Häufige Ursachen für langsame Intra-VLAN- und Inter-VLAN-Verbindungen in Campus Switch-Netzwerken

Inhalt

Einführung

Dieses Dokument behandelt die häufigsten Probleme, die zu einer Verlangsamung des Netzwerks beitragen können. In diesem Dokument werden häufige Symptome einer Netzwerkverlangsamung klassifiziert und Ansätze zur Problemdiagnose und -behebung skizziert.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

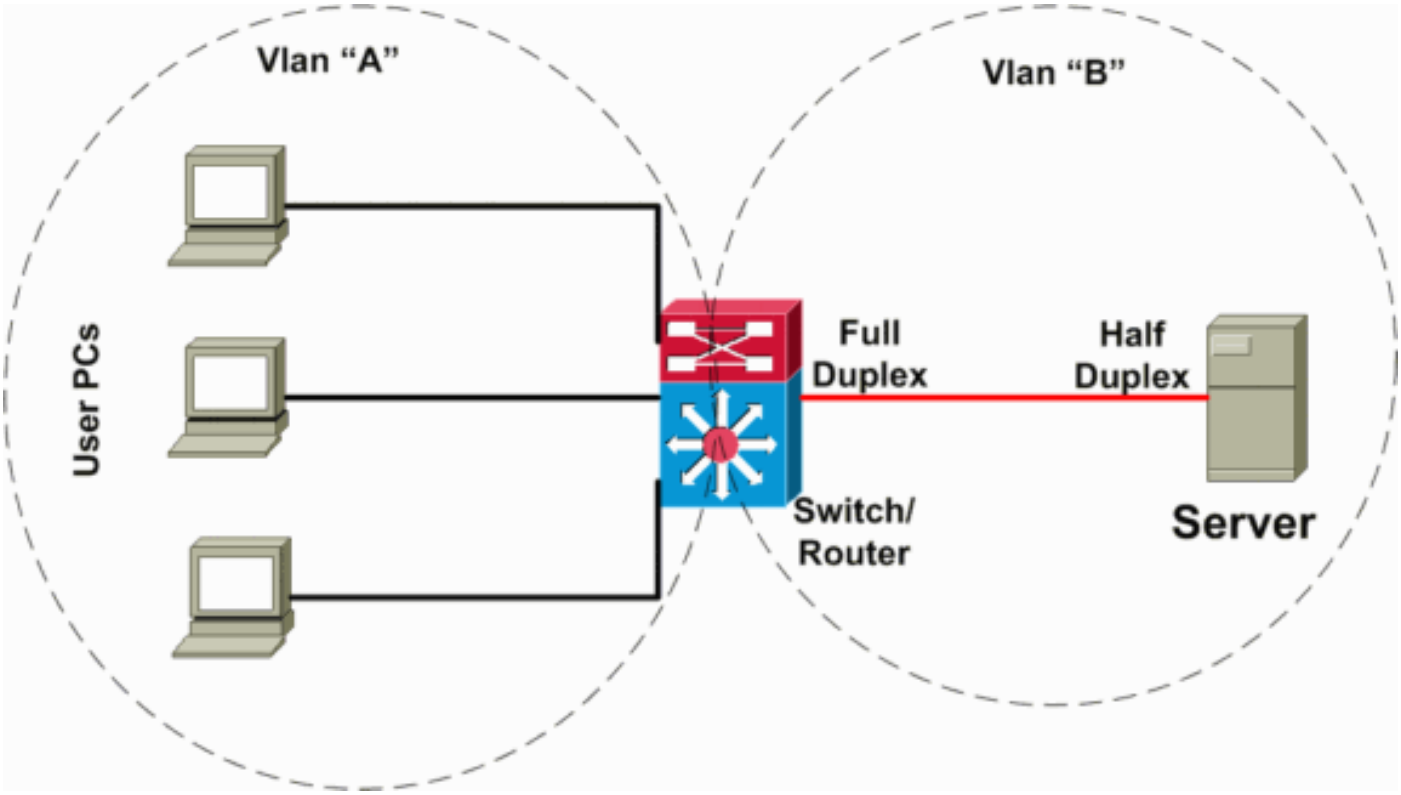
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Häufige Ursachen für langsame Intra-VLAN- und Inter-VLAN-Verbindungen

Die Symptome einer langsamen Verbindung in einem VLAN können durch mehrere Faktoren auf verschiedenen Netzwerkebenen verursacht werden. In der Regel tritt das Problem mit der Netzwerkgeschwindigkeit auf einer niedrigeren Ebene auf, aber die Symptome können auf einer höheren Ebene beobachtet werden, da sich das Problem unter dem Begriff "langsames VLAN" verschleiert. Zur Klarstellung: In diesem Dokument werden die folgenden neuen Begriffe definiert: "langsame Kollisionsdomäne", "langsame Broadcast-Domäne" (d. h. langsame VLANs) und "langsame VLAN-Weiterleitung". Diese werden im Abschnitt Drei Kategorien von Ursachen definiert, unten.

