Problemen met STP oplossen en verwante ontwerpoverwegingen

Inhoud

Inleiding

Dit document beschrijft aanbevelingen voor het implementeren van een veilig netwerk over het overbruggen van Cisco Catalyst-switches waarop Catalyst OS/Cisco IOS®-software wordt uitgevoerd.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

In dit document worden enkele veelvoorkomende oorzaken van STP-fouten (Spanning Tree Protocol) beschreven en hoe u de bron van het probleem kunt identificeren. Het toont ook het soort ontwerp dat het overspannen van boom-gerelateerde kwesties minimaliseert en gemakkelijk is om problemen op te lossen.

Dit document bespreekt niet de basiswerking van STP. Als u wilt weten hoe STP werkt, raadpleegt u dit document:

- Spanning Tree Protocol (STP) op Catalyst-switches begrijpen en configureren

Dit document heeft geen betrekking op Rapid STP (RSTP), zoals gedefinieerd in IEEE 802.1w. Ook wordt in dit document niet ingegaan op het protocol MST (Multiple Spanning Tree) dat in IEEE 802.1s is gedefinieerd. Raadpleeg voor meer informatie over RSTP en MST deze documenten:

- Meervoudige Spanning Tree Protocol (802.1s) begrijpen
- Inzicht in Rapid Spanning Tree Protocol (802.1w)

Raadpleeg het document Probleemoplossing STP op Catalyst-Switch met geïntegreerde IOS-software (Native Mode) voor een specifieker STP-document voor Catalyst-switches waarop Cisco IOS-software wordt uitgevoerd.

Spanning Tree Protocol-fout

De primaire functie van het Spanning-boomalgoritme (STA) is lijnen te snijden die overtollige verbindingen in brugnetwerken tot stand brengen. STP werkt bij Layer 2 van het Open System Interconnection (OSI) model. Door middel van Bridge Protocol Data Units (BPDU's) die tussen bruggen uitwisselen, selecteert STP de poorten die uiteindelijk verkeer doorsturen of blokkeren. Dit protocol kan in sommige specifieke gevallen mislukken en om problemen op te lossen kan de situatie dat resultaten zeer moeilijk zijn, die afhankelijk is van het ontwerp van het netwerk. In dit specifieke gebied, voert u het belangrijkste deel van het probleemoplossingsproces uit voordat het probleem zich voordoet.

Een storing in de STA leidt over het algemeen tot een overbruggingslus. De meeste klanten die Cisco Technical Support bellen voor het overspannen van drie problemen vermoeden een bug, maar een bug is zelden de oorzaak. Zelfs als de software het probleem is, komt een overbruggingslijn in een milieu STP nog uit een haven die kan blokkeren, maar in plaats daarvan voorwaarts verkeer.

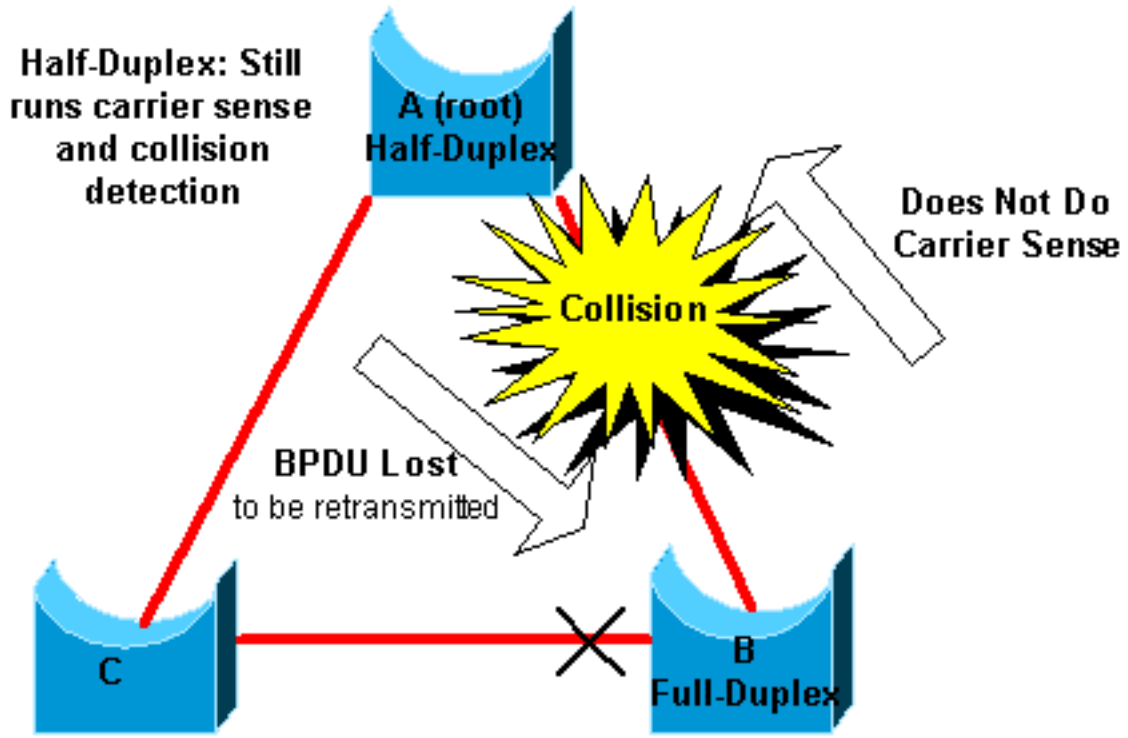
Spanning Tree-convergentie

Verwijs naar de video Spanning Tree om een voorbeeld te zien dat uitlegt hoe de Spanning Tree in eerste instantie convergeert. Het voorbeeld verklaart ook waarom een geblokkeerde poort in de doorstuurmodus terechtkomt vanwege een excessief verlies van BPDU's, wat resulteert in STA-storing.

De rest van dit document beschrijft de verschillende situaties die ervoor kunnen zorgen dat STA niet werkt. De meeste van deze fouten hebben te maken met een enorm verlies van BPDU's. Het verlies veroorzaakt geblokkeerde poorten naar overgang naar doorsturen modus.

Duplex-mismatch

De duplexwanverhouding op een punt-tot-punt verbinding is een zeer gemeenschappelijke configuratiefout. Als u de duplexmodus handmatig op Volledig op één kant van de link instelt en de andere kant in autonegotiation-modus laat, eindigt de link in half-duplex. (Een poort met een duplexmodus die is ingesteld op Volledig onderhandelt niet meer.)



Het slechtst-casescenario is wanneer een brug die BPDUs verzendt de duplexwijze heeft die aan half-duplex op een haven wordt geplaatst, maar de peer haven op ander eind van verbinding heeft de duplexwijze die aan volledig-duplex wordt geplaatst. In het vorige voorbeeld, kan de duplexwanverhouding op het verband tussen brug A en B gemakkelijk tot een het overbruggen lijn leiden. Omdat de brug B configuratie voor volledig-duplex heeft, voert het geen dragerbetekenis vóór verbindingstoegang uit. Bridge B begint frames te verzenden, zelfs als bridge A de link al gebruikt. Deze situatie is een probleem voor A; bridge A detecteert een botsing en voert het back-up algoritme uit voordat de brug een andere transmissie van het frame probeert. Als er genoeg verkeer van B aan A is, ondergaat elk pakket dat A verzendt, dat de BPDUs omvat, uitstel of botsing en wordt uiteindelijk gelaten vallen. Vanuit een STP-oogpunt heeft bridge B de root-brug verloren omdat bridge B niet meer BPDU's van A ontvangt. Dit brengt B ertoe om de poort te deblokkeren die is aangesloten op brug C, waardoor de lus wordt gemaakt.

