

Gemeenschappelijke oorzaken van langzame IntraVLAN en InterVLAN-connectiviteit in Campus Switch-netwerken

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Gemeenschappelijke oorzaken van langzame IntraVLAN en InterVLAN-connectiviteit](#)

[Drie categorieën oorzaken](#)

[Oorzaken voor netwerkvertraging](#)

[Probleemoplossing voor de oorzaak](#)

[Probleemoplossing voor problemen met deelgebied](#)

[Probleemoplossing voor langzaam IntraVLAN \(Broadcast Domain\)](#)

[Probleemoplossing met lage connectiviteit voor InterVLAN](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document behandelt de meest voorkomende problemen die kunnen bijdragen tot netwerkvertraging. Het document classificeert de gebruikelijke symptomen van netwerkvertraging en schetst een aanpak van problemdiagnose en oplossing.

[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.

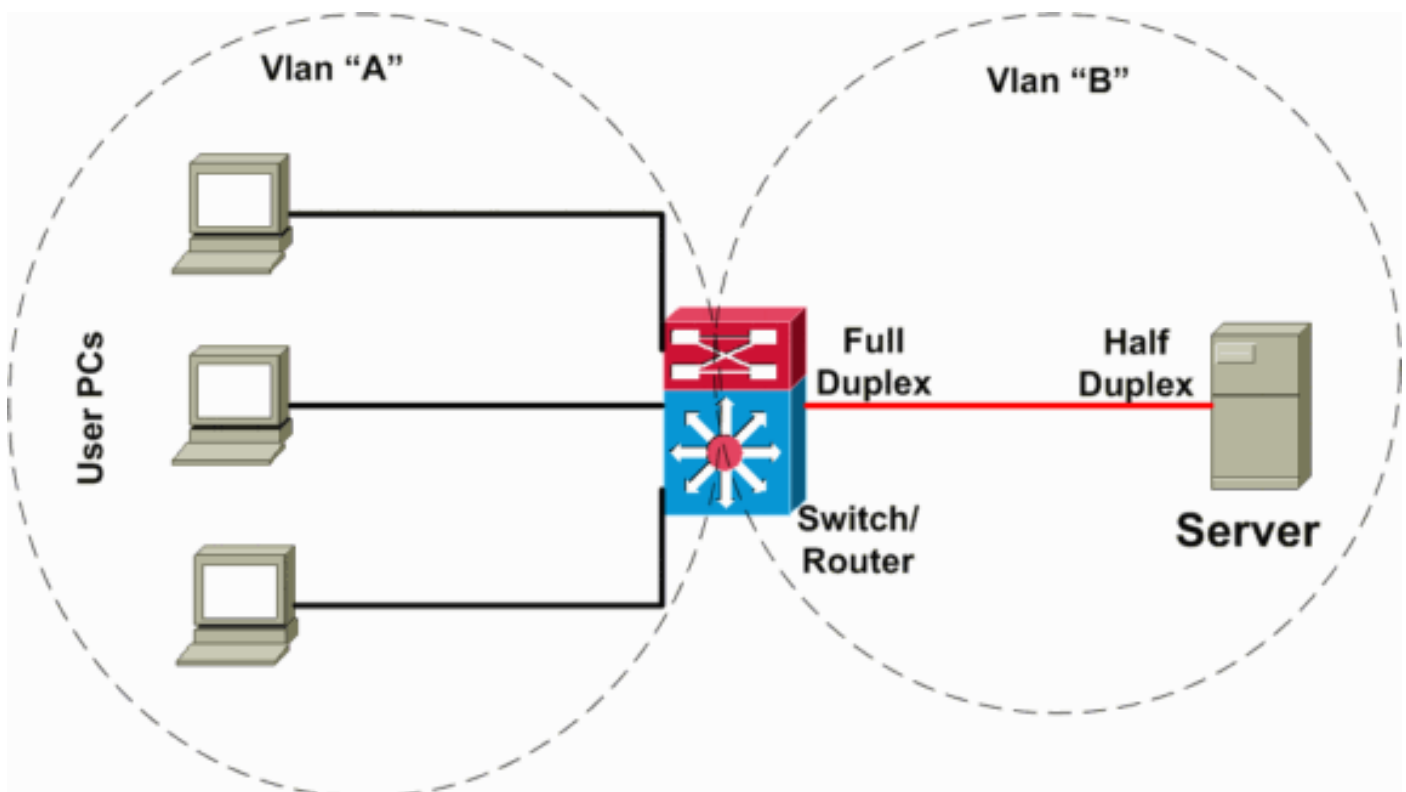
[Conventies](#)

Zie de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

Gemeenschappelijke oorzaken van langzame IntraVLAN en InterVLAN-connectiviteit

De symptomen van langzame connectiviteit op een VLAN kunnen door meerdere factoren op verschillende netwerklagen worden veroorzaakt. Meestal doet het probleem met de netwerksnelheid zich op een lager niveau voor, maar de symptomen kunnen op een hoger niveau worden waargenomen als het probleem zich maskeert onder het begrip "langzaam VLAN". Ter verduidelijking, dit document definieert de volgende nieuwe termen: "langzaam botsingsdomein", "langzaam uitzenden domein" (in andere woorden, langzaam VLAN), en "langzaam interVLAN door te sturen". Deze zijn gedefinieerd in de paragraaf [Drie categorieën oorzaken](#), hieronder.