Im folgenden Szenario (unten im Netzwerkdiagramm dargestellt) ist ein Layer-3-Switch (L3) vorhanden, der Inter-VLAN-Routing zwischen den Server- und Client-VLANs durchführt. In diesem Fehlerszenario ist ein Server mit einem Switch verbunden, und der Port-Duplexmodus wird auf Serverseite für Halbduplex und auf Switch-Seite für Vollduplex konfiguriert. Diese Fehlkonfiguration führt zu Paketverlusten und Verlangsamung, mit einem erhöhten Paketverlust, wenn auf der Verbindung mit dem Server höhere Datenverkehrsraten auftreten. Für die Clients, die mit diesem Server kommunizieren, sieht das Problem wie eine langsame VLAN-Weiterleitung aus, da sie kein Problem bei der Kommunikation mit anderen Geräten oder Clients im selben VLAN haben. Das Problem tritt nur bei der Kommunikation mit dem Server in einem anderen VLAN auf. Das Problem trat also in einer einzelnen Kollisionsdomäne auf, wird jedoch als langsame VLAN-übergreifende Weiterleitung angesehen.



Drei Kategorien von Ursachen

Die Ursachen der Verlangsamung lassen sich in drei Kategorien unterteilen:

Langsame Kollisionsdomänenanbindung

Kollisionsdomäne ist definiert als verbundene Geräte, die in einer Halbduplex-Portkonfiguration konfiguriert und miteinander oder mit einem Hub verbunden sind. Wenn ein Gerät an einen Switch-Port angeschlossen und der Vollduplex-Modus konfiguriert ist, ist eine solche Punkt-zu-Punkt-Verbindung kollisionslos. Langsamkeit in einem solchen Segment kann immer noch aus unterschiedlichen Gründen auftreten.

Langsame Broadcast-Domänenverbindung (langsames VLAN)

Eine langsame Broadcast-Domänenverbindung tritt auf, wenn das gesamte VLAN (d. h. alle Geräte im selben VLAN) langsam arbeitet.

Langsame VLAN-übergreifende Verbindungen (langsame Weiterleitung zwischen VLANs)

Eine langsame VLAN-Verbindung (langsame Weiterleitung zwischen VLANs) tritt auf, wenn das lokale VLAN nicht langsam funktioniert, der Datenverkehr jedoch an ein anderes VLAN weitergeleitet werden muss und nicht mit der erwarteten Geschwindigkeit weitergeleitet wird.

Ursachen für Netzwerkverzögerung

Paketverlust

In den meisten Fällen wird ein Netzwerk als langsam angesehen, wenn Protokolle höherer Schichten (Anwendungen) längere Zeit benötigen, um einen Vorgang abzuschließen, der in der Regel schneller ausgeführt wird. Diese Verlangsamung wird durch den Verlust einiger Pakete im Netzwerk verursacht, wodurch Protokolle auf höherer Ebene wie TCP oder Anwendungen das Zeitlimit überschreiten und eine erneute Übertragung initiieren.

Probleme mit der Hardware-Weiterleitung

Bei einer anderen Art von Verlangsamung, verursacht durch Netzwerkgeräte, erfolgt die Weiterleitung (ob Layer 2 [L2] oder L3) langsam. Dies liegt an einer Abweichung vom normalen (geplanten) Betrieb und dem Wechsel zur langsamen Pfadweiterleitung. Ein Beispiel hierfür ist, dass Multilayer Switching (MLS) auf dem Switch L3-Pakete zwischen VLANs in der Hardware weiterleitet. Aufgrund von Konfigurationsfehlern funktioniert MLS jedoch nicht ordnungsgemäß, und die Weiterleitung erfolgt durch den Router in der Software (wodurch die Weiterleitungsrate zwischen VLANs erheblich sinkt).

Fehlerbehebung

Fehlerbehebung bei Problemen mit Kollisionsdomänen

Wenn Ihr VLAN also langsam zu sein scheint, isolieren Sie zunächst die Probleme der Kollisionsdomäne. Sie müssen festlegen, ob nur Benutzer in derselben Kollisionsdomäne Verbindungsprobleme haben oder ob diese auf mehreren Domänen stattfinden. Führen Sie dazu eine Datenübertragung zwischen Benutzer-PCs in derselben Kollisionsdomäne durch, und vergleichen Sie diese Leistung mit der Leistung einer anderen Kollisionsdomäne oder mit der erwarteten Leistung.

Wenn Probleme nur in dieser Kollisionsdomäne auftreten und die Leistung anderer

Kollisionsdomänen im gleichen VLAN normal ist, sehen Sie sich die Port-Zähler am Switch an, um festzustellen, welche Probleme bei diesem Segment auftreten können. Höchstwahrscheinlich ist die Ursache einfach, z. B. eine Duplexungleichheit. Eine weitere, weniger häufige Ursache ist ein überladenes oder überbelegtes Segment. Weitere Informationen zur Behebung von Problemen in einem Segment finden Sie im Dokument Konfiguration und Fehlerbehebung bei Ethernet 10/100/1000MB Half/Vollduplex Auto-Negotiation.

Wenn Benutzer in verschiedenen Kollisionsdomänen (aber im selben VLAN) dieselben Leistungsprobleme haben, kann dies dennoch durch eine Duplexungleichheit in einem oder mehreren Ethernet-Segmenten zwischen Quelle und Ziel verursacht werden. Das folgende Szenario tritt häufig auf: Ein Switch wird manuell so konfiguriert, dass er an allen Ports im VLAN Vollduplex aufweist (die Standardeinstellung ist "auto"), während die mit den Ports verbundenen Benutzer (NICs) ein Verfahren zur automatischen Aushandlung ausführen. Dies führt zu Duplex-Diskrepanzen an allen Ports und damit zu schlechter Leistung an jedem Port (Kollisionsdomäne). Obwohl es so aussieht, als ob das gesamte VLAN (Broadcast-Domäne) ein Leistungsproblem aufweist, wird es für die Kollisionsdomäne jedes Ports immer noch als Duplex-Diskrepanz kategorisiert.