Wanneer er een duplexwanverhouding is, bevinden deze foutmeldingen zich op de switch-consoles van Catalyst switches waarop CatOS en Cisco IOS-software worden uitgevoerd:

CatOS

```
CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port [mod]/[port]
```

Cisco IOS-software

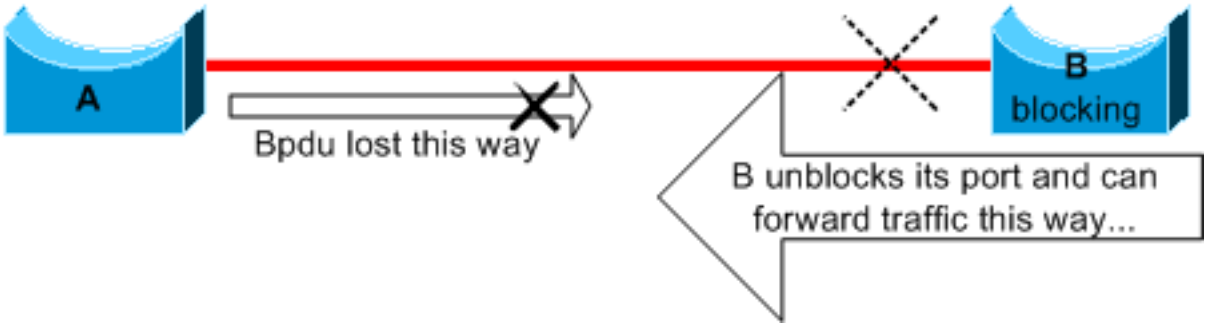
```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half
duplex), with TBA05071417(Cat6K-B) 4/1 (half duplex).
```

Controleer de duplexinstellingen en stel de configuratie correct in als de duplexconfiguratie niet overeenkomt.

Raadpleeg voor meer informatie over het oplossen van problemen bij een duplexfout het document Configuration and Troubleshooting Ethernet 10/100/1000Mb Half/Full duplex Auto-Negotiation.

Unidirectionele link

Unidirectionele links zijn een veel voorkomende oorzaak van een overbruggingslus. Op vezelverbindingen, veroorzaakt een mislukking die zonder opsporing vaak unidirectionele verbindingen gaat. Een andere oorzaak is een probleem met een transceiver. Alles wat een link kan leiden om omhoog te blijven en een unidirectionele communicatie te verstrekken is zeer gevaarlijk met betrekking tot STP. Dit voorbeeld verduidelijkt:



Stel hier dat het verband tussen A en B unidirectioneel is. De verbinding laat verkeer van A tot B vallen terwijl de verbinding verkeer van B aan A overbrengt. Veronderstel dat brug B blokkeerde alvorens de verbinding unidirectional werd. Een poort kan echter alleen blokkeren als deze BPDU's ontvangt van een brug met een hogere prioriteit. Omdat in dit geval alle BPDU's die van A komen verloren gaan, wordt brug B uiteindelijk overgeplaatst van de haven naar A naar het doorsturen van de staat en voorwaarts verkeer. Dit leidt tot een lijn. Als deze mislukking bij opstarten bestaat, correct convergeert STP niet. In het geval van een duplex mismatch helpt een reboot tijdelijk; maar in dit geval heeft een reboot van de bruggen absoluut geen effect.

Om de unidirectionele koppelingen te detecteren voordat de doorsturen-lus wordt gemaakt, heeft Cisco het UniDirectional Link Detection (UDLD) protocol ontworpen en geïmplementeerd. Deze eigenschap kan ongepaste aanleg van kabelnetten of unidirectionele verbindingen op Layer 2 ontdekken en automatisch resulterende lijnen breken door sommige havens onbruikbaar te maken. Voer UDLD waar mogelijk uit in een overbrugde omgeving.

Raadpleeg voor meer informatie over het gebruik van UDLD het document Inzicht in en configuratie van de functie Unidirectionele linkdetectie-protocol.

PacketCorruption

Packet corruptie kan ook leiden tot hetzelfde soort mislukking. Als een link een hoog aantal fysieke fouten heeft, kunt u een bepaald aantal opeenvolgende BPDU's verliezen. Dit verlies kan een blokkerende haven aan overgang naar het door:sturen van staat leiden. U ziet dit geval niet zeer vaak omdat STP standaardparameters zeer conservatief zijn. De blokkerende poort moet BPDU's 50 seconden missen voordat de overgang naar doorsturen plaatsvindt. De succesvolle transmissie van één BPDU doorbreekt de lus. Dit geval treedt doorgaans op met de onzorgvuldige aanpassing van STP-parameters. Een voorbeeld van een aanpassing is de vermindering van de max-leeftijd.

Duplex mismatch, slechte kabels of onjuiste kabellengte kan pakketcorruptie veroorzaken. Raadpleeg de poort- en interfaceproblemen bij de Switch voor probleemoplossing van het document voor een uitleg van de CatOS- en Cisco IOS-softwarefoutuitvoer.

