Fehlerbehebung in LAN-Switching-Umgebungen

Einleitung

In diesem Dokument werden die allgemeinen LAN-Switch-Funktionen und die Fehlerbehebung bei Problemen mit dem LAN-Switching beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Konventionen

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

Hintergrundinformationen

In den Abschnitten dieses Kapitels werden die allgemeinen LAN-Switch-Funktionen und -Lösungen für einige der häufigsten LAN-Switching-Probleme beschrieben. Folgende Themen werden behandelt:

LAN-Switching - Einführung

Vorschläge zur Fehlerbehebung bei allgemeinen Switches

Fehlerbehebung bei Verbindungsproblemen mit Ports

Fehlerbehebung: Automatische Aushandlung über 10/100-Mbit-Ethernet-Halb-/Vollduplex

ISL-Trunking auf Catalyst Switches der Serien 5000 und 6000

Konfigurieren des EtherChannel-Switch und Fehlerbehebung für den Switch

Verwenden Sie Portfast und andere Befehle, um Verbindungsprobleme beim Starten der Endstation zu beheben.

Multilayer-Switching konfigurieren und Fehlerbehebung dafür durchführen

LAN-Switching - Einführung

Wenn Sie LAN-Switching noch nicht kennen, werden Sie in diesen Abschnitten durch einige der wichtigsten Konzepte im Zusammenhang mit Switches geführt. Eine Voraussetzung für die Fehlerbehebung bei einem Gerät ist die Kenntnis der Regeln, nach denen es funktioniert. Switches sind in den letzten Jahren sehr viel komplexer geworden, da sie an Popularität und Komplexität gewonnen haben. In diesen Abschnitten werden einige der wichtigsten Konzepte im Zusammenhang mit Switches beschrieben.

Hubs und Switches

Aufgrund der großen Nachfrage nach lokalen Netzwerken wurde von einem Netzwerk mit gemeinsam genutzter Bandbreite, mit Hubs und Koaxialkabeln, zu einem Netzwerk mit dedizierter Bandbreite und Switches übergegangen. Über einen Hub können mehrere Geräte mit demselben Netzwerksegment verbunden werden. Die Geräte in diesem Segment teilen die Bandbreite untereinander. Wenn es sich um einen 10-Mbit/s-Hub handelt und sechs Geräte mit sechs verschiedenen Ports am Hub verbunden sind, teilen sich alle sechs Geräte die 10 Mbit/s Bandbreite untereinander. Ein 100 MB großer Hub nutzt 100 MB an Bandbreite für alle verbundenen Geräte. Für das OSI-Modell gilt ein Hub als Layer-1-Gerät (physische Schicht). Es hört ein elektrisches Signal am Kabel und leitet es an die anderen Ports weiter.

Ein Switch kann einen Hub in Ihrem Netzwerk physisch ersetzen. Mit einem Switch können mehrere Geräte mit demselben Netzwerk verbunden werden, genau wie mit einem Hub, aber hier endet die Ähnlichkeit. Mit einem Switch erhält jedes angeschlossene Gerät eine dedizierte Bandbreite anstelle einer gemeinsam genutzten. Die Bandbreite zwischen dem Switch und dem Gerät ist ausschließlich für die Kommunikation mit und von diesem Gerät reserviert. Sechs Geräte, die an sechs verschiedene Ports an einem 10-MB-Switch angeschlossen sind, verfügen jeweils über 10 MB Bandbreite, mit der sie arbeiten können, anstatt gemeinsam mit anderen Geräten auf Bandbreite zugreifen zu können. Ein Switch kann die verfügbare Bandbreite in Ihrem Netzwerk erheblich erhöhen, was zu einer verbesserten Netzwerkleistung führen kann.

Bridges und Switches

Ein Basis-Switch gilt als Layer-2-Gerät. Wenn Sie das Wort Layer verwenden, beziehen Sie sich auf das 7-Layer-OSI-Modell. Ein Schalter leitet nicht nur elektrische Signale weiter, wie es ein Hub tut, sondern fügt die Signale zu einem Rahmen (Schicht zwei) zusammen und entscheidet dann, was mit dem Rahmen geschehen soll. Ein Switch bestimmt, was mit einem Frame zu tun ist, wenn er sich einen Algorithmus von einem anderen gängigen Netzwerkgerät borgt: eine transparente Bridge. Ein Switch agiert logischerweise genau wie eine transparente Bridge, kann aber Frames viel schneller verarbeiten als eine transparente Bridge (aufgrund spezieller Hardware und Architektur). Sobald ein Switch entscheidet, wohin der Frame gesendet wird, leitet er den Frame an den entsprechenden Port (oder die entsprechenden Ports) weiter. Sie können sich einen Switch als ein Gerät vorstellen, das Frame für Frame sofortige Verbindungen zwischen verschiedenen Ports erstellt.

VLAN

Da der Switch Frame für Frame entscheidet, welche Ports Daten austauschen, ist es eine natürliche Erweiterung, dem Switch eine Logik hinzuzufügen, die es ihm ermöglicht, Ports für spezielle Gruppierungen auszuwählen. Diese Port-Gruppierung wird als Virtual Local Area Network (VLAN) bezeichnet. Der Switch stellt sicher, dass Datenverkehr von einer Portgruppe niemals an andere Portgruppen (die Routing-Geräte sind) gesendet wird. Diese Portgruppen (VLANs) können jeweils als einzelnes LAN-Segment betrachtet werden.

VLANs werden auch als Broadcast-Domänen bezeichnet. Der Grund hierfür ist der transparente

Bridging-Algorithmus, der vorsieht, dass Broadcast-Pakete (Pakete, die für die Adresse der *Geräte* bestimmt sind) von allen Ports derselben Gruppe (d. h. demselben VLAN) gesendet werden. Alle Ports im selben VLAN befinden sich ebenfalls in derselben Broadcast-Domäne.

Transparenter Bridging-Algorithmus

Der transparente Bridging-Algorithmus und Spanning Tree werden an anderer Stelle ausführlicher behandelt (Kapitel 20: Fehlerbehebung in transparenten Bridging-Umgebungen). Wenn ein Switch einen Frame empfängt, muss er entscheiden, was er mit diesem Frame tun möchte. Er könnte den Frame ignorieren, ihn an einen anderen Port weiterleiten oder den Frame an viele andere Ports weiterleiten.

Um zu erfahren, was mit dem Frame zu tun ist, erfährt der Switch den Standort aller Geräte im Segment. Diese Standortinformationen werden in einer Content-Addressable-Memory-Tabelle (CAM) abgelegt, die nach dem Speichertyp benannt wird, der zum Speichern dieser Tabellen verwendet wird. Die CAM-Tabelle zeigt für jedes Gerät die MAC-Adresse des Geräts, aus welchem Port diese MAC-Adresse zu finden ist und mit welchem VLAN dieser Port verbunden ist. Der Switch lernt fortlaufend, wenn Frames in den Switch empfangen werden. Die CAM-Tabelle des Switches wird laufend aktualisiert.

Anhand dieser Informationen in der CAM-Tabelle wird entschieden, wie ein empfangener Frame behandelt wird. Um zu entscheiden, wohin ein Frame gesendet werden soll, betrachtet der Switch die Ziel-MAC-Adresse in einem empfangenen Frame und sucht diese Ziel-MAC-Adresse in der CAM-Tabelle. Die CAM-Tabelle zeigt, welcher Port für den Frame ausgesendet werden muss, damit dieser die angegebene MAC-Zieladresse erreicht. Nachfolgend sind die grundlegenden Regeln aufgeführt, die ein Switch verwendet, um die Verantwortung für die Frame-Weiterleitung auszuführen:

Wenn die Ziel-MAC-Adresse in der CAM-Tabelle gefunden wird, sendet der Switch das Frame an den Port, der dieser Ziel-MAC-Adresse in der CAM-Tabelle zugeordnet ist. Dies wird als *Weiterleitung* bezeichnet.

Wenn der zugeordnete Port, an den der Frame gesendet wird, derselbe Port ist, an den der Frame ursprünglich gesendet wurde, muss der Frame nicht an denselben Port zurückgesendet werden, und der Frame wird ignoriert. Dies wird als *Filterung* bezeichnet.

Wenn die MAC-Zieladresse nicht in der CAM-Tabelle enthalten ist (die Adresse ist *unbekannt),* sendet der Switch den Frame an alle anderen Ports, die sich im selben VLAN wie der empfangene Frame befinden. Das nennt man Überschwemmung. Der Frame wird nicht über denselben Port geflutet, an dem der Frame empfangen wurde.

Wenn die Ziel-MAC-Adresse des empfangenen Frames die Broadcast-Adresse (FFFF.FFFF.FFFF) ist, wird der Frame an alle Ports gesendet, die sich im gleichen VLAN wie der empfangene Frame befinden. Dies wird auch als Überschwemmung bezeichnet. Der Frame wird nicht über denselben Port gesendet, über den der Frame empfangen wurde.

Spanning Tree Protocol

Wie Sie gesehen haben, flutet der transparente Bridging-Algorithmus unbekannte Frames und Broadcast-Frames von allen Ports, die sich im selben VLAN wie der empfangene Frame befinden.

Dies verursacht ein potenzielles Problem. Wenn die Netzwerkgeräte, die diesen Algorithmus ausführen, in einer physischen Schleife miteinander verbunden sind, werden geflutete Frames (wie Broadcasts) von Switch zu Switch weitergeleitet, und zwar für immer und rund um die Schleife. Abhängig von den physikalischen Verbindungen können sich die Frames aufgrund des Flooding-Algorithmus sogar exponentiell vervielfachen, was zu schwerwiegenden Netzwerkproblemen führen kann.

Ein physischer Loop in Ihrem Netzwerk hat den Vorteil, dass er Redundanz bietet. Wenn eine Verbindung ausfällt, gibt es noch eine andere Möglichkeit für den Datenverkehr, sein Ziel zu erreichen. Um die Vorteile der Redundanz zu nutzen und das Netzwerk nicht aufgrund von Flooding zu beschädigen, wurde ein Protokoll namens Spanning Tree erstellt. Spanning Tree wurde in der IEEE 802.1d-Spezifikation standardisiert.

Das Spanning Tree Protocol (STP) dient dazu, die Schleifen in einem Netzwerksegment oder VLAN zu identifizieren und vorübergehend zu blockieren. Auf den Switches wird STP ausgeführt, und es wird eine Root-Bridge oder ein Switch ausgewählt. Die anderen Switches messen ihren Abstand zum Root-Switch. Wenn es mehr als eine Möglichkeit gibt, zum Root-Switch zu gelangen, gibt es eine Schleife. Die Switches verfolgen den Algorithmus, um zu bestimmen, welche Ports blockiert werden müssen, damit die Schleife unterbrochen wird. STP ist dynamisch. Wenn eine Verbindung im Segment ausfällt, können Ports, die ursprünglich blockiert wurden, in den Weiterleitungsmodus geändert werden.

Trunking

Trunking ist ein Mechanismus, der am häufigsten verwendet wird, damit mehrere VLANs unabhängig über mehrere Switches hinweg funktionieren. Router und Server können ebenfalls Trunking verwenden, wodurch sie gleichzeitig auf mehreren VLANs arbeiten können. Wenn in Ihrem Netzwerk nur ein VLAN vorhanden ist, ist Trunking nicht zwingend erforderlich. Wenn Ihr Netzwerk jedoch über mehr als ein VLAN verfügt, sollten Sie die Vorteile von Trunking nutzen.

Ein Port auf einem Switch gehört normalerweise nur zu einem VLAN. Es wird angenommen, dass jeder über diesen Port empfangene oder gesendete Datenverkehr zu dem konfigurierten VLAN gehört. Ein Trunk-Port dagegen ist ein Port, der so konfiguriert werden kann, dass er Datenverkehr für viele VLANs sendet und empfängt. Dies wird erreicht, wenn VLAN-Informationen an jeden Frame angehängt werden. Dieser Prozess wird als *Tagging* des Frames bezeichnet. Außerdem muss das Trunking auf beiden Seiten der Verbindung aktiv sein; die andere Seite muss Frames erwarten, die VLAN-Informationen enthalten, damit eine ordnungsgemäße Kommunikation stattfinden kann.

Je nach verwendetem Medium stehen verschiedene Trunking-Methoden zur Verfügung. Trunking-Methoden für Fast Ethernet oder Gigabit Ethernet sind Inter-Switch Link (ISL) oder 802.1q. Beim Trunking über den ATM wird LANE verwendet. Trunking over FDDI verwendet 802.10.

EtherChannel

EtherChannel ist eine Technik, die verwendet wird, wenn mehrere Verbindungen zum gleichen Gerät bestehen. Anstatt dass jede Verbindung einzeln funktioniert, gruppiert der EtherChannel die Ports so, dass sie als eine Einheit fungieren. Sie verteilt den Datenverkehr auf alle Verbindungen und sorgt für Redundanz, wenn eine oder mehrere Verbindungen ausfallen. Die EtherChannel-Einstellungen müssen auf beiden Seiten der für den Kanal verwendeten Links identisch sein. Normalerweise würde Spanning Tree alle diese parallelen Verbindungen zwischen Geräten blockieren, da es sich um Schleifen handelt, aber EtherChannel läuft *unter* Spanning Tree, sodass Spanning Tree annimmt, dass alle Ports innerhalb eines bestimmten EtherChannels nur ein

einzelner Port sind.

Multilayer-Switching (MLS)

Multilayer Switching (MLS) ist die Fähigkeit eines Switches, Frames basierend auf Informationen im Layer-3- und manchmal auch Layer-4-Header weiterzuleiten. Dies gilt in der Regel für IP-Pakete, kann jetzt aber auch für IPX-Pakete auftreten. Der Switch lernt, wie mit diesen Paketen umzugehen ist, wenn er mit einem oder mehreren Routern kommuniziert. Vereinfacht lässt sich sagen, dass der Switch überwacht, wie der Router ein Paket verarbeitet, und dass der Switch anschließend zukünftige Pakete in diesem Datenfluss verarbeitet. In der Vergangenheit waren Switches bei Switching-Frames viel schneller als Router. Daher kann die Auslagerung des Datenverkehrs vom Router zu erheblichen Geschwindigkeitsverbesserungen führen. Wenn sich etwas im Netzwerk ändert, kann der Router den Switch anweisen, seinen Layer-3-Cache zu löschen und ihn im Verlauf der weiteren Entwicklung von Grund auf neu zu erstellen. Das Protokoll für die Kommunikation mit den Routern wird als Multilayer Switching Protocol (MLSP) bezeichnet.

Weitere Informationen zu diesen Funktionen

Dies sind nur einige der grundlegenden Funktionen, die von Switches unterstützt werden. Jeden Tag kommen weitere hinzu. Es ist wichtig zu wissen, wie Ihre Switches funktionieren, welche Funktionen Sie verwenden und wie diese Funktionen funktionieren müssen. Diese Informationen zu Cisco Switches finden Sie am besten auf der Cisco Website. Gehen Sie zum Abschnitt *Service & Support* und wählen Sie *Technische Dokumente aus*. Wählen Sie hier die *Startseite der Dokumentation* . Die Dokumentationssätze für alle Cisco Produkte finden Sie hier. Über den Link *Multilayer LAN Switches* gelangen Sie zur Dokumentation für alle Cisco LAN Switches. Weitere Informationen zu den Funktionen eines Switches finden Sie im *Software-Konfigurationsleitfaden* für die jeweilige Version der von Ihnen verwendeten Software. Die Software-Konfigurationsanleitungen enthalten Hintergrundinformationen zu den Funktionen und Befehlen, die Sie für die Switch-Konfiguration verwenden müssen. Alle diese Informationen sind kostenlos im Web. Sie benötigen nicht einmal ein Konto für diese Dokumentation; es ist für jeden verfügbar. Einige dieser Konfigurationsleitfäden können an einem Nachmittag gelesen werden und sind den Zeitaufwand wert.

Ein weiterer Teil der Cisco Website wird von der Cisco Support- und Dokumentations-Website bereitgestellt. Er enthält Informationen, die Ihnen bei der Implementierung, Wartung und Fehlerbehebung Ihres Netzwerks helfen. Auf der Website für Support und Dokumentation erhalten Sie detaillierte Support-Informationen zu bestimmten Produkten oder Technologien.

Vorschlag zur Fehlerbehebung bei allgemeinen Switches

Es gibt viele Möglichkeiten, einen Switch zu reparieren. Mit der Funktionserweiterung der Switches nehmen auch die Bruchmöglichkeiten zu. Für eine effektive Fehlerbehebung sollten Sie einen Ansatz oder einen Testplan entwickeln, anstatt einen "Hit-and-Miss"-Ansatz zu verfolgen. Hier einige allgemeine Vorschläge:

- Nehmen Sie sich die Zeit, sich mit dem normalen Switch-Betrieb vertraut zu machen. Auf der Cisco Website finden Sie eine Vielzahl technischer Informationen zur Funktionsweise der Switches, wie im vorherigen Abschnitt beschrieben. Insbesondere die Konfigurationsanleitungen sind sehr hilfreich. Es werden viele Tickets geöffnet, die mit Informationen aus den Produktkonfigurationsanleitungen gelöst werden.

- Erstellen Sie in komplexen Situationen eine präzise physische und logische Darstellung Ihres Netzwerks. Eine physische Karte zeigt, wie die Geräte und Kabel verbunden sind. Eine logische Zuordnung zeigt, welche Segmente (VLANs) in Ihrem Netzwerk vorhanden sind und welche Router Routing-Services für diese Segmente bereitstellen. Eine Spanning Tree Map ist sehr nützlich, um komplexe Probleme zu beheben. Da ein Switch mit der Implementierung von VLANs unterschiedliche Segmente erstellen kann, ist die physikalische Anbindung allein nicht das Geringste; man muss wissen, wie die Switches konfiguriert sind, um zu bestimmen, welche Segmente (VLANs) vorhanden sind, und um zu wissen, wie sie logisch verbunden sind.

  Einen Plan. Einige Probleme und Lösungen sind offensichtlich, andere nicht. Die Symptome, die Sie in Ihrem Netzwerk sehen, können das Ergebnis von Problemen in einem anderen Bereich oder Layer sein. Bevor Sie zu Schlussfolgerungen springen, versuchen Sie, in einer strukturierten Weise zu überprüfen, was funktioniert und was nicht. Da Netzwerke komplex sein können, ist es hilfreich, mögliche Problemdomänen zu isolieren. Eine Möglichkeit hierfür ist das OSI-Modell mit sieben Schichten. Prüfen Sie z. B. die physischen Verbindungen (Layer 1), Verbindungsprobleme innerhalb des VLAN (Layer 2) und Verbindungsprobleme zwischen verschiedenen VLANs (Layer 3) usw. Wenn der Switch korrekt konfiguriert ist, beziehen sich viele Probleme auf physische Layer-Probleme (physische Ports und Kabel). Switches sind heutzutage mit Layer-3- und Layer-4-Problemen konfrontiert, bei denen intelligente Funktionen zum Vermitteln von Paketen auf der Grundlage von Informationen von Routern zum Einsatz kommen oder bei denen im Switch Router vorhanden sind (Layer-3- oder Layer-4-Switching).

  Gehen Sie nicht davon aus, dass eine Komponente funktioniert, sondern überprüfen Sie sie zuerst. Dies kann Ihnen viel verschwendete Zeit ersparen. Wenn sich ein PC beispielsweise nicht bei einem Server im Netzwerk anmelden kann, können viele Dinge falsch sein. Überspringen Sie nicht die grundlegenden Dinge und gehen Sie davon aus, dass etwas funktioniert; jemand kann etwas geändert haben und nicht gesagt, Ihnen. Es dauert nur eine Minute, um einige der grundlegenden Dinge zu überprüfen (zum Beispiel, dass die betreffenden Ports an die richtige Stelle angeschlossen sind und aktiv sind), was Ihnen viele verschwendete Stunden sparen könnte.

Fehlerbehebung bei Verbindungsproblemen an Ports

Wenn der Port nicht funktioniert, funktioniert nichts! Ports bilden die Grundlage Ihres Switching-Netzwerks. Einige Ports sind aufgrund ihrer Position im Netzwerk und des von ihnen übertragenen Datenverkehrs von besonderer Bedeutung. Diese Ports umfassen Verbindungen zu anderen Switches, Routern und Servern. Die Fehlerbehebung für diese Ports kann komplizierter sein, da sie häufig spezielle Funktionen wie Trunking und EtherChannel nutzen. Die übrigen Ports sind ebenfalls von Bedeutung, da sie die eigentlichen Benutzer des Netzwerks verbinden.

Viele Faktoren können dazu führen, dass ein Port nicht funktioniert: Hardware-, Konfigurations- und Datenverkehrsprobleme. Diese Kategorien werden etwas genauer untersucht.

Hardware-Probleme

Allgemein

Für die Portfunktion sind zwei aktive Ports erforderlich, die über ein aktives Kabel (des richtigen

Typs) verbunden sind. Die meisten Cisco Switches verfügen standardmäßig über einen Port im Status "*Not Connect"*, d. h., dass derzeit keine Verbindung besteht, aber eine Verbindung hergestellt werden soll. Wenn Sie ein gutes Kabel an zwei Switch-Ports im Zustand "*Not Connect"* anschließen, leuchtet die Verbindungsleuchte für beide Ports grün, und der Port-Status lautet "*Connected" (Verbunden),* was bedeutet, dass der Port für Layer 1 aktiv ist. In diesen Abschnitten werden Elemente aufgeführt, bei denen überprüft werden muss, ob Schicht eins nicht aktiv ist.

Überprüfen Sie den Portstatus für beide beteiligten Ports. Vergewissern Sie sich, dass keiner der an der Verbindung beteiligten Ports heruntergefahren ist. Der Administrator kann möglicherweise einen oder beide Ports heruntergefahren haben. Software innerhalb des Switches kann den Port aufgrund von Konfigurationsfehlern heruntergefahren haben. Wenn eine Seite ausgeschaltet ist und die andere nicht, wird der Status auf der aktivierten Seite *nicht verbunden (*da kein Nachbar auf der anderen Seite des Kabels erkannt wird). Der Status auf der Seite zum Herunterfahren sagt etwas wie *disable* oder errDisable *(*abhängig davon, was den Port tatsächlich heruntergefahren hat) aus. Die Verbindung wird erst aktiviert, wenn beide Ports aktiviert sind.

Wenn Sie ein gutes Kabel (wenn es vom richtigen Typ ist) zwischen zwei aktivierten Ports anschließen, leuchtet innerhalb weniger Sekunden eine grüne Verbindung auf. Außerdem zeigt der Portstatus "*connected*" (*verbunden)* in der Befehlszeilenschnittstelle (CLI) an. Wenn Sie an diesem Punkt keine Verbindung haben, ist Ihr Problem auf drei Dinge beschränkt: den Port auf der einen Seite, den Port auf der anderen Seite oder das Kabel in der Mitte. In einigen Fällen sind andere Geräte beteiligt: Medienkonverter (Glasfaser zu Kupfer usw.), oder auf Gigabit-Verbindungen können Sie Gigabit-Schnittstellenverbindungen (GBICs) verwenden. Trotzdem ist dies ein relativ begrenzter Bereich, in dem gesucht werden kann.

Medienkonverter können einer Verbindung Rauschen hinzufügen oder das Signal schwächen, wenn sie nicht richtig funktionieren. Sie fügen außerdem zusätzliche Anschlüsse hinzu, die Probleme verursachen können, und sind eine weitere zu debuggende Komponente.

Suchen Sie nach losen Verbindungen. Manchmal scheint ein Kabel in der Buchse zu sitzen, aber das ist es nicht. Ziehen Sie das Kabel ab, und führen Sie es erneut ein. Sie müssen auch nach Schmutz, verlorenen oder gebrochenen Pins suchen. Führen Sie diesen Vorgang für beide an der Verbindung beteiligten Ports aus.

Das Kabel kann an den falschen Port angeschlossen werden, was in der Regel der Fall ist. Vergewissern Sie sich, dass beide Enden des Kabels an den gewünschten Stellen angeschlossen sind.

Sie können einen Link auf der einen Seite haben und nicht auf der anderen. Überprüfen Sie beide Seiten auf den Link. Ein einzelner unterbrochener Draht kann diese Art von Problem verursachen.

Eine Verbindungsleuchte garantiert nicht, dass das Kabel voll funktionsfähig ist. Es kann auf physische Belastung gestoßen sein, die dazu führt, dass es auf einer marginalen Ebene funktioniert. Normalerweise bemerken Sie dies an dem Port, der viele Paketfehler aufweist.

Ersetzen Sie das Kabel durch ein zweifelsfrei funktionierendes Kabel, um festzustellen, ob das Problem auf dem Kabel besteht. Tauschen Sie das Kabel nicht einfach durch ein anderes Kabel aus. Stellen Sie sicher, dass Sie es durch ein Kabel ersetzen, von dem Sie wissen, dass es gut ist und den richtigen Typ aufweist.

Wenn es sich um eine sehr lange Kabelführung handelt (unterirdisch, zum Beispiel über einen großen Campus), ist es schön, einen ausgeklügelten Kabeltester zu haben. Wenn Sie keinen Kabeltester haben, können Sie Folgendes berücksichtigen:

Testen Sie verschiedene Anschlüsse, um festzustellen, ob diese mit diesem langen Kabel geliefert werden.

Schließen Sie den betreffenden Port an einen anderen Port im selben Switch an, um zu sehen, ob der Port lokal verbunden ist.

Versetzen Sie die Switches vorübergehend in die Nähe, sodass Sie ein zweifelsfrei funktionierendes Kabel ausprobieren können.

Kupfer

Vergewissern Sie sich, dass Sie über das richtige Kabel für den Verbindungstyp verfügen. Kabel der Kategorie 3 können für 10-MB-UTP-Verbindungen verwendet werden, aber Kabel der Kategorie 5 müssen für 10/100-Verbindungen verwendet werden.