In het volgende scenario (geïllustreerd in het netwerkdiagram hieronder) is er een Layer 3 (L3) switch die routing tussen VLAN's tussen de server en client VLAN's uitvoert. In dit mislukkingsscenario wordt één server aangesloten op een switch, en de port duplex modus wordt halfduplex op de server en full-duplex op de switch kant ingesteld. Deze foutieve configuratie resulteert in een pakketverlies en een traagheid, met een verhoogd pakketverlies wanneer er hogere verkeerssnelheden optreden op de link waar de server is aangesloten. Voor de klanten die met deze server communiceren, ziet het probleem eruit als traag interVLAN het verzenden omdat zij geen probleem hebben dat aan andere apparaten of klanten op hetzelfde VLAN communiceert. Het probleem treedt alleen op bij het communiceren met de server op een ander VLAN. Dus kwam het probleem op één enkel botsingsdomein voor, maar wordt gezien als langzaam doorsturen interVLAN.



Drie categorieën oorzaken

De oorzaken van de traagheid kunnen als volgt in drie categorieën worden ingedeeld:

Connectiviteit met deelgebied traag

Het domein van de botsing wordt gedefinieerd als aangesloten apparaten die in een half-duplex havenconfiguratie worden gevormd, met elkaar of een hub verbonden. Als een apparaat op een switch poort is aangesloten en de full-duplex modus is ingesteld, is zo een point-to-point verbinding botsingsloos. Langzaamheid op zo een segment kan om verschillende redenen nog steeds voorkomen.

[Lage Broadcast Domain Connectivity \(langzaam VLAN\)](#)

Lage uitzending domeinconnectiviteit komt voor wanneer het gehele VLAN (dat wil zeggen, alle apparaten op het zelfde VLAN) vertraagt.

[Lage InterVLAN-connectiviteit \(langzaam doorsturen tussen VLAN's\)](#)

Lage interVLAN-connectiviteit (langzaam doorsturen tussen VLAN's) treedt op wanneer er geen traagheid op het lokale VLAN is, maar het verkeer moet worden doorgestuurd naar een ander VLAN en het wordt niet tegen het verwachte tempo doorgestuurd.

[Oorzaken voor netwerkvertraging](#)

[Packet Loss](#)

In de meeste gevallen wordt een netwerk gezien als langzaam wanneer de hoger-laagprotocollen (toepassingen) uitgebreide tijd nodig hebben om een operatie te voltooien die normaal sneller loopt. Die vertraging wordt veroorzaakt door het verlies van sommige pakketten op het netwerk, dat hoger-niveau protocollen zoals TCP of toepassingen veroorzaakt om uit te werken en hertransmissie te starten.

[Problemen met betrekking tot het doorsturen van hardware](#)

Met een ander type traagheid, veroorzaakt door netwerkkapparatuur, wordt het verzenden (of Layer 2 [L2] of L3) langzaam uitgevoerd. Dit is te wijten aan een afwijking van de normale (ontworpen) bediening en het overschakelen naar traag doorsturen. Een voorbeeld hiervan is wanneer MultiLayer Switching (MLS) op de switch L3-pakketten tussen VLAN's in de hardware doorstuurt, maar door een foutieve configuratie werkt MLS niet goed en wordt het verzenden uitgevoerd door de router in de software (waardoor de inter-VLAN-verzendsnelheid aanzienlijk wordt verlaagd).

[Probleemoplossing voor de oorzaak](#)

[Probleemoplossing voor problemen met deelgebied](#)

Dus als uw VLAN langzaam lijkt te zijn, isoleer eerst de problemen van het botsingsdomein. U moet instellen of alleen gebruikers op hetzelfde botsingsdomein aansluitingsproblemen ondervinden, of dat dit op meerdere domeinen gebeurt. Om dit te doen, maak een gegevensoverdracht tussen gebruiker PC's op het zelfde botsingsdomein, en vergelijk deze prestatie met de prestaties van een ander botsingsdomein, of met zijn verwachte prestaties.

Als problemen alleen op dat botsingsdomein voorkomen, en de prestaties van andere botsingsdomeinen in hetzelfde VLAN normaal is, dan kijk naar de haventellers op de switch om te bepalen welke problemen dit segment kan ervaren. Waarschijnlijk is de oorzaak eenvoudig, zoals

een duplex mismatch. Een andere, minder frequente oorzaak is een overbelast of oversubscript segment. Zie voor meer informatie over het oplossen van een probleem met één segment het document [Configureren en Problemen oplossen bij Ethernet 10/100/1000MB Half-Service/Full-Duplex automatische onderhandeling](#).