Ein anderer zu berücksichtigender Fall ist ein bestimmtes Problem mit der NIC-Leistung. Wenn eine Netzwerkkarte mit einem Leistungsproblem mit einem gemeinsam genutzten Segment verbunden ist, kann es vorkommen, dass ein ganzes Segment langsam ist, insbesondere wenn die Netzwerkkarte zu einem Server gehört, der auch andere Segmente oder VLANs bedient. Behalten Sie diesen Fall im Auge, da er Sie während der Fehlerbehebung irreführen kann. Auch hier besteht die beste Möglichkeit, dieses Problem einzugrenzen, darin, eine Datenübertragung zwischen zwei Hosts desselben Segments durchzuführen (wo die Netzwerkkarte mit dem angeblichen Problem verbunden ist), oder wenn sich nur die Netzwerkkarte an diesem Port befindet, ist die Isolierung nicht einfach. Versuchen Sie also, eine andere Netzwerkkarte in diesem Host zu verwenden, oder versuchen Sie, den verdächtigen Host an einem separaten Port anzuschließen, um die richtige Konfiguration des Ports und der Netzwerkkarte sicherzustellen.

Wenn das Problem weiterhin besteht, versuchen Sie, den Switch-Port zu beheben. Weitere Informationen finden Sie im Dokument Fehlerbehebung bei Switch-Port- und Schnittstellenproblemen.

Der schwerwiegendste Fall ist, wenn einige oder alle inkompatiblen NICs mit einem Cisco Switch verbunden sind. In diesem Fall scheint der Switch Leistungsprobleme zu haben. Informationen zur Überprüfung der Kompatibilität der NICs mit Cisco Switches finden Sie im Dokument Troubleshooting Cisco Catalyst Switches to NIC Compatibility Issues.

Sie müssen zwischen den ersten beiden Fällen (Behebung von Kollisionsdomänenverlangsamung und VLAN-Langsamkeit) unterscheiden, da diese beiden Ursachen unterschiedliche Domänen betreffen. Bei langsamer Kollisionsdomäne liegt das Problem entweder außerhalb des Switches (oder am Switch-Edge, an einem Switch-Port) oder außerhalb des Switches. Es kann sein, dass das Segment allein Probleme hat (z. B. ein überbelegtes Segment, das die Segmentlänge überschreitet, physische Probleme im Segment oder Hub/Repeater-Probleme). Bei langsamem VLAN liegt das Problem höchstwahrscheinlich im Switch (oder mehreren Switches). Wenn Sie das Problem falsch diagnostizieren, verschwenden Sie möglicherweise Zeit, um an der falschen Stelle nach dem Problem zu suchen.

Nachdem Sie ein Ticket diagnostiziert haben, überprüfen Sie die unten aufgeführten Punkte.

Bei einem gemeinsam genutzten Segment:

- Bestimmen, ob das Segment überlastet oder überbelegt ist
- Bestimmen Sie, ob das Segment gesund ist (einschließlich der korrekten Kabellänge, der normalen Dämpfung und der physischen Beschädigung des Mediums).
- Bestimmen Sie, ob der Netzwerkport und alle mit einem Segment verbundenen NICs kompatible Einstellungen aufweisen.
- Stellen Sie fest, ob die Netzwerkkarte gut funktioniert (und führen Sie den neuesten Treiber aus).
- Bestimmen Sie, ob der Netzwerk-Port weiterhin zunehmende Fehler aufweist.
- Bestimmen Sie, ob der Netzwerk-Port überladen ist (insbesondere wenn es sich um einen Server-Port handelt).

Bei einem gemeinsamen Point-to-Point-Segment oder einem kollisionslosen (Vollduplex) Segment:

- Bestimmen der Port- und NIC-kompatiblen Konfiguration
- den Zustand des Segments bestimmen
- Bestimmen der Integrität der Netzwerkkarte
- Suchen Sie nach Fehlern am Netzwerkport oder nach Überbelegung.

Fehlerbehebung: langsames Intra-VLAN (Broadcast-Domäne)

Nachdem Sie überprüft haben, dass keine Duplexungleichheit oder Kollisionsdomänenprobleme vorliegen, wie im obigen Abschnitt erläutert, können Sie jetzt die IntraVLAN-Langsamkeit beheben. Der nächste Schritt bei der Isolierung des Standorts der Verlangsamung ist die Durchführung einer Datenübertragung zwischen Hosts im gleichen VLAN (aber auf unterschiedlichen Ports). d. h. auf unterschiedlichen Kollisionsdomänen) und vergleicht die Leistung mit den gleichen Tests in alternativen VLANs.

