushandlung-*Modus/Port*-Deaktivierung festlegen	Verhandlungen können für einige alte GE-Geräte inkompatibel sein.

Zugehörige Informationen

- Häufige CatOS-Fehlermeldungen bei Catalyst Switches der Serien 4500 und 4000
- Häufige CatOS-Fehlermeldungen bei Catalyst Switches der Serien 5000 und 5500
- Häufige CatOS-Fehlermeldungen bei Catalyst Switches der Serien 6500 und 6000
- Produktsupport für Switches
- Unterstützung der LAN Switching-Technologie
- Technischer Support und Dokumentation - Cisco Systems