Als gebruikers op verschillende botsingsdomeinen (maar in het zelfde VLAN) de zelfde prestatiekwesties hebben kan het nog steeds door een duplex mismatch op één of meer Ethernet segmenten tussen de bron en de bestemming worden veroorzaakt. Het volgende scenario gebeurt vaak: Een switch is handmatig ingesteld om een full-duplex op alle poorten in het VLAN te hebben (de standaardinstelling is "auto"), terwijl gebruikers (netwerkinterfacekaarten [NIC's]) die op de poorten zijn aangesloten een onderhandelingsprocedure uitvoeren. Dit resulteert in dubbele mismatch op alle poorten en, daarom, slechte prestaties op elke poort (botsingsdomein). Dus alhoewel het lijkt alsof het hele VLAN (uitgezonden domein) een prestatiekwestie heeft, wordt het nog steeds gecategoriseerd als duplex mismatch, voor het botsingsdomein van elke poort.

Een ander geval dat in overweging moet worden genomen, is een specifiek probleem met de prestaties van de NIC. Als een NIC met een prestatieprobleem op een gedeeld segment wordt aangesloten, kan het lijken dat een heel segment trager is, vooral als de NIC aan een server behoort die ook andere segmenten of VLAN's dient. Houd deze case in gedachten omdat deze u kan misleiden als u een oplossing voor uw probleem bent. Nogmaals, de beste manier om dit probleem te vernauwen is een gegevensoverdracht tussen twee hosts op hetzelfde segment uit te voeren (waar de NIC met het veronderstelde probleem is verbonden), of indien slechts de NIC op die poort is, is de isolatie niet gemakkelijk, probeer dan een andere NIC in deze host, of probeer de vermoedelijke host op een afzonderlijke poort aan te sluiten, die een goede configuratie van de haven en de NIC waarborgt.

Als het probleem nog steeds bestaat, probeer dan de poort van de switch te vinden. Raadpleeg het document [Problemen oplossen bij Switch en interfaceproblemen](#).

Het meest ernstige geval is wanneer sommige of alle onverenigbare NIC's met een Cisco-switch zijn verbonden. In dit geval lijkt het erop dat de switch prestatiekwesties heeft. Om de compatibiliteit van de NIC's met Cisco-switches te controleren, raadpleegt u de [Cisco Catalyst-Switches voor probleemoplossing in](#) het document [aan](#) kwesties [met betrekking tot de compatibiliteit](#).

U moet onderscheid maken tussen de eerste twee gevallen (het oplossen van een botsing van het domein vertraagd en van VLAN) omdat deze twee oorzaken verschillende domeinen impliceren. Met een vertraagde botsing van het domein ligt het probleem buiten de switch (of aan de rand van de switch, op een switch poort) of buiten de switch. Het kan zijn dat het segment alleen problemen heeft (bijvoorbeeld een oversubscript segment, dat de segmentlengte overschrijdt, fysieke problemen op het segment of problemen met hub/repeater). In het geval van een vertraagde VLAN ligt het probleem waarschijnlijk binnen de switch (of meerdere switches). Als u het probleem verkeerd diagnosticeert, kunt u de tijd verspillen met het zoeken naar het probleem op de verkeerde plaats.

Controleer de hieronder genoemde onderdelen nadat u een probleem hebt gediagnosticeerd.

In het geval van een gedeeld segment:

- bepalen of het segment overbelast is of oversubscript is
- bepalen of het segment gezond is (inclusief als de kabellengte correct is, als de demping binnen de norm valt en er sprake is van fysieke schade van het medium)

- bepalen of de netwerkpoort en alle op een segment aangesloten NIC's compatibele instellingen hebben
- bepalen of de NIC goed presteert (en de laatste bestuurder runnen)
- bepalen als de netwerkpoort steeds grotere fouten toont
- bepalen als de netwerkpoort is overbelast (vooral als het een serverpoort is)

In het geval van een punt-tot-punt gedeeld segment, of botsingsloos (full-duplex) segment:

- bepalen de poort- en NIC-compatibele configuratie
- de gezondheid van het segment bepalen
- de gezondheid van de NIC bepalen
- kijk naar fouten in netwerkpoorten of overabonnement

[Probleemoplossing voor langzaam IntraVLAN \(Broadcast Domain\)](#)

Na het controleren van er geen duplex mismatch of conflict domein kwesties zijn zoals uitgelegd in de bovenstaande sectie, kunt u nu de vertraging in IntraVLAN oplossen. De volgende stap in het isoleren van de locatie van de vertraging is het uitvoeren van een gegevensoverdracht tussen hosts op hetzelfde VLAN (maar op verschillende poorten); dat wil zeggen, op verschillende botsingsdomeinen), en vergelijk de prestaties met de zelfde testen in afwisselende VLAN's.