Folgendes kann langsame VLANs verursachen:

- Verkehrsschleife
- überladenes oder überbelegtes VLAN
- Überlastung des In-Band-Pfads des Switches
- Switch-Management-Prozessor mit hoher CPU-Auslastung
- Eingangsfehler auf einem Cut-Through-Switch
- [1] Software- oder Hardware-Fehlkonfiguration
- [1] Software-Bugs
- [1] Hardwareprobleme

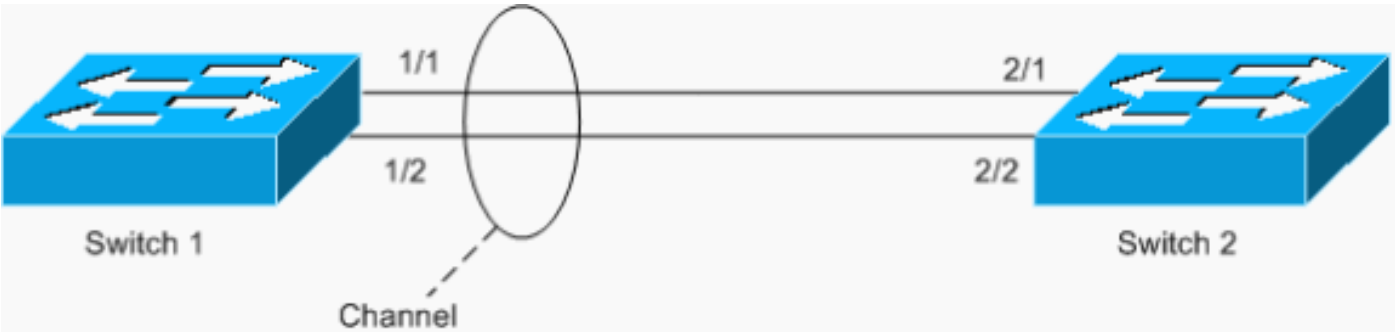
[1]Diese drei Ursachen einer langsamen Intra-VLAN-Verbindung gehen über den Rahmen dieses Dokuments hinaus und erfordern unter Umständen eine Fehlerbehebung durch einen Techniker der technischen Unterstützung von Cisco. Nachdem Sie die ersten fünf möglichen Ursachen aus der Liste oben ausgeschlossen haben, müssen Sie möglicherweise eine Serviceanfrage beim technischen Support von Cisco stellen.

Datenverkehrsschleife

Eine Datenverkehrsschleife ist die häufigste Ursache eines langsamen VLAN. Neben einer Schleife sollten Sie weitere Symptome sehen, die darauf hindeuten, dass Sie eine Schleife durchlaufen. Informationen zur Fehlerbehebung bei STP-Schleifen (Spanning Tree Protocol) finden Sie im Dokument Spanning Tree Protocol Problems and Related Design Considerations.

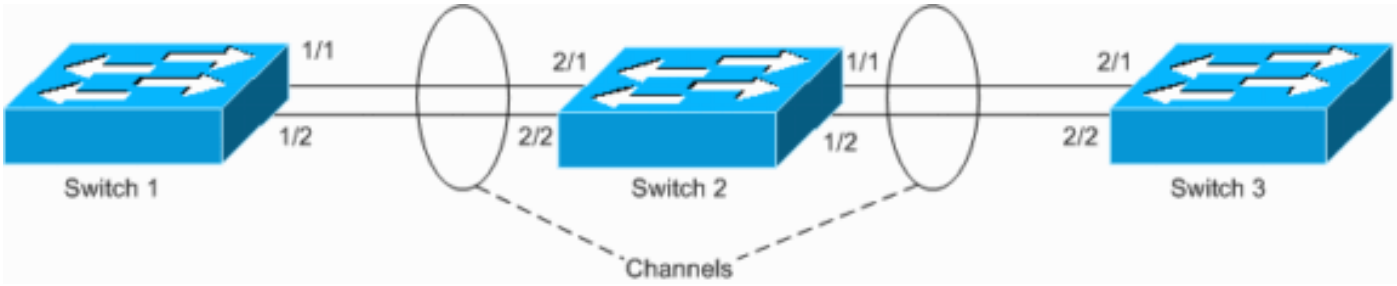
Obwohl leistungsstarke Switches (wie der Cisco Catalyst 6500/6000) mit Gigabit-fähigen Backplanes einige (STP)-Schleifen ohne Beeinträchtigung der Leistung der Management-CPU bewältigen können, können Looped-Pakete dazu führen, dass NICs in den Eingangspuffern überlaufen und Rx/Tx-Puffer (Rx/Tx) auf den Switches empfangen und die Performance beeinträchtigen.

Ein weiteres Beispiel für die Schleife ist ein asymmetrisch konfigurierter EtherChannel, wie im folgenden Szenario gezeigt:



In diesem Beispiel befinden sich die Ports 1/1 und 1/2 im Kanal, die Ports 2/1 und 2/2 jedoch nicht.

Switch 1 verfügt über einen konfigurierten Kanal (erzwungener Kanal) und Switch 2 über keine Kanalkonfiguration für die entsprechenden Ports. Wenn gefluteter Datenverkehr (mcast/bcast/unknown unicast) von Switch 1 zu Switch 2 fließt, wird er von Switch 2 zurück in den Kanal geschaltet. Es handelt sich nicht um eine vollständige Schleife, da der Datenverkehr nicht fortlaufend Schleifen durchläuft, sondern nur einmal reflektiert wird. Es ist die Hälfte der Gesamtschleife. Wenn Sie zwei derartige Fehlkonfigurationen haben, kann eine vollständige Schleife erstellt werden, wie im Beispiel unten gezeigt.



Die Gefahr einer solchen Fehlkonfiguration besteht darin, dass MAC-Adressen auf falschen Ports erfasst werden, da der Datenverkehr falsch umgeschaltet wird, was zu Paketverlusten führt. Beispiel: Ein Router mit aktivem Hot Standby Router Protocol (HSRP), der mit Switch 1 verbunden ist (wie im obigen Diagramm gezeigt). Nachdem der Router Pakete gesendet hat, wird seine MAC-Adresse von Switch 2 zurückgeleitet und von Switch 1 vom Kanal abgefragt, bis erneut ein Unicast-Paket vom Router gesendet wird.