Ein gerades RJ-45-Kabel dient dazu, Endgeräte, Router oder Server mit einem Switch oder Hub zu verbinden. Ein Ethernet-Crossover-Kabel wird für Switch-to-Switch- oder Hub-to-Switch-Verbindungen verwendet. Dies ist der Pin-Out für ein Ethernet-Crossover-Kabel. Die maximalen Entfernungen für Ethernet- oder Fast Ethernet-Kupferkabel betragen 100 Meter. Eine gute allgemeine Faustregel ist, dass Sie beim Überqueren einer OSI-Schicht, wie zwischen einem Switch und einem Router, ein Durchgangskabel verwenden. Wenn Sie zwei Geräte in derselben OSI-Schicht, wie zwischen zwei Routern oder zwei Switches, verbinden, verwenden Sie ein Crossover-Kabel. Behandeln Sie eine Workstation nur zu diesem Zweck wie einen Router.

Diese beiden Grafiken zeigen die Pin-Belegungen, die für ein Switch-to-Switch-Crossover-Kabel erforderlich sind.

Glasfaser

Stellen Sie bei Glasfaserkabeln sicher, dass Sie über das richtige Kabel für die erforderlichen Entfernungen verfügen und über die Art der verwendeten Glasfaserports (Single Mode, Multi Mode). Stellen Sie sicher, dass es sich bei den miteinander verbundenen Ports sowohl um Single-Mode- als auch um Multi-Mode-Ports handelt. Single-Mode-Fiber erreicht in der Regel 10 Kilometer, und Multi-Mode-Fiber kann in der Regel 2 Kilometer erreichen, aber es gibt den besonderen Fall von 100BaseFX Multi-Mode im Halbduplex-Modus verwendet, die nur 400 Meter gehen kann.

Achten Sie bei Glasfaserverbindungen darauf, dass die Übertragungsleitung eines Ports mit der Empfangsleitung des anderen Ports verbunden ist und umgekehrt. Senden zum Senden, Empfangen zum Empfangen funktioniert nicht.

Bei Gigabit-Verbindungen müssen die GBICs auf beiden Seiten der Verbindung abgeglichen werden. Je nach Kabel und Distanz gibt es verschiedene GBIC-Typen: Short Wavelength (SX), Long Wavelength/Long Haul (LX/LH) und Extended Distance (ZX).

Ein SX-GBIC muss mit einem SX-GBIC verbunden sein; ein SX-GBIC ist nicht mit einem LX-GBIC verbunden. Einige Gigabit-Verbindungen erfordern zudem Konditionierungskabel, die von den jeweiligen Längen abhängen. Siehe die GBIC-Installationshinweise.

Wenn Ihr Gigabit-Link nicht verfügbar ist, überprüfen Sie, ob die Einstellungen für Flusskontrolle und Port-Aushandlung auf beiden Seiten des Links konsistent sind. Die Implementierung dieser Funktionen kann inkompatibel sein, wenn die verbundenen Switches von verschiedenen Anbietern

stammen. Schalten Sie diese Funktionen im Zweifelsfall auf beiden Switches aus.

Konfigurationsprobleme

Eine weitere Ursache für Port-Verbindungsprobleme ist die falsche Softwarekonfiguration des Switches. Wenn ein Port über eine durchgehend orangefarbene Anzeige verfügt, bedeutet dies, dass die Software innerhalb des Switches den Port entweder über die Benutzeroberfläche oder durch interne Prozesse ausschaltet.

Stellen Sie sicher, dass der Administrator die betreffenden Ports nicht heruntergefahren hat (wie erwähnt). Der Administrator kann den Port auf der einen oder anderen Seite der Verbindung manuell heruntergefahren haben. Dieser Link wird erst aktiviert, wenn Sie den Port erneut aktivieren. Überprüfen Sie den Port-Status.

Einige Switches, z. B. Catalyst 4000/5000/6000, können den Port herunterfahren, wenn Softwareprozesse im Switch einen Fehler erkennen. Wenn Sie sich den Port-Status ansehen, lautet der Text *errDisable* . Sie müssen das Konfigurationsproblem beheben und dann den errDisable-Status des Ports manuell entfernen. Einige neuere Softwareversionen (CatOS 5.4(1) und höher) können einen Port nach einer konfigurierbaren Zeitspanne, die im errDisable-Zustand verbracht wurde, automatisch wieder aktivieren. Dies sind einige der Ursachen für diesen errDisable-Zustand:

EtherChannel Misconfiguration: Wenn eine Seite für den EtherChannel konfiguriert ist, die andere nicht, kann dies dazu führen, dass der Spanning Tree-Prozess den Port auf der für den EtherChannel konfigurierten Seite herunterfährt. Wenn Sie versuchen, einen EtherChannel zu konfigurieren, die betroffenen Ports jedoch nicht die gleichen Einstellungen (Geschwindigkeit, Duplex, Trunking-Modus usw.) haben wie ihre benachbarten Ports über den Link, kann dies den Status errDisable verursachen. Wenn Sie den EtherChannel verwenden möchten, empfiehlt es sich, für jede Seite den *gewünschten* EtherChannel-Modus festzulegen. In den folgenden Abschnitten wird ausführlich erläutert, wie Sie den EtherChannel konfigurieren.

Duplex-Konflikt: Wenn der Switch-Port viele späte Kollisionen empfängt, weist dies in der Regel auf ein Duplex-Konflikt-Problem hin. Es gibt noch andere Ursachen für späte Kollisionen: eine schlechte Netzwerkkarte, Kabelsegmente, die zu lang sind, aber der häufigste Grund heute ist eine Duplexungleichheit. Die Vollduplex-Seite denkt, dass sie senden kann, wann immer sie will. Auf der Halbduplex-Seite werden Pakete nur zu bestimmten Zeiten erwartet, nicht zu "irgendeiner" Zeit.

BPDU Port-Guard: Einige neuere Versionen der Switch-Software können überwachen, ob PortFast auf einem Port aktiviert ist. Ein Port, der portfast verwendet, muss mit einer Endstation verbunden werden, nicht mit Geräten, die Spanning Tree-Pakete, so genannte BPDUs, generieren. Wenn der Switch eine BPDU bemerkt, die in einem Port mit aktiviertem portfast vorhanden ist, versetzt er den Port in den errDisable-Modus.

UDLD: Unidirectional Link Detection ist ein Protokoll auf einigen neuen Softwareversionen, das feststellt, ob die Kommunikation über eine Verbindung nur in eine Richtung erfolgt. Ein beschädigtes Glasfaserkabel oder andere Probleme mit Kabeln/Ports können zu dieser unidirektionalen Kommunikation führen. Diese teilweise funktionsfähigen Verbindungen können Probleme verursachen, wenn die beteiligten Switches nicht wissen, dass die Verbindung teilweise unterbrochen ist. Spanning-Tree-Schleifen können bei diesem Problem

auftreten. UDLD kann so konfiguriert werden, dass ein Port den Status "errDisable" erhält, wenn eine unidirektionale Verbindung erkannt wird.

Native VLAN Mismatch: Bevor ein Port Trunking aktiviert hat, gehört er zu einem einzelnen VLAN. Wenn Trunking aktiviert ist, kann der Port Datenverkehr für viele VLANs übertragen. Der Port erinnert sich noch immer an das VLAN, in dem er sich vor dem Aktivieren des Trunking befand. Dieses VLAN wird als natives VLAN bezeichnet. Das native VLAN ist für das 802.1q-Trunking von zentraler Bedeutung. Wenn das native VLAN an beiden Enden der Verbindung nicht übereinstimmt, wechselt ein Port in den Status errDisable.

Sonstiges: Jeder Prozess innerhalb des Switches, der ein Problem mit dem Port erkennt, kann diesen in den Status *errDisable versetzen*.

Eine weitere Ursache für inaktive Ports besteht darin, dass das zugehörige VLAN nicht mehr verfügbar ist. Jeder Port eines Switches gehört zu einem VLAN. Wenn dieses VLAN gelöscht wird, wird der Port inaktiv. Einige Switches leuchten orange auf jedem Port, an dem dies geschehen ist. Wenn Sie eines Tages zur Arbeit kommen und Hunderte von orangefarbenen Anzeigen sehen, keine Panik; es könnte sein, dass alle Ports zum gleichen VLAN gehören und jemand versehentlich das VLAN gelöscht, zu dem die Ports gehörten. Wenn Sie das VLAN wieder der VLAN-Tabelle hinzufügen, werden die Ports wieder aktiv. Ein Port speichert das ihm zugewiesene VLAN.

Wenn Sie einen Link haben und die Ports als verbunden angezeigt werden, Sie aber nicht mit einem anderen Gerät kommunizieren können, kann dies besonders verblüffend sein. In der Regel weist dies auf ein höheres Problem hin als die physische Schicht: Layer 2 oder Layer 3. Probieren Sie diese Dinge aus.

Überprüfen Sie den Trunking-Modus auf beiden Seiten der Verbindung. Vergewissern Sie sich, dass sich beide Seiten im gleichen Modus befinden. Wenn Sie den Trunking-Modus für einen Port auf "on" (im Gegensatz zu "auto" oder "wünschenswert") setzen und der andere Port den Trunking-Modus

Modus auf "Aus" gesetzt ist, können sie nicht kommunizieren. Trunking ändert das Paketformat. Die Ports müssen sich darauf einigen, welches Format sie für die Verbindung verwenden, oder sie verstehen sich nicht.

Vergewissern Sie sich, dass sich alle Geräte im selben VLAN befinden. Wenn sie sich nicht im selben VLAN befinden, muss ein Router konfiguriert werden, der den Geräten die Kommunikation ermöglicht.

Vergewissern Sie sich, dass Ihre Layer-3-Adressierung korrekt konfiguriert ist.

Probleme mit dem Datenverkehr

In diesem Abschnitt werden einige der Lerninhalte beschrieben, die Sie lernen können, wenn Sie die Verkehrsinformationen eines Ports betrachten. Die meisten Switches haben eine Möglichkeit, Pakete zu verfolgen, wenn diese einen Port passieren oder diesen verlassen. Befehle, die diese Art von Ausgabe auf den Catalyst Switches der Serien 4000/5000/6000 generieren, sind show-

Port und show-Mac. Die Ausgabe dieser Befehle auf den 4000/5000/6000-Switches wird in den Switch-Befehlsreferenzen beschrieben.

Einige dieser Felder für den Port-Datenverkehr zeigen an, wie viele Daten auf dem Port übertragen und empfangen werden. Andere Felder zeigen an, wie viele Fehler-Frames auf dem Port aufgetreten sind. Bei großen Ausrichtungsfehlern, FCS-Fehlern oder verspäteten Kollisionen kann dies auf eine Duplexunstimmigkeit auf dem Kabel hinweisen. Weitere Ursachen für diese Art von Fehlern können fehlerhafte Netzwerkschnittstellenkarten oder Kabelprobleme sein. Wenn Sie eine große Anzahl von Frames mit verzögerter Verarbeitung haben, ist dies ein Zeichen dafür, dass Ihr Segment zu viel Datenverkehr hat. Der Switch kann nicht genügend Datenverkehr über die Leitung senden, um die Puffer zu leeren. Ziehen Sie in Betracht, einige Geräte aus einem anderen Segment zu entfernen.

Switch-Hardwarefehler

Wenn Sie alles ausprobiert haben, was Sie sich vorstellen können, und der Port nicht funktioniert, kann es fehlerhafte Hardware geben.

Manchmal werden Anschlüsse durch elektrostatische Entladung (ESD) beschädigt. Sie können oder können keinen Hinweis darauf sehen.

Prüfen Sie anhand der Ergebnisse des Selbsttests (POST), ob für einen Teil des Switches Fehler aufgetreten sind.

Wenn Sie ein Verhalten sehen, das nur als "seltsam" angesehen werden kann, kann dies auf Hardwareprobleme hinweisen, aber auch auf Softwareprobleme. Normalerweise ist es einfacher, die Software neu zu laden, als neue Hardware zu kaufen. Versuchen Sie zunächst, mit der Switch-Software zu arbeiten.

Das Betriebssystem kann einen Fehler aufweisen. Wenn Sie ein neueres Betriebssystem laden, könnte dies behoben werden. Sie können bekannte Fehler recherchieren, wenn Sie die Versionshinweise für die verwendete Codeversion lesen oder das Cisco Bug ToolKit verwenden.

Das Betriebssystem könnte beschädigt sein. Wenn Sie dieselbe Version des Betriebssystems neu laden, können Sie das Problem beheben.

Wenn die Statusanzeige am Switch orange blinkt, bedeutet dies in der Regel, dass ein Hardwareproblem mit dem Port, dem Modul oder dem Switch besteht. Dasselbe gilt, wenn der Port- oder Modulstatus *fehlerhaft* ist.

Bevor Sie die Switch-Hardware austauschen, können Sie einige Dinge ausprobieren:

Setzen Sie das Modul wieder in den Switch ein. Wenn Sie dies beim Einschalten durchführen, stellen Sie sicher, dass das Modul Hot-Swap-fähig ist. Schalten Sie im Zweifelsfall den Switch aus, bevor Sie das Modul wieder einsetzen, oder lesen Sie die Hardware-Installationsanleitung. Wenn der Port in den Switch integriert ist, ignorieren Sie diesen Schritt.

Neustarten des Switches. Manchmal verschwindet das Problem dadurch, es handelt sich um eine Problemumgehung und nicht um eine Lösung.

Überprüfen Sie die Switch-Software. Wenn es sich um eine Neuinstallation handelt, denken Sie daran, dass einige Komponenten nur mit bestimmten Softwareversionen funktionieren

können. Lesen Sie die Versionshinweise oder die Hardware-Installations- und Konfigurationsanleitung für die von Ihnen installierte Komponente.

Wenn Sie hinreichend sicher sind, dass Sie ein Hardwareproblem haben, ersetzen Sie die fehlerhafte Komponente.

Fehlerbehebung: Automatische Aushandlung über Ethernet mit 10/100 MB Halb-/Vollduplex

Ziele

Dieser Abschnitt enthält allgemeine Informationen zur Fehlerbehebung sowie eine Erläuterung der Verfahren zur Fehlerbehebung bei der automatischen Ethernet-Aushandlung.

In diesem Abschnitt wird gezeigt, wie das aktuelle Verhalten einer Verbindung bestimmt wird. Außerdem wird erläutert, wie Benutzer das Verhalten steuern können, und es werden Situationen erläutert, in denen die automatische Aushandlung fehlschlägt.

Viele verschiedene Cisco Catalyst Switches und Cisco Router unterstützen die automatische Aushandlung. Dieser Abschnitt behandelt die automatische Aushandlung zwischen Catalyst Switches der Serie 5000. Die hier erläuterten Konzepte können auch auf die anderen Gerätetypen angewendet werden.

Einleitung

Die automatische Aushandlung ist eine optionale Funktion des IEEE 802.3u Fast Ethernet-Standards, mit der es Geräten ermöglicht wird, Informationen über Geschwindigkeits- und Duplexfähigkeiten automatisch über einen Link auszutauschen.

Auto-Negotiation richtet sich an Ports, die Bereichen zugewiesen werden, in denen vorübergehende Benutzer oder Geräte eine Verbindung mit einem Netzwerk herstellen. Viele Unternehmen stellen beispielsweise gemeinsam genutzte Büroräume oder Würfel zur Verfügung, die Account Manager und Systemtechniker nutzen können, wenn sie sich im Büro und nicht unterwegs befinden. Jedes Büro bzw. jeder Cube verfügt über einen Ethernet-Port, der fest mit dem Netzwerk des Büros verbunden ist. Da nicht sichergestellt werden kann, dass jeder Benutzer entweder eine 10-Mbit/s-, eine 100-Mbit/s-Ethernet- oder eine 10/100-Mbit/s-Karte im Laptop hat, müssen die Switch-Ports, die diese Verbindungen verarbeiten, in der Lage sein, ihre Geschwindigkeit und ihren Duplexmodus auszuhandeln. Die Alternative ist in der Lage, in jedem Büro oder Würfel einen 10-Mbit- und einen 100-Mbit-Port bereitzustellen und diese entsprechend zu kennzeichnen.

Auto-Negotiation darf nicht für Ports verwendet werden, die Geräte der Netzwerkinfrastruktur unterstützen, z. B. Switches und Router oder andere nicht flüchtige Endsysteme wie Server und Drucker. Obwohl Auto-Negotiation für Geschwindigkeit und Duplex normalerweise das Standardverhalten für Switch-Ports ist, die dazu in der Lage sind, müssen Ports, die mit festen Geräten verbunden sind, immer für das richtige Verhalten konfiguriert werden, anstatt es aushandeln zu dürfen. Auf diese Weise werden potenzielle Verhandlungsprobleme vermieden und sichergestellt, dass Sie immer genau wissen, wie die Ports funktionieren müssen. Eine

10/100BaseTX-Ethernet-Switch-to-Switch-Verbindung, die beispielsweise für 100-Mbit/s-Vollduplex konfiguriert wurde, funktioniert nur mit dieser Geschwindigkeit und diesem Modus. Es besteht keine Möglichkeit für die Ports, die Verbindung innerhalb eines Port-Resets oder Switch-Resets auf eine langsamere Geschwindigkeit herabzusetzen. Falls die Ports nicht wie konfiguriert funktionieren, dürfen sie keinen Datenverkehr weiterleiten. Auf der anderen Seite kann eine Switch-to-Switch-Verbindung, die ihr Verhalten aushandeln darf, mit 10-Mbit/s-Halbduplex betrieben werden. Eine nicht funktionierende Verbindung ist in der Regel leichter zu erkennen als eine Verbindung, die betriebsbereit ist, aber nicht mit der erwarteten Geschwindigkeit oder dem erwarteten Modus funktioniert.

Eine der häufigsten Ursachen für Leistungsprobleme bei 10/100-Mbit-Ethernet-Verbindungen ist, wenn ein Port der Verbindung mit Halbduplex arbeitet, während der andere Port mit Vollduplex arbeitet. Dies kommt gelegentlich vor, wenn ein oder beide Ports einer Verbindung zurückgesetzt werden und die automatische Aushandlung nicht dazu führt, dass beide Verbindungspartner die gleiche Konfiguration haben. Es passiert auch, wenn Benutzer eine Seite eines Links neu konfigurieren und die andere Seite vergessen. Viele leistungsbezogene Support-Anfragen werden vermieden, wenn Sie eine Richtlinie erstellen, die vorschreibt, dass Ports für alle Nicht-Übergangsgeräte für ihr erforderliches Verhalten konfiguriert werden müssen, und die Richtlinie mit angemessenen Änderungskontrollmaßnahmen durchsetzen.

Fehlerbehebung für automatische Ethernet-Aushandlung zwischen Netzwerkinfrastrukturgeräten

Verfahren und/oder Szenarien

Szenario 1. Cat 5K mit Fast Ethernet

Tabelle 22-2: Verbindungsprobleme bei der automatischen Aushandlung

Mögliches Problem	Lösung
Wurde das aktuelle Verhalten der Verbindung automatisch ausgehandelt?	1. Verwenden Sie **den Befehl show port mod_num/port**_numum, um das aktuelle Verhalten der Verbindung zu ermitteln. Wenn beide Verbindungspartner (Schnittstellen an beiden Enden des Links) in ihren Feldern für den Duplex- und Geschwindigkeitsstatus ein "a-" Präfix angeben, war die automatische Aushandlung wahrscheinlich erfolgreich.
Automatische Aushandlung wird nicht unterstützt.	2. Geben Sie **den Befehl show port abilities mod_num/port**_numein ein, um zu überprüfen, ob Ihre Module Auto-Negotiation unterstützen.
auto-negotiation funktioniert nicht mit Catalyst Switches.	3. Verwenden Sie **den Befehl mod_num/port_num** autocommand auf einem Catalyst, um die automatische Aushandlung zu konfigurieren. 4. Verwenden Sie andere Ports oder Module. 5. Versuchen Sie, die Ports zurückzusetzen. 6. Verwenden Sie andere Patchkabel. 7. Schalten Sie die Geräte aus und wieder ein.
Auto-Negotiation funktioniert auf Cisco Routern nicht.	8. Geben Sie den richtigen Cisco IOS-Befehl ein, um die automatische Aushandlung zu aktivieren (falls verfügbar) 9. Probieren Sie andere Schnittstellen aus. 10. Versuchen Sie, die Schnittstellen zurückzusetzen. 11. Verwenden Sie andere Patchkabel. 12. Schalten Sie die Geräte aus und

wieder ein.

Beispiel für die automatische Aushandlung über Ethernet mit 10/100 MB und Fehlerbehebung

In diesem Abschnitt wird das Verhalten eines 10/100-Mbit-Ethernet-Ports untersucht, der Auto-Negotiation unterstützt. Außerdem wird gezeigt, wie Änderungen am Standardverhalten vorgenommen werden und wie dieses auf das Standardverhalten zurückgesetzt wird.

Auszuführende Aufgaben

Überprüfen Sie die Funktionen der Ports.

Konfigurieren Sie die automatische Aushandlung für Port 1/1 auf beiden Switches.

Bestimmen Sie, ob Geschwindigkeits- und Duplexmodus auf automatische Aushandlung eingestellt sind.

Ändern Sie die Geschwindigkeit von Port 1/1 in Switch A auf 10 MB.

Verständnis der Bedeutung des Präfix "a-" in den Duplex- und Geschwindigkeitsstatusfeldern

Sehen Sie den Duplexstatus von Port 1/1 auf Switch B an.

Sie müssen den Duplex-Diskrepanz-Fehler verstehen.

Sie müssen die Spanning Tree-Fehlermeldungen verstehen.

Ändern Sie den Duplexmodus auf Port 1/1 auf Switch A zu Halbduplex.

Stellen Sie den Duplexmodus und die Geschwindigkeit von Port 1/1 auf Switch B ein.

Stellen Sie auf beiden Switches den standardmäßigen Duplexmodus und die Geschwindigkeit auf Ports 1/1 ein.

Sehen Sie sich die Änderungen des Portstatus auf beiden Switches an.

Schritt für Schritt

Gehen Sie folgendermaßen vor:

Der Befehl **show port abilities 1/1** zeigt die Funktionen eines Ethernet 10/100BaseTX 1/1-Ports an Switch A an.

Geben Sie diesen Befehl für beide Ports ein, für die Sie eine Fehlerbehebung durchführen möchten. Beide Ports müssen die gezeigten Geschwindigkeits- und Duplexfunktionen unterstützen, wenn Auto-Negotiation verwendet werden soll.

```
Switch-A> (enable) show port capabilities 1/1
Model WS-X5530
Port 1/1
Type 10/100BaseTX
Speed auto,10,100
Duplex half, full
```

Auto-Negotiation wird für Geschwindigkeit und Duplexmodus an Port 1/1 beider Switches konfiguriert, wenn Sie den **Auto-**Befehl **set port speed 1/1** eingeben (auto ist die Standardeinstellung für Ports, die Auto-Negotiation unterstützen).

```
Switch-A> (enable) set port speed 1/1 auto
Port(s) 1/1 speed set to auto detect.
Switch-A (enable)
```

Hinweis: Mit dem **Befehl set port speed {mod_num/port_num} auto** wird der Duplexmodus ebenfalls auf auto gesetzt. Es gibt keinen Befehl set port duplex {mod_num/port_num} auto.

Der Befehl show port 1/1 zeigt den Status von ports 1/1 auf den Switches A und B an.

```
Switch-A> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- -----
 1/1               connected  1          normal a-full a-100 10/100BaseTX

Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- -----
 1/1               connected  1          normal a-full a-100 10/100BaseTX
```

Beachten Sie, dass der Großteil der normalen Ausgabe des Befehls **show port {mod_num/port_num}** weggelassen wurde.

Die Präfixe "a-" für "full" und "100" zeigen an, dass dieser Port nicht für einen bestimmten Duplexmodus oder eine bestimmte Geschwindigkeit fest codiert (konfiguriert) wurde. Daher kann es seinen Duplexmodus und seine Geschwindigkeit automatisch aushandeln, wenn das Gerät, mit dem es verbunden ist (der Link-Partner), auch seinen Duplexmodus und seine Geschwindigkeit automatisch aushandeln kann. Beachten Sie auch, dass der Status an beiden Ports "verbunden" ist, d. h. dass ein Verbindungsimpuls vom anderen Port erkannt wurde. Der Status kann auch dann "verbunden" sein, wenn der Duplex falsch ausgehandelt oder falsch konfiguriert wurde.

Um zu demonstrieren, was passiert, wenn ein Verbindungspartner automatisch aushandelt und der andere Verbindungspartner dies nicht tut, wird die Geschwindigkeit an Port 1/1 in Switch A mit dem Befehl **set port speed 1/1 10** auf 10 MB festgelegt.

```
Switch-A> (enable) set port speed 1/1 10
Port(s) 1/1 speed set to 10Mbps.
Switch-A> (enable)
```

Hinweis: Wenn Sie die Geschwindigkeit an einem Port fest codieren, werden alle Auto-Negotiation-Funktionen am Port für Geschwindigkeit und Duplex deaktiviert.

Wenn ein Port für eine Geschwindigkeit konfiguriert wurde, wird der Duplexmodus automatisch für den zuvor ausgehandelten Modus konfiguriert. In diesem Fall Vollduplex. Wenn Sie den Befehl **set port speed 1/1/10** eingeben, wird der Duplexmodus auf Port 1/1 so konfiguriert, als ob der Befehl **set port duplex 1/1 full** ebenfalls eingegeben wurde. Dies wird als Nächstes erläutert.

Verständnis der Bedeutung des Präfix "a-" in den Feldern Duplex und Geschwindigkeit

Das Fehlen des Präfix "a-" in den Statusfeldern der Ausgabe des Befehls **show port 1/1** an Switch A zeigt, dass der Duplexmodus jetzt für "full" (voll) und die Geschwindigkeit jetzt für "10" konfiguriert ist.

```
Switch-A> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal  full  10    10/100BaseTX
```

Der Befehl **show port 1/1** auf Switch B gibt an, dass der Port jetzt mit Halbduplex und 10 MB betrieben wird.

```
Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal a-half a-10  10/100BaseTX
```

Dieser Schritt zeigt, dass ein Link-Partner die Geschwindigkeit erkennen kann, mit der der andere Link-Partner betrieben wird, obwohl der andere Link-Partner nicht für die automatische Aushandlung konfiguriert ist. Die Erfassung der Art des eingehenden elektrischen Signals, um festzustellen, ob es sich um 10 MB oder 100 MB handelt, führt zu diesem Ergebnis. So hat Switch B festgelegt, dass Port 1/1 mit 10 MB betrieben werden muss.

