Best Practices voor Catalyst 6500/6000 Series en Catalyst 4500/4000 Series Switches die Cisco IOS-software uitvoeren

Inhoud

Inleiding

Dit document biedt optimale werkwijzen voor Catalyst 6500/6000 en 4500/4000 Series switches die Cisco IOS® software gebruiken op de Supervisor Engine.

De switches Catalyst 6500/6000 en Catalyst 4500/4000 Series ondersteunen een van deze twee besturingssystemen die op de Supervisor Engine werken:

- Catalyst OS (CatOS)
- Cisco IOS-software

Met CatOS is er de optie om Cisco IOS-software te starten op routerkleatiekaarten of -modules zoals:

- De functiekaart voor meerlaagse Switch (MSFC) in Catalyst 6500/6000
- De 4232 Layer 3 (L3) module in Catalyst 4500/4000

In deze modus zijn er twee opdrachtregels voor de configuratie:

- De CatOS-opdrachtregel voor switching
- De Cisco IOS-softwarerelease voor routing

CatOS is de systeemsoftware, die op de Supervisor Engine draait. Cisco IOS-software die op de routingmodule draait, is een optie die CatOS-systeemsoftware vereist.

Voor Cisco IOS-software is er slechts één opdrachtregel voor de configuratie. In deze modus is de functionaliteit van CatOS geïntegreerd in Cisco IOS-software. De integratie resulteert in één enkele opdrachtregel voor zowel de switching- als de routerconfiguratie. In deze modus is Cisco IOS-software de systeemsoftware en vervangt u CatOS.

Zowel CatOS- als Cisco IOS-softwarefunctiesystemen worden ingezet in kritieke netwerken. CatOS, met de Cisco IOS Software optie voor routerkaarten en -modules, wordt ondersteund in deze switch-serie:

- Catalyst 6500/6000
- Catalyst 5500/5000
- Catalyst 4500/4000

Cisco IOS-systeemsoftware wordt in deze switch-serie ondersteund:

- Catalyst 6500/6000
- Catalyst 4500/4000

Raadpleeg de beste praktijken bij document voor Catalyst 4500/4000, 5500/5000 en 6500/6000 Series Switches voor CatOS-configuratie en -beheer voor informatie over CatOS, omdat dit document Cisco IOS-systeemsoftware bestrijkt.

Cisco IOS-systeemsoftware biedt gebruikers een aantal van deze voordelen:

- Eén gebruikersinterface
- Een uniform netwerkbeheerplatform
- Uitgebreide QoS-functies
- Ondersteuning voor gedistribueerde switching

Dit document biedt modulaire configuratiehandleidingen. Daarom kunt u elke paragraaf

afzonderlijk lezen en wijzigingen aanbrengen in een gefaseerde benadering. Dit document is gebaseerd op een basisbegrip en een vertrouwdheid met de Cisco IOS-gebruikersinterface. Het document heeft geen betrekking op het totale ontwerp van een campus.

Voordat u begint

Achtergrond

De oplossingen die dit document biedt vertegenwoordigen jaren praktijkervaring van Cisco-engineers die met complexe netwerken en veel van de grootste klanten werken. Daarom wordt in dit document de nadruk gelegd op configuraties in de echte wereld die netwerken met succes maken. Dit document biedt de volgende oplossingen:

- Oplossingen die statistisch gezien de breedste blootstelling in het veld en dus het laagste risico hebben
- Eenvoudige oplossingen, die enige flexibiliteit inruilen voor deterministische resultaten
- Oplossingen die eenvoudig te beheren zijn en die teams van netwerkbewerkingen configureren
- Oplossingen die een hoge beschikbaarheid en hoge stabiliteit bevorderen

Referenties

Er zijn veel referentiesites voor de productlijnen Catalyst 6500/6000 en Catalyst 4500/4000 op Cisco.com. De verwijzingen die in deze sectie worden opgesomd, bieden een extra diepte in de onderwerpen die in dit document worden besproken.

Raadpleeg de ondersteuning voor LAN-switchingtechnologie voor meer informatie over de onderwerpen die in dit document worden besproken. De ondersteuningspagina biedt productdocumentatie en documenten voor de probleemoplossing en de configuratie.

Dit document bevat verwijzingen naar online-materiaal van het publiek, zodat u verder kunt lezen. Maar andere goede basis- en educatieve referenties zijn:

- Cisco ISP-basisproducten
- Vergelijking van Cisco Catalyst en Cisco IOS besturingssystemen voor Cisco Catalyst 6500 Series Switch
- Cisco LAN-switching (CCIE Professional Development Series)
- Bouwen aan Cisco Multilayer Switched Networks
- Prestaties en foutbeheer
- VEILIG: Een security blauwdruk voor ondernemingsnetwerken
- Cisco-veldhandleiding: Configuratie van Catalyst Switch

Basisconfiguratie

In deze sectie worden eigenschappen besproken die worden uitgevoerd wanneer u de meerderheid van Catalyst netwerken gebruikt.

Catalyst-besturingsplane-protocollen

In dit hoofdstuk worden protocollen geïntroduceerd die tussen switches worden uitgevoerd bij normaal gebruik. Een basisbegrip van de protocollen is handig als je elk onderdeel aanspreekt.

Supervisor Engine

De meeste eigenschappen die in een netwerk van de Catalyst worden toegelaten vereisen twee of meer switches om samen te werken. Om deze reden moet er een gecontroleerde uitwisseling van aandachtspunten, configuratieparameters en beheerveranderingen zijn. Of deze protocollen eigen zijn van Cisco, zoals Cisco Discovery Protocol (CDP) of op standaarden gebaseerde protocollen, zoals IEEE 802.1D (Spanning Tree Protocol [STP]), hebben allen bepaalde elementen gemeen wanneer de protocollen op de Catalyst-serie worden geïmplementeerd.

In het basisframe-doorsturen komen de gebruikersgegevensframes uit eindsystemen. Het bronadres (SA) en het bestemmingsadres (DA) van de gegevensframes worden niet gewijzigd door Layer 2 (L2)-switched domeinen. Content-Adressable memory (CAM) lookup-tabellen op elke switch Supervisor Engine zijn bevolkt door een SA learning-proces. De tabellen geven aan welke vrijlooppoort naar elk ontvangen frame wordt doorgestuurd. Als de bestemming onbekend is of het kader bestemd is voor een uitzending of multicast adres, is het proces van het adresleren onvolledig. Wanneer het proces onvolledig is, wordt het frame verzonden (overstroomd) naar alle poorten in dat VLAN. De switch moet ook herkennen welke frames door het systeem moeten worden geschakeld en welke frames naar de switch CPU zelf moeten worden gericht. De CPU van de switch wordt ook wel NMP-netwerkbeheerprocessor (Network Management Processor) genoemd.

Speciale items in de CAM-tabel worden gebruikt om het Catalyst-besturingsplane te maken. Deze speciale items worden systeemitems genoemd. Het bedieningspaneel ontvangt en stuurt verkeer naar de NMP via een binnenpoort van de switch. Met het gebruik van protocollen met welbekende MAC-adressen van de bestemming kan dus het verkeer van het besturingsplane worden gescheiden van het gegevensverkeer.

Cisco heeft een gereserveerde reeks Ethernet MAC- en protocoladressen, zoals de tabel in deze sectie toont. Dit document bevat een gedetailleerde beschrijving van elk gereserveerd adres, maar deze tabel bevat een samenvatting, voor het gemak:

Functie	SNAP[1] HDLC[2]-protocoltype	Destination Multicast MAC
PAgP[3]	0x0104	01-00-0c-cc-cc-cc
PVST+, RPVST+[4]	0x010b	01-00-0c-cc-cc-cd
VLAN-brug	0x010c	01-00-0c-cd-cd-ce
UDLD[5]	0x011	01-00-0c-cc-cc-cc
CDP	0x2000	01-00-0c-cc-cc-cc
DTP[6]	0x2004	01-00-0c-cc-cc-cc
STP-uplinkFast	0x200a	01-00-0c-cd-cd
IEEE 802.1D-boom	NB: DSAP[7] 42 SSAP[8] 42	01-80-c2-00-00-00
ISL[9]	N.v.t.	01-00-0c-00-00-00
	0x203	01-00-0c-cc-cc-cc

VTP[10]		
IEEE Pauze 802.3x	NVD — SAP 81 SAP 80	01-80-C2-00-00-00>0F

[1] SNAP = Subnetwork Access Protocol.

[2] HDLC = datalink-controle op hoog niveau.

[3] PAgP = Port Aggregation Protocol.

[4] PVST+ = Per VLAN Spanning Tree+ en RPVST+ = Rapid PVST+.

[5] UDLD = Unidirectionele koppeldetectie.

[6] DTP = Dynamic Trunking Protocol.

[7] DSAP = bestemming service access point.

[8] SSAP = toegangspunt voor de bronservice.

[9] ISL = Inter-Switch link.

[10] VTP = VLAN Trunk-protocol.

De meerderheid van de controleprotocollen van Cisco gebruikt een insluiting van IEEE 802.3, die Logical Link Control (LLC) 0xAAA03 en Organisationaal Uniforme Identifier (OUI) 0x0000C omvat. U kunt dit zien op een LAN-analyzer.

Deze protocollen gaan uit van point-to-point connectiviteit. Merk op dat het opzettelijke gebruik van multicast doeladressen twee Catalyst switches in staat stelt om op transparante wijze over niet-Cisco switches te communiceren. Apparaten die de frames niet begrijpen en onderscheppen, overspoelen ze simpelweg. Echter, point-to-multipoint connecties door multi-mode omgevingen kunnen resulteren in inconsequent gedrag. In het algemeen, vermijd point-to-multipoint verbindingen door multi-mode omgevingen. Deze protocollen eindigen op Layer 3 routers en werken alleen binnen een switch-domein. Deze protocollen krijgen prioriteit boven gebruikersgegevens door toepassingsspecifieke geïntegreerde schakeling (ASIC) te verwerken en te plannen.

De discussie gaat nu over de SA. Switch protocollen gebruiken een MAC-adres dat is afgeleid van een bank met beschikbare adressen. Een EPROM op het chassis verschaft de bank van beschikbare adressen. Geef de opdracht **show Module uit** om de adresbereiken weer te geven die beschikbaar zijn voor elke module voor het aanbesteden van verkeer zoals STP bridge Protocol Data Unit (BPDU's) of ISL-frames. Dit is een voorbeeldopdrachtoutput:

```
>show module
…

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------  -----------------
1   00-01-c9-da-0c-1e to 00-01-c9-da-0c-1f 2.2    6.1(3)      6.1(1d)
    00-01-c9-da-0c-1c to 00-01-c9-da-0c-1
    00-d0-ff-88-c8-00 to 00-d0-ff-88-cb-ff
!--- These are the MACs for sourcing traffic.
```

VLAN 1

VLAN 1 heeft een speciale betekenis in Catalyst netwerken.

Wanneer trunking, gebruikt de Supervisor Engine van de Catalyst altijd de standaard VLAN, VLAN 1, om een aantal controle en beheerprotocollen te taggen. Tot deze protocollen behoren CDP, VTP en PAgP. Alle switch poorten, die de interne sc0 interface omvatten, worden standaard ingesteld om lid te zijn van VLAN 1. Alle stammen dragen standaard VLAN 1.

Deze definities zijn nodig om een aantal goed gebruikte termen in een netwerk van Catalyst te verduidelijken:

- Het beheer VLAN is waar sc0 voor CatOS en low-end switches verblijft. U kunt dit VLAN wijzigen. Houd dit in gedachten wanneer u zowel CatOS- als Cisco IOS-switches onderling werkt.
- Het inheemse VLAN is het VLAN waaraan een haven terugkeert wanneer het niet trunking is. Ook, is het inheemse VLAN untagged VLAN op een stam van IEEE 802.1Q.

Er zijn verschillende goede redenen om een netwerk te stemmen en het gedrag van havens in VLAN 1 te veranderen:

- Wanneer de diameter van VLAN 1, zoals om het even welk ander VLAN, groot genoeg wordt om een risico voor stabiliteit te zijn, vooral vanuit een STP perspectief, moet u het VLAN terugsnoeren. Zie de sectie Switch Management Interface en Native VLAN voor meer informatie.
- U moet de gegevens van het besturingsplane op VLAN 1 gescheiden houden van de gebruikersgegevens, om de probleemoplossing te vereenvoudigen en de beschikbare CPU-cycli te maximaliseren. Vermijd Layer 2 loops in VLAN 1 wanneer u meerlaagse campusnetwerken zonder STP ontwerpt. Om de Laag 2 lijnen te vermijden, ontgrendel VLAN 1 handmatig van boomstampoorten.

Samengevat kan deze informatie over stammen worden aangetroffen:

- CDP, VTP en PAgP updates worden altijd op stammen met een VLAN 1 tag doorgestuurd. Dit is het geval zelfs als VLAN 1 van de trunks is ontruimd en niet het inheemse VLAN is. Als u VLAN 1 voor gebruikersgegevens wisst, heeft de actie geen impact op controlevliegtuigverkeer dat nog met het gebruik van VLAN 1 wordt verzonden.
- Op een ISL romp, worden de pakketten DTP op VLAN1 verzonden. Dit is de zaak zelfs als VLAN 1 van de boomstam is gewist en niet meer het autochtone VLAN. Op een stam van 802.1Q, worden de pakketten DTP op het inheemse VLAN verzonden. Dit is het geval zelfs als het inheemse VLAN van de boomstam is ontruimd.
- In PVST+, worden de 802.1Q IEEE BPDUs verzonden untagged op de gemeenschappelijke Spanning Tree VLAN 1 voor interoperabiliteit met andere verkopers, tenzij VLAN 1 van de boomstam is gewist. Dit is het geval ongeacht de native VLAN-configuratie. Cisco PVST+ BPDU's worden verzonden en gelabeld voor alle andere VLAN's. Zie het gedeelte Spanning Tree Protocol voor meer informatie.
- 802.1s Multiple Spanning Tree (MST) BPDU's worden altijd op VLAN 1 verzonden op zowel ISL- als 802.1Q-trunks. Dit is zelfs van toepassing wanneer VLAN 1 van de trunks wordt ontruimd.
- Schakel VLAN 1 op stammen tussen MST-bruggen en PVST+-bruggen niet uit of uit. Maar in het geval dat VLAN 1 wordt uitgeschakeld, moet de MST-brug wortel worden zodat alle

VLAN's de MST-bridge plaatsing van zijn grenspoorten in de root-inconsistente staat kunnen vermijden. Raadpleeg het gedeelte Multiple Spanning Tree Protocol (802.1s) voor meer informatie.

Standaardfuncties

In dit gedeelte van het document wordt de nadruk gelegd op fundamentele switching-functies die in elke omgeving gemeenschappelijk zijn. Configureer deze functies op alle Cisco IOS-softwarereleases van Catalyst in het klantnetwerk.

VLAN Trunk-protocol

doel

Een VTP-domein, dat ook een VLAN-beheerdomein wordt genoemd, bestaat uit een of meer onderling verbonden switches via een stam die dezelfde VTP-domeinnaam heeft. VTP is ontworpen om gebruikers in staat te stellen om de configuratie van VLAN op één of meer switches centraal te veranderen. VTP communiceert automatisch de veranderingen in alle andere switches in het (netwerk) VTP domein. U kunt een switch configureren om alleen in één VTP-domein te zijn. Voordat u VLAN's maakt, bepaalt u de VTP-modus die in het netwerk gebruikt moet worden.

Overzicht

VTP is een Layer 2-berichtenprotocol. VTP beheert de toevoeging, het wissen en het hernoemen van VLAN's op een netwerkbrede basis om de configuratie van VLAN te handhaven. VTP minimaliseert foute configuraties en configuratie inconsistenties die kunnen leiden tot een aantal problemen. De problemen omvatten dubbele namen van VLAN, onjuiste VLAN-type specificaties, en veiligheidsschendingen.

Standaard is de switch in de VTP server mode en in de no-management domeinstaat. Deze standaardinstellingen veranderen wanneer de switch een advertentie voor een domein via een truntorverbinding ontvangt of wanneer een beheerdomein is geconfigureerd.

VTP-protocol communiceert tussen switches met het gebruik van een bekende Ethernet-bestemming multicast MAC (10-00-0c-cc-cc-c) en SNAP HDLC-protocol type 0x203. Overeenkomstig andere intrinsieke protocollen gebruikt VTP ook een IEEE 802.3 SNAP-insluiting, die LLC 0xABBYY omvat AA03 en OUI 0x00000C. U kunt dit zien op een LAN-analyzer. VTP werkt niet over nonkofferpoorten. Daarom kunnen berichten niet worden verstuurd totdat DTP de romp omhoog heeft gebracht. Met andere woorden, VTP is een lading van ISL of 802.1Q.

Berichttypen zijn:

- Summary Adapters elke 300 seconden (sec)
- Bijkomende advertenties en aanvragen advertenties wanneer er wijzigingen zijn
- Samenvoegen als VTP-pruning is ingeschakeld

Het versienummer van de VTP-configuratie wordt met elke verandering op een server verhoogd en die tabel verspreidt zich over het domein.

Bij het wissen van een VLAN, gaan havens die vroeger een lid van VLAN waren een `inactieve` staat in. Op dezelfde manier worden als een switch in clientmodus niet in staat is de VTP VLAN-

tabel bij het opstarten te ontvangen, hetzij van een VTP-server of een andere VTP-client, alle poorten in VLAN's anders dan het standaard VLAN 1 gedeactiveerd.

U kunt de meeste Catalyst switches configureren om in een van deze VTP-modi te werken:

- Server-in VTP servermodus, kunt u:VLAN's makenVLAN's wijzigenVLAN's verwijderenSpecificeer andere configuratieparameters, zoals VTP-versie en VTP-pruning, voor het gehele VTP-domeinVTP-servers adverteren hun VLAN-configuratie met andere switches in hetzelfde VTP-domein. VTP-servers synchroniseren ook hun VLAN-configuratie met andere switches op basis van advertenties die via trunklinks worden ontvangen. VTP-server is de standaardmodus.
- Client-VTP-cliënten gedragen zich op dezelfde wijze als VTP-servers. Maar u kunt geen VLAN's op een VTP-client maken, wijzigen of verwijderen. Bovendien herinnert de client zich het VLAN na een herstart niet omdat geen informatie van VLAN in NVRAM wordt geschreven.
- Transparent-VTP transparante switches nemen niet deel aan VTP. Een transparante VTP-switch maakt geen reclame voor de VLAN-configuratie en synchroniseert de VLAN-configuratie niet op basis van ontvangen advertenties. Maar in VTP versie 2 sturen transparante switches VTP-advertenties door die de switches hun basisinterfaces ontvangen.

Functie	Server	Clientclient	Doorzichtig	Uit [1]
Source VTP-berichten	Ja	Ja	Nee	—
Luister naar VTP-berichten	Ja	Ja	Nee	—
VLAN's maken	Ja	Nee	Ja (alleen lokaal belangrijk)	—
Denk aan VLAN's	Ja	Nee	Ja (alleen lokaal belangrijk)	—

[1] Cisco IOS-software heeft niet de optie om VTP uit te schakelen met gebruik van de `uit`-modus.

Deze tabel is een samenvatting van de configuratie:

Functie	Standaardwaarde
VTP-domeinnaam	leeg
VTP-modus	Server
VTP-versie	Versie 1 is ingeschakeld
VTP-trunking	Uitgeschakeld

In VTP transparante modus worden VTP-updates simpelweg genegeerd. Het bekende VTP multicast MAC-adres wordt verwijderd van het systeem CAM dat normaal gebruikt wordt om beheerframes op te halen en deze naar de Supervisor Engine te sturen. Omdat het protocol een multicast adres gebruikt, spoelt de switch in transparante modus of een andere verkoper switch het kader eenvoudigweg met andere Cisco-switches in het domein.

VTP versie 2 (VTPv2) omvat de functionele flexibiliteit die deze lijst beschrijft. Maar VTPv2 is niet interoperabel met VTP versie 1 (VTPv1):

- Ondersteuning van Token Ring
- Niet-herkende VTP-informatieondersteuning—Switches verspreiden nu waarden die ze niet kunnen parsen.
- De versie-afhankelijke transparante modus wordt niet langer gecontroleerd door de domeinnaam. Dit maakt ondersteuning van meer dan één domein via een transparant domein mogelijk.
- Versie nummerpropagatie-als VTPv2 op alle switches mogelijk is, kunnen alle switches worden geactiveerd met de configuratie van één enkele switch.

Raadpleeg Inzicht VLAN Trunk Protocol (VTP) voor meer informatie.

VTP-werking in Cisco IOS-software

De configuratieveranderingen in CatOS worden onmiddellijk na een verandering naar NVRAM geschreven. In tegenstelling, slaat Cisco IOS Software geen configuratieveranderingen in NVRAM op tenzij u de opdracht van de **begininstelling van de kopieerrun** geeft. VTP client- en serversystemen vereisen dat VTP-updates van andere VTP-servers direct worden opgeslagen in NVRAM zonder tussenkomst van de gebruiker. Aan de vereisten van de VTP-update wordt door de standaard CatOS-handeling voldaan, maar het Cisco IOS-model voor de bijwerking van de software vereist een alternatieve update-handeling.

Voor deze verandering, werd een VLAN gegevensbestand geïntroduceerd in Cisco IOS Software voor Catalyst 6500 als methode om VTP updates voor VTP cliënten en servers onmiddellijk op te slaan. In sommige versies van software, is deze VLAN databank in de vorm van een afzonderlijk bestand in NVRAM, het vlan.dat bestand genoemd. Controleer uw softwareversie om te bepalen of er een back-up van de VLAN-database nodig is. U kunt VTP/VLAN-informatie bekijken die in het VLAN.dat-bestand voor de VTP-client of VTP-server is opgeslagen als u de opdracht **vtp-status** geeft.

De volledige configuratie VTP/VLAN wordt niet opgeslagen in het opstartconfiguratiebestand in NVRAM wanneer u de opdracht van de **begininstelling van** de **kopie** op deze systemen geeft. Dit is niet van toepassing op systemen die als transparant VTP werken. VTP transparante systemen bewaar de volledige configuratie van VTP/VLAN aan het opstartconfiguratiebestand in NVRAM wanneer u de opdracht **van de** begininstelling van de **kopieerrun** geeft.

In Cisco IOS-softwarereleases die eerder zijn dan Cisco IOS-softwarerelease 12.1(11b)E, kunt u VTP en VLAN's alleen configureren via de VLAN-databases. De VLAN-databases zijn een aparte modus voor de wereldwijde configuratiemodus. De reden voor deze configuratievereiste is dat, wanneer u het apparaat in de VTP mode server of VTP mode client vormt, de buren van VTP de VLAN databank dynamisch via VTP advertenties kunnen bijwerken. U wilt niet dat deze updates automatisch tot de configuratie overgaan. Daarom worden de VLAN-database en de VTP-informatie niet opgeslagen in de hoofdconfiguratie, maar opgeslagen in NVRAM in een bestand met de naam vlan.dat.

Dit voorbeeld toont hoe te om een Ethernet VLAN in de gegevensbank van VLAN te creëren:

```
Switch#vlan database
Switch(vlan)#vlan 3
VLAN 3 added:
Name: VLAN0003
Switch(vlan)#exit
APPLY completed.
```

```
Exiting....
```

In Cisco IOS-softwarerelease 12.1(11b)E en later kunt u VTP en VLAN's configureren via VLAN-databases of via de mondiale configuratiemodus. Op VTP mode server of VTP wijze transparant, werkt de configuratie van VLANs nog het vlan.dat dossier in NVRAM bij. Deze opdrachten worden echter niet in de configuratie opgeslagen. Daarom tonen de opdrachten niet in de actieve configuratie.

Raadpleeg het gedeelte *VLAN-configuratie in* de *Global Configuration-modus* van het document VLAN's configureren voor meer informatie.

Dit voorbeeld toont hoe te om een Ethernet VLAN in mondiale configuratiewijze te creëren en hoe te om de configuratie te verifiëren:

```
Switch#configure terminal
Switch(config#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config#vlan 3
Switch(config-vlan)#end
Switch#
OR
Switch#vlan database
Switch(vlan#vtp server
Switch device to VTP SERVER mode.
Switch(vlan#vlan 3
Switch(vlan#exit
APPLY completed.
Exiting....
Switch#
```

Opmerking: de VLAN-configuratie is opgeslagen in het bestand vlan.dat, dat in niet-vluchtig geheugen is opgeslagen. Om een volledige back-up van uw configuratie uit te voeren, neemt u het bestand vlan.dat in de back-up op, samen met de configuratie. Als de gehele switch of de module van de Supervisor Engine moet worden vervangen, moet de netwerkbeheerder beide bestanden uploaden om de volledige configuratie te kunnen herstellen:

- Het bestand vlan.dat
- Het configuratiebestand

VTP- en uitgebreide VLAN's

De functie Uitgebreide System-ID wordt gebruikt om VLAN-identificatie met uitgebreid bereik mogelijk te maken. Als Uitgebreide System-ID is ingeschakeld, schakelt deze de pool van MAC-adressen in die worden gebruikt voor de VLAN-overspannende boom en laat één MAC-adres achter dat de switch identificeert. Catalyst IOS-softwarerelease 12.1(11b)EX en 12.1(13)E introduceren uitgebreide ondersteuning voor Catalyst 6000/6500 om 4096 VLAN's te ondersteunen overeenkomstig de IEEE 802.1Q-standaard. Deze optie wordt geïntroduceerd in Cisco IOS-softwarerelease 12.1(12c)EW voor Catalyst 4000/4500 switches. Deze VLAN's zijn georganiseerd in verschillende reeksen, die elk verschillend kunnen worden gebruikt. Sommige van deze VLAN's worden naar andere switches in het netwerk verspreid wanneer u de VTP gebruikt. De VLAN's met uitgebreid bereik worden niet verspreid, dus u moet uitgebreide-bereik VLAN's handmatig op elk netwerkapparaat configureren. Deze uitgebreide optie van het Systeem ID is gelijk aan de optie MAC Address Reduction in Catalyst OS.

In deze tabel worden de VLAN-marges beschreven:

VLAN's	Bereik	Gebruik	Verspreid door VTP?
0 4095	voorbehouden	Uitsluitend voor systeemgebruik. U kunt deze VLAN's niet zien of gebruiken.	—
1	Normaal	Standaard Cisco. U kunt dit VLAN gebruiken, maar u kunt het niet verwijderen.	Ja
2–1001	Normaal	Voor Ethernet VLAN's. U kunt deze VLAN's maken, gebruiken en verwijderen.	Ja
1002–1005	Normaal	Standaardwaarden voor Cisco FDDI en Token Ring. U kunt VLAN's 1002-1005 niet verwijderen.	Ja
1006–4094	voorbehouden	Alleen voor Ethernet VLAN's.	Nee

Switch protocollen gebruiken een MAC-adres dat is overgenomen van een bank met beschikbare adressen die een EPROM op de chassis verstrekt als deel van bridge-identificatoren voor VLAN's die onder PVST+ en RPVST+ lopen. Catalyst 6000/6500 en Catalyst 4000/4500 switches ondersteunen 1024 of 64 MAC-adressen die afhankelijk zijn van het chassis type.

Catalyst switches met 1024 MAC-adressen maken uitgebreide systeem-ID standaard niet mogelijk. MAC-adressen worden sequentieel toegewezen, waarbij het eerste MAC-adres in het bereik is toegewezen aan VLAN 1, het tweede MAC-adres in het bereik toegewezen aan VLAN 2, enzovoort. Dit stelt de switches in om 1024 VLAN's te ondersteunen en elk VLAN gebruikt een unieke bridge identifier.

Type chassis	Chassis-adres
WS-C4003-S1, WS-C4006-S2	1024
WS-C4503, WS-C4506	641
WS-C6509-E, WS-C6509, WS-C6509-NEB, WS-C6506-E, WS-C6506, WS-C6009, WS-C6006, OSR-760 9-AC, OSR-7609-DC	1024
WS-C6513, WS-C6509-NEB-A, WS-C6504-E, WS-C6503-E, WS-C6503, CISCO7603, CISCO7606, CISCO76 09, CISCO 7613	641

[1] Chassis met 64 MAC-adressen maakt het mogelijk dat de id standaard uitgebreid is en dat de functie niet kan worden uitgeschakeld.

Raadpleeg het gedeelte *Bridge ID* van de configuratie van STP en IEEE 802.1s MST voor meer informatie.

Voor Catalyst serie switches met 1024 MAC-adressen, om uitgebreide systeem-ID in te

schakelen, maakt ondersteuning van 4096 VLAN's die werken onder PVST+ of 16 MISTP-instanties mogelijk om unieke identificatoren te hebben zonder de toename van het aantal MAC-adressen dat op de switch vereist is. Uitgebreide System-ID vermindert het aantal MAC-adressen die door STP vereist zijn van één per VLAN of MISTP-instantie naar één per switch.

Dit getal toont de bridge identifier wanneer uitgebreide ID van het systeem niet is ingeschakeld. De bridge identifier bestaat uit een overbruggingsprioriteit van 2 bytes en een MAC-adres van 6 bytes.

Extended System ID wijzigt het Spanning Tree Protocol (STP) Bridge Identifier-gedeelte van de Bridge Protocol Data Units (BPDU). Het oorspronkelijke prioriteitsveld van 2 bytes wordt in 2 velden verdeeld; Een prioriteitsveld met 4 bits en een 12-bits systeem-ID-uitbreiding waarmee VLAN-nummering van 0-4095 mogelijk is.

Wanneer uitgebreide System-ID op Catalyst switches is ingeschakeld om bereik van VLAN's uit te breiden, moet deze op alle switches binnen hetzelfde STP-domein zijn ingeschakeld. Dit is nodig om de STP root berekeningen op alle switches consistent te houden. Als uitgebreide ID voor het systeem is ingeschakeld, wordt de root-brug-prioriteit een veelvoud van 4096 plus de VLAN-id. Switches zonder uitgebreide id van het systeem kunnen mogelijk onopzettelijk wortel schieten omdat ze een fijnere granulariteit hebben in de selectie van hun bridge-ID.

Terwijl het wordt aanbevolen om consistente uitgebreide systeem-ID-configuratie binnen hetzelfde STP-domein te handhaven, is het niet praktisch om uitgebreide systeem-ID op alle netwerkapparaten af te dwingen wanneer u een nieuw chassis met 64 MAC-adres in het STP-domein introduceert. Maar het is belangrijk om te begrijpen wanneer twee systemen met de zelfde Spanning-Boom prioriteit worden gevormd, heeft het systeem zonder Uitgebreide Systeem ID een betere Spanning-Boom prioriteit. Geef deze opdracht uit om uitgebreide systeem-ID-configuratie mogelijk te maken:

in-boom-extender systeem-id

De interne VLAN's worden in oplopende volgorde toegewezen, vanaf VLAN 1006. Het wordt aanbevolen de gebruiker VLAN's zo dicht mogelijk bij VLAN 4094 toe te wijzen om conflicten tussen de gebruiker VLAN's en de interne VLAN's te voorkomen. Geef het commando uit **om VLAN intern gebruik** op een switch te **tonen** om de intern toegewezen VLAN's weer te geven.

```
Switch#show vlan internal usage

VLAN Usage
---- --------------------
1006 online diag vlan0
1007 online diag vlan1
1008 online diag vlan2
1009 online diag vlan3
```

```
1010 online diag vlan4
1011 online diag vlan5
1012 PM vlan process (trunk tagging)
1013 Port-channel100
1014 Control Plane Protection
1015 L3 multicast partial shortcuts for VPN 0
1016 vrf_0_vlan0
1017 Egress internal vlan
1018 Multicast VPN 0 QOS vlan
1019 IPv6 Multicast Egress multicast
1020 GigabitEthernet5/1
1021 ATM7/0/0
1022 ATM7/0/0.1
1023 FastEthernet3/1
1024 FastEthernet3/2
------deleted------
```

In native IOS kan het **VLAN-interne toewijzingsbeleid** naar **beneden** worden geconfigureerd zodat de interne VLAN's in dalende volgorde worden toegewezen. Het CLI-equivalent voor CatOS-software wordt niet officieel ondersteund.

vlan intern toewijzingsbeleid nadert

Cisco-configuratie-aanbeveling

VLAN's kunnen worden gemaakt wanneer een Catalyst 6500/6000 in VTP-servermodus is, zelfs zonder VTP-domeinnaam. Configureer eerst de VTP-domeinnaam voordat u VLAN's configureren op Catalyst 6500/6000 switches die Cisco IOS-systeemsoftware uitvoeren. Configuratie in deze volgorde zorgt voor consistentie met andere Catalyst switches die CatOS uitvoeren.

Er is geen specifieke aanbeveling over het al dan niet gebruiken van VTP client/server modi of VTP `transparante` modus. Sommige klanten geven de voorkeur aan het gemak van het beheer van VTP client/server mode, ondanks enkele overwegingen die in deze sectie worden opgemerkt. De aanbeveling is om in elk domein twee switches van de servermodus te hebben voor redundantie, meestal de twee switches van de distributielaag. Stel de rest van de switches in het domein in op de clientmodus. Wanneer u client/server mode met het gebruik van VTPv2 uitvoert, vergeet dan dat een hoger herzieningsnummer altijd in hetzelfde VTP-domein wordt geaccepteerd. Als een switch die is geconfigureerd in de VTP-client of in de servermodus in het VTP-domein wordt geïntroduceerd en een hoger revisienummer heeft dan de VTP-servers die bestaat, overschrijft dit de VLAN-database binnen het VTP-domein. Als de configuratieverandering onbedoeld is en VLAN's worden verwijderd, kan deze overschreven betekenen dat er een grote storing in het netwerk optreedt. Om ervoor te zorgen dat client of server switches altijd een configuratie revisie getal hebben dat lager is dan dat van de server, verander de client-VTP domeinnaam in iets anders dan de standaardnaam, en keer dan terug naar de standaard. Deze actie stelt de configuratie herziening op de client in op 0.

Er zijn voor- en nadelen aan de VTP-mogelijkheid om gemakkelijk wijzigingen aan te brengen in een netwerk. Veel ondernemingen geven de voorkeur aan een voorzichtige benadering en gebruiken om deze redenen `transparante VTP-`wijze:

- Deze praktijk stimuleert een goede veranderingscontrole omdat de eis om een VLAN op een switch of boomhaven aan te passen als één switch tegelijkertijd moet worden beschouwd.
- VTP transparante modus beperkt het risico van een beheerderfout, zoals het per ongeluk wissen van een VLAN. Zulke fouten kunnen het gehele domein beïnvloeden.
- VLAN's kunnen van trunks naar switches worden gesnoeid die geen poorten in het VLAN

hebben. Dit leidt tot een overstroming van het kader om bandbreedte-efficiënter te zijn. Handmatig snoeien heeft ook een kleinere overspanningsboomdiameter. Zie het gedeelte Dynamic Trunking Protocol voor meer informatie. Een configuratie per switch van VLAN moedigt deze praktijk ook aan.

- Er is geen risico van de introductie in het netwerk van een nieuwe switch met een hoger VTP-herzieningsnummer dat de gehele VLAN-configuratie overschrijft.
- Cisco IOS-software VTP-transparante modus wordt ondersteund in Campus Manager 3.2, dat deel uitmaakt van CiscoWorks2000. De eerdere beperking die u vereist dat u minimaal één server in een VTP-domein hebt, is verwijderd.

VTP-opdrachten	**Opmerkingen**
vtp-*domeinnaam*	CDP controleert de naam om te helpen voorkomen dat er fouten ontstaan tussen de domeinen. Domain Name is hoofdlettergevoelig.
VTP-modus {server | cliënt | transparant	VTP werkt op een van de drie modi.
VLAN *vlan_number*	Dit creëert een VLAN met de opgegeven ID.
toegestane switchpoort *vlan_range*	Dit is een interfaceopdracht die stammen in staat stelt om VLAN's te dragen waar nodig. Het standaard is alle VLAN's.
Switch-poort stam pruning *vlan_range*	Dit is een interfaceopdracht die de STP diameter door handdruk beperkt, zoals op stammen van de distributielaag aan toegangslaag, waar VLAN niet bestaat. Standaard zijn alle VLAN's prune-verkiesbaar.

Andere opties

VTPv2 is een vereiste in Token Ring-omgevingen, waar client/server-modus sterk aanbevolen is.

De sectie Cisco Configuration Aanbeveling van dit document bepleit de voordelen van het afdrukken van VLAN's om onnodige frame-overstromingen te voorkomen. De **vtp pruning**-opdracht snoeit VLAN's automatisch, wat de inefficiënte overstroming van frames tegenhoudt waar deze niet nodig zijn.

Opmerking: in tegenstelling tot handmatig afvoeren van VLAN beperkt automatisch afdrukken de overspannende-boomdiameter niet.

De IEEE heeft een op standaarden gebaseerde architectuur geproduceerd om VTP-vergelijkbare resultaten te bereiken. Als lid van het 802.1Q Generic Character Registration Protocol (GARP), maakt het Generic VLAN Registration Protocol (GVRP) VLAN-beheerinteroperabiliteit tussen verkopers mogelijk. GVRP is echter niet binnen het toepassingsgebied van dit document.

Opmerking: Cisco IOS-software heeft geen VTP uit-mode-mogelijkheid en ondersteunt alleen VTPv1 en VTPv2 met pruning.

Fast Ethernet-automatisering

doel

Automatische onderhandeling is een optionele functie van de IEEE 802.3u Fast Ethernet (FE) standaard. Automatische onderhandeling stelt apparaten in om automatisch informatie over snelheid en duplexvermogens over een verbinding uit te wisselen. Automatische onderhandeling werkt op Layer 1 (L1). De functie is gericht op poorten die worden toegewezen aan gebieden waar voorbijgaande gebruikers of apparaten met een netwerk verbonden zijn. De voorbeelden omvatten switches en knooppunten van de toegangslaag.

Overzicht

Automatische onderhandeling gebruikt een aangepaste versie van de test van de link integriteit voor 10BASE-T apparaten om snelheid te onderhandelen en andere autonome onderhandelingsparameters te ruilen. De oorspronkelijke test van de 10BASE-T-link wordt aangeduid als de normale Link Pulse (NLP). De aangepaste versie van de test van de verbindingsintegriteit voor 10/100-Mbps autonegotiation wordt aangeduid als Fast Link Pulse (FLP). De 10BASE-T apparaten verwachten een burst pulse elke 16 (+/-8) milliseconden (ms) als deel van de link integriteit test. FLP voor 10/100-Mbps autonome onderhandeling verstuurt deze bursten elke 16 (+/-8) ms met de extra pulsen elke 62,5 (+/-7) microseconden. De pulsen binnen de burst sequentie genereren codewoorden die gebruikt worden voor comptabiliteitsuitwisselingen tussen link partners.

In 10BASE-T wordt een link pols uitgezonden wanneer een station komt. Dit is één puls die elke 16 ms wordt verstuurd. De 10BASE-T apparaten verzenden ook een verbindingspuls elke 16 ms wanneer de link leeg is. Deze link pulsen worden ook hartslag of NLP genoemd.

Een 100BASE-T apparaat stuurt FLP uit. Deze puls wordt uitgezonden als een uitbarsting in plaats van één puls. De breuk wordt binnen 2 ms voltooid en elke 16 ms opnieuw. Na initialisering, geeft het apparaat een 16-bits FLP-bericht aan de venkelner door voor de onderhandeling van snelheid, duplex en stroomcontrole. Dit 16-bits bericht wordt herhaaldelijk verzonden totdat het bericht door de partner wordt erkend.

N.B.: Zoals in de specificatie van IEEE 802.3u, kunt u geen één verbindingspartner voor 100-Mbps volledig duplex handmatig configureren en nog steeds zelfstandig aan volledig duplex met de andere vennoot. Een poging om één verbindingspartner voor 100-Mbps volledig te vormen en de andere verbindingspartner voor autonomie resulteert in een duplex mismatch. Dubbele mismatch resultaten omdat één link partner autonegotiates en geen autonome onderhandelingsparameters van de andere link partner ziet. De eerste partner van de link is dan op de helft in duplex gestort.

Alle Catalyst 6500 Ethernet switchmodules ondersteunen 10/100 Mbps en half duplex of volledig

duplex. Geef de opdracht **show interface mogelijkheden uit** om deze functionaliteit op andere Catalyst switches te verifiëren.

Een van de meest algemene oorzaken van prestatiekwesties op 10/100 Mbps Ethernet verbindingen komt voor wanneer één poort op de verbinding bij half duplex werkt terwijl de andere poort bij volledig duplex werkt. Deze situatie gebeurt af en toe wanneer u een of beide poorten op een link terugstelt en het autonome onderhandelingsproces niet resulteert in dezelfde configuratie voor beide partners. De situatie gebeurt ook wanneer u de ene kant van een link opnieuw instelt en vergeet de andere kant opnieuw te configureren. U kunt de noodzaak om prestatiegerelateerde ondersteuningsoproepen te plaatsen vermijden als u:

- Maak een beleid dat de configuratie van poorten vereist voor het vereiste gedrag voor alle niet-transiente apparaten
- Handhaving van het beleid door adequate maatregelen om de veranderingen te beheersen

Typische symptomen van de prestatiekwestie toename frame check sequentie (FCS), cyclische redundantie controle (CRC), uitlijning of runt tellers op de switch.

In de halve duplexmodus hebt u één paar ontvangen en één paar zenddraden. Beide draden kunnen niet tegelijkertijd worden gebruikt. Het apparaat kan niet verzenden wanneer er een pakket aan de ontvangstzijde is.

In de volledige duplexmodus hebt u hetzelfde paar bedradingen ontvangen en verzenden. Beide kunnen echter tegelijkertijd worden gebruikt omdat de functies Carrier Sense en Botsing Detect zijn uitgeschakeld. Het apparaat kan tegelijkertijd verzenden en ontvangen.