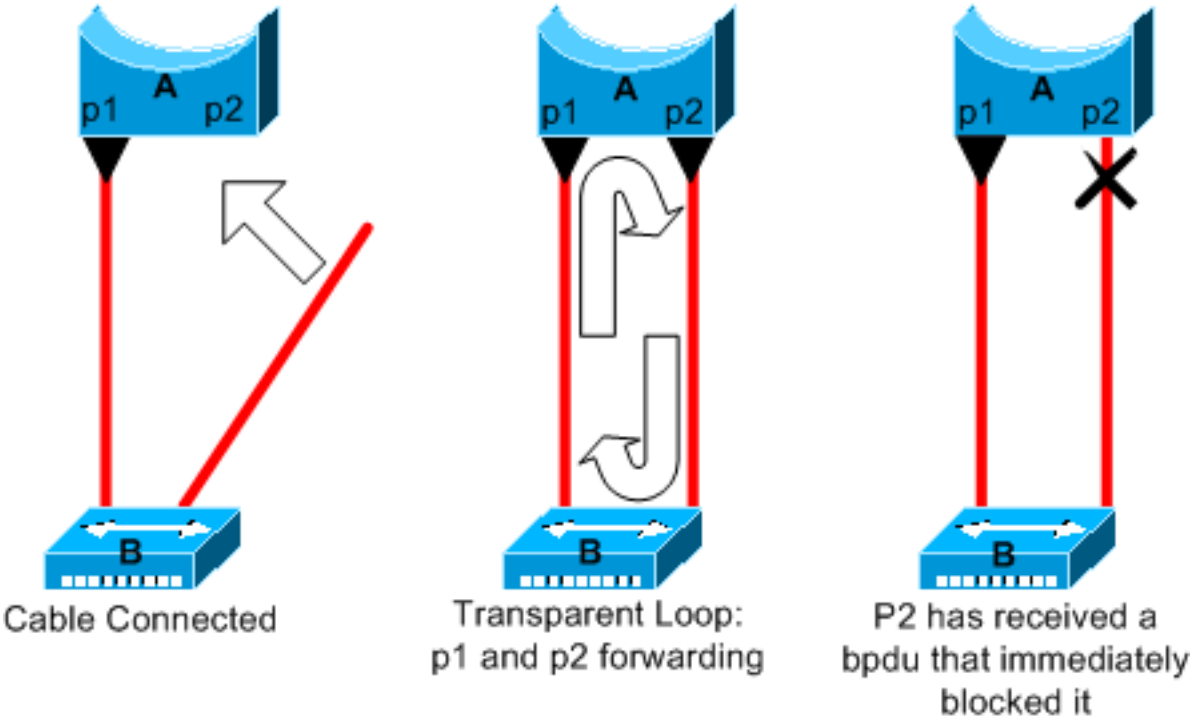
Resourcefouten

STP wordt geïmplementeerd in software, zelfs op high-end switches die de meeste switchingfuncties in hardware met gespecialiseerde Application-Specific Integrated Circuits (ASIC's) uitvoeren. Als er om welke reden dan ook een overgebruik van de CPU van de brug is, kunnen de middelen ontoereikend zijn voor de transmissie van BPDU's. De STA is over het algemeen niet processorintensief en heeft voorrang op andere processen. De sectie Resourcefouten opzoeken in dit document bevat richtlijnen over het aantal gevallen van STP dat een bepaald platform kan verwerken.

Configuratie-fout in PortFast

PortFast is een functie die u meestal alleen inschakelt voor een poort of interface die verbinding maakt met een host. Wanneer de verbinding op deze poort komt, slaat de brug de eerste fasen van de STA en directe overgangen naar de voorwaartse modus over.

> **Waarschuwing**: gebruik de functie PortFast niet op routerpoorten of interfaces die verbinding maken met andere switches, hubs of switches. Anders kunt u een netwerklus maken.



In dit voorbeeld, is apparaat A een brug met haven p1 reeds door:sturen. Port p2 heeft een PortFast-configuratie. Apparaat B is een hub. Zodra u de tweede kabel aansluit op A, gaat poort p2 naar de doorstuurmodus en maakt een lus tussen p1 en p2. Deze lus stopt zodra p1 of p2 een BPDU ontvangt die een van deze twee poorten in de blokkeringsmodus zet. Maar er is een probleem met dit soort van transiënte lus. Als het van een lus voorzien verkeer zeer intensief is, kan de brug problemen met de succesvolle transmissie van BPDU hebben die de lijn tegenhoudt. Dit probleem kan de convergentie aanzienlijk vertragen of in extreme gevallen het netwerk ondermijnen.

Raadpleeg voor meer informatie over het juiste gebruik van PortFast op switches waarop CatOS en Cisco IOS-software worden uitgevoerd het document Gebruik van PortFast en andere opdrachten om de vertragingen bij het opstarten van het werkstation te repareren.

Zelfs met PortFast-configuratie neemt de poort of interface nog steeds deel aan STP. Als een switch met een lagere brugprioriteit dan die van de huidige actieve root-brug aan een PortFast-

geconfigureerde poort of interface wordt bevestigd, kan deze als root-brug worden gekozen. Deze verandering van root-brug kan de actieve topologie ongunstig beïnvloeden STP en kan het netwerk suboptimaal maken. Om deze situatie te voorkomen, hebben de meeste Catalyst switches die CatOS en Cisco IOS-software uitvoeren een functie met de naam BPDU Guard. BPDU Guard schakelt een PortFast-geconfigureerde poort of interface uit als de poort of interface een BPDU ontvangt.

Raadpleeg voor meer informatie over het gebruik van de BPDU Guard-functie op switches waarop CatOS- en Cisco IOS-software worden uitgevoerd het document Spanning Tree Portfast BPDU Guard Verbetering.

Awkward STP-parameter afstemming en Diameter problemen

Een agressieve waarde voor de max-age parameter en de voorwaartse vertraging kan leiden tot een zeer onstabiele STP topologie. In dergelijke gevallen kan het verlies van een aantal BPDU's ervoor zorgen dat er een loop verschijnt. Een andere kwestie die niet goed bekend is, betreft de diameter van het bruggennet. De conservatieve standaardwaarden voor de STP-timers leggen een maximale netwerkdiameter van zeven op. Deze maximumnetwerkdiameter beperkt hoe ver weg van elkaar bruggen in het netwerk kunnen zijn. In dit geval mogen twee afzonderlijke bruggen niet meer dan zeven hop van elkaar verwijderd zijn. Een deel van deze beperking komt van het leeftijdsveld dat BPDU's dragen.

Wanneer een BPDU zich van de root-brug naar de bladeren van de boom verspreidt, neemt het leeftijdsveld toe telkens wanneer de BPDU door een brug gaat. Uiteindelijk, de brug verwerpt BPDU wanneer het leeftijdsgebied voorbij maximumleeftijd gaat. Als de wortel te ver van sommige bruggen van het netwerk is, kan deze kwestie voorkomen. Deze kwestie beïnvloedt convergentie van het overspannen - boom.

Wees extra voorzichtig als u STP-timers van de standaardwaarde wilt wijzigen. Er is gevaar als je op deze manier probeert om snellere reconvergentie te krijgen. Een STP-timerwijziging heeft invloed op de diameter van het netwerk en de stabiliteit van het STP. U kunt de overbruggingsprioriteit wijzigen om de root-brug te selecteren en de poortkosten of prioriteitsparameter wijzigen om redundantie en taakverdeling te beheren.

Cisco Catalyst-software biedt u macro's die de belangrijkste STP-parameters voor u fijnafstemmen:

- Het **set spantree root [secondary]** Het macro bevel vermindert de brugprioriteit zodat het wortel (of afwisselende wortel) wordt. Er is een aanvullende optie beschikbaar voor deze opdracht die resulteert in het afstemmen van de STP-timers door de diameter van uw netwerk te specificeren. Zelfs wanneer correct gedaan, timer tuning niet aanzienlijk verbeteren van de convergentietijd en introduceert enige instabiliteitsrisico's in het netwerk. Ook, dit soort afstemming moet worden bijgewerkt telkens als een apparaat in het netwerk wordt toegevoegd. Houd de conservatieve standaardwaarden aan, die aan netwerkingenieurs vertrouwd zijn.
- Het **set spantree uplinkfast** opdracht voor CatOS of de **spanning-tree uplinkfast** Met deze opdracht voor Cisco IOS-software wordt de switch verhoogd, zodat de switch geen hoofdmap kan zijn. Het bevel verhoogt de STP convergentietijd in het geval van een opstraalverbindingsmislukking. Gebruik deze opdracht op een distributie switch met dubbele verbinding met sommige core switches. Raadpleeg het document De Cisco UplinkFast-functie begrijpen en configureren.

- Het **set spantree backbonefast enable** opdracht voor CatOS of de **spanning-tree backbonefast** Met de opdracht voor Cisco IOS-software kan de STP-conversietijd van de switch worden verlengd in het geval van een onrechtstreekse koppelingsfout. BackboneFast is een bedrijfseigen functie van Cisco. Raadpleeg het document Backbone Fast begrijpen en configureren op Catalyst-Switches .