Überladenes oder überbelegtes VLAN

Achten Sie darauf, dass an einem beliebigen Ort Ihrer VLANs Engpässe (überbelegte Segmente) auftreten, und suchen Sie diese. Das erste Zeichen, dass Ihr VLAN überlastet ist, ist, wenn Rx- oder Tx-Puffer an einem Port überbelegt sind. Wenn Sie an einigen Ports Auskarten oder Indiscards sehen, überprüfen Sie, ob diese Ports überladen sind. (Eine Erhöhung der Anzahl an Indiscards deutet nicht nur auf einen vollen Rx-Puffer hin.) In Catalyst OS (CatOS) sind nützliche Befehle zur Ausgabe **show mac** *mod/port* **oder show top [***N***]**. In der Cisco IOS® Software (Nativ)

können Sie den Befehl **show interfaces** *slot#/port#* **counter errors** (**Anzeigeschnittstellen-***Steckplatzhalter* für Zähler) ausgeben, um Rückwürfe anzuzeigen. Das überladene oder überbelegte VLAN-Szenario und das Datenverkehrsschleifenszenario begleiten sich häufig gegenseitig, können aber auch separat existieren.

Häufig tritt eine Überlastung an den Backbone-Ports auf, wenn die aggregierte Bandbreite des Datenverkehrs unterschätzt wird. Um dieses Problem zu umgehen, müssen Sie am besten einen EtherChannel zwischen den Geräten konfigurieren, für die die Ports blockiert sind. Wenn das Netzwerksegment bereits ein Kanal ist, fügen Sie einer Kanalgruppe weitere Ports hinzu, um die Kanalkapazität zu erhöhen.

Beachten Sie auch das Problem mit der Polarisation von Cisco Express Forwarding (CEF). Dieses Problem tritt in Netzwerken auf, in denen der Datenverkehr durch die Router ausgeglichen wird. Aufgrund der einheitlichen Algorithmen von Cisco Express Forwarding wird der gesamte Datenverkehr jedoch polarisiert und auf dem nächsten Hop nicht Load Balancing ausgeführt. Dieses Problem tritt jedoch nicht häufig auf, da eine bestimmte Topologie mit L3-Links mit Lastausgleich erforderlich ist. Weitere Informationen zur Cisco Express-Weiterleitung und zum Lastenausgleich finden Sie unter Problembehebung bei Unicast IP Routing mit CEF auf Catalyst Switches der Serien 6500/6000 mit Supervisor Engine 2 und unter Ausführen der CatOS-Systemsoftware.

Eine weitere Ursache für das überladene VLAN ist ein asymmetrisches Routing-Problem. Diese Art der Konfiguration kann auch dazu führen, dass Ihre VLANs durch zu hohen Datenverkehr überflutet werden. Weitere Informationen finden Sie in *Ursache 1:* Abschnitt *"Asymmetric Routing"* im Dokument "Unicast Flooding in Switched Campus Networks".

Manchmal kann ein Engpass auch ein Netzwerkgerät selbst sein. Wenn Sie beispielsweise versuchen, 4-Gigabit-Datenverkehr über den Switch mit einer 3-Gigabit-Backplane zu pumpen, führt dies zu einem dramatischen Datenverkehrsverlust. Das Verständnis der Netzwerkswitch-Architektur wird in diesem Dokument nicht behandelt. Beachten Sie jedoch bei der Beurteilung der Kapazität eines Netzwerk-Switches die folgenden Aspekte:

- Backplane-Kapazität
- Head-of-Line-Blockierungsprobleme
- blockierende und nicht blockierende Switch/Port-Architektur

Überlastung des Switch-In-Band-Pfads

Engpässe im In-Band-Pfad des Switches können zu einer Spanning Tree-Schleife oder anderen Instabilitäten im Netzwerk führen. Der In-Band-Port eines Cisco Switches ist ein virtueller Port, der eine Schnittstelle für den Verwaltungsdatenverkehr (z. B. Cisco Discovery Protocol und Port Aggregation Protocol [PAgP]) zum Managementprozessor bereitstellt. Der In-Band-Port wird als virtuell angesehen, da er in einigen Architekturen vom Benutzer nicht angezeigt wird und die In-Band-Funktionen mit dem normalen Port-Betrieb kombiniert werden. Beispielsweise ist die SC0-Schnittstelle der Switches der Serien Catalyst 4000, Catalyst 5000 und Catalyst 6500/6000 (mit CatOS) eine Teilmenge des In-Band-Ports. Die Schnittstelle SC0 stellt nur einen IP-Stack für den Managementprozessor innerhalb des konfigurierten VLAN bereit, während der In-Band-Port Zugriff auf den Managementprozessor für Bridge Protocol Data Units (BPDUs) in einem der konfigurierten VLANs und für viele andere Managementprotokolle (wie Cisco Discovery Protocol, Internet Group Management Protocol [IGMP], Cisco Group Management Protocol und Dynamic Trunking Protocol [DTP]) bietet.

Wenn der In-Band-Port überlastet wird (aufgrund einer falsch konfigurierten Anwendung oder des Benutzerdatenverkehrs), kann dies zu Instabilität aller Protokolle führen, für die die Protokollstatusstabilität auf regulären Nachrichten oder empfangenen "hellos" beruht. Dieser Zustand kann zu temporären Schleifen, Schnittstellen-Flapping und anderen Problemen führen, die diese Art von Langsamkeit verursachen.