Daarom werkt een half-duplex aan volledig-duplex verbinding, maar er is een groot aantal botsingen aan de half-duplex kant die in slechte prestaties resulteren. De botsingen komen voor omdat het apparaat dat als volledige duplex wordt gevormd op het zelfde moment kan verzenden dat het apparaat gegevens ontvangt.

De documenten in deze lijst bespreken in detail de autonome onderhandelingen. Deze documenten leggen uit hoe autonomie werkt en bespreken verschillende configuratieopties:

- Automatische onderhandeling voor Ethernet 10/100/1000 Mb half/full duplex configureren en problemen ermee oplossen
- Troubleshooting Cisco Catalyst Switches to NIC Compatibility Issues (NIC-compatibiliteitsproblemen bij Cisco Catalyst-switches oplossen)

Een gemeenschappelijk misconceptie over autonegotiation is dat het mogelijk is om één verbindingspartner voor 100-Mbps volledig te vormen en autonegotiate aan volledig duplex met de andere verbindingspartner te vormen. Een poging om dit voor elkaar te krijgen resulteert in een dubbele wanverhouding. Dit is een gevolg omdat één verbinding partner autonegotiates, geen autonome onderhandelingsparameters van de andere verbindingspartner ziet, en defaults aan half duplex.

De meeste Catalyst Ethernet modules steunen 10/100 Mbps en half/volledig duplex. U kunt dit echter bevestigen als u de opdracht *Mod/Port*-**functies** van de **show-*interface*** geeft.

FEFI

Verre eindfoutmelding (FEFI) beschermt 100BASE-FX (glasvezel) en Gigabit interfaces, terwijl autonome onderhandeling 100BASE-TX (koper) beschermt tegen fysieke

laag/signaleringsgerelateerde fouten.

Een fout aan het eind is een fout in de verbinding die het één station kan detecteren terwijl het andere station niet kan. Een niet aangesloten zenddraad is een voorbeeld. In dit voorbeeld ontvangt het verzendende station nog geldige gegevens en detecteert het dat de link goed is via de monitor van de verbindingsintegriteit. Het verzendende station kan echter niet ontdekken dat het andere station de transmissie niet ontvangt. Een 100BASE-FX-station dat zo'n externe fout detecteert, kan de verzonden `IDLE`-stroom wijzigen om een speciaal bitpatroon te verzenden om de buurman van de externe fout op de hoogte te stellen. Het speciale bitpatroon wordt aangeduid als het `FEFI-IDLE` patroon. Het `FEFI-IDLE` patroon zet vervolgens een sluiting van de externe poort (`errOff`) in. Raadpleeg het gedeelte UniDirectional Link Detectie in dit document voor meer informatie over foutbescherming.

Deze modules/hardwareondersteuning FEFI:

- Catalyst 6500/6000 en 4500/4000:Alle 100BASE-FX modules en GE modules

Cisco-poortaanbeveling voor infrastructuur

Of u autonoom-onderhandeling kunt configureren op 10/100-Mbps links of op harde codesnelheid en duplex uiteindelijk hangt af van het type van de partner of het eindapparaat dat u hebt aangesloten op een poort van de switch van Catalyst. Autonome onderhandelingen tussen eindapparaten en Catalyst switches werken over het algemeen goed en Catalyst switches zijn compatibel met de IEEE 802.3u-specificatie. Wanneer de switches van de netwerkinterfacekaart (NIC) of van de verkoper niet precies in overeenstemming zijn, kunnen problemen resulteren. Bovendien kunnen leverancierspecifieke geavanceerde functies die niet worden beschreven in de IEEE 802.3u-specificatie voor 10/100 Mbps autonomie hardwareoncompatibiliteit en andere problemen veroorzaken. Deze geavanceerde functies zijn onder meer autopolariteit en kabelintegriteit. Dit document geeft een voorbeeld:

- Veldwaarschuwing: Prestatieprobleem met Intel Pro/1000T-NIC's die worden aangesloten op CAT4K/6K

In sommige situaties, moet u host, poortsnelheid en duplex instellen. Voltooi in het algemeen deze basisstappen voor het oplossen van problemen:

- Zorg ervoor dat de autonomie aan beide kanten van de link is ingesteld of dat de harde codering aan beide kanten is ingesteld.
- Controleer de opmerkingen voor algemene voorbehouden.
- Controleer de versie van het NIC-stuurprogramma of het besturingssysteem dat u gebruikt. Het laatste stuurprogramma of de laatste pleister is vaak nodig.

Als regel, gebruik eerst autonome onderhandeling voor elk type van verbindingspartner. Er zijn duidelijke voordelen voor de configuratie van autonome onderhandeling voor transient devices zoals laptops. Autononderhandeling werkt ook goed met andere apparaten, bijvoorbeeld:

- Met niet-transitionele apparaten zoals servers en vaste werkstations
- Van switch tot switch
- Van switch naar router

Maar om een aantal van de redenen dat dit paragraaf vermeldt kunnen zich onderhandelingskwesties voordoen. Raadpleeg de automatische onderhandeling over de configuratie en probleemoplossing van Ethernet 10/100/1000MB/1000Base-T voor automatische onderhandeling over de basisstappen voor het oplossen van problemen in deze gevallen.

Autonoom uitschakelen voor:

- poorten die netwerkinfrastructuurapparaten zoals switches en routers ondersteunen
- Andere niet-transitieve eindsystemen zoals servers en printers

Altijd moeilijk de snelheid en duplexinstellingen voor deze poorten te coderen.

Stel deze 10/100 Mbps verbindingsconfiguraties handmatig in voor snelheid en duplex, die gewoonlijk 100 Mbps volledig complex zijn:

- Switch-naar-switch
- Switch-naar-server
- Switch-naar-router

Als de poortsnelheid wordt ingesteld op auto op een 10/100 Mbps Ethernet poort, worden zowel de snelheid als de duplex autonegotiveerd. Geef deze interfaceopdracht uit om de poort in te stellen op auto:

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed auto
!--- This is the default.
```

Geef deze interfaceopdrachten uit om snelheid en duplex te configureren:

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed {10 | 100 | auto}
Switch(config-if)#duplex {full | half}
```

Cisco Access-poortaanbevelingen

Eindgebruikers, mobiele arbeiders, en tijdelijke gastheren hebben behoefte aan autonome onderhandeling om beheer van deze gastheren te minimaliseren. U kunt ook autonomie-onderhandeling maken met Catalyst switches. De meest recente NIC-stuurprogramma's zijn vaak vereist.

Geef deze globale opdrachten uit om autonegonderhandeling van snelheid voor de haven mogelijk te maken:

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed auto
```

Opmerking: Als u de poortsnelheid op auto op een 10/100 Mbps Ethernet poort instelt, worden zowel snelheid als duplex automatisch geregisseerd. U kunt de duplexmodus van de autonomiepoorten niet wijzigen.

Wanneer NIC's of leveranciersslangen niet precies aan de specificatie van IEEE 802.3u voldoen, kunnen problemen resulteren. Bovendien kunnen leverancierspecifieke geavanceerde functies die niet worden beschreven in de IEEE 802.3u-specificatie voor 10/100 Mbps autonomie hardwareoncompatibiliteit en andere problemen veroorzaken. Tot deze geavanceerde functies behoren autopolariteit en kabelintegriteit.

Andere opties

Wanneer de autonome onderhandeling tussen switches wordt uitgeschakeld, kan Layer 1-foutmelding ook bij bepaalde problemen verloren gaan. Gebruik Layer 2-protocollen om de detectie van fouten te verbeteren, zoals agressieve UDLD.

Autononderhandeling detecteert deze situaties niet, zelfs niet wanneer autonome onderhandelingen zijn ingeschakeld:

- De poorten zitten vast en ontvangen of verzenden niet
- De ene kant van de lijn is omhoog, maar de andere kant is omlaag gegaan
- Glasvezelkabels zijn niet goed bedraad

Deze problemen worden niet door de autonome onderhandelingen opgespoord omdat ze niet op de fysieke laag staan. De problemen kunnen leiden tot STP-mazen of zwarte gaten in het verkeer.

UDLD kan al deze gevallen detecteren en beide poorten op de link uitschakelen, als UDLD op beide uiteinden is geconfigureerd. Op deze manier voorkomt UDLD dat er sprake is van loops en zwarte gaten in het verkeer.

Gigabit Ethernet-automatisering

doel

Gigabit Ethernet (GE) heeft een autonome onderhandelingsprocedure die uitgebreider is dan de procedure die voor 10/100-Mbps Ethernet (IEEE 802.3z) wordt gebruikt. Met GE poorten wordt autonegotiation gebruikt voor uitwisseling:

- Stroomregelingsparameters
- Informatie over externe fout
- Dubbele informatie**Opmerking:** Catalyst serie GE poorten ondersteunen alleen full duplex mode.

IEEE 802.3z is vervangen door IEEE 802.3:2000-specificaties. Raadpleeg het abonnement op Local and Metropolitan Area Networks + Drafts (LAN/MAN 802s) Standards voor meer informatie.

Overzicht

In tegenstelling tot autonome onderhandeling met 10/100-Mbps FE, vereist GE autonome onderhandeling niet de onderhandeling over poortsnelheid. U kunt ook de **ingestelde** poortsnelheid niet uitgeven om autonegotiation uit te schakelen. GE poort onderhandeling is standaard ingeschakeld en de poorten op beide uiteinden van een GE link moeten dezelfde instelling hebben. De verbinding komt niet naar voren als de havens aan elk eind van de verbinding niet consistent zijn ingesteld, wat betekent dat de uitgewisselde parameters verschillend zijn.

Bijvoorbeeld, veronderstel dat er twee apparaten zijn, A en B. Elk apparaat kan autonegotiation aan of uitgeschakeld hebben. Dit is een tabel met mogelijke configuraties en hun respectieve verbindingsstaten:

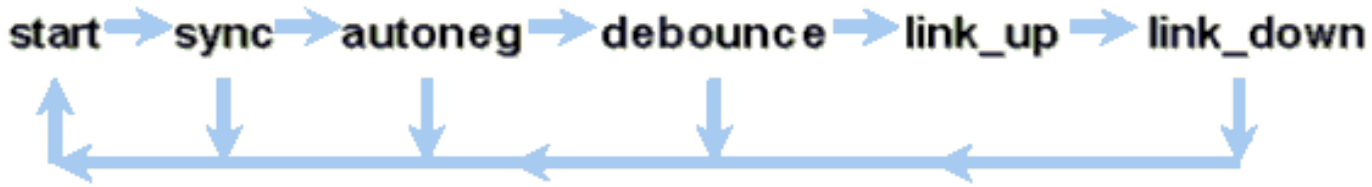
onderhandeling	B ingeschakeld	B Uitgeschakeld
Ingeschakeld	aan beide zijden	Een `beneden`, B `omhoog`
Een handicap	Een `omhoog`, B	aan beide zijden

	omlaag	

In GE, worden de synchronisatie en de autonome onderhandeling (als zij worden toegelaten) uitgevoerd bij verbinding opstarten door het gebruik van een speciale reeks gereserveerde woorden van de verbindingscode.

Opmerking: er is een woordenboek van geldige woorden en niet alle mogelijke woorden zijn geldig in GE.

De levensduur van een GE-verbinding kan als volgt worden gekarakteriseerd:



Een synchronisatieverlies betekent dat de MAC een link onderkent. Het synchronisatieverlies is van toepassing, ongeacht of het autonegotiation is ingeschakeld of uitgeschakeld. De synchronisatie is verloren onder bepaalde mislukte voorwaarden, zoals het ontvangen van drie ongeldige woorden in opeenvolging. Als deze conditie 10 ms blijft bestaan, wordt een sync faalconditie opgehaald en wordt de link veranderd in de `link_down` status. Nadat de synchronisatie is verloren, zijn er nog drie opeenvolgende geldige idles nodig om te resynchroniseren. Andere catastrofale gebeurtenissen, zoals een ontvangstsignaal (Rx) verlies, veroorzaken een link-down gebeurtenis.

Autononderhandeling is een onderdeel van het koppelingsproces. Wanneer de link omhoog is, is de autonome onderhandeling voorbij. De switch controleert echter nog steeds de status van de link. Als de autonome onderhandeling op een haven wordt uitgeschakeld, is de autonome fase niet langer een optie.

De GE koperspecificatie (1000BASE-T) ondersteunt autonome onderhandeling via een Next Page Exchange. Next Page Exchange maakt autonome onderhandeling mogelijk voor snelheden van 10/100/1000 Mbps op koperpoorten.

Opmerking: De GE-glasvezelspecificatie bevat echter alleen bepalingen voor het onderhandelen over duplex, stroomregeling en detectie van fouten op afstand. GE-glasvezelhavens onderhandelen niet over poortsnelheid. Raadpleeg de secties 28 en 37 van de specificatie IEEE 802.3-2002 voor meer informatie over autonomie.

De vertraging van het opnieuw opstarten van de synchronisatie is een softwarefunctie die de totale autonome onderhandelingstijd controleert. Als autonegotiation niet binnen deze tijd succesvol is, start de software opnieuw autonegotiation in geval er een impasse is. De opdracht **sync-start-start-vertraging** heeft alleen een effect als de autonomie is ingesteld om in te schakelen.

Cisco-poortaanbeveling voor infrastructuur

De configuratie van de autonomie is veel kritischer in een GE-omgeving dan in een 10/100 Mbps-omgeving. Alleen autonoom uitschakelen in deze situaties:

- Op switch poorten die aangesloten zijn op apparaten die onderhandeling niet kunnen ondersteunen

- Waar aansluitingsproblemen het gevolg zijn van interoperabiliteitsproblemen

Gigabit-onderhandeling inschakelen voor alle switch-to-switch links en, in het algemeen, voor alle GE-apparaten. De standaardwaarde op Gigabit interfaces is autonegotisering. Geef deze opdracht echter uit om er zeker van te zijn dat de autonome onderhandeling is ingeschakeld:

```
switch(config)#interface type slot/port
switch(config-If)#no speed
!--- This command sets the port to autonegotiate Gigabit parameters.
```

Eén bekende uitzondering is wanneer u verbinding maakt met een Gigabit Switch Router (GSR) die Cisco IOS-software draait die vroeger is dan Cisco IOS-softwarerelease 12.0(10)S, de release die stroomcontrole en autonomie toevoegt. Schakel deze twee functies uit. Als u deze functies niet uitschakelt, meldt de switch-poort niet aangesloten en rapporteert de GSR fouten. Dit is een sequentie van de steekproefinterface-opdracht:

```
flowcontrol receive off
flowcontrol send off
speed nonegotiate
```

Cisco Access-poortaanbevelingen

Aangezien FLPs tussen verkopers kan variëren, moet u de switch-aan-server verbindingen per geval bekijken. Cisco-klanten hebben problemen ondervonden met Gigabit onderhandeling op Sun, HP en IBM-servers. Laat alle apparaten de Gigabit-autonomie gebruiken tenzij de NIC-verkoper anders bepaalt.

Andere opties

Flow control is een optioneel onderdeel van de 802.3x-specificatie. De stroomregeling moet worden onderhandeld als je het gebruikt. Apparaten kunnen of kunnen onmogelijk naar een PAUSE-frame sturen en/of reageren (bekende MAC 01-80-C2-00-00-00 0F). En apparaten kunnen onmogelijk akkoord gaan met het flow-control verzoek van de verre buurman. Een poort met een invoerbuffer die begint op te vullen, verstuurt een PAUSE-kader naar de link partner. De verbindingspartner stopt de transmissie en houdt om het even welke extra kaders in de de uitvoerbuffers van de verbindingspartner vast. Deze functie lost geen problemen op met overabonnementen tussen de staten. Maar de functie maakt de invoerbuffer in feite groter door een fractie van de partneroutput buffer door middel van een uitbarsting.

De PAUSE-functie is ontworpen om de onnodige teruggooi van ontvangen frames door apparaten (switches, routers, of eindstations) door bufferoverloop te voorkomen vanwege de omstandigheden van tijdelijke verkeersoverbelasting op korte termijn. Een apparaat onder verkeersoverbelasting voorkomt interne bufferoverloop wanneer het apparaat een PAUSE-frame verstuurt. Het kader van PAUSE bevat een parameter die de lengte van tijd voor de volledige duplexpartner aangeeft om te wachten alvorens de partner meer gegevensframes verstuurt. De partner die het PAUSE-kader ontvangt, stuurt geen gegevens meer voor de gespecificeerde periode. Wanneer deze timer afloopt, begint het station opnieuw gegevensframes te versturen, van waar het station vertrok.

Een station dat een PAUSE (Pauze) uitgeeft kan een ander PAUSE frame uitgeven dat een parameter van nul tijd bevat. Met deze actie wordt de rest van de pauzatieperiode geannuleerd.

Een nieuw ontvangen PAUSE-frame heeft dus voorrang op elke PAUSE-handeling die momenteel wordt uitgevoerd. Ook kan het station dat het PAUSE-frame geeft de PAUZE-periode verlengen. Het station geeft een ander PAUSE frame uit dat een niet-nulpunt tijdparameter bevat vóór het verstrijken van de eerste PAUZE-periode.

Deze PAUSE-handeling is geen op snelheid gebaseerde stroomregeling. De bewerking is een eenvoudig start-stop mechanisme waarmee het apparaat onder verkeer, dat het PAUSE-frame heeft verstuurd, de kans krijgt om de buffercongestie te verminderen.

Het beste gebruik van deze optie is op verbindingen tussen toegangsppoorten en eindhosts, waar de buffer van de host-uitvoer potentieel even groot is als het virtuele geheugen. Switch-tot-switch gebruik heeft beperkte voordelen.

Geef deze interfaceopdrachten uit om dit in de switch-poorten te controleren:

```
flowcontrol {receive | send} {off | on | desired}
```

```
>show port flowcontrol

 Port  Send FlowControl    Receive FlowControl   RxPause TxPause
       admin    oper       admin    oper
-----  -------- --------   -------- --------     ------- -------
 6/1   off      off        on       on           0       0
 6/2   off      off        on       on           0       0
 6/3   off      off        on       on           0       0
```

Opmerking: Alle Catalyst modules reageren op een PAUSE frame indien onderhandeld. Sommige modules (bijvoorbeeld WS-X5410 en WS-X4306) sturen nooit pauzeknop, zelfs als ze onderhandelen om dit te doen, omdat ze niet blokkeren.

Dynamic Trunking Protocol

doel

Om VLAN's tussen apparaten uit te breiden, kunnen trunks tijdelijk de oorspronkelijke Ethernet frames identificeren en markeren (link lokaal). Deze actie maakt het mogelijk de frames te vermenigvuldigen via één link. De actie waarborgt ook dat de afzonderlijke uitzending- en beveiligingsdomeinen van VLAN tussen switches worden onderhouden. CAM-tabellen houden het kader in voor VLAN-mapping in de switches.

Overzicht

DTP is de tweede generatie van Dynamic ISL (DISL). DISL wordt alleen ondersteund door ISL. DTP ondersteunt ISL en 802.1Q. Deze ondersteuning zorgt ervoor dat de switches aan elk uiteinde van een stam het eens worden over de verschillende parameters van trunking frames. Deze parameters omvatten:

- Geconfigureren insluitingstype
- Native VLAN
- Hardware

De DTP-ondersteuning helpt ook bescherming te bieden tegen het overspoelen van gelabelde

frames door niet-boomstampoorten, wat een potentieel ernstig veiligheidsrisico is. DTP beschermt tegen dergelijke overstromingen omdat het garandeert dat havens en hun buren in consistente staten zijn.

Trunkmodus

DTP is een Layer 2 protocol dat onderhandelt over configuratieparameters tussen een switch poort en zijn buurman. DTP gebruikt een ander bekend multicast MAC-adres van 10-00-0c-cc-cc-cc en een SNAP-protocoltype van 0x2004. In deze tabel wordt de functie op elk van de mogelijke DTP-onderhandelingsmodi beschreven:

Modus	Functie	DTP-frames verzonden?	Eindstaat (lokale poort)
`Dynamisch auto` (vergelijkbaar met de `modus Auto` in CatOS)	Maakt de haven bereid om de verbinding naar een kofferbak om te zetten. De haven wordt een boomstamhaven als de aangrenzende haven `op` of `wenselijke` wijze wordt geplaatst.	Ja, periodiek	`trunking`
`Trunk` (gelijk aan de modus `ON` in CatOS)	Past de poort in permanente `trunking` mode en onderhandelt om de link in een kofferbak om te zetten. De haven wordt een boomhaven zelfs als de aangrenzende haven niet met de verandering instemt.	Ja, periodiek	`Trunking`, onvoorwaardelijk
`nonegotiaans`	Past de poort in permanente `trunking` modus maar staat niet toe dat de poort DTP-frames genereert. U moet de aangrenzende poort handmatig configureren als een	Nee	`Trunking`, onvoorwaardelijk

	boomstampoort om een boomstam verbinding op te zetten. Dit is handig voor apparaten die DTP niet ondersteunen.		
`Dynamisch wenselijk` (CatOS vergelijkbare opdracht is `wenselijk`)	Maakt de poort actief om de link naar een hoofdlink te converteren. De poort wordt een boomstampoort als de aangrenzende poort is ingesteld op `aan`, `wenselijk`, of `auto` mode.	Ja, periodiek	Het eindigt alleen in `trunking` toestand als de afstandsmodus `op`, `auto` of `wenselijk` is.
`Toegang`	Past de poort in permanente `niet-trunking` modus en onderhandelt om de link om te zetten in een niet-stam link. De haven wordt een niet boomstam haven zelfs als de aangrenzende haven niet met de verandering instemt.	Nee, in stabiele toestand, maar geeft informatie door om de afstandsdetectie te versnellen na een verandering van `in`.	`niet-trunking`

Opmerking: Het insluitingstype ISL en 802.1Q kan worden ingesteld of onderhandeld.

In de standaardconfiguratie neemt DTP deze kenmerken op de link in:

- Point-to-Point verbindingen en Cisco-apparaten ondersteunen 802.1Q kofferpoorten die alleen point-to-point zijn.
- Tijdens DTP-onderhandeling nemen de poorten niet deel aan STP. De poort wordt alleen aan STP toegevoegd nadat het poorttype een van deze drie typen wordt:ToegangISL802,1Q routerPAgP is het volgende proces dat moet worden uitgevoerd voordat de haven aan STP deelneemt. PAgP wordt gebruikt voor EtherChannel-autonomie.
- VLAN 1 is altijd aanwezig op de boomstampoort. Als de poort in ISL-modus is trunking, worden DTP-pakketten op VLAN 1 verzonden. Als de poort niet in ISL-modus is trunking, worden de DTP-pakketten verzonden op het inheemse VLAN (voor 802.1Q-trunking of niet-trunking-poorten).
- DTP-pakketten verzenden de VTP-domeinnaam plus de configuratie van de romp en de beheerstatus. De VTP domeinnaam moet overeenkomen om een onderhandelde boomstam te krijgen. Deze pakketten worden elke seconde door onderhandeling en elke 30 seconden na onderhandeling verzonden. Als een poort in `auto` of `wenselijke` modus geen DTP-pakket

binnen 5 minuten (min.) herkent, wordt de poort ingesteld als niet-stam.

Voorzichtig: U moet begrijpen dat de modi `boomstammen`, `nonegotiate`, en `toegang` expliciet specificeren in welke staat de haven eindigt. Een slechte configuratie kan leiden tot een gevaarlijke/inconsistente toestand waarin de ene kant trunking is en de andere niet trunking.

Raadpleeg ISL-trunking configureren op Catalyst 5500/5000 en 6500/6000 Series Switches voor meer ISL-details. Raadpleeg trunking tussen Catalyst 4500/4000, 5500/5000 en 6500/6000 Series Switches die 802.1Q insluiting gebruiken met Cisco CatOS-systeemsoftware voor meer 802.1Q details.

Type insluiting

ISL-operationeel overzicht

ISL is een trunking Protocol (VLAN-tagging scheme) van Cisco. ISL wordt al jaren gebruikt. 802.1Q is daarentegen veel nieuwer, maar 802.1Q is de IEEE-standaard.

ISL kapselt het originele frame volledig in in een tagging-programma met twee niveaus. Op deze manier is ISL in feite een tunneling protocol en heeft zij, als extra voordeel, niet-Ethernet frames. ISL voegt een kop van 26 bytes en een FCS van 4 bytes toe aan het standaard Ethernet-kader. Poorten die zijn ingesteld om stammen te zijn verwachten en behandelen de grotere Ethernet frames. ISL ondersteunt 1024 VLAN's.

Frame Relay-indeling - ISL-tag wordt beschadigd

40 Bits	4 Bits	4 Bits	48 Bits	16 Bits	24 Bits	24 Bits	15 Bits	1 Bit	16 Bits	16 Bits
DA	Type	USER	SA	LEN	SNAP LLC	HSA	VLAN	BPDU	INDEX	Reserve
01-00-0c-00-00					AAAA03	00000C				

Encapsulated Frame	FCS
Variable length	32 bits

Raadpleeg InterSwitch Link en IEEE 802.1Q frame-indeling voor meer informatie.

802.1Q operationeel overzicht

Hoewel de standaard IEEE 802.1Q alleen betrekking heeft op Ethernet, specificeert de standaard

veel meer dan insluitingstypen. 802.1Q omvat, naast andere GARP's (Generic Attribution Protocols), versterkingen van spanningsbomen en 802.1p QoS-markering. Raadpleeg IEEE Standards online voor meer informatie

Het 802.1Q frame-formaat behoudt de oorspronkelijke Ethernet SA en DA. Switches moeten nu echter verwachten om baby-gigantische frames te ontvangen, zelfs op toegangshavens waar gastheren het taggen kunnen gebruiken om 802.1p gebruikersprioriteit voor QoS-signalering uit te drukken. De tag is 4 bytes. De 802.1Q Ethernet v2-frames zijn 1522 bytes, wat een prestatie is van de IEEE 802.3ac-werkgroepreeks. Tevens ondersteunt 802.1Q nummeringsruimte voor 4096 VLAN's.

Alle gegevensframes die worden verzonden en ontvangen zijn 802.1Q gelabeld, behalve die gegevensframes die op het inheemse VLAN zijn weergegeven. In dit geval is er een impliciete tag die is gebaseerd op de poortconfiguratie van de ingress switch. Frames op het inheemse VLAN worden altijd zonder tag verzonden en worden normaal gesproken zonder tag ontvangen. Deze frames kunnen echter ook worden getagd.

Raadpleeg deze documenten voor meer informatie:

- VLAN-interoperabiliteit
- Trunking tussen Catalyst 4500/4000, 5500/5000 en 6500/6000 Series Switches met 802.1q insluiting met Cisco CatOS-systeemsoftware

Frame Relay 802.1Q/802.1p frame-indeling

		Tag Header						
		TPID	TCI					
48 bits	48 bits	16 bits	3 bits	1 bit	12 bits	16 bits	Variable length	32 bits
DA	SA	TPID	Priority	CFI	VLAN ID	Length/ Type	Data with PAD	FCS
		0x8100	0 – 7	0-1	0-4095			

Cisco-configuratie-aanbeveling

Eén primair Cisco-ontwerpbeginsel is bedoeld om te streven naar consistentie in het netwerk waar consistentie mogelijk is. Alle nieuwere Catalyst producten ondersteunen 802.1Q en sommige alleen 802.1Q, zoals eerdere modules in Catalyst 4500/4000 en Catalyst 6500 Series. Daarom moeten alle nieuwe implementaties deze IEEE 802.1Q standaard volgen en moeten oudere netwerken geleidelijk van ISL migreren.

Geef deze interfaceopdrachten uit om 802.1Q trunking op een bepaalde poort mogelijk te maken:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#switchport
!--- Configure the interface as a Layer 2 port. Switch(config-if)#switchport trunk encapsulation
dot1q
```

De IEEE-standaard maakt verkoopinteroperabiliteit mogelijk. De interoperabiliteit van de verkoper is voordelig in alle omgevingen van Cisco aangezien de nieuwe host 802.1p-geschikte NIC's en apparaten beschikbaar worden. Hoewel zowel ISL- als 802.1Q-implementaties solide zijn, heeft de IEEE-standaard uiteindelijk een grotere blootstelling aan velden en meer ondersteuning voor derden, wat ondersteuning voor netwerkanalyzers omvat. Bovendien is een minder belangrijke overweging dat de 802.1Q-standaard ook een lagere insluitingsoverhead heeft dan ISL.

Voor volledigheid, leidt het impliciete taggen op inheemse VLANs tot een veiligheidsoverweging. De transmissie van frames van één VLAN, VLAN X, naar een ander VLAN, VLAN Y, zonder een router is mogelijk. De transmissie kan zonder een router voorkomen als de bronpoort (VLAN X) in het zelfde VLAN zoals het inheemse VLAN van een 802.1Q stam op de zelfde switch is. De workround is om een dummy VLAN voor het inheemse VLAN van de boomstam te gebruiken.

Geef deze interfaceopdrachten uit om een VLAN als inheems (het standaard) voor 802.1Q trunking op een bepaalde poort in te stellen:

```
Switch(config)#interface type slot#/port#
Switch(config-If)#switchport trunk native vlan 999
```

Omdat alle nieuwere hardware 802.1Q ondersteunt, alle nieuwe implementaties de standaard IEEE 802.1Q hebben gevolgd en geleidelijk eerdere netwerken van ISL migreren. Tot voor kort hebben veel Catalyst 4500/4000 modules ISL niet ondersteund. Daarom is 802.1Q de enige optie voor Ethernet-trunking. Raadpleeg de uitvoer van de **opdracht** van de **show interface mogelijkheden** of de **show port mogelijkheden** opdracht voor CatOS. Omdat trunking-ondersteuning de juiste hardware vereist, kan een module die 802.1Q niet ondersteunt nooit 802.1Q ondersteunen. Een software-upgrade biedt geen ondersteuning voor 802.1Q. De meeste nieuwe hardware voor Catalyst 6500/6000 en Catalyst 4500/4000 switches ondersteunt zowel ISL als 802.1Q.

Als VLAN 1 van een stam wordt gewist, zoals de sectie van het Beheer van de Switch en inheemse VLAN bespreekt, hoewel geen gebruikersgegevens worden verzonden of ontvangen, blijft NMP controleprotocollen op VLAN 1 doorgeven. Voorbeelden van controleprotocollen omvatten CDP en VTP.

Bovendien, zoals de sectie VLAN 1 bespreekt, worden de pakketten CDP, VTP, en PAgP altijd op VLAN 1 verzonden wanneer de trunking. Met het gebruik van dot1q (802.1Q) insluiting, worden deze controleframes getagd met VLAN 1 als de switch native VLAN wordt gewijzigd. Als dot1q trunking naar een router en het autochtone VLAN op de switch wordt veranderd, is een subinterface in VLAN 1 nodig om de gelabelde CDP-frames te ontvangen en het CDP-buurtzicht op de router te bieden.

Opmerking: Er is een potentiële veiligheidsoverweging met punt1q die de impliciete tagging van het inheemse VLAN veroorzaakt. De transmissie van frames van het ene VLAN naar het andere zonder een router kan mogelijk zijn. Raadpleeg het gedeelte Inbraakdetectie voor meer informatie. De workround moet een VLAN ID voor het inheemse VLAN van de boomstam

gebruiken die niet voor de eindgebruikerstoegang gebruikt wordt. Om dit te bereiken, verlaat de meerderheid van de klanten van Cisco eenvoudig VLAN 1 als het autochtone VLAN op een boomstam en versleutel toegangspoorten aan VLANs anders dan VLAN 1.

Cisco raadt een expliciete configuratie van de `dynamische` boommodus aan aan beide uiteinden. Deze modus is de standaardmodus. In deze modus kunnen netwerkexploitanten de syslog- en de opdrachtregel-statusberichten vertrouwen dat een haven `omhoog` en trunking is. Deze modus is anders dan `in` de `on` mode, waardoor een poort kan worden geopend, ook al is de buur niet ingesteld. Daarnaast bieden `wenselijke` modemtrunks stabiliteit in situaties waarin één kant van de link geen stam kan worden of de `romp` staat laat vallen.

Als het insluitingstype tussen switches met het gebruik van DTP is overeengekomen, en ISL wordt standaard als winnaar geselecteerd als beide eindpunten het ondersteunen, moet u deze interfaceopdracht uitgeven om punt1q[1] te specificeren:

```
switchport trunk encapsulation dot1q
```

[1] Sommige modules, waaronder WS-X6548-GE-TX en WS-X6148-GE-TX, ondersteunen ISL-trunking niet. Deze modules accepteren geen **van de** commandopoort **insluiting *dot1q*.**

Opmerking: Geef de opdracht **toegangsmodus** uit om stammen in een poort uit te schakelen. Deze disablement helpt verspilling van onderhandelingstijd te elimineren wanneer de poorten van de gastheer worden opgevoed.

```
Switch(config-if)#switchport host
```

Andere opties

Een andere algemene klantconfiguratie gebruikt `dynamische wenselijke` modus op de distributielaag en de eenvoudigste standaardconfiguratie (`dynamische` automatische modus) op de toegangslaag. Sommige switches, zoals Catalyst 2900XL, Cisco IOS routers, of andere verkoopapparaten, ondersteunen momenteel geen boomstamonderhandeling via DTP. U kunt `nonegotiate` modus gebruiken om een poort onvoorwaardelijk in te stellen op stam met deze apparaten. Deze modus kan helpen bij het standaardiseren van een gemeenschappelijke instelling op de campus.

Cisco raadt `non-onderhandeling aan` wanneer u verbinding maakt met een Cisco IOS-router. Door het overbruggen, kunnen sommige DTP frames die van een haven worden ontvangen die met de **boomstam** van de **verbindingswijze** wordt gevormd naar de boomstampoort terugkeren. Op ontvangst van het DTP frame probeert de switch poort onnodig opnieuw te onderhandelen. Om opnieuw te onderhandelen brengt de haven van de switch de romp `omlaag` en `omhoog`. Als `nonegotiate` is ingeschakeld, stuurt de switch geen DTP-frames.

```
switch(config)#interface type slot#/port#
switch(config-if)#switchport mode dynamic desirable
!--- Configure the interface as trunking in desirable !--- mode for switch-to-switch links with
multiple VLANs. !--- And... switch(config-if)#switchport mode trunk
!--- Force the interface into trunk mode without negotiation of the trunk connection. !--- Or...
switch(config-if)#switchport nonegotiate
!--- Set trunking mode to not send DTP negotiation packets !--- for trunks to routers.
switch(config-if)#switchport access vlan vlan_number
```

```
!--- Configure a fallback VLAN for the interface. switch(config-if)#switchport trunk native vlan
999
!--- Set the native VLAN. switch(config-if)#switchport trunk allowed vlan vlan_number_or_range
!--- Configure the VLANs that are allowed on the trunk.
```

Spanning Tree Protocol

doel

Spanning tree behoudt een lijn-vrije Layer 2-omgeving in redundante geschakelde en bruggen netwerken. Zonder STP vermenigvuldigen frames en/of voor onbepaalde tijd. Dit voorval veroorzaakt een netwerkmeltdown omdat het hoge verkeer alle apparaten in het uitgezonden domein onderbreekt.

In sommige opzichten is STP een vroeg protocol dat oorspronkelijk was ontwikkeld voor langzame software-gebaseerde bridge specificaties (IEEE 802.1D). Maar STP kan gecompliceerd zijn om het succesvol uit te voeren in grote geschakelde netwerken die:

- Veel VLAN’s
- Veel switches in een domein
- Ondersteuning van meerdere leveranciers
- Nieuwe IEEE-verbeteringen

Cisco IOS-systeemsoftware heeft nieuwe STP-ontwikkelingen doorlopen. Nieuwe IEEE-standaarden die 802.1w Rapid STP en 802.1s Multiple Spanning Tree-protocollen bevatten, bieden snelle convergentie, taakverdeling en schaal van besturingsplane. Daarnaast bieden de functies voor versterking van STP zoals RootGuard, BPDU-filtering, Portfast BPDU Guard en LoopGuard extra bescherming tegen Layer 2-verzendlijnen.

PVST+ Overzicht

De root-brug verkiezing per VLAN wordt gewonnen door de switch met de laagste root-brug Identifier (BID). De BID is de overbrugingsprioriteit gecombineerd met het MAC-adres van de switch.

Aanvankelijk worden BPDU's vanuit alle switches verzonden en bevatten de BID van elke switch en de padkosten om die switch te bereiken. Dit maakt het mogelijk de root-brug te bepalen en het pad met de laagste kosten naar de wortel te nemen. Aanvullende configuratieparameters die in BPDU's van de wortel worden gedragen, omzeilen deze parameters die lokaal zijn geconfigureerd, zodat het hele netwerk consistente timers gebruikt. Voor elke BPDU die een switch van de wortel ontvangt, verwerkt het Catalyst centrale NMP een nieuwe BPDU en stuurt het uit met de basisinformatie.

De topologie converteert dan door deze stappen:

1. Er wordt één root-brug gekozen voor het gehele omspannende boomdomein.
2. Eén basispoort (die naar de root-brug gericht is) wordt op elke nonroot brug geselecteerd.
3. Een aangewezen poort wordt geselecteerd voor BPDU die op elk segment wordt verstuurd.
4. Niet-aangewezen havens worden geblokkeerd.

Raadpleeg deze documenten voor meer informatie:

- STP- en IEEE 802.1s MST configureren
- De betekenis van Rapid Spanning Tree Protocol (802.1w)

Standaard basistimers	Name	Functie
2 seconden	hallo	Bestuurt het vertrek van BPDU's.
15 seconden	voorwaartse vertraging (FWDM-vertraging)	Bestuurt de tijdsduur die een haven in `luisterstaat` en `leertoestand` doorbrengt en beïnvloedt het proces van topologie verandering.
20 seconden	maximum	Bestuurt de tijdsduur die de switch de huidige topologie handhaaft alvorens de switch een alternatief pad zoekt. Na de maximale verouderingstijd (maxage) wordt een BPDU als gestaal beschouwd en de switch zoekt een nieuwe wortelhaven uit de pool van blokkerende havens. Als er geen geblokkeerde haven beschikbaar is, beweert de switch zelf de wortel te zijn in de aangewezen havens.

Cisco raadt u aan geen timers te wijzigen omdat dit de stabiliteit nadelig kan beïnvloeden. De meeste netwerken die worden ingezet zijn niet aangepast. De eenvoudige STP timers die via de opdrachtregel toegankelijk zijn (zoals hallo-interval, maxage, etc.) zijn zelf samengesteld uit een complexe reeks andere veronderstelde en intrinsieke timers. Daarom is het moeilijk om timers af te stemmen en alle implicaties in overweging te nemen. Bovendien kunt u de UDLD-bescherming ondermijnen. Zie het gedeelte UniDirectional Link Detectie voor meer informatie.

Opmerking over STP-timers:

De standaard STP-timer waarden zijn gebaseerd op een berekening die rekening houdt met een netwerkdiameter van zeven switches (zeven switch hop van de bron naar de rand van het netwerk) en de tijd die nodig is voor een BPDU om van de root-brug naar de rand switches in het netwerk te gaan, die zeven hop weg zijn. Deze veronderstelling compileert timer waarden die voor de meeste netwerken acceptabel zijn. Maar, kunt u deze timers in meer optimale waarden veranderen om convergentietijden door de veranderingen van de netwerktopologie te versnellen.

U kunt de root-brug met de netwerkdiameter voor een specifiek VLAN configureren en de timer waarden dienovereenkomstig berekenen. Cisco raadt aan, als u veranderingen moet aanbrengen, enkel de diameter en de optionele hallo-tijdparameters op de root-brug voor VLAN te configureren.

```
spanning-tree vlan vlan-id [root {primary | secondary}] [diameter diameter-value [hello hello-time]]
!--- This command needs to be on one line.
```

Deze macro maakt de wortel van de switch voor het gespecificeerde VLAN, compileert nieuwe klokwaarden op basis van de diameter en de hallo tijd gespecificeerd, en verspreidt deze informatie in configuratie BPDUs aan alle andere switches in de topologie.

In de sectie New Port States en Port Roles wordt 802.1D STP beschreven en wordt 802.1D STP met Rapid STP (RSTP) vergeleken en gecontrasteerd. Raadpleeg het gedeelte Rapid Spanning Tree Protocol (802.1w) voor meer informatie over RSTP.

Nieuwe poortstaten en poortrollen

802.1D is gedefinieerd in vier verschillende havenstaten:

- Luisteren
- Leren
- Blokken
- Doorsturen

Zie de tabel in het gedeelte Port States voor meer informatie. De staat van de haven is gemengd (of het verkeer blokkeert of door), evenals de rol die de haven in de actieve topologie (wortelhaven, aangewezen haven, enz.) speelt. Vanuit operationeel oogpunt is er bijvoorbeeld geen verschil tussen een haven in een blokkerende staat en een haven in een luisterstaat. Ze gooien beide kaders weg en leren geen MAC adressen. Het echte verschil ligt in de rol die de omspannende boom aan de haven toewijst. U kunt er veilig van uitgaan dat een luisterpoort is aangewezen of wortel en op weg is naar de verzendende staat. Helaas, als de haven eenmaal in staat van vervoer is, is er geen manier om uit de havenstaat af te leiden of de haven wortel is of aangewezen. Dit toont aan dat deze op de staat gebaseerde terminologie mislukt. RSTP richt deze mislukking op omdat RSTP de rol en de staat van een haven ontkoppelt.

Poortstaten

Poortstaten in STP 802.1D

Staten van havens	Middelen	Standaard tijden voor de volgende fase
`Uitgeschakeld`	Administratief omlaag.	
`Blokken`	Ontvang BPDU's en stop gebruikersgegevens.	Toezicht op de ontvangst van BPDU's. 20 seconden wachten op maximale verloopdatum of onmiddellijke verandering als een directe/lokale link is gedetecteerd.
`Luisteren`	Zendt of ontvangt BPDU's om te controleren of terugkeer naar blokkering noodzakelijk is.	Wacht 15 seconden.
`Leren`	Hiermee bouwt u een topologie/CAM-tabel op.	Wacht 15 seconden.