Raadpleeg het document Understanding and Tuning Spanning Tree Protocol Timers voor meer informatie over STP-timers en de regels om deze bij absolute noodzaak af te stemmen.

Softwarefouten

Zoals in de Inleiding vermeld, is STP een van de eerste functies die in Cisco-producten is geïmplementeerd. U kunt verwachten dat deze functie zeer stabiel is. Slechts heeft de interactie met nieuwere eigenschappen, zoals EtherChannel, STP om in sommige zeer specifieke gevallen veroorzaakt te ontbreken die nu zijn gericht. Een aantal verschillende factoren kan een softwarebug veroorzaken en kan een aantal verschillende gevolgen hebben. Het is onmogelijk om de problemen die een virus kan veroorzaken adequaat te beschrijven. De gevaarlijkste situatie die voortvloeit uit softwarefouten is als u sommige BPDUs negeert of u een blokkerende havenovergang aan het door:sturen hebt.

Probleemoplossing voor een fout

Helaas is er geen systematische procedure voor het oplossen van een STP-probleem. In deze paragraaf worden echter enkele acties samengevat die u ter beschikking staan. De meeste stappen in deze sectie zijn van toepassing op het oplossen van problemen van overbruggingslijnen in het algemeen. U kunt een meer conventionele benadering gebruiken om andere mislukkingen van de STP te identificeren die tot een verlies van connectiviteit leiden. U kunt bijvoorbeeld het pad verkennen dat het verkeer dat een probleem ervaart.

> **Opmerking**: de meeste van deze stappen voor probleemoplossing veronderstellen connectiviteit met de verschillende apparaten van het brugnetwerk. Deze connectiviteit betekent dat u consoletoegang hebt. Tijdens een overbruggingslijn, bijvoorbeeld, kunt u waarschijnlijk geen verbinding van Telnet maken.

Als u de uitvoer van een **show-tech support** Met de opdracht van uw Cisco-apparaat kunt u Cisco CLI Analyzer (alleen geregistreerde klanten) gebruiken om potentiële problemen en oplossingen weer te geven.

Gebruik het diagram van het netwerk

Alvorens u een overbruggingslijn problemen oplost, moet u deze punten, minstens kennen:

- De topologie van het brugnetwerk
- De plaats van de root-brug
- De locatie van de geblokkeerde poorten en de redundante koppelingen

Deze kennis is om ten minste deze twee redenen van essentieel belang:

- Om te weten wat te repareren in het netwerk, moet u weten hoe het netwerk eruit ziet wanneer het correct werkt.

- De meeste stappen om problemen op te lossen gebruiken eenvoudig **show** opdrachten om te proberen foutvoorwaarden te identificeren. Kennis van het netwerk helpt u zich te concentreren op de kritieke poorten op de belangrijkste apparaten.

Een overbruggingslus identificeren

Vroeger was het zo dat een uitzendingsstorm rampzalige gevolgen voor het netwerk kon hebben. Vandaag de dag is het niet waarschijnlijk dat een enkele host, bijvoorbeeld een server, een netwerk onderuit haalt door uitzendingen, omdat er snelle verbindingen en apparaten zijn die switching op hardwareniveau bieden. De beste manier om een overbruggingslijn te identificeren is het verkeer op een verzadigde verbinding te vangen en te controleren dat u gelijkaardige pakketten meerdere malen ziet. Realistisch, echter, als alle gebruikers in een bepaald brugdomein connectiviteitskwesties tezelfdertijd hebben, kunt u reeds een overbruggingslijn verdenken.

Controleer het poortgebruik op uw apparaten en zoek naar abnormale waarden. Raadpleeg het gedeelte Poortgebruik controleren van dit document.

Op de Catalyst switches die CatOS uitvoeren, kunt u eenvoudig het algemene backplane gebruik controleren met de **show system** uit. De opdracht geeft het huidige gebruik van de backplane van de switch weer en specificeert ook het piekgebruik en de datum van het piekgebruik. Een ongebruikelijk piekgebruik toont u of er ooit een overbruggingslijn op dit apparaat is geweest.

Connectiviteit snel herstellen en voor een andere keer gereed zijn

Poorten uitschakelen om de lus te breken

Overbruggingslijnen hebben zeer ernstige gevolgen op een brugnetwerk. Beheerders hebben over het algemeen geen tijd om te zoeken naar de oorzaak van de lus en geven er de voorkeur aan om de verbinding zo snel mogelijk te herstellen. De makkelijke uitweg in dit geval is om elke poort die redundantie in het netwerk biedt handmatig uit te schakelen. Als u een deel van het netwerk kunt identificeren dat het meest wordt beïnvloed, kunt u poorten in dit gebied uitschakelen. Of, indien mogelijk, blokkeer eerst poorten die kunnen worden geblokkeerd. Elke keer dat u een poort uitschakelt, controleert u of u de connectiviteit in het netwerk hebt hersteld. Door te identificeren welke uitgeschakelde poort de lus stopt, identificeert u ook het redundante pad waar deze poort zich bevindt. Als deze haven heeft geblokkeerd, hebt u waarschijnlijk de verbinding gevonden waarop de mislukking verscheen.

Log STP-gebeurtenissen op apparaten die geblokkeerde poorten host

Als u niet precies de bron van het probleem kunt identificeren, of als het probleem voorbijgaand is, laat het registreren van gebeurtenissen STP op de bruggen en de switches van het netwerk toe dat de mislukking ervaart. Als u het aantal te configureren apparaten wilt beperken, dient u ten minste deze logboekregistratie in te schakelen op apparaten die geblokkeerde poorten hosten; de overgang van een geblokkeerde poort is wat een loop creëert.

- Cisco IOS-softwarerelease de exec-opdracht **debug spanning-tree events** om STP debug informatie in te schakelen. Geef het algemene bevel van de configuratiewijze uit **logging buffered** om dit op te nemen, debug informatie in de apparaatbuffers.
- CatOS-The **set logging level spantree 7 default** met deze opdracht wordt het standaardniveau verhoogd van gebeurtenissen die betrekking hebben op STP naar het debug-niveau. Zorg

ervoor dat u een maximum aantal berichten in de switch buffers met gebruik van de **set logging buffer 500** uit.

U kunt ook proberen om de debug uitvoer naar een syslog apparaat te verzenden. Helaas, wanneer een overbruggingslijn optreedt, onderhoudt u zelden verbinding met een syslog server.

Poorten controleren

De belangrijkste havens die eerst moeten worden onderzocht zijn de blokkerende havens. Deze sectie biedt een lijst van wat u kunt zoeken op de verschillende poorten, met een snelle beschrijving van de opdrachten die u kunt geven voor switches waarop CatOS en Cisco IOS-software worden uitgevoerd.

Controleer of geblokkeerde poorten BPDU's ontvangen

Controleer vooral bij geblokkeerde poorten en hoofdpoorten of u regelmatig BPDU's ontvangt. Verschillende problemen kunnen leiden tot een poortfout bij het ontvangen van pakketten of BPDU's.