Es ist nicht möglich, den korrekten Duplexmodus so zu erkennen, wie die korrekte Geschwindigkeit erkannt werden kann. Wenn in diesem Fall der 1/1-Port von Switch B für die automatische Aushandlung konfiguriert ist und der Port von Switch A nicht konfiguriert ist, wurde der 1/1-Port von Switch B gezwungen, den Standardduplex-Modus auszuwählen. Auf Catalyst Ethernet-Ports ist der Standardmodus Auto-Negotiation. Schlägt die Auto-

Negotiation fehl, wird Halbduplex verwendet.

Dieses Beispiel zeigt auch, dass ein Link auch bei nicht übereinstimmenden Duplexmodi erfolgreich verbunden werden kann. Port 1/1 an Switch A ist für Vollduplex konfiguriert, während Port 1/1 an Switch B standardmäßig auf Halbduplex festgelegt ist. Um dies zu vermeiden, sollten Sie immer beide Link-Partner konfigurieren.

Das Präfix "a-" in den Zustandsfeldern Duplex und Geschwindigkeit bedeutet nicht immer, dass das aktuelle Verhalten ausgehandelt wurde. Manchmal bedeutet dies nur, dass der Port nicht für einen Geschwindigkeits- oder Duplexmodus konfiguriert wurde. Die vorherige Ausgabe von Switch B zeigt den Duplex als "a-half" (halb) und die Geschwindigkeit als "a-10" an. Dies bedeutet, dass der Port im Halbduplex-Modus mit 10 MB betrieben wird. In diesem Beispiel ist der Verbindungspartner an diesem Port (Port 1/1 an Switch A) für "full" (voll) und "10Mb" (10 MB) konfiguriert. Das aktuelle Verhalten von Port 1/1 auf Switch B konnte nicht automatisch ausgehandelt werden. Dies beweist, dass das Präfix "a-" nur die Bereitschaft anzeigt, eine automatische Aushandlung auszuführen, jedoch nicht, dass die automatische Aushandlung tatsächlich stattgefunden hat.

Verstehen der Fehlermeldung "Duplex Mismatch" (Duplex-Abweichung).

Diese Meldung über eine Duplexmodus-Diskrepanz wird an Switch A angezeigt, nachdem die Geschwindigkeit an Port 1/1 auf 10 MB geändert wurde. Die Diskrepanz wurde durch den 1/1-Port von Switch B verursacht, der standardmäßig auf Halbduplex festgelegt ist, da er erkannte, dass der Link-Partner keine automatische Aushandlung mehr durchführen konnte.

```
%CDP-4-DUPLEXMISMATCH:Full/half-duplex mismatch detected o1
```

Beachten Sie, dass diese Nachricht mit dem Cisco Discovery Protocol (CDP) erstellt wurde, nicht mit dem 802.3 Auto-Negotiation-Protokoll. CDP kann Probleme melden, die es erkennt, behebt diese jedoch in der Regel nicht automatisch. Eine Duplexungleichheit kann zu einer Fehlermeldung führen. Ein weiteres Indiz für eine Duplexungleichheit sind die schnell zunehmenden FCS- und Ausrichtungsfehler auf der Halbduplex-Seite und "Runts" auf dem Vollduplex-Port (wie in einem **SH-Port {mod_num/port_num}** zu sehen).

Kenntnis der Spanning Tree-Meldungen

Zusätzlich zur Fehlermeldung "Duplex Mismatch" (Duplexdiskrepanz) werden diese Spanning Tree-Meldungen angezeigt, wenn Sie die Geschwindigkeit für einen Link ändern. Eine Erläuterung von Spanning Tree geht über den Rahmen dieses Dokuments hinaus. Weitere Informationen zu Spanning Tree finden Sie im Kapitel zu Spanning Tree.

```
%PAGP-5-PORTFROMSTP:Port 1/1 left bridge port 1/1
%PAGP-5-PORTTOSTP:Port 1/1 joined bridge port 1/1
```

Um zu demonstrieren, was passiert, wenn der Duplexmodus konfiguriert wurde, wird der Modus an Port 1/1 in Switch A mit dem Befehl **set port duplex 1/1 half** auf die Hälfte eingestellt.

```
Switch-A> (enable) set port duplex 1/1 half
Port(s) 1/1 set to half-duplex.
Switch-A> (enable)
```

Der Befehl **show port 1/1** zeigt die Änderung des Duplex-Modus an diesem Port an.

```
Switch-A> (enable) sh port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal half   10    10/100BaseTX
```

An dieser Stelle werden die Ports 1/1 auf beiden Switches im Halbduplex-Modus betrieben. Port 1/1 auf Switch B ist weiterhin für die automatische Aushandlung konfiguriert, wie in dieser Ausgabe des Befehls **show port 1/1** gezeigt.

```
Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal a-half a-10  10/100BaseTX
```

Dieser Schritt zeigt, wie der Duplexmodus an Port 1/1 in Switch B auf die Hälfte konfiguriert wird. Dies entspricht der empfohlenen Richtlinie zur Konfiguration beider Verbindungspartner auf die gleiche Weise.

Um die Richtlinie zur Konfiguration beider Verbindungspartner für dasselbe Verhalten zu implementieren, wird in diesem Schritt der Duplexmodus auf die Hälfte und die Geschwindigkeit auf 10 an Port 1/1 in Switch B gesetzt.

Die folgende Ausgabe wird ausgegeben, wenn Sie den Befehl **set port duplex 1/1 half** auf Switch B eingeben:

```
Switch-B> (enable) set port duplex 1/1 half
Port 1/1 is in auto-sensing mode.
Switch-B> (enable)
```

Der Befehl **set port duplex 1/1 half** ist fehlgeschlagen, da dieser Befehl ungültig ist, wenn die automatische Aushandlung aktiviert ist. Das bedeutet auch, dass die automatische Aushandlung durch diesen Befehl nicht deaktiviert wird. Die automatische Aushandlung kann nur mit der **festgelegten Portgeschwindigkeit {mod_num/port_num {10} deaktiviert werden. | 100} }** Befehl.

Die folgende Ausgabe wird ausgegeben, wenn Sie den Befehl **set port speed 1/1 10** auf Switch B eingeben:

```
Switch-B> (enable) set port speed 1/1 10
Port(s) 1/1 speed set to 10Mbps.
Switch-B> (enable)
```

Jetzt funktioniert der Befehl **set port duplex 1/1 half** auf Switch B:

```
Switch-A> (enable) set port duplex 1/1 half
Port(s) 1/1 set to half-duplex.
Switch-A> (enable)
```

Der Befehl **show port 1/1** auf Switch B zeigt an, dass die Ports jetzt für Halbduplex und 10 MB konfiguriert sind.

```
Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal half   10    10/100BaseTX
```

> **Hinweis**: Der **eingestellte Port-Duplex {mod_num/port_num {half} | full }}** Befehl hängt von der **eingestellten Portgeschwindigkeit ab {mod_num/port_num {10 | 100 }}** Befehl. Das bedeutet, Sie müssen die Geschwindigkeit festlegen, bevor Sie den Duplexmodus einstellen können.

Konfigurieren Sie die Ports 1/1 auf beiden Switches so, dass sie mit dem Befehl **set port speed 1/1 aut** automatisch ausgehandelt werden.

```
Switch-A> (enable) set port speed 1/1 auto
Port(s) 1/1 speed set to auto detect.
Switch-A> (enable)
```

> **Hinweis:** Wenn ein Duplexmodus eines Ports für einen anderen als den automatischen Modus konfiguriert wurde, können Sie den Port nur für die automatische Erkennung des Duplexmodus konfigurieren, indem Sie den **Befehl set port speed {mod_num/port_num} auto** eingeben. Es gibt keinen Befehl set port duplex {mod_num/port_num} auto. Mit anderen Worten: Wenn Sie den **Auto-**Befehl **set port speed {mod_num/port_num} ausführen,** werden sowohl die Port-Geschwindigkeitserkennung als auch die Duplexmoduserkennung auf auto zurückgesetzt.

Überprüfen Sie den Status der Ports 1/1 auf beiden Switches mit dem Befehl **show port 1/1**.

```
Switch-A> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal a-full a-100 10/100BaseTX
Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
```

```
1/1              connected  1          normal a-full a-100 10/100BaseTX
```

Für beide Ports wurde die automatische Aushandlung als Standardverhalten eingestellt. Beide Ports haben Vollduplex und 100 MB vereinbart.

Bevor Sie sich an den technischen Support von Cisco Systems wenden

Bevor Sie die Website des technischen Supports von Cisco Systems aufrufen, stellen Sie sicher, dass Sie diesen Artikel durchgelesen und die empfohlenen Maßnahmen für Ihre Systemprobleme durchgeführt haben. Dokumentieren Sie außerdem die Ergebnisse, damit Cisco Sie besser unterstützen kann:

Erfassen Sie die Ausgabe **von show** version von allen betroffenen Geräten.

Erfassen Sie die Ausgabe von **show port mod_num/port_num** von allen betroffenen Ports.

Erfassen Sie die Ausgabe von **show port mod_num/port_num**-Funktionen von allen betroffenen Ports.

Konfigurieren der EtherChannel Switch-to-Switch-Verbindungen auf Catalyst 4000/5000/6000-Switches

EtherChannel ermöglicht das Zusammenfassen mehrerer physischer Fast-Ethernet- oder Gigabit-Ethernet-Verbindungen zu einem logischen Kanal. Auf diese Weise kann der Datenverkehr zwischen den Links Lastenausgleich im Channel sowie Redundanz für den Fall erhalten, dass eine oder mehrere Links im Channel ausfallen. EtherChannel kann zur Verbindung von LAN-Switches, Routern, Servern und Clients über Unshielded Twisted-Pair (UTP)-Kabel oder Single- und Multimode-Glasfaser verwendet werden.

EtherChannel ist eine einfache Methode, Bandbreite zwischen kritischen Netzwerkgeräten zu aggregieren. Auf dem Catalyst 5000 kann ein Kanal aus zwei Ports erstellt werden, die ihn zu einer 200-Mbit/s-Verbindung (400-Mbit/s-Vollduplex) machen, oder aus vier Ports, die ihn zu einer 400-Mbit/s-Verbindung (800-Mbit/s-Vollduplex) machen. Einige Karten und Plattformen unterstützen auch Gigabit-EtherChannel und können zwei bis acht Ports in einem EtherChannel verwenden. Das Konzept ist unabhängig von Geschwindigkeit und Anzahl der Verbindungen identisch. Normalerweise betrachtet das Spanning Tree Protocol (STP) diese redundanten Verbindungen zwischen zwei Geräten als Schleifen und setzt die redundanten Verbindungen in den Blockierungsmodus. Dadurch werden diese Links inaktiv (die nur Backup-Funktionen bieten, wenn die Hauptverbindung ausfällt). Wenn Sie Cisco IOS 3.1.1 oder höher verwenden, behandelt Spanning Tree den Kanal als eine große Verbindung, sodass alle Ports im Kanal gleichzeitig aktiv sein können.

In diesem Abschnitt werden die Schritte zum Konfigurieren des EtherChannels zwischen zwei Catalyst 5000-Switches erläutert. Außerdem werden die Ergebnisse der Befehle bei ihrer Ausführung angezeigt. Die Catalyst Switches der Serien 4000 und 6000 hätten in den hier vorgestellten Szenarien verwendet werden können, um die gleichen Ergebnisse zu erzielen. Bei Catalyst 2900XL und 1900/2820 ist die Befehlssyntax unterschiedlich, aber die EtherChannel-Konzepte sind identisch.

Der EtherChannel kann manuell konfiguriert werden, wenn Sie die entsprechenden Befehle eingeben, oder er kann automatisch konfiguriert werden, wenn der Switch den Kanal mit der anderen Seite über das Port Aggregation Protocol (PAgP) aushandelt. Es wird empfohlen, den erwünschten PAgP-Modus zu verwenden, um den EtherChannel so weit wie möglich zu konfigurieren, da die manuelle Konfiguration des EtherChannels einige Komplikationen verursachen kann. Dieses Dokument enthält Beispiele für die manuelle Konfiguration des EtherChannels und für die Konfiguration des EtherChannels mit PAgP. Ebenfalls enthalten ist die Fehlerbehebung bei EtherChannel und die Verwendung von Trunking mit EtherChannel. In diesem Dokument beziehen sich die Begriffe "EtherChannel", "Fast EtherChannel", "Gigabit EtherChannel" oder "Channel" auf "EtherChannel".

Inhalt

Diese Abbildung zeigt diese Testumgebung. Die Konfiguration der Switches wurde mit dem Befehl **clear config all** gelöscht. Anschließend wurde die Eingabeaufforderung mit dem **Systemnamen set** geändert. Dem Switch wurden zu Verwaltungszwecken eine IP-Adresse und eine IP-Maske zugewiesen. Die Werte sind für SwitchA **in sc0 172.16.84.6 255.255.0** und **in sc0 172.16.84.17 255.255.1 festgelegt. 255.0< /strong>für SwitchB. Ein Standard-Gateway wurde beiden Switches mit dem festgelegten IP-Routenstandard 172.16.84.1 zugewiesen.**

Die Switch-Konfigurationen wurden gelöscht, sodass sie mit den Standardbedingungen beginnen. Den Switches wurden Namen zugewiesen, um sie über die Eingabeaufforderung in der Befehlszeile zu identifizieren. Die IP-Adressen wurden so zugewiesen, dass Sie Pings zwischen den Switches senden konnten, um sie zu testen. Das Standardgateway wurde nicht verwendet.Viele der Befehle zeigen mehr Ausgabe an, als erforderlich ist. Fremdausgaben werden aus diesem Dokument gelöscht.Aufgaben zur manuellen Konfiguration des EtherChannelsDies ist eine Zusammenfassung der Anweisungen zum manuellen Konfigurieren des EtherChannels:

- Zeigen Sie die in diesem Dokument verwendete Cisco IOS-Version und die verwendeten Module an.

[Stellen Sie sicher, dass der EtherChannel auf den Ports unterstützt wird.]

[Überprüfen Sie, ob die Ports angeschlossen und betriebsbereit sind.]

[Stellen Sie sicher, dass die zu gruppierenden Ports die gleichen Einstellungen aufweisen.]

[Identifizieren gültiger Portgruppen]

[Erstellen Sie den Kanal.]

Schritt für SchrittSo konfigurieren Sie den EtherChannel manuell.

Der Befehl show version zeigt die Softwareversion des Switches an. Der Befehl show module listet die im Switch installierten Module auf.

```
Switch-A show version
WS-C5505 Software, Version McpSW: 4.5(1) NmpSW: 4.5(1)
Copyright (c) 1995-1999 by Cisco Systems
?

Switch-A show module
Mod Module-Name          Ports Module-Type            Model    Serial-Num Status
--- -------------------- ----- ---------------------- --------- --------- -------
1                        0     Supervisor III         WS-X5530  006841805 ok
2                        24    10/100BaseTX Ethernet WS-X5225R 012785227 ok
?
```

Überprüfen Sie, ob EtherChannel auf den Ports unterstützt wird, und zeigen Sie die Portfunktionen in Version 4.x und höher an. Wenn Cisco IOS älter als 4.x ist, müssen Sie diesen Schritt überspringen. Nicht jedes Fast Ethernet-Modul unterstützt EtherChannel. Bei einigen der ursprünglichen EtherChannel-Module steht "Fast EtherChannel" in der linken unteren Ecke des Moduls (wie im Switch dargestellt). Daraus geht hervor, dass diese Funktion unterstützt wird. Diese Konvention wurde bei späteren Modulen aufgegeben. Die Module in diesem Test verwenden keinen "Fast EtherChannel", unterstützen jedoch die Funktion.

```
Switch-A show port capabilities
Model                     WS-X5225R
Port                      2/1
Type                      10/100BaseTX
Speed                     auto,10,100
Duplex                    half,full
Trunk encap type          802.1Q,ISL
Trunk mode                on,off,desirable,auto,nonegotiate
```

```
Channel                  2/1-2,2/1-4
Broadcast suppression    percentage(0-100)
Flow control             receive-(off,on),send-(off,on)
Security                 yes
Membership               static,dynamic
Fast start               yes
Rewrite                  yes
Switch-B show port capabilities
Model                    WS-X5234
Port                     2/1
Type                     10/100BaseTX
Speed                    auto,10,100
Duplex                   half,full
Trunk encap type         802.1Q,ISL
Trunk mode               on,off,desirable,auto,nonegotiate
Channel                  2/1-2,2/1-4
Broadcast suppression    percentage(0-100)
Flow control             receive-(off,on),send-(off,on)
Security                 yes
Membership               static,dynamic
Fast start               yes
Rewrite                  no
```

Ein Port, der keinen EtherChannel unterstützt, sieht wie folgt aus:

```
Switch show port capabilities
Model                    WS-X5213A
Port                     2/1
Type                     10/100BaseTX
Speed                    10,100,auto
Duplex                   half,full
Trunk encap type         ISL
Trunk mode               on,off,desirable,auto,nonegotiate
Channel                  no
Broadcast suppression    pps(0-150000)
Flow control             no
Security                 yes
Membership               static,dynamic
Fast start               yes
```

Überprüfen Sie, ob die Ports angeschlossen und betriebsbereit sind. Bevor Sie die Kabel anschließen, ist dies der Portstatus.

```
Switch-A show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
```

```
 2/1                      notconnect 1          normal   auto  auto 10/100BaseTX
 2/2                      notconnect 1          normal   auto  auto 10/100BaseTX
 2/3                      notconnect 1          normal   auto  auto 10/100BaseTX
 2/4                      notconnect 1          normal   auto  auto 10/100BaseTX
```

Nachdem Sie die Kabel zwischen den beiden Switches angeschlossen haben, wird dieser Status angezeigt.

```
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/4

Switch-A show port
Port  Name                 Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                      connected  1          normal a-full a-100 10/100BaseTX
 2/2                      connected  1          normal a-full a-100 10/100BaseTX
 2/3                      connected  1          normal a-full a-100 10/100BaseTX
 2/4                      connected  1          normal a-full a-100 10/100BaseTX
Switch-B show port
Port  Name                 Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                      connected  1          normal a-full a-100 10/100BaseTX
 2/2                      connected  1          normal a-full a-100 10/100BaseTX
 2/3                      connected  1          normal a-full a-100 10/100BaseTX
 2/4                      connected  1          normal a-full a-100 10/100BaseTX
```

Da die Switch-Konfigurationen vor dem Start dieses Tests gelöscht wurden, befinden sich die Ports im Standardzustand. Sie sind alle in vlan1, und ihre Geschwindigkeit und Duplex sind auf Auto eingestellt. Nach dem Anschluss der Kabel handeln sie eine Geschwindigkeit von 100Mbps und Vollduplex aus. Der Status ist verbunden, sodass Sie den anderen Switch pingen können.

```
Switch-A ping 172.16.84.17
172.16.84.17 is alive
```

In Ihrem Netzwerk können Sie die Geschwindigkeiten manuell auf 100 Mbit/s und Vollduplex einstellen, anstatt sich auf die automatische Aushandlung zu verlassen, da Sie wahrscheinlich möchten, dass Ihre Ports immer mit der schnellsten Geschwindigkeit laufen. Eine Erörterung der automatischen Aushandlung finden Sie im Abschnitt Problembehandlung bei der automatischen Aushandlung mit Ethernet (10/100Mb Halb/Halb/Vollduplex).

Stellen Sie sicher, dass die zu gruppierenden Ports die gleichen Einstellungen aufweisen. Dies ist ein wichtiger Punkt, der im Abschnitt Fehlerbehebung ausführlicher behandelt wird. Wenn der Befehl zum Einrichten des EtherChannels nicht funktioniert, liegt dies in der Regel

daran, dass die am Channel beteiligten Ports unterschiedliche Konfigurationen haben. Dazu gehören die Ports auf der anderen Seite des Links sowie die lokalen Ports. In diesem Fall befinden sich die Ports unter ihren Standardbedingungen, da die Switch-Konfigurationen vor dem Start dieses Tests gelöscht wurden. Sie sind alle in vlan1 enthalten; ihre Geschwindigkeit und ihr Duplex sind auf auto festgelegt, und alle Spanning Tree-Parameter für jeden Port sind identisch. Sie haben an der Ausgabe gesehen, dass die Ports nach dem Anschließen der Kabel eine Geschwindigkeit von 100 Mbit/s und eine Vollduplex-Übertragung aushandeln. Da Spanning Tree für jedes VLAN ausgeführt wird, ist es einfacher, den Kanal zu konfigurieren und auf Fehlermeldungen zu reagieren, als zu versuchen, jedes Spanning Tree-Feld auf seine Konsistenz für jeden Port und jedes VLAN im Kanal zu überprüfen.

Identifizieren Sie gültige Portgruppen. Auf dem Catalyst 5000 können nur bestimmte Ports zu einem Kanal zusammengefasst werden. Diese einschränkenden Abhängigkeiten gelten nicht für alle Plattformen. Die Ports in einem Kanal auf einem Catalyst 5000 müssen zusammenhängend sein. Beachten Sie, dass Portfunktionen für Port 2/1 die folgenden Kombinationen ermöglichen:

```
Switch-A show port capabilities
Model                     WS-X5225R
Port                      2/1
Channel                   2/1-2,2/1-4
```

Beachten Sie, dass dieser Port Teil einer Zweiergruppe (2/1-2) oder Teil einer Vierergruppe (2/1-4) sein kann. Das Modul verfügt über einen so genannten Ethernet Bundling Controller (EBC), der diese Konfigurationsbeschränkungen verursacht. Schauen Sie sich einen anderen Hafen an.

```
Switch-A show port capabilities 2/3
Model                     WS-X5225R
Port                      2/3
Channel                   2/3-4,2/1-4
```

Dieser Port kann in eine Gruppe mit zwei Ports (2/3-4) oder in eine Gruppe mit vier Ports (2/1-4) gruppiert werden.

Hinweis: Je nach Hardware können zusätzliche Einschränkungen bestehen. Bei bestimmten Modulen (WS-X5201 und WS-X5203) können Sie keinen EtherChannel mit den letzten beiden Ports in einer "Portgruppe" bilden, es sei denn, die ersten beiden Ports in der Gruppe bilden bereits einen EtherChannel. Eine "Portgruppe" ist eine Gruppe von Ports, die einen EtherChannel bilden dürfen (in diesem Beispiel ist 2/1-4 eine Portgruppe). Wenn Sie beispielsweise separate EtherChannels mit nur zwei Ports in einem Channel erstellen, können Sie die Ports 2/3-4 erst einem Channel zuweisen, wenn Sie die Ports 2/1-2 für einen Channel konfiguriert haben. Dies gilt für die Module, für die diese Einschränkung gilt! Ebenso müssen Sie die Ports 2/5-6 konfigurieren, bevor Sie die Ports 2/6-7 konfigurieren. Diese Einschränkung gilt nicht für die in diesem Dokument verwendeten Module (WS-X5225R, WS-X5234).

Da Sie eine Gruppe mit vier Ports (2/1-4) konfigurieren, gehört dies zu der genehmigten Gruppe. Sie können den Ports 2/3-6 keine Gruppe mit vier Ports zuweisen. Hierbei handelt

es sich um eine Gruppe zusammenhängender Ports, die jedoch nicht an der genehmigten Grenze beginnen, wie der Befehl how port Capabilities zeigt (gültige Gruppen wären die Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24).

Erstellen Sie den Kanal. Um den Kanal zu erstellen, verwenden Sie den Befehlssatz-Port-Channel <mod/port on für jeden Switch. Es wird empfohlen, die Ports auf der einen Seite des Kanals oder auf der anderen Seite mit dem Befehl port disable auszuschalten, bevor Sie EtherChannel manuell aktivieren. Dadurch werden mögliche Probleme mit Spanning Tree im Rahmen des Konfigurationsprozesses vermieden. Spanning Tree kann einige Ports deaktivieren (mit dem Portstatus "errdisable"), wenn eine Seite als Kanal konfiguriert ist, während die andere Seite als Kanal konfiguriert werden kann. Aufgrund dieser Möglichkeit ist es viel einfacher, EtherChannels mit PAgP zu erstellen, was später in diesem Dokument erläutert wird. Um dies zu vermeiden, deaktivieren Sie bei manueller Konfiguration des EtherChannels die Ports auf SwitchA, konfigurieren Sie den Kanal auf SwitchA, konfigurieren Sie den Kanal auf SwitchB, und aktivieren Sie dann die Ports auf SwitchA erneut.

Überprüfen Sie zunächst, ob die Kanalisierung *deaktiviert ist*.

```
Switch-A (enable) show port channel
No ports channelling
Switch-B (enable) show port channel
No ports channelling
```

Deaktivieren Sie nun die Ports auf SwitchA, bis beide Switches für den EtherChannel konfiguriert wurden, sodass Spanning Tree keine Fehler generiert, und fahren Sie die Ports herunter.

```
Switch-A (enable) set port disable 2/1-4
Ports 2/1-4 disabled.
[output from SwitchA upon disabling ports]
1999 Dec 15 00:06:40 %PAGP-5-PORTFROMSTP:Port 2/1 left bridg1
1999 Dec 15 00:06:40 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 15 00:06:40 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 15 00:06:40 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
```

Schalten Sie den Kanalmodus für SwitchA ein.

```
Switch-A (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.
```

Überprüfen Sie den Status des Kanals. Beachten Sie, dass der Channel-Modus *auf* eingestellt wurde, der Status der Ports jedoch deaktiviert ist (weil Sie zuvor deaktiviert haben). Der Kanal ist derzeit nicht betriebsbereit, wird jedoch betriebsbereit, wenn die Ports aktiviert sind.

```
Switch-A (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
```

```
                mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  disabled   on        channel
 2/2  disabled   on        channel
 2/3  disabled   on        channel
 2/4  disabled   on        channel
----- ---------- --------- ----------- ------------------------- ----------
```

Da die SwitchA-Ports (vorübergehend) deaktiviert wurden, haben die SwitchB-Ports keine Verbindung mehr. Diese Meldung wird auf der Konsole von SwitchB angezeigt, wenn die Ports von SwitchA deaktiviert wurden.

```
Switch-B (enable)
2000 Jan 13 22:30:03 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
2000 Jan 13 22:30:04 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 13 22:30:04 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 13 22:30:04 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
```

Schalten Sie den Kanal für Switch B ein.

```
Switch-B (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.
```

Überprüfen Sie, ob der Kanalmodus für SwitchB aktiviert ist.

```
Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  notconnect on        channel
 2/2  notconnect on        channel
 2/3  notconnect on        channel
 2/4  notconnect on        channel
----- ---------- --------- ----------- ------------------------- ----------
```

Beachten Sie, dass der Kanalmodus für SwitchB aktiv ist, der Status der Ports jedoch *nicht verbunden ist*. Dies liegt daran, dass die SwitchA-Ports weiterhin deaktiviert sind.