Doorsturen	Verstuurt/ontvangt gegevens.	

De totale basistopologie-verandering is:

- 20 + 2 (15) = 50 sec, indien het wachten op het verstrijken van de maxage
- 30 seconden voor falen van directe link

Er zijn slechts drie havenstaten die in RSTP overblijven, wat overeenkomt met de drie mogelijke operationele staten. De 802.1D-staten zijn uitgeschakeld, blokkeren en luisteren. Ze zijn samengevoegd tot een unieke 802.1w-teruggooistaat.

STP (802.1D) poortstaat	RSTP-poortstaat (802.1w)	Is poort opgenomen in actieve topologie?	Zijn de MAC-adressen van het leren van poorten?
Uitgeschakeld	ontslag	Nee	Nee
Blokken	ontslag	Nee	Nee
Luisteren	ontslag	Ja	Nee
Leren	Leren	Ja	Ja
Doorsturen	Doorsturen	Ja	Ja

Poortrollen

De rol is nu een variabele die aan een bepaalde haven wordt toegewezen. De wortelhaven en aangewezen havenrollen blijven, maar de blokkerende havenrol is nu verdeeld in de reserve en alternatieve havenrollen. Het overspannen van een boomalgoritme (STA) bepaalt de rol van een haven op de basis van BPDU's. Denk aan deze BPDU's om dingen eenvoudig te houden: er is altijd een manier om twee BPDU's te vergelijken en te beslissen of het ene bruikbaarder is dan het andere. De basis van het besluit is de waarde die is opgeslagen in de BPDU en, af en toe, de haven waarop de BPDU is ontvangen. In de rest van dit deel worden zeer praktische benaderingen met betrekking tot havenrollen toegelicht.

Root-poortrol

De poort die de beste BPDU op een brug ontvangt is de wortelhaven. Dit is de haven die qua padkosten het dichtst bij de root-brug staat. De STA kiest één root-brug in het hele bridging netwerk (per-VLAN). De root-brug stuurt BPDU's die nuttiger zijn dan die welke een andere brug kan sturen. De root-brug is de enige brug in het netwerk die geen wortelhaven heeft. Alle andere bruggen ontvangen BPDU's op ten minste één poort.

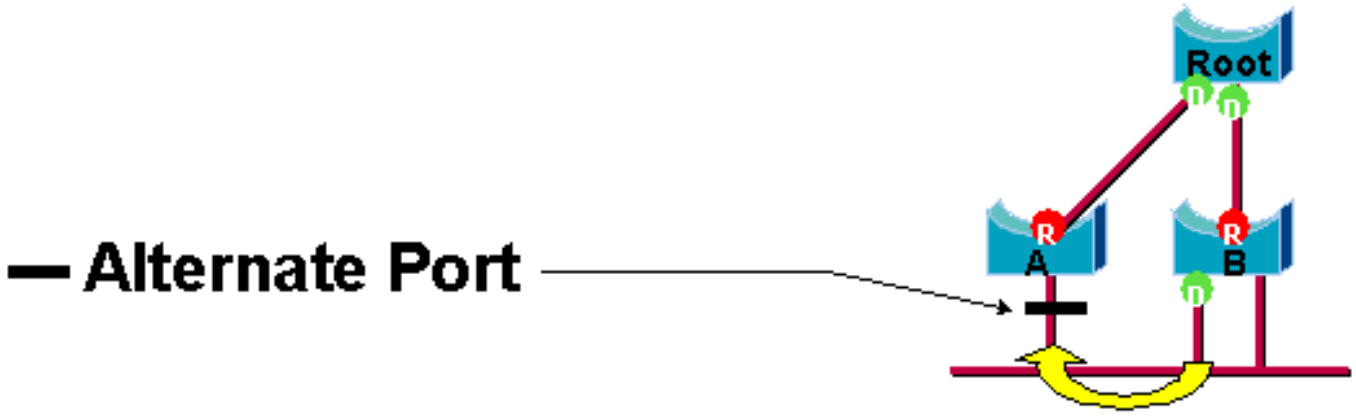
Aangewezen poortrol

Een poort wordt aangewezen als deze de beste BPDU op het segment kan verzenden naar wie de poort is aangesloten. 802.1D-bruggen verbinden verschillende segmenten (Ethernet-segmenten, bijvoorbeeld) om een overbrugd domein te creëren. Op een bepaald segment kan er maar één pad naar de root-brug worden afgelegd. Als er twee paden zijn, is er een overbruggingslus in het netwerk. Alle bruggen die op een bepaald segment zijn aangesloten, luisteren naar de BPDU's van de andere bruggen en stemmen in met de brug die de beste BPDU als de aangewezen brug voor het segment stuurt. De overeenkomstige haven op die brug is aangewezen.

Alternatieve en back-uppoortrollen

Deze twee poortrollen corresponderen met de blokkeringstoestand van 802.1D. De definitie van een geblokkeerde haven is een haven die niet de aangewezen of wortelhaven is. Een geblokkeerde poort ontvangt een bruikbaarder BPDU dan de BPDU die het op zijn segment verstuurt. Denk eraan dat een haven absoluut BPDU's moet ontvangen om geblokkeerd te blijven. RSTP voert deze twee rollen voor dit doel in.

Een alternatieve poort is een poort die wordt geblokkeerd door het ontvangen van bruikbaarder BPDU's van een andere brug. In dit schema wordt aangegeven:



Een reservepoort is een poort die wordt geblokkeerd door het ontvangen van bruikbaarder BPDU's van de zelfde brug die de haven aan is. In dit schema wordt aangegeven:

Dit onderscheid werd al intern binnen 802.1D gemaakt. Dit is in wezen hoe Cisco UplinkFast functioneert. De reden achter dit is dat een alternatieve poort een alternatieve route naar de root-brug biedt. Daarom kan deze poort de wortelpoort vervangen als het mislukt. Natuurlijk biedt een reservepoort redundante connectiviteit aan het zelfde segment en kan geen afwisselende verbinding aan de root-brug waarborgen. Daarom werd de back-uppoort van de uplink-groep uitgesloten.

Als resultaat hiervan berekent RSTP de definitieve topologie voor het overspannen van boom met gebruik van precies de zelfde criteria zoals 802.1D. Er is geen verandering in de manier waarop de verschillende brug- en havenprioriteiten worden gebruikt. De naam die wordt geblokkeerd wordt gebruikt voor de teruggooistatus in Cisco-implementatie. CatOS release 7.1 en latere releases tonen nog steeds de luister- en leerstaten, die zelfs meer informatie over een poort geven dan de IEEE-standaard nodig heeft. Maar het nieuwe kenmerk is dat er nu een verschil is tussen de rol die het protocol voor een haven heeft bepaald en de huidige status. Het is nu bijvoorbeeld volkomen geldig dat een haven tegelijkertijd wordt aangewezen en geblokkeerd. Hoewel dit doorgaans voor zeer korte periodes gebeurt, betekent het eenvoudigweg dat deze haven in een tijdelijke staat is naar aangewezen verzending.

STP-interacties met VLAN's

Er zijn drie verschillende manieren om VLAN's met Spanning Tree te correleren:

- Eén Spanning Tree Protocol (CST) voor alle VLAN's of Common Spanning Tree Protocol (CST), zoals IEEE 802.1D
- Een Spanning Tree per VLAN of gedeelde Spanning Tree zoals Cisco PVST

- Een Spanning Tree per set VLAN's, of meerdere Spanning Tree (MST), zoals IEEE 802.1s

Vanuit een configuratie standpunt, kunnen deze drie typen van het overspuiten van boommodi aangezien ze betrekking hebben op interactie met VLAN's in één van drie soorten modi worden geconfigureerd:

- Spanning Tree per-VLAN Dit implementeert werkelijk PVST+, maar wordt genoteerd in Cisco IOS Software als eenvoudig PVST.
- **rapid-pvst**—De evolutie van de 802.1D standaard verbetert de convergentietijden en neemt de op standaarden gebaseerde (802.1w) eigenschappen van UplinkFast en BackboneFast op.
- **mst**-Dit is de standaard 802.1s voor een het omspannen van boom per reeks VLAN's of MST's. Hierin is ook het snelle 802.1w-element in de norm opgenomen.

Een eenvoudige Spanning Tree voor alle VLAN's biedt slechts één actieve topologie en dus geen taakverdeling. Een STP blokkeerde poortblokken voor alle VLAN's en draagt geen gegevens.

Eén Spanning Tree per VLAN of PVST+ maakt taakverdeling mogelijk maar vereist meer BPDU CPU-verwerking naarmate het aantal VLAN's toeneemt.

De nieuwe standaard 802.1s (MST) staat de definitie van tot 16 actieve STP instanties/topologieën toe, en het in kaart brengen van alle VLAN's aan deze instanties. In een typische campusomgeving hoeven slechts twee gevallen te worden gedefinieerd. Deze techniek laat STP schaal toe aan vele duizenden VLAN's terwijl het lading in evenwicht brengt.

De ondersteuning voor Rapid-PVST en pre-standaard MST wordt geïntroduceerd in Cisco IOS-softwarerelease 12.1(11b)EX en 12.1(13)E voor Catalyst 6500. Catalyst 4500 met Cisco IOS-softwarerelease 12.1(12c)EW en latere releases - ondersteuning van pre-standaard MST. Snelle PVST-ondersteuning wordt toegevoegd aan Cisco IOS-softwarerelease 12.1(19)EW voor Catalyst 4500 platform. De standaard compatibele MST wordt ondersteund in Cisco IOS-softwarerelease 12.2(18)SXF voor Catalyst 6500 en Cisco IOS-softwarerelease 12.2(25)SG voor Catalyst 4500 Series switches.

Raadpleeg het gedeelte Rapid Spanning-Tree Protocol (802.1w) en Understanding Multiple Spanning-Tree Protocol (802.1s) voor meer informatie.

Logische poorten van Spanning Tree

De aantekeningen Catalyst 4500 en 6500 bieden advies over het aantal logische poorten in de Spanning Tree per switch. De som van alle logische poorten is gelijk aan het aantal stammen op de switch keer het aantal actieve VLAN's op de stammen, plus het aantal niet-trunking interfaces op de switch. Cisco IOS-software genereert een systeemlogbericht als het maximale aantal logische interfaces de beperking overschrijdt. Aanbevolen wordt de aanbevolen richtlijn niet te overschrijden.

In deze tabel wordt het aantal logische poorten vergeleken dat met verschillende STP-modi en supervisor type wordt ondersteund:

supervisor	PVST+	RPVST+	MST
Catalyst 6500 supervisor 1-module	6.000[1] totaal 1.200 per switchmodul	6.000 totaal 1.200 per switchmodule	25.000 totaal 3.000[2] per switchmodul

	e		e
Catalyst 6500 supervisor 2-module	13.000[1] totaal 1.800[2] per switchmodule	10.000 totaal 1.800[2] per switchmodule	50.000 totaal 6.000[2] per switchmodule
Catalyst 6500 supervisor 720	13.000 totaal 1.800[2] per switchmodule	10.000 totaal 1.800[2] per switchmodule	50.003 totaal 6.000[2] per switchmodule
Catalyst 4500 supervisor II-plus	1.500 totaal	1.500 totaal	25.000 totaal
Catalyst 4500 supervisor II-plus-10 GE switch	1.500 totaal	1.500 totaal	25.000 totaal
Catalyst 4500 supervisor IV-module	3.000 totaal	3.000 totaal	50.000 totaal
Catalyst 4500 supervisor V-module	3.000 totaal	3.000 totaal	50.000 totaal
Catalyst 4500 supervisor V 10 GE switch	3.000 totaal	3.000 totaal	80.000 totaal

[1] Het maximale aantal totale logische poorten die in PVST+ eerder dan Cisco IOS-softwarerelease 12.1(13)E worden ondersteund, is 4.500.

[2] 10 Mbps, 10/100 Mbps, en 100 Mbps switchmodules ondersteunen een maximum van 1.200 logische interfaces per module.

[3] Het maximale aantal totale logische poorten die in MST worden ondersteund voorafgaand aan Cisco IOS-softwarerelease 12.2(17b)SXA is 30.000.

Aanbeveling

Het is moeilijk om een aanbeveling van de in-boommodus te voorzien zonder gedetailleerde informatie zoals hardware, software, aantal apparaten en aantal VLAN's. In het algemeen, als het aantal logische havens niet het aanbevolen richtsnoer overschrijdt, wordt de Snelle PVST modus aanbevolen voor nieuwe netwerkplaatsing. Snelle PVST modus biedt snelle netwerkconvergentie zonder de noodzaak van extra configuratie zoals snel backbone en uplink snel. Geef deze volgende opdracht uit om de overspannende boom in snelle-PVST modus in te stellen:

```
spanning-tree mode rapid-pvst
```

Andere opties

In een netwerk met een combinatie van bestaande hardware en oudere software wordt de PVST+-modus aanbevolen. Geef deze opdracht uit om de overspannende-boom in PVST+ modus in te stellen:

```
spanning-tree mode pvst
----This is default and it shows in the configuration.
```

De modus MST wordt aanbevolen voor VLAN's overal en met een groot aantal VLAN's. Voor dit netwerk kan de som van de logische havens het richtsnoer voor PVST en Rapid-PVST overschrijden. Geef deze opdracht uit om de overspanningsboom in MST-modus in te stellen:

```
spanning-tree mode mst
```

BPDU-formaten

Om de standaard IEEE 802.1Q te ondersteunen, heeft Cisco het PVST-protocol uitgebreid dat bestaat om het PVST+ protocol te leveren. PVST+ voegt ondersteuning toe voor koppelingen tussen de IEEE 802.1Q mono-overspannende boomregio. PVST+ is compatibel met zowel IEEE 802.1Q mono die in een boom wordt gespaard en de Cisco PVST protocollen die bestaan. Daarnaast voegt PVST+ controlemechanismen toe om te verzekeren dat er geen configuratie inconsistentie van port trunking en VLAN ID over switches is. PVST+ is plug-and-play compatibel met PVST, zonder de vereiste van een nieuwe opdracht of configuratie van de opdrachtregel van de interface (CLI).

Hier zijn een paar hoogtepunten van de operationele theorie van het PVST+-protocol:

- PVST+ interopereert met 802.1Q mono omspannende boom. PVST+ interopereert met 802.1Q-conforme switches op gemeenschappelijke STP door 802.1Q trunking. De gemeenschappelijke overspanning van boom is op VLAN 1, het autochtone VLAN, door standaard. Eén gemeenschappelijk overspant-boom BPDU wordt verzonden of ontvangen met het standaard IEEE bridge-group MAC-adres (10-80-c2-00-00-00, protocol type 0x010c) via 802.1Q-links. Vaak omspannende bomen kunnen in de PVST of in mono omringende boomregio geworteld zijn.
- PVST+ tunnels de PVST BPDUs over het gebied van 802.1Q VLAN als multicast gegevens. Voor elk VLAN in een stam, worden BPDUs met het Cisco Shared STP (SSTP) MAC-adres (10-00c-cc-cd) verzonden of ontvangen. Voor VLAN's die gelijk zijn aan de Port VLAN-Identifier (PVID), wordt BPDU niet getagd. Voor alle andere VLAN's zijn BPDU's gelabeld.
- PVST+ is achterwaarts compatibel met de bestaande Cisco switch op PVST door ISL trunking. ISL-ingekapselde BPDU's worden verzonden of ontvangen via ISL-trunks, wat hetzelfde is als bij eerdere Cisco PVST.
- PVST+ controles op inconsistenties in poort en VLAN. PVST+ blokkeert die poorten die inconsistente BPDU's ontvangen om het voorvallen van het verzenden van loops te voorkomen. PVST+ informeert gebruikers via syslog ook over om het even welke inconsistentie.

Opmerking: In ISL-netwerken worden alle BPDU's verzonden met gebruik van het IEEE MAC-adres.

Cisco-configuratieaanbevelingen

Alle Catalyst switches hebben STP standaard ingeschakeld. Zelfs als u een ontwerp kiest dat Layer 2 loops niet omvat en STP wordt niet geactiveerd om een geblokkeerde poort actief te handhaven, laat de optie om deze redenen aan:

- Als er een loop is, voorkomt STP kwesties die door multicast en uitgezonden gegevens kunnen worden verergerd. Vaak leidt het fouilleren van een patroon, een slechte kabel of een andere oorzaak tot een lus.
- STP beschermt tegen een EtherChannel-defect.
- De meeste netwerken zijn ingesteld met STP en krijgen daarom een maximale blootstelling in het veld. Meer blootstelling komt over het algemeen overeen met een stabielere code.
- STP beschermt tegen dubbel-aangesloten NIC's wangedrag (of overbrugging ingeschakeld op servers).
- Veel protocollen zijn nauw verbonden met STP in code. Voorbeelden zijn:PAgPIGMP-communicatie (Internet Group Message Protocol)trunkingAls u zonder STP draait, kunt u ongewenste resultaten behalen.
- Tijdens een gemelde netwerkverstoring, suggereren de ingenieurs van Cisco gewoonlijk dat het niet gebruiken van STP het centrum van de fout is, als op alles mogelijk.

Om het overspannen van boom op alle VLAN's toe te laten, geef deze globale opdrachten uit:

```
Switch(config)#spanning-tree vlan vlan_id
!--- Specify the VLAN that you want to modify. Switch(config)#default spanning-tree vlan vlan_id
!--- Set spanning-tree parameters to default values.
```

Verandert de timer niet, wat de stabiliteit negatief kan beïnvloeden. De meeste netwerken die worden ingezet zijn niet aangepast. De eenvoudige STP timers die via de bevellijn, zoals hallo-interval en maxage, toegankelijk zijn hebben een complexe reeks andere veronderstelde en intrinsieke timers. Daarom kunt u problemen hebben als u probeert om timers te stemmen en alle implicaties in overweging te nemen. Bovendien kunt u de UDLD-bescherming ondermijnen.

Idealiter Houd gebruikersverkeer van het beheer VLAN. Dit is niet van toepassing op Catalyst 6500/6000 Cisco IOS-switch. Toch moet u deze aanbeveling op de kleinste-eind Cisco IOS switches en CatOS switches respecteren die een afzonderlijke beheersinterface kunnen hebben en met Cisco IOS switches moeten worden geïntegreerd. Met name met oudere Catalyst switch processors houdt u het beheer VLAN gescheiden van gebruikersgegevens om problemen met STP te voorkomen. Een verkeerd gedraaid eindstation kan de processor van de Supervisor Engine zo druk houden met uitgezonden pakketten dat de processor een of meer BPDU's kan missen. Maar nieuwere switches met krachtiger CPU’s en wentelende controles ontlasten deze overweging. Zie het gedeelte Switch Management Interface en Native VLAN van dit document voor meer informatie.

Overontwerp redundantie niet. Dit kan leiden tot te veel blokkerende havens en kan de stabiliteit op lange termijn negatief beïnvloeden. Bewaar de totale STP-diameter onder zeven hop. Probeer het model van de meerdere lagen van Cisco te ontwerpen waar dit ontwerp mogelijk is. De modelfuncties:

- Kleinere switched domeinen
- STP-driehoeken
- Bepalende geblokkeerde poorten

Invloed en weet waar root functionaliteit en geblokkeerde poorten wonen. Documenteer deze

informatie in het topologieschema. Weet uw overspant boomtopologie, die essentieel is om probleemoplossing te vinden. De geblokkeerde poorten zijn waar de problemen met STP worden opgelost. De oorzaak van de verandering van blokkeren in het verzenden is vaak het zeer belangrijke deel van de analyse van de worteloorzaak. Kies de distributie en de kernlagen als de locatie van de wortel/secundaire wortel omdat deze lagen als de meest stabiele delen van het netwerk worden beschouwd. Controleer voor optimale Layer 3 en Hot Standby Router Protocol (HSRP) met Layer 2 datatransmissiepaden.

Deze opdracht is een macro die de overbruggingsprioriteit vormt. De wortel stelt dat de prioriteit veel lager is dan de wanbetaling (32.768), en de tweede stelt dat de prioriteit redelijk lager is dan de standaardwaarde:

```
Switch(config)#interface type slot/port
Switch(config)#spanning-tree vlan vlan_id root primary
!--- Configure a switch as root for a particular VLAN.
```

Opmerking: deze macro stelt de basisprioriteit in op:

- 8192 standaard
- De huidige hoofdprioriteit minus 1, als een andere root-brug bekend is
- De huidige hoofdprioriteit, als zijn adres van MAC lager is dan de huidige wortel

Trek onnodige VLAN's van boomhavens af, wat een bidirectionele oefening is. De actie beperkt de diameter van STP en NMP verwerkingsoverhead op delen van het netwerk waar bepaalde VLAN's niet vereist zijn. VTP automatisch afdrukken verwijdert geen STP uit een romp. U kunt ook de standaard VLAN 1 uit trunks verwijderen.

Raadpleeg Spanning Tree Protocol-problemen en verwante ontwerpoverwegingen voor extra informatie.

Andere opties

Cisco heeft een ander STP-protocol, **VLAN-bridge**, dat werkt met het gebruik van een bekend MAC-adres van **100-0c-cd-cd-ce** en een protocoltype van 0x010c.

Dit protocol is het meest handig als er een noodzaak is om niet-routeerbare of legacy-protocollen tussen VLAN's te overbruggen zonder interferentie met de IEEE-boomorganen die op deze VLAN's lopen. Als VLAN-interfaces voor niet-hybride verkeer geblokkeerd worden voor Layer 2-verkeer, wordt ook het overlay Layer 3-verkeer onopzettelijk uitgeschakeld, wat een ongewenst neveneffect is. Deze Layer 2-blokkering kan eenvoudig worden uitgevoerd als de VLAN-interfaces voor niet-hybride verkeer aan dezelfde STP als IP VLAN's deelnemen. VLAN-bridge is een afzonderlijk geval van STP voor overbrugde protocollen. Het protocol biedt een afzonderlijke topologie die zonder een effect op IP-verkeer kan worden gemanipuleerd.

Start het VLAN-bridge protocol als er een overbrugging tussen VLAN's op Cisco-routers zoals de MSFC is vereist.

STP-poortadapter voor Fast

U kunt PortFast gebruiken om het normale overspannen van een boom op toegangsporten te omzeilen. PortFast versnelt connectiviteit tussen eindstations en de services waaraan eindstations moeten verbinden na initialisatie van een link. De implementatie van Microsoft DHCP moet de

toegangpoort in het doorsturen zien onmiddellijk nadat de verbindingsstaat omhoog gaat om een IP-adres te vragen en ontvangen. Sommige protocollen, zoals Internetwork Packet Exchange (IPX)/Sequfied Packet Exchange (SPX), moeten de toegangpoort in expediteursmodus zien direct nadat de verbindingsstaat omhoog gaat om problemen met de dichtstbijzijnde server (GNS) te voorkomen.

Raadpleeg PortFast of Andere opdrachten om de connectiviteitsvertraging bij het opstarten van het werkstation voor meer informatie op te heffen.

PortFast-operationeel Overzicht

PortFast slaat de normale luisterstaat, het leren en het doorsturen van STP-staten over. De optie verplaatst een poort direct van blokkeren naar doorsturen nadat de link omhoog wordt gezien. Als deze optie niet is ingeschakeld, gooit STP alle gebruikersgegevens weg tot het besluit dat de poort klaar is om naar de verzendende modus te worden verplaatst. Dit proces kan (2 x ForwardDelay) tijd in beslag nemen, die standaard 30 seconden is.

Portfast mode belemmert de productie van een STP Topology Change Kennisgeving (TCN) elke keer dat een havenstaat van leren naar het verzenden verandert. TCN's zijn normaal. Maar een golf van TCN's die de root-brug raakt kan de convergentietijd onnodig verlengen. Er vindt 's morgens een golf van TCN's plaats, die mensen 's morgens hun PC aanzetten.

Cisco-aanbeveling voor toegangspoortconfiguratie

Stel STP PortFast in op alle enabled host-poorten. Stel STP PortFast ook expliciet in op uit voor switch-switch links en poorten die niet in gebruik zijn.

Geef de maco-opdracht van de gastheer van de **switchpoort** uit in de interfaceconfiguratiemodus om de aanbevolen configuratie voor toegangsporten uit te voeren. De configuratie helpt ook belangrijke autonomie en verbindingsprestaties:

```
switch(config)#interface type slot#/port#

switch(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
!--- This macro command modifies these functions.
```

Opmerking: PortFast betekent niet dat het overspannen van de boom op de poorten helemaal niet draait. BPDU's worden nog steeds verzonden, ontvangen en verwerkt. Spanning Tree is essentieel voor een volledig functioneel LAN. Zonder lusdetectie en het blokkeren, kan een lus onbedoeld het gehele LAN snel omlaag brengen.

Schakel ook trunking en channeling uit voor alle host poorten. Elke toegangspoort is standaard ingeschakeld voor trunking en channeling, maar switch buren worden niet verwacht door design op host-poorten. Als u deze protocollen aan het onderhandelen overlaat, kan de vertraging in poortactivering leiden tot ongewenste situaties. De eerste pakketten van werkstations, zoals DHCP en IPX verzoeken, worden niet verzonden.

Een betere optie is om PortFast standaard in de mondiale configuratiemodus te configureren met gebruik van deze opdracht:

```
Switch(config)#spanning-tree portfast enable
```

Vervolgens, op elke toegangspoort die een hub of een switch in slechts één VLAN heeft, schakelt u de functie PortFast op elke interface uit met de interfaceopdracht:

```
Switch(config)#interface type slot_num/port_num
Switch(config-if)#spanning-tree portfast disable
```

Andere opties

PortFast BPDU-beveiliging biedt een methode om lusvorming te voorkomen. BPDU Guard verplaatst een niet-trunking poort naar een `errOff`-status bij de ontvangst van een BPDU op die poort.

Onder normale omstandigheden ontvangt u nooit BPDU-pakketten op een toegangspoort die is ingesteld voor PortFast. Een inkomende BPDU geeft een ongeldige configuratie aan. De beste actie is het afsluiten van de toegangshaven.

Cisco IOS-systeemsoftware biedt een nuttige wereldwijde opdracht die automatisch `BPDU-ROOT-GUARD` toestaat op elke poort die is ingeschakeld voor UplinkFast. Gebruik deze opdracht *altijd*. De opdracht werkt per switch en niet per poort.

Geef deze algemene opdracht uit om `BPDU-ROOT-GUARD` in te schakelen:

```
Switch(config)#spanning-tree portfast bpduguard default
```

Een Simple Network Management Protocol (SNMP)-val of systeembericht stelt de netwerkbeheerder op de hoogte als de poort wordt ingedrukt. U kunt ook een automatische terugwinningstijd instellen voor poorten `met` instelbare `schijf`. Zie het gedeelte UniDirectional Link Detectie van dit document voor meer informatie.

Raadpleeg de Verbetering in Spanning Tree PortFast BPDU Guard voor meer informatie.

Opmerking: PortFast voor kofferpoorten is geïntroduceerd in Cisco IOS-softwarerelease 12.1(11b)E. PortFast voor boomstampoorten is ontworpen om convergentietijden voor Layer 3 netwerken te verhogen. Wanneer u deze optie gebruikt, zorg er dan voor dat u BPDU-beveiliging en BPDU-filter op interfacebasis uitschakelt.

UplinkFast

doel

UplinkFast voorziet in snelle STP-convergentie na een onderbreking van de directe verbinding in de laag van de netwerktoegang. UplinkFast werkt zonder wijziging van STP. Het doel is de convergentie-tijd in specifieke omstandigheden te versnellen tot minder dan drie seconden, in plaats van de typische 30 seconden vertraging. Raadpleeg het begrip en de configuratie van de Cisco UplinkFast-functie.

Overzicht

Met het Cisco meerlaagse ontwerpmodel op de toegangslaag, wordt de blokkerende uplink onmiddellijk verplaatst naar een expediteits als de verzendende uplink verloren gaat. De functie wacht niet op de `luisterende` en `leerstatus`.

Een uplink-groep is een verzameling poorten per VLAN die u kunt beschouwen als een root-poort en een back-upwortelpoort. Onder normale omstandigheden zorgen de wortelhavens voor connectiviteit van de toegang tot de wortel. Als deze primaire basisverbinding om wat voor reden dan ook faalt, schakelt de back-up root link direct in, zonder dat de standaard 30 seconden conversievertraging nodig is.

Omdat UplinkFast effectief het normale proces van het behandelen van de topologie van STP (het `luisteren` en het `leren`) voorbij gaat, is een afwisselend correctiemechanisme voor de topologie nodig. Het mechanisme moet switches in het domein bijwerken met informatie dat de lokale eindstations bereikbaar zijn via een ander pad. Zodoende genereert de switch van de toegangslaag die UplinkFast runt ook frames voor elk MAC-adres in zijn CAM-tabel naar een bekend multicast MAC-adres (100-00c-cd-cd-cd HDLC-protocol 0x200a). Dit proces werkt de CAM tabel in alle switches in het domein met de nieuwe topologie bij.

Cisco-aanbeveling

Cisco raadt u aan UplinkFast voor access switches met geblokkeerde poorten in te schakelen als u 802.1D overspannende boom gebruikt. Gebruik UplinkFast niet op switches zonder de impliciete topologie kennis van een back-upwortelverbinding - meestal distributie en core switches in het Cisco meerlaagse ontwerp. In algemene termen, laat UplinkFast op een switch met meer dan twee manieren uit een netwerk niet toe. Als de switch in een complex toegangsklimaat zit en u meer dan één link blokkeert en één link doorsturen, vermijd dan gebruik van deze optie op de switch of raadpleeg uw Advanced Services engineer.

Geef deze globale opdracht uit om UplinkFast in te schakelen:

```
Switch(config)#spanning-tree uplinkfast
```

Deze opdracht in Cisco IOS-software past niet automatisch alle prioriteitswaarden van de brug aan een hoge waarde aan. In plaats daarvan wijzigt de opdracht alleen die VLAN's met een bridge prioriteit die niet handmatig is gewijzigd in een andere waarde. Daarnaast, in tegenstelling tot CatOS, wanneer u een switch herstelt die met UplinkFast was ingeschakeld, keert de geen vorm van deze opdracht (**geen omspanend-tree uplinkfast**) alle veranderde waarden terug naar hun standaardwaarden. Daarom *moet* u, wanneer u deze opdracht gebruikt, de huidige status van de brug prioriteiten voor en na controleren om te verzekeren dat het gewenste resultaat wordt bereikt.

Opmerking: U hebt het **alle protocollen** sleutelwoord voor de opdracht UplinkFast nodig wanneer de protocol filterfunctie is ingeschakeld. Omdat CAM het protocoltype evenals MAC en de informatie van VLAN vastlegt wanneer het protocol het filtreren wordt toegelaten, moet een UplinkFast frame voor elk protocol op elk adres van MAC worden gegenereerd. Het sleutelwoord **van het** tarief wijst op de pakketten per seconde van de UplinkFast topologie update frames. Deze standaard wordt aanbevolen. U hoeft UplinkFast niet met RSTP te configureren, omdat het mechanisme in plaats daarvan automatisch in RSTP is ingeschakeld en automatisch is ingeschakeld.

BackboneFast

doel

BackboneFast zorgt voor snelle convergentie van indirecte blunders. BackboneFast vermindert de convergentietijden van de standaardinstelling van 50 seconden tot, gewoonlijk, 30 seconden en voegt op deze manier functionaliteit toe aan STP. Deze optie is alleen van toepassing bij gebruik van 802.1D. Configureer de functie niet wanneer u snelle PVST of MST (wat de snelle component omvat) gebruikt.

Overzicht

BackboneFast wordt gestart wanneer een root poort of geblokkeerde poort op een switch inferieure BPDU's van de aangewezen brug ontvangt. De poort ontvangt doorgaans inferieure BPDU's wanneer een stroomafwaartse switch de verbinding met de wortel verliest en BPDU's begint te verzenden om een nieuwe wortel te selecteren. Een inferieure BPDU identificeert een switch als zowel de root-brug als de aangewezen brug.

Onder normaal omspant boomregels, negeert de ontvangende switch inferieure BPDU's voor de opgegeven maximale tijd. Standaard is de maximale snelheid 20 seconden. Maar met BackboneFast, ziet de switch de inferieure BPDU als een signaal van een mogelijke verandering in de topologie. De switch gebruikt Root Link Query (RLQ) BPDU's om te bepalen of deze een ander pad naar de root-brug heeft. Met deze RLQ-protocoltoevoeging kan een switch controleren of de oorsprong nog steeds beschikbaar is. RLQ beweegt een geblokkeerde poort om eerder `door te sturen` en waarschuwt de geïsoleerde switch die de inferieure BPDU heeft verstuurd dat de wortel er nog is.

Hier zijn een paar hoogtepunten van de protocolhandeling:

- Een switch geeft het RLQ-pakket alleen uit de wortelpoort door (wat betekent dat het pakket naar de wortelvorm gaat).
- Een switch die een RLQ ontvangt kan antwoorden als het de switch van de wortel is, of als die switch weet dat het verbinding met de wortel heeft verloren. Als de switch deze feiten niet kent, moet het de query naar zijn wortelpoort doorsturen.
- Als een switch de verbinding met de wortel heeft verloren, moet de switch in het negatieve antwoord op deze vraag beantwoorden.
- Het antwoord moet alleen worden verstuurd uit de haven waarvan de vraag afkomstig was.
- De root switch moet altijd reageren op deze query met een positief antwoord.
- Als het antwoord op een nonroot poort is ontvangen, dient u het antwoord weg.

De bewerking kan de STP-conversietijd met maximaal 20 seconden verminderen omdat het maxage-programma niet hoeft te verlopen. Raadpleeg het gedeelte Inzicht en backbone Fast configureren op Catalyst-Switches voor meer informatie.

Cisco-aanbeveling

Schakel BackboneFast op alle switches in die STP uitvoeren als het gehele omspannende-boomdomein deze optie kan ondersteunen. U kunt de functie toevoegen zonder dat dit ten koste gaat van een productienetwerk.

Geef deze globale opdracht uit om BackboneFast mogelijk te maken:

```
Switch(config)#spanning-tree backbonefast
```

Opmerking: U moet deze opdracht op mondiaal niveau op alle switches in een domein configureren. De opdracht voegt functionaliteit toe aan STP die alle switches moeten begrijpen.

Andere opties

BackboneFast wordt niet ondersteund op Catalyst 2900XL en 3500XL switches. In het algemeen, moet u BackboneFast inschakelen als het domein van de switch deze switches bevat naast Catalyst 4500/4000, 5500/5000 en 6500/6000 switches. Wanneer u Backbone Fast in omgevingen met XL switches uitvoert, onder strikte topologieën, kunt u de eigenschap inschakelen waar de XL switch de laatste switch in lijn is en alleen op twee plaatsen met de kern is verbonden. Voer deze optie niet uit als de XL-switches in een dagelijkse keten zijn opgebouwd.

U hoeft Backbone Fast niet met RSTP of 802.1w te configureren, omdat het mechanisme automatisch in RSTP is opgenomen en ingeschakeld.

Spanning Tree Loop Guard

Loop Guard is een bedrijfseigen optimalisatie van Cisco voor STP. Loop Guard beschermt Layer 2-netwerken tegen lusjes die voorkomen vanwege een storing in de netwerkinterface, een drukke CPU of iets dergelijks die het normale verzenden van BPDU's verhindert. Een STP lijn wordt gecreëerd wanneer een blokkerende haven in een overtollige topologie ten onrechte overschakelt naar de door:sturen staat. Dit gebeurt gewoonlijk omdat een van de havens in een fysiek redundante topologie (niet noodzakelijk de blokkerende haven) stopte met het ontvangen van BPDU's.

Loop Guard is alleen nuttig in geschakelde netwerken waar switches verbonden zijn door point-to-point links, zoals het geval is in de meeste moderne campus en datacenter netwerken. Het idee is dat, op een point-to-point link, een aangewezen brug niet kan verdwijnen zonder een inferieure BPDU te sturen of de link naar beneden te brengen. De functie STP-loop Guard is geïntroduceerd in Cisco IOS-softwarerelease 12.1(13)E van Catalyst Cisco IOS-software voor Catalyst 6500 en Cisco IOS-softwarerelease 12.1(9)EA1 voor Catalyst 4500 switches.

Raadpleeg Spanning-Tree Protocol-verbeteringen met Loop Guard en BPDU Skew Detectie-functies voor meer informatie over lusbeveiliging.

Overzicht

Loop Guard controleert of een wortelpoort of een alternatieve/back-up wortelpoort BPDU's ontvangt. Als de poort geen BPDU's ontvangt, zet loop Guard de poort in een inconsistente staat (blokkerend) tot het BPDU's opnieuw begint te ontvangen. Een poort in de inconsistente staat geeft geen BPDU's door. Als zo'n haven opnieuw BPDU's ontvangt, wordt de haven (en de verbinding) opnieuw levensvatbaar geacht. De lijn-inconsistente voorwaarde wordt verwijderd uit de haven, en STP bepaalt de havenstaat. Op deze manier is automatisch herstel mogelijk.

Loop Guard isoleert de mislukking en laat het omspannen van boom tot een stabiele topologie zonder de mislukte verbinding of brug samenvallen. Loop Guard voorkomt STP loops met de snelheid van de STP versie die in gebruik is. Er is geen afhankelijkheid van STP zelf (802.1D of 802.1w) of bij het afstemmen van de STP-timers. Om deze redenen raadt Cisco u aan loop Guard in combinatie met UDLD in topologieën toe te passen die op STP vertrouwen en waar de software de functies ondersteunt.

Wanneer loop Guard een inconsistente poort blokkeert, wordt dit bericht gelogd:

```
%SPANTREE-SP-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet2/1 on VLAN0010
```

Nadat de BPDU op een poort in een loop-inconsistente STP staat wordt ontvangen, de haven overgangen in een andere STP staat. Volgens de ontvangen BPDU betekent dit dat het herstel automatisch is en dat er geen interventie nodig is. Na herstel wordt dit bericht ingelogd:

```
%SPANTREE-SP-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet2/1 on
VLAN0010
```

Interactie met andere STP-functies

Root Guard

Root Guard dwingt een haven aan te wijzen. Loop Guard is alleen effectief als de haven een haven is of een alternatieve haven, wat betekent dat hun functies elkaar uitsluiten. Daarom kunnen loop Guard en root Guard niet tegelijkertijd op een poort worden ingeschakeld.

UplinkFast

Loop Guard is compatibel met UplinkFast. Als loop Guard een wortelpoort in een blokkerende staat zet, zet UplinkFast in het door:sturen van staat een nieuwe wortelpoort. Ook selecteert UplinkFast geen *loop-inconsistente poort* als wortelpoort.

BackboneFast

Loop Guard is compatibel met Backbone Fast. BackboneFast wordt geactiveerd door de ontvangst van een inferieure BPDU die van een aangewezen brug afkomstig is. Omdat BPDU's van deze link worden ontvangen, trapt loop Guard niet in. Daarom zijn BackboneFast en loop Guard compatibel.

PortFast

PortFast overschakelt een poort naar de verzendende aangewezen staat onmiddellijk na verbinding. Omdat een PortFast-enabled poort geen root/alternatieve poort is, zijn loop Guard en PortFast wederzijds exclusief.

PAgP

Loop Guard gebruikt de poorten die bekend zijn bij STP. Daarom kan loop Guard voordeel halen uit de abstractie van logische poorten die PAgP biedt. Maar om een kanaal te vormen, moeten alle fysieke poorten die in het kanaal zijn gegroepeerd compatibele configuraties hebben. PAgP zorgt voor een uniforme configuratie van de lus op alle fysieke poorten om een kanaal te vormen. Let op deze waarschuwingen wanneer u loop Guard op een EtherChannel configureren:

- STP gebruikt altijd de eerste operationele poort in het kanaal om de BPDU's te verzenden. Als die link unidirectioneel wordt, blokkeert loop Guard het kanaal, zelfs als andere links in het kanaal goed werken.
- Als een reeks poorten die al geblokkeerd zijn door loop Guard gegroepeerd zijn om een kanaal te vormen, verliest STP alle overheidsinformatie voor die havens, en de nieuwe kanaalpoort kan wellicht de verzendende staat met een aangewezen rol bereiken.
- Als een kanaal wordt geblokkeerd door loop Guard en het kanaal breekt, verliest STP alle staatsinformatie. De individuele fysieke havens kunnen de verzendende staat mogelijk

bereiken met een specifieke rol, zelfs als één of meer van de verbindingen die het kanaal vormden eenrichtings zijn.

In deze laatste twee gevallen is er een mogelijkheid van een lus tot UDLD de storing detecteert. Maar loop Guard kan het niet detecteren.

Loop Guard en UDLD-functievergelijking

Loop Guard en UDLD-functionaliteit overlappen gedeeltelijk, gedeeltelijk in de zin dat beide bescherming bieden tegen STP-fouten die unidirectionele koppelingen veroorzaken. Deze twee kenmerken verschillen in de aanpak van het probleem en ook in de functionaliteit. Met name zijn er specifieke unidirectionele tekortkomingen die UDLD niet kan detecteren, zoals fouten die worden veroorzaakt door een CPU die BPDU's niet verzenden. Daarnaast kan het gebruik van agressieve STP-timers en RSTP-modus resulteren in loops voordat UDLD de fouten kan detecteren.

Loop Guard werkt niet aan gedeelde verbindingen of in situaties waar de link zich sinds de koppeling in één richting heeft bevonden. In het geval van een link die unidirectioneel is geweest sinds de koppeling, ontvangt de haven nooit BPDU's en wordt het aangewezen. Dit kan normaal gedrag zijn, dus loop Guard doet dit specifieke geval niet. UDLD biedt bescherming tegen een dergelijk scenario.