- Cisco IOS-softwarerelease 12.0 of hoger, uitvoer van de **show spanning-tree bridge-group #** De opdracht heeft een `BPDU`-veld. Het veld geeft het aantal BPDU's weer dat voor elke interface wordt ontvangen. Geef de opdracht een of twee keer extra uit om te bepalen of het apparaat BPDU's ontvangt.Als u niet het `BPDU`-veld hebt in de uitvoer van **show spanning-tree** opdracht, kunt u STP-debug inschakelen met de **debug spanning-tree** bevel om het ontvangstbewijs van BPDUs te verifiëren.
- CatOS-The **show mac module/port** De opdracht vertelt u het aantal multicast pakketten dat een specifieke poort ontvangt. Maar de eenvoudigste opdracht die u kunt gebruiken is de **show spantree statistics module#/port# vlan#** uit. Dit bevel toont het nauwkeurige aantal configuratie BPDUs dat een specifieke haven, op specifiek VLAN ontving. Een poort kan tot verschillende VLAN's behoren, indien trunking plaatsvindt. Raadpleeg het gedeelte Een extra CatOS-opdracht van dit document.

Controleer op een duplexfout

Om een duplex wanverhouding te zoeken, moet u elke kant van de punt-tot-punt verbinding controleren.

- Cisco IOS-softwarerelease de **show interfaces [interface interface-number] status** bevel om de snelheid en de duplexstatus van de specifieke haven te controleren.
- CatOS-De allereerste lijnen van de output van de **show port module#/port#** het bevel geeft u de snelheid en de duplex volgens de poortconfiguratie.

Poortgebruik controleren

Een interface met verkeersoverbelasting kan belangrijke BPDU's niet verzenden. Een link overload geeft ook een mogelijke overbruggingslus aan.

- Cisco IOS-software - Gebruik de opdracht **show interfaces** om het gebruik op een interface te bepalen. Verschillende velden helpen u bij deze bepaling, zoals `load` en `packets input/output`.

Raadpleeg de Switch-poort en interfaceproblemen voor probleemoplossing in het document voor een uitleg van de **show interfaces** opdrachtoutput.

- CatOS-The **show mac module#/port#** het bevel toont statistieken over pakketten die een haven ontvangt en verzendt. Het **show top** Het bevel evalueert automatisch het poortgebruik over een periode van 30 seconden en toont het resultaat. De opdracht classificeert de resultaten op basis van het bandbreedtegebruik in procenten, hoewel er andere opties voor de classificatie van resultaten beschikbaar zijn. Ook de **show system** Het bevel geeft een aanwijzing van backplane gebruik, alhoewel het bevel niet aan een specifieke haven richt.

PacketCorruption controleren

- Cisco IOS-software - Let op toename van fouten in de teller van `invoerfouten` van de **show interfaces** uit. De foutentellers omvatten `runts, giganten, geen buffer, CRC, frame, overrun`, en `genegeerde tellingen`.Raadpleeg de Switch-poort en interfaceproblemen voor probleemoplossing in het document voor een uitleg van de **show interfaces** command output.
- CatOS-The opdracht **show port module#/port#** Hier vindt u informatie over de velden `Uitlijning-Err, FCS-Err, Xmit-Err, Rcv-Err` en `Undersize`. Het **show counters module#/port#** Het bevel verstrekt statistieken in nog meer detail.

Een extra CatOS-opdracht

Het commando **show spantree statistics module#/port# vlan#** geeft zeer nauwkeurige informatie over een specifieke haven. Geef deze opdracht op havens die u vermoedt en besteedt speciale aandacht aan deze velden:

- `Voorwaartse trans count`-Deze teller herinnert hoe vaak een poort overgaat van leren naar doorsturen. In een stabiele topologie toont deze teller altijd 1. Deze teller stelt aan 0 terug aangezien de haven en omhoog daalt. Zo, wijst een waarde die hoger is dan 1 erop dat de overgang die door de haven wordt ervaren het resultaat van een herberekening STP is. De overgang is niet het resultaat van een directe koppelingsmislukking.
- `Max leeftijd expiratie teller`-Deze teller volgt het aantal keren dat de max leeftijd is verlopen op deze link. Kort gezegd, een haven die verwacht dat BPDU's wacht op de maximumleeftijd voordat de haven overweegt dat de aangewezen brug verloren gaat. De maximale leeftijd is 20 seconden. Elke keer dat deze gebeurtenis zich voordoet, wordt de teller verhoogd. Wanneer de waarde niet 0 is, geeft dit aan dat de aangewezen brug voor dit LAN instabiel is of een probleem heeft met de transmissie van BPDU's.

Resourcefouten zoeken

Een hoog CPU-gebruik kan gevaarlijk zijn voor een systeem dat de STA uitvoert. Gebruik deze methode om te controleren of de CPU-bron geschikt is voor een apparaat:

- Cisco IOS-softwarerelease **activeert** de opdracht **cpu** van **showprocessen**. Controleer of het CPU-gebruik niet te hoog is. Raadpleeg voor switches uit de Catalyst 4500/4000-serie die CatOS- of Cisco IOS-software uitvoeren het document CPU-gebruik op Catalyst 4500/4000-, 2948G-, 2980G- en 4912G-Switches .
- CatOS-problemen oplossen **show proc cpu** command to display CPU utilization information. Check that the CPU utilization is not too high.

Er is een beperking op het aantal verschillende instanties van STP die een Supervisor Engine kan verwerken. Zorg ervoor dat het totale aantal logische poorten over alle instanties van STP voor verschillende VLAN's niet hoger is dan het maximale aantal dat wordt ondersteund voor elke Supervisor Engine type en geheugenconfiguratie.

Geef het **show spantree summary** opdracht voor switches die CatOS of de **show spanning-tree summary totals** opdracht voor switches waarop Cisco IOS-software wordt uitgevoerd. Deze opdrachten geven het aantal logische poorten of interfaces per VLAN in de `actieve` kolom `STP weer`. Het totaal verschijnt onderaan deze kolom. Het totaal vertegenwoordigt de som van alle logische poorten over alle instanties van STP voor de verschillende VLAN's. Zorg ervoor dat dit nummer niet hoger is dan het maximum aantal dat voor elk Supervisor Engine type wordt ondersteund.

> **Opmerking**: de formule om de som van logische poorten op de switch te berekenen is:

```
(number of non-ATM trunks * number of active Vlans on that trunk)
+ 2*(number of ATM trunks * number of active Vlans on that trunk)
+ number of non-trunking ports
```

Raadpleeg deze documenten voor een overzicht van de beperkingen voor STP die van toepassing zijn op Catalyst-switches:

Platform	CatOS STP-beperkingen	Cisco IOS-softwarereleases STP-beperkingen
Catalyst 6500/6000 Supervisor Engine I en II	STP-probleemoplossing	
Catalyst 6500/6000 Supervisor Engine 720	STP-probleemoplossing	Probleemoplossing voor Spanning Tr
Catalyst 4500/4000 Catalyst 3750	Spanning Tree	Problemen oplossen bij Spanning Tre STP configureren

Onnodige functies uitschakelen

Wanneer u problemen oplost, probeert u te identificeren wat momenteel verkeerd is in het netwerk. Schakel zoveel mogelijk functies uit. De invaliditeit helpt de netwerkstructuur te vereenvoudigen en maakt het gemakkelijker om het probleem te identificeren. EtherChannel is bijvoorbeeld een functie die vereist dat STP logischerwijze meerdere verschillende links in één link bundelt; het uitschakelen van deze functie tijdens het probleemoplossingsproces is zinvol. Als algemene regel, om de configuratie zo eenvoudig mogelijk te maken maakt het probleemoplossingsproces van het probleem veel gemakkelijker.