Der letzte Schritt schließlich ist die Aktivierung der Ports auf SwitchA.

```
Switch-A (enable) set port enable 2/1-4
Ports 2/1-4 enabled.
1999 Dec 15 00:08:40 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
1999 Dec 15 00:08:40 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
1999 Dec 15 00:08:40 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
1999 Dec 15 00:08:40 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4
```

Überprüfen der KonfigurationFühren Sie den Befehl show port channel aus, um sicherzustellen, dass der Kanal ordnungsgemäß eingerichtet ist.

```
Switch-A (enable) show port channel
Port   Status      Channel    Channel      Neighbor                  Neighbor
                   mode       status       device                    port
------ ----------- ---------- ------------ ------------------------- ----------
 2/1   connected   on         channel      WS-C5505    066509957(Sw  2/1
 2/2   connected   on         channel      WS-C5505    066509957(Sw  2/2
 2/3   connected   on         channel      WS-C5505    066509957(Sw  2/3
 2/4   connected   on         channel      WS-C5505    066509957(Sw  2/4
------ ----------- ---------- ------------ ------------------------- ----------

Switch-B (enable) show port channel
Port   Status      Channel    Channel      Neighbor                  Neighbor
                   mode       status       device                    port
------ ----------- ---------- ------------ ------------------------- ----------
 2/1   connected   on         channel      WS-C5505    066507453(Sw  2/1
 2/2   connected   on         channel      WS-C5505    066507453(Sw  2/2
 2/3   connected   on         channel      WS-C5505    066507453(Sw  2/3
 2/4   connected   on         channel      WS-C5505    066507453(Sw  2/4
------ ----------- ---------- ------------ ------------------------- ----------
```

Spanning Tree behandelt die Ports wie ein logischer Port in diesem Befehl. Wenn der Port als*2/1-4* aufgeführt ist, behandelt Spanning Tree die Ports 2/1, 2/2, 2/3 und 2/4 *als einen Port*.

```
Switch-A (enable) show spantree
VLAN 1
Spanning tree enabled
Spanning tree type          ieee

Designated Root             00-10-0d-b2-8c-00
Designated Root Priority    32768
Designated Root Cost        8
Designated Root Port        2/1-4
Root Max Age   20 sec    Hello Time 2  sec   Forward Delay 15 sec
```

```
Bridge ID MAC ADDR          00-90-92-b0-84-00

Bridge ID Priority          32768

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


Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-Method

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

 2/1-4    1     forwarding         8        32   disabled       channel
```

EtherChannel kann mit verschiedenen Methoden der Datenverkehrsverteilung über die Ports in einem Channel implementiert werden. Die EtherChannel-Spezifikation legt nicht fest, wie der Datenverkehr auf die Links in einem Kanal verteilt werden muss. Catalyst 5000 verwendet das letzte oder die letzten beiden Bit (abhängig von der Anzahl der Verbindungen im Kanal) der Quell- und Ziel-MAC-Adressen im Frame, um den zu verwendenden Port im Kanal zu bestimmen. Wenn Datenverkehr durch eine normale Verteilung von MAC-Adressen auf der einen oder anderen Seite des Kanals generiert wird, wird an jedem Port des Kanals ein ähnliches Datenverkehrsvolumen angezeigt. Um zu überprüfen, ob der Datenverkehr über alle Ports im Channel geleitet wird, können Sie die Option show mcommand verwenden. Wenn Ihre Ports vor der Konfiguration des EtherChannels aktiv waren, können Sie die Datenverkehrszähler durch den Befehl clear counters auf Null zurücksetzen. Anschließend geben die Datenverkehrswerte an, wie der EtherChannel den Datenverkehr verteilt hat.In dieser Testumgebung haben Sie keine Verteilung in der Praxis erhalten, da es keine Workstations, Server oder Router gibt, die Datenverkehr generieren. Die einzigen Geräte, die Datenverkehr generieren, sind die Switches selbst. Sie haben einige Pings von SwitchA an SwitchB ausgegeben, und Sie können erkennen, dass der Unicast-Datenverkehr den ersten Port im Kanal verwendet. Die Receive-Information in diesem Fall (Rcv-Unicast) zeigt, wie SwitchB den Datenverkehr über den Kanal an SwitchA verteilte. Etwas weiter unten in der Ausgabe zeigt die Transmit-Information (Xmit-Unicast), wie SwitchA den Datenverkehr über den Kanal an SwitchB verteilte. Sie sehen auch, dass ein kleiner Teil des vom Switch generierten Multicast-Datenverkehrs (Dynamic ISL, CDP) über alle vier Ports hinausgeht. Bei den Broadcast-Paketen handelt es sich um ARP-Abfragen (für das Standard-Gateway, das hier nicht vorhanden ist). Wenn Workstations Pakete über den Switch an ein Ziel auf der anderen Seite des Kanals senden, erwarten Sie Datenverkehr, der über jede der vier Verbindungen im Kanal läuft. Sie können die Paketverteilung in Ihrem eigenen Netzwerk mit der show mcommand überwachen.

```
Switch-A (enable) clear counters

This command will reset all MAC and port counters reported in CLI and SNMP.
```

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

MAC and Port counters cleared.

Switch-A (enable) show mac


Port     Rcv-Unicast           Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 2/1                        9                  320                  183
 2/2                        0                   51                    0
 2/3                        0                   47                    0
 2/4                        0                   47                    0
(...)

Port     Xmit-Unicast          Xmit-Multicast       Xmit-Broadcast
-------- -------------------- -------------------- --------------------
 2/1                        8                   47                  184
 2/2                        0                   47                    0
 2/3                        0                   47                    0
 2/4                        0                   47                    0
(...)

Port     Rcv-Octet             Xmit-Octet
-------- -------------------- --------------------
 2/1                    35176                17443
 2/2                     5304                 4851
 2/3                     5048                 4851
 2/4                     5048                 4851
(...)

Last-Time-Cleared
--------------------------
Wed Dec 15 1999, 01:05:33
```

PAgP zum Konfigurieren des EtherChannels verwenden (bevorzugte Methode)

Das Port Aggregation Protocol (PAgP) vereinfacht die automatische Erstellung von EtherChannel-

Verbindungen beim Austausch von Paketen zwischen kanalfähigen Ports. Das Protokoll erfasst die Funktionen von Portgruppen dynamisch und informiert die nahegelegenen Ports.Sobald PAgP die richtig gepaarten kanalfähigen Verbindungen erkennt, werden die Ports in einem Kanal gruppiert. Der Kanal wird dann dem Spanning Tree als einzelner Bridge-Port hinzugefügt. Ein bestimmtes ausgehendes Broadcast- oder Multicast-Paket wird nur an einem Port des Kanals und nicht an jedem Port des Kanals übertragen. Darüber hinaus werden ausgehende Broadcast- und Multicast-Pakete, die an einem Port in einem Channel übertragen werden, an einem anderen Port des Channels von ihrer Rückgabe blockiert.Es gibt vier vom Benutzer konfigurierbare Kanalmodi: "on", "off", "auto" und "desirable". PAgP-Pakete werden nur zwischen Ports im automatischen und erwünschten Modus ausgetauscht. Ports, die im OnOff-Modus konfiguriert wurden, tauschen keine PAgP-Pakete aus. Die empfohlenen Einstellungen für Switches, die Sie erstellen möchten, und für den EtherChannel sollten beide Switches auf den erwünschten Modus eingestellt sein. Dies ist das sicherste Verhalten, wenn auf der einen oder anderen Seite Fehlersituationen auftreten oder zurückgesetzt werden. Der Standardmodus des Kanals ist auto.Sowohl der automatische als auch der gewünschte Modus ermöglichen es Ports, mit verbundenen Ports zu verhandeln, um anhand von Kriterien wie Portgeschwindigkeit, Trunking-Status, natives VLAN usw. zu bestimmen, ob sie einen Kanal bilden können.Ports können einen EtherChannel bilden, wenn sie sich in unterschiedlichen Kanalmodi befinden, sofern diese miteinander kompatibel sind:

Ein Port im indizierbaren Modus kann erfolgreich einen EtherChannel mit einem anderen Port bilden, der indesirableorautomode ist.

Ein Port-Inautomode kann einen EtherChannel mit einem anderen Port-Indexierungsmodus bilden.

Ein Port-Inautomode kann keinen EtherChannel mit einem anderen Port bilden, der ebenfalls Inautomode ist, da keiner der Ports die Aushandlung initiiert.

Ein Port-Inonmode kann nur mit einem Port-Inonmode einen Kanal bilden, da Ports Inonmode PAgP-Pakete nicht austauschen.

Ein Port-Inoffmode bildet keinen Kanal mit einem Port.

Wenn Sie EtherChannel verwenden und eine Meldung wie "SPANTREE-2: Channel misconfig - x/x-x will be disabled" (SPANTREE-2: Kanalfehlkonfiguration - x/x-x wird deaktiviert) oder ein ähnliches Syslog angezeigt wird, weist dies auf eine Diskrepanz zwischen den EtherChannel-Modi an den verbundenen Ports hin. Sie empfehlen, die Konfiguration zu korrigieren und die Ports mit dem Befehl set port enableerneut zuaktivieren. Zu den gültigen EtherChannel-Konfigurationen gehören:Tabelle 2-5: Gültige EtherChannel-Konfigurationen

Port-Channel-Modus	Gültige benachbarte Port-Channel-Modus(e)

desirable (gewünscht)	wünschenswert oder automatisch
auto (Standard)	Wünschenswert oder Auto[1]
on	on
off	off

[1]Wenn sich sowohl der lokale als auch der benachbarte Port im Automatikmodus befinden, wird kein EtherChannel-Bündel gebildet.Im Folgenden finden Sie eine Zusammenfassung aller möglichen Szenarien für den Channeling-Modus. Einige dieser Kombinationen können dazu führen, dass Spanning Tree die Ports auf der Channeling-Seite in den deaktivierbaren Zustand versetzt (d. h. heruntergefahren).Tabelle 22-6: Szenarien für den Kanalisierungsmodus

Switch-A Channel-Modus	Switch-B Channel-Modus	Channel-Status
On	On	Kanal
On	Aus	Kein Kanal (errdisable)
On	Auto (automatisch)	Kein Kanal (errdisable)
On	Desirable (gewünscht)	Kein Kanal (errdisable)
Aus	On	Kein Kanal (errdisable)
Aus	Aus	Kein Kanal
Aus	Auto (automatisch)	Kein Kanal
Aus	Desirable (gewünscht)	Kein Kanal
Auto (automatisch)	On	Kein Kanal (errdisable)
Auto (automatisch)	Aus	Kein Kanal
Auto (automatisch)	Auto (automatisch)	Kein Kanal
Auto (automatisch)	Desirable (gewünscht)	Kanal
Desirable (gewünscht)	On	Kein Kanal (errdisable)
Desirable (gewünscht)	Aus	Kein Kanal
Desirable (gewünscht)	Auto (automatisch)	Kanal
Desirable (gewünscht)	Desirable (gewünscht)	Kanal

Mit diesem Befehl an SwitchA und SwitchB haben Sie den Kanal aus dem vorherigen Beispiel ausgeschaltet.

```
Switch-A (enable) set port channel 2/1-4 auto

Port(s) 2/1-4 channel mode set to auto.
```

Der Standardkanalmodus für einen Port, der Channels empfangen kann, ist auto. Geben Sie den folgenden Befehl ein, um dies zu überprüfen:

```
Switch-A (enable) show port channel 2/1

Port  Status     Channel   Channel     Neighbor                  Neighbor
```

```
                mode      status      device                    port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  connected  auto      not channel
```

Der vorherige Befehl zeigt außerdem an, dass die Ports derzeit keinen Channel-Zugang haben. Eine weitere Möglichkeit, den Kanalstatus zu überprüfen, ist diese.

```
Switch-A (enable) show port channel

No ports channelling

Switch-B (enable) show port channel

No ports channelling
```

Es ist wirklich sehr einfach, den Kanal mit PAgP zu verwenden. An diesem Punkt werden beide Switches auf den Auto-Modus gesetzt, d. h. sie senden einen Kanal, wenn ein verbundener Port eine PAgP-Anforderung an den Kanal sendet. Wenn Sie SwitchA auf "Desirable" (Erwünscht) setzen, SwitchA, sendet SwitchA PAgP-Pakete an den anderen Switch und fordert diesen auf, den Kanal zu verwenden.

```
Switch-A (enable) set port channel 2/1-4 desirable

Port(s) 2/1-4 channel mode set to desirable.

1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/1 left bridg1

1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2

1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3

1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4

1999 Dec 15 22:03:19 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2

1999 Dec 15 22:03:19 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3

1999 Dec 15 22:03:20 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4

1999 Dec 15 22:03:23 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4

1999 Dec 15 22:03:23 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4

1999 Dec 15 22:03:23 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4

1999 Dec 15 22:03:24 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4
```

Um den Kanal anzuzeigen, gehen Sie folgendermaßen vor.

```
Switch-A (enable) show port channel

Port  Status     Channel   Channel     Neighbor                  Neighbor
                mode      status      device                    port
----- ---------- --------- ----------- ------------------------ ----------
```

```
 2/1  connected  desirable channel     WS-C5505    066509957(Sw  2/1
 2/2  connected  desirable channel     WS-C5505    066509957(Sw  2/2
 2/3  connected  desirable channel     WS-C5505    066509957(Sw  2/3
 2/4  connected  desirable channel     WS-C5505    066509957(Sw  2/4
----- ---------- --------- ----------- ------------------------ ----------
```

Da SwitchB sich im automatischen Modus befand, reagierte er auf die PAgP-Pakete und erstellte einen Kanal mit SwitchA.

```
Switch-B (enable)
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/1 left bridg1
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
2000 Jan 14 20:26:45 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 14 20:26:45 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 14 20:26:45 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
2000 Jan 14 20:26:47 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
2000 Jan 14 20:26:47 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 14 20:26:47 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 14 20:26:48 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  connected  auto      channel     WS-C5505    066507453(Sw  2/1
 2/2  connected  auto      channel     WS-C5505    066507453(Sw  2/2
 2/3  connected  auto      channel     WS-C5505    066507453(Sw  2/3
 2/4  connected  auto      channel     WS-C5505    066507453(Sw  2/4
----- ---------- --------- ----------- ------------------------ ----------
```

Hinweis: Es wird empfohlen, beide Seiten des Kanals so einzustellen, dass beide Seiten versuchen, den Kanal zu initiieren, wenn eine Seite ausfällt. Wenn Sie die EtherChannel-Ports am SwitchB auf den erwünschten Modus setzen, stellt dies kein Problem dar, auch wenn der Kanal

derzeit aktiv und im Automatikmodus ist. Das ist der Befehl.

```
Switch-B (enable) set port channel 2/1-4 desirable

Port(s) 2/1-4 channel mode set to desirable.


Switch-B (enable) show port channel

Port   Status      Channel    Channel      Neighbor                  Neighbor
                   mode       status       device                    port
------ ----------- ---------- ------------ ------------------------- ----------
 2/1   connected   desirable  channel      WS-C5505     066507453(Sw  2/1
 2/2   connected   desirable  channel      WS-C5505     066507453(Sw  2/2
 2/3   connected   desirable  channel      WS-C5505     066507453(Sw  2/3
 2/4   connected   desirable  channel      WS-C5505     066507453(Sw  2/4
------ ----------- ---------- ------------ ------------------------- ----------
```

Wenn SwitchA jetzt aus irgendeinem Grund ausfällt oder wenn neue Hardware SwitchA ersetzt, versucht SwitchB, den Kanal neu einzurichten. Wenn die neuen Geräte keine Channels herstellen können, behandelt SwitchB seine Ports 1,2-4 als normale Nicht-Channeling-Ports. Dies ist einer der Vorteile der Verwendung des erwünschten Modus. Wenn auf dem Kanal der PAgP-Modus "Ein" konfiguriert wurde und auf einer Seite der Verbindung ein Fehler oder ein Reset auftritt, kann dies auf der anderen Seite zu einem errdisable-Status (shutdown) führen. Wenn PAgP auf beiden Seiten in den gewünschten Modus versetzt wird, stabilisiert und verhandelt der Kanal die EtherChannel-Verbindung neu.Trunking und EtherChannelDer EtherChannel ist unabhängig vom Trunking. Sie können das Trunking aktivieren oder deaktivieren. Sie können Trunking auch für alle Ports aktivieren, bevor Sie den Kanal erstellen, oder Sie können ihn aktivieren, nachdem Sie den Kanal erstellt haben (wie hier). Für den EtherChannel spielt dies keine Rolle. Trunking und EtherChannel sind völlig separate Funktionen. Entscheidend ist, dass alle beteiligten Ports sich im gleichen Modus befinden: Entweder sie sind alle Trunking-Ports, bevor Sie den Kanal konfigurieren, oder sie sind alle nicht Trunking-Ports, bevor Sie den Kanal konfigurieren. Alle Ports müssen sich im gleichen Trunking-Zustand befinden, bevor Sie den Channel erstellen können. Sobald ein Kanal gebildet ist, werden alle Änderungen an einem Port auch für die anderen Ports im Kanal geändert. Die in dieser Testumgebung verwendeten Module können ISL- oder 802.1q-Trunking unterstützen. Standardmäßig sind die Module auf den Modus für automatisches Trunking und Aushandlung eingestellt. Das bedeutet, dass sie Trunking verwenden, wenn die andere Seite sie bittet, Trunking durchzuführen, und dass sie aushandeln, ob sie die ISL- oder die 802.1q-Methode für das Trunking verwenden sollen. Wenn sie nicht gebeten werden, einen Trunk zu

starten, funktionieren sie als normale Nicht-Trunk-Ports.

```
Switch-A (enable) show trunk 2

Port      Mode         Encapsulation  Status        Native vlan

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

 2/1      auto         negotiate      not-trunking  1

 2/2      auto         negotiate      not-trunking  1

 2/3      auto         negotiate      not-trunking  1

 2/4      auto         negotiate      not-trunking  1
```

Es gibt verschiedene Möglichkeiten, das Trunking zu aktivieren. In diesem Beispiel legen Sie SwitchA auf "Wünschenswert" fest. SwitchA ist bereits für die Aushandlung festgelegt. Die Kombination aus erwünscht/verhandelt veranlasst SwitchA, SwitchB zu einem Trunk aufzufordern und den entsprechenden Trunking-Typ zu verhandeln (ISL oder 802.1q). Da SwitchB standardmäßig Auto-Negotiate verwendet, reagiert SwitchB auf die Anforderung von SwitchA. Diese Ergebnisse treten auf:

```
Switch-A (enable) set trunk 2/1 desirable

Port(s) 2/1-4 trunk mode set to desirable.

Switch-A (enable)

1999 Dec 18 20:46:25 %DTP-5-TRUNKPORTON:Port 2/1 has become isl trunk

1999 Dec 18 20:46:25 %DTP-5-TRUNKPORTON:Port 2/2 has become isl trunk

1999 Dec 18 20:46:25 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4

1999 Dec 18 20:46:25 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-4

1999 Dec 18 20:46:25 %DTP-5-TRUNKPORTON:Port 2/3 has become isl trunk

1999 Dec 18 20:46:26 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/1-4

1999 Dec 18 20:46:26 %DTP-5-TRUNKPORTON:Port 2/4 has become isl trunk

1999 Dec 18 20:46:26 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/1-4

1999 Dec 18 20:46:28 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4

1999 Dec 18 20:46:29 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4

1999 Dec 18 20:46:29 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4

1999 Dec 18 20:46:29 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4


Switch-A (enable) show trunk 2

Port      Mode         Encapsulation  Status        Native vlan

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

 2/1      desirable    n-isl          trunking      1
```

```
 2/2      desirable    n-isl          trunking      1

 2/3      desirable    n-isl          trunking      1

 2/4      desirable    n-isl          trunking      1
```

Der Trunk-Modus wurde auf "Desirable" (Erwünscht) gesetzt. Das Ergebnis war, dass der Trunking-Modus mit dem Nachbarswitch ausgehandelt wurde und ISL (n-isl) ausgewählt wurde. Der aktuelle Status wird jetzt getrennt. Dies geschah auf SwitchB aufgrund des Befehls, der auf SwitchA ausgegeben wurde.

```
Switch-B (enable)

2000 Jan 17 19:09:52 %DTP-5-TRUNKPORTON:Port 2/1 has become isl trunk

2000 Jan 17 19:09:52 %DTP-5-TRUNKPORTON:Port 2/2 has become isl trunk

2000 Jan 17 19:09:52 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4

2000 Jan 17 19:09:52 %DTP-5-TRUNKPORTON:Port 2/3 has become isl trunk

2000 Jan 17 19:09:52 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-4

2000 Jan 17 19:09:53 %DTP-5-TRUNKPORTON:Port 2/4 has become isl trunk

2000 Jan 17 19:09:53 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/1-4

2000 Jan 17 19:09:53 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/1-4

2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4

2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4

2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4

2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4


Switch-B (enable) show trunk 2

Port      Mode         Encapsulation  Status        Native vlan

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

 2/1      auto         n-isl          trunking      1

 2/2      auto         n-isl          trunking      1

 2/3      auto         n-isl          trunking      1

 2/4      auto         n-isl          trunking      1
```

Beachten Sie, dass alle vier Ports (2/1-4) zu Trunks wurden, obwohl Sie nur einen Port (2/1) in den gewünschten Port geändert haben. Dies ist ein Beispiel dafür, wie sich die Änderung eines Ports im Channel auf alle Ports auswirkt.Fehlerbehebung bei EtherChannelDie Herausforderungen für den EtherChannel lassen sich in zwei Hauptbereiche unterteilen: Fehlerbehebung innerhalb der Konfigurationsphase und Fehlerbehebung innerhalb der

Ausführungsphase. Konfigurationsfehler treten in der Regel aufgrund von nicht übereinstimmenden Parametern auf den betreffenden Ports auf (unterschiedliche Geschwindigkeiten, unterschiedliche Duplexwerte, unterschiedliche Spanning Tree-Portwerte usw.). Sie können auch Fehler in der Konfiguration generieren, wenn Sie den Kanal auf der einen Seite auf einstellen und zu lange warten, bevor Sie den Kanal auf der anderen Seite konfigurieren. Dies verursacht Spanning Tree-Schleifen, die einen Fehler verursachen, und fährt den Port herunter.Wenn bei der Konfiguration des EtherChannels ein Fehler auftritt, überprüfen Sie den Status der Ports, nachdem Sie die EtherChannel-Fehlersituation behoben haben. Wenn der Port-Status *errdisable lautet*, bedeutet dies, dass die Ports von der Software deaktiviert wurden und erst wieder aktiviert werden, wenn Sie den Befehl set port enable eingeben.Hinweis: Wenn der Port-Status *errdisable lautet*, müssen Sie die Ports mit dem Befehl set port enable explizit aktivieren, damit die Ports aktiviert werden. Derzeit können Sie alle EtherChannel-Probleme beheben, aber die Ports werden erst aktiviert, wenn sie wieder aktiviert sind. Künftige Versionen des Betriebssystems können periodisch überprüfen, ob iferrdisableports aktiviert sein müssen.Für diese Tests deaktivieren Sie Trunking und EtherChannel: Falsch zugeordnete Parameter; warten Sie zu lange, bevor Sie die andere Seite konfigurieren; korrigieren Sie den Ersetzungszustand und zeigen Sie, was passiert, wenn eine Verbindung unterbrochen wird und wiederhergestellt wird.Nicht übereinstimmende ParameterHier ein Beispiel für nicht übereinstimmende Parameter. Legen Sie Port 2/4 in VLAN 2 fest, während sich die anderen Ports noch in VLAN 1 befinden. Um ein neues VLAN zu erstellen, müssen Sie dem Switch eine VTP-Domäne zuweisen und das VLAN erstellen.

```
Switch-A (enable) show port channel

No ports channelling


Switch-A (enable) show port

Port  Name                 Status     Vlan       Level  Duplex Speed Type

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

 2/1                      connected  1          normal a-full a-100 10/100BaseTX

 2/2                      connected  1          normal a-full a-100 10/100BaseTX

 2/3                      connected  1          normal a-full a-100 10/100BaseTX

 2/4                      connected  1          normal a-full a-100 10/100BaseTX


Switch-A (enable) set vlan 2

Cannot add/modify VLANs on a VTP server without a domain name.
```

```
Switch-A (enable) set vtp domain testDomain
VTP domain testDomain modified

Switch-A (enable) set vlan 2 name vlan2
Vlan 2 configuration successful

Switch-A (enable) set vlan 2 2/4
VLAN 2 modified.
VLAN 1 modified.
VLAN  Mod/Ports
---- ----------------------
2     2/4

Switch-A (enable)
1999 Dec 19 00:19:34 %PAGP-5-PORTFROMSTP:Port 2/4 left bridg4

Switch-A (enable) show port
Port  Name                 Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                      connected  1          normal a-full a-100 10/100BaseTX
 2/2                      connected  1          normal a-full a-100 10/100BaseTX
 2/3                      connected  1          normal a-full a-100 10/100BaseTX
 2/4                      connected  2          normal a-full a-100 10/100BaseTX

Switch-A (enable) set port channel 2/1-4 desirable
Port(s) 2/1-4 channel mode set to desirable.