Het volgende kan een trage VLAN's veroorzaken:

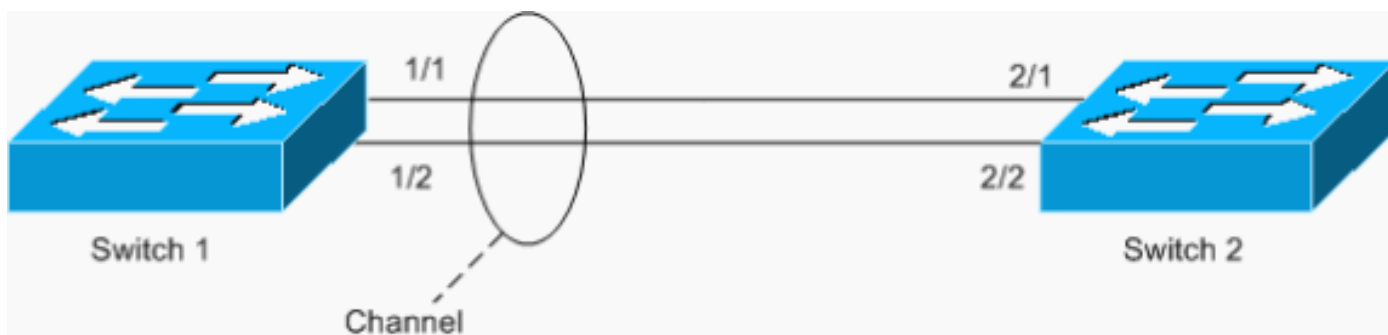
- [verkeerslijn](#)
- [overbelast of overschreven VLAN](#)
- [congestie op het switch - inband - pad](#)
- [switch Management processor met een hoog CPU-gebruik](#)
- [invoerfouten in een doorsnede switch](#)
- ¹ [verkeerde configuratie van software of hardware](#)
- ¹ [softwarebuisjes](#)
- ¹ [hardwareproblemen](#)

¹Deze drie oorzaken van langzame intraVLAN-connectiviteit zijn buiten het toepassingsgebied van dit document en kunnen problemen oplossen door een Cisco Technical Support Engineer. Nadat u de eerste vijf mogelijke oorzaken die hierboven zijn vermeld, hebt uitgesloten, moet u een servicestaanvraag openen met [Cisco Technical Support](#).

[verkeerslijn](#)

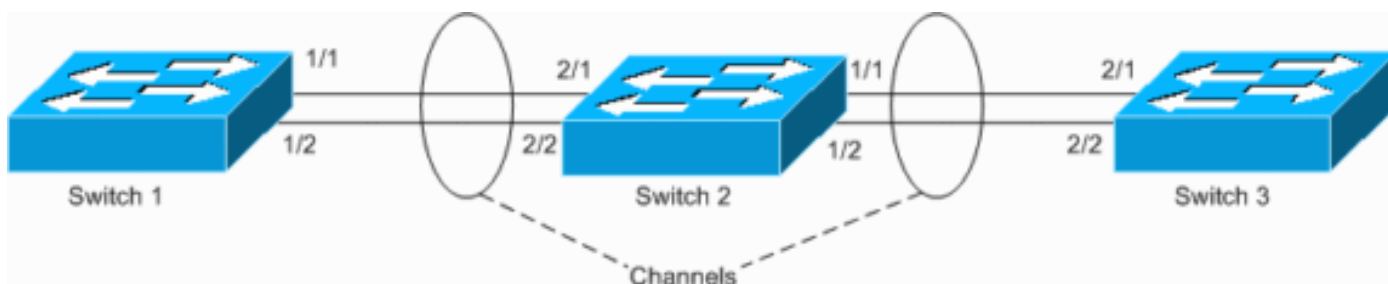
Een verkeerslijn is de meest gebruikelijke oorzaak van een langzaam VLAN. Samen met een lus moet je andere symptomen zien die erop wijzen dat je een lus ervaart. Raadpleeg voor het oplossen van Spanning Tree Protocol (STP)-lijnen het document [Spanning Tree Protocol-problemen en verwante Ontwerpoverwegingen](#). Hoewel krachtige switches (zoals Cisco Catalyst 6500/6000) met gigabit-compatibele backplanes een aantal (STP) maten kunnen verwerken zonder de prestaties van de beheerCPU te belemmeren, kunnen lusconici's bij het gebruik van een netwerk overstromen op NIC's veroorzaken en buffers (Rx/Tx) op de switches ontvangen/verzenden, wat tot trage prestaties leidt bij het aansluiten op andere apparaten.

Een ander voorbeeld van de lus is een asymmetrisch geconfigureerd EtherChannel, zoals in het volgende scenario wordt getoond:



In dit voorbeeld zijn de havens 1/1 en 1/2 in het kanaal, maar de havens 2/1 en 2/2 niet.

Switch 1 heeft een geconfigureerd kanaal (geforceerd kanaal) en Switch 2 heeft geen kanaalconfiguratie voor de corresponderende poorten. Als het overstroomde verkeer (mcast/bcast/onbekende unicast) van Switch 1 naar Switch 2 stroomt Switch 2 terug in het kanaal. Het is geen complete lus, omdat het verkeer niet continu wordt omgebogen, maar slechts eenmaal wordt gereflecteerd. Het is de helft van de totale lus. Het hebben van twee dergelijke misconfiguraties kan een volledige lus creëren, zoals in het onderstaande voorbeeld wordt getoond.