Handige opdrachten

Cisco IOS-softwareopdrachten

- **show interfaces**
- **show spanning-tree**
- **show bridge**
- **show processes cpu**
- **debug spanning-tree**
- **logging buffered**

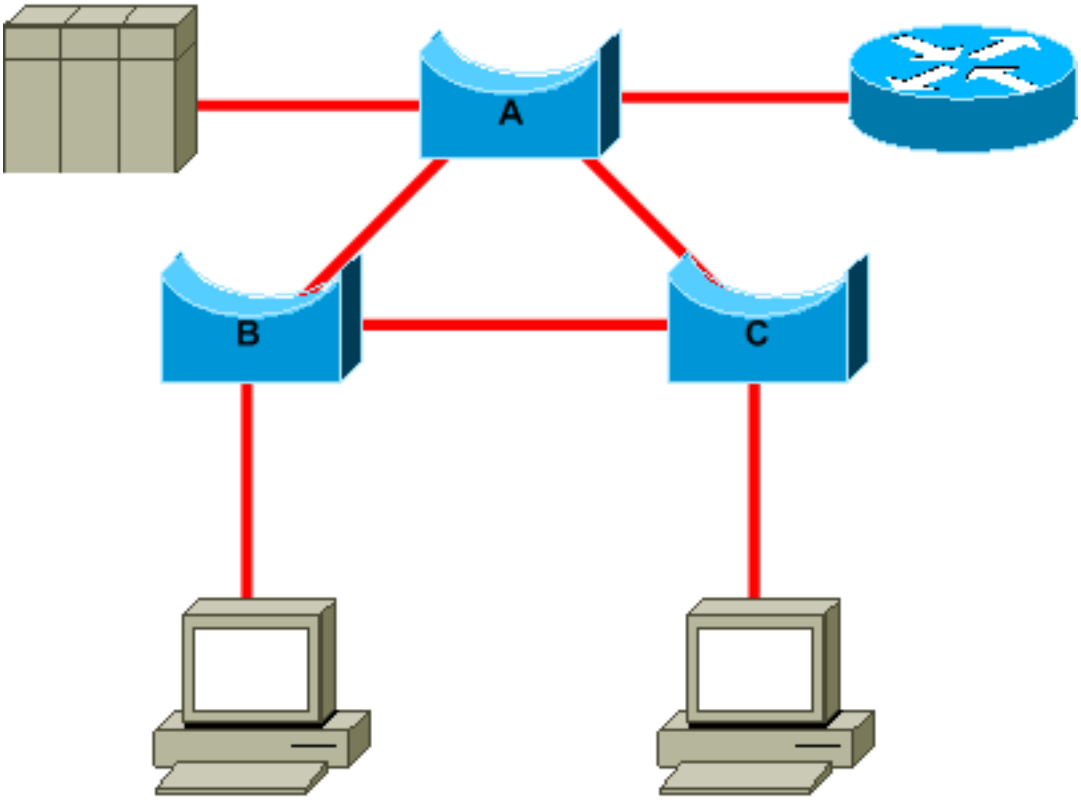
CatOS-opdrachten

- **show port**
- **show mac**
- **show spantree**
- **show spantree statistics**
- **show spantree blockedports**
- **show spantree summary**
- **show top**
- **show proc cpu**
- **show system**
- **show counters**
- **set spantree root [secondary]**
- **set spantree uplinkfast**
- **set logging level**
- **set logging buffered**

Design STP voor probleemvermijding

Weet waar de wortel is

Zeer vaak, is de informatie over de plaats van wortel niet beschikbaar in het oplossen van probleemoplossingstijd. Laat niet de STP beslissen welke brug wortel is. Voor elk VLAN, kunt u gewoonlijk identificeren welke switch het best als wortel kan dienen. Dit hangt af van het ontwerp van het netwerk. Kies een krachtige brug in het midden van het netwerk. Als u de root-brug in het midden van het netwerk plaatst met directe verbinding met de servers en routers, reduceert u over het algemeen de gemiddelde afstand van de clients tot de servers en routers.



Dit diagram toont:

- Als bridge B root is, wordt link A naar C geblokkeerd op bridge A of bridge C. In dit geval kunnen hosts die verbinding maken met switch B in twee stappen toegang krijgen tot de server en de router. Hosts die verbinding maken met bridge C kunnen de server en de router in drie stappen benaderen. De gemiddelde afstand is tweeënhalve hop.

- Als brug A wortel is, zijn de router en de server bereikbaar in twee hop voor beide gastheren die op B en C verbinden. De gemiddelde afstand is nu twee hop.

De logica achter dit eenvoudige voorbeeld brengt over naar complexere topologieën.

> **Opmerking**: voor elk VLAN worden de root-brug en de back-up root-brug vastgelegd met een reductie van de waarde van de STP-prioriteitsparameter. U kunt ook de ingestelde spantree root macro gebruiken.

Weet waar redundantie is

Plan de organisatie van uw redundante links. Vergeet de plug-and-play functie van de STP. Stel de STP-kostenparameter zodanig in dat deze bepaalt welke poorten blokkeren. Deze tuning is meestal niet nodig als je een hiërarchisch ontwerp en een root-brug in een goede locatie hebt.

> **Opmerking**: voor elk VLAN weet u welke poorten in het stabiele netwerk kunnen worden geblokkeerd. Heb een netwerkdiagram dat duidelijk elke fysieke lijn in het netwerk toont dat de geblokkeerde havens de lijnen breken.