Es ist schwierig, eine Überlastung des In-Band-Ports am Switch zu verursachen, obwohl böswillig gebildete DoS-Angriffe (Denial of Service) erfolgreich sein können. Es gibt keine Möglichkeit, den Datenverkehr am In-Band-Port zu begrenzen oder zu reduzieren. Eine Lösung erfordert Eingriffe und Analysen des Switch-Administrators. In-Band-Ports tolerieren im Allgemeinen eine hohe Überlastungstoleranz. Selten funktioniert der Inband-Port-Fehler oder bleibt in Rx- oder Tx-Richtung hängen. Dies würde schwerwiegende Hardwareausfälle verursachen und den gesamten Switch beeinträchtigen. Diese Bedingung ist schwer zu erkennen und wird in der Regel von Technikern des technischen Supports von Cisco diagnostiziert. Die Symptome sind, dass ein Switch plötzlich "taub" wird und keinen Steuerungsdatenverkehr mehr sieht, wie z. B. Updates des Nachbarn Cisco Discovery Protocol. Dies weist auf ein Rx-In-Band-Problem hin. (Wenn jedoch nur ein Nachbar des Cisco Discovery Protocol angezeigt wird, können Sie sicher sein, dass die In-Band-Funktion funktioniert.) Wenn also alle angeschlossenen Switches das Cisco Discovery Protocol von einem einzigen Switch (sowie alle anderen Management-Protokolle) verlieren, weist dies auf Tx-Probleme über die In-Band-Schnittstelle dieses Switches hin.

Switch-Management-Prozessor Hohe CPU-Auslastung

Wenn ein In-Band-Pfad überlastet wird, kann dies dazu führen, dass ein Switch hohe CPU-Bedingungen aufweist. Und da die CPU diesen unnötigen Datenverkehr verarbeitet, verschlechtert sich die Situation. Wenn eine hohe CPU-Auslastung durch einen überlasteten In-Band-Pfad oder ein anderes Problem verursacht wird, kann dies die Managementprotokolle wie im Abschnitt Überlastung auf dem Switch-In-Band-Pfad beschrieben beeinflussen.

Betrachten Sie die Management-CPU im Allgemeinen als einen verwundbaren Punkt jedes Switches. Ein korrekt konfigurierter Switch reduziert das Risiko von Problemen, die durch eine hohe CPU-Auslastung verursacht werden.

Die Architektur der Supervisor Engines I und II der Catalyst Switches der Serie 4000 ist so konzipiert, dass die Management-CPU in den Switching-Overhead eingebunden ist. Beachten Sie Folgendes:

- CPU programmiert ein Switch-Fabric, wenn ein neuer Pfad (die Supervisor Engine I und II sind Pfadbasiert) in den Switch eingeht. Wenn ein In-Band-Port überladen wird, wird ein neuer Pfad verworfen. Dies führt zu Paketverlusten (stille Rückwürfe) und Verlangsamung bei Protokollen höherer Schichten, wenn der Datenverkehr zwischen Ports umgeschaltet wird. (Siehe Abschnitt Überlastung auf In-Band-Pfad des Switches, oben.)
- Da die CPU teilweise Switching in der Supervisor Engine I und II durchführt, können hohe CPU-Bedingungen die Switching-Funktionen des Catalyst 4000 beeinträchtigen. Die hohe CPU-Auslastung der Supervisor Engines I und II kann durch den Switching-Overhead selbst verursacht werden.

Die Supervisor Engines II+, III und IV der Catalyst 4500/4000-Serie sind recht verkehrstolerant, aber das Lernen von MAC-Adressen in der Cisco IOS Software-basierten Supervisor Engine wird noch immer vollständig in der Software (durch die Management-CPU) durchgeführt. Es besteht die Möglichkeit, dass eine hohe CPU-Auslastung diesen Prozess beeinträchtigen und zu Verlangsamung führen kann. Wie bei den Supervisor Engines I und II kann auch bei den

Supervisor Engines II+, III und IV eine hohe CPU-Auslastung durch massives Lernen oder erneutes Lernen von MAC-Adressen entstehen.

Die CPU ist auch in die MAC-Lernfunktion der Catalyst Switches der Serien 3500XL und 2900XL involviert, sodass ein Prozess, der zu einer schnellen Adresserneuerung führt, die CPU-Leistung beeinflusst.

Der MAC-Adresserlernprozess (auch wenn er vollständig in der Hardware implementiert ist) ist im Vergleich zu einem Switching-Prozess relativ langsam. Wenn eine kontinuierlich hohe Rate an MAC-Adressen-erneuten Lernvorgängen besteht, muss die Ursache gefunden und beseitigt werden. Eine Spanning-Tree-Schleife im Netzwerk kann dazu führen, dass diese Art von MAC-Adressen neu gelernt wird. Das Umlernen von MAC-Adressen (oder Flapping von MAC-Adressen) kann auch durch Switches von Drittanbietern verursacht werden, die Port-basierte VLANs implementieren. Das bedeutet, dass MAC-Adressen nicht mit einem VLAN-Tag verknüpft werden. Wenn diese Switches in bestimmten Konfigurationen mit Cisco Switches verbunden sind, kann es zu MAC-Leaking zwischen VLANs kommen. Dies kann wiederum zu einer hohen Rate von MAC-Adressen-erneuten Lernvorgängen führen und die Leistung beeinträchtigen.