De inschakeling van zowel UDLD als loop Guard biedt het hoogste beschermingsniveau. Raadpleeg voor meer informatie over een functievergelijking tussen loop Guard en UDLD:

- *Loop Guard vs. Unidirectional Link Detection* sectie van Spanning-Tree Protocol-verbeteringen met Loop Guard en BPDU Skew Detectie-functies
- DLD-gedeelte van dit document

Cisco-aanbeveling

Cisco raadt u aan om lusbeveiliging wereldwijd op een netwerk van de switch met fysieke lijnen toe te laten. U kunt lus Guard mondiaal inschakelen op alle poorten. Deze optie is ingeschakeld voor alle point-to-point links. De point-to-point link wordt gedetecteerd door de duplexstatus van de link. Als duplex vol is, wordt de link beschouwd als point-to-point.

```
Switch(config)#spanning-tree loopguard default
```

Andere opties

Voor switches die geen mondiale configuratie van lijnwachters ondersteunen, wordt aanbevolen deze functie in alle afzonderlijke havens toe te staan, waaronder havenkanaalhavens. Hoewel er geen voordelen zijn als u loop Guard op een aangewezen haven toelaat, bedenk het geen probleem van het inschakelen. Bovendien kan een geldige oversparing boomreconversie een aangewezen haven in een wortelhaven in feite veranderen, wat de eigenschap op deze haven nuttig maakt.

```
Switch(config)#interface type slot#/port#
Switch(config-if)#spanning-tree guard loop
```

Netwerken met lus-vrije topologieën kunnen nog steeds van loopGuard profiteren in het geval dat de loops per ongeluk worden geïntroduceerd. Maar het inschakelen van loop Guard in dit type

topologie kan leiden tot problemen in de netwerkisolatie. Als u een lus-vrije topologie bouwt en netwerkisolatieproblemen wilt vermijden, kunt u lusGuard mondiaal of afzonderlijk verhinderen. Schakel lusbeveiliging niet op gedeelde koppelingen in.

```
Switch(config)#no spanning-tree loopguard default
!--- This is the global configuration.
```

of

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no spanning-tree guard loop
!--- This is the interface configuration.
```

Spanning Tree Root Guard

De eigenschap root Guard biedt een manier om de plaatsing van de root-brug in het netwerk af te dwingen. Root Guard zorgt ervoor dat de haven waarop root Guard is ingeschakeld de aangewezen haven is. Normaal gesproken zijn root-brug-poorten alle aangewezen havens, tenzij twee of meer havens van de root-brug met elkaar zijn verbonden. Als de brug superieure STP BPDU's op een root Guard-enabled poort ontvangt, beweegt de brug deze poort naar een root-inconsistente STP-staat. Deze fundamenteel onsamenhangende staat is in feite gelijk aan een luisterstaat. Er wordt geen verkeer doorgestuurd door deze poort. Op deze manier zorgt de wortelbeveiliging ervoor dat de positie van de root-brug wordt gehandhaafd. Root Guard is beschikbaar in de vroege Cisco IOS-softwarerelease 12.1E en hoger.

Overzicht

Root Guard is een ingebouwde STP-mechanisme. Root Guard heeft geen eigen timer en is alleen afhankelijk van de ontvangst van BPDU's. Als wortelbeveiliging wordt toegepast op een haven, ontkent het deze haven de mogelijkheid om een wortelhaven te worden. Als de ontvangst van een BPDU een omspannend boomconvergentie veroorzaakt die een aangewezen haven een wortelhaven maakt wordt, wordt de haven dan in een wortel onsamenhangende staat geplaatst. Dit syslogbericht illustreert:

```
%SPANTREE-SP-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet2/1 on VLAN0010
```

Nadat de poort is gestopt om superieure BPDU's te verzenden, wordt de poort opnieuw ontgrendeld. Via STP, gaat de haven van de luisterstaat naar de leerstaat, en uiteindelijk gaat de overstap naar de verzendstaat. Dit slogan-bericht laat de overgang zien:

```
%SPANTREE-SP-2-ROOTGUARD_UNBLOCK: Root guard unblocking port GigabitEthernet2/1
on VLAN0010
```

Herstel is automatisch. Er is geen menselijke interventie nodig.

Omdat root Guard een haven afdwingt om aan te wijzen en loop Guard alleen effectief is als de haven een wortelhaven of een alternatieve haven is, sluiten de functies elkaar uit. Daarom kunt u niet tegelijkertijd loop Guard en root Guard op een poort inschakelen.

Raadpleeg de Verbetering in Spanning Tree Protocol Root Guard voor meer informatie.

Cisco-aanbeveling

Cisco raadt u aan de functie root Guard in te schakelen op poorten die zijn aangesloten op netwerkapparaten die niet onder direct beheersysteem staan. Om root Guard te configureren gebruikt u deze opdrachten wanneer u zich in de interface-configuratiemodus bevindt:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#spanning-tree guard root
```

EtherChannel

doel

EtherChannel omvat een frame-distributiealgoritme dat efficiënt kaders over de component 10/100 Mbps of Gigabit-koppelingen multiplext. Het frame distributiealgoritme staat het omgekeerde multiplexing van meerdere kanalen in één logische link toe. Hoewel elk platform in implementatie verschilt van het volgende platform, moet u deze gemeenschappelijke eigenschappen begrijpen:

- Er moet een algoritme zijn om statistisch multiplex frames te multiplexen via meerdere kanalen. In Catalyst switches is dit hardware-gerelateerd. Hier zijn voorbeelden:Catalyst 5500/5000s-De aanwezigheid of het ontbreken van een Ethernet Bundling Chip (EBC) op de moduleCatalyst 6500/6000s - een algoritme dat verder in het kader en multiplex door IP adres kan lezen
- Er is de creatie van een logisch kanaal zodat één exemplaar van STP kan worden uitgevoerd of één enkele routing peering kan worden gebruikt, wat afhankelijk is van of Layer 2 of Layer 3 EtherChannel is.
- Er is een beheerprotocol om te controleren op de consistentie van parameters aan het eind van de verbinding en om te helpen bij het beheer van bundeling van herstel na een storing of toevoeging. Dit protocol kan een PAgP- of Link Aggregation Control Protocol (LACP) zijn.

Overzicht

EtherChannel omvat een frame-distributiealgoritme dat efficiënt kaders over de component 10/100-Mbps, Gigabit of 10-Gigabit-koppelingen multiplext. Verschillen in algoritmen per platform ontstaan door de mogelijkheid van elk type hardware om de informatie over de frame-header te extraheren om de distributie te beslissen.

Het algoritme van de belastingsverdeling is een globale optie voor beide kanaalcontroleprotocollen. PAgP en LACP gebruiken het frame distributiealgoritme omdat de IEEE-standaard geen specifieke distributie algoritmen toestaat. Maar, elk distributiealgoritme waarborgt dat, wanneer frames worden ontvangen, het algoritme niet het verkeerd bestellen van frames veroorzaakt die deel uitmaken van een bepaald gesprek of duplicatie van frames.

Deze tabel illustreert het frame distribution algoritme in detail voor elk opgesomd platform:

platform	Taaltaakverdeling
Catalyst 3750 Series-switche	Catalyst 3750 dat het algoritme van de de lading van Cisco IOS in werking stelt dat de adressen van MAC of IP adressen gebruikt, en of de bericht bron of bericht bestemming, of

s	beiden.
Catalyst 4500 Series-switches	Catalyst 4500 dat Cisco IOS-software-herkenningsalgoritme draait met MAC-adressen, IP-adressen of Layer 4 (L4) poortnummers en/of de bron- of berichtbestemming of beide.
Catalyst 6500/6000 Series-switches	Er zijn twee hashing algoritmen die kunnen worden gebruikt, wat van de hardware van de Supervisor Engine afhangt. De hash is een veelterm van zeventiende graden die in hardware wordt geïmplementeerd. In alle gevallen neemt de hash het MAC-, IP-adres of IP TCP/UDP-poortnummer en past het algoritme toe om een 3-bits waarde te genereren. Dit proces gebeurt afzonderlijk voor zowel de SA's als de DA's. De XOR-bewerking wordt vervolgens met de resultaten gebruikt om een andere 3-bits waarde te genereren. De waarde bepaalt welke poort in het kanaal wordt gebruikt om het pakket door te sturen. De kanalen op Catalyst 6500/6000 kunnen tussen havens op om het even welke module worden gevormd en kunnen tot acht havens zijn.

Deze tabel geeft de distributiemethoden aan die worden ondersteund op de verschillende modellen van Catalyst 6500/6000 Supervisor Engine. De tabel toont ook het standaardgedrag:

Hardware	Beschrijving	Distributiemethoden
WS-F6020A (Layer 2-motor) WS-F6K-PFC (Layer 3-motor)	Later Supervisor Engine I en Supervisor Engine IA Supervisor Engine IA/Policy functiekaart 1 (PFC1)	Layer 2 MAC: SA; DA; SA en DA Layer 3 IP: SA; DA; SA en DA (standaard)
WS-F6K-PFC 2	Supervisor Engine II/PFC2	Layer 2 MAC: SA; DA; SA en DA Layer 3 IP: SA; DA; SA en DA (standaard) Layer 4 sessie: S-poort; D-poort; S- en D-poort
WS-F6K-PFC3A WS-F6K-PFC3B WS-F6K-PFC3BXL	Supervisor Engine 720/PFC3A Supervisor Engine 720/Supervisor Engine 32/PFC3B Supervisor Engine 720/PFC3BXL	Layer 2 MAC: SA; DA; SA en DA Layer 3 IP: SA; DA; SA en DA (standaard) Layer 4 sessie: S-poort; D-poort; S- en D-poort

Opmerking: bij Layer 4-distributie gebruikt het eerste gefragmenteerde pakket Layer 4-distributie.

Alle volgende pakketten gebruiken Layer 3 distributie.

Opmerking: Raadpleeg deze documenten om meer informatie te vinden over EtherChannel-ondersteuning op andere platforms en de manier waarop u EtherChannel kunt configureren en probleemoplossing kunt realiseren:

- De betekenis van EtherChannel-taakverdeling en redundantie op Catalyst-Switches
- Layer 3 en Layer 2 EtherChannel configureren (Catalyst 6500 Series Cisco IOS-softwarerelease, 12.2SX)
- Layer 3 en Layer 2 EtherChannel configureren (Catalyst 6500 Series Cisco IOS-softwarerelease, 12.1E)
- EtherChannel configureren (Catalyst 4500 Series Switch Cisco IOS-softwarerelease, 12.2(31)SG)
- Software Configuration Guide voor Catalyst 3750 Switch, 12.2(25)SEE)
- EtherChannel configureren tussen Catalyst 4500/4000, 5500/5000 en 6500/6000 Switches die CatOS-systeemsoftware uitvoeren

Cisco-aanbeveling

Catalyst 3750, Catalyst 4500 en Catalyst 6500/6000 Series switches voor het uitvoeren van een taakverdeling door standaard zowel de bron- als bestemming IP-adressen te hakken. Dit wordt aanbevolen, met de veronderstelling dat IP het dominante protocol is. Geef deze opdracht uit om de taakverdeling in te stellen:

```
port-channel load-balance src-dst-ip
!--- This is the default.
```

Andere opties

Afhankelijk van de verkeersstromen kunt u Layer 4-distributie gebruiken om de taakverdeling te verbeteren wanneer het grootste deel van het verkeer tussen hetzelfde bron- en doeladres ligt. U moet begrijpen dat, wanneer Layer 4-distributie is geconfigureerd, het hashing alleen Layer 4 bron- en doelpoorten omvat. Layer 3 IP-adressen worden niet in het hashing-algoritme gecombineerd. Geef deze opdracht uit om de taakverdeling in te stellen:

```
port-channel load-balance src-dst-port
```

Opmerking: Layer 4 distributie is niet Configureerbaar op Catalyst 3750 Series switches.

Geef de opdracht **taakverdeling per kanaal** uit om het beleid voor de kaderdistributie te controleren.

Afhankelijk van de hardwareplatforms kunt u CLI-opdrachten gebruiken om te bepalen welke interface in EtherChannel de specifieke verkeersstroom doorgeeft, met het frame-distributiebeleid als basis.

Voor Catalyst 6500 switches geeft u de opdracht **switch op afstand** af om inloggen op afstand in de Switch Processor (SP)-console. Geef vervolgens het *nummer* van de **{ip *van het* testkanaal-**load-*balance* ***interface****-kanaal* uit **| l4port | mac} [*source_ip_add* |** *source_mac_add* | *source_l4_port*] [*dest_ip_add* | *dest_mac_add* | *dest_l4_port*]** opdracht.

Voor Catalyst 3750 switches, geef het **test** uit-**kanaal load-balances** ***interface-kanaal nummer*** **{ip | mac} [*source_ip_add* | *source_mac_add*] [*dest_ip_add* | *dest_mac_add*]** opdracht.

Voor Catalyst 4500 is de equivalente opdracht nog niet beschikbaar.

Richtlijnen en beperkingen voor EtherChannel-configuratie

EtherChannel verifieert poorteigenschappen op alle fysieke poorten voordat het compatibele poorten aggregeert in één logische poort. De configuratierichtlijnen en -beperkingen verschillen voor de verschillende switches. Voltooi deze richtsnoeren en beperkingen om problemen bij bundeling te voorkomen. Als QoS bijvoorbeeld is ingeschakeld, worden EtherChannel niet gevormd bij het bundelen van Catalyst 6500/6000 Series switchmodules met verschillende QoS-functies. Voor Catalyst 6500 switches die Cisco IOS-software starten, kunt u de QoS Port Attribution-controle van de EtherChannel-bundeling uitschakelen met de opdracht **niet MCS QoC-**kanaalinterface. De opdracht **toont interfacemodule** ***en poort*** **die** de QoS poortcapaciteit weergeeft en bepaalt of poorten compatibel zijn.

Raadpleeg deze richtlijnen voor verschillende platforms om configuratieproblemen te voorkomen:

- Layer 3 en Layer 2 EtherChannel configureren (Catalyst 6500 Series Cisco IOS-softwarerelease, 12.2SX)
- Layer 3 en Layer 2 EtherChannel configureren (Catalyst 6500 Series Cisco IOS-softwarerelease, 12.1E)
- EtherChannel configureren (Catalyst 4500 Series Switch Cisco IOS-softwarerelease, 12.2(31)SG)
- Software Configuration Guide voor Catalyst 3750 Switch, 12.2(25)SEE)

Het maximale aantal EtherChannel's dat wordt ondersteund, is ook afhankelijk van het hardwareplatform en de softwarereleases. Catalyst 6500 switches die Cisco IOS-softwarerelease 12.2(18)SXE uitvoeren en die later ondersteuning bieden aan maximaal 128 poort-kanaals interfaces. Softwarereleases die eerder zijn dan Cisco IOS-softwarerelease 12.2(18)SXE ondersteunen een maximum van 64-poorts-kanaalinterfaces. Het configureerbare groepsnummer kan 1 tot 256 zijn, ongeacht de softwarerelease. Catalyst 4500 Series switches ondersteunen een maximum van 64 EtherChannel. Voor Catalyst 3750 switches is de aanbeveling niet om meer dan 48 EtherChannel op de switch stapel te configureren.

Spanning Tree Port Cost Calculator

U moet de berekening van de boompoortkosten voor EtherChannel begrijpen. U kunt de overspannende boompoortkosten voor EtherChannel berekenen met de korte of lange methode. Standaard wordt de poortkosten berekend in de korte modus.

Deze tabel illustreert de overspannende kosten van boompoorten voor een Layer 2 EtherChannel op basis van de bandbreedte:

Bandbreedte	Oude STP-waarde	Nieuwe lange STP-waarde
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
N X 1 Gbps	3	6660
10 Gbps	2	2,000

100 Gbps	N.v.t.	200
1 Tbps	N.v.t.	20
10 Tbps	N.v.t.	2

Opmerking: In CatOS blijven de overspannende kosten van de boompoort voor een EtherChannel hetzelfde na het falen van de verbinding van het havenkanaallid. In Cisco IOS-software worden de poortkosten voor EtherChannel onmiddellijk bijgewerkt om de nieuwe beschikbare bandbreedte weer te geven. Als het gewenste gedrag om onnodig het overspannen van boomtopologie veranderingen te vermijden is kunt u statistisch het overspannen configureren van boomhavenkosten met gebruik van het **overspannen - de kosten *kosten* van de boom** opdracht.

Port Aggregation Protocol (PAgP)

doel

PAgP is een beheerprotocol dat op beide einde van de link controleert op parameterconsistentie. PAgP assisteert het kanaal ook met aanpassing om een mislukking of toevoeging te koppelen. Hier zijn de kenmerken van PAgP:

- PAgP vereist dat alle poorten in het kanaal tot hetzelfde VLAN behoren of als boomstampoorten zijn geconfigureerd. Omdat dynamische VLAN's de verandering van een poort in een ander VLAN kunnen forceren, worden dynamische VLAN's niet in EtherChannel-deelname opgenomen.
- Als er al een bundel bestaat en de configuratie van een haven wordt aangepast, worden alle havens in de bundel aangepast om die configuratie aan te passen. Een voorbeeld van een dergelijke verandering is een verandering van VLAN of een `trunking` mode verandering.
- PAgP groepeert geen poorten die met verschillende snelheden of poortduplex werken. Als snelheid en duplex worden veranderd wanneer een bundel bestaat, verandert PAgP de havensnelheid en duplex voor alle havens in de bundel.

Overzicht

De PAgP poort controleert elke individuele fysieke (of logische) poort die moet worden gegroepeerd. Het zelfde multicast adres van groep MAC dat voor CDP pakketten wordt gebruikt wordt gebruikt om PAgP pakketten te verzenden. Het MAC-adres is 01-00-0c-cc-cc-cc. Maar de protocolwaarde is 0x0104. Dit is een samenvatting van de protocolbewerking:

- Zolang de fysieke poort omhoog is, worden PAgP pakketten elke seconde tijdens detectie, en elke 30 seconden in steady-state verzonden.
- Als gegevenspakketten worden ontvangen maar geen PAgP pakketten worden ontvangen, wordt aangenomen dat de poort is aangesloten op een apparaat dat niet PAgP-Geschikt is.
- Luister voor PAgP pakketten die bewijzen dat de fysieke poort een bidirectionele verbinding met een ander PAgP-geschikt apparaat heeft.
- Zodra twee dergelijke pakketten op een groep fysieke poorten worden ontvangen, probeer dan een geaggregeerde poort te vormen.
- Als de PAgP-pakketten een periode worden geblokkeerd, wordt de `PAgP-`status afgebroken.

Normale verwerking

Deze concepten helpen het gedrag van het protocol aan te tonen:

- Agport-A logische poort die bestaat uit alle fysieke poorten in dezelfde aggregatie en kan geïdentificeerd worden door zijn eigen SNMP als Index. Een poort bevat geen niet-operationele poorten.
- Channel—Een aggregatie die voldoet aan de formatiecriteria. Een kanaal kan niet-operationele havens bevatten en is een superreeks van steun. Protocols, die STP en VTP omvatten maar CDP en DTP uitsluiten, draaien boven PAgP via de poorten. Geen van deze protocollen kan pakketten verzenden of ontvangen tot PAgP de poorten aan een of meer fysieke poorten bevestigt.
- Groepsvermogen-elke fysieke poort en agport bezit een configuratieparameter die de `groep-vermogen` wordt genoemd. Een fysieke poort kan worden geaggregeerd met elke andere fysieke poort die dezelfde `groepscapaciteit` heeft, en alleen met zo'n fysieke poort.
- Aggregatie procedure-Wanneer een fysieke poort de `UpData` of `UpPAgP` status bereikt, wordt de poort toegevoegd aan een geschikte poort. Als de haven een van deze staten voor een andere staat verlaat, is de haven van de haven afgesneden.

Deze tabel geeft meer informatie over de staten:

Staat	Betekenis
`UpData`	Er zijn geen PAgP-pakketten ontvangen. PAgP-pakketten worden verzonden. De fysieke poort is de enige poort die op de poort is aangesloten. De niet-PAgP pakketten worden in en uit tussen de fysieke haven en de haven doorgegeven.
`BiDir`	Er is precies één pakje PAgP ontvangen dat bewijst dat er een bidirectionele verbinding bestaat met precies één buur. De fysieke poort is niet op een willekeurige poort aangesloten. PAgP-pakketten worden verzonden en kunnen worden ontvangen.
`UpPAgP`	Deze fysieke poort, wellicht in associatie met andere fysieke poorten, wordt aangesloten op een poort. PAgP-pakketten worden verzonden en ontvangen op de fysieke poort. De niet-PAgP pakketten worden in en uit tussen de fysieke haven en de haven doorgegeven.

Beide uiteinden van beide verbindingen moeten het eens worden over de groepering. De groep wordt gedefinieerd als de grootste groep havens in de groep die beide uiteinden van de verbindingsvergunning heeft.

Wanneer een fysieke poort de staat `UpPAgP` bereikt, wordt de poort toegewezen aan de instantie die de lid fysieke poorten heeft die overeenkomen met de `groep-mogelijkheid` van de nieuwe fysieke poort en die in de `BiDir` staat of de `UpPAgP` staat zijn. Al deze `BiDir`-poorten worden tegelijkertijd verplaatst naar de `UpPAgP`-staat. Als er geen instantie is die samenstellende fysieke poortparameters heeft die compatibel zijn met de nieuwe kant-en-klare fysieke poort, wordt de poort toegewezen aan een instantie met geschikte parameters die geen geassocieerde fysieke poorten hebben.

Een PAgP tijd kan op de laatste buur voorkomen die op de fysieke haven bekend is. De haven die tijden buiten is wordt uit de haven verwijderd. Tegelijkertijd worden alle fysieke poorten op

dezelfde poort waar timers op staan die ook zijn uitgezet, verwijderd. Dit maakt het mogelijk dat een agentschap waarvan het andere doel is overleden, in één keer wordt afgebroken, in plaats van één fysieke haven tegelijk.

Gedrag in falen

Als een link in een kanaal dat bestaat mislukt is, wordt de poort bijgewerkt en wordt het verkeer over de links gehashed die zonder verlies blijven. Voorbeelden van een dergelijke storing zijn:

- De poort is niet aangesloten
- Gigabit-interfaceconverter (GBIC) wordt verwijderd
- Fibre is kapot

Opmerking: Als je een link in een kanaal niet aansluit met een uitloop of verwijdering van een module, dan kan het gedrag anders zijn. Per definitie vereist een kanaal twee fysieke poorten. Als één poort verloren is van het systeem in een twee-poorts kanaal, wordt de logische poort afgebroken en wordt de originele fysieke poort herinitialiseerd met betrekking tot het overspannen van bomen. Het verkeer kan worden weggegooid totdat STP de poort beschikbaar maakt voor gegevens.

Dit verschil in de twee mislukkingsmodi is belangrijk wanneer u het onderhoud van een netwerk plant. Er kan een STP topologie verandering zijn waarvan u rekening moet houden wanneer u een online verwijdering of plaatsing van een module uitvoert. U moet elke fysieke link in het kanaal beheren met het netwerkbeheersysteem (NMS) omdat de verbinding niet verstoord kan blijven door een storing.

Voltooi een van deze aanbevelingen om ongewenste topologische veranderingen op Catalyst 6500/6000 te verminderen:

- Als één poort per module wordt gebruikt om een kanaal te vormen, gebruik dan drie of meer modules (drie in totaal).
- Als het kanaal twee modules overslaat, gebruik dan twee poorten op elke module (vier totaal).
- Als een twee-poorts kanaal nodig over twee kaarten is, gebruik slechts de poorten van de Supervisor Engine.

Configuratieopties

U kunt EtherChannel op verschillende manieren configureren, zoals in deze tabel wordt samengevat:

Modus	Configureerbare opties
`Aan`	PAgP werkt niet. De havenkanalen, ongeacht hoe de buurhaven wordt gevormd. Als de buurpoortmodus is `ingeschakeld`, wordt een kanaal gevormd.
`Automatisch`	Aggregatie staat onder controle van PAgP. Een haven wordt in een passieve onderhandelingsstaat geplaatst. Er worden geen PAgP-pakketten op de interface verzonden tot ten minste één PAgP-pakket is ontvangen dat aangeeft dat de zender in de `gewenste` modus werkt.
`wenseli`	Aggregatie staat onder controle van PAgP. Een

jk	haven wordt in een actieve onderhandelingsstaat geplaatst, waarin de haven onderhandelingen met andere havens via de verzending van pakketten PAgP initieert. Een kanaal wordt gevormd met een andere poortgroep in of wenselijk of auto modus.
Niet-stil Dit is de standaard op Catalyst 5500/5000 vezel FE en GE poorten.	Een auto of wenselijk mode sleutelwoord. Als er geen gegevenspakketten op de interface worden ontvangen, wordt de interface nooit aan een poort toegevoegd en kan deze niet voor gegevens worden gebruikt. Deze bidirectionaliteitstoetsing werd verstrekt voor specifieke hardware van Catalyst 5500/5000 omdat een aantal fouten in de link leiden tot een breuk van het kanaal. Wanneer u niet-stille modus toelaat, is het nooit toegestaan om een terugtrekkende buurpoort te laten zien en het kanaal onnodig te breken. Versoepelere bundeling en verbeterde bidirectionaliteitscontroles zijn standaard aanwezig in Catalyst 4500/4000 en 6500/6000-Series hardware.
Silent This is the default voor alle Catalyst 6500/6000 en 4500/4000 poorten, alsook 5500/5000 koperpoorten.	Een auto of wenselijk mode sleutelwoord. Als er geen gegevenspakketten op de interface worden ontvangen, wordt na een periode van 15 seconden de interface alleen aan een poort toegevoegd. De interface kan dus worden gebruikt voor datatransmissie. De Silent Mode staat ook voor kanaalbediening toe wanneer de partner een analyzer of een server kan zijn die nooit PAgP verstuurt.

De stille/niet-stille instellingen beïnvloeden hoe havens reageren op situaties die eenrichtingsverkeer veroorzaken. Wanneer een poort niet kan verzenden vanwege een mislukte fysieke interface of een gebroken vezel of kabel, kan de buurpoort nog in een operationele status worden achtergelaten. De partner blijft gegevens verzenden. Maar gegevens gaan verloren omdat het retourverkeer niet kan worden ontvangen. Spanning-tree netwerken kunnen ook vormen vanwege het unidirectionele karakter van de link.

Sommige glasvezelhavens hebben de gewenste mogelijkheid om de haven naar een niet-operationele staat te brengen wanneer de haven zijn ontvangstsignaal (FEFI) verliest. Deze actie zorgt ervoor dat de partnerpoort niet operationeel wordt en zorgt er effectief voor dat de havens

aan beide uiteinden van de verbinding naar beneden gaan.

Wanneer u apparaten gebruikt die gegevens verzenden (BPDU's) en u kunt geen unidirectionele voorwaarden detecteren, gebruik dan de `niet-stille` modus zodat de poorten niet-operationeel kunnen blijven totdat er gegevens beschikbaar zijn en de link naar verluidt bidirectioneel is. De tijd die PAgP nodig heeft om een unidirectionele link te detecteren is ongeveer 3,5 * 30 seconden = 105 seconden. 30 seconden is de tijd tussen twee opeenvolgende PAgP berichten. Gebruik UDLD, een snellere detector van unidirectionele koppelingen.

Wanneer u apparaten gebruikt die geen gegevens verzenden, gebruik dan de `stille` modus. Het gebruik van `stille` modus dwingt de haven aan te sluiten en in gebruik te nemen, ongeacht of ontvangen gegevens al dan niet aanwezig zijn. Bovendien wordt, voor die poorten die de aanwezigheid van een eenrichtingsvoorwaarde kunnen detecteren, de `stille` modus standaard gebruikt. Voorbeelden van deze poorten zijn nieuwere platforms die Layer 1 FEFI en UDLD gebruiken.

Om het scannen op een interface uit te schakelen, geeft u het opdracht **geen kanaal-group** ***nummer*** uit:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no channel-group 1
```

Verificatie

De tabel in dit hoofdstuk geeft een samenvatting van alle mogelijke scenario's voor een PAgP-kanaalmodus tussen twee direct aangesloten switches, Switch A en Switch B. Sommige van deze combinaties kunnen ervoor zorgen dat STP de poorten aan de kantelzijde in `errOff`-toestand plaatst, wat betekent dat die combinaties de poorten aan de kantelzijde afsluiten. De functie EtherChannel voor het bewaken van de configuratie is standaard ingeschakeld.

Switch A-kanaalmodus	Switch B-kanaalmodus	Switch A Channel State	Switch B-kanaalstatus
Aan	Aan	Kanaal (niet-PAgP)	Kanaal (niet-PAgP)
Aan	Niet ingesteld	Geen kanaal (errOff)	Geen kanaal
Aan	Automatisch	Geen kanaal (errOff)	Geen kanaal
Aan	wenselijk	Geen kanaal (errOff)	Geen kanaal
Niet ingesteld	Aan	Geen kanaal	Geen kanaal (errOff)
Niet ingesteld	Niet ingesteld	Geen kanaal	Geen kanaal
Niet ingesteld	Automatisch	Geen kanaal	Geen kanaal
Niet ingesteld	wenselijk	Geen	Geen kanaal

		kanaal	
Automatisch	Aan	Geen kanaal	Geen kanaal (errOff)
Automatisch	Niet ingesteld	Geen kanaal	Geen kanaal
Automatisch	Automatisch	Geen kanaal	Geen kanaal
Automatisch	wenselijk	PAgP-kanaal	PAgP-kanaal
wenselijk	Aan	Geen kanaal	Geen kanaal
wenselijk	Niet ingesteld	Geen kanaal	Geen kanaal
wenselijk	Automatisch	PAgP-kanaal	PAgP-kanaal
wenselijk	wenselijk	PAgP-kanaal	PAgP-kanaal

Cisco Configuration voor L2-kanalen

Schakel PAgP in en gebruik een instelling van `wenselijk-wenselijk` op alle EtherChannel-koppelingen. Zie deze uitvoer voor meer informatie:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no ip address
!--- This ensures that there is no IP !--- address that is assigned to the LAN port.
Switch(config-if)#channel-group number mode desirable
!--- Specify the channel number and the PAgP mode.
```

Controleer de configuratie op deze manier:

```
Switch#show run interface port-channel number
Switch#show running-config interface type slot#/port#
Switch#show interfaces type slot#/port# etherchannel
Switch#show etherchannel number port-channel
```

EtherChannel-configuratieservice voorkomen

U kunt een EtherChannel verkeerd configureren en een omspannende boomlus maken. Deze verkeerde configuratie kan het switch-proces overweldigen. Cisco IOS systeemsoftware omvat de **overspannend-tree Ethernet Guard misconfiguratie** optie om dit probleem te voorkomen.

Geef deze configuratieopdracht uit op alle Catalyst-switches die Cisco IOS-software als systeemsoftware gebruiken:

```
Switch(config)#spanning-tree etherchannel guard misconfig
```

Andere opties

Bij het sturen van twee hulpmiddelen die geen steun bieden aan de PAgP maar de LACP ondersteunen, wordt aanbevolen LACP de configuratie van de LACP actief te laten zijn aan beide uiteinden van de apparatuur. Zie het gedeelte Link Aggregation Control Protocol (LACP) van dit document voor meer informatie.

Wanneer u naar apparaten gaat die PAgP of LACP niet ondersteunen, moet u hard het kanaal `aan` coderen. Dit voorschrift geldt voor deze voorbeeldinrichtingen:

- servers
- Plaatselijke directeur
- Content switches
- Routers
- Switches met eerdere software
- Catalyst 2900XL/3500XL switches
- Catalyst 8540s switch

Geef deze opdrachten uit:

```
Switch(config)#interface type slot#/port#
Switch(config-if)#channel-group number mode on
```

Link Aggregation Control Protocol (LACP)

LACP is een protocol dat havens met gelijkaardige eigenschappen toelaat om een kanaal door dynamische onderhandeling met aangrenzende switches te vormen. PAgP is een Cisco-eigen protocol dat u alleen kunt uitvoeren op Cisco-switches en op die switches die gelicentieerde verkopers vrijgeven. Maar LACP, die in IEEE 802.3ad gedefinieerd is, staat Cisco switches toe om Ethernet-kanalisatie te beheren met apparaten die aan de 802.3ad specificatie voldoen.

LACP wordt ondersteund door deze platforms en versies:

- Catalyst 6500/6000 Series met Cisco IOS-softwarerelease 12.1(11b)EX en later
- Catalyst 4500 Series met Cisco IOS-softwarerelease 12.1(13)EW en hoger
- Catalyst 3750 Series met Cisco IOS-softwarerelease 12.1(14)EA1 en hoger

Er is zeer weinig verschil tussen de LACP en de PAgP vanuit functioneel oogpunt. Beide protocollen ondersteunen een maximum van acht poorten in elk kanaal, en de zelfde eigenschappen van de haven worden gecontroleerd alvorens de bundel te vormen. Deze poorteigenschappen omvatten:

- Speed
- Duplex
- Native VLAN en trunking type

De opvallende verschillen tussen de LACP en de PAgP zijn:

- Het LACP-protocol kan alleen op full-duplex poorten lopen en steunt geen half-duplex poorten.
- LACP-protocol ondersteunt hot standby poorten. LACP probeert altijd het maximum aantal compatibele havens in een kanaal te vormen, tot het maximum dat de hardware toestaat (acht havens). Als de LACP niet in staat is om alle poorten die compatibel zijn samen te voegen (bijvoorbeeld als het afstandssysteem restrictievere hardwarebeperkingen heeft), worden alle

poorten die niet actief in het kanaal kunnen worden opgenomen in warme stand-by staat en alleen gebruikt als een van de gebruikte havens faalt.

Opmerking: voor Catalyst 4500 Series switches is het maximale aantal poorten waarvoor u dezelfde beheertoets kunt toewijzen 8. Voor Catalyst 6500 en 3750 switches die Cisco IOS-software uitvoeren, probeert LACP het maximale aantal compatibele poorten in een EtherChannel te configureren, tot het maximum dat de hardware toestaat (8 poorten). Een extra acht poorten kunnen worden geconfigureerd als hot standby-poorten.

Overzicht

De LACP controleert elke afzonderlijke fysieke (of logische) te bundelen haven. LACP-pakketten worden verzonden met gebruik van het multicast groep MAC-adres **01-80-c2-00-00-02**. De type-/veldwaarde is 0x8809 met een subtype van 0x01. Dit is een samenvatting van de protocolhandeling:

- Het protocol is gebaseerd op de middelen om hun aggregatiekansen en de overheidsinformatie bekend te maken. De transmissie wordt op regelmatige en periodieke basis op elke geaggregeerde koppeling verzonden.
- Zolang de fysieke haven omhoog is, worden LACP-pakketten elke seconde verzonden tijdens detectie en elke 30 seconden in stabiele toestand.
- De partners op een aggregeerbare link luisteren naar de informatie die binnen het protocol wordt verstuurd en beslissen welke actie of acties zij moeten ondernemen.
- Compatibele poorten worden ingesteld in een kanaal, tot het maximum dat de hardware toestaat (acht poorten).
- De aggregaties worden gehandhaafd door de regelmatige en tijdige uitwisseling van actuele overheidsinformatie tussen de koppelingspartners. Als de configuratie verandert (vanwege een fout in de link), nemen de protocol partners bijvoorbeeld de tijd uit en nemen ze de juiste actie op basis van de nieuwe status van het systeem.
- Naast de periodieke LACP-gegevenseenheid (LACPDU) die de overheidsinformatie wijzigt, zendt het protocol een door een gebeurtenis gedreven LACPDU aan de partners toe. De partners van het protocol nemen de passende maatregelen op basis van de nieuwe stand van het systeem.

LACP-parameters

Om de LACP in staat te stellen te bepalen of een reeks verbindingen met hetzelfde systeem verbonden is en of deze verbindingen vanuit het oogpunt van aggregatie compatibel zijn, moet het mogelijk zijn om vast te stellen:

- Een wereldwijd unieke identificator voor elk systeem dat deelneemt aan de aggregatie van de link.Elk LACP-systeem moet een prioriteit krijgen die automatisch (met de standaardprioriteit 32768) of door de beheerder kan worden gekozen. De systeemprioriteit wordt hoofdzakelijk gebruikt in combinatie met het MAC-adres van het systeem om de systeemidentificatie te vormen.
- Een middel om de reeks mogelijkheden te identificeren die met elke poort en met elke aggregator worden geassocieerd, zoals begrepen door een bepaald systeem.Elke poort in het systeem moet een prioriteit krijgen, hetzij automatisch (met de standaardprioriteit 128), hetzij door de beheerder. De prioriteit wordt gebruikt in combinatie met het havennummer om de havenidentificatiecode te vormen.
- Een manier om een link aggregatiegroep en de bijbehorende aggregator te identificeren.De

mogelijkheid van een poort om samen te voegen met een andere wordt samengevat door een simpele 16-bits integer parameter die strikt groter is dan nul die key wordt genoemd. Elke toets wordt bepaald op basis van verschillende factoren, zoals:De eigenschappen van de haven, die gegevenssnelheid, duplexiteit, en punt-tot-punt of gedeeld medium omvattenConfiguratiebeperkingen die door de netwerkbeheerder worden ingesteldElke poort bevat twee toetsen:Een administratieve sleutelEen operationele sleutelMet de administratieve toets kan de hoofdwaarden door het beheer worden gemanipuleerd en kan de gebruiker dus deze toets kiezen. De operationele sleutel wordt door het systeem gebruikt om aggregaties te vormen. De gebruiker kan deze toets niet rechtstreeks kiezen of wijzigen. De reeks havens in een bepaald systeem die dezelfde operationele hoofdwaarde hebben, wordt geacht deel uit te maken van dezelfde sleutelgroep.

Dus, gezien twee systemen en een reeks havens met dezelfde administratieve sleutel, probeert elk systeem de havens samen te voegen, beginnend bij de haven met de hoogste prioriteit in het systeem met de hoogste prioriteit. Dit gedrag is mogelijk omdat elk systeem deze prioriteiten kent:

- De eigen prioriteit, die door de gebruiker of software is toegewezen
- De partner prioriteit, die door LACP-pakketten werd ontdekt

Gedrag in falen

Het mislukkingsgedrag van LACP is hetzelfde als het mislukkingsgedrag van PAgP. Als een link in een bestaand kanaal niet is geslaagd (bijvoorbeeld, als een poort is verwijderd, wordt een GBIC verwijderd of een vezel kapot is), wordt de licentie bijgewerkt en wordt het verkeer binnen 1 seconde over de resterende links gehashed. Elk verkeer dat niet hoeft te worden hervat na de mislukking (het verkeer dat op dezelfde link blijft verzenden) lijdt niet onder enig verlies. Het herstellen van de mislukte verbinding leidt een andere update aan de haven in, en het verkeer wordt opnieuw gehashed.

Configuratieopties

U kunt LACP EtherChannel op verschillende manieren configureren, zoals deze tabel samenvat:

Modus	Configureerbare opties
Aan	Het verbindingsaggregaat moet worden gevormd zonder enige LACP-onderhandeling. De switch stuurt het LACP-pakket niet en verwerkt geen inkomend LACP-pakket. Als de buurhavenmodus is ingeschakeld, wordt er een kanaal gevormd.
Uit (of) niet ingesteld	De haven verandert niet, ongeacht hoe de buur wordt gevormd.
Passief (standaard)	Dit is vergelijkbaar met de **automatische** modus in PAgP. De switch start het kanaal niet, maar begrijpt wel de binnenkomende LACP-pakketten. De peer (in actieve staat) initieert onderhandeling (door een LACP-pakket te verzenden) die de switch ontvangt en waaraan de switch antwoordt, en uiteindelijk het aggregatiekanaal met de peer

	vormt.
Actief	Dit lijkt op de **gewenste** modus in PAgP. De switch start de onderhandeling om een geaggregeerde link te vormen. Het verbindingsaggregaat wordt gevormd als het andere uiteinde in de actieve of passieve LACP-modus loopt.

LACP gebruikt een 30-seconden interval timer (Slow_Periodic_Time) nadat de LACP EtherChannel is gevestigd. Het aantal seconden voor de annulering van ontvangen LACPDU-informatie bij gebruik van lange time-outs (3 keer de Slow_Periodic_Time) is 90. UDLD wordt aanbevolen als een snellere detector van unidirectionele koppelingen. U kunt de LACP-timers niet aanpassen en op dit punt kunt u de switches niet configureren om de Fast Protocol Data Unit (PDU)-transmissie (elke seconde) te gebruiken om het kanaal te onderhouden nadat het kanaal is gevormd.

Verificatie

In de tabel in dit deel wordt een samenvatting gegeven van alle mogelijke scenario's van de LACP-kanaliseringsmodus tussen twee direct verbonden switches (Switch A en Switch B). Sommige van deze combinaties kunnen EtherChannel-beveiliging veroorzaken om de poorten aan de kantelkant in de foutstatus te plaatsen. De functie EtherChannel voor het bewaken van de configuratie is standaard ingeschakeld.

Switch A-kanaalmodus	Switch B-kanaalmodus	Switch A Channel State	Switch B-kanaalstatus
Aan	Aan	Kanaal (niet-LACP)	Kanaal (niet-LACP)
Aan	Uit	Geen kanaal (errOff)	Geen kanaal
Aan	passief	Geen kanaal (errOff)	Geen kanaal
Aan	Actief	Geen kanaal (errOff)	Geen kanaal
Uit	Uit	Geen kanaal	Geen kanaal
Uit	passief	Geen kanaal	Geen kanaal
Uit	Actief	Geen kanaal	Geen kanaal
passief	passief	Geen kanaal	Geen kanaal
passief	Actief	LACP-kanaal	LACP-kanaal
Actief	Actief	LACP-kanaal	LACP-kanaal

Cisco-aanbevelingen

Cisco raadt u aan PAgP op kanaalverbindingen tussen Cisco-switches in te schakelen. Bij het sturen van twee hulpmiddelen die geen steun bieden aan de PAgP maar de LACP ondersteunen, wordt aanbevolen LACP de configuratie van de LACP actief te laten zijn aan beide uiteinden van de apparatuur.