Switch-A (enable)
1999 Dec 19 00:20:19 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
1999 Dec 19 00:20:19 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 19 00:20:19 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 19 00:20:20 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 19 00:20:20 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 19 00:20:22 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 19 00:20:22 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
```

```
1999 Dec 19 00:20:24 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-2

1999 Dec 19 00:20:25 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-2

1999 Dec 19 00:20:25 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3

1999 Dec 19 00:20:25 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/4


Switch-A (enable) show port channel

Port  Status     Channel   Channel     Neighbor                  Neighbor

                 mode      status      device                    port

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

 2/1  connected  desirable channel     WS-C5505    066509957(Sw  2/1

 2/2  connected  desirable channel     WS-C5505    066509957(Sw  2/2

----- ---------- --------- ----------- ------------------------ ----------
```

Beachten Sie, dass sich der Kanal nur zwischen den Ports 2/1-2 gebildet hat. Die Ports 2/3-4 wurden weggelassen, da sich Port 2/4 in einem anderen VLAN befand. Es gab keine Fehlermeldung; PAgP tat nur, was in der Lage war, den Kanal zum Laufen zu bringen. Sie müssen die Ergebnisse beim Erstellen des Kanals beobachten, um sicherzustellen, dass er Ihren Vorstellungen entspricht.Stellen Sie nun den Kanal manuell auf "on" (Ein) mit Port 2/4 in einem anderen VLAN ein, und beobachten Sie, was passiert. Zuerst setzen Sie den Channel-Modus wieder auf Auto, um den aktuellen Channel zu beenden, dann setzen Sie den Channel manuell auf "on".

```
Switch-A (enable) set port channel 2/1-4 auto

Port(s) 2/1-4 channel mode set to auto.

Switch-A (enable)

1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-2

1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-2

1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3

1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4

1999 Dec 19 00:26:18 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1

1999 Dec 19 00:26:19 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2

1999 Dec 19 00:26:19 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3

1999 Dec 19 00:26:19 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/4


Switch-A (enable) show port channel

No ports channelling
```

```
Switch-A (enable) set port channel 2/1-4 on
Mismatch in vlan number.
Failed to set port(s) 2/1-4 channel mode to on.

Switch-A (enable) show port channel
No ports channelling
```

Auf SwitchB können Sie den Kanal einschalten und feststellen, dass der Port-Kanal einwandfrei angezeigt wird, Sie wissen jedoch, dass SwitchA nicht richtig konfiguriert ist.

```
Switch-B (enable) show port channel
No ports channelling

Switch-B (enable) show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     connected  1          normal a-full a-100 10/100BaseTX
 2/2                     connected  1          normal a-full a-100 10/100BaseTX
 2/3                     connected  1          normal a-full a-100 10/100BaseTX
 2/4                     connected  1          normal a-full a-100 10/100BaseTX

Switch-B (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.

Switch-B (enable)
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
```

```
                mode      status      device                    port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  connected  on        channel     WS-C5505    066507453(Sw  2/1
 2/2  connected  on        channel     WS-C5505    066507453(Sw  2/2
 2/3  connected  on        channel     WS-C5505    066507453(Sw  2/3
 2/4  connected  on        channel     WS-C5505    066507453(Sw  2/4
----- ---------- --------- ----------- ------------------------ ----------
```

Dies macht deutlich, dass Sie beide Seiten des Kanals überprüfen müssen, wenn Sie den Kanal manuell konfigurieren, um sicherzustellen, dass beide Seiten oben sind, nicht nur eine Seite. Diese Ausgabe zeigt an, dass SwitchB für einen Kanal eingestellt ist, SwitchA jedoch keinen Kanal durchlässt, da ein Port im falschen VLAN vorhanden ist.Warten Sie zu lange, bevor Sie die andere Seite konfigurieren.In dieser Situation ist der EtherChannel für SwitchB aktiviert, bei SwitchA jedoch nicht, da ein VLAN-Konfigurationsfehler vorliegt (Ports 2/1-3 befinden sich in VLAN1, Port 2/4 in VLAN2). Dies geschieht, wenn eine Seite eines EtherChannels aktiviert ist, während sich die andere Seite noch im automatischen Modus befindet. SwitchB stellte seine Ports nach einigen Minuten aufgrund einer Erkennung eines Spanning Loops ein. Der Grund hierfür ist, dass die SwitchB-Ports 2/1-4 alle wie ein großer Port agieren, während die SwitchA-Ports 2/1-4 vollständig unabhängige Ports sind. Ein Broadcast, der von SwitchB an SwitchA an Port 2/1 gesendet wird, wird an SwitchB an den Ports 2/2, 2/3 und 2/4 zurückgesendet, da SwitchA diese Ports als unabhängige Ports behandelt. Aus diesem Grund meldet SwitchB, dass eine Spanning Tree-Schleife vorhanden ist. Beachten Sie, dass die Ports auf SwitchB jetzt deaktiviert sind und den Status oferrdisable *haben*.

```
Switch-B (enable)
2000 Jan 17 22:55:48 %SPANTREE-2-CHNMISCFG: STP loop - channel 2/1-4 is disabled in vlan 1.
2000 Jan 17 22:55:49 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4
2000 Jan 17 22:56:01 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-4
2000 Jan 17 22:56:13 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/1-4
2000 Jan 17 22:56:36 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/1-4

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  errdisable on        channel
```

```
 2/2  errdisable on        channel
 2/3  errdisable on        channel
 2/4  errdisable on        channel
----- ---------- --------- ----------- ------------------------ ----------
Switch-B (enable) show port
Port  Name                Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     errdisable 1          normal   auto  auto 10/100BaseTX
 2/2                     errdisable 1          normal   auto  auto 10/100BaseTX
 2/3                     errdisable 1          normal   auto  auto 10/100BaseTX
 2/4                     errdisable 1          normal   auto  auto 10/100BaseTX
```

Fehlerdeaktivierungsstatus korrigierenManchmal, wenn Sie versuchen, einen EtherChannel zu konfigurieren, die Ports jedoch nicht gleich konfiguriert sind, werden die Ports auf der einen oder anderen Seite des Kanals ausgeschaltet. Die Verbindungs-LEDs leuchten gelb am Port. Sie können dies an der Konsole erkennen, wenn Sie show port eingeben. Die Ports werden als *errdisable* aufgeführt. Um sich davon zu erholen, müssen Sie die falsch übereinstimmenden Parameter an den betroffenen Ports beheben und die Ports dann erneut aktivieren. Beachten Sie, dass die Ports erneut aktiviert werden müssen, damit sie wieder funktionieren.In diesem Beispiel wissen Sie, dass SwitchA eine VLAN-Diskrepanz aufweist. Sie gehen zu SwitchA und setzen Port 2/4 wieder in VLAN1 ein. Anschließend aktivieren Sie den Kanal für die Ports 2/1-4. SwitchA wird erst dann verbunden angezeigt, wenn Sie die SwitchB-Ports erneut aktivieren. Wenn Sie dann den SwitchA repariert und in den Channeling-Modus versetzt haben, kehren Sie zu SwitchB zurück und aktivieren die Ports erneut.

```
Switch-A (enable) set vlan 1 2/4
VLAN 1 modified.
VLAN 2 modified.
VLAN  Mod/Ports
---- ----------------------
1     2/1-24

Switch-A (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.
Switch-A (enable) sh port channel
Port  Status     Channel   Channel     Neighbor                 Neighbor
```

```
                mode      status      device                    port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  notconnect on        channel
 2/2  notconnect on        channel
 2/3  notconnect on        channel
 2/4  notconnect on        channel
----- ---------- --------- ----------- ------------------------ ----------

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                mode      status      device                    port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  errdisable on        channel
 2/2  errdisable on        channel
 2/3  errdisable on        channel
 2/4  errdisable on        channel
----- ---------- --------- ----------- ------------------------ ----------

Switch-B (enable) set port enable 2/1-4
Ports 2/1-4 enabled.
Switch-B (enable) 2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/1 joined bridg4
2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                mode      status      device                    port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  connected  on        channel
 2/2  connected  on        channel
 2/3  connected  on        channel
 2/4  connected  on        channel
----- ---------- --------- ----------- ------------------------ ----------
```

Anzeigen, was passiert, wenn ein Link unterbrochen wird und wiederhergestellt wirdWenn ein Port im Channel ausfällt, werden alle Pakete, die normalerweise über diesen Port gesendet werden, zum nächsten Port im Channel verschoben. Sie können überprüfen, ob dies mit der Show mcommand geschieht. In dieser Testumgebung sendet SwitchA Ping-Pakete an SwitchB, um festzustellen, welche Verbindung der Datenverkehr nutzt. Zuerst löschen Sie die Zähler, zeigen dann mac an, senden drei Pings und dann erneut show macagain, um zu sehen, auf welchem Kanal die Ping-Antworten empfangen wurden.

```
Switch-A (enable) clear counters
This command will reset all MAC and port counters reported in CLI and SNMP.
Do you want to continue (y/n) [n]? y
MAC and Port counters cleared.

Switch-A (enable) show port channel
Port   Status      Channel    Channel      Neighbor                    Neighbor
                   mode       status       device                      port
------ ----------- ---------- ------------ --------------------------- ----------
 2/1   connected   on         channel      WS-C5505    066509957(Sw    2/1
 2/2   connected   on         channel      WS-C5505    066509957(Sw    2/2
 2/3   connected   on         channel      WS-C5505    066509957(Sw    2/3
 2/4   connected   on         channel      WS-C5505    066509957(Sw    2/4
------ ----------- ---------- ------------ --------------------------- ----------

Switch-A (enable) show mac

Port      Rcv-Unicast           Rcv-Multicast         Rcv-Broadcast
--------- -------------------- --------------------- --------------------
 2/1                         0                    18                    0
 2/2                         0                     2                    0
 2/3                         0                     2                    0
 2/4                         0                     2                    0
Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
```

```
Switch-A (enable) ping 172.16.84.17

172.16.84.17 is alive

Switch-A (enable) show mac


Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast

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

 2/1                        3                   24                    0

 2/2                        0                    2                    0

 2/3                        0                    2                    0

 2/4                        0                    2                    0
```

An diesem Punkt haben Sie die Ping-Antworten auf Port 3/1 erhalten. Wenn die SwitchB-Konsole eine Antwort an SwitchA sendet, verwendet der EtherChannel den Port 2/1. Jetzt fahren Sie Port 2/1 auf SwitchB herunter. Von SwitchA senden Sie einen weiteren Ping-Befehl, um festzustellen, auf welchem Kanal die Antwort erfolgt. (SwitchA sendet über denselben Port, an den SwitchB angeschlossen ist. Sie zeigen nur die von SwitchB empfangenen Pakete an, da die Übertragungspakete weiter unten in der Anzeige für die Anzeige stehen.)

```
1999 Dec 19 01:30:23 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4


Switch-A (enable) ping 172.16.84.17

172.16.84.17 is alive

Switch-A (enable) show mac


Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast

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

 2/1                        3                   37                    0

 2/2                        1                   27                    0

 2/3                        0                    7                    0

 2/4                        0                    7                    0
```

Wenn Port 2/1 deaktiviert ist, verwendet der EtherChannel automatisch den nächsten Port im Kanal, 2/2. Jetzt können Sie Port 2/1 wieder aktivieren und warten, bis er der Bridge-Gruppe beitritt. Sie geben dann zwei weitere Pings aus.

```
1999 Dec 19 01:31:33 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
```

```
Switch-A (enable) ping 172.16.84.17

172.16.84.17 is alive

Switch-A (enable) ping 172.16.84.17

172.16.84.17 is alive

Switch-A (enable) show mac


Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast

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

 2/1                        5                   50                    0

 2/2                        1                   49                    0

 2/3                        0                   12                    0

 2/4                        0                   12                    0
```

Beachten Sie, dass diese Pings von Port 2/1 gesendet werden. Wenn die Verbindung wieder hergestellt ist, fügt der EtherChannel sie erneut dem Paket hinzu und verwendet sie. All dies geschieht für den Benutzer transparent.In diesem Abschnitt verwendete BefehleDies sind die Befehle, die in diesem Abschnitt verwendet wurden.Zum Festlegen der Konfiguration zu verwendende Befehle

Port-Channel aktivieren - um die EtherChannel-Funktion zu aktivieren.

Port-Channel automatisch festlegen - um die Ports auf ihren Standardmodus "Auto" zurückzusetzen.

Legen Sie den gewünschten Port-Channel fest, um PAgP-Pakete an die anderen Seite zu senden und einen Kanal zu erstellen.

set port enable: Die Ports werden nach set port disable oder errdisable aktiviert.

set port disable - Einen Port deaktivieren, während andere Konfigurationseinstellungen vorgenommen werden.

set trunk desirable - Trunking aktivieren und veranlassen, dass dieser Port eine Anforderung an den anderen Switch sendet, um anzuzeigen, dass es sich um eine Trunk-Verbindung handelt. Wenn der Port so konfiguriert ist, dass er aushandelt (die Standardeinstellung), um den Trunking-Typ auszuhandeln, der für die Verbindung verwendet werden soll (ISL oder 802.1q).

Befehle zum Überprüfen der Konfiguration

show version: Zeigt an, welche Softwareversion auf dem Switch ausgeführt wird.

show module: Zeigt an, welche Module im Switch installiert sind.

Show Port Capabilities: Bestimmen Sie, ob die Ports, die Sie verwenden möchten, EtherChannel unterstützen.

show port: Bestimmen Sie den Status des Ports (keine Verbindung, verbunden) sowie die Geschwindigkeits- und Duplexeinstellungen.

ping: Testen der Verbindung mit dem anderen Switch

show port channel: Zeigt den aktuellen Status des EtherChannel-Pakets an.

show port channel mod/port: Zeigt den Kanalstatus eines einzelnen Ports detaillierter an.

show spantree: Überprüfen, ob Spanning Tree den Channel als einen Link betrachtet.

show trunk: Anzeige des Trunking-Status der Ports

Befehle zur Fehlerbehebung bei der Konfiguration

show port channel: Zeigt den aktuellen Status des EtherChannel-Pakets an.

show port: Bestimmen Sie den Status des Ports (keine Verbindung, verbunden) sowie die Geschwindigkeits- und Duplexeinstellungen.

Zähler löschen: Die Zähler des Switch-Pakets werden auf Null zurückgesetzt. Die Zähler sind sichtbar mit der Show maccand.

show mac: Zeigt die vom Switch empfangenen und gesendeten Pakete an.

ping: Testen der Verbindung mit dem anderen Switch und Generieren von Datenverkehr, der mit der Show maccand angezeigt wird

Verwenden Sie PortFast und andere Befehle, um Verbindungsprobleme beim Starten der Endstation zu beheben.

Wenn Sie Workstations mit Switches verbunden haben, die sich nicht bei Ihrer Netzwerkdomäne (NT oder Novell) anmelden können oder keine DHCP-Adresse erhalten, können Sie die in diesem Dokument aufgeführten Vorschläge ausprobieren, bevor Sie andere Wege erkunden. Die Vorschläge sind relativ einfach zu implementieren und verursachen häufig Probleme mit der Verbindung zu Workstations, die während der Initialisierungs-/Startphase der Workstation auftreten.Bei immer mehr Benutzern, die Switching auf dem Desktop bereitstellen und ihre

gemeinsam genutzten Hubs durch Switches ersetzen, treten aufgrund dieser anfänglichen Verzögerung häufig Probleme in Client/Server-Umgebungen auf. Das größte Problem, das Sie sehen, ist, dass Windows 95/98/NT, Novell, VINES, IBM NetworkStation/IBM Thin Clients und AppleTalk Clients keine Verbindung zu ihren Servern herstellen können. Wenn die Software auf diesen Geräten nicht dauerhaft im Startvorgang enthalten ist, versuchen sie nicht mehr, eine Verbindung zu ihrem Server herzustellen, bevor der Switch den Datenverkehr überhaupt zugelassen hat.Hinweis: Diese anfängliche Verbindungsverzögerung äußert sich häufig als Fehler, die beim ersten Starten einer Workstation auftreten. Nachfolgend finden Sie einige Beispiele für Fehlermeldungen und -fehler:

Ein Microsoft-Netzwerkclient zeigt die Meldung "Keine Domänencontroller verfügbar" an.

DHCP-Berichte: "Keine DHCP-Server verfügbar."

Eine Novell IPX-Netzwerk-Workstation verfügt beim Start nicht über den "Novell Login Screen".

Ein AppleTalk-Netzwerk-Client zeigt Folgendes an: "Der Zugriff auf Ihr AppleTalk-Netzwerk wurde unterbrochen. Um die Verbindung wiederherzustellen, öffnen und schließen Sie das AppleTalk-Bedienfeld." Es ist auch möglich, dass die Anwendung AppleTalk Client Chooser entweder keine oder eine unvollständige Zonenliste anzeigt.

Die anfängliche Verbindungsverzögerung tritt häufig auch in Switching-Umgebungen auf, in denen Netzwerkadministratoren Software oder Treiber aktualisieren. In diesem Fall kann ein Anbieter die Treiber so optimieren, dass Netzwerkinitialisierungsprozesse früher während des Startprozesses des Clients erfolgen (bevor der Switch zur Verarbeitung der Pakete bereit ist).Dank der verschiedenen Funktionen, die jetzt in einigen Switches enthalten sind, kann es beinahe eine Minute dauern, bis ein Switch mit der Wartung einer neu verbundenen Workstation beginnt. Diese Verzögerung kann sich bei jedem Einschalten oder Neustart auf die Workstation auswirken. Dies sind die vier Hauptmerkmale, die diese Verzögerung verursachen:

Spanning Tree Protocol (STP)

EtherChannel-Aushandlung

Trunking-Aushandlung

Verbindungsgeschwindigkeits-/Duplex-Aushandlung zwischen Switch und Workstation

Die vier Funktionen werden in der Reihenfolge aufgelistet, bei der die größte Verzögerung

(Spanning-Tree Protocol) verursacht wird, die die geringste Verzögerung verursacht (Geschwindigkeit/Duplexaushandlung). Eine mit einem Switch verbundene Workstation verursacht normalerweise keine Spanning-Tree-Schleifen, benötigt in der Regel keinen EtherChannel und muss in der Regel keine Trunking-Methode aushandeln. (Wenn Sie die Aushandlung zur Verbindungsgeschwindigkeit/Erkennung deaktivieren, kann dies auch die Portverzögerung verringern, wenn Sie die Startzeit so weit wie möglich optimieren müssen.)In diesem Abschnitt wird die Implementierung von Befehlen zur Optimierung der Startgeschwindigkeit auf drei Catalyst Switch-Plattformen beschrieben. In den Zeitabschnitten zeigen Sie, wie und um wie viel die Switch-Port-Verzögerung verringert wird.Inhalt

Die Begriffe "Workstation", "Endstation", "Server" werden in diesem Abschnitt synonym verwendet. Sie beziehen sich auf jedes Gerät, das über eine einzelne NIC-Karte direkt mit einem Switch verbunden ist. Sie kann sich auch auf Geräte mit mehreren NIC-Karten beziehen, bei denen die NIC-Karte nur für die Redundanz verwendet wird, d. h. die Workstation oder der Server ist nicht als Bridge konfiguriert, sondern verfügt lediglich über mehrere NIC-Karten für die Redundanz.Hinweis: Es gibt einige Server-NIC-Karten, die Trunking und/oder EtherChannel unterstützen. In einigen Situationen muss der Server auf mehreren VLANs gleichzeitig ausgeführt werden (Trunking), oder der Server benötigt mehr Bandbreite über die Verbindung, die ihn mit dem Switch verbindet (EtherChannel). Schalten Sie in diesen Fällen PAgP und Trunking nicht aus. Zudem werden diese Geräte selten ausgeschaltet oder zurückgesetzt. Die Anweisungen in diesem Dokument gelten nicht für diese Gerätetypen.HintergrundDieser Abschnitt behandelt vier Funktionen, die bei einigen Switches vorhanden sind und anfängliche Verzögerungen

verursachen, wenn ein Gerät mit einem Switch verbunden wird. Normalerweise verursacht eine Workstation entweder kein Spanning Tree-Problem (Loops) oder benötigt die Funktion nicht (PAgP, DTP), sodass die Verzögerung nicht erforderlich ist.Spanning TreeWenn Sie vor kurzem damit begonnen haben, von einer Hub-Umgebung zu einer Switch-Umgebung zu wechseln, können diese Verbindungsprobleme auftreten, da ein Switch erheblich anders funktioniert als ein Hub. Ein Switch stellt die Verbindung auf der Datenverbindungsschicht und nicht auf der physischen Schicht bereit. Der Switch muss einen Bridging-Algorithmus verwenden, um zu entscheiden, ob Pakete, die an einem Port empfangen werden, über andere Ports übertragen werden müssen. Der Bridging-Algorithmus ist anfällig für physische Schleifen in der Netzwerktopologie. Aufgrund dieser Anfälligkeit für Schleifen führen Switches ein Protokoll aus, das als Spanning Tree Protocol (STP) bezeichnet wird und dazu führt, dass Schleifen in der Topologie eliminiert werden. Wenn STP ausgeführt wird, werden alle Ports, die im Spanning Tree-Prozess enthalten sind, sehr viel langsamer aktiv, als dies andernfalls der Fall wäre, da Schleifen erkannt und blockiert werden. Ein überbrücktes Netzwerk mit physischen Schleifen ohne Spanning Tree wird unterbrochen. Trotz des Zeitaufwands ist STP eine gute Sache. Der Spanning Tree, der auf Catalyst Switches ausgeführt wird, entspricht dem Industriestandard (IEEE 802.1d).Wenn ein Port auf dem Switch über einen Link verfügt und der Bridge-Gruppe beitritt, wird Spanning Tree auf diesem Port ausgeführt. Ein Port, der Spanning Tree ausführt, kann einen von fünf Status haben: Blockieren, Zuhören, Lernen, Weiterleiten und Deaktiviert. Spanning Tree gibt vor, dass der Port anfängt zu blockieren und sich dann sofort durch die Phasen Überwachen und Lernen bewegt. Standardmäßig verbringt es ca. 15 Sekunden mit dem Abhören und 15 Sekunden mit dem Lernen.Im Listening-Status versucht der Switch festzustellen, wo er in die Spanning-Tree-Topologie passt. Er möchte insbesondere wissen, ob dieser Port Teil eines physischen Loops ist. Wenn der Port Teil einer Schleife ist, kann er in den Blockierungsmodus versetzt werden. Blockierung bedeutet, dass keine Benutzerdaten gesendet oder empfangen werden, um Schleifen zu beseitigen. Wenn der Port nicht Teil einer Schleife ist, geht er in den Lernstatus über, bei dem ermittelt wird, welche MAC-Adressen von diesem Port leben. Dieser gesamte Spanning Tree-Initialisierungsvorgang dauert etwa 30 Sekunden.Wenn Sie eine Workstation oder einen Server mit einer einzelnen NIC-Karte mit einem Switch-Port verbinden, kann diese Verbindung keine physische Schleife erzeugen. Diese Verbindungen werden als Leaf-Knoten betrachtet. Es besteht kein Grund, die Workstation 30 Sekunden warten zu lassen, während der Switch nach Schleifen sucht, wenn die Workstation keine Schleife verursachen kann. Cisco hat daher eine Funktion mit der Bezeichnung "Portfast" oder "Fast-Start" hinzugefügt. Dies bedeutet, dass der Spanning Tree für diesen Port davon ausgehen kann, dass der Port nicht Teil einer Schleife ist, und dass er sofort in den Weiterleitungsstatus übergehen kann, um den Blockierungs-, Überwachungs- oder

Lernstatus zu überspringen. Das kann viel Zeit sparen. Mit diesem Befehl wird Spanning Tree nicht deaktiviert. Dadurch überspringt Spanning Tree am ausgewählten Port lediglich einige (in diesem Fall nicht erforderliche) Schritte am Anfang.Hinweis: Die Portfast-Funktion darf niemals auf Switch-Ports verwendet werden, die mit anderen Switches, Hubs oder Routern verbunden sind. Diese Verbindungen können physische Schleifen verursachen, und es ist sehr wichtig, dass Spanning Tree in diesen Situationen die vollständige Initialisierung durchläuft. Eine Spanning Tree Loop kann Ihr Netzwerk zum Absturz bringen. Wenn "portfast" für einen Port aktiviert ist, der Teil einer physischen Schleife ist, kann dies ein Zeitfenster verursachen, in dem Pakete möglicherweise kontinuierlich weitergeleitet (und sogar multipliziert) werden können, sodass das Netzwerk nicht mehr wiederhergestellt werden kann. In der neueren Catalyst-Betriebssystemsoftware (5.4(1)) gibt es eine Funktion namens Portfast BPDU-Guard, die den Empfang von BPDUs an Ports erkennt, auf denen Portfast aktiviert ist. Da dies niemals passieren darf, versetzt BPDU-Guard den Port in den Status "errDisable".EtherChannelEine weitere Funktion, die ein Switch haben kann, ist der EtherChannel (oder Fast EtherChannel oder Gigabit EtherChannel). Mit dieser Funktion können mehrere Verbindungen zwischen denselben beiden Geräten wie eine schnelle Verbindung funktionieren, wobei die Datenverkehrslast auf die Verbindungen verteilt wird. Ein Switch kann diese Pakete automatisch mit einem Nachbarn bilden, der über das Protokoll PAgP (Port Aggregation Protocol) verfügt. Switch-Ports, auf denen PAgP ausgeführt werden kann, verwenden standardmäßig den passiven Modus "auto". Das bedeutet, dass sie ein Bündel bilden können, wenn sie vom benachbarten Gerät über die Verbindung dazu aufgefordert werden. Wenn Sie das Protokoll im Auto-Modus ausführen, kann dies dazu führen, dass sich ein Port bis zu 15 Sekunden verzögert, bevor er die Kontrolle an den Spanning-Tree-Algorithmus übergibt (PAgP wird auf einem Port ausgeführt, bevor Spanning Tree dies tut). PAgP muss nicht an einem Port ausgeführt werden, der mit einer Workstation verbunden ist. Wenn Sie den PAgP-Modus des Switch-Ports auf "off" (Aus) setzen, wird diese Verzögerung eliminiert.TrunkingEine weitere Switch-Funktion ist die Fähigkeit eines Ports, einen Trunk zu bilden. Ein Trunk wird zwischen zwei Geräten konfiguriert, wenn sie Datenverkehr von mehreren Virtual Local Area Networks (VLANs) übertragen müssen. Ein VLAN wird von Switches so erstellt, dass eine Gruppe von Workstations in ihrem eigenen Segment oder ihrer eigenen Broadcast-Domäne erscheint. Trunk-Ports sorgen dafür, dass sich diese VLANs über mehrere Switches erstrecken, sodass ein einzelnes VLAN einen gesamten Campus abdecken kann. Hierzu werden den Paketen Tags hinzugefügt. Dadurch wird angegeben, zu welchem VLAN das Paket gehört.Es gibt verschiedene Arten von Trunking-Protokollen. Wenn ein Port zu einem Trunk werden kann, kann er auch automatisch einen Trunk erstellen und in einigen Fällen sogar aushandeln, welche Art von Trunking auf dem Port verwendet werden soll. Die Möglichkeit, die Trunking-Methode mit

dem anderen Gerät auszuhandeln, wird als Dynamic Trunking Protocol (DTP) bezeichnet. Der DTP-Vorläufer ist ein als Dynamic ISL (DISL) bezeichnetes Protokoll. Wenn diese Protokolle ausgeführt werden, können sie einen aktiven Port auf dem Switch verzögern.Normalerweise gehört ein Port, der mit einer Workstation verbunden ist, nur zu einem VLAN und muss daher nicht mit Trunk verbunden werden. Wenn ein Port die Bildung eines Trunks aushandeln kann, wechselt er in der Regel in den "Auto"-Modus. Wenn der Port in den Trunking-Modus "Aus" geändert wird, wird die Verzögerung eines aktiven Switch-Ports weiter reduziert.Geschwindigkeits- und Duplex-AushandlungSie müssen nur Portfast einschalten und PAgP (falls vorhanden) ausschalten, um das Problem zu beheben. Wenn Sie jedoch jede mögliche Sekunde eliminieren müssen, können Sie die Portgeschwindigkeit und die Duplexfunktion auch manuell auf dem Switch einstellen, wenn es sich um einen Port mit mehreren Geschwindigkeiten (10/100) handelt. Auto-Negotiation ist eine nette Funktion. Wenn Sie sie jedoch ausschalten, können Sie beim Catalyst 5000 2 Sekunden sparen (beim 2800 oder 2900XL hilft das nicht viel).Es kann jedoch zu Komplikationen kommen, wenn Sie die automatische Aushandlung auf dem Switch deaktivieren, ihn jedoch auf der Workstation aktiviert lassen. Da der Switch keine Verhandlungen mit dem Client aufnimmt, kann der Client die gleiche Duplexeinstellung auswählen, die der Switch verwendet oder nicht. Unter "Fehlerbehebung bei Ethernet 10/100Mb Half/Half/Full Duplex Auto-Negotiation" finden Sie weitere Informationen zu den Vorbehalten der Auto-Negotiation.So reduzieren Sie die Startverzögerung beim Catalyst 4000/5000/6000 SwitchDiese fünf Befehle zeigen, wie Portfast aktiviert, PAgP-Aushandlung deaktiviert, Trunking-Aushandlung (DISL, DTP) deaktiviert und Geschwindigkeit/Duplex-Aushandlung deaktiviert wird. Der Befehl set spantree portfast wird auf mehreren Ports gleichzeitig ausgeführt (set spantree portfast 2/1-12 enable). Normalerweise muss ein festgelegter Port-Channel mit einer gültigen Gruppe von Channel-fähigen Ports deaktiviert werden. In diesem Fall kann Modul 2 Channel mit den Ports 2/1-2 oder 2/1-4 verwenden, sodass beide Port-Gruppen gültig wären.Hinweis: Version 5.2 von Cat OS für Catalyst 4000/5000 verfügt über einen neuen Befehl namens "set port host". Hierbei handelt es sich um ein Makro, das diese Befehle in einem benutzerfreundlichen Befehl kombiniert (außer dass die Geschwindigkeits- und Duplexeinstellungen nicht geändert werden).Konfiguration