Eingehend-Fehler auf einem Cut-Through-Switch

Die Verbreitung von Cut-Through-Eingangs-Fehlerpaketen hängt mit der Slow Collision Domain Connectivity zusammen, aber da die Fehlerpakete an ein anderes Segment übertragen werden, scheint das Problem das Umschalten zwischen Segmenten zu sein. Cut-Through-Switches (z. B. die Catalyst Campus Switch Router der Serie 8500 und das Catalyst 2948G-L3- oder L3-Switching-Modul für die Catalyst Serie 4000) beginnen Paket-/Frame-Switching, sobald der Switch genügend Informationen vom Lesen des L2/L3-Headers des Pakets hat, um das Paket an den Zielport oder den Zielport weiterzuleiten Ports. Während das Paket also zwischen Eingangs- und Ausgangs-Ports umgeschaltet wird, wird der Anfang des Pakets bereits über den Ausgangsport weitergeleitet, während der Rest des Pakets weiterhin vom Eingangsport empfangen wird. Was passiert, wenn das Eingangssegment nicht gesund ist und einen CRC-Fehler (zyklische Redundanzprüfung) oder einen Runt-Fehler generiert? Der Switch erkennt dies nur, wenn er das Ende des Frames empfängt und zu diesem Zeitpunkt der Großteil des Frames aus dem Ausgangsport übertragen wird. Da es nicht sinnvoll ist, den Rest des fehlerhaften Frames zu übertragen, wird der Rest verworfen, der Ausgangsport erhöht den Fehler "unterlaufen" und der Eingangsport erhöht den entsprechenden Fehlerzähler. Wenn mehrere Eingangsports ungesund sind und ihr Server sich auf dem Ausgangsport befindet, scheint das Serversegment das Problem zu haben, obwohl dies nicht der Fall ist.

Achten Sie bei durchgehendem L3-Switch auf Fehler, und überprüfen Sie, wenn Sie diese sehen, alle Eingangsports auf Fehler.

Fehlkonfiguration von Software oder Hardware

Eine Fehlkonfiguration kann dazu führen, dass ein VLAN langsam arbeitet. Diese negativen Auswirkungen können darauf zurückzuführen sein, dass ein VLAN überbelegt oder überlastet ist. Meist jedoch resultieren sie aus einem fehlerhaften Design oder übersehenen Konfigurationen. Beispielsweise kann ein Segment (VLAN) leicht durch Multicast-Datenverkehr (z. B. Video- oder Audio-Stream) überlastet werden, wenn Techniken zur Einschränkung des Multicast-Datenverkehrs auf diesem VLAN nicht ordnungsgemäß konfiguriert sind. Dieser Multicast-Datenverkehr kann die Datenübertragung beeinträchtigen und für alle Benutzer einen Paketverlust in einem gesamten VLAN verursachen (und die Segmente der Benutzer überfluten, die die Multicast-Streams nicht empfangen wollten).

Softwarefehler und Hardwareprobleme

Software-Bugs und Hardware-Probleme lassen sich nur schwer identifizieren, da sie zu Abweichungen führen, die schwer zu beheben sind. Wenn Sie der Meinung sind, dass das Problem durch einen Softwarefehler oder ein Hardwareproblem verursacht wird, wenden Sie sich an die Techniker des technischen Supports von Cisco, um das Problem zu untersuchen.

Fehlerbehebung bei langsamer VLAN-Verbindung

Bevor Sie eine Fehlerbehebung für langsame VLAN-Verbindungen (zwischen VLANs) durchführen, sollten Sie die in den Abschnitten Troubleshoot Collision Domain Issues and Troubleshoot IntraVLAN (Broadcast Domain) dieses Dokuments besprochenen Probleme untersuchen und ausschließen.

In den meisten Fällen ist die langsame VLAN-Verbindung auf eine Fehlkonfiguration durch den Benutzer zurückzuführen. Wenn Sie beispielsweise MLS oder Multicast Multilayer Switching (MMLS) falsch konfiguriert haben, erfolgt die Paketweiterleitung über die Router-CPU, was ein langsamer Pfad ist. Um Fehlkonfigurationen zu vermeiden und bei Bedarf eine effiziente Fehlerbehebung vorzunehmen, sollten Sie den Mechanismus kennen, der von Ihrem L3-Weiterleitungsgerät verwendet wird. In den meisten Fällen basiert der L3-Weiterleitungsmechanismus auf einer Zusammenstellung von Routing- und ARP-Tabellen (Address Resolution Protocol) und der Programmierung extrahierter Paketweiterleitungsinformationen in die Hardware (Verknüpfungen). Jeglicher Fehler beim Programmieren von Verknüpfungen führt entweder zur Software-Paketweiterleitung (langsamer Pfad), zur Fehlinweiterleitung (Weiterleitung an einen falschen Port) oder zur Blackholing-Verarbeitung des Datenverkehrs.