Op switches die CatOS in werking stellen, gebruiken alle poorten op een Catalyst 4500/4000 en een Catalyst 6500/6000 het kanaalprotocol van PAgP. Om havens te vormen om LACP te gebruiken, moet u het kanaalprotocol op de modules aan LACP instellen. LACP en PAgP kunnen niet op dezelfde module lopen op switches die CatOS in werking stellen. Deze beperking is niet van toepassing op switches die Cisco IOS-software uitvoeren. Switches die Cisco IOS-software uitvoeren kunnen PAgP en LACP ondersteunen op dezelfde module. Geef deze opdrachten uit om de LACP-kanaalmodus in te stellen op actief en om een administratief sleutelnummer toe te wijzen:

```
Switch(config)#interface range type slot#/port#
Switch(config-if)#channel-group admin_key mode active
```

De opdracht **toont de samenvatting van het kanaal** toont een één lijn samenvatting per kanaalgroep die deze informatie omvat:

- Groepsnummers
- Poortkanaalnummers
- Status van de havens
- De havens die deel uitmaken van het kanaal

De opdracht **van het kanaal van poort-kanaal** toont gedetailleerde havenkanaalinformatie voor alle kanaalgroepen. De output bevat deze informatie:

- Status van het kanaal
- Protocol dat wordt gebruikt
- De tijd sinds de havens werden gebundeld

Om gedetailleerde informatie voor een bepaalde kanaalgroep te tonen, met de details van elke haven afzonderlijk wordt getoond, gebruik de opdracht **van de detail *van kanaal_number* detail**. De opdrachtoutput bevat de partnergegevens en de poortkanaalgegevens. Raadpleeg voor meer informatie de configuratie van LACP (802.3ad) tussen Catalyst 6500/6000 en Catalyst 4500/4000.

Andere opties

Met kanaalapparaten die PAgP of LACP niet ondersteunen moet u het kanaal moeilijk op coderen. Dit voorschrift geldt voor deze inrichtingen:

- servers
- Plaatselijke directeur
- Content switches
- Routers
- Switches met oudere software
- Catalyst 2900XL/3500XL switches
- Catalyst 8540s switch

Geef deze opdrachten uit:

```
Switch(config)#interface range type slot#/port#
Switch(config-if)#channel-group admin_key mode on
```

UniDirectionele koppeldetectie

doel

UDLD is een bedrijfseigen, lichtgewicht protocol van Cisco dat werd ontwikkeld om gevallen van unidirectionele communicatie tussen apparaten te detecteren. Er zijn andere methoden om de bidirectionele status van transmissiemedia te detecteren, zoals FEFI. Maar er zijn gevallen waarin Layer 1-detectiesystemen niet volstaan. Deze scenario's kunnen resulteren in:

- De onvoorspelbare werking van STP
- De onjuiste of overmatige overstroming van pakketten
- Het zwarte heilig van verkeer

De functie UDLD richt deze foutvoorwaarden op vezel en koper Ethernet interfaces:

- Controleert de fysieke bekabelde configuraties—sluit af als `err`Uitgeschakeld poorten.
- Bescherm tegen unidirectionele verbindingen - Bij het ontdekken van een unidirectionele verbinding die wegens media of haven/interface defect optreedt, wordt de getroffen haven afgesloten als `errDisease`. Er wordt een corresponderend syslogbericht gegenereerd.
- Bovendien controleert de agressieve modus van de UDLD of een eerder veronderstelde bidirectionele link geen connectiviteit verliest in het geval dat de verbinding wegens congestie onbruikbaar wordt. De agressieve modus van UDLD voert doorlopende connectiviteitstests over de link uit. Het primaire doel van de agressieve modus van de UDLD is het voorkomen van het zwart bekleden van verkeer in bepaalde mislukte omstandigheden die niet door de normale modus UDLD worden aangepakt.

Raadpleeg de optie Unidirectional Link Detection Protocol (UDLD) voor meer informatie.

Spanning Tree heeft een steady-state-unidirectionele BPDU-stroom en kan de fouten hebben die in deze sectie worden weergegeven. Een poort kan plotseling niet overdragen BPDU's, wat een STP staatsverandering van `blokkeren` naar `doorsturen` op de buur veroorzaakt. Toch bestaat er nog steeds een lus omdat de haven nog kan worden ontvangen.

Overzicht

UDLD is een Layer 2-protocol dat boven de LLC-laag werkt (doelMAC 100-0c-cc-cc, SNAP HDLC-protocol type 0x011). Wanneer u UDLD in combinatie met mechanismen van FEFI en autonegotiation Layer 1 gebruikt, kunt u de fysieke (L1) en logische (L2) integriteit van een link valideren.

UDLD heeft bepalingen voor functies en bescherming die FEFI en autonome onderhandeling niet kunnen uitvoeren. Deze functies zijn onder meer:

- De detectie en cache van buurtinformatie
- De afsluiten van niet-aangesloten poorten
- Detectie van logische interface-/poortfouten of fouten op koppelingen die niet point-to-point zijn**Opmerking:** wanneer links niet point-to-point zijn, verplaatsen ze media-converters of

hubs.

UDLD maakt gebruik van deze twee basismechanismen.

1. UDLD leert over de buren en houdt de informatie bij in een lokaal cache.
2. UDLD stuurt een trein van UDLD-sondes/echo-berichten (hallo) bij de detectie van een nieuwe buurman of wanneer een buurman om een herynchronisatie van de cache vraagt.

UDLD stuurt voortdurend sondes/echo-berichten op alle poorten. Bij ontvangst van een corresponderend UDLD-bericht in een poort worden een detectiefase en validatieproces gestart. De haven is ingeschakeld als aan alle geldige voorwaarden is voldaan. Aan de voorwaarden is voldaan als de haven in twee richtingen is en correct is aangesloten. Als niet aan de voorwaarden wordt voldaan is de haven `errDisEnabled`, wat dit syslogbericht in werking stelt:

```
UDLD-3-AGGRDISABLE: Neighbor(s) of port disappeared on bidirectional link.
   Port disabled
UDLD-3-AGGRDISABLEFAIL: Neighbor(s) of port disappeared on bidirectional link.
   Failed to disable port
UDLD-3-DISABLE: Unidirectional link detected on port disabled.
UDLD-3-DISABLEFAIL: Unidirectional link detected on port, failed to disable port.
UDLD-3-SENDFAIL: Transmit failure on port.
UDLD-4-ONEWAYPATH: A unidirectional link from port to port of device [chars]
   was detected.
```

Voor een volledige lijst van systeemberichten per faciliteit, die gebeurtenissen van UDLD omvat, verwijs naar UDLD Berichten (Cisco IOS systeemmeldingen, Volume 2 van 2).

Na het opzetten van een verbinding en de classificatie ervan als bidirectioneel, blijft UDLD sondes/echo-berichten adverteren met een standaardinterval van 15 seconden.

Deze tabel bevat informatie over havenstaten:

Poortstaat	Opmerking
onbepaald	Detectie gestart/naburige UDLD is uitgeschakeld.
Niet van toepassing	UDLD is uitgeschakeld.
Shutdown	Unidirectionele link is gedetecteerd en de poort is uitgeschakeld.
tweerichtings	Bidirectionele link is gedetecteerd.

Onderhoud van buurcache

UDLD stuurt regelmatig hallo-producten/echo-pakketten op elke actieve interface om de integriteit van het UDLD buurcache te behouden. Tijdens de ontvangst van een hallo bericht, wordt het bericht gecached en bewaard in het geheugen gedurende een maximum periode, die wordt gedefinieerd als de wachttijd. Wanneer de houdtijd verstrijkt, is de respectieve cache-ingang verouderd. Als er een nieuw hallo-bericht wordt ontvangen binnen de periode van de houdtijd, vervangt het nieuwe de oudere ingang en wordt de corresponderende tijd-to-live timer gereset.

Wanneer een UDLD-enabled-interface wordt uitgeschakeld of wanneer een apparaat wordt gereset, worden alle bestaande cache-items voor de interfaces waarvan de configuratie verandert, gewist. Deze klaring handhaaft de integriteit van de UDLD cache. UDLD stuurt ten minste één bericht om de respectieve buren te informeren over de noodzaak om de corresponderende cache-

items te spoelen.

Echo-detectiesysteem

Het echomechanisme vormt de basis van het detectiealgoritme. Wanneer een UDLD-apparaat over een nieuw buurland leert of een resynchronisatieverzoek van een uit-of-sync buurman ontvangt, start het apparaat het detectievenster aan zijn kant van de verbinding of herstart het en stuurt het een barst van echo-berichten in antwoord. Omdat dit gedrag in alle buren hetzelfde moet zijn, verwacht de echo zender de echo's terug te ontvangen in antwoord. Als het detectievenster niet wordt ontvangen van geldige antwoordberichten, wordt de link beschouwd als eenrichtings. Vanaf dit punt kan een proces voor het herstellen van een link of het afsluiten van een poort worden geactiveerd. Andere zeldzame anomalieën waarvoor de machine wordt gecontroleerd:

- Looped-back (Tx) vezels verzenden naar de RX-aansluiting van dezelfde poort
- Misbedrading in het geval van een gedeeld media interconnect (bijvoorbeeld een hub of een soortgelijk apparaat)

Convergentietijd

Om STP-netwerken te voorkomen, heeft Cisco IOS-softwarerelease 12.1 en later het standaardberichtinterval van UDLD van 60 seconden tot 15 seconden verlaagd. Dit interval werd veranderd om een unidirectionele verbinding te sluiten voordat een voorheen geblokkeerde poort in 802.1D omspannende boom in staat is om naar een staat van verzending over te schakelen. De waarde van het berichtinterval bepaalt de snelheid waarmee een buurman UDLD-sondes na de verbinding of de detectiefase verstuurt. Het berichtinterval hoeft niet op beide uiteinden van een verbinding aan te passen, alhoewel de consistente configuratie waar mogelijk wenselijk is. Wanneer de buren van UDLD worden gevestigd, wordt het gevormde berichtinterval naar de buur verzonden, en het timeout interval voor die peer wordt berekend als:

```
3 * (message interval)
```

Als zodanig wordt een peer relatie na drie opeenvolgende hellos (of sondes) gemist. Omdat de berichtintervallen aan elke kant verschillend zijn, is deze timeout waarde eenvoudig van elke kant verschillend en één kant herkent een mislukking sneller.

De benaderende tijd die nodig is voor UDLD om een unidirectionele mislukking van een eerder stabiele link te detecteren is ongeveer:

```
2.5 * (message interval) + 4 seconds
```

Dit is ongeveer 41 seconden met het standaardberichtinterval van 15 seconden. Deze hoeveelheid tijd is veel korter dan de 50 seconden die normaal nodig zijn voor STP om opnieuw te converteren. Als de NMP CPU bepaalde reservecycli heeft en de gebruiker het gebruiksniveau zorgvuldig controleert (een goede praktijk), is een vermindering van het berichtinterval (zelfs) tot een minimum van 7 seconden aanvaardbaar. Ook helpt deze bericht-interval reductie de detectie te versnellen met een belangrijke factor.

Opmerking: het minimum is 1 seconde in Cisco IOS-softwarerelease 12.2(25)SEC.

Daarom heeft UDLD een veronderstelde afhankelijkheid van het standaard overspuiten van boomtimers. Als STP is ingesteld om sneller samen te vallen dan UDLD, overweeg dan een

alternatief mechanisme, zoals de STP lus Guard optie. Overweeg in dit geval een alternatief mechanisme wanneer u ook RSTP (802.1w) implementeert, omdat RSTP convergentiekenmerken in ms heeft, afhankelijk van de topologie. Voor deze gevallen, gebruik loop Guard in combinatie met UDLD om de meeste bescherming te bieden. Loop Guard voorkomt STP loops met de snelheid van de STP versie die in gebruik is. En UDLD zorgt voor de detectie van unidirectionele verbindingen op individuele EtherChannel-koppelingen of in gevallen waarin BPDU's niet langs de gebroken richting lopen.

Opmerking: UDLD is onafhankelijk van STP. UDLD vangt niet elke STP-mislukkingssituatie, zoals de fouten die door een CPU worden veroorzaakt die BPDU's niet verzenden voor een tijd die groter is dan (2 * Vertraging + maxage). Om deze reden, raadt Cisco aan om UDLD in combinatie met loop Guard in topologieën toe te passen die op STP vertrouwen.

Waarschuwing: Let op van eerdere releases van UDLD in de 2900XL/3500XL-switches die een niet-configureerbare, 60-seconden standaardoplossing gebruiken. Ze zijn vatbaar voor de omspeer-boom lusvoorwaarden.

UDLD Aggressive Mode

Aggressieve UDLD werd gecreëerd om specifiek die paar gevallen aan te pakken waarin een doorlopende test van bidirectionele connectiviteit noodzakelijk is. Als zodanig biedt de functie agressieve mode meer bescherming tegen gevaarlijke unidirectionele voorwaarden in deze situaties:

- Wanneer het verlies van UDLD PDU's symmetrisch is en beide eindigen de tijd. In dit geval wordt geen van beide poorten geannuleerd.
- Aan één kant van een link zit een poort (zowel Tx als Rx).
- De ene kant van de link blijft omhoog, de andere kant van de link is omlaag gegaan.
- Automatische onderhandeling, of een ander Layer 1 foutdetectiemechanisme, is uitgeschakeld.
- Een vermindering van het vertrouwen op Layer 1 FEFI - mechanismen is wenselijk.
- U hebt maximale bescherming nodig tegen fouten in een unidirectionele link op een punt-tot-punt FE/GE-aansluiting. In het bijzonder kunnen, wanneer geen falen tussen twee buren toegestaan is, agressieve problemen van de UDLD als een hartslag beschouwd worden, waarvan de aanwezigheid de gezondheid van de link garandeert.

Het meest gebruikelijke geval voor een implementatie van een UDLD agressief is het uitvoeren van de connectiviteitscontrole op een lid van een bundel wanneer autonoom onderhandelen of een ander Layer 1 foutdetectiesysteem uitgeschakeld of onbruikbaar is. Het is met name nuttig met EtherChannel-verbindingen omdat PAgP en LACP, ook al zijn ze in staat, geen zeer lage hallo-timers gebruiken in stabiele toestand. In dit geval heeft UDLD-agressief als extra voordeel dat mogelijke omspanningsboomloops worden voorkomen.

Het is belangrijk om te begrijpen dat de normale UDLD-modus wel controleert op een eenrichtingsvoorwaarde, zelfs nadat een link de bidirectionele status heeft bereikt. UDLD is bedoeld om Layer 2-problemen te detecteren die STP-loops veroorzaken, en die problemen zijn doorgaans in één richting gericht (omdat BPDU’s in één richting stromen bij steady-state). Daarom is het gebruik van UDLD normaal in combinatie met autonegotiation en loop Guard (voor netwerken die op STP vertrouwen) vrijwel altijd voldoende. Als de agressieve modus van UDLD is ingeschakeld, nadat alle buren van een poort zijn uitgeput, in de advertentie of in de detectiefase, herstart de agressieve modus van UDLD de linkup sequentie in een poging om opnieuw te synchroniseren met potentieel out-of-sync-buren. Als na een snelle trein van berichten (acht

mislukte herhalingen) de link nog steeds onbepaald wordt geacht, wordt de poort in de foutmelding gezet.

N.B.: Sommige switches zijn niet agressief UDLD-compatibel. Op dit moment hebben Catalyst 2900XL en Catalyst 3500XL harde codeintervallen van 60 seconden. Dit wordt niet voldoende snel beschouwd om tegen mogelijke STP-lopen te beschermen (met de standaard STP-parameters aangenomen).

Automatisch herstel van UDLD-links

Terugwinning opnieuw uitschakelen is normaal gesproken uitgeschakeld. Nadat deze wereldwijd is geactiveerd, als een poort in de foutmelding staat, wordt deze automatisch na een geselecteerd tijdinterval opnieuw geactiveerd. De standaardtijd is 300 seconden, wat een globale timer is en voor alle poorten in een switch wordt onderhouden. Afhankelijk van de softwarerelease, kunt u een port reenablement handmatig voorkomen als u de foutmelding voor die poort instelt om uit te schakelen met gebruik van het foutloze timeout herstelmechanisme voor UDLD:

```
Switch(config)#errdisable recovery cause udld
```

Overweeg gebruik van de foutmelding wanneer u UDLD agressieve modus implementeert zonder out-of-band netwerkbeheerfuncties, in het bijzonder in de toegangslaag of op elk apparaat dat in geval van een foutmelding geïsoleerd kan raken van het netwerk.

Raadpleeg foutmelding voor herstel (Catalyst 6500 Series Cisco IOS Opdrachtreferentie, 12.1 E) voor meer informatie over het instellen van een tijdelijke periode voor poorten in de staat van uitschakelen.

Ermee-herstel kan met name van belang zijn voor UDLD in de toegangslaag wanneer de switches van de toegang over een campusomgeving worden verdeeld en het handmatige bezoek van elke switch om beide uplinks opnieuw in te schakelen aanzienlijk tijd vergt.

Cisco adviseert geen foutherstel in de kern van het netwerk uit te schakelen omdat er meestal meerdere ingangspunten in een kern zijn en automatisch herstel in de kern kan leiden tot terugkerende problemen. Daarom moet u een poort aan de kern handmatig opnieuw inschakelen als UDLD de poort uitschakelt.

UDLD op Routed Links

Voor deze discussie is een routed link een van deze twee soorten verbindingen:

- Point-to-Point tussen twee routerknooppunten (geconfigureerd met een 30-bits subnetmasker)
- Een VLAN met meerdere poorten, maar dat alleen routeverbindingen ondersteunt, zoals in een gesplitste Layer 2 kerntopologie

Elk Interior Gateway Routing Protocol (IGRP) heeft unieke kenmerken met betrekking tot de manier waarop het buurrelaties en routeconvergentie hanteert. Deze sectie beschrijft de kenmerken die relevant zijn voor deze discussie, die twee van de meer prevalente routingprotocollen die vandaag worden gebruikt, Open Shortest Path First (OSPF) Protocol en Enhanced IGRP (DHCP) contrasteert.

Opmerking: Een storing in Layer 1 of Layer 2 op een punt-tot-punt routed Network leidt tot een bijna onmiddellijke verwijdering van de Layer 3-verbinding. Omdat de enige poort op de switch in

dat VLAN overschakelingen naar een niet-verbonden staat op de mislukking van Layer 1/Layer 2, synchroniseert de eigenschappen van de interfaceauto-staat Layer 2 en Layer 3 poortstaten in ongeveer twee seconden en plaats de interface van Layer 3 VLAN in een omhoog/omlaag staat (lijnprotocol dat omlaag gaat).

Als u de standaardwaarden van de timer aanneemt, verstuurt OSPF hallo-berichten elke 10 seconden en heeft een doodinterval van 40 seconden (4 * hallo). Deze timers zijn consistent voor OSPF point-to-point en broadcast netwerken. Omdat OSPF tweevoudige communicatie vereist om een nabijheid te vormen, is de erger-case overlooptijd 40 seconden. Dit is zelfs waar als de mislukking van Layer 1/Layer 2 niet zuiver is op een point-to-point verbinding en een half-gebakken scenario verlaat waarmee het Layer 3-protocol moet worden behandeld. Omdat de detectietijd van UDLD zeer vergelijkbaar is met de detectietijd van een OSPF-dode timer (ongeveer 40 seconden) zijn de voordelen van de configuratie van UDLD-normale modus op een OSPF-Layer 3 point-to-point link beperkt.

In veel gevallen, converteert EHRM sneller dan OSPF. Maar het is belangrijk om op te merken dat bidirectionele communicatie geen vereiste is voor buren om routeinformatie uit te wisselen. In zeer specifieke halfbakken mislukkingsscenario's, is Ecu kwetsbaar voor het zwart houden van verkeer dat duurt tot een andere gebeurtenis de routes via die actieve buur brengt. De normale modus van UDLD kan deze omstandigheden verminderen omdat het de unidirectionele fout van de link detecteert en de poort wordt uitgeschakeld door een fout.

Voor Layer 3 routed connecties die elk routeringsprotocol gebruiken, biedt UDLD-standaard nog steeds bescherming tegen problemen die aanwezig zijn bij initiële linkactivering, zoals bedrading of defecte hardware. Daarnaast biedt de agressieve modus van UDLD deze voordelen op Layer 3 routed connecties:

- Voorkomt onnodig zwart roteren van verkeer (in sommige gevallen is dit vereist voor een minimum timer)
- Plaatst een flappende link in de foutstand
- Bescherm tegen lijnen die uit Layer 3 EtherChannel-configuraties resulteren

Standaardgedrag van UDLD

UDLD is mondiaal uitgeschakeld en standaard beschikbaar in leesbaarheid op glasvezelpoorten. Omdat UDLD een infrastructuurprotocol is dat alleen tussen switches nodig is, wordt UDLD standaard uitgeschakeld aan koperpoorten, die doorgaans worden gebruikt voor host-toegang. Merk op dat u UDLD mondiaal en op interfaceniveau moet inschakelen voordat buren bidirectionele status kunnen bereiken. Het standaardberichtinterval is 15 seconden. Maar, het standaardberichtinterval kan in sommige gevallen tonen als zeven seconden. Raadpleeg Cisco bug-ID CSCea70679 (alleen geregistreerde klanten) voor meer informatie. Het standaardberichtinterval is Configureerbaar tussen zeven en 90 seconden en de UDLD-agressieve modus is uitgeschakeld. Cisco IOS-softwarerelease 12.2(25)SEC beperkt deze minimale timer verder tot één seconde.

Cisco-configuratie-aanbeveling

In de meeste gevallen raadt Cisco u aan om UDLD normale modus in te schakelen op alle point-to-point FE/GE links tussen Cisco-switches en het UDLD-berichtinterval in te stellen op 15 seconden wanneer u de standaard 802.1D-overspannende drie timers gebruikt. Bovendien, waar netwerken voor redundantie en convergentie van STP op STP vertrouwen (wat betekent dat er één of meer poorten zijn in de STP-blokkerende staat in de topologie), gebruik UDLD in combinatie met de juiste functies en protocollen. Tot deze functies behoren FEFI, autonome

onderhandeling, lus Guard, enzovoort. Meestal, als autonome onderhandeling wordt geactiveerd, is de agressieve modus niet nodig omdat autonome onderhandeling de foutdetectie bij Layer 1 compenseert.

Geef een van deze twee opdrachtopties af om UDLD in staat te stellen:

Opmerking: de syntaxis is van verschillende platforms/versies veranderd.

- ```
  udld enable
  !--- Once globally enabled, all FE and GE fiber !--- ports have UDLD enabled by default.
  udld port
  ```

  of

- ```
  udld enable
  !--- The copper ports of some earlier Cisco IOS Software !--- releases can have UDLD enabled
  by individual port command.
  ```

U moet poorten handmatig inschakelen die zijn afgesloten vanwege de unidirectionele link-symptomen. Gebruik een van deze methoden:

```
udld reset
!--- Globally reset all interfaces that UDLD shut down. no udld port
udld port [aggressive]
!--- Per interface, reset and reenable interfaces that UDLD shut down.
```

De **foutmelding voor de oorzaak van herstel udld** en **foutmelding *interval* kan worden gebruikt om automatisch de fout-uitgeschakeld UDLD-toestand te herstellen.**

Cisco raadt u aan om alleen het uitschakelingsmechanisme in de toegangslaag van het netwerk te gebruiken, met terugwinningstijden van 20 minuten of meer, als de fysieke toegang tot de switch moeilijk is. De beste situatie is om tijd voor netwerkstabilisatie en probleemoplossing toe te staan, voordat de haven weer online wordt gezet en netwerkinstabiliteit veroorzaakt.

Cisco raadt u aan *niet* de terugwinningsmechanismen in de kern van het netwerk te gebruiken omdat dit instabiliteit kan veroorzaken die op convergentiegebeurtenissen betrekking heeft telkens als een defecte link wordt teruggebracht. Het overbodige ontwerp van een kernnetwerk biedt een reservepad voor een mislukte verbinding en laat tijd voor een onderzoek van de oorzaken van UDLD-falen toe.

UDLD gebruiken zonder STP-bewaking

Voor Layer 3 point-to-point, of Layer 2 links waar er een lus-free STP topologie is (geen poortblokkering) raadt Cisco u aan om agressieve UDLD op point-to-point FE/GE links tussen Cisco switches in te schakelen. In dit geval wordt het berichtinterval ingesteld op zeven seconden en wordt bij 802.1D STP gebruikgemaakt van een standaard timer.

UDLD op EtherChannel

Of STP loop Guard wordt ingezet of niet wordt ingezet, wordt de agressieve modus van UDLD aanbevolen voor elke EtherChannel-configuratie, in combinatie met de gewenste kanaalmodus. In

EtherChannel-configuraties kan een storing in de link van het kanaal die het overspuiten van bomen BPDU's en PAgP-controleverkeer vervoert onmiddellijke lijnen tussen de kanaalpartners veroorzaken als de kanaalverbindingen worden ontbundeld. De agressieve modus van UDLD sluit een mislukte poort af. PAgP (auto/wenselijke kanaalmodus) kan dan onderhandelen over een nieuwe controlelink en effectief een mislukte link van het kanaal elimineren.

UDLD met 802.1w Spanning Tree

Om loops te voorkomen wanneer u nieuwere omspanningsboomversies gebruikt, gebruik UDLD normale wijze en STP lus Guard met RSTPs zoals 802.1w. UDLD kan bescherming bieden tegen unidirectionele koppelingen tijdens een linkupfase. STP-lusbeveiliging kan STP-loops voorkomen in het geval dat de koppelingen *in* één richting worden *nadat* UDLD de koppelingen als bidirectioneel heeft gedefinieerd. Omdat u UDLD niet kunt configureren om kleiner te zijn dan de standaard 802.1w-timers, is STP loop Guard nodig om loops in redundante topologieën volledig te voorkomen.

Raadpleeg de optie Unidirectional Link Detection Protocol (UDLD) voor meer informatie.

UDLD testen en bewaken

UDLD is niet makkelijk te testen zonder een waarlijk defect/unidirectionele component in het lab, zoals een gebrekkige GBIC. Het protocol was ontworpen om minder vaak voorkomende mislukkingsscenario's te detecteren dan die scenario's die gewoonlijk in een lab worden gebruikt. Als u bijvoorbeeld een simpele test uitvoert zoals een streng van een vezel van de stekker loskoppelen om de gewenste `foutmelding` te zien, moet u eerst Layer 1 autonomie uitschakelen. Anders gaat de fysieke poort `naar beneden`, waarmee de UDLD-berichtcommunicatie wordt hersteld. Het afstandsgedeelte beweegt naar de `niet-`gedefinieerde toestand in de normale modus en beweegt alleen naar de onduidelijke status met behulp van de UDLD-agressieve modus.

Een extra testmethode simuleert het PDU-verlies van de buur voor UDLD. De methode is MAC-Layer filters te gebruiken om het UDLD/CDP hardwareadres te blokkeren terwijl u andere adressen toelaat om over te gaan. Sommige switches verzenden geen UDLD-frames wanneer de poort is geconfigureerd als een Switched Port Analyzer (SPAN)-bestemming, die een niet-reagerende UDLD-buurman simuleert.

Gebruik deze opdracht om UDLD te controleren:

```
show udld gigabitethernet1/1
Interface Gi1/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 7
Time out interval: 5
```

Verder kunt u vanaf het inschakelen van modus in Cisco IOS-softwarerelease 12.2(18)SXD of latere switches de verborgen opdracht **show** udld buurland uitgeven om de inhoud van het UDLD-cache te controleren (op de manier waarop CDP dat doet). Het is vaak zeer nuttig om het UDLD-cache te vergelijken met het CDP-cachegeheugen om te controleren of er een protocol-specifieke anomalie is. Wanneer ook CDP wordt beïnvloed, betekent dit doorgaans dat alle BPDU's/PDU's

worden beïnvloed. Controleer daarom ook STP. Controleer bijvoorbeeld op recente wijzigingen in de wortelidentiteit of wortel/aangewezen poortplaatsing.

U kunt de status en de configuratieconsistentie van UDLD met gebruik van de Cisco UDLD SNMP MIB-variabelen controleren.

Multilayer-switching

Overzicht

In Cisco IOS systeemsoftware wordt MultiLayer Switching (MLS) ondersteund op de Catalyst 6500/6000 Series en alleen intern. Dit betekent dat de router in de switch moet worden geïnstalleerd. nieuwere Catalyst 6500/6000 Supervisor Engine ondersteunen MLS CEF, waarin de routingtabel wordt gedownload naar elke kaart. Dit vereist extra hardware, die de aanwezigheid van een Distributed Forwarding Card (DFC) omvat. DFC's worden niet ondersteund in CatOS-software, zelfs als u ervoor kiest Cisco IOS-software te gebruiken op de routerkaart. DFC's worden alleen ondersteund in Cisco IOS-systeemsoftware.

Het MLS cache dat wordt gebruikt om NetFlow statistieken op Catalyst switches mogelijk te maken is het op stroom gebaseerde cache dat de Supervisor Engine I kaart en de legacy Catalyst switches gebruiken om Layer 3-switching in te schakelen. MLS is standaard ingeschakeld op Supervisor Engine 1 (of Supervisor Engine 1A) met MSFC of MSFC2. Er is geen extra MLS-configuratie nodig voor standaard MLS-functionaliteit. U kunt het MLS cache op een van de drie modi configureren:

- bestemming
- bronbestemming
- brondoelpoort

Het stroommasker wordt gebruikt om de MLS-modus van de switch te bepalen. Deze gegevens worden vervolgens gebruikt om Layer 3-stromen in de Catalyst switches van Supervisor Engine met voorzieningen in te schakelen. De messen van Supervisor Engine II gebruiken het MLS cache niet om pakketten te switches omdat deze kaart hardware CEF-enabled is, wat een veel schaalbare technologie is. Het MLS cache wordt in de Supervisor Engine II kaart bewaard om alleen de statistische export van NetFlow mogelijk te maken. Daarom kan Supervisor Engine II indien nodig worden ingeschakeld voor volledige stroom zonder negatieve impact op de switch.

Configuratie

De MLS verouderingstijd is van toepassing op alle MLS cache items. De verouderingswaarde wordt rechtstreeks op de veroudering van de doelmodus toegepast. U verdeelt de verouderingswaarde van MLS door twee om de bron-aan-bestemming verouderingstijd af te leiden. Verdeel de MLS verouderingswaarde met acht om de verouderingstijd volledig te vinden. De standaard MLS verouderingswaarde is 256 seconden.

U kunt de normale verouderingstijd in het bereik van 32 tot 4092 seconden configureren in acht seconden. Elke veroudering-tijd waarde die geen meerdere van acht seconden is wordt aangepast aan het dichtstbijzijnde veelvoud van 8 seconden. Zo wordt een waarde van 65 aangepast naar 64 en wordt een waarde van 127 aangepast naar 128.

Andere gebeurtenissen kunnen de zuivering van MLS-ingangen veroorzaken. Dergelijke gebeurtenissen omvatten:

- Routing-wijzigingen
- Een verandering in de verbindingsstaatDe PFC-link is bijvoorbeeld uitgeschakeld.

Om de MLS cache size onder 32.000 items te houden, schakelt u deze parameters in nadat u de **mls aging** opdracht geeft:

```
Normal: configures the wait before aging out and deleting shortcut entries in
the L3 table.

Fast aging: configures an efficient process to age out entries created for flows that
only switch a few packets and then are never used again. The fast aging parameter uses
the time keyword value to check if at least the threshold keyword value of packets has
been switched for each flow. If a flow has not switched the threshold number of packets
during the time interval, then the entry in the L3 table is aged out.

Long: configures entries for deletion that have been up for the specified value even if
the L3 entry is in use. Long aging is used to prevent counter wraparound, which could
cause inaccurate statistics.
```

Configuratie

Een typische cache-ingang die wordt verwijderd is de ingang voor stromen naar en van een Domain Name Server (DNS) of TFTP-server die mogelijk nooit meer kan worden gebruikt nadat de entry-functie is gecreëerd. De detectie en eliminatie van deze items bespaart ruimte in het MLS cache voor ander gegevensverkeer.

Als u MLS snelle verouderingstijd moet inschakelen, stelt u de aanvankelijke waarde in op 128 seconden. Als de grootte van de MLS cache meer dan 32.000 items blijft groeien, verlaagt u de instelling tot de cachegrootte onder 32.000 blijft. Als de cache meer dan 32.000 items blijft groeien, verlaagt u de normale MLS-verouderingstijd.

Cisco aanbevolen MLS-configuratie

Laat MLS op de standaardwaarde alleen bestemming achter, tenzij NetFlow-export vereist is. Als NetFlow vereist is, schakelt u MLS full flow alleen in op Supervisor Engine II systemen.

Geef deze opdracht uit om MLS-stroombestemming in te schakelen:

```
Switch(config)#mls flow ip destination
```

Jumboframes

Maximale transmissieeenheid

Het maximum transmissie-unit (MTU) is het grootste datagram of pakketformaat in bytes dat een interface kan verzenden of ontvangen zonder het pakket te fragmenteren.

Overeenkomstig de standaard IEEE 802.3 is de maximale grootte van Ethernet-frame:

- **1518 bytes** voor normale frames (1500 bytes plus 18 extra bytes van Ethernet-header en CRC-trailer)
- **1522 bytes** voor 802.1Q ingekapselde frames (1518 plus 4 bytes van het taggen)

Baby Giants: Met de functie Baby Giants kan de switch door/voorwaartse pakketten passeren die iets groter zijn dan de IEEE Ethernet MTU, in plaats van de frames te groot te verklaren en weg te gooien.

Jumbo: De definitie van de grootte van een frame is van een verkoper afhankelijk, omdat de grootte van de frames geen deel uitmaakt van de IEEE-standaard. Jumboframes zijn frames die groter zijn dan de standaard Ethernet frame size (dit is 1518 bytes), die de Layer 2 header en frame check sequentie [FCS] omvat).

De standaard MTU grootte is 9216 bytes nadat de ondersteuning van het frame-jumbo op de afzonderlijke poort is ingeschakeld.

Wanneer verwacht u pakketten die groter zijn dan 1518 bytes

Om het verkeer over geschakelde netwerken te kunnen transporteren, moet u er zeker van zijn dat de via de switch ondersteunde verkeers-MTU niet groter is dan die welke op de platformen wordt ondersteund. Er zijn verschillende redenen dat de grootte van bepaalde frames kan worden ingekort:

- **Verlener-specifieke vereisten**-Toepassingen en bepaalde NIC's kunnen een grootte van MTU specificeren die buiten de standaard 1500 bytes valt. Deze verandering is voorgekomen wegens studies die bewijzen dat een toename in de grootte van een Ethernet frame de gemiddelde doorvoersnelheid kan verhogen.
- **Trunking**-Om de informatie van VLAN ID tussen switches of andere netwerkapparaten over te brengen, is trunking gebruikt om het standaard Ethernet kader te vergroten. Vandaag de dag zijn de twee meest voorkomende vormen van trunking:Cisco eigen ISL-insluiting802,1Q router
- **Multiprotocol Label Switching (MPLS)** - Nadat u MPLS op een interface hebt ingeschakeld, kan MPLS de grootte van een pakket vergroten, wat afhankelijk is van het aantal labels in de labelstack voor een MPLS-gelabeld pakket. De totale grootte van een label is 4 bytes. De totale grootte van een labelstack is:
  ```
  n * 4 bytes
  ```
  Als een labelstack wordt gevormd, kunnen de frames groter zijn dan de MTU.
- **802.1Q tunneling**-802.1Q tunneling-pakketten bevatten twee 802.1Q tags, waarvan slechts één voor één zichtbaar is voor de hardware. Daarom voegt de interne tag 4 bytes toe aan de MTU-waarde (payload size).
- **Universal Transport Interface (UTI)/Layer 2 Tunneling Protocol, versie 3 (Layer 2 TPv3)**—UTI/Layer 2 TPv3 kapselt Layer 2 gegevens in die via het IP-netwerk moeten worden doorgestuurd. UTI/Layer 2 TPv3 kan de oorspronkelijke grootte van het frame met maximaal 50 bytes verhogen. Het nieuwe frame bevat een nieuwe IP-kop (20-bytes), Layer 2 TPv3-header (12-bytes) en een nieuwe Layer 2-header. De lading van Layer 2 TPv3 bestaat uit het volledige frame van Layer 2, dat Layer 2 omvat.

doel

Op hardware gebaseerde switching met hoge snelheid (1 Gbps en 10 Gbps) hebben jumboframes een zeer concrete oplossing gemaakt voor problemen met suboptimale doorvoersnelheid. Hoewel er geen officiële standaard is voor de grootte van een jumbo-frame, is een veel voorkomende waarde die in het veld vaak wordt gebruikt 9216 bytes (9 KB).

Naleving van netwerkefficiëntie

U kunt de netwerkefficiëntie voor een pakkettransport berekenen als u de payload-grootte indeelt door de som van de overhead-waarde en de payload-grootte.

Zelfs als de verhoging van de netwerkefficiëntie met jumboframes slechts bescheiden is en van 94.9% (1500 bytes) naar 99.1% (9216 bytes) gaat, wordt de verwerking overhead (CPU-gebruik) van de netwerkapparaten en de eindhosts proportioneel verlaagd naar de pakketgrootte. Dit is de reden dat krachtige LAN en WAN netwerktechnologieën de voorkeur geven aan nogal grote maximum kaderformaten.

Prestatieverbetering is alleen mogelijk wanneer de gegevensoverdrachten worden uitgevoerd. Voorbeelden van toepassingen zijn:

- Terug-naar-back communicatie van servers (bijvoorbeeld transacties in Network File System [NFS])
- serverclustering
- Snelle back-ups van gegevens
- Snelle supercomputerverbinding
- Grafische toepassingen gegevensoverdrachten

Naleving van netwerkprestaties

De prestaties van TCP via WANs (het internet) zijn uitgebreid bestudeerd. Deze vergelijking legt uit hoe TCP-doorvoersnelheid een bovengrens heeft gebaseerd op:

- Het maximum segmentformaat (MSS), dat de lengte MTU minus de lengte van de TCP/IP-headers is
- Ronde reistijd (RTT)
- Het pakketverlies

$$Throughput \leq\sim 0.7 \times MSS / \left(RTT \times \sqrt{packet\_loss}\right)$$

Volgens deze formule is de maximaal bereikbare TCP-doorvoersnelheid rechtstreeks evenredig met de MSS. Dit betekent dat, met constant RTT en pakketverlies, u de TCP doorvoersnelheid kunt verdubbelen als u de pakketgrootte verdubbelt. Op dezelfde manier kan een zesvoudige toename van de grootte, wanneer je jumboframes gebruikt in plaats van 1518-byte-frames, een mogelijke zesvoudige verbetering van de TCP-doorvoersnelheid van een Ethernet-verbinding opleveren.

Overzicht

De standaard IEEE 802.3-specificatie definieert een maximale Ethernet-frame-grootte van **1518**. De 802.1Q ingekapselde frames, met een lengte van tussen 1519 en 1522 bytes, werden in een later stadium aan de 802.3-specificatie toegevoegd via het IEEE Std 802.3ac-1998-addendum. Soms worden ze in de literatuur genoemd als **baby-reuzen**.

In het algemeen, worden pakketten geclassificeerd als **gigantische frames** wanneer zij de gespecificeerde maximum lengte Ethernet voor een specifieke Ethernet verbinding overschrijden. Gigante pakketten worden ook **jumboframes** genoemd.

Het belangrijkste punt van verwarring over jumboframes is de configuratie: verschillende interfaces ondersteunen verschillende maximale pakketformaten en behandelen soms grote pakketten op een beetje verschillende manier.

Catalyst 6500 Series-switches

In deze tabel wordt geprobeerd de grootte van MTU's samen te vatten die op dit moment door verschillende kaarten op Catalyst 6500 platform worden ondersteund:

Lijnkaart	MTU-grootte
Standaard	9216 bytes
WS-X6248-RJ-45, WS-X6248A-RJ-45, WS-X6248-TEL, WS-X6248A-TEL, WS-X6348-RJ-45, WS-X6348 RJ45V, WS-X6348-RJ-21 en WX-X6348-RJ21V	8092 bytes (beperkt door de PHY-chip)
WS-X6148-RJ-45(V), WS-X6148-RJ-21(V), WS-X6148-45AF en WS-X6148-21AF	9100 bytes (bij 100 Mbps) 9216 bytes (bij 10 Mbps)
WS-X6516 GE-TX switch	8092 bytes (100 Mbps) 9216 bytes (10 of 1000 Mbps)
WS-X6148(V)-GE-TX, WS-X6148-GE-45AF, WS-X6548(V)-GE-TX en WS-X6548-GE-45AF	1500 bytes
ATM optische servicesmodule (OC12c)	9180 bytes
OSM CHOC3, CHOC12, CHOC48 en CT3	9216 bytes (OCx en DS3) 7673 bytes (T1/E1)
FlexWAN	7673 bytes (CT3 T1/DS0) 9216 bytes (OC3c POS) 7673 bytes (T1)
WS-X6148-1 GE-TX en WS-X6548-1 GE-TX	Geen ondersteuning

Raadpleeg Ethernet, Fast Ethernet, Gigabit Ethernet en 10 Gigabit Ethernet-switching voor meer informatie.

Layer 2 en Layer 3 Jumbo-ondersteuning in Catalyst 6500/6000 Cisco IOS-software

Er is Layer 2 en Layer 3 jumboondersteuning met PFC/MSFC1, PFC/MSFC2 en PFC2/MSFC2 op alle GE poorten die zijn geconfigureerd als Layer 2 en Layer 3 fysieke interfaces. De steun bestaat ongeacht of deze havens afstammelingen of kanaliseren. Deze optie is beschikbaar in Cisco IOS-softwarerelease 12.1.1E en hoger.

- De grootte van de MTU van alle fysieke poorten die met jumbo zijn uitgerust, zijn verbonden. Een verandering in één ervan verandert allemaal. Ze houden altijd dezelfde grootte van een MTU van het Jumbo - frame nadat ze zijn ingeschakeld.
- Tijdens het configureren schakelt u alle poorten in hetzelfde VLAN in als jumbo-enabled, of

schakelt u geen van deze jumbo-enabled-poorten in.