```
Switch-A (enable) set spantree portfast 2/1 enable

Warning: Spantree port fast start should only be enabled on ports connected
to a single host. Connecting hubs, concentrators, switches, bridges, and so on to
a fast start port can cause temporary spanning tree loops.  Use with caution.

Spantree port 2/1 fast start enabled.
```

```
Switch-A (enable) set port channel 2/1-2 off

Port(s) 2/1-2 channel mode set to off.


Switch-A (enable) set trunk 2/1 off

Port(s) 2/1 trunk mode set to off.
```

Die Änderungen an der Konfiguration werden automatisch im NVRAM gespeichert.VerifizierungDie in diesem Dokument verwendete Version der Switch-Software ist 4.5(1). Die vollständige Ausgabe von show version und show module finden Sie in diesem Timing-Test-Abschnitt.

```
Switch-A (enable) show version

WS-C5505 Software,

Version McpSW: 4.5(1) NmpSW: 4.5(1)
```

Dieser Befehl zeigt, wie der aktuelle Status eines Ports in Bezug auf Spanning Tree angezeigt wird. Derzeit befindet sich der Port im Spanning-Tree-Weiterleitungsstatus (Senden und Empfangen von Paketen), und in der Spalte für den Schnellstart wird angezeigt, dass "portfast" aktuell deaktiviert ist. Mit anderen Worten: Der Port kann bei jeder Initialisierung mindestens 30 Sekunden benötigen, um in den Weiterleitungsstatus zu wechseln.

```
Switch-A (enable) show port spantree 2/1


Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-Method

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

 2/1      1     forwarding        19        32

disabled
```

Jetzt aktivieren Sie portfast auf diesem Switch-Port. Der Switch warnt uns, dass dieser Befehl nur an Ports verwendet werden darf, die mit einem einzelnen Host verbunden sind (einer Workstation, einem Server usw.), und niemals an Ports verwendet werden darf, die mit anderen Hubs oder Switches verbunden sind. Der Grund, warum Sie portfast aktivieren, ist, dass der Port sofort mit der Weiterleitung beginnt. Dies ist möglich, da eine Workstation oder ein Server keine Netzwerkschleife verursacht. Das kann Zeit verschwenden. Ein anderer Hub oder Switch kann jedoch eine Schleife verursachen, und Sie möchten immer die normalen Phasen des Zuhörens und Lernens durchlaufen, wenn Sie eine Verbindung mit diesen Gerätetypen herstellen.

```
Switch-A (enable) set spantree portfast 2/1 enable
```

```
Warning: Spantree port fast start should only be enabled on ports connected
to a single host.  Connecting hubs, concentrators, switches, bridges, and so on to
a fast start port can cause temporary spanning tree loops.  Use with caution.

Spantree port 2/1 fast start enabled.
```

Um zu überprüfen, ob Portfast für diesen Port aktiviert ist, führen Sie diesen Befehl aus.

```
Switch-A (enable) show port spantree 2/1

Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-Method
--------  ----  -------------  -----  --------  ----------  ------------
 2/1      1     forwarding        19        32
enabled
```

Eine andere Möglichkeit, die Portfast-Einstellungen für einen oder mehrere Ports anzuzeigen, besteht darin, die Spanning-Tree-Informationen für ein bestimmtes VLAN anzuzeigen. Später, im Timing-Abschnitt dieses Dokuments, zeigen Sie, wie der Switch jede Phase von Spanning Tree, die er durchläuft, in Echtzeit meldet. Dieser Ausgang zeigt auch die Vorwärtsverzögerungszeit (15 Sekunden) an. Dies gibt an, wie lange Spanning Tree im Überwachungsstatus und im Lernstatus für jeden Port im VLAN sein kann.

```
Switch-A (enable) show spantree 1
VLAN 1
Spanning tree enabled
Spanning tree type          ieee

Designated Root             00-e0-4f-94-b5-00
Designated Root Priority    8189
Designated Root Cost        19
Designated Root Port        2/24
Root Max Age   20 sec    Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-90-92-b0-84-00
Bridge ID Priority          32768
Bridge Max Age 20 sec    Hello Time 2  sec   Forward Delay 15 sec
```

```
Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-Method
--------- ----  -------------  -----  --------  ----------  ------------

 2/1      1     forwarding        19        32   enabled
...
```

Um zu überprüfen, ob PAgP deaktiviert ist, verwenden Sie den Befehl show port channel. Stellen Sie sicher, dass Sie die Modulnummer angeben (in diesem Fall 2), sodass der Befehl den Kanalmodus anzeigt, auch wenn kein Kanal gebildet ist. Wenn Sie Port-Channelohne Kanalbildung anzeigen, heißt es nur, dass keine Ports-Channeling ausgeführt wird. Sie möchten weitergehen und den aktuellen Channel-Modus anzeigen.

```
Switch-A (enable) show port channel
No ports channeling

Switch-A (enable) show port channel 2
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  notconnect auto      not channel
 2/2  notconnect auto      not channel
...
Switch-A (enable) set port channel 2/1-2 off
Port(s) 2/1-2 channel mode set to off.

Switch-A (enable) show port channel 2
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  off       not channel
 2/2  connected  off       not channel
...
```

Um zu überprüfen, ob die Trunking-Aushandlung deaktiviert ist, verwenden Sie den Befehl set trunk off. Sie zeigen den Standardstatus an. Dann schalten Sie Trunking auf aus und zeigen das

Ergebnis an. Geben Sie Modul 2 an, damit Sie den aktuellen Kanalmodus für die Ports in diesem Modul sehen können.

```
Switch-A (enable) show trunk 2

Port      Mode         Encapsulation  Status        Native vlan

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

 2/1      auto         negotiate      not-trunking  1

 2/2      auto         negotiate      not-trunking  1

...


Switch-A (enable) set trunk 2/1-2 off

Port(s) 2/1-2 trunk mode set to off.


Switch-A (enable) show trunk 2

Port      Mode         Encapsulation  Status        Native vlan

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

 2/1      off          negotiate      not-trunking  1

 2/2      off          negotiate      not-trunking  1
```

Außer in den seltensten Fällen ist es nicht notwendig, die automatische Geschwindigkeits-/Duplexaushandlung auszuschalten oder die Geschwindigkeit und die Duplexfunktion auf dem Switch manuell festzulegen. Ein Beispiel dafür finden Sie im Abschnitt Timing Tests With and Without DTP, PAgP und Portfast auf einem Catalyst 5000, wenn Sie es für Ihre Situation für notwendig halten.Timing-Tests mit und ohne DTP, PAgP und PortFast auf einem Catalyst 5000Dieser Test zeigt, was mit der Switch-Port-Initialisierung geschieht, wenn die verschiedenen Befehle angewendet werden. Die Standardeinstellungen des Ports werden zuerst verwendet, um einen Benchmark-Test zu erstellen. Sie haben "portfast" deaktiviert, der PAgP (EtherChannel)-Modus ist auf "auto" (Kanäle, wenn zum Kanalisieren aufgefordert wird) und der Trunking-Modus (DTP) ist auf "auto" (Trunks, wenn zum Trunk aufgefordert wird) eingestellt. Der Test schaltet dann portfast ein und misst die Zeit, dann schaltet PAgP aus und misst die Zeit, dann den Trunking aus und misst die Zeit. Schließlich schalten Sie die automatische Aushandlung aus und messen die Zeit. Alle diese Tests werden auf einem Catalyst 5000 mit einer 10/100 Fast Ethernet-Karte durchgeführt, die DTP und PAgP unterstützt.Hinweis: Wenn das Portfast aktiviert ist, ist dies nicht dasselbe wie das Deaktivieren von Spanning Tree (wie im Dokument beschrieben). Bei eingeschaltetem portfast wird Spanning Tree immer noch auf dem Port ausgeführt. Er blockiert, hört oder lernt einfach nicht und wechselt sofort in den

Weiterleitungsstatus. Die Deaktivierung von Spanning Tree wird nicht empfohlen, da sich dies auf das gesamte VLAN auswirkt und das Netzwerk anfällig für physische Topologieschleifen machen kann, was zu schwerwiegenden Netzwerkproblemen führen kann.

Switch-Version und -Konfiguration anzeigen (Version anzeigen, Modul anzeigen).

```
Switch-A (enable) show version
WS-C5505 Software, Version McpSW: 4.5(1) NmpSW: 4.5(1)
Copyright (c) 1995-1999 by Cisco Systems
NMP S/W compiled on Mar 29 1999, 16:09:01
MCP S/W compiled on Mar 29 1999, 16:06:50

System Bootstrap Version: 3.1.2

Hardware Version: 1.0  Model: WS-C5505  Serial #: 066507453

Mod Port Model      Serial #  Versions
--- ---- ---------- --------- ----------------------------------------
1   0    WS-X5530   006841805 Hw : 1.3
                               Fw : 3.1.2

                               Fw1: 3.1(2)
                               Sw : 4.5(1)
2   24   WS-X5225R  012785227 Hw : 3.2
                               Fw : 4.3(1)
                               Sw : 4.5(1)

       DRAM                    FLASH                   NVRAM
Module Total   Used    Free    Total   Used    Free    Total Used  Free
------ ------- ------- ------- ------- ------- ------- ----- ----- -----
1       32640K  13648K  18992K   8192K   4118K   4074K  512K  119K  393K

Uptime is 28 days, 18 hours, 54 minutes

Switch-A (enable) show module
Mod Module-Name         Ports Module-Type           Model    Serial-Num Status
--- ------------------- ----- --------------------- --------- --------- -------
1                       0     Supervisor III        WS-X5530  006841805 ok
2                       24    10/100BaseTX Ethernet WS-X5225R 012785227 ok

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------- -----------------
1   00-90-92-b0-84-00 to 00-90-92-b0-87-ff 1.3    3.1.2       4.5(1)
2   00-50-0f-b2-e2-60 to 00-50-0f-b2-e2-77 3.2    4.3(1)      4.5(1)

Mod Sub-Type Sub-Model Sub-Serial Sub-Hw
```

```
--- -------- --------- ---------- ------
1   NFFC     WS-F5521  0008728786 1.0
```

Stellen Sie die Protokollierung für Spanning Tree auf den ausführlichsten Punkt ein (Legen Sie die Protokollierungsebene auf Spanning Tree 7 fest). Dies ist die Standard-Protokollierungsebene (2) für Spanning Tree, d. h., dass nur kritische Situationen gemeldet werden.

```
Switch-A (enable) show logging

Logging buffer size:          500
        timestamp option:     enabled
Logging history size:         1
Logging console:              enabled
Logging server:               disabled
        server facility:      LOCAL7
        server severity:      warnings(4)

Facility            Default Severity         Current Session Severity
-------------       ------------------------ ------------------------
...
spantree            2                        2
...
0(emergencies)        1(alerts)             2(critical)
3(errors)             4(warnings)           5(notifications)
6(information)        7(debugging)
```

Die Ebene für Spanning Tree wurde in "7" (debug) geändert, sodass Sie sehen können, dass sich die Spanning Tree-Zustände am Port ändern. Diese Konfigurationsänderung dauert nur für die Terminalsitzung an und wird dann wieder normal durchgeführt.

```
Switch-A (enable) set logging level spantree 7
System logging facility <spantree for this session set to severity 7(debugging)

Switch-A (enable) show logging
...

Facility            Default Severity         Current Session Severity
-------------       ------------------------ ------------------------
...
spantree            2                        7
...
```

Beginnen Sie mit der Abschaltung des Ports am Katalysator.

```
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.
```

Jetzt die Zeit und aktivieren Sie den Port. Sie wollen sehen, wie lange es in jedem Zustand bleibt.

```
Switch-A (enable) show time
Fri Feb 25 2000, 12:20:17
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 12:20:39 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
2000 Feb 25 12:20:39 %SPANTREE-6-PORTBLK: port 2/1 state in vlan 1 changed to blocking.
2000 Feb 25 12:20:39 %SPANTREE-6-PORTLISTEN: port 2/1 state in vlane 1 changed to Listening
.
2000 Feb 25 12:20:53 %SPANTREE-6-PORTLEARN: port 2/1 state in vlan 1 changed to Learning.
2000 Feb 25 12:21:08 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 changed to forwarding.
```

Beachten Sie, dass die Ausgabe etwa 22 Sekunden (20:17 bis 20:39) dauerte, bis der Port mit der Spanning Tree-Blockierung begann. Dies war die Zeit, die zum Aushandeln der Verbindung und Durchführen von DTP- und PAgP-Aufgaben benötigt wurde. Wenn die Blockierung beginnt, befinden Sie sich jetzt im Spanning Tree-Bereich. Nachdem der Port blockiert wurde, lauschte er sofort (20:39 bis 20:39). Vom Hören bis zum Lernen dauerte es etwa 14 Sekunden (20:39 bis 20:53).

Der Lernvorgang bis zur Weiterleitung dauerte 15 Sekunden (20:53 bis 21:08). Die Gesamtzeit bis zur tatsächlichen Funktionsfähigkeit des Ports für den Datenverkehr betrug daher etwa 51 Sekunden (20:17 bis 21:08).

Hinweis: Technisch gesehen beträgt die Abhör- und die Lernphase 15 Sekunden, d. h., der Parameter für die Vorwärtsverzögerung wird für dieses VLAN festgelegt. Die Lernphase ist wahrscheinlich näher an 15 Sekunden als 14 Sekunden, wenn Sie genauere Messungen hatten. Keine der Messungen hier ist vollkommen korrekt. Sie haben gerade versucht, ein Gefühl dafür zu geben, wie lange die Dinge dauern.

Aus der Ausgabe und der Show spantreecommand wissen Sie, dass Spanning Tree auf diesem Port aktiv ist. Sehen wir uns andere Dinge an, die den Port verlangsamen könnten, wenn er den Weiterleitungsstatus erreicht. Der Befehl show port Capabilities zeigt, dass dieser Port in der Lage ist, einen Trunk zu starten und einen EtherChannel zu erstellen. Der Befehl show trunk gibt an, dass sich dieser Port im Auto-Modus befindet und dass er so eingestellt ist, dass der zu verwendende Trunking-Typ ausgehandelt wird (ISL oder 802.1q, ausgehandelt über Dynamic Trunking Protocol (DTP)).

```
Switch-A (enable) show port capabilities 2/1
Model                     WS-X5225R
Port                      2/1
Type                      10/100BaseTX
```

```
Speed                    auto,10,100
Duplex                   half,full
Trunk encap type         802.1Q,ISL
Trunk mode               on,off,desirable,auto,nonegotiate
Channel                  2/1-2,2/1-4
Broadcast suppression    percentage(0-100)
Flow control             receive-(off,on),send-(off,on)
Security                 yes
Membership               static,dynamic
Fast start               yes
Rewrite                  yes
Switch-A (enable) show trunk 2/1
Port      Mode          Encapsulation  Status        Native vlan
--------  ------------  -------------  ------------  -----------
 2/1      auto          negotiate      not-trunking  1
```

Zuerst können Sie Portfast auf dem Port aktivieren. Trunking Negotiation (DTP) befindet sich weiterhin im automatischen Modus, EtherChannel (PAgP) befindet sich weiterhin im automatischen Modus.

```
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.

Switch-A (enable) set spantree portfast 2/1 enable

Warning: Spantree port fast start should only be enabled on ports connected
to a single host.  Connecting hubs, concentrators, switches, bridges, and so on to
a fast start port can cause temporary spanning tree loops.  Use with caution.

Spantree port 2/1 fast start enabled.

Switch-A (enable) show time
Fri Feb 25 2000, 13:45:23
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
Switch-A (enable)
2000 Feb 25 13:45:43 %PAGP-5-PORTTOSTP:Port 2/1 joined bridgeport 2/1
2000 Feb 25 13:45:44 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 change to forwarding.
```

Jetzt haben Sie eine Gesamtzeit von 21 Sekunden!Es dauert 20 Sekunden, bis es der Brückengruppe beitritt (45:23 bis 45:43). Da Portfast aktiviert ist, dauert es jedoch nur eine Sekunde, bis STP mit der Weiterleitung beginnt (statt 30 Sekunden). Sie sparen 29 Sekunden, wenn Sie Portfast aktiviert haben. Versuchen Sie, die Verzögerung weiter zu reduzieren.

Jetzt schalten Sie den PAgP-Modus auf "off" (Aus). Aus dem Befehl show port channel (Port-

Kanal anzeigen) geht hervor, dass der PAgP-Modus *auf "auto" (*d. h. auf die Kanäle, wenn er von einem Nachbarn angefordert wird, der PAgP spricht) eingestellt ist. Sie müssen das Channeling für mindestens eine Gruppe von zwei Ports deaktivieren. Dies ist nicht nur für einen einzelnen Port möglich.

```
Switch-A (enable) show port channel 2/1
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  auto      not channel

Switch-A (enable) set port channel 2/1-2 off
Port(s) 2/1-2 channel mode set to off.
```

Fahren Sie den Port herunter und wiederholen Sie den Test.

```
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.

Switch-A (enable) show time
Fri Feb 25 2000, 13:56:23
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 13:56:32 %PAGP-5-PORTTOSTP:Port 2/1 joined bridgeport 2/1
2000 Feb 25 13:56:32 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 changed to forwarding.
```

Beachten Sie, dass es jetzt nur noch 9 Sekunden dauert, den Weiterleitungsstatus zu erreichen (56:23 bis 56:32), anstatt wie beim vorherigen Test 21 Sekunden. Durch das Ausschalten von PAgP aus dem Autotooff in diesem Test wurden etwa 12 Sekunden eingespart.

Schalten Sie Trunking auf aus (statt auf Auto), und prüfen Sie, wie sich dies auf die Zeit auswirkt, die der Port benötigt, um den Weiterleitungsstatus zu erreichen. Sie schalten den Port wieder aus und wieder ein und zeichnen die Zeit auf.

```
Switch-A (enable) set trunk 2/1 off
Port(s) 2/1 trunk mode set to off.
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.
```

Starten Sie den Test mit der Einstellung off für Trunking (anstatt auto).

```
Switch-A (enable) show time
Fri Feb 25 2000, 14:00:19
```

```
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 14:00:22 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
2000 Feb 25 14:00:23 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 change for forwarding.
```

Sie sparen zu Beginn ein paar Sekunden, da es nur 4 Sekunden dauerte, bis der Spanning Tree Forwarding-Status erreicht wurde (00:19 bis 00:22). Sie sparen etwa 5 Sekunden, wenn Sie den Trunking-Modus *von "autotooff"* ändern.

(Optional) Wenn das Problem in der Zeit der Switch-Port-Initialisierung bestand, muss es jetzt gelöst werden. Wenn Sie ein paar Sekunden mehr Zeit sparen müssen, können Sie die Geschwindigkeit und die Duplexfunktion des Ports manuell festlegen und keine automatische Aushandlung verwenden.

Wenn Sie die Geschwindigkeit und die Duplexfunktion auf dieser Seite manuell einstellen, müssen Sie auch die Geschwindigkeit und die Duplexfunktion auf der anderen Seite einstellen. Dies liegt daran, dass durch Festlegen der Portgeschwindigkeit und der Duplexfunktion die automatische Aushandlung am Port deaktiviert wird und das Gerät, das eine Verbindung herstellt, keine Parameter für die automatische Aushandlung sieht. Das Verbindungsgerät stellt nur eine Verbindung mit Halbduplex her, und die resultierende Duplexungleichheit führt zu schlechter Leistung und Portfehlern. Denken Sie daran: Wenn Sie Geschwindigkeit und Duplex auf einer Seite einstellen, müssen Sie auch Geschwindigkeit und Duplex auf dem Verbindungsgerät einstellen, um diese Probleme zu vermeiden.

Um den Port-Status nach dem Einstellen der Geschwindigkeit und Duplex-Doshow-Port.