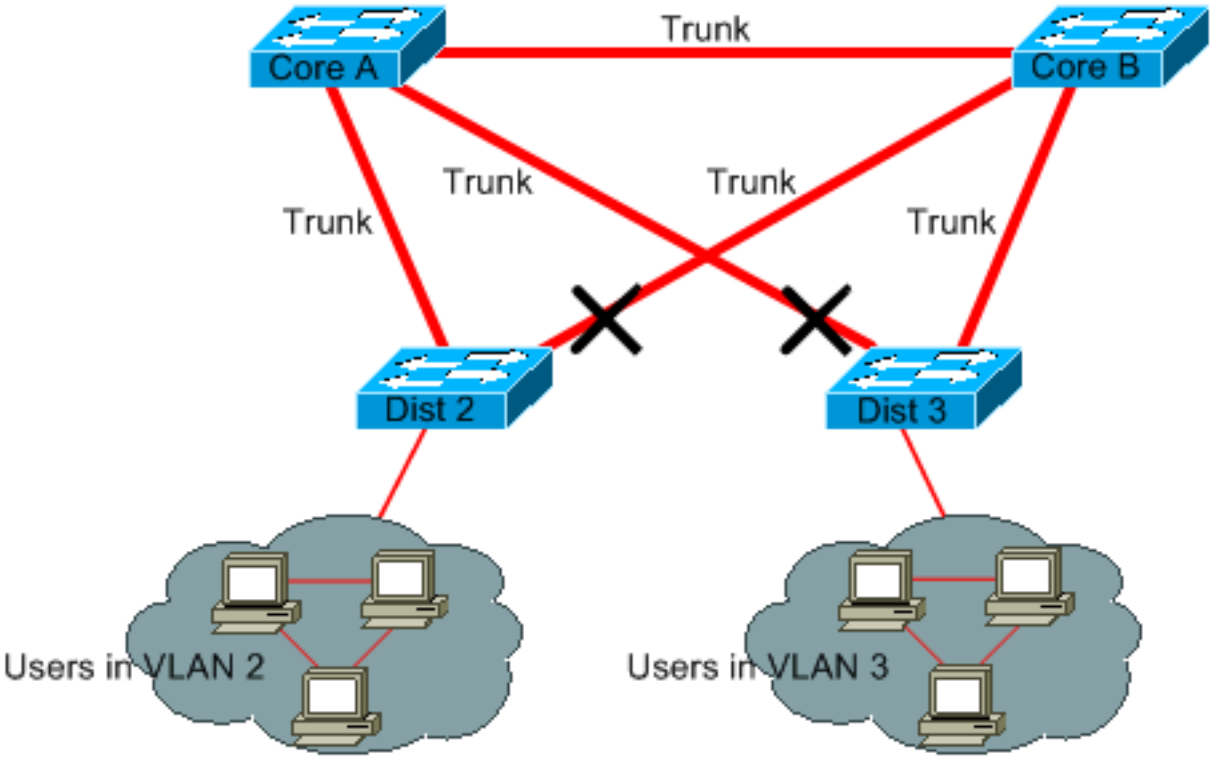
Kennis van de locatie van redundante links helpt u een toevallige overbruggingslus en de oorzaak te identificeren. Ook, kennis van de plaats van geblokkeerde havens staat u toe om de plaats van de fout te bepalen.

Het aantal geblokkeerde poorten minimaliseren

De enige kritieke actie die STP voert is het blokkeren van de poorten. Een enkele blokkerende poort die per ongeluk overgaat naar doorsturen kan een groot deel van het netwerk laten smelten. Een goede manier om het risico dat inherent is aan het gebruik van STV te beperken, is het aantal geblokkeerde poorten zoveel mogelijk te beperken.

VLAN's die u niet gebruikt, snoeien

U hebt niet meer dan twee redundante koppelingen tussen twee knooppunten in een brugnetwerk nodig. Deze configuratie is echter gebruikelijk:

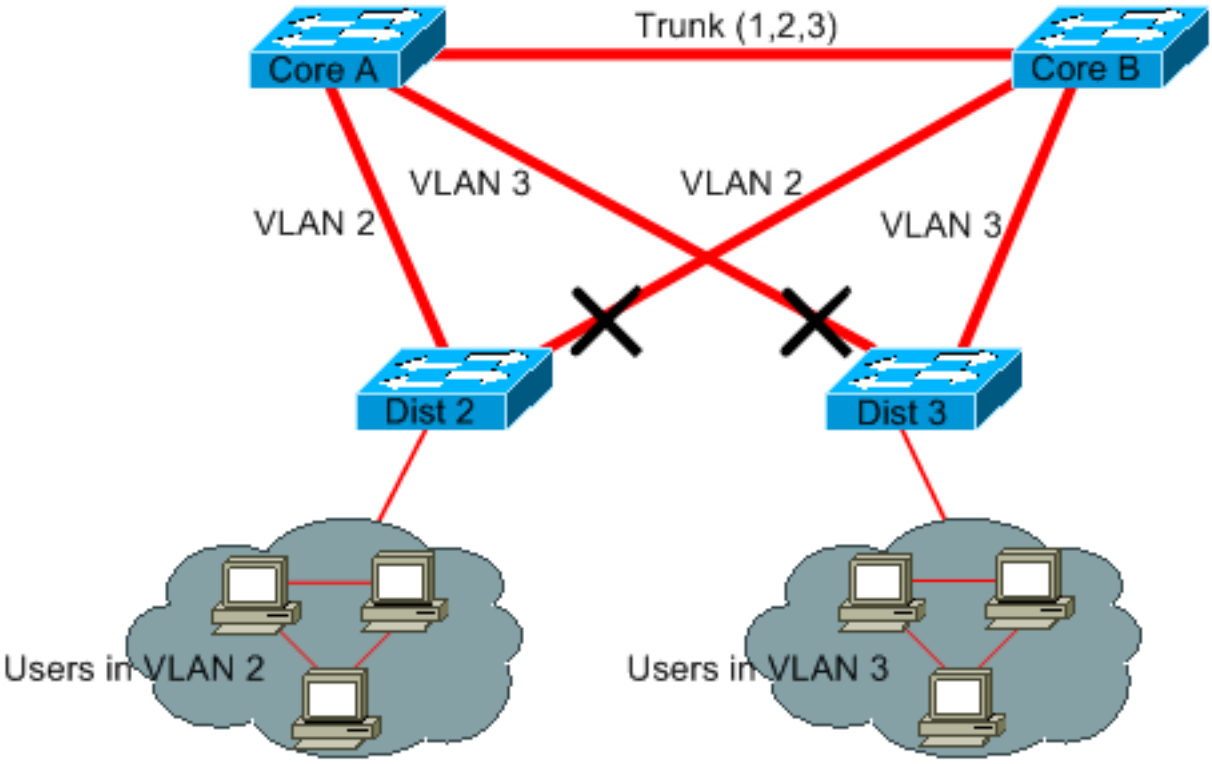


De switches van de distributie zijn dubbel-verbonden aan twee kern switches. Gebruikers die verbinding maken met distributie-switches bevinden zich alleen in een subset van de VLAN's die beschikbaar zijn in het netwerk. In dit voorbeeld zijn gebruikers die verbinding maken op lijst 2 allemaal in VLAN 2; lijst 3 verbindt alleen gebruikers in VLAN 3. Door gebrek, dragen de trunks al VLANs die in het domein van VLAN Trunk Protocol (VTP) worden bepaald. Alleen Dist 2 ontvangt onnodige uitzending en multicast verkeer voor VLAN 3, maar het blokkeert ook een van zijn poorten voor VLAN 3. Het resultaat is drie redundante paden tussen Core A en Core B. Deze redundantie resulteert in meer geblokkeerde poorten en een hogere kans op een loop.

Opmerking: snoei alle VLAN's die u niet nodig hebt van uw trunks.

Het snoeien VTP kan helpen, maar dit soort plug-and-play eigenschap is niet nodig in de kern van het netwerk.