Het gevaar van het hebben van dergelijke misconfiguratie is dat de adressen van MAC op onjuiste poorten worden geleerd aangezien het verkeer onjuist is geschakeld, wat pakketverlies veroorzaakt. Denk bijvoorbeeld aan een router met active Hot Standby Router Protocol (HSRP) die is aangesloten op Switch 1 (zoals in het diagram hierboven). Nadat de router pakketten uitzendt, wordt zijn MAC met Switch 2 terug van een netwerk voorzien en door Switch 1 van het kanaal geleerd, tot een unicast pakket van de router opnieuw wordt verzonden.

[Overladen of overSubscriber-VLAN](#)

Merk op als er knelpunten (oversubscript-segmenten) zijn op uw VLAN's en vul deze op. Het eerste teken dat uw VLAN wordt overbelast is als de buffers van Rx of Tx op een haven oversubscript zijn. Als u uitwerpselen of onCisco op sommige havens ziet, controleer om of die havens overbelast zijn. (Een stijging van de indexcijfers duidt niet alleen op een volledige RX-buffer.) In Catalyst OS (CatOS) worden nuttige opdrachten om uit te geven, **tonen mac mod/poort** of **tonen top [M]**. In Cisco IOS® Software (Native) kunt u de **show interfaces sleuf#/port#** tellers foutmelding uitgeven om teruggooi te zien. Het overbelaste of overgeplaatste VLAN-scenario en het [verkeerslusscenario](#) gaan elkaar vaak begeleiden, maar ze kunnen ook afzonderlijk bestaan.

Meestal gebeurt overbelasting op de backbone poorten wanneer de geaggregeerde bandbreedte van het verkeer wordt onderschat. De beste manier om rond dit probleem te werken is om een EtherChannel te vormen tussen de apparaten waarvoor de havens knelpunten hebben. Als het netwerksegment al een kanaal is, voegt u meer poorten toe in een kanaalgroep om de kanaalcapaciteit te vergroten.

Let ook op de polarisatie van Cisco Express Forwarding (CEF). Dit probleem doet zich voor op

netwerken waarin het verkeer gelijkmatig verdeeld is door routers, maar door de algoritme-uniformiteit van het doorsturen van Cisco Express, wordt al het verkeer gepolariseerd en bij de volgende hop is het niet gelijkmatig verdeeld. Dit probleem komt echter niet vaak voor, omdat het een bepaalde topologie met een lading-gebalanceerde L3 links vereist. Voor meer informatie over het doorsturen van Cisco Express en het in evenwicht brengen van de lading, zie [Problemen oplossen Unicast IP Routing met CEF op Catalyst 6500/6000 Series Switches met een Supervisor Engine 2 en CatOS-systeemsoftware uitvoeren](#).

Een andere oorzaak voor het overbelaste VLAN is een asymmetrisch routingprobleem. Dit type configuratie kan ook een te hoge hoeveelheid verkeer veroorzaken dat uw VLAN's overstroomt. Raadpleeg voor meer informatie het gedeelte *Oorzaak 1: Asymmetric Routing* gedeelte van het document [Unicast-overstromingen in Switched Campus-netwerken](#).

Soms kan een knelpunt een netwerkapparaat zelf zijn. Als je bijvoorbeeld 4 gigabit verkeer via de switch probeert te pompen met een backplane van 3 gigabit, dan kom je terecht bij een dramatisch verlies van het verkeer. De kennis van de netwerkarchitectuur van de switch valt buiten het toepassingsgebied van dit document; bij het overwegen van de capaciteit van een switch van het netwerk moet echter aandacht worden besteed aan de volgende aspecten :

- backplane capaciteit
- blokkeringsproblemen met het hoofd van de lijn
- switch/poortarchitectuur blokkeren en niet blokkeren

[Congestion on Switch Inband Path](#)

Congestion on the switch inband path kan resulteren in een omspant-boomlus of andere soorten instabiliteit op het netwerk. De inband poort op elke Cisco-switch is een virtuele poort die een interface biedt voor beheerverkeer (verkeer zoals Cisco Discovery Protocol en Port Aggregation Protocol [PAgP]) naar de beheerprocessor. De inband poort wordt als virtueel beschouwd omdat, in sommige architecturen, de gebruiker het niet kan zien en de inband functies worden gecombineerd met de normale poort. De SC0 interface op Catalyst 4000, Catalyst 5000 en Catalyst 6500/6000 Series switches (met CatOS) is bijvoorbeeld een subset van de inband poort. Interface SC0 biedt alleen een IP-stack voor de beheerprocessor binnen het geconfigureerde VLAN, terwijl de inband-poort toegang biedt tot de beheerprocessor voor bridge Protocol-gegevenseenheden (BPDU's) in een van de geconfigureerde VLAN's en voor veel andere beheerprotocollen (zoals Cisco Discovery Protocol, Internet Group Management Protocol [IGMP], Cisco Group Management Protocol en Dynamic Trunking Protocol [DTP]).