```
Switch-A (enable) set port speed 2/1 100
Port(s) 2/1 speed set to 100Mbps.
Switch-A (enable) set port duplex 2/1 full
Port(s) 2/1 set to full-duplex.
Switch-A (enable) show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     connected  1          normal   full   100 10/100BaseTX
...
```

Hier die Timing-Ergebnisse:

```
Switch-A (enable) show time
Fri Feb 25 2000, 140528 Eastern
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 140529 Eastern -0500 %PAGP-5-PORTTOSTP:Port 2/1 joined bridgeport 2/1
2000 Feb 25 140530 Eastern -0500 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 changed to
forwarding.
```

Das Endergebnis gibt eine Zeit von 2 Sekunden (0528 bis 0530).

Sie haben einen weiteren visuellen Zeittest durchgeführt, indem Sie einen kontinuierlichen Ping (ping -t) gestartet haben, der an den Switch auf einem an den Switch angeschlossenen PC gerichtet ist. Anschließend haben Sie das Kabel vom Switch getrennt. Die Ping-Signale begannen zu versagen. Dann haben Sie das Kabel wieder an den Switch angeschlossen und diese Uhren überprüft, um zu sehen, wie lange es gedauert hat, bis der Switch auf die Pings vom PC reagiert hat. Es dauerte etwa 5-6 Sekunden mit Auto-Negotiation für Geschwindigkeit und Duplex eingeschaltet und etwa 4 Sekunden mit Auto-Negotiation für Geschwindigkeit und Duplex ausgeschaltet.

Es gibt viele Variablen in diesem Test (PC-Initialisierung, PC-Software, Switch-Konsolen-Port-Antworten auf Anfragen usw.), aber Sie wollten nur ein Gefühl dafür bekommen, wie lange es dauern würde, um eine Antwort aus der Sicht der PCs zu erhalten. Alle Tests wurden aus Sicht der internen Debugging-Nachricht der Switches durchgeführt.

Reduzierung der Startverzögerung beim Catalyst Switch der Serie 2900XL/3500XL

Die 2900XL- und 3500XL-Modelle können über einen Webbrowser, SNMP oder über die Kommandozeile (CLI) konfiguriert werden. verwenden Sie die Kommandozeile. Dies ist ein Beispiel, bei dem Sie den Spanning-Tree-Status eines Ports anzeigen, "portfast" aktivieren und dann überprüfen, ob dieser aktiviert ist. Der 2900XL/3500XL unterstützt zwar EtherChannel und Trunking, unterstützt jedoch nicht die dynamische EtherChannel-Erstellung (PAgP) oder dynamische Trunk-Aushandlung (DTP) in der von Ihnen getesteten Version (11.2(8.2)SA6), sodass Sie sie in diesem Test nicht deaktivieren müssen. Nachdem Sie portfast eingeschaltet haben, ist die Zeit, die der Port benötigt, bereits weniger als 1 Sekunde, sodass es nicht viel Sinn macht, die Geschwindigkeit/Duplex-Verhandlungseinstellungen zu ändern, um die Dinge zu beschleunigen. Sie hoffen, dass eine Sekunde schnell genug ist! Standardmäßig ist PortFast auf den Switch-Ports deaktiviert. Die folgenden Befehle müssen portfast aktivieren:Konfiguration

```
2900XL#conf t

2900XL(config)#interface fastEthernet 0/1

2900XL(config-if)#spanning-tree portfast

2900XL(config-if)#exit

2900XL(config)#exit

2900XL#copy run start
```

Diese Plattform ähnelt dem Router Cisco IOS; Sie müssen die Konfiguration speichern (copy run start), wenn Sie sie dauerhaft speichern möchten.VerifizierungFühren Sie den folgenden Befehl aus, um zu überprüfen, ob Portfast aktiviert ist:

```
2900XL#show spanning-tree interface fastEthernet 0/1

Interface Fa0/1 (port 13) in Spanning tree 1 is FORWARDING
```

```
   Port path cost 19, Port priority 128
   Designated root has priority 8192, address 0010.0db1.7800
   Designated bridge has priority 32768, address 0050.8039.ec40
   Designated port is 13, path cost 19
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 2105, received 1
   The port is in the portfast mode
```

Beachten der Switch-Konfiguration

```
2900XL#show running-config
Building configuration...

Current configuration:
!
version 11.2
...
!
interface VLAN1
 ip address 172.16.84.5 255.255.255.0
 no ip route-cache
!
interface FastEthernet0/1
 spanning-tree portfast
!
interface FastEthernet0/2
!
...
```

Timing-Tests auf dem Catalyst 2900XLDies sind die Zeittests für den Catalyst 2900XL.

Für diese Tests wurde auf dem 2900XL die Version 11.2(8.2)SA6 verwendet.

```
Switch#show version
Cisco Internetwork Operating System Software
Cisco IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 11.2(8.2)SA6, MAINTENANCE
INTERIM SOFTWARE
Copyright (c) 1986-1999 by cisco Systems, Inc.
```

```
Compiled Wed 23-Jun-99 16:25 by boba
Image text-base: 0x00003000, data-base: 0x00259AEC

ROM: Bootstrap program is C2900XL boot loader

Switch uptime is 1 week, 4 days, 22 hours, 5 minutes
System restarted by power-on
System image file is "flash:c2900XL-c3h2s-mz-112.8.2-SA6.bin", booted via console

cisco WS-C2924-XL (PowerPC403GA) processor (revision 0x11) with 8192K/1024K bytes of
memory.
Processor board ID 0x0E, with hardware revision 0x01
Last reset from power-on

Processor is running Enterprise Edition Software
Cluster command switch capable
Cluster member switch capable
24 Ethernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:50:80:39:EC:40
Motherboard assembly number: 73-3382-04
Power supply part number: 34-0834-01
Motherboard serial number: FAA02499G7X
Model number: WS-C2924-XL-EN
System serial number: FAA0250U03P
Configuration register is 0xF
```

Sie möchten, dass der Switch uns mitteilt, was passiert, und wann dies geschieht. Geben Sie daher die folgenden Befehle ein:

```
2900XL(config)#service timestamps debug uptime
2900XL(config)#service timestamps log uptime
2900XL#debug spantree events
Spanning Tree event debugging is on
2900XL#show debug
General spanning tree:
  Spanning Tree event debugging is on
```

Dann schaltet man den betreffenden Port aus.

```
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#interface fastEthernet 0/1
2900XL(config-if)#shut
```

```
2900XL(config-if)#
00:31:28: ST: sent Topology Change Notice on FastEthernet0/6
00:31:28: ST: FastEthernet0/1 - blocking
00:31:28: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively
down
00:31:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down
2900XL(config-if)#exit
2900XL(config)#exit
2900XL#
```

An dieser Stelle fügen Sie diese Befehle aus der Zwischenablage in den Switch ein. Diese Befehle zeigen die Uhrzeit auf dem 2900XL an und schalten den Port wieder ein:

```
show clock
conf t
int f0/1
no shut
```

Standardmäßig ist Portfast deaktiviert. Sie können es auf zwei Arten bestätigen. Der erste Weg ist, dass der Befehl show spanning-tree interface Portfast nicht erwähnt. Die zweite Möglichkeit besteht darin, sich diese Konfiguration anzusehen, die ausgeführt wird und in der der Befehl espanning-tree portfastunter der Schnittstelle nicht angezeigt wird.

```
2900XL#show spanning-tree interface fastEthernet 0/1
Interface Fa0/1 (port 13) in Spanning tree 1 is FORWARDING
   Port path cost 19, Port priority 128
   Designated root has priority 8192, address 0010.0db1.7800
   Designated bridge has priority 32768, address 0050.8039.ec40
   Designated port is 13, path cost 19
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 887, received 1
[Note: there is no message about being in portfast mode is in this spot...]

2900XL#show running-config
Building configuration...
...
!
interface FastEthernet0/1
[Note: there is no spanning-tree portfast command under this interface...]
!
```

Hier ist der erste Timing-Test mit Portfast aus.

```
2900XL#show clock
*00:27:27.632 UTC Mon Mar 1 1993
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#int f0/1
2900XL(config-if)#no shut
2900XL(config-if)#
00:27:27: ST: FastEthernet0/1 - listening
00:27:27: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
00:27:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
00:27:42: ST: FastEthernet0/1 - learning
00:27:57: ST: sent Topology Change Notice on FastEthernet0/6
00:27:57: ST: FastEthernet0/1 - forwarding
```

Die Gesamtzeit vom Herunterfahren bis zum Start der Weiterleitung durch den Port betrug 30 Sekunden (27:27 bis 27:57).

Um Portfast zu aktivieren, gehen Sie folgendermaßen vor:

```
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#interface fastEthernet 0/1
2900XL(config-if)#spanning-tree portfast
2900XL(config-if)#exit
2900XL(config)#exit
2900XL#
```

Um zu überprüfen, ob Portfast aktiviert ist, verwenden Sie den Befehl show spanning-tree interface. Beachten Sie, dass die Befehlsausgabe (am Ende) anzeigt, dass Portfast aktiviert ist.

```
2900XL#show spanning-tree interface fastEthernet 0/1
Interface Fa0/1 (port 13) in Spanning tree 1 is FORWARDING
   Port path cost 19, Port priority 128
   Designated root has priority 8192, address 0010.0db1.7800
   Designated bridge has priority 32768, address 0050.8039.ec40
   Designated port is 13, path cost 19
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 1001, received 1

The port is in the portfast mode
```

Sie können auch sehen, dass Portfast in der Konfigurationsausgabe aktiviert ist.

```
2900XL#sh  ru
Building configuration...
...
interface FastEthernet0/1
 spanning-tree portfast

...
```

Jetzt Timing-Test mit Portfast aktiviert

```
2900XL#show clock
*00:23:45.139 UTC Mon Mar 1 1993
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#int f0/1
2900XL(config-if)#no shut
2900XL(config-if)#
00:23:45: ST: FastEthernet0/1 -jump to forwarding from blocking
00:23:45: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
00:23:45: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

In diesem Fall betrug die Gesamtzeit weniger als 1 Sekunde. Wenn die Port-Initialisierungsverzögerung auf dem Switch das Problem verursacht hat, muss es von portfast behoben werden.

Denken Sie daran, dass der Switch derzeit keine Trunk-Aushandlung unterstützt und Sie ihn daher nicht deaktivieren müssen. PAgP wird auch für Trunking nicht unterstützt, sodass Sie es nicht deaktivieren müssen. Der Switch unterstützt die automatische Aushandlung von Geschwindigkeit und Duplexmodus. Da die Verzögerung jedoch so gering ist, kann sie deaktiviert werden.

auch den Ping-Test von einer Workstation zum Switch durchgeführt. Es dauerte etwa 5-6 Sekunden, bis die Antwort vom Switch einging, unabhängig davon, ob die automatische Aushandlung für Geschwindigkeit und Duplex ein- oder ausgeschaltet war.

So reduzieren Sie die Startverzögerung beim Catalyst 1900/2800 SwitchDie

1900/2820 beziehen sich auf Portfast unter einem anderen Namen: Spantree Start-Forwarding. Für die Software-Version, die Sie ausführen (V8.01.05), gelten die folgenden Standardeinstellungen: Portfast ist an den Ethernet-Ports (10 Mbit/s) aktiviert, und Portfast ist an den Fast Ethernet-Ports (Uplink) deaktiviert. Wenn Sie also die Konfiguration anzeigen, wenn ein Ethernet-Port nichts über Portfast sagt, dann ist Portfast aktiviert. Wenn in der Konfiguration "no

spantree start-forwarding" angezeigt wird, ist Portfast deaktiviert. Bei einem FastEthernet-Port (100 Mbit/s) ist das Gegenteil der Fall: Bei einem FastEthernet-Port ist Portfast nur dann aktiviert, wenn der Port in der Konfiguration "Spantree start-forward" (Spannbaum-Startweiterleitung) anzeigt.Hier ist ein Beispiel für die Einstellung von Portfast auf einem FastEthernet-Port. In diesen Beispielen wird die Enterprise Edition-Software Version 8 verwendet. Der 1900 speichert die Konfiguration automatisch, nachdem die Änderungen vorgenommen wurden. Denken Sie daran, dass Sie Portfast nicht an jedem Port aktivieren möchten, der mit einem anderen Switch oder Hub verbunden ist, nur wenn der Port mit einer Endstation verbunden ist. Die Konfiguration wird automatisch im NVRAM gespeichert.Konfiguration

```
1900#show version
Cisco Catalyst 1900/2820 Enterprise Edition Software
Version V8.01.05
Copyright (c) Cisco Systems, Inc.  1993-1998
1900 uptime is 0day(s) 01hour(s) 10minute(s) 42second(s)
cisco Catalyst 1900 (486sxl) processor with 2048K/1024K bytes of memory
Hardware board revision is 5
Upgrade Status: No upgrade currently in progress.
Config File Status: No configuration upload/download is in progress
27 Fixed Ethernet/IEEE 802.3 interface(s)
Base Ethernet Address: 00-50-50-E1-A4-80
1900#conf t
Enter configuration commands, one per line.  End with CNTL/Z
1900(config)#interface FastEthernet 0/26
1900(config-if)#spantree start-forwarding
1900(config-if)#exit
1900(config)#exit
1900#
```

VerifizierungEine Möglichkeit, um zu überprüfen, ob PortFast aktiviert ist, ist die Konfiguration. Denken Sie daran, dass ein FastEthernet-Port angeben muss, dass er eingeschaltet ist. An einem Ethernet-Port ist er aktiviert, es sei denn, die Konfiguration zeigt an, dass er deaktiviert ist. In dieser Konfiguration ist die Schnittstelle Ethernet 0/1 portfast ausgeschaltet (Sie können den Befehl zum Ausschalten sehen), die Schnittstelle Ethernet 0/2 hat portfast eingeschaltet (Sie sehen nichts - was bedeutet, dass sie eingeschaltet ist) und die Schnittstelle FastEthernet 0/26 (Port A im Menüsystem) hat portfast eingeschaltet (Sie können den Befehl zum Einschalten

sehen).

```
1900#show running-config
Building configuration...
...
!
interface Ethernet 0/1

  no spantree start-forwarding
!
interface Ethernet 0/2


!
...
!
interface FastEthernet 0/26
  spantree start-forwarding
```

Der PortFast-Status lässt sich am einfachsten über das Menüsystem anzeigen. Wenn Sie (P) für Port-Konfiguration aus dem Hauptmenü wählen und dann Port wählen, zeigt die Ausgabe an, ob Port Fast Mode aktiviert ist. Diese Ausgabe ist für Port FastEthernet 0/26, also Port "A" auf diesem Switch.

```
        Catalyst 1900 - Port A Configuration

        Built-in 100Base-FX
        802.1d STP State:  Blocking     Forward Transitions:  0

    ---------------------- Settings ----------------------------------------
     [D] Description/name of port
     [S] Status of port                          Suspended-no-linkbeat
     [I] Port priority (spanning tree)           128 (80 hex)
     [C] Path cost (spanning tree)               10
     [H] Port fast mode (spanning tree)          Enabled
     [E] Enhanced congestion control             Disabled
     [F] Full duplex / Flow control              Half-Duplex
```

```
---------------------- Related Menus ----------------------------------

 [A] Port addressing            [V] View port statistics

 [N] Next port                  [G] Goto port

 [P] Previous port              [X] Exit to Main Menu


Enter Selection:
```

Timing-Tests auf dem Catalyst 1900

Die Zeitwerte sind auf einem 1900/2820 wegen des Fehlens von Debugging-Tools schwieriger zu überprüfen, sodass Sie gerade einen Ping von einem PC gestartet haben, der mit dem Switch verbunden ist, der an den Switch selbst gerichtet ist. Sie haben das Kabel getrennt und dann wieder angeschlossen und aufgezeichnet, wie lange es gedauert hat, bis der Switch mit Portfast an und mit Portfast aus auf den Ping reagiert hat. Für einen Ethernet-Port mit eingeschaltetem PortFast (Standardstatus) erhielt der PC innerhalb von 5-6 Sekunden eine Antwort. Mit Portfast aus dem PC erhielt eine Antwort in 34-35 Sekunden.

Ein zusätzlicher Vorteil für Portfast

Es gibt einen weiteren Spanning Tree-bezogenen Vorteil für die Verwendung von Portfast in Ihrem Netzwerk. Jedes Mal, wenn ein Link aktiv wird und in den Weiterleitungsstatus in Spanning Tree wechselt, sendet der Switch ein spezielles Spanning Tree-Paket, die Topology Change Notification (TCN). Die TCN-Benachrichtigung wird an den Root des Spanning Tree übergeben, wo sie an alle Switches im VLAN propagiert wird. Dies bewirkt, dass alle Switches ihre MAC-Adresstabelle mit dem Parameter für die Vorwärtsverzögerung veralten. Der Parameter für die Vorwärtsverzögerung wird normalerweise auf 15 Sekunden festgelegt. Jedes Mal, wenn eine Workstation der Bridge-Gruppe beitritt, werden die MAC-Adressen auf allen Switches nach 15 Sekunden veraltet anstatt nach den normalen 300 Sekunden.Da eine aktive Workstation die Topologie für alle Switches im VLAN nicht wesentlich ändert, müssen diese nicht die schnell alternde TCN-Phase durchlaufen. Wenn Sie PortFast aktivieren, sendet der Switch keine TCN-Pakete, wenn ein Port aktiv wird.

Befehle zum Überprüfen der Konfiguration

Dies ist eine Liste der Befehle, die Sie verwenden müssen, wenn Sie überprüfen, ob die Konfiguration funktioniert.4000/5000/6000

show port spantree 2/1- prüfen, ob "Fast-Start" (Portfast) aktiviert oder deaktiviert ist

show spantree 1 - alle Ports in VLAN 1 anzeigen, falls "Fast-Start" aktiviert ist

show port channel: Überprüfen, ob aktive Kanäle vorhanden sind

show port channel 2 - see the channel mode (auto, off, and so on) for each port on module 2

show trunk 2 - Anzeigen des Trunk-Modus (automatisch, aus usw.) für jeden Port auf Modul 2

show port - Anzeige des Status (verbunden, keine Verbindung usw.), der Geschwindigkeit und des Duplexmodus für alle Ports am Switch

2900XL/3500XL

show spanning-tree interface FastEthernet 0/1- to see if Portfast is enabled on this port (no note of Portfast means that it is not enabled)

show running-config: Wenn ein Port den Befehl "spanning-tree portfast" anzeigt, ist "Portfast" aktiviert.

1900/2800

show running-config - um die aktuellen Einstellungen anzuzeigen (einige Befehle sind unsichtbar, wenn sie die Standardeinstellungen des Switches darstellen)

Verwenden Sie das Menüsystem zum Bildschirm "Port Status".

Befehle zur Fehlerbehebung bei der KonfigurationDies ist eine Liste der Befehle, die zur Fehlerbehebung bei der Konfiguration verwendet werden müssen.4000/5000/6000

show port spantree 2/1- prüfen, ob "Fast-Start" (Portfast) aktiviert oder deaktiviert ist

show spantree 1 - alle Ports in VLAN 1 anzeigen, falls "Fast-Start" aktiviert ist

show port channel: Überprüfen, ob aktive Kanäle vorhanden sind

show port channel 2 - see the channel mode (auto, off, and so on) for each port on module 2

show trunk 2 - Anzeigen des Trunk-Modus (automatisch, aus usw.) für jeden Port auf Modul 2

show port - Anzeige von Status (verbunden, Verbindung nicht herstellen, eingeschaltet), Geschwindigkeit und Duplexmodus für alle Ports am Switch

show logging - Hier erfahren Sie, welche Art von Meldungen die Protokollierungsausgabe generieren.

set logging level spantree 7- setzt den Switch auf die Protokollierung des Spanning-Tree-Ports, zeigt Echtzeit auf der Konsole an

set port disable 2/1- schaltet den Port in der Software aus (wie "shutdown" auf dem Router)

set port enable 2/1- port in software einschalten (wie "no shutdown" auf dem router)

show time - Zeigt die aktuelle Zeit in Sekunden an (wird zu Beginn eines Zeittests verwendet)

Anzeigen von Port-Funktionen - Implementieren von Funktionen am Port

set trunk 2/1 off - set the trunking mode to off (to speed port initialization time)

set port channel 2/1-2 off- set the EtherChannel (PAgP) mode to off (to speed port initialization time)

Port-Geschwindigkeit auf 2/1 oder 100 einstellen- Port auf 100 Mbit/s einstellen und Auto-Negotiation deaktivieren

Port-Duplex 2/1 voll einstellen - Port-Duplex auf voll stellen

2900XL/3500XL

service timestamps debug uptime- Zeigt die Zeit mit den Debug-Meldungen an.

service timestamps log uptime- Zeigt die Zeit mit den Logmeldungen

debug spantree events - Zeigt an, wann der Port die Spanning Tree-Phasen durchläuft

show clock - zur Anzeige der aktuellen Uhrzeit (für die Zeittests)

show spanning-tree interface FastEthernet 0/1- to see if Portfast is enabled on this port (no note of Portfast means that it is not enabled)

Abschalten - Einen Port von der Software abschalten

kein Herunterfahren - Port über Software einschalten

1900/2800

show running-config - um die aktuellen Einstellungen anzuzeigen (einige Befehle sind unsichtbar, wenn sie die Standardeinstellungen des Switches darstellen)

Konfiguration und Fehlerbehebung für IP Multilayer Switching (MLS)Ziele

In diesem Dokument wird die Fehlerbehebung für Multilayer Switching (MLS) für IP beschrieben. Diese Funktion hat sich zu einer sehr erwünschten Methode entwickelt, um die Routing-Leistung durch den Einsatz dedizierter ASICs (Application Specific Integrated Circuits) zu

beschleunigen. Herkömmliches Routing erfolgt über eine zentrale CPU und Software; MLS lagert einen wesentlichen Teil des Routings (Paketumschreibung) an die Hardware aus und wird auch als Switching bezeichnet. MLS und Layer-3-Switching sind gleichwertige Begriffe. Die NetFlow-Funktion von Cisco IOS ist separat und wird in diesem Dokument nicht behandelt. MLS bietet auch Unterstützung für IPX (IPX MLS) und Multicasting (MPLS). Der Schwerpunkt dieses Dokuments liegt jedoch ausschließlich auf der Fehlerbehebung bei MLS IP.EinleitungJe höher die Anforderungen an Netzwerke sind, desto höher ist der Bedarf an höherer Leistung. Immer mehr PCs sind mit LANs, WANs und dem Internet verbunden, und ihre Benutzer benötigen schnellen Zugriff auf Datenbanken, Dateien/Webseiten, Netzwerkanwendungen, andere PCs und Video-Streaming. Um Verbindungen schnell und zuverlässig zu halten, müssen Netzwerke in der Lage sein, sich schnell an Veränderungen und Ausfälle anzupassen und den besten Weg zu finden, während sie für Endbenutzer so unsichtbar wie möglich bleiben. Endbenutzer, die bei minimaler Netzwerkverzögerung einen schnellen Informationsfluss zwischen ihrem PC und Server erleben, sind zufrieden. Die Bestimmung des besten Pfads ist die primäre Funktion von Routing-Protokollen. Dies kann ein CPU-intensiver Prozess sein; eine erhebliche Leistungssteigerung wird erzielt, indem ein Teil dieser Funktion an Switching-Hardware ausgelagert wird. Dies ist der Punkt der MLS-Funktion.Es gibt drei Hauptkomponenten von MLS: zwei davon sind MLS-RP und MLS-SE. Der MLS-RP ist der MLS-fähige Router, der die traditionelle Funktion des Routings zwischen Subnetzen/VLANs ausführt. Der MLS-SE ist ein MLS-fähiger Switch, für den normalerweise ein Router für das Routing zwischen Subnetzen/VLANs erforderlich ist, der jedoch mit spezieller Hardware und Software das Umschreiben des Pakets verarbeiten kann. Wenn ein Paket eine geroutete Schnittstelle passiert, werden Nicht-Daten-Teile des Pakets geändert (neu geschrieben), während es an sein Ziel übertragen wird, Hop für Hop. Hierbei kann es zu Verwirrung kommen, da ein Layer-2-Gerät eine Layer-3-Aufgabe übernimmt. Tatsächlich schreibt der Switch nur Layer-3-Informationen um und wechselt zwischen Subnetzen/VLANs. Der Router ist weiterhin für standardbasierte Routenberechnungen und die Bestimmung des besten Pfades verantwortlich. Ein Großteil dieser Verwirrung kann vermieden werden, wenn Sie die Routing- und Switching-Funktionen mental getrennt halten, insbesondere wenn sie, wie es häufig der Fall ist, im gleichen Chassis (wie bei einem internen MLS-RP) enthalten sind. Stellen Sie sich MLS als eine viel komplexere Methode vor, den Router im Cache zu speichern, wobei der Cache vom Router eines Switches getrennt bleibt. Sowohl der MLS-RP als auch der MLS-SE werden zusammen mit den jeweiligen Hard- und Software-Minima für MLS benötigt.Der MLS-RP kann intern (in einem Switch-Chassis installiert) oder extern (über ein Kabel mit einem Trunk-Port am Switch verbunden) sein. Beispiele für interne MLS-RPs sind das Route-Switch-Modul (RSM) und die Route-Switch Feature Card (RSFC), die jeweils in einem Steckplatz oder Supervisor eines

Mitglieds der Catalyst 5xxx-Familie installiert sind; dasselbe gilt für die Multilayer Switch Feature Card (MSFC) für die Catalyst 6xxx-Familie. Beispiele für externe MLS-RPs sind Cisco Router der Serien 7500, 7200, 4700, 4500 oder 3600. Zur Unterstützung der MLS IP-Funktion benötigen alle MLS-RPs generell eine Cisco IOS-Mindestversion in den 11.3WA- oder 12.0WA-Zügen. Weitere Informationen finden Sie in der Release-Dokumentation. Außerdem muss MLS aktiviert sein, damit ein Router ein MLS-RP sein kann.Der MLS-SE ist ein Switch mit spezieller Hardware. Für ein Mitglied der Catalyst 5xxx-Produktfamilie erfordert MLS, dass der Supervisor eine NetFlow Feature Card (NFC) installiert hat; die Supervisor IIG und IIIG haben standardmäßig eine. Darüber hinaus ist nur ein Minimum an Catalyst OS 4.1.1-Software erforderlich. Beachten Sie, dass der 4.x-Zug entweder die allgemeine Bereitstellung (General Deployment, GD) hinter sich hat oder rigorose Endbenutzer-Kriterien und Zielvorgaben für ein verbessertes Anwendererlebnis erfüllt hat. Die neuesten Versionen finden Sie auf der Cisco Website. IP MLS wird unterstützt und automatisch für Catalyst 6xxx Hardware und Software mit MSFC/PFC aktiviert (bei anderen Routern ist MLS standardmäßig deaktiviert). Beachten Sie, dass IPX MLS und MLS für Multicasting unterschiedliche Hardware- und Softwareanforderungen haben können (Cisco IOS und Catalyst OS). Mehr Cisco Plattformen unterstützen die MLS-Funktion. Außerdem muss MLS aktiviert sein, damit ein Switch eine MLS-SE sein kann.Die dritte Hauptkomponente von MLS ist das Multilayer Switching Protocol (MLSP). Dies liegt daran, dass wenn Sie die Grundlagen von MLSP verstehen, Sie das Herz von MLS erhalten, und dies ist wesentlich, um effektiv zu beheben das MLS. Der MLSP wird vom MLS-RP und der MLS-SE für die Kommunikation untereinander genutzt; es handelt sich um Aufgaben, die MLS aktivieren und Flüsse installieren, aktualisieren oder löschen (Cache-Informationen) sowie die Verwaltung und den Export der Flow-Statistiken (NetFlow Data Export wird in anderen Dokumentationen behandelt). Mit MLSP kann der MLS-SE außerdem die MAC-Adressen (Media Access Control, Layer 2) der MLS-fähigen Router-Schnittstellen abrufen, die Flussmaske des MLS-RP überprüfen (weiter unten in diesem Dokument erläutert) und bestätigen, dass der MLS-RP betriebsbereit ist. Der MLS-RP sendet alle 15 Sekunden Multicast-Hello-Pakete mit dem MLSP. Wenn drei dieser Intervalle verpasst werden, erkennt der MLS-SE, dass der MLS-RP ausgefallen ist oder die Verbindung zum MLS-RP unterbrochen wurde.