- De grootte van de switched virtuele interface (SVI) (VLAN-interface) wordt afzonderlijk ingesteld van de fysieke poorten MTU. Een verandering in de fysieke poorten MTU verandert de SVI MTU-grootte niet. Ook heeft een wijziging in de SVI MTU geen invloed op de fysieke poorten MTU.
- Layer 2 en Layer 3 jumbo frame-ondersteuning op FE-interfaces begonnen in Cisco IOS-softwarerelease 12.1(8a)EX01. De **mtu 1500** opdracht schakelt Jumbo op FE in en de **mtu 9216** opdracht maakt jumbo op FE in. Raadpleeg Cisco bug-ID CSCdv90450 (alleen geregistreerde klanten).
- Layer 3 jumboframes op VLAN-interfaces worden alleen ondersteund op:PFC/MSFC2 (Cisco IOS-softwarerelease 12.1(7a)E en hoger)PFC2/MSFC2 (Cisco IOS-softwarerelease 12.1(8a)E4 en hoger)
- Het wordt niet aanbevolen om jumboframes met PFC/MSFC1 voor VLAN-interfaces (SVIs) te gebruiken omdat MSFC1 mogelijk niet de fragmentatie naar wens kan verwerken.
- Geen fragmentatie wordt ondersteund voor pakketten binnen hetzelfde VLAN (Layer 2 jumbo).
- Packets die fragmentatie over VLAN's/subnetten (Layer 3 jumbo) nodig hebben worden naar software voor fragmentatie verzonden.

Ondersteuning van Jumbo-frame in Catalyst 6500/6000 Cisco IOS-software

Een jumboframe is een frame dat groter is dan het standaard Ethernet-frame. Om de ondersteuning van jumbo-frames mogelijk te maken, configureren u een groter-dan-standaard MTU-grootte op een poort of VLAN-interface en configureren u, met Cisco IOS-softwarerelease 12.1(13)E en later, de wereldwijde LAN-poort met MTU-grootte.

Geconsolideerde en Routed Traffic Size-controle in Cisco IOS-software

Lijnkaart	Ingoor	uitgang
10-, 10/100-, 100-Mbps poorten	Er wordt een groottecontrole van de MTU uitgevoerd. Ondersteuning van Jumbo-frames vergelijkt de grootte van het toegangsverkeer met de wereldwijde LAN-poort op MTU-grootte bij ingress, 10/100-, 10/100 Mbps Ethernet- en 10 GE LAN-poorten die een niet-standaard MTU-grootte hebben ingesteld. De poort laat verkeer vallen dat te groot is.	Er wordt niet gecontroleerd hoe groot de MTU is. poorten die zijn ingesteld met een niet-standaard MTU-grootte verzenden frames die pakketten bevatten van elke grootte die groter is dan 64 bytes. Als een niet-standaard MTU grootte is ingesteld, worden 10-, 10/100- en 100 Mbps Ethernet LAN-poorten niet gecontroleerd op overmaatse frames.
GE-poort	Er wordt niet gecontroleerd hoe groot	Er wordt een groottecontrole van

en	de MTU is. Poorten die zijn ingesteld met een niet standaard MTU formaat accepteren frames die elke grootte van meer dan 64 bytes bevatten en controleren niet op overmaatse ingangsframes.	de MTU uitgevoerd. Met de ondersteuning van een Jumbo-frame wordt de grootte van het buitensporige verkeer vergeleken met de grootte van de wereldwijde sterker LAN-poort met een MTU-grootte bij stap GE en 10 GE LAN-poorten die niet standaard zijn ingesteld met een MTU-grootte. De poort laat verkeer vallen dat te groot is.
10 GE-poort en	Er wordt een groottecontrole van de MTU uitgevoerd. De poort laat verkeer vallen dat te groot is.	Er wordt een groottecontrole van de MTU uitgevoerd. De poort laat verkeer vallen dat te groot is.
SVI	Er wordt niet gecontroleerd hoe groot de MTU is. De SVI controleert niet op de grootte van het frame aan de zijkant.	Er wordt een groottecontrole van de MTU uitgevoerd. De grootte van MTU wordt aan de bovenzijde van de SVI gecontroleerd.
	PFC	
Alle routeverkeer	Voor verkeer dat moet worden routeerd, vergelijkt de steun van het kader van Jumbo op de PFC verkeersgroottes met de gevormde afmetingen van de MTU en voorziet zij Layer 3 omschakeling voor jumboverkeer tussen interfaces die met afmetingen van de MTU die groot genoeg zijn om het verkeer aan te passen worden gevormd. Tussen interfaces die niet met een voldoende grootte van een MTU zijn geconfigureerd: • Als het bit Don Fragment (DF) niet is ingesteld, stuurt de PFC het verkeer naar de MSFC om gefragmenteerd en routeerd in software te zijn. • Als het PDF-bit is ingesteld, laat PFC het verkeer vallen.	

Cisco-aanbevelingen

Indien goed geïmplementeerd, kunnen jumboframes een mogelijke zesvoudige verbetering in de TCP-doorvoersnelheid van een Ethernet-verbinding bieden, met verminderde fragmentatie-

overhead (plus lagere CPU-overhead op eindapparaten).

U moet ervoor zorgen dat er geen mechanisme tussen is dat niet in staat is om de gespecificeerde grootte van MTU te verwerken. Als dit apparaat fragmenteert en de pakketten doorgeeft, vernietigt het het gehele proces. Dit kan op dit apparaat in extra overhead resulteren voor fragmentatie en het opnieuw samenvoegen van pakketten.

In dergelijke gevallen helpt de ontdekking van het IP-pad MTU zenders om de minimum gemeenschappelijke pakketlengte te vinden die geschikt is om verkeer langs elk pad te verzenden. In plaats hiervan kunt u de jumbo frame-bewuste host-apparaten configureren met een MTU-grootte die minimaal is van alle apparaten die op het netwerk worden ondersteund.

Controleer elk apparaat zorgvuldig om te zien of het de grootte van de MTU kan ondersteunen. Zie de tabel met ondersteuning van de grootte van een MTU in deze paragraaf.

Ondersteuning van Jumbo-frames kan op deze interfaces worden ingeschakeld:

- Poortkanaalinterface
- SVI
- Fysieke interface (Layer 2/Layer 3)

U kunt jumboframes inschakelen op het poortkanaal of de fysieke interfaces die deelnemen aan het poortkanaal. Het is van groot belang ervoor te zorgen dat de MTU op alle fysieke interfaces hetzelfde is. Anders kan er een geschorste interface ontstaan. Je moet de MTU van een havenkanaalinterface wijzigen omdat het de MTU van alle lidstaten verandert.

Opmerking: Als de MTU van een aangesloten haven niet kan worden gewijzigd in de nieuwe waarde omdat de aangesloten haven de blokkerende haven is, wordt het havenkanaal opgeschort.

Zorg er altijd voor dat alle fysieke interfaces in een VLAN zijn geconfigureerd voor jumboframes voordat u de ondersteuning van jumboframes op een SVI configureren. MTU van een pakje is niet ingeschakeld aan de ingangszijde van een VI. Maar het wordt wel gecontroleerd aan de bovenzijde van een VI. Als het pakket MTU groter is dan het vorige MTU, wordt het pakket door software gefragmenteerd (als het DF-bit niet is ingesteld), wat leidt tot slechte prestaties. Softwarefragmentatie gebeurt alleen voor Layer 3-switching. Wanneer een pakket naar een Layer 3 poort of een SVI met een kleinere MTU wordt doorgestuurd, komt de softwarefragmentatie voor.

MTU van een SVI moet altijd kleiner zijn dan de kleinste MTU van alle switch poorten in VLAN.

Catalyst 4500 Series-switches

Jumboframes worden voornamelijk ondersteund op de niet-blokkerende poorten van Catalyst 4500 lijnkaarten. Deze niet-blokkerende GE poorten hebben directe verbindingen met de Supervisor Engine switching fabric en ondersteunen jumboframes:

- Supervisor EngineWS-X4515, WS-X4516-2 poorten met uplinks GBIC op Supervisor Engine IV of VWS-X4516-10GE-2 10 GE uplinks en de vier 1 GE pluggable (SFP) uplinks met kleine vormfactorWS-X4013+-twee 1-GE uplinksWS-X4013+10 GE-Twee 10 GE uplinks en de vier 1 GE SFP-uplinksWS-X4013+TS-20 1-GE poorten
- LijnkaartenWS-X4306-GB—6-poorts 1000BASE-X (GBIC) GE-moduleWS-X4506-GB-T—6-poorts 10/100/1000 Mbps en 6-poorts SFPWS-X4302-GB—2-poorts 1000BASE-X (GBIC) GE-moduleDe eerste twee GBIC-poorten van een 18-poorts server-switching GE-module

(WS-X4418-GB) en GBIC-poorten van de WS-X4232-GB-RJ-module
- Switches voor vaste configuratieWS-C4948-Alle 48 1-GE poortenWS-C4948-10 GE-Alle 48 1-GE poorten en twee 10 GE poorten

U kunt deze niet-blokkerende GE poorten gebruiken om 9-KB jumboframes of hardware uitzending suppressie (alleen Supervisor Engine IV) te ondersteunen. Alle andere lijnkaarten ondersteunen babyreuzenframes. U kunt baby-reuzen gebruiken voor het overbruggen van MPLS of voor Q in Q passthrough met een maximale lading van 1552 bytes.

Opmerking: De grootte van het kader wordt verhoogd met ISL/802.1Q tags.

Baby-reuzen en jumboframes zijn transparant voor andere Cisco IOS-functies met Supervisor Engine IV en V.

Cisco IOS-softwarerelease

Functies voor basisbeveiliging

In een tijd werd er vaak over veiligheid heengekeken in campusontwerpen. Maar veiligheid is nu een essentieel onderdeel van elk ondernemingsnetwerk. Normaal gesproken heeft de klant al een beveiligingsbeleid ingesteld om te helpen definiëren welke tools en technologieën van Cisco van toepassing zijn.

Basiswachtwoordbeveiliging

De meeste Cisco IOS-softwarefuncties zijn geconfigureerd met twee wachtwoorden. Het eerste niveau is voor de toegang van het telnet tot het apparaat, dat ook bekend is als toegang van de Vty. Nadat de toegang vty is verleend, moet u toegang krijgen om modus of geprivilegieerde expressiemodus in te schakelen.

Beveiliging van de modus Inschakelen van de Switch

Met het wachtwoord activeren kunt u een gebruiker volledige toegang tot een apparaat verkrijgen. Geef het wachtwoord alleen aan vertrouwde mensen.

```
Switch(config)#enable secret password
```

Zorg ervoor dat het wachtwoord aan deze regels voldoet:

- Het wachtwoord moet tussen één en 25 hoofdletters en kleine alfanumerieke tekens bevatten.
- Het wachtwoord mag niet het eerste teken zijn.
- U kunt voorloopruimtes gebruiken, maar ze worden genegeerd. Tussenruimte en traagruimte worden herkend.
- De wachtwoordcontrole is hoofdlettergevoelig. Het wachtwoordgeheim is bijvoorbeeld anders dan het wachtwoordgeheim.

Opmerking: Schakel geheime opdracht in met een hashingfunctie van een cryptografisch bericht, Digest 5 (MD5). Als u het **tonen in werking stellen-beslist** bevel geeft, kunt u dit gecodeerde wachtwoord zien. Gebruik van de opdracht **Wachtwoord inschakelen** is een andere manier om het wachtwoord voor het inschakelen in te stellen. Maar het encryptiealgoritme dat met de opdracht

Enable password wordt gebruikt is zwak en kan eenvoudig worden omgekeerd om het wachtwoord te verkrijgen. Gebruik daarom niet de opdracht **Wachtwoord** activeren. Gebruik het **toestel** om **geheime** opdrachten te **plaatsen** voor een betere beveiliging. Raadpleeg Cisco IOS-wachtwoordencryptie voor meer informatie.

Beveiligde toegang via telnet/VTY tot de Switch

Standaard ondersteunt Cisco IOS-software vijf actieve Telnet-sessies. Deze sessies worden aangeduid als vty 0 tot 4. U kunt deze lijnen voor toegang inschakelen. Maar om inloggen mogelijk te maken, hebt u ook het wachtwoord voor deze regels nodig.

```
Switch(config)#line vty 0 4
Switch(config-line)#login
Switch(config-line)#password password
```

De inlogopdracht vormt deze lijnen voor de toegang tot telnet. De opdracht Wachtwoord vormt een wachtwoord. Zorg ervoor dat het wachtwoord aan deze regels voldoet:

- Het eerste teken kan geen getal zijn.
- De string kan alfanumerieke tekens bevatten, maximaal 80 tekens. De tekens bevatten spaties.
- U kunt het wachtwoord niet specificeren in het formaat nummer-ruimte-teken. De ruimte na het nummer veroorzaakt problemen. Hallo 21 is bijvoorbeeld een wettelijk wachtwoord, maar 21 hallo is geen wettelijk wachtwoord.
- De wachtwoordcontrole is hoofdlettergevoelig. Het wachtwoordgeheim is bijvoorbeeld anders dan het wachtwoordgeheim.

Opmerking: bij deze veelzijdige lijnconfiguratie slaat de switch het wachtwoord op in klettekst. Als iemand het **tonen in werking stellen-beslist** bevel uitgeeft, is dit wachtwoord zichtbaar. Gebruik de opdracht **Wachtwoord-encryptie voor** de **service** om deze situatie te voorkomen. De opdracht versleutelt het wachtwoord losjes. De opdracht versleutelt alleen het vty line wachtwoord en met de opdracht Wachtwoord invoeren dat is ingesteld met de opdracht **Wachtwoord** activeren. Schakel een wachtwoord in dat is ingesteld met de **optie maakt geheime** opdracht gebruik van een sterkere encryptie. De aanbevolen methode is de configuratie met de **instelling voor** een **geheim** bevel.

Opmerking: Om meer flexibiliteit in veiligheidsbeheer te hebben, zorg er dan voor dat alle Cisco IOS-softwarefuncties het verificatie-, autorisatie- en accounting (AAA) beveiligingsmodel implementeren. AAA kan lokale databases, RADIUS en TACACS+ gebruiken. Zie de sectie TACACS+ verificatie Configuration voor meer informatie.

AAA-beveiligingsservices

AAA - operationeel overzicht

Toegangsbeheer controleert wie toegang heeft tot de switch en welke diensten deze gebruikers kunnen gebruiken. AAA-netwerkbeveiligingsservices bieden het primaire kader voor het instellen van toegangscontrole op uw switch.

In dit deel worden de verschillende aspecten van AAA uitvoerig beschreven:

- Verificatie-Dit proces bevestigt de geclaimde identiteit van een eindgebruiker of een apparaat. Eerst worden de verschillende methoden gespecificeerd die kunnen worden gebruikt om de gebruiker voor authentiek te verklaren. Deze methoden definiëren het type van de uit te voeren verificatie (bijvoorbeeld TACACS+ of RADIUS). De volgorde waarin deze authenticatiemethoden moeten worden getracht, wordt ook gedefinieerd. De methoden worden vervolgens toegepast op de juiste interfaces, die de authenticatie activeren.
- Verificatie-Dit proces verleent toegangsrechten aan een gebruiker, groepen gebruikers, systeem of proces. Het AAA-proces kan een eenmalige autorisatie of autorisatie per taak uitvoeren. Het proces definieert eigenschappen (op de AAA-server) op wat de gebruiker de toestemming heeft om uit te voeren. Wanneer de gebruiker probeert een service te starten, vraagt de switch de AAA-server en vraagt hij om toestemming om de gebruiker te autoriseren. Als de AAA-server ondersteunt, is de gebruiker geautoriseerd. Als de AAA-server niet goedkeurt, krijgt de gebruiker geen toestemming om die service uit te voeren. U kunt dit proces gebruiken om aan te geven dat bepaalde gebruikers alleen bepaalde opdrachten kunnen uitvoeren.
- Accounting-Dit proces stelt u in staat om de services te volgen die gebruikers gebruiken en de hoeveelheid netwerkbronnen die de gebruikers gebruiken. Als accounting mogelijk is, rapporteert de switch gebruikersactiviteit aan de AAA server in de vorm van accounting records. Voorbeelden van gebruikersactiviteit die wordt gerapporteerd zijn de sessietijd en de begin- en stoptijd. Vervolgens kan de analyse van deze activiteit plaatsvinden voor het beheer of de facturering.

Hoewel AAA de primaire en aanbevolen methode voor toegangscontrole is, biedt Cisco IOS-software extra functies voor eenvoudige toegangscontrole die buiten het bereik van AAA vallen. Deze extra functies zijn onder meer:

- Lokale gebruikersnaam-verificatie
- Verificatie van lijnwachtwoord
- Wachtwoordverificatie inschakelen

Maar deze functies bieden niet dezelfde mate van toegangscontrole als mogelijk is met AAA.

Raadpleeg de volgende documenten voor een beter begrip van AAA:

- Verificatie, autorisatie en accounting (AAA)
- Basis AAA op een toegangsserver configureren
- Vergelijking van TACACS+ en RADIUS

In deze documenten wordt niet per se gesproken over switches. Maar de AAA-concepten die in de documenten worden beschreven, zijn van toepassing op switches.

TACACS+

doel

Standaard zijn de niet-geprivilegieerde en de geprivilegieerde wachtwoorden mondiaal. Deze wachtwoorden zijn van toepassing op elke gebruiker die toegang heeft tot de switch of router, vanaf de console poort of via een Telnet-sessie over het netwerk. De implementatie van deze wachtwoorden op netwerkapparaten is tijdrovend en niet-gecentraliseerd. U kunt ook problemen hebben met het implementeren van toegangsbeperkingen met het gebruik van toegangscontrolelijsten (ACL's) die kunnen worden blootgesteld aan configuratiefouten. Om deze problemen te overwinnen, volgt u een gecentraliseerde benadering wanneer u gebruikersnamen,

wachtwoorden en toegangsbeleid op een centrale server configureren. Deze server kan de Cisco Secure Access Control Server (ACS) of een server van derden zijn. De apparaten zijn zo geconfigureerd dat ze deze gecentraliseerde databases gebruiken voor AAA-functies. In dit geval zijn de apparaten Cisco IOS Software switches. Het protocol dat tussen de apparaten en de centrale server wordt gebruikt, kan zijn:

- TACACS+
- RADIUS
- Kerberos

TACACS+ is een gemeenschappelijke toepassing in de netwerken van Cisco en is de focus van deze sectie. TACACS+ biedt deze functies:

- Verificatie-het proces dat een gebruiker identificeert en verifieert. Er kunnen meerdere methoden worden gebruikt om een gebruiker te authentiseren. Maar de meest gebruikelijke methode is een combinatie van gebruikersnaam en wachtwoord.
- Verificatie-wanneer de gebruiker probeert een opdracht uit te voeren, kan de switch met de TACACS+ server controleren om te bepalen of de gebruiker toestemming heeft om die specifieke opdracht te gebruiken.
- Accounting-Dit proces registreert wat een gebruiker op het apparaat doet of heeft gedaan.

Raadpleeg TACACS+ en RADIUS-vergelijking voor een vergelijking tussen TACACS+ en RADIUS.

Overzicht

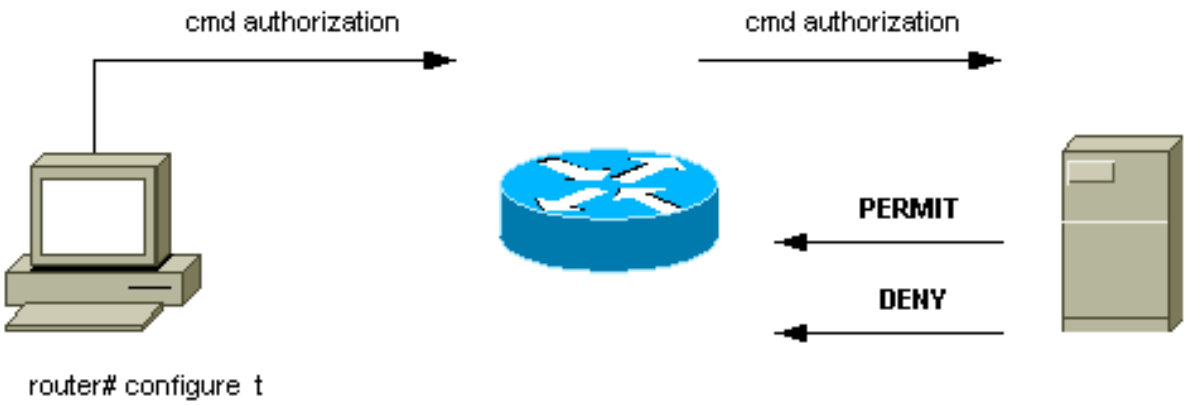
Het TACACS+ protocol stuurt gebruikersnamen en wachtwoorden naar de gecentraliseerde server door. De informatie wordt versleuteld via het netwerk met een MD5-handgreep. Raadpleeg RFC 1321 voor meer informatie. TACACS+ gebruikt TCP poort 49 als het transportprotocol dat deze voordelen ten opzichte van UDP biedt:

Opmerking: RADIUS gebruikt UDP.

- Op verbindingen gericht vervoer
- afzonderlijke erkenning dat een verzoek is ontvangen (TCP-erkenning [ACK]), ongeacht hoe geladen het back-end authenticatiemechanisme is
- Onmiddellijke indicatie van een serverongeluk (reset [RST]-pakketten)

Tijdens een sessie, als extra autorisatie nodig is, controleert de switch met TACACS+ om te bepalen of de gebruiker toestemming krijgt om een bepaalde opdracht te gebruiken. Deze stap biedt meer controle over de opdrachten die op de switch kunnen worden uitgevoerd en zorgt voor ontkoppeling van het verificatiemechanisme. Met gebruik van commando accounting kunt u de opdrachten controleren die een bepaalde gebruiker heeft afgegeven terwijl de gebruiker aan een bepaald netwerkapparaat is gekoppeld.

In dit schema is het vergunningsproces aangegeven dat van toepassing is:



Wanneer een gebruiker zich voor een netwerkapparaat bevestigt met behulp van TACACS+ in een eenvoudige ASCII-inlogpoging, gebeurt dit proces doorgaans:

- Wanneer de verbinding tot stand is gebracht, neemt de switch contact op met de TACACS+-daemon om een gebruikersnaam te verkrijgen. De switch geeft vervolgens de melding voor de gebruiker weer. De gebruiker voert een gebruikersnaam in en de switch neemt contact op met de TACACS+-naam om een wachtwoord te verkrijgen. De switch geeft de wachtwoordprompt weer voor de gebruiker, die een wachtwoord invoert dat ook naar de TACACS+-naam wordt verzonden.
- Het netwerkapparaat ontvangt uiteindelijk een van deze reacties van de TACACS+-datum:AANVAARDEN-De gebruiker is authentiek en de dienst kan beginnen. Als het netwerkapparaat is ingesteld op het moment dat u toestemming nodig hebt, begint de autorisatie.REJECT-De gebruiker is niet authentiek verklaard. De gebruiker krijgt geen toegang meer of wordt gevraagd de loginreeks opnieuw te proberen. Het resultaat is afhankelijk van de TACACS+-datum.FOUT-Een fout is op een bepaald moment tijdens verificatie opgetreden. De fout kan bij de daemon of in de netwerkverbinding tussen de daemon en de switch optreden. Als een FOUTrespons wordt ontvangen, probeert het netwerkapparaat gewoonlijk een alternatieve methode te gebruiken om de gebruiker voor de gek te houden.BLIJVEN —De gebruiker wordt gevraagd om extra informatie over de echtheidscontrole.
- Gebruikers moeten eerst de TACACS+-verificatie voltooien voordat ze naar een TACACS+-vergunning gaan.
- Indien een TACACS+-vergunning vereist is, wordt opnieuw contact opgenomen met de TACACS+-datum. De TACACS+-datum geeft een reactie op de vergunning terug of verwijst deze. Als een ACCEPT-respons wordt teruggegeven, bevat de respons gegevens in de vorm van eigenschappen die worden gebruikt om de EXEC- of NETWORK-sessie voor die gebruiker te sturen. Dit bepaalt welke opdrachten de gebruiker kan gebruiken.

Basisstappen van AAA-configuratie

De configuratie van de AAA is relatief eenvoudig nadat u het basisproces hebt begrepen. Om beveiliging op een Cisco router of toegangsserver met gebruik van AAA te configureren voert u deze stappen uit:

1. Geef de opdracht **nieuw-model** voor mondiale configuratie uit om AAA in te schakelen.
   ```
   Switch(config)#aaa new-model
   ```

Tip: Sla de configuratie op voordat u de AAA-opdrachten configureren. Sla de configuratie opnieuw op alleen nadat u al uw AAA-configuraties hebt voltooid en is tevreden dat de configuratie correct werkt. Vervolgens kunt u de switch opnieuw laden om indien nodig te herstellen van onvoorziene uitsluitingen (voordat u de configuratie opslaat).

2. Als u besluit een afzonderlijke beveiligingsserver te gebruiken, moet u security protocol parameters configureren zoals RADIUS, TACACS+ of Kerberos.
3. Gebruik de opdracht **AAA**-verificatie om de methodelijsten voor verificatie te definiëren.
4. Gebruik de opdracht **inlogverificatie** om de methodelijsten op een bepaalde interface of regel toe te passen.
5. Geef de optionele **aaa autorisatie** opdracht af om de autorisatie te configureren.
6. Geef de optionele **aaa accounting** opdracht af om accounting te configureren.
7. Configureer de externe AAA-server om de verificatie- en vergunningsaanvragen van de switch te verwerken.**Opmerking:** Raadpleeg uw AAA-serverdocumentatie voor meer informatie.

Configuratie van TACACS+ verificatie

Voer deze stappen uit om de verificatie van TACACS+ te configureren:

1. Geef de opdracht **nieuw-model uit** in de mondiale configuratiemodus om AAA in de switch mogelijk te maken.
2. Defineert de TACACS+ server en de bijbehorende sleutel.Deze toets wordt gebruikt om het verkeer tussen de TACACS+ server en de switch te versleutelen. In de opdracht **voor** de **tacacs-server host 1.1.1.1-toets** wordt de TACACS+ server geplaatst op IP-adres 1.1.1 en de encryptiesleutel is geheimzinnig. Om te verifiëren dat de switch de TACACS+ server kan bereiken, moet u een protocol van het Internet Control Message Protocol (ICMP) van de switch in werking stellen.
3. Defineert een methodelijst.Een methodelijst definieert de reeks van authenticatiemechanismen om voor verschillende diensten te proberen. De verschillende diensten zijn bijvoorbeeld:inschakelenAanmelden (voor toegang tot Vty/telnet)**N.B.:** Zie het gedeelte Basisbeveiligingsfuncties van dit document voor informatie over de toegang tot Vty/Telnet.consoleDit voorbeeld heeft alleen betrekking op **inloggen**. U moet de methodelijst op de interfaces/lijnen toepassen:

```
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group tacacs+ line
Switch(config)#line vty 0 4
Switch(config-line)#login authentication METHOD-LIST-LOGIN
Switch(config-line)#password hard_to_guess
```

In deze configuratie gebruikt de opdracht **voor** de **aanmelding van de verificatie** de naam van de lijst, METHOD-LIST-LOGIN, en gebruikt de methode tacacs++ voordat deze de methodelijn gebruikt. De gebruikers zijn geauthentiseerd met gebruik van de TACACS+ server als eerste methode. Als de TACACS+ server niet reageert of een FOUTbericht verstuurt, wordt het wachtwoord dat op de lijn is ingesteld, gebruikt als de tweede methode. Maar als de TACACS+ server de gebruiker ontkent en met een REJECT bericht reageert, beschouwt AAA de transactie als succesvol en gebruikt de tweede methode niet.**Opmerking:** de configuratie is niet voltooid voordat u de lijst (METHODE-LIST-LOGIN) op de Vty line toepast. Geef de opdracht **voor** de **aanmelding van de** authenticatiemethode-**LIST-LOGIN uit** in de regelconfiguratiemodus, zoals het voorbeeld laat zien.**Opmerking:** het voorbeeld maakt

een achterdeur voor wanneer de TACACS+ server niet beschikbaar is. De veiligheidsbeheerders kunnen of kunnen de implementatie van een achterdeur niet accepteren. Zorg ervoor dat het besluit om dergelijke achterdeuren te implementeren voldoet aan het beveiligingsbeleid van de locatie.

Configuratie van RADIUS-verificatie

De RADIUS-configuratie is vrijwel identiek aan de TACACS+-configuratie. Vervang het woord RADIUS voor TACACS in de configuratie. Dit is een voorbeeldconfiguratie van RADIUS voor COM poorttoegang:

```
Switch(config)#aaa new-model
Switch(config)#radius-server host 1.1.1.1 key mysecretkey
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group radius line
Switch(config)#line con 0
Switch(config-line)#login authentication METHOD-LIST-LOGIN
Switch(config-line)#password hard_to_guess
```

Login Banners

Maak geschikte apparaatbanners die specifiek aangeven welke acties bij onbevoegde toegang worden ondernomen. Geef de naam van de site of de netwerkinformatie niet door aan onbevoegde gebruikers. De spandoeken doen een beroep als een toestel in gevaar wordt gebracht en de dader wordt betrapt. Geef deze opdracht uit om logbanners te maken:

```
Switch(config)#banner motd ^C
*** Unauthorized Access Prohibited ***
^C
```

Fysieke beveiliging

Zorg ervoor dat een juiste toestemming noodzakelijk is om de hulpmiddelen fysiek toegankelijk te maken. Bewaar de apparatuur in een gecontroleerde (vergrendelde) ruimte. Zorg ervoor dat alle apparatuur:

- Een juiste ononderbroken voedingseenheid (UPS), met redundante bronnen waar mogelijk
- Temperatuurregeling (airconditioning)

Onthoud dat, als een persoon met kwaadwillige bedoeling fysieke toegang breekt, verstoring via wachtwoordterugwinning of andere middelen veel waarschijnlijker is.

Configuratie van beheer

Netwerkdiagrammen

doel

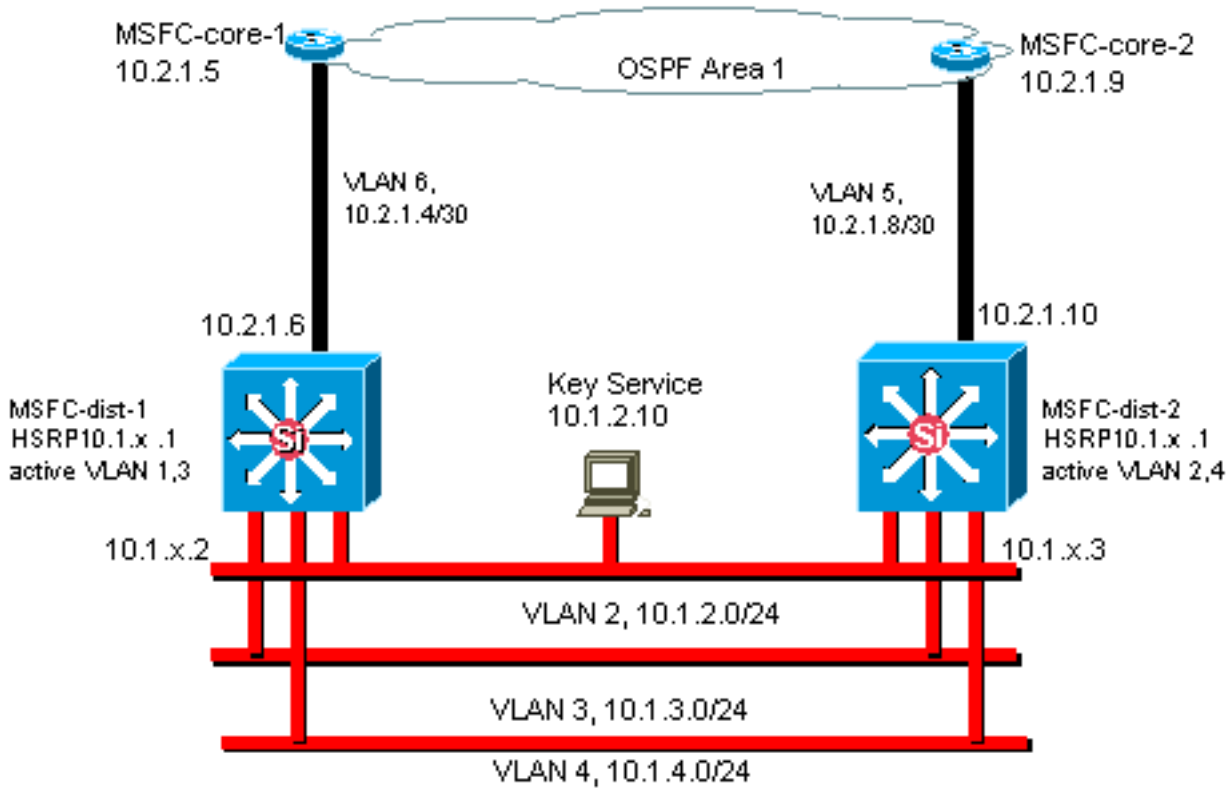
Duidelijke netwerkdiagrammen zijn een fundamenteel deel van netwerkoperaties. De diagrammen worden kritiek tijdens het oplossen van problemen, en zijn het enige belangrijkste vehikel voor het communiceren van informatie tijdens escalatie aan verkopers en partners tijdens een

stroomstoring. Onderschat de voorbereidingen, gereedheid en toegankelijkheid die netwerkdiagrammen bieden niet.

Aanbeveling

Deze drie soorten diagrammen zijn noodzakelijk:

- **Algemeen Diagram**-zelfs voor de grootste netwerken, is een diagram dat de eind-aan-eind fysieke of logische connectiviteit toont belangrijk. Vaak hebben bedrijven die elk laag afzonderlijk een hiërarchisch ontwerpdocument geïmplementeerd. Als je plannen maakt en problemen oplost, is een goede kennis van hoe de domeinen met elkaar verbinden wat er toe doet.
- **Fysiek Diagram**-Dit diagram toont alle switch en router hardware en bekabeling. Zorg ervoor dat het diagram elk van deze aspecten etiketteert:TrunkenLinksSnelhedenKanaalgroepenPoortnummersSleuvenChassis-typenSoftwareVTP-domeinenRoot-brugPrioriteit back-root-brugMAC-adresGeblokkeerde poorten per VLANVoor een betere helderheid, verf interne apparaten zoals Catalyst 6500/6000 MSFC router als router op een stok die via een boomstam is aangesloten.
- **Logisch Diagram**-Dit diagram toont slechts Layer 3 functionaliteit, wat betekent dat het routers als objecten en VLAN's als Ethernet-segmenten toont. Zorg ervoor dat het diagram deze aspecten etiketteert:IP-adressenSubnettenSecundaire adresseringHSRP actief en stand-byAccess-kerndistributielagenRouting-informatie



Switch Management-interface en Native VLAN

doel

In deze sectie worden de betekenis en mogelijke problemen van het gebruik van de standaard VLAN 1 beschreven. Deze sectie behandelt ook mogelijke problemen wanneer u beheerverkeer naar de switch in hetzelfde VLAN gebruikt als gebruikersverkeer op switches van de 6500/6000-serie.

De processors op de Supervisor Engine en MSFCs voor de Catalyst 6500/6000 Series gebruiken VLAN 1 voor een aantal controle- en beheerprotocollen. Voorbeelden zijn:

- Switch controleprotocollen:STP-BPDU’sVTPDTPCDP
- Beheerprotocollen:SNMPTelnetSecure Shell-protocol (SSH)Syslog

Wanneer het VLAN op deze manier wordt gebruikt, wordt het als het autochtone VLAN genoemd. De standaardconfiguratie van de switch stelt VLAN 1 in als de standaard autochtone VLAN op de boomstampoorten van de Catalyst. U kunt VLAN 1 als het inheemse VLAN verlaten. Maar houd in gedachten dat om het even welke switches die Cisco IOS systeemsoftware in uw netwerk lopen alle interfaces instellen die als Layer 2 switch poorten worden geconfigureerd om poorten in VLAN 1 standaard te benaderen. Waarschijnlijk gebruikt een switch ergens in het netwerk VLAN 1 als VLAN voor gebruikersverkeer.

De belangrijkste zorg met het gebruik van VLAN 1 is dat, in het algemeen, het NMP van de Supervisor Engine niet hoeft te worden onderbroken door veel van het uitzending en multicast verkeer dat eindstations genereren. Met name multicasttoepassingen hebben de neiging veel gegevens tussen servers en klanten te verzenden. De Supervisor Engine hoeft deze gegevens niet te zien. Als de middelen of buffers van de Supervisor Engine volledig bezet zijn terwijl de Supervisor Engine naar onnodig verkeer luistert, kan de Supervisor Engine niet bij beheerpakketten passen die een overspannend-boom lus of EtherChannel mislukking (in het ergste geval) kunnen veroorzaken.

De opdracht **tellers van de show interfaces** *interface_type sleuf/port* **tellers** en de **show ip verkeersopdracht kan u enige indicatie geven van:**

- Het aandeel van de uitzending in het verkeer van eenmalig gebruik
- Het aandeel van IP in niet-IP verkeer (dat niet typisch in beheer VLAN’s wordt gezien)

VLAN 1-tags en verwerkt het grootste deel van het besturingsplane-verkeer. VLAN 1 wordt standaard op alle stammen ingeschakeld. Met grotere campus netwerken, moet u voorzichtig zijn met de diameter van het VLAN 1 STP-domein. instabiliteit in één deel van het netwerk kan VLAN 1 beïnvloeden en kan de stabiliteit van het controlevliegtuig en STP stabiliteit voor alle andere VLAN's beïnvloeden. U kunt de VLAN 1-transmissie van gebruikersgegevens en de werking van STP op een interface beperken. Configureer het VLAN gewoon niet op de hoofdinterface.

Deze configuratie houdt de transmissie van besturingspakketten van switch naar switch in VLAN 1 niet tegen, zoals met een netwerkanalyzer. Maar er worden geen gegevens doorgestuurd en STP wordt niet via deze link uitgevoerd. Daarom kunt u deze techniek gebruiken om VLAN 1 te splitsen in kleinere mislukkingsdomeinen.

Opmerking: U kunt VLAN 1 niet wissen van trunks naar Catalyst 2900XL/3500XLs.

Zelfs als u voorzichtig bent om gebruiker VLANs aan relatief kleine switch domeinen en overeenkomstige klein mislukking/Layer 3 grenzen te beperken, zijn sommige klanten nog steeds in de verleiding om het beheer VLAN anders te behandelen. Deze klanten proberen het gehele netwerk met één enkel managementsubnetwerk te bedekken. Er is geen technische reden dat een centrale NMS-toepassing Layer 2-naast de apparaten moet zijn die de toepassing beheert, noch is dit een gekwalificeerd veiligheidsargument. Beperk de diameter van de beheer VLAN's aan de

zelfde routed domeinstructuur als die van gebruiker VLANs. Beschouw out-of-band beheer en/of SSH ondersteuning als een manier om de netwerkbeheerbeveiliging te verbeteren.

Andere opties

Er zijn ontwerpoverwegingen voor deze aanbevelingen van Cisco in sommige topologieën. Bijvoorbeeld, is een gewenst en gemeenschappelijk ontwerp van Cisco meerlaags één dat het gebruik van een actieve overspannende boom voorkomt. Op deze manier roept het ontwerp om de beperking van elk IP Subnet/VLAN aan één enkele switch van de toegangslaag (of cluster van switches). In deze ontwerpen kan geen trunking worden ingesteld op de toegangslaag.

Maakt u een afzonderlijk beheer VLAN en laat trunking toe om het tussen de Layer 2 toegang en Layer 3 distributielagen te dragen? Er is geen eenvoudig antwoord op deze vraag. Overweeg deze twee opties voor ontwerpreview met uw Cisco-engineer:

- **Optie 1**-Trunk twee of drie unieke VLAN's van de distributielaag tot elke switch van de toegangslaag. Deze configuratie staat voor een data-VLAN, een spraak-VLAN en een beheer-VLAN toe, en heeft nog het voordeel dat STP inactief is. Een extra configuratiestap is nodig om VLAN 1 van trunks te wissen. In deze oplossing zijn er ook ontwerppunten die in overweging moeten worden genomen om tijdelijk zwart bekleden van routeverkeer tijdens mislukkingen te voorkomen. Gebruik STP PortFast voor stammen (in de toekomst) of de automatische synchronisatie van VLAN met STP-transport.
- **Optie 2**-één VLAN voor gegevens en beheer kan aanvaardbaar zijn. Als u de sc0 interface los wilt houden van de gebruikersgegevens, maakt de nieuwere hardware van de switch dit scenario minder van een probleem dan het eens was. De nieuwere hardware biedt:Sterkere CPU's en besturingssysteembeperkingenEen ontwerp met relatief kleine uitzending domeinen zoals bepleit door het meerlaagse ontwerpOm een definitief besluit te nemen, onderzoek het uitzendverkeersprofiel voor VLAN en bespreek de mogelijkheden van de hardware van de switch met uw Cisco ingenieur. Als het beheerVLAN alle gebruikers op die switch van de toegangslaag bevat, gebruik IP-ingangsfilters om de switch van gebruikers te beveiligen, zoals in de sectie Cisco IOS-softwarebeveiliging wordt beschreven.

Cisco-beheerinterface en -native VLAN-aanbeveling

Management-interface

Cisco IOS systeemsoftware geeft u de optie om interfaces als Layer 3 interfaces of als Layer 2 switch poorten in een VLAN te configureren. Wanneer u de switchpoort-opdracht in Cisco IOS-software gebruikt, zijn alle switch-poorten standaard toegangspoorten in VLAN 1. Dus, tenzij u anders instelt, kunnen de gebruikersgegevens mogelijk ook standaard op VLAN 1 bestaan.