Als de inband poort overbelast wordt (door een foutieve toepassing of gebruikersverkeer) kan dit leiden tot instabiliteit van protocollen waarvoor de stabiliteit van het protocol gebaseerd is op reguliere berichten of ontvangen "hellos". Deze staat kan resulteren in tijdelijke loops, interfaces flapping, en andere kwesties, die dit soort vertraging veroorzaken.

Het is moeilijk om congestie van de bandpoort op de switch te veroorzaken, hoewel de verkeerd gevormde 'denial of Service'-aanvallen (DoS) kunnen slagen. Er is geen manier om de grenswaarde te verlagen of het verkeer op de binnenpoort te beperken. Voor een oplossing is ingrijpen en onderzoek door de switch nodig. Inbandhavens hebben over het algemeen een hoge tolerantie voor congestie. Er treedt zelden een storing op in de inband poort of het werkt niet in de X- of Tx-richting. Dit zou betekenen dat er sprake is van een ernstige storing van de hardware en zou de hele switch beïnvloeden. Deze voorwaarde is moeilijk te herkennen en wordt gewoonlijk gediagnosticeerd door [Cisco Technical Support](#) engineers. De symptomen zijn dat een switch plotseling "doof" wordt en geen controle verkeer meer ziet zoals de buurupdates van Cisco

Discovery Protocol. Dit duidt op een RX-inband probleem. (Als echter slechts één buurman van Cisco Discovery Protocol wordt gezien, kunt u er vertrouwen in hebben dat inband werkt.) Als alle aangesloten switches het Cisco Discovery Protocol van één switch verliezen (evenals alle andere beheerprotocollen), duidt dit X-problemen op vanuit de inband interface van die switch.

[Gebruik van switch Management 1000 Series met hoge CPU's](#)

Als een inband pad wordt overladen, kan dit een switch ertoe aanzetten hoge CPU-omstandigheden te ervaren; en naarmate de CPU al dat onnodige verkeer verwerkt, verslechtert de situatie. Als het gebruik van een hoge CPU wordt veroorzaakt door een overbelast inband-pad of een ander probleem, kan dit gevolgen hebben voor de beheerprotocollen zoals die in het bovenstaande gedeelte [Congestion on Switch Inband Path zijn](#) beschreven.

Beschouw de CPU in het algemeen als een kwetsbaar punt voor elke switch. Een correct geconfigureerd switch vermindert het risico op problemen die worden veroorzaakt door een hoog CPU-gebruik.

De architectuur van Supervisor Engine I en II van Catalyst 4000 Series switches is zodanig ontworpen dat de beheerCPU bij de overhead betrokken is. Houd het volgende in gedachten:

- CPU's voor een switch wanneer een nieuw pad (de Supervisor Engine I en II zijn op pad gebaseerd) de switch ingaat. Als een inband poort is overbelast, veroorzaakt dit dat elk nieuw pad wordt gedropt. Dit leidt tot verloren pakketverlies (stille weggooi) en traagheid in hoger gelegen protocollen wanneer het verkeer tussen poorten wordt geschakeld. (Raadpleeg het gedeelte [Congestion on Switch Inband Path](#), hierboven.)
- Aangezien de CPU gedeeltelijk overstapt in Supervisor Engine I en II, kunnen hoge CPU-voorwaarden van invloed zijn op de switchmogelijkheden van Catalyst 4000. Een hoog CPU-gebruik op Supervisor Engine I en II kan veroorzaakt worden door de overhead zelf.

Supervisor Engine II+, III en IV van de Catalyst 4500/4000-reeks zijn tamelijk verkeersbestendig, maar MAC-adresstudie in de Cisco IOS-software-gebaseerde Supervisor Engine is nog steeds volledig in software (door de CPU); er is een kans dat een hoog CPU-gebruik dit proces kan beïnvloeden en traagheid kan veroorzaken. Net als bij Supervisor Engine I en II kan een enorm MAC-adresleren of uitschakelen een hoog CPU-gebruik op Supervisor Engine II+, III en IV veroorzaken.

De CPU is ook betrokken bij het leren van MAC in de Catalyst 3500XL- en 2900XL-switches, zodat een proces dat resulteert in snel adressering beïnvloedt de prestaties van de CPU.

Ook is het MAC-adresleerproces (ook al wordt het volledig geïmplementeerd in hardware) een relatief traag proces in vergelijking met een switchingproces. Als er een onophoudelijk hoog percentage MAC-adres dat relevant is, moet de oorzaak gevonden en geëlimineerd worden. Een overspannende boomlus op het netwerk kan dit type van het ontlernen van MAC- adres veroorzaken. Het adres van MAC het relearning (of het adres van MAC het flapping) kan ook door derde switches worden veroorzaakt die op poort gebaseerde VLANs uitvoeren, wat betekent dat de adressen van MAC niet geassocieerd met een etiket van VLAN worden. Dit soort switch kan, wanneer aangesloten op Cisco-switches in bepaalde configuraties, resulteren in MAC-lekken tussen VLAN's. Dit kan op zijn beurt leiden tot een hoge mate van MAC-adresproductie en kan de prestaties nadelig beïnvloeden.