Das Diagramm zeigt drei grundlegende Schritte, die (mit MLSP) ausgeführt werden müssen, damit eine Verknüpfung erstellt werden kann: den Kandidaten, den Enabler und die Zwischenspeicherungsschritte. Der MLS-SE prüft auf einen zwischengespeicherten MLS-Eintrag. Wenn der MLS-Cache-Eintrag und die Paketinformationen übereinstimmen (ein Treffer), wird der Header des Pakets lokal auf dem Switch neu geschrieben (eine Verknüpfung oder ein Bypass des

Routers), anstatt wie üblich an den Router gesendet zu werden. Pakete, die nicht übereinstimmen und an den MLS-RP gesendet werden, sind potenzielle Pakete, d. h. es besteht die Möglichkeit, sie lokal zu vermitteln. Nachdem das Kandidatenpaket die MLS-Flussmaske durchlaufen hat (was in einem Abschnitt weiter unten erläutert wird) und die im Header des Pakets enthaltenen Informationen neu geschrieben wurden (der Datenabschnitt wird nicht berührt), sendet der Router das Paket entlang des Zielpfads zum nächsten Hop. Das Paket wird jetzt als Enabler-Paket bezeichnet. Wenn das Paket zu derselben MLS-SE zurückkehrt, von der es verlassen wurde, wird eine MLS-Verknüpfung erstellt und in den MLS-Cache eingefügt; das Umschreiben für dieses Paket und alle ähnlichen Pakete, die sie verfolgen (ein so genannter Flow), erfolgt nun lokal durch Switch-Hardware statt durch Router-Software.Dieselbe MLS-SE muss sowohl die Kandidaten- als auch die Aktivierungspakete für einen bestimmten Flow anzeigen, damit eine MLS-Verknüpfung erstellt werden kann (dies ist der Grund für die Netzwerktopologie) ist wichtig für MLS). Vergessen Sie nicht, dass der Zweck von MLS darin besteht, den Kommunikationspfad zwischen zwei Geräten in verschiedenen VLANs, die über denselben Switch verbunden sind, zu ermöglichen, den Router zu umgehen und die Netzwerkleistung zu verbessern.Durch die Verwendung der Flussmaske (im Wesentlichen eine Zugriffsliste) kann der Administrator den Ähnlichkeitsgrad dieser Pakete und den Umfang der Flüsse anpassen: Zieladresse, Ziel- und Quelladresse oder Ziel-, Quell- und Layer-4-Informationen. Beachten Sie, dass das erste Paket eines Datenflusses immer den Router durchläuft; von da an wird lokal geswitcht. Jeder Datenfluss ist unidirektional; für die Kommunikation zwischen PCs müssen beispielsweise zwei Verknüpfungen eingerichtet und verwendet werden. Der Hauptzweck von MLSP besteht darin, diese Tastenkombinationen einzurichten, zu erstellen und zu verwalten.Diese drei Komponenten (MLS-RP, MLS-SE und MLSP) geben wichtige Router-Ressourcen frei, wenn andere Netzwerkkomponenten einige ihrer Funktionen übernehmen können. Je nach Topologie und Konfiguration bietet MLS eine einfache und äußerst effektive Methode zur Steigerung der Netzwerkleistung im LAN.## Fehlerbehebung bei IP MLS-TechnologieEin Flussdiagramm zur Fehlerbehebung bei grundlegenden IP MLS-Funktionen wird erläutert. Es leitet sich von den gebräuchlichsten MLS-IP-Falltypen ab, die mit der Cisco Website für technischen Support geöffnet wurden und bis zur Erstellung dieses Dokuments von den Benutzern und Technikern des technischen Supports bearbeitet wurden. MLS ist eine robuste Funktion, und Sie dürfen keine Probleme damit haben; wenn ein Problem auftritt, hilft Ihnen dies, die Arten von IP MLS-Problemen zu lösen, mit denen Sie am wahrscheinlichsten konfrontiert sind. Es werden einige grundlegende Annahmen getroffen:

- Sie sind mit den grundlegenden Konfigurationsschritten vertraut, die zur Aktivierung von IP MLS auf dem Router und den Switches erforderlich sind, und haben folgende Schritte durchgeführt: Ausgezeichnetes Material finden Sie in den am Ende dieses Dokuments aufgeführten Ressourcen.

Das IP-Routing ist auf dem MLS-RP aktiviert (standardmäßig ist es aktiviert): Wenn der Befehl no ip routing in der globalen Konfiguration von ashow run angezeigt wird, wurde er deaktiviert, und IP MLS funktioniert nicht.

Zwischen MLS-RP und MLS-SE besteht eine IP-Verbindung: Senden Sie einen Ping an die IP-Adressen des Routers vom Switch, und suchen Sie nach Ausrufezeichen (sog. "bangs"), die im Gegenzug angezeigt werden.

Die MLS-RP-Schnittstellen befinden sich auf dem Router im Status "up/up": Geben Sie zur Bestätigung "typeshow ip interface" auf dem Router ein.

Warnung: Wenn Sie Konfigurationsänderungen an einem Router vornehmen, der permanent sein soll, denken Sie daran, diese Änderungen mit acopy running-config start-config (gekürzte Versionen dieses Befehls enthalten copy run startandwr mem) zu speichern. Konfigurationsänderungen gehen verloren, wenn der Router neu geladen oder zurückgesetzt wird. RSM, RSFC und MSFC sind Router, keine Switches. Im Gegensatz dazu werden Änderungen, die an der Switch-Eingabeaufforderung eines Mitglieds der Catalyst 5xxx- oder 6xxx-Produktfamilie vorgenommen werden, automatisch gespeichert.

In diesem Abschnitt werden Fehler bei der IP MLS-Technologie behoben.

Sind die Mindestanforderungen an Hardware und Software erfüllt?

Führen Sie ein Upgrade von MLS-RP und SE durch, um die Mindestanforderungen an Software und Hardware zu erfüllen. Für den MLS-RP ist keine zusätzliche Hardware erforderlich. Obwohl MLS auf nicht-gebündelten Schnittstellen konfiguriert werden kann, erfolgt die Verbindung zum MLS-SE in der Regel über VLAN-Schnittstellen (wie bei einem RSM) oder unterstützt Trunking (kann so konfiguriert werden, dass mehrere VLAN-Informationen übertragen werden, indem ISL oder 802.1q konfiguriert werden). Beachten Sie außerdem, dass zum Zeitpunkt der Veröffentlichung nur Mitglieder der Routerfamilien 7500, 7200, 4700, 4500 und 3600 MLS extern unterstützen. Derzeit können nur diese externen Router und die Router, die in die Catalyst 5xxx- oder 6xxx-Switch-Produktfamilien passen (wie RSM und RSFC für die Catalyst 5xxx-Produktfamilie und MSFC für die Catalyst 6xxx-Produktfamilie), MLS-RPs sein. Für die MSFC ist auch die Policy Feature Card (PFC) erforderlich, die beide auf dem Catalyst 6xx Supervisor installiert sind. IP MLS ist jetzt eine Standardfunktion der Router-Software Cisco IOS 12.0 und höher. Für eine Cisco IOS-Software mit einer niedrigeren Version als Cisco IOS 12.0 ist in der Regel ein spezieller Zug erforderlich. Installieren Sie für eine solche IP MLS-Unterstützung die neuesten Images in Cisco IOS 11.3, die die Buchstaben "WA" in den Dateinamen enthalten.

Für MLS-SE ist eine NetFlow Feature Card (NFFC) für ein Mitglied der Catalyst 5xxx Produktfamilie erforderlich. Diese Karte wird im Supervisor-Modul des Catalyst Switches installiert und ist standardmäßig in neueren Supervisor-Lösungen der Catalyst 5xxx Serie enthalten (d. h. seit 1999). Der NFFC wird von den Supervisoren I oder II nicht unterstützt und ist eine Option für frühe Supervisor IIIs. Außerdem ist mindestens 4.1.1 CatOS für IP MLS erforderlich. Im Gegensatz dazu wird für die Catalyst 6xxx-Familie die erforderliche Hardware standardmäßig mitgeliefert. IP MLS wird seit der ersten CatOS-Softwareversion 5.1.1 unterstützt (tatsächlich ist IP MLS eine grundlegende und standardmäßige

Komponente für seine hohe Leistung). Bei neuen Plattformen und Software, die IP MLS unterstützen, ist es wichtig, die Dokumentation und die Versionshinweise zu überprüfen und generell die neueste Version im niedrigsten Zug zu installieren, der Ihren Funktionsanforderungen entspricht. Lesen Sie die Versionshinweise, und wenden Sie sich an Ihre örtliche Vertriebsniederlassung bei Cisco, um Informationen zu neuen MLS-Support- und Funktionsentwicklungen zu erhalten.

Befehle zur Überprüfung der installierten Hardware und Software werden auf dem Router und auf dem Switch angezeigt.

Hinweis: Die Catalyst Switches der Serie 6xxx unterstützen derzeit KEINE externen MLS-RPs. Beim MLS-RP muss es sich um eine MSFC handeln.

Befinden sich die Quell- und Zielgeräte in verschiedenen VLANs derselben MLS-SE und nutzen einen gemeinsamen MLS-RP?

Eine grundlegende Topologieanforderung von MLS ist, dass der Router über einen Pfad zu jedem der VLANs verfügt. Denken Sie daran, dass der Zweck von MLS darin besteht, eine Verknüpfung zwischen zwei VLANs zu erstellen, sodass das Routing zwischen den beiden Endgeräten vom Switch durchgeführt werden kann. Dadurch wird der Router für andere Aufgaben frei. Der Switch routet nicht; er schreibt die Frames neu, sodass es für die Endgeräte den Anschein hat, dass sie durch den Router kommunizieren. Befinden sich die beiden Geräte im selben VLAN, schaltet das MLS-SE den Frame lokal ohne Verwendung von MLS, wie dies bei Switches in einer transparent überbrückten Umgebung der Fall ist, und es wird keine MLS-Verknüpfung erstellt. Es können mehrere Switches und Router im Netzwerk und sogar mehrere Switches entlang des Datenflusspfads vorhanden sein. Der Pfad zwischen den beiden Endgeräten, für die eine MLS-Verknüpfung gewünscht wird, muss jedoch einen einzigen MLS-RP in diesem VLAN für diesen Pfad enthalten. Mit anderen Worten: Der Fluss von der Quelle zum Ziel muss eine VLAN-Grenze auf demselben MLS-RP überschreiten, und ein Kandidaten- und Enabler-Paketpaar muss von demselben MLS-SE erkannt werden, damit die MLS-Verknüpfung erstellt werden kann. Wenn diese Kriterien nicht erfüllt sind, wird das Paket normal geroutet, ohne MLS zu verwenden. Schauen Sie sich die am Ende dieses Dokuments vorgeschlagenen Dokumente an, um Diagramme und Diskussionen zu unterstützten und nicht unterstützten Netzwerktopologien zu erhalten.

Enthält MLS-RP anmls rp ipstatement sowohl in der globalen als auch in der Schnittstellenkonfiguration?

Wenn keine vorhanden ist, geben Sie admls rp ipstatements auf dem MLS-RP entsprechend ein. Mit Ausnahme von Routern, für die IP MLS automatisch aktiviert wird (wie bei der Catalyst 6xxx MSFC), ist dies ein erforderlicher Konfigurationsschritt. Bei den meisten MLS-RPs (für IP MLS konfigurierte Router) muss diese Anweisung sowohl in der globalen Konfiguration als auch in der Schnittstellenkonfiguration angezeigt werden.

Hinweis: Denken Sie beim Konfigurieren des MLS-RP auch daran, den Befehl rp management-interface unter eine der zugehörigen IP-MLS-Schnittstellen zu platzieren. Dieser erforderliche Schritt teilt dem MLS-RP mit, von welcher Schnittstelle es MLSP-Nachrichten senden muss, um mit dem MLS-SE zu kommunizieren. Auch hier ist es notwendig, diesen Befehl nur unter einer Schnittstelle zu platzieren.

Sind auf dem MLS-RP irgendwelche Funktionen konfiguriert, die MLS auf dieser Schnittstelle automatisch deaktivieren?

Es gibt mehrere Konfigurationsoptionen auf dem Router, die nicht mit MLS kompatibel sind. Dazu gehören IP-Accounting, Verschlüsselung, Komprimierung, IP-Sicherheit, Network Address Translation (NAT) und Committed Access Rate (CAR). Weitere Informationen finden Sie unter den Links zur IP MLS-Konfiguration am Ende dieses Dokuments. Pakete, die eine mit diesen Funktionen konfigurierte Router-Schnittstelle durchlaufen, müssen normal weitergeleitet werden. Es wird keine MLS-Verknüpfung erstellt. Damit MLS funktioniert, deaktivieren Sie diese Funktionen auf der MLS-RP-Schnittstelle.

Ein weiteres wichtiges Merkmal, das MLS beeinflusst, sind Zugriffslisten, sowohl Eingabe als auch Ausgabe. Weitere Informationen zu dieser Option finden Sie unter "Flussmasken".

Erkennt die MLS-SE die MLS-RP-Adresse?

Damit MLS funktioniert, muss der Switch den Router als MLS-RP erkennen. Interne MLS-RPs (RSM oder RSFC in einem Mitglied der Catalyst 5xxx-Produktfamilie und MSFC in einem Mitglied der Catalyst 6xxx-Produktfamilie) werden automatisch vom MLS-SE erkannt, in dem sie installiert sind. Bei externen MLS-RPs muss der Switch explizit über die Adresse des Routers informiert werden. Bei dieser Adresse handelt es sich nicht um eine IP-Adresse, obwohl sie auf externen MLS-RPs aus der Liste der IP-Adressen ausgewählt wird, die auf den Schnittstellen des Routers konfiguriert wurden. Es handelt sich lediglich um eine Router-ID. Tatsächlich ist die MLS-ID für interne MLS-RPs normalerweise nicht einmal eine auf dem Router konfigurierte IP-Adresse; da interne MLS-RPs automatisch eingeschlossen werden, handelt es sich in der Regel um eine Loopback-Adresse (127.0.0.x). Damit MLS funktioniert, muss auf der MLS-SE die MLS-ID angegeben werden, die auf dem MLS-RP vorhanden ist.

Verwendet mls auf den Router, um die MLS-ID zu finden. Konfigurieren Sie diese ID dann auf dem Switch mit dem Befehl set mls include <MLS-ID>. Dies ist ein erforderlicher Konfigurationsschritt, wenn Sie externe MLS-RPs verwenden.

Hinweis: Wenn Sie die IP-Adresse von MLS-RP-Schnittstellen ändern und den Router dann neu laden, kann dies dazu führen, dass der MLS-Prozess auf dem Router eine neue MLS-ID auswählt. Diese neue MLS-ID kann sich von der MLS-ID unterscheiden, die manuell in die MLS-SE aufgenommen wurde, was dazu führen kann, dass MLS beendet wird. Dies ist kein Softwarefehler, sondern eine Auswirkung des Schalters, der versucht, mit einer nicht mehr gültigen MLS-ID zu kommunizieren. Schließen Sie diese neue MLS-ID unbedingt an den Switch an, damit das MLS wieder funktioniert. Möglicherweise muss auch IP MLS deaktiviert/aktiviert werden.

Hinweis: Wenn die MLS-SE nicht wie bei dieser Topologie direkt mit dem MLS-RP verbunden ist, kann die Adresse, die in der MLS-SE enthalten sein muss, als die genannte Loopback-Adresse erscheinen: ein zwischen MLS-SE und MLS-RP geschalteter Switch. Sie müssen die MLS-ID angeben, auch wenn der MLS-RP intern ist. Für den zweiten Switch erscheint der MLS-RP als externer Router, da MLS-RP und MLS-SE nicht im gleichen Chassis enthalten sind.

Befinden sich die MLS-RP-Schnittstelle und die MLS-SE in derselben aktivierten VTP-Domäne?

Für MLS müssen sich die MLS-Komponenten zusammen mit den Endstationen in derselben VTP-Domäne (Virtual Trunking Protocol) befinden. VTP ist ein Layer-2-Protokoll, das zur Verwaltung von VLANs auf mehreren Catalyst Switches über einen zentralen Switch verwendet wird. Mit dieser Funktion kann ein Administrator ein VLAN auf allen Switches in einer Domäne erstellen oder löschen, was nicht für jeden Switch in dieser Domäne

erforderlich ist. Das Multilayer Switching Protocol (MLSP), über das MLS-SE und MLS-RP miteinander kommunizieren, überschreitet keine VTP-Domänengrenze. Wenn der Netzwerkadministrator VTP auf den Switches aktiviert hat (VTP ist standardmäßig für Catalyst 5xxx- und 6xxx-Familienmitglieder aktiviert), verwenden Sie den Befehl how vtp domainauf dem Switch, um zu erfahren, in welcher VTP-Domäne das MLS-SE platziert wurde. Mit Ausnahme von Catalyst 6xxx MSFC, bei dem MLS im Wesentlichen eine *aplug-and*-play-Funktion ist, müssen Sie als Nächstes die VTP-Domäne zu jeder der MLS-Schnittstellen des Routers hinzufügen. Dadurch können sich MLSP-Multicasts zwischen MLS-RP und MLS-SE bewegen und MLS funktioniert.

Geben Sie im Schnittstellenkonfigurationsmodus von MLS-RP die folgenden Befehle ein:

no mls rp ipDisable MLS auf der betroffenen MLS-RP-Schnittstelle, bevor Sie die VTP-Domäne ändern.

mls rp vtp-domain < VTP domain name>Der VTP-Domänenname auf jeder MLS-fähigen Schnittstelle muss mit dem des Switches übereinstimmen.

mls rp vlan-id <VLAN #>Nur erforderlich für nicht ISL-basiertes Trunking, externe MLS-RP-Schnittstellen.

mls rp management-interfaceFühren Sie dies für nur eine Schnittstelle des MLS-RP aus. Dieser erforderliche Schritt teilt dem MLS-RP mit, von welcher Schnittstelle aus er MLSP-Nachrichten senden muss.

mls rp ipAktivieren Sie MLS erneut auf der Schnittstelle des MLS-RP.

Um den VTP-Domänennamen des MLS-SE zu ändern, verwenden Sie diesen Befehl an der Switch-CatOS-Aktivierungsaufforderung:

set vtp domain name <VTP-Domänenname>

Damit MLS funktioniert, stellen Sie sicher, dass VTP auf dem Switch aktiviert ist:

VTP-Aktivierung festlegen

Stimmen die Strömungsmasken auf MLS-RP und MLS-SE zu?

Eine Flussmaske ist ein von einem Netzwerkadministrator konfigurierter Filter, der von MLS verwendet wird, um zu bestimmen, ob eine Verknüpfung erstellt werden muss. Wie bei einer Zugriffsliste gilt: Je detaillierter die von Ihnen festgelegten Kriterien sind, desto tiefer muss der MLS-Prozess in das Paket eindringen, um zu überprüfen, ob das Paket diese Kriterien erfüllt. Um den Umfang der MLS-erzeugten Verknüpfungen einzustellen, kann die Strömungsmaske mehr oder weniger spezifisch ausgebildet sein; die Strömungsmaske ist im Wesentlichen eine Abstimmeinrichtung. Es gibt drei Arten von IP MLS-Modi: Ziel-IP, Ziel-Quelle-IP und Vollfluss-IP. Der Standard-IP-Zielmodus wird verwendet, wenn keine Zugriffsliste auf die MLS-fähige Schnittstelle des Routers angewendet wird. Der Source-Destination-IP-Modus wird verwendet, wenn eine Standard-Zugriffsliste angewendet wird. Full-Flow-IP ist für eine erweiterte Zugriffsliste aktiviert. Der MLS-Modus auf dem MLS-RP wird implizit durch den Typ der Zugriffsliste bestimmt, die auf die Schnittstelle angewendet wird. Der MLS-Modus auf der MLS-SE ist dagegen explizit konfiguriert. Wenn der entsprechende Modus gewählt wird, kann der Benutzer MLS so konfigurieren, dass nur die Zieladresse übereinstimmen muss, damit eine MLS-Verknüpfung oder sowohl Quell- als auch Zieladresse oder sogar Layer-4-Informationen wie TCP/UDP-Portnummern erstellt

werden können.

Der MLS-Modus kann sowohl auf dem MLS-RP als auch auf dem MLS-SE konfiguriert werden und muss im Allgemeinen übereinstimmen. Wenn entweder der Source-Destination-IP- oder der Full-Flow-IP MLS-Modus als erforderlich angesehen wird, empfiehlt es sich, ihn auf dem Router zu konfigurieren und die entsprechende Zugriffsliste anzuwenden. MLS wählt immer die spezifischste Maske aus. Sie gibt der im MLS-RP konfigurierten Maske Vorrang vor der im MLS-SE konfigurierten Maske. ACHTEN Sie DARAUF, wenn Sie den MLS-Modus des Switches von der Standard-Ziel-IP-Adresse ändern: Sie müssen sicherstellen, dass dieser mit dem MLS-Modus auf dem Router übereinstimmt, damit MLS funktioniert. Bei den Modi "source-destination-ip" und "full-flow-ip" muss die Zugriffsliste auf die entsprechende Router-Schnittstelle angewendet werden. Wenn keine Zugriffsliste angewendet wird, ist der MLS-Modus nur "destination-ip" (Standard), selbst wenn er konfiguriert ist.

Warnung: Bei jeder Änderung der Flussmaske, ob im MLS-RP oder MLS-SE, werden alle zwischengespeicherten MLS-Flüsse gelöscht, und der MLS-Prozess wird neu gestartet. Eine Bereinigung kann auch erfolgen, wenn Sie den BefehlClear ip route-cache auf den Router anwenden. Wenn Sie den Befehl für die globale Routerkonfiguration no ip routing anwenden, der das IP-Routing deaktiviert und den Router im Wesentlichen in eine transparente Bridge umwandelt, wird MLS gelöscht und deaktiviert (beachten Sie, dass das Routing eine Voraussetzung für MLS ist). Jede dieser Komponenten kann die Router-Leistung in einem Produktionsnetzwerk vorübergehend, aber erheblich beeinträchtigen. Die Last des Routers nimmt stark zu, bis die neuen Verknüpfungen erstellt werden, da er nun alle Datenflüsse verarbeiten muss, die zuvor vom Switch verarbeitet wurden.

Hinweis: Insbesondere bei einem Mitglied der Catalyst 5000-Familie als MLS-SE müssen Sie den sehr breiten Einsatz von FlowMasks vermeiden, die mit Layer-4-Informationen konfiguriert sind. Wenn der Router gezwungen ist, einen so tiefen Peer zu jedem Paket an der Schnittstelle zu bilden, werden viele der beabsichtigten Vorteile von MLS umgangen. Wenn Sie ein Mitglied der Catalyst 6xxx-Familie als MLS-SE verwenden, ist dies ein weitaus geringeres Problem, da die Switch-Ports selbst Layer-4-Informationen erkennen können.

Hinweis: Bis vor Kurzem unterstützte MLS keine in MLS-RPs eingehende, sondern ausgehende FlowMasks. Wenn Sie zusätzlich zu den normalen MLS-RP-Konfigurationsbefehlen auf einer Router-Schnittstelle den Befehl mls rp ip input-aclcommand verwenden, wird eine eingehende Flussmaske unterstützt.

Werden auf dem Switch mehr als ein paar *MLSTooo viele* Fehlermeldungen zu *movesangezeigt*?

Wie in der Anmerkung erwähnt, wird zum Ändern einer Flussmaske entweder der Routen-Cache gelöscht oder das IP-Routing global deaktiviert, um den Cache zu löschen. Andere Umstände können ebenfalls zu vollständigen oder zu vielen einzelnen Eintragsbereinigungen führen und MLS veranlassen, sich über *zu viele Züge* zu beschweren. Es gibt verschiedene Formen dieser Nachricht, aber jede enthält diese drei Wörter. Abgesehen von den bereits erwähnten Punkten besteht die häufigste Ursache für diesen Fehler darin, dass der Switch mehrere identische MAC-Adressen (Ethernet Media Access Control) innerhalb desselben VLAN empfängt. Ethernet-Standards lassen identische MAC-Adressen innerhalb desselben VLAN nicht zu. Wenn sie selten oder nur einige Male hintereinander auftauchen, gibt es keinen Grund zur Sorge. MLS ist eine robuste Funktion, und die Meldung kann einfach durch normale Netzwerkereignisse verursacht werden, wie z. B. eine PC-Verbindung, die zwischen Ports verschoben wird. Wenn sie mehrere Minuten lang andauernd beobachtet wird, ist sie

wahrscheinlich ein Symptom für ein ernsteres Problem.

Wenn eine solche Situation eintritt, liegt die Ursache in der Regel darin, dass zwei Geräte mit derselben MAC-Adresse tatsächlich mit einem VLAN oder einem physischen Loop innerhalb des VLAN verbunden sind (oder mehrere VLANs, wenn diese Broadcast-Domänen überbrückt werden). Fehlerbehebung mit Spanning-Tree (in anderen Dokumenten beschrieben) und dem Tipp, die Schleife zu finden und zu beseitigen. Außerdem können schnelle Topologieänderungen zu temporärer Instabilität des Netzwerks (und MLS) führen (Flapping-Router-Schnittstellen, fehlerhafte Netzwerkkarten usw.).

Tipp: Verwenden Sie die Befehle show mls notification und show looktable auf dem Switch, um Sie in Richtung der duplizierten MAC-Adresse oder des physischen Loops zu verweisen. Die erste liefert einen TA-Wert. Der Befehl show looktable <TA-Wert> gibt eine mögliche MAC-Adresse zurück, die auf die Ursache des Problems zurückgeführt werden kann.

Zugehörige Informationen

Inhalt

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.