In dit voorbeeld, slechts wordt een toegang VLAN gebruikt om de distributie switches met de kern te verbinden:



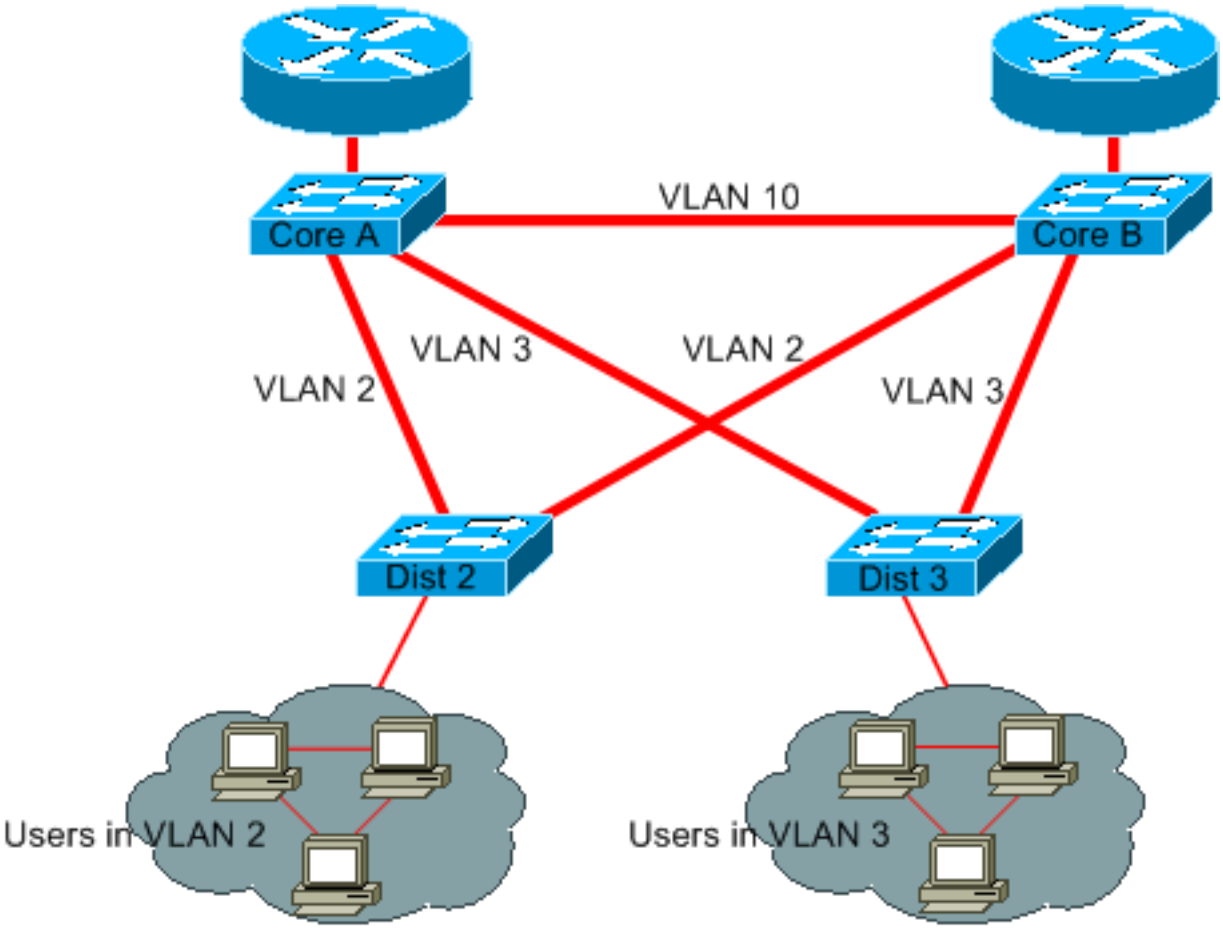
In dit ontwerp wordt slechts één poort per VLAN geblokkeerd. Met dit ontwerp kun je in één stap alle redundante links verwijderen als je Core A of Core B uitschakelt.

Layer 3-switching gebruiken

Layer 3-switching betekent ongeveer routing met de snelheid van switching. Een router voert twee belangrijke functies uit:

- Een router bouwt een het door:sturen lijst. De router ruilt over het algemeen informatie met peers door protocollen te verpletteren.
- Een router ontvangt pakketten en door:sturen hen aan de correcte interface die op het bestemmingsadres wordt gebaseerd.

High-end Cisco Layer 3-switches kunnen nu deze tweede functie uitvoeren, op dezelfde snelheid als de Layer 2-switchingfunctie. Als u een routinghop introduceert en een extra segmentatie van het netwerk maakt, is er geen snelheidssanctie. In dit diagram wordt het voorbeeld in de sectie VLAN's weghalen die u niet als basis gebruikt:



Core A en Core B zijn nu enkele Layer 3 switches. VLAN 2 en VLAN 3 zijn niet meer overbrugd tussen Core A en Core B, zodat er geen mogelijkheid is voor een STP-lus.

- Redundantie is nog steeds aanwezig, met een afhankelijkheid van Layer 3-routeringsprotocollen. Het ontwerp zorgt voor een reconvergentie die nog sneller is dan reconvergentie met STP.
- Er is niet langer één poort die door de STP wordt geblokkeerd. Daarom is er geen potentieel voor een overbruggingslijn.
- Er is geen snelheidsboete, wat betekent dat het VLAN door Layer 3-switching zo snel is als overbrugging binnen het VLAN.

Er is één nadeel aan dit ontwerp. Migratie naar dit soort ontwerp impliceert over het algemeen een herwerking van het adresseringsschema.

Houd STP bij, zelfs als dit niet nodig is

Zelfs als u erin geslaagd bent alle geblokkeerde poorten van uw netwerk te verwijderen en u geen fysieke redundantie hebt, schakelt u STP niet uit. STP is over het algemeen niet zeer processor-intensief; packet switching betreft niet de CPU in de meeste Cisco-switches. Ook verminderen de weinige BPDU's die op elke link worden verzonden de beschikbare bandbreedte niet aanzienlijk. Een brugnetwerk zonder STP kan echter in een fractie van een seconde smelten als een operator een fout maakt op bijvoorbeeld een patchpaneel. Over het algemeen is het uitschakelen van de STP in een brugnetwerk niet het risico waard.

Houd verkeer uit het beheerVLAN en heb geen enkele VLAN-reeks in het gehele netwerk

Een Cisco-switch heeft doorgaans één IP-adres dat aan een VLAN bindt, bekend als het beheerVLAN. In dit VLAN gedraagt de switch zich als een generieke IP-host. In het bijzonder wordt elk broadcast- of multicastpakket doorgestuurd naar de CPU. Een hoge snelheid van uitzending of multicast verkeer op het administratieve VLAN kan negatieve gevolgen hebben voor de CPU en de CPU-capaciteit om vitale BPDU's te verwerken. Houd daarom gebruikersverkeer uit het beheerVLAN.

Tot voor kort was er geen manier om VLAN 1 te verwijderen uit een trunk in Cisco-implementatie. VLAN 1 fungeert over het algemeen als een administratief VLAN, waar alle switches toegankelijk zijn in hetzelfde IP-subnetnummer. Hoewel nuttig, kan deze opstelling gevaarlijk zijn omdat een overbruggingslijn op VLAN 1 alle trunks beïnvloedt, die het gehele netwerk kunnen neerhalen. Natuurlijk, het zelfde probleem bestaat ongeacht welke kwestie VLAN u gebruikt. Probeer de overbruggingsdomeinen te segmenteren met behulp van snelle Layer 3-switches.

Vanaf CatOS versie 5.4 en Cisco IOS-softwarerelease 12.1(11b)E kunt u VLAN 1 uit trunks verwijderen. VLAN 1 bestaat nog steeds, maar het blokkeert verkeer, wat elke lusmogelijkheid voorkomt.

Gerelateerde informatie

- Tools en resources - Technische ondersteuning en documentatie
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.