[fouten in een doorsnede Switch aanbrengen](#)

Doorsnede-door-[inbraakpakketpropagatie](#) is gerelateerd aan [Trage Connectiviteit](#) van het [Gebied](#), maar omdat de foutpakketten worden overgebracht naar een ander segment, lijkt het probleem te zijn overgeschakeld tussen segmenten. Cut-door switches (zoals de Catalyst 8500 Series Campus Switch Routers (CSR's) en Catalyst 2948G-L3 of L3 switchmodule voor Catalyst 4000 Series) beginnen met een pakket/frame-switching zodra de switch genoeg informatie heeft uit het lezen van de L2/L3-header van het pakket om het pakket naar zijn doelpoort of poorten door te sturen. Dus terwijl het pakje tussen ingangen en poorten wordt overgeschakeld, is het begin van het pakje al verzonden uit de poort van het uitgang, terwijl de rest van het pakje nog steeds ontvangen wordt door de ingangspoort. Wat gebeurt als het ingress-segment niet gezond is en een CRC-fout (Cyclic redundantie) of een runt-fout genereert? De switch herkent dit alleen wanneer het einde van het frame wordt ontvangen en tegen die tijd wordt het meeste frame uit de spuitpoort overgebracht. Aangezien het niet zinvol is om de rest van het foutieve frame over te dragen, wordt de rest laten vallen, wordt de uitgang van de poort instelbaar als fout, en wordt de invoerpoort instelbaar als foutteller. Als meerdere ingangspoorten ongezond zijn en hun server op de poort ligt, lijkt het erop dat het serversegment het probleem heeft, ook al is dat niet het geval.

Voor doorsnede L3 switches, let op ondergangen en, wanneer je ze ziet, controleer alle ingangspoorten op fouten.

[Software of hardwareconfiguratie](#)

Misconfiguratie kan veroorzaken dat een VLAN langzaam wordt. Deze negatieve effecten kunnen het gevolg zijn van een VLAN dat wordt oversubscript of overbelast, maar meestal resulteren ze in een slecht ontwerp of overgekeken configuraties. Een segment (VLAN) kan bijvoorbeeld makkelijk overweldigd worden door multicast verkeer (bijvoorbeeld video of audio stream) als de multicast traffic shaping-technieken niet correct zijn geconfigureerd op dat VLAN. Zulk multicast verkeer kan gegevensoverdracht beïnvloeden, waardoor pakketverlies op een volledig VLAN voor alle gebruikers wordt veroorzaakt (en het overspoelen van de segmenten van gebruikers die niet van plan waren de multicast stromen te ontvangen).

[Software-bogen en hardwareproblemen](#)

Softwarefouten en hardwareproblemen zijn moeilijk te identificeren omdat ze een afwijking veroorzaken. Dit is moeilijk op te lossen. Als u gelooft dat het probleem wordt veroorzaakt door een softwarebug of hardwareprobleem, neem dan contact op met de [Cisco Technical Support](#) engineers om het probleem te laten onderzoeken.

[Probleemoplossing met lage connectiviteit voor InterVLAN](#)

Voordat u een oplossing zoekt voor de trage interVLAN-connectiviteit (tussen VLAN's), onderzoekt en sluit u de problemen uit die zijn besproken in de delen [van de problemen met de probleemoplossing bij de](#) problemen en de [probleemoplossing in de](#) delen van dit document [IntraVLAN \(Broadcast Domain\)](#).

Meestal wordt de langzame interVLAN-connectiviteit veroorzaakt door een verkeerde configuratie van de gebruiker. Als u bijvoorbeeld MMLS of Multicast Multilayer Switching (MMLS) niet correct hebt ingesteld, wordt het pakkettransport uitgevoerd door de router CPU, wat een langzaam pad is. Om foutieve configuratie te voorkomen en indien nodig efficiënt problemen op te lossen, dient u het mechanisme te begrijpen dat door uw L3-verzendapparaat wordt gebruikt. In de meeste gevallen is het L3-verzendmechanisme gebaseerd op een compilatie van ARP-tabellen bij Routing- en adresresolutie (adresresolutie) en op een uittrekbare pakketverzendinginformatie

naar hardware (sneltoetsen). Elke mislukking in het proces van het programmeren van sneltoetsen leidt tot het verzenden van software (een langzaam pad), het verkeerd doorsturen (doorsturen naar een verkeerde poort) of het zwart doorgeven van verkeer.