Maak het beheer VLAN een ander VLAN dan VLAN 1. Houd alle gebruikersgegevens uit het beheer VLAN. In plaats daarvan, vorm een loopback0 interface als beheersinterface op elke switch.

Opmerking: Als u OSPF-protocol gebruikt, wordt dit ook de OSPF-router-ID.

Verzeker dat de loopback interface een 32-bits subnetmasker heeft, en stel de loopback interface in als pure Layer 3 interface op de switch. Dit is een voorbeeld:

```
Switch(config)#interface loopback 0
Switch(config-if)#ip address 10.x.x.x 255.255.255.255
Switch(config-if)#end
Switch#
```

Native VLAN

Configureer het inheemse VLAN om een voor de hand liggende VLAN te zijn dat nooit op de router is ingeschakeld. Cisco aanbevolen VLAN 999 in het verleden, maar de keuze is puur willekeurig.

Geef deze interfaceopdrachten uit om een VLAN als inheemse (standaard) voor 802.1Q trunking op een bepaalde poort in te stellen:

```
Switch(config)#interface type slot/port
Switch(config-if)#switchport trunk native vlan 999
```

Zie het gedeelte Dynamic Trunking Protocol van dit document voor extra aanbevelingen voor de configuratie van trunking.

out-of-band beheer

doel

U kunt netwerkbeheer in hogere mate beschikbaar maken als u een afzonderlijke beheerinfrastructuur rond het productienetwerk bouwt. Deze instelling stelt apparaten in staat om extern bereikbaar te zijn, ondanks het verkeer dat wordt bestuurd of de gebeurtenissen in het bedieningspaneel die zich voordoen. Deze twee benaderingen zijn typisch:

- Out-of-band beheer met een exclusief LAN
- Out-of-band beheer met terminalservers

Overzicht

U kunt elke router en switch in het netwerk van een out-of-band Ethernet beheersinterface op een beheer VLAN voorzien. U vormt één Ethernet poort op elk apparaat in het beheer VLAN en kabelt het buiten het productienetwerk aan een afzonderlijk geschakeld beheernetwerk.

Opmerking: Catalyst 4500/4000 switches hebben een speciale me1 interface op de Supervisor Engine die alleen voor out-of-band beheer en niet als switch poort moet worden gebruikt.

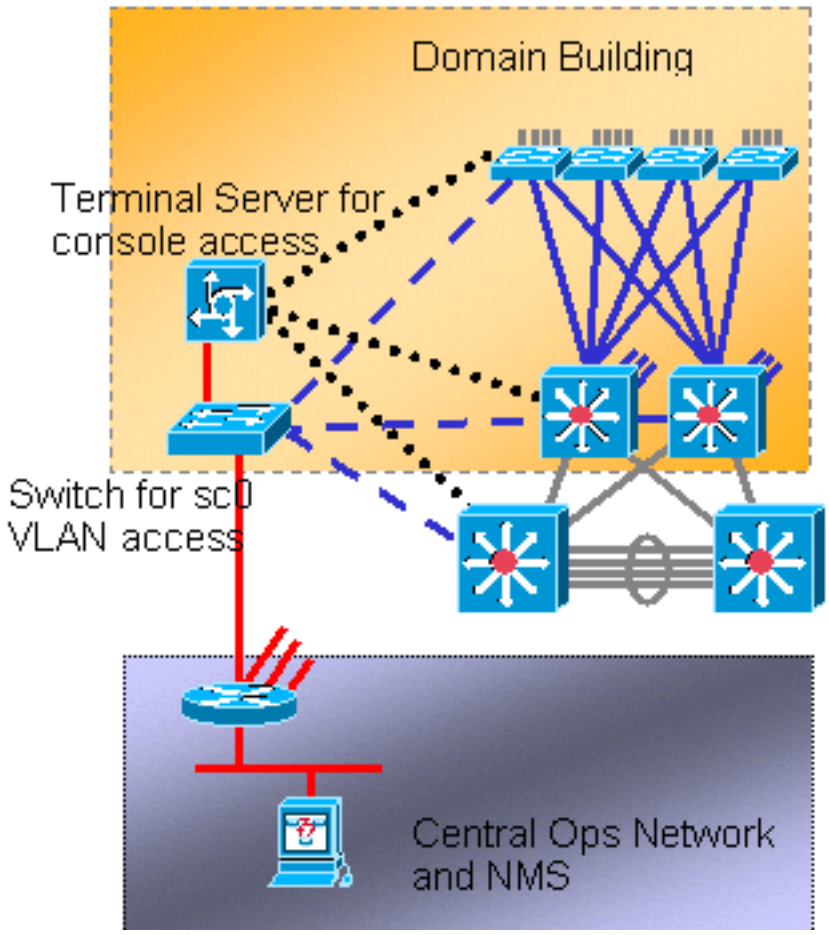
Daarnaast kunt u connectiviteit van de eindserver bereiken als u een router van Cisco 2600 of 3600 met RJ-45 seriële kabels vormt om tot de console van elke router en switch in de lay-out toegang te hebben. Het gebruik van een eindserver vermijdt ook de noodzaak om back-upscenario's te configureren, zoals modems op hulppoorten voor elk apparaat. U kunt één enkele modem op de hulphaven van de eindserver vormen. Deze configuratie biedt inbelservice voor de andere apparaten tijdens een storing van de netwerkconnectiviteit. Raadpleeg Een modem aan te sluiten op de Console-poort op Catalyst Switches voor meer informatie.

Aanbeveling

Met deze regeling, zijn twee out-of-band paden aan elke switch en router mogelijk, naast vele in-band paden. De regeling maakt een zeer beschikbaar netwerkbeheer mogelijk. De voordelen zijn:

- De indeling scheidt beheerverkeer van gebruikersgegevens.
- Het beheer-IP adres is in een afzonderlijk netto, VLAN en switch voor veiligheid.
- Er is meer zekerheid voor het leveren van beheergegevens tijdens netwerkstoringen.
- Er is geen actieve overspant boom in het beheer VLAN. Redundantie is hier niet cruciaal.

In dit schema is het out-of-band beheer opgenomen:



Vastlegging systeem

doel

Syrische berichten zijn Cisco-specifiek en kunnen meer responsieve en accurate informatie geven dan standaard SNMP. Bijvoorbeeld, beheerplatforms zoals Cisco Resource Manager Essentials (RME) en Network Analysis Toolkit (NATKit) maken krachtig gebruik van systematische informatie om inventaris en configuratieveranderingen te verzamelen.

Cisco SLOGISCHE CONFIGURATIE-AANBEVELING

Het registreren van het systeem is een gebruikelijk en geaccepteerd operationeel gebruik. Een UNIX-slang kan informatie/gebeurtenissen op de router opnemen en analyseren, zoals:

- Interfacestatus
- Beveiligingssignaleringen
- Milieuomstandigheden

- CPU-procesopslag
- Overige gebeurtenissen

Cisco IOS-software kan UNIX-vastlegging aan een UNIX-verzamelserver uitvoeren. Het Cisco UNIX-groepsformaat is compatibel met 4.3 Berkeley Standard Distribution (BSD) UNIX. Gebruik deze instellingen voor het Cisco IOS-softwarerelease:

- Standaard worden alle systeemberichten naar de systeemconsole verzonden. Console logging is een taak met hoge prioriteit in Cisco IOS-software. Deze functie was in de eerste plaats bedoeld om foutmeldingen aan de systeemexploitant te doen voordat het systeem uitvalt. Schakel console-loggen in alle apparaatconfiguraties uit om een situatie te voorkomen waarin de router/switch kan ophangen terwijl het apparaat wacht op een reactie van een terminal. Maar console berichten kunnen nuttig zijn tijdens problemen isolatie. In deze gevallen, schakelt u het registreren van console in. Geef de opdracht **houtkapconsole uit** om het gewenste niveau van berichtvastlegging te bereiken. De niveaus voor vastlegging zijn van 0 tot 7.
- **geen logmonitor**-deze opdracht schakelt het registreren voor andere eindlijnen dan de systeemconsole uit. Monitorloggen kan vereist zijn (met het gebruik van **logmonitor-debugging** of een andere opdrachtoptie). In dit geval, schakelt u de houtkap op het specifieke houtkap in dat voor de activiteit nodig is. Zie de optie **geen logconsole** in deze lijst voor meer informatie over logniveaus.
- **houtkap gebufferd 16384** — de **houtkap gebufferde** opdracht moet worden toegevoegd aan logsysteemmeldingen in de interne logbuffer. De houtbuffer is rond. Zodra de logbuffer is ingevuld, worden oudere items overschreven door nieuwere items. De grootte van de logingbuffer is gebruikersaanpasbaar en wordt in bytes gespecificeerd. De grootte van de systeembuffer varieert per platform. 16384 is een goed standaard die in de meeste gevallen voldoende houtkap biedt.
- **Meldingen in logval**—Deze opdracht biedt een waarschuwing van het (5) berichtenniveau aan de opgegeven syslogserver. Het standaard loggingniveau voor alle apparaten (console, monitor, buffer, en vallen) is het debuggen (niveau 7). Als u het niveau van de wildhoutkap op 7 laat, worden veel andere berichten geproduceerd die weinig of geen zorg voor de gezondheid van het netwerk zijn. Stel het standaardlogniveau voor vallen in op 5.
- **locale7**-Deze opdracht stelt de standaard houtkapinstallatie/niveau in voor UNIX-syslogging. Configureer de syslogserver die deze berichten voor dezelfde voorziening/niveau ontvangt.
- **loghost**-Deze opdracht stelt het IP-adres van de UNIX-logserver in.
- **bron-interface loopback 0**-Deze opdracht stelt de standaard IP SA in voor de syslog berichten. Harde code de houtkap SA om identificatie van de gastheer die het bericht verstuurde te vergemakkelijken.
- **De dienst timestamps debug van datetime localtime show-timezone msec**-By standaard, de logberichten zijn niet voorzien van een tijdstempel. U kunt deze opdracht gebruiken om timestamping van logberichten toe te staan en timestamping van systeem debug berichten te configureren. Time-stamping biedt de relatieve timing van geregistreerde gebeurtenissen en verbetert de configuratie in real-time. Deze informatie is vooral nuttig wanneer klanten het debuggen output naar uw technische ondersteuningspersoneel sturen voor hulp. Om timestamping van systeem debug boodschappen toe te laten, gebruik de opdracht in mondiale configuratiemodus. De opdracht heeft alleen een effect wanneer het debuggen is ingeschakeld.

Opmerking: Daarnaast maakt u houtkap mogelijk voor link status en gebundelde status op alle Gigabit-interfaces van de infrastructuur.

Cisco IOS-software biedt één mechanisme om de voorziening en het logniveau in te stellen voor alle systeemmeldingen die bestemd zijn voor een systeemserver. Stel het niveau van de logklem in op kennisgeving (niveau 5). Als u het niveau van de klem op kennisgeving instelt, kunt u het aantal informatieberichten minimaliseren dat aan de syslogserver wordt doorgestuurd. Deze instelling kan de hoeveelheid syslogverkeer op het netwerk aanzienlijk verminderen en kan de impact op de syslogserverbronnen beperken.

Voeg deze opdrachten toe aan elke router en switch die Cisco IOS-software uitvoeren om overseinen mogelijk te maken:

- configuratieopdrachten van Global SLOG:

```
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging host-ip
logging source-interface loopback 0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
```

- configuratieopdrachten voor de interfaceswitch:

```
logging event link-status
logging event bundle-status
```

SNMP

doel

U kunt SNMP gebruiken om statistieken, tellers, en tabellen terug te halen die in het netwerkapparaat MIBs worden opgeslagen. NMS zoals HP OpenView kunnen de informatie gebruiken om:

- Waarschuwingen in real-time genereren
- Beschikbaarheid meten
- Informatie over capaciteitsplanning produceren
- Help bij het uitvoeren van configuratie- en probleemoplossing

SNMP-beheerinterfacewerking

SNMP is een toepassing-layer protocol dat een berichtformaat voor communicatie tussen SNMP managers en agents biedt. SNMP biedt een gestandaardiseerd kader en een gemeenschappelijke taal voor de monitor en het beheer van apparaten in een netwerk.

Het SNMP-kader bestaat uit deze drie delen:

- Een SNMP-manager
- Een SNMP-agent
- A MIB

De SNMP manager is het systeem dat SNMP gebruikt om de activiteiten van netwerkhosts te controleren en te controleren. Het meest voorkomende beheersysteem wordt een NMS genoemd. U kunt de term NMS toepassen op een specifiek apparaat dat wordt gebruikt voor netwerkbeheer of de toepassingen die op een dergelijk apparaat worden gebruikt. Er zijn verschillende netwerkbeheertoepassingen beschikbaar voor gebruik met SNMP. Deze toepassingen variëren van eenvoudige CLI toepassingen tot eigenschap-rijke GUI's zoals de lijn CiscoWorks van producten.

De SNMP-agent is de softwarecomponent binnen het beheerde apparaat dat de gegevens voor het apparaat onderhoudt en deze gegevens, indien nodig, meldt aan het beheren van systemen. De agent en MIB wonen op het routeringsapparaat (de router, toegangsserver of switch). Om de SNMP agent op een Cisco routingapparaat toe te laten, moet u de verhouding tussen de manager en de agent definiëren.

De MIB is een virtueel opslaggebied voor informatie over netwerkbeheer. De MIB bestaat uit collecties van beheerde objecten. Binnen de MIB zijn er collecties van verwante objecten, gedefinieerd in MIB modules. MIB modules worden geschreven in de SNMP MIB moduletaal, zoals STD 58, RFC 2578 , RFC 2579 en RFC 2580 definiëren.

Toelichting: Individuele MIB - modules worden ook MIB's genoemd. De interfacegroep MIB (IF-MIB) is bijvoorbeeld een MIB-module binnen de MIB op uw systeem.

De SNMP-agent bevat MIB-variabelen, waarvan de waarden door de SNMP-manager kunnen worden aangevraagd of gewijzigd. Een manager kan een waarde van een agent krijgen of een waarde in die agent opslaan. De agent verzamelt gegevens van de MIB, de gegevensbank voor informatie over de parameters van het apparaat en netwerkgegevens. De agent kan ook reageren op directieverzoeken om gegevens te krijgen of in te stellen.

Een manager kan de agent verzoeken om MIB waarden te krijgen en in te stellen. De vertegenwoordiger kan op deze verzoeken reageren. Onafhankelijk van deze interactie kan de agent ongevraagde kennisgevingen (vallen of informatie) naar de beheerder sturen om de beheerder van de netwerkvoorwaarden op de hoogte te stellen. Met sommige beveiligingsmechanismen kan een NMS informatie in de MIB's `ophalen` en `volgende` verzoeken `krijgen`, en de **ingestelde** opdracht **uitgeven** om parameters te wijzigen. Daarnaast kunt u een netwerkapparaat instellen om een valbericht naar de NMS te genereren voor realtime-signaleringen. IP UDP-poort 161 en 162 wordt gebruikt voor vallen.

SNMP-meldingen - operationeel overzicht

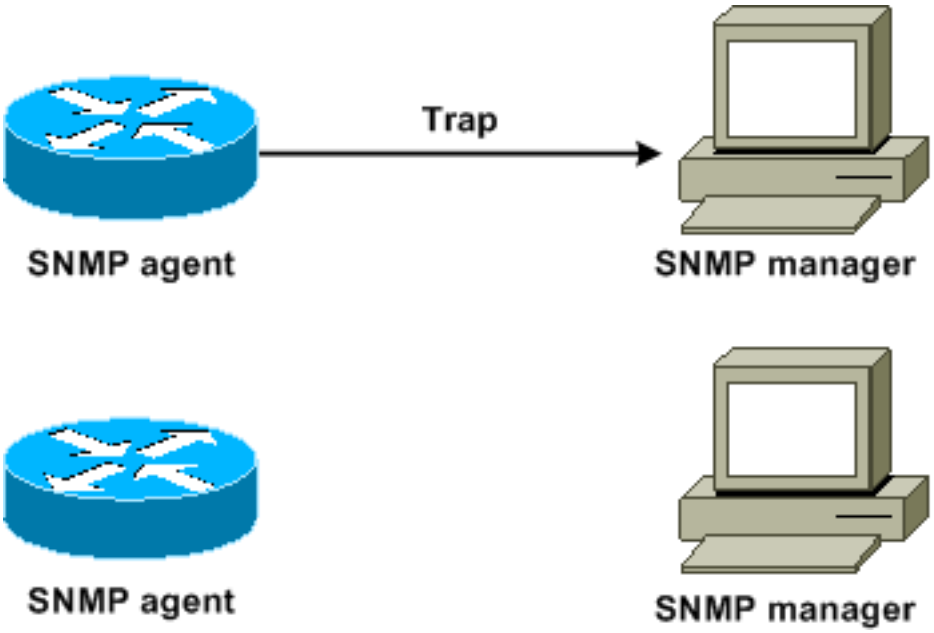
Een belangrijk kenmerk van SNMP is de mogelijkheid om kennisgevingen van een SNMP-agent te genereren. Voor deze kennisgevingen hoeven geen verzoeken van de SNMP-manager te worden verstuurd. Ongevraagde (asynchrone) kennisgevingen kunnen worden gegenereerd als vallen of als een informatieaanvraag worden ingediend. Traps zijn berichten die de SNMP-manager waarschuwen voor een conditie in het netwerk. Informatieverzoeken (informanten) zijn vallen die een verzoek om bevestiging van ontvangst van de SNMP-manager omvatten. Aanmeldingen kunnen wijzen op belangrijke gebeurtenissen zoals:

- Onjuiste gebruikersverificatie
- Herstart
- Het sluiten van een verbinding
- Het verlies van verbinding met een buurrouter
- Overige gebeurtenissen

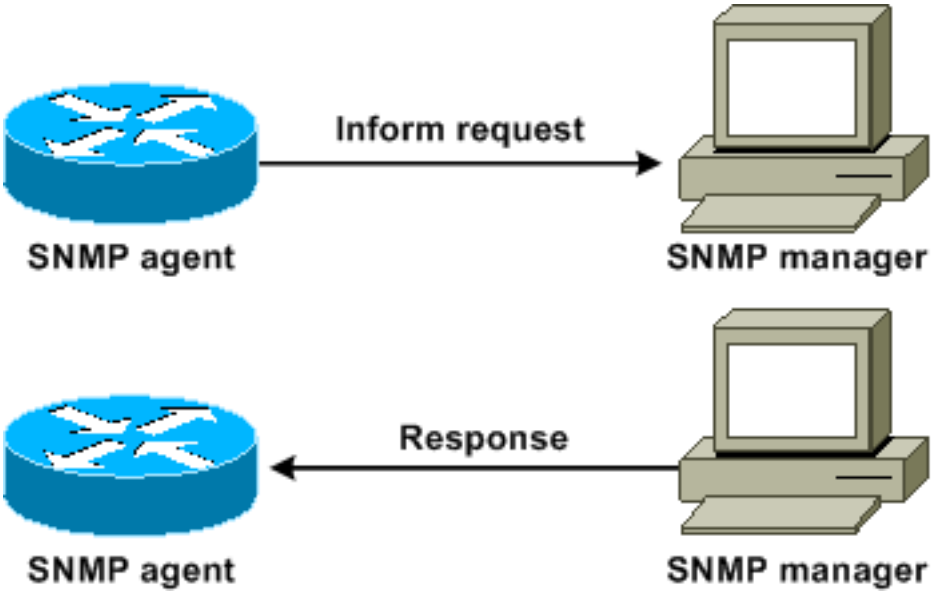
De vallen zijn minder betrouwbaar dan informanten omdat de ontvanger geen ontvangstbevestiging stuurt wanneer de ontvanger een val ontvangt. De zender kan niet bepalen of de val is ontvangen. Een SNMP-manager die een informatieve aanvraag ontvangt, erkent het bericht met een SNMP-gegevenseenheid (PDU) in het responsprotocol. Indien de manager geen informatieve aanvraag ontvangt, stuurt de manager geen antwoord. Als de afzender nooit een antwoord ontvangt, kan de afzender het informatieve verzoek opnieuw verzenden. Informaten hebben meer kans om de beoogde bestemming te bereiken.

Maar vallen hebben vaak de voorkeur omdat informanten meer middelen in de router en het netwerk gebruiken. Een val wordt weggegooid zodra het wordt verzonden. Een verzoek om informatie moet echter in herinnering worden gehouden totdat een antwoord is ontvangen of de termijn voor het indienen van verzoeken is verstreken. Verder worden vallen slechts één keer verstuurd, terwijl een informant meerdere keren kan worden herprobeerd. De herpogingen verhogen het verkeer en dragen bij aan een hogere overheadkosten op het netwerk. Dit betekent dat vallen en informatieverzoeken een ruil tussen betrouwbaarheid en middelen opleveren. Als u de SNMP manager nodig hebt om elk bericht te ontvangen, stelt het gebruik verzoeken in. Maar als u zorgen hebt over verkeer op uw netwerk of geheugen in de router en u hoeft niet elk bericht te ontvangen, gebruik dan vallen.

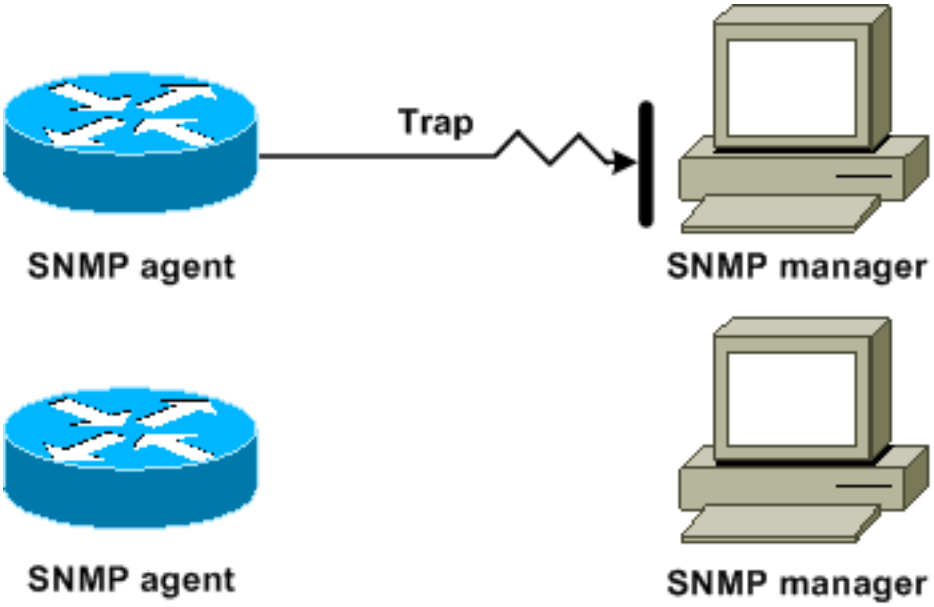
Deze diagrammen illustreren de verschillen tussen vallen en geven de volgende informatie:



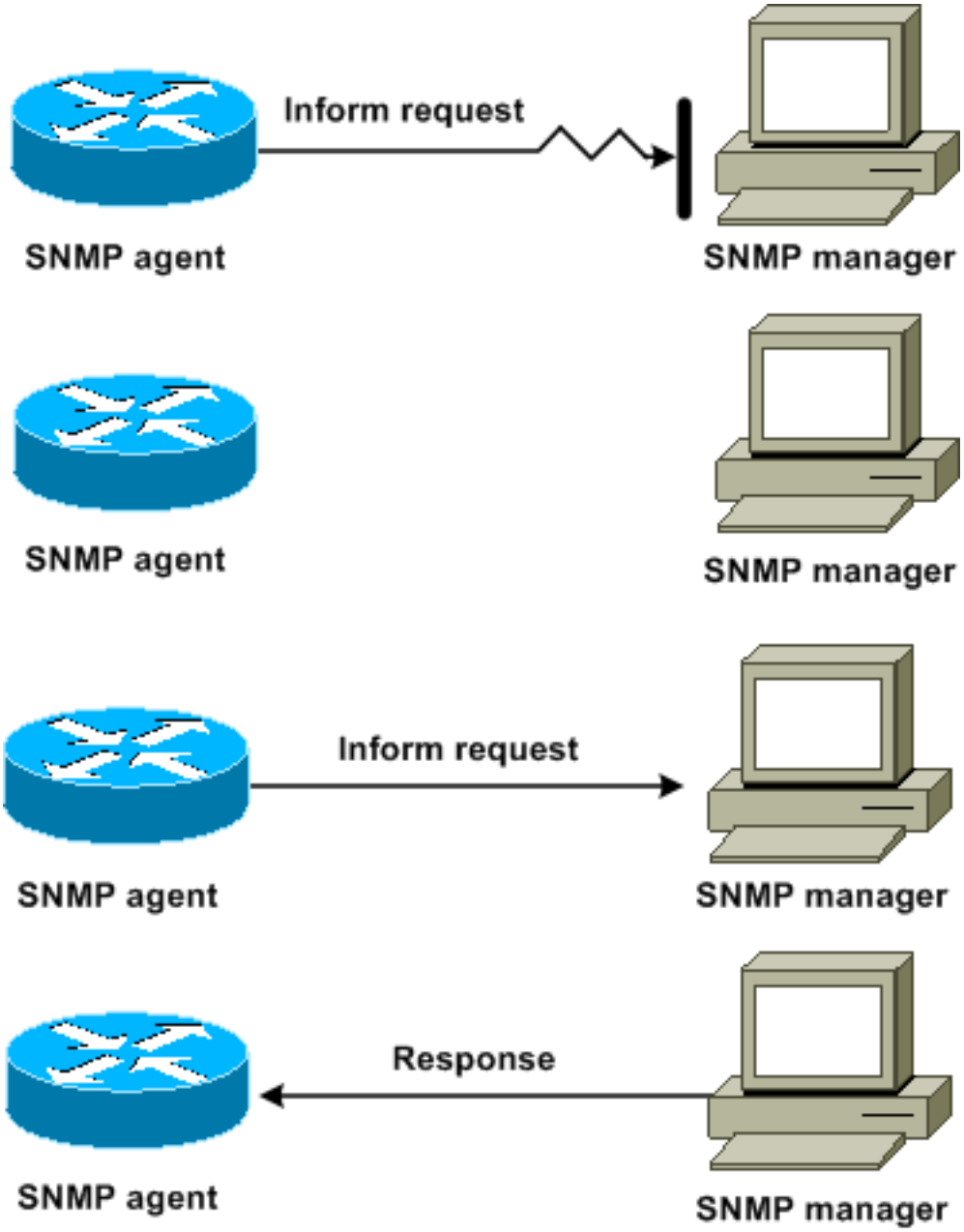
Dit diagram illustreert hoe de agent router met succes een val naar de SNMP-manager stuurt. Hoewel de beheerder de val ontvangt, stuurt de manager geen ontvangstbevestiging naar de agent. De agent weet niet of de val de bestemming heeft bereikt.



Dit diagram illustreert hoe de agent router met succes een informatief verzoek naar de manager stuurt. Wanneer de beheerder het informatieve verzoek ontvangt, stuurt de manager een antwoord naar de agent. Op deze manier weet de agent dat het informatieve verzoek de bestemming bereikte. Merk op dat er in dit voorbeeld twee keer zoveel verkeer is. Maar de agent weet dat de manager de kennisgeving heeft ontvangen.



In dit diagram stuurt de agent een val naar de manager, maar de val bereikt niet de manager. De agent kan niet weten dat de val de bestemming niet heeft bereikt, en dus wordt de val niet meer verstuurd. De manager ontvangt nooit de val.



In dit schema stuurt de agent een informatieve aanvraag naar de manager, maar de informatieve aanvraag komt niet bij de beheerder. Aangezien de manager het informatieve verzoek niet heeft ontvangen, is er geen antwoord. Na een bepaalde periode dient de vertegenwoordiger het informatieve verzoek in. De tweede keer ontvangt de beheerder het informatieve verzoek en antwoordt hij met een antwoord. In dit voorbeeld is er meer verkeer. Maar de melding bereikt de SNMP-manager.

Cisco MIB's en RFC's - referentie

RFC-documenten definiëren doorgaans MIB-modules. RFC-documenten worden voorgelegd aan de Internet Engineering Task Force (IETF), een internationale normalisatie-instelling. Individuen of groepen schrijven RFC's ter overweging door de Internet Society (ISOC) en de internetgemeenschap als geheel. Raadpleeg de homepage van de Internet Society om meer te weten te komen over het normalisatieproces en de activiteiten van de IETF. Raadpleeg de startpagina van IETF om de volledige tekst te lezen van alle RFC's, Internet Drafts (I-DS) en STD's die in Cisco-documenten worden bedoeld.

De implementatie van Cisco SNMP gebruikt:

- De definities van MIB II - variabelen die RFC 1213 beschrijft
- De definities van SNMP-vallen die RFC 1215 beschrijft

Cisco verstrekt zijn eigen privé MIB extensies met elk systeem. Cisco MIB's voor ondernemingen voldoen aan de richtlijnen die de relevante RFC's beschrijven, tenzij de documentatie anders opmerkt. U kunt de MIB de de moduledefinitiebestanden en een lijst van de MIBs vinden die op elk platform van Cisco op de homepage van Cisco MIB worden ondersteund.

SNMP-versies

Cisco IOS-software ondersteunt deze versies van SNMP:

- SNMPv1-A volledige Internet standaard die RFC 1157 definieert. RFC 1157 vervangt de eerdere versies die waren gepubliceerd als RFC 1067 en RFC 1098 . Beveiliging is gebaseerd op communautaire bepalingen.
- SNMPv2c-SNMPv2c is het op een string gebaseerde administratieve raamwerk van de gemeenschap voor SNMPv2. SNMPv2c (de c vertegenwoordigt de gemeenschap) is een experimenteel Internet protocol dat RFC 1901 , RFC 1905 , en RFC 1906 definieert. SNMPv2c is een update van de protocoloperaties en de gegevenstypen van SNMPv2p (SNMPv2 Classic). SNMPv2c gebruikt het op de gemeenschap gebaseerde veiligheidsmodel van SNMPv1.
- SNMPv3-SNMPv3 is een interoperabel op standaarden gebaseerd protocol dat RFC 2273 , RFC 2274 en RFC 2275 definieert. SNMPv3 biedt veilige toegang tot apparaten met een combinatie van authenticatie en pakketencryptie via het netwerk.De veiligheidseigenschappen die SNMPv3 verstrekt zijn:Berichtintegriteit - garandeert dat er niet met een pakket is geknoeid tijdens het transport.Verificatie-bepaalt dat het bericht uit een geldige bron afkomstig is.Versleuteling: verstopt de inhoud van een pakje, waardoor ontdekking door een niet-geautoriseerde bron wordt voorkomen.

Zowel SNMPv1 als SNMPv2c gebruiken een op de gemeenschap gebaseerde vorm van beveiliging. Een IP adres ACL en wachtwoord definiëren de gemeenschap van managers die tot de agent MIB kunnen toegang hebben.

SNMPv2c-ondersteuning omvat een bulkherkenningsmechanisme en meer gedetailleerde foutmelding aan beheerstations. Het bulkherstellingsmechanisme ondersteunt het terugvinden van tabellen en grote hoeveelheden informatie, waardoor het aantal retourvluchten dat nodig is tot een minimum wordt beperkt. De verbeterde ondersteuning van SNMPv2c voor foutenbehandeling omvat uitgebreide foutcodes die verschillende soorten foutomstandigheden onderscheiden. Deze voorwaarden worden door één enkele foutcode in SNMPv1 gerapporteerd. De foutmelding geeft nu het fouttype aan.

SNMPv3 biedt zowel beveiligingsmodellen als beveiligingsniveaus. Een beveiligingsmodel is een authenticatiestrategie die wordt opgezet voor een gebruiker en de groep waarin de gebruiker verblijft. Een veiligheidsniveau is het toegestane veiligheidsniveau binnen een beveiligingsmodel. De combinatie van een veiligheidsmodel en een veiligheidsniveau bepaalt welk beveiligingsmechanisme moet worden gebruikt wanneer een SNMP-pakket wordt verwerkt.

Algemene SNMP-configuratie

Geef deze opdrachten op alle switches van de klant uit om SNMP-beheer in staat te stellen:

- Opdracht voor SNMP ACL's:
  Switch(config)#**access-list 98 permit** *ip_address*
  !--- This is the SNMP device ACL.
- Mondiale SNMP-opdrachten:

```
!--- These are sample SNMP community strings. Switch(config)#snmp-server community RO-
community ro 98
snmp-server community RW-community rw 98
snmp-server contact Glen Rahn (Home Number)
snmp-server location text
```

SNMP-trap - aanbeveling

SNMP is de stichting voor netwerkbeheer, en wordt toegelaten en gebruikt op alle netwerken.

Een SNMP-agent kan met meerdere managers communiceren. Om deze reden, kunt u de software configureren om communicatie met één beheerstation met gebruik van SNMPv1 en een ander beheerstation met gebruik van SNMPv2 te ondersteunen. De meeste klanten en NMSs gebruiken nog steeds SNMPv1 en SNMPv2c omdat SNMPv3 netwerkapparaatondersteuning in NMS-platforms iets achterblijft.

SNMP-trap inschakelen voor alle functies die in gebruik zijn. U kunt andere functies desgewenst uitschakelen. Nadat u een val hebt ingeschakeld, kunt u de **test snmp**-opdracht uitgeven en de NMS-functie voor de fout instellen. Tot de voorbeelden van dergelijke behandelingen behoren een paginerwaakzaamheid of een pop-up.

Alle vallen zijn standaard uitgeschakeld. Schakel alle vallen op kernswitches in, zoals dit voorbeeld toont:

```
Switch(config)#snmp trap enable
Switch(config)#snmp-server trap-source loopback0
```

Schakel ook poortvallen voor belangrijke poorten in, zoals infrastructuurkoppelingen naar routers en switches en serverpoorten. Inschakelen is niet noodzakelijk voor andere havens, zoals de havens van de gastlanden. Geef deze opdracht uit om de poort te configureren en melding voor link omhoog/omlaag mogelijk te maken:

```
Switch(config-if)#snmp trap link-status
```

Specificeer vervolgens de apparatuur voor het ontvangen van de vallen en doe correct op de vallen. U kunt elke valbestemming nu configureren als een SNMPv1, SNMPv2 of SNMPv3-ontvanger. Voor SNMPv3-apparaten kunnen betrouwbare informatie worden verzonden in plaats van UDP-traps. Dit is de configuratie:

```
Switch(config)#snmp-server host ip_address [traps | informs] [version {1 | 2c | 3}] community-
string
!--- This command needs to be on one line. !--- These are sample host destinations for SNMP
traps and informs. snmp-server host 172.16.1.27 version 2c public
snmp-server host 172.16.1.111 version 1 public
snmp-server host 172.16.1.111 informs version 3 public
snmp-server host 172.16.1.33 public
```

[SNMP-stemaanbevelingen]

Zorg ervoor dat deze MIBs de belangrijkste MIBs zijn die in campusnetwerken worden ondervraagd of gecontroleerd:

Opmerking: Deze aanbeveling is afkomstig van de Cisco Network Management Consulting Group.

Object Name	Object Description	OID	Period	Max
MIB-II				
SysUpTime	system uptime in 1/100ths of seconds	1.3.6.1.2.1.1.3	5 min	< 30000
CISCO-STACK-MIB				
ChassisPs1status	Status of power supply 1	1.3.6.1.4.1.9.5.1.2.4	10 min	≠ 2
ChassisPs2Status	Status of power supply 2	1.3.6.1.4.1.9.5.1.2.7	10 min	≠ 2
ChassisFanStatus	Status of Chassis Fan	1.3.6.1.4.1.9.5.1.2.9	10 min	≠ 2
ChassisMinorAlarm	Chassis Minor Alarm Status	1.3.6.1.4.1.9.5.1.2.11	10 min	≠ 1
chassis MajorAlarm	Chassis Major Alarm Status	1.3.6.1.4.1.9.5.1.2.12	10 min	≠ 1

Object Name	Object Description	OID	Period	Max
ChassisTempAlarm	Chassis Temperature Alarm status	1.3.6.1.4.1.9.5.1.2.13	10 min	≠ 1
ModuleStatus	Operational Status of the module	1.3.6.1.4.1.9.5.1.3.1.1.10	30 min	≠ 2
CISCO-PROCESS-MIB				
CpmCPUTotal5min	The overall CPU busy percentage in the last 5 minute period. This object deprecates the avgBusy5 object from the OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.5	5 min	
CISCO-STACK-MIB				
SysTraffic	% of bandwidth utilization for the previous polling interval	1.3.6.1.4.1.9.5.1.1.8	30 min	

Object Name	Object Description	OID	Period	Max
SysTrafficPeak	Peak traffic meter value since the last time the port counters were cleared or the system started	1.3.6.1.4.1.9.5.1.1.19	30 min	
BRIDGE-MIB				
CiscoEsStackSwitchBufferOverruns	Number of times the switch was out of buffers	1.3.6.1.4.1.9.5.14.2.1.1.17	30 min	

Netwerktijdprotocol

doel

Het Network Time Protocol (NTP), RFC 1305 , synchroniseert de timing tussen een reeks gedistribueerde tijdservers en klanten. NTP maakt het mogelijk de correlatie tussen gebeurtenissen bij het maken van systeemlogbestanden te bepalen en wanneer andere tijdspecifieke gebeurtenissen zich voordoen.

Overzicht

RFC 958 gedocumenteerde NTP eerst. Maar NTP is geëvolueerd via RFC 1119 (NTP versie 2). RFC 1305 definieert nu NTP, wat in de derde versie ervan staat.

NTP synchroniseert de tijd van een computerclient of server naar een andere server of referentie tijdbron, zoals een radio, satellietontvanger of modem. NTP biedt een clientnauwkeurigheid die normaal gesproken binnen een ms op LAN's en tot een paar tientallen ms op WAN's, in vergelijking met een gesynchroniseerde primaire server. U kunt bijvoorbeeld NTP gebruiken om gecoördineerde Universal Time (UTC) te coördineren via een GPS-ontvanger (global positioning Service).

Typische NTP-configuraties gebruiken meerdere redundante servers en diverse netwerkpaden om een hoge nauwkeurigheid en betrouwbaarheid te bereiken. Sommige configuraties omvatten cryptografische authenticatie om accidentele of kwaadaardige protocolaanvallen te voorkomen.

NTP loopt over de UDP, die op zijn beurt over IP loopt. Alle NTP-communicatie gebruikt UTC, wat hetzelfde is als Greenwich Mean Time.

Momenteel zijn er NTP versie 3 (NTPv3) en NTP versie 4 (NTPv4) implementaties beschikbaar.

De meest recente softwarerelease waaraan wordt gewerkt is NTPv4, maar de officiële Internet-standaard is nog NTPv3. Daarnaast passen sommige besturingssysteemverkopers de implementatie van het protocol aan.

NTP-vrijwaringsmaatregelen

NTP-implementatie probeert ook synchronisatie naar een machine te vermijden waarbij de tijd onmogelijk nauwkeurig kan zijn. NTP doet dit op twee manieren:

- NTP synchroniseert niet naar een machine die niet gesynchroniseerd is.
- NTP vergelijkt altijd de tijd die door meerdere machines wordt gerapporteerd, en synchroniseert niet aan een machine waarop de tijd aanzienlijk anders is dan de andere, zelfs als die machine een lager stratum heeft.

Associaties

De communicatie tussen machines die NTP uitvoeren, die bekend staan als associaties, wordt gewoonlijk statistisch geconfigureerd. Elke machine krijgt de IP-adressen van alle machines waarmee ze associaties moet vormen. Een nauwkeurige tijdsbepaling is mogelijk door de uitwisseling van NTP - berichten tussen elk paar machines met een associatie. Maar in een LAN omgeving, kunt u NTP configureren om IP-uitzendingen te gebruiken. Met dit alternatief kunt u de machine configureren om uitgezonden berichten te verzenden of ontvangen, maar de nauwkeurigheid van het bewaren van de tijd wordt marginaal beperkt omdat de informatiestroom maar één kant op gaat.

Als het netwerk geïsoleerd is van het Internet, staat de implementatie van Cisco NTP u toe om een machine te vormen zodat het handelt alsof het met het gebruik van NTP gesynchroniseerd is, wanneer het de tijd met het gebruik van andere methodes eigenlijk heeft bepaald. Andere machines synchroniseren met die machine met NTP.

Een NTP-vereniging kan zijn:

- Een peer associationDit betekent dat dit systeem ofwel kan synchroniseren met het andere systeem of het andere systeem kan laten synchroniseren.
- Een serverassociatieDit betekent dat alleen dit systeem tegelijkertijd met het andere systeem verloopt. Het andere systeem synchroniseert niet met dit systeem.

Als u een NTP-associatie met een ander systeem wilt vormen, gebruikt u een van deze opdrachten in de wereldwijde configuratie-modus:

Opdracht	doel
ntp peer *ip-adres* [normaal-sync] [*versienummer*] [key *key-id*] [bron *interface*] [preferent]	Vormt een peer associatie met een ander systeem
IP-*adres van de* NTP-server [*versienummer*] [key *key-id*] [*source interface*] [preferent]	Vormt een serverassociatie met een ander systeem

Opmerking: er hoeft slechts één uiteinde van een associatie te zijn ingesteld. Het andere systeem stelt automatisch de associatie vast.

Toegang tot openbare tijdservers

NTP-net omvat momenteel meer dan 50 openbare primaire servers die rechtstreeks zijn gesynchroniseerd met UTC via radio, satelliet of modem. Normaal gesproken zijn werkstations en servers met een relatief klein aantal klanten niet synchroon met primaire servers. Er zijn ongeveer 100 openbare secundaire servers die gesynchroniseerd zijn op de primaire servers. Deze servers bieden synchronisatie aan een totaal van meer dan 100.000 klanten en servers op het internet. De pagina Openbare NTP-servers onderhoudt de huidige lijsten en wordt regelmatig bijgewerkt.