In der Regel ist ein Fehler bei der Shortcut-Programmierung oder die Erstellung unvollständiger Verknüpfungen (die auch zur Weiterleitung von Softwarepaketen, zu falscher Weiterleitung oder zum Blackholing von Datenverkehr führen können) das Ergebnis eines Softwarefehlers. Wenn Sie vermuten, dass dies der Fall ist, lassen Sie die Techniker des technischen Supports von Cisco dies untersuchen. Weitere Gründe für die langsame VLAN-Weiterleitung sind Hardware-Fehlfunktionen, die jedoch nicht in diesem Dokument behandelt werden. Hardware-Fehlfunktionen verhindern einfach die erfolgreiche Erstellung von Verknüpfungen in der Hardware und daher kann der Datenverkehr entweder einen langsamen (Software-) Pfad oder schwarz verschleiert sein. Hardwarefehler sollten auch von Technikern des technischen Supports von Cisco behoben werden.

Wenn Sie sicher sind, dass das Gerät korrekt konfiguriert ist, das Switching der Hardware jedoch nicht stattfindet, kann ein Softwarefehler oder eine Hardwarestörung die Ursache sein. Beachten Sie jedoch die Gerätefunktionen, bevor Sie diese Schlussfolgerung ziehen.

Die folgenden beiden Situationen treten am häufigsten auf, wenn die Hardware-Weiterleitung beendet wird oder gar nicht stattfindet:

- Der Speicher, der Verknüpfungen speichert, ist erschöpft. Sobald der Speicher voll ist, beendet die Software normalerweise die weitere Verknüpfungserstellung. (MLS, egal ob auf NetFlow oder Cisco Express Forwarding basiert, ist beispielsweise inaktiv, sobald kein Platz für neue Verknüpfungen besteht, und wechselt zur Software [slow path].)
- Hardware-Switching ist nicht vorgesehen, aber nicht offensichtlich. Beispielsweise wurden die Catalyst Supervisor Engines III der Serie 4000 und höher für die hardwarebasierte

Weiterleitung von IP-Datenverkehr entwickelt. Alle anderen Datenverkehrstypen werden von der CPU verarbeitet. Ein weiteres Beispiel ist die Konfiguration einer Zugriffskontrollliste (ACL), die CPU-Eingriffe erfordert (z. B. mit der Option "log"). Der Datenverkehr, der auf diese Regel angewendet wird, wird von der CPU in der Software verarbeitet.

Eingangs-Fehler auf einem Cut-Through-Switch können ebenfalls zu einer Verlangsamung des VLAN-übergreifenden Routings beitragen. Cut-Through-Switches verwenden die gleichen Architekturprinzipien für die Weiterleitung von L3- und L2-Datenverkehr. Die Fehlerbehebungsmethoden, die im Abschnitt Fehlerbehebung für langsames IntraVLAN (Broadcast Domain) oben bereitgestellt werden, können auch auf L2-Datenverkehr angewendet werden.

Eine weitere Fehlkonfiguration, die das Routing zwischen VLANs beeinflusst, ist die Fehlkonfiguration auf den Endbenutzergeräten (z. B. PC und Drucker). Eine häufige Situation ist ein falsch konfigurierter PC. Ein Standard-Gateway ist beispielsweise falsch konfiguriert, die ARP-Tabelle des PCs ist ungültig oder der IGMP-Client ist fehlerhaft. Häufig gibt es mehrere Router oder Routing-fähige Geräte, und einige oder alle Endbenutzer-PCs sind falsch konfiguriert, um das falsche Standard-Gateway zu verwenden. Dies ist möglicherweise der problematischste Fall, da alle Netzwerkgeräte konfiguriert sind und ordnungsgemäß funktionieren, die Endbenutzergeräte jedoch aufgrund dieser Fehlkonfiguration nicht verwenden.

Wenn es sich bei einem Gerät im Netzwerk um einen regulären Router handelt, der über keine Hardwarebeschleunigung verfügt (und nicht am NetFlow MLS teilnimmt), hängt die Weiterleitungsrate des Datenverkehrs vollständig von der Geschwindigkeit der CPU und davon ab, wie beschäftigt sie ist. Eine hohe CPU-Auslastung wirkt sich definitiv auf die Weiterleitungsrate aus. Auf L3-Switches wirken sich hohe CPU-Bedingungen jedoch nicht notwendigerweise auf die Weiterleitungsrate aus. Eine hohe CPU-Auslastung beeinträchtigt die Fähigkeit der CPU, eine Hardware-Verknüpfung zu erstellen (programmieren). Wenn die Verknüpfung bereits in der Hardware installiert ist, wird der Datenverkehr (für die programmierte Verknüpfung) in der Hardware umgeschaltet, bis die Verknüpfung ausgeschaltet (wenn ein Ablauftimer vorhanden ist) oder von der CPU entfernt wird. Wenn jedoch ein Router für eine beliebige Art der Softwarebeschleunigung konfiguriert ist (z. B. schnelles Switching oder Cisco Express Forwarding Switching), kann die Paketweiterleitung durch Software-Verknüpfungen beeinflusst werden. Wenn eine Verknüpfung unterbrochen wird oder der Mechanismus selbst ausfällt, wird statt der Weiterleitungsrate der Datenverkehr an die CPU geleitet, wodurch die Weiterleitungsrate verringert wird.

Zugehörige Informationen

- Fehlerbehebung: IP MultiLayer Switching
- Fehlerbehebung bei Unicast-IP-Routing mit CEF auf Catalyst Switches der Serien 6500/6000 mit Supervisor Engine 2 und CatOS-Systemsoftware
- Konfigurieren von Inter-VLAN-Routing mit Catalyst Switches der Serie 3550
- Produktsupport für Switches
- Unterstützung der LAN Switching-Technologie
- Technischer Support und Dokumentation - Cisco Systems