Meestal is een mislukking van de snelprogrammering of de creatie van onvolledige sneltoetsen (die ook kunnen leiden tot het verzenden van softwarepakketten, verkeerd doorsturen of zwart-verkeers) het resultaat van een softwarebug. Als u meent dat dit een geval is, laat de [Cisco Technical Support](#) engineers het onderzoeken. Andere redenen voor traag interVLAN-transport zijn hardwarestoringen, maar deze oorzaken vallen niet onder het toepassingsgebied van dit document. Hardware defecten voorkomen alleen dat er een succesvolle sneltoets in de hardware wordt aangemaakt en daarom kan het verkeer een langzaam (software) pad volgen of zwart zijn. Hardware defecten moeten ook door [Cisco Technical Support](#) Engineers worden verwerkt.

Als u er zeker van bent dat het apparaat correct is geconfigureerd, maar er niet wordt overgeschakeld op hardware, dan kan een softwarebug of hardwarestoring de oorzaak zijn. Let echter op de mogelijkheden van de apparatuur voordat u deze conclusie vormt.

De volgende twee meest frequente situaties waarin het doorsturen van hardware kan stoppen of helemaal niet plaatsvindt:

- Het geheugen dat de sneltoetsen opslaat, is op. Wanneer het geheugen vol is, stopt de software gewoonlijk met het maken van verdere sneltoetsen. (Bijvoorbeeld, MLS, of NetFlow of Cisco Express Forwarding-gebaseerd, wordt inactief wanneer er geen ruimte is voor nieuwe sneltoetsen, en het switch naar software [langzaam pad].)
- Apparatuur is niet ontworpen om hardware-switching uit te voeren, maar het is niet duidelijk. Bijvoorbeeld, Catalyst 4000 Series Supervisor Engine III en later worden ontworpen om alleen IP-verkeer op hardware-forward te sturen; alle andere typen verkeer zijn software die door de CPU wordt verwerkt. Een ander voorbeeld is de configuratie van een toegangscontrolelijst (ACL) die CPU-interventie vereist (bijvoorbeeld met de optie "log"). Het verkeer dat op deze regel van toepassing is, wordt in de software door de CPU verwerkt.

[Indrukfouten op een doorsnede-switch](#) kunnen ook bijdragen aan de routing tussen VLAN's. Doorsnede-switches maken gebruik van dezelfde architecturale principes om L3- en L2-verkeer door te sturen. De hierboven beschreven methoden voor het opsporen en verhelpen van problemen in de sectie [Troubleshoot Slow IntraVLAN \(Broadcast Domain\)](#) kunnen ook worden toegepast op L2-verkeer.

Een ander type configuratie dat de routing tussen VLAN beïnvloedt is verkeerde configuratie op de apparaten van de eindgebruiker (zoals de PC en printers). Een gemeenschappelijke situatie is een verkeerd geconfigureerd pc; Bijvoorbeeld, een standaardgateway wordt misvormd, de PC ARP tabel is ongeldig of de IGMP client werkt niet. Een veelvoorkomend geval is wanneer er meerdere routers of routingbare apparaten zijn, en sommige of alle pc's van de eindgebruiker zijn verkeerd geconfigureerd om de verkeerde standaardgateway te gebruiken. Dit kan het meeste problematische geval zijn, omdat alle netwerkapparaten ingesteld en correct werken. Maar de eindgebruikersapparaten gebruiken ze niet vanwege deze foutieve configuratie.

Als een apparaat in het netwerk een normale router is die geen type hardwareversnelling heeft (en niet deelneemt aan NetFlow MLS), dan is de snelheid van het doorsturen van verkeer volledig afhankelijk van de snelheid van de CPU en hoe druk het is. Een hoog CPU-gebruik heeft absoluut gevolgen voor het verzendingspercentage. Voor L3-switches hebben hoge CPU-omstandigheden echter niet noodzakelijkerwijs een invloed op het verzendingspercentage; een hoog CPU-gebruik heeft invloed op de mogelijkheden van de CPU om een sneltoets voor hardware te definiëren (programma's). Als de sneltoets al in de hardware is geïnstalleerd, dan wordt, zelfs als de CPU

sterk wordt gebruikt, het verkeer (voor de geprogrammeerde sneltoets) in hardware geschakeld totdat de sneltoets is verouderd (als er een verlooptimer is) of door de CPU is verwijderd. Als een router echter is ingesteld voor elk type software-versnelling (zoals snelle switching of Cisco Express Forwarding-switching), dan kan het doorsturen van pakketten worden beïnvloed door software-sneltoetsen. Als een sneltoets wordt doorbroken, of het mechanisme zelf faalt, wordt in plaats van de verzendsnelheid te versnellen, het verkeer gestraft naar de CPU, waardoor de gegevensdoorvoersnelheid wordt vertraagd.

[Gerelateerde informatie](#)

- [IP MultiLayer Switching voor probleemoplossing](#)
- [Troubleshoot Unicast IP-routing met behulp van CEF op Catalyst 6500/6000 Series Switches met een Supervisor Engine 2 en CatOS-systeemsoftware](#)
- [Inter-VLAN-routing met Catalyst 3550 Series Switches configureren](#)
- [Productondersteuning voor switches](#)
- [Ondersteuning voor LAN-switching technologie](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)