Bovendien zijn er talrijke particuliere primaire en secundaire servers die normaal niet voor het publiek beschikbaar zijn. Raadpleeg het Network Time Protocol Project (University of Delaware) voor een lijst met openbare NTP-servers en informatie over het gebruik ervan. Er is geen garantie dat deze openbare internet NTP-servers beschikbaar zijn en de juiste tijd produceren. Daarom moet u andere opties overwegen. Gebruik bijvoorbeeld verschillende standalone GPS-apparaten die rechtstreeks zijn aangesloten op een aantal routers.

Een andere optie is het gebruik van verschillende routers, ingesteld als Stratum 1 master. Maar het gebruik van zo'n router wordt niet aanbevolen.

Stratum

NTP gebruikt een stratum om het aantal NTP-uiteinden te beschrijven dat een machine van een gezaghebbende tijdbron verwijderd is. Een stratum 1-tijdserver heeft een radio- of atomaire kloktijd die direct is aangesloten. Een stratum 2 time server ontvangt zijn tijd van een stratum 1 time server, enzovoort. Een machine die NTP in werking stelt, kiest automatisch als tijdbron de machine met het laagste stratumnummer waarmee deze wordt ingesteld om door NTP te communiceren. Deze strategie bouwt in feite een zelf-organiserende boom van sprekers van NTP.

NTP vermijdt synchronisatie op een apparaat waar de tijd mogelijk niet nauwkeurig is. Zie het gedeelte *NTP*-waarborgen van het Network Time Protocol voor meer informatie.

Relatie tussen servers

- Een server reageert op clientverzoeken maar probeert geen datuminformatie uit een clientbron op te nemen.
- Een peer reageert op verzoeken van cliënten en probeert het verzoek van de cliënt te gebruiken als potentiële kandidaat voor een betere tijdbron en om de klokfrequentie ervan te stabiliseren.
- Om echte peers te zijn moeten beide kanten van de verbinding in een peer relatie treden, in plaats van een situatie waarin een gebruiker fungeert als peer en de andere gebruiker fungeert als server. Laat peers sleutels uitwisselen zodat alleen vertrouwde gastheren als gelijken met anderen kunnen praten.
- In een client verzoek aan een server, beantwoordt de server de client en vergeet dat de client een vraag stelde.
- In een client verzoek aan een peer, beantwoordt de server de client. De server houdt staatsinformatie over de cliënt bij om te volgen hoe goed de cliënt op tijd doet en welke stratumserver de client runt.

Een NTP server kan vele duizenden cliënten zonder probleem behandelen. Maar wanneer een NTP-server meer dan een paar klanten (tot een paar honderd) verwerkt, is er een geheugenimpact op de server mogelijkheid om staatsinformatie te behouden. Wanneer een NTP-server meer dan de aanbevolen hoeveelheid verwerkt, worden er meer CPU-bronnen en bandbreedte in het vak verbruikt.

Communicatiemodi met de NTP-server

Dit zijn twee afzonderlijke modi om met de server te communiceren:

- Breedbandmodus
- Clientmodus/servermodus

In de uitzendmodus luisteren de klanten. In client/server modus, poll de server. U kunt NTP-uitzending gebruiken als er geen WAN-link is betrokken vanwege de snelheid. Gebruik de client/server-modus (door opiniepeilingen) om over een WAN-link te gaan. De breedbandmodus is ontworpen voor een netwerk, waarin veel clients mogelijk de server moeten inroepen. Zonder uitzendmodus kan zulk opiniepeiling mogelijk een groot aantal pakketten op het netwerk genereren. NTP multicast is nog niet beschikbaar in NTPv3, maar is beschikbaar in NTPv4.

Standaard communiceert Cisco IOS-software met het gebruik van NTPv3. Maar de software is omgekeerd compatibel met eerdere versies van NTP.

Verkiezingen

Het NTP protocol staat een client toe om een server op elk moment te vragen.

Wanneer u voor het eerst NTP in een vakje van Cisco vormt, stuurt NTP acht vragen in snelle opeenvolging met tussenpozen `NTP_MINPOLL` (2^4=16 sec). De `NTP_MAXPOLL` is 2^14 seconden (16,384 seconden of 4 uur, 33 min., 4 seconden). Deze periode is de langste periode vóór de NTP - opiniepeilingen voor een respons. Op dit moment heeft Cisco geen methode om de gebruiker toe te staan de `POLL`-tijd handmatig te forceren.

De NTP-stemlokatie begint bij 2^6 (64) sec, of 1 min., 4 seconden. Deze tijd wordt verhoogd door krachten van 2, aangezien de twee servers met elkaar synchroniseren, tot 2^10. U kunt verwachten dat de sync-berichten met een interval van 64, 128, 256, 512, of 1024 seconden worden verzonden, zoals per server of peer configuratie. De langere tijd tussen de peilingen komt voor omdat de huidige klok stabieler wordt vanwege de fasevergrendelde rijen. De fase-vergrendelde lijnen maken de lokale kloktijd kristal tot 1024 seconden (17 min.) af.

De tijd varieert tussen 64 seconden en 1024 seconden als een vermogen van 2 (dat gelijk is aan elke 64, 128, 256, 512 of 1024 seconden). De tijd is gebaseerd op de fase-vergrendelde lus die pakketten verstuurt en ontvangt. Als er in die tijd veel kritiek is, vindt er vaker opiniepeiling plaats. Als de referentieklok nauwkeurig is en de netwerkconnectiviteit consistent is, converteren de poll-tijden tussen elke poll op 1024 seconden.

Het NTP poll interval verandert als de verbinding tussen de client en server verandert. Met een betere verbinding is het poll-interval langer. In dit geval betekent een betere verbinding dat de NTP-cliënt acht reacties heeft ontvangen voor de laatste acht verzoeken. Het poll-interval is dan verdubbeld. Een enkele gemiste reactie zorgt ervoor dat het poll interval met de helft wordt verminderd. Het poll-interval begint bij 64 seconden en duurt tot maximaal 1024 seconden. In de beste omstandigheden is de tijd die nodig is voor het poll-interval van 64 seconden tot 1024 seconden iets meer dan 2 uur.

Uitzending

NTP-uitzendingen worden nooit doorgestuurd. Als u de opdracht **ntp-uitzending** geeft, begint de router NTP-uitzendingen te genereren op de interface waarop deze is geconfigureerd.

Meestal geeft u de opdracht **ntp-uitzending uit** om NTP-uitzendingen naar een LAN te verzenden om de client-eindstations en -servers te kunnen bedienen.

Tijdsynchroniseren

Synchronisatie van een client naar een server bestaat uit meerdere pakketuitwisselingen. Elke uitwisseling is een verzoek/antwoordpaar. Wanneer een client een verzoek verstuurt, slaat de client de lokale tijd op in het verzonden pakket. Wanneer een server het pakket ontvangt, slaat het zijn eigen schatting van de huidige tijd in het pakket op en wordt het pakket teruggegeven. Wanneer het antwoord is ontvangen, logt de ontvanger opnieuw zijn eigen ontvangsttijd in om de reistijd van het pakket te schatten.

Deze tijdverschillen kunnen worden gebruikt om de tijd in te schatten die nodig was voor het pakket om van de server naar de aanvrager te verzenden. Voor een raming van de huidige tijd wordt rekening gehouden met die reistijd. Hoe korter de reistijd is, des te preciezer is de schatting van de huidige tijd.

De tijd wordt pas geaccepteerd als er verschillende pakketuitwisselingen zijn overeengekomen. Sommige essentiële waarden worden in meerfasefilters gezet om de kwaliteit van de monsters te schatten. Gewoonlijk zijn ongeveer 5 minuten nodig voor een NTP-client om te synchroniseren naar een server. Interessant genoeg geldt dit ook voor lokale referentieklokken die per definitie geen vertraging hebben.

Bovendien beïnvloedt de kwaliteit van de netwerkverbinding ook de uiteindelijke nauwkeurigheid. Lage en onvoorspelbare netwerken met verschillende vertragingen hebben een slecht effect op de tijdsynchronisatie.

Er is een tijdverschil van minder dan 128 ms vereist om NTP te kunnen synchroniseren. De typische nauwkeurigheid op het internet varieert van ongeveer 5 ms tot 100 ms, wat kan variëren met netwerkvertragingen.

NTP-verkeersniveaus

De bandbreedte die NTP gebruikt is minimaal. Het interval tussen opiniepeilingen die peers ruilen gaat meestal terug naar slechts één bericht per 17 min (1024 sec). Met zorgvuldige planning kunt u dit binnen routernetwerken behouden via de WAN-koppelingen. Zorg dat de NTP-klanten peer tot lokale NTP-servers en niet volledig over WAN naar de centrale-site kernrouters, dat zijn de Stratum 2-servers.

Een geconvergeerde NTP-client gebruikt ongeveer 0,6 bits per seconde (bps) gemiddelden per server.

Cisco NTP-aanbeveling

- Cisco raadt u aan meerdere tijdservers en verschillende netwerkpaden te gebruiken om een hoge nauwkeurigheid en betrouwbaarheid te bereiken. Sommige configuraties omvatten cryptografische authenticatie om accidentele of kwaadaardige protocolaanvallen te voorkomen.
- Volgens de RFC is NTP echt ontworpen om u in staat te stellen om verschillende tijdservers te kiezen en gecompliceerde statistische analyses te gebruiken om een geldige tijd te bedenken, zelfs als u niet zeker weet dat alle servers die u instelt, gezaghebbend zijn. NTP

schat de fouten van alle klokken. Daarom geven alle NTP-servers de tijd terug samen met een schatting van de huidige fout. Wanneer u meerdere tijdservers gebruikt, wil NTP ook dat deze servers het eens worden over enige tijd.

- De Cisco-implementatie van NTP ondersteunt stratum 1-service niet. U kunt geen verbinding maken met een radio- of atoomklok. Cisco raadt aan de tijdservice voor uw netwerk te afgeleid zijn van de openbare NTP-servers die op het IP-internet beschikbaar zijn.
- Schakel alle client-switches in om dagverzoeken regelmatig naar een NTP-server te verzenden. U kunt maximaal 10 server/peer adressen per client configureren zodat u een snelle synchronisatie kunt realiseren.
- Om de protocoloverhead te verminderen, verdelen de secundaire servers tijd via NTP aan de resterende lokale nethosts. In het belang van de betrouwbaarheid kunt u geselecteerde hosts voorzien van minder nauwkeurige maar minder dure klokken die u voor back-up kunt gebruiken in het geval van een storing van de primaire en/of secundaire servers of van het communicatiepad tussen deze servers.
- **NTP update-kalender**-NTP verandert gewoonlijk slechts de systeemklok. Met deze opdracht kan NTP de datum-/tijdinformatie op de kalender bijwerken. De update wordt uitsluitend uitgevoerd als de NTP-tijd gesynchroniseerd is. Anders behoudt de kalender zijn eigen tijd en wordt hij niet beïnvloed door de tijd of de systeemklok van het NTP. Gebruik dit altijd op de high-end routers.
- **Klokkalender-geldig**-Deze opdracht verklaart dat de kalenderinformatie geldig en gesynchroniseerd is. Gebruik deze optie op de NTP-master. Als dit niet wordt geconfigureerd, denkt de hoge-end router die de kalender heeft nog steeds dat de tijd ongezaghebbend is, zelfs als deze de NTP-hoofdlijn heeft.
- Elk stratumnummer dat meer dan 15 is, wordt als niet-gesynchroniseerd beschouwd. Dit is waarom u stratum 16 in de uitvoer van de opdracht ntp **status** van de **show** ziet op routers waarvoor de klokken niet gesynchroniseerd zijn. Als de master gesynchroniseerd is met een openbare NTP-server, zorg er dan voor dat het stratumnummer op de NTP-hoofdlijn één of twee hoger is dan het hoogste stratumnummer op de openbare servers die u instelt.
- Veel klanten hebben NTP ingesteld in servermodus op hun Cisco IOS-softwareplatforms, gesynchroniseerd vanaf verschillende betrouwbare feeds van het internet of een radiokloket. Intern, een eenvoudiger alternatief voor servermodus wanneer u een groot aantal switches in werking stelt is NTP in omroepmodus op het beheer VLAN in een geschakeld domein in te schakelen. Dit mechanisme staat de Catalyst toe om een klok van één uitzending te ontvangen. Maar de nauwkeurigheid van het bewaren van de tijd is marginaal verminderd omdat de informatiestroom eenrichtingsverkeer is.
- Het gebruik van loopback adressen als bron van updates kan ook helpen met consistentie. U kunt problemen op het gebied van beveiliging op twee manieren aanpakken:Met de controle van serverupdates, die Cisco raadtDoor authenticatie

NTP-opdrachten voor wereldwijde configuratie

```
!--- For the client: clock timezone EST  -5  ????
ntp source loopback 0 ?????
ntp server ip_address key 1
ntp peer ip_address
!--- This is for a peer association. ntp authenticate
ntp authentication-key 1 md5 xxxx
ntp trusted-key 1
```

```
!--- For the server: clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ntp source loopback0
ntp update-calendar

!--- This is optional: interface vlan_id ntp broadcast
!--- This sends NTP broadcast packets. ntp broadcast client
!--- This receives NTP broadcast packets. ntp authenticate
ntp authentication-key 1 md5 xxxxx
ntp trusted-key 1
ntp access-group access-list
!--- This provides further security, if needed.
```

NTP-statusopdracht

```
show ntp status

Clock is synchronized, stratum 8, reference is 127.127.7.1
nominal freq is 250.0000 Hz, actual freq is 249.9974 Hz, precision is 2**18
reference time is C6CF0C30.980CCA9D (01:34:00.593 IST Mon Sep 12 2005)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec
```

Dit is het referentieklokadres voor de Cisco-router wanneer de router als NTP-master fungeert. Als de router niet met een NTP-server is gesynchroniseerd, gebruikt de router dit adres als referentie-ID. Raadpleeg voor meer informatie over de configuratie en opdrachten het gedeelte *NTP-configureren* van het basissysteembeheer.

Cisco-detectieprotocol

doel

CDP loopt over Layer 2 (datalink-laag) op alle Cisco routers, bruggen, toegangsservers en switches. CDP laat netwerkbeheertoepassingen toe om apparaten van Cisco te ontdekken die buren van reeds bekende apparaten zijn. In het bijzonder kunnen de netwerkbeheertoepassingen buren ontdekken die laag transparante protocollen runnen. Met CDP kunnen de netwerkbeheertoepassingen het apparaattype en het SNMP-agent-adres van naburige apparaten leren. Deze optie stelt toepassingen in staat om SNMP vragen naar aangrenzende apparaten te verzenden.

De opdrachten **tonen** die met de CDP-functie zijn gekoppeld, stellen de netwerkingenieur in staat deze informatie te bepalen:

- Het module/poortnummer van andere, aangrenzende CDP-enabled-apparaten
- Deze adressen van het aangrenzende apparaat:MAC-adresIP-adresPoortkanaaladres
- De aangrenzende softwareversie van het apparaat
- Deze informatie over het aangrenzende apparaat:SpeedDuplexVTP-domeinInstelling Native VLAN

Het gedeelte Operationeel Overzicht benadrukt een aantal van de verbeteringen van CDP versie 2 (CDPv2) via CDP versie 1 (CDPv1).

Overzicht

CDP wordt uitgevoerd op alle LAN- en WAN-media die SNAP ondersteunen.

Elk door CDP ingesteld apparaat stuurt periodieke berichten naar een multicast adres. Elk apparaat adverteert minstens één adres waar het apparaat SNMP berichten kan ontvangen. De advertenties bevatten ook de tijd om de informatie te bewaren of te behouden. Deze informatie geeft de tijdsduur aan waarop een ontvangende machine CDP-informatie moet bewaren voordat deze wordt weggegooid.

CDP gebruikt SNAP-insluiting met type code 2000. Op Ethernet, ATM en FDDI, wordt het bestemming multicast adres 10-00-0c-cc-cc-cc gebruikt. Op Token Rings wordt het functionele adres c000.0800.000 gebruikt. CDP-frames worden elke minuut periodiek verzonden.

CDP-berichten bevatten een of meer berichten waarmee het doelapparaat informatie over elk buurapparaat kan verzamelen en opslaan.

Deze tabel bevat de parameters die CDPv1 ondersteunt:

Parameter	Type	Beschrijving
1	ApparaatID	Host name van het apparaat of het hardware-serienummer in ASCII
2	Adres	Layer 3 adres van de interface die de update stuurt
3	PoortID	De poort waarop de CDP-update wordt verzonden
4	Capaciteit	Beschrijft de functies van het apparaat: • router: 0x01 • SR[1]-brug: 0x04 • Switch: 0x08 (biedt Layer 2 en/of Layer 3 switching) • Host: 0x10 • IGMP voorwaardelijk filteren: 0x20 • Bridge of switch DOORSTUREN IGMP-rapportpakketten niet op routerpoorten.
5	Versie	Een tekenstring die de softwareversie bevat **Opmerking:** de opdrachtoutput van de **show versie** toont dezelfde informatie.
6	platform	Het hardwareplatform, bijvoorbeeld WS-C5000, WS-C6009 en Cisco RSP[2]

[1] SR = bronroute.

[2] RSP = RSP-Switch-processor.

In CDPv2 zijn een extra type, lengte, waarden (TLV's) geïntroduceerd. CDPv2 ondersteunt elke TLV. Maar deze tabel biedt de parameters die bijzonder nuttig kunnen zijn in geschakelde omgevingen en die Catalyst software gebruikt.

Wanneer een switch CDPv1 draait, laat de switch CDPv2-frames vallen. Wanneer een switch CDPv2 draait en een CDPv1 frame op een interface ontvangt, begint de switch CDPv1-frames uit die interface te verzenden, naast CDPv2-frames.

Parameter	Type	Beschrijving
9	VTP-domein	Het VTP-domein, als dit op het apparaat is ingesteld
10	Native VLAN	In punt1q, blijven de frames voor het VLAN, waar de haven in is als de haven niet trunking is, untagged. Dit wordt gewoonlijk aangeduid als het inheemse VLAN.
11	Full/Half-Duplex	Dit TLV bevat de duplexinstelling van de verzendende poort.
14	Applicatie VLAN-ID	Hiermee kan het VoIP-verkeer worden gedifferentieerd van ander verkeer door middel van een afzonderlijke VLAN-id (hulpVLAN).
16	Stroomverbruik	De maximale hoeveelheid vermogen die naar verwachting door het aangesloten apparaat in mW zal worden verbruikt.
17	MTU	De MTU van de interface waarmee het CDP-frame wordt doorgegeven.
18	Uitgebreid vertrouwen	Geeft aan dat de poort in Extended Trust mode is.
19	COS voor onvertrouwde poorten	De waarde van de klasse van de dienst (CoS) die moet worden gebruikt om alle pakketten te markeren die op de onvertrouwde poort van een aangesloten switchapparaat worden ontvangen.
20	SysName	Volledig gekwalificeerde domeinnaam van het apparaat (0, indien onbekend).
25	Vereiste voeding	Zend door een aandrijfsysteem om te onderhandelen over een geschikt vermogensniveau.
26	Beschikbaar	Door een switch verzonden. Hiermee kan worden onderhandeld en kan een geschikte stroominstelling worden geselecteerd.

CDPv2/Power over Ethernet

Sommige switches, zoals Catalyst 6500/6000 en 4500/4000, hebben de mogelijkheid om stroom via onafgeschermde getwiste paarkabels (UTP) aan voedbare apparaten te leveren. Informatie die wordt ontvangen via CDP (parameters 16, 25, 26) helpt bij de optimalisering van het energiebeheer van switches.

Interactie CDPv2/Cisco IP-telefoon

Cisco IP-telefoons bieden connectiviteit voor een extern aangesloten 10/100 Mbps Ethernet-apparaat. Deze connectiviteit wordt bereikt door de integratie van een interne drie-poorts Layer 2 switch binnen de IP telefoon. De binnenhavens van de switch worden aangeduid als:

- P0 (intern IP-telefoonapparaat)
- P1 (externe 10/100 Mbps poort)
- P2 (externe 10/100 Mbps poort die wordt aangesloten op de switch)

U kunt spraakverkeer op een afzonderlijk VLAN op de poort van de switch overbrengen als u de dot1q toegangshavens vormt. Dit extra VLAN is gekend als de hulp (CatOS) of spraak (Cisco IOS Software) VLAN. Dientengevolge, kan het punt1q gelabeld verkeer van de IP telefoon op de hulp/stem VLAN worden verzonden, en untagged verkeer kan via de externe 10/100-Mbps haven van de telefoon via het toegangsVLAN worden verzonden.

Catalyst switches kunnen een IP-telefoon van spraak VLAN-id via CDP (Parameter-14: applicatie VLAN-ID (TLV). Als resultaat hiervan worden alle VoIP-pakketten met de juiste VLAN-id en 802.1p prioriteit op de IP-telefoon gezet. Dit CDP-TLV wordt ook gebruikt om te bepalen of een IP-telefoon is aangesloten via de apparaat-ID-parameter.

Dit concept kan worden gebruikt wanneer u een QoS-beleid ontwikkelt. U kunt de Catalyst switch op drie manieren configureren om met de IP-telefoon te communiceren:

- Cisco IP-telefoon met vertrouwenVoorwaardelijk vertrouwen CoS slechts wanneer een IP-telefoon via CDP wordt gedetecteerd. Wanneer een IP-telefoon via CDP Parameter-14 wordt gedetecteerd, wordt de port trust state ingesteld op Trust COS. Als er geen IP-telefoon wordt gedetecteerd, is de poort onbetrouwbaar.
- Uitgebreid vertrouwenDe switch kan de IP-telefoon via CDP (Parameter-18) informeren om alle frames te vertrouwen die ontvangen worden op zijn externe 10/100 Mbps apparaatpoort.
- COS herschrijven voor onvertrouwde poortenDe switch kan de IP-telefoon via CDP (Parameter-19) informeren om de 802.1p CoS-waarden te herschrijven die worden ontvangen op zijn externe 10/100 Mbps apparaatpoort.**Opmerking:** Standaard is al het verkeer dat op de IP-telefoon externe 10/100 Mbps poorten ontvangt, onbetrouwbaar.

Opmerking: Dit is een voorbeeldconfiguratie voor het aansluiten van de niet-Cisco IP-telefoon op een switch.

Opmerking: Bijvoorbeeld:

```
Switch(config)#interface gigabitEthernet 2/1
Switch(config-if)#switchport mode trunk

!--- For example use VLAN 30 for voice VLAN, and VLAN 10 for access VLAN. Switch(config-
if)#switchport trunk native vlan 10
Switch(config-if)#switchport trunk allow vlan 10,30
Switch(config-if)#switchport voice vlan 30
Switch(config-if)#spanning-tree portfast trunk
```

```
!--- And besides that enable LLDP as Non Cisco IP Phone do not use CDP. Switch(config)#lldp run
```

Cisco-configuratie-aanbeveling

De informatie die CDP verstrekt kan zeer nuttig zijn wanneer u Layer 2 connectiviteit kwesties problematisch oplossen. Schakel CDP in op alle apparaten die de werking ervan ondersteunen. Geef deze opdrachten uit:

- Zo schakelt u CDP wereldwijd in op de switch:
  ```
  Switch(config)#cdp run
  ```
- Om CDP per poort mogelijk te maken:
  ```
  Switch(config)#interface type slot#/port#
  Switch(config-if)#cdp enable
  ```

Configuratiecontrolelijst

Mondiale opdrachten

Meld u aan, schakelt u de mondiale configuratiemodus in en voert u deze in om het installatieproces van de switch te starten.

```
Switch>enable
Switch#
Switch#configure terminal
Switch(Config)#
```

Generic Global Commands (Enterprise-Wide)

Deze sectie Global Commands maakt een lijst van de globale opdrachten die op alle switches in het netwerk van de klantonderneming van toepassing moeten zijn.

Deze configuratie bevat de aanbevolen globale opdrachten om aan de eerste configuratie toe te voegen. U moet de waarden in de uitvoer wijzigen voordat u de tekst naar de CLI kopieert en kleeft. Geef deze opdrachten uit om de mondiale configuratie toe te passen:

```
vtp domain domain_name
vtp mode transparent
spanning-tree portfast bpduguard
spanning-tree etherchannel guard misconfig
cdp run
no service pad
service password-encryption
enable secret password
clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ip subnet-zero
ip host tftpserver your_tftp_server
ip domain-name domain_name
ip name-server name_server_ip_address
```

```
ip name-server name_server_ip_address
ip classless
no ip domain-lookup
no ip http server
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging syslog_server_ip_address
logging syslog_server_ip_address
logging source-interface loopback0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
access-list 98 permit host_ip_address_of_primary_snmp_server
access-list 98 permit host_ip_address_of_secondary_snmp_server
snmp-server community public ro 98
snmp-server community laneng rw 98
snmp-server enable traps entity
snmp-server host host_address traps public
snmp-server host host_address traps public
banner motd ^CCCCC

This is a proprietary system, NOT for public or personal use.  All work products,
communications, files, data or information directly or indirectly created, input
or accessed on this system are and shall become the sole property of the company.
This system is actively monitored and accessed by the company.  By logging onto
this system, the user consents to such monitoring and access.

USE OF THIS SYSTEM WITHOUT OR IN EXCESS OF THE PROPER AUTHORIZATION MAY SUBJECT
THE USER TO DISCIPLINE AND/OR CIVIL AND CRIMINAL PENALTIES

^C
line console 0
exec-timeout 0 0
password cisco
login
transport input none
line vty 0 4
exec-timeout 0 0
password cisco
login
length 25
clock calendar-valid
ntp server ntp_server_ip_address
ntp server ntp_server_ip_address
ntp update-calendar
```

Mondiale opdrachten die specifiek zijn voor elk Switch-chassis

De globale opdrachten in dit gedeelte zijn specifiek voor elk switch chassis dat in het netwerk is geïnstalleerd.

Chassis-specifieke configuratievormen

Geef deze opdracht op om de datum en de tijd in te stellen:

```
Switch#clock set hh:mm:ss day month year
```

Om de naam van de apparaathost in te stellen, geeft u deze opdrachten uit:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Cat6500
```

Om loopback interface voor beheer te configureren geeft u deze opdrachten uit:

```
CbrCat6500(config)#interface loopback 0
Cat6500(config-if)#description Cat6000 - Loopback address and Router ID
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#exit
```

Om de Cisco IOS-softwareherziening van Supervisor Engine te tonen geeft u deze opdrachten uit:

```
Cbrcat6500#show version | include IOS
IOS (tm) MSFC Software (C6MSFC-DSV-M), Version 12.1(13)E9, EARLY DEPLOYMENT RELE
ASE SOFTWARE (fc1)
cat6500#
```

Geef deze opdracht op om de MSFC-revisie van een bestand te tonen:

```
Cat6500#dir bootflash:
Directory of bootflash:/
 1 -rw- 1879040 Aug 19 2003 19:03:29 c6msfc-boot-mz.121-19.E1a

15990784 bytes total (14111616 bytes free
```

Om de informatie en de plaats van het servercontact van SNMP te specificeren, geeft u deze opdrachten uit:

```
Cat6500(config)#snmp-server contact contact_information
Cat6500(config)#snmp-server location location_of_device
```

Om de opstartconfiguratie van een bestaande Supervisor Engine naar een nieuwe Supervisor Engine te kopiëren, kan er sprake zijn van verlies van configuratie, bijvoorbeeld, de configuratie op de interfaces van de bestaande supervisor. Cisco raadt aan de configuratie naar een tekstbestand te kopiëren en het in segmenten in de console te plakken om te zien of er configuratieproblemen zijn die voorkomen.

Interfaceopdrachten

Cisco functionele poorttypen

Switch poorten in Cisco IOS-software worden aangeduid als interfaces. Er zijn twee typen interfacemodi in Cisco IOS-software:

- Layer 3 routeinterface
- Layer 2 switch-interface

De interfacefunctie verwijst naar hoe u de poort hebt ingesteld. De poortconfiguratie kan zijn:

- Routed interface
- Switched virtuele interface (SVI)
- Access poort
- Trunk
- EtherChannel
- Een combinatie hiervan

Het interfacetype verwijst naar een poorttype. Het poorttype kan één van de volgende zijn:

- FE
- GE
- Poortkanaal

In deze lijst worden verschillende Cisco IOS-softwarefuncties kort beschreven:

- Routed Physical Interface (standaard) - Elke interface op de switch is een routed Layer 3 interface, die standaard gelijk is aan een Cisco-router. De routeinterface moet op een uniek IP-subtype vallen.
- Access switch poort-deze functie wordt gebruikt om interfaces in hetzelfde VLAN te plaatsen. De poorten moeten van een routeinterface naar een geschakelde interface worden geconverteerd.
- SVI-Een SVI kan met een VLAN worden geassocieerd dat de havens van de switch van de toegang voor de routing tussen VLAN bevat. Configureer de SVI met een VLAN dat wordt geassocieerd wanneer u een route of brug tussen de poorten van de switch van de toegang op verschillende VLAN's wilt hebben.
- Trunk switch poort interface-Deze functie wordt gebruikt om meerdere VLAN's naar een ander apparaat te dragen. De poorten moeten van een routeinterface worden geconverteerd naar een poort op de switch van de romp.
- EtherChannel-An EtherChannel wordt gebruikt om individuele poorten te bundelen in één logische poort voor redundantie en taakverdeling.

Aanbevelingen voor Cisco functioneel poorttype

Gebruik de informatie in deze sectie om te helpen de parameters te bepalen die op de interfaces van toepassing zijn.

N.B.: Sommige interface-specifieke opdrachten zijn waar mogelijk opgenomen.

Automatische onderhandeling

Gebruik geen autonome onderhandeling in een van deze situaties:

- Voor poorten die netwerkinfrastructurele apparaten zoals switches en routers ondersteunen
- Voor andere niet-transitieve eindsystemen zoals servers en printers

Configureer handmatig voor snelheid en duplex van deze 10/100 Mbps verbindingsconfiguraties. De configuraties zijn meestal 100-Mbps volledig-duplex:

- 100 MB link switch-naar-switch
- 100 MB link switch-naar-server
- 100 MB link switch-naar-router

U kunt deze instellingen als volgt configureren:

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed 100
Cat6500(config-if)#duplex full
```

Cisco raadt 10/100 Mbps linkconfiguraties aan voor eindgebruikers. Mobiele arbeiders en tijdelijke hosts hebben autonomie nodig, zoals dit voorbeeld laat zien:

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed auto
```

De standaardwaarde op Gigabit-interfaces is `automatische onderhandeling`. Maar geef deze opdrachten uit om er zeker van te zijn dat de autonomie is ingeschakeld. Cisco raadt aan om Gigabit-onderhandeling in te schakelen:

```
Cat6500(config-if)#interface gigabitethernet mod#/port#
Cat6500(config-if)#no speed
```

Spanning Tree Root

Met inachtneming van het ontwerp van het netwerk, identificeer de switch die het best geschikt is om de wortel voor elk VLAN te zijn. Kies in het algemeen een krachtige switch in het midden van het netwerk. Plaats de root-brug in het midden van het netwerk en sluit de root-brug rechtstreeks aan op de servers en routers. Deze instelling beperkt over het algemeen de gemiddelde afstand tussen de clients en de servers en routers. Raadpleeg Spanning Tree Protocol-problemen en verwante ontwerpoverwegingen voor meer informatie.

Om een switch te dwingen om de wortel voor een aangewezen VLAN te zijn, geef deze opdracht uit:

```
Cat6500(config)#spanning-tree vlan vlan_id root primary
```

Spanning Tree PortFast

PortFast passeert normaal overspant boomwerking op toegangsporten om de aanvankelijke connectiviteitsvertragingen te versnellen die wanneer eindstations met een switch worden verbonden. Raadpleeg PortFast en andere opdrachten om de Connectiviteit van het werkstation te verbeteren voor meer informatie over PortFast.

Stel STP PortFast in op On voor alle enabled access poorten die met één host zijn verbonden. Dit is een voorbeeld:

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
```

```
 Use with CAUTION
%Portfast has been configured on FastEthernet3/1 but will only have effect
when the interface is in a non-trunking mode.
```

UDLD

Schakel UDLD alleen in op met glasvezel verbonden infrastructuurpoorten of koperen Ethernet-kabels om de fysieke configuratie van de kabels te controleren. Geef deze opdrachten uit om UDLD in staat te stellen:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#udld enable
```

VLAN-configuratieinformatie

Configureer VLAN's met deze opdrachten:

```
Cat6500(config)#vlan vlan_number
Cat6500(config-vlan)#name vlan_name
Cat6500(config-vlan)#exit
Cat6500(config)#spanning-tree vlan vlan_id
Cat6500(config)#default spanning-tree vlan vlan_id
```

Herhaal de opdrachten voor elk VLAN en vervang de instructies. Deze opdracht geven:

```
Cat6500(config)#exit
```

Geef deze opdracht uit om alle VLAN's te controleren:

```
Cat6500#show vlan
```

Routed SVI's

Configureer de SVI's voor routing tussen VLAN's. Geef deze opdrachten uit:

```
Cat6500(config)#interface vlan vlan_id
Cat6500(config-if)#ip address svi_ip_address subnet_mask
Cat6500(config-if)#description interface_description
Cat6500(config-if)#no shutdown
```

Herhaal deze opdrachten voor elke interfacefunctie die een routed SVI bevat, en sluit vervolgens af. Deze opdracht geven:

```
Cat6500(config-if)#^Z
```

Routed single-fysieke interface

Geef deze opdrachten uit om de standaard routed Layer 3-interface te configureren:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#description interface_description
```

Herhaal deze opdrachten voor elke interfacefunctie die een routed Physical Interface bevat en dan afsluiten. Deze opdracht geven:

```
Cat6500(config-if)#^Z
```

Routed EtherChannel (L3)

Om EtherChannel op Layer 3 interfaces te configureren geeft u de opdrachten in deze sectie uit.

Configuratie van een logische haven-kanaal interface op deze manier:

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#description port_channel_description
Cat6500(config-if)#ip address port_channel_ip_address subnet_mask
Cat6500(config-if)#no shutdown
```

Voer de stappen in deze sectie uit voor de poorten die dat specifieke kanaal vormen. Pas de resterende informatie op het havenkanaal toe, zoals dit voorbeeld aantoont:

```
Cat6500(config)#interface range [type] mod/port_range
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#^Z
```

Opmerking: Nadat u EtherChannel hebt configureren heeft de configuratie die u toepast op de interface van het poortkanaal gevolgen voor EtherChannel. De configuratie die u op de LAN poorten toepast, heeft alleen gevolgen voor de LAN poort waar u de configuratie toepast.

EtherChannel (L2) met trunking

Configuratie van Layer 2 EtherChannel voor trunking op deze manier:

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport encapsulation encapsulation_type
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Voer de stappen in deze sectie alleen uit voor de poorten die dat specifieke kanaal vormen.

```
Cat6500(config)#interface range [type] mod/port_range
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Opmerking: Nadat u EtherChannel hebt configureren heeft de configuratie die u toepast op de interface van het poortkanaal gevolgen voor EtherChannel. De configuratie die u op de LAN poorten toepast, heeft alleen gevolgen voor de LAN poort waar u de configuratie toepast.

Controleer de aanmaak van alle EtherChannel en trunks. Dit is een voorbeeld:

```
Cat6500#show etherchannel summary
Cat6500#show interface trunk
```

Access-poorten

Als de interfacefunctie een toegangspoort is die als één interface is geconfigureerd, geeft u deze opdrachten uit:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport mode access
Cat6500(config-if)#switchport access vlan vlan_id
Cat6500(config-if)#exit
```

Herhaal deze opdrachten voor elke interface die moet worden geconfigureerd als een Layer 2-switch poort.

Als de switch poort op eindstations moet worden aangesloten, geeft u deze opdracht uit:

```
Cat6500(config-if)#spanning-tree portfast
```

Trunk-poort (één fysieke interface)

Als de interfacefunctie een boompoort is die als één interface wordt gevormd, geef deze opdrachten uit:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport trunk encapsulation dot1q
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Herhaal deze opdrachten voor elke interfacefunctie die moet worden geconfigureerd als een proefpoort.

Wachtwoordinformatie

geeft deze opdrachten uit voor wachtwoordinformatie:

```
Cat6500(config)#service password-encryption
Cat6500(config)#enable secret password
```

```
CbrCat6500(config)#line con 0
Cat6500(config-line)#password password

CbrCat6500(config-line)#line vty 0 4
Cat6500(config-line)#password password
Cat6500(config-line)#^Z
```

De configuratie opslaan

Geef deze opdracht uit om de configuratie op te slaan:

```
Cat6500#copy running-config startup-config
```

Nieuwe softwarefuncties in Cisco IOS-softwarerelease 12.1(13)E

Raadpleeg de Ondersteuning van Cisco IP-telefoon voor meer informatie over IP-telefonie.

Raadpleeg Network-Based Application Recognition en Distributed Network-Based Application Recognition voor meer informatie over Network-Based Application Recognition (NBAR) voor LAN-poorten.

Opmerkingen:

- NBAR voor LAN poorten wordt ondersteund in software op de MSFC2.
- PFC2 biedt hardwareondersteuning voor ingangsACL's op LAN-poorten waar u NBAR vormt.
- Wanneer PFC QoS is geactiveerd, het verkeer door LAN poorten waar u NBAR vormt passeert door de ingangen en stress wachtrijen en daalt drempels.
- Wanneer PFC QoS is ingeschakeld, stelt de MSFC2 een hogere serviceklasse (CoS) gelijk aan IP-voorrang.
- Na het verkeer door een toegangswachtrij wordt al het verkeer in de software verwerkt op de MSFC2-poorten waar u NBAR vormt.
- Gedistribueerde NBAR is beschikbaar op FlexWAN-interfaces met Cisco IOS-softwarerelease 12.1(6)E en hoger.

Verbeteringen in NetFlow Data Export (NDE) omvatten:

- Bestemmingsbron-interface- en full-interface stroommaskers
- NDE versie 5 van PFC2
- Steekproef NetFlow
- Een optie om deze extra velden in NDE-records te vullen:IP-adres van de volgende hoprouterInvoerinterface voor SNMP als IndexIP-interface voor SNMP als IndexBron-autonoom systeemnummer

Raadpleeg NDE configureren voor meer informatie over deze verbeteringen.

Andere functieverbeteringen zijn:

- UDLD configureren
- VTP configureren
- Web cacheservices configureren met WCCP

Deze opdrachten zijn nieuwe opdrachten:

- **standby-vertraging minimum herladen**
- **koppelen deblokkeren**
- **vlan intern toewijzingsbeleid (oplopende begroting) | dalend**
- **systeemjumbomtu**
- **heldere Catalyst 6000 verkeersmeter**

Deze opdrachten zijn verbeterd:

- **toon VLAN intern gebruik**-deze opdracht werd uitgebreid om VLAN**'s** te omvatten die de interfaces van WAN gebruiken.
- **toon VLAN id**-Dit bevel werd uitgebreid om de ingang van een reeks VLANs te steunen.
- **toon l2protocol-tunnel**-Deze opdracht werd uitgebreid om de ingang van een VLAN ID te steunen.

Cisco IOS-softwarerelease 12.1(13)E ondersteunt deze softwarefuncties, die eerder werden ondersteund in Cisco IOS-softwarerelease 12.1 EX releases:

- Configuratie van Layer 2 EtherChannel die interfaces op verschillende DFC-uitgeruste switchmodules omvattenRaadpleeg het gedeelte Opgeloste algemene beperkingen in release 12.1(13)E van Cisco bug ID CSCdt27074 (alleen geregistreerde klanten).
- Redundantie van routeprocessor plus (RPR+)Raadpleeg RPR of RPR+ Supervisor Engine redundantie.**Opmerking:** in Cisco IOS-softwarerelease 12.1(13)E en later vervangen de RPR- en RPR+ redundantie-functies de verbeterde redundantie met hoge systeembeschikbaarheid (EHSA).
- 4.096 Layer 2 VLAN's Raadpleeg VLAN's configureren.**Opmerking:** Cisco IOS-softwarerelease 12.1(13)E en latere releases-ondersteuningsconfiguratie van 4.096 Layer 3 VLAN-interfaces. Configureer een gecombineerd totaal van niet meer dan 2.000 Layer 3 VLAN-interfaces en Layer 3-poorten op een MSFC2 met ofwel een Supervisor Engine II of een Supervisor Engine I. Configureer een gecombineerd totaal van niet meer dan 1.000 Layer 3 VLAN-interfaces en Layer 3 poorten op een MSFC.
- IEEE 802.1Q-tunnelingRaadpleeg het gedeelte IEEE 802.1Q-tunneling en Layer 2-tunneling configureren.
- IEEE 802.1Q-protocoltunnelingRaadpleeg het gedeelte IEEE 802.1Q-tunneling en Layer 2-tunneling configureren.
- IEEE 802.1s meerdere Spanning Tree (MST)Raadpleeg STP- en IEEE 802.1s MST configureren.
- IEEE 802.1w snelle STP (RSTP)Raadpleeg STP- en IEEE 802.1s MST configureren.
- IEEE 802.3ad LACPRaadpleeg Layer 3 en Layer 2 EtherChannel configureren.
- PortFast BPDU-filteringRaadpleeg de functies STP configureren.
- Automatische creatie van Layer 3 VLAN-interfaces ter ondersteuning van VLAN ACL's (VACL's)Raadpleeg Netwerkbeveiliging configureren.
- VACL-opnamepoorten (Layer 2 Ethernet-poort) in elk VLANRaadpleeg Netwerkbeveiliging configureren.
- Configureerbare MTU-grootte op individuele fysieke Layer 3-poortenRaadpleeg het Overzicht van de interfaceconfiguratie.
- Configuratie van SPAN-poorten als stammen, zodat al het SPAN-verkeer van een label is voorzienZie Local en Remote SPAN configureren.

Gerelateerde informatie

- Tools en bronnen - Cisco-systemen
- Productondersteuning voor switches
- Ondersteuning voor LAN-switching technologie
- Technische ondersteuning en documentatie – Cisco Systems